aws

ユーザーガイド

Amazon Simple Storage Service

API バージョン 2006-03-01

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon Simple Storage Service: ユーザーガイド

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon の商標とトレードドレスは、Amazon 以外の製品またはサービスとの関連において、顧客に混乱を招いたり、Amazon の名誉または信用を毀損するような方法で使用することはできません。Amazon が所有しない商標はすべてそれぞれの所有者に所属します。所有者は必ずしも Amazon との提携や関連があるわけではありません。また、Amazon 支援を受けているとはかぎりません。

Table of Contents

Amazon S3 とは 1
Amazon S3 の機能 1
ストレージクラス 1
ストレージ管理 2
アクセス管理とセキュリティ 3
データ処理 4
ストレージのログ記録とモニタリング 4
分析とインサイト 5
強力な整合性 5
Amazon S3 の仕組み 6
バケット 6
オブジェクト 9
キー 9
S3 バージョニング 10
バージョン ID 10
バケットポリシー 10
S3 アクセスポイント 11
アクセスコントロールリスト (ACL) 11
リージョン 12
Amazon S3 のデータ整合性モデル 12
アプリケーションの同時実行 14
関連サービス 15
Amazon S3 へのアクセス 16
AWS Management Console 16
AWS Command Line Interface 16
AWS SDK 16
Amazon S3 REST API 17
Amazon S3 の支払い 17
PCI DSS コンプライアンス 18
入門 19
設定 19
AWS アカウントへのサインアップ 20
管理アクセスを持つユーザーを作成する 20
ステップ 1: バケットを作成する 22

ステップ 2: オブジェクトをアップロードする 29
ステップ 3: オブジェクトをダウンロードする 29
S3 コンソールの使用 30
ステップ 4: オブジェクトをコピーする 31
ステップ 5: オブジェクトとバケットを削除する 32
オブジェクトの削除 33
バケットを空にする 33
バケットの削除 34
次のステップ 34
一般的なユースケースを理解する 35
バケットとオブジェクトへのアクセスをコントロール 36
ストレージの保護とモニタリング 37
Amazon S3 を使用した開発 37
チュートリアルから学ぶ 39
トレーニングとサポートを見る 40
汎用バケットの使用 41
汎用バケットの概要 42
汎用バケットの概要 43
一般的な汎用バケットパターン 44
アクセス許可 44
汎用バケットのパブリックアクセスの管理 45
汎用バケットの設定 46
汎用バケットのオペレーション 49
汎用バケットのパフォーマンスモニタリング 49
一般的なバケットパターン 51
マルチテナント汎用バケットパターン 51
使用ごとのバケットパターン 52
名前付けルール 53
汎用バケットの命名規則 53
汎用バケット名の例 55
ベストプラクティス 56
バケット名で GUID を使用するバケットの作成 57
クォータ、制約、制限 58
バケットクォータ 58
オブジェクトとバケットの制限 59
バケットの名前付け 59

バケットへのアクセス 59
..... 59
汎用バケットの仮想ホスティング 63
汎用バケットの作成 72
汎用バケットの設定 73
バケットのプロパティの表示 87
バケットの一覧表示 90
汎用バケットを空にする 96
AWS CloudTrail が設定された汎用バケットを空にする 99
汎用バケットの削除 99
Mountpoint for Amazon S3 105
Mountpoint のインストール 106
Mountpoint の設定と使用 111
Mountpoint のトラブルシューティング 117
Storage Browser for Amazon S3 118
Storage Browser for S3 の使用 119
Storage Browser for S3 のインストール 120
Storage Browser for S3 の設定 121
Storage Browser for S3 の設定 135
Storage Browser for S3 のトラブルシューティング 136
Transfer Acceleration の設定 137
なぜ Transfer acceleration を使用するのですか? 137
Transfer Acceleration を使用するための要件 137
入門 139
Transfer Acceleration を有効にする 141
速度比較ツール 148
リクエスタ支払いの使用 149
リクエスタ支払いの課金の仕組み 151
リクエスタ支払の設定 151
requestPayment 設定の取得 153
リクエスタ支払いバケットからのオブジェクトのダウンロード 154
オブジェクトの使用 156
オブジェクトの概要 157
サブリソース 158
オブジェクトに命名する 159
オブジェクトキー名の選択 160

オブジェクトキーの命名のガイドライン 161
メタデータの使用 164
システムで定義されたオブジェクトメタデータ 165
ユーザー定義のオブジェクトメタデータ 169
オブジェクトのメタデータの編集 171
データ検出の高速化 175
オブジェクトのアップロード 214
オブジェクトのアップロード 216
同じキー名を持つオブジェクトのアップロードを禁止する 229
マルチパートアップロードの使用 229
条件付きリクエストの実行 307
メタデータに基づいてオブジェクトを取得またはコピーする方法 307
オブジェクトの上書きを防ぐ方法 310
オブジェクトのコピー、移動、名前の変更 321
オブジェクトをコピーするには 324
オブジェクトを移動するには 334
オブジェクトの名前を変更するには 336
オブジェクトのダウンロード 337
オブジェクトのダウンロード 338
複数のオブジェクトのダウンロード 340
オブジェクトの一部のダウンロード 342
別の AWS アカウントに属するオブジェクトのダウンロード 343
アーカイブされたオブジェクトのダウンロード 344
メタデータに基づくオブジェクトのダウンロード 344
オブジェクトのダウンロードに関するトラブルシューティング 344
Amazon S3 でのオブジェクトの整合性のチェック 345
サポートされているチェックサムアルゴリズムの使用 345
フルオブジェクトおよび複合チェックサムタイプ 347
マルチパートアップロードへのフルオブジェクトチェックサムの使用 349
マルチパートアップロードへのパートレベルのチェックサムの使用 350
チェックサムオペレーション 351
オブジェクトをアップロードするときに Content-MD5 を使用する 359
Content-MD5 と ETag を使用して、アップロードされたオブジェクトを検証する 360
追跡チェックサムの使用 361
オブジェクトの削除 366
オブジェクトを削除する前に考慮すべきベストプラクティス 367

バージョニングが有効なバケットからのオブジェクトの削除 ... 368
バージョニングが停止されたバケットからのオブジェクトの削除 ... 369
バージョン管理されていないバケットからのオブジェクトの削除 ... 369
MFA 対応のバケットからのオブジェクトの削除 ... 369
単一のオブジェクトの削除 ... 370
複数のオブジェクトの削除 ... 381
オブジェクトの整理とリスト化 ... 384
プレフィックスの使用 ... 385
オブジェクトのリスト化 ... 387
フォルダの使用 ... 390
オブジェクトのプロパティの表示 ... 395
タグを使用してオブジェクトを分類する ... 397
署名付き URL を使用してオブジェクトをダウンロードおよびアップロードする ... 411
署名付き URL を作成できるユーザー ... 412
署名付き URL の有効期限 ... 412
署名付き URL 機能の制限 ... 413
署名付き URL を使用したオブジェクトの共有 ... 415
署名付き URL を使用したオブジェクトのアップロード ... 418
オブジェクトの変換 ... 422
Object Lambda アクセスポイントの作成 ... 423
Amazon S3 Object Lambda アクセスポイントの使用 ... 439
セキュリティに関する考慮事項 ... 443
Lambda 関数の記述 ... 450
AWS で構築された関数の使用 ... 482
S3 Object Lambda のベストプラクティスとガイドライン ... 484
S3 Object Lambda のチュートリアル ... 485
S3 Object Lambda のトラブルシューティング ... 523
オブジェクトオペレーションを一括で実行する ... 524
バッチ操作の基本 ... 524
S3 バッチ操作のチュートリアル ... 526
アクセス許可の付与 ... 527
ジョブの作成 ... 537
サポートされているオペレーション ... 561
ジョブの管理 ... 605
ジョブステータスと完了レポートの追跡 ... 610
タグの使用 ... 625

バッチオペレーションを使用した Object Lock の管理 ... 640
チュートリアル: 動画のバッチトランスコーディング ... 665
バッチオペレーションのトラブルシューティング ... 706
所定のデータのクエリ ... 709
要件と制限 ... 710
リクエストの構築 ... 711
エラー ... 712
S3 Select の例 ... 712
SQL リファレンス ... 716
ディレクトリバケットの使用 ... 756
ディレクトリバケット名 ... 757
ディレクトリ ... 757
キー名 ... 757
アクセス管理 ... 758
ディレクトリバケットのクォータ ... 758
ディレクトリバケットの作成と使用 ... 759
ディレクトリバケットのユースケース ... 759
高性能ワークロード ... 760
データレジデンシーワークロード ... 818
ディレクトリバケットの違い ... 835
ディレクトリバケットの違い ... 836
ディレクトリバケットでサポートされている API オペレーション ... 838
ディレクトリバケットでサポートされていない Amazon S3 の機能 ... 839
ディレクトリバケットのネットワーク ... 840
エンドポイント ... 841
VPC ゲートウェイエンドポイントの設定 ... 841
ディレクトリバケットの命名規則 ... 842
プロパティの表示 ... 843
バケットポリシーの管理 ... 844
バケットポリシーの追加 ... 844
バケットポリシーの表示 ... 847
バケットポリシーを削除する ... 848
ディレクトリバケットを空にする ... 849
ディレクトリバケットの削除 ... 850
ディレクトリバケットの一覧表示 ... 852
バケットにアクセスできるかどうかの判断 ... 855

ディレクトリバケットでのオブジェクトの使用 857
ディレクトリバケットへのオブジェクトのインポート 857
S3 ライフサイクルの使用 859
S3 Express One Zone でのバッチオペレーションの使用 872
オブジェクトへのデータの追加 876
オブジェクトのアップロード 878
オブジェクトのコピー 911
オブジェクトの削除 918
オブジェクトのダウンロード 922
オブジェクトを共有するための署名付き URL の生成 924
オブジェクトメタデータの取得 924
オブジェクトのリスト化 926
ディレクトリバケットのセキュリティ 926
データ保護と暗号化 927
リクエストの認証と承認 950
セキュリティに関するベストプラクティス 985
ディレクトリバケットのアクセスポイントの使用 989
命名規則、制限、制限 990
ディレクトリバケットのアクセスポイントの参照 992
アクセスポイントオブジェクトオペレーション 992
IAM ポリシーの設定 993
モニタリングとログ記録 999
ディレクトリバケットのアクセスポイントの作成 1000
アクセスポイントの管理 1005
ディレクトリバケットの AWS CloudTrail を使用したログ記録 1017
ディレクトリバケットの CloudTrail 管理イベント 1018
ダイレクトバケットの CloudTrail データイベント 1019
..... 1020
ディレクトリバケットのパフォーマンスの最適化 1027
セッションベースの認証を使用する 1027
S3 の追加のチェックサムのベストプラクティス 1027
最新バージョンの AWS SDK と一般的なランタイムライブラリを使用する 1028
ディレクトリバケットを使用した開発 1028
ディレクトリバケットのリージョンエンドポイントとゾーンエンドポイント 1028
S3 コンソール、AWS CLI、AWS SDK を使用したディレクトリバケットの操作 1029
ディレクトリバケット API オペレーション 1031

Amazon S3 Tables とテーブルバケットの使用 1034
S3 Tables の機能 1034
関連サービス 1036
チュートリアル: S3 Tables の開始方法 1037
ステップ 1: テーブルバケットを作成し、AWS 分析サービスと統合する 1037
ステップ 2: テーブル名前空間とテーブルを作成する 1039
(オプション) ステップ 3: テーブルに対する Lake Formation 許可を付与する 1041
ステップ 4: Athena で SQL を使用してデータをクエリする 1043
テーブルバケット 1044
テーブルバケットの命名規則 1045
テーブルバケットを作成する 1047
テーブルバケットを削除する 1050
テーブルバケットの詳細の表示 1050
ポリシーの管理 1050
S3 Tables のメンテナンス 1052
S3 Tables メンテナンスジョブのステータス 1052
テーブルバケットのメンテナンス 1053
テーブルのメンテナンス 1055
考慮事項と制限事項 1058
名前空間 1061
名前空間を作成します。 1061
名前空間を削除する 1063
テーブル 1064
テーブルの作成 1065
テーブルの削除 1071
ポリシーの管理 1072
テーブルへのアクセス 1073
Amazon SageMaker Lakehouse 統合を通じたテーブルへのアクセス 1074
テーブルへの直接アクセス 1075
AWS 分析サービスで S3 Tables を使用する 1076
AWS Glue Iceberg REST エンドポイントを使用したテーブルへのアクセス 1089
Amazon S3 Tables Iceberg REST エンドポイントを使用したテーブルへのアクセス 1094
クライアントカタログを使用したテーブルへのアクセス 1100
Amazon Athena 1103
Amazon Redshift 1105
Amazon EMR 1105

QuickSight ... 1109
Amazon Data Firehose ... 1112
AWS Glue ETL ... 1117
AWS リージョン、エンドポイント、およびクォータ ... 1128
S3 Tables AWS リージョンとエンドポイント ... 1129
S3 Tables のクォータ ... 1133
S3 Tables のセキュリティ ... 1134
Encryption ... 1135
アクセス管理 ... 1149
VPC 接続 ... 1175
制約と制限 ... 1179
S3 Tablesの AWS CloudTrail を使用したログ記録 ... 1179
S3 Tables の CloudTrail 管理イベント ... 1180
S3 Tables の CloudTrail データイベント ... 1181
CloudTrail ログの例 ... 1182
アクセスコントロール ... 1186
S3 リソース ... 1187
ID ... 1192
バケットまたはリソース所有者 ... 1194
アクセス管理ツール ... 1195
アクション ... 1201
アクセス管理のユースケース ... 1202
アクセス管理のトラブルシューティング ... 1209
Identity and Access Management (IAM) ... 1211
対象者 ... 1212
アイデンティティによる認証 ... 1212
ポリシーを使用したアクセス権の管理 ... 1216
Amazon S3 での IAM の機能 ... 1219
承認を要求する ... 1246
S3 API オペレーションに必要なアクセス許可 ... 1256
ポリシーとアクセス許可 ... 1295
バケットポリシー ... 1299
アイデンティティベースのポリシー ... 1347
チュートリアル: ポリシーの使用 ... 1384
Amazon S3 ストレージレンズでのサービスにリンクされたロールの使用 ... 1426
Amazon S3 アイデンティティとアクセスのトラブルシューティング ... 1430

AWS マネージドポリシー 1455
汎用バケットのアクセスポイントの使用 1457
命名規則、制限、制限 1459
アクセスポイントの参照 1461
アクセスポイントの互換性 1465
IAM ポリシーの設定 1466
モニタリングとログ記録 1474
汎用バケットのアクセスポイントの作成 1476
アクセスポイントの管理 1483
アクセスポイントの使用 1487
S3 Access Grants でのアクセス管理 1500
S3 Access Grants の概念 1502
S3 Access Grants と社内ディレクトリのアイデンティティ 1507
S3 Access Grants の開始方法 1516
S3 Access Grants インスタンスの使用 1518
S3 Access Grants ロケーションの使用 1531
S3 Access Grants での許可の使用 1554
Access Grants を使用した S3 データの取得 1567
S3 Access は、クロスアカウントアクセスを許可します。 1583
S3 Access Grants での AWS タグの使用 1596
S3 Access Grants の制約 1599
S3 Access Grants の統合 1601
ACL によるアクセス管理 1602
ACL の概要 1604
ACL の設定 1624
ポリシーの例 1642
パブリックアクセスのブロック 1647
パブリックアクセスブロック設定 1649
アクセスポイントでのパブリックアクセスブロックオペレーションの実行 1652
「パブリック」の意味 1653
IAM Access Analyzer for S3 を使用したパブリックバケットの確認 1656
アクセス許可 1657
パブリックアクセスブロックの設定 1658
アカウント設定の構成 1658
バケットとアクセスポイントの設定 1661
バケットアクセスの確認 1664

IAM Access Analyzer for S3 はどのような情報を提供しますか？ 1666
IAM Access Analyzer for S3 の有効化 1667
すべてのパブリックアクセスのブロック 1667
バケットアクセスの確認と変更 1669
バケットの結果のアーカイブ 1670
アーカイブされたバケットの結果の有効化 1671
結果の詳細の表示 1671
IAM Access Analyzer for S3 レポートのダウンロード 1671
バケット所有者の確認 1672
バケット所有者条件を使用する状況 1673
バケット所有者の確認 1673
例 1674
制約と制限 1677
オブジェクト所有者の管理 1677
オブジェクトの所有権の設定 1679
ACL を無効にして導入された変更 1681
ACL を無効にする前提条件 1683
オブジェクトの所有者許可 1684
すべての新しいバケットの ACL を無効にします。 1684
レプリケーションとオブジェクトの所有権。 1684
オブジェクトの所有権の設定 1684
ACL を無効にする前提条件。 1685
バケットの作成 1701
オブジェクトの所有権の設定 1710
オブジェクトの所有権設定の表示 1714
すべての新しいバケットの ACL を無効にします。 1715
トラブルシューティング 1718
セキュリティ 1721
セキュリティに関するベストプラクティス 1723
Amazon S3 のセキュリティベストプラクティス 1723
Amazon S3 のモニタリングと監査のベストプラクティス 1729
データセキュリティのモニタリング 1733
データ保護 1736
データ暗号化 1737
サーバー側の暗号化 1740
クライアント側の暗号化の使用 1840

インターネットトラフィックのプライバシー 1841
サービスとオンプレミスのクライアントおよびアプリケーションとの間のトラフィック .. 1841
同じリージョン内の AWS リソース間のトラフィック 1842
AWS PrivateLink for Amazon S3 1842
コンプライアンス検証 1860
耐障害性 1862
バックアップの暗号化 1864
インフラストラクチャセキュリティ 1865
設定と脆弱性の分析 1866
アクセス管理 1866
データ保護 1869
リージョン内およびリージョン間でのオブジェクトのレプリケート 1871
レプリケーションを使用する理由 1872
クロスリージョンレプリケーションを使用する場合 1874
同一リージョンレプリケーションを使用する時 1874
双方向レプリケーションを使用する場合 1875
S3 バッチレプリケーションを使用する状況 1875
ワークロードの要件とライブレプリケーション 1876
レプリケーションとは何ですか? 1877
レプリケーションの要件と考慮事項 1881
ライブレプリケーションの設定 1884
ライブレプリケーションの管理または一時停止 1982
既存のオブジェクトのレプリケーション 1984
レプリケーションのトラブルシューティング 1999
進行状況のモニタリングとステータスの取得 2008
マルチリージョントラフィックの管理 2034
マルチリージョンアクセスポイントの作成 2036
マルチリージョンアクセスポイントの設定 2046
マルチリージョンアクセスポイントの使用 2050
オブジェクトの複数のバージョンを保持する 2104
バージョニングが無効なバケット、有効なバケット、停止されているバケット 2104
S3 ライフサイクルでの S3 バージョニングの使用 2105
S3 バージョニング 2106
バケットでのバージョニングの有効化 2110
MFA 削除の設定 2118
バージョニングが有効なオブジェクトの操作 2120

バージョニングが停止されたバケットの操作 2151
バージョニングのトラブルシューティング 2156
オブジェクトのロック 2161
S3 オブジェクトロックの仕組み 2162
オブジェクトロックの考慮事項 2166
オブジェクトロックの設定 2172
データのバックアップ 2183
コスト最適化 2185
請求および使用状況レポート 2186
コスト配分タグの使用 2186
請求レポート 2188
使用状況レポート 2191
請求および使用状況レポートの理解 2194
Amazon S3 のエラーレスポンスに対する請求 2221
ストレージクラスの理解と管理 2244
頻繁にアクセスされるオブジェクト 2245
アクセスパターンが変化する、またはアクセスパターンが不明なデータを自動的に最適化する 2246
アクセス頻度の低いオブジェクト 2248
アクセス頻度の低いオブジェクト 2250
Amazon S3 on Outposts 2251
ストレージクラスを比較する 2251
オブジェクトのストレージクラスを設定 2252
ストレージクラス分析 2257
Amazon S3 Intelligent-Tiering によるストレージコストの管理 2265
Amazon S3 Glacier ストレージクラス 2278
アーカイブされたオブジェクトの操作 2284
ライフサイクルの管理 2297
オブジェクトの完全なライフサイクルの管理 2299
オブジェクトの移行 2300
オブジェクトの有効期限 2308
ライフサイクル設定の指定 2311
他のバケットの設定の使用 2331
S3 ライフサイクルイベント通知の設定 2333
ライフサイクル設定の要素 2336
ライフサイクル設定の競合 2354

S3 ライフサイクル設定の例 2359
ライフサイクル問題のトラブルシューティング 2375
ログ記録とモニタリング 2383
モニタリングツール 2387
自動化ツール 2387
手動ツール 2387
ログ記録オプション 2388
CloudTrail によるログ記録 2391
CloudTrail ログを Amazon S3 サーバーアクセスログと CloudWatch Logs と併用する 2393
Amazon S3 SOAP API コールを使用した CloudTrail トラッキング 2393
CloudTrail のイベント 2395
ログファイルの例 2407
CloudTrail の有効化 2411
S3 リクエストの識別 2414
サーバーアクセスのログ記録 2422
ログ配信を有効にするにはどうすればよいですか? 2422
ログオブジェクトのキーフォーマット 2425
ログを配信する方法 2425
ベストエフォート型のサーバーログ配信 2426
バケットのログ記録ステータスの変更が有効になるまでには時間がかかる 2427
サーバーアクセスログ記録の有効化 2427
ログ形式 2450
ログファイルの削除 2465
S3 リクエストの識別 2466
サーバーのアクセスログ記録のトラブルシューティング 2474
CloudWatch によるメトリクスのモニタリング 2477
メトリクスとディメンション 2479
CloudWatch メトリクスへのアクセス 2498
CloudWatch メトリクスの設定 2500
Amazon S3 イベント通知 2509
概要 2509
通知のタイプおよび送信先 2511
SQS、SNS、および Lambda を使用します 2519
EventBridge の使用 2549
ストレージアクティビティと使用状況の視覚化 2559
S3 ストレージレンズのメトリクスと機能 2560

S3 ストレージレンズについて 2562
メトリクスの用語集 2573
許可の設定 2618
S3 Storage Lens の使用 2623
ストレージメトリクスの表示 2663
Organizations の使用 2723
S3 ストレージレンズグループの使用 2734
データのカタログ化と分析 2778
Amazon S3 インベントリのバケット 2779
インベントリリスト 2780
Amazon S3 インベントリの設定 2786
インベントリの検索 2796
インベントリ完了に関する通知の設定 2800
Athena でインベントリをクエリする 2801
空のバージョン ID 文字列を NULL 文字列に変換します。 2807
オブジェクト ACL フィールドの使用 2810
パフォーマンスの最適化 2813
Amazon S3 のパフォーマンスのガイドライン 2814
パフォーマンスを測定する 2815
水平にスケールする 2816
バイト範囲のフェッチを使用する 2816
リクエストを再試行する 2816
同じリージョンで Amazon S3 と Amazon EC2 を組み合わせる 2817
Transfer Acceleration を使用してレイテンシーを最小限に抑える 2817
最新の AWS SDK を使用する 2817
Amazon S3 のパフォーマンスの設計パターン 2818
頻繁にアクセスされるコンテンツをキャッシュする 2818
レイテンシーの影響を受けやすいアプリケーションのタイムアウトと再試行 2819
水平スケーリングとリクエスト並列化 2820
地理的に分散したデータ転送を高速化する 2821
静的ウェブサイトのホスティング 2823
ウェブサイトエンドポイント 2824
ウェブサイトエンドポイントの例 2826
DNS CNAME の追加 2826
Route 53 でのカスタムドメインの使用 2827
ウェブサイトエンドポイントと REST API エンドポイントの主な違い 2827

ウェブサイトのホスティングの有効化 2828
インデックスドキュメントの設定 2833
インデックスドキュメントとフォルダ 2834
インデックスドキュメントを設定する 2835
カスタムエラードキュメントの設定 2837
Amazon S3 HTTP レスポンスコード 2837
カスタムエラードキュメントの設定 2840
ウェブサイトアクセスのアクセス許可の設定 2841
ステップ 1: S3 のパブリックアクセスのブロック設定を編集する 2842
ステップ 2: バケットポリシーを追加する 2844
オブジェクトアクセスコントロールリスト 2846
ウェブトラフィックのログ記録 2847
リダイレクトの設定 2848
リクエストを別のホストにリダイレクトする 2848
リダイレクトルールの設定 2849
オブジェクトのリクエストをリダイレクトする 2857
CORS の使用 2860
Cross-Origin Resource Sharing: ユースケースのシナリオ 2860
Amazon S3 でのバケットの CORS 設定の評価方法 2861
Object Lambda アクセスポイントで CORS をサポートする方法 2861
CORS 設定のエレメント 2862
CORS の設定 2867
CORS のテスト 2876
CORS のトラブルシューティング 2878
静的ウェブサイトのチュートリアル 2883
動画ストリーミングのホスティング 2885
静的ウェブサイトの設定 2905
カスタムドメインを使用した静的ウェブサイトの設定 2914
Amazon S3 から Amplify への静的ウェブサイトのデプロイ 2941
クォータ 2944
クォータの引き上げ 2944
リファレンス 2945
ドキュメント履歴 2946
以前の更新 2997

Amazon S3 とは

Amazon Simple Storage Service (Amazon S3) は、業界をリードするスケーラビリティ、データ可用性、セキュリティ、およびパフォーマンスを提供するオブジェクトストレージサービスです。あらゆる規模や業界のお客様が、Amazon S3 を使用して、データレイク、ウェブサイト、モバイルアプリケーション、バックアップおよび復元、アーカイブ、エンタープライズアプリケーション、IoT デバイス、ビッグデータ分析など、広範なユースケースのデータを容量にかかわらず、保存して保護することができます。Amazon S3 には、特定のビジネス、組織、コンプライアンスの要件を満たすために、データへのアクセスを最適化、整理、設定できる管理機能があります。

> **Note**
>
> Amazon S3 Express One Zone ストレージクラスをディレクトリバケットで使用する方法の詳細については、「S3 Express One Zone」と「ディレクトリバケットの使用」を参照してください。

トピック

- Amazon S3 の機能
- Amazon S3 の仕組み
- Amazon S3 のデータ整合性モデル
- 関連サービス
- Amazon S3 へのアクセス
- Amazon S3 の支払い
- PCI DSS コンプライアンス

Amazon S3 の機能

ストレージクラス

Amazon S3 では、さまざまなユースケース向けに、幅広いストレージクラスが提供されています。例えば、ミッションクリティカルな本番環境のデータを S3 Standard または S3 Express One Zone に保存して頻繁にアクセスしたり、アクセス頻度の低いデータを S3 標準 – IA または S3 One Zone-

IA に保存してコストを節約したり、S3 Glacier Instant Retrieval、S3 Glacier Flexible Retrieval、S3 Glacier Deep Archive に最も低いコストでデータをアーカイブしたりできます。

Amazon S3 Express One Zone は、最もレイテンシーの影響を受けやすいアプリケーションに 1 桁のミリ秒単位で一貫したデータアクセスを提供することを目的として構築された、高パフォーマンスのシングルアベイラビリティーゾーンの Amazon S3 ストレージ クラスです。S3 Express One Zone は、現在入手可能なレイテンシーが最も低いクラウドオブジェクトストレージクラスで、データアクセス速度は最大 10 倍速く、リクエストコストは S3 スタンダードよりも 50% 低減されます。S3 Express One Zone は、オブジェクトストレージをコンピュートリソースと同じ場所に配置するオプションを備えた単一のアベイラビリティーゾーンを選択できる最初の S3 ストレージクラスです。これにより、最高レベルのアクセス速度を実現できます。アクセス速度をさらに向上させ、1 秒あたり数十万ものリクエストをサポートするために、データは新しいバケットタイプ、つまり Amazon S3 ディレクトリバケットに保存されます。詳細については、「S3 Express One Zone」および「ディレクトリバケットの使用」を参照してください。

S3 Intelligent-Tiering では、変更する、または不明なアクセスパターンを持つデータを保存できます。これにより、アクセスパターンが変更されたときに 4 つのアクセス層間でデータを自動的に移動することで、ストレージコストを最適化できます。4 つのアクセス階層にある、高頻度のアクセスと低頻度のアクセス用に最適化された 2 つの低レイテンシーのアクセス階層と、稀にしかアクセスされないデータ向けに設計された非同期アクセス用の 2 つのオプトインアーカイブアクセス階層があります。

詳細については、「Amazon S3 ストレージクラスの理解と管理」を参照してください。

ストレージ管理

Amazon S3 には、コストの管理、規制要件への対応、レイテンシーの削減、コンプライアンス要件のためのデータの複数の個別コピーの保存で使用できるストレージ管理機能があります。

- S3 ライフサイクル – オブジェクトを管理し、ライフサイクルを通じてコスト効率の高い方法で保存できるようにライフサイクル設定を使用します。オブジェクトを他の S3 ストレージクラスに移行したり、ライフタイムが終了したオブジェクトを期限切れにすることができます。
- S3 オブジェクトロック – Amazon S3 オブジェクトが固定期間または無期限に削除または上書きされるのを防止します。オブジェクトロックを使用して、write-once-read-many (WORM) ストレージを必要とする規制要件を満たしたり、オブジェクトの変更や削除に対する保護レイヤーを追加したりできます。
- S3 レプリケーション – オブジェクトおよびそれぞれのメタデータタグとオブジェクトタグを、同じまたは異なる AWS リージョン にある 1 つまたは複数のレプリケーション先バケットにレプリ

ケートして、レイテンシーの削減、コンプライアンス、セキュリティ、その他のユースケースで活用できます。

- S3 バッチ操作 – 1 つの S3 API リクエストまたは Amazon S3 コンソールで数回クリックするだけで、数十億のオブジェクトを大規模に管理できます。バッチ操作を使用すると、次のようなオペレーションを実行できます。コピー、AWS Lambda 関数の呼び出し、数百万または数十億のオブジェクトの復元。

アクセス管理とセキュリティ

Amazon S3 には、バケットとオブジェクトへのアクセスを監査および管理する機能があります。デフォルトでは、S3 バケットとオブジェクトはプライベートです。作成した S3 リソースにのみアクセスできます。以下の機能を使用して、特定のユースケースをサポートする詳細なリソース許可を付与したり、Amazon S3 リソースの許可を監査したりできます。

- S3 ブロックパブリックアクセス – S3 バケットおよびオブジェクトへのパブリックアクセスをブロックします。デフォルトでは、[パブリックアクセスをブロック] 設定はバケットレベルで有効になっています。ユースケースでオフにする必要のある設定が 1 つ以上あることがわかっている場合を除き、すべての [パブリックアクセスをブロック] 設定を有効にしておくことをお勧めします。詳細については、「S3 バケットへのパブリックアクセスブロック設定の構成」を参照してください。
- AWS Identity and Access Management (IAM) — IAM は、AWS リソース (Amazon S3 リソースなど) へのアクセスを安全に管理するためのウェブサービスです。IAM を使用すると、ユーザーがアクセスできる AWS のリソースを制御するアクセス許可を集中管理できます。IAM を使用して、誰を認証 (サインイン) し、誰にリソースの使用を認可する (アクセス許可を付与する) かを制御します。
- バケットポリシー – IAM ベースのポリシー言語を使用して、S3 バケットとその中のオブジェクトに対するリソースベースの許可を設定します。
- Amazon S3 アクセスポイント — 専用アクセスポリシーを持つ名前付きネットワークエンドポイントを設定して、Amazon S3 の共有データセットへの大規模なデータアクセスを管理します。
- アクセスコントロールリスト (ACL) – 個々のバケットおよびオブジェクトに対する読み取りおよび書き込みの許可を、承認されたユーザーに付与します。原則として、アクセスコントロールには ACL ではなく S3 リソースベースのポリシー (バケットポリシーとアクセスポイントポリシー) または IAM ユーザーポリシーを使用することをお勧めします。ポリシーとは、よりシンプルで柔軟なアクセス制御のオプションです。バケットポリシーとアクセスポイントポリシーを使用すると、Amazon S3 リソースに対するすべてのリクエストに広く適用されるルールを定義できます。

リソースベースのポリシーまたは IAM ユーザーポリシーの代わりに ACL を使用する場合の特定のケースの詳細については、「ACL によるアクセス管理」を参照してください。

- S3 オブジェクト所有権 - バケット内のすべてのオブジェクトの所有権を取得し、Amazon S3 に保存されているデータのアクセス管理を簡素化します。S3 オブジェクト所有権は、Amazon S3 バケットレベルの設定で、ACL を無効または有効にするのに使用できます。デフォルトでは、ACL は無効になっています。ACL を無効にすると、バケット所有者はバケット内のすべてのオブジェクトを所有し、アクセス管理ポリシーのみを使用してデータへのアクセスを管理します。
- IAM Access Analyzer for S3 – S3 バケットアクセスポリシーを評価およびモニタリングし、ポリシーが S3 リソースへの意図したアクセスのみを提供することを確認します。

データ処理

データを変換し、ワークフローをトリガーして、他のさまざまな処理アクティビティを大規模に自動化するには、次の機能を使用できます。

- S3 Object Lambda – S3 GET、HEAD、LIST リクエストに独自のコードを追加して、データがアプリケーションに返されるときにそのデータを変更および処理できます。行のフィルタリング、画像の動的なサイズ変更、機密データの編集などを行います。
- イベント通知 – S3 リソースに変更が加えられると、Amazon Simple Notification Service (Amazon SNS)、Amazon Simple Queue Service (Amazon SQS)、および AWS Lambda を使用するワークフローをトリガーします。

ストレージのログ記録とモニタリング

Amazon S3 には、Amazon S3 リソースの使用状況をモニタリングおよびコントロールするために使用できるロギングおよびモニタリングツールが用意されています。詳細については、「モニタリングツール 」を参照してください。

自動モニタリングツール

- Amazon S3 の Amazon CloudWatch メトリクス – TS3 リソースのオペレーション状態を追跡し、推定請求額がユーザー定義のしきい値に達したときに請求アラートを設定します。
- AWS CloudTrail – ユーザー、ロール、またはAmazon S3 で AWS のサービス によって行われるアクションを記録します。CloudTrail ログを使用すると、S3 バケットレベルおよびオブジェクトレベルのオペレーションの詳細な API 追跡が可能になります。

手動モニタリングツール

- サーバーアクセスログ – バケットに対するリクエストの詳細が記録されます。サーバーアクセスのログ記録を使用して、セキュリティとアクセスの監査、カスタマーベースに関するラーニング、Amazon S3 請求書の把握などの多くのユースケースに対応できます。
- AWSTrusted Advisor – AWS ベストプラクティスチェックを使用してアカウントを評価し、AWS インフラストラクチャを最適化し、セキュリティとパフォーマンスを向上させ、コストを削減し、サービスクォータを監視する方法を特定します。その後、推奨事項に従って、サービスとリソースを最適化できます。

分析とインサイト

Amazon S3 には、ストレージの使用状況を可視化するための機能が用意されています。これにより、ストレージを大規模に理解、分析し、最適化することができます。

- Amazon S3 Storage Lens – ストレージを理解、分析し、最適化します。S3 ストレージレンズは、使用状況およびアクティビティに関する 60 以上のメトリクスとインタラクティブなダッシュボードを提供し、組織全体、特定のアカウント、AWS リージョン、バケット、またはプレフィックスに関するデータを集約します。
- ストレージクラス分析 – ストレージアクセスパターンを分析して、よりコスト効果の高いストレージクラスにデータを移動するタイミングを決定します。
- インベントリ付き S3 インベントリレポート – オブジェクトとそれに対応するメタデータを監査してレポートし、インベントリレポートでアクションを実行するように他の Amazon S3 機能を設定します。例えば、オブジェクトのレプリケーションと暗号化のステータスをレポートできます。インベントリレポートの各オブジェクトで使用できるすべてのメタデータのリストについては、「Amazon S3 インベントリリスト」を参照してください。

強力な整合性

Amazon S3 には、すべての AWS リージョン にある Amazon S3 バケットの、オブジェクトの PUT と DELETE に関する、書き込み後読み取りの強力な整合性があります。この動作は、新しいオブジェクトへの書き込みと、既存のオブジェクトを上書きする PUT、そして DELETE リクエストにも適用されます。さらに、Amazon S3 Select、Amazon S3 アクセスコントロールリスト (ACL)、Amazon S3 オブジェクトタグ、オブジェクトメタデータ (HEAD オブジェクトなど) での読み込みオペレーションには、強力な整合性があります。詳細については、「Amazon S3 のデータ整合性モデル」を参照してください。

Amazon S3 の仕組み

Amazon S3 は、データをオブジェクト、階層データ、または表形式データとしてバケット内に保存するオブジェクトストレージサービスです。オブジェクトとは、ファイルと、そのファイルを記述している任意のメタデータのことです。バケット とは、オブジェクトのコンテナのことです。

Amazon S3 にデータを保存するには、まずバケットを作成し、バケット名および AWS リージョンを指定します。次に、Amazon S3 のオブジェクトとしてそのバケットにデータをアップロードします。各オブジェクトには、キー(またはキー名) があります。これは、バケット内のオブジェクトの一意の識別子です。

S3 には、特定のユースケースをサポートするように設定できる機能があります。例えば、S3 Versioning を使用すると、オブジェクトの複数のバージョンを同じバケットに保持し、誤って削除または上書きされたオブジェクトを復元することができます。

バケットとその中のオブジェクトはプライベートであり、アクセス許可を明示的に付与した場合にのみアクセスできます。バケットポリシー、AWS Identity and Access Management(IAM) ポリシー、アクセスコントロールリスト (ACL)、および S3 アクセスポイントを使用して、アクセスを管理できます。

トピック

- バケット
- オブジェクト
- キー
- S3 バージョニング
- バージョン ID
- バケットポリシー
- S3 アクセスポイント
- アクセスコントロールリスト (ACL)
- リージョン

バケット

Amazon S3 は、汎用バケット、ディレクトリバケット、テーブルバケットという 3 つのバケットタイプをサポートしています。バケットタイプごとに固有の機能セットが、さまざまなユースケース向けに用意されています。

汎用バケット は、ほとんどのユースケースやアクセスパターンに推奨される、オリジナルの S3 バケットタイプです。汎用バケットは、Amazon S3 に保存されているオブジェクトのコンテナであり、バケット内およびすべてのストレージクラス (S3 Express One Zone を除く) に任意の数のオブジェクトを保存できるため、複数のアベイラビリティーゾーンにオブジェクトを冗長的に保存できます。詳細については、「Amazon S3 汎用バケットの作成、設定、操作」を参照してください。

> **Note**
>
> デフォルトでは、すべての汎用バケットはプライベートです。ただし、汎用バケットへのパブリックアクセスは許可できます。汎用バケットへのアクセスは、バケット、プレフィックス (フォルダ)、またはオブジェクトタグの各レベルで制御できます。詳細については、「Amazon S3 でのアクセスコントロール」を参照してください。

ディレクトリバケット – 低レイテンシーのユースケースとデータレジデンシーのユースケースに推奨されます。デフォルトでは、最大 100 個のディレクトリバケットを AWS アカウントに作成できます。ディレクトリバケット内に保存できるオブジェクトの数に制限はありません。ディレクトリバケットは、汎用バケットのフラットなストレージ構造の代わりに、オブジェクトを階層ディレクトリ (プレフィックス) に整理します。このバケットタイプにはプレフィックス制限がなく、個々のディレクトリを水平にスケールできます。詳細については、「ディレクトリバケットの使用」を参照してください。

- 低レイテンシーのユースケースでは、ディレクトリバケットを単一の AWS アベイラビリティーゾーンに作成してデータを保存できます。アベイラビリティーゾーンのディレクトリバケットは、S3 Express One Zone ストレージクラスをサポートしています。S3 Express One Zone では、データは単一のアベイラビリティーゾーン内で冗長的に複数のデバイスに保存されます。S3 Express One Zone ストレージクラスは、アプリケーションがパフォーマンスの影響を受けやすく、1 桁ミリ秒の PUT および GET のレイテンシーから利点が得られる場合にお勧めします。アベイラビリティーゾーンでのディレクトリバケットの作成の詳細については、「高性能ワークロード」を参照してください。
- データレジデンシーのユースケースでは、ディレクトリバケットを単一の AWS 専有ローカルゾーン (DLZ) に作成してデータを保存できます。専有ローカルゾーンでは、S3 ディレクトリバケットを作成して特定のデータ境界にデータを保存できるため、データレジデンシーと分離のユースケースをサポートするのに役立ちます。Local Zones のディレクトリバケットは、S3 One Zone-Infrequent Access (S3 One Zone-IA、Z-IA) ストレージクラスをサポートしています。ローカルゾーンでのディレクトリバケットの作成の詳細については、「データレジデンシーワークロード」を参照してください。

> **Note**
>
> ディレクトリバケットでは、すべてのパブリックアクセスがデフォルトで無効になります。この動作は変更できません。ディレクトリバケットに保存されているオブジェクトへのアクセスは付与できません。アクセスは、ディレクトリバケットにたいしてのみ付与できます。詳細については、「リクエストの認証と承認」を参照してください。

テーブルバケット – 毎日の購入トランザクション、ストリーミングセンサーデータ、広告インプレッションなどの表形式データの保存に推奨されます。表形式データは、データベーステーブルのように列と行のデータを表します。テーブルバケットは、分析ワークロードと機械学習ワークロード向けに最適化された S3 ストレージを提供し、クエリのパフォーマンスの向上とテーブルのストレージコストの削減を継続的に行うように設計された機能を備えています。S3 Tables は、表形式データを Apache Iceberg 形式で保存するための専用サービスです。S3 Tables の表形式データは、Amazon Athena、Amazon Redshift、Apache Spark などの一般的なクエリエンジンを使用してクエリできます。デフォルトでは、AWS リージョンごとに AWS アカウントあたり最大 10 個のテーブルバケットと、テーブルバケットごとに最大 10,000 個のテーブルを作成できます。詳細については、「S3 Tables とテーブルバケットの使用」を参照してください。

> **Note**
>
> すべてのテーブルバケットとテーブルはプライベートであり、公開することはできません。これらのリソースにアクセスできるのは、明示的にアクセス許可が与えられているユーザーのみです。アクセスを許可するには、テーブルバケットとテーブルには IAM リソースベースのポリシーを使用し、ユーザーとロールには IAM アイデンティティベースのポリシーを使用します。詳細については、「S3 Tables のセキュリティ」を参照してください。

すべてのバケットタイプに関する追加情報

バケットを作成するときは、バケット名を入力し、バケットが存在する AWS リージョン を選択します。一度バケットを作成したら、そのバケット名またはリージョンを変更することはできません。バケット名は、以下のバケット命名規則に従う必要があります。

- 汎用バケットの命名規則
- ディレクトリバケットの命名規則
- テーブルバケットの命名規則

バケットは、以下も行います。

- 最も高いレベルで Amazon S3 名前空間を編成します。汎用バケットの場合、この名前空間は S3 です。ディレクトリバケットの場合、この名前空間は s3express です。テーブルバケットの場合、この名前空間は s3tables です。
- ストレージおよびデータ転送料金が課金されるアカウントを特定します。
- 使用状況レポートの集計単位として機能します。

オブジェクト

オブジェクトとは、Amazon S3 に保存される基本エンティティです。オブジェクトは、オブジェクトデータとメタデータで構成されます。メタデータは、オブジェクトを表現する名前と値のペアのセットです。これには最終更新日などのデフォルトメタデータや、Content-Type などの標準 HTTP メタデータが含まれます。また、オブジェクトの保存時にカスタムメタデータを指定することもできます。

すべてのオブジェクトはバケット内に保存されます。例えば、photos/puppy.jpg という名前のオブジェクトが米国西部 (オレゴン) リージョンの amzn-s3-demo-bucket 汎用バケットに保存されている場合、URL https://amzn-s3-demo-bucket.s3.us-west-2.amazonaws.com/photos/puppy.jpg を使用してアドレス可能です。詳細については、「バケットへのアクセス」を参照してください。

オブジェクトは、バケット内でキー (名前)とバージョン ID (バケットで S3 バージョニングが有効になっている場合) によって一意に特定されます。オブジェクトの詳細については、Amazon S3 オブジェクトの概要 を参照してください。

キー

オブジェクトキー (または キー名) は、バケット内のオブジェクトの固有の識別子です。バケット内のすべてのオブジェクトは、厳密に 1 個のキーを持ちます。バケット、オブジェクトキー、およびオプションでバージョン ID (バケットで S3 バージョニングが有効になっている場合) の組み合わせによって、各オブジェクトが一意に識別されます。そのため、Amazon S3 を「バケット + キー + バージョン」とオブジェクト自体の間での基本データマップと考えることができます。

Amazon S3 内の各オブジェクトは、ウェブサービスエンドポイント、バケット名、キー、およびオプションでバージョンを組み合わせることで一意にアドレスを指定できます。例えば、https://*amzn-s3-demo-bucket*.s3.us-west-2.amazonaws.com/photos/puppy.jpg

という URL で、「*amzn-s3-demo-bucket*」がバケットの名前で、「photos/puppy.jpg」がキーです。

オブジェクトキーの詳細については、「Amazon S3 オブジェクトに命名する」を参照してください。

S3 バージョニング

同じバケット内でオブジェクトの複数のバリアントを保持するには、S3 バージョニングを使用します。S3 バージョニングを使用すると、 バケットに保存されたあらゆるオブジェクトのあらゆるバージョンを保存、取得、復元することができます。バージョニングを使用すれば、意図しないユーザーアクションからもアプリケーション障害からも、簡単に復旧できます。

詳細については、「S3 バージョニングによる複数のバージョンのオブジェクトの保持」を参照してください。

バージョン ID

バケットで S3 バージョニングを有効にすると、Amazon S3 はバケットに追加されたすべてのオブジェクトに一意のバージョン ID を与えます。バージョニングを有効にした時点でバケットにすでに存在していたオブジェクトのバージョン ID は `null` です。これらの (またはその他の) オブジェクトを他のオペレーション (CopyObject および PutObject) で変更すると、新しいオブジェクトは一意のバージョン ID を取得します。

詳細については、「S3 バージョニングによる複数のバージョンのオブジェクトの保持」を参照してください。

バケットポリシー

バケットポリシーは、リソースベースの AWS Identity and Access Management (IAM) ポリシーを使用して、バケットとその中のオブジェクトへのアクセス許可を付与できます。バケット所有者のみが、ポリシーをバケットに関連付けることができます。バケットに添付された許可は、バケット所有者が所有するバケットのすべてのオブジェクトに適用されます。バケットポリシーのサイズは 20 KB に制限されています。

バケットポリシーは、AWS で標準である JSON ベースのアクセスポリシー言語を使用しています。バケットポリシーを使用して、バケット内のオブジェクトに対する許可を追加または拒否できます。バケットポリシーは、リクエスタ、S3 アクション、リソース、リクエストの側面または条件(リクエストの作成に使用された IP アドレスなど)など、ポリシー内のエレメントに基づいてリクエストを許

可または拒否します。例えば、バケット所有者がアップロードされたオブジェクトを完全にコントロールできるように、S3 バケットにオブジェクトをアップロードするクロスアカウント許可を付与するバケットポリシーを作成できます。詳細については、Amazon S3 バケットポリシーの例 を参照してください。

バケットポリシーでは、Amazon リソースネーム (ARN) やその他の値に対してワイルドカード文字を使用して、オブジェクトのサブセットに対する許可を付与できます。例えば、共通のプレフィックスで始まるか、.html などの特定の拡張子で終わるオブジェクトのグループへのアクセスをコントロールできます。

S3 アクセスポイント

Amazon S3 アクセスポイントは、そのエンドポイントを使用してデータにアクセスする方法を説明する専用のアクセスポリシーを持つ名前付きネットワークエンドポイントです。アクセスポイントは、GetObject や PutObject などの S3 オブジェクト操作の実行に使用できる汎用バケットまたはディレクトリバケットにアタッチされます。アクセスポイントは、Amazon S3 の共有データセットへの大規模なデータアクセスの管理を簡素化します。

各アクセスポイントには独自のアクセスポイントポリシーがあります。また、アクセスポイントごとにブロックパブリックアクセス設定を設定することもできます。仮想プライベートクラウド (VPC) からのリクエストだけを受け入れるようにアクセスポイントを設定することで、プライベートネットワークへの Amazon S3 データアクセスを制限できます。

汎用バケットのアクセスポイントの詳細については、「アクセスポイントを使用した汎用バケット内の共有データセットへのアクセスの管理」を参照してください。ディレクトリバケットのアクセスポイントの詳細については、「アクセスポイントを使用したディレクトリバケット内の共有データセットへのアクセスの管理」を参照してください。

アクセスコントロールリスト (ACL)

ACL を使用して、個々の汎用バケットとオブジェクトの読み取りと書き込みのアクセス許可を認証ユーザーに付与できます。各汎用バケットとオブジェクトには、サブリソースとして ACL がアタッチされています。ACL は、アクセスを付与する先の AWS アカウントまたはグループと、アクセスのタイプを定義します。ACL は IAM よりも優先されるアクセスコントロールメカニズムです。ACL の詳細については、「アクセスコントロールリスト (ACL) の概要」を参照してください。

S3 オブジェクト所有権は、Amazon S3 バケットレベルの設定で、バケットにアップロードされる新しいオブジェクト所有権を制御し、ACL を無効にするのに使用できます。デフォルトでは、オブジェクト所有権はバケット所有者の強制設定に設定され、すべての ACL は無効になります。ACL を

無効にすると、バケット所有者はバケット内のすべてのオブジェクトを所有し、アクセス管理ポリシーのみを使用してデータへのアクセスを管理します。

Amazon S3 の最新のユースケースの大部分では ACL を使用する必要がなくなっています。オブジェクトごとに個別に制御する必要がある通常ではない状況を除き、ACL は無効にしておくことをお勧めします。ACL を無効にすると、誰がオブジェクトをバケットにアップロードしたかに関係なく、ポリシーを使用してバケット内のすべてのオブジェクトへのアクセスを制御できます。詳細については、「オブジェクトの所有権の制御とバケットの ACL の無効化。」を参照してください。

リージョン

作成したバケットを Amazon S3 が保存する地理的な AWS リージョン を選択できます。レイテンシーを最適化し、コストを最小限に抑えて規制用件に対応できるリージョンを選ぶとよいでしょう。明示的に別のリージョンに移動またはレプリケートする場合を除き、AWS リージョン に保存されたオブジェクトは、そのリージョンから移動されることはありません。たとえば、欧州 (アイルランド) リージョンに格納されたオブジェクトは、ずっとそのリージョンに置かれたままです。

> **Note**
>
> 自分のアカウントで有効になっている AWS リージョン では、Amazon S3 とその機能にのみアクセスできます。リージョンで AWS リソースを作成および管理できるようにする方法の詳細については、「AWS 全般のリファレンス」の「AWS リージョン の管理」を参照してください。

Amazon S3 のリージョンとエンドポイントのリストについては、「AWS 全般のリファレンス」の「リージョンとエンドポイント」を参照してください。

Amazon S3 のデータ整合性モデル

Amazon S3 には、すべての AWS リージョン にある Amazon S3 バケットの、オブジェクトの PUT と DELETE に関する、書き込み後読み取りの強力な整合性があります。この動作は、新しいオブジェクトへの書き込みと、既存のオブジェクトを上書きする PUT リクエスト、そして DELETE リクエストにも適用されます。さらに、Amazon S3 Select、Amazon S3 アクセスコントロールリスト (ACL)、Amazon S3 オブジェクトタグ、オブジェクトメタデータ (HEAD オブジェクトなど) での読み込みオペレーションには、強力な整合性があります。

単一のキーに対する更新はアトミックです。例えば、あるスレッドから既存のキーに PUT リクエストを実行し、同時に同じキーに対して別のスレッドから GET リクエストを実行すると、古いデータ

または新しいデータを取得できますが、データの一部分だけが取得されることも、破損することもありません。

Amazon S3 は、AWS データセンターに配置された複数のサーバー間でデータを複製することにより、高可用性を実現します。PUT リクエストが成功した場合、データは安全に保存されています。成功した PUT 応答の受信後に開始された読み取り (GET または LIST) は、PUT リクエストによって書き込まれたデータを返します。この動作の例を示します。

- 新しいオブジェクトを Amazon S3 に書き込み、すぐにバケット内のキーを一覧表示します。新しいオブジェクトがリストに表示されます。
- 既存のオブジェクトを置換し、すぐにそのオブジェクトの読み取りを試みます。Amazon S3 が新しいデータを返します。
- 既存のオブジェクトを削除し、すぐにそのオブジェクトの読み取りを試みます。オブジェクトが削除されたため、Amazon S3 はデータを返しません。
- 既存のオブジェクトを削除し、すぐにバケット内のキーのリストを表示します。オブジェクトはリストに表示されません。

> **Note**
>
> - Amazon S3 は、同時書き込みのオブジェクトロックをサポートしていません。同じキーに対して 2 つの PUT リクエストが同時に行われた場合、最新のタイムスタンプを持つリクエストが優先されます。これが問題になる場合は、アプリケーション内にオブジェクトロックメカニズムを構築する必要があります。
> - 更新はキーベースです。複数キーにまたがるアトミックな更新を行う方法はありません。たとえば、ご自分で機能をアプリケーション設計に組み込まない限り、別のキーの更新に依存してキーを更新することはできません。

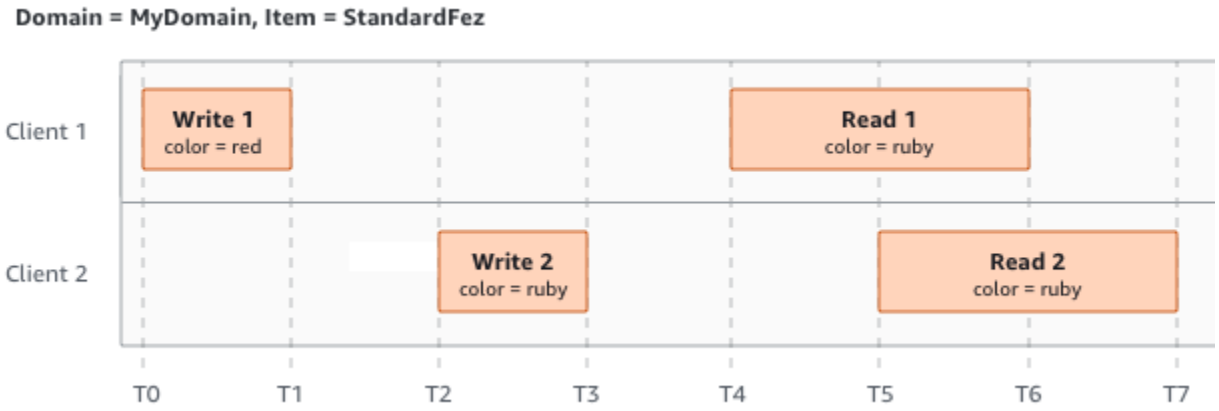
バケット設定には、結果整合性モデルがあります。具体的には、次のように処理されます。

- バケットを削除してすぐにすべてのバケットを一覧表示しても、削除されたバケットは引き続きリストに表示されます。
- バケットで初めてバージョニングを有効にしたときは、変更が完全に反映されるまでに、少し時間がかかることがあります。バケットへのオブジェクトの書き込みオペレーション (PUT または DELETE リクエスト) は、バージョニングを有効にして 15 分待ってから発行することをお勧めします。

アプリケーションの同時実行

このセクションでは、同じアイテムに複数のクライアントから書き込むときに、Amazon S3 で予想される動作の例を示します。

次の例では、R1 (読み取り 1) と R2 (読み取り 2) の開始前に W1 (書き込み 1) と W2 (書き込み 2) が完了しています。S3 には強固な整合性があるため、R1 と R2 はどちらも `color = ruby` を返します。



次の例では、R1 の開始前に、W2 は完了していません。したがって、R1 は `color = ruby` または `color = garnet` を返す可能性があります。ただし、R2 が開始する前に W1 と W2 が終了するため、R2 は `color = garnet` を返します。

最後の例では、W1 が受信確認を受け取る前に、W2 が開始します。したがって、これらは同時の書き込みとみなされます。どの書き込みを優先するのかを決定するにあたり、Amazon S3 は内部的に last-writer-wins セマンティクスを使用します。しかし、ネットワークレイテンシーなどのさまざまな要因により、Amazon S3 がリクエストを受信する順序や、アプリケーションが受信確認を受け取る順序を予測することはできません。例えば、W2 が同じリージョンにある Amazon EC2 インスタン

スによって開始される一方で、W1 は遠くにあるホストによって開始されるかもしれません。両方の書き込みの受信確認を受け取った後に、読み込みを実行することが、最終的な値を決定する最善の方法です。

関連サービス

Amazon S3 にロードしたデータは、他の AWS のサービスでも利用できます。よく使用すると思われるサービスは次のとおりです。

- Amazon Elastic Compute Cloud (Amazon EC2) – 安全でスケーラブルなコンピューティング容量を AWS クラウド で提供します。Amazon EC2 の使用により、ハードウェアに事前投資する必要がなくなり、アプリケーションをより速く開発およびデプロイできます。Amazon EC2 を使用すると、必要な数 (またはそれ以下) の仮想サーバーの起動、セキュリティおよびネットワーキングの構成、ストレージの管理ができます。
- Amazon EMR – ビジネス、研究者、データアナリスト、およびデベロッパーが、簡単かつ費用対効果の高い方法で、莫大な量のデータを処理できます。Amazon EMR は、Amazon EC2 および Amazon S3 のウェブスケールのインフラストラクチャ上で稼動するホストされた Hadoop フレームワークを使用しています。
- AWSSnow ファミリー– 厳しいデータセンター以外の環境や、一貫性のあるネットワーク接続がない場所で運用を実行する必要があるお客様を支援します。AWS Snow ファミリーデバイスを使用して、インターネットに接続できない環境で、ローカルでコスト効果の高い方法で AWS クラウドのストレージおよび処理能力にアクセスできます。
- AWS Transfer Family – セキュアシェル (SSH) ファイル転送プロトコル (SFTP)、SSL 経由ファイル転送プロトコル (FTPS)、およびファイル転送プロトコル (FTP) を使用して、Amazon S3 または Amazon Elastic File System (Amazon EFS) との間で直接ファイル転送を行う完全マネージドサポートを提供します。

Amazon S3 へのアクセス

Amazon S3 は次のいずれかの方法で使用できます。

AWS Management Console

コンソールは、Amazon S3 と AWS リソースを管理するためのウェブベースのユーザーインターフェイスです。AWS アカウント にサインアップ済みの場合は、AWS Management Console にサインインし、AWS Management Console ホームページから [S3] を選択することで、Amazon S3 コンソールにアクセスできます。

AWS Command Line Interface

AWS コマンドラインツールを使用して、コマンドを発行するか、システムのコマンドラインでスクリプトを作成して AWS (S3 を含む) タスクを実行します。

AWS Command Line Interface (AWS CLI) は、幅広い AWS のサービス のセットに対するコマンドを提供します。AWS CLI は、Windows、macOS、Linux でサポートされています。使用を開始するには、「 AWS Command Line Interfaceユーザーガイド」を参照してください。Amazon S3 用コマンドの詳細については、AWS CLIコマンドリファレンスの s3api および s3control を参照してください。

AWS SDK

AWS には、さまざまなプログラミング言語およびプラットフォーム (Java、Python、Ruby、.NET、iOS、Android など) のライブラリとサンプルコードで構成された SDK (ソフトウェア開発キット) が用意されています。AWS SDK は、S3 や AWS へのプログラムによるアクセスを作成するのに役立ちます。Amazon S3 は REST サービスです。AWS SDK ライブラリを使用して Amazon S3 にリクエストを送信できます。これは、基盤となる Amazon S3 REST API をラップし、プログラミングタスクを簡素化します。例えば、SDK は署名の計算、リクエストの暗号化による署名、エラーの管理、リクエストの自動再試行などのタスクを処理します。AWS SDK のダウンロードやインストールなどの詳細については、「AWS のツール」を参照してください。

Amazon S3 とのすべてのやり取りは認証されるか匿名で行われます。AWS SDK を使用している場合、指定したキーから、ライブラリによって認証のための署名が計算されます。Amazon S3 へのリクエストの作成方法の詳細については、「Making requests」を参照してください。

Amazon S3 REST API

Amazon S3 は、プログラミング言語に依存しないアーキテクチャとして設計されており、AWS がサポートされているインターフェイスを使用してオブジェクトを保存、取得します。Amazon S3 REST API を使用して、プログラムによって S3 や AWS にアクセスすることができます。REST API は、Amazon S3 に対する HTTP インターフェイスです。REST API では、標準 HTTP リクエストを使用してバケットとオブジェクトを作成、取得、削除できます。

REST API を使用する場合、HTTP をサポートする任意のツールキットを使用できます。匿名で読み取り可能なオブジェクトであれば、ブラウザを使用して取得することもできます。

REST API は標準の HTTP ヘッダーとステータスコードを使用するため、標準のブラウザとツールキットが予期したとおりに機能します。一部のエリアでは、HTTP に機能が追加されています (たとえば、アクセスコントロールをサポートするヘッダーを追加しました)。このように新機能を追加する場合、できるだけ標準 HTTP 書式の使用法に合致するように最善を尽くしました。

ただし、アプリケーションで直接 REST API を呼び出す場合、署名を計算するコードを作成し、それをリクエストに追加する必要があります。Amazon S3 にリクエストを行う方法の詳細については、「Amazon S3 リファレンス」の「Making requests」を参照してください。

> **Note**
>
> SOAP API のサポートは HTTP 経由では廃止されましたが、HTTPS 経由では引き続き利用可能です。新しい Amazon S3 機能は、SOAP ではサポートされません。REST API か AWS SDK を使用することをお勧めします。

Amazon S3 の支払い

Amazon S3 の料金は、アプリケーションのストレージ要件を考慮しなくてすむように設定されています。ほとんどのストレージプロバイダーでは、あらかじめ決められた量のストレージおよびネットワーク転送容量を購入する必要があります。このシナリオでは、その容量を超えると、サービスが停止されるか、高額な超過料金を支払う必要があります。その容量を超えない場合でも、全量を使用したものとして支払うことになります。

Amazon S3 では、実際に使用した分だけが請求されます。隠れた料金や超過料金はありません。このモデルでは、AWS インフラストラクチャのコスト面のメリットを得ながら、ビジネスの成長に応じた可変コストのサービスを利用することができます。詳細については、Amazon S3 の料金 を参照してください。

AWS にサインアップすると、Amazon S3 を含む AWS のすべてのサービスに対して AWS アカウント が自動的にサインアップされます。ただし、料金が発生するのは実際に使用したサービスの分だけです。Amazon S3 の新規のお客様は、Amazon S3 を無料で使い始めることができます。詳細については、「AWS 無料利用枠」を参照してください。

請求を表示するには、AWS Billing and Cost Management コンソールで請求およびコスト管理ダッシュボードに移動します。AWS アカウント 請求の詳細については、AWS Billing ユーザーガイドを参照してください。AWS 請求および AWS アカウント についてご質問がある場合は、AWS Support にお問い合わせください。

PCI DSS コンプライアンス

Amazon S3 は、マーチャントまたはサービスプロバイダーによるクレジットカードデータの処理、ストレージ、および伝送をサポートしており、Payment Card Industry (PCI) Data Security Standard (DSS) に準拠していることが確認されています。PCI DSS の詳細 (AWS PCI Compliance Package のコピーをリクエストする方法など) については、「PCI DSS レベル 1」を参照してください。

Amazon S3 の開始方法

Amazon S3 は、バケットとオブジェクトを操作することで、使用を開始できます。バケット とは、オブジェクトのコンテナのことです。オブジェクト とは、ファイルと、そのファイルを記述している任意のメタデータのことです。

Amazon S3 にオブジェクトを保存するには、バケットを作成し、そのバケットにオブジェクトをアップロードします。オブジェクトがバケットの中にあるときは、オブジェクトを開き、ダウンロードして、移動させます。オブジェクトまたはバケットが不要になったら、リソースをクリーンアップします。

Amazon S3 では、お支払いは実際に使用した分のみです。Amazon S3 の機能と料金の詳細については、「Amazon S3」を参照してください。Amazon S3 の新規のお客様は、Amazon S3 を無料で使い始めることができます。詳細については、AWS 無料利用枠 を参照してください。

> **Note**
>
> Amazon S3 Express One Zone ストレージクラスをディレクトリバケットで使用する方法の詳細については、「S3 Express One Zone」と「ディレクトリバケットの使用」を参照してください。

動画: Amazon S3 の開始方法

前提条件

開始する前に、必ず「Amazon S3 のセットアップ」の手順を完了させてください。

Amazon S3 のセットアップ

AWS にサインアップすると、Amazon S3 を含む AWS のすべてのサービスに対して AWS アカウント が自動的にサインアップされます。料金が発生するのは、実際に使用したサービスの分のみです。

Amazon S3 では、お支払いは実際に使用した分のみです。Amazon S3 の機能と料金の詳細については、「Amazon S3」を参照してください。Amazon S3 の新規のお客様は、Amazon S3 を無料で使い始めることができます。詳細については、「AWS 無料利用枠」を参照してください。

Amazon S3 をセットアップするには、以下のセクションのステップを使用します。

AWS にサインアップして Amazon S3 をセットアップする際に、オプションで AWS Management Console の表示言語を変更できます。詳細については、AWS Management Console 開始方法のガイドの AWS Management Console の言語の変更を参照してください。

トピック

- AWS アカウントへのサインアップ
- 管理アクセスを持つユーザーを作成する

AWS アカウントへのサインアップ

AWS アカウント がない場合は、以下のステップを実行して作成します。

AWS アカウントにサインアップするには

1. https://portal.aws.amazon.com/billing/signup を開きます。
2. オンラインの手順に従います。

   サインアップ手順の一環として、通話呼び出しを受け取り、電話キーパッドで検証コードを入力するように求められます。

   AWS アカウント にサインアップすると、AWS アカウントのルートユーザー が作成されます。ルートユーザーには、アカウントのすべての AWS のサービスとリソースへのアクセス権があります。セキュリティのベストプラクティスとして、ユーザーに管理アクセスを割り当て、ルートユーザーのみを使用してルートユーザーアクセスが必要なタスクを実行してください。

サインアップ処理が完了すると、AWS からユーザーに確認メールが送信されます。https://aws.amazon.com/ の [マイアカウント] をクリックして、いつでもアカウントの現在のアクティビティを表示し、アカウントを管理することができます。

管理アクセスを持つユーザーを作成する

AWS アカウント にサインアップしたら、AWS アカウントのルートユーザー をセキュリティで保護し、AWS IAM Identity Center を有効にして、管理ユーザーを作成します。これにより、日常的なタスクにルートユーザーを使用しないようにします。

AWS アカウントのルートユーザーをセキュリティで保護する

1. [ルートユーザー] を選択し、AWS アカウント のメールアドレスを入力して、アカウント所有者として AWS Management Console にサインインします。次のページでパスワードを入力します。

   ルートユーザーを使用してサインインする方法については、AWS サインイン ユーザーガイドのルートユーザーとしてサインインするを参照してください。
2. ルートユーザーの多要素認証 (MFA) を有効にします。

   手順については、「IAM ユーザーガイド」で AWS アカウントのルートユーザーの仮想 MFA デバイスを有効にする方法 (コンソール) を確認してください。

管理アクセスを持つユーザーを作成する

1. IAM アイデンティティセンターを有効にします。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「AWS IAM Identity Center の有効化」を参照してください。
2. IAM アイデンティティセンターで、ユーザーに管理アクセスを付与します。

   IAM アイデンティティセンターディレクトリ をアイデンティティソースとして使用するチュートリアルについては、「AWS IAM Identity Center ユーザーガイド」の「 Configure user access with the default IAM アイデンティティセンターディレクトリ」を参照してください。

管理アクセス権を持つユーザーとしてサインインする

- IAM アイデンティティセンターのユーザーとしてサインインするには、IAM アイデンティティセンターのユーザーの作成時に E メールアドレスに送信されたサインイン URL を使用します。

  IAM アイデンティティセンターユーザーを使用してサインインする方法については、「AWS サインイン User Guide」の「Signing in to the AWS access portal」を参照してください。

追加のユーザーにアクセス権を割り当てる

1. IAM アイデンティティセンターで、最小特権のアクセス許可を適用するというベストプラクティスに従ったアクセス許可セットを作成します。

手順については、「AWS IAM Identity Center ユーザーガイド」の「権限設定を作成する」を参照してください。

2. グループにユーザーを割り当て、そのグループにシングルサインオンアクセス権を割り当てます。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「グループの結合」を参照してください。

ステップ 1: 最初の S3 バケットを作成する

AWS にサインアップしたら、AWS Management Console を使っていつでも Amazon S3 にバケットを作成できます。Amazon S3 のオブジェクトはすべてバケットに保管されます。Amazon S3 にデータを保管する前に、バケットを作成する必要があります。

> **Note**
>
> Amazon S3 Express One Zone ストレージクラスをディレクトリバケットで使用する方法の詳細については、「S3 Express One Zone」と「ディレクトリバケットの使用」を参照してください。

> **Note**
>
> バケットの作成は課金対象にはなりません。バケット内にオブジェクトを保存した場合、およびバケット宛てまたはバケットからオブジェクトを転送した場合にのみ課金されます。このガイドの例に従って操作して発生する使用料はごくわずかです (1 USD 未満)。ストレージ料金の詳細については、「Amazon S3 の料金」を参照してください。

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ページ上部にあるナビゲーションバーで、現在表示されている AWS リージョン の名前をクリックします。次に、バケットを作成するリージョンを選択します。

> **Note**
>
> - 一旦バケットを作成したら、そのリージョンを変更することはできません。
> - レイテンシーとコストを最小化するため、さらに規制条件に対応するために、最寄りのリージョンを選択します。明示的に別のリージョンに移動する場合を除き、特定のリージョンに保管されたオブジェクトは、そのリージョンから移動されることはありません。Amazon S3 AWS リージョン のリストについては、「Amazon Web Services 全般のリファレンス」の「AWS のサービス エンドポイント」を参照してください。

3. 左のナビゲーションペインで、[汎用バケット] を選択します。
4. [Create bucket (バケットの作成)] を選択します。[バケットの作成] ページが開きます。
5. [バケット名] にバケットの名前を入力します。

   バケット名には次の条件があります。

   - パーティション内で一意にする必要があります。パーティションは、リージョンのグループです。AWS には、現在 aws (商用リージョン)、aws-cn (中国リージョン)、および aws-us-gov (AWS GovCloud (US) Regions) の 3 つのパーティションがあります。
   - 3～63 文字で指定する。
   - 小文字、数字、ピリオド (.)、ハイフン (-) のみで構成されます。互換性を最も高くするには、静的ウェブサイトホスティング専用のバケットを除き、バケット名にピリオド (.) を使用しないことをお勧めします。
   - 文字や数字で始まり、文字や数字で終わります。
   - バケットの命名規則の完全なリストについては、「汎用バケットの命名規則」を参照してください。

   > **Important**
   >
   > - バケットを作成したら、その名前を変更することはできません。
   > - バケット名に機密情報を含めないでください。バケット名は、バケット内のオブジェクトを参照する URL に表示されます。

6. (オプション) [全般設定] で、既存のバケットの設定を新しいバケットにコピーすることを選択できます。既存のバケットの設定をコピーしない場合は、次のステップにスキップします。

> **Note**
>
> このオプションの特徴:
>
> - AWS CLI では使用できません。Amazon S3 コンソールでのみ利用できます。
> - バケットポリシーは既存のバケットから新しいバケットにコピーしません。

既存のバケットの設定をコピーするには、[既存のバケットから設定をコピー] で [バケットを選択] をクリックします。[バケットを選択] ウィンドウが開きます。コピーする設定を持つバケットを検索して、[バケットを選択] をクリックします。[バケットを選択] ウィンドウが閉じて、[バケットを作成] ウィンドウが再び開きます。

[既存のバケットから設定をコピー] に、選択したバケットの名前が表示されるようになります。新しいバケットの設定が、選択したバケットの設定と一致するようになりました。コピーした設定を削除する場合は、[デフォルトを復元] を選択します。[バケットを作成] ページで、バケットの残りの設定を確認します。変更しない場合は、最後のステップに進みます。

7. [オブジェクト所有者] で、ACL を無効または有効にし、バケットにアップロードされたオブジェクトの所有権を制御するには、次のいずれかの設定を選択します。

   ACL は無効です

   - バケット所有者の強制 (デフォルト) – ACL は無効になり、バケット所有者は汎用バケット内のすべてのオブジェクトを自動的に所有し、完全に制御します。ACL は、S3 汎用バケット内のデータへのアクセス許可に影響を与えなくなりました。このバケットはアクセスコントロールを定義するためだけにポリシーを使用します。

     デフォルトでは、ACL は無効になっています。Amazon S3 の最新のユースケースの大部分では ACL を使用する必要がなくなっています。オブジェクトごとに個別に制御する必要がある通常ではない状況を除き、ACL は無効にしておくことをお勧めします。詳細については、「オブジェクトの所有権の制御とバケットの ACL の無効化。」を参照してください。

   ACL の有効化

   - 希望するバケット所有者 — バケット所有者は、他のアカウントが `bucket-owner-full-control` 既定 ACL でバケットに書き込む新しいオブジェクトを所有し、完全にコントロールできます。

[バケット所有者を推奨] 設定を適用して、すべての Amazon S3 アップロードに bucket-owner-full-control 既定 ACL を含めることを要求する場合は、この ACL を使用するオブジェクトアップロードのみを許可するバケットポリシーを追加できます。

- オブジェクトライター — オブジェクトをアップロードする AWS アカウント は、そのオブジェクトを所有し、そのオブジェクトを完全にコントロールし、ACL を介して他のユーザーにそのオブジェクトへのアクセス権を付与できます。

> **Note**
>
> デフォルト設定は [バケット所有者の強制] です。デフォルト設定を適用して ACL を無効のままにするのに必要なのは、s3:CreateBucket アクセス許可のみです。ACL を有効にするためには、s3:PutBucketOwnershipControls アクセス許可が必要です。

8. [このバケットのパブリックアクセスブロック設定] で、バケットに適用するブロックパブリックアクセス設定を選択します。

   デフォルトでは、4 つすべての [パブリックアクセスをブロック] 設定が有効になっています。特定のユースケースでオフにする必要のある設定が 1 つ以上あることがわかっている場合を除き、すべての設定を有効にしておくことをお勧めします。ブロックパブリックアクセスの詳細については、Amazon S3 ストレージへのパブリックアクセスのブロック を参照してください。

   > **Note**
   >
   > すべての [パブリックアクセスをブロック] 設定を有効にするのに必要なのは、s3:CreateBucket アクセス許可のみです。[パブリックアクセスをブロック] 設定をオフにするには、s3:PutBucketPublicAccessBlock アクセス許可が必要です。

9. (オプション) [バケットのバージョニング] は、デフォルトで無効になります。バージョニングとは、同じバケット内でオブジェクトの複数のバリアントを保持する手段です。バージョニングを使用して、 バケットに保存されたあらゆるオブジェクトのあらゆるバージョンを保存、取得、復元することができます。バージョニングを使用すれば、意図しないユーザーアクションからもアプリケーション障害からも、より簡単に復旧できます。バージョニングの詳細については、「S3 バージョニングによる複数のバージョンのオブジェクトの保持」を参照してください。

   バケットでバージョニングを有効にするには、[有効化] を選択します。

10. (オプション) [Tags] (タグ) では、バケットにタグを追加することを選択できます。AWS コスト配分では、バケットタグを使用してバケットの使用に対する請求に注釈を付けることができます。タグはキー/値ペアになっており、バケットに割り当てられるラベルを表します。詳細については、「the section called “コスト配分タグの使用”」を参照してください。

    (オプション) タグを追加するには、[キー] を入力してから、オプションの [値] を入力し、[タグの追加] を選択します。

11. [デフォルトの暗号化] を設定するには、[暗号化タイプ] で次のいずれかを選択します。

    - Amazon S3 マネージドキーを用いたサーバー側の暗号化 (SSE-S3)
    - AWS Key Management Service キーによるサーバー側の暗号化 (SSE-KMS)
    - AWS Key Management Service (AWS KMS) キーによる二層式サーバー側の暗号化 (DSSE-KMS)

    > **Important**
    >
    > デフォルト暗号化設定として SSE-KMS または DSSE-KMS オプションを使用する場合、AWS KMS の 1 秒あたりのリクエスト数 (RPS) 制限が適用されます。AWS KMS クォータの詳細およびクォータの引き上げをリクエストする方法については、「AWS Key Management Service デベロッパーガイド」の「クォータ」を参照してください。

    バケットと新しいオブジェクトは、暗号化設定の基本レベルとして Amazon S3 マネージドキー (SSE-S3) を使用したサーバー側の暗号化で暗号化されます。デフォルトの暗号化の詳細については、「Amazon S3 バケット向けのサーバー側のデフォルトの暗号化動作の設定」を参照してください。SSE-KMS に関する詳細は、「Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3)」を参照してください。

    サーバー側の暗号化を使用してデータを暗号化する方法の詳細については、「the section called “データ暗号化”」を参照してください。

12. Amazon S3 が管理するキー (SSE-S3) によるサーバー側の暗号化または AWS Key Management Service (AWS KMS) キーによる二層式サーバー側の暗号化 (DSSE-KMS) を選択した場合は、次の操作を行います。

    a. [AWS KMS キー] で、次のいずれかの方法で KMS キーを指定します。

- 使用可能な KMS キーのリストから選択するには、[AWS KMS keys から選択する] を選択し、使用可能なキーのリストから自分の KMS キーを選択します。

  AWS マネージドキー (aws/s3) とカスタマーマネージドキーの両方がこのリストに表示されます。カスタマーマネージドキーの詳細については、AWS Key Management Service デベロッパーガイドの「カスタマーキーと AWS キー」を参照してください。

- KMS キー ARN を入力するには、[AWS KMS key ARN を入力] を選択し、表示されるフィールドに KMS キー ARN を入力します。

- AWS KMS コンソールで新しいカスタマーマネージドキーを作成するには、[KMS キーを作成] を選択します。

  AWS KMS key の作成の詳細については、「AWS Key Management Service デベロッパーガイド」の「キーの作成」を参照してください。

> **Important**
>
> バケットと同じ AWS リージョン で使用可能な KMS キーのみを使用できます。Amazon S3 コンソールには、バケットと同じリージョンで最初の 100 個の KMS キーしか表示されません。リストに存在しない KMS キーを使用するには、KMS キー ARN を入力する必要があります。別のアカウントが所有している KMS キーを使用する場合は、まず、そのキーを使用するアクセス許可が必要であり、次に、KMS キー ARN を入力する必要があります。KMS キーのクロスアカウント権限の詳細については、「AWS Key Management Service デベロッパーガイド」の「他のアカウントで使用できる KMS キーを作成する」を参照してください。SSE-KMS に関する詳細は、「AWS KMS (SSE-KMS) によるサーバー側の暗号化の指定」を参照してください。DSSE-KMS に関する詳細については、「the section called “二層式サーバー側の暗号化 (DSSE-KMS) ”」を参照してください。Amazon S3 でサーバー側の暗号化に AWS KMS key を使用する場合は、対称暗号化 KMS キーを選択する必要があります。Amazon S3 では、対称暗号化 KMS キーのみがサポートされ、非対称暗号化 KMS キーはサポートされません。詳細については、AWS Key Management Service デベロッパーガイドの「Identifying symmetric and asymmetric KMS keys」(対称および非対称 KMS キーの識別) を参照してください。

b. SSE-KMS でデフォルトの暗号化を使用するようにバケットを設定する場合は、S3 バケットキーを使用することもできます。S3 バケットキーは、Amazon S3 から AWS KMS へ

のリクエストトラフィックを減らし、暗号化のコストを削減します。詳細については、「Amazon S3 バケットキーを使用した SSE-KMS のコストの削減」を参照してください。S3 バケットキーは DSSE-KMS ではサポートされていません。

デフォルトでは、S3 バケットキーは Amazon S3 コンソールで有効になっています。コストを削減するには、S3 バケットキーを有効にしておくことをお勧めします。バケットの S3 バケットキーを無効にするには、[バケットキー] で、[無効化] を選択します。

13. (オプション) S3 Object Lock は、新しいオブジェクトが削除または上書きされないように保護するのに役立ちます。詳細については、「S3 Object Lock を使用したオブジェクトのロック」を参照してください。S3 Object Lock を有効にする場合は、次の手順に従います。

    a. [詳細設定] を選択します。

    > **Important**
    >
    > バケットに対して Object Lock を有効にすると、自動でバージョニングも有効になります。バケットを有効にして正常に作成したら、バケットの [プロパティ] タブで Object Lock のデフォルトの保持とリーガルホールドの設定も設定する必要があります。

    b. オブジェクトロックを有効にする場合は、[Enable] (有効化) を選択し、表示される警告を読んだうえで承認します。

    > **Note**
    >
    > Object Lock が有効なバケットを作成するには、`s3:CreateBucket`、`s3:PutBucketVersioning` および `s3:PutBucketObjectLockConfiguration` の許可が必要です。

14. [Create bucket] (バケットの作成) をクリックします。

Amazon S3 にバケットが作成されました。

次のステップ

オブジェクトをバケットに追加するには、「ステップ 2: バケットにオブジェクトをアップロードする」を参照してください。

ステップ 2: バケットにオブジェクトをアップロードする

Amazon S3 でバケットを作成すると、オブジェクトをバケットにアップロードする準備が整います。オブジェクトは、テキストファイル、写真、ビデオなど、どのような種類のファイルでも可能です。

> **Note**
>
> Amazon S3 Express One Zone ストレージクラスをディレクトリバケットで使用する方法の詳細については、「S3 Express One Zone」と「ディレクトリバケットの使用」を参照してください。

オブジェクトをバケットにアップロードするには

1. Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. [Buckets (バケット)] リストで、オブジェクトのアップロード先のバケットの名前を選択します。
3. バケットの [オブジェクト] タブで、[アップロード] を選択します。
4. [Files and Folders (ファイルとフォルダ)] で、[Add files (ファイルを追加)] を選択します。
5. アップロードするファイルを選択し、続いて [オープン] を選択します。
6. [アップロード] を選択します。

オブジェクトがバケットに正常にアップロードされました。

次のステップ

オブジェクトを表示するには、「ステップ 3: オブジェクトをダウンロードする」を参照してください。

ステップ 3: オブジェクトをダウンロードする

バケットにオブジェクトをアップロード後、オブジェクトに関する情報を表示し、ローカルコンピュータにそのオブジェクトをダウンロードできます。

> **Note**
>
> Amazon S3 Express One Zone ストレージクラスをディレクトリバケットで使用する方法の詳細については、「S3 Express One Zone」と「ディレクトリバケットの使用」を参照してください。

S3 コンソールの使用

このセクションでは、Amazon S3 コンソールを使用して S3 バケットからオブジェクトをダウンロードする方法について説明します。

> **Note**
>
> - 一度にダウンロードできるオブジェクトは 1 つだけです。
> - Amazon S3 コンソールを使用して、キー名がピリオド (.) で終わるオブジェクトをダウンロードすると、ダウンロードしたオブジェクトのキー名からピリオドが削除されます。ダウンロードしたオブジェクトの名前の末尾のピリオドを保持するには、AWS Command Line Interface (AWS CLI)、AWS SDK、または Amazon S3 REST API を使用する必要があります。

S3 バケットからオブジェクトをダウンロードするには

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 左のナビゲーションペインで、[汎用バケット] または [ディレクトリバケット] を選択します。
3. バケットリストで、オブジェクトのダウンロード元になるバケット名を選択します。
4. 次のいずれかの方法で、S3 バケットからオブジェクトをダウンロードできます。
   - オブジェクトの横にあるチェックボックスを選択し、[ダウンロード] を選択します。オブジェクトを特定のフォルダにダウンロードする場合は、[アクション] メニューの [名前を付けてダウンロード] を選択します。
   - オブジェクトの特定のバージョンをダウンロードする場合は、[バージョンの表示] ボタンを選択します。目的のオブジェクトのバージョンの横にあるチェックボックスをオンにして、[ダ

ウンロード] を選択します。オブジェクトを特定のフォルダにダウンロードする場合は、[アクション] メニューの [名前を付けてダウンロード] を選択します。

オブジェクトが正常にダウンロードされました。

次のステップ

Amazon S3 内でオブジェクトをコピーして貼り付ける方法については、「ステップ 4: オブジェクトをフォルダにコピーする」を参照してください。

ステップ 4: オブジェクトをフォルダにコピーする

バケットにオブジェクトを追加し、そのオブジェクトをダウンロードできました。ここで、フォルダを作成し、オブジェクトをコピーしてフォルダに貼り付けます。

> **Note**
>
> Amazon S3 Express One Zone ストレージクラスをディレクトリバケットで使用する方法の詳細については、「S3 Express One Zone」と「ディレクトリバケットの使用」を参照してください。

オブジェクトをフォルダにコピーするには

1. [Buckets] (バケット) リストで、バケット名を選択します。
2. [Create folder] (フォルダの作成) を選択して、新しいフォルダを設定します。
   a. フォルダ名 (`favorite-pics` など) を入力します。
   b. 暗号化設定フォルダでは、[Disable] (無効) を選択します。
   c. [Save] (保存) を選択します。
3. コピーするオブジェクトを含む Amazon S3 バケットまたはフォルダに移動します。
4. コピーするオブジェクトの名前の左にあるチェックボックスをオンにします。
5. [Actions (アクション)] を選択し、表示されるオプションのリストから [Copy (コピー)] を選択します。

   または、右上のオプションから [Copy (コピー)] を選択します。
6. コピー先フォルダを選択します。

a. [S3 を参照] を選択します。

b. フォルダ名の左にあるオプションボタンを選択します。

フォルダ内に移動し、コピー先としてサブフォルダを選択するには、フォルダ名を選択します。

c. [コピー先の選択] を選択します。

コピー先フォルダへのパスが [コピー先] ボックスに表示されます。[コピー先] には、s3://*bucket-name*/*folder-name*/ などコピー先のパスを入力してもかまいません。

7. 右下の [コピー] を選択します。

Amazon S3 によってオブジェクトが送信先フォルダにコピーされます。

次のステップ

Amazon S3 でオブジェクトとバケットを削除するときは、「ステップ 5: オブジェクトとバケットを削除する」を参照してください。

ステップ 5: オブジェクトとバケットを削除する

オブジェクトまたはバケットが不要になった場合は、それ以上の料金が発生しないように、オブジェクトまたはバケットを削除することをお勧めします。この開始方法のチュートリアルを演習として完了し、バケットまたはオブジェクトを使用する予定がないときは、料金が発生しないようにするため、バケットを削除することをお勧めします。

バケットを削除する前に、バケットを空にするか、バケット内のオブジェクトを削除します。オブジェクトとバケットを削除すると、それらは使用できなくなります。

引き続き同じバケット名を使用したいときは、オブジェクトを削除するか、バケットを空にすることをお勧めします。ただし、バケットは削除しないでください。バケットを削除すると、その名前は再利用できるようになります。ただし、バケットを再利用する前に、別の AWS アカウント で同じ名前のバケットが作成される可能性があります。

> **Note**
>
> Amazon S3 Express One Zone ストレージクラスをディレクトリバケットで使用する方法の詳細については、「S3 Express One Zone」と「ディレクトリバケットの使用」を参照してください。

トピック

- オブジェクトの削除
- バケットを空にする
- バケットの削除

オブジェクトの削除

バケットからすべてのオブジェクトを空にせずに、削除するオブジェクトを選択する場合は、オブジェクトを削除できます。

1. [Buckets (バケット)] リストで、オブジェクトを削除するバケットの名前を選択します。
2. 削除するオブジェクトを選択します。
3. または、右上のオプションから [削除] を選択します。
4. [オブジェクトの削除] ページで、**delete** を入力して、オブジェクトの削除を確認します。
5. [オブジェクトの削除] を選択します。

バケットを空にする

バケットを削除する場合は、まずバケットを空にする必要があります。これにより、バケット内のすべてのオブジェクトが削除されます。

バケットを空にするには

1. [Buckets (バケット)] リストで、空にするバケットを選択し、[Empty (空にする)] を選択します。
2. バケットを空にして、バケット内のすべてのオブジェクトを削除することを確認するには、[Empty bucket] (バケットを空にする) で **permanently delete** を入力します。

> **Important**
>
> バケットを空にすると、元に戻すことはできません。バケットを空にするアクションの実行中にバケットに追加されたオブジェクトは削除されます。

3. バケットを空にしてバケット内のすべてのオブジェクトを削除するには、[Empty (空にする)] を選択します。

   [Empty bucket: Status (バケットを空にする: ステータス)] ページが開き、失敗したオブジェクトの削除と成功したオブジェクトの削除の概要を確認できます。
4. バケットリストに戻るには、[Exit (終了)] を選択します。

バケットの削除

バケットを空にするか、バケットからすべてのオブジェクトを削除した後、バケットを削除できます。

1. バケットを削除するには、[Buckets (バケット)] リストでバケットを選択します。
2. [削除] を選択します。
3. 削除を確認するには、[Delete bucket](バケットの削除) でバケットの名前を入力します。

> **Important**
>
> バケットを削除すると、元に戻すことはできません。バケット名は一意です。バケットを削除すると、別の AWS ユーザーがその名前を使用できます。同じバケット名を引き続き使用する場合は、バケットを削除しないでください。代わりに、バケットを空にして保管しておきます。

4. バケットを削除するには、[Delete bucket (バケットの削除)] を選択します。

次のステップ

上記の例で、いくつかの基本的な Amazon S3 のタスクをどのように実行するかを学びました。

次のトピックでは、Amazon S3 をより深く理解して、アプリケーションに実装できるようにするために使用できるラーニングパスについて説明します。

> **Note**
>
> Amazon S3 Express One Zone ストレージクラスをディレクトリバケットで使用する方法の詳細については、「S3 Express One Zone」と「ディレクトリバケットの使用」を参照してください。

トピック

- 一般的なユースケースを理解する
- バケットとオブジェクトへのアクセスをコントロール
- ストレージの保護とモニタリング
- Amazon S3 を使用した開発
- チュートリアルから学ぶ
- トレーニングとサポートを見る

一般的なユースケースを理解する

Amazon S3 を使用して、お客様固有のユースケースをサポートすることができます。AWSソリューションライブラリおよびAWS ブログは、ユースケース固有の情報とチュートリアルを提供します。Amazon S3 の一般的ユースケースは以下のとおりです。

- バックアップおよびストレージ – Amazon S3 の ストレージ管理機能を使用して、コストの管理、規制要件への対応、レイテンシーの短縮、コンプライアンス要件のためのデータの複数の異なるコピーの保存を行います。
- アプリケーションホスティング – 信頼性と拡張性が高く、低コストのウェブアプリケーションをデプロイ、インストール、管理できます。例えば、静的ウェブサイトホスティング用に Amazon S3 バケット を設定することができます。詳細については、「Amazon S3 を使用して静的ウェブサイトをホスティングする」を参照してください。
- メディアホスティング – 動画、写真、音楽のアップロードとダウンロードをホスティングし、高い可用性を備えるインフラストラクチャを構築します。
- ソフトウェア配信 – 顧客がダウンロードできるソフトウェアアプリケーションをホスティングします。

バケットとオブジェクトへのアクセスをコントロール

Amazon S3 には、さまざまなセキュリティ機能とツールが用意されています。概要については、「Amazon S3 でのアクセスコントロール」を参照してください。

デフォルトでは、S3 バケットとオブジェクトはプライベートです。作成した S3 リソースにのみアクセスできます。以下の機能を使用して、特定のユースケースをサポートする詳細なリソース許可を付与したり、Amazon S3 リソースの許可を監査したりできます。

- S3 パブリックアクセスをブロック – S3 バケットおよびオブジェクトへのパブリックアクセスをブロックします。デフォルトでは、[パブリックアクセスをブロック] 設定はバケットレベルで有効になっています。
- AWS Identity and Access Management (IAM) ID — IAM または AWS IAM Identity Center を使用して AWS アカウントで IAM ID を作成し、Amazon S3 のリソースへのアクセスを管理します。例えば、Amazon S3 で IAM を使用して、AWS アカウント が所有する Amazon S3 バケットの特定の部分に対するユーザーまたはユーザーグループのアクセス権のタイプをコントロールすることができます。IAM ID およびベストプラクティスの詳細については、IAM ユーザーガイドの「IAM ID (ユーザー、ユーザーグループ、ロール)」を参照してください。
- バケットポリシー – IAM ベースのポリシー言語を使用して、S3 バケットとその中のオブジェクトに対するリソースベースの許可を設定します。
- アクセスコントロールリスト (ACL) – 個々のバケットおよびオブジェクトに対する読み取りおよび書き込みの許可を、承認されたユーザーに付与します。原則として、アクセスコントロールには ACL ではなく S3 リソースベースのポリシー (バケットポリシーとアクセスポイントポリシー) または IAM ユーザーポリシーを使用することをお勧めします。ポリシーとは、よりシンプルで柔軟なアクセス制御のオプションです。バケットポリシーとアクセスポイントポリシーを使用すると、Amazon S3 リソースに対するすべてのリクエストに広く適用されるルールを定義できます。リソースベースのポリシーまたは IAM ユーザーポリシーの代わりに ACL を使用する場合の特定のケースの詳細については、「Amazon S3 用 Identity and Access Management」を参照してください。
- S3 オブジェクト所有権 - バケット内のすべてのオブジェクトの所有権を取得し、Amazon S3 に保存されているデータのアクセス管理を簡素化します。S3 オブジェクト所有権は、Amazon S3 バケットレベルの設定で、ACL を無効または有効にするのに使用できます。デフォルトでは、ACL は無効になっています。ACL を無効にすると、バケット所有者はバケット内のすべてのオブジェクトを所有し、アクセス管理ポリシーのみを使用してデータへのアクセスを管理します。
- IAM Access Analyzer for S3 – S3 バケットアクセスポリシーを評価およびモニタリングし、ポリシーが S3 リソースへの意図したアクセスのみを提供することを確認します。

ストレージの保護とモニタリング

- ストレージの保護 – Amazon S3 でバケットを作成してオブジェクトをアップロードすると、オブジェクトストレージを保護できるようになります。例えば、ディザスタリカバリには S3 バージョニング、S3 レプリケーション、マルチリージョンアクセスポイントのフェイルオーバーコントロールを使用し、データのバックアップには AWS Backup を使用し、保持期間の設定、削除や上書きの防止、コンプライアンス要件への準拠には S3 Object Lock を使用できます。
- ストレージのモニタリング – モニタリングは、Amazon S3 および AWS ソリューションの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。ストレージのアクティビティとコストを監視できます。また、マルチポイント障害が発生した場合は、その障害をより簡単にデバッグできるように、AWS ソリューションのすべての部分からモニタリングデータを収集することをお勧めします。

  また、Amazon S3 の分析とインサイトを使用して、ストレージの使用状況を把握、分析、最適化することができます。例えば、Amazon S3 Storage Lens を使用して、ストレージの把握、分析、最適化を行います。S3 Storage Lens には、組織全体、特定のアカウント、リージョン、バケット、またはプレフィックスのデータを集約するための 29 以上の使用状況およびアクティビティに関するメトリクスとインタラクティブなダッシュボードが用意されています。ストレージクラス分析を使用してストレージアクセスパターンを分析し、データをよりコスト効率の高いストレージクラスに移動するタイミングを決定します。コストを管理するには、S3 ライフサイクルを使用できます。

Amazon S3 を使用した開発

Amazon S3 は REST サービスです。REST API または、基礎となる Amazon S3 REST API をラップする AWS SDK ライブラリを使用して、Amazon S3 にリクエストを送信できます。これにより、プログラミング作業が簡易になります。また、AWS Command Line Interface (AWS CLI) を使用して、Amazon S3 API 呼び出しを行います。詳細については、「Amazon S3 API リファレンス」の「リクエストの実行」を参照してください。

Amazon S3 REST API は、Amazon S3 に対する HTTP インターフェイスです。REST API を使用すると、標準 HTTP リクエストを使用してバケットとオブジェクトを作成、取得、および削除することができます。REST API を使用する場合、HTTP をサポートする任意のツールキットを使用できます。匿名で読み取り可能なオブジェクトであれば、ブラウザを使用して取得することもできます。詳細については、「Amazon S3 API リファレンス」の「Amazon S3 での開発」を参照してください。

お客様が選択した言語を使用してアプリケーションを構築できるよう、以下のリソースを提供しています。

AWS CLI

AWS CLI を使用して、Amazon S3 の機能にアクセスできます。AWS CLI をダウンロードして設定するには、「Amazon S3 API リファレンス」の「AWS CLI を使用した Amazon S3 での開発」を参照してください。

AWS CLI は Amazon S3 にアクセスするための 2 つの階層のコマンドとして、高レベル (s3) コマンドと APIレベル (s3api および `s3control`) コマンドを提供しています。高レベル S3 コマンドは、オブジェクトおよびバケットの作成、操作、削除など、一般的なタスクの実行を簡素化します。s3api および s3control コマンドは、すべての Amazon S3 API オペレーションへの直接アクセスを提供します。これにより、高レベルコマンドだけでは不可能なアドバンスドオペレーションを実行することができます。

Amazon S3 AWS CLI コマンドのリストについては、s3、s3api、および s3control を参照してください。

AWS SDK と Explorer

Amazon S3 でのアプリケーション開発に AWS SDK を使用できます。AWS SDK は、基盤となる REST API をラップして、プログラミング作業を簡素化します。AWS を使用して、接続されるモバイルおよびウェブアプリケーションを構築するために、AWS Mobile SDK と Amplify JavaScript ライブラリも用意されています。

AWS SDK に加え、Visual Studio および Eclipse for Java IDE で使用できる AWS Explorer も提供されています。この場合、SDK と Explorer が、AWS ツールキットとしてバンドルされて提供されます。

詳細については、「Amazon S3 API リファレンス」の「AWS SDK を使用した Amazon S3 での開発」を参照してください。

サンプルコードおよびライブラリ

AWS デベロッパーセンターおよびAWS サンプルコードカタログには、Amazon S3 用に特別に作成されたサンプルコードとライブラリが用意されています。これらのサンプルコードを、Amazon S3 API の実装方法を理解する教材としてご利用いただけます。また、Amazon Simple Storage Service API リファレンスを参照して、Amazon S3 API オペレーションについて詳しく理解してください。

チュートリアルから学ぶ

ステップバイステップのチュートリアルを開始して、Amazon S3 の詳細について学びます。これらのチュートリアルはラボ型環境向けであり、架空の企業名やユーザー名などを使用しています。目的は、一般的なガイダンスを提供することです。お客様の組織環境に固有のニーズを満たすかどうかの十分な確認や調整をすることなく、本番環境で直接使用するためのものではありません。

入門

- チュートリアル: Amazon S3 によるファイルの保存と取得
- チュートリアル: S3 Intelligent-Tiering を使用した開始方法
- チュートリアル: Amazon S3 Glacier ストレージクラスを使用した開始方法

ストレージコストの最適化

- チュートリアル: S3 Intelligent-Tiering を使用した開始方法
- チュートリアル: Amazon S3 Glacier ストレージクラスを使用した開始方法
- チュートリアル: S3 ストレージレンズによるコストの最適化と使用状況の可視化

ストレージの管理

- チュートリアル: Amazon S3 マルチリージョンアクセスポイントの使用の開始方法
- チュートリアル: S3 バッチレプリケーションによる Amazon S3 バケット内の既存のオブジェクトのレプリケーション

動画とウェブサイトのホスティング

- チュートリアル: Amazon S3、Amazon CloudFront、Amazon Route 53 を使用したオンデマンドストリーミング動画のホスティング。
- チュートリアル: Amazon S3 での静的ウェブサイトの設定
- チュートリアル: Route 53 に登録されたカスタムドメインを使用した静的ウェブサイトの設定

データの処理

- チュートリアル: S3 Object Lambda を使用したアプリケーションのデータの変換

- チュートリアル: S3 Object Lambda と Amazon Comprehend を使用した PII データの検出と編集
- チュートリアル: S3 Object Lambda を使用して、取得時に画像に動的に透かしを入れる
- チュートリアル: S3 バッチオペレーションを使用した動画のバッチトランスコーディング

データの保護

- チュートリアル: チェックサムを追加して Amazon S3 のデータの整合性をチェックする
- チュートリアル: S3 レプリケーションを使用して AWS リージョン内およびリージョン間でデータをレプリケートする
- チュートリアル: S3 バージョニング、S3 オブジェクトロック、S3 レプリケーションを使用して、Amazon S3 上のデータを予期しない削除やアプリケーションのバグから保護する
- チュートリアル: S3 バッチレプリケーションによる Amazon S3 バケット内の既存のオブジェクトのレプリケーション

トレーニングとサポートを見る

AWS のエキスパートから学び、スキルを向上させ、目的を達成するために エキスパートの支援を受けることができます。

- トレーニング – トレーニングリソースは、Amazon S3 を学習するための実践的なアプローチです。詳細については、「AWS トレーニングと認定」および「AWS オンラインテクニカルトーク」を参照してください。
- ディスカッションフォーラム – フォーラムでは、投稿を確認して、Amazon S3 で何ができるのか、何ができないのかを理解することができます。質問を投稿することもできます。詳細については、「ディスカッションフォーラム」を参照してください。
- 技術サポート – さらにご質問がある場合は、技術サポートまでご連絡ください。

Amazon S3 汎用バケットの作成、設定、操作

Amazon S3 にデータを保存するには、バケットおよびオブジェクトと呼ばれるリソースを使用します。バケット とは、オブジェクトのコンテナのことです。オブジェクト とは、ファイルと、そのファイルを記述している任意のメタデータのことです。

Amazon S3 にオブジェクトを保存するには、バケットを作成してから、オブジェクトをバケットにアップロードします。オブジェクトがバケットの中にあるときは、オブジェクトを開き、ダウンロードして、移動させます。オブジェクトまたはバケットが不要になったら、リソースをクリーンアップします。

このセクションのトピックでは、Amazon S3 の汎用バケットの使用について概要を示します。汎用バケットの命名、作成、アクセス、削除について説明します。バケット内でのオブジェクトの表示および一覧表示について詳しくは、オブジェクトの整理、リスト化、使用 を参照してください。

Amazon S3 バケットにはいくつかのタイプがあります。バケットを作成する前に、アプリケーションとパフォーマンス要件に最適なバケットタイプを選択していることを確認します。さまざまなバケットタイプとそれぞれの適切なユースケースの詳細については、「バケット」を参照してください。

> **Note**
>
> Amazon S3 Express One Zone ストレージクラスをディレクトリバケットで使用する方法の詳細については、「S3 Express One Zone」と「ディレクトリバケットの使用」を参照してください。

> **Note**
>
> Amazon S3 では、お支払いは実際に使用した分のみです。Amazon S3 の機能と料金の詳細については、「Amazon S3」を参照してください。Amazon S3 の新規のお客様は、Amazon S3 を無料で使い始めることができます。詳細については、AWS 無料利用枠 を参照してください。

トピック

- 汎用バケットの概要

- Amazon S3 でアプリケーションを構築するための一般的な汎用バケットパターン
- 汎用バケットの命名規則
- 汎用バケットのクォータ、制限、制約
- Amazon S3 汎用バケットへのアクセス
- 汎用バケットの作成
- S3 汎用バケットのプロパティの表示
- Amazon S3 汎用バケットの一覧表示
- 汎用バケットを空にする
- 汎用バケットの削除
- Amazon S3 バケットをローカルファイルシステムとしてマウントする
- Storage Browser for Amazon S3 の使用
- Amazon S3 Transfer Acceleration を使用した高速かつ安全なファイル転送の設定
- ストレージの転送と使用にリクエスタ支払い汎用バケットを使用する

汎用バケットの概要

Amazon S3 にデータ (写真、動画、ドキュメントなど) をアップロードするには、いずれかの AWS リージョン に S3 バケットを作成する必要があります。

Amazon S3 バケットにはいくつかのタイプがあります。バケットを作成する前に、アプリケーションとパフォーマンス要件に最適なバケットタイプを選択していることを確認します。さまざまなバケットタイプとそれぞれの適切なユースケースの詳細については、「バケット」を参照してください。

以下のセクションでは、バケットの命名規則、クォータ、バケット設定の詳細など、汎用バケットに関する詳細情報を提供します。Amazon S3 バケットに関連する制約と制限のリストについては、「汎用バケットのクォータ、制限、制約」を参照してください。

トピック

- 汎用バケットの概要
- 一般的な汎用バケットパターン
- アクセス許可
- 汎用バケットのパブリックアクセスの管理
- 汎用バケットの設定オプション

- 汎用バケットのオペレーション
- 汎用バケットのパフォーマンスモニタリング

汎用バケットの概要

すべてのオブジェクトはバケット内に保存されます。例えば、photos/puppy.jpg という名前のオブジェクトが米国西部 (オレゴン) リージョンの amzn-s3-demo-bucket 汎用バケットに保存されている場合、URL https://amzn-s3-demo-bucket.s3.us-west-2.amazonaws.com/photos/puppy.jpg を使用してアドレス可能です。詳細については、「バケットへのアクセス」を参照してください。

- 商用リージョンの汎用バケットクォータは、米国東部 (バージニア北部) からのみ表示および管理できます。
- AWS GovCloud (US) の汎用バケットクォータは、AWS GovCloud (米国西部) からのみ表示および管理できます。

実装の面では、バケットとオブジェクトは AWS リソースであり、Amazon S3 はバケットやオブジェクトを管理するための API を提供します。たとえば、Amazon S3 API を使用してバケットの作成やオブジェクトのアップロードを行うことができます。これらの操作は Amazon S3 コンソールを使用して実行することもできます。コンソールは、Amazon S3 API を使用して Amazon S3 にリクエストを送信します。

このセクションでは、汎用バケットの使用方法について説明します。オブジェクトの操作方法の詳細については、Amazon S3 オブジェクトの概要 を参照してください。

Amazon S3 はグローバル汎用バケットをサポートしています。つまり、各バケット名は、パーティション内のすべての AWS リージョンのすべての AWS アカウントにわたって一意である必要があります。パーティションは、リージョンのグループです。AWS には、現在、aws (標準リージョン)、aws-cn (中国リージョン)、および aws-us-gov (AWS GovCloud (US)) の 3 つのパーティションがあります。

汎用バケットの作成後は、バケットを削除するまで、同じパーティションの別の AWS アカウントでそのバケットの名前を使用することはできません。可用性やセキュリティ検証の目的で、特定のバケット命名規則に依存しないでください。バケットの命名のガイドラインについては、汎用バケットの命名規則 を参照してください。

Amazon S3 は、指定したリージョンでバケットを作成します。レイテンシーを減らしてコストを最小化し、規制要件に対応するには、地理的に近い AWS リージョン を選択します。たとえば、ヨー

ロッパにお住まいの場合は、欧州 (アイルランド) または欧州 (フランクフルト) リージョンにバケットを作成するとよいでしょう。Amazon S3 のリージョンの一覧については、AWS 全般のリファレンスのリージョンとエンドポイントを参照してください。

> **Note**
>
> 特定の AWS リージョン に作成したバケットに属するオブジェクトは、お客様が明示的に他のリージョンに転送しない限り、そのリージョンから移動しません。たとえば、欧州 (アイルランド) リージョンに保存されているオブジェクトは、ずっとそのリージョンに置かれたままです。

一般的な汎用バケットパターン

Amazon S3 でアプリケーションを構築する場合、一意の汎用バケットを使用して、異なるデータセット間やワークロード間を分離できます。ユースケースに応じて、汎用バケットを使用するためのさまざまな設計パターンやベストプラクティスがあります。詳細については、「Amazon S3 でアプリケーションを構築するための一般的な汎用バケットパターン」を参照してください。

アクセス許可

AWS アカウントのルートユーザー の認証情報を使用して、汎用バケットを作成したり、その他の Amazon S3 オペレーションを実行したりできます。ただし、バケット作成などのリクエストを行う目的で AWS アカウント のルートユーザーの認証情報を使用しないことをお勧めします。代わりに、AWS Identity and Access Management (IAM) ユーザーを作成し、そのユーザーにフルアクセスを許可します (デフォルトではユーザーにアクセス許可はありません)。

これらのユーザーは、管理者と呼ばれます。アカウントのルートユーザーの認証情報ではなく、管理者ユーザーの認証情報を使用して、AWS を操作し、バケットの作成、ユーザーの作成、および許可の付与などのタスクを実行できます。

詳細については、AWS 全般のリファレンスの「AWS アカウントのルートユーザー認証情報と IAM ユーザー認証情報」と IAM ユーザーガイドの「IAM でのセキュリティのベストプラクティス」を参照してください。

リソースを作成する AWS アカウント は、そのリソースを所有しています。例えば、AWS アカウント に IAM ユーザーを作成し、そのユーザーにバケットを作成する許可を付与すると、ユーザーはバケットを作成できます。しかし、ユーザーはバケットを所有していません。ユーザーが属す

る AWS アカウント がバケットを所有しています。ユーザーがその他のバケットオペレーションを実行するには、リソース所有者から追加のアクセス許可を取得する必要があります。Amazon S3 リソースのアクセス許可を管理する方法の詳細については、「Amazon S3 用 Identity and Access Management」を参照してください。

汎用バケットのパブリックアクセスの管理

汎用バケットおよびオブジェクトへのパブリックアクセスは、アクセスコントロールリスト (ACL)、バケットポリシー、またはその両方を通じて付与されます。Amazon S3 には、パブリックアクセスをブロックする設定があり、Amazon S3 リソースへのパブリックアクセスを管理するのに役立ちます。Amazon S3 Block Public Access 設定では ACL およびバケットポリシーを上書きできるため、これらのリソースへのパブリックアクセスに均一な制限を適用できます。Block Public Access 設定は、個々のバケットまたはアカウント内のすべてのバケットに適用できます。

すべての Amazon S3 汎用バケットとオブジェクトへのパブリックアクセスを確実にブロックするために、バケットの新規作成時に、4 つすべてのブロックパブリックアクセス設定がデフォルトで有効になります。アカウントに対して [パブリックアクセスをブロック] の 4 つの設定をすべてオンにすることをお勧めします。これらの設定によって、現在および将来のバケットのパブリックアクセスはすべてブロックされます。

これらの設定を適用する前に、アプリケーションがパブリックアクセスなしで正しく動作することを確認してください。「Amazon S3 を使用して静的ウェブサイトをホスティングする」に示す静的なウェブサイトをホストする場合など、バケットやオブジェクトにある程度のパブリックアクセスが必要な場合は、ストレージのユースケースに合わせて個別に設定をカスタマイズできます。詳細については、「Amazon S3 ストレージへのパブリックアクセスのブロック」を参照してください。

ただし、[パブリックアクセスをブロック] 設定は、有効にしておくことを強くお勧めします。4 つすべての [パブリックアクセスをブロック] 設定を有効にしたまま、静的ウェブサイトをホストする場合は、Amazon CloudFront のオリジンアクセスコントロール (OAC) を使用できます。Amazon CloudFront は、セキュアな静的ウェブサイトをセットアップするために必要な機能を提供します。Amazon S3 静的ウェブサイトは、HTTP エンドポイントのみをサポートしています。Amazon CloudFront は、耐久性に優れた Amazon S3 のあるストレージを使用し、HTTPS などの、追加のセキュリティヘッダーを提供します。HTTPS では、通常の HTTP リクエストを暗号化し、一般的なサイバー攻撃から保護することで、セキュリティが強化されます。

詳細については、「Amazon CloudFront デベロッパーガイド」の「安全な静的ウェブサイトの使用開始」を参照してください。

> **Note**
>
> 汎用バケットとそのパブリックアクセス設定を一覧表示するときに Error が表示された場合は、必要なアクセス許可を持っていない可能性があります。以下のアクセス許可がユーザーポリシーまたはロールポリシーに追加されていることを確認します。
>
> ```
> s3:GetAccountPublicAccessBlock
> s3:GetBucketPublicAccessBlock
> s3:GetBucketPolicyStatus
> s3:GetBucketLocation
> s3:GetBucketAcl
> s3:ListAccessPoints
> s3:ListAllMyBuckets
> ```
>
> まれに、AWS リージョンの停止が原因で、リクエストが失敗することもあります。

汎用バケットの設定オプション

Amazon S3 では、汎用バケットを設定するためのさまざまなオプションをサポートしています。たとえば、バケットをウェブサイトのホスティング用に設定する、バケット内のオブジェクトのライフサイクルを管理するための設定を追加する、およびバケットへのアクセスをすべて記録するようにバケットを設定することができます。Amazon S3 では、バケットの設定情報を保存および管理するためのサブリソースをサポートしています。Amazon S3 API を使用して、これらのサブリソースを作成および管理できます。ただし、コンソールや AWS SDK を使用することもできます。

> **Note**
>
> また、オブジェクトレベルの設定もあります。たとえば、オブジェクトに固有のアクセスコントロールリスト (ACL) を設定することによって、オブジェクトレベルのアクセス許可を設定できます。

これらは、特定のバケットやオブジェクトのコンテキストに存在するため、サブリソースと呼ばれます。次の表に、バケット固有の設定を管理するためのサブリソースのリストを示します。

サブリソース	説明
cors (Cross-Origin Resource Sharing)	クロスオリジンリクエストを許可するようにバケットを設定できます。 詳細については、「Cross-Origin Resource Sharing (CORS) の使用」を参照してください。
イベントの通知	指定したバケットイベントの通知を送信するようにバケットを設定できます。 詳細については、「Amazon S3 イベント通知」を参照してください。
ライフサイクル	バケットのライフサイクルが明確に定義されていれば、バケット内のオブジェクトのライフサイクルルールを定義できます。たとえば、作成されてから 1 年後にオブジェクトアーカイブする、作成されてから 10 年後にオブジェクトを削除するなどのルールを定義できます。 詳細については、「オブジェクトのライフサイクルの管理」を参照してください。
location	バケットを作成するときには、Amazon S3 でバケットを作成する AWS リージョン を指定します。Amazon S3 では、この情報を location サブリソースに格納し、この情報を取得するための API をお客様に提供します。
logging	ログ記録によって、バケットへのアクセスのリクエストを追跡できます。各アクセスログレコードには、1 つのアクセスリクエストに関する詳細が含まれます。内容は、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、応答ステータス、およびエラーコード (存在する場合) です。アクセスログ情報は、セキュリティとアクセス監査に役立ちます。また、顧客基盤について知り、Amazon S3 の請求を理解することにも役立ちます。 詳細については、「サーバーアクセスログによるリクエストのログ記録」を参照してください。
オブジェクトのロック	S3 のオブジェクトのロックを使用するには、バケットに対して有効にする必要があります。オプションで、バケットに配置された新しいオブジェクトに適用されるデフォルトのリテンションモードと期間を設定することもできます。

サブリソース	説明
	詳細については、「S3 Object Lock を使用したオブジェクトのロック」を参照してください。
policy および ACL (アクセスコントロールリスト)	すべてのリソース (バケットやオブジェクトなど) はデフォルトではプライベートです。Amazon S3 では、バケットレベルのアクセス許可を付与および管理するために、バケットポリシーおよびアクセスコントロールリスト (ACL)の両方のオプションをサポートしています。Amazon S3 では、policy および acl サブリソースにアクセス許可情報を格納します。 詳細については、「Amazon S3 用 Identity and Access Management」を参照してください。
レプリケーション	レプリケーションは、同一または異なる AWS リージョン にあるバケット間でオブジェクトを自動的に非同期コピーする機能です。詳細については、「リージョン内およびリージョン間でのオブジェクトのレプリケート」を参照してください。
requestPayment	デフォルトでは、バケットを作成した AWS アカウント (バケット所有者) に、バケットからのダウンロードの料金をお支払いいただきます。バケット所有者は、このサブリソースを使用して、ダウンロードをリクエストするユーザーにダウンロードの料金が課金されるように指定できます。Amazon S3 では、このサブリソースを管理するための API も利用できます。 詳細については、「ストレージの転送と使用にリクエスタ支払い汎用バケットを使用する」を参照してください。
タグ付け	バケットにコスト配分タグを追加して、AWS コストを分類して追跡できます。Amazon S3 では、バケットのタグを保存、管理するために、tagging サブリソースを提供しています。タグを使用してバケットに適用すると、AWS によって、使用量とコストがタグごとに集計されたコスト配分レポートが生成されます。 詳細については、「Amazon S3 の請求および使用状況レポート」を参照してください。

サブリソース	説明
Transfer Acceleration	Transfer Acceleration を使用すると、クライアントと S3 バケットの間で、長距離にわたるファイル転送を高速、簡単、安全に行えるようになります。Transfer Acceleration は、Amazon CloudFront の世界中に点在するエッジロケーションを利用します。 詳細については、「Amazon S3 Transfer Acceleration を使用した高速かつ安全なファイル転送の設定」を参照してください。
バージョニング	バージョニングは、誤って上書き、削除した場合の回復に役立ちます。 誤って削除または上書きされたオブジェクトを回復するためのベストプラクティスとしてバージョニングをお勧めします。 詳細については、「S3 バージョニングによる複数のバージョンのオブジェクトの保持」を参照してください。
website	静的ウェブサイトホスティング用にバケットを設定できます。Amazon S3 では、website サブリソースを作成することによって、この設定を格納します。 詳細については、「Amazon S3 を使用して静的ウェブサイトをホスティングする」を参照してください。

汎用バケットのオペレーション

Amazon S3 の高可用性技術は、get、put、list、および delete オペレーションに重点を置いています。汎用バケットのオペレーションは、一元化されたグローバルリソーススペースに対して実行されるため、アプリケーションの高可用性コードパスでバケットを作成、削除、または設定しないようお勧めします。バケットの作成、削除、設定は、個別の初期化や、頻繁に実行しないセットアップルーチンで実行する方が適しています。

汎用バケットのパフォーマンスモニタリング

AWS リソースに依存する重要なアプリケーションやビジネスプロセスがある場合は、システムをモニタリングしてアラートを取得することが重要です。データのモニタリングは、Amazon S3 とお客様の AWS ソリューションの信頼性、可用性、パフォーマンスを維持するのに役立ちます。S3 バ

ケットのメトリクスとログを収集して集計するために使用できる AWS サービスがいくつかあります。

ユースケースに応じて、問題のデバッグ、データのモニタリング、ストレージコストの最適化、複数ポイントの問題のトラブルシューティングなど、組織のニーズに最適な AWS サービスを選択できます。例:

- S3 を使用するアプリケーションのパフォーマンスを向上させるには: CloudWatch アラームを設定することで、ストレージデータ、レプリケーションメトリクス、またはリクエストメトリクスをモニタリングします。
- ストレージの使用量を計画したり、ストレージコストを最適化したり、組織全体のストレージ容量を調べたりするには: Amazon S3 ストレージレンズを使用します。また、S3 ストレージレンズを使用してデータパフォーマンスを向上させることもできます。その場合は、高度なメトリクスを有効にし、詳細なステータスコードメトリクスを使用して、成功または失敗したリクエストの数を取得します。
- 運用状態の統合ビューを得るには: S3 ストレージレンズの使用状況とアクティビティのメトリクスを Amazon CloudWatch ダッシュボードに公開します。

  > **Note**
  >
  > Amazon CloudWatch 公開オプションは、アドバンストメトリクスとレコメンデーションにアップグレードされた S3 ストレージレンズダッシュボードで利用できます。S3 Storage Lens の新規または既存のダッシュボード設定に対して CloudWatch 公開オプションを有効にできます。

- ユーザー、ロール、または AWS サービスによって実行されたアクションの記録を取得するには: AWS CloudTrail ログを設定します。AWS CloudTrail ログを使用して、Amazon S3 への API コールをイベントとして確認することもできます。
- S3 バケットで特定のイベントが発生したときに通知を受け取るには: Amazon S3 イベント通知を設定します。
- S3 バケットに対して行われたリクエストの詳細なレコードを取得するには: S3 アクセスログを設定します。

データのモニタリングに使用できるさまざまな AWS サービスのリストについては、「Amazon S3 でのログ記録とモニタリング」を参照してください。

Amazon S3 でアプリケーションを構築するための一般的な汎用バケットパターン

Amazon S3 でアプリケーションを構築する場合、一意の汎用バケットを使用して、異なるデータセット間やワークロード間を分離できます。エンドユーザーやさまざまなユーザーグループに提供するアプリケーションを構築する場合は、ベストプラクティスの設計パターンを使用して、Amazon S3 の機能とスケーラビリティを最大限に活用できるアプリケーションを構築します。

> **Important**
>
> 予測不可能な汎用バケット名を作成することをお勧めします。バケットを既に作成していない限り、選択したバケット名を使用できるものと見なしてコードを記述しないでください。予測不可能なバケット名を作成する方法の 1 つは、バケット名にグローバル一意識別子 (GUID) を追加することです (例: `amzn-s3-demo-bucket-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`)。汎用バケットの命名規則の詳細については、「汎用バケットの命名規則」を参照してください。

トピック

- マルチテナント汎用バケットパターン
- 使用ごとのバケットパターン

マルチテナント汎用バケットパターン

マルチテナントバケットでは、チームまたはワークロードごとに 1 つの汎用バケットを作成します。バケットに保存するオブジェクトを整理するには、一意の S3 プレフィックスを使用します。プレフィックスは、オブジェクトキー名の先頭にある文字列です。プレフィックスには、オブジェクトキー名の最大長 (1,024 バイト) を条件として、任意の長さを指定できます。プレフィックスは、ディレクトリと同様の方法でデータを整理する方法と考えることができます。ただし、プレフィックスはディレクトリではありません。

例えば、都市に関する情報を保存するには、大陸、国、州、または都道府県の順に整理します。通常、これらの名前には句読点が含まれないため、区切り記号としてスラッシュ (/) を使用できます。以下の例では、スラッシュ (/) 区切り文字を使用して、大陸、国、州、または都道府県の順に都市名を整理するために使用しているプレフィックスを示します。

- 欧州/フランス/ヌーベルアキテーヌ/ボルドー

- 北米/カナダ/ケベック/モントリオール
- 北米/米国/ワシントン州/ベルビュー
- 北米/米国/ワシントン州/シアトル

このパターンは、汎用バケット内に数百の一意のデータセットがある場合に適切にスケールします。プレフィックスを使用すると、これらのデータセットを簡単に整理してグループ化できます。

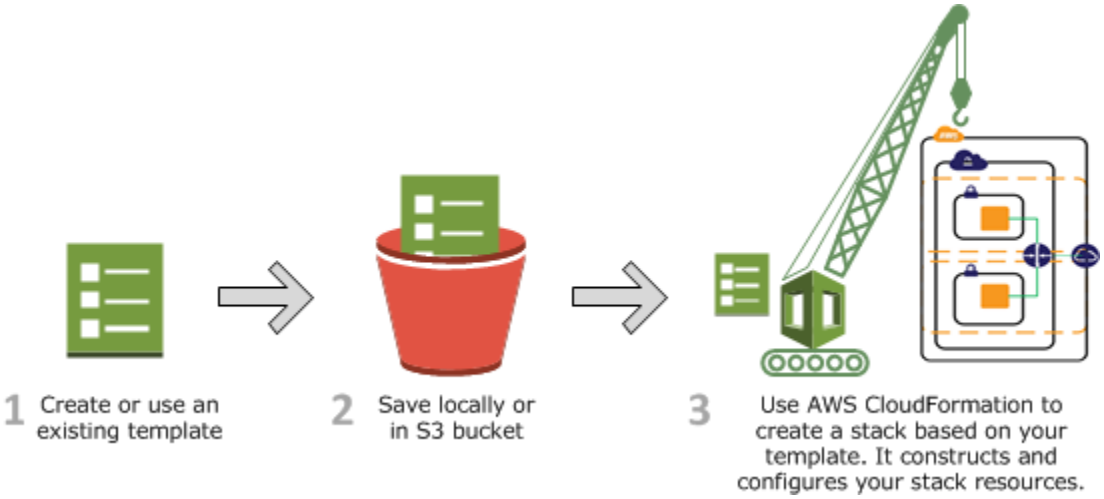
ただし、マルチテナント汎用バケットパターンの 1 つの潜在的な欠点は、デフォルトのバケット暗号化、S3 バージョニング、S3 リクエスタ支払いなど、S3 バケットレベルの多くの機能が、プレフィックスレベルではなく、バケットレベルで設定されることです。マルチテナントバケット内のデータセットごとに固有の要件がある場合、S3 バケットレベルの多くの機能をプレフィックスレベルで設定できないと、データセットごとに正しい設定を指定することが難しくなる可能性があります。さらに、マルチテナントバケットでは、特定のプレフィックスに関連付けられたストレージ、リクエスト、データ転送を理解しようとした場合に、コスト配分が複雑になる可能性があります。

使用ごとのバケットパターン

使用ごとのバケットパターンでは、個別のデータセット、エンドユーザー、またはチームごとに汎用バケットを作成します。これらのバケットごとに S3 バケットレベルの機能を設定できるため、このパターンを使用してバケットレベルの一意の設定を行うことができます。例えば、デフォルトのバケット暗号化、S3 バージョニング、S3 リクエスタ支払いなどの機能を設定する場合、各バケットのデータセットに合わせてカスタマイズできます。個別のデータセット、エンドユーザー、またはチームごとに 1 つのバケットを使用すると、アクセス管理とコスト配分戦略の両方を簡素化することもできます。

この戦略の潜在的な欠点は、数千のバケットを管理する必要があることです。すべての AWS アカウントでは、10,000 個の汎用バケットがデフォルトクォータになっています。クォータ引き上げリクエストを送信することで、アカウントのバケットクォータを増やすことができます。汎用バケットの引き上げをリクエストするには、Service Quotas コンソールにアクセスしてください。

使用ごとのバケットパターンを管理し、インフラストラクチャ管理を簡素化するには、AWS CloudFormation を使用できます。S3 汎用バケットに必要なすべての設定が定義済みであるパターン用のカスタム AWS CloudFormation テンプレートを作成すると、インフラストラクチャへの変更を簡単にデプロイして追跡できます。詳細については、「AWS CloudFormation ユーザーガイド」の「AWS::S3::Bucket」を参照してください。



汎用バケットの命名規則

汎用バケットを作成するときは、バケット名の長さ、有効な文字、形式、一意性を考慮してください。以下のセクションでは、命名規則やベストプラクティスなどの汎用バケットの命名に関する情報を提供し、グローバル一意識別子 (GUID) を含む名前を使用して汎用バケットを作成する例を示します。

オブジェクトキー名の詳細については、「オブジェクトキー名の作成」を参照してください。

汎用バケットを作成する方法については、「the section called “汎用バケットの作成”」を参照してください。

トピック

- 汎用バケットの命名規則
- 汎用バケット名の例
- ベストプラクティス
- バケット名で GUID を使用するバケットの作成

汎用バケットの命名規則

汎用バケットの命名については、次の命名規則が適用されます。

- バケット名は 3 (最少) ~ 63 (最大) 文字の長さにする必要があります。
- バケット名は、小文字、数字、ピリオド (.)、およびハイフン (-) のみで構成できます。
- バケット名は、文字または数字で開始および終了する必要があります。

- バケット名には、連続する 2 つのピリオドを含めることはできません。
- バケット名は IP アドレスの形式 (192.168.5.4 など) にはできません。
- バケット名のプレフィックスは xn-- で始まってはいけません。
- バケット名のプレフィックスは sthree- で始まってはいけません。
- バケット名のプレフィックスは amzn-s3-demo- で始まってはいけません。
- バケット名のサフィックスは -s3alias で終わってはいけません。このサフィックスは、アクセスポイントのエイリアス名用に予約されています。詳細については、「汎用バケットのアクセスポイントのエイリアス」を参照してください。
- バケット名のサフィックスは --ol-s3 で終わってはいけません。このサフィックスは、Object Lambda アクセスポイントのエイリアス名用に予約されています。詳細については、「S3 バケット Object Lambda アクセスポイントでのバケット形式のエイリアスの使用方法」を参照してください。
- バケット名のサフィックスは .mrap で終わってはいけません。このサフィックスは、マルチリージョンアクセスポイント名用に予約されています。詳細については、「Amazon S3 マルチリージョンアクセスポイントの命名規則」を参照してください。
- バケット名のサフィックスは --x-s3 で終わってはいけません。このサフィックスはディレクトリバケット用に予約されています。詳細については、「ディレクトリバケットの命名規則」を参照してください。
- バケット名のサフィックスは --table-s3 で終わってはいけません。このサフィックスは S3 Tables バケット用に予約されています。詳細については、「Amazon S3 テーブルバケット、テーブル、および名前空間の命名規則」を参照してください。
- Amazon S3 Transfer Acceleration で使用されるバケットの名前にピリオド (.) を使用することはできません。Transfer Acceleration の詳細については、「Amazon S3 Transfer Acceleration を使用した高速かつ安全なファイル転送の設定」を参照してください。

> **Important**
>
> - バケット名は、パーティション内のすべての AWS リージョンのすべての AWS アカウント全体で一意である必要があります。パーティションは、リージョンのグループです。AWS には、現在 aws (商用リージョン)、aws-cn (中国リージョン)、および aws-us-gov (AWS GovCloud (US) リージョン) の 3 つのパーティションがあります。
> - バケットが削除されるまで、バケット名を同じパーティション内の別の AWS アカウントで使用することはできません。バケットを削除した後、同じパーティション内にある別

の AWS アカウントが新しいバケットに同じバケット名を使用できるため、削除されたバケット宛てのリクエストを受け取る可能性があることに注意してください。これを防ぐ場合、または同じバケット名を使い続ける場合は、バケットを削除しないでください。バケットを空にして保持し、代わりに必要に応じてバケットリクエストをブロックすることをお勧めします。バケットがアクティブに使用されなくなった場合は、バケット自体を保持しながらコストを最小限に抑えるために、すべてのオブジェクトのバケットを空にすることをお勧めします。

- 汎用バケットの作成時にバケットの名前と作成先の AWS リージョンを選択します。汎用バケットの作成後は、バケットの名前もリージョンも変更できません。
- バケット名に機密情報を含めないでください。バケット名は、バケット内のオブジェクトを参照する URL に表示されます。

> **Note**
>
> 2018 年 3 月 1 日までは、米国東部 (バージニア北部) リージョンで作成したバケットの名前として最大 255 文字を使用し、大文字とアンダースコアを含めることができました。2018 年 3 月 1 日以降、米国東部 (バージニア北部) の新しいバケットは、他のすべてのリージョンに適用されている同じルールに準拠する必要があります。

汎用バケット名の例

次のバケット名は、汎用バケット名で許可される文字の例を示しています: a ~ z、0 ~ 9、およびハイフン (-)。amzn-s3-demo- 予約済みプレフィックスは、ここでは説明のためにのみ使用されます。予約済みプレフィックスであるため、amzn-s3-demo- で始まるバケット名を作成することはできません。

- `amzn-s3-demo-bucket1-a1b2c3d4-5678-90ab-cdef-example11111`
- `amzn-s3-demo-bucket`

次の例に示すバケット名は有効ですが、ピリオドを含んでいるため (.)、静的ウェブサイトホスティング以外の用途には推奨されません。

- `example.com`
- `www.example.com`

- my.example.s3.bucket

次の例に示すバケット名は無効です。

- amzn_s3_demo_bucket (アンダースコアが含まれている)
- AmznS3DemoBucket (大文字が含まれている)
- amzn-s3-demo-bucket- (amzn-s3-demo- プレフィックスで始まり、ハイフンで終わる)
- example..com (2 つのピリオドが連続して含まれる)
- 192.168.5.4 (IP アドレスの形式と一致する)

ベストプラクティス

汎用バケットに名前を付けるときは、以下のバケット命名のベストプラクティスを考慮してください。

命名の競合を引き起こす可能性が低いバケット命名スキームを選択する

アプリケーションが自動的にバットを作成する場合は、命名の衝突が起きないようなバケット命名スキームを使用してください。特定のバケット名が既に使用されている場合は、異なるバケット名をアプリケーションロジックが選択するようにしてください。

バケット名にグローバル一意識別子 (GUID) を追加する

予測不可能なバケット名を作成することをお勧めします。バケットを既に作成していない限り、選択したバケット名を使用できるものと見なしてコードを記述しないでください。予測不可能なバケット名を作成する方法の 1 つは、バケット名にグローバル一意識別子 (GUID) を追加することです (例: amzn-s3-demo-bucket-a1b2c3d4-5678-90ab-cdef-example11111)。詳細については、「the section called “バケット名で GUID を使用するバケットの作成”」を参照してください。

バケット名にピリオド (.) を使用しない

互換性を最も高くするには、静的ウェブサイトホスティング専用のバケットを除き、バケット名にピリオド (.) を使用しないことをお勧めします。バケット名にピリオドを含めると、証明書の検証を独自に実行しない限り、HTTPS 経由の仮想ホスト形式のアドレス指定は使用できません。バケット名にピリオドが含まれていると、バケットの仮想ホスティング用のセキュリティ証明書は機能しません。

静的ウェブサイトホスティングは HTTP 経由でのみ使用されるため、この制限は静的ウェブサイトホスティング用のバケットには影響しません。仮想ホスティング形式のアドレス指定の詳細について

は、「汎用バケットの仮想ホスティング」を参照してください。静的ウェブサイトホスティングの詳細については、「Amazon S3 を使用して静的ウェブサイトをホスティングする」を参照してください。

関連する名前を選択する

バケットに名前を付けるときは、ユーザーやユーザーのビジネスに関連する名前を選択します。他のユーザーに関連付けられている名前は使用しないでください。例えば、バケット名に AWS や Amazon を使用することを避けます。

バケット名を再利用するためにバケットを削除しないでください。

バケットが空の場合は削除できます。バケットが削除されると、その名前は再利用できるようになります。ただし、すぐに名前を再利用できる保証がないか、あるいはまったくありません。バケットを削除した後、その名前が再利用可能になるまでに、しばらく時間がかかる場合もあります。さらに、その名前を再利用できるようになる前に、別の AWS アカウントが同じ名前のバケットを作成する場合があります。

汎用バケットの削除後は、同じパーティション内の別の AWS アカウントが新しいバケットに同じバケット名を使用する場合があるため、削除した汎用バケットへのリクエストを受け取る可能性があることに注意してください。これを防ぐ場合、または同じ汎用バケット名を使い続ける場合は、汎用バケットを削除しないでください。バケットを空にして保持し、代わりに必要に応じてバケットリクエストをブロックすることをお勧めします。

バケット名で GUID を使用するバケットの作成

以下の例は、バケット名の最後に GUID を使用する汎用バケットの作成方法を示しています。

AWS CLI を使用する場合

次の AWS CLI の例では、グローバル一意識別子 (GUID) を名前に使用した汎用バケットを米国西部 (北カリフォルニア) リージョン (us-west-1) に作成します。このコマンド例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3api create-bucket \
    --bucket amzn-s3-demo-bucket1$(uuidgen | tr -d - | tr '[:upper:]' '[:lower:]' ) \
    --region us-west-1 \
    --create-bucket-configuration LocationConstraint=us-west-1
```

AWS SDK for Java の使用

次の例は、AWS SDK for Java を使用して、米国東部 (バージニア北部) リージョン (us-east-1) で名前の末尾に GUID を追加したバケットを作成する方法を示しています。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。その他の AWS SDK については、「AWS での構築ツール」を参照してください。

```
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.Bucket;
import com.amazonaws.services.s3.model.CreateBucketRequest;

import java.util.List;
import java.util.UUID;

public class CreateBucketWithUUID {
    public static void main(String[] args) {
        final AmazonS3 s3 =
 AmazonS3ClientBuilder.standard().withRegion(Regions.US_EAST_1).build();
        String bucketName = "amzn-s3-demo-bucket" +
 UUID.randomUUID().toString().replace("-", "");
        CreateBucketRequest createRequest = new CreateBucketRequest(bucketName);
        System.out.println(bucketName);
        s3.createBucket(createRequest);
    }
}
```

汎用バケットのクォータ、制限、制約

Amazon S3 汎用バケットは、それを作成した AWS アカウントが所有します。バケットの所有権を別のアカウントに譲渡することはできません。

バケットクォータ

デフォルトでは、AWS アカウントごとに最大 10,000 個の汎用バケットを作成できます。汎用バケットのクォータ引き上げをリクエストするには、Service Quotas コンソールにアクセスしてください。

> **Important**
>
> ページ分割された ListBuckets リクエストのみを使用することを強くお勧めします。ページ分割されていない ListBuckets リクエストは、デフォルトの汎用バケットクォータが 10,000 に設定されている AWS アカウントでのみサポートされています。承認された汎用バケットクォータが 10,000 を超えている場合は、ページ分割された ListBuckets リクエストを送信してアカウントのバケットを一覧表示する必要があります。汎用バケットクォータが 10,000 を超えている AWS アカウントの場合、ページ分割されていないすべての ListBuckets リクエストは拒否されます。

> **Note**
>
> クォータ、バケット使用率を表示したり、AWS アカウントの汎用バケットの引き上げをリクエストしたりするには、以下の AWS リージョンを使用する必要があります。
>
> - 商用リージョンの汎用バケットクォータは、米国東部 (バージニア北部) からのみ表示および管理できます。
> - AWS GovCloud (US) の汎用バケットクォータは、AWS GovCloud (米国西部) からのみ表示および管理できます。

Service Quotas の概要については、「Amazon Web Services 全般のリファレンス」の「AWS service quotas」を参照してください。

オブジェクトとバケットの制限

最大バケットサイズまたはバケットに保存できるオブジェクト数に制限はありません。すべてのオブジェクトを 1 つのバケットに格納してもかまいませんし、複数のバケットに分けて整理してもかまいません。ただし、別のバケット内からバケットを作成することはできません。

バケットの名前付け

バケットの作成時にバケットの名前と作成先の AWS リージョン を選択します。バケットの作成後はバケットの名前もリージョンも変更できません。バケットの命名の詳細については、「汎用バケットの命名規則」を参照してください。

Amazon S3 汎用バケットへのアクセス

Amazon S3 汎用バケットにアクセスするには、Amazon S3 コンソール、AWS Command Line Interface、AWS SDK、または Amazon S3 REST API を使用できます。S3 汎用バケットへのアクセス方法ごとにサポートされるユースケースは異なります。詳細については、次のセクションを参照してください。

トピック

- ユースケース
- Amazon S3 コンソール
- AWS CLI
- AWS SDK
- Amazon S3 REST API

ユースケース

Amazon S3 汎用バケットのユースケースに応じて、バケット内の基になるデータにアクセスするための推奨方法が異なります。以下のリストには、データにアクセスする一般的なユースケースが含まれています。

- 静的ウェブサイト – Amazon S3 を使用して静的ウェブサイトをホスティングできます。このユースケースでは、S3 汎用バケットをウェブサイトと同様に機能するよう設定できます。Amazon S3 上でウェブサイトをホスティングするステップを説明する例については、「チュートリアル: Amazon S3 での静的ウェブサイトの設定」を参照してください。

  パブリックアクセスをブロックするなどのセキュリティ設定を有効にして静的ウェブサイトをホストするには、Amazon CloudFront とオリジンアクセスコントロール (OAC) を使用し、HTTPS などの追加のセキュリティヘッダーを実装することをお勧めします。詳細については、「安全な静的ウェブサイトの使用開始」を参照してください。

  > **Note**
  >
  > Amazon S3 は、静的ウェブサイトアクセスの仮想ホスト形式とパス形式の URL の両方をサポートしています。バケットはパス形式の URL と仮想ホスト形式の URL を使用してアクセスできるため、DNS 準拠のバケット名を使用してバケットを作成することをお勧めします。詳細については、「汎用バケットのクォータ、制限、制約」を参照してください。

- 共有データセット — Amazon S3 でスケールする場合、マルチテナントモデルを採用して、共有汎用バケット内のプレフィックスごとに異なるエンドカスタマーまたはビジネスユニットを割り当て

るのが一般的です。Amazon S3 アクセスポイントを使用すると、共有データセットにアクセスする必要のあるアプリケーションごとに、1 つの大きなバケットポリシーを個別のアクセスポイントポリシーに分割できます。このアプローチにより、共有データセット内で他のアプリケーションが実行中の操作を中断することなく、アプリケーションに適したアクセスポリシーの構築に集中しやすくなります。詳細については、「アクセスポイントを使用した汎用バケット内の共有データセットへのアクセスの管理」を参照してください。

- 高スループットワークロード - Mountpoint for Amazon S3 は、Amazon S3 汎用バケットをローカルファイルシステムとしてマウントするための、高スループットのオープンソースファイルクライアントです。Mountpoint を使用すると、アプリケーションは、開く、読み取るなどのファイルシステム操作を通じて Amazon S3 に保存されているオブジェクトにアクセスできます。Mountpoint はこれらの操作を S3 オブジェクト API 呼び出しに自動的に変換し、アプリケーションが Amazon S3 のエラスティックなストレージとスループットにファイルインターフェイスを通じてアクセスできるようにします。詳細については、「Amazon S3 バケットをローカルファイルシステムとしてマウントする」を参照してください。
- マルチリージョンアプリケーション - Amazon S3 マルチリージョンアクセスポイントは、複数の AWS リージョンにある S3 汎用バケットからのリクエストを満たすためにアプリケーションで使用できるグローバルエンドポイントを提供します。マルチリージョンアクセスポイントを使用して、単一のリージョンで使用するのと同じシンプルなアーキテクチャでマルチリージョンアプリケーションを構築し、世界中のどこでもこれらのアプリケーションを実行することができます。マルチリージョンのアクセスポイントは、パブリックインターネット経由でリクエストを送信する代わりに、Amazon S3 へのインターネットベースのリクエストを高速化する組み込みのネットワーク耐障害性を実現します。詳細については、「マルチリージョンアクセスポイントを使用したマルチリージョントラフィックの管理」を参照してください。
- Secure Shell (SSH) File Transfer プロトコル (SFTP) — インターネット経由で機密データを安全に転送する場合は、Amazon S3 汎用バケットで SFTP 対応サーバーを使用できます。AWS SFTP は、SSH のセキュリティおよび認証機能を完全にサポートするネットワークプロトコルです。このプロトコルでは、ユーザー ID、権限、キーをきめ細かく制御したり、IAM ポリシーを使用してアクセスを管理したりできます。SFTP 対応サーバーを Amazon S3 バケットに関連付けるには、まず SFTP 対応サーバーを作成してください。次に、ユーザーアカウントを設定し、サーバーを Amazon S3 汎用バケットに関連付けます。このプロセスのウォークスルーについては、「AWS ブログ」の「Amazon S3 用のフルマネージド SFTP サービス」を参照してください。

Amazon S3 コンソール

コンソールは、Amazon S3 と AWS リソースを管理するためのウェブベースのユーザーインターフェイスです。Amazon S3 コンソールでは、バケットに簡単にアクセスしてバケットのプロパティ

を変更できます。コンソール UI を使用すると、コードを記述することなく、ほとんどのバケットオペレーションを実行することもできます。

AWS アカウント にサインアップ済みの場合は、Amazon S3 コンソールにサインインし、そのホームページで [S3] を選択することで、Amazon S3 コンソールにアクセスできます。こちらのリンク (https://console.aws.amazon.com/s3/) を使用して直接アクセスすることもできます。

AWS CLI

AWS CLI を使用すると、コマンドを発行したり、システムのコマンドラインでスクリプトを作成したりして、AWS (S3 を含む) のタスクを実行できます。例えば、複数のバケットにアクセスする必要がある場合は、AWS CLI を使用して一般的で反復的なタスクを自動化することで時間を節約できます。組織の規模が拡大するにつれて、一般的なアクションのスクリプト作成性と再現性が頻繁に検討されます。

AWS CLI は、幅広い AWS のサービスのセットに対するコマンドを提供しています。AWS CLI は、Windows、macOS、Linux でサポートされています。使用を開始するには、「AWS Command Line Interfaceユーザーガイド」を参照してください。Amazon S3 用コマンドの詳細については、AWS CLIコマンドリファレンスの s3api および s3control を参照してください。

AWS SDK

AWS には、さまざまなプログラミング言語およびプラットフォーム (Java、Python、Ruby、.NET、iOS、Android など) のライブラリとサンプルコードで構成された SDK (ソフトウェア開発キット) が用意されています。AWS SDK は、S3 や AWS へのプログラムによるアクセスを作成するのに役立ちます。Amazon S3 は REST サービスです。AWS SDK ライブラリを使用して Amazon S3 にリクエストを送信できます。これは、基盤となる Amazon S3 REST API をラップし、プログラミングタスクを簡素化します。例えば、SDK は署名の計算、リクエストの暗号化による署名、エラーの管理、リクエストの自動再試行などのタスクを処理します。AWS SDK のダウンロードやインストールなどの詳細については、「AWS のツール」を参照してください。

Amazon S3 とのすべてのやり取りは認証されるか匿名で行われます。AWS SDK を使用している場合、指定したキーから、ライブラリによって認証のための署名が計算されます。Amazon S3 へのリクエストの作成方法の詳細については、「Making requests」を参照してください。

Amazon S3 REST API

Amazon S3 は、プログラミング言語に依存しないアーキテクチャとして設計されており、AWS がサポートされているインターフェイスを使用してオブジェクトを保存、取得します。Amazon S3

REST API を使用して、プログラムによって S3 や AWS にアクセスすることができます。REST API は、Amazon S3 に対する HTTP インターフェイスです。REST API では、標準 HTTP リクエストを使用してバケットとオブジェクトを作成、取得、削除できます。

REST API を使用する場合、HTTP をサポートする任意のツールキットを使用できます。匿名で読み取り可能なオブジェクトであれば、ブラウザを使用して取得することもできます。

REST API は標準の HTTP ヘッダーとステータスコードを使用するため、標準のブラウザとツールキットが予期したとおりに機能します。一部のエリアでは、HTTP に機能が追加されています (たとえば、アクセスコントロールをサポートするヘッダーを追加しました)。このように新機能を追加する場合、できるだけ標準 HTTP 書式の使用法に合致するように最善を尽くしました。

ただし、アプリケーションで直接 REST API を呼び出す場合、署名を計算するコードを作成し、それをリクエストに追加する必要があります。Amazon S3 にリクエストを行う方法の詳細については、「Amazon S3 リファレンス」の「Making requests」を参照してください。

汎用バケットの仮想ホスティング

仮想ホスティングとは、単一のウェブサーバーから複数のウェブサイトにサービスを提供することです。Amazon S3 REST API リクエストでサイトを区別する方法の 1 つとして、単なる URI のパス名部分ではなく、リクエスト URI の明確なホスト名を使用します。通常の Amazon S3 REST リクエストは、リクエスト URI パスのスラッシュで区切られた先頭コンポーネントを使用してバケットを指定します。代わりに、Amazon S3 仮想ホスティングで HTTP `Host` ヘッダーを使用することで、REST API コールで汎用バケットをアドレス指定できます。実際には、Amazon S3 は `Host` を、ほとんどのバケットは `https://bucket-name.s3.region-code.amazonaws.com` で自動的にアクセス可能である意味であると解釈します (限定されたタイプのリクエストの場合)。Amazon S3 リージョンとエンドポイントの完全なリストについては、Amazon Web Services 全般のリファレンス の「Amazon S3 エンドポイントとクォータ」を参照してください。

仮想ホスティングには、他の利点もあります。さらに、登録されたドメイン名を使用してバケットの名前を指定し、その名前を Amazon S3 の DNS エイリアスにすることによって、Amazon S3 リソースの URL を完全にカスタマイズすることができます (例: `http://my.bucket-name.com/`)。バケットの仮想サーバーの「ルートディレクトリ」に公開することもできます。多くの既存のアプリケーションがこの標準ロケーションでファイルを検索するため、この機能は重要です。たとえば、`favicon.ico`、`robots.txt`、および `crossdomain.xml` はすべてルートで見つかることが見込まれています。

> **Important**
>
> SSL と共に仮想ホスト形式の汎用バケットを使用している場合、SSL ワイルドカード証明書は、ドット (「.」) を含まないバケットのみと一致します。この制限を回避するには、HTTP を使用するか、または独自の証明書検証ロジックを記述します。詳細については、AWS ニュースブログのAmazon S3 パスの非推奨化プランを参照してください。

トピック

- パス形式のリクエスト
- 仮想ホスト形式のリクエスト
- HTTP Host ヘッダーバケット仕様
- 例
- CNAME レコードを使用した Amazon S3 URL のカスタマイズ
- ホスト名を Amazon S3 バケットに関連付ける方法
- 制限
- 下位互換性

パス形式のリクエスト

現在、Amazon S3 では、すべての AWS リージョン で仮想ホスト形式の URL とパス形式の URL の両方をサポートしています。ただし、パス形式の URL は将来廃止される予定です。詳細については、次の重要な注記を参照してください。

Amazon S3 では、パス形式の URL は次の形式を使用します。

```
https://s3.region-code.amazonaws.com/bucket-name/key-name
```

例えば、amzn-s3-demo-bucket1 という名前のバケットを 米国西部 (オレゴン) リージョンで作成し、そのバケットで puppy.jpg オブジェクトにアクセスする場合、次のパス形式の URL を使用できます。

```
https://s3.us-west-2.amazonaws.com/amzn-s3-demo-bucket1/puppy.jpg
```

> **Important**
>
> 更新 (2020 年 9 月 23 日) – お客様が仮想ホスティング形式の URL への移行に必要な時間を確保できるように、パス形式 URL の非推奨化を延期することが決定しました。詳細については、AWS ニュースブログ の「Amazon S3 Path Deprecation Plan – The Rest of the Story」を参照してください。

> **Warning**
>
> ウェブブラウザからアクセスするウェブサイトのコンテンツをホストする場合は、生成元が同じブラウザのセキュリティモデルを妨げる可能性があるパススタイルの URL の使用を避けてください。ウェブサイトコンテンツをホストするには、S3 ウェブサイトエンドポイントまたは CloudFront ディストリビューションのいずれかを使用することをお勧めします。詳細については、「ウェブサイトエンドポイント」およびAWS 規範的ガイダンスパターンの「Deploy a React-based single-page application to Amazon S3 and CloudFront」(React ベースの単一ページアプリケーションを Amazon S3 と CloudFront にデプロイする) を参照してください。

仮想ホスト形式のリクエスト

仮想ホスティング形式の URI では、バケット名は URL のドメイン名の一部です。

Amazon S3 仮想ホスト形式の URL は、次の形式を使用します。

```
https://bucket-name.s3.region-code.amazonaws.com/key-name
```

この例では、amzn-s3-demo-bucket1 はバケット名、米国西部 (オレゴン) はリージョン、puppy.png はキー名です。

```
https://amzn-s3-demo-bucket1.s3.us-west-2.amazonaws.com/puppy.png
```

HTTP **Host** ヘッダーバケット仕様

GET リクエストが SSL エンドポイントを使用しないかぎり、HTTP Host ヘッダーを使用してリクエストに対してバケットを指定できます。REST リクエストの Host ヘッダーは、次のように解釈されます。

- Host ヘッダーが省略されるか、またはその値が s3.*region-code*.amazonaws.com である場合、リクエストのバケットはリクエスト URI のスラッシュで区切られた先頭コンポーネント、リクエストのキーはリクエスト URI の残りの部分になります。このセクションの最初および 2 つ目の例に示すように、これが通常の方式です。Host ヘッダーは、HTTP 1.0 リクエストでのみ省略可能です。
- 上記のいずれの条件も該当せず、Host ヘッダーの値が .s3.*region-code*.amazonaws.com で終わる場合、バケット名は Host ヘッダーの値のうち、先頭から .s3.*region-code*.amazonaws.com までの値になります。リクエストのキーはリクエスト URI になります。この解釈により、このセクションの 3 番目と 4 番目の例で示されているように、.s3.*region-code*.amazonaws.com のサブドメインとしてバケットが公開されます。
- それ以外の場合、リクエストのバケットは Host ヘッダーの小文字の値、リクエストのキーはリクエスト URI になります。この解釈は、バケット名と同じ DNS 名を登録してして、その名前を Amazon S3 の 正規名 (CNAME) エイリアスとして設定している場合に有用です。このドキュメントではドメイン名の登録および CNAME DNS レコードの設定の手順については扱いませんが、このセクションの最後の例にその結果を示します。

例

このセクションでは、URL およびリクエストの例を示します。

Example — パス形式の URL とリクエスト

この例では以下を使用しています。

- バケット名 - example.com
- リージョン - 米国東部 (バージニア北部)
- キー名 - homepage.html

URL は次のとおりです。

```
http://s3.us-east-1.amazonaws.com/example.com/homepage.html
```

リクエストは次のとおりです。

```
GET /example.com/homepage.html HTTP/1.1
Host: s3.us-east-1.amazonaws.com
```

HTTP 1.0 でのリクエストと Host ヘッダーの省略は次のとおりです。

```
GET /example.com/homepage.html HTTP/1.0
```

DNS 互換名については、「制約事項」を参照してください。キーの詳細については、「キー」を参照してください。

Example — 仮想ホスト形式の URL とリクエスト

この例では以下を使用しています。

- バケット名 - amzn-s3-demo-bucket1
- リージョン - 欧州 (アイルランド)
- キー名 - homepage.html

URL は次のとおりです。

```
http://amzn-s3-demo-bucket1.s3.eu-west-1.amazonaws.com/homepage.html
```

リクエストは次のとおりです。

```
GET /homepage.html HTTP/1.1
Host: amzn-s3-demo-bucket1.s3.eu-west-1.amazonaws.com
```

Example — CNAME エイリアス方式

この方式を使用するには、DNS 名を *bucket-name*.s3.us-east-1.amazonaws.com の CNAME エイリアスとして設定する必要があります。詳細については、「CNAME レコードを使用した Amazon S3 URL のカスタマイズ」を参照してください。

この例では以下を使用しています。

- バケット名 - example.com
- キー名 - homepage.html

URL は次のとおりです。

```
http://www.example.com/homepage.html
```

例は次のとおりです。

```
GET /homepage.html HTTP/1.1
Host: www.example.com
```

CNAME レコードを使用した Amazon S3 URL のカスタマイズ

要件によっては、「s3.*region-code*.amazonaws.com」をウェブサイトまたはサービスに表示したくない場合もあります。例えば、ウェブサイトの画像を Amazon S3 でホスティングしている場合に、http://images.example.com.s3.us-east-1.amazonaws.com/ ではなく http://images.example.com/ としたいとします。DNS 互換名を持つすべてのバケットは、http://*BucketName*.s3.*Region*.amazonaws.com/[*Filename*] のように参照できます (例: http://images.example.com.s3.us-east-1.amazonaws.com/mydog.jpg)。CNAME を使用すると、images.example.com を Amazon S3 のホスト名にマッピングできるため、この URL は http://images.example.com/mydog.jpg になります。

バケット名は CNAME と同じである必要があります。例えば、CNAME を作成して images.example.com を images.example.com.s3.us-east-1.amazonaws.com にマッピングした場合、http://images.example.com/filename と http://images.example.com.s3.us-east-1.amazonaws.com/filename はどちらも同じになります。

CNAME DNS レコードは、ドメイン名を適切な仮想ホスティング形式のホスト名にエイリアス設定する必要があります。たとえば、バケット名とドメイン名が images.example.com で、バケットが 米国東部 (バージニア北部) リージョンにある場合、CNAME レコードは images.example.com.s3.us-east-1.amazonaws.com のエイリアスであることが必要です。

```
images.example.com CNAME    images.example.com.s3.us-east-1.amazonaws.com.
```

Amazon S3 はホスト名を使用して、バケット名を決定します。そのため CNAME とバケット名は同じである必要があります。たとえば、www.example.com を www.example.com.s3.us-east-1.amazonaws.com の CNAME として設定したとします。http://www.example.com にアクセスすると、Amazon S3 は次のようなリクエストを受け取ります。

Example

```
GET / HTTP/1.1
Host: www.example.com
Date: date
```

```
Authorization: signatureValue
```

Amazon S3 は元のホスト名 www.example.com だけを認識し、リクエストを解決するために使用される CNAME マッピングを認識しません。

どの Amazon S3 エンドポイントも、CNAME エイリアスで使用できます。たとえば、s3.ap-southeast-1.amazonaws.com は CNAME エイリアスで使用できます。エンドポイントの詳細については、「Amazon S3 API リファレンス」の「リクエストエンドポイント」を参照してください。カスタムドメインを使用して静的ウェブサイトを作成するには、チュートリアル: Route 53 に登録されたカスタムドメインを使用した静的ウェブサイトの設定 を参照してください。

> **Important**
>
> CNAME でカスタム URL を使用する場合は、設定した CNAME またはエイリアスレコードに一致するバケットが存在することを確認する必要があります。たとえば、www.example.com と login.example.com の DNS エントリを作成し、S3 を使用してウェブコンテンツを公開するには、www.example.com と login.example.com の両方のバケットを作成する必要があります。
> CNAME またはエイリアスレコードが、一致するバケットがない S3 エンドポイントをポイントするように設定されている場合、AWS ユーザーは、所有権が同じでなくても、そのバケットを作成し、設定されたエイリアスでコンテンツを公開できます。
> 同じ理由で、バケットを削除するときは、対応する CNAME またはエイリアスを変更または削除することをお勧めします。

ホスト名を Amazon S3 バケットに関連付ける方法

CNAME エイリアスを使用してホスト名を Amazon S3 バケットに関連付けるには

1. 管理するドメインに属するホスト名を選択します。

   この例では、images ドメインの example.com サブドメインを使用します。
2. ホスト名と一致するバケットを作成します。

   この例では、ホスト名およびバケット名は images.example.com です。バケット名はホスト名と完全に一致する必要があります。
3. ホスト名を Amazon S3 バケットのエイリアスとして定義する CNAME DNS レコードを作成します。

例:

```
images.example.com CNAME images.example.com.s3.us-west-2.amazonaws.com
```

> **Important**
>
> リクエストルーティングの理由により、CNAME DNS レコードは、前述の例と完全に一致するように定義する必要があります。そうしない場合、正しく動作するように見えても、最終的には予期しない結果を招くことがあります。

CNAME DNS レコードを設定する手順は、お使いの DNS サーバーまたは DNS プロバイダーによって異なります。個別の情報については、お使いのサーバーのマニュアルをご覧になるか、プロバイダーにお問い合わせください。

制限

SOAP API は新規顧客には利用できず、2025 年 8 月 31 日にサポート終了 (EOL) となります。REST API か AWS SDK を使用することをお勧めします。

下位互換性

以下のセクションでは、パス形式および仮想ホスト形式の URL リクエストに関連する Amazon S3 の下位互換性のさまざまな側面について説明します。

レガシーエンドポイント

一部のリージョンでは、レガシーエンドポイントがサポートされています。これらのエンドポイントは、サーバーアクセスログまたは AWS CloudTrail ログに表示される場合があります。詳細については、次の情報を確認してください。Amazon S3 リージョンとエンドポイントの完全なリストについては、Amazon Web Services 全般のリファレンス の「Amazon S3 エンドポイントとクォータ」を参照してください。

> **Important**
>
> ログにレガシーエンドポイントが表示される場合もありますが、バケットにアクセスするには、常に標準のエンドポイント構文を使用することをお勧めします。
> Amazon S3 仮想ホスト形式の URL は、次の形式を使用します。

```
https://bucket-name.s3.region-code.amazonaws.com/key-name
```

Amazon S3 では、パス形式の URL は次の形式を使用します。

```
https://s3.region-code.amazonaws.com/bucket-name/key-name
```

s3-Region

一部の古い Amazon S3 リージョンでは、ドット (s3.us-west-2 など) ではなく、s3 とリージョンコードの間にダッシュ (-) を含むエンドポイント (s3-us-west-2 など) がサポートされています。バケットがこれらのリージョンのいずれかにある場合、サーバーアクセスログまたは CloudTrail ログに次のエンドポイント形式が表示されることがあります。

```
https://bucket-name.s3-region-code.amazonaws.com
```

この例では、バケット名は amzn-s3-demo-bucket1、リージョンは米国西部 (オレゴン) です。

```
https://amzn-s3-demo-bucket1.s3-us-west-2.amazonaws.com
```

レガシーグローバルエンドポイント

一部のリージョンでは、レガシーグローバルエンドポイントを使用して、リージョン固有のエンドポイントを指定しないリクエストを作成できます。レガシーグローバルエンドポイントポイントは次のとおりです。

```
bucket-name.s3.amazonaws.com
```

サーバーアクセスログまたは CloudTrail ログに、レガシーグローバルエンドポイントを使用するリクエストが表示される場合があります。この例では、バケット名は amzn-s3-demo-bucket1 であり、レガシーグローバルエンドポイントは次のとおりです。

```
https://amzn-s3-demo-bucket1.s3.amazonaws.com
```

米国東部 (バージニア北部) の仮想ホスト形式のリクエスト

レガシーグローバルエンドポイントで行われたリクエストは、デフォルトでは米国東部 (バージニア北部) リージョンに送信されます。したがって、レガシーグローバルエンドポイントは、米国東部

(バージニア北部) のリージョン別エンドポイントの代わりに使用されることがあります。米国東部 (バージニア北部) にバケットを作成し、グローバルエンドポイントを使用する場合、Amazon S3 はデフォルトでリクエストをこのリージョンにルーティングします。

他のリージョンに対する仮想ホスト形式のリクエスト

レガシーグローバルエンドポイントは、サポートされている他のリージョンでの仮想ホスト形式のリクエストにも使用されます。2019 年 3 月 20 日より前に開始されたリージョンにバケットを作成し、レガシーグローバルエンドポイントを使用すると、Amazon S3 は DNS レコードを更新してリクエストを正しいロケーションにルーティングします。この処理には時間がかかる場合があります。その間、デフォルトのルールが適用され、仮想ホスト形式のリクエストは米国東部 (バージニア北部) リージョンに送られます。次に、Amazon S3 は HTTP 307 一時的リダイレクトを使用して正しいリージョンにリダイレクトします。

2019 年 3 月 20 日より後に開始されたリージョンの S3 バケットの場合、DNS サーバーはリクエストをバケットが存在する AWS リージョン に直接ルーティングしません。代わりに HTTP 400 Bad Request エラーが返されます。詳細については、「Amazon S3 API リファレンス」の「Making requests」を参照してください。

パス形式のリクエスト

米国東部 (バージニア北部) リージョンでは、パス形式のリクエストにレガシーグローバルエンドポイントを使用できます。

他のすべてのリージョンでは、パススタイル構文の場合、バケットへのアクセスを試行するときにリージョン固有のエンドポイントを使用する必要があります。レガシーグローバルエンドポイント、またはバケットが存在するリージョンのエンドポイントとは異なる別のエンドポイントを使用してバケットにアクセスしようとすると、HTTP レスポンスコード 301 Permanent Redirect エラーと、リソースの正しい URI を示すメッセージが表示されます。例えば、米国西部 (オレゴン) リージョンで作成されたバケットに `https://s3.amazonaws.com/bucket-name` を使用すると、HTTP 301 Permanent Redirect エラーが発生します。

汎用バケットの作成

Amazon S3 にデータをアップロードするには、まず、いずれかの AWS リージョン に S3 汎用バケットを作成する必要があります。バケットを作成する AWS アカウント は、そのバケットを所有します。バケットを作成するときは、バケット名とリージョンを選択します。作成プロセスの間、必要に応じて、このバケットに他のストレージ管理オプションを選択できます。

> **Important**
>
> 一度バケットを作成したら、そのバケット名、バケット所有者、またはリージョンを変更することはできません。バケットの命名の詳細については、「the section called “名前付けルール”」を参照してください。

デフォルトでは、AWS アカウントごとに最大 10,000 個の汎用バケットを作成できます。汎用バケットのクォータ引き上げをリクエストするには、Service Quotas コンソールにアクセスしてください。

バケットには、オブジェクトをいくつでも保存できます。Amazon S3 汎用バケットに関する制約と制限のリストについては、「汎用バケットのクォータ、制限、制約」を参照してください。

汎用バケットの設定

汎用バケットの作成時に、次の設定を使用してバケットの動作のさまざまな側面を制御できます。

- S3 オブジェクト所有権 – S3 オブジェクト所有権は、Amazon S3 バケットレベルの設定で、バケットにアップロードされる新しいオブジェクト所有権を制御し、アクセスコントロールリスト (ACL) を無効にするのに使用できます。デフォルトでは、オブジェクト所有権はバケット所有者の強制設定に設定され、すべての ACL は無効になります。ACL を無効にすると、バケット所有者はバケット内のすべてのオブジェクトを所有し、ポリシーのみを使用してデータへのアクセスを管理します。詳細については、「オブジェクトの所有権の制御とバケットの ACL の無効化。」を参照してください。
- S3 Object Lock – S3 Object Lock は、Amazon S3 オブジェクトが一定期間または無期限に削除または上書きされるのを防ぐのに役立ちます。オブジェクトロックは、write-once-read-many (WORM) モデルを使用してオブジェクトを保存します。Object Lock を使用して、WORM ストレージを必要とする規制要件を満たしたり、オブジェクトの変更や削除に対する保護レイヤーを追加したりできます。詳細については、「the section called “オブジェクトのロック”」を参照してください。

汎用バケットの作成後、または Amazon S3 コンソールで汎用バケットの作成時に、次の設定を使用してバケットの動作の他の側面を制御することもできます。

- S3 Block Public Access – S3 の Block Public Access 機能は、Amazon S3 のリソースへのパブリックアクセスの管理に役立つ、アクセスポイント、バケット、アカウントの設定を提供します。デフォルトでは、新しいバケット、アクセスポイント、およびオブジェクトはパブリックアクセス

を許可しません。ただし、ユーザーはバケットポリシー、アクセスポイントポリシー、またはオブジェクトのアクセス許可を変更することで、パブリックアクセスを許可できます。S3 ブロックパブリックアクセス設定は、これらのポリシーやアクセス許可を上書きして、これらのリソースへのパブリックアクセスを制限できるようにします。詳細については、「the section called “パブリックアクセスのブロック”」を参照してください。

- S3 バージョニング – S3 バージョニングとは、同じバケット内でオブジェクトの複数のバリアントを保持する手段です。バージョニングを使用して、 バケットに保存されたあらゆるオブジェクトのあらゆるバージョンを保存、取得、復元することができます。バージョニングを使用すれば、意図しないユーザーアクションからもアプリケーション障害からも、簡単に復旧できます。バージョニングは、バケットに対してデフォルトで無効になります。詳細については、「the section called “オブジェクトの複数のバージョンを保持する”」を参照してください。
- デフォルトの暗号化 – バケット内のすべてのオブジェクトのデフォルトの暗号化タイプを設定できます。Amazon S3 マネージドキーによるサーバーサイド暗号化 (SSE-S3) は、Amazon S3 のすべてのバケットに対する暗号化設定の基本レベルです。S3 バケットにアップロードされたすべての新しいオブジェクトは、暗号化の基本レベルとして SSE-S3 を使用して自動的に暗号化されます。別のデフォルトの暗号化タイプを使用する場合は、AWS Key Management Service (AWS KMS) キーによるサーバー側の暗号化 (SSE-KMS)、AWS KMS キーによる二層式サーバー側の暗号化 (DSSE-KMS)、または顧客提供のキーによるサーバー側の暗号化 (SSE-C) を指定できます。詳細については、「Amazon S3 バケット向けのサーバー側のデフォルトの暗号化動作の設定」を参照してください。

汎用バケットを作成するには、Amazon S3 コンソール、Amazon S3 REST API、AWS Command Line Interface (AWS CLI)、または AWS SDK を使用できます。汎用バケットの作成に必要なアクセス許可の詳細については、「Amazon Simple Storage Service API Reference」の「CreateBucket」を参照してください。

Amazon S3 バケットの作成に問題がある場合は、AWS re:Post で「Amazon S3 バケットを作成する際のエラーをトラブルシューティングする方法を教えてください」を参照してください。

S3 コンソールの使用

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. ページ上部にあるナビゲーションバーで、現在表示されている AWS リージョン の名前をクリックします。次に、バケットを作成するリージョンを選択します。

> **Note**
>
> - 一旦バケットを作成したら、そのリージョンを変更することはできません。
> - レイテンシーとコストを最小化するため、さらに規制条件に対応するために、最寄りのリージョンを選択します。明示的に別のリージョンに移動する場合を除き、特定のリージョンに保管されたオブジェクトは、そのリージョンから移動されることはありません。Amazon S3 AWS リージョン のリストについては、「Amazon Web Services 全般のリファレンス」の「AWS のサービス エンドポイント」を参照してください。

3. 左のナビゲーションペインで、[汎用バケット] を選択します。
4. [Create bucket (バケットの作成)] を選択します。[バケットの作成] ページが開きます。
5. [バケット名] にバケットの名前を入力します。

   バケット名には次の条件があります。

   - パーティション内で一意にする必要があります。パーティションは、リージョンのグループです。AWS には、現在 aws (商用リージョン)、aws-cn (中国リージョン)、および aws-us-gov (AWS GovCloud (US) Regions) の 3 つのパーティションがあります。
   - 3 ~ 63 文字で指定する。
   - 小文字、数字、ピリオド (.)、ハイフン (-) のみで構成されます。互換性を最も高くするには、静的ウェブサイトホスティング専用のバケットを除き、バケット名にピリオド (.) を使用しないことをお勧めします。
   - 文字や数字で始まり、文字や数字で終わります。
   - バケットの命名規則の完全なリストについては、「汎用バケットの命名規則」を参照してください。

   > **Important**
   >
   > - バケットを作成したら、その名前を変更することはできません。
   > - バケット名に機密情報を含めないでください。バケット名は、バケット内のオブジェクトを参照する URL に表示されます。

6. (オプション) [全般設定] で、既存のバケットの設定を新しいバケットにコピーすることを選択できます。既存のバケットの設定をコピーしない場合は、次のステップにスキップします。

> **Note**
>
> このオプションの特徴:
>
> - AWS CLI では使用できません。Amazon S3 コンソールでのみ利用できます。
> - バケットポリシーは既存のバケットから新しいバケットにコピーしません。

既存のバケットの設定をコピーするには、[既存のバケットから設定をコピー] で [バケットを選択] をクリックします。[バケットを選択] ウィンドウが開きます。コピーする設定を持つバケットを検索して、[バケットを選択] をクリックします。[バケットを選択] ウィンドウが閉じて、[バケットを作成] ウィンドウが再び開きます。

[既存のバケットから設定をコピー] に、選択したバケットの名前が表示されるようになります。新しいバケットの設定が、選択したバケットの設定と一致するようになりました。コピーした設定を削除する場合は、[デフォルトを復元] を選択します。[バケットを作成] ページで、バケットの残りの設定を確認します。変更しない場合は、最後のステップに進みます。

7. [オブジェクト所有者] で、ACL を無効または有効にし、バケットにアップロードされたオブジェクトの所有権を制御するには、次のいずれかの設定を選択します。

   ACL は無効です

   - バケット所有者の強制 (デフォルト) – ACL は無効になり、バケット所有者は汎用バケット内のすべてのオブジェクトを自動的に所有し、完全に制御します。ACL は、S3 汎用バケット内のデータへのアクセス許可に影響を与えなくなりました。このバケットはアクセスコントロールを定義するためだけにポリシーを使用します。

     デフォルトでは、ACL は無効になっています。Amazon S3 の最新のユースケースの大部分では ACL を使用する必要がなくなっています。オブジェクトごとに個別に制御する必要がある通常ではない状況を除き、ACL は無効にしておくことをお勧めします。詳細については、「オブジェクトの所有権の制御とバケットの ACL の無効化。」を参照してください。

   ACL の有効化

   - 希望するバケット所有者 — バケット所有者は、他のアカウントが `bucket-owner-full-control` 既定 ACL でバケットに書き込む新しいオブジェクトを所有し、完全にコントロールできます。

[バケット所有者を推奨] 設定を適用して、すべての Amazon S3 アップロードに bucket-owner-full-control 既定 ACL を含めることを要求する場合は、この ACL を使用するオブジェクトアップロードのみを許可するバケットポリシーを追加できます。

- オブジェクトライター — オブジェクトをアップロードする AWS アカウント は、そのオブジェクトを所有し、そのオブジェクトを完全にコントロールし、ACL を介して他のユーザーにそのオブジェクトへのアクセス権を付与できます。

> **Note**
>
> デフォルト設定は [バケット所有者の強制] です。デフォルト設定を適用して ACL を無効のままにするのに必要なのは、s3:CreateBucket アクセス許可のみです。ACL を有効にするためには、s3:PutBucketOwnershipControls アクセス許可が必要です。

8. [このバケットのパブリックアクセスブロック設定] で、バケットに適用するブロックパブリックアクセス設定を選択します。

   デフォルトでは、4 つすべての [パブリックアクセスをブロック] 設定が有効になっています。特定のユースケースでオフにする必要のある設定が 1 つ以上あることがわかっている場合を除き、すべての設定を有効にしておくことをお勧めします。ブロックパブリックアクセスの詳細については、Amazon S3 ストレージへのパブリックアクセスのブロック を参照してください。

   > **Note**
   >
   > すべての [パブリックアクセスをブロック] 設定を有効にするのに必要なのは、s3:CreateBucket アクセス許可のみです。[パブリックアクセスをブロック] 設定をオフにするには、s3:PutBucketPublicAccessBlock アクセス許可が必要です。

9. (オプション) [バケットのバージョニング] は、デフォルトで無効になります。バージョニングとは、同じバケット内でオブジェクトの複数のバリアントを保持する手段です。バージョニングを使用して、 バケットに保存されたあらゆるオブジェクトのあらゆるバージョンを保存、取得、復元することができます。バージョニングを使用すれば、意図しないユーザーアクションからもアプリケーション障害からも、より簡単に復旧できます。バージョニングの詳細については、「S3 バージョニングによる複数のバージョンのオブジェクトの保持」を参照してください。

   バケットでバージョニングを有効にするには、[有効化] を選択します。

10. (オプション) [Tags] (タグ) では、バケットにタグを追加することを選択できます。AWS コスト配分では、バケットタグを使用してバケットの使用に対する請求に注釈を付けることができます。タグはキー/値ペアになっており、バケットに割り当てられるラベルを表します。詳細については、「the section called “コスト配分タグの使用”」を参照してください。

    (オプション) タグを追加するには、[キー] を入力してから、オプションの [値] を入力し、[タグの追加] を選択します。

11. [デフォルトの暗号化] を設定するには、[暗号化タイプ] で次のいずれかを選択します。

    - Amazon S3 マネージドキーを用いたサーバー側の暗号化 (SSE-S3)
    - AWS Key Management Service キーによるサーバー側の暗号化 (SSE-KMS)
    - AWS Key Management Service (AWS KMS) キーによる二層式サーバー側の暗号化 (DSSE-KMS)

    > **Important**
    >
    > デフォルト暗号化設定として SSE-KMS または DSSE-KMS オプションを使用する場合、AWS KMS の 1 秒あたりのリクエスト数 (RPS) 制限が適用されます。AWS KMS クォータの詳細およびクォータの引き上げをリクエストする方法については、「AWS Key Management Service デベロッパーガイド」の「クォータ」を参照してください。

    バケットと新しいオブジェクトは、暗号化設定の基本レベルとして Amazon S3 マネージドキー (SSE-S3) を使用したサーバー側の暗号化で暗号化されます。デフォルトの暗号化の詳細については、「Amazon S3 バケット向けのサーバー側のデフォルトの暗号化動作の設定」を参照してください。SSE-KMS に関する詳細は、「Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3)」を参照してください。

    サーバー側の暗号化を使用してデータを暗号化する方法の詳細については、「the section called “データ暗号化”」を参照してください。

12. Amazon S3 が管理するキー (SSE-S3) によるサーバー側の暗号化または AWS Key Management Service (AWS KMS) キーによる二層式サーバー側の暗号化 (DSSE-KMS) を選択した場合は、次の操作を行います。

    a. [AWS KMS キー] で、次のいずれかの方法で KMS キーを指定します。

- 使用可能な KMS キーのリストから選択するには、[AWS KMS keys から選択する] を選択し、使用可能なキーのリストから自分の KMS キーを選択します。

  AWS マネージドキー (aws/s3) とカスタマーマネージドキーの両方がこのリストに表示されます。カスタマーマネージドキーの詳細については、AWS Key Management Service デベロッパーガイドの「カスタマーキーと AWS キー」を参照してください。

- KMS キー ARN を入力するには、[AWS KMS key ARN を入力] を選択し、表示されるフィールドに KMS キー ARN を入力します。

- AWS KMS コンソールで新しいカスタマーマネージドキーを作成するには、[KMS キーを作成] を選択します。

  AWS KMS key の作成の詳細については、「AWS Key Management Service デベロッパーガイド」の「キーの作成」を参照してください。

> **Important**
>
> バケットと同じ AWS リージョン で使用可能な KMS キーのみを使用できます。Amazon S3 コンソールには、バケットと同じリージョンで最初の 100 個の KMS キーしか表示されません。リストに存在しない KMS キーを使用するには、KMS キー ARN を入力する必要があります。別のアカウントが所有している KMS キーを使用する場合は、まず、そのキーを使用するアクセス許可が必要であり、次に、KMS キー ARN を入力する必要があります。KMS キーのクロスアカウント権限の詳細については、「AWS Key Management Service デベロッパーガイド」の「他のアカウントで使用できる KMS キーを作成する」を参照してください。SSE-KMS に関する詳細は、「AWS KMS (SSE-KMS) によるサーバー側の暗号化の指定」を参照してください。DSSE-KMS に関する詳細については、「the section called “二層式サーバー側の暗号化 (DSSE-KMS) ”」を参照してください。Amazon S3 でサーバー側の暗号化に AWS KMS key を使用する場合は、対称暗号化 KMS キーを選択する必要があります。Amazon S3 では、対称暗号化 KMS キーのみがサポートされ、非対称暗号化 KMS キーはサポートされません。詳細については、AWS Key Management Service デベロッパーガイドの「Identifying symmetric and asymmetric KMS keys」(対称および非対称 KMS キーの識別) を参照してください。

b. SSE-KMS でデフォルトの暗号化を使用するようにバケットを設定する場合は、S3 バケットキーを使用することもできます。S3 バケットキーは、Amazon S3 から AWS KMS へ

のリクエストトラフィックを減らし、暗号化のコストを削減します。詳細については、「Amazon S3 バケットキーを使用した SSE-KMS のコストの削減」を参照してください。S3 バケットキーは DSSE-KMS ではサポートされていません。

デフォルトでは、S3 バケットキーは Amazon S3 コンソールで有効になっています。コストを削減するには、S3 バケットキーを有効にしておくことをお勧めします。バケットの S3 バケットキーを無効にするには、[バケットキー] で、[無効化] を選択します。

13. (オプション) S3 Object Lock は、新しいオブジェクトが削除または上書きされないように保護するのに役立ちます。詳細については、「S3 Object Lock を使用したオブジェクトのロック」を参照してください。S3 Object Lock を有効にする場合は、次の手順に従います。

    a. [詳細設定] を選択します。

    > **Important**
    >
    > バケットに対して Object Lock を有効にすると、自動でバージョニングも有効になります。バケットを有効にして正常に作成したら、バケットの [プロパティ] タブで Object Lock のデフォルトの保持とリーガルホールドの設定も設定する必要があります。

    b. オブジェクトロックを有効にする場合は、[Enable] (有効化) を選択し、表示される警告を読んだうえで承認します。

    > **Note**
    >
    > Object Lock が有効なバケットを作成するには、`s3:CreateBucket`、`s3:PutBucketVersioning` および `s3:PutBucketObjectLockConfiguration` の許可が必要です。

14. [バケットを作成する] を選択します。

AWS SDKs の使用

AWS SDK を使用して汎用バケットを作成する場合は、最初にクライアントを作成し、次にそのクライアントを使用してバケットを作成するためのリクエストを送信します。ベストプラクティスとして、クライアントとバケットを同じ AWS リージョン で作成する必要があります。クライアントまたはバケットの作成時にリージョンを指定しない場合、Amazon S3 ではデフォルトのリージョンで

ある米国東部 (バージニア北部) が使用されます。バケットの作成を特定の AWS リージョンに制限したい場合は、LocationConstraint 条件キーを使用します。

デュアルスタックのエンドポイントにアクセスするためにクライアントを作成するには、AWS リージョン を指定する必要があります。詳細については、「Amazon S3 API リファレンス」の「Using Amazon S3 dual-stack endpoints」を参照してください。利用可能な AWS リージョンのリストについては、「AWS 全般のリファレンス」の「Amazon Simple Storage Service のエンドポイントとクォータ」を参照してください。

クライアントを作成すると、リージョンはリージョン固有のエンドポイントにマッピングされます。クライアントは、このエンドポイントを使用して Amazon S3 と通信します。`s3.region.amazonaws.com`。リージョンがローンチされたのが 2019 年 3 月 20 日以降である場合は、クライアントとバケットは同じリージョン内にある必要があります。2019 年 3 月 20 日以前にローンチされたリージョンの場合は、米国東部 (バージニア北部) のリージョンでクライアントを使用することによりバケットを作成できます。詳細については、「レガシーエンドポイント」を参照してください。

AWS SDK コード例が、以下のタスクを実行します。

- AWS リージョン を明示的に指定してクライアントを作成する - この例では、クライアントは `s3.us-west-2.amazonaws.com` エンドポイントを使用して Amazon S3 と通信します。任意の AWS リージョン を指定できます。AWS リージョン の一覧については、「AWS 全般のリファレンス」の「リージョンとエンドポイント」を参照してください。
- バケット名のみを指定してバケット作成リクエストを送信する - クライアントが Amazon S3 にリクエストを送信し、クライアントが作成されたリージョンにバケットを作成します。
- バケットの場所情報を取得する - Amazon S3 が、バケットの場所情報を、そのバケットに関連付けられている場所のサブリソースに保存します。

その他の AWS SDK の例と他の言語の例については、「Amazon Simple Storage Service API リファレンス」の「AWS SDK または CLI で CreateBucket を使用する」を参照してください。

Java

Example バケット名でグローバル一意識別子 (GUID) を使用するバケットを作成する

次の例は、AWS SDK for Java を使用して、米国東部 (バージニア北部) リージョン (`us-east-1`) で名前の末尾に GUID を追加したバケットを作成する方法を示しています。この例を実行するには、*`user input placeholders`* をユーザー自身の情報に置き換えます。その他の AWS SDK については、「AWS での構築ツール」を参照してください。

```
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.Bucket;
import com.amazonaws.services.s3.model.CreateBucketRequest;

import java.util.List;
import java.util.UUID;

public class CreateBucketWithUUID {
    public static void main(String[] args) {
        final AmazonS3 s3 =
 AmazonS3ClientBuilder.standard().withRegion(Regions.US_EAST_1).build();
        String bucketName = "amzn-s3-demo-bucket" +
 UUID.randomUUID().toString().replace("-", "");
        CreateBucketRequest createRequest = new CreateBucketRequest(bucketName);
        System.out.println(bucketName);
        s3.createBucket(createRequest);
    }
}
```

Example 汎用バケットを作成する

この例では、AWS SDK for Java を使用して Amazon S3 バケットを作成する方法を示します。作業サンプルの作成およびテストの手順については、「AWS SDK for Java 2.x デベロッパーガイド」を参照してください。

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.CreateBucketRequest;
import com.amazonaws.services.s3.model.GetBucketLocationRequest;

import java.io.IOException;

public class CreateBucket2 {

    public static void main(String[] args) throws IOException {
```

```
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();

            if (!s3Client.doesBucketExistV2(bucketName)) {
                // Because the CreateBucketRequest object doesn't specify a region,
 the
                // bucket is created in the region specified in the client.
                s3Client.createBucket(new CreateBucketRequest(bucketName));

                // Verify that the bucket was created by retrieving it and checking
 its
                // location.
                String bucketLocation = s3Client.getBucketLocation(new
 GetBucketLocationRequest(bucketName));
                System.out.println("Bucket location: " + bucketLocation);
            }
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

.NET

作業サンプルの作成およびテストの手順については、「AWS SDK for .NET Version 3 API Reference」を参照してください。

Example

```
using Amazon;
using Amazon.S3;
```

```
using Amazon.S3.Model;
using Amazon.S3.Util;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class CreateBucketTest
    {
        private const string bucketName = "*** bucket name ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;
        public static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            CreateBucketAsync().Wait();
        }

        static async Task CreateBucketAsync()
        {
            try
            {
                if (!(await AmazonS3Util.DoesS3BucketExistAsync(s3Client,
 bucketName)))
                {
                    var putBucketRequest = new PutBucketRequest
                    {
                        BucketName = bucketName,
                        UseClientRegion = true
                    };

                    PutBucketResponse putBucketResponse = await
 s3Client.PutBucketAsync(putBucketRequest);
                }
                // Retrieve the bucket location.
                string bucketLocation = await FindBucketLocationAsync(s3Client);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
```

```
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
        }
        static async Task<string> FindBucketLocationAsync(IAmazonS3 client)
        {
            string bucketLocation;
            var request = new GetBucketLocationRequest()
            {
                BucketName = bucketName
            };
            GetBucketLocationResponse response = await
 client.GetBucketLocationAsync(request);
            bucketLocation = response.Location.ToString();
            return bucketLocation;
        }
    }
}
```

Ruby

作業サンプルの作成およびテストの手順については、「AWS SDK for Ruby - Version 3」を参照してください。

Example

```
require 'aws-sdk-s3'

# Wraps Amazon S3 bucket actions.
class BucketCreateWrapper
  attr_reader :bucket

  # @param bucket [Aws::S3::Bucket] An Amazon S3 bucket initialized with a name.
 This is a client-side object until
  #                                 create is called.
  def initialize(bucket)
    @bucket = bucket
  end

  # Creates an Amazon S3 bucket in the specified AWS Region.
  #
```

```
  # @param region [String] The Region where the bucket is created.
  # @return [Boolean] True when the bucket is created; otherwise, false.
  def create?(region)
    @bucket.create(create_bucket_configuration: { location_constraint: region })
    true
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't create bucket. Here's why: #{e.message}"
    false
  end

  # Gets the Region where the bucket is located.
  #
  # @return [String] The location of the bucket.
  def location
    if @bucket.nil?
      'None. You must create a bucket before you can get its location!'
    else
      @bucket.client.get_bucket_location(bucket: @bucket.name).location_constraint
    end
  rescue Aws::Errors::ServiceError => e
    "Couldn't get the location of #{@bucket.name}. Here's why: #{e.message}"
  end
end

# Example usage:
def run_demo
  region = "us-west-2"
  wrapper = BucketCreateWrapper.new(Aws::S3::Bucket.new("amzn-s3-demo-bucket-
#{Random.uuid}"))
  return unless wrapper.create?(region)

  puts "Created bucket #{wrapper.bucket.name}."
  puts "Your bucket's region is: #{wrapper.location}"
end

run_demo if $PROGRAM_NAME == __FILE__
```

AWS CLI を使用する場合

次の AWS CLI の例では、グローバル一意識別子 (GUID) を名前に使用した汎用バケットを米国西部 (北カリフォルニア) リージョン (us-west-1) に作成します。このコマンド例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3api create-bucket \
    --bucket amzn-s3-demo-bucket1$(uuidgen | tr -d - | tr '[:upper:]' '[:lower:]' ) \
    --region us-west-1 \
    --create-bucket-configuration LocationConstraint=us-west-1
```

詳細と追加の例については、「AWS CLI コマンドリファレンス」の「create-bucket」を参照してください。

S3 汎用バケットのプロパティの表示

所有しているすべての Amazon S3 バケットのプロパティを表示できます。これらの設定には以下が含まれます。

- バケットのバージョニング – バージョニングを使用すると、1 つの汎用バケットでオブジェクトの複数のバージョンを保持できます。バージョニングは、新しいバケットに対してデフォルトで無効になります。バージョニングを有効にする詳細については、「バケットでのバージョニングの有効化」を参照してください。
- タグ – AWS コスト配分では、バケットタグを使用して汎用バケットの使用に対する請求に注釈を付けることができます。タグはキー/値ペアになっており、バケットに割り当てられるラベルを表します。詳細については、「S3 バケットタグでのコスト配分タグの使用」を参照してください。
- デフォルトの暗号化 – デフォルトの暗号化を有効にすると、サーバー側の自動暗号化が可能になります。Amazon S3 は、ディスクに保存する前にオブジェクトを暗号化し、ダウンロード時にオブジェクトを復号化します。詳細については、「Amazon S3 バケット向けのサーバー側のデフォルトの暗号化動作の設定」を参照してください。
- サーバーアクセスのログ記録 – サーバーアクセスのログ記録で汎用バケットに対するリクエストの詳細な記録を取得します。デフォルトでは、Amazon S3 によってサーバーアクセスログは収集されません。サーバーアクセスログ記録の有効化については、「Amazon S3 サーバーアクセスログを有効にします。」を参照してください。
- AWS CloudTrail データイベント – CloudTrail を使用してデータイベントをログに記録します。デフォルトでは、証跡はデータイベントを記録しません。追加の変更がイベントデータに適用されます。詳細については、AWS CloudTrail ユーザーガイドの証跡へのデータイベントのログ記録を参照してください。
- イベント通知 – イベントが発生するたびに送信先へ通知メッセージを送信するには、Amazon S3 汎用バケットイベントを有効にします。詳細については、「Amazon S3 コンソールを使用したイベント通知の有効化と設定」を参照してください。

- Transfer Acceleration – クライアントと S3 バケットの間で、長距離にわたるファイル転送を高速、簡単、安全に行えるようになります。Transfer Acceleration の有効化の詳細については、「S3 Transfer Acceleration の有効化と使用」を参照してください。
- オブジェクトロック – S3 オブジェクトロックを使って、オブジェクトが固定期間または無期限に削除または上書きされることを防止できます。詳細については、「S3 Object Lock を使用したオブジェクトのロック」を参照してください。
- リクエスタ支払い – 汎用バケット所有者ではなく、リクエスタがリクエストとデータ転送の料金を支払うようにするには、リクエスタ支払いを有効にします。詳細については、「ストレージの転送と使用にリクエスタ支払い汎用バケットを使用する」を参照してください。
- 静的ウェブサイトホスティング – 静的ウェブサイトを Amazon S3 でホスティングできます。詳細については、「Amazon S3 を使用して静的ウェブサイトをホスティングする」を参照してください。

バケットプロパティは、AWS Management Console、AWS CLI、または AWS SDK を使用して表示できます。

S3 コンソールの使用

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 左のナビゲーションペインで、[汎用バケット] または [ディレクトリバケット] を選択します。
3. バケットリストで、プロパティを表示するバケットの名前を選択します。
4. [プロパティ] タブを選択します。
5. [プロパティ] ページで、バケットの上記プロパティを設定できます。

AWS CLI を使用する場合

AWS CLI を使用したバケットプロパティの表示

以下のコマンドは、AWS CLI を使用して汎用バケットのさまざまなプロパティを一覧表示する方法を示しています。

以下は、バケット *amzn-s3-demo-bucket1* に関連付けられたタグセットを返します。バケットタグの詳細については、「S3 バケットタグでのコスト配分タグの使用」を参照してください。

```
aws s3api get-bucket-tagging --bucket amzn-s3-demo-bucket1
```

詳細と例については、「AWS CLI コマンドリファレンス」の「get-bucket-tagging」を参照してください。

以下は、バケット *amzn-s3-demo-bucket1* のバージョニング状態を返します。バケットのバージョニングの詳細については、「S3 バージョニングによる複数のバージョンのオブジェクトの保持」を参照してください。

```
aws s3api get-bucket-versioning --bucket amzn-s3-demo-bucket1
```

詳細と例については、「AWS CLI コマンドリファレンス」の「get-bucket-versioning」を参照してください。

以下は、バケット *amzn-s3-demo-bucket1* のデフォルトの暗号化設定を返します。デフォルトでは、すべてのバケットには、Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3) を使用するデフォルトの暗号化設定が指定されています。デフォルトのバケット暗号化の詳細については、「Amazon S3 バケット向けのサーバー側のデフォルトの暗号化動作の設定」を参照してください。

```
aws s3api get-bucket-encryption --bucket amzn-s3-demo-bucket1
```

詳細と例については、「AWS CLI コマンドリファレンス」の「get-bucket-encryption」を参照してください。

以下は、バケット *amzn-s3-demo-bucket1* の通知設定を返します。バケットイベント通知については、「Amazon S3 イベント通知」を参照してください。

```
aws s3api get-bucket-notification-configuration --bucket amzn-s3-demo-bucket1
```

詳細と例については、「AWS CLI コマンドリファレンス」の「get-bucket-notification-configuration」を参照してください。

以下は、バケット *amzn-s3-demo-bucket1* のログ記録ステータスを返します。バケットのログ記録については、「サーバーアクセスログによるリクエストのログ記録」を参照してください。

```
aws s3api get-bucket-logging --bucket amzn-s3-demo-bucket1
```

詳細については、「AWS CLI コマンドリファレンス」の「get-bucket-logging」を参照してください。

AWS SDK の使用

AWS SDKを使用して汎用バケットのプロパティ (バージョニングやタグなど) を返す方法の例については、「Amazon S3 API Reference」の「Code examples」を参照してください。

さまざまな AWS SDK の使用に関する一般的な情報については、「Amazon S3 API リファレンス」の「Developing with Amazon S3 using the AWS SDKs」を参照してください。

Amazon S3 汎用バケットの一覧表示

所有している汎用バケットのリストを返すには、ListBuckets を使用できます。バケットは、Amazon S3 コンソール、AWS Command Line Interface、または AWS SDK を使用して一覧表示できます。AWS CLI、AWS SDK、Amazon S3 REST API を使用した `ListBuckets` リクエストの場合、バケットのデフォルトのサービスクォータ (10,000 バケット) を使用する AWS アカウントは、ページ分割されたリクエストとページ分割されていないリクエストの両方をサポートしています。アカウント内のバケットの数に関係なく、1 ~ 10,000 個のバケットのページサイズを作成して、すべてのバケットを一覧表示できます。ページ分割されたリクエストの場合、`ListBuckets` リクエストはバケット名と各バケットに対応する AWS リージョン の両方を返します。次の AWS Command Line Interfaceと AWS SDK の例は、`ListBuckets` リクエストでページ分割を使用する方法を示しています。一部の AWS SDK はページ分割をサポートしていることに注意してください。

アクセス許可

すべての汎用バケットを一覧表示するには、`s3:ListAllMyBuckets` アクセス許可が必要です。`HTTP Access Denied (403 Forbidden)` エラーが発生した場合は、「Amazon S3 でのアクセス拒否 (403 Forbidden) エラーのトラブルシューティング」を参照してください。

> **Important**
>
> ページ分割された `ListBuckets` リクエストのみを使用することを強くお勧めします。ページ分割されていない `ListBuckets` リクエストは、デフォルトの汎用バケットクォータが 10,000 に設定されている AWS アカウントでのみサポートされています。承認された汎用バケットクォータが 10,000 を超えている場合は、ページ分割された `ListBuckets` リクエストを送信してアカウントのバケットを一覧表示する必要があります。汎用バケットクォータが 10,000 を超えている AWS アカウントの場合、ページ分割されていないすべての `ListBuckets` リクエストは拒否されます。

S3 コンソールの使用

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 左のナビゲーションペインで、[汎用バケット] を選択します。
3. [汎用バケット] タブには、汎用バケットのリストが表示されます。
4. バケットを名前で検索するには、[バケットを名前で検索] フィールドにバケット名を入力します。

AWS CLI を使用する場合

AWS CLI を使用して汎用バケットのリストを生成するには、`ls` コマンドまたは `list-buckets` コマンドを使用できます。以下の例は、ページ分割された `list-buckets` リクエストとページ分割されていない `ls` リクエストを作成する方法を示しています。これらの例を使用するには、*#######*を置き換えます。

Example – アカウント内のすべてのバケットを **`ls`** で一覧表示する (ページ分割なし)

次のコマンド例では、ページ分割されていない 1 回の呼び出しで、アカウント内のすべての汎用バケットを一覧表示します。この呼び出しは、アカウント内のすべてのバケットのリスト (最大 10,000 件の結果) を返します。

```
$ aws s3 ls
```

詳細および例については、「バケットおよびオブジェクトを一覧表示する」を参照してください。

Example – アカウント内のすべてのバケットを **`ls`** で一覧表示する (ページ分割)

次のコマンド例では、1 つ以上のページ分割された呼び出しを実行して、アカウント内のすべての汎用バケットを一覧表示し、ページあたり 100 個のバケットを返します。

```
$ aws s3 ls --page-size 100
```

詳細および例については、「バケットおよびオブジェクトを一覧表示する」を参照してください。

Example — アカウント内のすべてのバケットを一覧表示する (ページ分割)

次の例は、アカウント内のすべての汎用バケットを一覧表示するためのページ分割された list-buckets コマンドを示しています。--max-items オプションおよび --page-size オプションでは、一覧表示するバケットの数をページあたり 100 個に制限します。

```
$ aws s3api list-buckets /
    --max-items 100 /
    --page-size 100
```

出力の項目数 (--max-items) が基本の API コールが返す合計項目数より少ない場合、出力には starting-token 引数で指定した継続トークンが含まれます。このトークンを後続のコマンドに渡して、次の項目のセットを取得できます。次の例は、前の例で返された starting-token 値を使用する方法を示しています。starting-code を指定して、次の 100 個のバケットを取得できます。

```
$ aws s3api list-buckets /
    --max-items 100 /
    --page-size 100 /
    --starting-token eyJNYXJrZXIiOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQiOiAxfQ==
```

Example — AWS リージョン 内のすべてのバケットを一覧表示する (ページ分割)

次のコマンド例では、--bucket-regionパラメータを使用して、us-east-2 リージョンにあるアカウント内のバケットを最大 100 個一覧表示します。--bucket-region パラメータで指定した値とは異なるリージョンエンドポイントにリクエストを行うことは、サポートされていません。例えば、us-east-2 のバケットに対するレスポンスを制限する場合は、us-east-2 のエンドポイントにリクエストを行う必要があります。

```
$ aws s3api list-buckets /
    --region us-east-2 /
    --max-items 100 /
    --page-size 100 /
    --bucket-region us-east-2
```

Example — 特定のバケット名のプレフィックスで始まるすべてのバケットを一覧表示する (ページ分割)

次のコマンド例では、*amzn-s3-demo-bucket* プレフィックスで始まる名前を持つバケットを最大 100 個一覧表示します。

```
$ aws s3api list-buckets /
    --max-items 100 /
    --page-size 100 /
    --prefix amzn-s3-demo-bucket
```

AWS SDK の使用

次の例は、AWS SDK を使用して汎用バケットを一覧表示する方法を示しています。

SDK for Python

Example – ListBuckets リクエスト (ページ分割)

```
import boto3

s3 = boto3.client('s3')
response = s3.list_buckets(MaxBuckets=100)
```

Example – ListBuckets レスポンス (ページ分割)

```
import boto3

s3 = boto3.client('s3')
response =
 s3.list_buckets(MaxBuckets=1,ContinuationToken="eyJNYXJrZXIiOiBudWxsLCAiYm90b190cnVuY2F0ZVS
```

SDK for Java

```
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.Bucket;
import com.amazonaws.services.s3.model.ListBucketsPaginatedRequest;
import com.amazonaws.services.s3.model.ListBucketsPaginatedResult;

import java.util.List;

public class ListBuckets {
    public static void main(String[] args) {
        final AmazonS3 s3 =
 AmazonS3ClientBuilder.standard().withRegion(Regions.DEFAULT_REGION).build();
```

```
        ListBucketsPaginatedRequest listBucketsPaginatedRequest = new
 ListBucketsPaginatedRequest().withMaxBuckets(1);
        ListBucketsPaginatedResult listBucketsPaginatedResult =
 s3.listBuckets(listBucketsPaginatedRequest);
        List<Bucket> buckets = listBucketsPaginatedResult.getBuckets();
        System.out.println("Your Amazon S3 buckets are:");
        for (Bucket b : buckets) {
            System.out.println("* " + b.getName() + " region: " + b.getRegion());
        }
        System.out.println("continuation token: " +
 listBucketsPaginatedResult.getContinuationToken());
    }
}
```

SDK for Java 2.x

```
import software.amazon.awssdk.auth.credentials.DefaultCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.services.s3.model.Bucket;
import software.amazon.awssdk.services.s3.model.ListBucketsRequest;
import software.amazon.awssdk.services.s3.model.ListBucketsResponse;

import java.util.List;

public class ListBuckets {
    public static void main(String[] args) {
        // Create an S3 client
        S3Client s3 = S3Client.builder()
                .region(Region.US_EAST_1) // Replace with your preferred region
                .credentialsProvider(DefaultCredentialsProvider.create())
                .build();

        try {
            // List buckets
            ListBucketsRequest listBucketsRequest = ListBucketsRequest.builder()
                    .maxBuckets(10)
                    .build();
            ListBucketsResponse listBucketsResponse =
 s3.listBuckets(listBucketsRequest);
            List<Bucket> buckets = listBucketsResponse.buckets();

            // Print bucket names
```

```
            System.out.println("Your Amazon S3 buckets are:");
            for (Bucket bucket : buckets) {
                System.out.println(bucket.name());
                System.out.println(bucket.getBucketRegion());
            }

        } catch (Exception e) {
            System.err.println("Error listing buckets: " + e.getMessage());
            e.printStackTrace();
        } finally {
            // Close the S3 client to release resources
            s3.close();
        }
    }
}
```

SDK for Go

```
package main
import (
 "context"
 "fmt"
 "log"
 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/config"
 "github.com/aws/aws-sdk-go-v2/service/s3"
)
func main() {
 cfg, err := config.LoadDefaultConfig(context.TODO(), config.WithRegion("us-
east-2"))
 if err != nil {
  log.Fatal(err)
 }
 client := s3.NewFromConfig(cfg)
 maxBuckets := 1000
 resp, err := client.ListBuckets(context.TODO(), management
 portals3.ListBucketsInput{MaxBuckets: aws.Int32(int32(maxBuckets))})
 if err != nil {
  log.Fatal(err)
 }
 fmt.Println("S3 Buckets:")
 for _, bucket := range resp.Buckets {
     fmt.Println("- Name:", *bucket.Name)
```

```
            fmt.Println("-BucketRegion", *bucket.BucketRegion)
        }
        fmt.Println(resp.ContinuationToken == nil)
        fmt.Println(resp.Prefix == nil)
    }
```

汎用バケットを空にする

汎用バケットの内容は、Amazon S3 コンソール、AWS SDK、または AWS Command Line Interface (AWS CLI) を使用して空にすることができます。汎用バケットを空にすると、すべてのオブジェクトが削除されますが、バケットは保持されます。バケットを空にすると、元に戻すことはできません。バケットを空にするアクションの実行中にバケットに追加されたオブジェクトは、削除される場合があります。バケット自体を削除する前に、バケット内のすべてのオブジェクト (すべてのオブジェクトバージョンと削除マーカーを含む) を削除する必要があります。

S3 バージョニングが有効または一時停止になっている汎用バケットを空にすると、バケット内のすべてのオブジェクトのすべてのバージョンが削除されます。詳細については、「バージョニングが有効なバケットでのオブジェクトの操作」を参照してください。

バケットを空にする場合は、すべての未完了のマルチパートアップロードも削除することをお勧めします。スループットを向上させ、ネットワーク問題からより迅速に復旧するため、マルチパートアップロードを使用して超大型のオブジェクト (最大 5 TB) を複数のパートから成るセットとしてアップロードすることができます。マルチパートアップロードのプロセスが完了しなかった場合、未完了のなパートが使用不可能な状態でバケットに残ります。これらの未完了のパートには、アップロードプロセスが完了するか、未完了の部分が削除されるまで、ストレージコストが発生します。詳細については、「Amazon S3 でのマルチパートアップロードを使用したオブジェクトのアップロードとコピー」を参照してください。

ベストプラクティスとして、ライフサイクルルールを設定して、特定の日数を過ぎたオブジェクトや未完了のマルチパートアップロードを期限切れにすることをお勧めします。未完了のマルチパートアップロードを期限切れにするライフサイクルルールを作成する場合は、7 日間から始めることをお勧めします。詳細については、「バケットに S3 ライフサイクル設定を設定する」を参照してください。

ライフサイクルの有効期限は非同期プロセスであるため、バケットが空になるまでルールの実行に数日かかる場合があります。Amazon S3 が初めてルールを実行すると、有効期限の対象となるすべてのオブジェクトに削除対象のマークが付けられます。削除対象としてマークされたオブジェクトに

ついては、請求が発生しなくなります。詳細については、「ライフサイクル設定ルールを使用して Amazon S3 バケットを空にするにはどうすればよいですか?」を参照してください。

S3 コンソールの使用

Amazon S3 コンソールを使用して汎用バケットを空にできます。バケット内のすべてのオブジェクトが削除され、バケット自体は削除されません。

S3 バケットを空にする

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[汎用バケット] を選択します。
3. バケットリストで、空にするバケットの名前の横にあるバケットアイコンを選択し、[空にする] を選択します。
4. [バケットを空にする] ページで、テキストフィールドにバケット名を入力することでバケットを空にすることを確定し、[Empty (空にする)] を選択します。
5. [バケットを空にする: ステータス] ページで、バケットを空にするプロセスの進行状況をモニタリングします。

AWS CLI の使用

AWS CLI を使用して汎用バケットを空にできるのは、バケットのバージョニングが有効になっていない場合のみです。バージョニングが有効化されていない場合は、AWS CLI コマンドの `rm` (削除) と `--recursive` パラメータを使って、バケットを空にすることができます (または、特定のキーネームプレフィックスを持つオブジェクトのサブセットを削除できます)。

次の `rm` コマンドは、たとえば doc や doc/doc1 といった、キーネームプレフィックス doc/doc2 を持つオブジェクトを削除します。

```
$ aws s3 rm s3://bucket-name/doc --recursive
```

プレフィックスを指定せずにすべてのオブジェクトを削除するには、次のコマンドを使用します。

```
$ aws s3 rm s3://bucket-name --recursive
```

詳細については、AWS Command Line Interface ユーザーガイドの「AWS CLI でのハイレベルな S3 コマンドの使用」を参照してください。

> **Note**
>
> バージョニングが有効化されたバケットから、オブジェクトを削除することはできません。Amazon S3 は、オブジェクトが削除される際に、このコマンドの目的である削除マーカーを追加します。S3 バケットのバージョニングの詳細については、「S3 バージョニングによる複数のバージョンのオブジェクトの保持」を参照してください。

AWS SDKs の使用

AWS SDK を使用して、汎用バケットを空にしたり、特定のキー名のプレフィックスを持つオブジェクトのサブセットを削除したりできます。

AWS SDK for Java を使ってバケットを空にする方法の例については、「汎用バケットの削除」を参照してください。このコードは、バケットのバージョニングが有効化されてるか否かにかかわらず、すべてのオブジェクトを削除します。それによって、このバケットは削除されます。単にバケットを空にしたいときは、バケットを削除するステートメントが解除されていることを確認します。

その他の AWS SDK の使用方法についての詳細は、「アマゾン ウェブ サービスのツール」を参照してください。

ライフサイクル設定の使用

大きな汎用バケットを空にするには、S3 ライフサイクル設定ルールを使用することをお勧めします。ライフサイクルの有効期限は非同期プロセスであるため、バケットが空になるまでのルールの実行には数日かかる場合があります。Amazon S3 が初めてルールを実行すると、有効期限の対象となるすべてのオブジェクトに削除対象のマークが付けられます。削除対象としてマークされたオブジェクトについては、請求が発生しなくなります。詳細については、「ライフサイクル設定ルールを使用して Amazon S3 バケットを空にするにはどうすればよいですか?」を参照してください。

ライフサイクル設定を使用してバケットを空にする場合、設定には、最新バージョン、最新でないバージョン、削除マーカー、および不完全なマルチパートアップロードが含まれている必要があります。

すべてのオブジェクト、または特定のキーネームプレフィックスが付いたオブジェクトのサブセットの期限が終了するようにライフサイクルの設定ルールを追加できます。たとえば、バケット内のすべてのオブジェクトを削除するには、作成後 1 日でオブジェクトが期限切れするようにライフサイクルのルールを設定できます。

Amazon S3 は、バケットライフサイクルルールがサポートしています。このルールを使用すると、開始後指定された日数内に完了しないマルチパートアップロードを停止できます。ストレージコストを最小限に抑えるように、このライフサイクルルールを設定することをお勧めします。詳細については、「不完全なマルチパートアップロードを削除するためのバケットライフサイクル設定の設定」を参照してください。

ライフサイクル設定を使用してバケットを空にする方法の詳細については、バケットに S3 ライフサイクル設定を設定する および オブジェクトの有効期限 を参照してください。

AWS CloudTrail が設定された汎用バケットを空にする

AWS CloudTrail は、Amazon S3 汎用バケット内のオブジェクトレベルのデータイベント (オブジェクトの削除など) を追跡します。CloudTrail イベントのログ記録先として汎用バケットを使用している場合、同じバケットからオブジェクトを削除してバケットを空にするときに新しいオブジェクトが作成される可能性があります。これを防ぐには、AWS CloudTrail 証跡を中止します。CloudTrail 証跡がイベントをログに記録しないようにする方法の詳細については、「AWS CloudTrail ユーザーガイド」の「証跡のログ記録をオフにする」を参照してください。

CloudTrail 証跡がバケットに追加されないようにするもう 1 つの方法は、バケットポリシーに `s3:PutObject` ステートメントを追加することです。後で新しいオブジェクトをバケットに保存する場合は、この deny `s3:PutObject` ステートメントを削除する必要があります。詳細については、「オブジェクト操作」および「IAM ユーザーガイド」の「IAM JSON ポリシー要素: 効果」を参照してください。

汎用バケットの削除

空の Amazon S3 汎用バケットを削除できます。汎用バケットを空にする方法については、「the section called “汎用バケットを空にする”」を参照してください。

Amazon S3 コンソール、AWS Command Line Interface (AWS CLI)、AWS SDK、または Amazon S3 REST API を使用してバケットを削除できます。

> **Important**
>
> 汎用バケットを削除する前に、以下の点を考慮してください。
>
> - 汎用バケット名はグローバル名前空間内で一意です。バケットを削除した場合、別の AWS アカウントが新しいバケットに同じ汎用バケット名を使用できるため、削除したバケットへのリクエストを受け取る可能性があることに注意してください。これを防ぐ場

合、または同じバケット名を使い続ける場合は、バケットを削除しないでください。バケットを空にして保持し、代わりに必要に応じてバケットリクエストをブロックすることをお勧めします。バケットがアクティブに使用されなくなった場合は、バケット自体を保持しながらコストを最小限に抑えるために、すべてのオブジェクトのバケットを空にすることをお勧めします。

- 汎用バケットを削除しても、バケットがすぐに削除されない場合があります。代わりに、Amazon S3 はバケットを削除キューに入れます。Amazon S3 は AWS リージョン全体に分散されるため、削除プロセスが完全に伝達され、システム全体で一貫性を実現するには時間がかかります。
- バケットが静的ウェブサイトをホストしていて、Amazon Route 53 ホストゾーンがチュートリアル: Route 53 に登録されたカスタムドメインを使用した静的ウェブサイトの設定 の説明通りに作成され設定されている場合は、バケットに関連する Route 53 ホストゾーンの設定をクリーンアップする必要があります。詳細については、「ステップ 2: Route 53 ホストゾーンを削除する」を参照してください。
- バケットに Elastic Load Balancing (ELB) からログデータを配信している場合は、バケットを削除する前に、バケットへの ELB ログの配信を停止することをお勧めします。バケットの削除後に、別のユーザーが同じ名前でバケットを作成した場合、そのバケットにログデータが配信される可能性があります。ELB アクセスログの詳細については、「Classic Load Balancer のユーザーガイド」の「Access logs for your Classic Load Balancer」、および「Application Load Balancer のユーザーガイド」の「Access logs for your Application Load Balancer」を参照してください。

トラブルシューティング

Amazon S3 汎用バケットを削除できない場合は、次の点を考慮してください。

- バケットが空であることを確認する — バケット内にオブジェクトがないバケットのみ削除できます。バケットが空であることを確認します。バケットを空にする方法については、「the section called “汎用バケットを空にする”」を参照してください。
- アクセスポイントがアタッチされていないことを確認する – バケットを削除できるのは、同じアカウント内に S3 アクセスポイントまたはマルチリージョンアクセスポイントがアタッチされていない場合に限ります。バケットを削除する前に、バケットにアタッチされている同一アカウントのアクセスポイントをすべて削除します。
- **`s3:DeleteBucket`** アクセス許可があることを確認する – バケットを削除できない場合は、IAM 管理者と協力して、`s3:DeleteBucket` アクセス許可があることを確認してください。IAM アク

セス許可を表示または更新する方法については、IAM ユーザーガイドの「IAM ユーザーの許可の変更」を参照してください。トラブルシューティング情報については、「the section called “アクセス拒否 (403 Forbidden) エラーのトラブルシューティング”」を参照してください。

- AWS Organizations サービスコントロールポリシー (SCP) とリソースコントロールポリシー (RCP) で **`s3:DeleteBucket Deny`** ステートメントを確認する – SCP と RCP は、バケットに対する削除のアクセス許可を拒否できます。詳細については、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシー」と「リソースコントロールポリシー」を参照してください。
- バケットポリシーの **`s3:DeleteBucket Deny`** ステートメントを確認する – IAM ユーザーまたはロールのポリシーに `s3:DeleteBucket` アクセス許可があり、バケットを削除できない場合は、バケットポリシーに `s3:DeleteBucket` に対する `Deny` ステートメントが含まれている場合があります。AWS Elastic Beanstalk によって作成されたバケットは、デフォルトでこのステートメントを含むポリシーを持っています。バケットを削除する前に、このステートメントまたはバケットポリシーを削除する必要があります。

前提条件

汎用バケットを削除するには、事前にバケットを空にする必要があります。バケットを空にする方法については、「the section called “汎用バケットを空にする”」を参照してください。

S3 コンソールの使用

S3 バケットを削除するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[汎用バケット] を選択します。
3. バケットリストで、削除するバケットの名前の横にあるオプションボタンを選択してから、ページの上部にある [削除] を選択します。
4. [バケットの削除] ページで、テキストフィールドにバケット名を入力することでバケットを削除することを確認し、[バケットを削除] を選択します。

> **Note**
>
> バケットにオブジェクトが含まれている場合は、[このバケットは空ではありません] というエラーアラートの [バケットを空にする] ボタンを選択し、[バケットを空にする]

ページの指示に従って、バケットを空にしてから削除します。次に、[バケットを削除する] ページに戻り、バケットを削除します。

5. バケットを削除したことを確認するには、[汎用バケット] リストを開き、削除したバケットの名前を入力します。バケットが見つからない場合、削除は成功しています。

AWS SDK for Java の使用

次の例は、AWS SDK for Java を使用して汎用バケットを空にして削除する方法を示しています。このコードは、まず汎用バケット内のすべてのオブジェクトを削除し、次にバケットを削除します。

他の言語の例については、「Amazon Simple Storage Service API リファレンス」の「AWS SDK または CLI で DeleteBucket を使用する」を参照してください。その他の AWS SDK の使用方法については、「Tools for Amazon Web Services」を参照してください。

Java

次の Java の例では、オブジェクトが含まれているバケットを削除します。すべてのオブジェクトを削除した後で、バケットを削除します。この例は、バージョニングの有無を問わず、使用できます。

> **Note**
>
> バージョニングが有効になっていないバケットの場合、すべてのオブジェクトを直接削除し、その後でバケットを削除できます。バージョニングが有効なバケットの場合は、バケットを削除する前に、すべてのオブジェクトバージョンを削除する必要があります。

作業サンプルの作成およびテストの手順については、「AWS SDK for Java 2.x デベロッパーガイド」を参照してください。

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.*;
```

```
import java.util.Iterator;

public class DeleteBucket2 {

    public static void main(String[] args) {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();

            // Delete all objects from the bucket. This is sufficient
            // for unversioned buckets. For versioned buckets, when you attempt to
 delete
            // objects, Amazon S3 inserts
            // delete markers for all objects, but doesn't delete the object
 versions.
            // To delete objects from versioned buckets, delete all of the object
 versions
            // before deleting
            // the bucket (see below for an example).
            ObjectListing objectListing = s3Client.listObjects(bucketName);
            while (true) {
                Iterator<S3ObjectSummary> objIter =
 objectListing.getObjectSummaries().iterator();
                while (objIter.hasNext()) {
                    s3Client.deleteObject(bucketName, objIter.next().getKey());
                }

                // If the bucket contains many objects, the listObjects() call
                // might not return all of the objects in the first listing. Check
 to
                // see whether the listing was truncated. If so, retrieve the next
 page of
                // objects
                // and delete them.
                if (objectListing.isTruncated()) {
                    objectListing = s3Client.listNextBatchOfObjects(objectListing);
                } else {
                    break;
                }
```

```
            }

            // Delete all object versions (required for versioned buckets).
            VersionListing versionList = s3Client.listVersions(new
 ListVersionsRequest().withBucketName(bucketName));
            while (true) {
                Iterator<S3VersionSummary> versionIter =
 versionList.getVersionSummaries().iterator();
                while (versionIter.hasNext()) {
                    S3VersionSummary vs = versionIter.next();
                    s3Client.deleteVersion(bucketName, vs.getKey(),
 vs.getVersionId());
                }

                if (versionList.isTruncated()) {
                    versionList = s3Client.listNextBatchOfVersions(versionList);
                } else {
                    break;
                }
            }

            // After all objects and object versions are deleted, delete the bucket.
            s3Client.deleteBucket(bucketName);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
 couldn't
            // parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

AWS CLI を使用する場合

オブジェクトを含む汎用バケットでバージョニングが有効になっていない場合は、バケットを AWS CLI で削除できます。オブジェクトを含むバケットを削除すると、S3 Glacier Flexible Retrieval スト

レージクラスに移行済みのオブジェクトを含む、そのバケット内にあるすべてのオブジェクトが完全に削除されます。

バケットのバージョニングが有効になっていない場合は、rb (バケット削除) の AWS CLI コマンドを --force パラメータと共に使用することで、バケットとその内部のオブジェクトのすべてを削除できます。このコマンドは、すべてのオブジェクトを削除した後にバケットを削除します。

バージョニングが有効になっている場合、--force パラメータと共に rb コマンドを使用しても、バージョニングされたオブジェクトは削除されず、バケットが空にならないため、バケットの削除は失敗します。バージョニングされたオブジェクトの削除については、「オブジェクトバージョンの削除」を参照してください。

次のコマンドを使用するには、*amzn-s3-demo-bucket* を削除するバケットの名前に置き換えます。

```
$ aws s3 rb s3://amzn-s3-demo-bucket --force
```

詳細については、「AWS Command Line Interface ユーザーガイド」の「Using High-Level S3 Commands with the AWS Command Line Interface」を参照してください。

Amazon S3 バケットをローカルファイルシステムとしてマウントする

Mountpoint for Amazon S3 は、Amazon S3 バケットをローカルファイルシステムとしてマウントするための、高スループットのオープンソースファイルクライアントです。Mountpoint を使用すると、アプリケーションは、開く、読み取るなどのファイルシステム操作を通じて Amazon S3 に保存されているオブジェクトにアクセスできます。Mountpoint はこれらの操作を S3 オブジェクト API 呼び出しに自動的に変換し、アプリケーションが Amazon S3 のエラスティックなストレージとスループットにファイルインターフェイスを通じてアクセスできるようにします。

Mountpoint for Amazon S3 は、データレイク、機械学習トレーニング、画像レンダリング、自動運転車シミュレーション、抽出、変換、ロード (ETL) など、本番環境での大規模な読み取り負荷の高いアプリケーション用に提供されています。

Mountpoint は基本的なファイルシステム操作をサポートし、最大 5 TB のサイズのファイルを読み取ることができます。既存のファイルを一覧表示して読み取ったり、新しいファイルを作成したりできます。既存のファイルの変更やディレクトリの削除はできません。シンボリックリンクやファイルロックもサポートしていません。Mountpoint は、共有ファイルシステムの機能や POSIX 形式のアクセス許可のすべては必要としないが、大規模な S3 データセットの読み書きに Amazon S3 のエラ

スティックなスループットを必要とするアプリケーションに最適です。詳細については、GitHub の「Mountpoint ファイルシステムの動作」を参照してください。POSIX の完全サポートを必要とするワークロードには、Amazon FSx for Lustre とその Amazon S3 バケットのリンクのサポートが推奨されます。

Mountpoint for Amazon S3 は、Linux オペレーティングシステム専用です。Mountpoint を使用して、S3 Glacier Flexible Retrieval、S3 Glacier Deep Archive、S3 Intelligent-Tiering Archive アクセス階層、および S3 Intelligent-Tiering Deep Archive アクセス階層を除くすべてのストレージクラスの S3 オブジェクトにアクセスできます。

トピック

- Mountpoint のインストール
- Mountpoint の設定と使用
- Mountpoint のトラブルシューティング

Mountpoint のインストール

Mountpoint for Amazon S3 のビルド済みパッケージの場合、コマンドラインを使用してダウンロードしてインストールできます。Mountpoint をダウンロードしてインストールする手順は、使用している Linux オペレーティングシステムによって異なります。

トピック

- RPM ベースのディストリビューション (Amazon Linux、Fedora、CentOS、RHEL)
- DEB ベースのディストリビューション (Debian、Ubuntu)
- 他の Linux ディストリビューション
- Mountpoint for Amazon S3 パッケージの署名を検証します。

RPM ベースのディストリビューション (Amazon Linux、Fedora、CentOS、RHEL)

1. 以下のダウンロード URL をアーキテクチャ用にコピーしてください。

   x86_64:

   ```
   https://s3.amazonaws.com/mountpoint-s3-release/latest/x86_64/mount-s3.rpm
   ```

   ARM64 (Graviton):

```
https://s3.amazonaws.com/mountpoint-s3-release/latest/arm64/mount-s3.rpm
```

2. Mountpoint for Amazon S3 パッケージをダウンロードします。*download-link* を、前のステップの適切なダウンロード URL に置き換えてください。

```
wget download-link
```

3. (オプション) ダウンロードしたファイルの整合性と信頼性を検証します。まず、アーキテクチャに適した署名 URL をコピーします。

   x86_64:

```
https://s3.amazonaws.com/mountpoint-s3-release/latest/x86_64/mount-s3.rpm.asc
```

   ARM64 (Graviton):

```
https://s3.amazonaws.com/mountpoint-s3-release/latest/arm64/mount-s3.rpm.asc
```

   次に、「Mountpoint for Amazon S3 パッケージの署名の検証」を参照してください。

4. 次のコマンドを使用して パッケージをインストールします。

```
sudo yum install ./mount-s3.rpm
```

5. 次のコマンドを入力して、Mountpoint が正常にインストールされていることを確認します。

```
mount-s3 --version
```

   次のような出力が表示されます:

```
mount-s3 1.3.1
```

DEB ベースのディストリビューション (Debian、Ubuntu)

1. ダウンロード URL をアーキテクチャ用にコピーしてください。

   x86_64:

```
https://s3.amazonaws.com/mountpoint-s3-release/latest/x86_64/mount-s3.deb
```

ARM64 (Graviton):

```
https://s3.amazonaws.com/mountpoint-s3-release/latest/arm64/mount-s3.deb
```

2. Mountpoint for Amazon S3 パッケージをダウンロードします。*download-link* を、前のステップの適切なダウンロード URL に置き換えてください。

```
wget download-link
```

3. (オプション) ダウンロードしたファイルの整合性と信頼性を検証します。まず、アーキテクチャに署名 URL をコピーします。

   x86_64:

```
https://s3.amazonaws.com/mountpoint-s3-release/latest/x86_64/mount-s3.deb.asc
```

   ARM64 (Graviton):

```
https://s3.amazonaws.com/mountpoint-s3-release/latest/arm64/mount-s3.deb.asc
```

   次に、「Mountpoint for Amazon S3 パッケージの署名の検証」を参照してください。

4. 次のコマンドを使用してパッケージをインストールします。

```
sudo apt-get install ./mount-s3.deb
```

5. 次のコマンドを実行して、Mountpoint for Amazon S3 が正常にインストールされていることを確認します。

```
mount-s3 --version
```

   次のような出力が表示されます:

```
mount-s3 1.3.1
```

他の Linux ディストリビューション

1. オペレーティングシステムのマニュアルを参照して、必須の FUSE と libfuse2 パッケージ。をインストールしてください。
2. ダウンロード URL をアーキテクチャ用にコピーしてください。

   x86_64:

   ```
   https://s3.amazonaws.com/mountpoint-s3-release/latest/x86_64/mount-s3.tar.gz
   ```

   ARM64 (Graviton):

   ```
   https://s3.amazonaws.com/mountpoint-s3-release/latest/arm64/mount-s3.tar.gz
   ```

3. Mountpoint for Amazon S3 パッケージをダウンロードします。*download-link* を、前のステップの適切なダウンロード URL に置き換えてください。

   ```
   wget download-link
   ```

4. (オプション) ダウンロードしたファイルの整合性と信頼性を検証します。まず、アーキテクチャに署名 URL をコピーします。

   x86_64:

   ```
   https://s3.amazonaws.com/mountpoint-s3-release/latest/x86_64/mount-s3.tar.gz.asc
   ```

   ARM64 (Graviton):

   ```
   https://s3.amazonaws.com/mountpoint-s3-release/latest/arm64/mount-s3.tar.gz.asc
   ```

   次に、「Mountpoint for Amazon S3 パッケージの署名の検証」を参照してください。
5. 次のコマンドを使用してパッケージをインストールします。

   ```
   sudo mkdir -p /opt/aws/mountpoint-s3 && sudo tar -C /opt/aws/mountpoint-s3 -xzf ./
   mount-s3.tar.gz
   ```

6. mount-s3 バイナリを PATH 環境変数に追加します。$HOME/.profile ファイルに、次の行を追加します。

```
export PATH=$PATH:/opt/aws/mountpoint-s3/bin
```

.profile ファイルを保存し、次のコマンドを実行します。

```
source $HOME/.profile
```

7. 次のコマンドを実行して、Mountpoint for Amazon S3 が正常にインストールされていることを確認します。

```
mount-s3 --version
```

次のような出力が表示されます:

```
mount-s3 1.3.1
```

Mountpoint for Amazon S3 パッケージの署名を検証します。

1. GnuPG (gpg コマンド) をインストールします。ダウンロードした Mountpoint for Amazon S3 の信頼性と整合性を検証するために必要です。GnuPG は、Amazon Linux Amazon マシンイメージ (AMI) にはデフォルトでインストールされます。GnuPG をインストール後、ステップ 2 に進みます。
2. 以下のコマンドを実行して Mountpoint パブリックキーをダウンロードします。

```
wget https://s3.amazonaws.com/mountpoint-s3-release/public_keys/KEYS
```

3. 以下のコマンドを実行して、Mountpoint パブリックキーをキーリングにインポートします。

```
gpg --import KEYS
```

4. 次のコマンドを実行して、Mountpoint パブリックキーのフィンガープリントを検証します。

```
gpg --fingerprint mountpoint-s3@amazon.com
```

表示されたフィンガープリント文字列が以下と一致することを確認します。

```
673F E406 1506 BB46 9A0E  F857 BE39 7A52 B086 DA5A
```

フィンガープリント文字列が一致しない場合は、Mountpoint のインストールを完了せずに AWS サポート に問い合わせてください。

5. パッケージ署名ファイルをダウンロードします。*signature-link* を、前のセクションの適切な署名リンクと置き換えます。

```
wget signature-link
```

6. 次のコマンドを実行して、ダウンロードしたパッケージの署名を検証します。*signature-filename* を、前のステップのファイル名に置き換えます。

```
gpg --verify signature-filename
```

例えば、RPM ベースのディストリビューション (Amazon Linux を含む) の場合は、次のコマンドを実行します。

```
gpg --verify mount-s3.rpm.asc
```

7. 出力にフレーズ `Good signature` が含まれている必要があります。出力にフレーズ `BAD signature` が含まれている場合、Mountpoint パッケージファイルを再ダウンロードし、上記の手順を繰り返します。問題が解決しない場合は、Mountpoint のインストールを完了せずに AWS サポート に問い合わせてください。

出力には、信頼できる署名に関する警告が含まれる場合があります。これは問題を示すものではありません。これは、Mountpoint パブリックキーを独自に検証していないことを意味するだけです。

Mountpoint の設定と使用

Mountpoint for Amazon S3 を使用するには、マウントする Amazon S3 バケットにアクセスできる有効な AWS 認証情報がホストに必要です。さまざまな認証方法については、GitHub の「Mountpoint AWS 認証情報」を参照してください。

たとえば、新しい AWS Identity and Access Management (IAM) ユーザーとロールをこの目的を作成できます。このロールに、マウントしたい 1 つまたは複数のバケットへのアクセス権があることを確認してください。インスタンスプロファイルを使って、IAM ロールを Amazon EC2 インスタンスに渡すことができます。

トピック

- Mountpoint for Amazon S3 の使用
- Mountpoint でのキャッシュの設定

Mountpoint for Amazon S3 の使用

Mountpoint for Amazon S3 を使用して次の操作を行います。

1. Amazon S3 バケットをマウントします。

   a. `mount-s3` コマンドを使用して、Amazon S3 バケットを手動でマウントできます。

      以下の例では、*amzn-s3-demo-bucket* を S3 バケットの名前に置き換え、*~/mnt* を S3 バケットをマウントしたいホスト上のディレクトリに置き換えます。

      ```
      mkdir ~/mnt
      mount-s3 amzn-s3-demo-bucket ~/mnt
      ```

      デフォルトでは Mountpoint クライアントがバックグラウンドで実行されるため、*~/mnt* ディレクトリから Amazon S3 バケット内のオブジェクトにアクセスできるようになりました。

   b. または、インスタンスの起動時または再起動時に Amazon S3 バケットを自動的にマウントするように設定することもできます。

      既存または実行中の Amazon EC2 インスタンスの場合は、Linux システムの `/etc/fstab` ディレクトリで `fstab` ファイルを見つけます。次に、`fstab` ファイルに 1 行追加します。例えば、プレフィックス `example-prefix/` を使用して *amzn-s3-demo-bucket* をシステムパス `/mnt/mountpoint` にマウントするには、以下を参照してください。次の例を使用する際は、*###############*を独自の情報に置き換えます。

      ```
      s3://amzn-s3-demo-bucket/example-prefix/ /mnt/mountpoint mount-s3
       _netdev,nosuid,nodev,nofail,rw 0 0
      ```

      この例で使用されているオプションの説明については、次の表を参照してください。

オプション	説明
_netdev	ファイルシステムのマウントにネットワーク接続が必要であることを指定します。
nosuid	ファイルシステムに設定されたユーザー ID ファイルを含めることができないことを指定します。
nodev	ファイルシステムに特別デバイスを含めることができないことを指定します。
nofail	ファイルシステムのマウントに失敗しても、システムの起動を許可することを指定します。
rw	マウントポイントが読み取りおよび書き込みアクセス許可で作成されることを指定します。読み取り専用の場合は ro を使用します。

新しい Amazon EC2 インスタンスの場合、Amazon EC2 テンプレートのユーザーデータを変更し、fstab ファイルを次のように設定できます。次の例を使用する際は、*########*を独自の情報に置き換えます。

```
#!/bin/bash -e
MP_RPM=$(mktemp --suffix=.rpm)
curl https://s3.amazonaws.com/mountpoint-s3-release/latest/x86_64/mount-s3.rpm
 > $MP_RPM
yum install -y $MP_RPM
rm $MP_RPM

MNT_PATH=/mnt/mountpoint
echo "s3://amzn-s3-demo-bucket/ ${MNT_PATH} mount-s3
 _netdev,nosuid,nodev,rw,allow-other,nofail" >> /etc/fstab
mkdir $MNT_PATH

systemctl daemon-reload
```

```
mount -a
```

2. Mountpoint を通じて Amazon S3 バケット内のオブジェクトにアクセスします。

   バケットをローカルにマウントしたら、`cat` や `ls` などの一般的な Linux コマンドして、S3 オブジェクトを操作することができます。Mountpoint for Amazon S3 は、Amazon S3 バケット内のキーをフォワードスラッシュ (/) 文字で分割することでファイルシステムパスとして解釈します。たとえば、`Data/2023-01-01.csv` バケットにオブジェクトキーがある場合、Mountpoint ファイルに `Data` という名前のディレクトリがあり、その中には `2023-01-01.csv` という名前のファイルがあります。

   Mountpoint for Amazon S3 は、ファイルシステムに意図的に完全な POSIX 標準仕様を実装していません。Mountpoint は、ファイルシステムインターフェイスを通じて Amazon S3 に保存されているデータへの高スループットの読み取り/書き込みアクセスを必要しながらも、それ以外はファイルシステム機能に依存しないワークロード向けに最適化されています。詳細については、GitHub の「Mountpoint for Amazon S3 ファイルシステムの動作」を参照してください。より豊富なファイルシステムセマンティクスを必要とするお客様は、他の AWS ファイルサービス (例: Amazon Elastic File System (Amazon EFS) または Amazon FSx) などを検討してください。

3. `umount` コマンドを使用して Amazon S3 バケットをアンマウントします。このコマンドは S3 バケットをアンマウントし、マウントポイントを終了します。

   以下のコマンド例を使用するには、*`~/mnt`* を S3 バケットがマウントされているホスト上のディレクトリに置き換えます。

   ```
   umount ~/mnt
   ```

   > **Note**
   >
   > このコマンドのオプションのリストを取得するには、`umount --help` を実行します。

マウントポイント設定の詳細については、GitHub の「Amazon S3 bucket configuration」、および「file system configuration」を参照してください。

Mountpoint でのキャッシュの設定

Mountpoint for Amazon S3 は、さまざまなタイプのデータキャッシュをサポートしています。繰り返しの読み取りリクエストを高速化するには、以下にオプトインできます。

- ローカルキャッシュ – Amazon EC2 インスタンスストレージまたは Amazon Elastic Block Store ボリュームでローカルキャッシュを使用できます。同じコンピューティングインスタンスから同じデータを繰り返し読み取り、繰り返し読み取るデータセット用のローカルインスタンスストレージに未使用のスペースがある場合は、ローカルキャッシュにオプトインします。
- 共有キャッシュ – S3 Express One Zone で共有キャッシュを使用できます。複数のコンピューティングインスタンスから小さなオブジェクトを繰り返し読み取る場合、または繰り返し読み取るデータセットのサイズが不明で、キャッシュサイズの伸縮性を活用する場合は、共有キャッシュにオプトインします。オプトインすると、Mountpoint は、S3 Express One Zone を使用するディレクトリバケットに最大 1 メガバイトのサイズのオブジェクトを保持します。
- ローカルキャッシュと共有キャッシュの組み合わせ — ローカルキャッシュに未使用のスペースがあるが、複数のインスタンス間で共有キャッシュも必要な場合は、ローカルキャッシュと共有キャッシュの両方にオプトインできます。

Mountpoint でのキャッシュは、複数の読み取り中に変更されない同じデータを繰り返し読み取るユースケースに最適です。たとえば、モデルの精度を向上させるためにトレーニングデータセットを複数回読み取る必要がある機械学習トレーニングジョブでキャッシュを使用できます。

Mountpoint でキャッシュを設定する方法の詳細については、以下の例を参照してください。

トピック

- ローカルキャッシュ
- 共有キャッシュ
- ローカルキャッシュと共有キャッシュの組み合わせ

ローカルキャッシュ

`--cache` *`CACHE_PATH`* フラグを使用してローカルキャッシュにオプトインできます。次の例の、*`CACHE_PATH`* は、データをキャッシュするディレクトリへのファイルパスに置き換えます。*`amzn-s3-demo-bucket`* は Amazon S3 バケット名に置き換え、*`~/mnt`* を S3 バケットをマウントするホスト上のディレクトリに置き換えます。

```
mkdir ~/mnt
mount-s3 --cache CACHE_PATH amzn-s3-demo-bucket ~/mnt
```

Amazon S3 バケットをマウントするときにローカルキャッシュにオプトインすると、Mountpoint は設定されたキャッシュの場所に空のサブディレクトリを作成します (そのサブディレクトリがまだ存

在しない場合)。最初にバケットをマウントするときと、マウントを解除するときに、Mountpoint はローカルキャッシュのコンテンツを削除します。

> **Important**
>
> ローカルキャッシュを有効にすると、Mountpoint は、マウントした Amazon S3 バケットの暗号化されていないオブジェクトのコンテンツを、マウント時に指定したローカルキャッシュの場所に保持します。データを保護するには、ファイルシステムのアクセスコントロールメカニズムを使用して、データキャッシュの場所へのアクセスを制限する必要があります。

共有キャッシュ

複数のコンピューティングインスタンスから小さなオブジェクト (最大 1 MB) を繰り返し読み取る場合、または繰り返し読み取るデータセットのサイズがローカルキャッシュのサイズを頻繁に超える場合は、S3 Express One Zone の共有キャッシュを使用する必要があります。複数のインスタンスから同じデータを繰り返し読み取る場合、マウントした Amazon S3 バケットへの冗長なリクエストを回避することで、レイテンシーが向上します。

共有キャッシュにオプトインすると、S3 Express One Zone のディレクトリバケットにキャッシュされたデータに対して料金が発生します。また、S3 Express One Zone のディレクトリバケットのデータに対して行ったリクエストに対しても料金が発生します。詳細については、「Amazon S3 の料金」を参照してください。Mountpoint は、ディレクトリバケットからキャッシュされたオブジェクトを削除することはありません。ストレージコストを管理するには、指定した期間後に S3 Express One Zone にキャッシュされたデータの有効期限が切れるように、ディレクトリバケットにライフサイクルポリシーを設定する必要があります。詳細については、GitHub で Mountpoint for Amazon S3 のキャッシュ設定に関する情報を参照してください。

コンピューティングインスタンスに Amazon S3 バケットをマウントするときに S3 Express One Zone のキャッシュにオプトインするには、`--cache-xz` フラグを使用して、キャッシュの場所としてディレクトリバケットを指定します。次の例で、*##############*を置き換えます。

```
mount-s3 amzn-s3-demo-bucket ~/mnt --cache-xz amzn-s3-demo-bucket--usw2-az1--x-s3
```

ローカルキャッシュと共有キャッシュの組み合わせ

インスタンスに未使用のスペースがあるが、複数のインスタンスで共有キャッシュも使用する場合は、ローカルキャッシュと共有キャッシュの両方にオプトインできます。このキャッシュ設定では、

必要なデータをローカルストレージにキャッシュするときに、同じインスタンスからディレクトリバケットの共有キャッシュへの冗長な読み取りリクエストを回避できます。これにより、リクエストのコストを削減し、パフォーマンスを改善できます。

Amazon S3 バケットをマウントするときにローカルキャッシュと共有キャッシュの両方にオプトインするには、--cache フラグと --cache-xz フラグを使用して両方のキャッシュの場所を指定します。次の例を使用してローカルキャッシュと共有キャッシュの両方にオプトインするには、*##### #########*を置き換えます。

```
mount -s3 amzn-s3-demo-bucket ~/mnt --cache /path/to/mountpoint/cache --cache -xz amzn-s3-demo-bucket--usw2-az1--x-s3
```

詳細については、GitHub で Mountpoint for Amazon S3 のキャッシュ設定に関する情報を参照してください。

> **Important**
>
> 共有キャッシュを有効にすると、Mountpoint は、マウントされた Amazon S3 バケットのオブジェクトコンテンツを、共有キャッシュの場所として指定した S3 ディレクトリバケットにコピーし、S3 ディレクトリバケットにアクセスできる任意の発信者がアクセスできるようにします。キャッシュされたデータを保護するには、Amazon S3 のセキュリティのベストプラクティス に従って、バケットが正しいポリシーを使用していること、およびパブリックにアクセスできないことを確認する必要があります。Mountpoint 共有キャッシュ専用のディレクトリバケットを使用し、Mountpoint クライアントにのみアクセスを許可する必要があります。

Mountpoint のトラブルシューティング

Mountpoint for Amazon S3 は、サポート によってサポートされています。サポートが必要な場合は、AWS サポート センターまでご連絡ください。

GitHub の Mountpoint 問題を確認して提出することもできます。

このプロジェクトで潜在的なセキュリティ上の問題を発見した場合、脆弱性報告ページから AWS セキュリティにその旨をお知らせください。GitHub で公開されている問題はご報告いただく必要はありません。

アプリケーションが Mountpoint で予期しない動作をする場合は、ログ情報を調べて問題を診断できます。

ログ記録

デフォルトでは、Mountpoint は重要度の高いログ情報をに syslog に出力します。

Amazon Linux を含む最新の Linux ディストリビューションを表示するには、`journald` コマンドを実行します。

```
journalctl -e SYSLOG_IDENTIFIER=mount-s3
```

その他の Linux システムでは、`syslog` エントリは `/var/log/syslog` のようなファイルに書き込まれる可能性があります

これらのログは、アプリケーションのトラブルシューティングに使用できます。たとえば、アプリケーションが既存のファイルを上書きしようとすると操作は失敗し、ログには次のような行が表示されます。

```
[WARN] open{req=12 ino=2}: mountpoint_s3::fuse: open failed: inode error: inode 2 (full
 key "README.md") is not writable
```

詳細については、GitHub の「Mountpoint for Amazon S3 ログ記録」を参照してください。

Storage Browser for Amazon S3 の使用

Storage Browser for S3 は、エンドユーザーに Amazon S3 に保存されたデータ用のシンプルなグラフィカルインターフェイスを提供するために、ウェブアプリケーションに追加できるオープンソースコンポーネントです。Storage Browser for S3 を使用すると、承認されたエンドユーザーに、S3 内のデータを独自のアプリケーションから直接参照、ダウンロード、アップロード、コピー、削除するためのアクセスを提供できます。

Storage Browser for S3 では、ファイルに対して `LIST`、`GET`、`PUT`、`COPY`、`UPLOAD`、および `DELETE` のオペレーションがサポートされています。高スループットのデータ転送を実現するために、Storage Browser for S3 には、エンドユーザーがアクセスを許可されているデータのみが表示され、アップロードリクエストが最適化されます。また、Storage Browser は、パフォーマンスを最適化してロード時間を短縮し、エンドユーザーがアップロードするデータのチェックサムを計算し、パブリックインターネット上でデータの整合性が (転送中に) 維持されたことを確認した後にオブジェ

クトを受け入れます。AWS セキュリティおよび ID サービス、または独自のマネージドサービスを使用して、エンドユーザーの ID に基づいてデータへのアクセスを制御できます。既存のアプリケーションの設計やブランドに合わせて Storage Browser をカスタマイズすることもできます。

Storage Browser for S3 は、React フレームワーク上のウェブおよびイントラネットアプリケーションでのみ使用できます。Storage Browser を使用して、S3 Glacier Flexible Retrieval、S3 Glacier Deep Archive、S3 Intelligent-Tiering Archive アクセス階層、および S3 Intelligent-Tiering Deep Archive アクセス階層を除くすべてのストレージクラスの Amazon S3 オブジェクトにアクセスできます。

Storage Browser for S3 は、AWS Amplify React ライブラリのウェブアプリケーションで使用できます。Storage Browser の詳細については、「Storage Browser for S3」を参照してください。

トピック

- Storage Browser for S3 の使用
- Storage Browser for S3 のインストール
- Storage Browser for S3 の設定
- Storage Browser for S3 の設定
- Storage Browser for S3 のトラブルシューティング

Storage Browser for S3 の使用

Storage Browser for S3 の場合、場所とは S3 汎用バケットまたはプレフィックスのことで、S3 Access Grants、IAM ポリシー、または独自のマネージド認可サービスを使用するアクセス権をエンドユーザーに付与します。エンドユーザーが特定の場所にアクセスすることを認証したら、その場所内の任意のデータを操作できます。

Storage Browser for S3 ユーザーインターフェイスには、次の 4 つのメインビューがあります。

- ホームページ: ホームページには、ユーザーがアクセスできる S3 の場所と、それぞれのアクセス許可が一覧表示されます。これは、エンドユーザーがアクセスできるルートレベルの S3 リソースと、各 S3 の場所に対するアクセス許可 (READ/WRITE/READWRITE) を表示するユーザーの初期ビューです。
- 場所の詳細: このビューでは、ユーザーは S3 内のファイルとフォルダを参照し、ファイルをアップロードまたはダウンロードできます。(Storage Browser for S3 では、オブジェクトはファイル、プレフィックスとバケットはフォルダと呼ばれます。)

- 場所のアクション: ユーザーが Storage Browser でアクション ([アップロード] など) を選択すると、ファイルの場所の別のビューが開きます。
- 縦の省略記号: 縦の省略記号のアイコンは、アクションのドロップダウンリストを開きます。

Storage Browser for S3 を使用する場合は、次の制限事項に注意してください。

- ドット (.) で始まる、または終わるフォルダはサポートされていません。
- WRITE のみのアクセス許可を持つ S3 Access Grants はサポートされていません。
- Storage Browser for S3 は、最大 160 GB のサイズのファイルに対する PUT オペレーションをサポートします。
- Storage Browser for S3 は、5 GB 未満のファイルに対してのみ COPY オペレーションをサポートします。ファイルサイズが 5 GB を超えると、Storage Browser はリクエストに失敗します。

Storage Browser for S3 のインストール

Storage Browser の使用を開始する最も簡単な方法は、GitHub のサンプルプロジェクトの 1 つをクローンすることです。これらのサンプルプロジェクトを利用すると、AWS Identity and Access Management 用の AWS サービスが事前に統合された、Storage Browser 向けの本番稼働用ウェブアプリケーションを簡単にデプロイして、承認されたエンドユーザーを S3 のデータにすばやく接続できます。

詳細については、「Amplify Dev Center」の「Quick start」を参照してください。

GitHub からの Storage Browser for S3 のインストール

または、aws-amplify GitHub リポジトリの最新バージョンの `aws-amplify/ui-react-storage` および `aws-amplify` パッケージから Storage Browser for S3 をインストールして、既存のアプリケーションへの Storage Browser の統合を開始することもできます。Storage Browser for S3 をインストールするときは、次の依存関係を `package.json` ファイルに追加してください。

```
"dependencies": {
    "aws-amplify/ui-react-storage": "latest",
    "aws-amplify": "latest",
  }
```

または、Node Package Manager (NPM) を使用して依存関係を追加することもできます。

```
npm i --save @aws-amplify/ui-react-storage aws-amplify
```

Storage Browser for S3 の設定

エンドユーザーを Amazon S3 の場所に接続するには、まず認証と認可の方法を設定する必要があります。Storage Browser で認証と認可の方法を設定するには、次の 3 つの方法があります。

- 方法 1: 顧客およびサードパーティーパートナーのデータアクセスの管理
- 方法 2: AWS アカウント用 IAM プリンシパルのデータアクセスの管理
- 方法 3: 大規模なデータアクセスの管理

方法 1: 顧客およびサードパーティーパートナーのデータアクセスの管理

この方法では、AWS Amplify Auth を使用してファイルのアクセスコントロールとセキュリティを管理できます。この方法は、顧客またはサードパーティーのパートナーを S3 のデータに接続する場合に最適です。このオプションを使用すると、顧客はソーシャル ID プロバイダーまたはエンタープライズ ID プロバイダーを使用して認証できます。

Amplify Storage を使用するように設定された S3 バケットで AWS Amplify Auth を使用して、エンドユーザーとサードパーティーのパートナーに IAM 認証情報を提供します。AWS AmplifyAuth は、フルマネージドの顧客 ID およびアクセス管理サービスである Amazon Cognito 上に構築されており、組み込みのユーザーディレクトリまたはエンタープライズディレクトリ、またはコンシューマー ID プロバイダーからユーザーを認証および認可できます。Amplify 認可モデルは、現在の認証済みユーザーがアクセスできるプレフィックスを定義します。AWS Amplify に対する認可を設定する方法の詳細については、「Set up storage」を参照してください。

Amplify 認証およびストレージメソッドを使用してコンポーネントを初期化するには、ウェブアプリケーションに次のコードスニペットを追加します。

```
import {
  createAmplifyAuthAdapter,
  createStorageBrowser,
} from '@aws-amplify/ui-react-storage/browser';
import "@aws-amplify/ui-react-storage/styles.css";

import config from './amplify_outputs.json';

Amplify.configure(config);
```

```
export const { StorageBrowser } = createStorageBrowser({
  config: createAmplifyAuthAdapter(),
});
```

方法 2: AWS アカウント用 IAM プリンシパルのデータアクセスの管理

IAM プリンシパルまたは AWS アカウントへのアクセスを直接管理する場合は、GetDataAccess S3 API オペレーションを呼び出すアクセス許可を持つ IAM ロールを作成できます。これを設定するには、S3 Access Grants インスタンスを作成して、S3 汎用バケットとプレフィックスのアクセス許可を指定先の IAM ID にマッピングする必要があります。Storage Browser コンポーネント (IAM 認証情報を取得した後にクライアント側で呼び出す必要がある) は、次に ListCallerAccessGrants S3 API オペレーションを呼び出して、ID リクエスタに使用可能な権限を取得し、コンポーネント内の場所を入力します。`s3:GetDataAccess` アクセス許可を取得すると、Storage Browser コンポーネントはそれらの認証情報を使用して S3 へのデータアクセスをリクエストします。

```
import {
  createManagedAuthAdapter,
  createStorageBrowser,
} from '@aws-amplify/ui-react-storage/browser';
import "@aws-amplify/ui-react-storage/styles.css";

export const { StorageBrowser } = createStorageBrowser({
  config: createManagedAuthAdapter({
    credentialsProvider: async (options?: { forceRefresh?: boolean }) => {
      // return your credentials object
      return {
        credentials: {
          accessKeyId: 'my-access-key-id',
          secretAccessKey: 'my-secret-access-key',
          sessionToken: 'my-session-token',
          expiration: new Date()
        },
      }
    },
    // AWS `region` and `accountId`
    region: '',
    accountId: '',
    // call `onAuthStateChange` when end user auth state changes
    // to clear sensitive data from the `StorageBrowser` state
    registerAuthListener: (onAuthStateChange) => {},
  })
```

```
});
```

方法 3: 大規模なデータアクセスの管理

S3 Access Grants インスタンスを IAM アイデンティティセンターに関連付けて、よりスケーラブルなソリューション (会社全体にデータアクセスを提供するなど) を行う場合は、現在の認証済みユーザーに代わって Amazon S3 にデータをリクエストできます。例えば、企業ディレクトリ内のユーザーグループに S3 内のデータへのアクセスを許可できます。このアプローチにより、Microsoft Entra、Okta などの外部プロバイダーでホストされているアクセス許可など、ユーザーとグループの S3 Access Grants アクセス許可を一元管理できます。

この方法を使用する場合、IAM アイデンティティセンターとの統合により、既存のユーザーディレクトリを使用できます。IAM アイデンティティセンターの信頼できる ID の伝播のもう 1 つの利点は、Amazon S3 の AWS CloudTrail データイベントそれぞれに、S3 データにアクセスしたエンドユーザー ID への直接参照が含まれていることです。

OAuth 2.0 をサポートするアプリケーションがあり、ユーザーがこれらのアプリケーションから AWS サービスにアクセスする必要がある場合、信頼できる ID の伝播を使用することをお勧めします。信頼できる ID の伝播を使用すると、ユーザーはアプリケーションにサインインでき、そのアプリケーションは AWS サービス内のデータにアクセスするすべてのリクエストにユーザーの ID を渡すことができます。このアプリケーションは、認証されたユーザーに代わって IAM アイデンティティセンターとやり取りします。詳細については、「Using trusted identity propagation with customer managed applications」を参照してください。

信頼された ID の伝播は、接続された AWS のサービス の管理者がサービスデータへのアクセスを許可および監査するために使用できる AWS IAM Identity Center 機能です。このデータへのアクセスは、グループの関連付けなどのユーザー属性に基づいています。信頼された ID の伝播を設定するには、接続された AWS のサービス の管理者と IAM アイデンティティセンターの管理者とのコラボレーションが必要です。詳細については、「Prerequisites and considerations」を参照してください。

セットアップ

S3 Access Grants と IAM アイデンティティセンターの信頼できる ID 伝播を使用して AWS Management Console で Storage Browser 認証を設定するには、アプリケーションが現在の認証済みユーザーに代わって Amazon S3 にデータをリクエストする必要があります。この方法では、企業ディレクトリのユーザーまたはユーザーのグループに S3 バケット、プレフィックス、またはオブジェクトへの直接アクセスを許可できます。つまり、アプリケーションはユーザーを IAM プリンシパルにマッピングする必要はありません。

次のワークフローは、IAM アイデンティティセンターと S3 Access Grants を使用して Storage Browser for S3 を設定する手順の概要を示しています。

ステップ	説明
1	AWS Organizations で IAM アイデンティティセンターを有効にする
2	AWS Identity and Access Management アイデンティティセンターフェデレーションを設定する
3	AWS Identity and Access Management アイデンティティセンターコンソールで信頼できるトークン発行者を追加する 信頼されたトークン発行者は、IAM アイデンティティセンター内の外部 ID プロバイダー (IdP) を表し、アプリケーションの認証済みユーザーの ID トークンを認識できるようにします。
4	`bootstrap` アプリケーションと `identity bearer` 用の IAM ロールを作成する
5	IAM アイデンティティセンターでアプリケーションを作成および設定する このアプリケーションは、認証されたユーザーに代わって IAM アイデンティティセンターとやり取りします。
6	S3 Access Grants を ID 伝播用の信頼されたアプリケーションとして追加する このステップでは、アプリケーションを S3 Access Grants に接続し、認証されたユーザーに代わって S3 Access Grants にリクエストできるようにします。
7	ユーザーまたはグループへの許可を作成する このステップでは、AWS Identity and Access Management アイデンティティセンターのユーザーをクロスドメインアイデンティティ管理 (SCIM) のシステムと同期します。SCIM は、IAM

ステップ	説明
	アイデンティティセンターの ID と ID プロバイダー (IdP) の ID を同期させます。
8	Storage Browser for S3 コンポーネントを作成する

AWS Organizations で IAM アイデンティティセンターを有効にする

IAM アイデンティティセンターを有効にするには、以下の手順に従います。

1. 次のいずれかの方法を使用して、AWS Management Consoleにサインインします。
    1. [新規の AWS (ルートユーザー)] – [ルートユーザー] を選択し、AWS アカウント E メールアドレスを入力して、アカウント所有者としてサインインします。次のページでパスワードを入力します。
    2. [既に使用している AWS (IAM 認証情報)] — 管理者権限を持つ IAM 認証情報を使用してサインインします。
2. IAM Identity Center コンソール を開きます。
3. [IAM Identity Center を有効にする] で、[有効にする] を選択します。

> **Note**
>
> IAM アイデンティティセンターには AWS Organizations の設定が必要です。組織をまだ設定していない場合は、AWS が作成するように選択できます。このプロセスを完了するには、 AWS 組織の作成 を選択します。

4. [AWS Organizations で有効化] を選択します。
5. [続行] をクリックしてください。
6. (オプション) この組織インスタンスに関連付けるタグを追加します。
7. (オプション) 委任管理を設定します。

> **Note**
>
> マルチアカウント環境を使用している場合は、委任管理を設定することをお勧めします。委任管理では、AWS Organizations の管理アカウントへのアクセスを必要とする

ユーザーの数を制限できます。詳細については、「Delegated admin」を参照してください。

8. [保存] を選択します。

AWS Organizations は、管理アカウントに関連付けられているアドレスに確認 E メールを自動的に送信します。検証 E メールの受信には時間がかかる場合があります。検証 E メールの有効期限が切れる前に、必ず 24 時間以内に E メールアドレスを確認してください。

AWS Identity and Access Management アイデンティティセンターフェデレーションを設定する

企業ディレクトリユーザーで Storage Browser for S3 を使用するには、外部 ID プロバイダー (IdP) を使用するように IAM アイデンティティセンターを設定する必要があります。選択した推奨 ID プロバイダーを使用できます。ただし、各 ID プロバイダーは異なる構成設定を使用することに注意してください。さまざまな外部 ID プロバイダーの使用に関するチュートリアルについては、「IAM Identity Center source tutorials」を参照してください。

> **Note**
>
> 設定した ID プロバイダーの発行者 URL と対象者属性は、後のステップで参照する必要があるため、必ず記録してください。IdP の設定に必要なアクセス許可またはアクセス許可がない場合は、外部 IdP の管理者に連絡して取得する必要がある場合があります。

AWS Identity and Access Management アイデンティティセンターコンソールで信頼できるトークン発行者を追加する

信頼できるトークン発行者は、AWS Identity and Access Management アイデンティティセンターの外部 ID プロバイダーを表し、アプリケーションの認証済みユーザーのトークンを認識します。AWS Organizations の IAM アイデンティティセンターインスタンスのアカウント所有者は、以下の手順を実行する必要があります。これらの手順は、IAM アイデンティティセンターコンソールまたはプログラムで実行できます。

AWS Identity and Access Management アイデンティティセンターコンソールで信頼できるトークン発行者を追加するには、次の手順を実行します。

1. IAM Identity Center コンソール を開きます。
2. [設定] を選択します。
3. [認証] タブを選択します。

4. [信頼できるトークン発行者] セクションに移動し、次の詳細を入力します。

    1. [発行者 URL] に、信頼できるトークン発行者として機能する外部 IdP の URL を入力します。この情報を取得するには、外部 IdP の管理者に連絡する必要がある場合があります。詳細については、「Using applications with a trusted token issuer」を参照してください。
    2. [信頼できるトークン発行者名] に、信頼できるトークン発行者の名前を入力します。この名前は、アプリケーションリソースが ID の伝播用に設定されている場合、ステップ 8 で選択できる信頼できるトークン発行者のリストに表示されます。
5. [マップ属性] を任意のアプリケーション属性に更新します。ここで、各 ID プロバイダー属性は IAM アイデンティティセンター属性にマッピングされます。例えば、IAM アイデンティティセンターのユーザー属性 `email` にアプリケーション属性 `email` をマッピングする場合があります。IAM アイデンティティセンターで許可されるユーザー属性のリストを確認するには、「Attribute mappings for AWS Managed Microsoft AD directory」の表を参照してください。
6. (オプション) リソースタグを追加する場合は、キーと値のペアを入力します。複数のリソースタグを追加するには、[新しいタグを追加] を選択して新しいエントリを生成し、キーと値のペアを入力します。
7. [信頼できるトークン発行者を作成] を選択します。
8. 信頼できるトークン発行者の作成が完了したら、アプリケーション管理者に連絡して信頼できるトークン発行者の名前を伝えて、管理者が信頼できるトークン発行者が該当するコンソールに表示されることを確認できるようにします。
9. アプリケーション管理者が、必ず該当するコンソールでこの信頼できるトークン発行者を選択していることを確認してください。これにより、信頼できる ID が伝播されるように構成されたアプリケーションからユーザーがアプリケーションにアクセスできるようになります。

bootstrap アプリケーションと **identity bearer** 用の IAM ロールを作成する

`bootstrap` アプリケーションと `identity bearer` ユーザーが適切に連携できるようにするには、必ず IAM ロールを 2 つ作成してください。`bootstrap` アプリケーションに 1 つの IAM ロールが必要であり、ID ベアラー、つまり S3 Access Grants を介してアクセスをリクエストするウェブアプリケーションにアクセスするエンドユーザーがもう 1 つの IAM ロールを使用する必要があります。`bootstrap` アプリケーションは、ID プロバイダーによって発行されたトークンを受け取り、`CreateTokenWithIAM` API を呼び出し、このトークンをアイデンティティセンターによって発行されたトークンと交換します。

次のようなアクセス許可を持つ `bootstrap-role` などの IAM ロールを作成します。次の IAM ポリシーの例では、トークン交換を実行するためのアクセス許可を `bootstrap-role` に付与します。

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": [
            "sso-oauth:CreateTokenWithIAM",
        ],
        "Resource": "arn:${Partition}:sso::${AccountId}:application/${InstanceId}/
${ApplicationId}",
        "Effect": "Allow"
    },
    {
        "Action": [
            "sts:AssumeRole",
            "sts:SetContext"
        ],
        "Resource": "arn:aws:iam::${AccountId}:role/identity-bearer-role",
        "Effect": "Allow"
    }]
}
```

次に、ID ブローカーが IAM 認証情報の生成に使用する、2 番目の IAM ロール (identity-bearer-role など) を作成します。ID ブローカーからウェブアプリケーションに返される IAM 認証情報は、S3 データへのアクセスを許可するために Storage Browser for S3 コンポーネントによって使用されます。

```
{
    "Action": [
        "s3:GetDataAccess",
        "s3:ListCallerAccessGrants",
    ],
    "Resource": "arn:${Partition}:s3:${Region}:${Account}:access-grants/default",
    "Effect": "Allow"
}
```

この IAM ロール (identity-bearer-role) は、次のステートメントを含む信頼ポリシーを使用する必要があります。

```
{
   "Effect": "Allow",
   "Principal": {
      "AWS": "arn:${Partition}:iam::${Account}:role/${RoleNameWithPath}"
```

```
    },
    "Action": [
        "sts:AssumeRole",
        "sts:SetContext"
    ]
}
```

IAM アイデンティティセンターでアプリケーションを作成および設定する

> **Note**
>
> 開始する前に、前のステップで必要な IAM ロールが作成されていることを確認してください。このステップでは、これらの IAM ロールのいずれかを指定する必要があります。

AWS IAM アイデンティティセンターでカスタマーマネージドアプリケーションを作成して設定するには、次の手順を実行します。

1. IAM Identity Center コンソール を開きます。
2. [Applications] (アプリケーション) を選択します。
3. [カスタマーマネージド] タブを選択します。
4. [アプリケーションの追加] を選択します。
5. [アプリケーションタイプを選択] ページの [セットアッププリファレンス] で、[セットアップしたいアプリケーションがある] を選択します。
6. [アプリケーションタイプ] で [OAuth 2.0] を選択します。
7. [次へ] を選択します。[アプリケーションを指定] ページが表示されます。
8. [アプリケーションの名前と説明] セクションで、**`storage-browser-oauth`** のようなアプリケーションの [表示名] を入力します。
9. [Description] を入力します。アプリケーションの説明は IAM アイデンティティセンターコンソールと API リクエストに表示されますが、AWS アクセスポータルには表示されません。
10. [ユーザーとグループの割り当て方法] で、[割り当ては不要] を選択します。このオプションは、権限のあるすべての IAM アイデンティティセンターユーザーとグループにこのアプリケーションへのアクセスを許可します。
11. [AWS アクセスポータル] で、ユーザーがアプリケーションにアクセスできるアプリケーション URL を入力します。

12. (オプション) リソースタグを追加する場合は、キーと値のペアを入力します。複数のリソースタグを追加するには、[新しいタグを追加] を選択して新しいエントリを生成し、キーと値のペアを入力します。
13. [次へ] を選択します。[認証の指定ページ] が表示されます。
14. [信頼できるトークン発行者による認証] で、チェックボックスを使用して、以前に作成した信頼できるトークン発行者を選択します。
15. [選択した信頼できるトークン発行者を設定] で、[aud クレーム] を入力します。[aud クレーム] は JSON ウェブトークン (JWT) の対象者を識別し、信頼できるトークン発行者がこのアプリケーションを識別するための名前です。

    > **Note**
    >
    > この情報を取得するには、外部 IdP の管理者に連絡する必要がある場合があります。

16. [次へ] を選択します。[認証情報の指定] ページが表示されます。
17. [設定方法] で、[1 つ以上の IAM ロールを入力] を選択します。
18. [IAM ロールを入力] で、ID ベアラートークンの IAM ロールまたは Amazon リソースネーム (ARN) を追加します。ID ブローカーアプリケーション用に前のステップで作成した IAM ロール (例: **`bootstrap-role`**) を入力する必要があります。
19. [次へ] を選択します。
20. [確認と設定] ページで、アプリケーション設定の詳細を確認します。設定を変更する必要がある場合は、[編集] を選択して変更するセクションの編集を選択します。
21. [Submit] を選択してください。追加したアプリケーションの詳細ページが表示されます。

アプリケーションの設定が完了したら、ユーザーは作成したアクセス許可のセットと割り当てたユーザーアクセスに基づき、AWS アクセスポータル内からアプリケーションにアクセスできます。

S3 Access Grants を ID 伝播用の信頼されたアプリケーションとして追加する

カスタマーマネージドアプリケーションを設定したら、ID 伝播用に S3 Access Grants を指定する必要があります。S3 Access Grants は、ユーザーが Amazon S3 データにアクセスするための認証情報を提供します。カスタマーマネージドアプリケーションにサインインすると、S3 Access Grants はユーザーの ID を信頼できるアプリケーションに渡します。

前提条件: 以下の手順を実行する前に、S3 Access Grants が設定されていることを確認してください (S3 Access Grants インスタンスの作成や場所の登録など)。詳細については、「S3 Access Grants の開始方法」を参照してください。

ID 伝播用の S3 Access Grants をカスタマーマネージドアプリケーションに追加するには、次の手順を実行します。

1. IAM Identity Center コンソール を開きます。
2. [Applications] (アプリケーション) を選択します。
3. [カスタマーマネージド] タブを選択します。
4. [カスタマーマネージドアプリケーション] リストで、アクセスのリクエストを開始する OAuth 2.0 アプリケーションを選択します。これはユーザーがサインインするアプリケーションです。
5. [詳細ページ] の [ID の伝播のための信頼されたアプリケーション] で、[信頼されたアプリケーションを指定] を選択します。
6. [セットアップタイプ] で、[個々のアプリケーションとアクセスの指定] を選択して、[次へ] を選択します。
7. [サービスを選択] ページで、[S3 Access Grants] を選択します。S3 Access Grants には、信頼できる ID の伝播用に独自のウェブアプリケーションを定義するために使用できるアプリケーションがあります。
8. [次へ] を選択します。次のステップで、アプリケーションを選択します。
9. [アプリケーションを選択] ページで、[個々のアプリケーション] を選択し、アクセスのリクエストを受信できる各アプリケーションのチェックボックスをオンにして、[次へ] を選択します。
10. [アクセスを設定] ページの [設定方法] で、次のいずれかを選択します。

    - [アプリケーションごとにアクセスを選択] — このオプションを選択すると、アプリケーションごとに異なるアクセスレベルを設定できます。アクセスレベルを設定するアプリケーションを選択し、[アクセスを編集] を選択します。[適用するアクセスのレベル] で、必要に応じてアクセスレベルを変更し、[変更の保存] を選択します。
    - [すべてのアプリケーションに同じアクセスレベルを適用] — アプリケーションごとにアクセスレベルを設定する必要がない場合は、このオプションを選択します。

11. [次へ] を選択します。
12. [設定を確認] ページで、選択した内容を確認します。

> **Note**
>
> ユーザーに `s3:access_grants:read_write` アクセス許可が付与されていることを必ず確認します。このアクセス許可により、ユーザーは Amazon S3 にアクセスするための認証情報を取得できます。書き込みオペレーションへのアクセスを制限するには、前に作成した IAM ポリシーまたは S3 Access Grants のいずれかを使用してください。

13. 変更を加えるには、変更する構成セクションの [編集] を選択します。次に、必要な変更を行い、[変更を保存] を選択します。
14. [信頼されたアプリケーション] を選択して、ID の伝播用に信頼されたアプリケーションを追加します。

ユーザーまたはグループへの許可を作成する

このステップでは、IAM アイデンティティセンターを使用してユーザーをプロビジョニングします。SCIM は、ユーザーとグループの自動または手動プロビジョニングに使用できます。SCIM は、IAM アイデンティティセンターの ID と ID プロバイダー (IdP) の ID を同期させます。これには、IdP と IAM アイデンティティセンターの間で行われるユーザーのプロビジョニング、アップデート、デプロビジョニングが含まれます。

> **Note**
>
> S3 Access Grants を IAM アイデンティティセンターで使用すると、ローカルの IAM アイデンティティセンターのユーザーは使用されないため、このステップが必要になります。代わりに、ユーザーを ID プロバイダーから IAM アイデンティティセンターと同期する必要があります。

ID プロバイダーのユーザーを IAM アイデンティティセンターと同期するには、次の手順を実行します。

1. 自動プロビジョニングを有効にします。
2. アクセストークンを生成します。

特定のユースケース用に IAM アイデンティティセンターを使用して ID プロバイダーを設定する方法の例については、「IAM Identity Center Identity source tutorials」を参照してください。

Storage Browser for S3 コンポーネントを作成する

IAM アイデンティティセンターインスタンスを設定し、S3 Access Grants で許可を作成したら、React アプリケーションを開きます。React アプリケーションで、`createManagedAuthAdapter` を使用して承認ルールを設定します。IAM アイデンティティセンターから取得した認証情報を返すには、認証情報プロバイダーを指定する必要があります。次に、`createStorageBrowser` を呼び出して、Storage Browser for S3 コンポーネントを初期化できます。

```
import {
    createManagedAuthAdapter,
    createStorageBrowser,
} from '@aws-amplify/ui-react-storage/browser';
import '@aws-amplify/ui-react-storage/styles.css';

export const { StorageBrowser } = createStorageBrowser({
   config: createManagedAuthAdapter({
    credentialsProvider: async (options?: { forceRefresh?: boolean }) => {
      // return your credentials object
      return {
        credentials: {
          accessKeyId: 'my-access-key-id',
          secretAccessKey: 'my-secret-access-key',
          sessionToken: 'my-session-token',
          expiration: new Date(),
        },
      }
    },
    // AWS `region` and `accountId` of the S3 Access Grants Instance.
    region: '',
    accountId: '',
    // call `onAuthStateChange` when end user auth state changes
    // to clear sensitive data from the `StorageBrowser` state
    registerAuthListener: (onAuthStateChange) => {},
  })
});
```

次に、ウェブアプリケーションの JSON ウェブトークン (JWT) を IAM アイデンティティセンターの IAM 認証情報と交換するメカニズムを作成します。JWT の交換方法の詳細については、次のリソースを参照してください。

- AWS Storage Blog の「How to develop a user-facing data application with IAM Identity Center and S3 Access Grants」の投稿
- AWS Storage Blog の「Scaling data access with S3 Access Grants」の投稿
- AWS workshop studio の「S3 Access Grants workshop」
- GitHub の「S3 Access Grants workshop」

次に、認証情報の取得リクエストを処理する API エンドポイントを設定します。JSON ウェブトークン (JWT) 交換を検証するには、次の手順を実行します。

1. 受信リクエストの認可ヘッダーから JSON ウェブトークンを取得します。
2. 指定された JSON ウェブキーセット (JWKS) URL のパブリックキーを使用してトークンを検証します。
3. トークンの有効期限、発行者、件名、対象者のクレームを確認します。

ID プロバイダーの JSON ウェブトークンを AWS IAM 認証情報と交換するには、次の手順を実行します。

> **Tip**
>
> 機密情報をログに記録しないようにしてください。認可の不足、トークンの有効期限切れ、その他の例外には、エラー処理コントロールを使用することをお勧めします。詳細については、AWS Compute Blog の「Implementing AWS Lambda error handling patterns 」の投稿を参照してください。

1. 必要な [アクセス許可] と [スコープ] のパラメータがリクエストで指定されていることを確認します。
2. CreateTokenWithIAM API を使用して、JSON ウェブトークンを IAM アイデンティティセンタートークンと交換します。

> **Note**
>
> IdP JSON ウェブトークンを使用した後は、再度使用することはできません。IAM アイデンティティセンターと交換するには、新しいトークンを使用する必要があります。

3. IAM アイデンティティセンタートークンを使用して一時的なロールを引き受けるには、AssumeRole API オペレーションを使用します。ID ベアラーロールを必ず使用してください。これは、認証情報をリクエストするために ID コンテキスト (**identity-bearer-role** など) を保持するロールとも呼ばれます。
4. IAM 認証情報をウェブアプリケーションに返します。

> **Note**
>
> 適切なログ記録メカニズムが設定されていることを確認してください。レスポンスは、適切な HTTP ステータスコードを含む標準化された JSON 形式で返されます。

Storage Browser for S3 の設定

S3 バケットへのアクセスを Storage Browser for S3 に許可するために、Storage Browser コンポーネントは Amazon S3 への REST API コールを行います。デフォルトでは、Cross-Origin Resource Sharing (CORS) は S3 バケットでは有効になっていません。そのため、Storage Browser がデータにアクセスしている S3 バケットごとに CORS を有効にする必要があります。

例えば、S3 バケットで CORS を有効にするには、次のように CORS ポリシーを更新できます。

```
[
    {
        "ID": "S3CORSRuleId1",
        "AllowedHeaders": [
            "*"
        ],
        "AllowedMethods": [
            "GET",
            "HEAD",
            "PUT",
            "POST",
            "DELETE"
        ],
        "AllowedOrigins": [
            "*"
        ],
        "ExposeHeaders": [
            "last-modified",
            "content-type",
            "content-length",
```

```
            "etag",
            "x-amz-version-id",
            "x-amz-request-id",
            "x-amz-id-2",
            "x-amz-cf-id",
            "x-amz-storage-class",
            "date",
            "access-control-expose-headers"
        ],
        "MaxAgeSeconds": 3000
    }
]
```

Storage Browser for S3 のトラブルシューティング

Storage Browser for S3 で問題が発生した場合は、次のトラブルシューティングのヒントを確認してください。

- 複数のリクエストに同じトークン (idToken または accessToken) を使用しないでください。トークンは再利用できません。これにより、リクエストが失敗します。
- Storage Browser コンポーネントに提供する IAM 認証情報に、s3:GetDataAccess オペレーションを呼び出すためのアクセス許可が含まれていることを確認します。含まれていない場合、エンドユーザーはデータにアクセスできなくなります。

または、次のリソースを確認することもできます。

- Storage Browser for S3 は AWS サポートによってサポートされています。サポートが必要な場合は、AWS センターに問い合わせてください。
- Storage Browser for S3 で問題が発生した場合、またはフィードバックを送信する場合は、「Amplify GitHub ページ」にアクセスしてください。
- このプロジェクトで潜在的なセキュリティ上の問題を発見した場合、「AWS 脆弱性レポートページ」から AWS セキュリティに知らせてください。

Amazon S3 Transfer Acceleration を使用した高速かつ安全なファイル転送の設定

Amazon S3 Transfer Acceleration は、クライアントと S3 汎用バケットの間で、ファイルの長距離転送を高速、簡単、安全に実行できるようにするバケットレベルの機能です。Transfer Acceleration は、世界中からの S3 汎用バケットへの転送の速度を最適化するように設計されています。Transfer Acceleration は、Amazon CloudFront の世界中に点在するエッジロケーションを利用します。エッジロケーションに到着したデータは、最適化されたネットワークパスで Amazon S3 にルーティングされます。

Transfer Acceleration を使用する場合、追加のデータ転送料金が発生することがあります。料金に関する詳細については、「Amazon S3 の料金」を参照してください。

なぜ Transfer acceleration を使用するのですか?

汎用バケットでの Transfer Acceleration の使用は、さまざまな理由で役立つ場合があります。

- 顧客は、世界中から一元化された汎用バケットにアップロードします。
- 大陸間で定期的にギガバイトからテラバイト単位のデータを転送する。
- Amazon S3 にアップロードする際に、インターネット経由で利用可能な帯域幅をすべて使用することはできません。

Transfer Acceleration の使用が適している場合の詳細については、[Amazon S3 のよくある質問] を参照してください。

Transfer Acceleration を使用するための要件

S3 バケットで Transfer Acceleration を使用するための要件を以下に示します。

- Transfer Acceleration は仮想ホスト形式のリクエストでのみサポートされます。仮想ホスト形式のリクエストの詳細については、「Amazon S3 API リファレンス」の「Making requests using the REST API」を参照してください。
- Transfer Acceleration で使用するバケットは、ピリオド (".") が含まれていない DNS 準拠の名前にする必要があります。
- Transfer Acceleration は、バケットに対して有効にする必要があります。詳細については、[S3 Transfer Acceleration の有効化と使用] を参照してください。

バケットで Transfer Acceleration を有効にした後、バケットへのデータ転送速度が上昇するまでに最大 20 分かかることがあります。

> **Note**
>
> 現在、Transfer Acceleration は以下のリージョンにあるバケットでサポートされています。
>
> - アジアパシフィック (東京) (ap-northeast-1)
> - アジアパシフィック (ソウル) (ap-northeast-2)
> - アジアパシフィック (ムンバイ) (ap-south-1)
> - アジアパシフィック (シンガポール) (ap-southeast-1)
> - アジアパシフィック (シドニー) (ap-southeast-2)
> - カナダ (中部) (ca-central-1)
> - ヨーロッパ (フランクフルト) (eu-central-1)
> - 欧州 (アイルランド) (eu-west-1)
> - ヨーロッパ (ロンドン) (eu-west-2)
> - 欧州 (パリ) (eu-west-3)
> - 南米 (サンパウロ) (sa-east-1)
> - 米国東部 (バージニア北部) (us-east-1)
> - 米国東部 (オハイオ) (us-east-2)
> - 米国西部 (北カリフォルニア) (us-west-1)
> - 米国西部 (オレゴン) (us-west-2)

- Transfer Acceleration が有効になっているバケットにアクセスするには、エンドポイント *bucket-name*.s3-accelerate.amazonaws.com を使用する必要があります。または、デュアルスタックのエンドポイント *bucket-name*.s3-accelerate.dualstack.amazonaws.com を使用して、IPv6 経由で有効なバケットに接続します。標準のデータ転送では、通常のエンドポイントを引き続き使用できます。
- 転送状態として高速化を設定するには、バケット所有者である必要があります。バケット所有者は他のユーザーに対し、バケットに高速化状態を設定するためのアクセス許可を割り当てることができます。s3:PutAccelerateConfiguration アクセス許可では、ユーザーがバケットで Transfer Acceleration を有効または無効にすることができます。ま

た、`s3:GetAccelerateConfiguration` アクセス許可では、ユーザーはバケットの Transfer Acceleration 状態 (`Enabled` または `Suspended`.) を返すことができます。

以下のセクションでは、Amazon S3 Transfer Acceleration の開始方法と、それを使用してデータを転送する方法について説明します。

トピック

- Amazon S3 Transfer Acceleration の開始方法
- S3 Transfer Acceleration の有効化と使用
- Amazon S3 Transfer Acceleration の速度比較ツールの使用

Amazon S3 Transfer Acceleration の開始方法

Amazon S3 Transfer Acceleration を使用すると、クライアントと S3 バケットの間で、長距離にわたるファイル転送を高速、簡単、安全に行えるようになります。Transfer Acceleration では、Amazon CloudFront の世界中に分散したエッジロケーションを使用します。エッジロケーションに到着したデータは、最適化されたネットワークパスで Amazon S3 にルーティングされます。

Amazon S3 Transfer Acceleration の使用を開始するには、以下の手順を実行します。

1. バケットで Transfer Acceleration を有効にする

   バケットでは、次のいずれかの方法で Transfer Acceleration を有効にすることができます。

   - Amazon S3 コンソールを使用します。
   - REST API PutBucketAccelerateConfiguration オペレーションを使用します。
   - AWS CLI および AWS SDK を使用します。詳細については、「Amazon S3 API リファレンス」の「Developing with Amazon S3 using the AWS SDKs」を参照してください。

   詳細については、「S3 Transfer Acceleration の有効化と使用」を参照してください。

   > **Note**
   >
   > バケットで Transfer Acceleration を使用するには、バケット名にピリオド (.) が含まれず、DNS 命名要件に準拠している必要があります。

2. 高速化を有効にしたバケットとの間でデータを転送する

次の s3-accelerate エンドポイントのドメイン名の 1 つを使用します。

- 高速化を有効にしたバケットにアクセスするには、*bucket-name*.s3-accelerate.amazonaws.com を使用します。
- IPv6 経由で高速化を有効にしたバケットにアクセスするには、*bucket-name*.s3-accelerate.dualstack.amazonaws.com を使用します。

  Amazon S3 デュアルスタックエンドポイントは、IPv6 および IPv4 を使用した S3 バケットへのリクエストをサポートしています。Transfer Acceleration デュアルスタックエンドポイントのみが、仮想ホスト形式のエンドポイント名を使用します。詳細については、「Amazon S3 API リファレンス」の「Making requests to Amazon S3 over IPv6」および「Amazon S3 API リファレンス」の「Using Amazon S3 dual-stack endpoints」を参照してください。

> **Note**
>
> データ転送を高速化するには、データ転送アプリケーションがバケットにアクセスするために使用する 2 種類のエンドポイント (デュアルスタックエンドポイント用の .s3-accelerate.amazonaws.com または .s3-accelerate.dualstack.amazonaws.com) のどちらかを指定する必要があります。標準のデータ転送を使用する場合は、通常のエンドポイントを引き続き使用できます。

Transfer Acceleration を有効にした後、Amazon S3 の PUT オブジェクトおよび GET オブジェクトのリクエストの送信先として s3-accelerate エンドポイントドメイン名を指定できます。例えば、現在 PutObject を使用する REST API アプリケーションがあり、PUT リクエストで *amzn-s3-demo-bucket*.s3.us-east-1.amazonaws.com というホスト名を使用しているとします。PUT を高速化するには、リクエストのホスト名を *amzn-s3-demo-bucket*.s3-accelerate.amazonaws.com に変更します。標準のアップロード速度に戻すには、名前を *amzn-s3-demo-bucket*.s3.us-east-1.amazonaws.com に戻します。

Transfer Acceleration を有効にしたあと、パフォーマンス上の利点が感じられるまでには最長で 20 分ほどかかります。ただし、高速化エンドポイントは、Transfer Acceleration を有効にするとすぐに利用できます。

AWS CLI、AWS SDK、または他のツールで Amazon S3 との間でデータをやり取りする場合、高速化エンドポイントを使用して転送できます。AWS SDK を使用している場合、サポートされている一部の言語では高速化エンドポイントのクライアント設定フラグを使用できるため、Transfer Acceleration 用のエンドポイントを明示的に *bucket-name*.s3-accelerate.amazonaws.com

に設定する必要はありません。高速化エンドポイントのクライアント設定フラグを使用する方法の例については、[S3 Transfer Acceleration の有効化と使用] を参照してください。

Transfer Acceleration エンドポイントでは、以下を除くすべての Amazon S3 オペレーションを使用できます。

- ListBuckets
- CreateBucket
- DeleteBucket

また、Amazon S3 Transfer Acceleration は、CopyObject を使用したクロスリージョンコピーをサポートしていません。

S3 Transfer Acceleration の有効化と使用

Amazon S3 Transfer Acceleration を使用すると、クライアントと S3 汎用バケットの間で、ファイルの長距離転送を迅速かつ安全に行うことができます。S3 コンソール、AWS Command Line Interface (AWS CLI)、API、または AWS SDK を使用して Transfer Acceleration を有効にすることができます。

このセクションでは、バケットに対する Amazon S3 Transfer Acceleration を有効にして、有効にしたバケットに高速化エンドポイントを使用する方法の例を示します。

Transfer Acceleration の要件の詳細については、[Amazon S3 Transfer Acceleration を使用した高速かつ安全なファイル転送の設定] を参照してください。

S3 コンソールの使用

> **Note**
>
> 高速アップロード速度と非高速アップロード速度を比較する場合は、Amazon S3 Transfer Acceleration 速度比較ツールを開きます。
> 速度比較ツールでは、マルチパートアップロードを使用して、ブラウザからさまざまな AWS リージョンにファイルを転送し、Amazon S3 Transfer Acceleration を使用した場合と使用していない場合の速度を比較します。リージョン別に、ダイレクトアップロードの速度と、高速化アップロードの速度を比較できます。

S3 汎用バケット用の Transfer Acceleration を有効にするには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[汎用バケット] を選択します。
3. [汎用バケット] リストで、Transfer Acceleration を有効にするバケットの名前を選択します。
4. [プロパティ] を選択します。
5. [Transfer Acceleration] で、[編集] を選択します。
6. [有効化] を選択し、[変更を保存] を選択します。

高速データ転送にアクセスするには

1. Amazon S3 によってバケットの Transfer Acceleration が有効になると、バケットの プロパティ タブが表示されます。
2. Transfer acceleration の 高速化エンドポイント には、バケットの Transfer Acceleration エンドポイントが表示されます。このエンドポイントを使用して、バケットとの間の高速データ転送にアクセスします。

   Transfer Acceleration を停止した場合、高速化エンドポイントは機能しなくなります。

AWS CLI の使用

以下は、Transfer Acceleration で使用される AWS CLI コマンドの例です。AWS CLI の設定手順については、「Amazon S3 API リファレンス」の「AWS CLI を使用した Amazon S3 での開発」を参照してください。

バケットでの Transfer Acceleration の有効化

AWS CLI put-bucket-accelerate-configuration コマンドを使用して、バケットの Transfer Acceleration を有効または一時停止します。

次の例では、`Status=Enabled` を設定して、*`amzn-s3-demo-bucket`* という名前のバケットで Transfer Acceleration を有効にしています。Transfer Acceleration を一時停止するには、`Status=Suspended` を使用します。

Example

```
$ aws s3api put-bucket-accelerate-configuration --bucket amzn-s3-demo-bucket --
accelerate-configuration Status=Enabled
```

Transfer Acceleration の使用

s3 および s3api AWS CLI コマンドによって行われるすべての Amazon S3 リクエストを高速化エンドポイント s3-accelerate.amazonaws.com に送信できます。これを行うには、AWS Config ファイルのプロファイルで設定値 use_accelerate_endpoint を true に設定します。高速化エンドポイントを使用するには、バケットに対する Transfer Acceleration を有効にしておく必要があります。

すべてのリクエストはバケットアドレス指定の仮想スタイル (*amzn-s3-demo-bucket*.s3-accelerate.amazonaws.com) を使用して送信されます。高速化エンドポイントでは、これらのオペレーションをサポートしていないため、ListBuckets、CreateBucket、DeleteBucket リクエストは高速化エンドポイントには送信されません。

use_accelerate_endpoint の詳細については、AWS CLI CLI コマンドリファレンスの「AWS CLI S3 の設定」を参照してください。

次の例では、デフォルトのプロファイル内で use_accelerate_endpoint を true に設定しています。

Example

```
$ aws configure set default.s3.use_accelerate_endpoint true
```

一部の AWS CLI コマンドについてのみ高速化エンドポイントを使用するには、次のいずれかの方法を使用できます。

- s3 または s3api コマンドで高速化エンドポイントを使用するには、必ず --endpoint-url パラメータを https://s3-accelerate.amazonaws.com に設定します。
- AWS Config ファイルで別々のプロファイルを設定できます。たとえば、use_accelerate_endpoint を true に設定するプロファイルと use_accelerate_endpoint を設定しないプロファイルを作成します。コマンドを実行する際は、高速化エンドポイントを使用するかどうかによって、適切なプロファイルを指定します。

Transfer Acceleration が有効になっているバケットにオブジェクトをアップロードする

次の例では、高速化エンドポイントを使用するように設定されたデフォルトプロファイルを使用して、Transfer Acceleration が有効になっている *amzn-s3-demo-bucket* という名前のバケットにファイルをアップロードします。

Example

```
$ aws s3 cp file.txt s3://amzn-s3-demo-bucket/key-name --region region
```

次の例では、`--endpoint-url` パラメータで高速化エンドポイントを指定して、Transfer Acceleration が有効になっているバケットにファイルをアップロードします。

Example

```
$ aws configure set s3.addressing_style virtual
$ aws s3 cp file.txt s3://amzn-s3-demo-bucket/key-name --region region --endpoint-url
 https://s3-accelerate.amazonaws.com
```

AWS SDK の使用

以下は、AWS SDK で Transfer Acceleration を使用して Amazon S3 にオブジェクトをアップロードする例です。AWS SDK でサポートされている一部の言語 (Java や .NET など) では、高速化エンドポイントのクライアント設定フラグを使用するため、Transfer Acceleration 用のエンドポイントを明示的に *bucket-name*`.s3-accelerate.amazonaws.com` に設定する必要はありません。

Java

Example

次の例では、高速化エンドポイントを使用して、オブジェクトを Amazon S3 にアップロードする方法を示しています。この例では、次のような処理を実行します。

- 高速化エンドポイントを使用するために設定される `AmazonS3Client` を作成します。クライアントがアクセスするすべてのバケットで、Transfer Acceleration が有効になっている必要があります。
- 指定したバケットで Transfer Acceleration を有効にします。このステップは、指定したバケットで Transfer Acceleration が有効になっていない場合に限り必要です。
- 指定されたバケットで Transfer Acceleration が有効になっていることを確認します。

- バケットの高速化エンドポイントを使用して、指定されたバケットに新しいオブジェクトをアップロードします。

Transfer Acceleration の使用方法については、「Amazon S3 Transfer Acceleration の開始方法」を参照してください。作業サンプルの作成およびテストの手順については、「AWS SDK for Java のデベロッパーガイド」の「使用開始」を参照してください。

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.BucketAccelerateConfiguration;
import com.amazonaws.services.s3.model.BucketAccelerateStatus;
import com.amazonaws.services.s3.model.GetBucketAccelerateConfigurationRequest;
import com.amazonaws.services.s3.model.SetBucketAccelerateConfigurationRequest;

public class TransferAcceleration {
    public static void main(String[] args) {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String keyName = "*** Key name ***";

        try {
            // Create an Amazon S3 client that is configured to use the accelerate
 endpoint.
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withRegion(clientRegion)
                    .withCredentials(new ProfileCredentialsProvider())
                    .enableAccelerateMode()
                    .build();

            // Enable Transfer Acceleration for the specified bucket.
            s3Client.setBucketAccelerateConfiguration(
                    new SetBucketAccelerateConfigurationRequest(bucketName,
                            new BucketAccelerateConfiguration(
                                    BucketAccelerateStatus.Enabled)));

            // Verify that transfer acceleration is enabled for the bucket.
            String accelerateStatus = s3Client.getBucketAccelerateConfiguration(
```

```
                    new GetBucketAccelerateConfigurationRequest(bucketName))
                    .getStatus();
            System.out.println("Bucket accelerate status: " + accelerateStatus);

            // Upload a new object using the accelerate endpoint.
            s3Client.putObject(bucketName, keyName, "Test object for transfer
 acceleration");
            System.out.println("Object \"" + keyName + "\" uploaded with transfer
 acceleration.");
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

.NET

次の例では、AWS SDK for .NET を設定することにより、バケットに対する Transfer Acceleration を有効にする方法を示しています。コード例を設定および実行する方法の詳細については、「AWS SDK for .NET デベロッパーガイド」の「AWS SDK for .NET の開始方法」を参照してください。

Example

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class TransferAccelerationTest
    {
        private const string bucketName = "*** bucket name ***";
        // Specify your bucket region (an example region is shown).
```

```
        private static readonly RegionEndpoint bucketRegion =
RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;
        public static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            EnableAccelerationAsync().Wait();
        }

        static async Task EnableAccelerationAsync()
        {
                try
                {
                    var putRequest = new PutBucketAccelerateConfigurationRequest
                    {
                        BucketName = bucketName,
                        AccelerateConfiguration = new AccelerateConfiguration
                        {
                            Status = BucketAccelerateStatus.Enabled
                        }
                    };
                    await
s3Client.PutBucketAccelerateConfigurationAsync(putRequest);

                    var getRequest = new GetBucketAccelerateConfigurationRequest
                    {
                        BucketName = bucketName
                    };
                    var response = await
s3Client.GetBucketAccelerateConfigurationAsync(getRequest);

                    Console.WriteLine("Acceleration state = '{0}' ",
response.Status);
                }
                catch (AmazonS3Exception amazonS3Exception)
                {
                    Console.WriteLine(
                        "Error occurred. Message:'{0}' when setting transfer
acceleration",
                        amazonS3Exception.Message);
                }
        }
    }
```

```
}
```

Transfer Acceleration が有効になっているバケットにオブジェクトをアップロードする際は、クライアントの作成時に高速化エンドポイントの使用を指定します。

```
var client = new AmazonS3Client(new AmazonS3Config
            {
                RegionEndpoint = TestRegionEndpoint,
                UseAccelerateEndpoint = true
            }
```

JavaScript

AWS SDK for JavaScript を使用して Transfer Acceleration を有効にする例については、「AWS SDK for JavaScript API リファレンス」の「PutBucketAccelerateConfiguration コマンド」を参照してください。

Python (Boto)

SDK for Python を使用して Transfer Acceleration を有効にする例については、「AWS SDK for Python (Boto3) API リファレンス」の「put_bucket_accelerate_configuration」を参照してください。

Other

他の AWS SDK の使用については、サンプルコードとライブラリのページを参照してください。

REST API の使用

REST API `PutBucketAccelerateConfiguration` オペレーションを使用して、既存のバケットでアクセラレーション設定を有効にします。

詳細については、「Amazon Simple Storage Service API リファレンス」の「PutBucketAccelerateConfiguration」を参照してください。

Amazon S3 Transfer Acceleration の速度比較ツールの使用

Amazon S3 Transfer Acceleration の速度比較ツールを使用すると、高速化した場合と高速化していない場合の Amazon S3 リージョン間でのアップロード速度を比較できます。速度比較ツールでは、マルチパートアップロードを使用して、ブラウザからさまざまな Amazon S3 リージョンへのファイル転送を行い、Transfer Acceleration を使用した場合と使用していない場合の比較が行われます。

速度比較ツールには、次のいずれかの方法でアクセスできます。

- 次の URL をブラウザウィンドウにコピーします。このとき、*region* は使用している AWS リージョン (us-west-2 など) に、*amzn-s3-demo-bucket* は評価するバケットの名前に置き換えてください。

  ```
  https://s3-accelerate-speedtest.s3-accelerate.amazonaws.com/en/accelerate-speed-comparsion.html?region=region&origBucketName=amzn-s3-demo-bucket
  ```

  Amazon S3 でサポートされているリージョンのリストについては、「AWS 全般のリファレンス」の「Amazon S3 エンドポイントとクォータ」を参照してください。
- Amazon S3 コンソールを使用します。

ストレージの転送と使用にリクエスタ支払い汎用バケットを使用する

一般に、Amazon S3 のバケットのストレージおよびデータ転送にかかるコストはすべて、そのバケット所有者が負担します。ただし、汎用バケットをリクエスタ支払いバケットとして設定できます。リクエスタ支払いバケットの場合、リクエストおよびバケットからのデータのダウンロードにかかるコストは、所有者でなくリクエストを実行したリクエスタが支払います。データの保管にかかるコストは常にバケット所有者が支払います。

通常は、データを共有したいが、他者がデータにアクセスする際に発生する費用を負担したくない場合に、リクエスタ支払いバケットをバケットに設定します。例えば、郵便番号リスト、参照データ、地理空間情報、ウェブクロールデータといった、大規模なデータセットを利用できるようにする際にリクエスタ支払いバケットを設定することができます。

> **Important**
>
> 汎用バケットでリクエスタ支払いを有効にすると、そのバケットへの匿名アクセスは許可されなくなります。

リクエスタ支払いバケットに関するリクエストはすべて認証する必要があります。リクエストの認証により、Amazon S3 はリクエスタを特定し、リクエスタ支払いバケットの使用に対して課金できるようになります。

リクエスタがリクエストを送る前に AWS Identity and Access Management (IAM) ロールを引き受ける際に、ロールが属するアカウントにリクエストの料金が発生します。IAM ロールの詳細については、「IAM ユーザーガイド」の「IAM ロール」を参照してください。

バケットをリクエスタ支払いバケットとして設定した後、リクエスタはリクエストとデータダウンロードに対して課金されることを理解している旨を示す必要があります。料金を受け入れることを示すには、リクエスタが DELETE、GET、HEAD、POST、PUT リクエストの API リクエストにヘッダーとして `x-amz-request-payer` を含めるか、REST リクエストに `RequestPayer` パラメータを追加する必要があります。CLI リクエストの場合、リクエスタは `--request-payer` パラメータを使用できます。

Example – オブジェクトの削除時にリクエスタ支払いを使用する

次の DeleteObjectVersion API の例を使用するには、*`user input placeholders`* をユーザー自身の情報に置き換えます。

```
DELETE /Key+?versionId=VersionId HTTP/1.1
Host: Bucket.s3.amazonaws.com
x-amz-mfa: MFA
x-amz-request-payer: RequestPayer
x-amz-bypass-governance-retention: BypassGovernanceRetention
x-amz-expected-bucket-owner: ExpectedBucketOwner
```

リクエスタが RestoreObject API を使用してオブジェクトを復元する場合、`x-amz-request-payer` ヘッダーまたは `RequestPayer` パラメータがリクエストに含まれている限りリクエスタ支払いがサポートされます。ただし、リクエスタはリクエストのコストのみを支払います。バケット所有者が取り出し料金を支払います。

リクエスタ支払いバケットは、次の場合サポートしていません。

- 匿名リクエスト
- SOAP リクエスト
- リクエスタ支払いバケットをエンドユーザーログのターゲットバケットとして使用する場合、あるいはその逆。ただし、ターゲットバケットがリクエスタ支払いバケットでない場合は、リクエスタ支払いバケット上でエンドユーザーのログを有効にできます。

リクエスタ支払いの課金の仕組み

成功したリクエスタ支払いリクエストに対する課金はシンプルです。リクエスタは、転送されたデータとリクエストに対して支払い、バケット所有者はデータのストレージに対して支払います。ただし以下の条件では、リクエストに対してバケット所有者が課金されます。

- このリクエストにより `AccessDenied` (HTTP `403 Forbidden`) エラーが返され、リクエストがバケット所有者の個別の AWS アカウントまたは AWS 組織内で開始される。
- リクエストが SOAP リクエストの場合

リクエスタ支払いの詳細については、以下のトピックを参照してください。

トピック

- バケットでのリクエスタ支払いの設定
- REST API を使用した requestPayment 設定の取得
- リクエスタ支払いバケットからのオブジェクトのダウンロード

バケットでのリクエスタ支払いの設定

Amazon S3 バケットをリクエスタ支払いバケットに設定して、バケット所有者の代わりにリクエスタがリクエストとデータダウンロードの費用を支払うようにすることができます。

このセクションでは、コンソールと REST API を使用して Amazon S3 バケットでリクエスタ支払いを設定する方法の例を示します。

S3 コンソールの使用

S3 汎用バケットのリクエスタ支払いを有効にするには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[汎用バケット] を選択します。
3. [汎用バケット] のリストで、リクエスタ支払いを有効にするバケットの名前を選択します。
4. [プロパティ] を選択します。
5. [リクエスタ支払い] で、[編集] を選択します。
6. [有効化] を選択し、[変更を保存] を選択します。

Amazon S3 は、[バケットのリクエスタ支払い] を有効にし、[バケットの概要] を表示します。[リクエスタ支払い] の下に、[有効] と表示されます

REST API の使用

バケット所有者のみが、バケットのRequestPaymentConfiguration.payerの設定値をBucketOwner (デフォルト) またはRequesterに設定できます。requestPayment リソースの設定はオプションです。デフォルトでは、バケットはリクエスタ支払いバケットではありません。

リクエスタ支払いバケットを通常のバケットに戻すには、値 BucketOwner を使用します。通常、Amazon S3 バケットにデータをアップロードする際に BucketOwner を使用し、その後、バケット内のオブジェクトを公開する前に値を Requester に設定します。

requestPayment を設定するには

- PUT リクエストを使用して、指定したバケットの Payer の値を Requester に設定します。

```
PUT ?requestPayment HTTP/1.1
Host: [BucketName].s3.amazonaws.com
Content-Length: 173
Date: Wed, 01 Mar 2009 12:00:00 GMT
Authorization: AWS [Signature]

<RequestPaymentConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
<Payer>Requester</Payer>
</RequestPaymentConfiguration>
```

リクエストが成功すると、Amazon S3 は、以下のようなレスポンスを返します。

```
HTTP/1.1 200 OK
x-amz-id-2: [id]
x-amz-request-id: [request_id]
Date: Wed, 01 Mar 2009 12:00:00 GMT
Content-Length: 0
Connection: close
Server: AmazonS3
x-amz-request-charged:requester
```

リクエスタ支払いは、バケットレベルでのみ設定できます。バケット内の特定のオブジェクトに対してリクエスタ支払いを設定することはできません。

バケットは、いつでも自由に `BucketOwner` または `Requester` に設定できます。ただし、新しい設定値が有効になるまでに数分かかる場合があります。

> **Note**
>
> 特に URL の有効期限がとても長い場合、署名付き URL を提供するバケット所有者は、バケットをリクエスタ支払いに設定する前によく検討してください。バケット所有者は、バケット所有者の認証情報を使用する署名付き URL をリクエスタが使用するたびに課金されます。

REST API を使用した requestPayment 設定の取得

バケットに設定された `Payer` 値を取得するには、リソース `requestPayment` をリクエストします。

requestPayment リソースを返すには

- 以下のリクエストに示すように、GET リクエストを使用して `requestPayment` リソースを取得します。

```
GET ?requestPayment HTTP/1.1
Host: [BucketName].s3.amazonaws.com
Date: Wed, 01 Mar 2009 12:00:00 GMT
Authorization: AWS [Signature]
```

リクエストが成功すると、Amazon S3 は、以下のようなレスポンスを返します。

```
HTTP/1.1 200 OK
x-amz-id-2: [id]
x-amz-request-id: [request_id]
Date: Wed, 01 Mar 2009 12:00:00 GMT
Content-Type: [type]
Content-Length: [length]
Connection: close
Server: AmazonS3
```

```
<?xml version="1.0" encoding="UTF-8"?>
<RequestPaymentConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
<Payer>Requester</Payer>
</RequestPaymentConfiguration>
```

このレスポンスでは、payer 値が Requester に設定されていることが示されています。

リクエスタ支払いバケットからのオブジェクトのダウンロード

リクエスタ支払いバケットからデータをダウンロードするとリクエスタに対して課金されるため、リクエストには、リクエスタが課金について認識していることを示すパラメータ x-amz-request-payer を含める必要があります。リクエスタ支払いバケット内のオブジェクトにアクセスするには、リクエストに以下のいずれかを含める必要があります。

- DELETE、GET、HEAD、POST、PUT リクエストの場合は、ヘッダーに x-amz-request-payer : requester を含めます
- 署名付き URL の場合は、リクエストに x-amz-request-payer=requester を含めます

リクエストが成功してリクエスタが課金されると、レスポンスには x-amz-request-charged:requester ヘッダーが含まれます。リクエスト内に x-amz-request-payer がない場合、Amazon S3 は 403 エラーを返し、リクエストに対してバケット所有者が課金されます。

> **Note**
>
> バケット所有者は、リクエストに x-amz-request-payer を含める必要はありません。署名計算内に x-amz-request-payer とその値を含めたことを確認してください。詳細については、「Amazon S3 API リファレンス」の「Using an Authorization Header」を参照してください。

REST API の使用

リクエスタ支払いバケットからオブジェクトをダウンロードするには

- リクエスタ支払いバケットからオブジェクトをダウンロードするには、以下のリクエストに示すように、GET リクエストを使用します。

```
GET / [destinationObject] HTTP/1.1
Host: [BucketName].s3.amazonaws.com
```

```
x-amz-request-payer : requester
Date: Wed, 01 Mar 2009 12:00:00 GMT
Authorization: AWS [Signature]
```

GET リクエストが成功してリクエスタが課金されると、レスポンスには `x-amz-request-charged:requester` が含まれます。

Amazon S3 は、リクエスタ支払いバケットからオブジェクトを取得するリクエストに対して `Access Denied` エラーを返すことがあります。詳細については、Amazon Simple Storage Service API リファレンスの Error Responses をご参照ください。

AWS CLI の使用

AWS CLI を使用してリクエスタ支払いバケットからオブジェクトをダウンロードするには、`get-object` リクエストの一部として `--request-payer requester` を指定します。詳細については、AWS CLI リファレンスの get-object を参照してください。

Amazon S3 オブジェクトの使用

Amazon S3 にデータを保存するには、バケットおよびオブジェクトと呼ばれるリソースを使用します。バケット とは、オブジェクトのコンテナのことです。オブジェクト とは、ファイルと、そのファイルを記述している任意のメタデータのことです。

Amazon S3 にオブジェクトを保存するには、バケットを作成してから、オブジェクトをバケットにアップロードします。オブジェクトがバケットの中にあるときは、オブジェクトを開き、ダウンロードして、コピーできます。オブジェクトまたはバケットが不要になった場合は、これらのリソースをクリーンアップできます。

> **Note**
>
> Amazon S3 Express One Zone ストレージクラスをディレクトリバケットで使用する方法の詳細については、「S3 Express One Zone」と「ディレクトリバケットの使用」を参照してください。

> **Important**
>
> Amazon S3 コンソールで、オブジェクトに [Open] (開く) または [Download As] (名前を付けてダウンロード) を選択すると、これらのオペレーションによって署名付き URL が作成されます。5 分間、これらの署名付き URL にアクセスできる人なら誰でもオブジェクトにアクセスできるようになります。署名付き URL の詳細については、「署名付き URL の使用」を参照してください。

Amazon S3 では、お支払いは実際に使用した分のみです。Amazon S3 の機能と料金の詳細については、「Amazon S3」を参照してください。Amazon S3 の新規のお客様は、Amazon S3 を無料で使い始めることができます。詳細については、AWS 無料利用枠 を参照してください。

トピック

- Amazon S3 オブジェクトの概要
- Amazon S3 オブジェクトに命名する
- オブジェクトメタデータの使用
- オブジェクトのアップロード

- 条件付きリクエストを使用して S3 オペレーションに前提条件を追加する
- オブジェクトのコピー、移動、名前の変更
- オブジェクトのダウンロード
- Amazon S3 でのオブジェクトの整合性のチェック
- Amazon S3 オブジェクトの削除
- オブジェクトの整理、リスト化、使用
- 署名付き URL を使用したオブジェクトのダウンロードおよびアップロード
- S3 Object Lambda を使用したオブジェクトの変換
- バッチオペレーションでオブジェクトオペレーションを一括で実行する
- Amazon S3 Select で所定のデータをクエリする

Amazon S3 オブジェクトの概要

Amazon S3 は、一意のキー値を使用して、必要な数のオブジェクトを保存できるオブジェクトストアです。これらのオブジェクトは 1 つ以上のバケットに保存し、各オブジェクトのサイズは最大 5 TB です。オブジェクトの構成エレメントを以下に示します。

キー

オブジェクトに割り当てる名前です。オブジェクトを取得するには、オブジェクトキーを使用します。詳細については、Working with Object Metadata を参照してください。

バージョン ID

バケット内ではキーとバージョン ID がオブジェクトを一意に識別します。バージョン ID は、バケットにオブジェクトを追加すると Amazon S3 によって生成される文字列です。詳細については、S3 バージョニングによる複数のバージョンのオブジェクトの保持 を参照してください。

値

保存するコンテンツです。

オブジェクトの値は任意のバイトシーケンスです。オブジェクトのサイズは、0 から 5 TB までの範囲です。詳細については、オブジェクトのアップロード を参照してください。

メタデータ

オブジェクトに関する情報を保存するために使用できる名前と値のペアのセットです。Amazon S3 内のオブジェクトには、ユーザー定義メタデータと呼ばれるメタデータを割り当てることが

できます。Amazon S3 では、オブジェクトの管理目的で使用されるシステムメタデータもオブジェクトに割り当てられます。詳細については、Working with Object Metadata を参照してください。

サブリソース

Amazon S3 では、オブジェクト固有の追加情報を保存するためにサブリソースメカニズムを使用します。サブリソースはオブジェクトの従属物なので、オブジェクトやバケットといった他のエンティティに常に関連付けられます。詳細については、オブジェクトのサブリソース を参照してください。

アクセスコントロールの情報

Amazon S3 に保存するオブジェクトへのアクセスを制御できます。Amazon S3 は、アクセスコントロールリスト (ACL) やバケットポリシーなどのリソースベースのアクセスコントロールと、ユーザーベースのアクセスコントロールをサポートしています。アクセスコントロールの詳細については、以下を参照してください。

- Amazon S3 でのアクセスコントロール
- Amazon S3 用 Identity and Access Management
- ACL の設定

Amazon S3 リソース (バケットやオブジェクトなど) はデフォルトでプライベートです。他のユーザーがそれらのリソースにアクセスできるようにするには、明示的にアクセス許可を与える必要があります。オブジェクトの共有の詳細については、署名付き URL を使用したオブジェクトの共有 を参照してください。

[タグ]

タグを使用して、保存されているオブジェクトを分類し、アクセスコントロールやコスト配分を行うことができます。詳細については、「タグを使用してストレージを分類する」を参照してください。

オブジェクトのサブリソース

Amazon S3 では、バケットとオブジェクトに関連付ける一連のサブリソースが定義されています。サブリソースはオブジェクトの下位に属します。つまり、サブリソースは単独では存在しません。常に、オブジェクトやバケットなどの他のエンティティに関連付けられています。

次の表は、Amazon S3 のオブジェクトに関連付けられるサブリソースをまとめたものです。

サブリソース	説明
acl	アクセス許可の被付与者と付与されるアクセス許可を識別するリストが含まれます。オブジェクトを作成するとき、acl を使用することで、オブジェクト所有者がオブジェクトに対して完全なコントロールを持つことを指定します。オブジェクト ACL の取得や、更新されたアクセス許可のリストで置き換えることができます。ACL を更新するときは必ず既存の ACL を置き換える必要があります。ACL の詳細については、「アクセスコントロールリスト (ACL) の概要」を参照してください。

Amazon S3 オブジェクトに命名する

オブジェクトキー (またはキー名) によって、Amazon S3 バケット内のオブジェクトは一意に識別されます。オブジェクトの作成時にキー名を指定できます。例えば、Amazon S3 コンソールでは、バケットを選択すると、そのバケットに含まれるオブジェクトのリストが表示されます。表示される名前がオブジェクトキーです。

オブジェクトキー名は、UTF-8 でエンコードされた一連の Unicode 文字で構成され、最大長は 1,024 バイト、または約 1,024 個のラテン文字です。ロケールによっては、1 文字でエンコードに 2 バイトが必要になる場合があります。オブジェクトに名前を付けるときは、次の点に注意してください。

- オブジェクトキー名では大文字と小文字が区別されます。
- オブジェクトキー名には、プレフィックス (コンソールではフォルダと呼ばれます) が含まれます。例えば、Development/Projects.xls は Development プレフィックス (またはフォルダ) 内にある Projects.xls オブジェクトのフルオブジェクトキー名です。プレフィックス、区切り記号 (/)、およびオブジェクトの名前は、オブジェクトキー名の 1,024 バイトの制限に含まれます。プレフィックスとフォルダの詳細については、「the section called “オブジェクトキー名の選択”」を参照してください。
- 特定の文字をオブジェクトキー名で使用する際には、特別な処理が必要になる場合があります。詳細については、「the section called “オブジェクトキーの命名のガイドライン”」を参照してください。

> **Note**
>
> 値 "soap" を持つオブジェクトキー名は、仮想ホスト形式のリクエストではサポートされていません。"soap" が使用されるオブジェクトキー名値の場合、代わりにパス形式の URL を使用する必要があります。

オブジェクトキー名の選択

Amazon S3 のデータモデルはフラットな構造をしています。バケットを作成し、バケットにオブジェクトを保存します。サブバケットやサブフォルダの階層はありません。ただし、Amazon S3 コンソールで使用されているようなキー名のプレフィックスや区切り記号を使用して論理的な階層を暗示できます。Amazon S3 コンソールでは、フォルダの概念をサポートしています。Amazon S3 コンソールからメタデータを編集する方法の詳細については、Amazon S3 コンソールでのオブジェクトメタデータの編集 を参照してください。

バケット (admin-created) に、次のようなオブジェクトキーを持つ 4 つのオブジェクトがあるとします。

```
Development/Projects.xls

Finance/statement1.pdf

Private/taxdocument.pdf

s3-dg.pdf
```

コンソールでは、キー名のプレフィックス (Development/、Finance/、Private/) および区切り記号 (/) を使用して、フォルダ構造を表します。s3-dg.pdf キーにはスラッシュで区切られたプレフィックスが含まれていないため、そのオブジェクトはバケットのルートレベルに直接表示されます。Development/ フォルダを開くと、Projects.xlsx オブジェクトが表示されます。

- Amazon S3 ではバケットとオブジェクトをサポートしており、階層はありません。ただし、オブジェクトキー名のプレフィックスと区切り記号により、Amazon S3 コンソールや AWS SDK で階層を暗示し、フォルダの概念を導入できます。
- Amazon S3 コンソールは、フォルダのプレフィックスと区切り記号の値をキーとしてゼロバイトのオブジェクトを作成することにより、フォルダオブジェクトの作成を実装します。これらのフォルダオブジェクトはコンソールに表示されません。それ以外の場合は、他のオブジェクトと同様に動作し、REST API、AWS CLI、および AWS SDK を使用して表示および操作できます。

オブジェクトキーの命名のガイドライン

オブジェクトキー名には UTF-8 文字を使用できます。ただし、キー名に特定の文字を使用すると、一部のアプリケーションやプロトコルで問題が発生することがあります。以下のガイドラインは、DNS、ウェブセーフ文字、XML パーサー、その他の API とのコンプライアンスを最大化するのに役立ちます。

セーフ文字

以下の文字セットは、一般的にキー名で使用しても安全です。

Alphanumeric characters	• 0-9 • a ~ z • A ~ Z
Special characters	• 感嘆符 (!) • ハイフン (-) • 下線 (_) • ピリオド (.) • アスタリスク (*) • 一重引用符 (') • 左丸括弧 (() • 右丸括弧 ())

有効なオブジェクトキー名の例を次に示します。

- `4my-organization`
- `my.great_photos-2014/jan/myvacation.jpg`
- `videos/2014/birthday/video1.wmv`

> **Note**
>
> Amazon S3 コンソールを使用して、キー名がピリオド (.) で終わるオブジェクトをダウンロードすると、ダウンロードしたオブジェクトのキー名の末尾からピリオドが削除され

ます。ダウンロードしたオブジェクトのキー名の末尾のピリオドを保持するには、AWS Command Line Interface (AWS CLI)、AWS SDK、または Amazon S3 REST API を使用する必要があります。
また、以下のプレフィックスの制約についても注意してください。

- プレフィックスが `./` のオブジェクトは、AWS CLI、AWS SDK、または REST API を使用してアップロードまたはダウンロードします。Amazon S3 コンソールを使用してこれらのオブジェクトをアップロードすることはできません。
- 相対パス要素を含むオブジェクトキー (例: `../`) は、左から右に解析したときに、相対パスセグメントの累積数が、検出された非相対パス要素の数を超えない場合に有効です。このルールは、Amazon S3 コンソール、Amazon S3 REST API、AWS CLI、および AWS SDK を使用して行われたすべてのリクエストに適用されます。

  例:

  - `videos/2014/../../video1.wmv` は有効です。
  - `videos/../../video1.wmv` は無効です。
  - `videos/../../2014/video1.wmv` は無効です。

特殊な処理を必要とする可能性がある文字

キー名で以下の文字を使用すると、追加のコード処理が必要になる場合があり、ほとんどの場合、16 進数として URL エンコードまたは参照することが必要になります。これらの文字の一部は表示不可能な文字であり、ブラウザで処理されない場合があります。この場合も、特殊な処理が必要です。

- アンパサンド (&)
- ドル記号 ($)
- 16 進数の 00 ~ 1F (10 進数の 0 ~ 31) の範囲および 7F (10 進数の 127) の ASCII 文字
- アットマーク (@)
- 等号 (=)
- セミコロン (;)
- スラッシュ (/)
- コロン (:)
- プラス記号 (+)

- スペース – 場合によっては、大幅に連続しているスペースが失われる可能性があります (特に複数のスペース)。
- カンマ (,)
- 疑問符 (?)

使用しない方がよい文字

すべてのアプリケーションで一貫性を維持するには相当な量の特殊な処理が必要になるため、キー名には以下の文字を使用しないことをお勧めします。

- バックスラッシュ (\)
- 左中括弧 ({)
- 表示不可能な ASCII 文字 (10 進数の 128 ~ 255 の文字)
- キャレットまたはサーカムフレックス (^)
- 右中括弧 (})
- パーセント記号 (%)
- 重アクセントまたはバックティック (`)
- 右角括弧 (])
- 引用符 (")
- 大なり記号 (>)
- 左角括弧 ([)
- チルダ (~)
- 小なり記号 (<)
- シャープ記号 (#)
- 縦棒またはパイプ (|)

XML 関連のオブジェクトキーの制約

行末処理に関する XML 標準で規定されているとおり、すべての XML テキストは正規化され、1 つのキャリッジリターン (ASCII コード 13) および、改行文字とも呼ばれる改行の直後のキャリッジリターン (ASCII コード 10) が単一の改行文字に置き換えられます。XML リクエストでオブジェクトキーを正しく解析するには、キャリッジリターンやその他の特殊文字を XML タグ内に挿入するときに、同等の XML エンティティコードに置き換える必要があります。

以下では、当該特殊文字とそれに相当する XML エンティティコードのリストを示しています。

- アポストロフィ (') は ' に置き換える必要があります
- 引用符 (") は " に置き換える必要があります
- アンパサンド (&) は & に置き換える必要があります
- 小なり記号 (<) は < に置き換える必要があります
- 大なり記号 (>>) は > に置き換える必要があります
- キャリッジリターン (\r) は
 または
 に置き換える必要があります
- 改行 (\n) は
 または
 に置き換える必要があります

Example

次の例では、キャリッジリターンの代わりに XML エンティティコードを使用する方法を示しています。この DeleteObjects リクエストにより、key パラメータ /some/prefix/objectwith \rcarriagereturn (\r はキャリッジリターン) を持つオブジェクトが削除されます。

```
<Delete xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Object>
    <Key>/some/prefix/objectwith&#13;carriagereturn</Key>
  </Object>
</Delete>
```

オブジェクトメタデータの使用

Amazon S3 には、システム定義メタデータとユーザー定義メタデータの 2 種類のオブジェクトメタデータがあります。システム定義メタデータには、オブジェクトの作成日、サイズ、ストレージクラスなどのメタデータが含まれます。ユーザー定義メタデータは、オブジェクトのアップロード時に設定できるメタデータです。このユーザー定義メタデータは、名前と値のペアのセットです。詳細については、「the section called “システムで定義されたオブジェクトメタデータ”」および「the section called “ユーザー定義のオブジェクトメタデータ”」を参照してください。

オブジェクトを作成するときは、Amazon S3 バケット内のオブジェクトを一意に識別するオブジェクトキー (またはキー名) を指定します。詳細については、「Amazon S3 オブジェクトに命名する」を参照してください。オブジェクトをアップロードする時に Amazon S3 でユーザー定義メタデータを設定することもできます。

オブジェクトをアップロードした後で、このユーザー定義メタデータを変更することはできません。このメタデータを変更する唯一の方法は、オブジェクトのコピーを作成し、メタデータを設定することです。Amazon S3 コンソールを使用したメタデータの編集の詳細については、「Amazon S3 コンソールでのオブジェクトメタデータの編集」を参照してください。

S3 メタデータを使用してメタデータをクエリし、データ検出を高速化する

S3 オブジェクトのメタデータを簡単に検索、保存、クエリするには、S3 メタデータを使用できます。S3 メタデータを使用すると、ビジネス分析、コンテンツ取得、人工知能と機械学習 (AI/ML) モデルトレーニングなどで使用するデータをすばやく準備できます。

S3 メタデータは、汎用バケット内のオブジェクトのメタデータを自動的にキャプチャし、クエリできる読み取り専用のフルマネージド Apache Iceberg テーブルに保存することで、データ検出を高速化します。これらの読み取り専用テーブルはメタデータテーブルと呼ばれます。オブジェクトが汎用バケットに追加、更新、削除されると、S3 メタデータは対応するメタデータテーブルを自動的に更新して、最新の変更を反映します。

デフォルトでは、S3 メタデータは、オブジェクトの作成時刻やストレージクラスなどのシステム定義のオブジェクトメタデータ、およびオブジェクトのアップロード中に含められたタグやユーザー定義のメタデータなどのカスタムメタデータを提供します。S3 メタデータは、オブジェクトが更新または削除されたときや、リクエストを行った AWS アカウントなどのイベントメタデータも提供します。

メタデータテーブルは、表形式データ用に最適化されたストレージを提供する S3 テーブルバケットに保存されます。メタデータをクエリするために、テーブルバケットを Amazon Athena、Amazon Redshift、Amazon QuickSight などの AWS 分析サービスと統合できます。

S3 メタデータの詳細については、「the section called “データ検出の高速化”」を参照してください。

システムで定義されたオブジェクトメタデータ

Amazon S3 では、バケットに格納されるオブジェクトごとに、一連のシステムメタデータが維持されます。Amazon S3 はこのシステムメタデータを必要に応じて処理します。例えば、Amazon S3 ではオブジェクトの作成日とサイズに関するメタデータが維持され、オブジェクト管理の目的でこの情報が使用されます。

システムメタデータには 2 つのカテゴリがあります。

- システム制御 – オブジェクトの作成日などのメタデータはシステムによって制御されます。つまり、Amazon S3 だけがその日付値を変更できることを意味します。

- ユーザー制御 – 他のシステムメタデータ (オブジェクトに設定済みのストレージクラスや、オブジェクトでサーバー側の暗号化が有効になっているかどうかなど) は、ユーザーが値を制御するシステムメタデータの例です。バケットをウェブサイトとして設定している場合、ページリクエストを別のページか外部 URL のいずれかにリダイレクトする場合があります。この場合、ウェブページはバケット内のオブジェクトです。Amazon S3 は、ページリダイレクト値をシステムメタデータとして保存し、ユーザーがその値を制御できます。

  オブジェクトを作成するときに、このようなシステムメタデータ項目の値を設定したり、必要に応じてその値を更新したりできます。ストレージクラスの詳細については、「Amazon S3 ストレージクラスの理解と管理」を参照してください。

  Amazon S3 は Amazon S3 オブジェクトを暗号化する AWS KMS キーを使用します。AWS KMS はオブジェクトデータのみを暗号化します。チェックサムと指定されたアルゴリズムは、オブジェクトのメタデータの一部として保存されます。サーバー側でオブジェクトに対する暗号化が要求された場合、チェックサムは暗号化された形式で保存されます。サーバーサイドの暗号化の詳細については、「暗号化によるデータの保護」を参照してください。

> **Note**
>
> PUT リクエストヘッダーのサイズは 8 KB に制限されています。PUT リクエストヘッダー内のシステム定義メタデータのサイズは 2 KB に制限されています。システム定義メタデータのサイズは、キーと値の各ペアを US-ASCII にエンコードしたバイト数の合計に基づいて測定されます。

次の表は、システム定義のメタデータのリストとユーザーがそれを更新できるかどうかをまとめたものです。

名前	説明	ユーザーが値を変更することはできますか?
`Date`	現在の日付と時刻。	いいえ
`Cache-Control`	キャッシュポリシーを指定するために使用される一般的なヘッダーフィールド。	はい

名前	説明	ユーザーが値を変更することはできますか?
Content-Disposition	オブジェクトのプレゼンテーション情報。	はい
Content-Length	オブジェクトのサイズ (バイト単位)。	いいえ
Content-Type	オブジェクトのタイプ。	はい
Last-Modified	オブジェクト作成日または最終更新日のいずれか遅い方。マルチパートアップロードの場合、オブジェクトの作成日はマルチパートアップロードの開始日です。	いいえ
ETag	オブジェクトのエンティティタグ (ETag) は、そのオブジェクトの特定のバージョンを表します。マルチパートアップロードとしてアップロードされず、暗号化されていない、または Simple Storage Service (Amazon S3) 管理キー (SSE-S3) を使用したサーバー側の暗号化によって暗号化されているオブジェクトの場合、ETag はデータの MD5 ダイジェストです。	いいえ
x-amz-server-side-encryption	オブジェクトでサーバー側の暗号化が有効であるか、そして暗号化が AWS Key Management Service (AWS KMS) または Amazon S3 で管理された暗号化 (SSE-S3) によるものかを示すヘッダー。詳細については、「サーバー側の暗号化によるデータの保護」を参照してください。	はい

名前	説明	ユーザーが値を変更することはできますか?
x-amz-checksum-crc64nvme , x-amz-checksum-crc32 , x-amz-checksum-crc32c , x-amz-checksum-sha1 , x-amz-checksum-sha256	オブジェクトのチェックサムまたはダイジェストが含まれるヘッダー。Amazon S3 に使用するように指示したチェックサムアルゴリズムに応じて、これらのヘッダーの最大 1 つが一度に設定されます。チェックサムアルゴリズムの選択の詳細については、「Amazon S3 でのオブジェクトの整合性のチェック」を参照してください。	いいえ
x-amz-checksum-type	チェックサムタイプ。マルチパートオブジェクトのオブジェクトレベルのチェックサムを作成するために、パートレベルのチェックサムをどのように組み合わせるかを決定します。	はい
x-amz-version-id	オブジェクトのバージョン。バケットのバージョニングを有効にすると、Amazon S3 ではバケットに追加されたオブジェクトにバージョン ID が割り当てられます。詳細については、「S3 バージョニングによる複数のバージョンのオブジェクトの保持」を参照してください。	いいえ
x-amz-delete-marker	オブジェクトが削除マーカーであるかどうかを示すブール値マーカー。このマーカーは、バージョニングが有効になっているバケットでのみ使用されます。	いいえ
x-amz-storage-class	オブジェクトの保存に使われるストレージクラス。詳細については、「Amazon S3 ストレージクラスの理解と管理」を参照してください。	はい

名前	説明	ユーザーが値を変更することはできますか?
x-amz-website-redirect-location	関連付けられたオブジェクトのリクエストを同じバケット内の別のオブジェクトまたは外部 URL にリダイレクトするヘッダー。詳細については、「(オプション) ウェブページリダイレクトの設定」を参照してください。	はい
x-amz-server-side-encryption-aws-kms-key-id	オブジェクトの暗号化に使用された AWS KMS 対称暗号化 KMS キーの ID を示すヘッダー。このヘッダーは、x-amz-server-side-encryption ヘッダーが存在し、値が aws:kms である場合にのみ使用されます。	はい
x-amz-server-side-encryption-customer-algorithm	お客様が用意した暗号化キーを使用したサーバー側の暗号化 (SSE-C) が有効であるかどうかを示すヘッダー。詳細については、「お客様が指定したキーによるサーバー側の暗号化 (SSE-C) の使用」を参照してください。	はい
x-amz-tagging	オブジェクトのタグセット。タグセットは URL クエリパラメータとしてエンコードする必要があります。	はい

ユーザー定義のオブジェクトメタデータ

オブジェクトをアップロードするときに、そのオブジェクトにメタデータを割り当てることもできます。このオプション情報は、オブジェクトを作成するための PUT リクエストまたは POST リクエストを送信するときに、名前と値 (キーと値) のペアとして指定します。REST API を使用してオブジェクトをアップロードするときは、オプションのユーザー定義メタデータ名を「x-amz-meta-」で始め、他の HTTP ヘッダーと区別する必要があります。REST API を使用してオブジェクトを取得するときは、このプレフィックスが返されます。SOAP API を使用してオブジェクトをアップロードする場合、このプレフィックスは不要です。SOAP API を使用してオブジェクトを取得するときは、オブジェクトのアップロードに使用した API にかかわらず、プレフィックスは削除されます。

> **Note**
>
> SOAP API は新規顧客には利用できず、2025 年 8 月 31 日にサポート終了 (EOL) となります。REST API か AWS SDK を使用することをお勧めします。

REST API を介してメタデータを取得するとき、同じ名前を持つヘッダー (大文字と小文字は区別されません) は Amazon S3 によってカンマ区切りリストに結合されます。出力不可能な文字が含まれているメタデータは返されません。その代わりに、`x-amz-missing-meta` ヘッダーが、出力不可能なメタデータエントリの数を示す値と共に返されます。`HeadObject` アクションは、オブジェクト自体を返さずに、オブジェクトからメタデータを取得します。このオペレーションは、オブジェクトのメタデータのみに関心がある場合に役立ちます。`HEAD` を使用するには、オブジェクトへの `READ` アクセス権が必要です。詳細については、Amazon Simple Storage Service API リファレンスの「HeadObject」を参照してください。

ユーザー定義メタデータはキーと値のペアのセットです。Amazon S3 はユーザー定義メタデータキーを小文字で保存します。

Amazon S3 では、任意の Unicode 文字をメタデータ値で使用できます。

これらのメタデータ値の表示に関連した問題を回避するために、REST を使用する場合は US-ASCII 文字を使用してください。SOAP またはブラウザベースのアップロードを `POST` 経由で使用する場合は UTF-8 を使用してください。

US-ASCII 以外の文字をメタデータ値で使用すると、指定した Unicode 文字列に US-ASCII 以外の文字が含まれていないかどうか調べられます。そのようなヘッダーの値は、保存される前に RFC 2047 に従って文字デコードされます。さらに、RFC 2047 に従ってエンコードされ、メールセーフになってから返されます。文字列に US-ASCII 文字のみが含まれている場合は、そのまま表示されます。

以下に例を示します。

```
PUT /Key HTTP/1.1
Host: amzn-s3-demo-bucket.s3.amazonaws.com
x-amz-meta-nonascii: ÄMÄZÕÑ S3

HEAD /Key HTTP/1.1
Host: amzn-s3-demo-bucket.s3.amazonaws.com
x-amz-meta-nonascii: =?UTF-8?B?w4PChE3Dg8KEWsODwpXDg8KRIFMz?=
```

```
PUT /Key HTTP/1.1
Host: amzn-s3-demo-bucket.s3.amazonaws.com
x-amz-meta-ascii: AMAZONS3

HEAD /Key HTTP/1.1
Host: amzn-s3-demo-bucket.s3.amazonaws.com
x-amz-meta-ascii: AMAZONS3
```

> **Note**
>
> PUT リクエストヘッダーのサイズは 8 KB に制限されています。PUT リクエストヘッダー内のユーザー定義メタデータのサイズは 2 KB に制限されています。ユーザー定義メタデータのサイズは、キーと値それぞれの UTF-8 エンコーディングの合計バイト数を使用して測定されます。

アップロード済みオブジェクトのメタデータの変更 (オブジェクトのコピーを作成し、それを変更して古いオブジェクトと置き換える場合、または新しいバージョンを作成する場合) については、Amazon S3 コンソールでのオブジェクトメタデータの編集 を参照してください。

Amazon S3 コンソールでのオブジェクトメタデータの編集

Amazon S3 コンソールを使用して、[コピー] アクションを使用して既存の S3 オブジェクトのメタデータを編集できます。メタデータを編集するには、オブジェクトを同じ宛先にコピーし、適用する新しいメタデータを指定します。これにより、オブジェクトの古いメタデータが置き換えられます。一部のメタデータは、オブジェクトをアップロードするときに Amazon S3 によって設定されます。例えば、`Content-Length` および `Last-Modified` は、ユーザーが変更できない、システム定義のオブジェクトメタデータフィールドです。

また、オブジェクトのアップロード時にユーザー定義のメタデータを設定し、必要に応じて後で置き換えることもできます。例えば、STANDARD ストレージクラスに最初に保存したオブジェクトのセットがあるとします。時間の経過とともに、このデータを高可用性にする必要がなくなる可能性があります。そのため、`x-amz-storage-class` キーの値を `STANDARD` から `GLACIER` に置き換えて、ストレージクラスを `GLACIER` に変更できます。

> **Note**
>
> Amazon S3 でオブジェクトメタデータを置き換える場合は、次のことを考慮してください。

- 保持する既存のメタデータ、追加するメタデータ、および編集するメタデータを指定する必要があります。
- オブジェクトが 5 GB 未満の場合は、S3 コンソールで [コピー] アクションを使用してオブジェクトメタデータを置き換えることができます。オブジェクトが 5 GB を超える場合は、AWS CLI または AWS SDK を使用してオブジェクトをマルチパートアップロードでコピーするときに、オブジェクトメタデータを置き換えることができます。詳細については、「マルチパートアップロードを使用したオブジェクトのコピー」を参照してください。
- メタデータを置き換えるために必要な追加のアクセス許可のリストについては、「the section called “S3 API オペレーションに必要なアクセス許可”」を参照してください。このアクセス許可を付与するポリシーの例については、「the section called “アイデンティティベースのポリシーの例”」を参照してください。
- このアクションにより、更新された設定と最終更新日を持つオブジェクトのコピーが作成されます。S3 バージョニングが有効になっている場合は、オブジェクトの新しいバージョンが作成され、既存のオブジェクトが古いバージョンになります。S3 バージョニングが有効になっていない場合は、元のオブジェクトがオブジェクトの新しいコピーに置き換えられます。プロパティを変更する IAM ロールに関連付けられた AWS アカウント も、新しいオブジェクトまたは (オブジェクトバージョン) の所有者になります。
- メタデータを編集すると、既存のキー名の値が置き換えられます。
- お客様が用意した暗号化キー (SSE-C) で暗号化されたオブジェクトは、コンソールを使用してコピーすることはできません。AWS CLI、AWS SDK、または Amazon S3 REST API を使用する必要があります。
- Amazon S3 コンソールを使用してオブジェクトをコピーすると、"Copied metadata can't be verified." というエラーメッセージが表示されることがあります。コンソールは、ヘッダーを使用してオブジェクトのメタデータを取得し、設定します。ネットワークまたはブラウザの設定によってネットワークリクエストが変更された場合、この動作により、コピーしたオブジェクトに意図しないメタデータ (変更された `Cache-Control` ヘッダーなど) が書き込まれる可能性があります。Amazon S3 はこの意図しないメタデータを検証できません。

  この問題に対処するには、ネットワークとブラウザの設定をチェックして、`Cache-Control` などのヘッダーが変更されていないことを確認します。詳細については、「The Shared Responsibility Model」を参照してください。

> **Warning**
>
> フォルダのメタデータを置き換える場合は、[コピー] アクションが完了するのを待ってから、フォルダに新しいオブジェクトを追加します。そうしないと、新しいオブジェクトも編集される可能性があります。

以下のトピックでは、Amazon S3 コンソールで [コピー] アクションを使用してオブジェクトのメタデータを置き換える方法について説明します。

システム定義メタデータの置き換え

S3 オブジェクトのシステム定義メタデータを置き換えられます。システム定義のメタデータと変更可能な値のリストについては、「システムで定義されたオブジェクトメタデータ」を参照してください。

オブジェクトのシステム定義メタデータを置き換えるには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[汎用バケット] または [ディレクトリバケット] を選択します。
3. バケットのリストで、変更するオブジェクトが含まれるバケットの名前を選択します。
4. 変更するオブジェクトのチェックボックスをオンにします。
5. [アクション] メニューに表示されるオプションのリストから [コピー] を選択します。
6. 送信先パスを指定するには、[S3 の参照] を選択し、ソースオブジェクトと同じ送信先に移動して、送信先にあるチェックボックスをオンにします。右下の [Choose destination] (送信先を選択する) を選択します。

   または、送信先パスを入力します。
7. バケットバージョニングを有効にしていない場合は、バケットバージョニングを有効にして、オブジェクトを意図しない上書きまたは削除から保護することを推奨する警告が表示されます。このバケットのオブジェクトの全バージョンを保持する場合は、[バケットのバージョニングを有効にする] をクリックします。[送信先の詳細] で、デフォルトの暗号化プロパティと Object Lock プロパティを確認することもできます。
8. [追加のコピー設定] で、[設定を指定] を選択して、[メタデータ] の設定を指定します。
9. [メタデータ] セクションまでスクロールし、[すべてのメタデータを置き換え] を選択します。

10. [メタデータの追加] を選択します。
11. メタデータの [Type (タイプ)] には、[System-defined (システム定義)] を選択します。
12. 一意の [Key (キー)] とメタデータの [Value (値)] を指定します。
13. 追加のメタデータを編集するには、[Add metadata (メタデータの追加)] を選択します。[削除] をクリックして、タイプ、キー、値のセットを削除することもできます。
14. [コピー] を選択します。Amazon S3 はメタデータの変更を保存します。

ユーザー定義メタデータの置き換え

メタデータプレフィックス、`x-amz-meta-`、およびカスタムキーを作成するために選択した名前を組み合わせて、オブジェクトのユーザー定義メタデータを置き換えられます。例えば、カスタム名 `alt-name` を追加した場合、メタデータキーは `x-amz-meta-alt-name` になります。

ユーザー定義メタデータの合計サイズは最大 2 KB です。ユーザー定義メタデータの合計サイズを計算するには、キーと値ごとの UTF-8 エンコーディングのバイト数を合計します。キーと値の両方が US-ASCII 標準に従っている必要があります。詳細については、「ユーザー定義のオブジェクトメタデータ」を参照してください。

オブジェクトのユーザー定義メタデータを置き換えるには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ナビゲーションペインで [バケット] を選択してから、[汎用バケット] または [ディレクトリバケット] タブをクリックします。変更するオブジェクトを含む Amazon S3 バケットまたはフォルダに移動します。
3. 変更するオブジェクトのチェックボックスをオンにします。
4. [アクション] メニューに表示されるオプションのリストから [コピー] を選択します。
5. 送信先パスを指定するには、[S3 の参照] を選択し、ソースオブジェクトと同じ送信先に移動して、送信先にあるチェックボックスをオンにします。[コピー先の選択] を選択します。

   または、送信先パスを入力します。
6. バケットバージョニングを有効にしていない場合は、バケットバージョニングを有効にして、オブジェクトを意図しない上書きまたは削除から保護することを推奨する警告が表示されます。このバケットのオブジェクトの全バージョンを保持する場合は、[バケットのバージョニングを有効にする] をクリックします。[送信先の詳細] で、デフォルトの暗号化プロパティと Object Lock プロパティを確認することもできます。

7. [追加のコピー設定] で、[設定を指定] を選択して、[メタデータ] の設定を指定します。
8. [メタデータ] セクションまでスクロールし、[すべてのメタデータを置き換え] を選択します。
9. [メタデータの追加] を選択します。
10. メタデータの [タイプ] には [ユーザー定義] を選択します。
11. `x-amz-meta-` に続いて、一意のカスタム [キー] を入力します。メタデータの [Value (値)] も入力します。
12. さらにメタデータを追加するには、[Add metadata (メタデータの追加)] を選択します。[削除] をクリックして、タイプ、キー、値のセットを削除することもできます。
13. [コピー] を選択します。Amazon S3 はメタデータの変更を保存します。

S3 メタデータによるデータ検出の高速化

Amazon S3 メタデータは、汎用バケット内のオブジェクトのメタデータを自動的にキャプチャし、クエリできる読み取り専用のフルマネージド Apache Iceberg テーブルに保存することで、データ検出を高速化します。これらの読み取り専用テーブルはメタデータテーブルと呼ばれます。オブジェクトが汎用バケットに追加、更新、削除されると、S3 メタデータは対応するメタデータテーブルを自動的に更新して、最新の変更を反映します。

デフォルトでは、S3 メタデータは次の 3 種類のメタデータを提供します。

- オブジェクトの作成時刻やストレージクラスなどのシステム定義メタデータ
- オブジェクトのアップロード時に含められたタグやユーザー定義メタデータなどのカスタムメタデータ
- オブジェクトが更新または削除されたときや、リクエストを行った AWS アカウントなどのイベントメタデータ

メタデータテーブルに保存されるデータの詳細については、「the section called “メタデータテーブルスキーマ”」を参照してください。

S3 メタデータを使用すると、S3 オブジェクトのメタデータを簡単に検索、保存、クエリできるため、ビジネス分析、コンテンツ取得、人工知能と機械学習 (AI/ML) モデルトレーニングなどで使用するデータをすばやく準備できます。

メタデータテーブルは、表形式データ用に最適化されたストレージを提供する S3 テーブルバケットに保存されます。メタデータを簡単にクエリするために、テーブルバケットを AWS Glue Data Catalog と統合できます。テーブルバケットが AWS Glue Data Catalog と統合されると、Amazon

Athena、Amazon EMR、Amazon Redshift、Apache Spark、Trino などのクエリエンジンを使用してメタデータテーブルを直接クエリできます。Apache Iceberg 形式をサポートする他のアプリケーションを使用してメタデータテーブルをクエリすることもできます。メタデータテーブルからダッシュボードを作成するには、Amazon QuickSight を使用します。

S3 メタデータの料金については、「Amazon S3 の料金」を参照してください。

メタデータテーブルの仕組み

メタデータテーブルは Amazon S3 によって管理され、Amazon S3 自体の外部にある IAM プリンシパルによって変更することはできません。(ただし、メタデータテーブルを削除することはできます。) その結果、メタデータテーブルは読み取り専用になり、バケットの内容が正しく反映されます。

Apache Iceberg メタデータテーブルのパフォーマンスを最適な状態に維持するために、Amazon S3 は、圧縮や参照されていないファイルの削除などの定期的なメンテナンスアクティビティをテーブルに対して実行します。これらのメンテナンスアクティビティは、メタデータテーブルの保存コストを最小限に抑え、クエリのパフォーマンスを最適化するのに役立ちます。このテーブルのメンテナンスは自動的に行われるため、オプトインや継続的な管理は必要ありません。ただし、必要に応じて、これらのテーブルメンテナンスアクティビティを設定できます。詳細については、「Table bucket maintenance」を参照してください。

> **Note**
>
> S3 メタデータは、汎用バケットに変更を加えるときにメタデータテーブルに継続的に追加されるように設計されています。それぞれの更新で、メタデータテーブルの新しいバージョンであるスナップショットが作成されます。メタデータテーブルは読み取り専用であるため、メタデータテーブル内のレコードを削除することはできません。また、S3 テーブルのスナップショットの有効期限機能を使用して、メタデータテーブルの古いスナップショットを期限切れにすることもできません。
>
> コストを最小限に抑えるために、メタデータテーブル設定とメタデータテーブルを定期的に削除してから再作成することができます。詳細については、「the section called “メタデータテーブル設定の削除”」および「the section called “メタデータテーブルの削除”」を参照してください。

オブジェクトメタデータを生成して S3 マネージドメタデータテーブルに保存するには、汎用バケットのメタデータテーブル設定を作成します。Amazon S3 は、バケットで設定がアクティブである限

り、メタデータテーブルを継続的に更新してデータへの最新の変更を反映するように設計されています。

メタデータテーブル設定を作成するには、メタデータテーブルを作成および管理するために必要な AWS Identity and Access Management (IAM) アクセス許可があることを確認する必要があります。詳細については、「the section called “メタデータテーブルのアクセス許可”」を参照してください。また、メタデータテーブルを保存する S3 テーブルバケットを作成または指定する必要があります。このテーブルバケットは、汎用バケットと同じ AWS リージョンおよびアカウントにある必要があります。テーブルバケットの作成の詳細については、「Creating table buckets」を参照してください。

> **Note**
>
> S3 メタデータは、メタデータテーブル設定を作成する前に汎用バケットに既に存在していたオブジェクトには適用されません。つまり、S3 メタデータは、メタデータテーブル設定を作成した後に発生する変更イベント (アップロード、更新、削除など) のメタデータのみをキャプチャします。

メタデータテーブル設定の更新をモニタリングするには、AWS CloudTrail を使用できます。詳細については、「the section called “CloudTrail ログ記録によって追跡される Amazon S3 バケットレベルのアクション”」を参照してください。

トピック

- メタデータテーブルの制限と制約
- S3 メタデータテーブルスキーマ
- メタデータテーブルの設定
- メタデータテーブルのクエリ

メタデータテーブルの制限と制約

メタデータテーブル設定を作成する前に、次の制限と制約に注意してください。

- S3 メタデータは現在、米国東部 (バージニア北部)、米国東部 (オハイオ)、および米国西部 (オレゴン) リージョンでのみ使用できます。
- S3 メタデータは、以下を除くすべてのストレージクラスをサポートします。
  - S3 Express One Zone ストレージクラス

- Local Zones のディレクトリバケットにある S3 One Zone-Infrequent Access (S3 One Zone-IA、Z-IA) ストレージクラス

> **Note**
>
> S3 Intelligent-Tiering ストレージクラスの場合、特定の階層はメタデータテーブルに表示されません。

- メタデータテーブル設定を作成するには、メタデータテーブルを保存する S3 テーブルバケットを作成または指定する必要があります。このテーブルバケットは、汎用バケットと同じ AWS リージョンおよび AWS アカウントにある必要があります。
- S3 メタデータは、ディレクトリバケットまたはテーブルバケットではサポートされていません。メタデータテーブル設定は、汎用バケットに対してのみ作成できます。
- S3 メタデータは、メタデータテーブル設定を作成する前に汎用バケットに既に存在していたオブジェクトには適用されません。つまり、S3 メタデータは、メタデータテーブル設定を作成した後に発生する変更イベント (アップロード、更新、削除など) のメタデータのみをキャプチャします。
- S3 メタデータは、汎用バケットに変更を加えるときにメタデータテーブルに継続的に追加されるように設計されています。それぞれの更新で、メタデータテーブルの新しいバージョンであるスナップショットが作成されます。メタデータテーブルは読み取り専用であるため、メタデータテーブル内のレコードを削除することはできません。また、S3 テーブルのスナップショットの有効期限機能を使用して、メタデータテーブルの古いスナップショットを期限切れにすることもできません。

  コストを最小限に抑えるために、メタデータテーブル設定とメタデータテーブルを定期的に削除してから再作成することができます。詳細については、「the section called “メタデータテーブル設定の削除”」および「the section called “メタデータテーブルの削除”」を参照してください。
- テーブルバケットまたはテーブルポリシーを作成または更新するときは、Amazon S3 がテーブルバケットまたはメタデータテーブルに書き込むことを制限しないようにしてください。Amazon S3 がテーブルバケットまたはメタデータテーブルに書き込めない場合は、メタデータテーブル設定とメタデータテーブルを削除してから新しい設定を作成し、新しいメタデータテーブルを作成する必要があります。
- メタデータテーブルを削除する前に、まず汎用バケット上の関連するメタデータテーブル設定を削除する必要があります。
- メタデータテーブル設定は、汎用バケット全体に対してのみ作成できます。プレフィックスレベルでメタデータテーブル設定を適用することはできません。

- メタデータテーブルの更新を一時停止および再開することはできません。代わりに、関連付けられているメタデータテーブル設定を削除することで、メタデータテーブルの更新を停止できます。更新の受信を再開するには、新しいメタデータテーブル設定を作成し、新しいメタデータテーブルを作成する必要があります。
- メタデータテーブルには、S3 インベントリまたは Amazon S3 REST API で利用できるメタデータと同じものがすべて含まれているわけではありません。例えば、次の情報はメタデータテーブルでは使用できません。
  - S3 ライフサイクルの有効期限または移行ステータス
  - Object Lock の保持期間またはガバナンスモード
  - オブジェクトのアクセスコントロールリスト (ACL) 情報
  - レプリケーションステータス
- メタデータテーブルのパーティショニングまたはソートを調整することはできません。その結果、一部のクエリではテーブルスキャンが必要になる可能性があり、効率が低下する可能性があります。

S3 メタデータテーブルスキーマ

Amazon S3 メタデータテーブルには行と列が含まれています。各行は、汎用バケット内のオブジェクトを作成、更新、または削除したミューテーションイベントを表します。これらのイベントの大部分はさまざまなユーザーアクションの結果ですが、これらのイベントの一部は、S3 ライフサイクルの有効期限切れやストレージクラスの移行など、Amazon S3 がユーザーに代わって実行したアクションの結果です。

S3 メタデータは、汎用バケットで発生した変更とメタデータテーブルを最終的に一致させるように設計されたイベント処理パイプラインです。オブジェクトが作成または更新されたことが S3 メタデータに通知されるまでに、そのオブジェクトがバケットで既に上書きまたは削除されている可能性があることに注意してください。デフォルトでは、S3 バケットオペレーションごとにテーブル行が作成されます。ただし、オブジェクトメタデータが削除または上書きされた場合、またはオブジェクトを取得できなくなった場合、一部の列には欠落しているメタデータスキーマを示す NULL 値が表示されることがあります。

以下は、`amzn-s3-demo-bucket:` という名前の汎用バケットのメタデータテーブルの例です。

```
bucket               key                      sequence_number
                                                                record_type
 record_timestamp          version_id   is_delete_marker   size   last_modified_date
```

```
   e_tag                            storage_class  is_multipart   encryption_status
 is_bucket_key_enabled   kms_key_arn
               checksum_algorithm   object_tags   user_metadata

    requester      source_ip_address   request_id
amzn-s3-demo-bucket   Finance/statement1.pdf
 80e737d8b4d82f776afffffffffffffff006737d8b4d82f776a00000000000000000000000000000000000000000000000
   CREATE        2024-11-15 23:26:44.899                 FALSE
 6223   11/15/2024 23:26     e131b86632dda753aac4018f72192b83    STANDARD
 FALSE          SSE-KMS             FALSE                   arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890df   SSECRC32             {}
            {count -> Asia, customs -> false, family -> true, location -> Mary, name ->
 football, user -> United States}                       111122223333   192.0.2.1
    CVK8FWYRW0M9JW65
amzn-s3-demo-bucket   s3-dg.pdf
 80e737d8b4e39f1dbdfffffffffffffff006737d8b4e39f1dbd00000000000000000000000000000000000000000000000
   CREATE        2024-11-15 23:26:44.942                 FALSE
 3554   11/15/2024 23:26     9bb49efc2d92c05558ddffbbde8636d5    STANDARD
 FALSE          DSSE-KMS            FALSE                   arn:aws:kms:us-
east-1:936810216292:key/0dcebce6-49fd-4cae-b2e2-5512ad281afd   SSESHA1              {}
           {}
                                                    111122223333   192.0.2.1
   CVKAQDRAZEG7KXAY
amzn-s3-demo-bucket   Development/Projects.xls
 80e737d8b4ed9ac5c6fffffffffffffff006737d8b4ed9ac5c600000000000000000000000000000000000000000000000
   CREATE        2024-11-15 23:26:44.966                 FALSE              7746
 11/15/2024 23:26     729a6863e47fb9955b31bfabce984908    STANDARD   FALSE
 SSE-S3              FALSE                   NULL
                                  SSECRC32             {}            {count -> Asia,
 customs -> Canada, family -> Billiards, filter -> true, location -> Europe, name ->
 Asia, user -> United States}   111122223333   192.0.2.1           CVK7Z6XQTQ90BSRV
```

メタデータテーブルには次のスキーマがあります。

列名	必須?	データ型	
bucket	はい	String	汎用バケット名。詳細については、「the section called “名前付けルール”」を参照してください。

列名	必須?	データ型	
key	はい	String	バケット内のオブジェクトを一意に識別するオブジェクトのキー名 (またはキー)。詳細については、「the section called "オブジェクトに命名する"」を参照してください。
sequence_number	はい	String	シーケンス番号。特定のオブジェクトのレコードに含まれる序数です。同じバケットとキーのレコードを順に並べるには、sequence_number でソートできます。特定のバケットとキーについて、sequence_number 値が辞書順で大きいほど、レコードがより最近バケットに導入されたことを意味します。

列名	必須?	データ型	
record_type	はい	String	このレコードのタイプ。CREATE、UPDATE_METADATA 、または DELETE のいずれかです。 CREATE レコードは、新しいオブジェクト (またはオブジェクトの新しいバージョン) がバケットに書き込まれたことを示します。 UPDATE_METADATA レコードは、ストレージクラスやタグなど、既存のオブジェクトの変更可能なメタデータへの変更をキャプチャします。 DELETE レコードは、このオブジェクト (またはオブジェクトのこのバージョン) が削除されたことを示します。バージョニングが有効になっている場合、DELETE レコードは削除マーカーまたは永続的な削除のいずれかを表します。削除マーカーの record_ty

列名	必須?	データ型	
			pe 値は DELETE で、is_delete_marker 値は True です。完全削除レコードは、bucket、key、sequence number 、record_type 、record_timestamp 、version_id を除く他のすべての列の値が null です。詳細については、「the section called “オブジェクトバージョンの削除”」を参照してください。
record_timestamp	はい	Timestamp NTZ (タイムゾーンなし)	このレコードに関連付けられているタイムスタンプ。

列名	必須?	データ型	
version_id	いいえ	String	オブジェクトのバージョン ID。バケットのバージョニングを有効にすると、Amazon S3 はバケットに追加されたオブジェクトにバージョン番号を割り当てます。詳細については、「the section called “オブジェクトの複数のバージョンを保持する”」を参照してください。 バージョニング状態を設定する前にバケットに保存されたオブジェクトのバージョン ID は null です。

列名	必須?	データ型	
is_delete_marker	いいえ	ブール値	オブジェクトの削除マーカーのステータス。オブジェクトが削除マーカーの場合、この値は True です。それ以外の場合は、False です。詳細については、「the section called “削除マーカーの使用”」を参照してください。 **Note** 削除マーカーに追加される行の record_type 値は DELETE ではなく UPDATE_METADATA です。S3 ライフサイクルの有効期限が切れた結果として削除マーカーが作成された場合、requester 値は s3.amazon

列名	必須?	データ型	
			aws.com です。
size	いいえ	Long	バイト単位のオブジェクトサイズ。不完全なマルチパートアップロードまたはオブジェクトメタデータのサイズは含まれません。is_delete_marker が True の場合、サイズは 0 です。詳細については、「the section called “システムで定義されたオブジェクトメタデータ”」を参照してください。
last_modified_date	いいえ	Timestamp NTZ (タイムゾーンなし)	オブジェクト作成日または最終更新日のいずれか遅い方。マルチパートアップロードの場合、オブジェクトの作成日はマルチパートアップロードが開始された日付です。詳細については、「the section called “システムで定義されたオブジェクトメタデータ”」を参照してください。

列名	必須?	データ型	
e_tag	いいえ	String	エンティティタグ (ETag) は、オブジェクトのハッシュです。ETag は、変更をオブジェクトのコンテンツにのみ反映し、メタデータには反映しません。ETag は、オブジェクトデータの MD5 ダイジェストである場合があります。ETag が MD5 ダイジェストであるかどうかは、オブジェクトの作成方法と暗号化方法によって異なります。詳細については、「Amazon S3 API リファレンス」の「Object」を参照してください。

列名	必須?	データ型	
storage_class	いいえ	String	オブジェクトの保存に使用されるストレージクラス。STANDARD、REDUCED_REDUNDANCY 、STANDARD_IA 、ONEZONE_IA 、INTELLIGENT_TIERING 、GLACIER、DEEP_ARCHIVE 、GLACIER_IR のいずれかです。詳細については、「the section called “ストレージクラスの理解と管理”」を参照してください。
is_multipart	いいえ	ブール値	オブジェクトのアップロードタイプ。オブジェクトがマルチパートアップロードとしてアップロードされた場合、この値は True です。それ以外の場合は、False です。詳細については、「the section called “マルチパートアップロードの使用”」を参照してください。

列名	必須?	データ型	
encryption_status	いいえ	String	使用される暗号化キーの種類に応じた、オブジェクトのサーバー側の暗号化ステータス。Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3)、AWS Key Management Service (AWS KMS) キーによるサーバー側の暗号化 (SSE-KMS)、AWS KMS keys による二層式サーバー側の暗号化 (DSSE-KMS)、またはお客様が指定したキーによるサーバー側の暗号化 (SSE-C) のいずれかとなります。オブジェクトが暗号化されていない場合、この値は null です。可能な値は、SSE-S3、SSE-KMS、DSSE-KMS、SSE-C、または null です。詳細については、「the section called “データ暗号化”」を参照してください。

列名	必須?	データ型	
is_bucket_key_enabled	いいえ	ブール値	オブジェクトの S3 バケットキーの有効化ステータス。オブジェクトが SSE-KMS に S3 バケットキーを使用する場合、この値は True です。それ以外の場合は、False です。詳細については、「the section called “オブジェクトの S3 バケットキーを設定する”」を参照してください。

列名	必須?	データ型	
kms_key_arn	いいえ	String	encryption_status が SSE-KMS または DSSE-KMS の行の場合、オブジェクトの暗号化に使用される KMS キーの Amazon リソースネーム (ARN)。オブジェクトが SSE-KMS または DSSE-KMS で暗号化されていない場合、値は null です。詳細については、「the section called “AWS KMS に保存された KMS キー (SSE-KMS)”」および「the section called “二層式サーバー側の暗号化 (DSSE-KMS) ”」を参照してください。 **Note** 行が、削除または上書きイベントが処理された時点で存在しなくなったオブジェクトバージョンを表す場合、encryptio

列名	必須?	データ型	
			n_status 列の値が SSE-KMS または DSSE-KMS であっても、kms_key_arn には null 値が含まれます。
checksum_algorithm	いいえ	String	オブジェクトのチェックサムを作成するために使用されるアルゴリズム。CRC64-NVME 、CRC32、CRC32C、SHA1、または SHA256 のいずれかです。チェックサムが存在しない場合、この値は null です。詳細については、「the section called “サポートされているチェックサムアルゴリズムの使用”」を参照してください。

列名	必須?	データ型	
object_tags	いいえ	Map <String, String>	オブジェクトに関連付けられたオブジェクトタグ。オブジェクトタグは、キーと値のペアのマップとして保存されます。オブジェクトにオブジェクトタグがない場合、空のマップ ({}) が保存されます。詳細については、the section called "タグを使用してオブジェクトを分類する"を参照してください。 **Note** record_type 値が DELETE の場合、object_tags 列には null 値が含まれます。record_type 値が CREATE または UPDATE_METADATA の場合、削除または上書きイベント

列名	必須?	データ型	
			が処理された時点で存在しなくなったオブジェクトバージョンを表す行には、object_tags 列に null 値が含まれます。

列名	必須?	データ型	
user_metadata	いいえ	Map <String, String>	オブジェクトに関連付けられているユーザーメタデータ。ユーザーメタデータは、キーと値のペアのマップとして保存されます。オブジェクトにユーザーメタデータがない場合、空のマップ ({}) が保存されます。詳細については、「the section called “ユーザー定義のオブジェクトメタデータ”」を参照してください。 **Note** record_type 値が DELETE の場合、user_metadata 列には null 値が含まれます。record_type 値が CREATE または UPDATE_METADATA の場合、削除または上書きイベント

列名	必須?	データ型	
			が処理された時点で存在しなくなったオブジェクトバージョンを表す行には、user_metadata 列に null 値が含まれます。
requester	いいえ	String	リクエストを行ったリクエスタまたは AWS のサービスプリンシパルの AWS アカウント ID。
source_ip_address	いいえ	String	リクエストの送信元 IP アドレス。ユーザーリクエストによって生成されたレコードの場合、この列にはリクエストの送信元 IP アドレスが含まれます。ユーザーに代わって Amazon S3 または別の AWS のサービスによって実行されたアクションの場合、この列には null 値が含まれます。

列名	必須?	データ型	
request_id	いいえ	String	リクエストに関連付けられたリクエスト ID。

メタデータテーブルの設定

Amazon S3 メタデータは、汎用バケット内のオブジェクトのメタデータを自動的にキャプチャし、クエリできる読み取り専用のフルマネージド Apache Iceberg テーブルに保存することで、データ検出を高速化します。これらの読み取り専用テーブルはメタデータテーブルと呼ばれます。オブジェクトが汎用バケットに追加、更新、削除されると、S3 メタデータは対応するメタデータテーブルを自動的に更新して、最新の変更を反映します。

S3 メタデータを使用すると、S3 オブジェクトのメタデータを簡単に検索、保存、クエリできるため、ビジネス分析、人工知能と機械学習 (AI/ML) モデルトレーニングなどで使用するデータをすばやく準備できます。

オブジェクトメタデータを生成して S3 マネージドメタデータテーブルに保存するには、汎用バケットのメタデータテーブル設定を作成します。Amazon S3 は、バケットで設定がアクティブである限り、メタデータテーブルを継続的に更新してデータへの最新の変更を反映するように設計されています。さらに、Amazon S3 はメタデータテーブルを継続的に最適化して、ストレージコストを削減し、分析クエリのパフォーマンスを向上させます。

メタデータテーブル設定を作成するには、メタデータテーブルを作成および管理するために必要な AWS Identity and Access Management (IAM) アクセス許可があることを確認してください。また、メタデータテーブルを保存する S3 テーブルバケットを作成または指定する必要があります。このテーブルバケットは、汎用バケットと同じ AWS リージョンおよび AWS アカウントにある必要があります。

メタデータテーブル設定の更新をモニタリングするには、AWS CloudTrail を使用できます。詳細については、「the section called “CloudTrail ログ記録によって追跡される Amazon S3 バケットレベルのアクション”」を参照してください。

トピック

- メタデータテーブルを設定するためのアクセス許可の設定
- メタデータテーブル設定の作成

- メタデータテーブルへのアクセスの制御
- メタデータテーブル設定の削除
- メタデータテーブルの削除

メタデータテーブルを設定するためのアクセス許可の設定

メタデータテーブル設定を作成するには、メタデータテーブル設定の作成と管理、およびメタデータテーブルとメタデータテーブルが保存されているテーブルバケットの作成と管理の両方に必要な AWS Identity and Access Management (IAM) アクセス許可を持っている必要があります。

メタデータテーブル設定を作成および管理するには、次のアクセス許可が必要です。

- `s3:CreateBucketMetadataTableConfiguration` – このアクセス許可により、汎用バケットのメタデータテーブル設定を作成できます。
- `s3:GetBucketMetadataTableConfiguration` – このアクセス許可により、メタデータテーブル設定に関する情報を取得できます。
- `s3:DeleteBucketMetadataTableConfiguration` – このアクセス許可により、メタデータテーブル設定を削除できます。

テーブルとテーブルバケットを作成して操作するには、特定の `s3tables` アクセス許可が必要です。メタデータテーブル設定を作成するには、少なくとも次の `s3tables` アクセス許可が必要です。

- `s3tables:CreateNamespace` – このアクセス許可により、テーブルバケットに名前空間を作成できます。メタデータテーブルはデフォルトの `aws_s3_metadata` 名前空間を使用します。
- `s3tables:GetTable` – このアクセス許可により、メタデータテーブルに関する情報を取得できます。
- `s3tables:CreateTable` – このアクセス許可により、メタデータテーブルを作成できます。
- `s3tables:PutTablePolicy` – このアクセス許可により、メタデータテーブルポリシーを追加または更新できます。

すべてのテーブルとテーブルバケットのアクセス許可の詳細については、「Access management for S3 Tables」を参照してください。

Important

- メタデータテーブルをクエリできるようにテーブルバケットを AWS 分析サービスと統合する場合は、追加のアクセス許可が必要です。詳細については、「Integrating Amazon S3 Tables with AWS analytics services」を参照してください。
- テーブルバケットで AWS Key Management Service (AWS KMS) キーによるサーバー側の暗号化 (SSE-KMS) を使用している場合は、アクセス許可として `kms:GenerateDataKey` および `kms:Decrypt` も必要です。さらに、`metadata.s3.amazonaws.com` および `maintenance.s3tables.amazonaws.com` サービスプリンシパルが KMS キーにアクセスするためのアクセス許可を付与する必要があります。詳細については、「S3 メタデータサービスプリンシパルに KMS キーを使用するアクセス許可を付与する」を参照してください。

メタデータテーブルとテーブルバケットを作成して操作するには、次のポリシー例を使用できます。このポリシーでは、メタデータテーブル設定を適用する汎用バケットを *amzn-s3-demo-source-bucket* と呼びます。メタデータテーブルを保存するテーブルバケットは、*amzn-s3-demo-bucket* と呼ばれます。このポリシーを使用するには、これらのバケット名と *user input placeholders* をユーザー自身の情報に置き換えます。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"PermissionsToWorkWithMetadataTables",
         "Effect":"Allow",
         "Action":[
            "s3:CreateBucketMetadataTableConfiguration",
            "s3:GetBucketMetadataTableConfiguration",
            "s3:DeleteBucketMetadataTableConfiguration",
            "s3tables:*"
         ],
         "Resource":[
            "arn:aws:s3:::bucket/amzn-s3-demo-source-bucket",
            "arn:aws:s3tables:region:account_id:bucket/amzn-s3-demo-bucket",
            "arn:aws:s3tables:region:account_id:bucket/amzn-s3-demo-bucket/table/*"
         ]
      }
   ]
```

```
}
```

メタデータテーブル設定の作成

Amazon S3 メタデータを生成してフルマネージド Apache Iceberg メタデータテーブルに保存するには、汎用バケットのメタデータテーブル設定を作成します。Amazon S3 は、バケットで設定がアクティブである限り、メタデータテーブルを継続的に更新してデータへの最新の変更を反映するように設計されています。さらに、Amazon S3 はメタデータテーブルを継続的に最適化して、ストレージコストを削減し、分析クエリのパフォーマンスを向上させます。

メタデータテーブルの Amazon リソースネーム (ARN) 形式は次のようになります。

`arn:aws:s3tables:`*`region-code`*`:`*`account-id`*`:bucket/`*`table-bucket-name`*`/table/`*`metadata_table_name`*

Amazon S3 フルマネージドメタデータテーブルは、テーブルバケットの `aws_s3_metadata` 名前空間に保存されます。テーブルバケットの名前空間の詳細については、「Table namespaces」を参照してください。

メタデータテーブル設定は、Amazon S3 コンソール、AWS Command Line Interface (AWS CLI)、AWS SDK、または Amazon S3 REST API を使用して作成できます。

前提条件

メタデータテーブル設定を作成するには、まず以下を実行する必要があります。

- メタデータテーブルを作成および管理するために必要な AWS Identity and Access Management (IAM) アクセス許可があることを確認してください。詳細については、「the section called “メタデータテーブルのアクセス許可”」を参照してください。
- メタデータテーブルを保存する S3 テーブルバケットを作成します。このテーブルバケットは、汎用バケットと同じ AWS リージョンおよび AWS アカウントにある必要があります。テーブルバケットの作成の詳細については、「Creating table buckets」を参照してください。Amazon S3 コンソールを使用して設定を作成する場合は、そのプロセスの一環としてこのステップを実行できます。
- テーブルバケットを AWS Glue Data Catalog と統合して、Amazon Athena、Amazon EMR、Amazon Redshift、Apache Spark、Apache Trino、および Apache Iceberg 形式をサポートする他のアプリケーションなどのクエリエンジンでメタデータテーブルを直接クエリできるようにします。詳細については、「the section called “AWS 分析サービスを使用したメタデータテーブルのクエリ”」を参照してください。

メタデータテーブル設定を作成する

S3 コンソールの使用

メタデータテーブル設定を作成するには

メタデータテーブル設定を作成する前に、必ず前提条件を確認して満たし、the section called “制限と制約” を確認してください。

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[汎用バケット] を選択します。
3. メタデータテーブル設定を作成する汎用バケットを選択します。

   > **Note**
   >
   > この汎用バケットが、テーブルバケットが使用可能な AWS リージョンであることを確認します。テーブルバケットは、米国東部 (バージニア北部)、米国東部 (オハイオ)、および米国西部 (オレゴン) リージョンでのみ使用できます。

4. バケットの詳細ページで、[メタデータ] タブを選択します。
5. [メタデータ] タブで、[メタデータ設定を作成] を選択します。
6. [メタデータ設定を作成] ページの [送信先テーブルバケット] で、メタデータテーブルを保存するテーブルバケットを指定します。テーブルバケットは、汎用バケットと同じ AWS アカウントおよび AWS リージョンにある必要があります。

   テーブルバケットがまだない場合は、[テーブルバケットを作成] を選択します。テーブルバケット名は 3～63 文字で、選択した AWS リージョンの AWS アカウント内で一意である必要があります。有効な文字は、a～z、0～9、ハイフン (-) です。テーブルバケットの作成の詳細については、「Creating table buckets」を参照してください。

   テーブルバケットを作成するときは、必ず AWS Glue Data Catalog と統合してください。詳細については、「the section called “AWS 分析サービスを使用したメタデータテーブルのクエリ”」を参照してください。
7. [メタデータテーブル名] には、テーブルに使用する名前を指定します。メタデータテーブル名は 1～255 文字で、テーブルバケットの `aws_s3_metadata` 名前空間内で一意である必要があります。有効な文字は、小文字、数字、アンダースコア (_) です。
8. [メタデータテーブル設定を作成] を選択します。

メタデータテーブルの設定が成功すると、メタデータテーブルの ARN が、指定されたテーブルバケットとメタデータテーブル名とともに [メタデータ] タブに表示されます。

メタデータテーブル設定の更新をモニタリングするには、AWS CloudTrail を使用できます。詳細については、「the section called “CloudTrail 口グ記録によって追跡される Amazon S3 バケットレベルのアクション”」を参照してください。

AWS CLI の使用

次のコマンドを実行するには、AWS CLI をインストールして設定する必要があります。AWS CLI をまだインストールしていない場合は、「AWS Command Line Interface ユーザーガイド」の「AWS CLI の最新バージョンのインストールまたは更新」を参照してください。

別の方法として、AWS CloudShell を使用してコンソールから AWS CLI コマンドを実行することもできます。AWS CloudShell は、AWS Management Consoleから直接起動できる、ブラウザベースの事前認証済みシェルです。詳細については、「AWS CloudShell ユーザーガイド」の「CloudShell とは」と「AWS CloudShell の使用開始」を参照してください。

AWS CLI を使用してメタデータテーブル設定を作成するには

メタデータテーブル設定を作成する前に、必ず前提条件を確認して満たし、the section called “制限と制約” を確認してください。

次のコマンド例を使用する際は、*user input placeholders* をユーザー自身の情報に置き換えます。

1. テーブルバケットがまだない場合は、次のコマンドを使用して、メタデータテーブルを保存するテーブルバケットを作成します。テーブルバケットが、メタデータテーブル設定を作成する汎用バケットと同じ AWS リージョンにあることを確認します。

```
aws s3tables create-table-bucket --name amzn-s3-demo-bucket --region us-east-2
```

2. 次のコマンドを使用して、テーブルバケットが作成されたことを確認します。

```
aws s3tables list-table-buckets --region us-east-2
```

3. メタデータテーブル設定を含む JSON ファイルを作成し、保存します (例: `metadata-config.json`)。以下は、設定例です。

テーブルバケット名は 3～63 文字で、選択した AWS リージョンの AWS アカウント内で一意である必要があります。有効な文字は、a～z、0～9、ハイフン (-) です。テーブルバケットの作成の詳細については、「Creating table buckets」を参照してください。

メタデータテーブル名は 1～255 文字で、テーブルバケットの aws_s3_metadata 名前空間内で一意である必要があります。有効な文字は、小文字、数字、アンダースコア (_) です。

```
{
  "S3TablesDestination": {
    "TableBucketArn": "arn:aws:s3tables:us-east-2:111122223333:bucket/amzn-s3-demo-bucket",
    "TableName": "test_metadata_table"
  }
}
```

4. 次のコマンドを使用して、メタデータテーブル設定を汎用バケット (例: *amzn-s3-demo-source-bucket*) に適用します。

```
aws s3api create-bucket-metadata-table-configuration \
--bucket amzn-s3-demo-source-bucket \
--metadata-table-configuration  file://./metadata-config.json \
--region us-east-2
```

5. 設定が作成されたことを確認するには、次のコマンドを使用します。

```
aws s3api get-bucket-metadata-table-configuration \
--bucket amzn-s3-demo-source-bucket \
--region us-east-2
```

メタデータテーブル設定の更新をモニタリングするには、AWS CloudTrail を使用できます。詳細については、「the section called “CloudTrail 口グ記録によって追跡される Amazon S3 バケットレベルのアクション”」を参照してください。

REST API の使用

REST リクエストを送信して、メタデータテーブル設定を作成できます。詳細については、「Amazon S3 API リファレンス」の「CreateBucketMetadataTableConfiguration」を参照してください。

AWS SDK の使用

AWS SDK を使用して、Amazon S3 でメタデータテーブル設定を作成できます。詳細については、「Amazon S3 API Reference」にある「サポートされる SDK のリスト」を参照してください。

メタデータテーブルへのアクセスの制御

Amazon S3 メタデータテーブルへのアクセスを制御するには、テーブルバケットとメタデータテーブルにアタッチされている AWS Identity and Access Management (IAM) リソースベースのポリシーを使用できます。つまり、テーブルバケットレベルとテーブルレベルの両方でメタデータテーブルへのアクセスを制御できます。

テーブルバケットとテーブルへのアクセスの制御の詳細については、「Access management for S3 Tables」を参照してください。

> **Important**
>
> Amazon S3 によるテーブルバケットまたはメタデータテーブルへの書き込みが制限されていないことを確認してください。Amazon S3 がテーブルバケットまたはメタデータテーブルに書き込めない場合は、メタデータテーブル設定を削除してから新しい設定を作成し、新しいメタデータテーブルを作成する必要があります。

AWS Lake Formation を使用して、メタデータテーブルの行と列へのアクセスを制御することもできます。詳細については、「AWS Lake Formation Developer Guide」の「Managing Lake Formation permissions」と「Data filtering and cell-level security in Lake Formation」を参照してください。

メタデータテーブル設定の削除

Amazon S3 汎用バケットのメタデータテーブル設定の更新を停止する場合は、バケットにアタッチされているメタデータテーブル設定を削除できます。メタデータテーブル設定を削除すると、設定のみが削除されます。メタデータテーブル設定を削除しても、テーブルバケットとメタデータテーブルは引き続き存在します。ただし、メタデータテーブルは更新されなくなります。

メタデータテーブルを削除するには、「the section called “メタデータテーブルを削除する”」を参照してください。テーブルバケットを削除するには、「Amazon S3 API Reference」の「Deleting table buckets」および「DeleteTableBucket」を参照してください。

メタデータテーブル設定は、Amazon S3 コンソール、AWS Command Line Interface (AWS CLI)、AWS SDK、または Amazon S3 REST API を使用して削除できます。

メタデータテーブル設定を削除する

S3 コンソールの使用

メタデータテーブル設定を削除するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[汎用バケット] を選択します。
3. メタデータテーブル設定を削除する汎用バケットを選択します。
4. バケットの詳細ページで、[メタデータ] タブを選択します。
5. [メタデータ] タブで、[削除] を選択します。
6. [メタデータ設定を削除] ダイアログボックスで、「**confirm**」と入力して、設定を削除することを確認します。その後、[削除] をクリックします。

AWS CLI を使用する場合

次のコマンドを実行するには、AWS CLI をインストールして設定する必要があります。AWS CLI をまだインストールしていない場合は、「AWS Command Line Interface ユーザーガイド」の「AWS CLI の最新バージョンのインストールまたは更新」を参照してください。

別の方法として、AWS CloudShell を使用してコンソールから AWS CLI コマンドを実行することもできます。AWS CloudShell は、AWS Management Consoleから直接起動できる、ブラウザベースの事前認証済みシェルです。詳細については、「AWS CloudShell ユーザーガイド」の「CloudShell とは」と「AWS CloudShell の使用開始」を参照してください。

AWS CLI を使用してメタデータテーブル設定を削除するには

次のコマンド例を使用する際は、*user input placeholders* をユーザー自身の情報に置き換えます。

1. 次のコマンドを使用して、メタデータテーブル設定を汎用バケット (例: *amzn-s3-demo-source-bucket*) から削除します。

```
aws s3api delete-bucket-metadata-table-configuration \
--bucket amzn-s3-demo-source-bucket \
--region us-east-2
```

2. 設定が削除されたことを確認するには、次のコマンドを使用します。

```
aws s3api get-bucket-metadata-table-configuration \
--bucket amzn-s3-demo-source-bucket \
--region us-east-2
```

REST API の使用

REST リクエストを送信して、メタデータテーブル設定を削除できます。詳細については、「DeleteBucketMetadataTableConfiguration」を参照してください。

AWS SDK の使用

AWS SDK を使用して、Amazon S3 でメタデータテーブル設定を削除できます。詳細については、「サポートされる SDK のリスト」を参照してください。

メタデータテーブルの削除

Amazon S3 汎用バケット用に作成したメタデータテーブルを削除する場合は、テーブルバケットからメタデータテーブルを削除できます。

> **Note**
>
> メタデータテーブルを削除する前に、まず汎用バケット上の関連するメタデータテーブル設定を削除することをお勧めします。詳細については、「the section called “メタデータテーブル設定の削除”」を参照してください。

テーブルバケットを削除するには、「Amazon S3 API Reference」の「Deleting table buckets」および「DeleteTableBucket」を参照してください。

メタデータテーブルは、AWS Command Line Interface (AWS CLI)、AWS SDK、または Amazon S3 REST API を使用して削除できます。

メタデータテーブルを削除する

AWS CLI を使用する場合

次のコマンドを実行するには、AWS CLI をインストールして設定する必要があります。AWS CLI をまだインストールしていない場合は、「AWS Command Line Interface ユーザーガイド」の「AWS CLI の最新バージョンのインストールまたは更新」を参照してください。

別の方法として、AWS CloudShell を使用してコンソールから AWS CLI コマンドを実行することもできます。AWS CloudShell は、AWS Management Consoleから直接起動できる、ブラウザベースの事前認証済みシェルです。詳細については、「AWS CloudShell ユーザーガイド」の「CloudShell とは」と「AWS CloudShell の使用開始」を参照してください。

AWS CLI を使用してメタデータテーブル設定を削除するには

次のコマンド例を使用する際は、*user input placeholders* をユーザー自身の情報に置き換えます。

1. 次のコマンドを使用して、メタデータテーブルをテーブルバケット (例: *amzn-s3-demo-bucket*) から削除します。

```
aws s3tables delete-table \
--table-bucket-arn arn:aws:s3tables:us-east-2:111122223333:bucket/amzn-s3-demo-bucket \
--namespace aws_s3_metadata \
--name test_metadata_table \
--region us-east-2
```

2. テーブルが削除されたことを確認するには、次のコマンドを使用します。

```
aws s3tables get-table \
--table-bucket-arn arn:aws:s3tables:us-east-2:111122223333:bucket/amzn-s3-demo-bucket \
--namespace aws_s3_metadata \
--name test_metadata_table \
--region us-east-2
```

REST API の使用

REST リクエストを送信して、メタデータテーブル設定を削除できます。詳細については、「Amazon S3 API リファレンス」の「DeleteTable」を参照してください。

AWS SDK の使用

AWS SDK を使用して、Amazon S3 でメタデータテーブル設定を削除できます。詳細については、「Amazon S3 API Reference」にある「サポートされる SDK のリスト」を参照してください。

メタデータテーブルのクエリ

Amazon S3 メタデータを使用すると、Apache Iceberg 形式をサポートする任意のクエリエンジンを使用して S3 マネージドメタデータテーブルを分析できます。S3 テーブルバケットを AWS 分析サービスと統合すると、Amazon Athena、Amazon Redshift などのサービスを使用して、メタデータテーブルで次のことを行えます。

- ストレージの使用パターンと傾向を確認する
- オブジェクト全体の AWS Key Management Service (AWS KMS) 暗号化キーの使用状況を監査する
- ユーザー定義メタデータとオブジェクトタグでオブジェクトを検索する
- オブジェクトメタデータの経時的な変化を理解する
- リクエストを行った AWS アカウント ID や IP アドレスなど、オブジェクトがいつ更新または削除されたかを知る

テーブルバケットが AWS 分析サービスと統合された後、メタデータテーブルに対してクエリを実行できます。これには、S3 マネージドメタデータテーブルとカスタムメタデータテーブルの結合が含まれます。メタデータテーブルが同じテーブルバケットに保存されている限り、複数のデータセット間でクエリを実行できます。

そこから、Amazon QuickSight を使用して、クエリデータでインタラクティブなダッシュボードを作成できます。

クエリ料金に関する考慮事項

メタデータテーブルでクエリを実行する場合は、追加料金が適用されます。詳細については、使用しているクエリエンジンの料金情報を参照してください。

クエリのコスト効率を高める方法については、「メタデータテーブルのクエリパフォーマンスの最適化」を参照してください。

トピック

- AWS 分析サービスを使用したメタデータテーブルのクエリ
- オープンソースのクエリエンジンを使用したメタデータテーブルのクエリ
- メタデータテーブルのクエリパフォーマンスの最適化
- メタデータテーブルクエリの例
- カスタムメタデータと S3 メタデータテーブルの結合

- Amazon QuickSight を使用したメタデータテーブルデータの視覚化

AWS 分析サービスを使用したメタデータテーブルのクエリ

Amazon Athena、Amazon Redshift、Amazon EMR などの AWS 分析サービスを使用して、S3 マネージドメタデータテーブルをクエリできます。

クエリを実行する前に、まず AWS アカウント およびリージョンの S3 テーブルバケットを AWS 分析サービスと統合する必要があります。

Amazon Athena を使用したメタデータテーブルのクエリ

AWS 分析サービスと S3 テーブルバケットを統合したら、Athena でメタデータテーブルのクエリを開始できます。クエリで、カタログを `s3tablescatalog` に、データベースを `aws_s3_metadata` (メタデータテーブルの名前空間) に指定します。詳細については、「Querying Amazon S3 tables with Athena」を参照してください。

Amazon Redshift を使用したメタデータテーブルのクエリ

AWS 分析サービスと S3 テーブルバケットを統合したら、メタデータテーブル名前空間 (`aws_s3_metadata`) へのリソースリンクを作成します。これが完了すると、Amazon Redshift コンソールでメタデータテーブルのクエリを開始できます。詳細については、「Accessing Amazon S3 tables with Amazon Redshift」を参照してください。

Amazon EMR を使用したメタデータテーブルのクエリ

Amazon EMR を使用してメタデータテーブルをクエリするには、Apache Iceberg 用に設定された Amazon EMR クラスターを作成し、Apache Spark を使用してメタデータテーブルに接続します。これを設定するには、S3 テーブルバケットを AWS 分析サービスと統合するか、オープンソースの Iceberg クライアントカタログ用 Amazon S3 Tables Catalog を使用します。

詳細については、「Accessing Amazon S3 tables with Amazon EMR」を参照してください。

オープンソースのクエリエンジンを使用したメタデータテーブルのクエリ

Apache Spark などのオープンソースのクエリエンジンを使用して、S3 マネージドメタデータテーブルをクエリできます。メタデータテーブルをクエリするには、Apache Iceberg クライアントカタログ用 Amazon S3 Tables Catalog (AWS Labs がホストするオープンソースライブラリ) が必要です。

詳細については、「Querying Amazon S3 tables with Apache Spark」を参照してください。

メタデータテーブルのクエリパフォーマンスの最適化

S3 メタデータは Apache Iceberg テーブル形式に基づいているため、特定の時間範囲を使用することで、メタデータテーブルクエリのパフォーマンスとコストを最適化できます。

例えば、次の SQL クエリは、S3 汎用バケット内の新しいオブジェクトの機密レベルを提供します。

```
SELECT key, object_tags['SensitivityLevel']
FROM aws_s3_metadata.my_metadata_table
WHERE record_type = 'CREATE'
GROUP BY object_tags['SensitivityLevel']
```

このクエリはメタデータテーブル全体をスキャンするため、実行に時間がかかる場合があります。パフォーマンスを向上させるには、特定の時間範囲に焦点を絞る `record_timestamp` 列を含めることができます。以下は、過去 1 か月の新しいオブジェクトを調べる、以前のクエリが更新されたバージョンです。

```
SELECT key, object_tags['SensitivityLevel']
FROM aws_s3_metadata.my_metadata_table
WHERE record_type = 'CREATE'
AND record_timestamp > (CURRENT_TIMESTAMP - interval '1' month)
GROUP BY object_tags['SensitivityLevel']
```

メタデータテーブルクエリの例

次の例は、標準 SQL クエリを使用して S3 メタデータテーブルからさまざまなタイプの情報を取得する方法を示しています。

これらの例を使用する際は、次の点に注意してください。

- 例は、Amazon Athena で動作するように記述されています。別のクエリエンジンで動作するためには、例を変更する必要がある場合があります。
- クエリを最適化する方法を理解していることを確認してください。
- *amzn-s3-demo-bucket* を、メタデータテーブルを保存する S3 テーブルバケットの名前に置き換えます。
- *my_metadata_table* を、クエリするメタデータテーブルの名前に置き換えます。
- サポートされている列の完全なリストについては、「S3 メタデータテーブルスキーマ」を参照してください。

ファイル拡張子によるオブジェクトの検索

次のクエリは、特定のファイル拡張子 (この場合は .jpg) を持つオブジェクトを返します。

```
SELECT key FROM "s3tablescatalog/amzn-s3-demo-
bucket"."aws_s3_metadata"."my_metadata_table"
WHERE key LIKE '%.jpg'
AND record_type = 'CREATE'
```

オブジェクトの削除の一覧表示

次のクエリは、リクエストを行った AWS アカウント ID または AWS サービスプリンシパルを含むオブジェクト削除イベントを返します。

```
SELECT DISTINCT bucket, key, sequence_number, record_type, record_timestamp, requester,
 source_ip_address, version_id
FROM "s3tablescatalog/amzn-s3-demo-bucket"."aws_s3_metadata"."my_metadata_table"
WHERE record_type = 'DELETE';
```

オブジェクトで使用される AWS KMS 暗号化キーの一覧表示

次のクエリは、オブジェクトを暗号化する AWS Key Management Service (AWS KMS) キーの ARN を返します。

```
SELECT DISTINCT kms_key_arn
FROM "s3tablescatalog/amzn-s3-demo-bucket"."aws_s3_metadata"."my_metadata_table";
```

KMS キーを使用しないオブジェクトの一覧表示

次のクエリは、AWS KMS キーで暗号化されていないオブジェクトを返します。

```
SELECT DISTINCT kms_key_arn
FROM "s3tablescatalog/amzn-s3-demo-bucket"."aws_s3_metadata"."my_metadata_table"
WHERE encryption_status NOT IN ('SSE-KMS', 'DSSE-KMS')
AND record_type = 'CREATE';
```

Amazon Bedrock が提供するメタデータの表示

一部の AWS サービス (Amazon Bedrock など) は、Amazon S3 にオブジェクトをアップロードします。これらのサービスによって提供されるオブジェクトメタデータをクエリできます。例えば、次の

クエリには、Amazon Bedrock によって汎用バケットにアップロードされたオブジェクトがあるかどうかを判断する user_metadata 列が含まれています。

```
SELECT DISTINCT bucket, key, sequence_number, record_type, record_timestamp,
 user_metadata
FROM "s3tablescatalog/amzn-s3-demo-bucket"."aws_s3_metadata"."my_metadata_table"
WHERE record_type = 'CREATE'
AND user_metadata['content-source'] = 'AmazonBedrock';
```

Amazon Bedrock がバケットにオブジェクトをアップロードした場合、user_metadata 列には、クエリ結果のオブジェクトに関連付けられた次のメタデータが表示されます。

```
user_metadata
{content-additional-params -> requestid="CVK8FWYRW0M9JW65",
 signedContentSHA384="38b060a751ac96384cd9327eb1b1e36a21fdb71114be07434c0cc7bf63f6e1da274edebfe
 content-model-id -> bedrock-model-arn, content-source -> AmazonBedrock}
```

オブジェクトの現状の把握

次のクエリは、オブジェクトの現在の状態を判断するのに役立ちます。クエリは、各オブジェクトの最新バージョンを識別し、削除されたオブジェクトを除外し、シーケンス番号に基づいて各オブジェクトの最新バージョンをマークします。結果は、bucket、key、および sequence_number 列で順序付けられます。

```
WITH records_of_interest as (
   -- Start with a query that can narrow down the records of interest.
    SELECT * from "s3tablescatalog/amzn-s3-demo-
bucket"."aws_s3_metadata"."my_metadata_table"
),

version_stacks as (
   SELECT *,
          -- Introduce a column called 'next_sequence_number', which is the next larger
          -- sequence_number for the same key version_id in sorted order.
          LEAD(sequence_number, 1) over (partition by (bucket, key,
 coalesce(version_id, '')) order by sequence_number ASC) as next_sequence_number
   from records_of_interest
),

-- Pick the 'tip' of each version stack triple: (bucket, key, version_id).
-- The tip of the version stack is the row of that triple with the largest sequencer.
```

```
-- Selecting only the tip filters out any row duplicates.
-- This isn't typical, but some events can be delivered more than once to the table
-- and include rows that might no longer exist in the bucket (since the
-- table contains rows for both extant and extinct objects).
-- In the next subquery, eliminate the rows that contain deleted objects.
current_versions as (
    SELECT * from version_stacks where next_sequence_number is NULL
),

-- Eliminate the rows that are extinct from the bucket by filtering with
-- record_type. An object version has been deleted from the bucket if its tip is
-- record_type==DELETE.
existing_current_versions as (
    SELECT * from current_versions where not (record_type = 'DELETE' and
 is_delete_marker = FALSE)
),

-- Optionally, to determine which of several object versions is the 'latest',
-- you can compare their sequence numbers. A version_id is the latest if its
-- tip's sequencer is the largest among all other tips in the same key.
with_is_latest as (
    SELECT *,
           -- Determine if the sequence_number of this row is the same as the largest
 sequencer for the key that still exists.
           sequence_number = (MAX(sequence_number) over (partition by (bucket, key)))
 as is_latest_version
    FROM existing_current_versions
)

SELECT * from with_is_latest
ORDER BY bucket, key, sequence_number;
```

カスタムメタデータと S3 メタデータテーブルの結合

S3 マネージドメタデータテーブルとカスタマー (セルフマネージド) メタデータテーブル全体のデータを分析できます。標準の SQL JOIN 演算子を使用すると、これらの複数のソースからのデータをクエリできます。

次の SQL クエリの例は、S3 マネージドメタデータテーブル (*my_s3_metadata_table*) とセルフマネージドメタデータテーブル (*my_self_managed_metadata_table*) の間で一致するレコードを検索します。また、クエリは、新しいオブジェクト (またはオブジェクトの新しいバージョン) がバケットに書き込まれたことを示す CREATE イベントに基づいて情報をフィルタリングします。(詳細については、S3 メタデータテーブルスキーマ を参照してください。)

```
SELECT *
FROM aws_s3_metadata.my_s3_metadata_table a
JOIN my_namespace.my_self_managed_metadata_table b
ON a.bucket = b.bucket AND a.key = b.key AND a.version_id = b.version_id
WHERE a.record_type = 'CREATE';
```

Amazon QuickSight を使用したメタデータテーブルデータの視覚化

Amazon QuickSight を使用すると、インタラクティブなダッシュボードを作成して、S3 マネージドメタデータテーブルに関する SQL クエリ結果を分析および視覚化できます。QuickSight ダッシュボードは、統計のモニタリング、変更の追跡、メタデータテーブルに関する運用上のインサイトの取得に役立ちます。

メタデータテーブルに関するダッシュボードには、以下が表示される場合があります。

- 異なるストレージクラスにあるオブジェクトの数
- ストレージデータのうち、大きいオブジェクトと比較した小さいオブジェクトの比率
- バケット内に存在するオブジェクトのタイプ
- オブジェクトのうち、削除数と比較したアップロード数の比率

AWS 分析サービスと S3 テーブルバケットを統合したら、メタデータテーブルからデータセットを作成し、SPICE またはクエリエンジンからの直接 SQL クエリを使用して Amazon QuickSight で操作できるようになります。QuickSight は、データソースとして Amazon Athena と Amazon Redshift をサポートしています。

詳細については、「Visualizing table data with Amazon QuickSight」を参照してください。

オブジェクトのアップロード

Amazon S3 にファイルをアップロードすると、S3 オブジェクトとして保存されます。オブジェクトは、オブジェクトを記述するファイルデータとメタデータから構成されます。バケット内のオブジェクトの数に制限はありません。Amazon S3 バケットにファイルをアップロードするには、バケットに対する書き込みアクセス許可が必要です。アクセス許可の詳細については、Amazon S3 用 Identity and Access Management を参照してください。

ファイルタイプ (イメージ、バックアップ、データ、ムービーなど) を問わず、各種のファイルを S3 バケットにアップロードできます。Amazon S3 コンソールを使用すると、アップロードできるファ

イルの最大サイズが 160 GB になります。160 GB を超えるファイルをアップロードするには、AWS Command Line Interface (AWS CLI)、AWS SDK、または Amazon S3 REST API を使用します。

バージョニングが有効なバケットに既に存在するキー名の付いたオブジェクトをアップロードした場合、Amazon S3 は既存のオブジェクトを置き換える代わりにオブジェクトの別バージョンを作成します。バージョニングを有効にする方法の詳細については、「バケットでのバージョニングの有効化」を参照してください。

アップロードするデータのサイズに応じて、Amazon S3 には以下のオプションが用意されています。

- AWS SDK、REST API、または AWS CLI を使用して 1 回のオペレーションでオブジェクトをアップロードする — 1 回の PUT オペレーションでは、最大 5 GB の単一のオブジェクトをアップロードできます。
- Amazon S3 コンソールを使用して 1 つのオブジェクトをアップロードする — Amazon S3 コンソールでは、最大 160 GB のオブジェクトをアップロードできます。
- AWS SDK、REST API、または AWS CLI を使用してオブジェクトをいくつかに分けてアップロードする — マルチパートアップロード API を使用すると、最大 5 TB のサイズの単一の大容量オブジェクトをアップロードできます。

  マルチパートアップロード API オペレーションは大容量オブジェクトのアップロードを効率よく行えるように設計されています。1 つのオブジェクトをいくつかに分けてアップロードできます。オブジェクトのパートは、単独で、任意の順序で、または並行してアップロードできます。マルチパートアップロードは 5 MB ~ 5 TB のオブジェクトで使用できます。詳細については、「Amazon S3 でのマルチパートアップロードを使用したオブジェクトのアップロードとコピー」を参照してください。

オブジェクトをアップロードすると、そのオブジェクトは、デフォルトでは Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3) を使用して自動的に暗号化されます。ダウンロードすると、オブジェクトは復号化されます。詳細については、「Amazon S3 バケット向けのサーバー側のデフォルトの暗号化動作の設定」および「暗号化によるデータの保護」を参照してください。

オブジェクトをアップロードするときに、別の種類のデフォルト暗号化を使用する場合は、S3 PUT リクエストで AWS Key Management Service (AWS KMS) キーによるサーバー側の暗号化 (SSE-KMS) を指定するか、SSE-KMS を使用してデータを暗号化するように送信先バケットのデフォルトの暗号化設定を設定することもできます。SSE-KMS に関する詳細は、「AWS KMS (SSE-KMS) によるサーバー側の暗号化の指定」を参照してください。別のアカウントが所有している KMS キーを使用する場合は、そのキーを使用するアクセス許可が必要です。KMS キーのクロスアカウント権限

の詳細については、「AWS Key Management Service デベロッパーガイド」の「他のアカウントで使用できる KMS キーを作成する」を参照してください。

Amazon S3 でアクセス拒否 (403 Forbidden) エラーが発生したとき、一般的な原因の詳細については「Amazon S3 でのアクセス拒否 (403 Forbidden) エラーのトラブルシューティング 」を参照してください。

オブジェクトのアップロード

S3 コンソールの使用

この手順では、コンソールを使用してオブジェクトおよびフォルダを Amazon S3 バケットにアップロードする方法について説明します。

オブジェクトをアップロードする場合、オブジェクトキー名はファイル名および任意のプレフィックスになります。Amazon S3 コンソールでは、フォルダを作成してオブジェクトを整理できます。Amazon S3 では、フォルダはオブジェクトキー名に表示されるプレフィックスとして表されます。Amazon S3 コンソールのフォルダに個々のオブジェクトをアップロードする場合、フォルダ名はオブジェクトキー名に含まれます。

例えば、「sample1.jpg」という名前のオブジェクトを「backup」という名前のフォルダにアップロードすると、キー名は「backup/sample1.jpg」になります。ただし、オブジェクトはコンソールの sample1.jpg フォルダ内で backup として表示されます。有効なキー名の詳細については、オブジェクトメタデータの使用 を参照してください。

> **Note**
>
> Amazon S3 コンソールでオブジェクトの名前を変更したり、ストレージクラス、暗号化、またはメタデータなどのプロパティを変更したりすると、新しいオブジェクトが作成され、古いオブジェクトが置き換えられます。S3 バージョニングが有効になっている場合は、オブジェクトの新しいバージョンが作成され、既存のオブジェクトが古いバージョンになります。また、プロパティを変更するロールは、新しいオブジェクト (またはオブジェクトのバージョン) の所有者になります。

フォルダをアップロードすると、Amazon S3 は、そのフォルダからすべてのファイルとサブフォルダをバケットにアップロードします。その後、アップロードしたファイルの名前とフォルダの名前を組み合わせたオブジェクトキー名が割り当てられます。例えば、/images と sample1.jpg の 2 つのファイルを含む sample2.jpg というフォルダをアップロードすると、Amazon S3 はファイ

ルのアップロード後に、対応するキー名である images/sample1.jpg と images/sample2.jpg を割り当てます。キー名にはプレフィックスとしてフォルダ名が含まれています。Amazon S3 コンソールには、最後の / に続くキー名の部分のみが表示されます。例えば、images フォルダ内では images/sample1.jpg オブジェクトと images/sample2.jpg オブジェクトが sample1.jpg および sample2.jpg として表示されます。

フォルダとファイルを S3 バケットにアップロードするには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。
3. [Buckets (バケット)] リストで、フォルダやファイルのアップロード先のバケットの名前を選択します。
4. [Upload (アップロード)] を選択します。
5. [Upload] (アップロード) ウィンドウで、次のいずれかの操作を行います。
   - ファイルとフォルダを [Upload] (アップロード) ウィンドウにドラッグアンドドロップします。
   - [ファイルの追加] または [フォルダの追加] を選択し、アップロードするファイルまたはフォルダを選択して [開く] を選択します。
6. バージョニングを有効にするには、[Destination] (送信先) で [Enable Bucket Versioning] (バケットバージョニングを有効化) を選択します。
7. 追加のアップロードオプションを設定せずにリストされたファイルとフォルダをアップロードするには、ページの下部で [Upload] (アップロード) を選択します。

   Amazon S3 はオブジェクトとフォルダをアップロードします。アップロードが完了すると、[アップロード: ステータス] ページに成功のメッセージが表示されます。

追加のオブジェクトプロパティを設定するには

1. アクセスコントロールリストの許可を変更するには、[Permissions] (許可) を選択します。
2. [Access control list (ACL)] (アクセスコントロールリスト (ACL) で、許可を編集します。

   オブジェクトのアクセス許可については、S3 コンソールを使用した、オブジェクトの ACL アクセス権限の設定 を参照してください。アップロードするすべてのファイルについて、オブジェクトの読み取りアクセスをパブリック (世界中のすべてのユーザー) に付与できます。ただし、パブリック読み取りアクセスのデフォルト設定を変更しないことをお勧めします。パブリック読

み取りアクセス権限の付与は、バケットがウェブサイトなどに使用されるなど、ユースケースの小さいサブセットに適用されます。オブジェクトをアップロードした後で、オブジェクトの許可をいつでも変更できます。

3. その他の追加プロパティを設定するには、[Properties] (プロパティ) を選択します。
4. [ストレージクラス] で、アップロードするファイルのストレージクラスを選択します。

   ストレージクラスの詳細については、Amazon S3 ストレージクラスの理解と管理 を参照してください。
5. オブジェクトの暗号化設定を更新するには、[Server-side encryption settings] (サーバー側の暗号化設定) で、次の操作を行います。

   a. [Specify an encryption key] (暗号化キーを指定する) を選択します。

   b. [暗号化設定] で、[デフォルトの暗号化にバケット設定を使用する] または [デフォルトの暗号化にバケット設定を上書きする] を選択します。

   c. [デフォルトの暗号化にバケット設定を上書きする] を選択した場合は、次の暗号化設定を設定する必要があります。

      - Amazon S3 管理のキーを使用してアップロードされたファイルを暗号化するには、[Amazon S3 マネージドキー (SSE-S3)] を選択します。

        詳細については、「Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3)」を参照してください。
      - AWS Key Management Service (AWS KMS) に保存されているキーを使用してアップロード済みファイルを暗号化するには、AWS Key Management Service キー (SSE-KMS) を選択します。次に、AWS KMS キーについて、以下のいずれかのオプションを選択します。
        - 使用可能な KMS キーのリストから選択するには、[AWS KMS keys から選択する] を選択し、使用可能なキーのリストから自分の KMS キーを選択します。

          AWS マネージドキー (aws/s3) とカスタマーマネージドキーの両方がこのリストに表示されます。カスタマーマネージドキーの詳細については、AWS Key Management Serviceデベロッパーガイドの「カスタマーキーと AWS キー」を参照してください。
        - KMS キー ARN を入力するには、[AWS KMS key ARN を入力] を選択し、表示されるフィールドに KMS キー ARN を入力します。
        - AWS KMS コンソールで新しいカスタマーマネージドキーを作成するには、[KMS キーを作成] を選択します。

AWS KMS key の作成の詳細については、「AWS Key Management Service デベロッパーガイド」の「キーの作成」を参照してください。

> **Important**
>
> バケットと同じ AWS リージョン で使用可能な KMS キーのみを使用できます。Amazon S3 コンソールには、バケットと同じリージョンで最初の 100 個の KMS キーしか表示されません。リストに存在しない KMS キーを使用するには、KMS キー ARN を入力する必要があります。別のアカウントが所有している KMS キーを使用する場合は、まずそのキーを使用するアクセス許可が必要であり、次に KMS キー ARN を入力する必要があります。
> Amazon S3 では、対称暗号化 KMS キーのみがサポートされ、非対称暗号化 KMS キーはサポートされません。詳細については、AWS Key Management Service デベロッパーガイドの「Identifying symmetric and asymmetric KMS keys」(対称および非対称 KMS キーの識別) を参照してください。

6. 追加のチェックサムを使用するには、[On] (オン) を選択します。次に、[Checksum function] (チェックサム関数) で、使用する関数を選択します。Amazon S3 は、オブジェクト全体を受け取った後、チェックサム値を計算して保存します。[Precalculated value] (事前計算された値) ボックスを使用して、事前計算された値を指定できます。その場合、Amazon S3 は、指定した値と計算した値を比較します。2 つの値が一致しない場合、Amazon S3 はエラーを生成します。

   追加のチェックサムを使用すると、データの検証に使用するチェックサムアルゴリズムを指定できます。追加のチェックサムの詳細については、「Amazon S3 でのオブジェクトの整合性のチェック」を参照してください。

7. アップロードするすべてのオブジェクトにタグを追加するには、[Add tag (タグの追加)] を選択します。[キー] フィールドにタグ名を入力します。タグの値を入力します。

   オブジェクトのタグ付けにより、ストレージを分類する方法が提供されます。各タグはキーと値のペアです。キーとタグ値は大文字と小文字が区別されます。オブジェクトごとに最大 10 個のタグを持つことができます。タグキーには最大 128 個の Unicode 文字、タグ値には最大 255 個の Unicode 文字を使用できます。オブジェクトタグの詳細については、タグを使用してストレージを分類するを参照してください。

8. メタデータを追加するには、[Add metadata] (メタデータの追加) を選択します。

a. [Type] (タイプ) で、[System defined] (システム定義) または [User defined] (ユーザー定義) を選択します。

   システム定義のメタデータの場合は、Content-Type や Content-Disposition などの一般的な HTTP ヘッダーを選択できます。システム定義のメタデータのリストと値を追加できるかどうかについては、システムで定義されたオブジェクトメタデータ を参照してください。プレフィックス `x-amz-meta-` で始まるメタデータはすべてユーザー定義のメタデータとして扱われます。ユーザー定義メタデータはオブジェクトと共に保存され、オブジェクトのダウンロード時に返されます。キーと値の両方が US-ASCII 標準に従っている必要があります。ユーザー定義メタデータのサイズは最大 2 KB です。システム定義メタデータとユーザー定義メタデータの詳細については、オブジェクトメタデータの使用 を参照してください。

b. [Key] (キー) で、キーを選択します。

c. キーの値を入力します。

9. オブジェクトをアップロードするには、[Upload] (アップロード) を選択します。

   Amazon S3 はオブジェクトをアップロードします。アップロードが完了すると、[Upload: status] (アップロード: ステータス) ページに成功のメッセージが表示されます。

10. [終了] を選択します。

AWS CLI の使用

単一のオペレーションで、最大 5 GB のオブジェクトをアップロードする PUT リクエストを送信できます。詳細については、`PutObject`AWS CLI コマンドリファレンスでの例を参照してください。

REST API の使用

REST リクエストを送信してオブジェクトをアップロードできます。PUT リクエストを送信して 1 回のオペレーションでデータをアップロードできます。詳細については、「PutObject」を参照してください。

AWS SDK の使用

AWS SDK を使用して、Amazon S3 にオブジェクトをアップロードできます。SDK にはデータを容易にアップロードできるラッパーライブラリが用意されています。詳細については、サポートされている SDK のリスト を参照してください。

次に、いくつかの SDK を選択した例を数例挙げます。

.NET

次の C# コード例では、2 つの PutObjectRequest リクエストで 2 つのオブジェクトを作成します。

- 最初の PutObjectRequest リクエストでは、サンプルオブジェクトデータとしてテキスト文字列を保存します。また、バケット名とオブジェクトキー名を指定します。
- 2 番目の PutObjectRequest リクエストでは、ファイル名を指定してファイルをアップロードします。また、このリクエストは、ContentType ヘッダーとオプションのオブジェクトメタデータ (タイトル) を指定します。

コード例を設定および実行する方法の詳細については、「AWS SDK for .NET デベロッパーガイド」の「AWS SDK for .NET の開始方法」 を参照してください。

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class UploadObjectTest
    {
        private const string bucketName = "*** bucket name ***";
        // For simplicity the example creates two objects from the same file.
        // You specify key names for these objects.
        private const string keyName1 = "*** key name for first object created ***";
        private const string keyName2 = "*** key name for second object created
 ***";
        private const string filePath = @"*** file path ***";
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.EUWest1;

        private static IAmazonS3 client;

        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            WritingAnObjectAsync().Wait();
        }
```

```
        static async Task WritingAnObjectAsync()
        {
            try
            {
                // 1. Put object-specify only key name for the new object.
                var putRequest1 = new PutObjectRequest
                {
                    BucketName = bucketName,
                    Key = keyName1,
                    ContentBody = "sample text"
                };

                PutObjectResponse response1 = await
client.PutObjectAsync(putRequest1);

                // 2. Put the object-set ContentType and add metadata.
                var putRequest2 = new PutObjectRequest
                {
                    BucketName = bucketName,
                    Key = keyName2,
                    FilePath = filePath,
                    ContentType = "text/plain"
                };

                putRequest2.Metadata.Add("x-amz-meta-title", "someTitle");
                PutObjectResponse response2 = await
client.PutObjectAsync(putRequest2);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine(
                        "Error encountered ***. Message:'{0}' when writing an
object"
                        , e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine(
                    "Unknown encountered on server. Message:'{0}' when writing an
object"
                    , e.Message);
            }
        }
```

```
    }
}
```

Java

次の例では 2 つのオブジェクトを作成します。最初のオブジェクトにはデータとしてテキスト文字列があり、2 番目のオブジェクトはファイルです。この例では、AmazonS3Client.putObject() への呼び出しでバケット名、オブジェクトキー、およびテキストデータを直接指定して、最初のオブジェクトを作成します。例では、バケット名、オブジェクトキー、およびファイルパスを指定する PutObjectRequest を指定して 2 番目のオブジェクトを作成します。PutObjectRequest では、ContentType ヘッダーとタイトルメタデータも指定します。

作業サンプルの作成およびテストの手順については、「AWS SDK for Java のデベロッパーガイド」の「使用開始」を参照してください。

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.ObjectMetadata;
import com.amazonaws.services.s3.model.PutObjectRequest;

import java.io.File;
import java.io.IOException;

public class UploadObject {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String stringObjKeyName = "*** String object key name ***";
        String fileObjKeyName = "*** File object key name ***";
        String fileName = "*** Path to file to upload ***";

        try {
            // This code expects that you have AWS credentials set up per:
            // https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/setup-
credentials.html
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
```

```
                    .withRegion(clientRegion)
                    .build();

            // Upload a text string as a new object.
            s3Client.putObject(bucketName, stringObjKeyName, "Uploaded String
 Object");

            // Upload a file as a new object with ContentType and title specified.
            PutObjectRequest request = new PutObjectRequest(bucketName,
 fileObjKeyName, new File(fileName));
            ObjectMetadata metadata = new ObjectMetadata();
            metadata.setContentType("plain/text");
            metadata.addUserMetadata("title", "someTitle");
            request.setMetadata(metadata);
            s3Client.putObject(request);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

JavaScript

次の例では、特定のリージョンの Amazon S3 バケットに既存のファイルをアップロードします。

```
import { readFile } from "node:fs/promises";

import {
  PutObjectCommand,
  S3Client,
  S3ServiceException,
} from "@aws-sdk/client-s3";

/**
 * Upload a file to an S3 bucket.
```

```
 * @param {{ bucketName: string, key: string, filePath: string }}
 */
export const main = async ({ bucketName, key, filePath }) => {
  const client = new S3Client({});
  const command = new PutObjectCommand({
    Bucket: bucketName,
    Key: key,
    Body: await readFile(filePath),
  });

  try {
    const response = await client.send(command);
    console.log(response);
  } catch (caught) {
    if (
      caught instanceof S3ServiceException &&
      caught.name === "EntityTooLarge"
    ) {
      console.error(
        `Error from S3 while uploading object to ${bucketName}. \
The object was too large. To upload objects larger than 5GB, use the S3 console
 (160GB max) \
or the multipart upload API (5TB max).`,
      );
    } else if (caught instanceof S3ServiceException) {
      console.error(
        `Error from S3 while uploading object to ${bucketName}.  ${caught.name}:
 ${caught.message}`,
      );
    } else {
      throw caught;
    }
  }
};
```

PHP

この例では、AWS SDK for PHP のクラスを使用して、5 GB までのサイズのオブジェクトをアップロードする手順を示します。ファイルのサイズが大きい場合には、マルチパートアップロード API オペレーションを使用する必要があります。詳細については、「Amazon S3 でのマルチパートアップロードを使用したオブジェクトのアップロードとコピー」を参照してください。

AWS SDK for Ruby API の詳細については、AWS SDK for Ruby - バージョン 2 を参照してください。

Example - データをアップロードして Amazon S3 バケットにオブジェクトを作成する

以下の PHP コード例では、putObject() メソッドを使用してデータをアップロードすることで、指定されたバケットにオブジェクトを作成しています。

```
 require 'vendor/autoload.php';

use Aws\S3\Exception\S3Exception;
use Aws\S3\S3Client;

$bucket = '*** Your Bucket Name ***';
$keyname = '*** Your Object Key ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

try {
    // Upload data.
    $result = $s3->putObject([
        'Bucket' => $bucket,
        'Key'    => $keyname,
        'Body'   => 'Hello, world!',
        'ACL'    => 'public-read'
    ]);

    // Print the URL to the object.
    echo $result['ObjectURL'] . PHP_EOL;
} catch (S3Exception $e) {
    echo $e->getMessage() . PHP_EOL;
}
```

Ruby

AWS SDK for Ruby – バージョン 3 には、Amazon S3 にオブジェクトをアップロードする 2 つの方法があります。1 つ目の方法では、ディスクから任意のサイズのファイルを簡単にアップロードできる、マネージド型ファイルアップローダーを使用します。マネージド型ファイルアップローダーによる方法を使用するには、次の操作を行います。

1. Aws::S3::Resource クラスのインスタンスを作成します。
2. バケット名とキーで、ターゲットオブジェクトを参照します。オブジェクトはバケット内に保持され、各オブジェクトを特定するための一意のキーを持っています。
3. オブジェクトで #upload_file を呼び出します。

Example

```
require 'aws-sdk-s3'

# Wraps Amazon S3 object actions.
class ObjectUploadFileWrapper
  attr_reader :object

  # @param object [Aws::S3::Object] An existing Amazon S3 object.
  def initialize(object)
    @object = object
  end

  # Uploads a file to an Amazon S3 object by using a managed uploader.
  #
  # @param file_path [String] The path to the file to upload.
  # @return [Boolean] True when the file is uploaded; otherwise false.
  def upload_file(file_path)
    @object.upload_file(file_path)
    true
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't upload file #{file_path} to #{@object.key}. Here's why:
 #{e.message}"
    false
  end
end

# Example usage:
def run_demo
  bucket_name = "amzn-s3-demo-bucket"
  object_key = "my-uploaded-file"
  file_path = "object_upload_file.rb"

  wrapper = ObjectUploadFileWrapper.new(Aws::S3::Object.new(bucket_name,
 object_key))
  return unless wrapper.upload_file(file_path)
```

```
  puts "File #{file_path} successfully uploaded to #{bucket_name}:#{object_key}."
end

run_demo if $PROGRAM_NAME == __FILE__
```

AWS SDK for Ruby – バージョン 3 でオブジェクトをアップロードできる 2 つ目の方法では、#put の Aws::S3::Object メソッドを使用します。この方法は、オブジェクトが文字列であるか、ディスク上のファイルではない I/O オブジェクトである場合に役立ちます。この方法を使用するには、次の操作を行います。

1. Aws::S3::Resource クラスのインスタンスを作成します。
2. バケット名とキーで、ターゲットオブジェクトを参照します。
3. #put を呼び出し、文字列または I/O オブジェクトを渡します。

Example

```
require 'aws-sdk-s3'

# Wraps Amazon S3 object actions.
class ObjectPutWrapper
  attr_reader :object

  # @param object [Aws::S3::Object] An existing Amazon S3 object.
  def initialize(object)
    @object = object
  end

  def put_object(source_file_path)
    File.open(source_file_path, 'rb') do |file|
      @object.put(body: file)
    end
    true
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't put #{source_file_path} to #{object.key}. Here's why:
 #{e.message}"
    false
  end
end

# Example usage:
def run_demo
```

```
  bucket_name = "amzn-s3-demo-bucket"
  object_key = "my-object-key"
  file_path = "my-local-file.txt"

  wrapper = ObjectPutWrapper.new(Aws::S3::Object.new(bucket_name, object_key))
  success = wrapper.put_object(file_path)
  return unless success

  puts "Put file #{file_path} into #{object_key} in #{bucket_name}."
end

run_demo if $PROGRAM_NAME == __FILE__
```

同じキー名を持つオブジェクトのアップロードを禁止する

アップロード時の条件付き書き込みオペレーションを使用して、バケット内にオブジェクトが存在するかどうかを確認してからオブジェクトを作成できるようになりました。これにより、既存のデータの上書きを阻止できます。条件付き書き込みでは、アップロードする際にバケット内に同じキー名を持つ既存のオブジェクトが存在しないことを検証します。

条件付き書き込みは、PutObject リクエストまたは CompleteMultipartUpload リクエストに使用できます。

条件付きリクエストの詳細については、「条件付きリクエストを使用して S3 オペレーションに前提条件を追加する」を参照してください。

Amazon S3 でのマルチパートアップロードを使用したオブジェクトのアップロードとコピー

マルチパートアップロードを使用すると、単一のオブジェクトをパートのセットとして Amazon S3 にアップロードすることができます。各パートは、オブジェクトのデータの連続する部分です。これらのオブジェクトパートは、任意の順序で個別にアップロードできます。アップロードの場合、更新された AWS クライアントはオブジェクトのチェックサムを自動的に計算し、リクエストの一部としてオブジェクトのサイズとともに Amazon S3 に送信します。いずれかのパートの送信が失敗すると、他のパートに影響を与えることなくそのパートを再送することができます。オブジェクトのすべてのパートがアップロードされたら、Amazon S3 はこれらを組み立ててオブジェクトを作成します。100 MB 以上のオブジェクトは、単一のオペレーションでアップロードするのではなく、マルチパートアップロードを使用するのがベストプラクティスです。

マルチパートアップロードの使用には、次の利点があります。

- スループットの向上 – パートを並列にアップロードすることで、スループットを向上させることができます。
- ネットワーク問題からの迅速な回復 – パートサイズが小さいほど、ネットワークエラーにより失敗したアップロードを再開する際の影響を最小限に抑えることができます。
- オブジェクトのアップロードの一時停止と再開 – オブジェクトの複数のパートを徐々にアップロードできます。マルチパートアップロードを開始した後は終了期限がありません。マルチパートアップロードは明示的に完了または停止する必要があります。
- オブジェクトの最終的なサイズが不明な状態でアップロードを開始 – オブジェクトを作成しながらアップロードできます。

次の方法でマルチパートアップロードを使用することをお勧めします。

- 安定した高帯域幅ネットワーク経由で大きなオブジェクトをアップロードする場合は、複数スレッドのパフォーマンスのために並行してオブジェクトパートをアップロードすることにより、マルチパートアップロードを使用して使用可能な帯域幅の使用を最大化します。
- むらがあるネットワークでアップロードを実行する場合は、マルチパートアップロードを使用して、アップロードの再開を回避することで、ネットワークエラーに対する弾力性を高めます。マルチパートアップロードを使用するときには、アップロード中に中断されたパートのアップロードを再試行するだけで済みます。最初からオブジェクトのアップロードを再開する必要はありません。

> **Note**
>
> Amazon S3 Express One Zone ストレージクラスをディレクトリバケットで使用する方法の詳細については、「S3 Express One Zone」と「ディレクトリバケットの使用」を参照してください。S3 Express One Zone とディレクトリバケットでマルチパートアップロードを使用する方法の詳細については、「ディレクトリバケットでのマルチパートアップロードの使用」を参照してください。

マルチパートアップロードのプロセス

マルチパートアップロードは 3 つのステップで構成されるプロセスです。アップロードを開始し、オブジェクトのパートをアップロードします。すべてのパートをアップロードし終わったら、マルチパートアップロードを完了します。Amazon S3 の側では、マルチパートアップロードの完了リクエ

ストを受け取ると同時に、アップロードされたパートからオブジェクトを構築します。構築されたオブジェクトは、バケット内の他のオブジェクトと同じようにアクセスできます。

進行中のすべてのマルチパートアップロードをリストしたり、特定のマルチパートアップロードにおいてアップロードが完了したパートのリスト表示を取得したりできます。このようなオペレーションのそれぞれについて、このセクションで説明します。

マルチパートアップロードの開始

マルチパートアップロードを開始するリクエストを送信するときは、必ずチェックサムタイプを指定してください。その後、Amazon S3 は、マルチパートアップロードの一意の識別子であるアップロード ID を含むレスポンスを返します。このアップロード ID は、パートのアップロード、パートのリスト、アップロードの完了、アップロードの停止を行うときは常に必要になります。アップロードするオブジェクトの説明となるメタデータを指定する場合は、マルチパートアップロードの開始リクエストの中で指定する必要があります。匿名ユーザーはマルチパートアップロードを開始できません。

パートのアップロード

パートをアップロードするときは、アップロード ID に加えて、パート番号を指定する必要があります。1 ~ 10,000 の範囲で任意のパート番号を選択できます。パート番号によって、アップロードするオブジェクトに含まれるパートとその位置が一意に識別されます。選択するパート番号は、連続している必要はありません (例えば、1、5、14 など)。以前にアップロードしたパートと同じパート番号を使って新しいパートをアップロードした場合、以前のパートは上書きされることに注意してください。

パートをアップロードすると、Amazon S3 は各パートのチェックサム値を含むチェックサムアルゴリズムタイプをレスポンスのヘッダーとして返します。パートのアップロードごとに、パート番号と ETag 値を記録する必要があります。マルチパートアップロードを完了するためには、残りのリクエストにこれらの値を含める必要があります。各パートには、アップロード時に独自の ETag が設定されます。ただし、マルチパートアップロードが完了し、すべてのパートが統合されると、チェックサムのチェックサムとしてすべてのパートが 1 つの ETag に属することになります。

> **Important**
>
> マルチパートアップロードを開始して、1 つまたは複数のパートをアップロードした後は、マルチパートアップロードを完了するか停止しない限り、アップロードしたパートのストレージに対する課金を停止できません。マルチパートアップロードを完了または停止した後でのみ、Amazon S3 はパートのストレージを解放して、パートのストレージに対する課金を停止します。

マルチパートアップロードを停止した後は、再度同じアップロード ID を使ってパートをアップロードすることはできません。パートのアップロードが進行中だった場合、アップロードを停止した後も、パートのアップロードは成功または失敗する可能性があります。すべてのパートによって使用されているストレージをすべて解放するには、すべてのパートのアップロードが完了した後でマルチパートアップロードを停止する必要があります。

マルチパートアップロードの完了

マルチパートアップロードを完了すると、パート番号に基づいて昇順に連結されたオブジェクトが Amazon S3 によって作成されます。マルチパートアップロードの開始リクエストにオブジェクトメタデータが指定されている場合、Amazon S3 によってそのメタデータはオブジェクトに関連付けられます。完了リクエストが正常に処理されると、個々のパートはなくなります。

マルチパートアップロードの完了リクエストには、アップロード ID と、パート番号およびそれに対応する ETag 値のリストが含まれている必要があります。Amazon S3 からのレスポンスには、結合されるオブジェクトデータを一意に識別する ETag が含まれます。この ETag が、オブジェクトデータの MD5 ハッシュになるとは限りません。

マルチパートアップロード中にフルオブジェクトチェックサムを指定すると、AWS SDK はそのチェックサムを Amazon S3 に渡し、S3 はオブジェクトの整合性をサーバー側で検証して、受信した値と比較します。次に、値が一致すると、S3 はオブジェクトを保存します。2 つの値が一致しない場合、Amazon S3 は `BadDigest` エラーでリクエストに失敗します。オブジェクトのチェックサムはオブジェクトメタデータにも保存され、後でオブジェクトのデータ整合性を検証するために使用します。

マルチパートアップロードのサンプル呼び出し

この例では、100 GB ファイルのマルチパートアップロードを生成していると仮定します。この場合、プロセス全体に対して次の API コールが実行されます。合計 1,002 回の API コールが実行されます。

- プロセスを開始する `CreateMultipartUpload` の呼び出し。
- それぞれ 100 MB の一部をアップロードし、合計サイズは 100 GB となる、1,000 回の個別の `UploadPart` の呼び出し。
- プロセスを完了するための `CompleteMultipartUpload` 呼び出し。

マルチパートアップロードのリスト化

特定のマルチパートアップロードのパートや、進行中のすべてのマルチパートアップロードをリスト表示できます。パートのリストオペレーションでは、特定のマルチパートアップロードについて既にアップロードしたパートの情報が返されます。パートのリストリクエストを送信するたびに、指定したマルチパートアップロードのパート情報 (最大で 1,000 個のパート) が Amazon S3 から返されます。マルチパートアップロードに 1,000 個を超えるパートが含まれる場合、すべてのパートを取得するにはパートのリストリクエストを追加で送信する必要があります。返されるパートのリストには、アップロードが完了していないパートは含まれていないことに注意してください。マルチパートアップロードの一覧表示オペレーションを使用すると、進行中のマルチパートアップロードのリストを取得できます。

進行中のマルチパートアップロードとは、開始されているものの、まだ完了または停止されていないアップロードを意味します。各リクエストに最大 1,000 個のマルチパートアップロードが返されます。進行中のマルチパートアップロードが 1,000 個を超える場合、残りのマルチパートアップロードを取得するには、リクエストを追加で送信する必要があります。返されたリストは確認の目的でのみ使用してください。

> **Important**
>
> マルチパートアップロードの完了リクエストを送信するときに、このリストの結果を使用しないでください。代わりに、パートのアップロード時に指定したパート番号と、それに対応する、Amazon S3 から返される ETag 値の独自のリストを維持しておいてください。

マルチパートアップロードオペレーションを使用したチェックサム

Amazon S3 にオブジェクトをアップロードするときに、使用する Amazon S3 のチェックサムアルゴリズムを指定できます。デフォルトでは、AWS SDK および S3 コンソールはすべてのオブジェクトアップロードにアルゴリズムを使用します。これは上書きできます。古い SDK を使用していて、アップロードされたオブジェクトに指定されたチェックサムがない場合、Amazon S3 は自動的に CRC-64/NVME (CRC64NVME) チェックサムアルゴリズムを使用します。(これは、効率的なデータ整合性の検証に推奨されるオプションでもあります。) CRC-64/NVME を使用する場合、Amazon S3 はマルチパートまたはシングルパートのアップロードの完了後に、フルオブジェクトのチェックサムを計算します。CRC-64/NVME チェックサムアルゴリズムは、オブジェクト全体の直接チェックサム、または個々のパートごとにチェックサムのチェックサムを計算するために使用されます。

マルチパートアップロードを使用してオブジェクトを S3 にアップロードすると、Amazon S3 は各パートまたはフルオブジェクトのチェックサム値を計算し、その値を保存します。S3 API または AWS SDK を使用して、次の方法でチェックサム値を取得できます。

- 個々のパートには、GetObject または HeadObject を使用できます。まだ処理中のマルチパートアップロードの個々の部分のチェックサム値を取得したい場合は、ListParts を使用できます。
- オブジェクト全体に対しては、PutObject を使用できます。フルオブジェクトのチェックサムを使用してマルチパートアップロードを実行する場合は、フルオブジェクトのチェックサムタイプを指定して、CreateMultipartUpload と CompleteMultipartUpload を使用します。オブジェクト全体のチェックサム値を検証するか、マルチパートアップロードで使用されているチェックサムタイプを確認するには、ListParts を使用します。

> **Important**
>
> [チェックサム] を含むマルチパートアップロードを使用している場合、各パートのアップロード (マルチパートアップロードに含まれる) のパート番号は、連続しており 1 から始まる必要があります。[チェックサム] を使用している場合、連続しないパート番号でマルチパートアップロードリクエストを完了しようとすると、Amazon S3 は HTTP 500 Internal Server エラーを生成します。

マルチパートアップロードオブジェクトでのチェックサムの動作の詳細については、「Amazon S3 でのオブジェクトの整合性のチェック」を参照してください。

追加のチェックサムを含むマルチパートアップロードを使用してオブジェクトをアップロードする方法を示すエンドツーエンドの手順については、「チュートリアル: マルチパートアップロードでオブジェクトをアップロードして、データ整合性を検証する」を参照してください。

マルチパートアップロードの同時オペレーション

分散開発環境においては、アプリケーションから同じオブジェクトに対して複数の更新が同時に開始されることもありえます。同じオブジェクトキーを使ってアプリケーションから複数のマルチパートアップロードが開始される可能性もあります。そのようなアップロードごとに、アプリケーションからパートのアップロードが行われ、アップロードの完了リクエストが Amazon S3 に送信されて、オブジェクトが作成されます。バケットで S3 バージョニングが有効になっているときには、マルチパートアップロードを完了するたびに新しいバージョンが作成されます。バージョニングが有効なバケットで、同じオブジェクトキーを使用する複数のマルチパートアップロードを開始した場合、オブジェクトの最新バージョンは、どのアップロードが最後に開始されたか (createdDate) によって決まります。

例えば、オブジェクトの CreateMultipartUpload リクエストを午前 10 時に開始します。次に、同じオブジェクトに対する 2 番目の CreateMultipartUpload リクエストを午前 11 時に送信したとします。この場合は、2 番目のリクエストが最後に送信されたため、2 番目のリクエストの後に最初のアップロードが完了したとしても、午前 11 時 のリクエストでアップロードされたオブジェクトが最新バージョンになります。バージョニングが有効になっていないバケットの場合は、マルチパートアップロードの開始から完了までの間に受信された他の何らかのリクエストが優先される可能性もあります。

同時マルチパートアップロードリクエストが優先されるもう 1 つの例は、そのキーを使用してマルチパートアップロードを開始した後に、別のオペレーションでキーが削除される場合です。オペレーションを完了する前に、マルチパートアップロードの完了レスポンスによって、オブジェクトを確認できなくても、オブジェクト作成の成功が示される可能性があります。

マルチパートアップロード中に同じキー名を持つオブジェクトのアップロードを禁止する

アップロード時の条件付き書き込みオペレーションを使用して、バケット内にオブジェクトが存在するかどうかを確認してからオブジェクトを作成できるようになりました。これにより、既存のデータの上書きを阻止できます。条件付き書き込みでは、アップロードする際にバケット内に同じキー名を持つ既存のオブジェクトが存在しないことを検証します。

条件付き書き込みは、PutObject リクエストまたは CompleteMultipartUpload リクエストに使用できます。

条件付きリクエストの詳細については、「条件付きリクエストを使用して S3 オペレーションに前提条件を追加する」を参照してください。

マルチパートアップロードと料金

マルチパートアップロードを開始すると、アップロードを完了または中止するまですべてのパートが Amazon S3 によって保持されます。マルチパートアップロードの実行期間を通して、アップロードとそれに関連するパートのために使用されるすべてのストレージ、帯域幅、リクエストに対して課金が行われます。

これらのパートは、パートのアップロード時に指定されたストレージクラスに従って課金されます。ただし、これらのパートが S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive にアップロードされた場合、料金は請求されません。S3 Glacier Flexible Retrieval ストレージクラスへの PUT リクエストに対する処理中のマルチパートパートは、アップロードが完了するまで S3 Glacier Flexible Retrieval ステージングストレージとして S3 標準ストレージ料金で請求され

ます。さらに、CreateMultipartUpload と UploadPart の両方が S3 標準料金で請求されます。CompleteMultipartUpload リクエストのみが、S3 Glacier Flexible Retrieval 料金で請求されます。同様に、S3 Glacier Deep Archive ストレージクラスへの PUT の処理中のマルチパートパートは、アップロードが完了するまで S3 Glacier Flexible Retrieval ステージングストレージとして S3 標準ストレージ料金で請求されます。CompleteMultipartUpload リクエストのみが、S3 Glacier Deep Archive 料金で請求されます。

マルチパートアップロードを停止した場合、Amazon S3 はアップロードアーティファクトおよびアップロードしたすべてのパートを削除します。これらのアーティファクトについては請求されません。指定されたストレージクラスに関係なく、不完全なマルチパートアップロードの削除に伴う早期削除料金はありません。料金に関する詳細については、[Amazon S3 の料金] を参照してください。

> **Note**
>
> ストレージコストを最小限に抑えるため、AbortIncompleteMultipartUpload アクションを使用して指定した日数が経過した後に不完全なマルチパートアップロードを削除するようにライフサイクルルールを設定することをお勧めします。不完全なマルチパートアップロードを削除するライフサイクルルールの作成の詳細については、「不完全なマルチパートアップロードを中止するためのバケットライフサイクルポリシーの設定」を参照してください。

マルチパートアップロードの API サポート

Amazon Simple Storage Service API リファレンスの以下のセクションでは、マルチパートアップロードの REST API について説明しています。

AWS Lambda 関数を使用するマルチパートアップロードのチュートリアルについては、「Uploading large objects to Amazon S3 using multipart upload and transfer acceleration」を参照してください。

- マルチパートアップロードを作成する
- Upload Part
- Upload Part (Copy)
- Complete Multipart Upload
- マルチパートアップロードの中止
- パートのリスト
- マルチパートアップロードのリスト

マルチパートアップロードの AWS Command Line Interface サポート

マルチパートアップロードのオペレーションについては、AWS Command Line Interface の以下のトピックを参照してください。

- Initiate Multipart Upload
- Upload Part
- Upload Part (Copy)
- Complete Multipart Upload
- マルチパートアップロードの中止
- パートのリスト
- マルチパートアップロードのリスト

マルチパートアップロードの AWS SDK サポート

AWS SDK を使用して、オブジェクトを部分的にアップロードできます。API アクションでサポートされる AWS SDK のリストについては、次を参照してください。

- マルチパートアップロードを作成する
- Upload Part
- Upload Part (Copy)
- Complete Multipart Upload
- マルチパートアップロードの中止
- パートのリスト
- マルチパートアップロードのリスト

マルチパートアップロード API とアクセス許可

マルチパートアップロードオペレーションを使用するには、必要なアクセス権限を有している必要があります。マルチパートアップロードオペレーションを実行するためのアクセス許可を付与するには、アクセスコントロールリスト (ACL)、バケットポリシー、ユーザーポリシーを使用できます。ACL、バケットポリシー、またはユーザーポリシーを使用して割り当てることのできる、さまざまなマルチパートアップロードオペレーションに必要なアクセス許可を次の表に示します。

アクション	必要なアクセス許可
マルチパートアップロードの作成	マルチパートアップロードのリクエストを作成するには、オブジェクトに対して s3:PutObject アクションを実行するための許可が必要です。 バケット所有者は他のプリンシパルに対して s3:PutObject アクションの実行を許可できます。
Initiate Multipart Upload	マルチパートアップロードを開始するには、オブジェクトに対して s3:PutObject アクションを実行するための許可が必要です。 バケット所有者は他のプリンシパルに対して s3:PutObject アクションの実行を許可できます。
イニシエータ	マルチパートアップロード開始者を識別するコンテナエレメント。イニシエータが AWS アカウント である場合、このエレメントは所有者エレメントと同じ情報を提供します。イニシエータが IAM ユーザーである場合、このエレメントはユーザー ARN と表示名を提供します。
Upload Part	パートをアップロードするには、オブジェクトに対して s3:PutObject アクションを実行するための許可が必要です。 マルチパートアップロードの開始者がオブジェクトのパートをアップロードできるようにするため、バケット所有者はその開始者に対しオブジェクトへの s3:PutObject アクションの実行を許可する必要があります。
パートのアップロード (コピー)	パートをアップロードするには、オブジェクトに対して s3:PutObject アクションを実行するための許可が必要です。既存のオブジェクトからパートをアップロードするので、ソースオブジェクトに対して s3:GetObject を実行するための許可が必要です。 開始者がオブジェクトのパートをアップロードするには、バケット所有者が、開始者にそのオブジェクトでの s3:PutObject アクションの実行を許可する必要があります。
Complete Multipart Upload	マルチパートアップロードを完了するには、オブジェクトに対して s3:PutObject アクションを実行するための許可が必要です。

アクション	必要なアクセス許可
	マルチパートアップロードの開始者がオブジェクトのアップロードを完了できるようにするため、バケット所有者はその開始者に対しオブジェクトへの s3:PutObject アクションの実行を許可する必要があります。
マルチパートアップロードの中止	マルチパートアップロードを停止するには、s3:AbortMultipartUpload アクションを実行するための許可が必要です。 デフォルトでは、バケット所有者とマルチパートアップロードの開始者が、IAM と S3 バケットポリシーの一部として、このアクションの実行を許可されます。開始者が IAM ユーザーである場合、そのユーザーの AWS アカウント もそのマルチパートアップロードを停止できます。VPC エンドポイントポリシーでは、マルチパートアップロードのイニシエータは、s3:AbortMultipartUpload アクションを実行する許可を自動的に取得しません。 このようなデフォルト設定に加え、バケット所有者は他のプリンシパルに対してオブジェクトへの s3:AbortMultipartUpload アクションの実行を許可できます。バケット所有者は任意のプリンシパルに対し、s3:AbortMultipartUpload アクションを実行する権限を無効にすることができます。
パートのリスト	マルチパートアップロードに含まれるパートをリストするには、s3:ListMultipartUploadParts アクションを実行するための許可が必要です。 デフォルトではバケット所有者が、バケットに対する任意のマルチパートアップロードについてパートのリストを許可されています。マルチパートアップロードの開始者は、特定のマルチパートアップロードについてパートのリストを許可されます。マルチパートアップロードの開始者が IAM ユーザーである場合、その IAM ユーザーを管理している AWS アカウント もそのアップロードのパートのリストへのアクセス許可を付与されます。 このようなデフォルト設定に加え、バケット所有者は他のプリンシパルに対してオブジェクトへの s3:ListMultipartUploadParts アクションの実行を許可できます。バケット所有者は任意のプリンシパルに対し、s3:ListMultipartUploadParts アクションを実行する権限を無効にすることもできます。

アクション	必要なアクセス許可
マルチパートアップロードのリスト	バケットに対して進行中のマルチパートアップロードをリストするには、そのバケットに対して s3:ListBucketMultipartUploads アクションを実行するための許可が必要です。 デフォルト設定に加え、バケット所有者は他のプリンシパルに対してバケットへの s3:ListBucketMultipartUploads アクションの実行を許可できます。
AWS KMS 暗号化および復号関連のアクセス許可	AWS Key Management Service (AWS KMS) KMS キーを使用した暗号化を伴うマルチパートアップロードを実行するには、リクエスタに以下のアクセス許可が必要です。 • キーに対する kms:Decrypt および kms:GenerateDataKey アクション。 • CreateMultipartUpload API に対する kms:GenerateDataKey アクション。 • UploadPart および UploadPartCopy API に対する kms:Decrypt アクション。 マルチパートアップロードを完了する前に、暗号化されたファイル部分からデータを復号して読み取る必要があるため、Amazon S3 にはこれらの許可が必要です。また、オブジェクトのチェックサム値を取得するには、kms:Decrypt アクセス許可と、お客様が提供した暗号化キーによるサーバー側の暗号化も必要です。CompleteMultipartUpload API の使用時にこれらの必要なアクセス許可がない場合、オブジェクトはチェックサム値なしで作成されます。 IAM ユーザーまたはロールが KMS キーと同じ AWS アカウントにある場合、キーと IAM ポリシーの両方にアクセス許可があることを確認してください。IAM ユーザーまたはロールが KMS キーとは異なるアカウントに属している場合、キーポリシーと IAM ユーザーまたはロールの両方に対する許可が必要です。

アクション	必要なアクセス許可
SSE-C (お客様が用意した暗号化キーによるサーバー側の暗号化)	CompleteMultipartUpload API を使用する場合は、SSE-C (お客様が用意した暗号化キーによるサーバー側の暗号化) を指定する必要があります。指定しない場合、オブジェクトはチェックサムなしで作成され、チェックサム値は返されません。

ACL アクセス権限とアクセスポリシーのアクセス許可との関係については、ACL アクセス許可とアクセスポリシーのアクセス許可のマッピング を参照してください。IAM ユーザー、グループ、ロール、ベストプラクティスの詳細については、IAM ユーザーガイドの「IAM ID (ユーザー、グループ、ロール)」を参照してください。

マルチパートアップロードオペレーションを使用したチェックサム

実際のマルチパートアップロードを実行するために使用される Amazon S3 API は CreateMultipartUpload、UploadPart、および CompleteMultipartUpload の 3 つです。次の表は、各 API に提供する必要があるチェックサムヘッダーと値を示しています。

チェックサムアルゴリズム	チェックサムタイプ	**CreateMultipartUpload**	**UploadPart**	**CompleteMultipartUpoad**

CRC-64/NVME (CRC64NVME)	フルオブジェクト	必要なヘッダー:
		
		`x-amz-checksum-algorithm`
			オプションヘッダー:
			
			`x-amz-checksum-crc64nvme`
				オプションヘッダー:
				
				`x-amz-checksum-algorithm`
				
				`x-amz-crc64`

CRC-32 (CRC32) CRC 32-C (CRC32C)	フルオブジェクト	必要なヘッダー: `x-amz-checksum-algorithm`	オプションヘッダー: `x-amz-checksum-crc64nvme`	オプションヘッダー: `x-amz-checksum-algorithm`

チェックサムアルゴリズム	チェックサムタイプ	**CreateMultipartUpload**	**UploadPart**	**CompleteMultipartUpload**

		`x-amz-checksum-type`		`x-amz-crc32`
				
				`x-amz-crc32c`

CRC-32 (CRC32)
 	
CRC-32C (CRC32C)
 	
SHA-1 (SHA1)
 	
SHA-256 (SHA256)
	複合	必要なヘッダー:
		
		`x-amz-checksum-algorithm`
			必要なヘッダー:
			
			`x-amz-checksum-crc32`
			
			`x-amz-checksum-crc32c`
			
			`x-amz-checksum-sha1`
			
			`x-amz-checksum-sha256`
				必要なヘッダー:
				
				すべてのパートレベルのチェックサムを CompleteMultiPartUpload リクエストに含める必要があります。
				
				オプションヘッダー:
				
				`x-amz-crc32`
				
				`x-amz-crc32c`
				
				`x-amz-sha1`
				
				`x-amz-sha256`

トピック

- 不完全なマルチパートアップロードを削除するためのバケットライフサイクル設定の設定
- マルチパートアップロードを使用したオブジェクトのアップロード
- 高レベルの .NET TransferUtility クラスを使用してディレクトリをアップロードする
- マルチパートアップロードのリスト化

- AWS SDK を使用したマルチパートアップロードの追跡
- マルチパートアップロードの中止
- マルチパートアップロードを使用したオブジェクトのコピー
- チュートリアル: マルチパートアップロードでオブジェクトをアップロードして、データ整合性を検証する
- Amazon S3 マルチパートアップロードの制限

不完全なマルチパートアップロードを削除するためのバケットライフサイクル設定の設定

ベストプラクティスとして、ストレージコストを最小限に抑えるため、AbortIncompleteMultipartUpload アクションを使用してライフサイクルルールを設定することをお勧めします。マルチパートアップロードを中止する方法の詳細については、マルチパートアップロードの中止 を参照してください。

Amazon S3 は、バケットライフサイクルルールをサポートしています。このルールを使用すると、開始後指定された日数内に完了しないマルチパートアップロードを停止するよう Amazon S3 に指示できます。マルチパートアップロードが指定された時間内に完了しない場合、中止操作の対象となります。Amazon S3 は、マルチパートアップロードを中止し、マルチパートアップロードに関連付けられているすべてのパートを削除します。このルールは、既存のマルチパートアップロードと後で作成するマルチパートアップロードの両方に適用されます。

AbortIncompleteMultipartUpload アクションにルールを指定するライフサイクル設定の例を次に示します。

```
<LifecycleConfiguration>
    <Rule>
        <ID>sample-rule</ID>
        <Prefix></Prefix>
        <Status>Enabled</Status>
        <AbortIncompleteMultipartUpload>
          <DaysAfterInitiation>7</DaysAfterInitiation>
        </AbortIncompleteMultipartUpload>
    </Rule>
</LifecycleConfiguration>
```

この例のルールでは、Prefix エレメントの値 (オブジェクトキー名のプレフィックス) を指定しません。したがって、これはマルチパートアップロードを開始したバケット内のすべてのオブジェクト

に適用されます。開始されてから 7 日以内に完了しなかったマルチパートアップロード、中止オペレーションのターゲットとなります。中止アクションは、完了したマルチパートアップロードに影響を与えません。

バケットライフサイクル設定についての詳細は、オブジェクトのライフサイクルの管理 を参照してください。

> **Note**
>
> マルチパートアップロードが、ルールで指定された日数内に完了した場合、`AbortIncompleteMultipartUpload` ライフサイクルアクションは適用されません (つまり Amazon S3 はアクションを実行しません)。また、このアクションはオブジェクトには適用されません。このライフサイクルアクションによって削除されるオブジェクトはありません。また、不完全なマルチパートアップロード部分を削除しても、S3 ライフサイクルの早期削除料金は発生しません。

S3 コンソールの使用

未完了のマルチパートアップロードを自動的に管理するため、S3 コンソールを使用して、指定された日数後にバケットから未完了のマルチパートアップロードのバイトを失効させるライフサイクルポリシーを作成できます。次の手順は、7 日後に未完了のマルチパートアップロードを削除するためのライフサイクルルールを追加する方法を示しています。ライフサイクルルールの追加に関する詳細については、「バケットに S3 ライフサイクル設定を設定する」を参照してください。

7 日以上経過した未完了のマルチパートアップロードを中止するライフサイクルルールを追加するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. [Buckets (バケット)] リストで、ライフサイクルルールを作成するバケットの名前を選択します。
3. [Management (管理)] タブを選択して、[Create lifecycle rule (ライフサイクルルールを作成する)] を選択します。
4. [Lifecycle rule name (ライフサイクルルール名)] に、ルールの名前を入力します。

   その名前はバケット内で一意である必要があります。
5. ライフサイクルルールのスコープを選択します。

- 特定のプレフィックスを持つすべてのオブジェクトに対してライフサイクルルールを作成するには、[1 つまたは複数のフィルタを使用してこのルールの適用範囲を制限] を選択し、[プレフィックス] にプレフィックスを入力します。
- このライフサイクルルールをバケット内のすべてのオブジェクトに作成するには、[This rule applies to all objects in the bucket] (このルールをバケット内のすべてのオブジェクトに適用する) を選択して、[I acknowledge that this lifecycle rule will apply to all objects in the bucket] (このライフサイクルルールがバケット内のすべてのオブジェクトに適用されることを了承します) を選択します。

6. [Lifecycle rule actions] (ライフサイクルルールアクション) で、[Delete expired object delete markers or incomplete multipart uploads] (期限切れのオブジェクト削除マーカーまたは未完了のマルチパートアップロードを削除) を選択します。
7. [Delete expired object delete markers or incomplete multipart uploads] (期限切れオブジェクト削除マーカーまたは未完了のマルチパートアップロードを削除する) で、[Delete incomplete multipart uploads] (未完了のマルチパートアップロードを削除) を選択します。
8. [Number of days] (日数) フィールドに、未完了のマルチパートアップロードを削除するまでの日数 (この例では 7 日) を入力します。
9. [Create rule] を選択してください。

AWS CLI を使用する場合

以下の `put-bucket-lifecycle-configuration` AWS Command Line Interface (AWS CLI) コマンドは、指定したバケットのライフサイクル設定を追加します。このコマンドを使用するには、*`user input placeholders`* を自分の情報に置き換えます。

```
aws s3api put-bucket-lifecycle-configuration  \
        --bucket amzn-s3-demo-bucket  \
        --lifecycle-configuration filename-containing-lifecycle-configuration
```

次の例は、AWS CLI を使用して未完了のマルチパートアップロードを中止するライフサイクルルールを追加する方法を示しています。これには、7 日以上経過した未完了のマルチパートアップロードを中止する JSON ライフサイクル設定の例が含まれています。

この例の CLI コマンドを使用するには、*`user input placeholders`* を自分の情報に置き換えてください。

未完了のマルチパートアップロードを中止するためのライフサイクルルールを追加するには

1. AWS CLI のセットアップ。手順については、「Amazon S3 API リファレンス」の「Developing with Amazon S3 using the AWS CLI」を参照してください。
2. 次のサンプルライフサイクル設定をファイル (例、*lifecycle.json*) に保存します。このサンプル設定では、空のプレフィックスが指定されているため、バケット内のすべてのオブジェクトに適用されます。設定がオブジェクトのサブセットに制限されるようにプレフィックスを指定できます。

```
{
    "Rules": [
        {
            "ID": "Test Rule",
            "Status": "Enabled",
            "Filter": {
                "Prefix": ""
            },
            "AbortIncompleteMultipartUpload": {
                "DaysAfterInitiation": 7
            }
        }
    ]
}
```

3. 次の CLI コマンドを実行して、バケットにこのライフサイクル設定を指定します。

```
aws s3api put-bucket-lifecycle-configuration   \
--bucket amzn-s3-demo-bucket  \
--lifecycle-configuration file://lifecycle.json
```

4. ライフサイクル設定がバケットに設定されていることを確認するには、次の `get-bucket-lifecycle` コマンドを使用してライフサイクル設定を取得します。

```
aws s3api get-bucket-lifecycle  \
--bucket amzn-s3-demo-bucket
```

5. ライフサイクル設定を削除するには、次の `delete-bucket-lifecycle` コマンドを使用します。

```
aws s3api delete-bucket-lifecycle \
--bucket amzn-s3-demo-bucket
```

マルチパートアップロードを使用したオブジェクトのアップロード

マルチパートアップロードを使用して、プログラムで 1 つのオブジェクトを Amazon S3 にアップロードできます。各オブジェクトは一連のパートとしてアップロードされます。各パートは、オブジェクトのデータの連続する部分です。これらのオブジェクトパートは、任意の順序で個別にアップロードできます。いずれかのパートの送信が失敗すると、他のパートに影響を与えることなくそのパートを再送することができます。オブジェクトのすべてのパートがアップロードされたら、Amazon S3 はこれらのパートを組み立ててオブジェクトを作成します。匿名ユーザーはマルチパートアップロードを開始できません。

マルチパートアップロードで追加のチェックサムを含むオブジェクトをアップロードするエンドツーエンドの手順については、「チュートリアル: マルチパートアップロードでオブジェクトをアップロードして、データ整合性を検証する」を参照してください。

次のセクションでは、AWS Command Line Interface、AWS SDK でマルチパートアップロードを使用する方法を示します。

S3 コンソールの使用

ファイルタイプ (イメージ、バックアップ、データ、ムービーなど) を問わず、各種のファイルを S3 バケットにアップロードできます。Amazon S3 コンソールを使用すると、アップロードできるファイルの最大サイズが 160 GB になります。160 GB を超えるファイルをアップロードするには、AWS Command Line Interface (AWS CLI)、AWS SDK、または Amazon S3 REST API を使用します。

AWS Management Console でオブジェクトをアップロードする手順については、「オブジェクトのアップロード」を参照してください。

AWS CLI を使用する場合

AWS CLI を使用したマルチパートアップロードの Amazon S3 オペレーションについては、以下で説明しています。

- Initiate Multipart Upload
- Upload Part
- Upload Part (Copy)
- Complete Multipart Upload
- マルチパートアップロードの中止
- パートのリスト

- マルチパートアップロードのリスト

REST API の使用

Amazon Simple Storage Service API リファレンスの以下のセクションでは、マルチパートアップロードの REST API について説明しています。

- Initiate Multipart Upload
- Upload Part
- Complete Multipart Upload
- マルチパートアップロードの中止
- パートのリスト
- マルチパートアップロードのリスト

AWS SDK (高レベル API) の使用

一部の AWS SDK は、マルチパートアップロードを完了するために必要なさまざまな API オペレーションを 1 つのオペレーションに結合することで、マルチパートアップロードを簡素化する高レベル API を公開しています。詳細については、「Amazon S3 でのマルチパートアップロードを使用したオブジェクトのアップロードとコピー」を参照してください。

マルチパートアップロードを一時停止して再開する場合、アップロード中にパートサイズを変更する場合、またはデータのサイズが事前にわからない場合は、低レベル API メソッドを使用します。マルチパートアップロード用の低レベル API メソッドは、追加の機能も提供します。詳細については、「AWS SDK の使用 (低レベル API)」を参照してください。

.NET

S3 バケットにファイルをアップロードするには、`TransferUtility` クラスを使用します。ファイルからデータをアップロードする場合は、オブジェクトのキー名を指定する必要があります。指定しないと、API ではキー名としてファイル名を使用します。ストリームからデータをアップロードする場合は、オブジェクトのキー名を指定する必要があります。

高度なアップロードオプション (パートのサイズ、複数のパーツを同時にアップロードする際のスレッド数、メタデータ、ストレージクラス、ACL など) を設定するには、`TransferUtilityUploadRequest` クラスを使用します。

> **Note**
>
> データのソースにストリームを使っている場合、TransferUtility クラスは同時アップロードを実行しません。

次の C# の例では、ファイルを複数のパートに分割して Amazon S3 バケットにアップロードします。さまざまな TransferUtility.Upload オーバーロードを使用してファイルをアップロードする方法を示します。後続のアップロード呼び出しが行われるたびに、前のアップロードが置き換えられます。コード例を設定および実行する方法の詳細については、「AWS SDK for .NET デベロッパーガイド」の「AWS SDK for .NET の開始方法」 を参照してください。

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Transfer;
using System;
using System.IO;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class UploadFileMPUHighLevelAPITest
    {
        private const string bucketName = "*** provide bucket name ***";
        private const string keyName = "*** provide a name for the uploaded object
 ***";
        private const string filePath = "*** provide the full path name of the file
 to upload ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;

        public static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            UploadFileAsync().Wait();
        }

        private static async Task UploadFileAsync()
        {
            try
```

```
            {
                var fileTransferUtility =
                    new TransferUtility(s3Client);

                // Option 1. Upload a file. The file name is used as the object key
name.
                await fileTransferUtility.UploadAsync(filePath, bucketName);
                Console.WriteLine("Upload 1 completed");

                // Option 2. Specify object key name explicitly.
                await fileTransferUtility.UploadAsync(filePath, bucketName,
keyName);
                Console.WriteLine("Upload 2 completed");

                // Option 3. Upload data from a type of System.IO.Stream.
                using (var fileToUpload =
                    new FileStream(filePath, FileMode.Open, FileAccess.Read))
                {
                    await fileTransferUtility.UploadAsync(fileToUpload,
                                               bucketName, keyName);
                }
                Console.WriteLine("Upload 3 completed");

                // Option 4. Specify advanced settings.
                var fileTransferUtilityRequest = new TransferUtilityUploadRequest
                {
                    BucketName = bucketName,
                    FilePath = filePath,
                    StorageClass = S3StorageClass.StandardInfrequentAccess,
                    PartSize = 6291456, // 6 MB.
                    Key = keyName,
                    CannedACL = S3CannedACL.PublicRead
                };
                fileTransferUtilityRequest.Metadata.Add("param1", "Value1");
                fileTransferUtilityRequest.Metadata.Add("param2", "Value2");

                await fileTransferUtility.UploadAsync(fileTransferUtilityRequest);
                Console.WriteLine("Upload 4 completed");
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
writing an object", e.Message);
            }
```

```
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }

        }
    }
}
```

JavaScript

Example

サイズの大きいファイルをアップロードします。

```
import { S3Client } from "@aws-sdk/client-s3";
import { Upload } from "@aws-sdk/lib-storage";

import {
  ProgressBar,
  logger,
} from "@aws-doc-sdk-examples/lib/utils/util-log.js";

const twentyFiveMB = 25 * 1024 * 1024;

export const createString = (size = twentyFiveMB) => {
  return "x".repeat(size);
};

/**
 * Create a 25MB file and upload it in parts to the specified
 * Amazon S3 bucket.
 * @param {{ bucketName: string, key: string }}
 */
export const main = async ({ bucketName, key }) => {
  const str = createString();
  const buffer = Buffer.from(str, "utf8");
  const progressBar = new ProgressBar({
    description: `Uploading "${key}" to "${bucketName}"`,
    barLength: 30,
  });

  try {
```

```
    const upload = new Upload({
      client: new S3Client({}),
      params: {
        Bucket: bucketName,
        Key: key,
        Body: buffer,
      },
    });

    upload.on("httpUploadProgress", ({ loaded, total }) => {
      progressBar.update({ current: loaded, total });
    });

    await upload.done();
  } catch (caught) {
    if (caught instanceof Error && caught.name === "AbortError") {
      logger.error(`Multipart upload was aborted. ${caught.message}`);
    } else {
      throw caught;
    }
  }
};
```

Example

サイズの大きいファイルをダウンロードします。

```
import { fileURLToPath } from "node:url";
import { GetObjectCommand, NoSuchKey, S3Client } from "@aws-sdk/client-s3";
import { createWriteStream, rmSync } from "node:fs";

const s3Client = new S3Client({});
const oneMB = 1024 * 1024;

export const getObjectRange = ({ bucket, key, start, end }) => {
  const command = new GetObjectCommand({
    Bucket: bucket,
    Key: key,
    Range: `bytes=${start}-${end}`,
  });

  return s3Client.send(command);
};
```

```
/**
 * @param {string | undefined} contentRange
 */
export const getRangeAndLength = (contentRange) => {
  const [range, length] = contentRange.split("/");
  const [start, end] = range.split("-");
  return {
    start: Number.parseInt(start),
    end: Number.parseInt(end),
    length: Number.parseInt(length),
  };
};

export const isComplete = ({ end, length }) => end === length - 1;

const downloadInChunks = async ({ bucket, key }) => {
  const writeStream = createWriteStream(
    fileURLToPath(new URL(`./${key}`, import.meta.url)),
  ).on("error", (err) => console.error(err));

  let rangeAndLength = { start: -1, end: -1, length: -1 };

  while (!isComplete(rangeAndLength)) {
    const { end } = rangeAndLength;
    const nextRange = { start: end + 1, end: end + oneMB };

    const { ContentRange, Body } = await getObjectRange({
      bucket,
      key,
      ...nextRange,
    });
    console.log(`Downloaded bytes ${nextRange.start} to ${nextRange.end}`);

    writeStream.write(await Body.transformToByteArray());
    rangeAndLength = getRangeAndLength(ContentRange);
  }
};

/**
 * Download a large object from and Amazon S3 bucket.
 *
 * When downloading a large file, you might want to break it down into
 * smaller pieces. Amazon S3 accepts a Range header to specify the start
```

```
 * and end of the byte range to be downloaded.
 *
 * @param {{ bucketName: string, key: string }}
 */
export const main = async ({ bucketName, key }) => {
  try {
    await downloadInChunks({
      bucket: bucketName,
      key: key,
    });
  } catch (caught) {
    if (caught instanceof NoSuchKey) {
      console.error(`Failed to download object. No such key "${key}".`);
      rmSync(key);
    }
  }
};
```

Go

マルチパートアップロードの Go コード例の詳細については、「Upload or download large files to and from Amazon S3 using an AWS SDK」を参照してください。

Example

アップロードマネージャーを使用してデータを分割し、同時にアップロードすることで、大きなオブジェクトをアップロードすることができます。

```
import (
 "bytes"
 "context"
 "errors"
 "fmt"
 "io"
 "log"
 "os"
 "time"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/feature/s3/manager"
 "github.com/aws/aws-sdk-go-v2/service/s3"
 "github.com/aws/aws-sdk-go-v2/service/s3/types"
```

```
 "github.com/aws/smithy-go"
)

// BucketBasics encapsulates the Amazon Simple Storage Service (Amazon S3) actions
// used in the examples.
// It contains S3Client, an Amazon S3 service client that is used to perform bucket
// and object actions.
type BucketBasics struct {
 S3Client *s3.Client
}
```

```
// UploadLargeObject uses an upload manager to upload data to an object in a bucket.
// The upload manager breaks large data into parts and uploads the parts
 concurrently.
func (basics BucketBasics) UploadLargeObject(ctx context.Context, bucketName string,
 objectKey string, largeObject []byte) error {
 largeBuffer := bytes.NewReader(largeObject)
 var partMiBs int64 = 10
 uploader := manager.NewUploader(basics.S3Client, func(u *manager.Uploader) {
  u.PartSize = partMiBs * 1024 * 1024
 })
 _, err := uploader.Upload(ctx, &s3.PutObjectInput{
  Bucket: aws.String(bucketName),
  Key:    aws.String(objectKey),
  Body:   largeBuffer,
 })
 if err != nil {
  var apiErr smithy.APIError
  if errors.As(err, &apiErr) && apiErr.ErrorCode() == "EntityTooLarge" {
   log.Printf("Error while uploading object to %s. The object is too large.\n"+
    "The maximum size for a multipart upload is 5TB.", bucketName)
  } else {
   log.Printf("Couldn't upload large object to %v:%v. Here's why: %v\n",
    bucketName, objectKey, err)
  }
 } else {
  err = s3.NewObjectExistsWaiter(basics.S3Client).Wait(
   ctx, &s3.HeadObjectInput{Bucket: aws.String(bucketName), Key:
 aws.String(objectKey)}, time.Minute)
  if err != nil {
   log.Printf("Failed attempt to wait for object %s to exist.\n", objectKey)
```

```
  }
 }

 return err
}
```

Example

ダウンロードマネージャーを使用して、データを分割して取得し、同時にダウンロードすることで、大きなオブジェクトをダウンロードすることができます。

```
// DownloadLargeObject uses a download manager to download an object from a bucket.
// The download manager gets the data in parts and writes them to a buffer until all
 of
// the data has been downloaded.
func (basics BucketBasics) DownloadLargeObject(ctx context.Context, bucketName
 string, objectKey string) ([]byte, error) {
 var partMiBs int64 = 10
 downloader := manager.NewDownloader(basics.S3Client, func(d *manager.Downloader) {
  d.PartSize = partMiBs * 1024 * 1024
 })
 buffer := manager.NewWriteAtBuffer([]byte{})
 _, err := downloader.Download(ctx, buffer, &s3.GetObjectInput{
  Bucket: aws.String(bucketName),
  Key:    aws.String(objectKey),
 })
 if err != nil {
  log.Printf("Couldn't download large object from %v:%v. Here's why: %v\n",
   bucketName, objectKey, err)
 }
 return buffer.Bytes(), err
}
```

PHP

このトピックでは、マルチパートファイルのアップロードの Aws\S3\Model\MultipartUpload\UploadBuilder からの高レベルの AWS SDK for PHP クラスを使用する方法について説明します。AWS SDK for Ruby API の詳細については、AWS SDK for Ruby - バージョン 2 を参照してください。

以下の PHP サンプルは、ファイルを Amazon S3 バケットにアップロードします。この例では、MultipartUploader オブジェクトのパラメータを設定する方法を示します。

```
 require 'vendor/autoload.php';

use Aws\Exception\MultipartUploadException;
use Aws\S3\MultipartUploader;
use Aws\S3\S3Client;

$bucket = '*** Your Bucket Name ***';
$keyname = '*** Your Object Key ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

// Prepare the upload parameters.
$uploader = new MultipartUploader($s3, '/path/to/large/file.zip', [
    'bucket' => $bucket,
    'key'    => $keyname
]);

// Perform the upload.
try {
    $result = $uploader->upload();
    echo "Upload complete: {$result['ObjectURL']}" . PHP_EOL;
} catch (MultipartUploadException $e) {
    echo $e->getMessage() . PHP_EOL;
}
```

Python

次の例では、高レベルマルチパートアップロード Python API (TransferManager クラス) を使用して、オブジェクトをロードします。

```
import sys
import threading

import boto3
from boto3.s3.transfer import TransferConfig
```

```
MB = 1024 * 1024
s3 = boto3.resource("s3")


class TransferCallback:
    """
    Handle callbacks from the transfer manager.

    The transfer manager periodically calls the __call__ method throughout
    the upload and download process so that it can take action, such as
    displaying progress to the user and collecting data about the transfer.
    """

    def __init__(self, target_size):
        self._target_size = target_size
        self._total_transferred = 0
        self._lock = threading.Lock()
        self.thread_info = {}

    def __call__(self, bytes_transferred):
        """
        The callback method that is called by the transfer manager.

        Display progress during file transfer and collect per-thread transfer
        data. This method can be called by multiple threads, so shared instance
        data is protected by a thread lock.
        """
        thread = threading.current_thread()
        with self._lock:
            self._total_transferred += bytes_transferred
            if thread.ident not in self.thread_info.keys():
                self.thread_info[thread.ident] = bytes_transferred
            else:
                self.thread_info[thread.ident] += bytes_transferred

            target = self._target_size * MB
            sys.stdout.write(
                f"\r{self._total_transferred} of {target} transferred "
                f"({(self._total_transferred / target) * 100:.2f}%)."
            )
            sys.stdout.flush()
```

```
def upload_with_default_configuration(
    local_file_path, bucket_name, object_key, file_size_mb
):
    """
    Upload a file from a local folder to an Amazon S3 bucket, using the default
    configuration.
    """
    transfer_callback = TransferCallback(file_size_mb)
    s3.Bucket(bucket_name).upload_file(
        local_file_path, object_key, Callback=transfer_callback
    )
    return transfer_callback.thread_info


def upload_with_chunksize_and_meta(
    local_file_path, bucket_name, object_key, file_size_mb, metadata=None
):
    """
    Upload a file from a local folder to an Amazon S3 bucket, setting a
    multipart chunk size and adding metadata to the Amazon S3 object.

    The multipart chunk size controls the size of the chunks of data that are
    sent in the request. A smaller chunk size typically results in the transfer
    manager using more threads for the upload.

    The metadata is a set of key-value pairs that are stored with the object
    in Amazon S3.
    """
    transfer_callback = TransferCallback(file_size_mb)

    config = TransferConfig(multipart_chunksize=1 * MB)
    extra_args = {"Metadata": metadata} if metadata else None
    s3.Bucket(bucket_name).upload_file(
        local_file_path,
        object_key,
        Config=config,
        ExtraArgs=extra_args,
        Callback=transfer_callback,
    )
    return transfer_callback.thread_info


def upload_with_high_threshold(local_file_path, bucket_name, object_key,
 file_size_mb):
```

```
    """
    Upload a file from a local folder to an Amazon S3 bucket, setting a
    multipart threshold larger than the size of the file.

    Setting a multipart threshold larger than the size of the file results
    in the transfer manager sending the file as a standard upload instead of
    a multipart upload.
    """
    transfer_callback = TransferCallback(file_size_mb)
    config = TransferConfig(multipart_threshold=file_size_mb * 2 * MB)
    s3.Bucket(bucket_name).upload_file(
        local_file_path, object_key, Config=config, Callback=transfer_callback
    )
    return transfer_callback.thread_info


def upload_with_sse(
    local_file_path, bucket_name, object_key, file_size_mb, sse_key=None
):
    """
    Upload a file from a local folder to an Amazon S3 bucket, adding server-side
    encryption with customer-provided encryption keys to the object.

    When this kind of encryption is specified, Amazon S3 encrypts the object
    at rest and allows downloads only when the expected encryption key is
    provided in the download request.
    """
    transfer_callback = TransferCallback(file_size_mb)
    if sse_key:
        extra_args = {"SSECustomerAlgorithm": "AES256", "SSECustomerKey": sse_key}
    else:
        extra_args = None
    s3.Bucket(bucket_name).upload_file(
        local_file_path, object_key, ExtraArgs=extra_args,
 Callback=transfer_callback
    )
    return transfer_callback.thread_info


def download_with_default_configuration(
    bucket_name, object_key, download_file_path, file_size_mb
):
    """
    Download a file from an Amazon S3 bucket to a local folder, using the
```

```
    default configuration.
    """
    transfer_callback = TransferCallback(file_size_mb)
    s3.Bucket(bucket_name).Object(object_key).download_file(
        download_file_path, Callback=transfer_callback
    )
    return transfer_callback.thread_info


def download_with_single_thread(
    bucket_name, object_key, download_file_path, file_size_mb
):
    """
    Download a file from an Amazon S3 bucket to a local folder, using a
    single thread.
    """
    transfer_callback = TransferCallback(file_size_mb)
    config = TransferConfig(use_threads=False)
    s3.Bucket(bucket_name).Object(object_key).download_file(
        download_file_path, Config=config, Callback=transfer_callback
    )
    return transfer_callback.thread_info


def download_with_high_threshold(
    bucket_name, object_key, download_file_path, file_size_mb
):
    """
    Download a file from an Amazon S3 bucket to a local folder, setting a
    multipart threshold larger than the size of the file.

    Setting a multipart threshold larger than the size of the file results
    in the transfer manager sending the file as a standard download instead
    of a multipart download.
    """
    transfer_callback = TransferCallback(file_size_mb)
    config = TransferConfig(multipart_threshold=file_size_mb * 2 * MB)
    s3.Bucket(bucket_name).Object(object_key).download_file(
        download_file_path, Config=config, Callback=transfer_callback
    )
    return transfer_callback.thread_info


def download_with_sse(
```

```
    bucket_name, object_key, download_file_path, file_size_mb, sse_key
):
    """
    Download a file from an Amazon S3 bucket to a local folder, adding a
    customer-provided encryption key to the request.

    When this kind of encryption is specified, Amazon S3 encrypts the object
    at rest and allows downloads only when the expected encryption key is
    provided in the download request.
    """
    transfer_callback = TransferCallback(file_size_mb)

    if sse_key:
        extra_args = {"SSECustomerAlgorithm": "AES256", "SSECustomerKey": sse_key}
    else:
        extra_args = None
    s3.Bucket(bucket_name).Object(object_key).download_file(
        download_file_path, ExtraArgs=extra_args, Callback=transfer_callback
    )
    return transfer_callback.thread_info
```

AWS SDK の使用 (低レベル API)

AWS SDK は、Amazon S3 REST API に非常によく似たマルチパートアップロード用の下位 API を公開しています (Amazon S3 でのマルチパートアップロードを使用したオブジェクトのアップロードとコピー を参照)。マルチパートアップロードを一時停止して再開する必要がある場合やアップロード中にパートサイズを変更する場合、またはアップロードデータのサイズが事前にわからない場合は、低レベル API を使用します。これらの要件がない場合は、高レベル API (AWS SDK (高レベル API) の使用 を参照) を使用します。

Java

次の例では、低レベル Java クラスを使用してファイルをアップロードする方法を示します。以下のステップが実行されます。

- `AmazonS3Client.initiateMultipartUpload()` メソッドを使用してマルチパートアップロードを開始し、`InitiateMultipartUploadRequest` オブジェクトを渡します。

- AmazonS3Client.initiateMultipartUpload() メソッドが返すアップロード ID を保存します。以降、マルチパートアップロードオペレーションのたびに、このアップロード ID を指定する必要があります。
- オブジェクトのパートをアップロードします。パートごとに、AmazonS3Client.uploadPart() メソッドを呼び出します。UploadPartRequest オブジェクトを使用して、パートアップロード情報を指定します。
- 各パートで、リストの AmazonS3Client.uploadPart() メソッドのレスポンスから ETag を保存します。ETag 値を使用して、マルチパートアップロードを完了します。
- AmazonS3Client.completeMultipartUpload() メソッドを呼び出して、マルチパートアップロードを完了します。

Example

作業サンプルの作成およびテストの手順については、「AWS SDK for Java のデベロッパーガイド」の「使用開始」を参照してください。

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.*;

import java.io.File;
import java.io.IOException;
import java.util.ArrayList;
import java.util.List;

public class LowLevelMultipartUpload {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String keyName = "*** Key name ***";
        String filePath = "*** Path to file to upload ***";

        File file = new File(filePath);
        long contentLength = file.length();
```

```
        long partSize = 5 * 1024 * 1024; // Set part size to 5 MB.

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withRegion(clientRegion)
                    .withCredentials(new ProfileCredentialsProvider())
                    .build();

            // Create a list of ETag objects. You retrieve ETags for each object
part
            // uploaded,
            // then, after each individual part has been uploaded, pass the list of
ETags to
            // the request to complete the upload.
            List<PartETag> partETags = new ArrayList<PartETag>();

            // Initiate the multipart upload.
            InitiateMultipartUploadRequest initRequest = new
InitiateMultipartUploadRequest(bucketName, keyName);
            InitiateMultipartUploadResult initResponse =
s3Client.initiateMultipartUpload(initRequest);

            // Upload the file parts.
            long filePosition = 0;
            for (int i = 1; filePosition < contentLength; i++) {
                // Because the last part could be less than 5 MB, adjust the part
size as
                // needed.
                partSize = Math.min(partSize, (contentLength - filePosition));

                // Create the request to upload a part.
                UploadPartRequest uploadRequest = new UploadPartRequest()
                        .withBucketName(bucketName)
                        .withKey(keyName)
                        .withUploadId(initResponse.getUploadId())
                        .withPartNumber(i)
                        .withFileOffset(filePosition)
                        .withFile(file)
                        .withPartSize(partSize);

                // Upload the part and add the response's ETag to our list.
                UploadPartResult uploadResult = s3Client.uploadPart(uploadRequest);
                partETags.add(uploadResult.getPartETag());
```

```
                filePosition += partSize;
            }

            // Complete the multipart upload.
            CompleteMultipartUploadRequest compRequest = new
 CompleteMultipartUploadRequest(bucketName, keyName,
                    initResponse.getUploadId(), partETags);
            s3Client.completeMultipartUpload(compRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

.NET

次の C# の例では、低レベルの SDK for .NET マルチパートアップロード API を使用して S3 バケットにファイルをアップロードする方法を示します。Amazon S3 のマルチパートアップロードの詳細については、Amazon S3 でのマルチパートアップロードを使用したオブジェクトのアップロードとコピー を参照してください。

> **Note**
>
> SDK for .NET API を使用して大きなオブジェクトをアップロードする場合、リクエストストリームへのデータの書き込み中に、タイムアウトが発生することがあります。`UploadPartRequest` を使用して、明示的なタイムアウトを設定できます。

次 C# の例では、低レベルのマルチパートアップロード API を使用して S3 バケットにファイルをアップロードします。コード例を設定および実行する方法の詳細については、「AWS SDK for .NET デベロッパーガイド」の「AWS SDK for .NET の開始方法」 を参照してください。

```
using Amazon;
using Amazon.Runtime;
using Amazon.S3;
```

```
using Amazon.S3.Model;
using System;
using System.Collections.Generic;
using System.IO;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class UploadFileMPULowLevelAPITest
    {
        private const string bucketName = "*** provide bucket name ***";
        private const string keyName = "*** provide a name for the uploaded object
 ***";
        private const string filePath = "*** provide the full path name of the file
 to upload ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;

        public static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            Console.WriteLine("Uploading an object");
            UploadObjectAsync().Wait();
        }

        private static async Task UploadObjectAsync()
        {
            // Create list to store upload part responses.
            List<UploadPartResponse> uploadResponses = new
 List<UploadPartResponse>();

            // Setup information required to initiate the multipart upload.
            InitiateMultipartUploadRequest initiateRequest = new
 InitiateMultipartUploadRequest
            {
                BucketName = bucketName,
                Key = keyName
            };

            // Initiate the upload.
            InitiateMultipartUploadResponse initResponse =
                await s3Client.InitiateMultipartUploadAsync(initiateRequest);
```

```
            // Upload parts.
            long contentLength = new FileInfo(filePath).Length;
            long partSize = 5 * (long)Math.Pow(2, 20); // 5 MB

            try
            {
                Console.WriteLine("Uploading parts");

                long filePosition = 0;
                for (int i = 1; filePosition < contentLength; i++)
                {
                    UploadPartRequest uploadRequest = new UploadPartRequest
                        {
                            BucketName = bucketName,
                            Key = keyName,
                            UploadId = initResponse.UploadId,
                            PartNumber = i,
                            PartSize = partSize,
                            FilePosition = filePosition,
                            FilePath = filePath
                        };

                    // Track upload progress.
                    uploadRequest.StreamTransferProgress +=
                        new
EventHandler<StreamTransferProgressArgs>(UploadPartProgressEventCallback);

                    // Upload a part and add the response to our list.
                    uploadResponses.Add(await
s3Client.UploadPartAsync(uploadRequest));

                    filePosition += partSize;
                }

                // Setup to complete the upload.
                CompleteMultipartUploadRequest completeRequest = new
CompleteMultipartUploadRequest
                    {
                        BucketName = bucketName,
                        Key = keyName,
                        UploadId = initResponse.UploadId
                     };
                completeRequest.AddPartETags(uploadResponses);
```

```
                // Complete the upload.
                CompleteMultipartUploadResponse completeUploadResponse =
                    await s3Client.CompleteMultipartUploadAsync(completeRequest);
            }
            catch (Exception exception)
            {
                Console.WriteLine("An AmazonS3Exception was thrown: { 0}",
 exception.Message);

                // Abort the upload.
                AbortMultipartUploadRequest abortMPURequest = new
 AbortMultipartUploadRequest
                {
                    BucketName = bucketName,
                    Key = keyName,
                    UploadId = initResponse.UploadId
                };
               await s3Client.AbortMultipartUploadAsync(abortMPURequest);
            }
        }
        public static void UploadPartProgressEventCallback(object sender,
 StreamTransferProgressArgs e)
        {
            // Process event.
            Console.WriteLine("{0}/{1}", e.TransferredBytes, e.TotalBytes);
        }
    }
}
```

PHP

このトピックガイドでは、uploadPart のバージョン 3 から低レベルの AWS SDK for PHP メソッドを使用してファイルを複数のパートに分割してアップロードする方法について説明します。AWS SDK for Ruby API の詳細については、AWS SDK for Ruby - バージョン 2 を参照してください。

次の PHP の例では、下位の PHP API マルチパートアップロードを使用して、Amazon S3 バケットにファイルをアップロードします。

```
 require 'vendor/autoload.php';

use Aws\S3\Exception\S3Exception;
```

```
use Aws\S3\S3Client;

$bucket = '*** Your Bucket Name ***';
$keyname = '*** Your Object Key ***';
$filename = '*** Path to and Name of the File to Upload ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

$result = $s3->createMultipartUpload([
    'Bucket'       => $bucket,
    'Key'          => $keyname,
    'StorageClass' => 'REDUCED_REDUNDANCY',
    'Metadata'     => [
        'param1' => 'value 1',
        'param2' => 'value 2',
        'param3' => 'value 3'
    ]
]);
$uploadId = $result['UploadId'];

// Upload the file in parts.
try {
    $file = fopen($filename, 'r');
    $partNumber = 1;
    while (!feof($file)) {
        $result = $s3->uploadPart([
            'Bucket'     => $bucket,
            'Key'        => $keyname,
            'UploadId'   => $uploadId,
            'PartNumber' => $partNumber,
            'Body'       => fread($file, 5 * 1024 * 1024),
        ]);
        $parts['Parts'][$partNumber] = [
            'PartNumber' => $partNumber,
            'ETag' => $result['ETag'],
        ];
        $partNumber++;

        echo "Uploading part $partNumber of $filename." . PHP_EOL;
    }
    fclose($file);
```

```
} catch (S3Exception $e) {
    $result = $s3->abortMultipartUpload([
        'Bucket'   => $bucket,
        'Key'      => $keyname,
        'UploadId' => $uploadId
    ]);

    echo "Upload of $filename failed." . PHP_EOL;
}

// Complete the multipart upload.
$result = $s3->completeMultipartUpload([
    'Bucket'   => $bucket,
    'Key'      => $keyname,
    'UploadId' => $uploadId,
    'MultipartUpload'    => $parts,
]);
$url = $result['Location'];

echo "Uploaded $filename to $url." . PHP_EOL;
```

AWS SDK for Ruby を使用する場合

AWS SDK for Ruby バージョン 3 では、2 つの方法で Amazon S3 マルチパートアップロードがサポートされています。1 つ目のオプションとして、マネージドファイルアップロードを使用できます。詳細については、AWS 開発者ブログの Amazon S3 にファイルをアップロードするを参照してください。マネージドファイルアップロードは、バケットにファイルをアップロードするための推奨される方法です。これらのアップロードには次の利点があります。

- 15 MB より大きなオブジェクトのマルチパートアップロードを管理します。
- エンコードの問題を回避するために、バイナリモードでファイルを正しく開きます。
- 大きなオブジェクトの複数パートを並行してアップロードするために、複数のスレッドを使用します。

次に示すマルチパートアップロードクライアントオペレーションを直接使用することもできます。

- create_multipart_upload – マルチパートアップロードを開始し、アップロード ID を返します。
- upload_part – マルチパートアップロードでパートをアップロードします。

- upload_part_copy – データソースとして既存のオブジェクトからデータをコピーすることで、パートをアップロードします。
- complete_multipart_upload – 以前にアップロードしたパートを組み合わせることで、マルチパートアップロードを完了します。
- abort_multipart_upload – マルチパートアップロードを停止します。

高レベルの .NET TransferUtility クラスを使用してディレクトリをアップロードする

ディレクトリ全体をアップロードするには、TransferUtility クラスを使用できます。デフォルトでは、API でアップロードされるのは、指定したディレクトリのルートにあるファイルのみです。ただし、すべてのサブディレクトリでファイルを再帰的にアップロードするように指定できます。

フィルタ基準に基づいて指定したディレクトリのファイルを選択するには、フィルタ式を指定します。例えば、ディレクトリから PDF ファイルのみをアップロードするには、"*.pdf" フィルタ式を指定します。

ディレクトリからファイルをアップロードする場合は、結果のオブジェクトのキー名を指定しません。キー名は、元のファイルパスを使用して Amazon S3 で作成されます。例えば、以下の構造の c:\myfolder ディレクトリがあるとします。

Example

```
C:\myfolder
      \a.txt
      \b.pdf
      \media\
             An.mp3
```

このディレクトリをアップロードすると、Amazon S3 では次のキー名が使用されます。

Example

```
a.txt
b.pdf
media/An.mp3
```

Example

以下の C# コード例では、ディレクトリを Amazon S3 バケットにアップロードしています。さまざまな TransferUtility.UploadDirectory オーバーロードを使用してディレクトリをアップ

ロードする方法を示します。後続のアップロード呼び出しが行われるたびに、前のアップロードが置き換えられます。コード例を設定および実行する方法の詳細については、「AWS SDK for .NET デベロッパーガイド」の「AWS SDK for .NET の開始方法」を参照してください。

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Transfer;
using System;
using System.IO;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class UploadDirMPUHighLevelAPITest
    {
        private const string existingBucketName = "*** bucket name ***";
        private const string directoryPath = @"*** directory path ***";
        // The example uploads only .txt files.
        private const string wildCard = "*.txt";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion = RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;
        static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            UploadDirAsync().Wait();
        }

        private static async Task UploadDirAsync()
        {
            try
            {
                var directoryTransferUtility =
                    new TransferUtility(s3Client);

                // 1. Upload a directory.
                await directoryTransferUtility.UploadDirectoryAsync(directoryPath,
                    existingBucketName);
                Console.WriteLine("Upload statement 1 completed");

                // 2. Upload only the .txt files from a directory
                //    and search recursively.
                await directoryTransferUtility.UploadDirectoryAsync(
```

```
                                            directoryPath,
                                            existingBucketName,
                                            wildCard,
                                            SearchOption.AllDirectories);
                Console.WriteLine("Upload statement 2 completed");

                // 3. The same as Step 2 and some optional configuration.
                //    Search recursively for .txt files to upload.
                var request = new TransferUtilityUploadDirectoryRequest
                {
                    BucketName = existingBucketName,
                    Directory = directoryPath,
                    SearchOption = SearchOption.AllDirectories,
                    SearchPattern = wildCard
                };

                await directoryTransferUtility.UploadDirectoryAsync(request);
                Console.WriteLine("Upload statement 3 completed");
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine(
                        "Error encountered ***. Message:'{0}' when writing an object",
 e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine(
                    "Unknown encountered on server. Message:'{0}' when writing an
 object", e.Message);
            }
        }
    }
}
```

マルチパートアップロードのリスト化

AWS CLI、REST API、AWS SDK を使用して、Amazon S3 で進行中のマルチパートアップロードのリストを取得できます。マルチパートアップロードを使用して、プログラムで 1 つのオブジェクトを Amazon S3 にアップロードできます。マルチパートアップロードでは、オブジェクトのデータの一部を一度に移動することで、オブジェクトを Amazon S3 に移動させます。マルチパートアップ

ロードに関する一般的な情報については、「Amazon S3 でのマルチパートアップロードを使用したオブジェクトのアップロードとコピー」を参照してください。

マルチパートアップロードで追加のチェックサムを含むオブジェクトをアップロードするエンドツーエンドの手順については、「チュートリアル: マルチパートアップロードでオブジェクトをアップロードして、データ整合性を検証する」を参照してください。

次のセクションでは、AWS Command Line Interface、Amazon S3 REST API、および AWS SDK を使用して、進行中のマルチパートアップロードを一覧表示する方法を示します。

AWS CLI を使用したマルチパートアップロードのリスト化

マルチパートアップロードのオペレーションについては、AWS Command Line Interface の以下のセクションを参照してください。

- list-parts - 特定のマルチパートアップロードでアップロードされた部分を一覧表示します。
- list-multipart-uploads - 進行中のマルチパートアップロードを一覧表示します。

REST API を使用したマルチパートアップロードのリスト化

Amazon Simple Storage Service API リファレンスの以下のセクションでは、マルチパートアップロードをリスト化するための REST API について説明します。

- ListParts - 特定のマルチパートアップロードでアップロードされた部分を一覧表示します。
- ListMultipartUploads - 進行中のマルチパートアップロードを一覧表示します。

AWS SDK (低レベル API) を使用したマルチパートアップロードのリスト化

Java

以下のタスクは、低レベル Java クラスを使用して、バケットで進行中のすべてのマルチパートアップロードをリストする手順を示しています。

低レベル API のマルチパートアップロードのリスト化プロセス

1	`ListMultipartUploadsRequest` クラスのインスタンスを作成し、バケット名を指定します。

2	AmazonS3Client.listMultipartUploads メソッドを実行します。このメソッドは、進行中のマルチパートアップロードに関する情報を提供する MultipartUploadListing クラスのインスタンスを返します。

以下の Java コード例は、前述のタスクの例です。

Example

```
ListMultipartUploadsRequest allMultpartUploadsRequest =
     new ListMultipartUploadsRequest(existingBucketName);
MultipartUploadListing multipartUploadListing =
     s3Client.listMultipartUploads(allMultpartUploadsRequest);
```

.NET

特定のバケットですべての進行中のマルチパートアップロードを一覧表示するには、SDK for .NET の低レベルのマルチパートアップロード API の ListMultipartUploadsRequest クラスを使用します。AmazonS3Client.ListMultipartUploads メソッドは、ListMultipartUploadsResponse クラスのインスタンスを返し、進行中のマルチパートアップロードに関する情報を提供します。

進行中のマルチパートアップロードとは、マルチパートアップロードの開始リクエストによって開始されてから、まだ完了または中止されていないマルチパートアップロードです。Amazon S3 マルチパートアップロードの詳細については、Amazon S3 でのマルチパートアップロードを使用したオブジェクトのアップロードとコピー を参照してください。

次の C# の例では、SDK for .NET を使用してバケットで進行中のマルチパートアップロードを一覧表示する方法を示します。コード例を設定および実行する方法の詳細については、「AWS SDK for .NET デベロッパーガイド」の「AWS SDK for .NET の開始方法」 を参照してください。

```
ListMultipartUploadsRequest request = new ListMultipartUploadsRequest
{
  BucketName = bucketName // Bucket receiving the uploads.
};

ListMultipartUploadsResponse response = await
 AmazonS3Client.ListMultipartUploadsAsync(request);
```

PHP

このトピックでは、バージョン 3 の AWS SDK for PHP の低レベル API クラスを使用して、バケットで進行中のすべてのマルチパートアップロードを一覧表示する方法を示します。AWS SDK for Ruby API の詳細については、AWS SDK for Ruby - バージョン 2 を参照してください。

次の PHP の例では、バケットで進行中のすべてのマルチパートアップロードを一覧表示します。

```
 require 'vendor/autoload.php';

use Aws\S3\S3Client;

$bucket = '*** Your Bucket Name ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

// Retrieve a list of the current multipart uploads.
$result = $s3->listMultipartUploads([
    'Bucket' => $bucket
]);

// Write the list of uploads to the page.
print_r($result->toArray());
```

AWS SDK を使用したマルチパートアップロードの追跡

リッスンインターフェイスを使用して、オブジェクトの Amazon S3 へのアップロードの進行状況を追跡できます。高レベルのマルチパートアップロード API は、`ProgressListener` と呼ばれるリッスンインターフェイスを提供します。進行状況に関するイベントが定期的に発生し、バイトが転送されたことをリスナーに通知します。マルチパートアップロードに関する一般的な情報については、「Amazon S3 でのマルチパートアップロードを使用したオブジェクトのアップロードとコピー」を参照してください。

マルチパートアップロードで追加のチェックサムを含むオブジェクトをアップロードするエンドツーエンドの手順については、「チュートリアル: マルチパートアップロードでオブジェクトをアップロードして、データ整合性を検証する」を参照してください。

次のセクションでは、AWS SDK を使用してマルチパートアップロードを追跡する方法を示します。

Java

Example

```
TransferManager tm = new TransferManager(new ProfileCredentialsProvider());

PutObjectRequest request = new PutObjectRequest(
    existingBucketName, keyName, new File(filePath));

// Subscribe to the event and provide event handler.
request.setProgressListener(new ProgressListener() {
   public void progressChanged(ProgressEvent event) {
    System.out.println("Transferred bytes: " +
      event.getBytesTransfered());
            }
});
```

Example

以下の Java コードは、ファイルをアップロードし、ProgressListener を使用してアップロードの進行状況を追跡します。作業サンプルの作成方法およびテスト方法については、「AWS SDK for Java のデベロッパーガイド」の「使用開始」を参照してください。

```
import java.io.File;

import com.amazonaws.AmazonClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.event.ProgressEvent;
import com.amazonaws.event.ProgressListener;
import com.amazonaws.services.s3.model.PutObjectRequest;
import com.amazonaws.services.s3.transfer.TransferManager;
import com.amazonaws.services.s3.transfer.Upload;

public class TrackMPUProgressUsingHighLevelAPI {

    public static void main(String[] args) throws Exception {
        String existingBucketName = "*** Provide bucket name ***";
        String keyName            = "*** Provide object key ***";
        String filePath           = "*** file to upload ***";
```

```
        TransferManager tm = new TransferManager(new ProfileCredentialsProvider());


        // For more advanced uploads, you can create a request object
        // and supply additional request parameters (ex: progress listeners,
        // canned ACLs, etc.)
        PutObjectRequest request = new PutObjectRequest(
          existingBucketName, keyName, new File(filePath));

        // You can ask the upload for its progress, or you can
        // add a ProgressListener to your request to receive notifications
        // when bytes are transferred.
        request.setGeneralProgressListener(new ProgressListener() {
   @Override
   public void progressChanged(ProgressEvent progressEvent) {
    System.out.println("Transferred bytes: " +
      progressEvent.getBytesTransferred());
   }
  });

        // TransferManager processes all transfers asynchronously,
        // so this call will return immediately.
        Upload upload = tm.upload(request);

        try {
         // You can block and wait for the upload to finish
         upload.waitForCompletion();
        } catch (AmazonClientException amazonClientException) {
         System.out.println("Unable to upload file, upload aborted.");
         amazonClientException.printStackTrace();
        }
    }
}
```

.NET

次の C# の例では、TransferUtility クラスを使用して S3 バケットにファイルをアップロードし、アップロードの進行状況を追跡します。コード例を設定および実行する方法の詳細については、「AWS SDK for .NET デベロッパーガイド」の「AWS SDK for .NET の開始方法」 を参照してください。

```
using Amazon;
using Amazon.S3;
```

```
using Amazon.S3.Transfer;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class TrackMPUUsingHighLevelAPITest
    {
        private const string bucketName = "*** provide the bucket name ***";
        private const string keyName = "*** provide the name for the uploaded object
 ***";
        private const string filePath = " *** provide the full path name of the file
 to upload **";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;


        public static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            TrackMPUAsync().Wait();
        }

        private static async Task TrackMPUAsync()
        {
            try
            {
                var fileTransferUtility = new TransferUtility(s3Client);

                // Use TransferUtilityUploadRequest to configure options.
                // In this example we subscribe to an event.
                var uploadRequest =
                    new TransferUtilityUploadRequest
                    {
                        BucketName = bucketName,
                        FilePath = filePath,
                        Key = keyName
                    };

                uploadRequest.UploadProgressEvent +=
                    new EventHandler<UploadProgressArgs>
                        (uploadRequest_UploadPartProgressEvent);
```

```
                await fileTransferUtility.UploadAsync(uploadRequest);
                Console.WriteLine("Upload completed");
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
        }

        static void uploadRequest_UploadPartProgressEvent(object sender,
 UploadProgressArgs e)
        {
            // Process event.
            Console.WriteLine("{0}/{1}", e.TransferredBytes, e.TotalBytes);
        }
    }
}
```

マルチパートアップロードの中止

マルチパートアップロードを開始したら、パートをアップロードし始めます。Amazon S3 はこれらのパートを保存し、すべてのパートをアップロードしてマルチパートアップロードを完了するリクエストを送信した後にのみオブジェクトを作成します。マルチパートアップロードの完了リクエストを受け取ると、Amazon S3 はパートを組み立ててオブジェクトを作成します。マルチパートアップロードの完了リクエストが正常に送信されなかった場合、S3 はパートを組み立てず、オブジェクトも作成しません。パートのアップロード後にマルチパートアップロードを完了しない場合は、マルチパートアップロードを中止する必要があります。

アップロードされたパートに関連のあるすべてのストレージに対して料金が請求されます。常にマルチパートアップロードを完了させるか、マルチパートアップロードを停止してアップロードされたパートを削除することをお勧めします。料金の詳細については、「マルチパートアップロードと料金」を参照してください。

バケットライフサイクル設定を使用して、完了しないマルチパートアップロードを中止することもできます。詳細については、「不完全なマルチパートアップロードを削除するためのバケットライフサイクル設定の設定」を参照してください。

次のセクションでは、AWS Command Line Interface、REST API、および AWS SDK を使用して、Amazon S3 で進行中のマルチパートアップロードを停止する方法を示します。

AWS CLI を使用する場合

AWS CLI を使用してマルチパートアップロードを中止する方法の詳細については、AWS CLI コマンドリファレンスの abort-multipart-upload を参照してください。

REST API の使用

REST API を使用してマルチパートアップロードを中止する方法の詳細については、Amazon Simple Storage Service API リファレンスの AbortMultiPartUpload を参照してください。

AWS SDK (高レベル API) の使用

Java

`TransferManager` クラスは、進行中のマルチパートアップロードを中止する `abortMultipartUploads` メソッドを提供します。アップロードを開始すると、そのアップロードを完了または中止するまで進行中とみなされます。`Date` 値を指定すると、この API が、そのバケットで指定した `Date` の前に開始された進行中のすべてのマルチパートアップロードを中止します。

以下のタスクでは、高レベル Java クラスを使用してマルチパートアップロードを中止する手順を説明します。

高レベル API のマルチパートアップロード中止プロセス

1	`TransferManager` クラスのインスタンスを作成します。
2	バケット名および `TransferManager.abortMultipartUploads` 値を渡して `Date` メソッドを実行します。

次の Java コードでは、1 週間以上前に特定のバケットで開始された進行中のマルチパートアップロードをすべて中止します。作業サンプルの作成方法およびテスト方法については、「AWS SDK for Java のデベロッパーガイド」の「使用開始」を参照してください。

```
import java.util.Date;

import com.amazonaws.AmazonClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3.transfer.TransferManager;

public class AbortMPUUsingHighLevelAPI {

    public static void main(String[] args) throws Exception {
        String existingBucketName = "*** Provide existing bucket name ***";

        TransferManager tm = new TransferManager(new ProfileCredentialsProvider());


        int sevenDays = 1000 * 60 * 60 * 24 * 7;
  Date oneWeekAgo = new Date(System.currentTimeMillis() - sevenDays);

        try {
         tm.abortMultipartUploads(existingBucketName, oneWeekAgo);
        } catch (AmazonClientException amazonClientException) {
         System.out.println("Unable to upload file, upload was aborted.");
         amazonClientException.printStackTrace();
        }
    }
}
```

> **Note**
>
> 特定のマルチパートアップロードを中止することもできます。詳細については、AWS SDK の使用 (低レベル API) を参照してください。

.NET

次の C# の例では、1 週間以上前に特定のバケットで開始された進行中のマルチパートアップロードをすべて中止します。コード例を設定および実行する方法の詳細については、「AWS SDK for .NET デベロッパーガイド」の「AWS SDK for .NET の開始方法」 を参照してください。

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Transfer;
using System;
```

```
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class AbortMPUUsingHighLevelAPITest
    {
        private const string bucketName = "*** provide bucket name ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;

        public static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            AbortMPUAsync().Wait();
        }

        private static async Task AbortMPUAsync()
        {
            try
            {
                var transferUtility = new TransferUtility(s3Client);

                // Abort all in-progress uploads initiated before the specified
 date.
                await transferUtility.AbortMultipartUploadsAsync(
                    bucketName, DateTime.Now.AddDays(-7));
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
        }
    }
}
```

> **Note**
>
> 特定のマルチパートアップロードを中止することもできます。詳細については、AWS SDK の使用 (低レベル API) を参照してください。

AWS SDK の使用 (低レベル API)

`AmazonS3.abortMultipartUpload` メソッドを呼び出すと、進行中のマルチパートアップロードを中止できます。このメソッドは、Amazon S3 にアップロードされたすべてのパートを削除し、リソースを解放します。アップロード ID、バケット名、およびキー名を指定する必要があります。以下の Java コードの例では、進行中のマルチパートアップロードを中止する方法を示します。

マルチパートアップロードを中止するには、アップロード ID とアップロードで使用しているバケット名とキー名を指定します。マルチパートアップロードを中止した後は、同じアップロード ID を使用して追加のパートをアップロードすることはできません。Amazon S3 マルチパートアップロードの詳細については、Amazon S3 でのマルチパートアップロードを使用したオブジェクトのアップロードとコピー を参照してください。

Java

次の Java コード例では、進行中のマルチパートアップロードを中止します。

Example

```
InitiateMultipartUploadRequest initRequest =
    new InitiateMultipartUploadRequest(existingBucketName, keyName);
InitiateMultipartUploadResult initResponse =
               s3Client.initiateMultipartUpload(initRequest);

AmazonS3 s3Client = new AmazonS3Client(new ProfileCredentialsProvider());
s3Client.abortMultipartUpload(new AbortMultipartUploadRequest(
            existingBucketName, keyName, initResponse.getUploadId()));
```

> **Note**
>
> 特定のマルチパートアップロードではなく、特定の時刻より前に開始された進行中のマルチパートアップロードをすべて中止することができます。このクリーンアップオペレーションは、開始したが完了または中止していない古いマルチパートアップロードを中止す

る場合に役に立ちます。詳細については、AWS SDK (高レベル API) の使用 を参照してください。

.NET

次の C# の例は、マルチパートアップロードを中止する方法を示しています。次のコードを含む完全な C# のサンプルについては、AWS SDK の使用 (低レベル API) を参照してください。

```
AbortMultipartUploadRequest abortMPURequest = new AbortMultipartUploadRequest
{
    BucketName = existingBucketName,
    Key = keyName,
    UploadId = initResponse.UploadId
};
await AmazonS3Client.AbortMultipartUploadAsync(abortMPURequest);
```

特定の時刻までに開始されたすべての進行中のマルチパートアップロードを中止することもできます。このクリーンアップオペレーションは、完了または中止していないマルチパートアップロードを中止する場合に役立ちます。詳細については、AWS SDK (高レベル API) の使用 を参照してください。

PHP

この例では、バージョン 3 の AWS SDK for PHP のクラスを使用して、進行中のマルチパートアップロードを中止する方法を示します。AWS SDK for Ruby API の詳細については、AWS SDK for Ruby - バージョン 2 を参照してください。`abortMultipartUpload()` メソッドの例です。

AWS SDK for Ruby API の詳細については、AWS SDK for Ruby - バージョン 2 を参照してください。

```
 require 'vendor/autoload.php';

use Aws\S3\S3Client;

$bucket = '*** Your Bucket Name ***';
$keyname = '*** Your Object Key ***';
$uploadId = '*** Upload ID of upload to Abort ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
```

```
]);

// Abort the multipart upload.
$s3->abortMultipartUpload([
    'Bucket'   => $bucket,
    'Key'      => $keyname,
    'UploadId' => $uploadId,
]);
```

マルチパートアップロードを使用したオブジェクトのコピー

マルチパートアップロードを使用すると、オブジェクトをパートのセットとしてコピーすることができます。このセクションの例は、Multipart Upload API を使用して 5 GB よりも大きいオブジェクトをコピーする方法を示しています。マルチパートアップロードの詳細については、「Amazon S3 でのマルチパートアップロードを使用したオブジェクトのアップロードとコピー」を参照してください。

マルチパートアップロード API を使用せずに、1 回のオペレーションで 5 GB 未満のオブジェクトをコピーできます。AWS Management Console、AWS CLI、REST API、または AWS SDK を使用して、5 GB 未満のオブジェクトをコピーできます。詳細については、「オブジェクトのコピー、移動、名前の変更」を参照してください。

マルチパートアップロードで追加のチェックサムを含むオブジェクトをアップロードするエンドツーエンドの手順については、「チュートリアル: マルチパートアップロードでオブジェクトをアップロードして、データ整合性を検証する」を参照してください。

次のセクションでは、REST API または AWS SDK を使用してマルチパートアップロードでオブジェクトをコピーする方法を示します。

REST API の使用

Amazon Simple Storage Service API リファレンスの以下のセクションでは、マルチパートアップロードの REST API について説明しています。既存のオブジェクトをコピーするには、UploadPart (Copy) API を使用し、リクエストに `x-amz-copy-source` リクエストヘッダーを追加してコピー元オブジェクトを指定します。

- Initiate Multipart Upload
- Upload Part
- Upload Part (Copy)

- Complete Multipart Upload
- マルチパートアップロードの中止
- パートのリスト
- マルチパートアップロードのリスト

これらの API を使用して独自の REST リクエストを作成するか、提供されている SDK のいずれかを使用できます。AWS CLI でマルチパートアップロードを使用する方法の詳細については、AWS CLI を使用する場合 を参照してください。SDK の詳細については、「マルチパートアップロードの AWS SDK サポート」を参照してください。

AWS SDK の使用

低レベル API を使用してオブジェクトをコピーするには、次の手順を実行します。

- `AmazonS3Client.initiateMultipartUpload()` メソッドを呼び出して、マルチパートアップロードを開始します。
- `AmazonS3Client.initiateMultipartUpload()` メソッドから返されたレスポンスオブジェクトのアップロード ID を保存します。このアップロード ID は、パートのアップロードオペレーションごとに指定します。
- すべてのパートをコピーします。コピーする必要があるパートごとに、`CopyPartRequest` クラスの新しいインスタンスを作成します。パート情報として、送信元と送信先のバケット名、送信元と送信先のオブジェクトキー、アップロード ID、パートの最初と最後のバイトの場所、パート番号などを指定します。
- `AmazonS3Client.copyPart()` メソッド呼び出しのレスポンスを保存します。各レスポンスには、アップロードしたパートの `ETag` 値とパート番号が含まれています。この情報は、マルチパートアップロードを完了するために必要です。
- `AmazonS3Client.completeMultipartUpload()` メソッドを呼び出してコピーオペレーションを完了します。

Java

Example

次の例では、Amazon S3 の下位 Java API を使用してマルチパートコピーを実行する方法を示します。作業サンプルの作成およびテストの手順については、「AWS SDK for Java のデベロッパーガイド」の「使用開始」を参照してください。

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.*;

import java.io.IOException;
import java.util.ArrayList;
import java.util.List;

public class LowLevelMultipartCopy {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String sourceBucketName = "*** Source bucket name ***";
        String sourceObjectKey = "*** Source object key ***";
        String destBucketName = "*** Target bucket name ***";
        String destObjectKey = "*** Target object key ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();

            // Initiate the multipart upload.
            InitiateMultipartUploadRequest initRequest = new
 InitiateMultipartUploadRequest(destBucketName,
                    destObjectKey);
            InitiateMultipartUploadResult initResult =
 s3Client.initiateMultipartUpload(initRequest);

            // Get the object size to track the end of the copy operation.
            GetObjectMetadataRequest metadataRequest = new
 GetObjectMetadataRequest(sourceBucketName, sourceObjectKey);
            ObjectMetadata metadataResult =
 s3Client.getObjectMetadata(metadataRequest);
            long objectSize = metadataResult.getContentLength();

            // Copy the object using 5 MB parts.
```

```
            long partSize = 5 * 1024 * 1024;
            long bytePosition = 0;
            int partNum = 1;
            List<CopyPartResult> copyResponses = new ArrayList<CopyPartResult>();
            while (bytePosition < objectSize) {
                // The last part might be smaller than partSize, so check to make
sure
                // that lastByte isn't beyond the end of the object.
                long lastByte = Math.min(bytePosition + partSize - 1, objectSize -
1);

                // Copy this part.
                CopyPartRequest copyRequest = new CopyPartRequest()
                        .withSourceBucketName(sourceBucketName)
                        .withSourceKey(sourceObjectKey)
                        .withDestinationBucketName(destBucketName)
                        .withDestinationKey(destObjectKey)
                        .withUploadId(initResult.getUploadId())
                        .withFirstByte(bytePosition)
                        .withLastByte(lastByte)
                        .withPartNumber(partNum++);
                copyResponses.add(s3Client.copyPart(copyRequest));
                bytePosition += partSize;
            }

            // Complete the upload request to concatenate all uploaded parts and
make the
            // copied object available.
            CompleteMultipartUploadRequest completeRequest = new
CompleteMultipartUploadRequest(
                    destBucketName,
                    destObjectKey,
                    initResult.getUploadId(),
                    getETags(copyResponses));
            s3Client.completeMultipartUpload(completeRequest);
            System.out.println("Multipart copy complete.");
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
```

```
        }
    }

    // This is a helper function to construct a list of ETags.
    private static List<PartETag> getETags(List<CopyPartResult> responses) {
        List<PartETag> etags = new ArrayList<PartETag>();
        for (CopyPartResult response : responses) {
            etags.add(new PartETag(response.getPartNumber(), response.getETag()));
        }
        return etags;
    }
}
```

.NET

次の C# の例では、SDK for .NET を使用して 5 GB を超える Amazon S3 オブジェクトをコピー元からコピー先 (あるバケットから別のバケットなど) にコピーする方法を示します。5 GB 未満のオブジェクトをコピーするには、1 回のオペレーションでコピーする手順を使用します (AWS SDK の使用 を参照)。Amazon S3 マルチパートアップロードの詳細については、Amazon S3 でのマルチパートアップロードを使用したオブジェクトのアップロードとコピー を参照してください。

この例では、SDK for .NET マルチパートアップロード API を使用して、5 GB を超える Amazon S3 オブジェクトを S3 バケットから別のバケットにコピーする方法を示します。

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Collections.Generic;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class CopyObjectUsingMPUapiTest
    {
        private const string sourceBucket = "*** provide the name of the bucket with
 source object ***";
        private const string targetBucket = "*** provide the name of the bucket to
 copy the object to ***";
        private const string sourceObjectKey = "*** provide the name of object to
 copy ***";
```

```
        private const string targetObjectKey = "*** provide the name of the object
copy ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;

        public static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            Console.WriteLine("Copying an object");
            MPUCopyObjectAsync().Wait();
        }
        private static async Task MPUCopyObjectAsync()
        {
            // Create a list to store the upload part responses.
            List<UploadPartResponse> uploadResponses = new
List<UploadPartResponse>();
            List<CopyPartResponse> copyResponses = new List<CopyPartResponse>();

            // Setup information required to initiate the multipart upload.
            InitiateMultipartUploadRequest initiateRequest =
                new InitiateMultipartUploadRequest
                {
                    BucketName = targetBucket,
                    Key = targetObjectKey
                };

            // Initiate the upload.
            InitiateMultipartUploadResponse initResponse =
                await s3Client.InitiateMultipartUploadAsync(initiateRequest);

            // Save the upload ID.
            String uploadId = initResponse.UploadId;

            try
            {
                // Get the size of the object.
                GetObjectMetadataRequest metadataRequest = new
GetObjectMetadataRequest
                {
                    BucketName = sourceBucket,
                    Key = sourceObjectKey
                };
```

```
                GetObjectMetadataResponse metadataResponse =
                    await s3Client.GetObjectMetadataAsync(metadataRequest);
                long objectSize = metadataResponse.ContentLength; // Length in
bytes.

                // Copy the parts.
                long partSize = 5 * (long)Math.Pow(2, 20); // Part size is 5 MB.

                long bytePosition = 0;
                for (int i = 1; bytePosition < objectSize; i++)
                {
                    CopyPartRequest copyRequest = new CopyPartRequest
                    {
                        DestinationBucket = targetBucket,
                        DestinationKey = targetObjectKey,
                        SourceBucket = sourceBucket,
                        SourceKey = sourceObjectKey,
                        UploadId = uploadId,
                        FirstByte = bytePosition,
                        LastByte = bytePosition + partSize - 1 >= objectSize ?
objectSize - 1 : bytePosition + partSize - 1,
                        PartNumber = i
                    };

                    copyResponses.Add(await s3Client.CopyPartAsync(copyRequest));

                    bytePosition += partSize;
                }

                // Set up to complete the copy.
                CompleteMultipartUploadRequest completeRequest =
                new CompleteMultipartUploadRequest
                {
                    BucketName = targetBucket,
                    Key = targetObjectKey,
                    UploadId = initResponse.UploadId
                };
                completeRequest.AddPartETags(copyResponses);

                // Complete the copy.
                CompleteMultipartUploadResponse completeUploadResponse =
                    await s3Client.CompleteMultipartUploadAsync(completeRequest);
            }
```

```
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
        }
    }
}
```

チュートリアル: マルチパートアップロードでオブジェクトをアップロードして、データ整合性を検証する

マルチパートアップロードを使用すると、単一のオブジェクトをパートのセットとしてアップロードすることができます。各パートは、オブジェクトのデータの連続する部分です。これらのオブジェクトパートは、任意の順序で個別にアップロードできます。いずれかのパートの送信が失敗すると、他のパートに影響を与えることなくそのパートを再送することができます。オブジェクトのすべてのパートがアップロードされたら、Amazon S3 はこれらのパートを組み立ててオブジェクトを作成します。通常、オブジェクトサイズが 100 MB 以上の場合は、単一のオペレーションでオブジェクトをアップロードする代わりに、マルチパートアップロードを使用することを考慮してください。マルチパートアップロードの詳細については、「Amazon S3 でのマルチパートアップロードを使用したオブジェクトのアップロードとコピー」を参照してください。マルチパートアップロードに関する制限については、「Amazon S3 マルチパートアップロードの制限」を参照してください。

チェックサムを使用して、コピー時にアセットが変更されていないことを確認できます。チェックサムを実行するには、アルゴリズムを使用してファイル内のバイトごとに順番に反復処理を行います。Amazon S3 は、データの整合性をチェックするための複数のチェックサムオプションを提供しています。耐久性のベストプラクティスとして、このような整合性チェックを実行し、すべてのバイトが変更されずに転送されることを確認することをお勧めします。Amazon S3 は、SHA-1、SHA-256、CRC32、CRC32C のアルゴリズムもサポートしています。Amazon S3 は、このようなアルゴリズムの 1 つまたは複数使用して、追加のチェックサム値を計算し、オブジェクトメタデータの一部として保存します。チェックサムの詳細については、「Amazon S3 でのオブジェクトの整合性のチェック」を参照してください。

目的

このチュートリアルでは、AWS コマンドラインインターフェイス (AWS CLI) を介してマルチパートアップロードと追加の SHA-256 チェックサムを使って、オブジェクトを Amazon S3 にアップロードする方法を説明します。アップロードしたオブジェクトの MD5 ハッシュと SHA-256 チェックサムを計算することで、オブジェクトのデータ整合性を確認する方法についても説明します。

トピック

- 前提条件
- ステップ 1: サイズが大きいファイルを作成する
- ステップ 2: ファイルを複数のファイルに分割する
- ステップ 3: 追加のチェックサムを使用してマルチパートアップロードを作成する
- ステップ 4: マルチパートアップロードのパートをアップロードする
- ステップ 5: マルチパートアップロードのすべてのパートを一覧表示する
- ステップ 6: マルチアップロードを完了する
- ステップ 7: オブジェクトがバケットにアップロードされていることを確認する
- ステップ 8: MD5 チェックサムを使用してオブジェクトの整合性を検証する
- ステップ 9: 追加のチェックサムを使用してオブジェクトの整合性を検証する
- ステップ 10: リソースをクリーンアップする

前提条件

- このチュートリアルを開始する前に、アップロード先の Amazon S3 バケットにアクセスできることを確認してください。詳細については、「汎用バケットの作成」を参照してください。
- AWS CLI がインストールされて、設定されている必要があります。AWS CLI をまだインストールしていない場合は、「AWS Command Line Interface ユーザーガイド」の「AWS CLI の最新バージョンをインストールまたは更新する」を参照してください。
- 別の方法として、AWS CloudShell を使用してコンソールから AWS CLI コマンドを実行することもできます。AWS CloudShell は、AWS Management Consoleから直接起動できる、ブラウザベースの事前認証済みシェルです。詳細については、「AWS CloudShell ユーザーガイド」の「CloudShell とは」と「AWS CloudShell の使用開始」を参照してください。

ステップ 1: サイズが大きいファイルを作成する

アップロードするファイルが既にある場合は、このチュートリアルでそのファイルを使用できます。ない場合は、次の手順で 15 MB のファイルを作成します。マルチパートアップロードに関する制限については、「Amazon S3 マルチパートアップロードの制限」を参照してください。

サイズが大きいファイルを作成するには

使用しているオペレーティングシステムに応じて、次のいずれかのコマンドを使用してファイルを作成します。

Linux または macOS

15 MB のファイルを作成するには、ローカルターミナルを開いて、次のコマンドを実行します。

```
dd if=/dev/urandom of=census-data.bin bs=1M count=15
```

このコマンドは、ランダムなバイトが入力された、サイズが 15 MB の census-data.bin という名前のファイルを作成します。

Windows

15 MB のファイルを作成するには、ローカルターミナルを開いて、次のコマンドを実行します。

```
fsutil file createnew census-data.bin 15728640
```

このコマンドは、サイズが 15 MB (15,728,640 バイト) の任意のデータが入力された、census-data.bin という名前のファイルを作成します。

ステップ 2: ファイルを複数のファイルに分割する

マルチパートアップロードを実行するには、サイズの大きいファイルを小さいサイズのパートに分割する必要があります。その後、マルチパートアップロードプロセスを使用して、小さいサイズのパートをアップロードできます。このステップでは、ステップ 1 で作成したサイズの大きいファイルを小さいパートに分割する方法を説明します。次の例では、census-data.bin という名前の 15 MB のファイルを使用します。

サイズの大きいファイルをパートに分割するには

Linux または macOS

サイズの大きいファイルを 5 MB のパートに分割するには、split コマンドを使用します。ターミナルを開いて、次のコマンドを実行します。

```
split -b 5M -d census-data.bin census-part
```

このコマンドは、census-data.bin を census-part** という名前の 5 MB のパートに分割します。** は 00 から始まる数値のサフィックスです。

Windows

サイズの大きいファイルを分割するには、PowerShell を使用します。PowerShell を開いて、次のスクリプトを実行します。

```


$inputFile = "census-data.bin"
$outputFilePrefix = "census-part"
$chunkSize = 5MB

$fs = [System.IO.File]::OpenRead($inputFile)
$buffer = New-Object byte[] $chunkSize
$fileNumber = 0

while ($fs.Position -lt $fs.Length) {
$bytesRead = $fs.Read($buffer, 0, $chunkSize)
$outputFile = "{0}{1:D2}" -f $outputFilePrefix, $fileNumber
$fileStream = [System.IO.File]::Create($outputFile)
$fileStream.Write($buffer, 0, $bytesRead)
$fileStream.Close()
$fileNumber++
}

$fs.Close()
```

この PowerShell スクリプトは、サイズの大きいファイルを 5 MB のチャンクで読み取り、各チャンクを数値のサフィックス付きの新しいファイルに書き込みます。

適切なコマンドを実行後、コマンドを実行したディレクトリに複数のパートがあるのを確認できるはずです。各パートには、次の例のとおり、パート番号に対応するサフィックスが付けられています。

```
census-part00 census-part01 census-part02
```

ステップ 3: 追加のチェックサムを使用してマルチパートアップロードを作成する

マルチパートアップロードプロセスを開始するには、マルチパートアップロードリクエストを作成する必要があります。このステップでは、マルチパートアップロードを開始し、データの整合性に関す

る追加のチェックサムを指定します。次の例では、SHA-256 チェックサムを使用しています。アップロードするオブジェクトの説明となるメタデータを指定する場合は、マルチパートアップロードの開始リクエストの中で指定する必要があります。

> **Note**
>
> このチュートリアルでは、このステップと以降のステップで SHA-256 の追加アルゴリズムを使用します。このようなステップでは、必要に応じて、CRC32、CRC32C、または SHA-1 などの追加のチェックサムを使用できます。別のアルゴリズムを使用する場合は、このチュートリアルのステップ全体で、同じアルゴリズムを使用する必要があります。

マルチパートアップロードを開始するには

ターミナルで、次の `create-multipart-upload` コマンドを使用してバケットのマルチパートアップロードを開始します。*amzn-s3-demo-bucket1* を実際のバケット名に置き換えます。`census_data_file` も選択したファイル名に置き換えます。このファイル名は、アップロードが完了するとオブジェクトキーになります。

```
aws s3api create-multipart-upload --bucket amzn-s3-demo-bucket1 --key
 'census_data_file' --checksum-algorithm sha256
```

リクエストが正常に完了すると、次のような JSON 出力が表示されます。

```
{
    "ServerSideEncryption": "AES256",
    "ChecksumAlgorithm": "SHA256",
    "Bucket": "amzn-s3-demo-bucket1",
    "Key": "census_data_file",
    "UploadId":
 "cNV6KCSNANFZapz1LUGPC5XwUVi1n6yUoIeSP138sNOKPeMhpKQRrbT9k0ePmgoOTCj9K83T4e2Gb5hQvNoNpCKqyb8m3
}
```

> **Note**
>
> リクエストを送信すると、アップロード ID を含むレスポンスが Amazon S3 から返されます。アップロード ID はマルチパートアップロードの一意の識別子です。パートのアップロード、パートのリスト、アップロードの完了、アップロードの停止を行うときは常に、こ

のアップロード ID を指定する必要があります。UploadId、Key、Bucket の値は、後半のステップで使用する必要があるため、必ず保存します。
追加のチェックサムがあるマルチパートアップロードを使用する場合、マルチパート番号には連続するパート番号を使用する必要があります。連続していないパート番号を使用すると、complete-multipart-upload リクエストで HTTP 500 Internal Server Error が発生する可能性があります。

ステップ 4: マルチパートアップロードのパートをアップロードする

このステップでは、マルチパートアップロードのパートを S3 バケットにアップロードします。upload-part コマンドを使用して、各パートを個別にアップロードします。このプロセスでは、アップロード ID、パート番号、パートごとにアップロードするファイルを指定する必要があります。

パートをアップロードするには

1. パートをアップロードする際は、アップロード ID 以外にも、--part-number 引数を使用して、パート番号を指定する必要があります。1 ~ 10,000 の範囲で任意のパート番号を選択できます。パート番号によって、アップロードするオブジェクトに含まれるパートとその位置が一意に識別されます。選択するパート番号は、連続している必要があります (1、2、3 など)。以前にアップロードしたパートと同じパート番号を使って新しいパートをアップロードした場合、以前のパートは上書きされます。
2. upload-part コマンドを使用して、マルチパートアップロードの各パートを個別にアップロードします。--upload-id は、ステップ 3 で create-multipart-upload コマンドを使って作成した出力と同じものです。データの最初のパートをアップロードするには、次のコマンドを使用します。

```
aws s3api upload-part --bucket amzn-s3-demo-bucket1 --key
 'census_data_file' --part-number 1 --body census-part00 --upload-id
 "cNV6KCSNANFZapz1LUGPC5XwUVi1n6yUoIeSP138sNOKPeMhpKQRrbT9k0ePmgoOTCj9K83T4e2Gb5hQvNoNpCKqy
 --checksum-algorithm SHA256
```

各 upload-part コマンドが完了すると、次の例のような出力が表示されるはずです。

```
{
    "ServerSideEncryption": "AES256",
    "ETag": "\"e611693805e812ef37f96c9937605e69\"",
```

```
    "ChecksumSHA256": "QLl8R4i4+SaJlrl8ZIcutc5TbZtwt2NwB8lTXkd3GH0="
}
```

3. 以降のパートについては、順番にパート番号を増分します。

```
aws s3api upload-part --bucket amzn-s3-demo-bucket1 --key 'census_data_file' --
part-number <part-number> --body <file-path> --upload-id "<your-upload-id>" --
checksum-algorithm SHA256
```

例えば、2 番目のパートをアップロードするには、次のコマンドを使用します。

```
aws s3api upload-part --bucket amzn-s3-demo-bucket1 --key
 'census_data_file' --part-number 2 --body census-part01 --upload-id
 "cNV6KCSNANFZapz1LUGPC5XwUVi1n6yUoIeSP138sNOKPeMhpKQRrbT9k0ePmgoOTCj9K83T4e2Gb5hQvNoNpCKqy
 --checksum-algorithm SHA256
```

Amazon S3 は、エンティティタグ (ETag) と、アップロードされた各パートの追加チェックサムをレスポンスのヘッダーとして返します。

4. オブジェクトのすべてのパートのアップロードが完了するまで、upload-part コマンドを引き続き使用します。

ステップ 5: マルチパートアップロードのすべてのパートを一覧表示する

マルチパートアップロードを完了するには、特定のマルチパートアップロードでアップロードされたすべてのパートの一覧が必要です。list-parts コマンドからの出力は、バケット名、キー、アップロード ID、パート番号、ETag、追加のチェックサムなどの情報を提供します。この出力をファイルに保存して、マルチパートアップロードプロセスの完了に向けた次のステップで使用できるようにすると便利です。次の方法を使用して、parts.json という名前の JSON 出力ファイルを作成できます。

すべてのパートを一覧表示するファイルを作成するには

1. アップロードしたすべてのパートの詳細を含む JSON ファイルを生成するには、次の list-parts コマンドを使用します。***amzn-s3-demo-bucket1*** は実際のバケット名、**<your-upload-id>** は、ステップ 3 で取得したアップロード ID に置き換えます。list-parts コマンドの詳細については、「AWS Command Line Interface ユーザーガイド」の「list-parts」を参照してください。

```
aws s3api list-parts --bucket amzn-s3-demo-bucket1 --key 'census_data_file' --
upload-id <your-upload-id> --query '{Parts: Parts[*].{PartNumber: PartNumber, ETag:
 ETag, ChecksumSHA256: ChecksumSHA256}}' --output json > parts.json
```

parts.json という名前の新しいファイルが生成されます。このファイルには、アップロードしたすべてのパートの JSON 形式の情報が含まれています。parts.json ファイルには、マルチパートアップロードプロセスを完了するために必要な、パート番号や対応する ETag 値など、マルチパートアップロードの各パートについての重要な情報が含まれています。

2. 任意のテキストエディタを使用するか、ターミナルで parts.json を開きます。以下は出力の例です。

```
{
    "Parts": [
        {
            "PartNumber": 1,
            "ETag": "\"3c3097f89e2a2fece47ac54b243c9d97\"",
            "ChecksumSHA256": "fTPVHfyNHdv5VkR4S3EewdyioXECv7JBxN+d4FXYYTw="
        },
        {
            "PartNumber": 2,
            "ETag": "\"03c71cc160261b20ab74f6d2c476b450\"",
            "ChecksumSHA256": "VDWTa8enjOvULBAO3W2a6C+5/7ZnNjrnLApa1QVc3FE="
        },
        {
            "PartNumber": 3,
            "ETag": "\"81ae0937404429a97967dffa7eb4affb\"",
            "ChecksumSHA256": "cVVkXehUlzcwrBrXgPIM+EKQXPUvWist8mlUTCs4bg8="
        }
    ]
}
```

ステップ 6: マルチアップロードを完了する

マルチパートアップロードのすべてのパートをアップロードして一覧表示した後の最後のステップは、マルチパートアップロードを完了することです。このステップでは、アップロードしたすべてのパートを S3 バケット内の単一のオブジェクトにマージします。

> **Note**
>
> リクエストに --checksum-sha256 を含めることで、complete-multipart-upload を呼び出す前にオブジェクトのチェックサムを計算できます。チェックサムが一致しない場合、リクエストは Amazon S3 で失敗します。詳細については、AWS Command Line Interface ユーザーガイドの complete-multipart-uploadを参照してください。

マルチパートアップロードを完了するには

マルチパートアップロードを最終化するには、complete-multipart-upload コマンドを使用します。このコマンドには、ステップ 5 で作成した parts.json ファイル、バケット名、アップロード ID が必要です。**<*amzn-s3-demo-bucket1*>** は実際のバケット名、**<your-upload-id>** は parts.json のアップロード ID に置き換えます。

```
aws s3api complete-multipart-upload --multipart-upload file://parts.json --bucket amzn-s3-demo-bucket1 --key 'census_data_file' --upload-id <your-upload-id>
```

以下は出力の例です。

```
{
    "ServerSideEncryption": "AES256",
    "Location": "https://amzn-s3-demo-bucket1.s3.us-east-2.amazonaws.com/census_data_file",
    "Bucket": "amzn-s3-demo-bucket1",
    "Key": "census_data_file",
    "ETag": "\"f453c6dccca969c457efdf9b1361e291-3\"",
    "ChecksumSHA256": "aI8EoktCdotjU8Bq46DrPCxQCGuGcPIhJ51noWs6hvk=-3"
}
```

> **Note**
>
> この時点では、個別のパートファイルの削除は行いません。マージ後のオブジェクトの整合性を検証するためにチェックサムを実行するには、個別のパートが必要です。

ステップ 7: オブジェクトがバケットにアップロードされていることを確認する

マルチパートアップロードが完了したら、オブジェクトが S3 バケットに正常にアップロードされたことを確認できます。バケット内のオブジェクトを一覧表示して、新しくアップロードされたファイルが存在することを確認するには、 `list-objects-v2` コマンドを使用します。

アップロードしたオブジェクトを一覧表示するには

バケット内のオブジェクトを一覧表示するには、`list-objects-v2` コマンドを使用します。次の ***amzn-s3-demo-bucket1*** は、実際のバケット名に置き換えます。

```
aws s3api list-objects-v2 --bucket amzn-s3-demo-bucket1
```

このコマンドは、バケット内のオブジェクトの一覧を返します。オブジェクトの一覧で、アップロードしたファイル (census_data_file など) を検索します。

詳細については、「AWS Command Line Interface ユーザーガイド」の「list-objects-v2 コマンドの例」セクションを参照してください。

ステップ 8: MD5 チェックサムを使用してオブジェクトの整合性を検証する

オブジェクトをアップロードする際に、Amazon S3 が使用するチェックサムのアルゴリズムを指定できます。デフォルトでは、Amazon S3 は複数のバイトの MD5 ダイジェストをオブジェクトの ETag として保存します。マルチパートアップロードの場合、ETag はオブジェクト全体のチェックサムではなく、個別のパートのチェックサムの複合体です。

MD5 チェックサムを使用してオブジェクトの整合性を検証するには

1. アップロードしたオブジェクトの ETag を取得するには、次のとおり `head-object` リクエストを実行します。

   ```
   aws s3api head-object --bucket amzn-s3-demo-bucket1 --key census_data_file
   ```

   以下は出力の例です。

   ```
   {
       "AcceptRanges": "bytes",
       "LastModified": "2024-07-26T19:04:13+00:00",
       "ContentLength": 16106127360,
       "ETag": "\"f453c6dccca969c457efdf9b1361e291-3\"",
   ```

```
    "ContentType": "binary/octet-stream",
    "ServerSideEncryption": "AES256",
    "Metadata": {}
}
```

この ETag の末尾には「-3」が追加されています。これは、このオブジェクトがマルチパートアップロードを使用して 3 つのパートでアップロードされたことを意味します。

2. 次に、md5sum コマンドを使用して各パートの MD5 チェックサムを計算します。パートファイルへの適切なパスを指定する必要があります。

```
md5sum census-part*
```

以下は出力の例です。

```
e611693805e812ef37f96c9937605e69 census-part00
63d2d5da159178785bfd6b6a5c635854 census-part01
95b87c7db852451bb38b3b44a4e6d310 census-part02
```

3. このステップでは、MD5 ハッシュを手動で単一の文字列にまとめます。次に、以下のコマンドを実行して、文字列をバイナリに変換し、バイナリ値の MD5 チェックサムを計算します。

```
echo
 "e611693805e812ef37f96c9937605e6963d2d5da159178785bfd6b6a5c63585495b87c7db852451bb38b3b44a
 | xxd -r -p | md5sum
```

以下は出力の例です。

```
f453c6dccca969c457efdf9b1361e291 -
```

このハッシュ値は、census_data_file オブジェクトの整合性を検証する ステップ 1 の元の ETag 値のハッシュ値と一致する必要があります。

追加のチェックサムを使用するように Amazon S3 に指示すると、Amazon S3 は各パートのチェックサム値を計算し、その値を保存します。マルチパートアップロード処理中の個別のパートのチェックサム値を取得する場合は、list-parts を使用できます。

マルチパートアップロードオブジェクトでのチェックサムの動作の詳細については、「Amazon S3 でのオブジェクトの整合性のチェック」を参照してください。

ステップ 9: 追加のチェックサムを使用してオブジェクトの整合性を検証する

このチュートリアルでは、オブジェクトの整合性を検証するための追加のチェックサムとして、このステップで SHA-256 を使用します。別の追加のチェックサムを使用した場合は、代わりにそのチェックサム値を使用します。

SHA256 チェックサムを使用してオブジェクトの整合性を検証するには

1. ターミナルで --checksum-mode enabled 引数を含む次のコマンドを実行して、オブジェクトの ChecksumSHA256 値を表示します。

```
aws s3api head-object --bucket amzn-s3-demo-bucket1 --key census_data_file --
checksum-mode enabled
```

以下は出力の例です。

```
{
    "AcceptRanges": "bytes",
    "LastModified": "2024-07-26T19:04:13+00:00",
    "ContentLength": 16106127360,
    "ChecksumSHA256": "aI8EoktCdotjU8Bq46DrPCxQCGuGcPIhJ51noWs6hvk=-3",
    "ETag": "\"f453c6dccca969c457efdf9b1361e291-3\"",
    "ContentType": "binary/octet-stream",
    "ServerSideEncryption": "AES256",
    "Metadata": {}
}
```

2. 次のコマンドを使用して、個別のパートの ChecksumSHA256 値を base64 にデコードし、outfile という名前のバイナリファイルに保存します。これらの値は parts.json ファイルにあります。base64 文字列の例を実際の ChecksumSHA256 値に置き換えます。

```
echo "QLl8R4i4+SaJlrl8ZIcutc5TbZtwt2NwB8lTXkd3GH0=" | base64 --decode >> outfile
echo "xCdgs1K5Bm4jWETYw/CmGYr+m6O2DcGfpckx5NVokvE=" | base64 --decode >> outfile
echo "f5wsfsa5bB+yXuwzqG1Bst91uYneqGD3CCidpb54mAo=" | base64 --decode >> outfile
```

3. 次のコマンドを実行して、outfile の SHA256 チェックサムを計算します。

```
sha256sum outfile
```

以下は出力の例です。

```
688f04a24b42768b6353c06ae3a0eb3c2c50086b8670f221279d67a16b3a86f9 outfile
```

次のステップでは、ハッシュ値を取得して、バイナリ値に変換します。このバイナリ値は、ステップ 1 のチェックサムの ChecksumSHA256 値と一致する必要があります。

4. ステップ 3 の SHA256 チェックサムをバイナリに変換し、これを base64 にエンコードして、ステップ 1 の ChecksumSHA256 値と一致することを検証します。

```
echo "688f04a24b42768b6353c06ae3a0eb3c2c50086b8670f221279d67a16b3a86f9" | xxd -r -p
 | base64
```

以下は出力の例です。

```
aI8EoktCdotjU8Bq46DrPCxQCGuGcPIhJ51noWs6hvk=
```

この出力は、base64 出力が head-object コマンド出力からの ChecksumSHA256 値と一致することを確認します。この出力がチェックサム値と一致すれば、このオブジェクトは有効です。

> **Important**
>
> - 追加のチェックサムを使用するように Amazon S3 に指示すると、Amazon S3 は各パートのチェックサム値を計算し、その値を保存します。
> - マルチパートアップロード処理中の個別のパートのチェックサム値を取得する場合は、list-parts コマンドを使用できます。

ステップ 10: リソースをクリーンアップする

このチュートリアルで作成したファイルをクリーンアップする場合は、次の方法を使用します。S3 バケットにアップロードしたファイルを削除する手順については、「Amazon S3 オブジェクトの削除」を参照してください。

ステップ 1 で作成したローカルファイルを削除する:

マルチパートアップロードのために作成したファイルを削除するには、作業ディレクトリから次のコマンドを実行します。

```
rm census-data.bin census-part* outfile parts.json
```

Amazon S3 マルチパートアップロードの制限

マルチパートアップロードを使用すると、単一のオブジェクトをパートのセットとしてアップロードすることができます。各パートは、オブジェクトのデータの連続する部分です。オブジェクトのすべてのパートがアップロードされたら、Amazon S3 はこれらのパートを組み立ててオブジェクトを作成します。通常、オブジェクトサイズが 100 MB 以上の場合は、単一のオペレーションでオブジェクトをアップロードする代わりに、マルチパートアップロードを使用することを考慮してください。マルチパートアップロードの詳細については、「Amazon S3 でのマルチパートアップロードを使用したオブジェクトのアップロードとコピー」を参照してください。

次の表は、マルチパートアップロードの主な仕様をまとめたものです。これには、オブジェクトの最大サイズ、パーツの最大数、パーツの最大サイズなどが含まれます。マルチパートアップロードの最後のパートには、最小サイズの制限はありません。

項目	仕様
最大オブジェクトサイズ	5 TiB
アップロードあたりの最大パート数	10,000
パート番号	1 ~ 10,000
パートサイズ	5 MiB から 5 GiB。マルチパートアップロードの最後のパートには、最小サイズの制限はありません。
パートのリストリクエストで返されるパートの最大数	1,000
マルチパートアップロードのリストリクエストで返されるマルチパートアップロードの最大数	1,000

条件付きリクエストを使用して S3 オペレーションに前提条件を追加する

条件付きリクエストを使用すると、S3 オペレーションに前提条件を追加できます。条件付きリクエストを使用するには、Amazon S3 API オペレーションにヘッダーを追加します。このヘッダーを使用して、条件が満たされないと S3 オペレーションが失敗する条件を指定します。

条件付き読み込みは GET、HEAD、および COPY リクエストでサポートされています。オブジェクトのエンティティタグ (ETag) または最終更新日に基づいてオブジェクトを返すかコピーするための前提条件を追加できます。これにより、S3 オペレーションが、指定した日付以降に更新されたオブジェクトに制限される場合があります。S3 オペレーションを特定の ETag に制限することもできます。これにより、特定のオブジェクトバージョンのみを返すかコピーできます。オブジェクトメタデータの詳細については、オブジェクトメタデータの使用 を参照してください。

条件付き書き込みでは、PUT オペレーション中にバケットに同じキー名を持つ既存のオブジェクトがないことを確認できます。これにより、同じキー名を持つ既存のオブジェクトが上書きされるのを防ぐことができます。同様に、条件付き書き込みを使用して、オブジェクトを更新する前にオブジェクトの ETag が変更されていないかどうかを確認できます。これにより、オブジェクトのコンテンツの状態を知らずに、意図せず上書きすることを防げます。条件付き書き込みは、PutObject または CompleteMultipartUpload リクエストに使用できます。有効なキー名の詳細については、Amazon S3 オブジェクトに命名する を参照してください。

条件付き読み取りまたは条件付き書き込みには追加料金はかかりません。失敗したリクエストも含め、該当するリクエストに対してのみ既存の料金が請求されます。Amazon S3 の機能と料金の詳細については、「Amazon S3 の料金」を参照してください。

トピック

- 条件付き読み取りでメタデータに基づいてオブジェクトを取得またはコピーする方法
- 条件付き書き込みによるオブジェクトの上書きを防ぐ方法

条件付き読み取りでメタデータに基づいてオブジェクトを取得またはコピーする方法

条件付き読み取りでは、S3 オペレーションに前提条件を追加するために、読み取りリクエストにヘッダーを追加できます。これらの前提条件が満たされない場合、読み取りリクエストは失敗します。

GET、HEAD、または COPY リクエストの条件付き読み取りを使用して、メタデータに基づいてのみオブジェクトを返すことができます。

オブジェクトをアップロードすると、Amazon S3 は S3 によってのみ変更できるシステム制御メタデータを作成します。エンティティタグ (ETag) と最終更新日は、システム制御メタデータの例です。オブジェクトの ETag は、オブジェクトの特定のバージョンを表す文字列です。最終更新日は、オブジェクトの作成日または最終更新日のどちらか新しい方を表すメタデータです。

条件付き読み取りを使用すると、オブジェクトの ETag または最終更新日に基づいてオブジェクトを返すことができます。リクエストで ETag 値を指定し、ETag 値が一致する場合にのみオブジェクトを返すことができます。これにより、オブジェクトの特定のバージョンのみを返すかコピーできます。指定した日付以降にオブジェクトが変更されている場合にのみ、読み取りリクエストで最終更新日の値を指定してオブジェクトを返すことができます。

サポートされている API

条件付き読み取りの使用をサポートする S3 API は、次のとおりです。

- GetObject
- HeadObject
- CopyObject

以下のヘッダーを使用して、エンティティタグ (ETag) または最終変更日に基づくオブジェクトを返すことができます。ETag や最終変更日などのオブジェクトメタデータの詳細については、「the section called “システムで定義されたオブジェクトメタデータ”」を参照してください。

GetObject

- `If-Match` — オブジェクトの ETag が指定した値と一致する場合にのみオブジェクトを返します。
- `If-Modified-Since` — 指定された時刻以降に変更されたオブジェクトのみを返します。
- `If-None-Match` — オブジェクトの ETag が指定した値と一致しない場合にのみオブジェクトを返します。
- `If-Unmodified-Since` — 指定された時刻以降に変更されていないオブジェクトのみを返します。

このようなヘッダー、返されるエラー、S3 が単一のリクエストで複数の条件付きヘッダーを処理する順序の詳細については、「Amazon Simple Storage Service API リファレンス」の「GetObject」を参照してください。

HeadObject

- `If-Match` — オブジェクトの ETag が指定した値と一致する場合にのみオブジェクトを返します。
- `If-Modified-Since` — 指定された時刻以降に変更されたオブジェクトのみを返します。
- `If-None-Match` — オブジェクトの ETag が指定した値と一致しない場合にのみオブジェクトを返します。
- `If-Unmodified-Since` — 指定された時刻以降に変更されていないオブジェクトのみを返します。

このようなヘッダー、返されるエラー、S3 が単一のリクエストで複数の条件付きヘッダーを処理する順序の詳細については、「Amazon Simple Storage Service API リファレンス」の「HeadObject」を参照してください。

CopyObject

- `x-amz-copy-source-if-match` — オブジェクトの ETag が指定した値と一致する場合にのみ、ソースオブジェクトをコピーします。
- `x-amz-copy-source-if-modified-since` — 指定された時刻以降に変更されたソースオブジェクトのみをコピーします。
- `x-amz-copy-source-if-none-match` — オブジェクトの ETag が指定した値と一致しない場合にのみソースオブジェクトをコピーします。
- `x-amz-copy-source-if-unmodified-since` — 指定された時刻以降に変更されていないソースオブジェクトのみをコピーします。

このようなヘッダー、返されるエラー、S3 が単一のリクエストで複数の条件付きヘッダーを処理する順序の詳細については、「Amazon Simple Storage Service API リファレンス」の「CopyObject」を参照してください。

条件付き書き込みによるオブジェクトの上書きを防ぐ方法

条件付き書き込みを使用することで、WRITE リクエストにヘッダーを追加して、Amazon S3 オペレーションの前提条件を指定できます。オブジェクトを条件付きで書き込むには、HTTP If-None-Match または If-Match ヘッダーを追加します。

If-None-Match ヘッダーは、バケットに既に同じキー名を持つオブジェクトがないことを検証することで、既存のデータの上書きを防ぎます。

または、If-Match ヘッダーを追加して、オブジェクトを書き込む前にオブジェクトのエンティティタグ (ETag) をチェックすることもできます。このヘッダーを使用すると、Amazon S3 は指定された ETag 値と S3 内のオブジェクトの ETag 値を比較します。ETag 値が一致しない場合、オペレーションは失敗となります。

バケット所有者は、バケットポリシーを使用して、アップロードされたオブジェクトに条件付き書き込みを強制できます。詳細については、「the section called “条件付き書き込みを強制する”」を参照してください。

> **Note**
>
> 条件付き書き込みを使用するには、HTTPS (TLS) 経由でリクエストを行うか、AWS Signature Version 4 を使用してリクエストに署名する必要があります。

トピック

- キー名に基づくオブジェクトの上書きを防ぐ方法
- オブジェクトが変更された場合に上書きを防ぐ方法
- 条件付き書き込みの動作
- 条件付き書き込みシナリオ
- Amazon S3 バケットに条件付き書き込みを強制する

キー名に基づくオブジェクトの上書きを防ぐ方法

HTTP If-None-Match 条件付きヘッダーを使用して、オブジェクトを作成する前に、そのキー名に基づいて、指定されたバケットにオブジェクトが既に存在するかどうかを確認できます。Amazon S3 にオブジェクトをアップロードするときは、キー名を指定します。キー名は、バケット内のオブジェクトの大文字と小文字を区別する一意の識別子です。HTTP If-None-Match ヘッダーがない

と、バージョン管理されていないバケットまたはバージョニングが停止されたバケットに同じキー名を持つオブジェクトをアップロードすると、オブジェクトは上書きされます。バージョニングされたバケットでは、最後にアップロードしたオブジェクトがそのオブジェクトの最新バージョンになります。HTTP `If-None-Match` ヘッダーによる条件付き書き込みは、`WRITE` オペレーション中にオブジェクトの存在をチェックします。バケット内で同じキー名が見つかると、オペレーションは失敗します。キー名を使用する方法の詳細については、「the section called “オブジェクトに命名する”」を参照してください。

HTTP `If-None-Match` ヘッダーによる条件付き書き込みを実行するには、`s3:PutObject` アクセス許可が必要です。これにより、呼び出し元はバケット内のオブジェクトの存在を確認できます。`If-None-Match` ヘッダーには * (アスタリスク) 値が必要です。

`If-None-Match` ヘッダーは、次の API で使用できます。

- PutObject
- CompleteMultipartUpload

AWS CLI を使用する場合

次の `put-object` コマンド例は、キー名が `dir-1/my_images.tar.bz2` のオブジェクトに対して条件付き書き込みを実行しようとします。

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key dir-1/my_images.tar.bz2 --body
 my_images.tar.bz2 --if-none-match "*"
```

詳細については、AWS CLI コマンドリファレンスの「put-object」を参照してください。

AWS CLI の詳細については、「AWS Command Line Interface ユーザーガイド」の「AWS Command Line Interface とは」を参照してください。

オブジェクトが変更された場合に上書きを防ぐ方法

オブジェクトの ETag は、オブジェクトに固有の文字列であり、オブジェクトのコンテンツへの変更を反映します。`If-Match` ヘッダーを使用して、Amazon S3 バケット内のオブジェクトの ETag 値を、`WRITE` オペレーション中に指定した値と比較できます。ETag 値が一致しない場合、オペレーションは失敗となります。ETag の詳細については、「the section called “Content-MD5 と ETag を使用して、アップロードされたオブジェクトを検証する”」を参照してください。

HTTP `If-Match` ヘッダーによる条件付き書き込みを実行するには、`s3:PutObject` と `s3:GetObject` のアクセス許可が必要です。これにより、呼び出し元は ETag をチェックし、バ

ケット内のオブジェクトの状態を確認できます。If-Match ヘッダーには、文字列としての ETag 値が必要です。

If-Match ヘッダーは、次の API で使用できます。

- PutObject
- CompleteMultipartUpload

AWS CLI を使用する場合

次の put-object コマンド例は、指定された ETag 値 6805f2cfc46c0f04559748bb039d69ae を使用して条件付き書き込みを実行しようとします。

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key dir-1/my_images.tar.bz2 --body
 my_images.tar.bz2 --if-match "6805f2cfc46c0f04559748bb039d69ae"
```

詳細については、AWS CLI コマンドリファレンスの「put-object」を参照してください。

AWS CLI の詳細については、「AWS Command Line Interface ユーザーガイド」の「AWS Command Line Interface とは」を参照してください。

条件付き書き込みの動作

If-None-Match ヘッダーを使用した条件付き書き込み

If-None-Match ヘッダーを使用した条件付き書き込みは、バケット内の既存のオブジェクトに対して評価を実行します。バケットに同じキー名を持つ既存のオブジェクトがない場合、書き込みオペレーションは成功し、200 OK レスポンスが返されます。既存のオブジェクトがある場合、書き込みオペレーションは失敗し、412 Precondition Failed レスポンスが返されます。

バージョニングが有効なバケットでは、同じ名前の現在のオブジェクトバージョンが存在しない場合、または現在のオブジェクトバージョンに削除マーカーがある場合、書き込みオペレーションは成功します。それ以外の場合は、書き込みオペレーションは失敗して、412 Precondition Failed レスポンスを返します。

同じオブジェクト名に対して複数の条件付き書き込みが発生すると、最初の書き込みオペレーションは成功します。その後、Amazon S3 は以降の書き込みを失敗として、412 Precondition Failed レスポンスを返します。

同時リクエストが発生した場合、そのオブジェクトに対する条件付き書き込みオペレーションが完了する前に、そのオブジェクトへの削除リクエストが成功すると、409 Conflict レスポンスも受け取ることができます。PutObject で条件付き書き込みを使用する場合、409 Conflict エラーを受け取った後にアップロードが再試行される場合があります。CompleteMultipartUpload を使用する場合、409 Conflict エラーを受け取った後にオブジェクトを再度アップロードするには、CreateMultipartUpload を使用してマルチパートアップロード全体を再開する必要があります。

If-Match ヘッダーを使用した条件付き書き込み

If-Match ヘッダーは、バケット内の既存のオブジェクトに対して評価されます。同じキー名を持ち、ETag が一致する既存のオブジェクトがある場合、書き込みオペレーションは成功し、200 OK レスポンスが返されます。ETag が一致しない場合、書き込みオペレーションは 412 Precondition Failed レスポンスで失敗します。

同時リクエストの場合には 409 Conflict レスポンスを受け取ることもできます。

オブジェクトに対する条件付き書き込みオペレーションが完了する前にそのオブジェクトへの削除リクエストが成功すると、オブジェクトキーが存在しなくなるため、404 Not Found を受け取ることになります。404 Not Found レスポンスを受け取ったら、オブジェクトを再アップロードする必要があります。

同じ名前の現在のオブジェクトバージョンが存在しない場合、または現在のオブジェクトバージョンに削除マーカーがある場合、オペレーションは 404 Not Found エラーで失敗します。

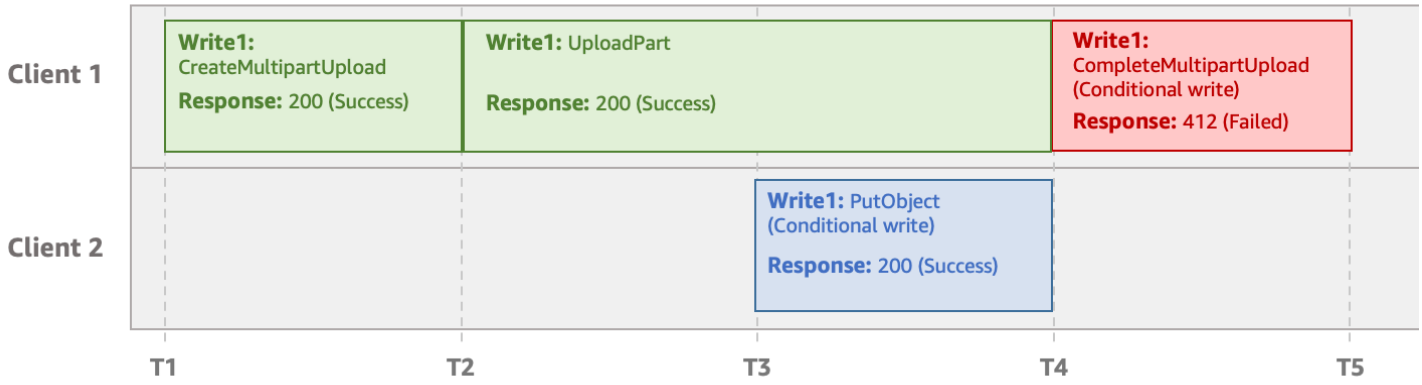
条件付き書き込みシナリオ

2 つのクライアントが同じバケットでオペレーションを実行しているような、以下のシナリオについて考えてみましょう。

マルチパートアップロード中の条件付き書き込み

実行中のマルチパートアップロードリクエストは完全には書き込まれていないため、条件付き書き込みでは考慮されません。クライアント 1 がマルチパートアップロードを使用してオブジェクトをアップロード中である、次の例を考えてみましょう。このマルチパートアップロード中、クライアント 2 は条件付き書き込みオペレーションを使用して同じオブジェクトの書き込みを正常に実行できます。その後、クライアント 1 が条件付き書き込みを使用してマルチパートアップロードを完了しようとすると、アップロードは失敗します。

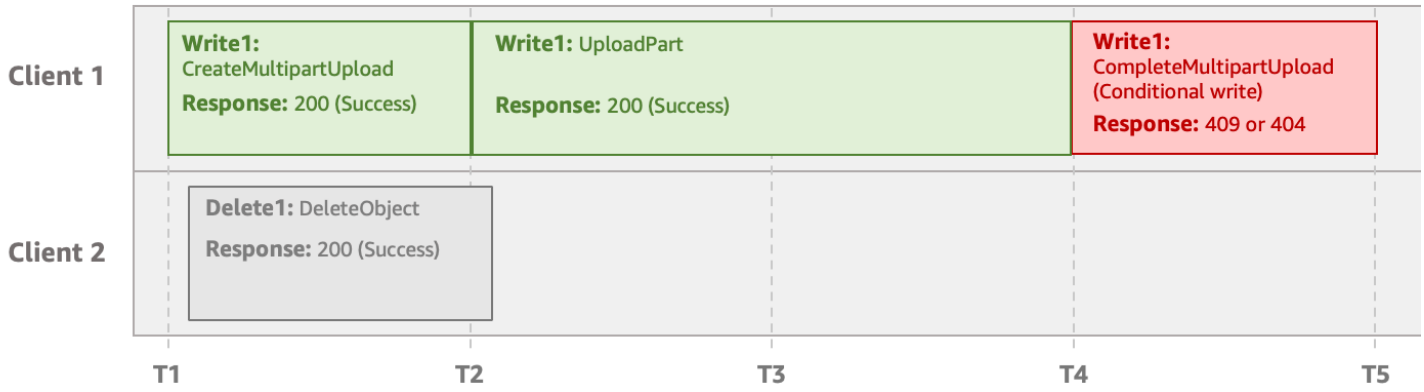
> **Note**
>
> このシナリオでは、If-None-Match と If-Match ヘッダーの両方に 412 Precondition Failed レスポンスが返されます。



マルチパートアップロード中の同時削除

条件付き書き込みリクエストが完了する前に削除リクエストが正常に完了すると、Amazon S3 は書き込みオペレーションについて 409 Conflict または 404 Not Found レスポンスを返します。これは、先に開始された削除リクエストが条件付き書き込みオペレーションよりも優先されるためです。このような場合、新しいマルチパートアップロードを開始する必要があります。

> **Note**
>
> このシナリオでは、If-None-Match ヘッダーに対する 409 Conflict レスポンスと If-Match ヘッダーに対する 404 Not Found レスポンスが生成されます。



> **Note**
>
> ストレージコストを最小限に抑えるため、AbortIncompleteMultipartUpload アクションを使用して指定した日数が経過した後に不完全なマルチパートアップロードを削除するようにライフサイクルルールを設定することをお勧めします。不完全なマルチパートアップロードを削除するライフサイクルルールの作成の詳細については、「不完全なマルチパートアップロードを中止するためのバケットライフサイクルポリシーの設定」を参照してください。

Amazon S3 バケットに条件付き書き込みを強制する

Amazon S3 バケットポリシーを使用すると、汎用バケット内のオブジェクトアップロードに条件付き書き込みを強制できます。

バケットポリシーは、Amazon S3 バケットとその中のオブジェクトへのアクセス許可を付与できるリソースベースのポリシーです。バケット所有者のみが、ポリシーをバケットに関連付けることができます。バケットポリシーの詳細については、「the section called “バケットポリシー”」を参照してください。

条件キー s3:if-match または s3:if-none-match をオプションの Condition 要素または Condition ブロックとして使用して、ポリシーが有効になるタイミングを指定できます。これらの API は条件付きヘッダーを受け付けないため、マルチパートアップロードの場合、CreateMultipartUpload、UploadPart、および UploadPartCopy オペレーションを除外するには、s3:ObjectCreationOperation 条件キーを指定する必要があります。バケットで条件を使用する方法の詳細については、「the section called “条件キーの例”」を参照してください。

> **Note**
>
> バケットポリシーを使用して条件付き書き込みを強制する場合、バケットポリシーで指定されたバケットまたはプレフィックスにコピーオペレーションを実行することはできません。If-None-Match または If-Match HTTP ヘッダーのない CopyObject リクエストは 403 Access Denied エラーで失敗します。これらの HTTP ヘッダーにより行われた CopyObject リクエストは、501 Not Implemented レスポンスで失敗します。

次の例は、バケットポリシーで条件を使用して、クライアントに If-None-Match または If-Match HTTP ヘッダーの使用を強制する方法を示しています。

トピック

- 例 1: if-none-match ヘッダーを含む PutObject および CompleteMultipartUpload リクエストを使用したオブジェクトのアップロードのみを許可する
- 例 2: if-match ヘッダーを含む PutObject および CompleteMultipartUpload リクエストを使用したオブジェクトのアップロードのみを許可する
- 例 3: if-none-match または if-match ヘッダーを含むオブジェクトのアップロードリクエストのみを許可する

例 1: **if-none-match** ヘッダーを含む **PutObject** および **CompleteMultipartUpload** リクエストを使用したオブジェクトのアップロードのみを許可する

このポリシーでは、リクエストに if-none-match ヘッダーが含まれている場合、アカウント 111122223333、ユーザー Alice が *amzn-s3-demo-bucket1* バケットに書き込むことを許可し、オブジェクトキーがバケットにまだ存在しないことを確認します。指定されたバケットへのすべての PutObject および CompleteMultipartUpload リクエストには、正常に実行するために if-none-match ヘッダーが含まれている必要があります。このヘッダーを使用すると、オブジェクトキーがバケットに存在しない場合にのみ、お客様はこのバケットに書き込むことができます。

> **Note**
>
> このポリシーは、CreateMultipartUpload、UploadPart、および UploadPartCopy API を使用したマルチパートアップロードを許可する s3:ObjectCreationOperation 条件キーも設定します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowConditionalPut",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Alice"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
            "Condition": {
                "Null": {
                    "s3:if-none-match": "false"
                }
            }
        },
        {
            "Sid": "AllowConditionalPutwithMPUs",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Alice"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
            "Condition": {
                "Bool": {
                    "s3:ObjectCreationOperation": "false"
                }
            }
        }
    ]
}
```

例 2: **if-match** ヘッダーを含む **PutObject** および **CompleteMultipartUpload** リクエストを使用したオブジェクトのアップロードのみを許可する

このポリシーでは、リクエストに if-match ヘッダーが含まれている場合にのみ、アカウント 111122223333、ユーザー Alice が *amzn-s3-demo-bucket1* に書き込むことができます。このヘッダーは、S3 内のオブジェクトの ETag 値を、WRITE オペレーション中に指定した値と比較します。ETag 値が一致しない場合、オペレーションは失敗します。指定されたバケットへのすべて

の PutObject および CompleteMultipartUpload リクエストには、正常に実行するために if-match ヘッダーが含まれている必要があります。

> **Note**
>
> このポリシーは、CreateMultipartUpload、UploadPart、および UploadPartCopy API を使用したマルチパートアップロードを許可する s3:ObjectCreationOperation 条件キーも設定します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowPutObject",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Alice"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
        },
        {
            "Sid": "BlockNonConditionalObjectCreation",
            "Effect": "Deny",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Alice"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
            "Condition": {
                "Null": {
                    "s3:if-match": "true"
                },
                "Bool": {
                    "s3:ObjectCreationOperation": "true"
                }
            }
        },
        {
            "Sid": "AllowGetObjectBecauseConditionalPutIfMatchETag",
            "Effect": "Allow",
```

```
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Alice"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*"
        }
    ]
}
```

例 3: **if-none-match** または **if-match** ヘッダーを含むオブジェクトのアップロードリクエストのみを許可する

このポリシーでは、リクエストに if-none-match または if-match ヘッダーが含まれている場合、アカウント 111122223333、ユーザー Alice が *amzn-s3-demo-bucket1* に書き込むことを許可します。これにより、Alice はバケットにキー名が存在しないオブジェクトをアップロードできます。キー名が存在する場合、オブジェクトの ETag が PUT リクエストで指定された ETag と一致すれば、Alice はオブジェクトを上書きできます。

> **Note**
>
> このポリシーは、CreateMultipartUpload、UploadPart、および UploadPartCopy API を使用したマルチパートアップロードを許可する s3:ObjectCreationOperation 条件キーも設定します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": " AllowConditionalPutifAbsent",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Alice"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
            "Condition": {
                "Null": {
                    "s3:if-none-match": "false"
                }
            }
```

```
        },
        {
            "Sid": "AllowConditionalPutIfMatchEtag",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Alice"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
            "Condition": {
                "Null": {
                    "s3:if-match": "false"
                }
            }
        },
        {
            "Sid": "AllowConditionalObjectCreation",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Alice"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
            "Condition": {
                "Bool": {
                    "s3:ObjectCreationOperation": "false"
                }
            }
        },
        {
            "Sid": " AllowGetObjectBecauseConditionalPutIfMatchETag",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Alice"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*"
        }
    ]
}
```

オブジェクトのコピー、移動、名前の変更

CopyObject オペレーションを使用すると、Amazon S3 内に既に保存されているオブジェクトのコピーを作成できます。

1 回のアトミックオペレーションでコピーできるオブジェクトのサイズは最大 5 GB です。ただし、5 GB を超えるオブジェクトをコピーする場合は、AWS CLI または AWS SDK を使用してマルチパートアップロードを使用する必要があります。詳細については、「マルチパートアップロードを使用したオブジェクトのコピー」を参照してください。

> **Note**
>
> マルチパートアップロードを使用してアップロードしたオブジェクトのパフォーマンス上の利点を維持するには、S3 コンソールの代わりに AWS CLI または AWS SDK を使用して、マルチパートアップロードを使用してオブジェクトをコピーする必要があります。詳細については、「マルチパートアップロードを使用したオブジェクトのコピー」を参照してください。

CopyObject オペレーションを使用すると、以下のことができます。

- オブジェクトの追加のコピーを作成します。
- オブジェクトをコピーし、元のオブジェクトを削除して、オブジェクトの名前を変更します。
- 複数の AWS リージョン 間 (us-west-1 から eu-west-2 へなど) を含め、オブジェクトをあるバケットから別のバケットにコピーしたり、移動したりします。オブジェクトを移動する場合、Amazon S3 はオブジェクトを指定されたコピー先にコピーしてから、コピー元のオブジェクトを削除します。

  > **Note**
  >
  > AWS リージョン 間でオブジェクトをコピーすると、帯域コストが発生します。詳細については、Amazon S3 の料金 を参照してください。

- オブジェクトのメタデータを変更する 各 Amazon S3 オブジェクトにはメタデータがあります。このメタデータは、名前と値のペアのセットです。オブジェクトメタデータは、オブジェクトをアップロードする際に設定できます。オブジェクトのアップロード後にオブジェクトメタデータを変更することはできません。オブジェクトメタデータを変更する唯一の方法は、オブジェクトのコピー

を作成し、メタデータを設定することです。これを行うには、コピーオペレーションで、コピー元とコピー先として同じオブジェクトを指定します。

オブジェクトのメタデータによっては、システムメタデータであったり、ユーザー定義メタデータである場合もあります。システムメタデータによっては、制御できます。例えば、オブジェクトに使用するストレージクラスやサーバー側の暗号化の種類を制御できます。オブジェクトをコピーするときは、ユーザーが制御するシステムメタデータとユーザー定義メタデータもコピーされます。システムが制御するメタデータは Amazon S3 によってリセットされます。たとえば、オブジェクトをコピーすると、コピーしたオブジェクトの作成日が Amazon S3 によってリセットされます。コピーリクエストでは、このようなシステム制御のメタデータ値を設定する必要はありません。

オブジェクトをコピーするときは、一部のメタデータ値を更新することができます。例えば、コピー元のオブジェクトが S3 標準ストレージを使用するように設定されている場合、オブジェクトコピーに S3 Intelligent-Tiering を使用することができます。また、コピー元のオブジェクトに存在するユーザー定義メタデータの一部を変更することもできます。オブジェクトのユーザー設定可能なメタデータ (システムまたはユーザー定義) をコピー時に更新する場合、メタデータ値の 1 つだけを変更する場合でも、コピー元オブジェクトに存在するすべてのユーザー設定可能メタデータをリクエスト内で明示的に指定する必要があります。

> **Note**
>
> Amazon S3 コンソールを使用してオブジェクトをコピーすると、"Copied metadata can't be verified." というエラーメッセージが表示されることがあります。コンソールは、ヘッダーを使用してオブジェクトのメタデータを取得し、設定します。ネットワークまたはブラウザの設定によってネットワークリクエストが変更された場合、この動作により、コピーしたオブジェクトに意図しないメタデータ (変更された `Cache-Control` ヘッダーなど) が書き込まれる可能性があります。Amazon S3 はこの意図しないメタデータを検証できません。
>
> この問題に対処するには、ネットワークとブラウザの設定をチェックして、`Cache-Control` などのヘッダーが変更されていないことを確認します。詳細については、「The Shared Responsibility Model」を参照してください。

オブジェクトメタデータの詳細については、オブジェクトメタデータの使用 を参照してください。

アーカイブされたオブジェクトや復元されたオブジェクトのコピー

ソースオブジェクトが S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive にアーカイブされている場合は、オブジェクトを他のバケットにコピーする前に、一時コピーを復元する必要があります。オブジェクトのアーカイブについては、アーカイブされたオブジェクトの操作 を参照してください。

Amazon S3 コンソールのコピーオペレーションは、S3 Glacier Flexible Retrieval や S3 Glacier Deep Archive ストレージクラスの復元されたオブジェクトではサポートされていません。復元されたこのようなオブジェクトをコピーするには、AWS Command Line Interface (AWS CLI)、AWS SDK、または Amazon S3 REST API を使用します。

暗号化されたオブジェクトのコピー

Amazon S3 は、S3 バケットにコピーされたすべての新しいオブジェクトを自動的に暗号化します。コピーリクエストで暗号化情報を指定しない場合、ターゲットオブジェクトの暗号化設定は送信先バケットのデフォルトの暗号化設定に設定されます。デフォルトでは、すべてのバケットには、Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3) を使用します。送信先バケットに AWS Key Management Service (AWS KMS) キー (SSE-KMS) によるサーバー側の暗号化またはお客様が指定した暗号化キー (SSE-C) を使用するデフォルトの暗号化設定がある場合、Amazon S3 は対応する KMS キーまたはお客さんが指定したキーを使用してターゲットオブジェクトのコピーを暗号化します。

オブジェクトをコピーする際、ターゲットオブジェクトに別のタイプの暗号化設定を使用する場合は、Amazon S3 が KMS キー、Amazon S3 マネージドキー、またはお客様が提供するキーを使用してターゲットオブジェクトを暗号化するようにリクエストできます。リクエストの暗号化設定が送信先バケットのデフォルトの暗号化設定と異なる場合は、リクエストの暗号化設定が優先されます。コピー元のオブジェクトが SSE-C を使用して暗号化されている場合、Amazon S3 がコピーするオブジェクトを復号化できるように、リクエストで必要な暗号化情報を指定する必要があります。詳細については、「暗号化によるデータの保護」を参照してください。

オブジェクトコピー時のチェックサムの使用

オブジェクトをコピーするとき、オブジェクトに対して別のチェックサムアルゴリズムを使用するように選択できます。同じアルゴリズムを使用するか、新しいアルゴリズムを使用するかにかかわらず、Amazon S3 はオブジェクトのコピー後に新しいチェックサム値を計算します。Amazon S3 は、チェックサムの値を直接コピーしません。チェックサムがなく、送信先チェックサムアルゴリズムが指定されていない、コピーされたオブジェクトはすべて、CRC-64NVME チェックサムアルゴリズムを自動的に取得します。チェックサムの計算方法の詳細については、「Amazon S3 でのマルチパートアップロードを使用したオブジェクトのアップロードとコピー」を参照してください。

単一のリクエストでの複数オブジェクトのコピー

単一のリクエストで複数の Amazon S3 オブジェクトをコピーするには、Amazon S3 バッチオペレーションを使用することもできます。S3 バッチオペレーションには、オペレーションターゲットのオブジェクトのリストを指定します。S3 バッチオペレーションは、各 API オペレーションを呼び出して、指定されたオペレーションを実行します。1 つのバッチオペレーションジョブで、エクサバイトのデータを含む数十億ものオブジェクトに対して、指定されたオペレーションを実行できます。

S3 バッチオペレーション機能は、進捗状況の追跡、通知の送信、すべてのアクションの詳細な完了レポートの保存を行い、フルマネージドの監査可能なサーバーレスエクスペリエンスを提供します。S3 バッチオペレーションは、Amazon S3 コンソール、AWS CLI、AWS SDK、または REST API を通じて使用できます。詳細については、「the section called “バッチ操作の基本”」を参照してください。

オブジェクトのディレクトリバケットへのコピー

オブジェクトをディレクトリバケットにコピーする方法の詳細については、「ディレクトリバケットから、またはディレクトリバケットへのオブジェクトのコピー」を参照してください。Amazon S3 Express One Zone ストレージ クラスをディレクトリバケットで使用する方法については、「S3 Express One Zone」と「ディレクトリバケットの使用」を参照してください。

オブジェクトをコピーするには

オブジェクトをコピーするには、以下のメソッドを使用します。

S3 コンソールの使用

> **Note**
>
> コンソールでオブジェクトをコピーする際の制約と制限は次のとおりです。
>
> - オブジェクトが 5 GB 未満の場合は、オブジェクトをコピーできます。オブジェクトが 5 GB を超える場合は、AWS CLI または AWS SDK を使用してオブジェクトをコピーする必要があります。
> - オブジェクトのコピーに必要な追加のアクセス許可のリストについては、「the section called “S3 API オペレーションに必要なアクセス許可”」を参照してください。このアクセス許可を付与するポリシーの例については、「the section called “アイデンティティベースのポリシーの例”」を参照してください。
> - この Copy アクションは、指定されたフォルダ (プレフィックス) 内のすべてのオブジェクトに適用されます。アクションの進行中にこれらのフォルダに追加されたオブジェクトが影響を受ける可能性があります。

- SSE-KMS で暗号化されたオブジェクトのクロスリージョンコピーは、Amazon S3 コンソールではサポートされていません。SSE-KMS で暗号化されたオブジェクトをリージョン間でコピーするには、AWS CLI、AWS SDK、または Amazon S3 REST API を使用します。
- お客様が提供する暗号化キー (SSE-C) で暗号化されたオブジェクトは、S3 コンソールを使用してコピーすることはできません。SSE-C で暗号化されたオブジェクトをコピーするには、AWS CLI、AWS SDK、または Amazon S3 REST API を使用します。
- コピーされたオブジェクトは、元のオブジェクトの Object Lock 設定を保持しません。
- オブジェクトのコピー元のバケットが S3 オブジェクト所有者にバケット所有者強制設定を使用している場合、オブジェクト ACL は指定された宛先にコピーされません。
- S3 オブジェクト所有者にバケット所有者強制設定を使用するバケットにオブジェクトをコピーする場合は、ソースバケットでもバケット所有者強制設定が使用されていることを確認するか、他の AWS アカウントおよびグループへのオブジェクト ACL 許可を削除します。

オブジェクトをコピーするには

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 左のナビゲーションペインで、[汎用バケット] または [ディレクトリバケット] を選択します。
3. バケットのリストで、コピーするオブジェクトが含まれるバケットの名前を選択します。
4. コピーするオブジェクトの名前の左にあるチェックボックスをオンにします。
5. [アクション] メニューに表示されるオプションのリストから [コピー] を選択します。
6. 送信先タイプと送信先アカウントを選択します。送信先パスを指定するには、[S3 の参照] を選択し、送信先に移動して、送信先の左側にあるチェックボックスをオンにします。右下の [Choose destination] (送信先を選択する) を選択します。

   または、送信先パスを入力します。
7. バケットバージョニングを有効にしていない場合は、バケットバージョニングを有効にして、オブジェクトを意図しない上書きまたは削除から保護することを推奨する警告が表示されます。このバケットのオブジェクトの全バージョンを保持する場合は、[バケットのバージョニングを有効にする] をクリックします。[送信先の詳細] で、デフォルトの暗号化プロパティと S3 Object Lock プロパティを確認することもできます。

8. [追加のコピー設定] で、[ソース設定をコピー] するか、[設定を指定しない] か、[設定を指定] するかを選択します。[ソース設定をコピー] がデフォルトのオプションです。ソース設定の属性なしでオブジェクトのみをコピーする場合は、[設定を指定しない] を選択します。ストレージクラス、ACL、オブジェクトタグ、メタデータ、サーバー側の暗号化、その他のチェックサムの設定を指定するには、[設定を指定] を選択します。
9. 右下の [Copy] (コピー) を選択します。Amazon S3 によってオブジェクトがコピー先にコピーされます。

AWS SDK の使用

このセクションの例は、1 回のオペレーションで最大 5 GB のオブジェクトをコピーする方法を示しています。5 GB を超えるオブジェクトをコピーする場合は、マルチパートアップロード API を使用する必要があります。詳細については、「マルチパートアップロードを使用したオブジェクトのコピー」を参照してください。

Java

Example

次の例では、AWS SDK for Java を使用して Amazon S3 にオブジェクトをコピーします。作業サンプルの作成およびテストの手順については、「AWS SDK for Java のデベロッパーガイド」の「使用開始」を参照してください。

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.CopyObjectRequest;

import java.io.IOException;

public class CopyObjectSingleOperation {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String sourceKey = "*** Source object key *** ";
        String destinationKey = "*** Destination object key ***";
```

```
        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();

            // Copy the object into a new object in the same bucket.
            CopyObjectRequest copyObjRequest = new CopyObjectRequest(bucketName,
 sourceKey, bucketName, destinationKey);
            s3Client.copyObject(copyObjRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

.NET

次の C# の例では、高レベルの SDK for .NET を使用して、1 回のオペレーションで 5 GB の大きさのオブジェクトをコピーします。5 GB を超えるオブジェクトには、マルチパートアップロードを使用したオブジェクトのコピー で説明しているマルチパートアップロードコピーの例を使用します。

この例では、最大 5 GB のオブジェクトのコピーを作成します。コード例を設定および実行する方法の詳細については、「AWS SDK for .NET デベロッパーガイド」の「AWS SDK for .NET の開始方法」 を参照してください。

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
```

```
   class CopyObjectTest
   {
       private const string sourceBucket = "*** provide the name of the bucket with
source object ***";
       private const string destinationBucket = "*** provide the name of the bucket
to copy the object to ***";
       private const string objectKey = "*** provide the name of object to copy
***";
       private const string destObjectKey = "*** provide the destination object key
name ***";
       // Specify your bucket region (an example region is shown).
       private static readonly RegionEndpoint bucketRegion =
RegionEndpoint.USWest2;
       private static IAmazonS3 s3Client;

       public static void Main()
       {
           s3Client = new AmazonS3Client(bucketRegion);
           Console.WriteLine("Copying an object");
           CopyingObjectAsync().Wait();
       }

       private static async Task CopyingObjectAsync()
       {
           try
           {
               CopyObjectRequest request = new CopyObjectRequest
               {
                   SourceBucket = sourceBucket,
                   SourceKey = objectKey,
                   DestinationBucket = destinationBucket,
                   DestinationKey = destObjectKey
               };
               CopyObjectResponse response = await
s3Client.CopyObjectAsync(request);
           }
           catch (AmazonS3Exception e)
           {
               Console.WriteLine("Error encountered on server. Message:'{0}' when
writing an object", e.Message);
           }
           catch (Exception e)
           {
```

```
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
        }
    }
}
```

PHP

このトピックでは、バージョン 3 の AWS SDK for PHP のクラスを使用して、Amazon S3 内の 1 つまたは複数のオブジェクトを、特定のバケットから別のバケットへ、または同じバケット内にコピーする手順を示します。

AWS SDK for Ruby API の詳細については、AWS SDK for Ruby - バージョン 2 を参照してください。

以下の PHP の例は、copyObject() メソッドを使用して Amazon S3 内の単一つのオブジェクトをコピーする方法を説明しています。getcommand() メソッドを使用して、CopyObject 呼び出しのバッチを使用して、オブジェクトの複数コピーを作成する例も示します。

オブジェクトのコピー

1	Aws\S3\S3Client クラスのコンストラクタを使用して、Amazon S3 クライアントのインスタンスを作成します。
2	オブジェクトの複数のコピーを作成するには、Amazon S3 クライアントの getCommand() メソッドへの呼び出しのバッチを実行します。このメソッドは、Aws\CommandInterface クラスから継承されています。最初の引数として CopyObject コマンドを指定し、2 番目の引数としてコピー元のバケット、コピー元のキー名、コピー先のバケット、コピー先のキー名を含む array を指定します。

```
 require 'vendor/autoload.php';

use Aws\CommandPool;
use Aws\Exception\AwsException;
use Aws\ResultInterface;
use Aws\S3\S3Client;

$sourceBucket = '*** Your Source Bucket Name ***';
```

```
$sourceKeyname = '*** Your Source Object Key ***';
$targetBucket = '*** Your Target Bucket Name ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region' => 'us-east-1'
]);

// Copy an object.
$s3->copyObject([
    'Bucket' => $targetBucket,
    'Key' => "$sourceKeyname-copy",
    'CopySource' => "$sourceBucket/$sourceKeyname",
]);

// Perform a batch of CopyObject operations.
$batch = array();
for ($i = 1; $i <= 3; $i++) {
    $batch[] = $s3->getCommand('CopyObject', [
        'Bucket' => $targetBucket,
        'Key' => "{targetKeyname}-$i",
        'CopySource' => "$sourceBucket/$sourceKeyname",
    ]);
}
try {
    $results = CommandPool::batch($s3, $batch);
    foreach ($results as $result) {
        if ($result instanceof ResultInterface) {
            // Result handling here
        }
        if ($result instanceof AwsException) {
            // AwsException handling here
        }
    }
} catch (Exception $e) {
    // General error handling here
}
```

Python

```
class ObjectWrapper:
    """Encapsulates S3 object actions."""
```

```
    def __init__(self, s3_object):
        """
        :param s3_object: A Boto3 Object resource. This is a high-level resource in
Boto3
                          that wraps object actions in a class-like structure.
        """
        self.object = s3_object
        self.key = self.object.key
```

```
    def copy(self, dest_object):
        """
        Copies the object to another bucket.

        :param dest_object: The destination object initialized with a bucket and
key.
                            This is a Boto3 Object resource.
        """
        try:
            dest_object.copy_from(
                CopySource={"Bucket": self.object.bucket_name, "Key":
self.object.key}
            )
            dest_object.wait_until_exists()
            logger.info(
                "Copied object from %s:%s to %s:%s.",
                self.object.bucket_name,
                self.object.key,
                dest_object.bucket_name,
                dest_object.key,
            )
        except ClientError:
            logger.exception(
                "Couldn't copy object from %s/%s to %s/%s.",
                self.object.bucket_name,
                self.object.key,
                dest_object.bucket_name,
                dest_object.key,
            )
            raise
```

Ruby

以下のタスクでは、Ruby クラスを使用して、Amazon S3 内のバケット間または同一バケット内でオブジェクトをコピーする方法を説明します。

オブジェクトのコピー

1	AWS SDK for Ruby のバージョン 3 には Amazon S3 のモジュール化された gem を使用し、`aws-sdk-s3` を要求し、AWS 認証情報を指定します。認証情報を提供する方法の詳細については、「Amazon S3 API リファレンス」の「Making requests using AWS account or IAM user credentials」を参照してください。
2	コピー元のバケット名、コピー元のキー名、コピー先のバケット名、コピー先のキー名などのリクエスト情報を指定します。

次の Ruby サンプルコードは、前のタスクについて、`#copy_object` メソッドを使用して、バケット間でオブジェクトをコピーする方法を説明しています。

```
require 'aws-sdk-s3'

# Wraps Amazon S3 object actions.
class ObjectCopyWrapper
  attr_reader :source_object

  # @param source_object [Aws::S3::Object] An existing Amazon S3 object. This is
 used as the source object for
  #                                        copy actions.
  def initialize(source_object)
    @source_object = source_object
  end

  # Copy the source object to the specified target bucket and rename it with the
 target key.
  #
  # @param target_bucket [Aws::S3::Bucket] An existing Amazon S3 bucket where the
 object is copied.
  # @param target_object_key [String] The key to give the copy of the object.
  # @return [Aws::S3::Object, nil] The copied object when successful; otherwise,
 nil.
  def copy_object(target_bucket, target_object_key)
    @source_object.copy_to(bucket: target_bucket.name, key: target_object_key)
```

```
    target_bucket.object(target_object_key)
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't copy #{@source_object.key} to #{target_object_key}. Here's why:
 #{e.message}"
  end
end

# Example usage:
def run_demo
  source_bucket_name = "amzn-s3-demo-bucket1"
  source_key = "my-source-file.txt"
  target_bucket_name = "amzn-s3-demo-bucket2"
  target_key = "my-target-file.txt"

  source_bucket = Aws::S3::Bucket.new(source_bucket_name)
  wrapper = ObjectCopyWrapper.new(source_bucket.object(source_key))
  target_bucket = Aws::S3::Bucket.new(target_bucket_name)
  target_object = wrapper.copy_object(target_bucket, target_key)
  return unless target_object

  puts "Copied #{source_key} from #{source_bucket_name} to
 #{target_object.bucket_name}:#{target_object.key}."
end

run_demo if $PROGRAM_NAME == __FILE__
```

REST API の使用

この例では、Amazon S3 REST API を使用してオブジェクトをコピーする方法について説明します。REST API の詳細については、CopyObject を参照してください。

このサンプルは、flotsam オブジェクト (*amzn-s3-demo-bucket1* バケット) を jetsam オブジェクト (*amzn-s3-demo-bucket2* バケット) にコピーし、そのメタデータを維持します。

```
PUT /jetsam HTTP/1.1
Host: amzn-s3-demo-bucket2.s3.amazonaws.com
x-amz-copy-source: /amzn-s3-demo-bucket1/flotsam
Authorization: AWS AKIAIOSFODNN7EXAMPLE:ENoSbxYByFA0UGLZUqJN5EUnLDg=
Date: Wed, 20 Feb 2008 22:12:21 +0000
```

署名は次の情報から生成されています。

```
PUT\r\n
\r\n
\r\n
Wed, 20 Feb 2008 22:12:21 +0000\r\n

x-amz-copy-source:/amzn-s3-demo-bucket1/flotsam\r\n
/amzn-s3-demo-bucket2/jetsam
```

Amazon S3 から、オブジェクトの ETag と最終変更日を示す次のレスポンスが返されます。

```
HTTP/1.1 200 OK
x-amz-id-2: Vyaxt7qEbzv34BnSu5hctyyNSlHTYZFMWK4FtzO+iX8JQNyaLdTshL0KxatbaOZt
x-amz-request-id: 6B13C3C5B34AF333
Date: Wed, 20 Feb 2008 22:13:01 +0000

Content-Type: application/xml
Transfer-Encoding: chunked
Connection: close
Server: AmazonS3
<?xml version="1.0" encoding="UTF-8"?>

<CopyObjectResult>
   <LastModified>2008-02-20T22:13:01</LastModified>
   <ETag>"7e9c608af58950deeb370c98608ed097"</ETag>
</CopyObjectResult>
```

AWS CLI を使用する場合

また、AWS Command Line Interface (AWS CLI) を使用して、S3 バケットをコピーすることもできます。詳細については、AWS CLI コマンドリファレンスの「copy-object」を参照してください。

AWS CLI の詳細については、「AWS Command Line Interface ユーザーガイド」の「AWS Command Line Interface とは」を参照してください。

オブジェクトを移動するには

オブジェクトを移動するには、次の方法を使用します。

S3 コンソールの使用

> **Note**
>
> - オブジェクトが 5 GB 未満の場合は、オブジェクトを移動できます。オブジェクトが 5 GB を超える場合は、AWS CLI または AWS SDK を使用してオブジェクトを移動する必要があります。
> - オブジェクトの移動に必要な追加のアクセス許可のリストについては、「the section called “S3 API オペレーションに必要なアクセス許可”」を参照してください。このアクセス許可を付与するポリシーの例については、「the section called “アイデンティティベースのポリシーの例”」を参照してください。
> - お客様が提供する暗号化キー (SSE-C) で暗号化されたオブジェクトは、Amazon S3 コンソールを使用して移動することはできません。SSE-C で暗号化されたオブジェクトを移動するには、AWS CLI、AWS SDK、または Amazon S3 REST API を使用します。
> - フォルダを移動する場合、フォルダをさらに変更するには、移動オペレーションが完了するまで待ちます。
> - Amazon S3 コンソールの 移動オペレーションの移動元または移動先として S3 アクセスポイントのエイリアスを使用することはできません。

オブジェクトを移動するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。移動するオブジェクトが含まれている Amazon S3 のバケットまたはフォルダに移動します。
3. 移動するオブジェクトのチェックボックスをオンにします。
4. [アクション] メニューで、[移動] を選択します。
5. コピー先のパスを指定するには、[S3 の参照] を選択し、コピー先に移動して、コピー先のチェックボックスをオンにします。[コピー先の選択] を選択します。

   または、送信先パスを入力します。
6. バケットバージョニングを有効にしていない場合は、バケットバージョニングを有効にして、オブジェクトを意図しない上書きまたは削除から保護することを推奨する警告が表示されます。このバケットのオブジェクトの全バージョンを保持する場合は、[バケットのバージョニングを有

効にする] をクリックします。[送信先の詳細] で、デフォルトの暗号化プロパティと Object Lock プロパティを確認することもできます。

7. [追加のコピー設定] で、[ソース設定をコピー] するか、[設定を指定しない] か、[設定を指定] するかを選択します。[ソース設定をコピー] がデフォルトのオプションです。ソース設定の属性なしでオブジェクトのみをコピーする場合は、[設定を指定しない] を選択します。ストレージクラス、ACL、オブジェクトタグ、メタデータ、サーバー側の暗号化、その他のチェックサムの設定を指定するには、[設定を指定] を選択します。
8. 右下の [Move] (移動) を選択します。Amazon S3 は、オブジェクトを移動先に移動します。

AWS CLI を使用する場合

また、AWS Command Line Interface (AWS CLI) を使用して、S3 バケットを移動することもできます。詳細については、AWS CLI コマンドリファレンスの「mv」を参照してください。

AWS CLI の詳細については、「AWS Command Line Interface ユーザーガイド」の「AWS Command Line Interface とは」を参照してください。

オブジェクトの名前を変更するには

オブジェクトの名前を変更するには、以下の手順を使用します。

> **Note**
>
> - オブジェクトが 5 GB 未満の場合は、オブジェクトの名前を変更できます。5 GB を超えるオブジェクトの名前を変更するには、AWS CLI または AWS SDK を使用して新しい名前でオブジェクトをコピーし、元のオブジェクトを削除する必要があります。
> - オブジェクトのコピーに必要な追加のアクセス許可のリストについては、「the section called “S3 API オペレーションに必要なアクセス許可”」を参照してください。このアクセス許可を付与するポリシーの例については、「the section called “アイデンティティベースのポリシーの例”」を参照してください。
> - オブジェクトの名前を変更すると、オブジェクトのコピーが新しい最終更新日で作成され、元のオブジェクトに削除マーカーが追加されます。
> - デフォルトの暗号化のバケット設定が、暗号化されていない指定されたオブジェクトに自動的に適用されます。
> - Amazon S3 コンソールを使用して、顧客が提供した暗号化キー (SSE-C) を使用してオブジェクトの名前を変更することはできません。SSE-C で暗号化されたオブジェクトの名

前を変更するには、AWS CLI、AWS SDK、または Amazon S3 REST API を使用して、新しい名前でこれらのオブジェクトをコピーします。

- このバケットが S3 オブジェクトの所有権のバケット所有者の強制設定を使用している場合、オブジェクトアクセスコントロールリスト (ACL) はコピーされません。

オブジェクトの名前を変更するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ナビゲーションペインで [バケット] を選択してから、[汎用バケット] タブをクリックします。名前を変更するオブジェクトを含む Amazon S3 バケットまたはフォルダに移動します。
3. 名前を変更するオブジェクトのチェックボックスをオンにします。
4. [アクション] メニューで [オブジェクトの名前変更] を選択します。
5. [新しいオブジェクト名] ボックスに、オブジェクトの新しい名前を入力します。
6. [追加のコピー設定] で、[ソース設定をコピー] するか、[設定を指定しない] か、[設定を指定] するかを選択します。[ソース設定をコピー] がデフォルトのオプションです。ソース設定の属性なしでオブジェクトのみをコピーする場合は、[設定を指定しない] を選択します。ストレージクラス、ACL、オブジェクトタグ、メタデータ、サーバー側の暗号化、その他のチェックサムの設定を指定するには、[設定を指定] を選択します。
7. [Save changes] (変更の保存) をクリックします。Amazon S3 によりオブジェクトの名前が変更されます。

オブジェクトのダウンロード

このセクションでは、Amazon S3 バケットからオブジェクトをダウンロードする方法について説明します。Amazon S3 では、オブジェクトを 1 つ以上のバケットに保存できます。各オブジェクトの最大サイズは 5 TB です。アーカイブされていない Amazon S3 オブジェクトには、リアルタイムでアクセスできます。ただし、オブジェクトがアーカイブされている場合は、ダウンロードする前に復元する必要があります。アーカイブされたオブジェクトのダウンロードの詳細については、「the section called “アーカイブされたオブジェクトのダウンロード”」を参照してください。

Amazon S3 コンソール、AWS Command Line Interface (AWS CLI)、AWS SDK、または Amazon S3 REST API を使用して 1 つのオブジェクトをダウンロードできます。コードを記述したり、コマンドを実行したりせずに、S3 からオブジェクトをダウンロードするには、S3 コンソールを使用します。詳細については、「the section called “オブジェクトのダウンロード”」を参照してください。

複数のオブジェクトをダウンロードするには、AWS CloudShell、AWS CLI、または AWS SDK を使用します。詳細については、「the section called “複数のオブジェクトのダウンロード”」を参照してください。

オブジェクトの一部をダウンロードする必要がある場合は、AWS CLI または REST API で追加のパラメータを使用して、ダウンロードするバイトのみを指定します。詳細については、「the section called “オブジェクトの一部のダウンロード”」を参照してください。

所有していないオブジェクトをダウンロードする必要がある場合は、オブジェクトの所有者に、そのオブジェクトのダウンロードを許可する署名付き URL を生成するよう依頼します。詳細については、「the section called “別の AWS アカウントに属するオブジェクトのダウンロード”」を参照してください。

AWS ネットワーク外のオブジェクトをダウンロードする場合は、データ転送料金が適用されます。AWS ネットワーク内でのデータ転送は、同じ AWS リージョン内では無料ですが、GET リクエストに対しては料金がかかります。データ転送コストとデータ取得料金の詳細については、「Amazon S3 の料金」を参照してください。

トピック

- オブジェクトのダウンロード
- 複数のオブジェクトのダウンロード
- オブジェクトの一部のダウンロード
- 別の AWS アカウントに属するオブジェクトのダウンロード
- アーカイブされたオブジェクトのダウンロード
- メタデータに基づくオブジェクトのダウンロード
- オブジェクトのダウンロードに関するトラブルシューティング

オブジェクトのダウンロード

Amazon S3 コンソール、AWS CLI、AWS SDK、または REST API を使用してオブジェクトをダウンロードできます。

S3 コンソールの使用

このセクションでは、Amazon S3 コンソールを使用して S3 バケットからオブジェクトをダウンロードする方法について説明します。

> **Note**
>
> - 一度にダウンロードできるオブジェクトは 1 つだけです。
> - Amazon S3 コンソールを使用して、キー名がピリオド (.) で終わるオブジェクトをダウンロードすると、ダウンロードしたオブジェクトのキー名からピリオドが削除されます。ダウンロードしたオブジェクトの名前の末尾のピリオドを保持するには、AWS Command Line Interface (AWS CLI)、AWS SDK、または Amazon S3 REST API を使用する必要があります。

S3 バケットからオブジェクトをダウンロードするには

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 左のナビゲーションペインで、[汎用バケット] または [ディレクトリバケット] を選択します。
3. バケットリストで、オブジェクトのダウンロード元になるバケット名を選択します。
4. 次のいずれかの方法で、S3 バケットからオブジェクトをダウンロードできます。
   - オブジェクトの横にあるチェックボックスを選択し、[ダウンロード] を選択します。オブジェクトを特定のフォルダにダウンロードする場合は、[アクション] メニューの [名前を付けてダウンロード] を選択します。
   - オブジェクトの特定のバージョンをダウンロードする場合は、[バージョンの表示] ボタンを選択します。目的のオブジェクトのバージョンの横にあるチェックボックスをオンにして、[ダウンロード] を選択します。オブジェクトを特定のフォルダにダウンロードする場合は、[アクション] メニューの [名前を付けてダウンロード] を選択します。

AWS CLI を使用する場合

次の `get-object` コマンド例は、AWS CLI を使用して Amazon S3 からオブジェクトをダウンロードする方法を示しています。このコマンドは、バケット *amzn-s3-demo-bucket1* からオブジェクト *folder/my_image* を取得します。*my_downloaded_image.jpg* など、ダウンロードしたオブジェクトのファイル名である `outfile` を含める必要があります。

```
aws s3api get-object --bucket amzn-s3-demo-bucket1 --key folder/
my_image my_downloaded_image.jpg
```

詳細については、「AWS CLI コマンドリファレンス」の「get-object」を参照してください。

AWS SDK の使用

AWS SDK を使用してオブジェクトをダウンロードする方法の例については、「Amazon S3 API リファレンス」の「コードの例」を参照してください。

さまざまな AWS SDK の使用に関する一般的な情報については、「Amazon S3 API リファレンス」の「Developing with Amazon S3 using the AWS SDKs」を参照してください。

REST API の使用

REST API を使用して Amazon S3 からオブジェクトを取得できます。詳細については、「Amazon Simple Storage Service API リファレンス」の「GetObject」を参照してください。

複数のオブジェクトのダウンロード

AWS CloudShell、AWS CLI、または AWS SDK を使用して複数のオブジェクトをダウンロードできます。

AWS Management Console で AWS CloudShell を使用する

AWS CloudShell はブラウザベースの事前に認証されたシェルで、AWS Management Console から直接起動できます。

AWS CloudShell の詳細については、「AWS CloudShell ユーザーガイド」の「CloudShell とは」を参照してください。

> **Important**
>
> AWS CloudShell の場合、ホームディレクトリのストレージは AWS リージョンごとに最大 1 GB です。そのため、合計がこの量を超えるオブジェクトとバケットを同期することはできません。その他の制限については、「AWS CloudShell ユーザーガイド」の「サービスクォータと制限」を参照してください。

AWS CloudShell を使用してオブジェクトをダウンロードするには

1. AWS Management Console にサインインして、CloudWatch コンソール (https://console.aws.amazon.com/cloudwatch/) を開きます。

2. 次のコマンドを実行して、バケット内のオブジェクトを CloudShell に同期します。次のコマンドでは、*amzn-s3-demo-bucket1* という名前のバケットのオブジェクトを同期し、CloudShell に *temp* という名前のフォルダを作成します。CloudShell はオブジェクトをこのフォルダに同期します。このコマンドを使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3 sync s3://amzn-s3-demo-bucket1 ./temp
```

> **Note**
>
> sync コマンドはディレクトリバケットに対応していません。
> パターンマッチングを実行して特定のオブジェクトを除外するか含めるには、`--exclude "value"` パラメータや `--include "value"` パラメータを sync コマンドで使用できます。

3. 次のコマンドを実行して、*temp* という名前のフォルダのオブジェクトを、*temp.zip* という名前のファイルに圧縮します。

```
zip temp.zip -r temp/
```

4. [アクション] を選択し、[ファイルをダウンロード] を選択します。
5. ファイル名として「**temp.zip**」と入力し、[ダウンロード] を選択します。
6. (オプション) CloudShell で *temp.zip* ファイルと *temp* フォルダに同期されているオブジェクトを削除します。AWS CloudShell の場合、永続的ストレージは AWS リージョンごとに最大 1 GB です。

   次のコマンド例を使用して、.zip ファイルとフォルダを削除できます。このコマンド例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
rm temp.zip && rm -rf temp/
```

AWS CLI を使用する場合

次の例では、AWS CLI を使用して、指定したディレクトリまたはプレフィックスの下にあるすべてのファイルまたはオブジェクトをダウンロードする方法を示しています。このコマンドは、バケット *amzn-s3-demo-bucket1* 内のすべてのオブジェクトを現在のディレクトリにコピーします。このコマンド例を使用するには、*amzn-s3-demo-bucket1* の代わりにバケット名を使用します。

```
aws s3 cp s3://amzn-s3-demo-bucket1 . --recursive
```

次のコマンドは、バケット *amzn-s3-demo-bucket1* 内のプレフィックス *logs* の下にあるすべてのオブジェクトを現在のディレクトリにダウンロードします。また、--exclude パラメータと --include パラメータを使用して、サフィックス *.log* が付いたオブジェクトのみをコピーします。このコマンド例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3 cp s3://amzn-s3-demo-bucket1/logs/ . --recursive --exclude "*" --include "*.log"
```

詳細については、「AWS CLI コマンドリファレンス」の「cp」を参照してください。

AWS SDK の使用

AWS SDK を使用して Amazon S3 バケット内のすべてのオブジェクトをダウンロードする方法の例については、「Amazon S3 API リファレンス」の「コードの例」を参照してください。

さまざまな AWS SDK の使用に関する一般的な情報については、「Amazon S3 API リファレンス」の「Developing with Amazon S3 using the AWS SDKs」を参照してください。

オブジェクトの一部のダウンロード

AWS CLI または REST API を使用してオブジェクトの一部をダウンロードできます。そのためには、追加のパラメータを使用して、オブジェクトのどの部分をダウンロードするかを指定します。

AWS CLI を使用する場合

次のコマンド例は、*amzn-s3-demo-bucket1* という名前のバケットの *folder/my_data* という名前のオブジェクトの特定のバイト範囲に対する GET リクエストを行います。リクエストでは、バイト範囲にプレフィックスとして bytes= を付ける必要があります。オブジェクト部分は、*my_data_range* という名前の出力ファイルにダウンロードされます。このコマンド例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3api get-object --bucket amzn-s3-demo-bucket1 --key folder/my_data --range
 bytes=0-500 my_data_range
```

詳細と例については、「AWS CLI コマンドリファレンス」の「get-object」を参照してください。

HTTP Range ヘッダーの詳細については、RFC Editor ウェブサイトで「RFC 9110」を参照してください。

> **Note**
>
> Amazon S3 は、1 回の GET リクエストで複数範囲のデータを取得することはサポートしていません。

REST API の使用

Amazon S3 から複数のオブジェクト部分を取得するには、REST API で `partNumber` パラメータと `Range` パラメータを使用できます。詳細については、「Amazon Simple Storage Service API リファレンス」の「GetObject」を参照してください。

別の AWS アカウントに属するオブジェクトのダウンロード

署名付き URL を使用して、バケットポリシーを更新せずに、オブジェクトへの時間制限付きのアクセスを他のユーザーに許可できます。

署名付き URL をブラウザに入力するか、プログラムで使用してオブジェクトをダウンロードできます。URL で使用する認証情報は、URL を生成した AWS ユーザーの認証情報です。URL を作成すると、署名付き URL を持つすべてのユーザーが、URL の有効期限が切れるまで該当するオブジェクトをダウンロードできます。

S3 コンソールでの署名付き URL の使用

Amazon S3 コンソールを使用して、汎用バケット内のオブジェクトを共有するための署名付き URL を以下の手順で生成できます。コンソールを使用する場合、署名付き URL の最大有効期限は作成時点から 12 時間です。

Amazon S3 コンソールを使用して署名付き URL を生成するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[汎用バケット] を選択します。
3. バケットリストで、署名付き URL を取得するオブジェクトが含まれているバケットの名前を選択します。
4. [オブジェクト] リストで、署名付き URL を作成するオブジェクトを選択します。
5. [オブジェクトアクション] メニューで、[署名付き URL で共有] を選択します。
6. 署名付き URL の有効期間を指定します。
7. [Create presigned URL] (署名付き URL を作成) を選択します。

8. 確認メッセージが表示されると、URL は自動的にクリップボードにコピーされます。署名済み URL を再度コピーする必要がある場合は、署名済み URL をコピーするボタンが表示されます。
9. オブジェクトをダウンロードするには、URL を任意のブラウザに貼り付けると、オブジェクトのダウンロードが試行されます。

署名付き URL とその作成方法の詳細については、「署名付き URL を使用したオブジェクトのダウンロードおよびアップロード」を参照してください。

アーカイブされたオブジェクトのダウンロード

アクセス頻度の低いオブジェクトのストレージコストを削減するには、それらのオブジェクトをアーカイブできます。オブジェクトをアーカイブすると、そのオブジェクトは低コストのストレージに移動されるため、リアルタイムでアクセスすることはできません。アーカイブされたオブジェクトをダウンロードするには、まず復元する必要があります。

ストレージクラスに応じて、アーカイブされたオブジェクトは、数分または数時間で復元できます。アーカイブされたオブジェクトは、Amazon S3 コンソール、S3 バッチオペレーション、Amazon S3 REST API、AWS SDK、および AWS Command Line Interface (AWS CLI) を使用して復元できます。

手順については、「アーカイブされたオブジェクトの復元」を参照してください。アーカイブされたオブジェクトは、復元後にダウンロードできます。

メタデータに基づくオブジェクトのダウンロード

条件付き読み取りリクエストを使用して、メタデータに基づいてオブジェクトをダウンロードするための前提条件を追加できます。オブジェクトは、エンティティタグ (ETag) または最終更新日に基づいて返すことができます。これにより、S3 オペレーションを指定した日付以降に更新されたオブジェクトに制限したり、特定のオブジェクトバージョンのみを返したりできます。

条件付き書き込みは、GetObject または HeadObject リクエストに使用できます。

条件付きリクエストの詳細については、「条件付きリクエストを使用して S3 オペレーションに前提条件を追加する」を参照してください。

オブジェクトのダウンロードに関するトラブルシューティング

Amazon S3 からオブジェクトをダウンロードする場合、アクセス許可が不十分だったり、バケットや AWS Identity and Access Management (IAM) ユーザーポリシーが正しくなかったりすると、エ

ラーが発生する可能性があります。これらの問題により、アクセス拒否 (403 Forbidden) エラーが発生し、Amazon S3 がリソースへのアクセスを許可できない場合があります。

アクセス拒否 (403 Forbidden) エラーの一般的な原因については、「Amazon S3 でのアクセス拒否 (403 Forbidden) エラーのトラブルシューティング」を参照してください。

オブジェクトにアクセスしようとしたときに 404 NoSuchKey エラーが発生した場合は、AWS re:Post 情報センターの「Amazon S3 で発生する 404 NoSuchKey エラーのトラブルシューティング方法を教えてください」を参照してください。

Amazon S3 でのオブジェクトの整合性のチェック

Amazon S3 は、チェックサム値を使用して、アップロードまたはダウンロードするデータの整合性を検証します。さらに、Amazon S3 に保存するオブジェクトについて、別のチェックサム値を計算するようにリクエストすることもできます。データをアップロード、コピー、またはバッチコピーするときに使用するチェックサムアルゴリズムを選択できます。

データをアップロードすると、Amazon S3 は選択したアルゴリズムを使用してサーバー側でチェックサムを計算し、指定された値で検証してから、オブジェクトを保存し、チェックサムをオブジェクトメタデータの一部として保存します。この検証は、シングルパートアップロードとマルチパートアップロードの両方に対して、暗号化モード、オブジェクトサイズ、ストレージクラス間で一貫して機能します。ただし、データをコピーまたはバッチコピーすると、Amazon S3 はソースオブジェクトのチェックサムを計算し、送信先オブジェクトに移動します。

> **Note**
>
> シングルパートまたはマルチパートアップロードを実行する場合、オプションで、事前計算されたチェックサムをリクエストの一部として含め、フルオブジェクトチェックサムタイプを使用することができます。複数のオブジェクトで事前計算された値を使用するには、AWS CLI または AWS SDK を使用します。

サポートされているチェックサムアルゴリズムの使用

Amazon S3 では、チェックサムアルゴリズムを選択して、アップロード中にデータを検証できます。その後、指定されたチェックサムアルゴリズムがオブジェクトとともに保存され、ダウンロード中にデータの整合性を検証するために使用できます。チェックサム値を計算するには、セキュアハッ

シュアルゴリズム (SHA) または巡回冗長検査 (CRC) チェックアルゴリズムのいずれかを選択できます。

- CRC-64/NVME (CRC64NVME)
- CRC-32 (CRC32)
- CRC-32C (CRC32C)
- SHA-1 (SHA1)
- SHA-256 (SHA256)

さらに、Content-MD5 ヘッダーを使用して、各リクエストにチェックサムを提供できます。

オブジェクトをアップロードするときに、使用するアルゴリズムを指定します。

- AWS Management Console を使用するときには、使用するチェックサムアルゴリズムを選択します。オプションでオブジェクトのチェックサム値を指定できます。Amazon S3 は、オブジェクトを受信すると、指定したアルゴリズムを使用してチェックサムを計算します。2 つの値が一致しない場合、Amazon S3 はエラーを生成します。
- SDK を使用するときには、以下について注意してください。
  - `ChecksumAlgorithm` パラメータを Amazon S3 で使用するアルゴリズムに設定します。事前に計算されたチェックサムが既にある場合は、チェックサム値を AWS SDK に渡すと、SDK はリクエストにその値を含めます。チェックサム値を渡さないか、チェックサムアルゴリズムを指定しない場合、SDK はチェックサム値を自動的に計算し、リクエストに含めて整合性の保護を提供します。個々のチェックサム値がチェックサムアルゴリズムの設定値と一致しない場合、Amazon S3 は `BadDigest` エラーでリクエストに失敗します。
  - アップグレードされた AWS SDK を使用している場合、SDK がチェックサムアルゴリズムを選択します。ただし、このチェックサムアルゴリズムは上書きできます。
  - チェックサムアルゴリズムを指定せず、SDK もチェックサムを計算しない場合、S3 は自動的に CRC-64/NVME (CRC64NVME) チェックサムアルゴリズムを選択します。
- REST API を使用しているときには、`x-amz-sdk-checksum-algorithm` パラメータを使用しないでください。代わりに、アルゴリズム固有のヘッダーのいずれかを使用します (例: `x-amz-checksum-crc32`)。

Amazon S3 に既にアップロードされているオブジェクトにこれらのチェックサム値のいずれかを適用するには、オブジェクトをコピーして、既存のチェックサムアルゴリズムを使用するか、新しいチェックサムアルゴリズムを使用するかを指定します。アルゴリズムを指定しない場合、S3 は既存

のアルゴリズムを使用します。ソースオブジェクトに指定されたチェックサムアルゴリズムまたはチェックサム値がない場合、Amazon S3 は CRC-64/NVME アルゴリズムを使用して送信先オブジェクトのチェックサム値を計算します。S3 バッチオペレーションを使用してオブジェクトをコピーするときに、チェックサムアルゴリズムを指定することもできます。

> **Important**
>
> 複合 (またはパートレベル) チェックサムの [チェックサム] でマルチパートアップロードを使用する場合、マルチパートアップロードのパート番号は、連続しており 1 から始まる必要があります。連続しないパート番号でマルチパートアップロードリクエストを完了しようとすると、Amazon S3 は `HTTP 500 Internal Server` エラーを生成します。

フルオブジェクトおよび複合チェックサムタイプ

Amazon S3 では、次の 2 つのタイプのチェックサムがサポートされています。

- フルオブジェクトチェックサム: フルオブジェクトチェックサムは、マルチパートアップロードのすべてのコンテンツに基づいて計算され、最初のパートの最初のバイトから最後のパートの最後のバイトまでのすべてのデータをカバーします。

  > **Note**
  >
  > すべての PUT リクエストには、フルオブジェクトのチェックサムタイプが必要です。

- 複合チェックサム: 複合チェックサムは、マルチパートアップロードの各パートの個々のチェックサムに基づいて計算されます。このアプローチでは、すべてのデータコンテンツに基づいてチェックサムを計算する代わりに、パートレベルのチェックサム (最初の部分から最後の部分まで) を集計して、完全なオブジェクトに対する単一の複合チェックサムを生成します。

  > **Note**
  >
  > オブジェクトがマルチパートアップロードとしてアップロードされるとき、オブジェクトのエンティティタグ (ETag) はオブジェクト全体の MD5 ダイジェストではありません。代わりに、Amazon S3 は、アップロードされた個々のパートの MD5 ダイジェストを計算します。MD5 ダイジェストは、最終的なオブジェクトの ETag を決定するために使用されます。Amazon S3 は MD5 ダイジェストのバイトを連結し、これらの連結値の MD5 ダイ

ジェストを計算します。ETag 作成最終ステップの間に、Amazon S3 はパートの総数を含むダッシュを末尾に追加します。

Amazon S3 は、次のフルオブジェクトおよび複合チェックサムアルゴリズムタイプをサポートしています。

- CRC-64/NVME (CRC64NVME): フルオブジェクトのアルゴリズムタイプのみをサポートします。
- CRC-32 (CRC32): フルオブジェクトアルゴリズムタイプと複合アルゴリズムタイプの両方をサポートします。
- CRC-32C (CRC32C): フルオブジェクトアルゴリズムタイプと複合アルゴリズムタイプの両方をサポートします。
- SHA-1 (SHA1): フルオブジェクトアルゴリズムタイプと複合アルゴリズムタイプの両方をサポートします。
- SHA-256 (SHA256): フルオブジェクトアルゴリズムタイプと複合アルゴリズムタイプの両方をサポートします。

> **Note**
>
> マルチパートアップロードに SHA-1 または SHA-256 チェックサムアルゴリズムを使用している場合は、複合アルゴリズムタイプを使用する必要があります。単一パートのアップロードに SHA-1 または SHA-256 チェックサムアルゴリズムを使用している場合、完全なオブジェクトアルゴリズムタイプのみがサポートされます。

シングルパートアップロード

シングルパートでアップロード (PutObject を使用) されたオブジェクトのチェックサムは、フルオブジェクトチェックサムとして扱われます。Amazon S3 コンソールでオブジェクトをアップロードするときに、S3 で使用するチェックサムアルゴリズムを選択し、(オプションで) 事前に計算された値を指定することもできます。次に、Amazon S3 は、オブジェクトとそのチェックサム値を保存する前に、このチェックサムを検証します。オブジェクトのダウンロード中にチェックサム値をリクエストするときに、オブジェクトのデータ整合性を検証できます。

マルチパートアップロード

MultipartUpload API を使用してオブジェクトを複数のパートに分けてアップロードする場合、Amazon S3 で使用するチェックサムアルゴリズムとチェックサムタイプ (フルオブジェクトまたは複合) を指定できます。

次の表は、マルチパートアップロードの各チェックサムアルゴリズムでサポートされているチェックサムアルゴリズムタイプを示しています。

チェックサムアルゴリズム	フルオブジェクト	複合
CRC-64/NVME (CRC64NVME)	はい	いいえ
CRC-32 (CRC32)	はい	はい
CRC-32C (CRC32C)	はい	はい
SHA-1 (SHA1)	いいえ	はい
SHA-256 (SHA256)	いいえ	はい

マルチパートアップロードへのフルオブジェクトチェックサムの使用

マルチパートアップロードを作成または実行するときは、アップロード時の検証にフルオブジェクトチェックサムを使用できます。つまり、MultipartUpload API にチェックサムアルゴリズムを提供できることを意味します。アップロードされたオブジェクトのパート境界を追跡する必要がなくなるため、整合性検証ツールを簡素化できます。オブジェクト全体のチェックサムとオブジェクトサイズを CompleteMultipartUpload リクエストで指定できます。

マルチパートアップロード中にフルオブジェクトチェックサムを指定すると、AWS SDK はそのチェックサムを Amazon S3 に渡し、S3 はオブジェクトの整合性をサーバー側で検証して、受信した値と比較します。次に、値が一致すると、Amazon S3 はオブジェクトを保存します。2 つの値が一致しない場合、S3 は BadDigest エラーでリクエストに失敗します。オブジェクトのチェックサムはオブジェクトメタデータにも保存され、後でオブジェクトのデータ整合性を検証するために使用します。

フルオブジェクトチェックサムには、S3 で CRC-64/NVME (CRC64NVME)、CRC-32 (CRC32)、または CRC-32C (CRC32C) チェックサムアルゴリズムを使用できます。マルチパートアップロードのフ

ルオブジェクトチェックサムは、フルオブジェクトチェックサムに線形化できるため、CRC ベースのチェックサムでのみ使用できます。この線形化により、Amazon S3 はリクエストを並列化してパフォーマンスを向上させることができます。特に、S3 はパートレベルのチェックサムからオブジェクト全体のチェックサムを計算できます。このタイプの検証は、SHA や MD5 などの他のアルゴリズムでは使用できません。S3 にはデフォルトの整合性保護があるため、チェックサムなしでオブジェクトをアップロードすると、S3 は推奨されるフルオブジェクト CRC-64/NVME (CRC64NVME) チェックサムアルゴリズムをオブジェクトに自動的にアタッチします。

> **Note**
>
> マルチパートアップロードを開始するには、チェックサムアルゴリズムとフルオブジェクトチェックサムタイプを指定できます。チェックサムアルゴリズムとフルオブジェクトチェックサムタイプを指定した後、マルチパートアップロードのフルオブジェクトチェックサム値を指定できます。

マルチパートアップロードへのパートレベルのチェックサムの使用

オブジェクトが Amazon S3 にアップロードされるときには、単一のオブジェクトとしてアップロードされるか、マルチパートアップロードプロセスを使用してパートに分割してアップロードされます。マルチパートアップロードの [チェックサム] タイプを選択できます。マルチパートアップロードのパートレベルのチェックサム (または複合チェックサム) の場合、Amazon S3 は指定されたチェックサムアルゴリズムを使用して個々のパートのチェックサムを計算します。`UploadPart` を使用して、各パートのチェックサム値を指定できます。Amazon S3 コンソールでアップロードしようとしているオブジェクトが CRC-64/NVME (CRC64NVME) チェックサムアルゴリズムを使用するように設定されていて、16 MB を超える場合は、自動的にフルオブジェクトチェックサムとして指定されます。

次に、Amazon S3 は保存されたパートレベルのチェックサム値を使用して、各パートが正しくアップロードされたことを確認します。各パートのチェックサム (オブジェクト全体) を指定すると、S3 は各パートの保存されたチェックサム値を使用して、指定されたチェックサム値と比較し、フルオブジェクトチェックサムを内部的に計算します。これにより、S3 はパートのチェックサムを使用してオブジェクト全体のチェックサムを計算でき、コンピューティングコストが最小限に抑えられます。マルチパートアップロードの詳細については、「Amazon S3 でのマルチパートアップロードを使用したオブジェクトのアップロードとコピー」と「マルチパートアップロードへのフルオブジェクトチェックサムの使用」を参照してください。

オブジェクトが完全にアップロードされたら、最後に計算されたチェックサムを使用して、オブジェクトのデータ整合性を検証できます。

マルチパートアップロードの一部をアップロードするときは、次の点に注意してください。

- オブジェクト全体を構成するパートの数など、オブジェクトに関する情報を取得するには、`GetObjectAttributes` オペレーションを使用します。追加のチェックサムを使用すると、パートのチェックサム値を含む個々のパートの情報を回復することもできます。
- 完了したアップロードでは、`GetObject` または `HeadObject` オペレーションを使用して、シングルパートのパート番号またはバイト範囲を指定することにより、個々のパートのチェックサムを取得することもできます。マルチパートアップロード処理中の個別のパートのチェックサム値を取得する場合は、`ListParts` を使用できます。
- Amazon S3 はマルチパートオブジェクトのチェックサムを計算するので、オブジェクトをコピーした場合、チェックサム値が変更されることがあります。SDK または REST API を使用しており、`CopyObject` を呼び出した場合、Amazon S3 は `CopyObject` API オペレーションのサイズ制限までオブジェクトをコピーします。Amazon S3 は、オブジェクトが単一のリクエストでアップロードされたか、マルチパートアップロードの一部としてアップロードされたかにかかわらず、このコピーを単一のアクションとして実行します。copy コマンドでは、オブジェクトのチェックサムは、完全なオブジェクトの直接チェックサムです。オブジェクトが最初にマルチパートアップロードを使用してアップロードされた場合、データに変更がない場合でも、チェックサム値が変更されます。
- `CopyObject` API オペレーションのサイズ制限よりも大きいオブジェクトは、マルチパートアップロード copy コマンドを使用する必要があります。
- AWS Management Console を使用していくつかの操作を実行するとき、オブジェクトのサイズが 16 MB より大きい場合、Amazon S3 はマルチパートアップロードを使用します。

チェックサムオペレーション

オブジェクトをアップロードした後、チェックサム値を取得し、事前計算済みまたは以前に保存された同じアルゴリズムタイプのチェックサム値と比較できます。次の例は、データの整合性を検証するために使用できるチェックサムオペレーションまたは方法を示しています。

S3 コンソールの使用

コンソールの使用方法およびオブジェクトのアップロード時に使用するチェックサムアルゴリズムの指定方法の詳細については、「オブジェクトのアップロード」および「チュートリアル: チェックサムを追加して Amazon S3 のデータの整合性をチェックする」を参照してください。

AWS SDK の使用

次の例は、AWS SDK を使用して、マルチパートアップロードで大きなファイルをアップロードする方法、大きなファイルをダウンロードする方法、およびマルチパートアップロードファイルを検証する方法を示しています。ファイル検証にはすべて SHA-256 を使用しています。

Java

Example 例: SHA-256 を使用して大きなファイルをアップロード、ダウンロード、および検証する

作業サンプルの作成およびテストの手順については、「AWS SDK for Java のデベロッパーガイド」の「使用開始」を参照してください。

```
import software.amazon.awssdk.auth.credentials.AwsCredentials;
import software.amazon.awssdk.auth.credentials.AwsCredentialsProvider;
import software.amazon.awssdk.core.ResponseInputStream;
import software.amazon.awssdk.core.sync.RequestBody;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.services.s3.model.AbortMultipartUploadRequest;
import software.amazon.awssdk.services.s3.model.ChecksumAlgorithm;
import software.amazon.awssdk.services.s3.model.ChecksumMode;
import software.amazon.awssdk.services.s3.model.CompleteMultipartUploadRequest;
import software.amazon.awssdk.services.s3.model.CompleteMultipartUploadResponse;
import software.amazon.awssdk.services.s3.model.CompletedMultipartUpload;
import software.amazon.awssdk.services.s3.model.CompletedPart;
import software.amazon.awssdk.services.s3.model.CreateMultipartUploadRequest;
import software.amazon.awssdk.services.s3.model.CreateMultipartUploadResponse;
import software.amazon.awssdk.services.s3.model.GetObjectAttributesRequest;
import software.amazon.awssdk.services.s3.model.GetObjectAttributesResponse;
import software.amazon.awssdk.services.s3.model.GetObjectRequest;
import software.amazon.awssdk.services.s3.model.GetObjectResponse;
import software.amazon.awssdk.services.s3.model.GetObjectTaggingRequest;
import software.amazon.awssdk.services.s3.model.ObjectAttributes;
import software.amazon.awssdk.services.s3.model.PutObjectTaggingRequest;
import software.amazon.awssdk.services.s3.model.Tag;
import software.amazon.awssdk.services.s3.model.Tagging;
import software.amazon.awssdk.services.s3.model.UploadPartRequest;
import software.amazon.awssdk.services.s3.model.UploadPartResponse;

import java.io.File;
import java.io.FileInputStream;
```

```
    import java.io.FileOutputStream;
    import java.io.IOException;
    import java.io.InputStream;
    import java.io.OutputStream;
    import java.nio.ByteBuffer;
    import java.security.MessageDigest;
    import java.security.NoSuchAlgorithmException;
    import java.util.ArrayList;
    import java.util.Base64;
    import java.util.List;

    public class LargeObjectValidation {
        private static String FILE_NAME = "sample.file";
        private static String BUCKET = "sample-bucket";
        //Optional, if you want a method of storing the full multipart object
 checksum in S3.
        private static String CHECKSUM_TAG_KEYNAME = "fullObjectChecksum";
        //If you have existing full-object checksums that you need to validate
 against, you can do the full object validation on a sequential upload.
        private static String SHA256_FILE_BYTES = "htCM5g7ZNdoSw8bN/
mkgiAhXt5MFoVowVg+LE9aIQmI=";
        //Example Chunk Size - this must be greater than or equal to 5MB.
        private static int CHUNK_SIZE = 5 * 1024 * 1024;

        public static void main(String[] args) {
            S3Client s3Client = S3Client.builder()
                    .region(Region.US_EAST_1)
                    .credentialsProvider(new AwsCredentialsProvider() {
                        @Override
                        public AwsCredentials resolveCredentials() {
                            return new AwsCredentials() {
                                @Override
                                public String accessKeyId() {
                                    return Constants.ACCESS_KEY;
                                }

                                @Override
                                public String secretAccessKey() {
                                    return Constants.SECRET;
                                }
                            };
                        }
                    })
                    .build();
```

```
            uploadLargeFileBracketedByChecksum(s3Client);
            downloadLargeFileBracketedByChecksum(s3Client);
            validateExistingFileAgainstS3Checksum(s3Client);
        }

        public static void uploadLargeFileBracketedByChecksum(S3Client s3Client) {
            System.out.println("Starting uploading file validation");
            File file = new File(FILE_NAME);
            try (InputStream in = new FileInputStream(file)) {
                MessageDigest sha256 = MessageDigest.getInstance("SHA-256");
                CreateMultipartUploadRequest createMultipartUploadRequest =
CreateMultipartUploadRequest.builder()
                        .bucket(BUCKET)
                        .key(FILE_NAME)
                        .checksumAlgorithm(ChecksumAlgorithm.SHA256)
                        .build();
                CreateMultipartUploadResponse createdUpload =
s3Client.createMultipartUpload(createMultipartUploadRequest);
                List<CompletedPart> completedParts = new ArrayList<CompletedPart>();
                int partNumber = 1;
                byte[] buffer = new byte[CHUNK_SIZE];
                int read = in.read(buffer);
                while (read != -1) {
                    UploadPartRequest uploadPartRequest =
UploadPartRequest.builder()

.partNumber(partNumber).uploadId(createdUpload.uploadId()).key(FILE_NAME).bucket(BUCKET).ch
                    UploadPartResponse uploadedPart =
s3Client.uploadPart(uploadPartRequest,
RequestBody.fromByteBuffer(ByteBuffer.wrap(buffer, 0, read)));
                    CompletedPart part =
CompletedPart.builder().partNumber(partNumber).checksumSHA256(uploadedPart.checksumSHA256()
                    completedParts.add(part);
                    sha256.update(buffer, 0, read);
                    read = in.read(buffer);
                    partNumber++;
                }
                String fullObjectChecksum =
Base64.getEncoder().encodeToString(sha256.digest());
                if (!fullObjectChecksum.equals(SHA256_FILE_BYTES)) {
                    //Because the SHA256 is uploaded after the part is uploaded; the
upload is bracketed and the full object can be fully validated.

s3Client.abortMultipartUpload(AbortMultipartUploadRequest.builder().bucket(BUCKET).key(FILE
```

```
                    throw new IOException("Byte mismatch between stored checksum and
upload, do not proceed with upload and cleanup");
                }
                CompletedMultipartUpload completedMultipartUpload =
CompletedMultipartUpload.builder().parts(completedParts).build();
                CompleteMultipartUploadResponse completedUploadResponse =
s3Client.completeMultipartUpload(

CompleteMultipartUploadRequest.builder().bucket(BUCKET).key(FILE_NAME).uploadId(createdUplo
                Tag checksumTag =
Tag.builder().key(CHECKSUM_TAG_KEYNAME).value(fullObjectChecksum).build();
                //Optionally, if you need the full object checksum stored with the
file; you could add it as a tag after completion.

s3Client.putObjectTagging(PutObjectTaggingRequest.builder().bucket(BUCKET).key(FILE_NAME).t
            } catch (IOException | NoSuchAlgorithmException e) {
                e.printStackTrace();
            }
            GetObjectAttributesResponse
                    objectAttributes =
s3Client.getObjectAttributes(GetObjectAttributesRequest.builder().bucket(BUCKET).key(FILE_N
                    .objectAttributes(ObjectAttributes.OBJECT_PARTS,
ObjectAttributes.CHECKSUM).build());
            System.out.println(objectAttributes.objectParts().parts());
            System.out.println(objectAttributes.checksum().checksumSHA256());
        }

        public static void downloadLargeFileBracketedByChecksum(S3Client s3Client) {
            System.out.println("Starting downloading file validation");
            File file = new File("DOWNLOADED_" + FILE_NAME);
            try (OutputStream out = new FileOutputStream(file)) {
                GetObjectAttributesResponse
                        objectAttributes =
s3Client.getObjectAttributes(GetObjectAttributesRequest.builder().bucket(BUCKET).key(FILE_N
                        .objectAttributes(ObjectAttributes.OBJECT_PARTS,
ObjectAttributes.CHECKSUM).build());
                //Optionally if you need the full object checksum, you can grab a
tag you added on the upload
                List<Tag> objectTags =
s3Client.getObjectTagging(GetObjectTaggingRequest.builder().bucket(BUCKET).key(FILE_NAME).b
                String fullObjectChecksum = null;
                for (Tag objectTag : objectTags) {
                    if (objectTag.key().equals(CHECKSUM_TAG_KEYNAME)) {
                        fullObjectChecksum = objectTag.value();
```

```
                        break;
                    }
                }
                MessageDigest sha256FullObject =
 MessageDigest.getInstance("SHA-256");
                MessageDigest sha256ChecksumOfChecksums =
 MessageDigest.getInstance("SHA-256");

                //If you retrieve the object in parts, and set the ChecksumMode to
 enabled, the SDK will automatically validate the part checksum
                for (int partNumber = 1; partNumber <=
 objectAttributes.objectParts().totalPartsCount(); partNumber++) {
                    MessageDigest sha256Part = MessageDigest.getInstance("SHA-256");
                    ResponseInputStream<GetObjectResponse> response =
 s3Client.getObject(GetObjectRequest.builder().bucket(BUCKET).key(FILE_NAME).partNumber(part
                    GetObjectResponse getObjectResponse = response.response();
                    byte[] buffer = new byte[CHUNK_SIZE];
                    int read = response.read(buffer);
                    while (read != -1) {
                        out.write(buffer, 0, read);
                        sha256FullObject.update(buffer, 0, read);
                        sha256Part.update(buffer, 0, read);
                        read = response.read(buffer);
                    }
                    byte[] sha256PartBytes = sha256Part.digest();
                    sha256ChecksumOfChecksums.update(sha256PartBytes);
                    //Optionally, you can do an additional manual validation again
 the part checksum if needed in addition to the SDK check
                    String base64PartChecksum =
 Base64.getEncoder().encodeToString(sha256PartBytes);
                    String base64PartChecksumFromObjectAttributes =
 objectAttributes.objectParts().parts().get(partNumber - 1).checksumSHA256();
                    if (!
base64PartChecksum.equals(getObjectResponse.checksumSHA256()) || !
base64PartChecksum.equals(base64PartChecksumFromObjectAttributes)) {
                        throw new IOException("Part checksum didn't match for the
 part");
                    }
                    System.out.println(partNumber + " " + base64PartChecksum);
                }
                //Before finalizing, do the final checksum validation.
                String base64FullObject =
 Base64.getEncoder().encodeToString(sha256FullObject.digest());
```

```
                String base64ChecksumOfChecksums =
 Base64.getEncoder().encodeToString(sha256ChecksumOfChecksums.digest());
                if (fullObjectChecksum != null && !
fullObjectChecksum.equals(base64FullObject)) {
                    throw new IOException("Failed checksum validation for full
 object");
                }
                System.out.println(fullObjectChecksum);
                String base64ChecksumOfChecksumFromAttributes =
 objectAttributes.checksum().checksumSHA256();
                if (base64ChecksumOfChecksumFromAttributes != null && !
base64ChecksumOfChecksums.equals(base64ChecksumOfChecksumFromAttributes)) {
                    throw new IOException("Failed checksum validation for full
 object checksum of checksums");
                }
                System.out.println(base64ChecksumOfChecksumFromAttributes);
                out.flush();
            } catch (IOException | NoSuchAlgorithmException e) {
                //Cleanup bad file
                file.delete();
                e.printStackTrace();
            }
        }

        public static void validateExistingFileAgainstS3Checksum(S3Client s3Client)
 {
            System.out.println("Starting existing file validation");
            File file = new File("DOWNLOADED_" + FILE_NAME);
            GetObjectAttributesResponse
                    objectAttributes =
 s3Client.getObjectAttributes(GetObjectAttributesRequest.builder().bucket(BUCKET).key(FILE_N
                    .objectAttributes(ObjectAttributes.OBJECT_PARTS,
 ObjectAttributes.CHECKSUM).build());
            try (InputStream in = new FileInputStream(file)) {
                MessageDigest sha256ChecksumOfChecksums =
 MessageDigest.getInstance("SHA-256");
                MessageDigest sha256Part = MessageDigest.getInstance("SHA-256");
                byte[] buffer = new byte[CHUNK_SIZE];
                int currentPart = 0;
                int partBreak =
 objectAttributes.objectParts().parts().get(currentPart).size();
                int totalRead = 0;
                int read = in.read(buffer);
                while (read != -1) {
```

```
                    totalRead += read;
                    if (totalRead >= partBreak) {
                        int difference = totalRead - partBreak;
                        byte[] partChecksum;
                        if (totalRead != partBreak) {
                            sha256Part.update(buffer, 0, read - difference);
                            partChecksum = sha256Part.digest();
                            sha256ChecksumOfChecksums.update(partChecksum);
                            sha256Part.reset();
                            sha256Part.update(buffer, read - difference,
 difference);
                        } else {
                            sha256Part.update(buffer, 0, read);
                            partChecksum = sha256Part.digest();
                            sha256ChecksumOfChecksums.update(partChecksum);
                            sha256Part.reset();
                        }
                        String base64PartChecksum =
 Base64.getEncoder().encodeToString(partChecksum);
                        if (!
base64PartChecksum.equals(objectAttributes.objectParts().parts().get(currentPart).checksumSH
 {
                            throw new IOException("Part checksum didn't match S3");
                        }
                        currentPart++;
                        System.out.println(currentPart + " " + base64PartChecksum);
                        if (currentPart <
 objectAttributes.objectParts().totalPartsCount()) {
                            partBreak +=
 objectAttributes.objectParts().parts().get(currentPart - 1).size();
                        }
                    } else {
                        sha256Part.update(buffer, 0, read);
                    }
                    read = in.read(buffer);
                }
                if (currentPart != objectAttributes.objectParts().totalPartsCount())
 {
                    currentPart++;
                    byte[] partChecksum = sha256Part.digest();
                    sha256ChecksumOfChecksums.update(partChecksum);
                    String base64PartChecksum =
 Base64.getEncoder().encodeToString(partChecksum);
                    System.out.println(currentPart + " " + base64PartChecksum);
```

```
                }

                String base64CalculatedChecksumOfChecksums =
 Base64.getEncoder().encodeToString(sha256ChecksumOfChecksums.digest());
                System.out.println(base64CalculatedChecksumOfChecksums);
                System.out.println(objectAttributes.checksum().checksumSHA256());
                if (!
base64CalculatedChecksumOfChecksums.equals(objectAttributes.checksum().checksumSHA256()))
 {
                    throw new IOException("Full object checksum of checksums don't
 match S3");
                }

            } catch (IOException | NoSuchAlgorithmException e) {
                e.printStackTrace();
            }
        }
    }
```

REST API の使用

REST リクエストを送信して、チェックサムの値を持つオブジェクトをアップロードし、PutObject でデータの整合性を検証できます。GetObject または HeadObject を使用して、オブジェクトのチェックサムの値を取得することもできます。

AWS CLI の使用

単一のオペレーションで、最大 5 GB のオブジェクトをアップロードする PUT リクエストを送信できます。詳細については、「AWS CLI コマンドリファレンス」の `PutObject` を参照してください。また、`get-object` と `head-object` を使用して、すでにアップロードされたオブジェクトのチェックサムを取得し、データの整合性を検証することもできます。

詳細については、「AWS Command Line Interface ユーザーガイド」の「Amazon S3 CLI のよくある質問」を参照してください。

オブジェクトをアップロードするときに Content-MD5 を使用する

アップロード後にオブジェクトの整合性を検証するもう 1 つの方法は、アップロード時にオブジェクトの MD5 ダイジェストを指定することです。オブジェクトの MD5 ダイジェストを計算した場合、`Content-MD5` ヘッダーを使用することで、PUT コマンドでダイジェストを指定できます。

オブジェクトをアップロードした後、Amazon S3 はオブジェクトの MD5 ダイジェストを計算し、指定した値と比較します。リクエストは、2 つのダイジェストが一致した場合にのみ成功します。

MD5 ダイジェストを指定する必要はありませんが、アップロードプロセスの一環としてオブジェクトの整合性を検証するために使用できます。

Content-MD5 と ETag を使用して、アップロードされたオブジェクトを検証する

オブジェクトのエンティティタグ (ETag) は、そのオブジェクトの特定のバージョンを表します。ETag は、オブジェクトのコンテンツに加えられた変更のみを反映し、メタデータに加えられた変更は反映しないことに注意してください。オブジェクトのメタデータのみが変更された場合、ETag は同じままです。

オブジェクトによっては、オブジェクトの ETag がオブジェクトデータの MD5 ダイジェストである場合があります。

- オブジェクトが `PutObject`、`PostObject`、または `CopyObject` オペレーションによって、または AWS Management Console を介して作成され、そのオブジェクトがプレーンテキストか、Amazon S3 マネージドキーを使用したサーバー側の暗号化 (SSE-S3) によって暗号化されている場合、そのオブジェクトの ETag は、オブジェクトデータの MD5 ダイジェストです。
- オブジェクトが `PutObject`、`PostObject`、または `CopyObject` オペレーションによって、または AWS Management Console を介して作成され、そのオブジェクトがお客様が用意したキーを使用したサーバー側の暗号化 (SSE-C) または AWS Key Management Service (AWS KMS) キーを使用したサーバー側の暗号化 (SSE-KMS) によって暗号化されている場合、そのオブジェクトの ETag は、オブジェクトデータの MD5 ダイジェストではありません。
- オブジェクトがマルチパートアップロードのプロセスまたは `UploadPartCopy` オペレーションによって作成された場合、暗号化の方法に関係なく、オブジェクトの ETag は MD5 ダイジェストではありません。オブジェクトが 16 MB より大きい場合、AWS Management Console はそのオブジェクトをマルチパートアップロードとしてアップロードまたはコピーするため、ETag は MD5 ダイジェストではありません。

ETag がオブジェクトの `Content-MD5` ダイジェストであるオブジェクトの場合、オブジェクトの ETag 値を計算済みまたは以前に保存した `Content-MD5` ダイジェストと比較できます。

追跡チェックサムの使用

Amazon S3 にオブジェクトをアップロードするときには、オブジェクトの事前計算されたチェックサムを指定するか、AWS SDK を使用して、チャンクアップロード用の追跡チェックサムを自動的に作成できます。追跡チェックサムを使用する場合、Amazon S3 は指定されたアルゴリズムを使用してチェックサムを自動的に生成し、オブジェクトのアップロード時に、チャンクアップロードでオブジェクトの整合性を検証します。

AWS SDK を使用しているときに追跡チェックサムを作成するには、`ChecksumAlgorithm` パラメータに任意のアルゴリズムを指定します。SDK は、そのアルゴリズムを使用してオブジェクト (またはオブジェクトパート) のチェックサムを計算し、チャンクアップロードリクエストの最後に自動的に追加します。この動作により、Amazon S3 はデータの検証とアップロードを単一のパスで実行するため、時間を節約できます。

> **Important**
>
> S3 オブジェクト Lambda を使用している場合、S3 オブジェクト Lambda へのすべてのリクエストは、`s3` の代わりに `s3-object-lambda` を使用して署名されます。この動作は、追跡チェックサム値のシグネチャに影響します。S3 Object Lambda, の詳細については、「S3 Object Lambda を使用したオブジェクトの変換」を参照してください。

末尾のチェックサムヘッダー

チャンクコンテンツエンコードのリクエストを行うために、Amazon S3 では、リクエストを正しく解析するためにクライアントに複数のヘッダーを含める必要があります。クライアントには、次のヘッダーを含める必要があります。

- **`x-amz-decoded-content-length`**: このヘッダーは、リクエストとともに Amazon S3 にアップロードされる実際のデータのプレーンテキストサイズを示します。
- **`x-amz-content-sha256`**: このヘッダーは、リクエストに含まれるチャンクアップロードのタイプを示します。チェックサムが末尾にあるチャンクアップロードの場合、ヘッダー値は、ペイロード署名を使用しないリクエストの場合は `STREAMING-UNSIGNED-PAYLOAD-TRAILER`、SigV4 ペイロード署名を使用するリクエストの場合は `STREAMING-AWS4-HMAC-SHA256-PAYLOAD-TRAILER` です。(署名付きペイロードの実装の詳細については、「Signature calculations for the authorization header: Transferring a payload in multiple chunks」を参照してください。)
- **`x-amz-trailer`**: このヘッダーは、リクエストの末尾のヘッダーの名前を示します。末尾のチェックサムが存在する場合 (AWS SDK がエンコードされたリクエスト本文にチェックサムを追

加する場合)、x-amz-trailer ヘッダー値には x-amz-checksum- プレフィックスが含まれ、アルゴリズム名で終わります。現在、次の x-amz-trailer 値がサポートされています。

- x-amz-checksum-crc32
- x-amz-checksum-crc32c
- x-amz-checksum-crc64nvme
- x-amz-checksum-sha1
- x-amz-checksum-sha256

> **Note**
>
> リクエストには、チャンク化された値を含む Content-Encoding ヘッダーを含めることもできます。このヘッダーは必須ではありませんが、このヘッダーを含めることで、エンコードされたデータを送信する際の HTTP プロキシの問題を最小限に抑えることができます。リクエストに別の Content-Encoding ヘッダー (gzip など) が存在する場合、Content-Encoding ヘッダーには、エンコードのカンマ区切りリストにチャンク化された値が含まれます。例えば、Content-Encoding: aws-chunked, gzip。

チャンクパーツ

チャンクエンコードを使用して Amazon S3 にオブジェクトをアップロードする場合、アップロードリクエストには次のタイプのチャンク (リストされた順序でフォーマット) が含まれます。

- オブジェクト本体のチャンク: チャンクアップロードリクエストに関連付けられた本体チャンクは、1 つ、複数、またはゼロの場合があります。
- 完了チャンク: チャンクアップロードリクエストに関連付けられた本体チャンクは、1 つ、複数、またはゼロの場合があります。
- 末尾チャンク: 末尾のチェックサムは、完了チャンクの後に表示されます。末尾のチャンクは 1 つだけ許可されます。

> **Note**
>
> チャンクアップロードはすべて、リクエストの終了を示すために、最後の CRLF (\r\n など) で終わる必要があります。

チャンク形式の例については、「例: 末尾にチェックサムが付いたチャンクアップロード」を参照してください。

オブジェクト本体のチャンク

オブジェクト本体のチャンクは、S3 にアップロードされる実際のオブジェクトデータを含むチャンクです。これらのチャンクには、一貫したサイズと形式の制約があります。

オブジェクト本体のチャンクサイズ

これらのチャンクには、少なくとも 8,192 バイト (または 8 KiB) のオブジェクトデータが含まれている必要があります。ただし、最後の本体チャンクは小さい場合があります。明示的な最大チャンクサイズはありませんが、すべてのチャンクが 5 GB の最大アップロードサイズより小さくなることが予想されます。チャンクサイズは、クライアントサーバーの実装に応じてチャンクごとに異なる場合があります。

オブジェクト本体のチャンク形式

オブジェクト本体のチャンクは、オブジェクト本体チャンク内のバイト数の 16 進エンコードで始まり、CRLF (キャリッジリターンラインフィード)、そのチャンクのオブジェクトバイト、および別の CRLF が続きます。

例:

```
hex-encoding-of-object-bytes-in-chunk\r\n
chunk-object-bytes\r\n
```

ただし、チャンクが署名されている場合、オブジェクト本体のチャンクは別の形式に従います。この形式では、署名がセミコロン区切り文字でチャンクサイズに追加されます。例:

```
hex-encoding-of-object-bytes-in-chunk;chunk-signature\r\n
 chunk-object-bytes\r\n
```

チャンク署名の詳細については、「Signature calculations for the Authorization Header: Transferring a payload in multiple chunks (AWS Signature Version 4)」を参照してください。チャンクの形式の詳細については、RFC Editor ウェブサイトの「Chunked transfer encoding」を参照してください。

完了チャンク

完了チャンクは、すべてのチャンクアップロードの最後のオブジェクト本体チャンクである必要があります。完了チャンクの形式は本体チャンクに似ていますが、常に 0 バイトのオブジェクトデータ

が含まれています。(オブジェクトデータの 0 バイトは、すべてのデータがアップロードされたことを示します。) チャンクアップロードには、次のような形式に従って、最後のオブジェクト本体チャンクとして完了チャンクを含める必要があります。

```
0\r\n
```

ただし、コンテンツエンコードリクエストでペイロード署名が使用されている場合、代わりに次の形式に従います。

```
0;chunk-signature\r\n
```

トレーラーチャンク

トレーラーチャンクは、すべての S3 アップロードリクエストの計算されたチェックサムを保持します。トレーラーチャンクには、ヘッダー名フィールド 1 つとヘッダー値フィールド 1 つの 2 つのフィールドが含まれます。アップロードリクエストのヘッダー名フィールドは、`x-amz-trailer` リクエストヘッダーに渡された値と一致する必要があります。例えば、リクエストに `x-amz-trailer: x-amz-checksum-crc32` が含まれており、トレーラーチャンクにヘッダー名 `x-amz-checksum-sha1` がある場合、リクエストは失敗します。トレーラーチャンクの値フィールドには、そのオブジェクトのビッグエンディアンチェックサム値の base64 エンコードが含まれます。(ビッグエンディアンの順序では、最上位バイトのデータが最小のメモリアドレスに、最下位バイトが最大メモリアドレスに保存されます)。このチェックサムの計算に使用されるアルゴリズムは、ヘッダー名のサフィックス (例: `crc32`) と同じです。

トレーラーチャンク形式

トレーラーチャンクは、署名なしペイロードリクエストに次の形式を使用します。

```
x-amz-checksum-lowercase-checksum-algorithm-name:base64-checksum-value\n\r\n\r\n
```

SigV4 署名付きペイロードを使用したリクエストの場合、トレーラーチャンクには、トレーラーチャンクの後にトレーラー署名が含まれます。

```
trailer-checksum\n\r\n
trailer-signature\r\n
```

また、CRLF を base64 チェックサム値の末尾に直接追加することもできます。例:

```
x-amz-checksum-lowercase-checksum-algorithm-name:base64-checksum-value\r\n\r\n
```

例: 末尾にチェックサムが付いたチャンクアップロード

Amazon S3 は、PutObject に aws-chunked コンテンツエンコードを使用するチャンクアップロードと、末尾のチェックサムを含む UploadPart リクエストをサポートします。

Example 1 – 末尾に CRC-32 チェックサムが付いた署名なしチャンク **PutObject** リクエスト

以下は、末尾に CRC-32 チェックサムが付いたチャンク PutObject リクエストの例です。この例では、クライアントは 3 つの署名なしチャンクに 17 KB のオブジェクトをアップロードし、x-amz-checksum-crc32 ヘッダーを使用して末尾に CRC-32 チェックサムチャンクを追加します。

```
PUT /Key+ HTTP/1.1
Host: amzn-s3-demo-bucket
Content-Encoding: aws-chunked
x-amz-decoded-content-length: 17408
x-amz-content-sha256: STREAMING-UNSIGNED-PAYLOAD-TRAILER
x-amz-trailer: x-amz-checksum-crc32

2000\r\n                                    // Object body chunk 1 (8192 bytes)
object-bytes\r\n
2000\r\n                                    // Object body chunk 2 (8192 bytes)
object-bytes\r\n
400\r\n                                     // Object body chunk 3 (1024 bytes)
object-bytes\r\n
0\r\n                                       // Completion chunk
x-amz-checksum-crc32:YABb/g==\n\r\n\r\n     // Trailer chunk (note optional \n
 character)
\r\n                                          // CRLF
```

レスポンスの例を次に示します。

```
HTTP/1.1 200
ETag: ETag
x-amz-checksum-crc32: YABb/g==
```

> **Note**
>
> チェックサム値の最後にあるラインフィード \n の使用は、クライアントによって異なる場合があります。

Example 2 – 末尾に CRC-32 (**CRC32**) チェックサムが付いた SigV4 署名付きチャンク **PutObject** リクエスト

以下は、末尾に CRC-32 チェックサムが付いたチャンク PutObject リクエストの例です。このリクエストは SigV4 ペイロード署名を使用します。この例では、クライアントは 3 つの署名付きチャンクに 17 KB のオブジェクトをアップロードします。object body チャンクに加えて、completion chunk と trailer chunk も署名されています。

```
PUT /Key+ HTTP/1.1
Host: amzn-s3-demo-bucket.s3.amazonaws.com
Content-Encoding: aws-chunked
x-amz-decoded-content-length: 17408
x-amz-content-sha256: STREAMING-AWS4-HMAC-SHA256-PAYLOAD-TRAILER
x-amz-trailer: x-amz-checksum-crc32

authorization-code                              // SigV4 headers authorization

2000;chunk-signature=signature-value...\r\n     // Object body chunk 1 (8192 bytes)
object-bytes\r\n
2000;chunk-signature\r\n                        // Object body chunk 2 (8192 bytes)
object-bytes\r\n
400;chunk-signature\r\n                         // Object body chunk 3 (1024 bytes)
object-bytes\r\n
0;chunk-signature\r\n                           // Completion chunk
x-amz-checksum-crc32:YABb/g==\n\r\n             // Trailer chunk (note optional \n
 character)
trailer-signature\r\n
\r\n                                            // CRLF
```

レスポンスの例を次に示します。

```
HTTP/1.1 200
ETag: ETag
x-amz-checksum-crc32: YABb/g==
```

Amazon S3 オブジェクトの削除

Amazon S3 コンソール、AWS SDK、AWS Command Line Interface (AWS CLI)、または REST API を使用して、Amazon S3 から 1 つ以上のオブジェクトを直接削除できます。例えば、ログファイルを収集している場合は、不要になったファイルを削除することをお勧めします。ログファイルなどのオブジェクトを自動的に削除する S3 ライフサイクルルールをセットアップできます。

オブジェクトを削除するには、次のいずれかの API オペレーションを使用できます。

- 単一のオブジェクトの削除 - Amazon S3 では DELETE (DeleteObject) API オペレーションを提供しています。これを使用すると、単一の HTTP リクエストで 1 つのオブジェクトを削除できます。
- 複数のオブジェクトの削除 - Amazon S3 では Multi-Object Delete (DeleteObjects) API を提供しています。これを使用すると、単一の HTTP リクエストで最大 1,000 個のオブジェクトを削除できます。

バージョニングが有効でないバケットからオブジェクトを削除する場合、オブジェクトキー名のみを指定します。ただし、バージョニングが有効なバケットからオブジェクトを削除する場合は、オブジェクトのバージョン ID を指定して、特定のバージョンのオブジェクトを削除することができます。

オブジェクトを削除する前に考慮すべきベストプラクティス

オブジェクトを削除する前に、次のベストプラクティスを考慮してください。

- バケットのバージョニングを有効にします。S3 バージョニングは、単純な DeleteObject リクエストに対する保護を追加し、誤って削除されないようにします。バージョニングされたバケットで、オブジェクトの現在のバージョンを削除するか、削除リクエストで特定のバージョン ID が指定されていない場合、Amazon S3 はオブジェクトを完全に削除しません。代わりに、S3 は削除マーカーを追加し、オブジェクトのソフト削除を発行します。削除マーカーは、新しいバージョン ID を持つオブジェクトの現在の (または最新の) バージョンになります。詳細については、「バージョニングが有効なバケットからのオブジェクトバージョンの削除」を参照してください。
- 多数のオブジェクトを削除する場合や、オブジェクト作成日に基づいてプログラムでオブジェクトを削除する場合は、バケットに S3 ライフサイクル設定を設定します。これらの削除をモニタリングするには、S3 ライフサイクルイベント通知を使用することをお勧めします。S3 ライフサイクル通知を設定すると、s3:LifecycleExpiration:Delete イベントタイプはバケット内のオブジェクトが削除されたときに通知します。また、S3 ライフサイクル設定によってオブジェクトバージョンが完全に削除された場合にも通知されます。s3:LifecycleExpiration:DeleteMarkerCreated イベントタイプは、S3 ライフサイクルが削除マーカーを作成するときに通知します。削除マーカーは、バージョニングされているバケット内のオブジェクトの最新バージョンが削除されると作成されます。
- S3 ライフサイクル設定を更新する前に、ライフサイクルが意図したすべてのオブジェクトに対するアクションを完了したことを確認します。詳細については、「バケットにライフサイクル設定を

設定する」の「ライフサイクルルールの更新、無効化、または削除」セクションを参照してください。

> **Note**
>
> S3 ライフサイクルルールは、意図しない削除を防ぐために、オブジェクトの正しいサブセットに適用する必要があります。ライフサイクルルールの作成時に、プレフィックス、オブジェクトタグ、またはオブジェクトサイズでオブジェクトをフィルタリングできます。

- ユーザーがバケットからオブジェクトを削除してしまうことを制限することを検討してください。ユーザーを制限するには、Amazon S3 バケットポリシーで次のアクションのアクセス許可を明示的に拒否する必要があります。
  - `s3:DeleteObject`、`s3:DeleteObjectVersion` (API リクエストを使用してオブジェクトを削除できるユーザーを制御するため)
  - `s3:PutLifecycleConfiguration` (S3 ライフサイクルの有効期限ルールを追加できるユーザーを制御するため)
- S3 レプリケーションを使用してデータの複数のコピーを作成し、一度に複数の場所にレプリケートすることを検討してください。必要に応じて、送信先バケットをいくつでも選択できます。さらに、オブジェクトが意図せずに削除された場合でも、データのコピーは保持されます。

バージョニングが有効なバケットからのオブジェクトの削除

バージョニングが有効なバケットの場合、同じオブジェクトの複数のバージョンがバケット内に存在する可能性があります。バージョニングが有効なバケットを操作する場合は、`Delete` API オペレーションで以下のオプションが可能です。

- バージョンを指定しない削除リクエストの指定 - オブジェクトのキーのみを指定し、バージョン ID は指定しません。この場合、Amazon S3 はオブジェクトの最新バージョンに対して削除マーカーを作成し、レスポンスでバージョン ID を返します。オブジェクトはバケットから消去されます。オブジェクトのバージョニングと削除マーカーの概念については、S3 バージョニングによる複数のバージョンのオブジェクトの保持 を参照してください。
- バージョンを指定した削除リクエストの指定 – キーとバージョン ID の両方を指定します。この場合、以下の結果が想定されます。
  - バージョン ID が特定のオブジェクトバージョンにマッピングされている場合、Amazon S3 はその特定のバージョンのオブジェクトを削除します。

- バージョン ID がそのオブジェクトの削除マーカーに対応する場合、Amazon S3 は削除マーカーを削除します。削除マーカーが削除されると、オブジェクトがバケットに再表示されます。

バージョニングが停止されたバケットからのオブジェクトの削除

バケットのバージョニングが一時停止されている場合、Delete API オペレーションは、バージョニングが有効になっているバケットに対して同じように動作します (現在のバージョンに null バージョン ID がある場合を除く)。詳細については、「バージョニングが停止されたバケットからのオブジェクトの削除」を参照してください。

バージョン管理されていないバケットからのオブジェクトの削除

バケットがバージョン変更されていない場合は、Delete API オペレーションでオブジェクトのキーを指定できます。Amazon S3 はオブジェクトを完全に削除します。オブジェクトの永続的な削除を防ぐには、バケットのバージョニングを有効にします。

MFA 対応のバケットからのオブジェクトの削除

多エレメント認証 (MFA) 対応のバケットからオブジェクトを削除する場合は、以下の点に注意してください。

- 無効な MFA トークンを指定した場合、リクエストは常に失敗します。
- MFA 対応のバケットがあり、バージョンを指定した削除リクエストを行う (オブジェクトのキーとバージョン ID を指定する) 場合、有効な MFA トークンを指定しないとリクエストは失敗します。さらに、MFA 対応バケットに対してマルチオブジェクト Delete API オペレーションを使用する際、いずれかの削除がバージョンを指定した削除リクエストである場合 (つまり、オブジェクトのキーとバージョン ID を指定した場合)、MFA トークンを指定しないとリクエスト全体が失敗します。

ただし、以下の場合、リクエストは成功します。

- MFA 対応バケットを使用していて、バージョンを指定しない削除リクエストを行う (バージョニングされたオブジェクトを削除しない) 場合、MFA トークンを指定しなくても削除は成功します。
- Multi-Object Delete リクエストで、MFA 対応バケットからバージョニング非対応のオブジェクトのみを削除するように指定した場合、MFA トークンを指定しなくても削除は成功します。

MFA 削除の詳細については、「MFA 削除の設定」を参照してください。

トピック

- 単一のオブジェクトの削除
- 複数のオブジェクトの削除

単一のオブジェクトの削除

Amazon S3 コンソールまたは DELETE API を使用して、S3 バケットから 1 つの既存のオブジェクトを削除できます。Amazon S3 でのオブジェクト削除の詳細については、「Amazon S3 オブジェクトの削除」を参照してください。

S3 バケット内のすべてのオブジェクトによりストレージコストが生じるため、不要になったオブジェクトを削除する必要があります。例えば、ログファイルを収集している場合は、不要になったファイルを削除することをお勧めします。ログファイルなどのオブジェクトを自動的に削除するライフサイクルルールをセットアップできます。詳細については、the section called “ライフサイクル設定の指定” を参照してください。

Amazon S3 の機能と料金の詳細については、Amazon S3 料金を参照してください。

S3 コンソールの使用

Amazon S3 コンソールを使用してバケットから 1 つのオブジェクトを削除するには、以下の手順に従ってください。

> **Warning**
>
> Amazon S3 コンソールでオブジェクトまたは指定されたオブジェクトバージョンを完全に削除した場合、削除を元に戻すことはできません。

バージョニングが有効化または停止されているオブジェクトを削除するには

> **Note**
>
> バージョニングが停止されたバケット内のオブジェクトのバージョン ID が NULL とマークされている場合、S3 は以前のバージョンが存在しないためオブジェクトを完全に削除します。ただし、バージョニングが停止されたバケット内のオブジェクトに有効なバージョン ID が一覧表示されている場合、S3 は削除されたオブジェクトの削除マーカーを作成し、オブジェクトの以前のバージョンを保持します。

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[汎用バケット] または [ディレクトリバケット] を選択します。
3. バケットリストで、オブジェクトを削除するバケットの名前を選択します。
4. オブジェクトを選択した後、[削除] を選択します。
5. [指定されたオブジェクト] に表示されているオブジェクトが削除されていることを確認するには、[オブジェクトを削除しますか?] テキスト ボックスに「**delete**」と入力します。

バージョニングが有効なバケット内の特定のオブジェクトバージョンを完全に削除するには

> **Warning**
>
> Amazon S3 で指定されたオブジェクトバージョンを完全に削除した場合、削除を元に戻すことはできません。

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. [バケット] リストで、オブジェクトを削除するバケットの名前を選択します。
3. 削除するオブジェクトを選択します。
4. [バージョンを表示] トグルを選択します。
5. オブジェクトバージョンを選択した後、[削除] を選択します。
6. [指定されたオブジェクト] に表示されている特定のオブジェクトバージョンが完全に削除されていることを確認するには、[オブジェクトを削除しますか?] テキスト ボックスに 「完全に削除」と入力します。Amazon S3 がその特定のオブジェクトバージョンを完全に削除します。

バージョニングが有効になっていない Amazon S3 バケット内のオブジェクトを完全に削除するには

> **Warning**
>
> Amazon S3 でオブジェクトを完全に削除した場合、削除を元に戻すことはできません。また、バージョニングが有効になっていないバケットの場合、削除は恒久的です。

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[汎用バケット] を選択します。
3. バケットリストで、オブジェクトを削除するバケットの名前を選択します。
4. オブジェクトを選択した後、[削除] を選択します。
5. [指定されたオブジェクト] に表示されているオブジェクトが完全に削除されていることを確認するには、[オブジェクトを削除しますか?] テキスト ボックスに [完全に削除] と入力します。

> **Note**
>
> オブジェクトの削除に問題がある場合は、「バージョニングされたオブジェクトを完全に削除する」を参照してください。

AWS CLI を使用する場合

1 件のリクエストで 1 つのオブジェクトを削除するには、DELETE API を使用します。詳細については、DELETE オブジェクトを参照してください。CLI を使用してオブジェクトを削除する方法の詳細については、delete-object」参照してください。

REST API の使用

AWS SDK を使用して、1 つのオブジェクトを削除できます。ただし、アプリケーションで必要な場合は、REST リクエストを直接送信できます。詳細については、Amazon Simple Storage Service API リファレンスの DELETE Object を参照してください。

AWS SDK の使用

以下の例では、AWS SDK を使用してバケットからオブジェクトを削除する方法を示します。詳細については、Amazon Simple Storage Service API リファレンスの DELETE Object を参照してください。

バケットで S3 バージョニングが有効化されている場合は、以下のオプションを使用できます。

- バージョン ID を指定して、特定のオブジェクトバージョンを削除します。
- バージョン ID を指定しないでオブジェクトを削除します。この場合、Amazon S3 によってオブジェクトに削除マーカーが追加されます。

S3 バージョニングの詳細については、S3 バージョニングによる複数のバージョンのオブジェクトの保持 を参照してください。

その他の例や、他の言語での例については、「Amazon S3 API reference」の「Use DeleteObject with an AWS SDK or CLI」を参照してください。

Java

Example 例 1: オブジェクトを削除する (バージョニング非対応のバケット)

この例では、バケットでバージョン管理が有効になっておらず、オブジェクトにバージョン ID がないことを前提としてます。削除リクエストで、オブジェクトキーのみを指定し、バージョン ID を指定しません。

作業サンプルの作成およびテストの手順については、「AWS SDK for Java のデベロッパーガイド」の「使用開始」を参照してください。

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.DeleteObjectRequest;

import java.io.IOException;

public class DeleteObjectNonVersionedBucket {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String keyName = "*** Key name ****";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();

            s3Client.deleteObject(new DeleteObjectRequest(bucketName, keyName));
        } catch (AmazonServiceException e) {
```

```
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Example 例 2: オブジェクトを削除する (バージョニング対応のバケット)

次の例では、バージョニング対応のバケットからオブジェクトを削除します。オブジェクトのキー名とバージョン ID を指定して特定のオブジェクトを削除します。

この例では、次のような処理を実行します。

1. サンプルオブジェクトをバケットに追加します。Amazon S3 は新しく追加されたオブジェクトのバージョン ID を返します。この例では、このバージョン ID を削除リクエストで使用します。
2. オブジェクトのキー名とバージョン ID の両方を指定してオブジェクトバージョンを削除します。オブジェクトに他のバージョンがない場合、Amazon S3 はオブジェクトを完全に削除します。それ以外の場合、Amazon S3 は指定されたバージョンのみを削除します。

> **Note**
>
> オブジェクトのバージョン ID は、`ListVersions` リクエストを送信して取得できます。

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.BucketVersioningConfiguration;
import com.amazonaws.services.s3.model.DeleteVersionRequest;
```

```
import com.amazonaws.services.s3.model.PutObjectResult;

import java.io.IOException;

public class DeleteObjectVersionEnabledBucket {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String keyName = "*** Key name ****";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();

            // Check to ensure that the bucket is versioning-enabled.
            String bucketVersionStatus =
 s3Client.getBucketVersioningConfiguration(bucketName).getStatus();
            if (!bucketVersionStatus.equals(BucketVersioningConfiguration.ENABLED))
 {
                System.out.printf("Bucket %s is not versioning-enabled.",
 bucketName);
            } else {
                // Add an object.
                PutObjectResult putResult = s3Client.putObject(bucketName, keyName,
                        "Sample content for deletion example.");
                System.out.printf("Object %s added to bucket %s\n", keyName,
 bucketName);

                // Delete the version of the object that we just created.
                System.out.println("Deleting versioned object " + keyName);
                s3Client.deleteVersion(new DeleteVersionRequest(bucketName, keyName,
 putResult.getVersionId()));
                System.out.printf("Object %s, version %s deleted\n", keyName,
 putResult.getVersionId());
            }
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
```

```
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

.NET

以下の例では、バージョニング対応および非対応のバケットからオブジェクトを削除する方法を示します。S3 バージョニングの詳細については、S3 バージョニングによる複数のバージョンのオブジェクトの保持 を参照してください。

Example バージョニング非対応バケットからのオブジェクトの削除

次の C# の例では、バージョニング非対応のバケットからオブジェクトを削除します。この例では、オブジェクトにバージョン ID がないため、バージョン ID を指定しないものとします。オブジェクトキーのみ指定します。

コード例を設定および実行する方法の詳細については、「AWS SDK for .NET デベロッパーガイド」の「AWS SDK for .NET の開始方法」 を参照してください。

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class DeleteObjectNonVersionedBucketTest
    {
        private const string bucketName = "*** bucket name ***";
        private const string keyName = "*** object key ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 client;

        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            DeleteObjectNonVersionedBucketAsync().Wait();
```

```
        }
        private static async Task DeleteObjectNonVersionedBucketAsync()
        {
            try
            {
                var deleteObjectRequest = new DeleteObjectRequest
                {
                    BucketName = bucketName,
                    Key = keyName
                };

                Console.WriteLine("Deleting an object");
                await client.DeleteObjectAsync(deleteObjectRequest);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
 deleting an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 deleting an object", e.Message);
            }
        }
    }
}
```

Example バージョニング対応バケットからのオブジェクトの削除

次の C# の例では、バージョニング対応のバケットからオブジェクトを削除します。オブジェクトのキー名とバージョン ID を指定してオブジェクトの特定のバージョンを削除します。

このコードでは、以下のタスクを実行します。

1. 指定したバケットの S3 バージョニングを有効にします (S3 バージョニングが既に有効になっている場合は効果がありません)。
2. サンプルオブジェクトをバケットに追加します。レスポンスとして、Amazon S3 は新しく追加されたオブジェクトのバージョン ID を返します。この例では、このバージョン ID を削除リクエストで使用します。
3. オブジェクトのキー名とバージョン ID の両方を指定してサンプルオブジェクトを削除します。

> **Note**
>
> オブジェクトのバージョン ID は、ListVersions リクエストを送信して取得することもできます。
>
> ```
> var listResponse = client.ListVersions(new ListVersionsRequest { BucketName
>  = bucketName, Prefix = keyName });
> ```

コード例を設定および実行する方法の詳細については、「AWS SDK for .NET デベロッパーガイド」の「AWS SDK for .NET の開始方法」 を参照してください。

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class DeleteObjectVersion
    {
        private const string bucketName = "*** versioning-enabled bucket name ***";
        private const string keyName = "*** Object Key Name ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 client;

        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            CreateAndDeleteObjectVersionAsync().Wait();
        }

        private static async Task CreateAndDeleteObjectVersionAsync()
        {
            try
            {
                // Add a sample object.
                string versionID = await PutAnObject(keyName);
```

```
                // Delete the object by specifying an object key and a version ID.
                DeleteObjectRequest request = new DeleteObjectRequest
                {
                    BucketName = bucketName,
                    Key = keyName,
                    VersionId = versionID
                };
                Console.WriteLine("Deleting an object");
                await client.DeleteObjectAsync(request);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
 deleting an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 deleting an object", e.Message);
            }
        }

        static async Task<string> PutAnObject(string objectKey)
        {
            PutObjectRequest request = new PutObjectRequest
            {
                BucketName = bucketName,
                Key = objectKey,
                ContentBody = "This is the content body!"
            };
            PutObjectResponse response = await client.PutObjectAsync(request);
            return response.VersionId;
        }
    }
}
```

PHP

このトピックでは、バージョン 3 の AWS SDK for PHP のクラスを使用して、バージョニング非対応のバケットからオブジェクトを削除する方法を示します。バージョニング対応のバケットから 1 つのオブジェクトを削除する方法については、REST API の使用 を参照してください。

AWS SDK for Ruby API の詳細については、AWS SDK for Ruby - バージョン 2 を参照してください。

次の PHP の例では、バケットからオブジェクトを削除します。この例で示す方法では、バージョニング非対応のバケットからオブジェクトを削除するため、削除リクエストではバケット名とオブジェクトキーのみを指定し、バージョン ID は指定しません。

```
<?php

require 'vendor/autoload.php';

use Aws\S3\S3Client;
use Aws\S3\Exception\S3Exception;

$bucket = '*** Your Bucket Name ***';
$keyname = '*** Your Object Key ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

// 1. Delete the object from the bucket.
try
{
    echo 'Attempting to delete ' . $keyname . '...' . PHP_EOL;

    $result = $s3->deleteObject([
        'Bucket' => $bucket,
        'Key'    => $keyname
    ]);

    if ($result['DeleteMarker'])
    {
        echo $keyname . ' was deleted or does not exist.' . PHP_EOL;
    } else {
        exit('Error: ' . $keyname . ' was not deleted.' . PHP_EOL);
    }
}
catch (S3Exception $e) {
    exit('Error: ' . $e->getAwsErrorMessage() . PHP_EOL);
}
```

```
// 2. Check to see if the object was deleted.
try
{
    echo 'Checking to see if ' . $keyname . ' still exists...' . PHP_EOL;

    $result = $s3->getObject([
        'Bucket' => $bucket,
        'Key'    => $keyname
    ]);

    echo 'Error: ' . $keyname . ' still exists.';
}
catch (S3Exception $e) {
    exit($e->getAwsErrorMessage());
}
```

Javascript

```
import { DeleteObjectCommand } from "@aws-sdk/client-s3";
import { s3Client } from "./libs/s3Client.js" // Helper function that creates Amazon
 S3 service client module.

export const bucketParams = { Bucket: "BUCKET_NAME", Key: "KEY" };

export const run = async () => {
  try {
    const data = await s3Client.send(new DeleteObjectCommand(bucketParams));
    console.log("Success. Object deleted.", data);
    return data; // For unit tests.
  } catch (err) {
    console.log("Error", err);
  }
};
run();
```

複数のオブジェクトの削除

S3 バケット内のすべてのオブジェクトによりストレージコストが生じるため、不要になったオブジェクトを削除する必要があります。例えば、ログファイルを収集している場合は、不要になったファイルを削除することをお勧めします。ログファイルなどのオブジェクトを自動的に削除するライ

フサイクルルールをセットアップできます。詳細については、the section called “ライフサイクル設定の指定” を参照してください。

Amazon S3 の機能と料金の詳細については、「Amazon S3 の料金」を参照してください。

Amazon S3 コンソール、AWS SDK、または REST API を使用して、S3 バケットから複数のオブジェクトを同時に削除できます。

S3 コンソールの使用

Amazon S3 コンソールを使用してバケットから複数のオブジェクトを削除するには、以下の手順に従ってください。

Warning

- 指定されたオブジェクトを削除すると元に戻せません。
- このアクションは、指定されたすべてのオブジェクトを削除します。フォルダを削除する場合は、削除アクションが完了するのを待ってから、フォルダに新しいオブジェクトを追加します。そうしなければ、新しいオブジェクトも削除される可能性があります。
- ディレクトリバケットを含め、バージョニングが有効でないバケットのオブジェクトを削除すると、Amazon S3 はオブジェクトを恒久的に削除します。
- バケットバージョニングが有効または停止のバケットのオブジェクトを削除すると、Amazon S3 が削除マーカーを作成します。詳細については、「削除マーカーの使用」を参照してください。

バージョニングが有効化または停止されているオブジェクトを削除するには

Note

バージョニングが停止されたバケット内のオブジェクトのバージョン ID が NULL とマークされている場合、S3 は以前のバージョンが存在しないためオブジェクトを完全に削除します。ただし、バージョニングが停止されたバケット内のオブジェクトに有効なバージョン ID が一覧表示されている場合、S3 は削除されたオブジェクトの削除マーカーを作成し、オブジェクトの以前のバージョンを保持します。

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[汎用バケット] を選択します。
3. バケットリストで、オブジェクトを削除するバケットの名前を選択します。
4. オブジェクトを選択した後、[削除] を選択します。
5. [指定されたオブジェクト] に表示されているオブジェクトが削除されていることを確認するには、[オブジェクトを削除しますか?] テキスト ボックスに「**delete**」と入力します。

バージョニングが有効なバケット内の特定のオブジェクトバージョンを完全に削除するには

> **Warning**
>
> Amazon S3 で指定されたオブジェクトバージョンを完全に削除した場合、削除を元に戻すことはできません。

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[汎用バケット] を選択します。
3. バケットリストで、オブジェクトを削除するバケットの名前を選択します。
4. 削除したい オブジェクトを選択します。
5. [バージョンを表示] トグルを選択します。
6. オブジェクトバージョンを選択した後、[削除] を選択します。
7. [指定されたオブジェクト] に表示されている特定のオブジェクトバージョンが完全に削除されていることを確認するには、[オブジェクトを削除しますか?] テキスト ボックスに 「完全に削除」と入力します。Amazon S3 がその特定のオブジェクトバージョンを完全に削除します。

バージョニングが有効になっていない Amazon S3 バケット内のオブジェクトを完全に削除するには

> **Warning**
>
> Amazon S3 でオブジェクトを完全に削除した場合、削除を元に戻すことはできません。また、ディレクトリバケットを含め、バージョニングが有効になっていないバケットの場合、削除は恒久的です。

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[汎用バケット] または [ディレクトリバケット] を選択します。
3. バケットリストで、オブジェクトを削除するバケットの名前を選択します。
4. オブジェクトを選択した後、[削除] を選択します。
5. [指定されたオブジェクト] に表示されているオブジェクトが完全に削除されていることを確認するには、[オブジェクトを削除しますか?] テキスト ボックスに [完全に削除] と入力します。

> **Note**
>
> オブジェクトの削除に問題がある場合は、「バージョニングされたオブジェクトを完全に削除する」を参照してください。

AWS SDK の使用

AWS SDK を使用して複数のオブジェクトを削除する方法の例については、「Amazon S3 API リファレンス」の「コードの例」を参照してください。

さまざまな AWS SDK の使用に関する一般的な情報については、「Amazon S3 API リファレンス」の「Developing with Amazon S3 using the AWS SDKs」を参照してください。

REST API の使用

AWS SDK を使用して、Multi-Object Delete API で複数のオブジェクトを削除できます。ただし、アプリケーションで必要な場合は、REST リクエストを直接送信できます。

詳細については、Amazon Simple Storage Service API リファレンスの複数オブジェクトの削除を参照してください。

オブジェクトの整理、リスト化、使用

Amazon S3 では、プレフィックスを使用してストレージを整理できます。プレフィックスは、バケット内のオブジェクトの論理グループです。プレフィックス値は、バケット内の同じディレクトリに同様のデータを保存するためのディレクトリ名に似ています。プログラムでオブジェクトをアップロードする場合は、プレフィックスを使用してデータを整理できます。

Amazon S3 コンソールでは、プレフィックスはフォルダと呼ばれます。バケットに移動すると、S3 コンソールですべてのオブジェクトとフォルダを表示できます。また、オブジェクトのプロパティなど、各オブジェクトに関する情報を表示することもできます。

Amazon S3 でのデータのリスト化と整理の詳細については、以下のトピックを参照してください。

トピック

- プレフィックスを使用してオブジェクトを整理する
- プログラムによるオブジェクトキーのリスト化
- フォルダを使用して Amazon S3 コンソールのオブジェクトを整理する
- Amazon S3 コンソールでのオブジェクトのプロパティの表示
- タグを使用してストレージを分類する

プレフィックスを使用してオブジェクトを整理する

プレフィックスを使用して、Amazon S3 バケットに保存するデータを整理できます。プレフィックスは、オブジェクトキー名の先頭にある文字列です。プレフィックスには、オブジェクトキー名の最大長 (1,024 バイト) を条件として、任意の長さを指定できます。プレフィックスは、ディレクトリと同様の方法でデータを整理する方法と考えることができます。ただし、プレフィックスはディレクトリではありません。

プレフィックスで検索すると、指定されたプレフィックスで始まるキーだけに結果が限定されます。区切り記号を使用すると、リストオペレーションによって、共通のプレフィックスを共有するすべてのキーが単一の要約リスト結果にまとめられます。

プレフィックスと区切り記号のパラメータの目的は、キーを階層的に構成および参照できるようにすることです。そのためには、まずバケットで使用する区切り記号を選択します。スラッシュ (/) など、キーの名前には使われないような記号を使用します。別の文字を区切り文字として使用できます。スラッシュ (/) 文字に特徴はありませんが、非常に一般的なプレフィックスの区切り文字です。次に、階層に含まれるすべてのレベルを連結し、各レベルを区切り記号で区切ることで、キーの名前を構成します。

例えば、都市に関する情報を格納するとしたら、大陸、国、州または県の順に情報を整理するのが自然でしょう。通常、これらの名前には句読点が含まれないため、区切り記号としてスラッシュ (/) を使用できます。以下の例ではスラッシュ (/) 区切り記号を使用しています。

- Europe/France/Nouvelle-Aquitaine/Bordeaux

- North America/Canada/Quebec/Montreal
- 北米/米国/ワシントン州/ベルビュー
- 北米/米国/ワシントン州/シアトル

世界中の全都市のデータをこの方法で格納した場合、階層のないフラットなキーネームスペースは管理しにくくなります。リストオペレーションで Prefix と Delimiter を使用することで、データをリストするために作成した階層を利用できます。例えば、米国のすべての州をリストするには、Delimiter='/' および Prefix='North America/USA/' をセットします。データが存在するカナダのすべての州をリストするには、Delimiter='/' および Prefix='North America/Canada/' をセットします。

区切り文字、プレフィックス、ネストフォルダの詳細については、「プレフィックスとネストされたフォルダの違い」を参照してください。

プレフィックスと区切り記号を使用したオブジェクトのリスト化

区切り記号付きのリストリクエストを発行すると、1 レベルの階層だけを参照でき、それより深いレベルで入れ子にされている (場合によっては数百万もの) キーはスキップおよび集約されます。例えば、次のキーを持つバケット (*amzn-s3-demo-bucket*) があるとします。

```
sample.jpg

photos/2006/January/sample.jpg

photos/2006/February/sample2.jpg

photos/2006/February/sample3.jpg

photos/2006/February/sample4.jpg
```

このサンプルバケットはルートレベルに sample.jpg オブジェクトだけを持ちます。バケット内のルートレベルオブジェクトだけを一覧表示するには、バケットに対する GET リクエストをスラッシュ (/) の区切り文字と共に送信します。Simple Storage Service (Amazon S3) からのレスポンスでは sample.jpg オブジェクトキーが返されます。このキーには / の区切り文字が含まれないためです。その他すべてのキーには区切り文字が含まれます。Amazon S3 によってこれらのキーがグループ化され、特定のプレフィックス値を持つ 1 つの CommonPrefixes 要素が返されます。この場合のプレフィックス値は photos/ であり、これはキーの先頭から、指定した区切り文字の最初の出現までのサブ文字列です。

Example

```
<ListBucketResult xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Name>amzn-s3-demo-bucket</Name>
  <Prefix></Prefix>
  <Marker></Marker>
  <MaxKeys>1000</MaxKeys>
  <Delimiter>/</Delimiter>
  <IsTruncated>false</IsTruncated>
  <Contents>
    <Key>sample.jpg</Key>
    <LastModified>2011-07-24T19:39:30.000Z</LastModified>
    <ETag>&quot;d1a7fb5eab1c16cb4f7cf341cf188c3d&quot;</ETag>
    <Size>6</Size>
    <Owner>
      <ID>75cc57f09aa0c8caeab4f8c24e99d10f8e7faeebf76c078efc7c6caea54ba06a</ID>
      <DisplayName>displayname</DisplayName>
    </Owner>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  <CommonPrefixes>
    <Prefix>photos/</Prefix>
  </CommonPrefixes>
</ListBucketResult>
```

プログラムによるオブジェクトキーのリスト化の詳細については、「プログラムによるオブジェクトキーのリスト化」を参照してください 。

プログラムによるオブジェクトキーのリスト化

Amazon S3 では、キーはプレフィックス別に一覧表示できます。関連するキーの名前に共通のプレフィックスを選択し、階層を区切る特殊文字でこれらのキーをマークすることができます。その後、リストオペレーションを使用して、キーを階層的に選択および参照できます。これは、ファイルシステムにおいてディレクトリ内にファイルを格納するしくみに似ています。

Amazon S3 では、バケット内のキーを列挙するためのリストオペレーションを公開します。キーはバケット別またはプレフィックス別にリストされます。例えば、すべての英単語のキーを含む「dictionary」という名前のバケットがあるとします。そして、そのバケット内の文字「q」で始まるキーをすべてリストするための呼び出しを行うとします。リストの結果は常に UTF-8 バイナリ順で返されます。

SOAP および REST のリストオペレーションではいずれも、条件に一致するキーの名前と、各キーによって識別されるオブジェクトに関する情報を含む XML ドキュメントが返されます。

> **Note**
>
> SOAP API は新規顧客には利用できず、2025 年 8 月 31 日にサポート終了 (EOL) となります。REST API か AWS SDK を使用することをお勧めします。

特殊な区切り記号で終わるプレフィックスを共有するキーのグループは、リストの目的で、その共通のプレフィックスによってロールアップできます。このような機能によりアプリケーションでは、キーを階層的に構成および参照できるようになります。ファイルシステムにおいてファイルをディレクトリに分けて整理するのに似ています。

例えば、英語以外の単語も含まれるように dictionary バケットを拡張するには、各単語にその言語と区切り記号のプレフィックスを付けることでキーを形成できます (「`French/logical`」など)。この命名スキームと階層リスト機能を使用すれば、フランス語の単語のリストだけを取得することもできます。また、対応している言語の最上位レベルのリストを参照することで、それより下の階層間に介在するすべてのキーを反復処理する必要もなくなります。リスト化における階層の役割については、プレフィックスを使用してオブジェクトを整理する を参照してください。

REST API

アプリケーションで必要な場合は、REST リクエストを直接送信できます。GET リクエストを送信して、バケット内の一部またはすべてのオブジェクトを返すことができます。または選択条件を使用して、バケット内のオブジェクトのサブセットを返すことができます。詳細については、Amazon Simple Storage Service API リファレンスの GET バケット (オブジェクトのリスト化) バージョン 2 を参照してください。

リスト実装の効率性

リスト化のパフォーマンスは、バケット内のキーの総数によって大きく影響されることはありません。`prefix`、`marker`、`maxkeys` または `delimiter` 引数の有無によって影響されることもありません。

複数ページの結果に対する反復処理

バケットに入れることのできるキーの数は実質的に無制限であるため、リストのクエリによっては結果が膨大な量になる可能性があります。大規模な結果セットを管理するため、Amazon S3 API で

はページ分割をサポートして結果セットを複数のレスポンスに分割します。キーリストのレスポンスごとに最大 1,000 個のキーを含むページと、レスポンスが切り捨てられているかどうかを示すインジケータが返されます。すべてのキーを受信するまで、一連のキーリストリクエストを送信します。AWSこのページ分割は、SDK ラッパーライブラリでも行うことができます。

例

バケット内のすべてのオブジェクトを一覧表示するときは、`s3:ListBucket` 権限が必要であることに注意してください。

CLI

list-objects

次の例は、`list-objects` コマンドを使用して、指定されたバケット内のすべてのオブジェクトの名前を表示します。

```
aws s3api list-objects --bucket text-content --query 'Contents[].{Key: Key, Size: Size}'
```

この例では、`--query` 引数を使用して `list-objects` の出力を各オブジェクトのキー値とサイズでフィルタリングしています。

オブジェクトの詳細については、Amazon S3 オブジェクトの使用 を参照してください。

- API の詳細については、「AWS CLI コマンドリファレンス」の「ListObjects」を参照してください。

ls

次の例では、`ls` コマンドを使用してバケット内のすべてのオブジェクトとプレフィックスを一覧表示します。

この例のコマンドを使うには、*amzn-s3-demo-bucket* を自分のバケットの名前に置き換えます。

```
$ aws s3 ls s3://amzn-s3-demo-bucket
```

- 高レベルコマンド `ls` の詳細については、「AWS Command Line Interface ユーザーガイド」の「バケットとオブジェクトの一覧表示」を参照してください。

PowerShell

Tools for PowerShell V4

例 1: このコマンドは、バケット「test-files」内のすべての項目に関する情報を取得します。

```
Get-S3Object -BucketName amzn-s3-demo-bucket
```

例 2: このコマンドは、バケット「test-files」内の項目「sample.txt」に関する情報を取得します。

```
Get-S3Object -BucketName amzn-s3-demo-bucket -Key sample.txt
```

例 3: このコマンドは、バケット「test-files」からプレフィックス「sample」を持つすべての項目に関する情報を取得します。

```
Get-S3Object -BucketName amzn-s3-demo-bucket -KeyPrefix sample
```

- API の詳細については、「AWS Tools for PowerShell Cmdlet Reference(V4)」の「ListObjects」を参照してください。

フォルダを使用して Amazon S3 コンソールのオブジェクトを整理する

Amazon S3 の汎用バケットでは、オブジェクトが主要なリソースであり、オブジェクトはバケットに格納されます。Amazon S3 汎用バケットはフラットな構造であり、ファイルシステムに見られるような階層はありません。ただし、構造を分かりやすくするため、Amazon S3 コンソールでは、オブジェクトのグループ化の方法としてフォルダの概念をサポートしています。コンソールでは、これを行うために、グループ化したオブジェクトに共有名のプレフィックスを使用します。つまり、グループ化したオブジェクトに共通の文字列で始まる名前が付けられます。この共通の文字列 (共有プレフィックス) がフォルダ名です。オブジェクト名はキー名とも呼ばれます。

例えば、コンソールの汎用バケットに photos という名前のフォルダを作成し、その中に myphoto.jpg という名前のオブジェクトを保存できます。このオブジェクトはキー名 photos/myphoto.jpg で保存され、photos/ がプレフィックスになります。

ここでは、さらに 2 つの例を示します。

- 汎用バケットに logs/date1.txt、logs/date2.txt、logs/date3.txt という 3 つのオブジェクトがある場合、コンソールには logs という名前のフォルダが表示されます。コンソールで

フォルダを開くと、date1.txt、date2.txt、date3.txt という 3 つのオブジェクトが表示されます。

- photos/2017/example.jpg という名前のオブジェクトがある場合、コンソールには、フォルダ 2017 を含む photos という名前のフォルダが表示されます。フォルダ 2017 にはオブジェクト example.jpg が含まれます。

フォルダ内にフォルダを作成できますが、バケット内にバケットを作成することはできません。オブジェクトをフォルダに直接アップロードしてコピーできます。フォルダは、作成、削除、公開することができますが、名前を変更することはできません。オブジェクトはフォルダ間でコピーすることができます。

Important

Amazon S3 コンソールでフォルダを作成すると、S3 は 0 バイトのオブジェクトを作成します。このオブジェクトキーには、指定したフォルダ名と末尾のスラッシュ (/) 文字が設定されます。例えば、Amazon S3 コンソールで、バケットに photos という名前のフォルダを作成した場合、Amazon S3 コンソールは photos/ キーを使用して 0 バイトのオブジェクトを作成します。コンソールは、フォルダの考え方をサポートするために、このオブジェクトを作成します。

また、末尾にスラッシュ文字 (/) を含む名前が付いている既存のオブジェクトは、Amazon S3 コンソールにフォルダとして表示されます。例えば、キー名 examplekeyname/ のオブジェクトは、Amazon S3 コンソールのフォルダとして表示され、オブジェクトとしては表示されません。それ以外の場合は、他のオブジェクトと同様に動作し、AWS Command Line Interface (AWS CLI)、AWS SDK、または REST API を使用して表示および操作できます。

さらに、キー名の末尾がスラッシュ文字 (/) のオブジェクトは、Amazon S3 コンソールを使用してアップロードすることができません。ただし、名前の末尾がスラッシュ (/) 文字のオブジェクトは、AWS Command Line Interface (AWS CLI)、AWS SDK、または REST API を使用してアップロードできます。

さらに、Amazon S3 コンソールは、他のオブジェクトのようにフォルダオブジェクトのコンテンツとメタデータを表示することはしません。コンソールを使用して名前の末尾がスラッシュ文字 (/) のオブジェクトをコピーすると、コピー先の場所に新しいフォルダが作成されますが、オブジェクトのデータとメタデータはコピーされません。また、オブジェクトキー名のスラッシュ (/) には特別な処理が必要になる場合があります。詳細については、「Amazon S3 オブジェクトに命名する」を参照してください。

ディレクトリバケットにフォルダを作成するには、フォルダをアップロードします。詳細については、「ディレクトリバケットへのオブジェクトのアップロード」を参照してください。

トピック

- フォルダの作成
- フォルダの公開
- フォルダサイズの計算
- フォルダの削除

フォルダの作成

このセクションでは、Amazon S3 コンソールを使用してフォルダを作成する方法について説明します。

> **Important**
>
> バケットポリシーが原因で、このバケットへのオブジェクトのアップロードを、タグ、メタデータ、またはアクセスコントロールリスト (ACL) の被付与者なしで行うことができない場合は、次の手順を使用してフォルダを作成することはできません。代わりに、空のフォルダをアップロードし、以下の設定をアップロード設定で指定します。

フォルダを作成するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[汎用バケット] を選択します。
3. バケットリストで、フォルダの作成先となるバケットの名前を選択します。
4. [オブジェクト] タブから、[フォルダの作成] を選択します。
5. フォルダの名前 (例: **`favorite-pics`**) を入力します。

> **Note**
>
> フォルダ名には特定の制限とガイドラインが適用され、オブジェクトのオブジェクトキー名の一部と見なされて、1,024 バイトに制限されます。詳細については、「the section called “オブジェクトに命名する”」を参照してください。

6. (オプション) バケットポリシーで特定の暗号化キーでオブジェクトを暗号化する必要がある場合は、[サーバー側の暗号化] で、[暗号化キーを指定する] を選択し、フォルダの作成時に同じ暗号化キーを指定する必要があります。指定しない場合、フォルダの作成は失敗します。
7. Create folder (フォルダの作成) を選択します。

フォルダの公開

パブリックフォルダまたはバケットが特別に必要な場合を除き、Amazon S3 フォルダまたはバケットへのすべてのパブリックアクセスをブロックすることをお勧めします。フォルダを公開すると、インターネット上の誰もがフォルダ内でグループ化されたすべてのオブジェクトを表示できます。

Amazon S3 コンソールでは、フォルダをパブリックにすることができます。データへのアクセスをプレフィックスで制限するバケットポリシーを作成して、フォルダを公開することもできます。詳細については、「Amazon S3 用 Identity and Access Management」を参照してください。

> **Warning**
>
> Amazon S3 コンソールでフォルダを公開した後は、非公開に戻すことはできません。代わりに、非公開にするパブリックフォルダ内の各オブジェクトのアクセス許可の設定で、オブジェクトへのパブリックアクセスを禁止する必要があります。詳細については、「ACL の設定」を参照してください。

トピック

- フォルダサイズの計算
- フォルダの削除

フォルダサイズの計算

このセクションでは、Amazon S3 コンソールを使用してフォルダのサイズを計算する方法について説明します。

フォルダのサイズを計算するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[汎用バケット] を選択します。

3. [汎用バケット] リストで、フォルダが保存されているバケットの名前を選択します。
4. [オブジェクト] リストで、フォルダの名前の横にあるチェックボックスをオンにします。
5. [Actions] (アクション) を選択し、[Calculate total size] (合計サイズを計算する) を選択します。

> **Note**
>
> ページから移動すると、フォルダ情報 (合計サイズを含む) は利用できなくなります。合計サイズを再度表示するには、計算をやり直す必要があります。

> **Important**
>
> バケット内の指定されたオブジェクトまたはフォルダで [Calculate total size] (合計サイズを計算する) アクションを使用すると、Amazon S3 はオブジェクトの総数と合計ストレージサイズを計算します。ただし、不完全または進行中のマルチパートのアップロード、および以前のバージョンまたは最新ではないバージョンは、オブジェクトの総数または合計サイズには含まれません。このアクションは、バケットに保存されている各オブジェクトの現在のバージョンまたは最新バージョンのオブジェクトの総数と合計サイズのみを計算します。例えば、バケット内に 2 つのバージョンのオブジェクトがある場合、Amazon S3 のストレージ計算ツールはそれらを 1 つのオブジェクトとしてしかカウントしません。そのため、Amazon S3 コンソールで計算されるオブジェクトの総数は、S3 ストレージレンズに表示される [オブジェクト数] メトリクスや Amazon CloudWatch メトリクス、`NumberOfObjects` によって報告される数と異なる場合があります。同様に、ストレージの合計サイズは、S3 Storage Lens に表示される [Total Storage] (ストレージの合計) メトリクスや CloudWatch に表示される `BucketSizeBytes` メトリクスと異なる場合があります。

フォルダの削除

このセクションでは、Amazon S3 コンソールを使用して S3 バケットからフォルダを削除する方法について説明します。

Amazon S3 の機能と料金の詳細については、Amazon S3 を参照してください。

S3 バケットからフォルダを削除するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[汎用バケット] を選択します。
3. [汎用バケット] リストで、フォルダを削除するバケットの名前を選択します。
4. [オブジェクト] リストで、削除するフォルダとオブジェクトの横にあるチェックボックスをオンにします。
5. [削除] を選択します。
6. [オブジェクトの削除] ページで、削除するために選択したフォルダとオブジェクトの名前が、[指定されたオブジェクト] の下にリストされていることを確認します。
7. [オブジェクトの削除] ボックスに「**delete**」と入力し、[オブジェクトの削除] をクリックします。

> **Warning**
>
> このアクションは、指定されたすべてのオブジェクトを削除します。フォルダを削除する場合は、削除アクションが完了するのを待ってから、フォルダに新しいオブジェクトを追加します。そうしなければ、新しいオブジェクトも削除される可能性があります。

Amazon S3 コンソールでのオブジェクトのプロパティの表示

Amazon S3 コンソールを使用して、ストレージクラス、暗号化設定、タグ、メタデータなどのオブジェクトのプロパティを表示できます。

オブジェクトのプロパティを表示するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[汎用バケット] または [ディレクトリバケット] を選択します。
3. バケットリストで、そのオブジェクトを含むバケットの名前を選択します。
4. [オブジェクト] リストで、プロパティを表示するオブジェクトの名前を選択します。

   オブジェクトの [オブジェクトの概要] が開きます。下にスクロールすると、オブジェクトのプロパティを表示できます。

5. [オブジェクトの概要] ページでは、以下のオブジェクトのプロパティを表示または設定できます。

> **Note**
>
> - ストレージクラス、暗号化、メタデータなどのプロパティを変更すると、新しいオブジェクトが作成され、古いオブジェクトが置き換えられます。S3 バージョニングが有効になっている場合は、オブジェクトの新しいバージョンが作成され、既存のオブジェクトが古いバージョンになります。また、プロパティを変更するロールは、新しいオブジェクト (オブジェクトのバージョン) の所有者になります。
> - ユーザー定義タグを持つオブジェクトのストレージクラス、暗号化 、またはメタデータプロパティを変更する場合は、`s3:GetObjectTagging` アクセス許可が必要です。ユーザー定義タグがなく、サイズが 16 MB を超えるオブジェクトのプロパティを変更する場合は、`s3:GetObjectTagging` アクセス許可も必要です。
>
> ターゲットバケットポリシーによって `s3:GetObjectTagging` アクションが拒否されると、オブジェクトのこれらのプロパティは更新されますが、ユーザー定義タグはオブジェクトから削除され、エラーが発生します。

a. Storage class – Amazon S3 内にある各オブジェクトには、ストレージクラスが関連付けられています。オブジェクトにアクセスする頻度に応じて、使用するストレージクラスを選択します。汎用バケット内の S3 オブジェクトのデフォルトのストレージクラスは STANDARD です。ディレクトリバケット内の S3 オブジェクトのデフォルトストレージクラスは、S3 Express One Zone です。オブジェクトをアップロードするときに使用するストレージクラス選択します。ストレージクラスの詳細については、Amazon S3 ストレージクラスの理解と管理 を参照してください。

   オブジェクトを汎用バケットにアップロードした後にストレージクラスを変更するには、[ストレージクラス] を選択します。目的のストレージクラスを選択し、[保存] を選択します。

   > **Note**
   >
   > ディレクトリバケット内のオブジェクトのストレージクラスは変更できません。

b. サーバー側の暗号化設定 - サーバー側の暗号化を使用して S3 オブジェクトを暗号化できます。詳細については、AWS KMS (SSE-KMS) によるサーバー側の暗号化の指定 または Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3) の指定 を参照してください。

c. Metadata – Amazon S3 内の各オブジェクトには、それぞれのメタデータを表す一連の名前/値ペアがあります。S3 オブジェクトにメタデータを追加する方法については、「Amazon S3 コンソールでのオブジェクトメタデータの編集」を参照してください。

d. [タグ] - 汎用バケット内の S3 オブジェクトにタグを追加して、ストレージを分類します。詳細については、「タグを使用してストレージを分類する」を参照してください。

e. [オブジェクトロックリーガルホールドと保持] - 汎用バケット内のオブジェクトが削除されないようにすることができます。詳細については、「S3 Object Lock を使用したオブジェクトのロック」を参照してください。

タグを使用してストレージを分類する

オブジェクトのタグ付けを使用してストレージを分類します。各タグはキーと値のペアです。

新しいオブジェクトのアップロード時のタグ付け、または既存のオブジェクトのタグ付けを行うことができます

- 1 つのオブジェクトに最大 10 個のタグを関連付けることができます。オブジェクトに関連付けるタグには一意のタグキーが必要です。
- タグキーには最大 128 個の Unicode 文字、タグ値には最大 256 個の Unicode 文字を使用できます。Amazon S3 オブジェクトタグは、内部的に UTF-16 で表現されています。UTF-16 では、文字は 1 文字または 2 文字の位置を消費することに注意してください。
- キーと値は大文字と小文字が区別されます。
- タグの制限の詳細については、「AWS Billing and Cost Management ユーザーガイド」の「User-defined tag restrictions」を参照してください。基本的なタグの制限については、「Amazon EC2 ユーザーガイド」の「タグの制限」を参照してください。

例

次のタグ付けの例について説明します。

Example PHI 情報

保護されるべき医療情報 (PHI) データがオブジェクトに含まれているとします。このオブジェクトは次に示すキーと値のペアを使用してタグ付けできます。

```
PHI=True
```

または

```
Classification=PHI
```

Example プロジェクトのファイル

プロジェクトファイルを S3 バケットに保存するとします。このようなオブジェクトは、Project というキーと値を使用して次のようにタグ付けします。

```
Project=Blue
```

Example 複数のタグ

次に示すように複数のタグを 1 つのオブジェクトに付けることができます。

```
Project=x
Classification=confidential
```

キー名のプレフィックスとタグ

オブジェクトキー名のプレフィックスにより、ストレージを分類することもできます。ただし、プレフィックスベースの分類は 1 次元的です。次のオブジェクトキー名について説明します。

```
photos/photo1.jpg
project/projectx/document.pdf
project/projecty/document2.pdf
```

これらのキー名には、プレフィックスとして photos/、project/projectx/、および project/projecty/ が付いています。このプレフィックスによって 1 つのディメンションでの分類が行われます。つまり、1 つのプレフィックスのオブジェクトすべてが 1 つのカテゴリになります。たとえば、プレフィックス project/projectx はプロジェクト x に関連するすべてのドキュメントを識別します。

タグ付けによってもう 1 つのディメンションを設定できます。プロジェクト x カテゴリ内に photo1 が必要な場合、そのようにオブジェクトにタグ付けできます。

追加の利点

データの分類だけでなく、タグ付けには以下に示すような利点もあります。

- オブジェクトのタグを使用するとアクセス許可をきめ細かく制御できます。例えば、特定のタグが付けられた読み取り専用オブジェクトへのアクセス許可をユーザーに付与できます。
- オブジェクトのタグを使用すると、ライフサイクルルールでキー名プレフィックスに加えてタグに基づくフィルタを指定でき、オブジェクトライフサイクルをきめ細かく管理できます。
- Amazon S3 分析を使用する場合は、フィルターを設定することで、分析対象のオブジェクトをオブジェクトタグまたはキー名のプレフィックスに基づいてグループ化するか、プレフィックスとタグの両方に基づいてグループ化することができます。
- また、Amazon CloudWatch メトリクスをカスタマイズして、特定のタグフィルターごとに情報を表示することもできます。詳細については次のセクションで説明します。

> **Important**
>
> 機密データ (個人を特定できる情報 (PII) または保護すべき医療情報 (PHI) を含むオブジェクトのラベルとしてタグを使用できます。しかし、タグそのものに機密情報を含めることはできません。

1 つのリクエストで複数の Amazon S3 オブジェクトにオブジェクトタグセットを追加する

1 つのリクエストでオブジェクトタグセットを複数の Amazon S3 オブジェクトに追加するには、S3 バッチオペレーションを使用できます。S3 バッチオペレーションには、オペレーション対象のオブジェクトのリストを指定します。S3 バッチオペレーションは、各 API オペレーションを呼び出して、指定されたオペレーションを実行します。1 つのバッチオペレーションジョブで、エクサバイトのデータを含む数十億ものオブジェクトに対して、指定されたオペレーションを実行できます。

S3 バッチオペレーション機能は、進捗状況の追跡、通知の送信、すべてのアクションの詳細な完了レポートの保存を行い、フルマネージドの監査可能なサーバーレスエクスペリエンスを提供します。S3 バッチオペレーションは、Amazon S3 コンソール、AWS CLI、AWS SDK、または REST API を通じて使用できます。詳細については、「the section called “バッチ操作の基本”」を参照してください。

オブジェクトタグの詳細については、オブジェクトタグの管理を参照してください。

オブジェクトのタグ付けに関連する API オペレーション

Amazon S3 では、特にオブジェクトのタグ付けについて次の API オペレーションがサポートされています。

オブジェクトの API オペレーション

- PUT Object tagging – オブジェクトのタグを置換します。リクエストボディにタグを指定します。この API を使用したオブジェクトタグ管理の 2 つのシナリオは次のとおりです。
  - オブジェクトにタグがない – この API を使用して一連のタグをオブジェクトに付けることができます (オブジェクトには事前にタグが付いていない)。
  - オブジェクトに既存のタグセットがある – 既存のタグセットを変更するには、最初に既存のタグセットを取得してクライアント側で変更してから、この API を使用してタグセットを置換する必要があります。

    > **Note**
    >
    > タグセットを空にしてこのリクエストを送信すると、Amazon S3 によってオブジェクトの既存のタグセットが削除されます。この方法を使用すると、範囲 1 リクエスト (PUT) に対して料金が発生します。詳細については、Amazon S3 の料金 を参照してください。
    > 料金が発生することなく同じ結果が得られるため、DELETE Object tagging リクエストが推奨されます。

- GET Object tagging – オブジェクトに関連付けられているタグセットを返します。Amazon S3 によってレスポンス本文でオブジェクトタグが返されます。
- DELETE Object tagging – オブジェクトに関連付けられているタグセットを削除します。

タグ付けをサポートする他の API オペレーション

- PUT Object および Initiate Multipart Upload – オブジェクトを作成するときにタグを指定できます。`x-amz-tagging` リクエストヘッダーを使用してタグを指定します。
- GET Object – Amazon S3 はタグセットを返さずに、`x-amz-tag-count` ヘッダーでオブジェクトのタグ数を返します (リクエスタにタグの読み取りアクセス許可がある場合のみ)。これは、ヘッダーのレスポンスサイズが 8 KB に制限されるためです。タグを表示するには、GET Object tagging API オペレーションで別のリクエストを作成します。

- POST Object – POST リクエストでタグを指定できます。

  リクエスト内のタグが 8 KB の HTTP リクエストヘッダーサイズ制限を超えない場合は、PUT Object API を使用してタグ付きのオブジェクトを作成できます。指定するタグがヘッダーサイズ制限を超える場合は、この POST メソッドを使用して本文にタグを指定できます。

  PUT Object - Copy – リクエストに x-amz-tagging-directive を指定し、タグをコピー (デフォルト動作) するか、リクエストに指定された新しいタグセットでタグを置換するように Amazon S3 に指示します。

次の点に注意してください。

- S3 オブジェクトのタグ付けには強固な整合性があります。詳細については、「Amazon S3 のデータ整合性モデル」を参照してください。

追加の設定

このセクションでは、オブジェクトのタグ付けが他の設定にどのように関連するかを説明します。

オブジェクトのタグ付けとライフサイクル管理

バケットライフサイクル設定では、ルールを適用するオブジェクトのサブセットを選択するためにフィルタを指定できます。キー名プレフィックスまたはオブジェクトタグ (あるいは両方) に基づいてフィルタを指定できます。

Amazon S3 バケットに写真 (RAW 形式および完成形式) を保存するとします。このようなオブジェクトには次のようにタグ付けできます。

```
phototype=raw
or
phototype=finished
```

写真の作成後、しばらくしてから RAW 写真を S3 Glacier にアーカイブすることを検討する場合があります。特定のタグ (photos/) を持つキー名プレフィックス (phototype=raw) でオブジェクトのサブセットを特定するフィルタを使用して、ライフサイクルルールを設定できます。

詳細については、「オブジェクトのライフサイクルの管理」を参照してください。

オブジェクトのタグ付けとレプリケーション

レプリケーションをバケットに設定した場合、タグを読み取るアクセス許可を Amazon S3 に付与すると、Amazon S3 によってタグがレプリケートされます。詳細については、「ライブレプリケーションの設定の概要」を参照してください。

オブジェクトタグ付けイベント通知

オブジェクトタグがオブジェクトに追加または削除されたときに通知を受け取るように、Amazon S3 イベント通知を設定できます。`s3:ObjectTagging:Put` イベントタイプは、タグがオブジェクト上に置かれたとき、または既存のタグが更新されたときに通知します。`s3:ObjectTagging:Delete` イベントタイプは、タグがオブジェクトから削除されたときに通知します。詳細については、イベント通知を有効 を参照してください。

オブジェクトのタグ付けの詳細については、次のトピックを参照してください。

トピック

- タグ付けとアクセスコントロールポリシー
- オブジェクトタグの管理

タグ付けとアクセスコントロールポリシー

アクセス許可ポリシー (バケットポリシーとユーザーポリシー) を使用して、オブジェクトのタグ付けに関連するアクセス許可を管理することもできます。ポリシーアクションについては次のトピックを参照してください。

- オブジェクト操作
- バケットオペレーション

オブジェクトのタグを使用して、アクセス許可を管理するためのきめ細かいアクセスコントロールが可能になります。オブジェクトタグに基づいて条件付きアクセス許可を与えることができます。Amazon S3 でサポートされる次の条件キーを使用すると、オブジェクトタグに基づいて条件付きアクセス許可を付与できます。

- `s3:ExistingObjectTag/<tag-key>` – この条件キーを使用して、既存のオブジェクトタグに特定のタグキーと値があることを確認します。

> **Note**
>
> PUT Object オペレーションおよび DELETE Object オペレーションのアクセス許可を与える場合、この条件キーはサポートされません。つまり、オブジェクトをその既存のタグに基づいて削除または上書きするアクセス許可を、ユーザーに許可または拒否するポリシーは作成できません。

- `s3:RequestObjectTagKeys` – この条件キーを使用して、オブジェクトに指定できるタグキーを制限します。これが役立つのは、PutObjectTagging、PutObject および POST Object リクエストを使用してオブジェクトにタグを付けるときです。
- `s3:RequestObjectTag/<tag-key>` – この条件キーを使用して、オブジェクトに指定できるタグキーと値を制限します。これが役立つのは、PutObjectTagging、PutObject、および POST Bucket リクエストを使用してオブジェクトにタグを付けるときです。

Amazon S3 サービス固有の条件キーの詳細なリストについては、「条件キーを使用したバケットポリシーの例」を参照してください。次のアクセス許可ポリシーを使用して、オブジェクトのタグ付けによってきめ細かいアクセス許可管理がどのように実現するかを説明します。

Example 1: 特定のタグキーと値を持つオブジェクトの読み取りのみをユーザーに許可する

以下のアクセス許可ポリシーでは、environment: production タグキーと値を持つオブジェクトのみを読み取れるように制限しています。このポリシーは s3:ExistingObjectTag 条件キーを使用してタグキーと値を指定します。

```
{
  "Version": "2012-10-17",
  "Statement": [
  {
    "Principal": {
      "AWS": [
        "arn:aws:iam::111122223333:role/JohnDoe"
      ]
    },
    "Effect": "Allow",
    "Action": ["s3:GetObject", "s3:GetObjectVersion"],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
    "Condition": {
      "StringEquals":
        {"s3:ExistingObjectTag/environment": "production"}
```

```
    }
  }
  ]
}
```

Example 2: ユーザーが追加できるオブジェクトタグキーを制限する

次のアクセス許可ポリシーは、s3:PutObjectTagging アクションを実行する権限をユーザーに許可します (ユーザーが既存のオブジェクトにタグを付けることができます)。この条件は s3:RequestObjectTagKeys 条件キーを使用して、Owner や CreationDate などの許可されたタグキーを指定します。詳細については、「IAM ユーザーガイド」の「複数のキーの値をテストする条件の作成」を参照してください。

このポリシーは、リクエストで指定されたすべてのタグキーが承認されたタグキーであることを保証します。条件の ForAnyValue 修飾子によって、指定したキーの少なくとも 1 つがリクエストに存在することが保証されます。

```
{
   "Version": "2012-10-17",
  "Statement": [
    {"Principal":{"AWS":[
            "arn:aws:iam::111122223333:role/JohnDoe"
         ]
       },
 "Effect": "Allow",
      "Action": [
        "s3:PutObjectTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ],
      "Condition": {"ForAnyValue:StringEquals": {"s3:RequestObjectTagKeys": [
            "Owner",
            "CreationDate"
          ]
        }
      }
    }
  ]
}
```

Example 3: ユーザーにオブジェクトタグの追加を許可する場合は特定のタグキーと値が必要

次のポリシーの例では、s3:PutObjectTagging アクションを実行するアクセス許可をユーザーに付与します (ユーザーが既存のオブジェクトにタグを追加することができます)。この条件により、値が *X* に設定された特定のタグキー (*Project* など) をユーザーが含めることが求められます。

```
{
   "Version": "2012-10-17",
  "Statement": [
    {"Principal":{"AWS":[
       "arn:aws:iam::111122223333:user/JohnDoe"
         ]
       },
      "Effect": "Allow",
      "Action": [
        "s3:PutObjectTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ],
      "Condition": {"StringEquals": {"s3:RequestObjectTag/Project": "X"
        }
      }
    }
  ]
}
```

オブジェクトタグの管理

このセクションでは、AWS SDK for Java および .NET、または Amazon S3 コンソールを使用してオブジェクトタグを管理する方法について説明します。

オブジェクトのタグ付けにより、汎用バケット内のストレージを分類できます。各タグは、以下のルールに準拠したキーと値のペアです。

- 1 つのオブジェクトに最大 10 個のタグを関連付けることができます。オブジェクトに関連付けるタグには一意のタグキーが必要です。
- タグキーには最大 128 個の Unicode 文字、タグ値には最大 256 個の Unicode 文字を使用できます。Amazon S3 オブジェクトタグは、内部的に UTF-16 で表現されています。UTF-16 では、文字は 1 文字または 2 文字の位置を消費することに注意してください。
- キーと値は大文字と小文字が区別されます。

オブジェクトタグの詳細については、タグを使用してストレージを分類するを参照してください。タグの制限の詳細については、AWS Billing and Cost Management ユーザーガイドのユーザー定義タグの制限を参照してください。

S3 コンソールの使用

オブジェクトにタグを追加するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[汎用バケット] を選択します。
3. バケットリストで、そのオブジェクトを含むバケットの名前を選択します。
4. 変更するオブジェクトの名前の左にあるチェックボックスをオンにします。
5. [Actions] メニューで、[Edit tags] を選択します。
6. リストされたオブジェクトを確認し、[タグの追加] を選択します。
7. 各オブジェクトタグはキーと値のペアです。キーと値を入力します。別のタグを追加するには、[タグの追加] を選択します。

   オブジェクトには最大 10 個のタグを入力できます。
8. [Save changes] (変更を保存) をクリックします。

   Amazon S3 が指定されたオブジェクトにタグを追加します。

詳細については、このガイドの「Amazon S3 コンソールでのオブジェクトのプロパティの表示」および「オブジェクトのアップロード」も参照してください。

AWS SDKs の使用

Java

次の例では、AWS SDK for Java を使用して新しいオブジェクトのタグを設定し、既存のオブジェクトのタグを取得または置き換える方法を示します。オブジェクトのタグ付けの詳細については、「タグを使用してストレージを分類する」を参照してください。作業サンプルの作成およびテストの手順については、「AWS SDK for Java のデベロッパーガイド」の「使用開始」を参照してください。

```
import com.amazonaws.AmazonServiceException;
```

```
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.*;

import java.io.File;
import java.util.ArrayList;
import java.util.List;

public class ManagingObjectTags {

    public static void main(String[] args) {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String keyName = "*** Object key ***";
        String filePath = "*** File path ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();

            // Create an object, add two new tags, and upload the object to Amazon
 S3.
            PutObjectRequest putRequest = new PutObjectRequest(bucketName, keyName,
 new File(filePath));
            List<Tag> tags = new ArrayList<Tag>();
            tags.add(new Tag("Tag 1", "This is tag 1"));
            tags.add(new Tag("Tag 2", "This is tag 2"));
            putRequest.setTagging(new ObjectTagging(tags));
            PutObjectResult putResult = s3Client.putObject(putRequest);

            // Retrieve the object's tags.
            GetObjectTaggingRequest getTaggingRequest = new
 GetObjectTaggingRequest(bucketName, keyName);
            GetObjectTaggingResult getTagsResult =
 s3Client.getObjectTagging(getTaggingRequest);

            // Replace the object's tags with two new tags.
            List<Tag> newTags = new ArrayList<Tag>();
            newTags.add(new Tag("Tag 3", "This is tag 3"));
```

```
            newTags.add(new Tag("Tag 4", "This is tag 4"));
            s3Client.setObjectTagging(new SetObjectTaggingRequest(bucketName,
 keyName, new ObjectTagging(newTags)));
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

.NET

次の例では、AWS SDK for .NET タグを使用して新しいオブジェクトのタグを設定し、既存のオブジェクトのタグを取得または置き換える方法を示します。オブジェクトのタグ付けの詳細については、「タグを使用してストレージを分類する」を参照してください。

コード例を設定および実行する方法の詳細については、「AWS SDK for .NET デベロッパーガイド」の「AWS SDK for .NET の開始方法」 を参照してください。

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Collections.Generic;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    public class ObjectTagsTest
    {
        private const string bucketName = "*** bucket name ***";
        private const string keyName = "*** key name for the new object ***";
        private const string filePath = @"*** file path ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 client;
```

```
        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            PutObjectWithTagsTestAsync().Wait();
        }

        static async Task PutObjectWithTagsTestAsync()
        {
            try
            {
                // 1. Put an object with tags.
                var putRequest = new PutObjectRequest
                {
                    BucketName = bucketName,
                    Key = keyName,
                    FilePath = filePath,
                    TagSet = new List<Tag>{
                        new Tag { Key = "Keyx1", Value = "Value1"},
                        new Tag { Key = "Keyx2", Value = "Value2" }
                    }
                };

                PutObjectResponse response = await
client.PutObjectAsync(putRequest);
                // 2. Retrieve the object's tags.
                GetObjectTaggingRequest getTagsRequest = new GetObjectTaggingRequest
                {
                    BucketName = bucketName,
                    Key = keyName
                };

                GetObjectTaggingResponse objectTags = await
client.GetObjectTaggingAsync(getTagsRequest);
                for (int i = 0; i < objectTags.Tagging.Count; i++)
                    Console.WriteLine("Key: {0}, Value: {1}",
objectTags.Tagging[i].Key, objectTags.Tagging[i].Value);


                // 3. Replace the tagset.

                Tagging newTagSet = new Tagging();
                newTagSet.TagSet = new List<Tag>{
                    new Tag { Key = "Key3", Value = "Value3"},
```

```
                    new Tag { Key = "Key4", Value = "Value4" }
                };


                PutObjectTaggingRequest putObjTagsRequest = new
PutObjectTaggingRequest()
                {
                    BucketName = bucketName,
                    Key = keyName,
                    Tagging = newTagSet
                };
                PutObjectTaggingResponse response2 = await
client.PutObjectTaggingAsync(putObjTagsRequest);

                // 4. Retrieve the object's tags.
                GetObjectTaggingRequest getTagsRequest2 = new
GetObjectTaggingRequest();
                getTagsRequest2.BucketName = bucketName;
                getTagsRequest2.Key = keyName;
                GetObjectTaggingResponse objectTags2 = await
client.GetObjectTaggingAsync(getTagsRequest2);
                for (int i = 0; i < objectTags2.Tagging.Count; i++)
                    Console.WriteLine("Key: {0}, Value: {1}",
objectTags2.Tagging[i].Key, objectTags2.Tagging[i].Value);

            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine(
                        "Error encountered ***. Message:'{0}' when writing an
object"
                        , e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine(
                    "Encountered an error. Message:'{0}' when writing an object"
                    , e.Message);
            }
        }
    }
}
```

署名付き URL を使用したオブジェクトのダウンロードおよびアップロード

バケットポリシーを更新せずに、Amazon S3 内のオブジェクトへの時間制限付きのアクセス権を付与するには、署名付き URL を使用できます。署名付き URL をブラウザに入力するか、プログラムで使用してオブジェクトをダウンロードできます。署名付き URL で使用される認証情報は、URL を生成した AWS ユーザーのものです。

また、署名付き URL を使用して、Amazon S3 バケットに対する特定のオブジェクトのアップロードを他のユーザーに許可することもできます。これにより、他のユーザーは AWS のセキュリティ認証情報やアクセス許可を持たなくてもアップロードできます。署名付き URL で指定したのと同じキーを持つオブジェクトがバケット内に既に存在する場合、Amazon S3 は既存のオブジェクトをアップロードしたオブジェクトで置き換えます。

署名付き URL は、有効期限日時まで複数回使用できます。

署名付き URL を作成する場合には、ご自身のセキュリティ認証情報を設定し、さらに次の情報を指定する必要があります。

- Amazon S3 バケット
- オブジェクトキー (オブジェクトのダウンロード先は Amazon S3 バケット、アップロード先はアップロード先のファイル名)
- HTTP メソッド (オブジェクトのダウンロードの `GET`、アップロードの `PUT`、オブジェクトメタデータの読み取りの `HEAD` など)
- 有効期限の時間間隔

現在、Amazon S3 の署名付き URL では、オブジェクトをアップロードする際に次のデータ整合性チェックサムアルゴリズム (CRC32、CRC32C、SHA-1、SHA-256) を使用することはできません。アップロード後にオブジェクトの整合性を確認するには、署名付き URL でアップロードするときに、オブジェクトの MD5 ダイジェストを指定できます。オブジェクトの整合性の詳細については、「Amazon S3 でのオブジェクトの整合性のチェック」を参照してください。

トピック

- 署名付き URL を作成できるユーザー
- 署名付き URL の有効期限
- 署名付き URL 機能の制限

- 署名付き URL を使用したオブジェクトの共有
- 署名付き URL を使用したオブジェクトのアップロード

署名付き URL を作成できるユーザー

有効なセキュリティ認証情報を持つすべてのユーザーが、署名付き URL を作成できます。しかし、何らかの理由でオブジェクトに正常にアクセスするには、署名付き URL を使用して行うオペレーションの実行許可を持っているユーザーが、署名付き URL を作成する必要があります。

署名付き URL の作成に使用できる認証情報のタイプは以下のとおりです。

- IAM インスタンスプロファイル – 最大 6 時間有効。
- AWS Security Token Service — 長期のセキュリティ認証情報を使用して署名した場合、または一時的な認証情報の有効期間 (どちらか早い方) で最長 36 時間有効です。
- IAM ユーザー – AWS Signature Version 4 を使用している場合は、最大 7 日間まで有効。

  最大 7 日間有効な署名付き URL を作成するには、まず、署名付き URL の作成に使用するメソッドへの IAM ユーザー認証情報 (アクセスキーとシークレットキー) の委任を行います。

> **Note**
>
> 一時的な認証情報を使用して署名付き URL を作成した場合、その認証情報が有効期限切れになると、URL は失効します。一般に、署名付き URL は、作成に使用した認証情報が取り消された場合、削除された場合、または非アクティブ化された場合は、期限切れになります。URL の有効期限がより長い場合でも失効します。一時的なセキュリティ認証情報の有効期間については、IAM ユーザーガイドの「AWS STS API オペレーションの比較」を参照してください。

署名付き URL の有効期限

署名付き URL は、URL の生成時に指定した期間にわたって有効です。Amazon S3 コンソールで署名付き URL を作成した場合、有効期限は 1 分から 12 時間の間で設定できます。AWS CLI または AWS SDK を使用する場合、有効期限は最大 7 日間に設定できます。

一時トークンを使用して署名付き URL を作成した場合、そのトークンが有効期限切れになると、URL は期限切れになります。一般に、署名付き URL は、作成に使用した認証情報が取り消され

た場合、削除された場合、または非アクティブ化された場合は、期限切れになります。URL の有効期限がより長い場合でも失効します。認証情報の使用が有効期限にどのように影響するかについては、「署名付き URL を作成できるユーザー」を参照してください。

Amazon S3 は、HTTP リクエスト時に署名付き URL の有効期限日時を確認します。例えば、有効期限が切れる時刻の直前にクライアントが大きなファイルのダウンロードを開始した場合は、ダウンロード中に有効期限時刻が経過しても、そのダウンロードは継続されます。しかし、接続が中断し、クライアントがダウンロードを再開しようとした時点で有効期限切れの時刻が経過している場合には、そのダウンロードは失敗します。

署名付き URL 機能の制限

署名付き URL の機能は、それを作成したユーザーの許可によって制限されます。本質的に署名付き URL は、それらを保有しているユーザーに対しアクセスを許可するためのベアラートークンです。そのため、適切に保護することをお勧めします。署名付き URL の使用を制限するために使用できるいくつかの方法を以下に示します。

AWS Signature Version 4 (SigV4)

署名済み URL リクエストが AWS Signature Version 4 (SigV4) により認証される際に実行する特定の動作を適用するには、バケットポリシーとアクセスポイントポリシーで条件キーを使用します。例えば、次のバケットポリシーでは、s3:signatureAge 条件を使用することで、署名が作成後 10 分を超えている場合、*amzn-s3-demo-bucket* バケット内のオブジェクトに対する Amazon S3 の署名付き URL リクエストをすべて拒否します。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Deny a presigned URL request if the signature is more than 10 min
 old",
         "Effect": "Deny",
         "Principal": {"AWS":"*"},
         "Action": "s3:*",
         "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
         "Condition": {
            "NumericGreaterThan": {
               "s3:signatureAge": 600000
            }
         }
```

```
      }
   ]
}
```

AWS Signature Version 4 に関連するポリシーキーの詳細については、「Amazon Simple Storage Service API リファレンス」の「AWS Signature Version 4 認証固有のポリシーキー」を参照してください。

ネットワークパスでの制限

署名付き URL の使用と、特定のネットワークパスへのすべての Amazon S3 アクセスを制限する場合は、AWS Identity and Access Management (IAM) ポリシーを記述できます。これらのポリシーは、呼び出しを作成する IAM プリンシパル、Simple Storage Service (Amazon S3) バケット、またはその両方に設定できます。

IAM プリンシパルでのネットワークパスの制限では、これらの認証情報のユーザーは、指定したネットワークからリクエストを送信する必要があります。バケットまたはアクセスポイントの制限により、そのリソースに対するすべてのリクエストは、指定したネットワークから発信される必要があります。これらの制限は、署名付き URL のシナリオ以外でも適用されます。

どの IAM グローバル条件キーを使用するかは、エンドポイントのタイプによって異なります。Amazon S3 のパブリックエンドポイントを使用している場合は、`aws:SourceIp` を使用します。Amazon S3 への仮想プライベートクラウド (VPC) エンドポイントを使用している場合は、`aws:SourceVpc` または `aws:SourceVpce` を使用します。

次の IAM ポリシーステートメントでは、プリンシパルは、指定されたネットワーク範囲からのみ AWS にアクセスする必要があります。このポリシーステートメントでは、すべてのアクセスがその範囲から発信される必要があります。これは、Amazon S3 の署名付き URL を使用しているユーザーにも当てはまります。この例を実行するには、*`user input placeholders`* をユーザー自身の情報に置き換えます。

```
{
    "Sid": "NetworkRestrictionForIAMPrincipal",
    "Effect": "Deny",
    "Action": "*",
    "Resource": "*",
    "Condition": {
        "NotIpAddressIfExists": {"aws:SourceIp": "IP-address-range"},
        "BoolIfExists": {"aws:ViaAWSService": "false"}
    }
```

```
}
```

署名付き URL を使用したオブジェクトの共有

デフォルトでは、すべての Amazon S3 オブジェクトはプライベートであり、オブジェクトの所有者のみがアクセスできます。ただし、オブジェクトの所有者は、署名付き URL を作成することで、他のユーザーとオブジェクトを共有できます。署名済み URL は、セキュリティ認証情報を使用してオブジェクトをダウンロードするアクセス許可を期限付きで付与します。署名付き URL をブラウザに入力するか、プログラムで使用してオブジェクトをダウンロードできます。署名付き URL で使用される認証情報は、URL を生成した AWS ユーザーのものです。

署名付き URL の一般的な情報については、「署名付き URL を使用したオブジェクトのダウンロードおよびアップロード」を参照してください。

オブジェクトを共有するための署名付き URL は、Amazon S3 コンソール、AWS Explorer for Visual Studio (Windows)、または AWS Toolkit for Visual Studio Code を使用してコードを記述せずに作成できます。AWS Command Line Interface (AWS CLI) または AWS SDK を使用して、署名付き URL をプログラムで生成することもできます。

S3 コンソールの使用

Amazon S3 コンソールで次の手順に従い、オブジェクトを共有するための署名付き URL を生成できます。コンソールを使用した場合、署名付き URL の最大有効期限は作成時点から 12 時間です。

Amazon S3 コンソールを使用して署名付き URL を生成するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。
3. [バケット] リストで、署名付き URL を取得するオブジェクトが含まれているバケットの名前を選択します。
4. [オブジェクト] リストで、署名付き URL を作成するオブジェクトを選択します。
5. [オブジェクトアクション] メニューで、[署名付き URL で共有] を選択します。
6. 署名付き URL の有効期間を指定します。
7. [Create presigned URL] (署名付き URL を作成) を選択します。
8. 確認が表示されると、URL は自動的にクリップボードにコピーされます。署名済み URL を再度コピーする必要がある場合は、署名済み URL をコピーするボタンが表示されます。

AWS CLI を使用する場合

次の例では、AWS CLI コマンドにより、Amazon S3 バケットのオブジェクトを共有するための署名付き URL を生成します。AWS CLI を使用する場合、署名付き URL の最大有効期限は、作成時点から 7 日間です。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3 presign s3://amzn-s3-demo-bucket/mydoc.txt --expires-in 604800
```

> **Note**
>
> 2019 年 3 月 20 日より後に開設されたすべての AWS リージョンでは、リクエストで endpoint-url と AWS #####を指定する必要があります。すべての Amazon S3 のリージョンとエンドポイントのリストについては、「AWS 全般のリファレンス」の「リージョンとエンドポイント」を参照してください。

```
aws s3 presign s3://amzn-s3-demo-bucket/mydoc.txt --expires-in 604800 --region af-south-1 --endpoint-url https://s3.af-south-1.amazonaws.com
```

詳細については、AWS CLI コマンドリファレンスの「presign」を参照してください。

AWS SDK の使用

AWS SDK を使用してオブジェクトを共有するための署名付き URL を生成する例については、「AWS SDK を使用して Amazon S3 の署名付き URL を作成する」を参照してください。

署名付き URL の生成に AWS SDK を使用した場合、最大有効期限は、作成時点から 7 日間となります。

> **Note**
>
> 2019 年 3 月 20 日より後に開設されたすべての AWS リージョンでは、リクエストで endpoint-url と AWS #####を指定する必要があります。すべての Amazon S3 のリージョンとエンドポイントのリストについては、「AWS 全般のリファレンス」の「リージョンとエンドポイント」を参照してください。

> **Note**
>
> AWS SDK を使用する場合、Tagging 属性はクエリパラメータではなく、ヘッダーでなければなりません。他のすべての属性は、署名済み URL のパラメータとして渡すことができます。

AWS Toolkit for Visual Studio の使用 (Windows)

> **Note**
>
> 現時点では、AWS Toolkit for Visual Studio は Visual Studio for Mac をサポートしていません。

1. 「AWS Toolkit for Visual Studio ユーザーガイド」の「Toolkit for Visual Studio のインストールとセットアップ」の手順に従って、AWS Toolkit for Visual Studio をインストールします。
2. 「AWS Toolkit for Visual Studio ユーザーガイド」の「AWS に接続する」の手順に従って、AWS に接続します。
3. AWS Explorer というラベルの左側のパネルで、オブジェクトを含むバケットをダブルクリックします。
4. 署名付き URL を生成するオブジェクトを右クリックし、[署名付き URL を作成...] を選択します。
5. ポップアップウィンドウで、署名付き URL の有効期限日時を設定します。
6. [オブジェクトキー] は、選択したオブジェクトに基づいて事前に入力されている必要があります。
7. [GET] を選択して、この署名付き URL をオブジェクトのダウンロードに使用するように指定します。
8. [生成] ボタンを選択します。
9. URL をクリップボードにコピーするには、[コピー] を選択します。
10. 生成された署名付き URL を使用するには、URL を任意のブラウザに貼り付けます。

AWS Toolkit for Visual Studio Code の使用

Visual Studio Code を使用している場合は、AWS Toolkit for Visual Studio Code を使用してコードを一切記述せずに、オブジェクトを共有するための署名付き URL を生成できます。一般的な情報につ

いては、「AWS Toolkit for Visual Studio Code ユーザーガイド」の「AWS Toolkit for Visual Studio Code」を参照してください。

AWS Toolkit for Visual Studio Code のインストール手順については、「AWS Toolkit for Visual Studio Code ユーザーガイド」の「AWS Toolkit for Visual Studio Code のインストール」を参照してください。

1. AWS に接続します (AWS Toolkit for Visual Studio Code ユーザーガイド」の「AWS Toolkit for Visual Studio Code に接続する」の手順に従います。
2. Visual Studio Code の左側のパネルで AWS ロゴを選択します。
3. [エクスプローラー] で、[S3] を選択します。
4. バケットとファイルを選択し、右クリックしてコンテキストメニューを開きます。
5. [署名済み URL を生成] を選択し、有効期限 (分単位) を設定します。
6. Enter キーを押すと、署名付き URL がクリップボードにコピーされます。

署名付き URL を使用したオブジェクトのアップロード

署名付き URL を使用して、自分の Amazon S3 バケットにオブジェクトをアップロードすることを他のユーザーに許可できます。署名付き URL を使用すると、他のユーザーは AWS セキュリティ認証情報やアクセス許可を持っていなくてもアップロードできます。署名付き URL は、それを作成したユーザーのアクセス許可によって制限されます。つまり、オブジェクトをアップロードするための署名付き URL を受け取った場合、オブジェクトをアップロードできるのは、署名付き URL の作成者がそのオブジェクトのアップロードに必要なアクセス許可を持っている場合のみです。

この URL を使用してオブジェクトをアップロードすると、Amazon S3 は指定されたバケットにオブジェクトを作成します。署名付き URL で指定したのと同じキーを持つオブジェクトがバケット内に既存する場合、Amazon S3 は既存のオブジェクトをアップロードしたオブジェクトで置き換えます。アップロード後は、バケット所有者がオブジェクトを所有します。

署名付き URL の一般的な情報については、「署名付き URL を使用したオブジェクトのダウンロードおよびアップロード」を参照してください。

AWS Explorer for Visual Studio を使用すると、コードを一切記述せずに、オブジェクトをアップロードするための署名付き URL を作成できます。AWS SDK を使用して署名付き URL をプログラムで生成することもできます。

> **Note**
>
> 現時点では、AWS Toolkit for Visual Studio は Visual Studio for Mac をサポートしていません。

AWS Toolkit for Visual Studio の使用 (Windows)

1. 「AWS Toolkit for Visual Studio ユーザーガイド」の「Toolkit for Visual Studio のインストールとセットアップ」の手順に従って、AWS Toolkit for Visual Studio をインストールします。
2. 「AWS Toolkit for Visual Studio ユーザーガイド」の「AWS に接続する」の手順に従って、AWS に接続します。
3. [AWS Explorer] というラベルの左側のパネルで、オブジェクトをアップロードするバケットを右クリックします。
4. [署名付き URL を作成] を選択します。
5. ポップアップウィンドウで、署名付き URL の有効期限日時を設定します。
6. [オブジェクトキー] で、アップロードするファイルの名前を設定します。アップロードするファイルは、この名前と正確に一致する必要があります。バケットに同じキーを持つオブジェクトがバケット内に既に存在する場合、Amazon S3 は既存のオブジェクトを新しくアップロードしたオブジェクトで置き換えます。
7. [PUT] を選択し、この署名付き URL をオブジェクトのアップロードに使用するように指定します。
8. [生成] ボタンを選択します。
9. URL をクリップボードにコピーするには、[コピー] を選択します。
10. この URL を使用するには、`curl` コマンドを使って PUT リクエストを送信できます。ファイルへのフルパスと署名付き URL 自体を含めます。

```
curl -X PUT -T "/path/to/file" "presigned URL"
```

ファイルをアップロードするための **PUT** 署名付き URL の生成に AWS SDK を使用

S3 アクションを期間限定で実行できる署名付き URL を生成できます。

> **Note**
>
> AWS CLI または AWS SDK を使用する場合、署名付き URL の有効期限は最大 7 日間に設定できます。詳細については、「署名付き URL の有効期限」を参照してください。

Python

次の Python スクリプトは、オブジェクトを S3 汎用バケットにアップロードするための PUT 署名付き URL を生成します。

1. スクリプトの内容をコピーし、「*put-only-url.py*」ファイルとして保存します。次の例を使用する際は、*###############*を独自の情報 (ファイル名など) に置き換えます。

```
import argparse
import boto3
from botocore.exceptions import ClientError

def generate_presigned_url(s3_client, client_method, method_parameters,
 expires_in):
    """
    Generate a presigned Amazon S3 URL that can be used to perform an action.

    :param s3_client: A Boto3 Amazon S3 client.
    :param client_method: The name of the client method that the URL performs.
    :param method_parameters: The parameters of the specified client method.
    :param expires_in: The number of seconds the presigned URL is valid for.
    :return: The presigned URL.
    """
    try:
        url = s3_client.generate_presigned_url(
            ClientMethod=client_method,
            Params=method_parameters,
            ExpiresIn=expires_in
        )
    except ClientError:
        print(f"Couldn't get a presigned URL for client method
 '{client_method}'.")
        raise
    return url

def main():
```

```
    parser = argparse.ArgumentParser()
    parser.add_argument("bucket", help="The name of the bucket.")
    parser.add_argument(
        "key", help="The key (path and filename) in the S3 bucket.",
    )
    args = parser.parse_args()

    # By default, this will use credentials from ~/.aws/credentials
    s3_client = boto3.client("s3")

    # The presigned URL is specified to expire in 1000 seconds
    url = generate_presigned_url(
        s3_client,
        "put_object",
        {"Bucket": args.bucket, "Key": args.key},
        1000
    )
    print(f"Generated PUT presigned URL: {url}")

if __name__ == "__main__":
    main()
```

2. ファイルをアップロードするための PUT 署名付き URL を生成するには、バケット名と目的のオブジェクトパスを使用して次のスクリプトを実行します。

   次のコマンドでは、値の例を使用しています。*###############*を独自の情報に置き換えます。

   ```
   python put-only-url.py amzn-s3-demo-bucket <object-path>
   ```

   スクリプトは以下の PUT 署名付き URL を出力します。

   ```
   Generated PUT presigned URL: https://amzn-s3-demo-
   bucket.s3.amazonaws.com/object.txt?
   AWSAccessKeyId=AKIAIOSFODNN7EXAMPLE&Signature=vjbyNxybdZaMmLa
   %2ByT372YEAiv4%3D&Expires=1741978496
   ```

3. 生成された署名付き URL と curl を使用してファイルをアップロードできるようになりました。

   ```
   curl -X PUT -T "path/to/your/local/file" "generated-presigned-url"
   ```

AWS SDK を使用してオブジェクトをアップロードするための署名付き URL を生成する例の詳細については、「AWS SDK を使用して Amazon S3 の署名付き URL を作成する」を参照してください。

S3 Object Lambda を使用したオブジェクトの変換

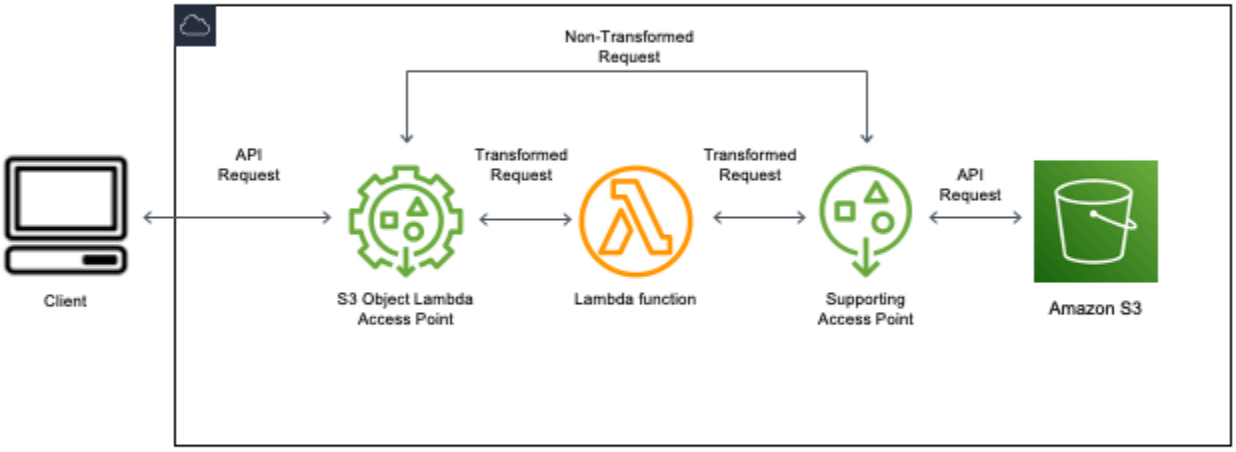
Amazon S3 Object Lambda を使用すると、Amazon S3 GET、LIST、HEAD リクエストに独自のコードを追加して、データがアプリケーションに返されるときにそのデータを変更および処理できます。カスタムコードを使用すると、S3 GET リクエストによって返されるデータを変更し、行のフィルタリング、画像の動的なサイズ変更と透かし、機密データの編集などを行うことができます。また、S3 Object Lambda を使用して、バケット内のすべてのオブジェクトのカスタムビューを作成する S3 LIST リクエストの出力や、オブジェクト名やサイズなどのオブジェクトメタデータを変更する S3 HEAD リクエストの出力を変更することもできます。S3 Object Lambda を Amazon CloudFront ディストリビューションのオリジンとして使用して、画像の自動サイズ変更、古い形式 (JPEG から WebP など) のトランスコーディング、メタデータの削除など、エンドユーザー向けにデータを調整できます。詳細については、AWS ブログの「Use Amazon S3 Object Lambda with Amazon CloudFront」(Amazon S3 Object Lambda を Amazon CloudFront で使用する) を参照してください。AWS Lambda 関数を利用しているため、コードは AWS によって完全に管理されたインフラストラクチャ上で実行されます。S3 Object Lambda を使用すると、データの派生コピーを作成して保存したり、プロキシを実行したりする必要が少なくなり、アプリケーションに変更を加える必要もなくなります。

S3 オブジェクト Lambda の仕組み

S3 Object Lambda は AWS Lambda 関数を使用して、標準の S3 GET、LIST、HEAD リクエストの出力を自動的に処理します。AWS Lambda は、基盤となるコンピューティングリソースの管理を必要とせずに、顧客定義のコードを実行するサーバーレスコンピューティングサービスです。データ変換を特定のユースケースに合わせて調整し、独自のカスタム Lambda 関数を作成して実行することができます。

Lambda 関数を設定したら、Object Lambda アクセスポイントと呼ばれる S3 Object Lambda サービスエンドポイントにアタッチします。Object Lambda アクセスポイントは、サポートアクセスポイントと呼ばれる、標準の S3 アクセスポイントを使用して Amazon S3 にアクセスします。

Object Lambda アクセスポイントにリクエストを送信すると、Amazon S3 は自動的に Lambda 関数を呼び出します。その後、S3 Object Lambda アクセスポイントを介して S3 GET、LIST、または HEAD リクエストを使用して取得されたデータは、変換された結果をアプリケーションに返します。次の図に示すように、他のすべてのリクエストは通常どおりに処理されます。



このセクションのトピックでは、S3 Object Lambda の使用方法について説明します。

トピック

- Object Lambda アクセスポイントの作成
- Amazon S3 Object Lambda アクセスポイントの使用
- S3 Object Lambda アクセスポイントのセキュリティに関する考慮事項
- S3 Object Lambda アクセスポイントの Lambda 関数の記述
- AWS で構築された Lambda 関数の使用
- S3 Object Lambda のベストプラクティスとガイドライン
- S3 Object Lambda のチュートリアル
- S3 Object Lambda のデバッグとトラブルシューティング

Object Lambda アクセスポイントの作成

Object Lambda アクセスポイントは、厳密に 1 つの標準アクセスポイントと 1 つの Amazon S3 バケットに関連付けられます。Object Lambda アクセスポイントを作成するには、次のリソースが必要です。

- Amazon S3 バケット。バケットの作成については、「the section called “汎用バケットの作成”」を参照してください。
- 標準 S3 アクセスポイント。Object Lambda アクセスポイントを使用する場合、この標準アクセスポイントはサポートアクセスポイントと呼ばれます。標準アクセスポイントの作成については、「the section called “汎用バケットのアクセスポイントの作成”」を参照してください。
- AWS Lambda 関数。独自の Lambda 関数を作成することも、事前に構築された関数を使用することもできます。Lambda 関数の詳細については、「the section called “Lambda 関数の記述”」を参照してください。事前構築された関数の詳細については、「AWS で構築された Lambda 関数の使用」を参照してください。
- (オプション) AWS Identity and Access Management (IAM) ポリシー。Amazon S3 アクセスポイントは IAM リソースポリシーをサポートしています。これにより、リソース、ユーザー、またはその他の条件別にアクセスポイントの使用を制御できます。これらのポリシーの作成の詳細については、「the section called “IAM ポリシーの設定”」を参照してください。

以下のセクションでは、下記を使用して Object Lambda アクセスポイントを作成する方法について説明します。

- AWS Management Console
- AWS Command Line Interface (AWS CLI)
- AWS CloudFormation テンプレート
- AWS Cloud Development Kit (AWS CDK)

REST API を使用して Object Lambda アクセスポイントを作成する方法については、Amazon Simple Storage Service API リファレンスの「`CreateAccessPointForObjectLambda`」を参照してください。

Object Lambda アクセスポイントの作成

次のいずれかの手順に従って Object Lambda アクセスポイントを作成します。

S3 コンソールの使用

コンソールを使用して Object Lambda のアクセスポイントを作成するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。

2. ナビゲーションバーで、現在表示されている AWS リージョン の名前をクリックします。次に、切り替え先のリージョンを選択します。
3. 左のナビゲーションペインで、[Object Lambda アクセスポイント] を選択します。
4. [Object Lambda アクセスポイント] ページで、[Object Lambda アクセスポイントの作成] を選択します。
5. [Object Lambda Access Point name] (Object Lambda アクセスポイント名) に、アクセスポイントに使用する名前を入力します。

   標準のアクセスポイントと同様に、Object Lambda には命名規則があります。詳細については、「汎用バケットの Amazon S3 アクセスポイントの命名規則」を参照してください。
6. [Supporting Access Point] (サポートアクセスポイント) で、使用する標準アクセスポイントを入力または参照します。アクセスポイントは、変換するオブジェクトと同じ AWS リージョン に存在する必要があります。標準アクセスポイントの作成については、「the section called “汎用バケットのアクセスポイントの作成”」を参照してください。
7. [変換の設定] で、Object Lambda アクセスポイントのデータを変換する関数を追加できます。次のいずれかを行います：

   - アカウントに既に AWS Lambda 関数がある場合は、[Invoke Lambda function] (Lambda 関数の呼び出し) で選択できます。ここで、AWS アカウント で Lambda 関数の Amazon リソースネーム (ARN) を入力するか、ドロップダウンメニューから Lambda 関数を選択できます。
   - AWS で構築された関数を使用する場合は、[AWS で構築された関数] で関数名を選択し、[Lambda 関数を作成] を選択します。これにより Lambda コンソールが表示され、そこで構築した関数を AWS アカウント にデプロイできます。構築した関数の詳細については、「AWS で構築された Lambda 関数の使用」を参照してください。

   [S3 APIs] で、呼び出す API オペレーションを 1 つ以上選択します。選択した各 API に対して、呼び出す Lambda 関数を指定する必要があります。
8. (オプション) [Payload] (ペイロード) に、入力として Lambda 関数に提供する JSON テキストを追加します。同じ Lambda 関数を呼び出す異なる Object Lambda アクセスポイントに対して、異なるパラメータを使用してペイロードを設定できます。これにより、Lambda 関数の柔軟性が向上します。

> **Important**
>
> Object Lambda アクセスポイントを使用する場合、ペイロードには機密情報を一切含めないでください。

9. (オプション) [Range and part number] (範囲とパート番号) では、範囲とパート番号ヘッダーで GET および HEAD リクエストを処理するには、このオプションを有効にする必要があります。このオプションを有効にすると、Lambda 関数がこれらのリクエストを認識して処理できることが確認されます。範囲ヘッダーとパート番号の詳細については、Range および partNumber ヘッダーの操作 を参照してください。
10. (オプション) [リクエストのメトリクス] で、[有効化] または [無効化] を選択して、Amazon S3 モニタリングを Object Lambda アクセスポイントに追加します。リクエストメトリクスには、Amazon CloudWatch の標準料金が課金されます。
11. (オプション) [Object Lambda Access Point policy] (Object Lambda アクセスポイントポリシー) で、リソースポリシーを設定します。リソースポリシーは、指定された Object Lambda アクセスポイントにアクセス許可を付与し、リソース、ユーザー、その他の条件別にアクセスポイントの使用を制御します。Object Lambda アクセスポイントのリソースポリシーの詳細については、「Object Lambda アクセスポイントの IAM ポリシーの設定」を参照してください。
12. [Block Public Access settings for this Object Lambda Access Point] (この Object Lambda アクセスポイントのパブリックアクセス設定をブロック) で、適用するパブリックアクセスブロック設定を選択します。新しい Object Lambda アクセスポイントでは、すべてのパブリックアクセスブロック設定がデフォルトで有効になります。デフォルトの設定のままにしておくことをお勧めします。Amazon S3 は、現在、Object Lambda アクセスポイントの作成後における Object Lambda アクセスポイントのパブリックアクセスブロック設定の変更をサポートしていません。

    Amazon S3 パブリックアクセスブロックの詳細については、「汎用バケットのアクセスポイントへのパブリックアクセスの管理」を参照してください。
13. [Create Object Lambda Access Point] (Object Lambda アクセスポイントの作成) を選択します。

AWS CLI を使用する場合

AWS CloudFormation テンプレートを使用して Object Lambda アクセスポイントを作成するには

> **Note**
>
> 次のコマンドを使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

1. S3 Object Lambda のデフォルト設定で、AWS Lambda 関数デプロイパッケージ `s3objectlambda_deployment_package.zip` をダウンロードします。
2. 次の `put-object` コマンドを実行して、Amazon S3 バケットにパッケージをアップロードします。

```
aws s3api put-object --bucket Amazon S3 bucket name --key
 s3objectlambda_deployment_package.zip --body release/
s3objectlambda_deployment_package.zip
```

3. S3 Object Lambda のデフォルト設定で AWS CloudFormation テンプレート `s3objectlambda_defaultconfig.yaml` をダウンロードします。
4. 次の `deploy` コマンドを実行して、テンプレートを AWS アカウント にデプロイします。

```
aws cloudformation deploy --template-file s3objectlambda_defaultconfig.yaml \
 --stack-name AWS CloudFormation stack name \
 --parameter-overrides ObjectLambdaAccessPointName=Object Lambda Access Point name
 \
  SupportingAccessPointName=Amazon S3 access point S3BucketName=Amazon S3 bucket \
  LambdaFunctionS3BucketName=Amazon S3 bucket containing your Lambda package \
  LambdaFunctionS3Key=Lambda object key LambdaFunctionS3ObjectVersion=Lambda object
 version \
  LambdaFunctionRuntime=Lambda function runtime --capabilities capability_IAM
```

GET、HEAD、および LIST API オペレーションで Lambda を呼び出すようにこの AWS CloudFormation テンプレートを設定できます。テンプレートのデフォルト設定の変更の詳細については、「the section called “AWS CloudFormation を使用して、S3 Object Lambda のセットアップを自動化します。”」を参照してください。

AWS CLI を使用して Object Lambda アクセスポイントを作成するには

> **Note**
>
> 次のコマンドを使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

以下の例では、アカウント *111122223333* のバケット *amzn-s3-demo-bucket1* に「*my-object-lambda-ap*」という名前の Object Lambda アクセスポイントを作成します。この例では、「*example-ap*」という名前の標準アクセスポイントが既に作成されていることを前提としています。標準アクセスポイントの作成については、the section called “汎用バケットのアクセスポイントの作成” を参照してください。

この例では、AWS の事前構築された関数 decompress を使用しています。事前構築された関数の詳細については、「the section called “AWS で構築された関数の使用”」を参照してください。

1. バケットを作成します。この例では、*amzn-s3-demo-bucket1* を使用します。バケットの作成については、「the section called “汎用バケットの作成”」を参照してください。
2. 標準アクセスポイントを作成し、バケットにアタッチします。この例では、*example-ap* を使用します。標準アクセスポイントの作成については、「the section called “汎用バケットのアクセスポイントの作成”」を参照してください。
3. 次のいずれかを行います：

   - Amazon S3 オブジェクトの変換に使用する Lambda 関数をアカウント内に作成します。Lambda 関数の詳細については、「the section called “Lambda 関数の記述”」を参照してください。AWS CLI でカスタム関数を使用するには、「AWS Lambda 開発者ガイド」の「AWS CLI での Lambda の使用」を参照してください。
   - AWS の事前構築された Lambda 関数を使用します。事前構築された関数の詳細については、「AWS で構築された Lambda 関数の使用」を参照してください。
4. my-olap-configuration.json という名前の JSON 設定ファイルを作成します。この設定では、前のステップで作成した Lambda 関数のサポートアクセスポイントと Amazon リソースネーム (ARN)、または使用している事前構築された関数の ARN を指定します。

   Example

```
{
```

```
    "SupportingAccessPoint" : "arn:aws:s3:us-
east-1:111122223333:accesspoint/example-ap",
    "TransformationConfigurations": [{
        "Actions" : ["GetObject", "HeadObject", "ListObjects", "ListObjectsV2"],
        "ContentTransformation" : {
            "AwsLambda": {
                "FunctionPayload" : "{\"compressionType\":\"gzip\"}",
                "FunctionArn" : "arn:aws:lambda:us-east-1:111122223333:function/
compress"
            }
        }
    }]
}
```

5. `create-access-point-for-object-lambda` コマンドを実行して Object Lambda アクセスポイントを作成します。

```
aws s3control create-access-point-for-object-lambda --account-id 111122223333 --
name my-object-lambda-ap --configuration file://my-olap-configuration.json
```

6. (オプション) `my-olap-policy.json` という名前の JSON ポリシーファイルを作成します。

   Object Lambda アクセスポイントのリソースポリシーを追加することで、リソース、ユーザー、その他の条件別にアクセスポイントの使用を制御することができます。このリソースポリシーは、アカウント *444455556666* に指定された Object Lambda アクセスポイントへの `GetObject` 許可を付与します。

   Example

```
{
    "Version": "2008-10-17",
    "Statement": [
        {
            "Sid": "Grant account 444455556666 GetObject access",
            "Effect": "Allow",
            "Action": "s3-object-lambda:GetObject",
            "Principal": {
                "AWS": "arn:aws:iam::444455556666:root"
            },
            "Resource": "your-object-lambda-access-point-arn"
        }
    ]
```

```
}
```

7. (オプション) put-access-point-policy-for-object-lambda コマンドを実行して、リソースポリシーを設定します。

```
aws s3control put-access-point-policy-for-object-lambda --account-id 111122223333
 --name my-object-lambda-ap --policy file://my-olap-policy.json
```

8. (オプション) ペイロードを規定します。

   ペイロードは、AWS Lambda 関数に入力として提供できるオプションの JSON です。同じ Lambda 関数を呼び出す異なる Object Lambda アクセスポイントに対して、異なるパラメータを使用してペイロードを設定できます。これにより、Lambda 関数の柔軟性が向上します。

   次の Object Lambda アクセスポイントの設定は、2 つのパラメータを持つペイロードを示しています。

```
{
 "SupportingAccessPoint": "AccessPointArn",
 "CloudWatchMetricsEnabled": false,
 "TransformationConfigurations": [{
  "Actions": ["GetObject", "HeadObject", "ListObjects", "ListObjectsV2"],
  "ContentTransformation": {
   "AwsLambda": {
    "FunctionArn": "FunctionArn",
    "FunctionPayload": "{\"res-x\": \"100\",\"res-y\": \"100\"}"
   }
  }
 }]
}
```

   次の Object Lambda アクセスポイント設定は、パラメータが 1 つあり、GetObject-Range、GetObject-PartNumber、HeadObject-Range、および HeadObject-PartNumber が有効になっているペイロードを示しています。

```
{
    "SupportingAccessPoint":"AccessPointArn",
    "CloudWatchMetricsEnabled": false,
    "AllowedFeatures": ["GetObject-Range", "GetObject-PartNumber", "HeadObject-
Range", "HeadObject-PartNumber"],
    "TransformationConfigurations": [{
```

```
        "Action": ["GetObject", "HeadObject", "ListObjects", "ListObjectsV2"],
        "ContentTransformation": {
            "AwsLambda": {
                "FunctionArn":"FunctionArn",
                "FunctionPayload": "{\"compression-amount\": \"5\"}"
            }
        }
    }]
}
```

> **Important**
>
> Object Lambda アクセスポイントを使用する場合、ペイロードには機密情報を一切含めないでください。

AWS CloudFormation コンソールとテンプレートの使用。

Amazon S3 が提供するデフォルト設定を使用して、Object Lambda アクセスポイントを作成できます。GitHub リポジトリ から AWS CloudFormation テンプレートと Lambda 関数のソースコードのリソースをダウンロードして、これらのリソースをデプロイして、Object Lambda アクセスポイントを設定します。

AWS CloudFormation テンプレートのデフォルト設定の変更の詳細については、「the section called “AWS CloudFormation を使用して、S3 Object Lambda のセットアップを自動化します。”」を参照してください。

テンプレートなしで AWS CloudFormation を使用する Object Lambda アクセスポイントの設定の詳細については、AWS CloudFormation ユーザーガイドの「AWS::S3ObjectLambda::AccessPoint」を参照してください。

Lambda 関数のデプロイパッケージをアップロードします

1. S3 Object Lambda のデフォルト設定で、AWS Lambda 関数デプロイパッケージ `s3objectlambda_deployment_package.zip` をダウンロードします。
2. Amazon S3 バケットにパッケージをアップロードします。

AWS CloudFormation コンソールを使用して Object Lambda のアクセスポイントを作成するには

1. S3 Object Lambda のデフォルト設定で AWS CloudFormation テンプレート `s3objectlambda_defaultconfig.yaml` をダウンロードします。
2. AWS マネジメントコンソール にサインインした後、https://console.aws.amazon.com/cloudformation/ で AWS CloudFormation コンソールを開きます。
3. 次のいずれかを行います：
   - AWS CloudFormation を初めて使用する場合は、AWS CloudFormation ホームページで [Create stack] (スタックの作成) を選択します。
   - 以前に AWS CloudFormation を使用したことがある場合は、左側のナビゲーションペインで [Stacks] (スタック) を選択します。[Create stack] (スタックの作成) を選択し、[With new resources (standard)] (新しいリソースを使用 (標準)) を選択します。
4. 前提条件 – テンプレートの準備で、テンプレートの準備完了を選択します。
5. [Specify template] (テンプレートの指定) で、[Upload a template file] (テンプレートファイルのアップロード) を選択して `s3objectlambda_defaultconfig.yaml` をアップロードします。
6. [次へ] を選択します。
7. スタックの詳細の指定ページで、スタックの名前を入力します。
8. [Parameters] (パラメータ) セクションで、スタックテンプレートで定義されている次のパラメータを指定します。
   a. [CreateNewSupportingAccessPoint] では、次のいずれかを実行します。
      - テンプレートをアップロードした S3 バケット用のサポートアクセスポイントが既にある場合は、[false] を選択します。
      - このバケット用に新しいアクセスポイントを作成する場合は、[true] を選択します。
   b. [EnableCloudWatchMonitoring] では、Amazon CloudWatch リクエストメトリクスとアラームを有効にするかどうかに応じて、[true] または [false] を選択します。
   c. (オプション) [LambdaFunctionPayload] に、入力として Lambda 関数に提供する JSON テキストを追加します。同じ Lambda 関数を呼び出す異なる Object Lambda アクセスポイントに対して、異なるパラメータを使用してペイロードを設定できます。これにより、Lambda 関数の柔軟性が向上します。

> **Important**
>
> Object Lambda アクセスポイントを使用する場合、ペイロードには機密情報を一切含めないでください。

d. [LambdaFunctionRuntime] で、Lambda 関数に希望するランタイムを入力します。使用可能な選択は次のとおりです。`nodejs14.x`、`python3.9`、`java11`。

e. [LambdaFunctionS3BucketName] で、デプロイパッケージをアップロードした Amazon S3 バケット名を入力します。

f. [LambdaFunctionS3Key] で、デプロイパッケージをアップロードした Amazon S3 オブジェクトキーを入力します。

g. [LambdaFunctionS3ObjectVersion] で、デプロイパッケージをアップロードした Amazon S3 オブジェクトバージョンを入力します。

h. [ObjectLambdaAccessPointName] で、Object Lambda アクセスポイント名を入力します。

i. [S3BucketName] で、Object Lambda アクセスポイントと関連付けられる Amazon S3 のバケット名を入力します。

j. [SupportingAccessPointName] で、サポートアクセスポイント名を入力します。

> **Note**
>
> これは前のステップで選択した Amazon S3 バケットに関連付けられたアクセスポイントです。Amazon S3 バケットに関連付けられているアクセスポイントがない場合は、[CreateNewSupportingAccessPoint] で [true] を選択すると、テンプレートを作成するようにテンプレートを構成できます。

9. [次へ] を選択します。
10. [スタックオプションの設定] ページで、[次へ] を選択します。

    このページのオプション設定の詳細については、「AWS CloudFormation ユーザーガイド」の「AWS CloudFormation スタックオプションの設定」を参照してください。
11. [確認] ページで [スタックの作成] を選択します。

AWS Cloud Development Kit (AWS CDK) を使用する場合

AWS CDK を使用した Object Lambda アクセスポイントの設定の詳細については、AWS Cloud Development Kit (AWS CDK) API リファレンスの「AWS::S3ObjectLambda Construct Library」を参照してください。

CloudFormation テンプレートを使用して S3 Object Lambda のセットアップを自動化する

AWS CloudFormation テンプレートを使用すると、Amazon S3 Object Lambda アクセスポイントをすばやく作成できます。CloudFormation テンプレートは、関連するリソースを自動的に作成し、AWS Identity and Access Management (IAM) ロールを設定し、Object Lambda アクセスポイントを介してリクエストを自動的に処理する AWS Lambda 関数を設定します。CloudFormation テンプレートでベストプラクティスを実装し、セキュリティ体制を改善し、マニュアルプロセスによって引き起こされるエラーを減らすことができます。

この GitHub リポジトリには、CloudFormation テンプレートと Lambda 関数のソースコードが含まれています。テンプレートの使用方法については、「the section called “Object Lambda アクセスポイントの作成”」を参照してください。

テンプレートで提供される Lambda 関数が変換を実行することはありません。代わりに、S3 バケットからオブジェクトをそのまま返します。関数をクローン化し、独自の変換コードを追加して、データがアプリケーションに返されるときに変更および処理できます。関数の変更の詳細については、「the section called “Lambda 関数の変更”」と「the section called “Lambda 関数の記述”」を参照してください。

テンプレートの変更

新しいサポートアクセスポイントの作成

S3 Object Lambda は、Object Lambda アクセスポイントと、サポートアクセスポイントと呼ばれる、標準の S3 アクセスポイントの 2 つのアクセスポイントを使用します。Object Lambda アクセスポイントにリクエストを行うと、S3 は S3 Object Lambda の設定に応じて、ユーザーに代わって Lambda を呼び出すか、サポートアクセスポイントにリクエストを委任します。テンプレートのデプロイ時に、`aws cloudformation deploy` コマンドの一部として次のパラメータを渡すことにより、新しいサポートアクセスポイントを作成できます。

```
CreateNewSupportingAccessPoint=true
```

関数ペイロードの設定。

テンプレートをデプロイするときに `aws cloudformation deploy` コマンドの一部として、次のパラメータを渡すことにより、Lambda 関数に補足データを提供するようにペイロードを設定できます。

```
LambdaFunctionPayload="format=json"
```

Amazon CloudWatch モニタリングを有効にします。

テンプレートをデプロイするときに `aws cloudformation deploy` コマンドの一部として<次のパラメータを渡すことで、CloudWatch モニタリングを有効にできます。

```
EnableCloudWatchMonitoring=true
```

このパラメータにより、Amazon S3 リクエストメトリクスの Object Lambda アクセスポイントが有効になり、クライアント側とサーバー側のエラーをモニタリングする 2 つの CloudWatch アラームが作成されます。

> **Note**
>
> Amazon CloudWatch の使用には追加コストが発生します。Amazon S3 リクエストメトリクスの詳細については、「汎用バケットのアクセスポイントのモニタリングとログ記録」を参照してください。
> 料金表については、「CloudWatch 料金表」を参照してください。

プロビジョニング済み同時実行の設定

レイテンシーを低減するために、Object Lambda アクセスポイントをサポートする Lambda 関数にプロビジョニングされた同時実行を設定するには、テンプレートを編集して、`Resources` の以下の行を含めます。

```
LambdaFunctionVersion:
      Type: AWS::Lambda::Version
      Properties:
        FunctionName: !Ref LambdaFunction
        ProvisionedConcurrencyConfig:
            ProvisionedConcurrentExecutions: Integer
```

> **Note**
>
> 同時実行のプロビジョニングには追加料金が発生します。プロビジョニングされた同時実行の詳細については、「AWS Lambdaデベロッパーガイド」の「Lambda プロビジョニング済み同時実行数の管理」を参照してください。
> 料金の詳細については、「AWS Lambda の料金表」を参照してください。

Lambda 関数の変更

`GetObject` リクエストのヘッダー値の変更

デフォルトでは、Lambda 関数は `Content-Length` と `ETag` を除くすべてのヘッダーを、署名付き URL リクエストから `GetObject` クライアントに転送します。Lambda 関数の変換コードに基づいて、新しいヘッダー値を `GetObject` クライアントに送信を選択できます。

Lambda 関数を更新して、新しいヘッダー値を `WriteGetObjectResponse` API オペレーションで渡すことで送信できます。

例えば、Lambda 関数が Amazon S3 オブジェクトのテキストを別の言語に変換する場合、`Content-Language` ヘッダーに新しい値を渡すことができます。これを行うには、以下のように `writeResponse` 関数を変更します。

```
async function writeResponse (s3Client: S3, requestContext: GetObjectContext,
 transformedObject: Buffer,
  headers: Headers): Promise<PromiseResult<{}, AWSError>> {
  const { algorithm, digest } = getChecksum(transformedObject);

  return s3Client.writeGetObjectResponse({
    RequestRoute: requestContext.outputRoute,
    RequestToken: requestContext.outputToken,
    Body: transformedObject,
    Metadata: {
      'body-checksum-algorithm': algorithm,
      'body-checksum-digest': digest
    },
    ...headers,
    ContentLanguage: 'my-new-language'
  }).promise();
}
```

サポートされているヘッダーの完全なリストについては、Amazon Simple Storage Service API リファレンスの WriteGetObjectResponse を参照してください。

メタデータヘッダーを返します。

Lambda 関数を更新して、新しいヘッダー値を WriteGetObjectResponse API オペレーションリクエストで渡すことで送信できます。

```
async function writeResponse (s3Client: S3, requestContext: GetObjectContext,
 transformedObject: Buffer,
  headers: Headers): Promise<PromiseResult<{}, AWSError>> {
  const { algorithm, digest } = getChecksum(transformedObject);

  return s3Client.writeGetObjectResponse({
    RequestRoute: requestContext.outputRoute,
    RequestToken: requestContext.outputToken,
    Body: transformedObject,
    Metadata: {
      'body-checksum-algorithm': algorithm,
      'body-checksum-digest': digest,
      'my-new-header': 'my-new-value'
    },
    ...headers
  }).promise();
}
```

新しいステータスコードを返します。

カスタムステータスコードを WriteGetObjectResponse API オペレーションリクエストで渡すことにより、GetObject クライアントに返すことができます。

```
async function writeResponse (s3Client: S3, requestContext: GetObjectContext,
 transformedObject: Buffer,
  headers: Headers): Promise<PromiseResult<{}, AWSError>> {
  const { algorithm, digest } = getChecksum(transformedObject);

  return s3Client.writeGetObjectResponse({
    RequestRoute: requestContext.outputRoute,
    RequestToken: requestContext.outputToken,
    Body: transformedObject,
    Metadata: {
      'body-checksum-algorithm': algorithm,
      'body-checksum-digest': digest
```

```
    },
    ...headers,
    StatusCode: Integer
  }).promise();
}
```

サポートされているステータスコードの完全なリストについては、Amazon Simple Storage Service API リファレンスの WriteGetObjectResponse を参照してください。

ソースオブジェクトに **Range** と **partNumber** パラメータを適用します。

デフォルトでは、CloudFormation テンプレートによって作成された Object Lambda アクセスポイントは、Range と partNumber のパラメータを処理できます。Lambda 関数は、要求された範囲または部品番号を変換されたオブジェクトに適用します。これを行うには、関数がオブジェクト全体をダウンロードして変換を実行する必要があります。場合によっては、変換されたオブジェクト範囲がソースオブジェクトの範囲に正確にマップされることがあります。つまり、ソースオブジェクトでバイト範囲 A–B を要求して変換を実行すると、オブジェクト全体を要求して変換を実行し、変換されたオブジェクトでバイト範囲 A–B を返すのと同じ結果が得られる可能性があります。

このような場合、Lambda 関数の実装を変更して、範囲または部品番号をソースオブジェクトに直接適用できます。このアプローチにより、関数全体のレイテンシーと必要なメモリが軽減されます。詳細については、「the section called “Range および partNumber ヘッダーの操作”」を参照してください。

Range と **partNumber** 処理の無効化

デフォルトでは、CloudFormation テンプレートによって作成された Object Lambda アクセスポイントは、Range と partNumber のパラメータを処理できます。この動作が不要な場合は、テンプレートから次の行を削除して無効化することができます。

```
AllowedFeatures:
  - GetObject-Range
  - GetObject-PartNumber
  - HeadObject-Range
  - HeadObject-PartNumber
```

大きなオブジェクトの変換

デフォルトでは、Lambda 関数は、S3 Object Lambda への応答のストリーミングをスタートする前に、メモリ内のオブジェクト全体を処理します。関数を変更して、変換の実行時に応答をストリーミ

ングできます。これにより、変換のレイテンシーと Lambda 関数のメモリサイズを軽減できます。実装例については、ストリーミング圧縮コンテンツの例を参照してください。

Amazon S3 Object Lambda アクセスポイントの使用

Amazon S3 Object Lambda アクセスポイントを介してリクエストを行うことは、他のアクセスポイントを介してリクエストを行う場合と同様に機能します。アクセスポイントを介してリクエストを行う方法の詳細については、「汎用バケットでの Amazon S3 アクセスポイントの使用」を参照してください。Amazon S3 コンソール、AWS Command Line Interface、(AWS CLI)、AWS SDK、または Amazon S3 REST API を使用して Object Lambda アクセスポイントを介し、リクエストを行うことができます。

> **Important**
>
> Object Lambda アクセスポイントの Amazon リソースネーム (ARN) では、`s3-object-lambda` のサービス名が使用されます。したがって、Object Lambda アクセスポイントの ARN は、`arn:aws:s3` の代わりに `arn:aws:s3-object-lambda` で始まり、他のアクセスポイントと共に使用されます。

Object Lambda アクセスポイントの ARN を見つける方法

AWS CLI または AWS SDK で Object Lambda アクセスポイントを使用するには、Object Lambda アクセスポイントの Amazon リソースネーム (ARN) を知る必要があります。以下の例では、Amazon S3 コンソールまたは AWS CLI を使用して Object Lambda アクセスポイントの ARN を検索する方法を示します。

S3 コンソールの使用

コンソールを使用して Object Lambda アクセスポイントの ARN を見つける方法

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[Object Lambda Access Points] (Object Lambda アクセスポイント)を選択します。
3. ARN をコピーする Object Lambda アクセスポイントの横にあるオプションボタンを選択します。
4. [ARN のコピー] を選択します。

AWS CLI を使用する場合

AWS CLI を使用して Object Lambda アクセスポイントの ARN を見つける方法

1. AWS アカウント に関連付けられている Object Lambda アクセスポイントのリストを取得するにはで、以下のコマンドを実行します。コマンドを実行する前に、アカウント ID *111122223333* と AWS アカウント ID を交換してください。

```
aws s3control list-access-points-for-object-lambda --account-id 111122223333
```

2. コマンド出力を確認して、使用するオブジェクト Lambda アクセスポイント ARN を見つけます。先ほどのコマンドの出力は、次の例のようになります。

```
{
    "ObjectLambdaAccessPointList": [
        {
            "Name": "my-object-lambda-ap",
            "ObjectLambdaAccessPointArn": "arn:aws:s3-object-lambda:us-
east-1:111122223333:accesspoint/my-object-lambda-ap"
        },
        ...
    ]
}
```

S3 バケット Object Lambda アクセスポイントでのバケット形式のエイリアスの使用方法

Object Lambda アクセスポイントを作成すると、Amazon S3 は Object Lambda アクセスポイントの固有のエイリアスを自動的に生成します。アクセスポイントのデータプレーンオペレーションのリクエストで、Amazon S3 バケット名や Object Lambda アクセスポイント Amazon Resource Name (ARN) の代わりに、このエイリアスを使用することができます。これらのオペレーションのリストについては、「汎用バケットのアクセスポイントの互換性」を参照してください。

Object Lambda アクセスポイントのエイリアス名は、Amazon S3 バケットと同じ名前空間内に作成されます。このエイリアス名は自動的に生成され、変更できません。既存の Object Lambda アクセスポイントには、エイリアスが自動的に割り当てられて使用されます。Object Lambda アクセスポイントのエイリアス名は、有効な Amazon S3 バケット名のすべての要件を満たしており、次の部分で構成されています。

Object Lambda Access Point name prefix-*metadata*--ol-s3

> **Note**
>
> `--ol-s3` サフィックスは、Object Lambda アクセスポイントのエイリアス名用に予約されており、バケット名や Object Lambda アクセスポイント名には使用できません。Amazon S3 バケット命名規則の詳細については、「汎用バケットの命名規則」を参照してください。

以下は、*my-object-lambda-access-point* という名前の Object Lambda アクセスポイントの ARN と Object Lambda アクセスポイントのエイリアスの例です。

- ARN — `arn:aws:s3-object-lambda:`*region*`:`*account-id*`:accesspoint/`*my-object-lambda-access-point*
- Object Lambda アクセスポイントのエイリアス — *my-object-lambda-acc-1a4n8yjrb3kda96f67zwrwiiuse1a*`--ol-s3`

Object Lambda アクセスポイントを使用する場合、コードを大幅に変更しなくても Object Lambda アクセスポイントのエイリアス名を使用できます。

Object Lambda アクセスポイントを削除すると、Object Lambda アクセスポイントのエイリアス名は非アクティブになり、プロビジョニングも解除されます。

Object Lambda アクセスポイントのエイリアスを見つける方法

S3 コンソールの使用

コンソールを使用して Object Lambda アクセスポイントのエイリアスを見つけるには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[Object Lambda Access Points] (Object Lambda アクセスポイント)を選択します。
3. 使用する Object Lambda アクセスポイントについて、Object Lambda アクセスポイントのエイリアス値をコピーします。

AWS CLI を使用する場合

Object Lambda アクセスポイントを作成すると、次のコマンド例に示すように、Amazon S3 によって Object Lambda アクセスポイントのエイリアス名が自動的に生成されます。このコマンドを実行

するには、*user input placeholders* をユーザー自身の情報に置き換えます。AWS CLI を使用して Object Lambda アクセスポイントを作成する方法については、「AWS CLI を使用して Object Lambda アクセスポイントを作成するには」を参照してください。

```
aws s3control create-access-point-for-object-lambda --account-id 111122223333 --
name my-object-lambda-access-point --configuration file://my-olap-configuration.json
{
    "ObjectLambdaAccessPointArn": "arn:aws:s3:region:111122223333:accesspoint/my-
access-point",
    "Alias": {
        "Value": "my-object-lambda-acc-1a4n8yjrb3kda96f67zwrwiiuse1a--ol-s3",
        "Status": "READY"
    }
}
```

生成された Object Lambda アクセスポイントのエイリアス名には 2 つのフィールドがあります。

- `Value` フィールドは、Obda Lambda アクセスポイントのエイリアス値です。
- `Status` フィールドは、Object Lambda アクセスポイントのエイリアスのステータスです。ステータスが `PROVISIONING` の場合、Amazon S3 は Object Lambda Access Point エイリアスをプロビジョニング中ですが、エイリアスはまだ使用できる状態ではありません。ステータスが `READY` の場合、Object Lambda Access Point エイリアスは正常にプロビジョニングされ、使用できる状態になっています。

REST API `ObjectLambdaAccessPointAlias` データ型の詳細については、Amazon Simple Storage Service API リファレンス の「CreateAccessPointForObjectLambda」および「ObjectLambdaAccessPointAlias」を参照してください。

Object Lambda アクセスポイントのエイリアスの使用方法

汎用バケットのアクセスポイントの互換性 に示されているオペレーションには、Amazon S3 バケット名の代わりに Object Lambda Access Point エイリアスを使用できます。

`get-bucket-location` コマンドの次の AWS CLI 例は、バケットのアクセスポイントエイリアスを使用して、バケットが置かれている AWS リージョン を返します。このコマンドを実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3api get-bucket-location --bucket my-object-lambda-
acc-w7i37nq6xuzgax3jw3oqtifiusw2a--ol-s3
```

```
{
    "LocationConstraint": "us-west-2"
}
```

リクエスト内の Object Lambda アクセスポイントのエイリアスが有効でない場合、エラーコード `InvalidAccessPointAliasError` が返されます。`InvalidAccessPointAliasError` の詳細については、Amazon Simple Storage Service API リファレンスの「List of Error Codes」(エラーコードのリスト) を参照してください。

Object Lambda アクセスポイントエイリアスの制限は、アクセスポイントエイリアスの制限と同じです。アクセスポイントエイリアスの制限の詳細については、「アクセスポイントエイリアスの制限」を参照してください。

S3 Object Lambda アクセスポイントのセキュリティに関する考慮事項

Amazon S3 Object Lambda では、コンピューティングプラットフォームとして AWS Lambda のスケールと柔軟性を利用して、Amazon S3 を離れたデータに対してカスタム変換を実行できます。S3 と Lambda はデフォルトで安全なままですが、この安全性を維持するためには、Lambda 関数の作成者による特別な考慮が必要です。S3 Object Lambda では、すべてのアクセスが、認証されたプリンシパル (匿名アクセスなし) により、HTTPS 経由で行われる必要があります。

セキュリティリスクを軽減するために、以下を推奨します。

- Lambda 実行ロールの範囲を、可能な限り最小の権限セットに設定します。
- 可能な限り、提供された署名付き URL を通じて Lambda 関数が Amazon S3 にアクセスするようにしてください。

IAM ポリシーの設定

S3 アクセスポイントは AWS Identity and Access Management (IAM) リソースポリシーをサポートしています。これにより、リソース、ユーザー、その他の条件別にアクセスポイントの使用を制御できます。詳細については、Object Lambda アクセスポイントの IAM ポリシーの設定 を参照してください。

暗号化動作

Object Lambda アクセスポイントは Amazon S3 と AWS Lambda の両方を使用するため、暗号化の動作には違いがあります。デフォルトの S3 暗号化の動作の詳細については、Amazon S3 バケット向けのサーバー側のデフォルトの暗号化動作の設定 を参照してください。

- Object Lambda アクセスポイントで S3 サーバー側の暗号化を使用している場合、オブジェクトは Lambda に送信される前に復号化されます。オブジェクトが Lambda に送信されると、暗号化されずに処理されます (GET または HEAD リクエストの場合)。
- 暗号化キーがログに記録されないようにするため、S3 は、お客様が指定したキーを使用したサーバー側の暗号化 (SSE-C) で暗号化されたオブジェクトに対する GET および HEAD リクエストを拒否します。ただし、Lambda 関数は、クライアントが指定したキーにアクセスできる場合、これらのオブジェクトを取得する可能性があります。
- Object Lambda アクセスポイントで S3 クライアント側の暗号化を使用する際は、Lambda がオブジェクトを復号および再暗号化するための暗号化キーにアクセスできることを確認してください。

アクセスポイントセキュリティ

S3 Object Lambda は、Object Lambda アクセスポイントと、サポートアクセスポイントと呼ばれる、標準の S3 アクセスポイントの 2 つのアクセスポイントを使用します。Object Lambda アクセスポイントにリクエストを行うと、S3 は S3 Object Lambda の設定に応じて、ユーザーに代わって Lambda を呼び出すか、サポートアクセスポイントにリクエストを委任します。Lambda がリクエストに対して呼び出されると、S3 は、サポートアクセスポイントを通じて、ユーザーに代わってオブジェクトへの署名付き URL を生成します。Lambda 関数は、関数が呼び出されたときにこの URL を入力として受け取ります。

S3 を直接呼び出すのではなく、この署名付き URL を使用して元のオブジェクトを取得するように Lambda 関数を設定できます。このモデルを使用することで、より優れたセキュリティ境界をオブジェクトに適用できます。S3 バケットまたは S3 アクセスポイント経由のオブジェクト直接アクセスを、限定された IAM ロールまたはユーザーのセットに制限できます。このアプローチにより、Lambda 関数が「混乱した代理問題」のターゲットになることを防げます。これは、呼び出し元とは異なるアクセス許可を持つ誤って設定された関数が、本来は許可または拒否すべきでないオブジェクトへのアクセスを許可または拒否する可能性があるというものです。

Object Lambda アクセスポイントのパブリックアクセス

S3 Object Lambda は匿名またはパブリックアクセスを許可しません。これは、Amazon S3 が S3 Object Lambda リクエストを完了するために ID を承認する必要があるためです。Object Lambda アクセスポイントを介してリクエストを呼び出す際には、設定された Lambda 関数の `lambda:InvokeFunction` 許可が必要となります。同様に、Object Lambda アクセスポイントを介して他の API オペレーションを呼び出す際には、必須の `s3:*` 許可が必要となります。

これらのアクセス許可がないと、Lambda の呼び出しまたは S3 への委任のリクエストは HTTP 403 (Forbidden) エラーとして失敗します。すべてのアクセスは、認証されたプリンシパルによって行わ

れる必要があります。パブリックアクセスが必要な場合は、Lambda@Edge を代替として使用できます。詳細については、Amazon CloudFront 開発者ガイドの Lambda@Edge を使用したエッジでのカスタマイズを参照してください。

Object Lambda アクセスポイント IP アドレス

`describe-managed-prefix-lists` サブネットはゲートウェイ仮想プライベートクラウド (VPC) エンドポイントをサポートしており、VPC エンドポイントのルーティングテーブルに関連しています。Object Lambda アクセスポイントはゲートウェイ VPC をサポートしていないため、その IP 範囲は欠落しています。欠落している範囲は Amazon S3 に属しますが、ゲートウェイ VPC エンドポイントではサポートされていません。`describe-managed-prefix-lists` の詳細については、「Amazon EC2 API リファレンス」の「DescribeManagedPrefixLists」と「AWS 全般のリファレンス」の「AWS IP アドレスの範囲」を参照してください。

Object Lambda アクセスポイントの IAM ポリシーの設定

Amazon S3 アクセスポイントは AWS Identity and Access Management (IAM) リソースポリシーをサポートしています。これにより、リソース、ユーザー、またはその他の条件別にアクセスポイントの使用を制御できます。Object Lambda アクセスポイントのオプションリソースポリシー、またはサポートアクセスポイントのリソースポリシーを使用してアクセスを制御できます。詳細な例については、チュートリアル: S3 Object Lambda を使用したアプリケーションのデータの変換 および チュートリアル: S3 Object Lambda と Amazon Comprehend を使用した PII データの検出と編集 を参照してください。

次の 4 つのリソースに Object Lambda アクセスポイントを使用するための許可が付与されている必要があります。

- ユーザーやロールなどの IAM ID。IAM ID およびベストプラクティスの詳細については、IAM ユーザーガイドの「IAM ID (ユーザー、ユーザーグループ、ロール)」を参照してください。
- バケットおよび関連する標準アクセスポイント。Object Lambda アクセスポイントを使用する場合、この標準アクセスポイントはサポートアクセスポイントと呼ばれます。
- Object Lambda アクセスポイント。
- AWS Lambda 関数。

> **Important**
>
> ポリシーを保存する前に、AWS Identity and Access Management Access Analyzer からのセキュリティ警告、エラー、一般的な警告、および提案を解決してください。IAM Access

Analyzer は、IAM ポリシーの文法とベストプラクティスに照らしてポリシーチェックを行います。これらのチェックにより、機能的でセキュリティのベストプラクティスに準拠したポリシーを作成するのに、役立つ結果と実行可能なレコメンデーションが示されます。IAM Access Analyzer を使用したポリシーの検証の詳細については、「IAM ユーザーガイド」の「IAM Access Analyzer のポリシーの検証」を参照してください。IAM Access Analyzer によって返される警告、エラー、および提案のリストを表示するには、「IAM Access Analyzer ポリシーチェックリファレンス」を参照してください。

以下のポリシーは、次のリソースがあることを前提としています。

- 次の Amazon リソースネーム (ARN) を持つ Amazon S3 バケット:

  `arn:aws:s3:::amzn-s3-demo-bucket1`
- このバケット上の Amazon S3 Standard アクセスポイントに次の ARN があること。

  `arn:aws:s3:us-east-1:111122223333:accesspoint/my-access-point`
- Object Lambda アクセスポイントに次の ARN があること。

  `arn:aws:s3-object-lambda:us-east-1:111122223333:accesspoint/my-object-lambda-ap`
- AWS Lambda 関数に次の ARN があること。

  `arn:aws:lambda:us-east-1:111122223333:function:MyObjectLambdaFunction`

> **Note**
>
> アカウントから Lambda 関数を使用する場合は、ポリシーステートメントに特定の関数のバージョンを含める必要があります。次の ARN の例では、バージョンは *1* で示されています。
> `arn:aws:lambda:us-east-1:111122223333:function:MyObjectLambdaFunction:1`
> Lambda は、バージョン $LATEST への IAM ポリシーの追加をサポートしていません。Lambda 関数のバージョンの詳細については、「AWS Lambda 開発者ガイド」の「Lambda 関数のバージョン」を参照してください。

Example - アクセスコントロールを標準アクセスポイントに委任するバケットポリシー

次の S3 バケットポリシーの例は、バケットのアクセスコントロールをバケットの標準アクセスポイントに委任します。このポリシーでは、バケット所有者のアカウントが所有するすべてのアクセスポイントへのフルアクセスを許可しています。したがって、このバケットへのすべてのアクセスは、そのアクセスポイントにアタッチされているポリシーによってコントロールされます。ユーザーはアクセスポイントを介してのみバケットから読み取ることができます。つまり、オペレーションは、アクセスポイントを介してのみ呼び出すことができます。詳細については、「アクセスポイントへのアクセスコントロールの委任」を参照してください。

```
{
    "Version": "2012-10-17",
    "Statement" : [
    {
        "Effect": "Allow",
        "Principal" : { "AWS":"account-ARN"},
        "Action" : "*",
        "Resource" : [
            "arn:aws:s3:::amzn-s3-demo-bucket1",
            "arn:aws:s3:::amzn-s3-demo-bucket1/*"
        ],
        "Condition": {
            "StringEquals" : { "s3:DataAccessPointAccount" : "Bucket owner's account
 ID" }
        }
    }]
}
```

Example — Object Lambda アクセスポイントを使用するために必要なアクセス許可をユーザーに付与する IAM ポリシー

次の IAM ポリシーは、Lambda 関数、標準アクセスポイント、および Object Lambda アクセスポイントに対するアクセス許可をユーザーに付与します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowLambdaInvocation",
      "Action": [
        "lambda:InvokeFunction"
      ],
```

```
      "Effect": "Allow",
      "Resource": "arn:aws:lambda:us-
east-1:111122223333:function:MyObjectLambdaFunction:1",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:CalledVia": [
            "s3-object-lambda.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "AllowStandardAccessPointAccess",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:us-east-1:111122223333:accesspoint/my-access-point/*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:CalledVia": [
            "s3-object-lambda.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "AllowObjectLambdaAccess",
      "Action": [
        "s3-object-lambda:Get*",
        "s3-object-lambda:List*"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3-object-lambda:us-east-1:111122223333:accesspoint/my-
object-lambda-ap"
    }
  ]
}
```

Lambda 実行ロールの許可を有効化する

Object Lambda アクセスポイントに GET リクエストが行われた場合、Lambda 関数には、S3 Object Lambda アクセスポイントにデータを送信する許可が必要です。このアクセス許可は、Lambda 関数の実行ロールで `s3-object-lambda:WriteGetObjectResponse` 許可を有効にすることで提供されます。新しい実行ロールを使作成することも、既存のロールを更新することもできます。

> **Note**
>
> 関数に `s3-object-lambda:WriteGetObjectResponse` 許可が必要なのは、GET リクエストを行う場合のみです。

IAM コンソールで実行ロールを作成するには

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. 左のナビゲーションペインで、[ロール] を選択してください。
3. [ロールの作成] を選択してください。
4. [一般的なユースケース] で、[Lambda] を選択します。
5. [次へ] を選択します。
6. [Add permissions] (許可の追加) ページで、AWS マネージドポリシー `AmazonS3ObjectLambdaExecutionRolePolicy` を検索し、ポリシー名の横にあるチェックボックスをオンにします。

   このポリシーには `s3-object-lambda:WriteGetObjectResponse` アクションを含める必要があります。
7. [次へ] を選択します。
8. [Name, review, and create] (名前、確認、作成) ページで、[Role name] (ロール名) に **`s3-object-lambda-role`** と入力します。
9. (オプション) このロールの説明とタグを追加します。
10. [ロールの作成] を選択してください。
11. 新しく作成した **`s3-object-lambda-role`** を Lambda 関数の実行ロールとして適用します。これは、Lambda コンソールで Lambda 関数の作成中または作成後に実行できます。

実行ロールの詳細については、「AWS Lambda デベロッパーガイド」の「Lambda 実行ロール」を参照してください。

Object Lambda アクセスポイントでのコンテキストキーの使用

S3 Object Lambda は、リクエストの接続や署名に関連する `s3-object-lambda:TlsVersion` や `s3-object-lambda:AuthType` などのコンテキストキーを評価します。`s3:prefix` など、他のすべてのコンテキストキーは、Amazon S3 によって評価されます。

Object Lambda アクセスポイントの CORS サポート

S3 Object Lambda がブラウザからリクエストを受信するか、リクエストに `Origin` ヘッダーが含まれている場合、S3 Object Lambda は常に `"AllowedOrigins":"*"` ヘッダーフィールドを追加します。

詳細については、「Cross-Origin Resource Sharing (CORS) の使用」を参照してください。

S3 Object Lambda アクセスポイントの Lambda 関数の記述

このセクションでは、Amazon S3 Object Lambda アクセスポイントで使用するための AWS Lambda 関数を記述する方法について詳述します。

S3 Object Lambda の一部のタスクにおける完全なエンドツーエンド手順については、以下を参照してください。

- チュートリアル: S3 Object Lambda を使用したアプリケーションのデータの変換
- チュートリアル: S3 Object Lambda と Amazon Comprehend を使用した PII データの検出と編集
- チュートリアル: S3 Object Lambda を使用して、取得時に画像に動的に透かしを入れる

トピック

- Lambda での GetObject リクエストの使用
- Lambdaでの HeadObject リクエストの処理
- Lambda での ListObjects リクエストの使用
- Lambda での ListObjectsV2 リクエストの使用
- イベントコンテキストの形式と使用法
- Range および partNumber ヘッダーの操作

Lambda での `GetObject` リクエストの使用

このセクションでは、Object Lambda アクセスポイントが `GetObject` 用に Lambda 関数を呼び出すように設定されていることを前提としています。S3 Object Lambda には、Amazon S3 API オペ

レーション、WriteGetObjectResponse が含まれています。これにより、Lambda 関数は、カスタマイズされたデータとレスポンスヘッダーを GetObject 発信者に提供できるようになります。

WriteGetObjectResponse は、処理のニーズに基づいて、ステータスコード、レスポンスヘッダー、レスポンス本文を広範囲に制御できます。WriteGetObjectResponse を使用すると、変換されたオブジェクト全体、変換されたオブジェクトの一部、またはアプリケーションのコンテキストに基づくその他のレスポンスに対して応答することができます。次のセクションでは、WriteGetObjectResponse API オペレーションを使用した一意の例を示します。

- 例 1: HTTP ステータスコード 403 (Forbidden) で応答します。
- 例 2: 変換された画像で応答する
- 例 3: 圧縮されたコンテンツをストリーミングする

例 1: HTTP ステータスコード 403 (Forbidden) で応答します。

WriteGetObjectResponse を使用して、オブジェクトの内容に基づいて HTTP ステータスコード 403 (Forbidden) で応答できます。

Java

```
package com.amazon.s3.objectlambda;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.events.S3ObjectLambdaEvent;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3Client;
import com.amazonaws.services.s3.model.WriteGetObjectResponseRequest;

import java.io.ByteArrayInputStream;
import java.net.URI;
import java.net.http.HttpClient;
import java.net.http.HttpRequest;
import java.net.http.HttpResponse;

public class Example1 {

    public void handleRequest(S3ObjectLambdaEvent event, Context context) throws
 Exception {
        AmazonS3 s3Client = AmazonS3Client.builder().build();
```

```
        // Check to see if the request contains all of the necessary information.
        // If it does not, send a 4XX response and a custom error code and message.
        // Otherwise, retrieve the object from S3 and stream it
        // to the client unchanged.
        var tokenIsNotPresent = !
event.getUserRequest().getHeaders().containsKey("requiredToken");
        if (tokenIsNotPresent) {
            s3Client.writeGetObjectResponse(new WriteGetObjectResponseRequest()
                    .withRequestRoute(event.outputRoute())
                    .withRequestToken(event.outputToken())
                    .withStatusCode(403)
                    .withContentLength(0L).withInputStream(new
 ByteArrayInputStream(new byte[0]))
                    .withErrorCode("MissingRequiredToken")
                    .withErrorMessage("The required token was not present in the
 request."));
            return;
        }

        // Prepare the presigned URL for use and make the request to S3.
        HttpClient httpClient = HttpClient.newBuilder().build();
        var presignedResponse = httpClient.send(
                HttpRequest.newBuilder(new URI(event.inputS3Url())).GET().build(),
                HttpResponse.BodyHandlers.ofInputStream());

        // Stream the original bytes back to the caller.
        s3Client.writeGetObjectResponse(new WriteGetObjectResponseRequest()
                .withRequestRoute(event.outputRoute())
                .withRequestToken(event.outputToken())
                .withInputStream(presignedResponse.body()));
    }
}
```

Python

```
import boto3
import requests

def handler(event, context):
    s3 = boto3.client('s3')

    """
```

```
   Retrieve the operation context object from the event. This object indicates
where the WriteGetObjectResponse request
   should be delivered and contains a presigned URL in 'inputS3Url' where we can
download the requested object from.
   The 'userRequest' object has information related to the user who made this
'GetObject' request to
   S3 Object Lambda.
   """
   get_context = event["getObjectContext"]
   user_request_headers = event["userRequest"]["headers"]

   route = get_context["outputRoute"]
   token = get_context["outputToken"]
   s3_url = get_context["inputS3Url"]

   # Check for the presence of a 'CustomHeader' header and deny or allow based on
that header.
   is_token_present = "SuperSecretToken" in user_request_headers

   if is_token_present:
       # If the user presented our custom 'SuperSecretToken' header, we send the
requested object back to the user.
       response = requests.get(s3_url)
       s3.write_get_object_response(RequestRoute=route, RequestToken=token,
Body=response.content)
   else:
       # If the token is not present, we send an error back to the user.
       s3.write_get_object_response(RequestRoute=route, RequestToken=token,
StatusCode=403,
       ErrorCode="NoSuperSecretTokenFound", ErrorMessage="The request was not
secret enough.")

   # Gracefully exit the Lambda function.
   return { 'status_code': 200 }
```

Node.js

```
const { S3 } = require('aws-sdk');
const axios = require('axios').default;

exports.handler = async (event) => {
    const s3 = new S3();
```

```
    // Retrieve the operation context object from the event. This object indicates
 where the WriteGetObjectResponse request
    // should be delivered and contains a presigned URL in 'inputS3Url' where we can
 download the requested object from.
    // The 'userRequest' object has information related to the user who made this
 'GetObject' request to S3 Object Lambda.
    const { userRequest, getObjectContext } = event;
    const { outputRoute, outputToken, inputS3Url } = getObjectContext;

    // Check for the presence of a 'CustomHeader' header and deny or allow based on
 that header.
    const isTokenPresent = Object
        .keys(userRequest.headers)
        .includes("SuperSecretToken");

    if (!isTokenPresent) {
        // If the token is not present, we send an error back to the user. The
 'await' in front of the request
        // indicates that we want to wait for this request to finish sending before
 moving on.
        await s3.writeGetObjectResponse({
            RequestRoute: outputRoute,
            RequestToken: outputToken,
            StatusCode: 403,
            ErrorCode: "NoSuperSecretTokenFound",
            ErrorMessage: "The request was not secret enough.",
        }).promise();
    } else {
        // If the user presented our custom 'SuperSecretToken' header, we send the
 requested object back to the user.
        // Again, note the presence of 'await'.
        const presignedResponse = await axios.get(inputS3Url);
        await s3.writeGetObjectResponse({
            RequestRoute: outputRoute,
            RequestToken: outputToken,
            Body: presignedResponse.data,
        }).promise();
    }

    // Gracefully exit the Lambda function.
    return { statusCode: 200 };
}
```

例 2: 変換された画像で応答する

画像変換を実行する場合、ソースオブジェクトの処理を開始する前に、ソースオブジェクトのすべてのバイトが必要になる可能性があります。この場合、WriteGetObjectResponse リクエストは、オブジェクト全体を 1 回の呼び出しでリクエスト元のアプリケーションに返します。

Java

```
package com.amazon.s3.objectlambda;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.events.S3ObjectLambdaEvent;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3Client;
import com.amazonaws.services.s3.model.WriteGetObjectResponseRequest;

import javax.imageio.ImageIO;
import java.awt.image.BufferedImage;
import java.awt.Image;
import java.io.ByteArrayInputStream;
import java.io.ByteArrayOutputStream;
import java.net.URI;
import java.net.http.HttpClient;
import java.net.http.HttpRequest;
import java.net.http.HttpResponse;

public class Example2 {

    private static final int HEIGHT = 250;
    private static final int WIDTH = 250;

    public void handleRequest(S3ObjectLambdaEvent event, Context context) throws
 Exception {
        AmazonS3 s3Client = AmazonS3Client.builder().build();
        HttpClient httpClient = HttpClient.newBuilder().build();

        // Prepare the presigned URL for use and make the request to S3.
        var presignedResponse = httpClient.send(
                HttpRequest.newBuilder(new URI(event.inputS3Url())).GET().build(),
                HttpResponse.BodyHandlers.ofInputStream());

        // The entire image is loaded into memory here so that we can resize it.
        // Once the resizing is completed, we write the bytes into the body
```

```
        // of the WriteGetObjectResponse request.
        var originalImage = ImageIO.read(presignedResponse.body());
        var resizingImage = originalImage.getScaledInstance(WIDTH, HEIGHT,
 Image.SCALE_DEFAULT);
        var resizedImage = new BufferedImage(WIDTH, HEIGHT,
 BufferedImage.TYPE_INT_RGB);
        resizedImage.createGraphics().drawImage(resizingImage, 0, 0, WIDTH, HEIGHT,
 null);

        var baos = new ByteArrayOutputStream();
        ImageIO.write(resizedImage, "png", baos);

        // Stream the bytes back to the caller.
        s3Client.writeGetObjectResponse(new WriteGetObjectResponseRequest()
                .withRequestRoute(event.outputRoute())
                .withRequestToken(event.outputToken())
                .withInputStream(new ByteArrayInputStream(baos.toByteArray())));
    }
}
```

Python

```
import boto3
import requests
import io
from PIL import Image

def handler(event, context):
    """
    Retrieve the operation context object from the event. This object indicates
 where the WriteGetObjectResponse request
    should be delivered and has a presigned URL in 'inputS3Url' where we can
 download the requested object from.
    The 'userRequest' object has information related to the user who made this
 'GetObject' request to
    S3 Object Lambda.
    """
    get_context = event["getObjectContext"]
    route = get_context["outputRoute"]
    token = get_context["outputToken"]
    s3_url = get_context["inputS3Url"]

    """
```

```
    In this case, we're resizing .png images that are stored in S3 and are
 accessible through the presigned URL
    'inputS3Url'.
    """
    image_request = requests.get(s3_url)
    image = Image.open(io.BytesIO(image_request.content))
    image.thumbnail((256,256), Image.ANTIALIAS)

    transformed = io.BytesIO()
    image.save(transformed, "png")

    # Send the resized image back to the client.
    s3 = boto3.client('s3')
    s3.write_get_object_response(Body=transformed.getvalue(), RequestRoute=route,
 RequestToken=token)

    # Gracefully exit the Lambda function.
    return { 'status_code': 200 }
```

Node.js

```
const { S3 } = require('aws-sdk');
const axios = require('axios').default;
const sharp = require('sharp');

exports.handler = async (event) => {
    const s3 = new S3();

    // Retrieve the operation context object from the event. This object indicates
 where the WriteGetObjectResponse request
    // should be delivered and has a presigned URL in 'inputS3Url' where we can
 download the requested object from.
    const { getObjectContext } = event;
    const { outputRoute, outputToken, inputS3Url } = getObjectContext;

    // In this case, we're resizing .png images that are stored in S3 and are
 accessible through the presigned URL
    // 'inputS3Url'.
    const { data } = await axios.get(inputS3Url, { responseType: 'arraybuffer' });

    // Resize the image.
    const resized = await sharp(data)
        .resize({ width: 256, height: 256 })
```

```
        .toBuffer();

    // Send the resized image back to the client.
    await s3.writeGetObjectResponse({
        RequestRoute: outputRoute,
        RequestToken: outputToken,
        Body: resized,
    }).promise();

    // Gracefully exit the Lambda function.
    return { statusCode: 200 };
}
```

例 3: 圧縮されたコンテンツをストリーミングする

オブジェクトを圧縮すると、圧縮データは増分的に生成されます。したがって、準備ができたらすぐに圧縮されたデータを返すために、WriteGetObjectResponse リクエストを使用できます。この例で示すように、完了した変換の長さを知る必要はありません。

Java

```
package com.amazon.s3.objectlambda;

import com.amazonaws.services.lambda.runtime.events.S3ObjectLambdaEvent;
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3Client;
import com.amazonaws.services.s3.model.WriteGetObjectResponseRequest;

import java.net.URI;
import java.net.http.HttpClient;
import java.net.http.HttpRequest;
import java.net.http.HttpResponse;

public class Example3 {

    public void handleRequest(S3ObjectLambdaEvent event, Context context) throws
 Exception {
        AmazonS3 s3Client = AmazonS3Client.builder().build();
        HttpClient httpClient = HttpClient.newBuilder().build();

        // Request the original object from S3.
```

```
        var presignedResponse = httpClient.send(
                HttpRequest.newBuilder(new URI(event.inputS3Url())).GET().build(),
                HttpResponse.BodyHandlers.ofInputStream());

        // Consume the incoming response body from the presigned request,
        // apply our transformation on that data, and emit the transformed bytes
        // into the body of the WriteGetObjectResponse request as soon as they're
 ready.
        // This example compresses the data from S3, but any processing pertinent
        // to your application can be performed here.
        var bodyStream = new GZIPCompressingInputStream(presignedResponse.body());

        // Stream the bytes back to the caller.
        s3Client.writeGetObjectResponse(new WriteGetObjectResponseRequest()
                .withRequestRoute(event.outputRoute())
                .withRequestToken(event.outputToken())
                .withInputStream(bodyStream));
    }

}
```

Python

```
import boto3
import requests
import zlib
from botocore.config import Config


"""
A helper class to work with content iterators. Takes an interator and compresses the
 bytes that come from it. It
implements 'read' and '__iter__' so that the SDK can stream the response.
"""
class Compress:
    def __init__(self, content_iter):
        self.content = content_iter
        self.compressed_obj = zlib.compressobj()

    def read(self, _size):
        for data in self.__iter__()
            return data
```

```
    def __iter__(self):
        while True:
            data = next(self.content)
            chunk = self.compressed_obj.compress(data)
            if not chunk:
                break

            yield chunk

        yield self.compressed_obj.flush()


def handler(event, context):
    """
    Setting the 'payload_signing_enabled' property to False allows us to send a
 streamed response back to the client.
    in this scenario, a streamed response means that the bytes are not buffered into
 memory as we're compressing them,
    but instead are sent straight to the user.
    """
    my_config = Config(
        region_name='eu-west-1',
        signature_version='s3v4',
        s3={
            "payload_signing_enabled": False
        }
    )
    s3 = boto3.client('s3', config=my_config)

    """
    Retrieve the operation context object from the event. This object indicates
 where the WriteGetObjectResponse request
    should be delivered and has a presigned URL in 'inputS3Url' where we can
 download the requested object from.
    The 'userRequest' object has information related to the user who made this
 'GetObject' request to S3 Object Lambda.
    """
    get_context = event["getObjectContext"]
    route = get_context["outputRoute"]
    token = get_context["outputToken"]
    s3_url = get_context["inputS3Url"]

    # Compress the 'get' request stream.
    with requests.get(s3_url, stream=True) as r:
```

```
        compressed = Compress(r.iter_content())

        # Send the stream back to the client.
        s3.write_get_object_response(Body=compressed, RequestRoute=route,
 RequestToken=token, ContentType="text/plain",
                                     ContentEncoding="gzip")

    # Gracefully exit the Lambda function.
    return {'status_code': 200}
```

Node.js

```
const { S3 } = require('aws-sdk');
const axios = require('axios').default;
const zlib = require('zlib');

exports.handler = async (event) => {
    const s3 = new S3();

    // Retrieve the operation context object from the event. This object indicates
 where the WriteGetObjectResponse request
    // should be delivered and has a presigned URL in 'inputS3Url' where we can
 download the requested object from.
    const { getObjectContext } = event;
    const { outputRoute, outputToken, inputS3Url } = getObjectContext;

    // Download the object from S3 and process it as a stream, because it might be a
 huge object and we don't want to
    // buffer it in memory. Note the use of 'await' because we want to wait for
 'writeGetObjectResponse' to finish
    // before we can exit the Lambda function.
    await axios({
        method: 'GET',
        url: inputS3Url,
        responseType: 'stream',
    }).then(
        // Gzip the stream.
        response => response.data.pipe(zlib.createGzip())
    ).then(
        // Finally send the gzip-ed stream back to the client.
        stream => s3.writeGetObjectResponse({
            RequestRoute: outputRoute,
            RequestToken: outputToken,
```

```
            Body: stream,
            ContentType: "text/plain",
            ContentEncoding: "gzip",
        }).promise()
    );

    // Gracefully exit the Lambda function.
    return { statusCode: 200 };
}
```

> **Note**
>
> S3 Object Lambda では、発信者に完全なレスポンスを送信するのに最大 60 秒かかります。`WriteGetObjectResponse` リクエストの場合、実際の利用可能な時間は短くなる可能性があります。例えば、Lambda 関数のタイムアウトが 60 秒未満である可能性があります。それ以外にも、発信者のタイムアウトがより厳しい場合があります。

元の発信者が HTTP ステータスコード 500 以外のレスポンス (内部サーバエラー) を受信するには、`WriteGetObjectResponse` コールが完了する必要があります。`WriteGetObjectResponse` API オペレーションが呼び出される前に、Lambda 関数が例外的に、またはその他の方法で返された場合、元の発信者は 500 (内部サーバーエラー) レスポンスを受け取ります。レスポンスが完了するまでの間にスローされた例外は、発信者へのレスポンスが切り捨てられます。Lambda 関数が `WriteGetObjectResponse` API コールから HTTP ステータスコード 200 (OK) レスポンスを受信した場合、元の発信者は完全なリクエストを送信しています。例外がスローされたかどうかにかかわらず、Lambda 関数のレスポンスは S3 Object Lambda では無視されます。

この `WriteGetObjectResponse` API オペレーションを呼び出すとき、Amazon S3 はイベントコンテキストからのルートトークンとリクエストトークンを必要とします。詳細については、「イベントコンテキストの形式と使用法」を参照してください。

ルートトークンとリクエストトークンのパラメータは、`WriteGetObjectResult` レスポンスを元の発信者に接続するために必要です。通常、500 (内部サーバーエラー) レスポンスを再試行するのが適切ですが、リクエストトークンはワンタイムトークンであることに注意してください。それ以降に使用を試みると、HTTP ステータスコード 400 (Bad Request) レスポンスが返されることになる可能性があります。ルートトークンとリクエストトークンを使用した `WriteGetObjectResponse` への呼び出しは、呼び出された Lambda 関数から作成する必要はありませんが、同じアカウント内のア

イデンティティによって作成する必要があります。この呼び出しは、Lambda 関数の実行を完了する前に完了する必要があります。

Lambdaでの **HeadObject** リクエストの処理

このセクションでは、Object Lambda アクセスポイントが HeadObject 用に Lambda 関数を呼び出すように設定されていることを前提としています。Lambda は headObjectContext というキーを含む JSON ペイロードを受け取ります。コンテキスト内には、inputS3Url というプロパティが 1 つあります。これは、HeadObject をサポートしているアクセスポイントの署名付き URL です。

署名付き URL に次のプロパティが指定されている場合、署名付き URL にはそれらが含まれます。

- versionId (クエリパラメータ内)
- requestPayer (x-amz-request-payer ヘッダー内)
- expectedBucketOwner (x-amz-expected-bucket-owner ヘッダー内)

他のプロパティは署名付きではないため、含まれません。ヘッダーとして送信される署名されていないオプションは、userRequest ヘッダーにある署名付き URL を呼び出すときに、手動でリクエストに追加できます。サーバー側の暗号化オプションは、HeadObject ではサポートされていません。

リクエスト構文 URI パラメータについては、「Amazon Simple Storage Service API リファレンス」の「HeadObject」を参照してください。

次の例は、HeadObject の Lambda JSON 入力ペイロードを示しています。

```
{
  "xAmzRequestId": "requestId",
  "**headObjectContext**": {
    "**inputS3Url**": "https://my-s3-ap-111122223333.s3-accesspoint.us-
east-1.amazonaws.com/example?X-Amz-Security-Token=<snip>"
  },
  "configuration": {
        "accessPointArn": "arn:aws:s3-object-lambda:us-
east-1:111122223333:accesspoint/example-object-lambda-ap",
        "supportingAccessPointArn": "arn:aws:s3:us-
east-1:111122223333:accesspoint/example-ap",
        "payload": "{}"
  },
  "userRequest": {
```

```
        "url": "https://object-lambda-111122223333.s3-object-lambda.us-
east-1.amazonaws.com/example",
        "headers": {
            "Host": "object-lambda-111122223333.s3-object-lambda.us-
east-1.amazonaws.com",
            "Accept-Encoding": "identity",
            "X-Amz-Content-SHA256": "e3b0c44298fc1example"
        }
    },
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "principalId",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/example",
        "accountId": "111122223333",
        "accessKeyId": "accessKeyId",
        "sessionContext": {
             "attributes": {
             "mfaAuthenticated": "false",
             "creationDate": "Wed Mar 10 23:41:52 UTC 2021"
        },
        "sessionIssuer": {
             "type": "Role",
             "principalId": "principalId",
             "arn": "arn:aws:iam::111122223333:role/Admin",
             "accountId": "111122223333",
             "userName": "Admin"
             }
        }
     },
   "protocolVersion": "1.00"
}
```

Lambda 関数は、HeadObject 呼び出しで返されるヘッダーと値を含む JSON オブジェクトを返します。

次の例は、HeadObject の Lambda レスポンス JSON の構造を示しています。

```
{
    "statusCode": <number>; // Required
    "errorCode": <string>;
    "errorMessage": <string>;
    "headers": {
        "Accept-Ranges": <string>,
```

```
        "x-amz-archive-status": <string>,
        "x-amz-server-side-encryption-bucket-key-enabled": <boolean>,
        "Cache-Control": <string>,
        "Content-Disposition": <string>,
        "Content-Encoding": <string>,
        "Content-Language": <string>,
        "Content-Length": <number>, // Required
        "Content-Type": <string>,
        "x-amz-delete-marker": <boolean>,
        "ETag": <string>,
        "Expires": <string>,
        "x-amz-expiration": <string>,
        "Last-Modified": <string>,
        "x-amz-missing-meta": <number>,
        "x-amz-object-lock-mode": <string>,
        "x-amz-object-lock-legal-hold": <string>,
        "x-amz-object-lock-retain-until-date": <string>,
        "x-amz-mp-parts-count": <number>,
        "x-amz-replication-status": <string>,
        "x-amz-request-charged": <string>,
        "x-amz-restore": <string>,
        "x-amz-server-side-encryption": <string>,
        "x-amz-server-side-encryption-customer-algorithm": <string>,
        "x-amz-server-side-encryption-aws-kms-key-id": <string>,
        "x-amz-server-side-encryption-customer-key-MD5": <string>,
        "x-amz-storage-class": <string>,
        "x-amz-tagging-count": <number>,
        "x-amz-version-id": <string>,
        <x-amz-meta-headers>: <string>, // user-defined metadata
        "x-amz-meta-meta1": <string>, // example of the user-defined metadata header,
 it will need the x-amz-meta prefix
        "x-amz-meta-meta2": <string>
        ...
    };
}
```

次の例は、JSON を返す前に必要に応じてヘッダー値を変更することにより、署名付き URL を使用してレスポンスを入力する方法を示しています。

Python

```
import requests
```

```
def lambda_handler(event, context):
    print(event)

    # Extract the presigned URL from the input.
    s3_url = event["headObjectContext"]["inputS3Url"]

    # Get the head of the object from S3.
    response = requests.head(s3_url)

    # Return the error to S3 Object Lambda (if applicable).
    if (response.status_code >= 400):
        return {
            "statusCode": response.status_code,
            "errorCode": "RequestFailure",
            "errorMessage": "Request to S3 failed"
    }

    # Store the headers in a dictionary.
    response_headers = dict(response.headers)

    # This obscures Content-Type in a transformation, it is optional to add
    response_headers["Content-Type"] = ""

    # Return the headers to S3 Object Lambda.
    return {
        "statusCode": response.status_code,
        "headers": response_headers
        }
```

Lambda での **ListObjects** リクエストの使用

このセクションでは、Object Lambda アクセスポイントが `ListObjects` 用に Lambda 関数を呼び出すように設定されていることを前提としています。Lambda は、`listObjectsContext` という新しいオブジェクトを持つ JSON ペイロードを受け取ります。`listObjectsContext` には、`inputS3Url` という単一のプロパティが含まれており、これは `ListObjects` をサポートしているアクセスポイント用の署名付き URL です。

`GetObject` や `HeadObject` とは異なり、署名付き URL には、次のプロパティが指定されている場合はそれらが含まれます。

- すべてのクエリパラメータ

- `requestPayer` (`x-amz-request-payer` ヘッダー内)
- `expectedBucketOwner` (`x-amz-expected-bucket-owner` ヘッダー内)

リクエスト構文 URI パラメータについては、「Amazon Simple Storage Service API リファレンス」の「ListObjects」を参照してください。

> **Important**
>
> アプリケーションを開発する場合は、新しいバージョンの ListObjectSv2 を使用することをお勧めします。Amazon S3 は、下位互換性のために、引き続き `ListObjects` をサポートしています。

次の例は、`ListObjects` の Lambda JSON 入力ペイロードを示しています。

```
{
    "xAmzRequestId": "requestId",
     "**listObjectsContext**": {
     "**inputS3Url**": "https://my-s3-ap-111122223333.s3-accesspoint.us-
east-1.amazonaws.com/?X-Amz-Security-Token=<snip>",
     },
    "configuration": {
        "accessPointArn": "arn:aws:s3-object-lambda:us-
east-1:111122223333:accesspoint/example-object-lambda-ap",
        "supportingAccessPointArn": "arn:aws:s3:us-
east-1:111122223333:accesspoint/example-ap",
        "payload": "{}"
    },
    "userRequest": {
        "url": "https://object-lambda-111122223333.s3-object-lambda.us-
east-1.amazonaws.com/example",
        "headers": {
            "Host": "object-lambda-111122223333.s3-object-lambda.us-
east-1.amazonaws.com",
            "Accept-Encoding": "identity",
            "X-Amz-Content-SHA256": "e3b0c44298fc1example"
        }
    },
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "principalId",
```

```
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/example",
        "accountId": "111122223333",
        "accessKeyId": "accessKeyId",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "Wed Mar 10 23:41:52 UTC 2021"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "principalId",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            }
        }
    },
  "protocolVersion": "1.00"
}
```

Lambda 関数は、S3 Object Lambda から返されるステータスコード、XML 結果のリスト、またはエラー情報を含む JSON オブジェクトを返します。

S3 Object Lambda は `listResultXml` の処理も検証もせず、代わりに `ListObjects` 呼び出し元に転送します。`listBucketResult` については、S3 Object Lambda は特定のプロパティが特定のタイプであることを想定し、解析できない場合は例外をスローします。 `listResultXml` および `listBucketResult` を同時に提供することはできません。

次の例は、署名付き URL を使用して Amazon S3 を呼び出し、その結果を使用してエラーチェックを含むレスポンスを入力する方法を示しています。

Python

```
import requests
import xmltodict

def lambda_handler(event, context):
    # Extract the presigned URL from the input.
    s3_url = event["listObjectsContext"]["inputS3Url"]


    # Get the head of the object from Amazon S3.
    response = requests.get(s3_url)
```

```
    # Return the error to S3 Object Lambda (if applicable).
    if (response.status_code >= 400):
        error = xmltodict.parse(response.content)
        return {
            "statusCode": response.status_code,
            "errorCode": error["Error"]["Code"],
            "errorMessage": error["Error"]["Message"]
        }

    # Store the XML result in a dict.
    response_dict = xmltodict.parse(response.content)

    # This obscures StorageClass in a transformation, it is optional to add
    for item in response_dict['ListBucketResult']['Contents']:
        item['StorageClass'] = ""

    # Convert back to XML.
    listResultXml = xmltodict.unparse(response_dict)

    # Create response with listResultXml.
    response_with_list_result_xml = {
        'statusCode': 200,
        'listResultXml': listResultXml
    }

    # Create response with listBucketResult.
    response_dict['ListBucketResult'] =
 sanitize_response_dict(response_dict['ListBucketResult'])
    response_with_list_bucket_result = {
        'statusCode': 200,
        'listBucketResult': response_dict['ListBucketResult']
    }

    # Return the list to S3 Object Lambda.
    # Can return response_with_list_result_xml or response_with_list_bucket_result
    return response_with_list_result_xml

# Converting the response_dict's key to correct casing
def sanitize_response_dict(response_dict: dict):
    new_response_dict = dict()
    for key, value in response_dict.items():
        new_key = key[0].lower() + key[1:] if key != "ID" else 'id'
        if type(value) == list:
```

```
            newlist = []
            for element in value:
                if type(element) == type(dict()):
                    element = sanitize_response_dict(element)
                newlist.append(element)
            value = newlist
        elif type(value) == dict:
            value = sanitize_response_dict(value)
        new_response_dict[new_key] = value
    return new_response_dict
```

次の例は、ListObjects の Lambda レスポンス JSON の構造を示しています。

```
{
  "statusCode": <number>; // Required
  "errorCode": <string>;
  "errorMessage": <string>;
  "listResultXml": <string>; // This can also be Error XML string in case S3 returned
 error response when calling the pre-signed URL

  "listBucketResult": {  // listBucketResult can be provided instead of listResultXml,
 however they can not both be provided in the JSON response
       "name": <string>,  // Required for 'listBucketResult'
       "prefix": <string>,
       "marker": <string>,
       "nextMarker": <string>,
       "maxKeys": <int>,   // Required for 'listBucketResult'
       "delimiter": <string>,
       "encodingType": <string>
       "isTruncated": <boolean>,  // Required for 'listBucketResult'
       "contents": [  {
           "key": <string>,  // Required for 'content'
           "lastModified": <string>,
           "eTag": <string>,
           "checksumAlgorithm": <string>,   // CRC32,  CRC32C,  SHA1,  SHA256
           "size": <int>,   // Required for 'content'
           "owner": {
               "displayName": <string>,  // Required for 'owner'
               "id": <string>,  // Required for 'owner'
           },
           "storageClass": <string>
           },
```

```
        ...
        ],
        "commonPrefixes": [  {
            "prefix": <string>   // Required for 'commonPrefix'
        },
        ...
        ],
    }
}
```

Lambda での **ListObjectsV2** リクエストの使用

このセクションでは、Object Lambda アクセスポイントが ListObjectsV2 用に Lambda 関数を呼び出すように設定されていることを前提としています。Lambda は、listObjectsV2Context という新しいオブジェクトを持つ JSON ペイロードを受け取ります。listObjectsV2Context には、inputS3Url という単一のプロパティが含まれており、これは ListObjectsV2 をサポートしているアクセスポイント用の署名付き URL です。

GetObject や HeadObject とは異なり、署名付き URL には、次のプロパティが指定されている場合はそれらが含まれます。

- すべてのクエリパラメータ
- requestPayer (x-amz-request-payer ヘッダー内)
- expectedBucketOwner (x-amz-expected-bucket-owner ヘッダー内)

リクエスト構文 URI パラメータについては、「Amazon Simple Storage Service API リファレンス」の「ListObjectsV2」を参照してください。

次の例は、ListObjectsV2 の Lambda JSON 入力ペイロードを示しています。

```
{
    "xAmzRequestId": "requestId",
     "**listObjectsV2Context**": {
     "**inputS3Url**": "https://my-s3-ap-111122223333.s3-accesspoint.us-
east-1.amazonaws.com/?list-type=2&X-Amz-Security-Token=<snip>",
     },
    "configuration": {
        "accessPointArn": "arn:aws:s3-object-lambda:us-
east-1:111122223333:accesspoint/example-object-lambda-ap",
        "supportingAccessPointArn": "arn:aws:s3:us-
east-1:111122223333:accesspoint/example-ap",
```

```
        "payload": "{}"
    },
    "userRequest": {
        "url": "https://object-lambda-111122223333.s3-object-lambda.us-
east-1.amazonaws.com/example",
        "headers": {
            "Host": "object-lambda-111122223333.s3-object-lambda.us-
east-1.amazonaws.com",
            "Accept-Encoding": "identity",
            "X-Amz-Content-SHA256": "e3b0c44298fc1example"
        }
    },
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "principalId",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/example",
        "accountId": "111122223333",
        "accessKeyId": "accessKeyId",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "Wed Mar 10 23:41:52 UTC 2021"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "principalId",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            }
        }
    },
  "protocolVersion": "1.00"
}
```

Lambda 関数は、S3 Object Lambda から返されるステータスコード、XML 結果のリスト、またはエラー情報を含む JSON オブジェクトを返します。

S3 Object Lambda は `listResultXml` の処理も検証もせず、代わりに `ListObjectsV2` 呼び出し元に転送します。`listBucketResult` については、S3 Object Lambda は特定のプロパティが特定のタイプであることを想定し、解析できない場合は例外をスローします。 `listResultXml` および `listBucketResult` を同時に提供することはできません。

次の例は、署名付き URL を使用して Amazon S3 を呼び出し、その結果を使用してエラーチェックを含むレスポンスを入力する方法を示しています。

Python

```
import requests
import xmltodict

def lambda_handler(event, context):
    # Extract the presigned URL from the input.
    s3_url = event["listObjectsV2Context"]["inputS3Url"]


    # Get the head of the object from Amazon S3.
    response = requests.get(s3_url)

    # Return the error to S3 Object Lambda (if applicable).
    if (response.status_code >= 400):
        error = xmltodict.parse(response.content)
        return {
            "statusCode": response.status_code,
            "errorCode": error["Error"]["Code"],
            "errorMessage": error["Error"]["Message"]
        }

    # Store the XML result in a dict.
    response_dict = xmltodict.parse(response.content)

    # This obscures StorageClass in a transformation, it is optional to add
    for item in response_dict['ListBucketResult']['Contents']:
        item['StorageClass'] = ""

    # Convert back to XML.
    listResultXml = xmltodict.unparse(response_dict)

    # Create response with listResultXml.
    response_with_list_result_xml = {
        'statusCode': 200,
        'listResultXml': listResultXml
    }

    # Create response with listBucketResult.
```

```
    response_dict['ListBucketResult'] =
 sanitize_response_dict(response_dict['ListBucketResult'])
    response_with_list_bucket_result = {
        'statusCode': 200,
        'listBucketResult': response_dict['ListBucketResult']
    }

    # Return the list to S3 Object Lambda.
    # Can return response_with_list_result_xml or response_with_list_bucket_result
    return response_with_list_result_xml

# Converting the response_dict's key to correct casing
def sanitize_response_dict(response_dict: dict):
    new_response_dict = dict()
    for key, value in response_dict.items():
        new_key = key[0].lower() + key[1:] if key != "ID" else 'id'
        if type(value) == list:
            newlist = []
            for element in value:
                if type(element) == type(dict()):
                    element = sanitize_response_dict(element)
                newlist.append(element)
            value = newlist
        elif type(value) == dict:
            value = sanitize_response_dict(value)
        new_response_dict[new_key] = value
    return new_response_dict
```

次の例は、ListObjectsV2 の Lambda レスポンス JSON の構造を示しています。

```
{
    "statusCode": <number>; // Required
    "errorCode": <string>;
    "errorMessage": <string>;
    "listResultXml": <string>; // This can also be Error XML string in case S3 returned
 error response when calling the pre-signed URL

    "listBucketResult": {  // listBucketResult can be provided instead of
 listResultXml, however they can not both be provided in the JSON response
        "name": <string>, // Required for 'listBucketResult'
        "prefix": <string>,
        "startAfter": <string>,
```

```
        "continuationToken": <string>,
        "nextContinuationToken": <string>,
        "keyCount": <int>, // Required for 'listBucketResult'
        "maxKeys": <int>, // Required for 'listBucketResult'
        "delimiter": <string>,
        "encodingType": <string>
        "isTruncated": <boolean>, // Required for 'listBucketResult'
        "contents": [ {
            "key": <string>, // Required for 'content'
            "lastModified": <string>,
            "eTag": <string>,
            "checksumAlgorithm": <string>, // CRC32, CRC32C, SHA1, SHA256
            "size": <int>, // Required for 'content'
            "owner": {
                "displayName": <string>, // Required for 'owner'
                "id": <string>, // Required for 'owner'
            },
            "storageClass": <string>
            },
            ...
        ],
        "commonPrefixes": [ {
            "prefix": <string> // Required for 'commonPrefix'
            },
        ...
        ],
    }
}
```

イベントコンテキストの形式と使用法

Amazon S3 Object Lambda は、AWS Lambda 関数に渡されたイベントで行われたリクエストに関するコンテキストを提供します。リクエストの例を次に示します。フィールドの説明は例の後に含まれています。

```
{
    "xAmzRequestId": "requestId",
    "getObjectContext": {
        "inputS3Url": "https://my-s3-ap-111122223333.s3-accesspoint.us-
east-1.amazonaws.com/example?X-Amz-Security-Token=<snip>",
        "outputRoute": "io-use1-001",
        "outputToken": "OutputToken"
    },
```

```
    "configuration": {
        "accessPointArn": "arn:aws:s3-object-lambda:us-
east-1:111122223333:accesspoint/example-object-lambda-ap",
        "supportingAccessPointArn": "arn:aws:s3:us-
east-1:111122223333:accesspoint/example-ap",
        "payload": "{}"
    },
    "userRequest": {
        "url": "https://object-lambda-111122223333.s3-object-lambda.us-
east-1.amazonaws.com/example",
        "headers": {
            "Host": "object-lambda-111122223333.s3-object-lambda.us-
east-1.amazonaws.com",
            "Accept-Encoding": "identity",
            "X-Amz-Content-SHA256": "e3b0c44298fc1example"
        }
    },
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "principalId",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/example",
        "accountId": "111122223333",
        "accessKeyId": "accessKeyId",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "Wed Mar 10 23:41:52 UTC 2021"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "principalId",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            }
        }
    },
    "protocolVersion": "1.00"
}
```

リクエストには次のフィールドが含まれます。

- `xAmzRequestId` - このリクエストの Amazon S3 リクエスト ID。デバッグに役立つように、この値をログに記録することをお勧めします。
- `getObjectContext` - Amazon S3 および S3 Object Lambda への接続に関する入力および出力の詳細。
  - `inputS3Url` - Amazon S3 から元のオブジェクトを取得するために使用できる署名付き URL。URL は元の発信者のアイデンティティを使用して署名され、URL が使用されるときにそのユーザーのアクセス許可が適用されます。URL に署名されたヘッダーがある場合、Lambda 関数では、`Host` ヘッダーを除き、Amazon S3 への呼び出しにこれらのヘッダーを含める必要があります。
  - `outputRoute` – Lambda 関数が `WriteGetObjectResponse` を呼び出すときに S3 Object Lambda URL に追加されるルーティングトークン。
  - `outputToken` - `WriteGetObjectResponse` 呼び出しを元の発信者と一致させるために、S3 Object Lambda によって使用される不透明なトークン。
- `configuration` - Object Lambda アクセスポイントに関する設定情報。
  - `accessPointArn` - このリクエストを受信した Object Lambda アクセスポイントの Amazon リソースネーム (ARN)。
  - `supportingAccessPointArn` - Object Lambda アクセスポイント設定で指定されているサポートアクセスポイントの ARN。
  - `payload` - Object Lambda アクセスポイント設定に適用されるカスタムデータ。S3 Object Lambda はこのデータを不透明な文字列として扱うため、使用前にデコードする必要がある場合があります。
- `userRequest` - S3 Object Lambda への元の呼び出しに関する情報。
  - `url` - S3 Object Lambda で受信したリクエストのデコードされた URL。認可関連のクエリパラメータは除きます。
  - `headers` - HTTP ヘッダーと元の呼び出しからの値を含む文字列への文字列マップ。認可関連のヘッダーは含まれません。同じヘッダーが複数回表示される場合、同じヘッダーの各インスタンスからの値は、コンマ区切りのリストに結合されます。元のヘッダーの大文字と小文字は、このマップに保持されます。
- `userIdentity` – S3 Object Lambda への呼び出しを行ったアイデンティティの詳細。詳細については、「AWS CloudTrail ユーザーガイド」の「証跡のデータイベントの記録」を参照してください。
  - `type` – アイデンティティのタイプ。
  - `accountId` - アイデンティティが属するAWS アカウント。

  - `userName` - 呼び出しを行ったアイデンティティのわかりやすい名前。
  - `principalId` - 呼び出しを行ったアイデンティティの一意の識別子。
  - `arn` – 呼び出しを行ったプリンシパルの ARN。ARN の最後のセクションには、呼び出しを行ったユーザーまたはロールが含まれています。
  - `sessionContext` - リクエストが、一時的セキュリティ認証情報を使用して行われた場合、このエレメントはこれらの認証情報のために作成されたセッションに関する情報を提供します。
  - `invokedBy` – Amazon EC2 Auto Scaling や AWS Elastic Beanstalk など、リクエストを行った AWS のサービス の名前。
  - `sessionIssuer` - リクエストが一時的セキュリティ認証情報を使用して行われた場合、このエレメントは認証情報がどのように取得されたかに関する情報を提供します。
- `protocolVersion` – 提供されるコンテキストのバージョン ID。このフィールドの形式は `{Major Version}.{Minor Version}` です。マイナーバージョン番号は、常に 2 桁の数字です。フィールドのセマンティクスを削除または変更する場合は、メジャーバージョンバンプが必要となり、アクティブなオプトインが必要になります。Amazon S3 ではいつでも新しいフィールドを追加できます。この時点で、マイナーバージョンのバンプが発生する可能性があります。ソフトウェアのロールアウトの性質上、一度に複数のマイナーバージョンが使用されている場合があります。

Range および partNumber ヘッダーの操作

Amazon S3 Object Lambda で大規模なオブジェクトを操作する場合は、`Range` HTTP ヘッダーを使用して、オブジェクトから指定されたバイト範囲をダウンロードできます。同じオブジェクトのさまざまなバイト範囲をフェッチするには、Amazon S3 への同時接続を使用できます。また、オブジェクトの指定されたパートに対して範囲リクエストを実行する `partNumber` パラメータ(1 ~ 10,000 の整数) を指定することもできます。

`Range` または `partNumber` のパラメータを含んだリクエストを処理するには、複数の方法があるため、S3 オブジェクト Lambda ではこれらのパラメータを変換されたオブジェクトに適用しません。代わりに、AWS Lambda 関数は、アプリケーションで必要に応じてこの機能を実装する必要があります。

S3 Object Lambda で `Range` および `partNumber` パラメータを使用するには、次の操作を行います。

- Object Lambda アクセスポイントの設定でこれらのパラメータを有効にします。
- これらのパラメータを含むリクエストを処理できる Lambda 関数を作成します。

次のステップでそのやり方を説明します。

ステップ 1: Object Lambda アクセスポイントの設定

デフォルトでは、オブジェクト Lambda アクセスポイントは、ヘッダーまたはクエリパラメータに Range または partNumber パラメータを含む GetObject または HeadObject リクエストに対して、HTTP ステータスコード 501 (未実装) エラーで応答します。

Object Lambda アクセスポイントがこのようなリクエストを有効にするには、Object Lambda アクセスポイント設定の AllowedFeatures セクションに GetObject-Range、GetObject-PartNumber、HeadObject-Range、または HeadObject-PartNumber を含める必要があります。Object Lambda アクセスポイントの設定の更新の詳細については、「Object Lambda アクセスポイントの作成」を参照してください。

ステップ 2: Lambda 関数で **Range** または **partNumber** 処理を実装する

Object Lambda アクセスポイントが範囲 GetObject または HeadObject のリクエストで Lambda 関数を呼び出すとき、Range または partNumber パラメータはイベントコンテキストに含まれます。イベントコンテキストでのパラメータの場所は、次の表で説明するように、使用されたパラメータと Object Lambda アクセスポイントへの元のリクエストにどのように Lambda 含まれていたかによって異なります。

パラメータ	イベントコンテキストの場所
Range (ヘッダー)	userRequest.headers.Range
Range (クエリパラメータ)	userRequest.url (クエリパラメータ Range)
partNumber	userRequest.url (クエリパラメータ partNumber)

> **Important**
>
> 指定された Object Lambda アクセスポイントの署名付き URL には、元のリクエストの Range または partNumber パラメータが含まれていません。AWS Lambda 関数でこれらのパラメータを処理する方法については、以下のオプションを参照してください。

Range または partNumber の値を抽出した後に、アプリケーションのニーズに基づいて、次のいずれかの方法を使用できます。

A. リクエストされた **Range** または **partNumber** を変換されたオブジェクトにマッピングします (推奨)。

   Range または partNumber リクエストを処理する最も確実な方法は、以下を実行することです。

   - Amazon S3 から完全なオブジェクトを取得します。
   - オブジェクトを変換します。
   - リクエストされた Range または partNumber パラメータを変換後のオブジェクトに適用します。

   これを行うには、指定された署名付き URL を使用して Amazon S3 からオブジェクト全体をフェッチし、必要に応じてオブジェクトを処理します。例の Lambda 関数では、この方法で Range パラメータを設定し、AWS サンプル GitHub リポジトリの「このサンプル」を参照してください。

B. リクエストされた Range を署名付き URL にマッピングします。

   場合によっては、Lambda 関数でリクエストされた Range を署名済み URL に直接マッピングして、Amazon S3 からオブジェクトの一部のみを取得できます。このアプローチは、変換が次の両方の条件を満たしている場合にのみ適切です。

   1. 変換関数は、部分的なオブジェクト範囲に適用できます。
   2. 変換関数の前または後に Range パラメータを指定すると、同じ変換後のオブジェクトになります。

   たとえば、ASCII エンコードオブジェクト内のすべての文字を大文字に変換する変換関数は、上記の両方の条件を満たします。変換はオブジェクトの一部に適用でき、変換前に Range パラメータを適用すると、変換後にパラメータを適用するのと同じ結果が得られます。

   対照的に、ASCII エンコードされたオブジェクトの文字を反転する関数は、これらの条件を満たしていません。このような関数は、部分的なオブジェクト範囲に適用できるため、基準 1 を満たしています。ただし、基準 2 を満たしていません。なぜなら、Range パラメータを変換前に適用した場合と、変換後にパラメータを適用する場合とは結果が異なるためです。

   コンテンツ abcdefg を含むオブジェクトの最初の 3 文字に関数を適用するリクエストを考えてみましょう。変換前にの Range パラメータを適用すると abc のみが取得され、その後、データ

を逆にして戻すと cba が取得されます。しかし、変換後にパラメータが適用された場合、関数はオブジェクト全体を取得し、それを反転し、Range パラメータを適用して、gfe を返します。これらの結果は異なるため、この関数は Amazon S3 からオブジェクトを取得する際に、Range パラメータを適用すべきではありません。代わりに、オブジェクト全体を取得し、変換を実行してから、Range パラメータを適用する必要があります。

> **Warning**
>
> 多くの場合、Range パラメータを署名済み URL に適用すると、Lambda 関数またはリクエスト元のクライアントによる予期しない動作が発生します。Amazon S3 から部分的なオブジェクトのみを取得するときにアプリケーションが正常に動作することが確実でない限り、アプローチ A で前述したように、完全なオブジェクトを取得して変換することをお勧めします。

アプリケーションがアプローチ B の基準を満たしていれば、要求されたオブジェクト範囲のみをフェッチし、その範囲で変換を実行することで、AWS Lambda 関数を単純化することができます。

次の Java コードの例では、次の処理を実行する方法を示します。

- GetObject リクエストから Range ヘッダーを取得します。
- Lambda が Amazon S3 からリクエストされた範囲を取得するために使用できる署名付き URL に Range ヘッダーを追加します。

```
private HttpRequest.Builder applyRangeHeader(ObjectLambdaEvent event,
 HttpRequest.Builder presignedRequest) {
    var header = event.getUserRequest().getHeaders().entrySet().stream()
            .filter(e -> e.getKey().toLowerCase(Locale.ROOT).equals("range"))
            .findFirst();

    // Add check in the query string itself.
    header.ifPresent(entry -> presignedRequest.header(entry.getKey(),
 entry.getValue()));
    return presignedRequest;
}
```

AWS で構築された Lambda 関数の使用

AWS には、あらかじめ構築された AWS Lambda 関数が用意されています。これを Amazon S3 Object Lambda と共に使用して、個人を特定できる情報 (PII) を検出して編集したり、S3 オブジェクトを解凍したりできます。これらの Lambda 関数は AWS Serverless Application Repository にあります。これらの関数は、Object Lambda アクセスポイントの作成時に AWS Management Console から選択できます。

AWS Serverless Application Repository からサーバーレスアプリケーションをデプロイする方法の詳細については、「AWS Serverless Application Repository デベロッパーガイド」の「アプリケーションのデプロイ」を参照してください。

> **Note**
>
> 次の例は `GetObject` リクエストでのみ使用できます。

例 1: PII アクセスコントロール

Lambda 関数は Amazon Comprehend を使用します。これは、機械学習を使用してテキスト内でインサイトや関係性を検出する自然言語処理 (NLP) サービスです。この関数は、Amazon S3 バケット内のドキュメントから、名前、住所、日付、クレジットカード番号、社会保障番号などの個人を特定できる情報 (PII) を自動的に検出します。バケットに PII を含むドキュメントがある場合、PII アクセスコントロール関数を設定して、PII エンティティタイプを検出し、許可されていないユーザーへのアクセスを制限できます。

使用開始するには、アカウントに次の Lambda 関数をデプロイし、関数の Amazon リソースネーム (ARN) を Object Lambda アクセスポイント設定に追加します。

この関数の ARN の例を以下に示します。

```
arn:aws:serverlessrepo:us-east-1:111122223333:applications/
ComprehendPiiAccessControlS3ObjectLambda
```

AWS Management Console でこの関数をビューに追加するには、次の AWS Serverless Application Repository リンクを使用します。ComprehendPiiAccessControlS3ObjectLambda

GitHub でこの関数を表示するには、「Amazon Comprehend S3 Object Lambda」 を参照してください。

例 2: PII Redaction

Lambda 関数は Amazon Comprehend を使用します。これは、機械学習を使用してテキスト内でインサイトや関係性を検出する自然言語処理 (NLP) サービスです。この関数は、Amazon S3 バケット内のドキュメントから、名前、住所、日付、クレジットカード番号、社会保障番号などの個人を特定できる情報 (PII) を自動的にマスキングします。

クレジットカード番号や銀行口座情報などの情報を含むドキュメントがバケットにある場合は、PII Redaction S3 Object Lambda 関数を設定して、PII を検出し、PII エンティティタイプがマスキングされたドキュメントのコピーを返すように設定できます。

使用開始するには、アカウントに次の Lambda 関数をデプロイし、関数の ARN を Object Lambda アクセスポイント設定に追加します。

この関数の ARN の例を以下に示します。

```
arn:aws:serverlessrepo:us-east-1:111122223333::applications/
ComprehendPiiRedactionS3ObjectLambda
```

AWS Management Console にこの関数を表示または追加するには、次の AWS Serverless Application Repository リンクを使用します。ComprehendPiiRedactionS3ObjectLambda

GitHub でこの関数を表示するには、「Amazon Comprehend S3 Object Lambda」を参照してください。

PII リダクションにおけるいくつかの S3 Object Lambda タスクにおけるエンドツーエンドの一連の手順については、「チュートリアル: S3 Object Lambda と Amazon Comprehend を使用した PII データの検出と編集」を参照してください。

例 3: 解凍

Lambda 関数 `S3ObjectLambdaDecompression` は、Amazon S3 に格納されているオブジェクトを、次の 6 つの圧縮ファイル形式のうちの 1 つで解凍できます。`bzip2`、`gzip`、`snappy`、`zlib`、`zstandard`、および `ZIP`。

使用開始するには、アカウントに次の Lambda 関数をデプロイし、関数の ARN を Object Lambda アクセスポイント設定に追加します。

この関数の ARN の例を以下に示します。

```
arn:aws:serverlessrepo:us-east-1:111122223333::applications/S3ObjectLambdaDecompression
```

AWS Management Console でこの関数をビューに追加するには、次の AWS Serverless Application Repository リンクを使用します。S3ObjectLambdaDecompression

GitHub でこの関数を表示するには、「S3 Object Lambda Decompression」(S3 Object Lambda の解凍) を参照してください。

S3 Object Lambda のベストプラクティスとガイドライン

S3 Object Lambda を使用する場合は、操作とパフォーマンスを最適化するには、以下のベストプラクティスとガイドラインに従ってください。

トピック

- S3 Object Lambda の使用
- S3 Object Lambda に関連して使用される AWS のサービス
- Range および partNumber ヘッダー
- expiry-date の変換
- AWS CLI と AWS SDK の使用

S3 Object Lambda の使用

S3 Object Lambda は、GET、LIST、および HEAD リクエストの処理のみをサポートします。他のリクエストは AWS Lambda を呼び出さず、標準の変換されていない API レスポンスを返します。リージョンごとに AWS アカウント あたり最大 1,000 個の Object Lambda アクセスポイントを作成できます。使用する AWS Lambda 関数は、Object Lambda アクセスポイントと同じ AWS アカウントおよびリージョンに存在する必要があります。

S3 Object Lambda では、発信者に完全なレスポンスをストリームするのに最大 60 秒かかります。関数には、AWS Lambda のデフォルトクォータも適用されます。詳細については、AWS Lambda デベロッパーガイドの Lambda のクォータを参照してください。

S3 Object Lambda が指定された Lambda 関数を呼び出す場合、データが指定された Lambda 関数またはアプリケーションによって意図的に上書きまたは Amazon S3 から削除され、それが正しいことを確認する責任は、ユーザーにあります。

S3 Object Lambda は、オブジェクトに対する操作の実行にのみ使用できます。S3 Object Lambda を使用して、バケットの変更や削除など、他の Amazon S3 オペレーションを実行することはできません。アクセスポイントをサポートする S3 オペレーションの詳細なリストについては、「汎用バケットのアクセスポイントと S3 オペレーションとの互換性」を参照してください。

このリストに加えて、Object Lambda アクセスポイントは `POST Object`、`CopyObject` (ソースとして)、および `SelectObjectContent` API オペレーションをサポートしていません。

S3 Object Lambda に関連して使用される AWS のサービス

S3 Object Lambda は、Amazon S3、AWS Lambda、およびオプションで、リクエストしているアプリケーションに関連するオブジェクトを配信するために選択した他の AWS のサービス を接続します。S3 Object Lambda で使用されるすべての AWS のサービス は、それぞれのサービスレベルアグリーメント (SLA) に準拠します。例えば、AWS のサービス がサービスコミットメントを満たさない場合は、そのサービスの SLA に記されたとおり、ユーザーにはサービスクレジットを受け取る資格が発生します。

`Range` および `partNumber` ヘッダー

大規模なオブジェクトを操作する場合は、Range HTTP ヘッダーを使用して、オブジェクトから指定されたバイト範囲をダウンロードできます。`Range` ヘッダーを使用すると、リクエストはオブジェクトの指定された部分のみをフェッチします。`partNumber` ヘッダーは、オブジェクトから指定されたパートに対して範囲リクエストを実行するためにも使用できます。

詳細については、「Range および partNumber ヘッダーの操作」を参照してください。

`expiry-date` の変換

AWS Management Console の Object Lambda アクセスポイントから、変換されたオブジェクトを開いたり、ダウンロードしたりできます。これらのオブジェクトは、期限が切れていないものである必要があります。Lambda 関数でオブジェクトの `expiry-date` を変換すると、開いたりダウンロードしたりできない期限切れのオブジェクトが表示されることがあります。この動作は、S3 Glacier Flexible Retrieval、および S3 Glacier Deep Archive の復元されたオブジェクトにのみ適用されます。

AWS CLI と AWS SDK の使用

AWS Command Line Interface (AWS CLI) S3 サブコマンド (`cp`、`mv`、および `sync`)、および AWS SDK for Java `TransferManager` クラスについては、S3 Object Lambda での使用はサポートされていません。

S3 Object Lambda のチュートリアル

次のチュートリアルでは、いくつかの S3 Object Lambda タスクにおけるエンドツーエンドの一連の手順について説明します。

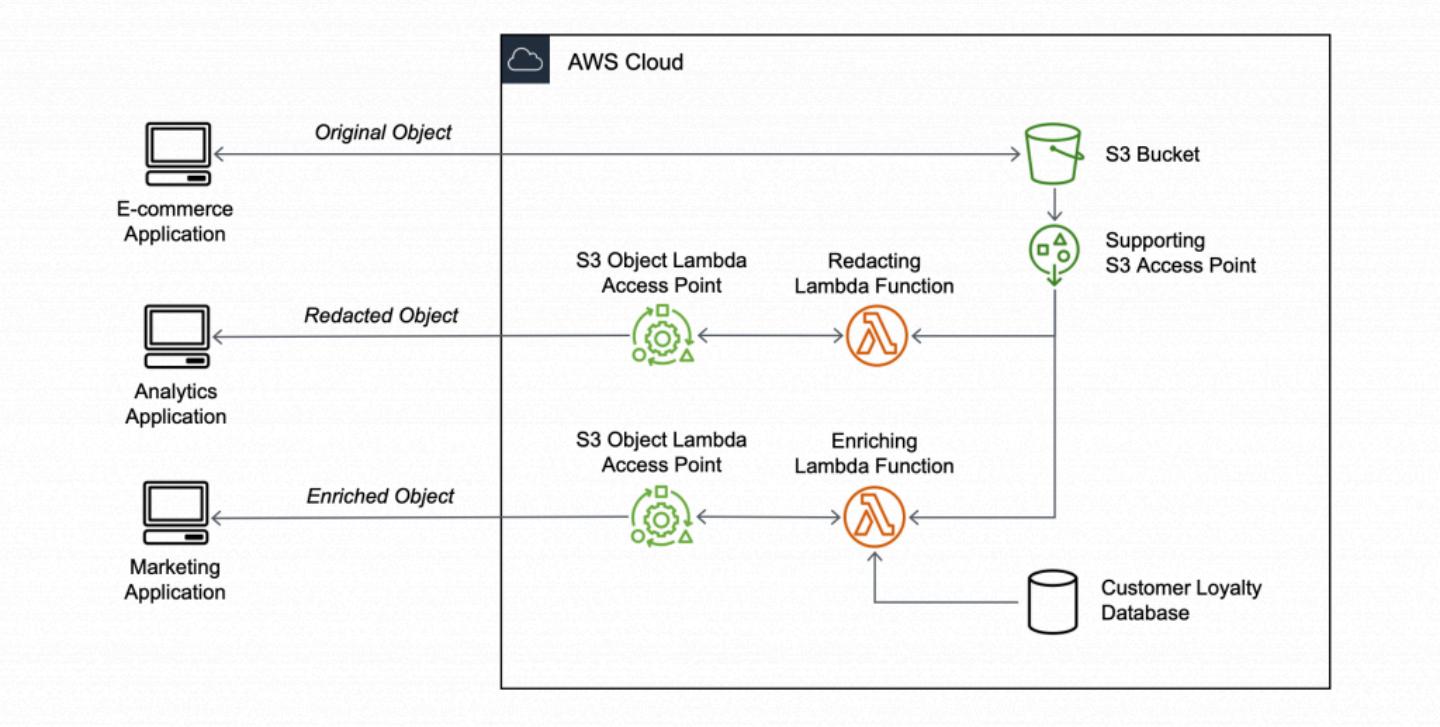
S3 Object Lambda を使用すると、独自のコードを追加して、データがアプリケーションに返される前に S3 からのデータを処理できます。以下のチュートリアルでは、既存のオブジェクトを変更したり、データの複数のコピーを維持したりすることなく、Amazon S3 から取得されるデータを変更します。最初のチュートリアルでは、S3 GET リクエストに AWS Lambda 関数を追加して、S3 から取得したオブジェクトを変更する方法について説明します。2 番目のチュートリアルでは、Amazon Comprehend を搭載した構築済みの Lambda 関数を使用して、S3 から取得した個人を特定できる情報 (PII) をアプリケーションに返す前に保護する方法を示します。3 番目のチュートリアルでは、S3 Object Lambda を使用してAmazon S3から取得されるイメージに透かしを追加します。

- チュートリアル: S3 Object Lambda を使用したアプリケーションのデータの変換
- チュートリアル: S3 Object Lambda と Amazon Comprehend を使用した PII データの検出と編集
- チュートリアル: S3 Object Lambda を使用して、取得時に画像に動的に透かしを入れる

チュートリアル: S3 Object Lambda を使用したアプリケーションのデータの変換

Amazon S3 にデータを保管すると、複数のアプリケーションで使用するために簡単にデータを共有できます。ただし、各アプリケーションには固有のデータ形式の要件があり、特定のユースケースでデータの変更や処理が必要になる場合があります。例えば、e コマースアプリケーションによって作成されたデータセットには、個人を特定できる情報 (PII) が含まれている場合があります。分析のために同じデータが処理される場合、この PII は必要ないため、編集する必要があります。ただし、同じデータセットをマーケティングキャンペーンに使用する場合は、顧客ロイヤルティデータベースからの情報など、追加の詳細でデータを充実させる必要がある場合があります。

S3 Object Lambda を使用すると、独自のコードを追加して、データがアプリケーションに返される前に S3 からのデータを処理できます。具体的には、AWS Lambda 関数を設定して、S3 Object Lambda アクセスポイントにアタッチします。アプリケーションが S3 Object Lambda アクセスポイントを介して 標準 S3 GET リクエスト を送信すると、指定された Lambda 関数が呼び出され、サポートする S3 アクセスポイントを介して S3 バケットから取得されたデータが処理されます。その後、S3 Object Lambda アクセスポイントは、変換された結果をアプリケーションに返します。独自のカスタム Lambda 関数を作成して実行し、S3 Object Lambda データ変換を特定のユースケースに合わせて調整できます。すべて、アプリケーションの変更は不要です。



目的

このチュートリアルでは、標準の S3 GET リクエストにカスタムコードを追加して、リクエストしたクライアントまたはアプリケーションのニーズに合うように、S3 から取得したリクエストされたオブジェクトを変更する方法を学習します。具体的には、S3 に保存されている元のオブジェクトのすべてのテキストを S3 Object Lambda を使用して大文字に変換する方法を学習します。

> **Note**
>
> このチュートリアルでは、Python コードを使用してデータを変換します。他の AWS SDK の使用例については、AWS SDK コードサンプルライブラリの「S3 Object Lambda でアプリケーションのデータを変換する」を参照してください。

トピック

- 前提条件
- ステップ 1: S3 バケットを作成する。
- ステップ 2: S3 バケットにファイルをアップロード
- ステップ 3: S3 アクセスポイントの作成
- ステップ 4: Lambda 関数を作成する

- ステップ 5: Lambda 関数の実行ロールの IAM ポリシーを設定する
- ステップ 6: Object Lambda アクセスポイントの作成
- ステップ 7: 変換されたデータを表示する
- ステップ 8: クリーンアップする
- 次のステップ

前提条件

このチュートリアルを開始する前に、適切な許可が付与された AWS Identity and Access Management (IAM) ユーザーとしてサインインできる AWS アカウントが必要です。また、バージョン 3.8 以降の Python をインストールする必要があります。

サブステップ

- AWS アカウントでアクセス許可を持つ IAM ユーザーを作成します (コンソール)。
- ローカルマシンに Python 3.8 以降をインストールする

AWS アカウントでアクセス許可を持つ IAM ユーザーを作成します (コンソール)。

チュートリアル用の IAM ユーザーを作成できます。このチュートリアルを完了するには、IAM ユーザーが次の IAM ポリシーをアタッチして、関連する AWS リソースにアクセスし、特定のアクションを実行する必要があります。IAM ユーザーを作成する方法の詳細については、「IAM ユーザーガイド」の「IAM ユーザーの作成 (コンソール)」を参照してください。

IAM ユーザーには次のポリシーが必要です。

- AmazonS3FullAccess – Object Lambda アクセスポイントを作成および使用するための許可を含む、すべての Amazon S3 アクションに対する許可を付与します。
- AWSLambda_FullAccess – すべての Lambda アクションに許可を付与します。
- IAMFullAccess – すべての IAM アクションに許可を付与します。
- IAMAccessAnalyzerReadOnlyAccess – IAM Access Analyzer によって提供されるすべてのアクセス情報を読み取る許可を付与します。
- CloudWatchLogsFullAccess – CloudWatch Logs へのフルアクセスを付与します。

> **Note**
>
> このチュートリアルでは、わかりやすいように IAM ユーザーを作成して使用します。このチュートリアルを完了したら、忘れずに「IAM ユーザーを削除する」を行います。本番環境で使用する場合は、IAM ユーザーガイドの「IAM でのセキュリティのベストプラクティス」に従うことをお勧めします。ベストプラクティスでは、人間のユーザーと ID プロバイダーとのフェデレーションにより、一時的な認証情報を使用して AWS にアクセスする必要があります。追加のベストプラクティスとして、ワークロードでは一時的な認証情報で IAM ロールを使用し、AWS にアクセス必要があります。AWS IAM Identity Center を使用して一時的な認証情報を持つユーザーを作成する方法については、「AWS IAM Identity Center ユーザーガイド」の「開始方法」を参照してください。
> このチュートリアルでは、フルアクセス権を持つ AWS マネージドポリシーも使用します。実稼働環境では、代わりに、セキュリティのベストプラクティスに従って、ユースケースに必要な最小限の許可のみを付与することをお勧めします。

ローカルマシンに Python 3.8 以降をインストールする

次の手順に従って、Python 3.8 以降をローカルマシンにインストールします。インストール手順については、Python の Beginner Guide で「Python のダウンロード」ページを参照してください。

1. ローカルターミナルまたはシェルを開き、次のコマンドを実行して、Python がすでにインストールされているかどうか、インストールされている場合は、どのバージョンがインストールされているかを確認します。

   ```
   python --version
   ```

2. Python 3.8 以降をお持ちでない場合は、ローカルマシンに適した Python 3.8 以降の公式インストーラをダウンロードします。
3. ダウンロードしたファイルをダブルクリックしてインストーラを実行し、手順に従ってインストールを完了します。

   Windows ユーザーの場合、インストールウィザードで [Python 3.X を PATH に追加] を選択してから、[今すぐ、インストール] を選択します。
4. ターミナルを閉じて再度開いて、再起動します。
5. 次のコマンドを実行して、Python 3.8 以降が正しくインストールされていることを確認します。

macOS ユーザーの場合は、このコマンドを実行します。

```
python3 --version
```

Windows ユーザーの場合は、このコマンドを実行します。

```
python --version
```

6. 次のコマンドを実行して、pip3 パッケージマネージャーがインストールされていることを確認します。コマンド応答に pip のバージョン番号と python 3.8 以降が表示された場合、pip3 パッケージマネージャが正常にインストールされていることを意味します。

```
pip --version
```

ステップ 1: S3 バケットを作成する。

変換する元のデータを保存するバケットを作成します。

バケットを作成するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。
3. [Create bucket (バケットの作成)] を選択します。

   [バケットの作成] ページが開きます。
4. [バケット名] に、バケットの名前 (例、**tutorial-bucket**) を入力します。

   Amazon S3 のバケット命名規則の詳細については、「汎用バケットの命名規則」を参照してください。
5. [リージョン] で、バケットを保存する AWS リージョン を選択します。

   バケットのリージョンの詳細については、「汎用バケットの概要」を参照してください。
6. [このバケットのパブリックアクセス設定をブロック] で、デフォルト設定 (ブロックすべてパブリックアクセスが有効) のままであることを確認します。

ユースケースでオフにする必要のある設定が 1 つ以上あることがわかっている場合を除き、すべてのブロックパブリックアクセス設定を有効にしておくことをお勧めします。パブリックアクセスのブロックの詳細については、Amazon S3 ストレージへのパブリックアクセスのブロックを参照してください。

7. 残りの設定はデフォルトのままにしておきます。

   (オプション) 特定のユースケースに追加のバケット設定を設定する場合は、「汎用バケットの作成」を参照してください。

8. [バケットを作成] を選択します。

ステップ 2: S3 バケットにファイルをアップロード

S3 バケットにテキストファイルをアップロードします。このテキストファイルには、このチュートリアルの後半で大文字に変換する元のデータが含まれています。

例えば、次のテキストが含まれている `tutorial.txt` ファイルをアップロードできます。

```
Amazon S3 Object Lambda Tutorial:
You can add your own code to process data retrieved from S3 before
returning it to an application.
```

バケットにファイルをアップロードするには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。
3. [バケット] リストで、ステップ 1 で作成したバケットの名前を選択し (**`tutorial-bucket`** など)、ファイルをアップロードします。
4. バケットの [オブジェクト] タブで、[アップロード] を選択します。
5. [アップロード] ページの [ファイルとフォルダ] の下で、[ファイルを追加] を選択します。
6. アップロードするファイルを選択し、続いて [オープン] を選択します。例えば、前述した `tutorial.txt` ファイルの例をアップロードできます。
7. [アップロード] を選択します。

ステップ 3: S3 アクセスポイントの作成

S3 Object Lambda アクセスポイントを使用して元のデータにアクセスし、変換するには、S3 アクセスポイントを作成し、ステップ 1 で作成した S3 バケットに関連付けます。アクセスポイントは、変換するオブジェクトと同じ AWS リージョン に存在する必要があります。

このチュートリアルの後半では、このアクセスポイントを Object Lambda アクセスポイントのサポートアクセスポイントとして使用します。

アクセスポイントを作成するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[アクセスポイント] を選択します。
3. [アクセスポイント] ページで、[アクセスポイントの作成] を選択します。
4. [アクセスポイント名] フィールドに、アクセスポイントの名前を入力します (**tutorial-access-point** など)。

   アクセスポイントの名前付けの詳細については、「汎用バケットの Amazon S3 アクセスポイントの命名規則」を参照してください。
5. [バケット名] フィールドに、ステップ 1 で作成したバケットの名前を入力します(**tutorial-bucket** など)。S3 は、アクセスポイントをこのバケットにアタッチします。

   (オプション) [S3 を参照] を選択して、アカウント内のバケットを参照および検索できます。[S3 を参照] を選択した場合は、目的のバケットを選択し、[パスの選択] を選択して、[バケット名] フィールドにバケットの名前を入力します。
6. [ネットワークオリジン] で、[インターネット] を選択します。

   アクセスポイントのネットワークオリジンの詳細については、「仮想プライベートクラウドに制限された汎用バケットのアクセスポイントの作成」を参照してください。
7. デフォルトでは、アクセスポイントに対してすべてのブロックパブリックアクセス設定が有効になります。パブリックアクセスブロック設定は、すべてを有効にしておくことを推奨します。

   詳細については、「汎用バケットのアクセスポイントへのパブリックアクセスの管理」を参照してください。
8. その他のすべてのアクセスポイント設定で、デフォルトの設定を保持します。

(オプション) アクセスポイントの設定は、ユースケースをサポートするように変更できます。このチュートリアルでは、デフォルトの設定を保持することをお勧めします。

(オプション) アクセスポイントへのアクセスを管理する必要がある場合は、アクセスポイントポリシーを指定できます。詳細については、「汎用バケットのアクセスポイントのポリシー例」を参照してください。

9. [アクセスポイントを作成] を選択します。

ステップ 4: Lambda 関数を作成する

元のデータを変換するには、S3 Object Lambda アクセスポイントで使用する Lambda 関数を作成します。

サブステップ

- Lambda 関数コードを記述し、仮想環境でデプロイパッケージを作成する
- 実行ロールを使用した Lambda 関数の作成 (コンソール)
- .zip ファイルアーカイブを使用して Lambda 関数コードをデプロイし、Lambda 関数を設定 (コンソール)

Lambda 関数コードを記述し、仮想環境でデプロイパッケージを作成する

1. ローカルマシンで、このチュートリアルの後半で使用する仮想環境に対して、フォルダ名が `object-lambda` であるフォルダを作成します。
2. `object-lambda` フォルダで、元のオブジェクトのすべてのテキストを大文字に変更する Lambda 関数を含むファイルを作成します。例えば、Python で記述された次の関数を使用できます。この関数は、`transform.py` という名前のファイルに保存してください。

```
import boto3
import requests
from botocore.config import Config

# This function capitalizes all text in the original object
def lambda_handler(event, context):
    object_context = event["getObjectContext"]
    # Get the presigned URL to fetch the requested original object
    # from S3
    s3_url = object_context["inputS3Url"]
```

```
    # Extract the route and request token from the input context
    request_route = object_context["outputRoute"]
    request_token = object_context["outputToken"]

    # Get the original S3 object using the presigned URL
    response = requests.get(s3_url)
    original_object = response.content.decode("utf-8")

    # Transform all text in the original object to uppercase
    # You can replace it with your custom code based on your use case
    transformed_object = original_object.upper()

    # Write object back to S3 Object Lambda
    s3 = boto3.client('s3', config=Config(signature_version='s3v4'))
    # The WriteGetObjectResponse API sends the transformed data
    # back to S3 Object Lambda and then to the user
    s3.write_get_object_response(
        Body=transformed_object,
        RequestRoute=request_route,
        RequestToken=request_token)

    # Exit the Lambda function: return the status code
    return {'status_code': 200}
```

> **Note**
>
> 前述の例の Lambda 関数は、リクエストされたオブジェクト全体をメモリにロードしてから、変換してクライアントに返します。または、オブジェクト全体をメモリにロードしないようにするために、S3 からオブジェクトをストリーミングすることもできます。この方法は、大きなオブジェクトを扱うときに役立ちます。Object Lambda アクセスポイントを使用したレスポンスのストリーミングの詳細については、Lambda での GetObject リクエストの使用 にあるストリーミングの例を参照してください。

S3 Object Lambda アクセスポイントで使用する Lambda 関数を記述する場合、この関数は S3 Object Lambda が Lambda 関数に提供する入力イベントコンテキストに基づいています。イベントコンテキストは、S3 Object Lambda から Lambda に渡されたイベントで行われたリクエストに関する情報を提供します。これには、Lambda 関数の作成に使用するパラメータが含まれています。

前述の Lambda 関数の作成に使用されるフィールドは次のとおりです。

`getObjectContext` のフィールドは、Amazon S3 および S3 Object Lambda への接続に関する入力および出力の詳細を意味します。以下のフィールドがあります。

- `inputS3Url` – Lambda 関数がサポートするアクセスポイントから元のオブジェクトをダウンロードするために使用できる署名付き URL です。Lambda 関数は、署名付き URL を使用することにより、元のオブジェクトを取得するために Amazon S3 の読み取り許可を必要とせず、呼び出しごとに処理されたオブジェクトにのみアクセスできます。
- `outputRoute` – Lambda 関数が変換したオブジェクトを戻すために `WriteGetObjectResponse` を呼び出すときに S3 Object Lambda URL に追加されるルーティングトークン。
- `outputToken` – 変換されたオブジェクトを送り返すときに、`WriteGetObjectResponse` 呼び出しを元の呼び出し元と照合するために S3 Object Lambda によって使用されるトークンです。

イベントコンテキスト内のすべてのフィールドの詳細については、「イベントコンテキストの形式と使用法 および S3 Object Lambda アクセスポイントの Lambda 関数の記述」を参照してください。

3. ローカルターミナルで次のコマンドを入力し、`virtualenv` パッケージをインストールします。

```
python -m pip install virtualenv
```

4. ローカルターミナルで、前に作成した `object-lambda` フォルダを開き、次のコマンドを入力して、`venv` という名前の仮想環境を作成し、初期化します。

```
python -m virtualenv venv
```

5. 仮想環境をアクティブ化するには、次のコマンドを入力して環境のフォルダから `activate` ファイルを実行します。

macOS ユーザーの場合は、このコマンドを実行します。

```
source venv/bin/activate
```

Windows ユーザーの場合は、このコマンドを実行します。

```
.\venv\Scripts\activate
```

ここで、コマンドプロンプトが変わり、仮想環境がアクティブであることを示す (venv) が表示されます。

6. 必要なライブラリをインストールするには、venv 仮想環境で、以下のコマンドを行単位で実行します。

   これらのコマンドは、lambda_handler Lambda 関数の依存関係の更新バージョンをインストールします。これらの依存関係は、AWS SDK for Python (Boto3) とリクエストモジュールです。

   ```
   pip3 install boto3
   ```

   ```
   pip3 install requests
   ```

7. 仮想環境を無効にするには、次のコマンドを実行します。

   ```
   deactivate
   ```

8. インストール済みライブラリを含むデプロイパッケージを object-lambda ディレクトリのルートにある lambda.zip という名前の .zip ファイルで作成し、以下のコマンドをローカルターミナルで行単位で実行します。

   > **Tip**
   >
   > 以下のコマンドは、特定の環境で動作するように調整する必要がある場合があります。例えば、ライブラリは site-packages または dist-packages であり、最初のフォルダはlib または lib64 です。また、python フォルダには、別の Python バージョンで名前が付けられている可能性があります。特定のパッケージを見つけるには、pip show コマンドを使用します。

   macOS ユーザーの場合は、このコマンドを実行します。

   ```
   cd venv/lib/python3.8/site-packages
   ```

```
zip -r ../../../../lambda.zip .
```

Windows ユーザーの場合は、このコマンドを実行します。

```
cd .\venv\Lib\site-packages\
```

```
powershell Compress-Archive * ../../../lambda.zip
```

最後のコマンドは、デプロイメントパッケージを object-lambda ディレクトリのルートに保存します。

9. デプロイパッケージのルートに関数コードファイル transform.py を追加します。

macOS ユーザーの場合は、このコマンドを実行します。

```
cd ../../../../
```

```
zip -g lambda.zip transform.py
```

Windows ユーザーの場合は、このコマンドを実行します。

```
cd ..\..\..\
```

```
powershell Compress-Archive -update transform.py lambda.zip
```

このステップを完了すると、以下のようなディレクトリ構造になります。

```
lambda.zip$
  # transform.py
  # __pycache__
  | boto3/
  # certifi/
  # pip/
  # requests/
  ...
```

実行ロールを使用した Lambda 関数の作成 (コンソール)

1. AWS Management Console にサインインして AWS Lambda コンソール (https://console.aws.amazon.com/lambda/) を開きます。
2. 左側のナビゲーションペインで、[関数] を選択します。
3. 関数の作成 を選択します。
4. Author from scratch を選択します。
5. 基本的な情報 で、以下の作業を行います。
   a. [関数名] に「**tutorial-object-lambda-function**」と入力します。
   b. [ランタイム] で、Python 3.8 またはそれ以降のバージョンを選択します。
6. [デフォルト実行ロールの変更] セクションを展開します。[実行ロール] で、[基本的な Lambda 許可で新しいロールを作成] を選択します。

   このチュートリアルのステップ 5 で、AmazonS3ObjectLambdaExecutionRolePolicy をこの Lambda 関数の実行ロールにアタッチします。
7. 残りの設定はデフォルト値のままにしておきます。
8. [関数の作成] を選択してください。

.zip ファイルアーカイブを使用して Lambda 関数コードをデプロイし、Lambda 関数を設定 (コンソール)

1. AWS Lambda コンソール (https://console.aws.amazon.com/lambda/) で、左のナビゲーションペインの関数を選択します。
2. 前に作成した Lambda 関数を選択します (例、**tutorial-object-lambda-function**)。
3. Lambda 関数の詳細ページで、[コード] を選択します。[コードソース] セクションで、[からアップロード]、[.zip ファイル] の順に選択します。
4. [アップロード] を選択して、ローカルの `.zip` ファイルを選択します。
5. 前に作成した `lambda.zip` ファイルを選択し、[開く] を選択します。
6. [保存] を選択します。
7. [ランタイム設定] セクションで、[編集] を選択します。
8. [ランタイム設定の編集] ページで、ランタイムが Python 3.8 またはそれ以降のバージョンに設定されていることを確認します。

9. Lambda ランタイムに Lambda 関数コード内のどのハンドラメソッドを呼び出すかを指示するには、[ハンドラー] に **`transform.lambda_handler`** を入力します。

   Python で関数を設定するとき、ハンドラー設定の値は、ファイル名と、ハンドラーモジュールの名前を、ドットで区切ったものになります。例えば、`transform.lambda_handler` は、`transform.py` ファイルで定義された `lambda_handler` メソッドを呼び出します。

10. [保存] を選択します。

11. (オプション) Lambda 関数の詳細ページで、[設定] タブを選択します。左のナビゲーションペインで、[一般的な設定] を選択してから、[編集] を選択します。[タイムアウト] フィールドに、**`1`** 分 **`0`** 秒と入力します。残りの設定はデフォルト値のままにして、[保存] を選択します。

    タイムアウトは、Lambda で関数が停止するまでに許可される実行時間の長さです。デフォルト値は 3 秒です。S3 Object Lambda によって使用される Lambda 関数の最大持続時間は 60 秒です。料金は、設定されたメモリの量とコードの実行時間に基づいて請求されます。

ステップ 5: Lambda 関数の実行ロールの IAM ポリシーを設定する

Lambda 関数がカスタマイズされたデータと応答ヘッダーを `GetObject` 呼び出し元に提供できるようにするには、Lambda 関数の実行ロールに `WriteGetObjectResponse` API を呼び出すための IAM 許可が必要です。

IAM ポリシーを Lambda 関数ロールにアタッチするには

1. AWS Lambda コンソール (https://console.aws.amazon.com/lambda/) で、左のナビゲーションペインの関数を選択します。
2. ステップ 4 で作成した関数 (たとえば、**`tutorial-object-lambda-function`**) を選択します。
3. Lambda 関数の詳細ページで、[設定] タブを選択してから、左のナビゲーションペインの [許可] を選択します。
4. [実行ロール] で、[ロール名] のリンクを選択します。IAM コンソールが開きます。
5. Lambda 関数の実行ロールの IAM コンソールの [Summary] (概要) ページで、[Permissions] (許可) タブを選択します。[Add Permissions] (許可を追加) メニューから [Attach policies] (ポリシーを添付) を選択します。
6. [許可のアタッチ] ページで、[検索] ボックスに **`AmazonS3ObjectLambdaExecutionRolePolicy`** を入力して、ポリシーのリストをフィルタ

リングします。AmazonS3ObjectLambdaExecutionRolePolicy ポリシーの名前の横にあるチェックボックスを選択します。

7. [ポリシーのアタッチ] を選択します。

ステップ 6: Object Lambda アクセスポイントの作成

S3 Object Lambda アクセスポイントは、S3 GET リクエストから Lambda 関数を直接呼び出す柔軟性を提供し、関数が S3 アクセスポイントから取得したデータを処理できるようにします。S3 Object Lambda アクセスポイントを作成および設定するときは、Lambda が使用するカスタムパラメータとして JSON 形式のイベントコンテキストを呼び出し、提供する Lambda 関数を指定する必要があります。

S3 Object Lambda アクセスポイントを作成するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[Object Lambda アクセスポイント] を選択します。
3. [Object Lambda アクセスポイント] ページで、[Object Lambda アクセスポイントの作成] を選択します。
4. Object Lambda アクセスポイント名] に、Object Lambda アクセスポイントに使用する名前を入力します (例、**`tutorial-object-lambda-accesspoint`**)。
5. [サポートするアクセスポイント] で、ステップ 3 で作成した標準アクセスポイントを入力または参照します (**`tutorial-access-point`** など)。次に、[サポートするアクセスポイントの選択] を選択します。
6. S3 API の場合、Lambda 関数が処理する S3 バケットからオブジェクトを取得するには、[GetObject] を選択します。
7. [Lambda 関数の呼び出し] では、このチュートリアルでは、次の 2 つのオプションのいずれかを選択できます。
   - [アカウントの関数から選ぶ] を選択し、[Lambda 関数] ドロップダウンリストから、ステップ 4 で作成した Lambda 関数を選択します (例、**`tutorial-object-lambda-function`**)。
   - [ARN を入力] を選択し、ステップ 4 で作成した Lambda 関数の Amazon リソースネーム (ARN) を入力します。
8. [Lambda 関数のバージョン] で、$LATEST (ステップ 4 で作成した Lambda 関数の最新バージョン) を選択します。

9. (オプション) Lambda 関数で、範囲とパート番号によって GET リクエストを認識および処理する必要がある場合は、[Lambda 関数は、範囲を使用してリクエストをサポート] および [Lambda 関数は、パート番号を使用してリクエストをサポート] を選択します。それ以外の場合は、これらの 2 つのチェックボックスをオフにします。

   S3 Object Lambda で範囲またはパート番号を使用する方法の詳細については、「Range および partNumber ヘッダーの操作」を参照してください。

10. (オプション) [ペイロード - オプション] で JSON テキストを追加して、Lambda 関数に追加情報を提供します。

    ペイロードは、特定の S3 Object Lambda アクセスポイントからのすべての呼び出しに対する入力として、Lambda 関数に提供できるオプションの JSON テキストです。同じ Lambda 関数を呼び出す複数の Object Lambda アクセスポイントの動作をカスタマイズして、異なるパラメータを使用してペイロードを設定できます。これにより、Lambda 関数の柔軟性が向上します。

    ペイロードの詳細については、「イベントコンテキストの形式と使用法」を参照してください。

11. (オプション) [リクエストメトリクス - オプション] で、[無効] または [有効] を選択して、Amazon S3 モニタリングを Object Lambda アクセスポイントに追加します。リクエストメトリクスには、Amazon CloudWatch の標準料金が課金されます。詳細については、「CloudWatch 料金表」を参照してください。

12. [Object Lambda アクセスポイントポリシー-オプション] で、デフォルトの設定を保持します。

    (オプション) リソースポリシーを設定できます。このリソースポリシーは、指定された Object Lambda アクセスポイントを使用する `GetObject` API 許可を付与します。

13. 残りの設定はデフォルト値のままにしておき、[Object Lambda アクセスポイントの作成] を選択します。

ステップ 7: 変換されたデータを表示する

これで、S3 Object Lambda は、ユースケースに合わせてデータを変換する準備が整いました。このチュートリアルでは、S3 Object Lambda はオブジェクト内のすべてのテキストを大文字に変換します。

サブステップ

- S3 Object Lambda アクセスポイントの変換済みデータの表示
- Python スクリプトを実行して、元のデータと変換されたデータを出力する

S3 Object Lambda アクセスポイントの変換済みデータの表示

S3 Object Lambda アクセスポイントを使用してファイルの取得をリクエストすると、S3 Object Lambda への `GetObject` API 呼び出しが行われます。S3 Object Lambda は Lambda 関数を呼び出してデータを変換し、変換されたデータを標準 S3 `GetObject` API への応答として返します。

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[Object Lambda アクセスポイント] を選択します。
3. [Object Lambda アクセスポイント] ページで、ステップ 6 で作成した S3 Object Lambda アクセスポイントを選択します (例、**`tutorial-object-lambda-accesspoint`**)。
4. S3 Object Lambda アクセスポイントの [オブジェクト] タブで、ステップ 2 で S3 バケットにアップロードしたファイルと同じ名前のファイルを選択します(例、`tutorial.txt`)。

   このファイルには、変換されたすべてのデータが含まれているはずです。
5. 変換されたデータを表示するには、[開く] または [ダウンロード] を選択します。

Python スクリプトを実行して、元のデータと変換されたデータを出力する

S3 Object Lambda は、既存のアプリケーションで使用できます。これを行うには、アプリケーション設定を更新して、ステップ 6 で、S3 からのデータを作成した新しい S3 Object Lambda アクセスポイント ARN を使用してデータを取得します。

次の Python スクリプトの例では、S3 バケットからの元のデータと S3 Object Lambda アクセスポイントからの変換されたデータの両方を出力します。

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[Object Lambda アクセスポイント] を選択します。
3. [Object Lambda アクセスポイント] ページで、ステップ 6 で作成した S3 Object Lambda アクセスポイントの左にあるラジオボタンを選択します (例、**`tutorial-object-lambda-accesspoint`**)。
4. [ARN のコピー] を選択します。
5. 後で使用するために ARN を保存します。
6. ローカルマシンで Python スクリプトを記述して、S3 バケットからの元のデータ (例えば、`tutorial.txt`) と S3 Object Lambda アクセスポイントからの変換されたデータ (例えば、`tutorial.txt`) の両方を出力します。次のサンプルスクリプトを使用できます。

```
import boto3
from botocore.config import Config

s3 = boto3.client('s3', config=Config(signature_version='s3v4'))

def getObject(bucket, key):
    objectBody = s3.get_object(Bucket = bucket, Key = key)
    print(objectBody["Body"].read().decode("utf-8"))
    print("\n")

print('Original object from the S3 bucket:')
# Replace the two input parameters of getObject() below with
# the S3 bucket name that you created in Step 1 and
# the name of the file that you uploaded to the S3 bucket in Step 2
getObject("tutorial-bucket",
          "tutorial.txt")

print('Object transformed by S3 Object Lambda:')
# Replace the two input parameters of getObject() below with
# the ARN of your S3 Object Lambda Access Point that you saved earlier and
# the name of the file with the transformed data (which in this case is
# the same as the name of the file that you uploaded to the S3 bucket
# in Step 2)
getObject("arn:aws:s3-object-lambda:us-west-2:111122223333:accesspoint/tutorial-
object-lambda-accesspoint",
          "tutorial.txt")
```

7. Python スクリプトにカスタム名 (tutorial_print.py など) を付けて、ステップ 4 でローカルマシンに作成したフォルダ (object-lambda など) に保存します。
8. ローカルターミナルで、ステップ 4 で作成したディレクトリ (例えば、object-lambda) のルートから次のコマンドを実行します。

```
python3 tutorial_print.py
```

元のデータと変換されたデータ(すべて大文字)の両方がターミナルに表示されます。例えば、次のようなテキストが表示されます。

```
Original object from the S3 bucket:
Amazon S3 Object Lambda Tutorial:
You can add your own code to process data retrieved from S3 before
returning it to an application.
```

```
Object transformed by S3 Object Lambda:
AMAZON S3 OBJECT LAMBDA TUTORIAL:
YOU CAN ADD YOUR OWN CODE TO PROCESS DATA RETRIEVED FROM S3 BEFORE
RETURNING IT TO AN APPLICATION.
```

ステップ 8: クリーンアップする

学習のためだけに S3 Object Lambda によってデータを変換した場合は、割り当てた AWS リソースを削除して、料金が発生しないようにします。

サブステップ

- Object Lambda アクセスポイントの削除
- S3 アクセスポイントを削除する
- Lambda 関数の実行ロールを削除する
- Lambda 関数を削除する
- CloudWatch Logs グループを削除する
- S3 ソースバケットの元のファイルを削除する
- S3 ソースバケットを削除する
- IAM ユーザーを削除する

Object Lambda アクセスポイントの削除

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[Object Lambda アクセスポイント] を選択します。
3. [Object Lambda アクセスポイント] ページで、ステップ 6 で作成した S3 Object Lambda アクセスポイントの左にあるラジオボタンを選択します (例、**`tutorial-object-lambda-accesspoint`**)。
4. [削除] を選択します。
5. 表示されるテキストフィールドにアクセスポイントの名前を入力して、[削除] を選択し、bject Lambda アクセスポイントを削除することを確認します。

S3 アクセスポイントを削除する

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[アクセスポイント] を選択します。
3. ステップ 3 で作成したアクセスポイントに移動し (例、**tutorial-access-point**)、アクセスポイントの名前の横にあるラジオボタンを選択します。
4. [削除] を選択します。
5. 表示されるテキストフィールドにアクセスポイントの名前を入力して、アクセスポイントを削除することを確認し、[削除] を選択します。

Lambda 関数の実行ロールを削除する

1. AWS Management Console にサインインして AWS Lambda コンソール (https://console.aws.amazon.com/lambda/) を開きます。
2. 左側のナビゲーションペインで、[関数] を選択します。
3. ステップ 4 で作成した関数 (例、**tutorial-object-lambda-function**) を選択します。
4. Lambda 関数の詳細ページで、[設定] タブを選択してから、左のナビゲーションペインの [許可] を選択します。
5. [実行ロール] で、[ロール名] のリンクを選択します。IAM コンソールが開きます。
6. Lambda 関数の実行ロールの IAM コンソールの [概要] ページで、[ロールの削除] を選択します。
7. ロールの削除ダイアログボックスで、[はい、削除します] をクリックします。

Lambda 関数を削除する

1. AWS Lambda コンソール (https://console.aws.amazon.com/lambda/) で、左のナビゲーションペインの関数を選択します。
2. ステップ 4 で作成した関数名の左にあるチェックボックスを選択します (例、**tutorial-object-lambda-function**)。
3. [アクション] を選択し、[削除] を選択します。
4. [関数の削除] ダイアログボックスで、[削除] を選択します。

CloudWatch Logs グループを削除する

1. CloudWatch コンソールの https://console.aws.amazon.com/cloudwatch/ を開いてください。
2. 左側のナビゲーションペインで、[ロググループ] をクリックします。
3. ステップ 4 で作成した Lambda 関数で終わる名前のロググループを検索します (例、**tutorial-object-lambda-function**)。
4. ロググループの名前の左にあるチェックボックスを選択します。
5. [アクション] を選択してから、[ロググループの削除] を選択します。
6. [ロググループの削除] ダイアログボックスで、[削除] をクリックします。

S3 ソースバケットの元のファイルを削除する

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。
3. バケット名] リストで、ステップ 2 で元のファイルをアップロードしたバケットの名前を選択します(例、**tutorial-bucket**)。
4. 削除するオブジェクトの名前の左にあるチェックボックスを選択します (例、`tutorial.txt`)。
5. [削除] を選択します。
6. [オブジェクトの削除] ページの [オブジェクトを完全に削除しますか?] セクションで、テキストボックスに「**permanently delete**」と入力して、このオブジェクトを削除することを確認します。
7. [オブジェクトの削除] を選択します。

S3 ソースバケットを削除する

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。
3. [バケット] リストで、ステップ 1 で作成したバケットの名前の横にあるラジオボタンを選択します (例、**tutorial-bucket**)。
4. [削除] を選択します。

5. [バケットを削除する] ページで、テキストフィールドにバケット名を入力することでバケットを削除することを確認し、[バケットを削除する] を選択します。

IAM ユーザーを削除する

1. AWS Management Console にサインインして、IAM コンソール https://console.aws.amazon.com/iam/ を開きます。
2. 左のナビゲーションペインで、[ユーザー] を選択し、削除するユーザー名の横にあるチェックボックスを選択します。
3. ページの上部で、[削除] を選択します。
4. [*****を削除しますか?] ダイアログボックスで、テキスト入力フィールドにユーザー名を入力し、ユーザーの削除を確認します。[削除] を選択します。

次のステップ

このチュートリアルを完了すると、ユースケースの Lambda 関数をカスタマイズし、標準 S3 GET リクエストによって返されるデータを変更できます。

S3 Object Lambda の一般的なユースケースを以下に示します。

- セキュリティとコンプライアンスのために機密データをマスキングします。

  詳細については、「チュートリアル: S3 Object Lambda と Amazon Comprehend を使用した PII データの検出と編集」を参照してください。
- 特定の情報を配信するために、特定のデータ行をフィルタリングします。
- 他のサービスやデータベースからの情報でデータ強化します。
- アプリケーション互換性のために XML から JSON への変換など、データ形式間の変換を行います。
- ダウンロード中のファイルを圧縮または解凍します。
- 画像のサイズ変更とウォーターマークを行います。

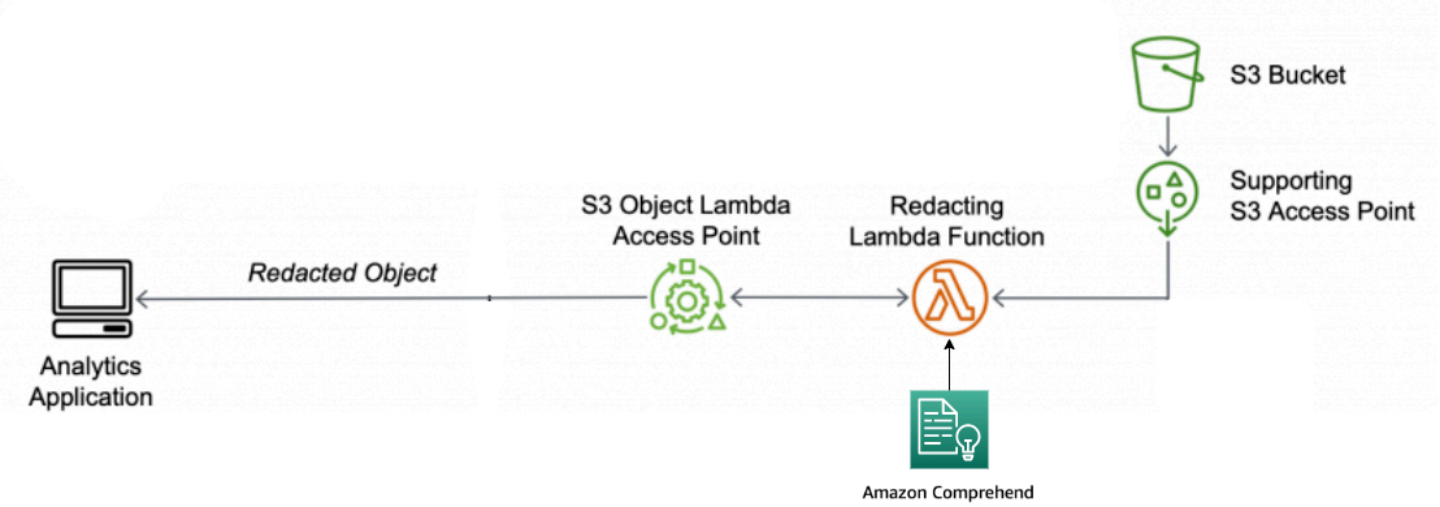
  詳細については、「チュートリアル: S3 Object Lambda を使用して、取得時に画像に動的に透かしを入れる」を参照してください。
- データにアクセスするためのカスタム承認規則を実装します。

S3 Object Lambda, の詳細については、「S3 Object Lambda を使用したオブジェクトの変換」を参照してください。

チュートリアル: S3 Object Lambda と Amazon Comprehend を使用した PII データの検出と編集

複数のアプリケーションおよびユーザーがアクセスするための共有データセットに Amazon S3 を使用する場合、個人を特定できる情報 (PII) などの特権情報を許可されたエンティティのみに制限することが重要です。例えば、マーケティングアプリケーションが PII を含むデータを使用する場合、データのプライバシー要件を満たすために、まず PII データをマスクする必要があります。また、分析アプリケーションで製造オーダーのインベントリデータセットを使用する場合、意図しないデータ漏洩を防ぐために、まず顧客のクレジットカード情報を編集する必要があります。

S3 Object Lambda と Amazon Comprehend により事前に構築された AWS Lambda 関数を使用すると、S3 から取得した PII データを、アプリケーションに返す前に保護できます。具体的な内容は以下のとおりです。組み込みの Lambda 関数を編集関数として作使用し、S3 Object Lambda アクセスポイントにアタッチします。アプリケーション (Analytics アプリケーションなど) が標準 S3 GET リクエストを送信する場合、S3 Object Lambda アクセスポイントを介して行われたこれらのリクエストは、事前作成された編集用 Lambda 関数を呼び出し、サポートしている S3 アクセスポイントを介して S3 バケットから取得した PII データを検出して修正します。次に、S3 Object Lambda アクセスポイントは、編集された結果をアプリケーションに返します。



プロセスでは、事前に構築された Lambda 関数は Amazon Comprehend (自然言語処理 (NLP) サービス) を使用して、PII がテキストにどのように存在するかに関係なく (数値、または単語と数字の組み合わせなど)、PII の表現方法のバリエーションをキャプチャします。Amazon Comprehend は、テキスト内のコンテキストを使用して、4 桁の数字が PIN、社会保障番号 (SSN) の最後の 4 桁の数字であるか、または年であるかを理解することもできます。Amazon Comprehend は UTF-8 形

式のテキストファイルを処理し、精度に影響を与えずに PII を大規模に保護します。詳細については、Amazon Comprehend デベロッパーガイドの「Amazon Comprehend とは?」を参照してください。

目的

このチュートリアルでは、事前に構築された Lambda 関数 `ComprehendPiiRedactionS3ObjectLambda` で S3 Object Lambda を使用する方法を学習します。この関数は、Amazon Comprehend を使用して PII エンティティを検出します。次に、これらのエンティティをアスタリスクに置き換えて墨消しします。PII を編集することで、機密データを隠すことができ、セキュリティとコンプライアンスに役立ちます。

また、AWS Serverless Application Repository で事前作成された AWS Lambda 関数を操作して、S3 Object Lambda と連携してデプロイメントを容易にする方法も学びます。

トピック

- 前提条件: 許可を持つ IAM ユーザーを作成する
- ステップ 1: S3 バケットを作成する。
- ステップ 2: S3 バケットにファイルをアップロード
- ステップ 3: S3 アクセスポイントの作成
- ステップ 4: 事前構築された Lambda 関数の設定とデプロイ
- ステップ 5: S3 Object Lambda アクセスポイントの作成
- ステップ 6: S3 Object Lambda アクセスポイントを使用して、編集されたファイルを取得する
- ステップ 7: クリーンアップする
- 次のステップ

前提条件: 許可を持つ IAM ユーザーを作成する

このチュートリアルを開始する前に、正しいアクセス許可を持つ AWS Identity and Access Management ユーザー (IAM ユーザー) としてサインインできる AWS アカウントが必要です。

チュートリアル用の IAM ユーザーを作成できます。このチュートリアルを完了するには、IAM ユーザーが次の IAM ポリシーをアタッチして、関連する AWS リソースにアクセスし、特定のアクションを実行する必要があります。

> **Note**
>
> このチュートリアルでは、わかりやすいように IAM ユーザーを作成して使用します。このチュートリアルを完了したら、忘れずに「IAM ユーザーを削除する」を行います。本番環境で使用する場合は、IAM ユーザーガイドの「IAM でのセキュリティのベストプラクティス」に従うことをお勧めします。ベストプラクティスでは、人間のユーザーと ID プロバイダーとのフェデレーションにより、一時的な認証情報を使用して AWS にアクセスする必要があります。追加のベストプラクティスとして、ワークロードでは一時的な認証情報で IAM ロールを使用し、AWS にアクセス必要があります。AWS IAM Identity Center を使用して一時的な認証情報を持つユーザーを作成する方法については、「AWS IAM Identity Center ユーザーガイド」の「開始方法」を参照してください。
> このチュートリアルでは、フルアクセスポリシーも使用します。実稼働環境では、代わりに、セキュリティのベストプラクティスに従って、ユースケースに必要な最小限の許可のみを付与することをお勧めします。

IAM ユーザーには次のものが必要です。AWS マネージドポリシー:

- AmazonS3FullAccess – Object Lambda アクセスポイントを作成および使用するための許可を含む、すべての Amazon S3 アクションに対する許可を付与します。
- AWSLambda_FullAccess – すべての Lambda アクションに許可を付与します。
- AWSCloudFormationFullAccess – すべてのAWS CloudFormationのアクションに許可を付与します。
- IAMFullAccess – すべての IAM アクションに許可を付与します。
- IAMAccessAnalyzerReadOnlyAccess – IAM Access Analyzer によって提供されるすべてのアクセス情報を読み取る許可を付与します。

IAM ユーザーを作成するときに、これらの既存のポリシーを直接アタッチできます。IAM ユーザーを作成する方法の詳細については、「IAM ユーザーガイド」の「IAM ユーザーの作成 (コンソール)」を参照してください。

さらに、IAM ユーザーにはカスタマーマネージドポリシーが必要です。IAM ユーザーにすべての AWS Serverless Application Repository リソースとアクションへの許可を付与するには、IAM ポリシーを作成し、ポリシーを IAM ユーザーにアタッチする必要があります。

IAM ポリシーを作成して IAM ユーザーにアタッチするには

1. AWS Management Console にサインインして、IAM コンソール https://console.aws.amazon.com/iam/ を開きます。
2. 左のナビゲーションペインの [ポリシー] を選択します。
3. [Create policy (ポリシーの作成)] を選択します。
4. Service の [Visual editor] タブで、[サービスの選択] を選択します。次に、[Serverless Application Repository] を選択します。
5. [アクション] の [手動アクション] の下で、このチュートリアルでは、[すべての Serverless Application Repository アクション (serverlessrepo:*)] を選択します。

   セキュリティのベストプラクティスとは、ユーザーが必要とするアクションとリソースに対する許可を、ユースケースに基づいて付与することです。詳細については、IAM ユーザーガイドの「IAM でのセキュリティベストプラクティス」を参照してください。
6. [リソース] で、このチュートリアルでは、[すべてのリソース] を選択します。

   ベストプラクティスは、特定のアカウントの特定のリソースに対してのみ許可を定義することです。または、条件キーを使用して、最小の特権を付与することもできます。詳細については、IAM ユーザーガイドの「最小限の特権を付与」を参照してください。
7. [Next: Tags (次へ: タグ)] を選択します。
8. [次へ: レビュー] を選択します。
9. [ポリシーの確認] ページで、作成するポリシーの [名前] (例、**`tutorial-serverless-application-repository`**) と [説明] (オプション) を入力します。ポリシー概要を確認して、目的のアクセス許可を付与していることを確認し、[Create policy] (ポリシーの作成) を選択して新しいポリシーを保存します。
10. 左のナビゲーションペインで、[ユーザー] を選択します。次に、このチュートリアルの IAM ユーザーを選択します。
11. 選択したユーザーの [概要] ページで、[許可] タブを選択してから、[許可を追加] を選択します。
12. [権限の付与] で、[既存のポリシーを直接アタッチします] を選択します。
13. 今、作成したポリシーの横にあるチェックボックスを選択し (例、**`tutorial-serverless-application-repository`**)、次に [次へ: レビュー] を選択します。
14. [許可概要] で、概要を確認し、意図したポリシーを付与したことを確認します。次に、[許可を追加] を選択します。

ステップ 1: S3 バケットを作成する。

変換する元のデータを保存するバケットを作成します。

バケットを作成するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。
3. [Create bucket (バケットの作成)] を選択します。

   [バケットの作成] ページが開きます。
4. [バケット名] に、バケットの名前 (例、**tutorial-bucket**) を入力します。

   Amazon S3 のバケット命名規則の詳細については、「汎用バケットの命名規則」を参照してください。
5. [リージョン] で、バケットを保存する AWS リージョン を選択します。

   バケットのリージョンの詳細については、「汎用バケットの概要」を参照してください。
6. [このバケットのパブリックアクセス設定をブロック] で、デフォルト設定 (ブロックすべてパブリックアクセスが有効) のままであることを確認します。

   ユースケースでオフにする必要のある設定が 1 つ以上あることがわかっている場合を除き、すべてのブロックパブリックアクセス設定を有効にしておくことをお勧めします。パブリックアクセスのブロックの詳細については、Amazon S3 ストレージへのパブリックアクセスのブロックを参照してください。
7. 残りの設定はデフォルトのままにしておきます。

   (オプション) 特定のユースケースに追加のバケット設定を設定する場合は、「汎用バケットの作成」を参照してください。
8. [バケットを作成] を選択します。

ステップ 2: S3 バケットにファイルをアップロード

名前、銀行情報、電話番号、SSN など、さまざまなタイプの既知の PII データを含むテキストファイルを S3 バケットにアップロードします。このテキストファイルは、このチュートリアルの後半で PII を編集します。

例えば、次の tutorial.txt ファイルをアップロードできます。これは、Amazon Comprehend からの入力ファイルの例です。

```
Hello Zhang Wei, I am John. Your AnyCompany Financial Services,
LLC credit card account 1111-0000-1111-0008 has a minimum payment
of $24.53 that is due by July 31st. Based on your autopay settings,
we will withdraw your payment on the due date from your
bank account number XXXXXX1111 with the routing number XXXXX0000.

Your latest statement was mailed to 100 Main Street, Any City,
WA 98121.
After your payment is received, you will receive a confirmation
text message at 206-555-0100.
If you have questions about your bill, AnyCompany Customer Service
is available by phone at 206-555-0199 or
email at support@anycompany.com.
```

バケットにファイルをアップロードするには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。
3. [バケット] リストで、ステップ 1 で作成したバケットの名前を選択し (**tutorial-bucket** など)、ファイルをアップロードします。
4. バケットの [オブジェクト] タブで、[アップロード] を選択します。
5. [アップロード] ページの [ファイルとフォルダ] の下で、[ファイルを追加] を選択します。
6. アップロードするファイルを選択し、続いて [オープン] を選択します。例えば、前述した tutorial.txt ファイルの例をアップロードできます。
7. [アップロード] を選択します。

ステップ 3: S3 アクセスポイントの作成

S3 Object Lambda アクセスポイントを使用して元のデータにアクセスし、変換するには、S3 アクセスポイントを作成し、ステップ 1 で作成した S3 バケットに関連付けます。アクセスポイントは、変換するオブジェクトと同じ AWS リージョン に存在する必要があります。

このチュートリアルの後半では、このアクセスポイントを Object Lambda アクセスポイントのサポートアクセスポイントとして使用します。

アクセスポイントを作成するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[アクセスポイント] を選択します。
3. [アクセスポイント] ページで、[アクセスポイントの作成] を選択します。
4. [アクセスポイント名] フィールドに、アクセスポイントの名前を入力します (**tutorial-pii-access-point** など)。

   アクセスポイントの名前付けの詳細については、「汎用バケットの Amazon S3 アクセスポイントの命名規則」を参照してください。
5. [バケット名] フィールドに、ステップ 1 で作成したバケットの名前を入力します(**tutorial-bucket** など)。S3 は、アクセスポイントをこのバケットにアタッチします。

   (オプション) [S3 を参照] を選択して、アカウント内のバケットを参照および検索できます。[S3 を参照] を選択した場合は、目的のバケットを選択し、[パスの選択] を選択して、[バケット名] フィールドにバケットの名前を入力します。
6. [ネットワークオリジン] で、[インターネット] を選択します。

   アクセスポイントのネットワークオリジンの詳細については、「仮想プライベートクラウドに制限された汎用バケットのアクセスポイントの作成」を参照してください。
7. デフォルトでは、アクセスポイントに対してすべてのブロックパブリックアクセス設定が有効になります。パブリックアクセスブロック設定は、すべてを有効にしておくことを推奨します。詳細については、「汎用バケットのアクセスポイントへのパブリックアクセスの管理」を参照してください。
8. その他のすべてのアクセスポイント設定で、デフォルトの設定を保持します。

   (オプション) アクセスポイントの設定は、ユースケースをサポートするように変更できます。このチュートリアルでは、デフォルトの設定を保持することをお勧めします。

   (オプション) アクセスポイントへのアクセスを管理する必要がある場合は、アクセスポイントポリシーを指定できます。詳細については、「汎用バケットのアクセスポイントのポリシー例」を参照してください。
9. [アクセスポイントを作成] を選択します。

ステップ 4: 事前構築された Lambda 関数の設定とデプロイ

PII データを編集するには、事前に構築された AWS Lambda関数 `ComprehendPiiRedactionS3ObjectLambda` を S3 Object Lambda アクセスポイントと共に設定、デプロイします。

Lambda 関数の設定とデプロイ

1. AWS Management Console にサインインし、AWS Serverless Application Repository で `ComprehendPiiRedactionS3ObjectLambda` 関数を表示します。
2. [アプリケーション名] の下の [アプリケーションの設定] では、このチュートリアルのデフォルト値 (`ComprehendPiiRedactionS3ObjectLambda`) を保持します。

   (オプション) このアプリケーションに付ける名前を入力できます。同じ共有データセットに対して異なるアクセスニーズを持つ複数の Lambda 関数を設定する場合は、これを行うことをお勧めします。
3. [MaskCharacter] で、デフォルト値 (*) を保持します。マスク文字は、編集された PII エンティティの各文字を置き換えます。
4. [MaskMode] で、デフォルト値 (MASK) を保持します。MaskMode の値は、PII エンティティを `MASK` 文字または `PII_ENTITY_TYPE` 値に変更することを指定します。
5. 指定したタイプのデータを墨消しするには、[PiiEntityTypes] で、デフォルト値の ALL を保持します。PiiEntityTypes の値は、墨消しの対象となる PII エンティティタイプを指定します。

   サポートされる PII エンティティタイプの一覧の詳細については、Amazon Comprehend デベロッパーガイドの個人を特定できる情報 (PII) の検出を参照してください。
6. 残りの設定はデフォルト値のままにしておきます。

   (オプション) 特定のユースケースに対して追加の設定を構成する場合は、ページの左側の Readme ファイルセクションを参照してください。
7. [I acknowledge that this app creates custom IAM roles (このアプリでカスタム IAM ロールを作成することを認識しています)] チェックボックスをオンにします。
8. [デプロイ] を選択します。
9. 新しいアプリケーションのページの [リソース] で、デプロイする Lambda 関数の [論理 ID] を選択して、Lambda 関数ページで関数を確認します。

ステップ 5: S3 Object Lambda アクセスポイントの作成

S3 Object Lambda アクセスポイントは、S3 GET リクエストから Lambda 関数を直接呼び出す柔軟性を提供し、関数が S3 アクセスポイントから取得した PII データを編集できるようにします。S3 Object Lambda アクセスポイントを作成および設定するときは、変更する Lambda 関数を指定して、Lambda が使用するカスタムパラメータとして JSON 形式のイベントコンテキストを呼び出し、提供する必要があります。

イベントコンテキストは、S3 Object Lambda から Lambda に渡されたイベントで行われたリクエストに関する情報を提供します。イベントコンテキスト内のすべてのフィールドの詳細については、「イベントコンテキストの形式と使用法」を参照してください。

S3 Object Lambda アクセスポイントを作成するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[Object Lambda アクセスポイント] を選択します。
3. [Object Lambda アクセスポイント] ページで、[Object Lambda アクセスポイントの作成] を選択します。
4. Object Lambda アクセスポイント名] に、Object Lambda アクセスポイントに使用する名前を入力します (例、**`tutorial-pii-object-lambda-accesspoint`**)。
5. [サポートするアクセスポイント] で、ステップ 3 で作成した標準アクセスポイントを入力または参照します (**`tutorial-pii-access-point`** など)。次に、[サポートするアクセスポイントの選択] を選択します。
6. S3 API の場合、Lambda 関数が処理する S3 バケットからオブジェクトを取得するには、[GetObject] を選択します。
7. [Lambda 関数の呼び出し] では、このチュートリアルでは、次の 2 つのオプションのいずれかを選択できます。
   - [アカウントの関数から選ぶ] を選択し、[Lambda 関数] ドロップダウンリストから、ステップ 4 でデプロイした Lambda 関数を選択します (例、**`serverlessrepo-ComprehendPiiRedactionS3ObjectLambda`**)。
   - ARN を入力] を選択し、ステップ 4 で作成した Lambda 関数の Amazon リソースネーム (ARN) を入力します。
8. [Lambda 関数のバージョン] で、$LATEST (ステップ 4 でデプロイした Lambda 関数の最新バージョン) を選択します。

9. (オプション) Lambda 関数で、範囲とパート番号によって GET リクエストを認識および処理する必要がある場合は、[Lambda 関数は、範囲を使用してリクエストをサポート] および [Lambda 関数は、パート番号を使用してリクエストをサポート] を選択します。それ以外の場合は、これらの 2 つのチェックボックスをオフにします。

   S3 Object Lambda で範囲またはパート番号を使用する方法の詳細については、「Range および partNumber ヘッダーの操作」を参照してください。

10. (オプション) [ペイロード - オプション] で JSON テキストを追加して、Lambda 関数に追加情報を提供します。

    ペイロードは、特定の S3 Object Lambda アクセスポイントからのすべての呼び出しに対する入力として、Lambda 関数に提供できるオプションの JSON テキストです。同じ Lambda 関数を呼び出す複数の Object Lambda アクセスポイントの動作をカスタマイズして、異なるパラメータを使用してペイロードを設定できます。これにより、Lambda 関数の柔軟性が向上します。

    ペイロードの詳細については、「イベントコンテキストの形式と使用法」を参照してください。

11. (オプション) [リクエストメトリクス - オプション] で、[無効] または [有効] を選択して、Amazon S3 モニタリングを Object Lambda アクセスポイントに追加します。リクエストメトリクスには、Amazon CloudWatch の標準料金が課金されます。詳細については、「CloudWatch 料金表」を参照してください。

12. [Object Lambda アクセスポイントポリシー-オプション] で、デフォルトの設定を保持します。

    (オプション) リソースポリシーを設定できます。このリソースポリシーは、指定された Object Lambda アクセスポイントを使用する `GetObject` API 許可を付与します。

13. 残りの設定はデフォルト値のままにしておき、[Object Lambda アクセスポイントの作成] を選択します。

ステップ 6: S3 Object Lambda アクセスポイントを使用して、編集されたファイルを取得する

これで、S3 Object Lambda は元のファイルから PII データを編集する準備が整いました。

S3 Object Lambda アクセスポイントを使用して、編集されたファイルを取得するには

S3 Object Lambda アクセスポイントを使用してファイルの取得をリクエストすると、S3 Object Lambda への `GetObject` API 呼び出しが行われます。S3 Object Lambda は Lambda 関数を呼び出して PII データを変換し、変換されたデータを標準 S3 `GetObject` API への応答として返します。

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[Object Lambda アクセスポイント] を選択します。
3. [Object Lambda アクセスポイント] ページで、ステップ 5 で作成した S3 Object Lambda アクセスポイントを選択します (例、**tutorial-pii-object-lambda-accesspoint**)。
4. S3 Object Lambda アクセスポイントの [オブジェクト] タブで、ステップ 2 で S3 バケットにアップロードしたファイルと同じ名前のファイルを選択します(例、`tutorial.txt`)。

   このファイルには、変換されたすべてのデータが含まれているはずです。
5. 変換されたデータを表示するには、[開く] または [ダウンロード] を選択します。

   次の例に示すように、編集されたファイルを確認できます。

```
Hello *********. Your AnyCompany Financial Services,
LLC credit card account ****************** has a minimum payment
of $24.53 that is due by *********. Based on your autopay settings,
we will withdraw your payment on the due date from your
bank account ********** with the routing number *********.

Your latest statement was mailed to **********************************.
After your payment is received, you will receive a confirmation
text message at ************.
If you have questions about your bill, AnyCompany Customer Service
is available by phone at ************ or
email at **********************.
```

ステップ 7: クリーンアップする

学習のためだけに S3 Object Lambda によってデータを編集した場合は、割り当てた AWS リソースを削除して、料金が発生しないようにします。

サブステップ

- Object Lambda アクセスポイントの削除
- S3 アクセスポイントを削除する
- Lambda 関数を削除する
- CloudWatch Logs グループを削除する

- S3 ソースバケットの元のファイルを削除する
- S3 ソースバケットを削除する
- Lambda 関数の IAM ロールを削除する
- IAM ユーザーのカスタマーマネージドポリシーを削除する
- IAM ユーザーを削除する

Object Lambda アクセスポイントの削除

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[Object Lambda アクセスポイント] を選択します。
3. [Object Lambda アクセスポイント] ページで、ステップ 5 で作成した S3 Object Lambda アクセスポイントの左にあるオプションブタンを選択します (例、**`tutorial-pii-object-lambda-accesspoint`**)。
4. [削除] を選択します。
5. 表示されるテキストフィールドにアクセスポイントの名前を入力して、[削除] を選択し、bject Lambda アクセスポイントを削除することを確認します。

S3 アクセスポイントを削除する

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[アクセスポイント] を選択します。
3. ステップ 3 で作成したアクセスポイントに移動し (例、**`tutorial-pii-access-point`**)、アクセスポイントの名前の横にあるオプションボタンを選択します。
4. [削除] を選択します。
5. 表示されるテキストフィールドにアクセスポイントの名前を入力して、アクセスポイントを削除することを確認し、[削除] を選択します。

Lambda 関数を削除する

1. AWS Lambda コンソール (https://console.aws.amazon.com/lambda/) で、左のナビゲーションペインの関数を選択します。

2. ステップ 4 で作成した関数 (例、**serverlessrepo-ComprehendPiiRedactionS3ObjectLambda**) を選択します。
3. [アクション] を選択し、[削除] を選択します。
4. [関数の削除] ダイアログボックスで、[削除] を選択します。

CloudWatch Logs グループを削除する

1. CloudWatch コンソールの https://console.aws.amazon.com/cloudwatch/ を開いてください。
2. 左側のナビゲーションペインで、[ロググループ] をクリックします。
3. ステップ 4 で作成した Lambda 関数で終わる名前のロググループを検索します (例、**serverlessrepo-ComprehendPiiRedactionS3ObjectLambda**)。
4. [アクション] を選択してから、[ロググループの削除] を選択します。
5. [ロググループの削除] ダイアログボックスで、[削除] をクリックします。

S3 ソースバケットの元のファイルを削除する

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。
3. バケット名] リストで、ステップ 2 で元のファイルをアップロードしたバケットの名前を選択します(例、**tutorial-bucket**)。
4. 削除するオブジェクトの名前の左にあるチェックボックスを選択します (例、`tutorial.txt`)。
5. [削除] を選択します。
6. [オブジェクトの削除] ページの [オブジェクトを完全に削除しますか?] セクションで、テキストボックスに「**permanently delete**」と入力して、このオブジェクトを削除することを確認します。
7. [オブジェクトの削除] を選択します。

S3 ソースバケットを削除する

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。

3. [バケット] リストで、ステップ 1 で作成したバケットの名前の横にあるラジオボタンを選択します (例、**tutorial-bucket**)。
4. [削除] を選択します。
5. [バケットを削除する] ページで、テキストフィールドにバケット名を入力することでバケットを削除することを確認し、[バケットを削除する] を選択します。

Lambda 関数の IAM ロールを削除する

1. AWS Management Console にサインインして、IAM コンソール https://console.aws.amazon.com/iam/ を開きます。
2. 左のナビゲーションペインで、[ロール] を選択し、削除するロール名の隣にあるチェックボックスを選択します。ロール名は、ステップ 4 でデプロイした Lambda 関数の名前で始まります (例、**serverlessrepo-ComprehendPiiRedactionS3ObjectLambda**)。
3. [削除] を選択します。
4. [削除] ダイアログボックスで、テキスト入力フィールドにロール名を入力し、ユーザーの削除を確認します。その後、[削除] をクリックします。

IAM ユーザーのカスタマーマネージドポリシーを削除する

1. AWS Management Console にサインインして、IAM コンソール https://console.aws.amazon.com/iam/ を開きます。
2. 左のナビゲーションペインの [ポリシー] を選択します。
3. [ポリシー] ページで、[前提条件] で作成したカスタマーマネージドポリシーの名前 (例、**tutorial-serverless-application-repository**) を検索ボックスに入力して、ポリシーのリストをフィルタリングします。削除するアポリシーの名前の横にあるオプションボタンを選択します。
4. [アクション] を選択し、[削除] を選択します。
5. 表示されるテキストフィールドにポリシーの名前を入力して、このポリシーを削除することを確認し、[削除] を選択します。

IAM ユーザーを削除する

1. AWS Management Console にサインインして、IAM コンソール https://console.aws.amazon.com/iam/ を開きます。

2. 左のナビゲーションペインで、[ユーザー] を選択し、削除するユーザー名の横にあるチェックボックスを選択します。
3. ページの上部で、[削除] を選択します。
4. [*****を削除しますか?] ダイアログボックスで、テキスト入力フィールドにユーザー名を入力し、ユーザーの削除を確認します。[削除] を選択します。

次のステップ

このチュートリアルを完了すると、次の関連するユースケースをさらに調べることができます。

- 複数の S3 Object Lambda アクセスポイントを作成し、データアクセサーのビジネスニーズに応じて特定の種類の PII を変更するように構成された事前構築済みの Lambda 関数でそれらを有効にすることができます。

  各タイプのユーザーは IAM ロールを引き受け、1 つの S3 Object Lambda アクセスポイント(IAM ポリシーで管理)にのみアクセスできます。次に、異なる編集ユースケース用に設定されたそれぞれの `ComprehendPiiRedactionS3ObjectLambda` Lambda 関数を異なる S3 Object Lambda アクセスポイントにアタッチします。S3 Object Lambda アクセスポイントごとに、共有データセットを保存する S3 バケットからデータを読み取るためのサポートする S3 アクセスポイントを持つことができます。

  ユーザーが、S3 アクセスポイントを介してのみバケットから読み取ることを許可する、S3 バケットポリシーを作成する方法については、「汎用バケットのアクセスポイントを使用するための IAM ポリシーの設定」を参照してください。

  Lambda 関数、S3 アクセスポイント、および S3 Object Lambda アクセスポイントにアクセスする許可をユーザーに付与する方法の詳細については、「Object Lambda アクセスポイントの IAM ポリシーの設定」を参照してください。
- 独自の Lambda 関数を構築し、カスタマイズした Lambda 関数で S3 Object Lambda を使用し、特定のデータニーズを満たすことができます。

  例えば、さまざまなデータ値を調べるには、S3 Object Lambda と、追加の Amazon Comprehend の機能(エンティティ認識、キーフレーズ認識、センチメント分析、ドキュメントの分類など)を使用して、データを処理できます。また、S3 Object Lambda を Amazon Comprehend Medical (HIPAA 適格な NLP サービス) と共に使用して、コンテキストに応じた方法でデータを分析および抽出できます。

S3 Object Lambda および独自の Lambda 関数を使用してデータを変換する方法の詳細については、「チュートリアル: S3 Object Lambda を使用したアプリケーションのデータの変換」を参照してください。

S3 Object Lambda のデバッグとトラブルシューティング

Amazon S3 Object Lambda アクセスポイントへのリクエストにより、Lambda 関数の呼び出しまたは実行で何か問題が発生したときに、新しいエラーレスポンスが発生することがあります。このようなエラーは、標準の Amazon S3 エラーと同じ形式に従います。S3 Object Lambda エラーについては、Amazon Simple Storage Service API リファレンスの S3 Object Lambda エラーコードリストを参照してください。

一般的な Lambda 関数のデバッグの詳細については、AWS Lambda デベロッパーガイドの「Lambda アプリケーションのモニタリングとトラブルシューティング」を参照してください。

Amazon S3 の標準エラーについては、Amazon Simple Storage Service API リファレンスのエラーレスポンスを参照してください。

Object Lambda アクセスポイントに対して Amazon CloudWatch のリクエストメトリクスを有効にできます。このメトリクスは、アクセスポイントの動作パフォーマンスのモニタリングに役立ちます。リクエストメトリクスは、Object Lambda アクセスポイントの作成中もしくは作成後に有効にできます。詳細については、「CloudWatch の S3 Object Lambda リクエスト」を参照してください。

Object Lambda アクセスポイントに対して行われたリクエストについて、より詳細なログを取得するには、AWS CloudTrail データイベントを有効にできます。詳細については、AWS CloudTrail ユーザーガイドの「証跡へのデータイベントのログ記録」を参照してください。

S3 Object Lambda チュートリアルについては、以下を参照してください。

- チュートリアル: S3 Object Lambda を使用したアプリケーションのデータの変換
- チュートリアル: S3 Object Lambda と Amazon Comprehend を使用した PII データの検出と編集
- チュートリアル: S3 Object Lambda を使用して、取得時に画像に動的に透かしを入れる

標準のアクセスポイントの詳細については、アクセスポイントを使用した汎用バケット内の共有データセットへのアクセスの管理 を参照してください。

バケットの操作方法の詳細については、「汎用バケットの概要」を参照してください。オブジェクトの操作方法の詳細については、Amazon S3 オブジェクトの概要 を参照してください。

バッチオペレーションでオブジェクトオペレーションを一括で実行する

S3 バッチ操作を使用すると、Amazon S3 のオブジェクトに対して大規模なバッチ操作を実行することができます。S3 バッチ操作では、指定した Amazon S3 のオブジェクトのリストに対して、1 つのオペレーションを実行できます。1 つのジョブで、エクサバイトのデータを含む数十億ものオブジェクトに対して、指定されたオペレーションを実行できます。Amazon S3 は、進捗状況の追跡、通知の送信、すべてのアクションの詳細な完了レポートの保存を行い、フルマネージド型の監査可能なサーバーレスエクスペリエンスを提供します。S3 バッチオペレーションは、Amazon S3 コンソール、AWS CLI、AWS SDK、または Amazon S3 REST API を通じて使用できます。

S3 バッチ操作は、オブジェクトをコピーしたり、オブジェクトにタグやアクセスコントロールリスト (ACL) を設定したりするために使用できます。また、S3 Glacier Flexible Retrieval からオブジェクトの復元を行ったり、AWS Lambda 関数を呼び出してオブジェクトを使用してカスタムアクションを実行したりすることもできます。これらのオペレーションは、指定したオブジェクトのカスタムリストに対して実行できます。また、Amazon S3 インベントリレポートを使用して、オブジェクトのリストを簡単に作成することもできます。Amazon S3 バッチオペレーションは、Amazon S3 で既に使用しているのと同じ Amazon S3 API オペレーションを使用します。

> **Note**
>
> Amazon S3 Express One Zone ストレージクラスをディレクトリバケットで使用する方法の詳細については、「S3 Express One Zone」と「ディレクトリバケットの使用」を参照してください。S3 Express One Zone とディレクトリバケットでのバッチオペレーションの使用の詳細については、「ディレクトリバケットでのバッチオペレーションの使用」を参照してください。

S3 バッチ操作の基本

S3 バッチ操作を使用すると、Amazon S3 のオブジェクトに対して大規模なバッチ操作を実行することができます。S3 バッチ操作では、指定した Amazon S3 のオブジェクトのリストに対して、1 つのオペレーションまたはアクションを実行できます。

用語

このセクションでは、次のように定義されるマニフェスト、ジョブ、オペレーション、およびタスクの用語を使用します。

マニフェスト

マニフェストは、Amazon S3 が動作するオブジェクトキーを含む Amazon S3 オブジェクトです。バッチオペレーションジョブを作成する場合は、マニフェストを指定する必要があります。ユーザーが生成したマニフェストには、各オブジェクトのバケット名、オブジェクトキー、およびオプションでオブジェクトバージョンを含める必要があります。ユーザーが作成したマニフェストを提供する場合は、Amazon S3 インベントリレポートまたは CSV ファイルの形式である必要があります。

ジョブの作成時に指定したオブジェクトフィルター条件に基づいてマニフェストを自動的に生成するように Amazon S3 に指示できます。このオプションは、Amazon S3 コンソールで作成した S3 バッチレプリケーションジョブ、または AWS Command Line Interface (AWS CLI)、AWS SDK、または Amazon S3 REST API を使用して作成した任意のジョブタイプで使用できます。

ジョブ

ジョブは、S3 バッチ操作の基本単位です。ジョブには、マニフェストにリストされているオブジェクトに対して指定されたオペレーションを実行するために必要なすべての情報が含まれています。この情報を入力してからジョブの開始をリクエストすると、ジョブはマニフェスト内の各オブジェクトにおいてオペレーションを実行します。

オペレーション

オペレーションは、バッチ操作のジョブで実行する API のアクションの種類 (オブジェクトのコピーなど) です。各ジョブは、マニフェストで指定されているすべてのオブジェクトに対して 1 種類のオペレーションを実行します。

タスク

タスクは、ジョブ実行の単位です。タスクは、1 つのオブジェクトに対してジョブのオペレーションを実行するための Amazon S3 または AWS Lambda API のオペレーションの 1 回の呼び出しを表します。S3 バッチ操作は、ジョブの実行中に、マニフェストで指定されている各オブジェクトに対して 1 つのタスクを作成します。

S3 バッチ操作のジョブの仕組み

ジョブは、S3 バッチ操作の基本単位です。ジョブには、オブジェクトのリストに対して指定されたオペレーションを実行するために必要なすべての情報が含まれています。ジョブを作成するには、S3 バッチ操作にオブジェクトのリストを渡し、それらのオブジェクトに対して実行するアクションを指定します。

S3 バッチ操作がサポートするオペレーションの詳細については、S3 バッチ操作でサポートされるオペレーション を参照してください。

バッチジョブは、そのマニフェストに含まれるすべてのオブジェクトで指定されたオペレーションを実行します。マニフェストには、バッチジョブで処理するオブジェクトが一覧表示され、オブジェクトとしてバケットに保存されます。カンマ区切り値 (CSV) 形式の S3 インベントリを使用したデータのカタログ化と分析 レポートをマニフェストとして使用できます。これにより、バケット内に配置されたオブジェクトの大きなリストを簡単に作成できます。1 つのバケット内に含まれるカスタマイズされたオブジェクトのリストに対してバッチ操作を実行できるように、シンプルな CSV 形式でマニフェストを指定することもできます。

ジョブを作成すると、Amazon S3 はマニフェストにリストされているオブジェクトを処理し、指定されたオペレーションをそれぞれのオブジェクトに対して実行します。ジョブの実行中は、プログラムまたは Amazon S3 コンソールで進捗状況をモニタリングできます。終了時に完了レポートを生成するようにジョブを設定することもできます。完了レポートには、ジョブによって実行された各タスクの結果が示されます。ジョブのモニタリングの詳細については、「S3 バッチ操作ジョブの管理」を参照してください。

S3 バッチオペレーションにはコストがかかります。バッチオペレーションジョブの作成 (完了前にキャンセルしたジョブを含む) に対して課金されます。詳細については、「Amazon S3 の料金」を参照してください。

S3 バッチオペレーションジョブはデフォルトで、すべてのオペレーションで最大 40 億個のオブジェクトを処理できます。具体的には、コピー、オブジェクトのタグ付け、Object Lock、AWS Lambda 関数の呼び出し、バッチレプリケーションジョブは、最大 200 億個のオブジェクトをサポートできます。AWS アカウントごとにアクティブなバッチレプリケーションジョブは 6 つに制限されています。バッチオペレーションジョブの作成を開始するには、「S3 バッチオペレーションジョブの作成」を参照してください。

S3 バッチ操作のチュートリアル

次のチュートリアルでは、いくつかのバッチ操作タスクにおけるエンドツーエンドの一連の手順について説明します。

- チュートリアル: S3 バッチオペレーションを使用した動画のバッチトランスコーディング

バッチオペレーションに対するアクセス許可の付与

S3 バッチ操作ジョブを作成して実行する前に、必要な許可を付与する必要があります。Amazon S3 バッチ操作ジョブを作成するには、`s3:CreateJob` ユーザー許可が必要です。ジョブを作成する同じエンティティには、ジョブに対して指定された AWS Identity and Access Management (IAM) ロールをバッチオペレーションに渡すための `iam:PassRole` 許可も必要です。

IAM リソースの指定に関する一般的な情報については、IAM ユーザーガイドの IAM JSON ポリシー、リソース要素を参照してください。以下のセクションでは、IAM ロールの作成とポリシーのアタッチについて説明します。

トピック

- S3 バッチ操作の IAM ロールの作成
- 許可ポリシーのアタッチ

S3 バッチ操作の IAM ロールの作成

Amazon S3 には、ユーザーに代わって S3 バッチ操作を実行するための許可が必要です。AWS Identity and Access Management (IAM) ロールを介してこれらのアクセス許可を付与します。このセクションでは、IAM ロールを作成するときに使用する信頼ポリシーとアクセス許可ポリシーの例を示します。詳細については、IAM ユーザーガイドの IAM ロールを参照してください。例については、ジョブタグを使用したバッチオペレーションのアクセス許可の制御 および S3 バッチ操作を使用したオブジェクトのコピー を参照してください。

IAM ポリシーでは、条件キーを使用して、S3 バッチ操作ジョブのアクセス許可をフィルタリングすることもできます。Amazon S3 固有の条件キーの詳細な情報と完全なリストについては、「サービス認可リファレンス」の「Actions, resources, and condition keys for Amazon S3」を参照してください。

S3 リソースタイプ別の S3 API オペレーションへのアクセス許可の詳細については、「Amazon S3 API オペレーションに必要なアクセス許可」を参照してください。

信頼ポリシー

S3 バッチ操作のサービスプリンシパルが IAM ロールを引き受けることを許可するには、ロールに次の信頼ポリシーをアタッチします。

```
{
```

```
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"batchoperations.s3.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

許可ポリシーのアタッチ

オペレーションのタイプに応じて、以下のいずれかのポリシーをアタッチできます。

アクセス権限を設定する前に、以下の点にご留意ください。

- オペレーションに関係なく、Amazon S3 には S3 バケットからマニフェストオブジェクトを読み込み、またオプションでバケットにレポートを書き込むアクセス許可が必要です。そのため、次のポリシーにはすべて、これらのアクセス許可が含まれます。
- Amazon S3 インベントリレポートマニフェストの場合、S3 バッチ操作では manifest.json オブジェクトおよび関連するすべての CSV データファイルを読み込むためのアクセス許可が必要です。
- オブジェクトのバージョン ID を指定している場合にのみ、`s3:GetObjectVersion` などのバージョン固有のアクセス許可が必要です。
- 暗号化されたオブジェクトに対して S3 バッチ操作を実行している場合、IAM ロールには、暗号化に使用される AWS KMS キーへのアクセス許可も必要です。
- インベントリレポートマニフェストを AWS KMS で暗号化して送信する場合、IAM ポリシーでは manifest.json オブジェクトおよび関連するすべての CSV データファイルに対するアクセス許可の `"kms:Decrypt"` と `"kms:GenerateDataKey"` が必要です。
- バッチオペレーションジョブにより、アクセスコントロールリスト (ACL) が有効で、別の AWS アカウントのバケットにマニフェストを生成する場合は、そのバッチジョブ用に設定された IAM ロールの IAM ポリシーで `s3:PutObjectAcl` 権限を付与する必要があります。この権限を含めない場合、バッチジョブは `Error occurred when preparing manifest: Failed to write manifest` エラーで失敗します。

オブジェクトのコピー: PutObject

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:PutObject",
                "s3:PutObjectAcl",
                "s3:PutObjectTagging"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectTagging",
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-source-bucket",
                "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
```

```
            ]
        }
    ]
}
```

オブジェクトのタグ付けの置き換え: PutObjectTagging

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObjectTagging",
        "s3:PutObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
      ]
    },
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObject"
      ],
      "Resource":[
        "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
      ]
    }
  ]
}
```

オブジェクトタグの削除: DeleteObjectTagging

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
              "s3:DeleteObjectTagging",
              "s3:DeleteObjectVersionTagging"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
            ]
        }
    ]
}
```

アクセスコントロールリストの置き換え: PutObjectAcl

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObjectAcl",
```

```
        "s3:PutObjectVersionAcl"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
      ]
    },
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObject"
      ],
      "Resource":[
        "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
      ]
    }
  ]
}
```

オブジェクトの復元: RestoreObject

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
          "s3:RestoreObject"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
```

```
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
      ]
    },
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObject"
      ],
      "Resource":[
        "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
      ]
    }
  ]
}
```

Object Lock 保持の適用: PutObjectRetention

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:GetBucketObjectLockConfiguration",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-destination-bucket"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObjectRetention",
                "s3:BypassGovernanceRetention"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
```

```
                "s3:GetObjectVersion"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
            ]
        }
    ]
}
```

Object Lock のリーガルホールド: PutObjectLegalHold

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:GetBucketObjectLockConfiguration",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-destination-bucket"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "s3:PutObjectLegalHold",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
```

```
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
            ]
        }
    ]
}
```

既存のオブジェクトのレプリケート: S3 で生成されたマニフェストによる InitiateReplication

S3 で生成されたマニフェストを使用して保存する場合にはこのポリシーを使用します。バッチオペレーションを使用して既存のオブジェクトをレプリケートする方法の詳細は、「バッチレプリケーションを使用した既存のオブジェクトのレプリケーション」を参照してください。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Action":[
            "s3:InitiateReplication"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
         ]
      },
      {
         "Action":[
            "s3:GetReplicationConfiguration",
            "s3:PutInventoryConfiguration"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket"
         ]
```

```
      },
      {
         "Action":[
            "s3:GetObject",
            "s3:GetObjectVersion"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:PutObject"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*",
            "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
         ]
      }
   ]
}
```

既存のオブジェクトのレプリケート: ユーザーマニフェストによる InitiateReplication

ユーザー指定のマニフェストを使用する場合にはこののポリシーを使用します。バッチオペレーションを使用して既存のオブジェクトをレプリケートする方法の詳細は、「バッチレプリケーションを使用した既存のオブジェクトのレプリケーション」を参照してください。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Action":[
            "s3:InitiateReplication"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
         ]
      },
      {
```

```
            "Action":[
               "s3:GetObject",
               "s3:GetObjectVersion"
            ],
            "Effect":"Allow",
            "Resource":[
               "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
            ]
         },
         {
            "Effect":"Allow",
            "Action":[
               "s3:PutObject"
            ],
            "Resource":[
               "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
            ]
         }
      ]
}
```

S3 バッチオペレーションジョブの作成

Amazon S3 バッチオペレーションを使用すると、特定の Amazon S3 オブジェクトのリストに対して大規模なバッチオペレーションを実行できます。このセクションでは、S3 バッチ操作ジョブの作成に必要な情報と `CreateJob` リクエストの結果について説明します。また、AWS Command Line Interface (AWS CLI)、AWS SDK for Java を使用したバッチオペレーションジョブの作成手順についても説明します。

S3 バッチオペレーションジョブを作成するときに、すべてのタスクまたは失敗したタスクについてのみ完了レポートをリクエストできます。少なくとも 1 つのタスクが正常に呼び出される限り、S3 バッチオペレーションは、完了、失敗、またはキャンセルされたジョブに関するレポートを生成します。詳細については、「例: S3 バッチ操作完了レポート」を参照してください。

トピック

- バッチ操作ジョブのリクエストの要素
- マニフェストの指定

バッチ操作ジョブのリクエストの要素

S3 バッチ操作ジョブを作成するには、次の情報を指定する必要があります。

オペレーション

S3 バッチ操作でマニフェストのオブジェクトに対して実行するオペレーションを指定します。オペレーションのタイプごとに、そのオペレーションに固有のパラメータを受け入れます。バッチオペレーションを使用すると、オペレーションを一括で実行でき、各オブジェクトに対してそのオペレーションを 1 つずつ実行した場合と同じ結果が得られます。

マニフェスト

マニフェストは、S3 バッチオペレーションで指定したアクションを実行するすべてのオブジェクトのリストです。バッチオペレーションジョブのマニフェストは、次の方法で指定できます。

- カスタマイズした CSV 形式の独自のオブジェクトリストを手動で作成します。
- 既存の CSV-形式の S3 インベントリを使用したデータのカタログ化と分析 レポートを選択します。
- 直接バッチオペレーションでは、ジョブの作成時に指定したオブジェクトフィルター条件に基づいてマニフェストを自動的に生成します。このオプションは、Amazon S3 コンソールで作成したバッチレプリケーションジョブ、AWS CLI、AWS SDK、または Amazon S3 REST API を使用して作成した任意のジョブタイプで使用できます。

> **Note**
>
> - マニフェストの指定方法を問わず、リスト自体は汎用バケットに保存する必要があります。バッチオペレーションでは、既存のマニフェストをディレクトリバケットからインポートしたり、生成されたマニフェストをディレクトリバケットに保存したりすることはできません。ただし、マニフェスト内に記述されたオブジェクトはディレクトリバケットに保存できます。詳細については、「ディレクトリバケット」を参照してください。
> - マニフェスト内のオブジェクトがバージョニング対象のバケット内にある場合は、そのオブジェクトのバージョン ID を指定すると特定のバージョンに対してオペレーションが実行されます。バージョン ID が指定されていない場合、バッチオペレーションはオブジェクトの最新バージョンに対してオペレーションを実行します。マニフェストにバージョン ID フィールドが含まれている場合は、マニフェスト内にあるすべてのオブジェクトのバージョン ID を指定する必要があります。

詳細については、「マニフェストの指定」を参照してください。

優先度

ジョブの優先順位を使用して、自分のアカウントで実行中の他のユーザーに対するこのジョブの相対的な優先順位を示します。番号が大きいほど、優先度が高いことを表します。

ジョブの優先度は、同じアカウントとリージョンの他のジョブに設定された優先度に相対して解釈されます。お客様に合った番号付け体系を選択できます。例えば、すべての [復元] (`RestoreObject`) ジョブに優先度 1、すべての [コピー] (`CopyObject`) ジョブに優先度 2、すべての [アクセスコントロールリスト (ACL) に置き換える] (`PutObjectAcl`) ジョブに優先度 3 を割り当てることができます。

S3 バッチオペレーションでは、優先度の数字に従ってジョブに優先順位が付けられます。ただし、厳密に順序付けされるとは限りません。そのため、いずれかのジョブをその他のジョブよりも前に開始または終了させるためにジョブの優先度は使用すべきではありません。厳密な順序付けする必要がある場合は、1 つのジョブが終了するまで待ってから次のジョブを開始します。

RoleArn

ジョブを実行する AWS Identity and Access Management (IAM) ロールを指定します。使用する IAM ロールには、そのジョブで指定されているオペレーションを実行するための十分なアクセス許可が必要です。例えば、`CopyObject` ジョブを実行するには、IAM ロールに、ソースバケットに対する `s3:GetObject` アクセス許可と、送信先バケットに対する `s3:PutObject` アクセス許可が必要です。このロールには、マニフェストを読み取り、ジョブ完了レポートを書き込むためのアクセス許可も必要です。

IAM ロールの詳細については、「IAM ユーザーガイド」の「IAM ロール」を参照してください。

Amazon S3 のアクセス許可の詳細については、「Amazon S3 のポリシーアクション」を参照してください。

> **Note**
>
> ディレクトリバケットに対してアクションを実行するバッチオペレーションジョブには、特定のアクセス許可が必要です。詳細については、S3 Express One Zone 向け AWS Identity and Access Management (IAM)」を参照してください。

レポートを行う

S3 バッチ操作で完了レポートを生成するかどうかを指定します。ジョブ完了レポートをリクエストする場合、この要素にレポートのパラメータも指定する必要があります。必要な情報には以下が含まれます。

- レポートを保存するバケット。

> **Note**
>
> レポートは汎用バケットに保存する必要があります。バッチオペレーションではレポートをディレクトリバケットに保存できません。詳細については、「ディレクトリバケット」を参照してください。

- レポートの形式。
- レポートに、すべてのタスクの詳細を含めるか、失敗したタスクのみを含めるかを指定します。
- オプションのプレフィックス文字列

> **Note**
>
> 完了レポートは、常に Amazon S3 マネージドキー (SSE-S3) によるサーバー側の暗号化で暗号化されます。

[タグ (省略可能)]

タグを追加することで、S3 バッチ操作ジョブへのラベル付けとアクセスの制御を実行できます。タグを使用して、バッチオペレーションジョブの担当者を識別したり、ユーザーがバッチオペレーションジョブを操作する方法を制御したりできます。ジョブタグがあることで、ユーザーによるジョブのキャンセル、確認状態にあるジョブの有効化、ジョブの優先度レベルの変更を許可したり制限したりできます。例えば、ジョブが `"Department=Finance"` タグ付きで作成されている場合、`CreateJob` オペレーションを呼び出すアクセス許可をユーザーに付与できます。

タグをアタッチしてジョブを作成し、後でジョブにタグを追加できます。

詳細については、「the section called “タグの使用”」を参照してください。

Description (オプション)

ジョブを追跡および監視するために、最大 256 文字の説明を指定することもできます。Amazon S3 では、ジョブに関する情報を返すか、Amazon S3 コンソールにジョブの詳細を表示するたびに、この説明が含まれます。これによって、入力した説明に応じて簡単にジョブを並べ替えたりフィルタリングしたりできます。説明は一意である必要はないので、類似したジョブのグループを追跡するのに役立つように、説明をカテゴリとして使用することができます (「Weekly Log Copy Jobs」など)。

マニフェストの指定

マニフェストは、Amazon S3 が動作するオブジェクトキーを含む Amazon S3 オブジェクトです。次のいずれかの方法でマニフェストを提供できます。

- 新しいマニフェストファイルを手動で作成する。
- 既存のマニフェストを使用する。
- 直接バッチオペレーションでは、ジョブの作成時に指定したオブジェクトフィルター条件に基づいてマニフェストを自動的に生成します。このオプションは、Amazon S3 コンソールで作成したバッチレプリケーションジョブ、または AWS CLI、AWS、Amazon S3 REST API を使用して作成した任意のジョブタイプで使用できます。

> **Note**
>
> - Amazon S3 バッチオペレーションは、クロスリージョンマニフェストの生成をサポートしていません。
> - マニフェストの指定方法を問わず、リスト自体は汎用バケットに保存する必要があります。バッチオペレーションでは、既存のマニフェストをディレクトリバケットからインポートしたり、生成されたマニフェストをディレクトリバケットに保存したりすることはできません。ただし、マニフェスト内に記述されたオブジェクトはディレクトリバケットに保存できます。詳細については、「ディレクトリバケット」を参照してください。

マニフェストファイルの作成

ジョブのマニフェストを手動で作成するには、マニフェストオブジェクトキー、ETag (エンティティタグ)、オプションでバージョン ID を CSV 形式のリストで指定します。マニフェストの内容は URL エンコードされている必要があります。

デフォルトでは、Amazon S3 は、Amazon S3 マネージドキー (SSE-S3) を使用したサーバー側暗号化を自動的に使用して、Amazon S3 バケットにアップロードされるマニフェストを暗号化します。顧客指定のキーを使用したサーバー側の暗号化 (SSE-C) を使用するマニフェストはサポートされていません。AWS Key Management Service (AWS KMS) キー (SSE-KMS) でサーバー側の暗号化を使用するマニフェストは、CSV 形式のインベントリレポートを使用する場合にのみサポートされます。AWS KMS を使用したマニフェストの手動作成はサポートされていません。

マニフェストには、各オブジェクトのバケット名、オブジェクトキー、およびオプションでオブジェクトバージョンを含める必要があります。マニフェストのその他のフィールドは、S3 バッチ操作では使用されません。

> **Note**
>
> マニフェスト内のオブジェクトがバージョニング対象のバケット内にある場合は、そのオブジェクトのバージョン ID を指定すると特定のバージョンに対してオペレーションが実行されます。バージョン ID が指定されていない場合、バッチオペレーションはオブジェクトの最新バージョンに対してオペレーションを実行します。マニフェストにバージョン ID フィールドが含まれている場合は、マニフェスト内にあるすべてのオブジェクトのバージョン ID を指定する必要があります。

CSV 形式のマニフェスト (バージョン ID なし) の例を以下に示します。

```
amzn-s3-demo-bucket1,objectkey1
amzn-s3-demo-bucket1,objectkey2
amzn-s3-demo-bucket1,objectkey3
amzn-s3-demo-bucket1,photos/jpgs/objectkey4
amzn-s3-demo-bucket1,photos/jpgs/newjersey/objectkey5
amzn-s3-demo-bucket1,object%20key%20with%20spaces
```

バージョン ID を含む CSV 形式のマニフェストの例は次のとおりです。

```
amzn-s3-demo-bucket1,objectkey1,PZ9ibn9D5lP6p298B7S9_ceqx1n5EJ0p
```

```
amzn-s3-demo-bucket1,objectkey2,YY_ouuAJByNW1LRBfFMfxMge7XQWxMBF
amzn-s3-demo-bucket1,objectkey3,jbo9_jhdPEyB4RrmOxWS0kU0EoNrU_oI
amzn-s3-demo-bucket1,photos/jpgs/objectkey4,6EqlikJJxLTsHsnbZbSRffn24_eh5Ny4
amzn-s3-demo-bucket1,photos/jpgs/newjersey/objectkey5,imHf3FAiRsvBW_EHB8GOu.NHunHO1gVs
amzn-s3-demo-bucket1,object%20key%20with%20spaces,9HkPvDaZY5MVbMhn6TMn1YTb5ArQAo3w
```

既存のマニフェストファイルの指定

次の 2 つの形式のいずれかを使用して、ジョブ作成リクエストのマニフェストファイルを指定できます。

- Amazon S3 インベントリレポート - CSV 形式の Amazon S3 インベントリレポートである必要があります。インベントリレポートに関連付けられた `manifest.json` ファイルを指定する必要があります。インベントリレポートの詳細については、「S3 インベントリを使用したデータのカタログ化と分析」を参照してください。インベントリレポートにバージョン ID が含まれている場合、S3 バッチ操作は特定のオブジェクトのバージョンに対して実行されます。

  > **Note**
  >
  > - S3 バッチオペレーションは、SSE-KMS で暗号化された CSV インベントリレポートをサポートしています。
  > - SSE-KMS で暗号化されたインベントリレポートマニフェストを送信する場合、IAM ポリシーには、`"kms:Decrypt"`、`manifest.json` オブジェクトのための `"kms:GenerateDataKey"`、関連するすべての CSV データ ファイルに対するアクセス許可が含まれている必要があります。

- CSV ファイル – ファイルの各行には、バケット名とオブジェクトのキーを含める必要があります。また、任意でオブジェクトのバージョンを含めることができます。オブジェクトキーは、次の例に示されているように、URL エンコードする必要があります。マニフェストには、すべてのオブジェクトのバージョン ID を含めるか、すべてのオブジェクトのバージョン ID を省略する必要があります。CSV マニフェスト形式の詳細については、「Amazon Simple Storage Service API リファレンス」の「JobManifestSpec」を参照してください。.

  > **Note**
  >
  > S3 バッチオペレーションは、SSE-KMS で暗号化された CSV マニフェストファイルをサポートしていません。

> **Important**
>
> 手動で作成したマニフェストとバージョニング対応のバケットを使用する場合は、そのオブジェクトのバージョン ID を指定することをお勧めします。ジョブを作成すると、S3 バッチ操作はジョブを実行する前にマニフェスト全体を解析します。ただし、これによってバケットの状態は「スナップショット」されません。
> マニフェストには数十億のオブジェクトが含まれる可能性があるため、ジョブの実行に時間がかかる可能性があり、その結果ジョブが動作するオブジェクトのバージョンに影響を与える場合があります。ジョブの実行中にオブジェクトを新しいバージョンで上書きして、そのオブジェクトのバージョン ID を指定しなかったとします。この場合、Amazon S3 は、ジョブの作成時に存在していたバージョンではなく、オブジェクトの最新バージョンに対してオペレーションを実行します。この動作を回避する唯一の方法は、マニフェスト内でリストされたオブジェクトにバージョン ID を指定することです。

マニフェストの自動的生成

ジョブの作成時に指定したオブジェクトフィルター条件に基づいてマニフェストを自動的に生成するように Amazon S3 に指示できます。このオプションは、Amazon S3 コンソールで作成したバッチレプリケーションジョブ、AWS CLI、AWS SDK、または Amazon S3 REST API を使用して作成した任意のジョブタイプで使用できます。バッチレプリケーションの詳細については、「バッチレプリケーションを使用した既存のオブジェクトのレプリケーション」を参照してください。

マニフェストを自動的に生成するには、ジョブ作成リクエストの一環として次の要素を指定します。

- バケット所有者や Amazon リソースネーム (ARN) など、ソースオブジェクトが含まれるバケットに関する情報
- マニフェストファイルを作成するためのフラグ、出力バケット所有者、ARN、プレフィックス、ファイル形式、暗号化タイプなど、マニフェスト出力に関する情報
- 作成日、キー名、サイズ、ストレージクラスでオブジェクトをフィルタリングするためのオプションの条件 レプリケーションジョブの場合は、タグを使用してオブジェクトをフィルタリングすることもできます。

オブジェクトフィルターの条件

自動生成されたマニフェストに含まれるオブジェクトのリストをフィルタリングするには、次の条件を指定できます。詳細については、「Amazon S3 API リファレンス」の「JobManifestGeneratorFilter」を参照してください。

CreatedAfter

指定した場合、生成されたマニフェストには、この時間以降に作成されたソースバケットオブジェクトのみが含まれます。

CreatedBefore

指定した場合、生成されたマニフェストには、この時間以降に作成されたソースバケットオブジェクトのみが含まれます。

EligibleForReplication

指定した場合、生成されたマニフェストには、ソースバケットのレプリケーション設定に従ってレプリケーションの対象となるオブジェクトのみが含まれます。

KeyNameConstraint

指定された場合、生成されたマニフェストには、オブジェクトキーが MatchAnySubstring、MatchAnyPrefix、MatchAnySuffix に指定された文字列制約と一致するソースバケットオブジェクトのみが含まれます。

MatchAnySubstring – 指定した場合、指定された文字列がオブジェクトキー文字列内のいずれかの部分に出現する場合、生成されたマニフェストにそのオブジェクトが含まれます。

MatchAnyPrefix – 指定すると、指定された文字列がオブジェクトキー文字列の先頭に現れる場合、生成されたマニフェストにオブジェクトが含まれます。

MatchAnySuffix – 指定した場合、指定された文字列がオブジェクトキー文字列の末尾に出現する場合、生成されたマニフェストにオブジェクトが含まれます。

MatchAnyStorageClass

指定した場合、生成されたマニフェストには、指定されたストレージクラスで保存されているソースバケットオブジェクトのみが含まれます。

ObjectReplicationStatuses

指定した場合、生成されたマニフェストには、指定されたレプリケーションステータスのいずれかを持つソースバケットオブジェクトのみが含まれます。

ObjectSizeGreaterThanBytes

指定した場合、生成されたマニフェストには、ファイルサイズが指定されたバイト数以上のソースバケットオブジェクトのみが含まれます。

ObjectSizeLessThanBytes

指定した場合、生成されたマニフェストには、ファイルサイズが指定されたバイト数未満のソースバケット オブジェクトのみが含まれます。

> **Note**
>
> マニフェストが自動的に生成されたほとんどのジョブはクローンの作成はできません。バッチ レプリケーション ジョブは`KeyNameConstraint`、`MatchAnyStorageClass`、`ObjectSizeGreaterThanBytes`、または `ObjectSizeLessThanBytes` マニフェストフィルター条件を使用する場合を除き、クローンを作成できます。

マニフェスト条件を指定する構文は、ジョブの作成に使用する方法に応じて異なります。例については「ジョブの作成」を参照してください。

ジョブの作成

Amazon S3 コンソール、AWS CLI、AWS SDK、または Amazon S3 REST API を使用して S3 バッチオペレーションジョブを作成できます。

ジョブリクエストの作成の詳細については、バッチ操作ジョブのリクエストの要素 を参照してください。

前提条件

バッチオペレーションジョブを作成する前に、関連するアクセス許可が設定されていることを確認します。詳細については、「バッチオペレーションに対するアクセス許可の付与」を参照してください。

S3 コンソールの使用

バッチジョブを作成するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ページ上部にあるナビゲーションバーで、現在表示されている AWS リージョン の名前をクリックします。次に、ジョブを作成するリージョンを選択します。

> **Note**
>
> コピーオペレーションの場合は、コピー先バケットと同じリージョンにジョブを作成する必要があります。その他すべてのオペレーションの場合は、マニフェスト内のオブジェクトと同じリージョンにジョブを作成する必要があります。

3. Amazon S3 コンソールのナビゲーションペインで [バッチオペレーション] を選択します。
4. [ジョブの作成] を選択します。
5. ジョブを作成する AWS リージョン を確認します。
6. [マニフェストの形式] で、使用するマニフェストオブジェクトのタイプを選択します。

   - [S3 inventory report (S3 インベントリレポート)] を選択する場合、CSV 形式のインベントリレポートの一部として Amazon S3 が生成する manifest.json オブジェクトへのパスと、最新のバージョンではなく特定のバージョンを使用する場合には、オプションでマニフェストオブジェクトのバージョン ID を入力します。
   - [CSV] を選択する場合は、CSV 形式のマニフェストオブジェクトへのパスを入力します。マニフェストオブジェクトは、コンソールで説明される形式に従う必要があります。最新のバージョンではなく特定のバージョンを使用する場合には、マニフェストオブジェクトのバージョン ID をオプションで含めることもできます。

   > **Note**
   >
   > Amazon S3 コンソールは、バッチレプリケーションジョブのみの自動マニフェスト生成をサポートします。その他のすべてのジョブタイプで、指定したフィルタ条件に基づいて Amazon S3 がマニフェストを自動的に生成するようにするには、AWS CLI、AWS SDK、または Amazon S3 REST API を使用してジョブを設定する必要があります。

7. [次へ] を選択します。
8. [Operation (オペレーション)] で、マニフェストに登録されたすべてのオブジェクトを実行するオペレーションを選択します。選択したオペレーションに関する情報を入力して、[次へ] を選択します。
9. [追加オプションの設定] に関する情報を入力して、[次へ] を選択します。
10. [Review (確認)] で、設定を確認します。変更が必要な場合は、[戻る] を選択します。それ以外の場合は、[ジョブの作成] を選択します。

AWS CLI を使用する場合

AWS CLI を使用してバッチオペレーションジョブを作成するには、既存のマニフェストを指定するか、マニフェストを自動的に生成するかに応じて、次のいずれかの例を選択します。

Specify manifest

AWS CLI を使用して、既存のマニフェストファイルにリストされているオブジェクトに対して動作する S3 バッチオペレーション S3PutObjectTagging ジョブを作成する方法は、次の例のとおりです。

マニフェストを指定してバッチオペレーション **S3PutObjectTagging** ジョブを作成するには

1. 次のコマンドを使用して AWS Identity and Access Management (IAM) ロールを作成してから、IAM ポリシーを作成して関連するアクセス許可を割り当てます。次のロールとポリシーは、オブジェクト タグを追加するための Amazon S3 アクセス許可を付与します。このアクセス許可は、以降のステップでジョブを作成する際に必要になります。

   a. 次のコマンド例を使用して、バッチオペレーションで使用する IAM ロールを作成します。このコマンド例を使用するには、*S3BatchJobRole* をロールにつける名前に置き換えます。

```
aws iam create-role \
 --role-name S3BatchJobRole \
 --assume-role-policy-document '{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"batchoperations.s3.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}'
```

   ロールの Amazon リソースネーム (ARN) を記録します。ジョブの作成時にこの ARN が必要となります。

b. 次のコマンド例を使用して、必要なアクセス許可を持つ IAM ポリシーを作成して、前の手順で作成した IAM ロールにアタッチします。必要なアクセス権限の詳細については、「バッチオペレーションに対するアクセス許可の付与」を参照してください。

> **Note**
>
> ディレクトリバケットに対してアクションを実行するバッチオペレーションジョブには、特定のアクセス許可が必要です。詳細については、S3 Express One Zone 向け AWS Identity and Access Management (IAM)」を参照してください。

このサンプルコマンドを使用するには、*user input placeholders* を次のとおり置き換えます。

- *S3BatchJobRole* は、IAM ロール名に置き換えます。この名前が以前に使用した名前と一致することを確認します。
- *PutObjectTaggingBatchJobPolicy* は、IAM ポリシーにつける名前に置き換えます。
- *amzn-s3-demo-destination-bucket* は、タグを付けるオブジェクトがあるバケット名と置き換えます。
- *amzn-s3-demo-manifest-bucket* は、マニフェストがあるバケットの名前と置き換えます。
- *amzn-s3-demo-completion-report-bucket* は、完了レポートの配信先のバケット名と置き換えます。

```
aws iam put-role-policy \
  --role-name S3BatchJobRole \
  --policy-name PutObjectTaggingBatchJobPolicy \
  --policy-document '{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObjectTagging",
        "s3:PutObjectVersionTagging"
      ],
```

```
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetBucketLocation"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket",
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
      ]
    },
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObject",
        "s3:GetBucketLocation"
      ],
      "Resource":[
        "arn:aws:s3:::amzn-s3-demo-completion-report-bucket",
        "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
      ]
    }
  ]
}'
```

2. 次のコマンド例を使用して、S3PutObjectTagging ジョブを作成します。

   manifest.csv ファイルは、バケットのリストとオブジェクトキー値を提供します。このジョブは、マニフェストで識別されたオブジェクトに指定されたタグを適用します。ETag は manifest.csv オブジェクトの ETag であり、Amazon S3 コンソールから取得できます。このリクエストは no-confirmation-required パラメータを指定するため、update-job-status コマンドで確認しなくてもジョブを実行できます。詳細については、AWS CLI コマンドリファレンスの「create-job」を参照してください。

   このコマンド例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。*IAM-role* を先ほど作成した IAM ロールの ARN に置き換えます。

```
aws s3control create-job \
    --region us-west-2 \
```

```
    --account-id acct-id \
    --operation '{"S3PutObjectTagging": { "TagSet": [{"Key":"keyOne",
 "Value":"ValueOne"}] }}' \
    --manifest '{"Spec":{"Format":"S3BatchOperations_CSV_20180820","Fields":
["Bucket","Key"]},"Location":{"ObjectArn":"arn:aws:s3:::amzn-s3-demo-manifest-
bucket/manifest.csv","ETag":"60e460c9d1046e73f7dde5043ac3ae85"}}' \
    --report '{"Bucket":"arn:aws:s3:::amzn-s3-demo-
completion-report-bucket","Prefix":"final-reports",
 "Format":"Report_CSV_20180820","Enabled":true,"ReportScope":"AllTasks"}' \
    --priority 42 \
    --role-arn IAM-role \
    --client-request-token $(uuidgen) \
    --description "job description" \
    --no-confirmation-required
```

応答として、Amazon S3 はジョブ ID (など `00e123a4-c0d8-41f4-a0eb-b46f9ba5b07c`) を返します。ジョブの識別、モニタリング、変更にはこのジョブ ID が必要です。

Generate manifest

オブジェクトフィルター条件に基づいてマニフェストを自動的に生成する S3 バッチオペレーション `S3DeleteObjectTagging` ジョブを作成する方法は、次の例のとおりです。この条件には、作成日、キー名、サイズ、ストレージクラス、タグが含まれます。

マニフェストを生成してバッチオペレーション **`S3DeleteObjectTagging`** ジョブを作成するには

1. 次のコマンドを使用して AWS Identity and Access Management (IAM) ロールを作成してから、IAM ポリシーを作成してアクセス許可を割り当てます。次のロールとポリシーは、オブジェクト タグを削除するための Amazon S3 アクセス許可を付与します。このアクセス許可は、以降のステップでジョブを作成する際に必要になります。

   a. 次のコマンド例を使用して、バッチオペレーションで使用する IAM ロールを作成します。このコマンド例を使用するには、*`S3BatchJobRole`* をロールにつける名前に置き換えます。

   ```
   aws iam create-role \
    --role-name S3BatchJobRole \
    --assume-role-policy-document '{
   ```

```
    "Version":"2012-10-17",
    "Statement":[
       {
          "Effect":"Allow",
          "Principal":{
             "Service":"batchoperations.s3.amazonaws.com"
          },
          "Action":"sts:AssumeRole"
       }
    ]
}'
```

ロールの Amazon リソースネーム (ARN) を記録します。ジョブの作成時にこの ARN が必要となります。

b. 次のコマンド例を使用して、必要なアクセス許可を持つ IAM ポリシーを作成して、前の手順で作成した IAM ロールにアタッチします。必要なアクセス権限の詳細については、「バッチオペレーションに対するアクセス許可の付与」を参照してください。

> **Note**
>
> ディレクトリバケットに対してアクションを実行するバッチオペレーションジョブには、特定のアクセス許可が必要です。詳細については、S3 Express One Zone 向け AWS Identity and Access Management (IAM)」を参照してください。

このサンプルコマンドを使用するには、*user input placeholders* を次のとおり置き換えます。

- *S3BatchJobRole* は、IAM ロール名に置き換えます。この名前が以前に使用した名前と一致することを確認します。
- *DeleteObjectTaggingBatchJobPolicy* は、IAM ポリシーにつける名前に置き換えます。
- *amzn-s3-demo-destination-bucket* は、タグを付けるオブジェクトがあるバケット名と置き換えます。
- *amzn-s3-demo-manifest-bucket* は、マニフェストの保存先バケット名と置き換えます。
- *amzn-s3-demo-completion-report-bucket* は、完了レポートの配信先のバケット名と置き換えます。

```
aws iam put-role-policy \
  --role-name S3BatchJobRole \
  --policy-name DeleteObjectTaggingBatchJobPolicy \
  --policy-document '{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "s3:DeleteObjectTagging",
        "s3:DeleteObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    },
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutInventoryConfiguration"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket",
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
      ]
    },
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObject",
        "s3:ListBucket"
      ],
      "Resource":[
        "arn:aws:s3:::amzn-s3-demo-completion-report-bucket",
        "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*",
```

```
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
      ]
    }
  ]
}'
```

2. 次のコマンド例を使用して、S3DeleteObjectTagging ジョブを作成します。

   この例では、--report セクション内の値によって、生成されるジョブレポートのバケット、プレフィックス、形式、範囲が指定されます。--manifest-generator セクションでは、ジョブの対象となるオブジェクトを含むソースバケットに関する情報、ジョブに対して生成されるマニフェスト出力リストに関する情報、マニフェストに含めるオブジェクトの範囲を作成日、名前の制約、サイズ、ストレージクラスによって絞り込むためのフィルター条件を指定します。このコマンドでは、ジョブの優先度、IAM ロール、AWS リージョン も指定します。

   詳細については、AWS CLI コマンドリファレンスの「create-job」を参照してください。

   このコマンド例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。*IAM-role* を先ほど作成した IAM ロールの ARN に置き換えます。

```
aws s3control create-job \
    --account-id 012345678901 \
    --operation '{
        "S3DeleteObjectTagging": {}
    }' \
    --report '{
        "Bucket":"arn:aws:s3:::amzn-s3-demo-completion-report-bucket",
        "Prefix":"reports",
        "Format":"Report_CSV_20180820",
        "Enabled":true,
        "ReportScope":"AllTasks"
    }' \
    --manifest-generator '{
        "S3JobManifestGenerator": {
          "ExpectedBucketOwner": "012345678901",
          "SourceBucket": "arn:aws:s3:::amzn-s3-demo-source-bucket",
          "EnableManifestOutput": true,
          "ManifestOutputLocation": {
            "ExpectedManifestBucketOwner": "012345678901",
            "Bucket": "arn:aws:s3:::amzn-s3-demo-manifest-bucket",
```

```
            "ManifestPrefix": "prefix",
            "ManifestFormat": "S3InventoryReport_CSV_20211130"
          },
          "Filter": {
            "CreatedAfter": "2023-09-01",
            "CreatedBefore": "2023-10-01",
            "KeyNameConstraint": {
              "MatchAnyPrefix": [
                "prefix"
              ],
              "MatchAnySuffix": [
                "suffix"
              ]
            },
            "ObjectSizeGreaterThanBytes": 100,
            "ObjectSizeLessThanBytes": 200,
            "MatchAnyStorageClass": [
              "STANDARD",
              "STANDARD_IA"
            ]
          }
        }
      }' \
    --priority 2 \
    --role-arn IAM-role \
    --region us-east-1
```

応答として、Amazon S3 はジョブ ID (など `00e123a4-c0d8-41f4-a0eb-b46f9ba5b07c`) を返します。ジョブの識別、モニタリング、変更にはこのジョブ ID が必要です。

AWS SDK for Java を使用する場合

AWS SDK for Java を使用してバッチオペレーションジョブを作成するには、既存のマニフェストを指定するか、マニフェストを自動的に生成するかに応じて、次のいずれかの例を選択します。

Specify manifest

既存のマニフェスト ファイルにリストされているオブジェクトに対して動作する S3 バッチオペレーション S3PutObjectTagging ジョブを作成する方法は、次の例のとおりです。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

Example

```
package aws.example.s3control;



import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.*;

import java.util.UUID;
import java.util.ArrayList;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class CreateJob {
    public static void main(String[] args) {
        String accountId = "Account ID";
        String iamRoleArn = "IAM Role ARN";
        String reportBucketName = "arn:aws:s3:::amzn-s3-demo-completion-report-
bucket";
        String uuid = UUID.randomUUID().toString();

        ArrayList tagSet = new ArrayList<S3Tag>();
        tagSet.add(new S3Tag().withKey("keyOne").withValue("ValueOne"));


        try {
            JobOperation jobOperation = new JobOperation()
                    .withS3PutObjectTagging(new S3SetObjectTaggingOperation()
                            .withTagSet(tagSet)
                    );

            JobManifest manifest = new JobManifest()
                    .withSpec(new JobManifestSpec()
                            .withFormat("S3BatchOperations_CSV_20180820")
                            .withFields(new String[]{
                                    "Bucket", "Key"
                            }))
                    .withLocation(new JobManifestLocation()
                            .withObjectArn("arn:aws:s3:::my_manifests/manifest.csv")
```

```
                            .withETag("60e460c9d1046e73f7dde5043ac3ae85"));
            JobReport jobReport = new JobReport()
                    .withBucket(reportBucketName)
                    .withPrefix("reports")
                    .withFormat("Report_CSV_20180820")
                    .withEnabled(true)
                    .withReportScope("AllTasks");

            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            s3ControlClient.createJob(new CreateJobRequest()
                    .withAccountId(accountId)
                    .withOperation(jobOperation)
                    .withManifest(manifest)
                    .withReport(jobReport)
                    .withPriority(42)
                    .withRoleArn(iamRoleArn)
                    .withClientRequestToken(uuid)
                    .withDescription("job description")
                    .withConfirmationRequired(false)
            );

        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Generate manifest

次の例は、作成日、キー名、サイズなどのオブジェクトフィルター条件に基づいてマニフェストを自動的に生成する S3 バッチオペレーション s3PutObjectCopy ジョブを作成する方法は、次の例のとおりです。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

Example

```
        package aws.example.s3control;

    import com.amazonaws.AmazonServiceException;
    import com.amazonaws.SdkClientException;
    import com.amazonaws.auth.profile.ProfileCredentialsProvider;
    import com.amazonaws.services.s3control.AWSS3Control;
    import com.amazonaws.services.s3control.AWSS3ControlClient;
    import com.amazonaws.services.s3control.model.CreateJobRequest;
    import com.amazonaws.services.s3control.model.CreateJobResult;
    import com.amazonaws.services.s3control.model.JobManifestGenerator;
    import com.amazonaws.services.s3control.model.JobManifestGeneratorFilter;
    import com.amazonaws.services.s3control.model.JobOperation;
    import com.amazonaws.services.s3control.model.JobReport;
    import com.amazonaws.services.s3control.model.KeyNameConstraint;
    import com.amazonaws.services.s3control.model.S3JobManifestGenerator;
    import com.amazonaws.services.s3control.model.S3ManifestOutputLocation;
    import com.amazonaws.services.s3control.model.S3SetObjectTaggingOperation;
    import com.amazonaws.services.s3control.model.S3Tag;

    import java.time.Instant;
    import java.util.Date;
    import java.util.UUID;
    import java.util.ArrayList;

    import static com.amazonaws.regions.Regions.US_WEST_2;

    public class test {
        public static void main(String[] args) {
            String accountId = "012345678901";
            String iamRoleArn = "arn:aws:iam::012345678901:role/ROLE";
            String sourceBucketName = "arn:aws:s3:::amzn-s3-demo-source-bucket";
            String reportBucketName = "arn:aws:s3:::amzn-s3-demo-completion-report-
bucket";
            String manifestOutputBucketName = "arn:aws:s3:::amzn-s3-demo-manifest-
bucket";
            String uuid = UUID.randomUUID().toString();
            long minimumObjectSize = 100L;

            ArrayList<S3Tag> tagSet = new ArrayList<>();
            tagSet.add(new S3Tag().withKey("keyOne").withValue("ValueOne"));

            ArrayList<String> prefixes = new ArrayList<>();
```

```
            prefixes.add("s3KeyStartsWith");

            try {
                JobOperation jobOperation = new JobOperation()
                        .withS3PutObjectTagging(new S3SetObjectTaggingOperation()
                                .withTagSet(tagSet)
                        );
                S3ManifestOutputLocation manifestOutputLocation = new
S3ManifestOutputLocation()
                        .withBucket(manifestOutputBucketName)
                        .withManifestPrefix("manifests")
                        .withExpectedManifestBucketOwner(accountId)
                        .withManifestFormat("S3InventoryReport_CSV_20211130");

                JobManifestGeneratorFilter jobManifestGeneratorFilter = new
JobManifestGeneratorFilter()
                        .withEligibleForReplication(true)
                        .withKeyNameConstraint(
                                new KeyNameConstraint()
                                        .withMatchAnyPrefix(prefixes))
                        .withCreatedBefore(Date.from(Instant.now()))
                        .withObjectSizeGreaterThanBytes(minimumObjectSize);

                S3JobManifestGenerator s3JobManifestGenerator = new
S3JobManifestGenerator()
                        .withEnableManifestOutput(true)
                        .withManifestOutputLocation(manifestOutputLocation)
                        .withFilter(jobManifestGeneratorFilter)
                        .withSourceBucket(sourceBucketName);

                JobManifestGenerator jobManifestGenerator = new
JobManifestGenerator()
                        .withS3JobManifestGenerator(s3JobManifestGenerator);

                JobReport jobReport = new JobReport()
                        .withBucket(reportBucketName)
                        .withPrefix("reports")
                        .withFormat("Report_CSV_20180820")
                        .withEnabled(true)
                        .withReportScope("AllTasks");

                AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                        .withCredentials(new ProfileCredentialsProvider())
                        .withRegion(US_WEST_2)
```

```
                        .build();

                CreateJobResult createJobResult = s3ControlClient.createJob(new
CreateJobRequest()
                        .withAccountId(accountId)
                        .withOperation(jobOperation)
                        .withManifestGenerator(jobManifestGenerator)
                        .withReport(jobReport)
                        .withPriority(42)
                        .withRoleArn(iamRoleArn)
                        .withClientRequestToken(uuid)
                        .withDescription("job description")
                        .withConfirmationRequired(true)
                );

                System.out.println("Created job " + createJobResult.getJobId());

            } catch (AmazonServiceException e) {
                // The call was transmitted successfully, but Amazon S3 couldn't
process
                // it and returned an error response.
                e.printStackTrace();
            } catch (SdkClientException e) {
                // Amazon S3 couldn't be contacted for a response, or the client
                // couldn't parse the response from Amazon S3.
                e.printStackTrace();
            }
        }
    }
```

REST API の使用

REST API を使用して、バッチ操作ジョブを作成できます。詳細については、「Amazon Simple Storage Service API リファレンス」の「CreateJob」を参照してください。

ジョブのレスポンス

CreateJob リクエストが成功すると、Amazon S3 はジョブ ID を返します。ジョブ ID は Amazon S3 が自動的に生成する一意の識別子であるため、バッチ操作ジョブを識別してそのステータスを監視できます。

AWS CLI、AWS SDK または REST API を介してジョブを作成する場合、S3 バッチオペレーションを設定してジョブを自動処理を開始できます。ジョブはより高い優先度のジョブを待機せずに、準備が整うと直ちに実行されます。

Amazon S3 コンソールを使用してジョブを作成する際は、バッチオペレーションでジョブの処理を開始する前に、ジョブの詳細を確認し、ジョブを実行できるかを確認する必要があります。ジョブが 30 日以上停止状態のままになると、失敗します。

S3 バッチ操作でサポートされるオペレーション

S3 バッチ操作を使用すると、Amazon S3 のオブジェクトに対して大規模なバッチ操作を実行することができます。S3 バッチ操作では、指定した Amazon S3 のオブジェクトのリストに対して、1 つのオペレーションを実行できます。1 つのジョブで、エクサバイトのデータを含む数十億ものオブジェクトに対して、指定されたオペレーションを実行できます。Amazon S3 は、進捗状況の追跡、通知の送信、すべてのアクションの詳細な完了レポートの保存を行い、フルマネージド型の監査可能なサーバーレスエクスペリエンスを提供します。S3 バッチオペレーションは、Amazon S3 コンソール、AWS CLI、AWS SDK、または Amazon S3 REST API を通じて使用できます。

S3 バッチオペレーションでは、以下のオペレーションがサポートされています。

オブジェクトのコピー

Amazon S3 バッチオペレーションを使用すると、Amazon S3 のオブジェクトに対して大規模なバッチオペレーションを実行できます。バッチオペレーション Copy オペレーションは、マニフェストで指定した各オブジェクトをコピーします。オブジェクトを同じ AWS リージョンのバケットにコピーしたり、別のリージョンのバケットにコピーしたりできます。S3 バッチ操作では、Amazon S3 のオブジェクトのコピーで使用できるほとんどのオプションがサポートされています。このオプションには、オブジェクトのメタデータの設定、アクセス許可の設定およびオブジェクトのストレージクラスの変更が含まれます。

Copy オペレーションを使用して、既存の暗号化されていないオブジェクトをコピーし、同じバケットに暗号化されたオブジェクトとして書き込むこともできます。詳細については、「Encrypting objects with Amazon S3 Batch Operations」を参照してください。

オブジェクトをコピーするときに、オブジェクトのチェックサムの計算に使用されるチェックサムアルゴリズムを変更できます。オブジェクトの追加のチェックサムが計算されていない場合は、使用する Amazon S3 のチェックサムアルゴリズムを指定して追加することもできます。詳細については、「Amazon S3 でのオブジェクトの整合性のチェック」を参照してください。

Amazon S3 でのオブジェクトのコピー、および必須パラメータとオプションのパラメータの詳細については、このガイドの「オブジェクトのコピー、移動、名前の変更」および「Amazon Simple Storage Service API リファレンス」の「CopyObject」を参照してください。

制約と制限

バッチオペレーション Copy オペレーションを使用している場合は、以下の制約と制限が適用されます。

- すべてのソースオブジェクトは 1 つのバケットにある必要があります。
- すべての送信先オブジェクトは 1 つのバケットにある必要があります。
- 送信元バケットへの読み込み許可および送信先バケットへの書き込み許可を保持していることが必要です。
- コピーできるオブジェクトのサイズは 5 GB までです。
- S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive クラスから S3 Standard ストレージクラスにオブジェクトをコピーする場合は、まずこれらのオブジェクトを復元する必要があります。詳細については、「アーカイブされたオブジェクトの復元」を参照してください。
- バッチオペレーション Copy コピージョブは、コピー先リージョン (オブジェクトをコピーする先のリージョン) で作成する必要があります。
- 条件式によるエンティティタグ (ETag) の確認とお客様が用意した暗号化キーを使用したサーバー側の暗号化 (SSE-C) を除く、すべての `CopyObject` オプションがサポートされています。
- 送信先バケットがバージョン化されていない場合、同じキー名を持つオブジェクトを上書きできます。
- オブジェクトは、マニフェストに表示されている順序と同じ順序でコピーされるとは限りません。バージョン管理されたバケットで、現在のバージョンまたは以前のバージョンの順序を維持することが必要な場合は、最初に以前のバージョンをすべてコピーします。次に、最初のジョブが完了したら、後続のジョブで現在のバージョンをコピーします。
- 低冗長化ストレージ (RRS) クラスへのオブジェクトのコピーはサポートされていません。
- 1 つのバッチオペレーションコピージョブで、最大 200 億個のオブジェクトを持つマニフェストをサポートできます。

S3 バッチ操作を使用したオブジェクトのコピー

Amazon S3 バッチオペレーションを使用すると、Amazon S3 のオブジェクトに対して大規模なバッチオペレーションを実行できます。S3 バッチオペレーションを使用して Copy (`CopyObject`) ジョブを作成し、同じアカウント内または別の送信先アカウントにオブジェクトをコピーできます。

次のセクションでは、別のアカウントにあるマニフェストを保存して使用する方法の例を示します。最初の例は、Amazon S3 インベントリからインベントリレポートをコピー先アカウントに配信して、ジョブの作成時に使用する方法を示しています。2 番目の例は、送信元または送信先アカウントでカンマ区切り値 (CSV) マニフェストを使用する方法を示しています。3 番目の例は、Copy オペレーションを使用して、AWS Key Management Service (AWS KMS) キーによるサーバー側の暗号化 (SSE-KMS) を使用し、暗号化された既存のオブジェクトの S3 バケットキーを有効にする方法を示しています。

コピーオペレーションの例

- インベントリレポートを使用して AWS アカウント 間でオブジェクトをコピーする
- CSV マニフェストを使用して AWS アカウント 間でオブジェクトをコピーする
- バッチオペレーションを使用して SSE-KMS の S3 バケットキーを有効にする

インベントリレポートを使用して AWS アカウント 間でオブジェクトをコピーする

Amazon S3 バッチオペレーションを使用すると、Amazon S3 のオブジェクトに対して大規模なバッチオペレーションを実行できます。S3 バッチオペレーションを使用して Copy (`CopyObject`) コピージョブを作成し、同じアカウント内または別の送信先アカウントにオブジェクトをコピーできます。

Amazon S3 インベントリを使用してインベントリレポートを作成し、そのレポートを使用して、S3 バッチオペレーションでコピーするオブジェクトのリスト (マニフェスト) を作成できます。ソースアカウントまたは送信先アカウントでの CSV マニフェストの使用について詳しくは、the section called “CSV マニフェストを使用して AWS アカウント 間でオブジェクトをコピーする” を参照してください。

Amazon S3 インベントリは、バケット内のオブジェクトのインベントリを生成します。結果のリストは出力ファイルに公開されます。インベントリ対象となるバケットはソースバケットと呼ばれ、インベントリレポートファイルが保存されているバケットは送信先バケットと呼ばれます。

Amazon S3 インベントリレポートは、別の AWS アカウント に配信されるように設定できます。これにより、送信先アカウントでジョブが作成されたときに S3 バッチオペレーションがインベントリレポートを読み取ることができます。

Amazon S3 インベントリのコピー元およびコピー先バケットの詳細については、「ソースバケットと保存先バケット」を参照してください。

インベントリを設定する最も簡単な方法は、Amazon S3 を使用することですが、REST API、AWS Command Line Interface (AWS CLI)、または AWS SDK を使用することもできます。

以下のコンソールの手順には、S3 バッチ操作ジョブに対するアクセス許可を設定するための大まかなステップが含まれています。この手順では、オブジェクトを送信元アカウントから送信先アカウントにコピーし、インベントリレポートを送信先アカウントに保存します。

さまざまなアカウントが所有する送信元および送信先バケットの Amazon S3 インベントリを設定する方法

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。
3. インベントリレポートを保存するための送信先マニフェストバケットを決定 (または作成) します。この手順では、送信先アカウントは、送信先マニフェストバケットとオブジェクトのコピー先バケットの両方を所有するアカウントです。
4. ソースバケットのインベントリレポートを設定します。コンソールを使用してインベントリリストを設定する方法またはインベントリリストファイルを暗号化する方法については、「Amazon S3 インベントリの設定」を参照してください。

   インベントリレポートを設定する場合は、リストを保存する送信先バケットを指定します。ソースバケットのインベントリレポートが送信先バケットに発行されます。この手順では、ソースアカウントは、ソースバケットを所有するアカウントです。

   出力形式として [CSV] を選択してください。

   送信先バケットの情報を入力したら、[Buckets in another account (別のアカウントのバケット)] を選択します。次に、送信先マニフェストバケットの名前を入力します。必要に応じて、送信先アカウントのアカウント ID を入力できます。

   インベントリ設定が保存されると、コンソールに次のようなメッセージが表示されます。

   Amazon S3 は送信先バケットにバケットポリシーを作成できませんでした。Amazon S3 が送信先バケットに対してデータの保存ができるよう、送信先バケット所有者に次のバケットポリシーの追加を依頼してください。

   コンソールには、送信先バケットに使用できるバケットポリシーが表示されます。
5. コンソールに表示される送信先バケットポリシーをコピーします。
6. 送信先アカウントで、インベントリレポートが格納されている送信先マニフェストバケットにコピーしたバケットポリシーを追加します。

7. S3 バッチ操作信頼ポリシーに基づいて、送信先アカウントにロールを作成します。この信頼ポリシーの詳細については、「信頼ポリシー」を参照してください。

   ロールの作成について詳しくは、「IAM ユーザーガイド」の「AWS のサービスにアクセス許可を委任するロールを作成する」を参照してください。

   ロールの名前を入力します (以下の例では *BatchOperationsDestinationRoleCOPY* という名前を使用しています)。[S3] サービスを選択してから、信頼ポリシーをロールに適用する [S3 バッチオペレーション] ユースケースを選択します。

   次に [ポリシーの作成]を選択して、ロールに次のポリシーをアタッチします。このポリシーを使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowBatchOperationsDestinationObjectCOPY",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:PutObjectVersionAcl",
        "s3:PutObjectAcl",
        "s3:PutObjectVersionTagging",
        "s3:PutObjectTagging",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-destination-bucket/*",
        "arn:aws:s3:::amzn-s3-demo-source-bucket/*",
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
      ]
    }
  ]
}
```

ロールはポリシーを使用して、送信先バケットのマニフェストを読み取るための batchoperations.s3.amazonaws.com アクセス許可を付与します。さらに、ソースオブジェクトバケット内の GET オブジェクト、アクセスコントロールリスト (ACL)、タグ、およびバージョンにアクセス許可を付与します。また、PUT オブジェクト、ACL、タグ、およびバージョンに送信先オブジェクトバケットへのアクセス許可を付与します。

8. ソースアカウントで、前の手順で作成したロールにソースバケット内のオブジェクト、ACL、タグ、およびバージョンの GET を付与する、ソースバケットのバケットポリシーを作成します。このステップにより、S3 バッチ操作は信頼できるロールを介して送信元バケットからオブジェクトを取得できます。

   以下は、ソースアカウントのバケットポリシーの例です。このポリシーを使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowBatchOperationsSourceObjectCOPY",
      "Effect": "Allow",
      "Principal": {
        "AWS":
 "arn:aws:iam::DestinationAccountNumber:role/BatchOperationsDestinationRoleCOPY"
      },
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
    }
  ]
}
```

9. インベントリレポートが使用可能になったら、送信先アカウントで S3 バッチオペレーション Copy (CopyObject) ジョブを作成し、送信先マニフェストバケットから在庫レポートを選択します。送信先アカウントで作成した IAM ロールの ARN が必要です。

ジョブの作成に関する全般情報については、「S3 バッチオペレーションジョブの作成」を参照してください。

コンソールを使用してジョブを作成する方法については、「S3 バッチオペレーションジョブの作成」を参照してください。

CSV マニフェストを使用して AWS アカウント 間でオブジェクトをコピーする

Amazon S3 バッチオペレーションを使用すると、Amazon S3 のオブジェクトに対して大規模なバッチオペレーションを実行できます。S3 バッチオペレーションを使用して Copy (`CopyObject`) ジョブを作成し、同じアカウント内または別の送信先アカウントにオブジェクトをコピーできます。

ソースアカウントに保存された CSV マニフェストを使用して、S3 バッチオペレーションによって AWS アカウント間でオブジェクトをコピーできます。S3 インベントリレポートをマニフェストとして使用するには、「the section called “インベントリレポートを使用して AWS アカウント 間でオブジェクトをコピーする”」を参照してください。

CSV 形式のマニフェストファイルの例については、「the section called “マニフェストファイルの作成”」を参照してください。

次の手順は、S3 バッチオペレーションジョブを使用して、ソースアカウントに保存されている CSV マニフェストファイルによってソースアカウントから送信先アカウントにオブジェクトをコピーするときに、アクセス許可を設定する方法を示しています。

CSV マニフェストを使用して AWS アカウント間でオブジェクトをコピーするには

1. S3 バッチオペレーション信頼ポリシーに基づいて、送信先アカウントに AWS Identity and Access Management (IAM) ロールを作成します。この手順では、送信先アカウントは、オブジェクトのコピー先のアカウントです。

   信頼ポリシーの詳細については、「信頼ポリシー」を参照してください。

   ロールの作成について詳しくは、「IAM ユーザーガイド」の「AWS のサービスにアクセス許可を委任するロールを作成する」を参照してください。

   コンソールを使用してロールを作成する場合は、ロールの名前を入力します (以下のサンプルロールでは *`BatchOperationsDestinationRoleCOPY`* という名前が使用されています)。[S3] サービスを選択してから、信頼ポリシーをロールに適用する [S3 バッチオペレーション] ユースケースを選択します。

次に [ポリシーの作成]を選択して、ロールに次のポリシーをアタッチします。このポリシーを使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowBatchOperationsDestinationObjectCOPY",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:PutObjectVersionAcl",
        "s3:PutObjectAcl",
        "s3:PutObjectVersionTagging",
        "s3:PutObjectTagging",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-destination-bucket/*",
        "arn:aws:s3:::amzn-s3-demo-source-bucket/*",
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
      ]
    }
  ]
}
```

このポリシーを使用して、ロールはソースマニフェストバケットのマニフェストを読み取るための batchoperations.s3.amazonaws.com アクセス許可を付与します。ソースオブジェクトバケット内のオブジェクト、アクセスコントロールリスト (ACL)、タグ、およびバージョンを GET するアクセス許可を付与し、また、送信先のオブジェクトバケットへオブジェクト、ACL、タグ、およびバージョンを PUT するアクセス許可も付与します。

2. 前のステップで作成したロールにソースマニフェストバケット内のオブジェクトとバージョンを GET するアクセス許可を付与するために、ソースアカウントで、マニフェストが含まれるバケットに適用するバケットポリシーを作成します。

このステップにより、信頼できるロールを使用して、S3 バッチオペレーションでマニフェストを読み取ることができます。マニフェストを含むバケットにバケットポリシーを適用します。

以下は、ソースマニフェストバケットに適用するバケットポリシーの例です。このポリシーを使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowBatchOperationsSourceManfiestRead",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::DestinationAccountNumber:user/ConsoleUserCreatingJob",

 "arn:aws:iam::DestinationAccountNumber:role/BatchOperationsDestinationRoleCOPY"
        ]
      },
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
    }
  ]
}
```

このポリシーでは、送信先アカウントでジョブを作成しているコンソールユーザーに、同じバケットポリシーを介してソースマニフェストバケットでも同じアクセス許可を許可する権限も付与されます。

3. 前の手順で作成したロールにソースオブジェクトバケット内のオブジェクト、ACL、タグ、およびバージョンを GET するアクセス許可を付与するために、ソースアカウントで、ソースバケットに適用するバケットポリシーを作成します。S3 バッチ操作は、信頼できるロールを使用して送信元バケットからオブジェクトを取得できます。

   以下は、ソースオブジェクトを含むバケットのバケットポリシーの例です。このポリシーを使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowBatchOperationsSourceObjectCOPY",
      "Effect": "Allow",
      "Principal": {
        "AWS":
 "arn:aws:iam::DestinationAccountNumber:role/BatchOperationsDestinationRoleCOPY"
      },
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
    }
  ]
}
```

4. 送信先アカウントで S3 バッチ操作ジョブを作成します。送信先アカウントで作成したロールの Amazon リソースネーム (ARN) が必要です。ジョブの作成の詳細については、「S3 バッチオペレーションジョブの作成」を参照してください。

バッチオペレーションを使用して SSE-KMS の S3 バケットキーを有効にする

S3 バケットキーは、Amazon S3 から AWS KMS へのリクエストトラフィックを減らすことにより、AWS Key Management Service (AWS KMS) (SSE-KMS) を使用したサーバー側の暗号化のコストを削減します。詳細については、「Amazon S3 バケットキーを使用した SSE-KMS のコストの削減」および「新しいオブジェクトで SSE-KMS の S3 バケットキーを使用するようにバケットを設定する」を参照してください。REST API、AWS SDK、または AWS CLI を使用して `CopyObject` オペレーションを実行する際、`true` または `false` の値の付いた `x-amz-server-side-encryption-bucket-key-enabled` リスエストヘッダーを追加して、オブジェクトレベルで S3 バケットキーを有効または無効にできます。

`CopyObject` オペレーションを使用してオブジェクトの S3 バケットキーを設定すると、Amazon S3 では、そのオブジェクトの設定のみが更新されます。送信先バケットの S3 バケットキーの設定は変更されません。AWS KMS で暗号化されたオブジェクトの `CopyObject` リクエストを S3 バケットキーが有効になっているバケットに送信すると、リクエストヘッダーのキーを無効にしない限

り、オブジェクトレベルのオペレーションでは自動的に S3 バケットキーが使用されます。オブジェクトに S3 バケットキーを指定しない場合、Amazon S3 ではレプリケート先バケットの S3 バケットキーの設定がオブジェクトに適用されます。

既存の Amazon S3 オブジェクトを暗号化するには、S3 バッチオペレーションを使用します。バッチオペレーションのコピーオペレーションを使用して、既存の暗号化されていないオブジェクトをコピーし、同じバケットに新しい暗号化されたオブジェクトを書き込めます。詳細については、「AWS ストレージブログ」の「Encrypting objects with Amazon S3 Batch Operations」を参照してください。

次の例では、バッチオペレーションの Copy オペレーションを使用して、既存のオブジェクトで S3 バケットキーを有効にします。詳細については、「the section called “オブジェクトの S3 バケットキーを設定する”」を参照してください。

トピック

- S3 バッチオペレーションを使用し、有効になっている S3 バケットキーでオブジェクトを暗号化する際の考慮事項
- 前提条件
- ステップ 1: Amazon S3 インベントリを使用してオブジェクトのリストを取得する
- ステップ 2: S3 Select を使用してオブジェクトリストをフィルタリングする
- ステップ 3: S3 バッチオペレーションジョブをセットアップして実行する

S3 バッチオペレーションを使用し、有効になっている S3 バケットキーでオブジェクトを暗号化する際の考慮事項

S3 バッチオペレーションを使用し、有効になっている S3 バケットキーを使ってオブジェクトを暗号化するときは、次の問題を考慮してください。

- S3 バッチオペレーションがお客様に代わって実行するデータ転送、リクエスト、その他の料金などのオペレーションに関連する料金に加えて、S3 バッチオペレーションジョブ、オブジェクト、およびリクエストに対して課金されます。詳細については、「Amazon S3 の料金」を参照してください。
- バージョニングされたバケットを使用する場合、実行される各 S3 バッチオペレーションジョブは、オブジェクトの新しい暗号化されたバージョンを作成します。また、S3 バケットキーが設定されていない、前のバージョンも維持されます。古いバージョンを削除するには、ライフサイクル設定の要素 で説明されているように、最新でないバージョンに対して S3 ライフサイクルの有効期限ポリシーをセットアップします。

- コピーオペレーションでは、新しい作成日を持つ新しいオブジェクトが作成されます。これは、アーカイブなどのライフサイクルアクションに影響を与える可能性があります。バケット内のすべてのオブジェクトをコピーすると、新しいすべてのコピーの作成日が同一になるか類似する日付になります。これらのオブジェクトをさらに識別し、さまざまなデータサブセットに対して異なるライフサイクルルールを作成するには、オブジェクトタグの使用を検討してください。

前提条件

S3 バケットキーを使用するようオブジェクトを設定する前に、「S3 バケットキーを有効にする前に注意するべき変更点」を確認してください。

この例を使用するには、AWS アカウントと、作業ファイルと暗号化された結果を保持するために少なくとも 1 つの S3 バケットが必要です。また、以下のトピックを含む、既存の S3 バッチオペレーションのドキュメントの多くが役立つ場合があります。

- S3 バッチ操作の基本
- S3 バッチオペレーションジョブの作成
- S3 バッチ操作でサポートされるオペレーション
- S3 バッチ操作ジョブの管理

ステップ 1: Amazon S3 インベントリを使用してオブジェクトのリストを取得する

まずはじめに、暗号化するオブジェクトを含む S3 バケットを特定し、その内容のリストを取得します。Amazon S3 インベントリレポートは、この実行に最も便利で手頃な方法です。レポートには、バケット内のオブジェクトのリストと、関連するメタデータが表示されます。このステップでは、ソースバケットはインベントリ対象のバケットで、送信先バケットは、インベントリレポートファイルを保存するバケットです。Amazon S3 インベントリのコピー元およびコピー先バケットの詳細については、「S3 インベントリを使用したデータのカタログ化と分析」を参照してください。

インベントリをセットアップする最も簡単な方法は、AWS Management Console を使用することです。ただし、REST API、AWS Command Line Interface (AWS CLI)、または AWS SDK も使用できます。これらのステップを実行する前に、必ずコンソールにサインインして Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開いてください。アクセス許可拒否エラーが発生した場合は、バケットポリシーを送信先バケットに追加します。詳細については、「S3 インベントリおよび S3 分析に対するアクセス許可の付与」を参照してください。

S3 インベントリを使用してオブジェクトのリストを取得するには、次のようにします。

1. Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. ナビゲーションペインで、[バケット] を選択し、暗号化するオブジェクトを含むバケットを選択します。
3. [Management] (管理) タブの [Inventory configurations] (インベントリ設定) セクションに移動し、[Create inventory configuration] (インベントリ設定の作成) を選択します。
4. 新しいインベントリに名前を付け、送信先 S3 バケットの名前を入力し、オプションで Amazon S3 の送信先プレフィックスを作成して、そのバケット内のオブジェクトを割り当てます。
5. [Output format] (出力形式) として [CSV] を選択します。
6. [追加フィールド - オプション] セクションで、[暗号化] と、関心のあるその他の任意のレポートフィールドを選択します。レポート配信の頻度を [Daily] (毎日) に設定して、最初のレポートが早くバケットに配信されるようにします。
7. [Create] (作成) を選択して設定を保存します。

Amazon S3 では最初のレポートが配信されるまでに最大で 48 時間かかることがあります。最初のレポートが到着したら確認してください。最初のレポートを受け取ったら、次のステップに進み、S3 インベントリレポートの内容をフィルタリングします。このバケットのインベントリレポートを受信する必要がなくなった場合は、S3 インベントリ設定を削除します。削除しない場合、Amazon S3 は毎日または毎週のスケジュールでレポートの配信を継続します。

インベントリ・リストは、すべてのオブジェクトの単一のポイント・イン・タイム・ビューではありません。インベントリリストはバケットアイテムのローリングスナップショットであり、最終的には整合します (たとえば、最近追加されたオブジェクトや削除されたオブジェクトはリストに含まれない可能性があります)。静的オブジェクトや、2 日以上前に作成したオブジェクトセットを操作するときには、S3 インベントリと S3 バッチオペレーションの組み合わせが最適です。より新しいデータを操作するには、ListObjectsV2 (GET バケット) API オペレーションを使用して、オブジェクトのリストを手動で作成します。必要に応じて、このプロセスを数日間、またはインベントリレポートにすべてのオブジェクトが必要なステータスで表示されるまで繰り返します。

ステップ 2: S3 Select を使用してオブジェクトリストをフィルタリングする

S3 インベントリレポートを受信後、レポートの内容をフィルタリングして、有効になっている S3 バケットキーを使用して暗号化されていないオブジェクトのみをリストできます。バケットのすべてのオブジェクトを、有効になっている S3 バケットキーを使用して暗号化する場合は、このステップを無視できます。ただし、この段階で S3 インベントリレポートをフィルタリングすると、有効に

なっている S3 バケットキーを使って以前に暗号化したオブジェクトを再暗号化する時間とコストが削減されます。

以下のステップは、Amazon S3 Select を使用してフィルタリングする方法を示していますが、Amazon Athena を使用することもできます。使用するツールを決定するには、S3 インベントリレポートの `manifest.json` ファイルを開きます。このファイルには、そのレポートに関連付けられているデータファイルの数がリストされます。数が多い場合は、Amazon Athena を使用してください。Amazon Athena は複数の S3 オブジェクトに対して実行されますが、S3 Select は一度に 1 つのオブジェクトに対して動作するためです。Amazon S3 と Athena を一緒に使用する方法について詳しくは、「Amazon Athena で Amazon S3 インベントリをクエリする」と、AWS ブログ投稿「Encrypting objects with Amazon S3 Batch Operations」の「Using Athena」を参照してください。

S3 Select を使用して S3 インベントリレポートをフィルタリングするには

1. インベントリレポートの `manifest.json` ファイルを開き、JSON の `fileSchema` セクションを探します。このセクションは、データに対して実行するクエリに情報を提供します。

   次の JSON は、バージョニングが有効なバケットの CSV 形式のインベントリに対する `manifest.json` ファイルの例です。インベントリレポートの設定方法に応じて、マニフェストの内容は異なる場合があります。

```
  {
    "sourceBucket": "batchoperationsdemo",
    "destinationBucket": "arn:aws:s3:::amzn-s3-demo-destination-bucket",
    "version": "2021-05-22",
    "creationTimestamp": "1558656000000",
    "fileFormat": "CSV",
    "fileSchema": "Bucket, Key, VersionId, IsLatest, IsDeleteMarker,
 BucketKeyStatus",
    "files": [
      {
        "key": "demoinv/batchoperationsdemo/DemoInventory/data/009a40e4-
f053-4c16-8c75-6100f8892202.csv.gz",
        "size": 72691,
        "MD5checksum": "c24c831717a099f0ebe4a9d1c5d3935c"
      }
    ]
  }
```

バケットでバージョニングが有効になっていない場合、または最新バージョンのレポートを実行することを選択した場合、fileSchema は、Bucket、Key、および BucketKeyStatus です。

バージョニングが有効になっている場合、インベントリレポートのセットアップ方法に応じて、fileSchema に Bucket、Key、VersionId、IsLatest、IsDeleteMarker、BucketKeyStatus が含まれる場合があります。このため、クエリを実行するときは、列 1、2、3、および 6 に注意してください。

S3 バッチオペレーションは、ジョブを実行するための入力として、検索条件のフィールド (BucketKeyStatus) に加えて、バケット、キー、およびバージョン ID を必要とします。VersionID フィールドは必要ありませんが、バージョニング対応バケットを操作するときには VersionID フィールドを指定すると便利です。詳細については、「バージョニングが有効なバケットでのオブジェクトの操作」を参照してください。

2. インベントリレポートのデータファイルを見つけます。manifest.json オブジェクトの files の下に、データファイルがリストされます。
3. S3 コンソールでデータファイルを見つけて選択したら、[Actions] (アクション) を選択し、[Query with S3 Select] (S3 Select を使用したクエリ) を選択します。
4. プリセットの [CSV]、[Comma] (カンマ)、および [GZIP] の各フィールドを選択したままにして、[Next] (次へ) を選択します。
5. 先に進む前にインベントリレポートの形式を確認するには、[Show file preview] (ファイルプレビューの表示) を選択します。
6. 参照する列を [SQL expression] (SQL 式) フィールドに入力し、[Run SQL] (SQL の実行) を選択します。次の式は、S3 バケットキー が設定されていないすべてのオブジェクトの列 1 ~ 3 を返します。

```
select s._1, s._2, s._3 from s3object s where s._6 = 'DISABLED'
```

結果の例は次のとおりです。

```
batchoperationsdemo,0100059%7Ethumb.jpg,lsrtIxksLu0R0ZkYPL.LhgD5caTYn6vu
batchoperationsdemo,0100074%7Ethumb.jpg,sd2M60g6Fdazoi6D5kNARIE7KzUibmHR
batchoperationsdemo,0100075%7Ethumb.jpg,TLYESLnl1mXD5c4BwiOIinqFrktddkoL
batchoperationsdemo,0200147%7Ethumb.jpg,amufzfMi_fEw0Rs99rxR_HrDFlE.l3Y0
batchoperationsdemo,0301420%7Ethumb.jpg,9qGU2SEscL.C.c_sK89trmXYIwooABSh
batchoperationsdemo,0401524%7Ethumb.jpg,ORnEWNuB1QhHrrYAGFsZhbyvEYJ3DUor
```

```
      batchoperationsdemo,200907200065HQ
%7Ethumb.jpg,d8LgvIVjbDR5mUVwW6pu9ahTfReyn5V4
      batchoperationsdemo,200907200076HQ
%7Ethumb.jpg,XUT25d7.gK40u_GmnupdaZg3BVx2jN40
      batchoperationsdemo,201103190002HQ
%7Ethumb.jpg,z.2sVRh0myqVi0BuIrngWlsRPQdb7qOS
```

7. 結果をダウンロードし、CSV 形式で保存し、S3 バッチオペレーションジョブのオブジェクトのリストとして Amazon S3 にアップロードします。
8. マニフェストファイルが複数ある場合は、それらに対して S3 Select を使用したクエリも実行します。結果のサイズに応じて、リストを組み合わせて単一の S3 バッチオペレーションジョブを実行することも、各リストを個別のジョブとして実行することもできます。実行するジョブ数を決定するときは、各 S3 バッチオペレーションジョブを実行する料金を考慮してください。

ステップ 3: S3 バッチオペレーションジョブをセットアップして実行する

これで、S3 オブジェクトの CSV リストがフィルタリングされたため、S3 バッチオペレーションジョブを開始して、有効になっている S3 バケットキーでオブジェクトを暗号化できます。

ジョブは、指定されるオブジェクトのリスト (マニフェスト)、実行されるオペレーション、および指定されたパラメータの総称です。有効になっている S3 バケットキーでこのオブジェクトのセットを暗号化する最も簡単な方法は、Copy オペレーションを使用し、マニフェストにリストされているオブジェクトと同じ送信先プレフィックスを指定することです。バージョン設定されていないバケットでは、このオペレーションによって既存のオブジェクトが上書きされます。バージョニングが有効になっているバケットでは、このオペレーションにより、オブジェクトの暗号化された新しいバージョンが作成されます。

オブジェクトのコピーの一環として、Amazon S3 が SSE-KMS 暗号化を使用してオブジェクトを暗号化するように指定します。このジョブはオブジェクトをコピーするため、Amazon S3 に最初に追加した日時に関係なく、完了時にすべてのオブジェクトについて更新された作成日が表示されます。また、S3 バッチオペレーションジョブの一環として、オブジェクトタグやストレージクラスなどのオブジェクトのセットの他のプロパティを指定します。

サブステップ

- IAM ポリシーをセットアップする
- バッチオペレーションの IAM ロールのセットアップ
- 既存のバケットに対して S3 バケットキーを有効にする
- バッチオペレーションジョブを作成する

- バッチオペレーションジョブを実行する

IAM ポリシーをセットアップする

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. 左のナビゲーションペインで、[ポリシー] を選択し、[ポリシーの作成] を選択します。
3. [JSON] タブを選択します。[Edit policy] (ポリシーの編集) を選択し、次のコードブロックに表示される IAM ポリシーの例を追加します。

   ポリシーの例を IAM コンソールにコピーしたら、次の項目を置き換えます。

   a. *amzn-s3-demo-source-bucket* をオブジェクトのコピー元であるソースバケットの名前に置き換えます。

   b. *amzn-s3-demo-destination-bucket* を、オブジェクトをコピーする宛先のバケットの名前に置き換えます。

   c. *amzn-s3-demo-manifest-bucket*/*manifest-key* を、マニフェストオブジェクトの名前に置き換えます。

   d. *amzn-s3-demo-completion-report-bucket* を、完了レポートを保存するバケットの名前に置き換えます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CopyObjectsToEncrypt",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:PutObjectTagging",
        "s3:PutObjectAcl",
        "s3:PutObjectVersionTagging",
        "s3:PutObjectVersionAcl",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionTagging"
```

```
        ],
        "Resource": [
          "arn:aws:s3:::amzn-s3-demo-source-bucket/*",
          "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
        ]
      },
      {
        "Sid": "ReadManifest",
        "Effect": "Allow",
        "Action": [
          "s3:GetObject",
          "s3:GetObjectVersion"
        ],
        "Resource": "arn:aws:s3:::amzn-s3-demo-manifest-bucket/manifest-key"
      },
      {
        "Sid": "WriteReport",
        "Effect": "Allow",
        "Action": [
          "s3:PutObject"
        ],
        "Resource": "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
      }
    ]
}
```

4. [Next: Tags] (次へ: タグ) を選択します。
5. 必要なタグを追加し (オプション)、[Next: Review] (次へ: 確認) を選択します。
6. ポリシー名と、オプションで説明を追加追加し、[Create Policy] (ポリシーの作成) を選択します。
7. [Review policy] (ポリシーの確認) を選択し、[Save changes] (変更の保存) を選択します。
8. S3 バッチオペレーションポリシーが完了したため、コンソールが IAM の [Policies] (ポリシー) ページに戻ります。ポリシー名をフィルタリングし、ポリシー名の左にあるボタンを選択します。次に、[Policy actions] (ポリシーアクション) を選択し、[Attach] (アタッチ) を選択します。

   新しく作成したポリシーを IAM ロールにアタッチするには、アカウントで該当するユーザー、グループ、またはロールを選択し、[Attach policy] (ポリシーのアタッチ) を選択します。これにより、IAM コンソールに戻ります。

バッチオペレーションの IAM ロールのセットアップ

1. IAM コンソールのナビゲーションペインで、[ロール]、[ロールの作成] の順に選択します。
2. [AWS のサービス]、[S3]、および [S3 バッチオペレーション] を選択します。続いて、[Next: Permissions] を選択します。
3. 先ほど作成した IAM ポリシーの名前の入力を開始します。表示されるポリシー名のチェックボックスをオンにし、[Next: Tags] (次: タグ) を選択します。
4. (オプション) この演習では、タグを追加するか、キーと値のフィールドを空白のままにします。[Next: Review] を選択します。
5. ロール名を入力し、デフォルトの説明をそのまま使用するか、独自の説明を追加します。[ロールの作成] を選択します。
6. ジョブを作成するユーザーに、次の例の権限があることを確認します。

   account-id を AWS アカウント ID に、*IAM-role-name* を後でバッチオペレーションジョブの作成ステップで作成する IAM ロールに適用する予定の名前に置き換えます。詳細については、「バッチオペレーションに対するアクセス許可の付与」を参照してください。

```
{
"Sid": "AddIamPermissions",
"Effect": "Allow",
"Action": [
"iam:GetRole",
"iam:PassRole"
],
"Resource": "arn:aws:iam::account-id:role/IAM-role-name"
}
```

既存のバケットに対して S3 バケットキーを有効にする

1. Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. [バケット] リストで、S3 バケットキーを有効にするバケットを選択します。
3. [プロパティ] を選択します。
4. [Default encryption (デフォルトの暗号化)] で、[Edit (編集)] を選択します。
5. [暗号化タイプ] で、[Amazon S3 マネージドキー (SSE-S3)] または [AWS Key Management Service キー (SSE-KMS] を選択できます。

6. [AWS Key Management Service キー (SSE-KMS)] を選択した場合は、AWS KMS key で、以下のオプションのいずれかを使用して AWS KMS キーを指定できます。

   - 使用可能な KMS キーのリストから選択するには、[AWS KMS キーから選択する] を選びます。使用可能なキーのリストから、バケットと同じリージョンの対称暗号化 KMS キーを選択します。AWS マネージドキー (aws/s3) とカスタマーマネージドキーの両方がリストに表示されます。
   - KMS キー ARN を入力するには、[AWS KMS キー ARN を入力] を選択し、表示されたフィールドに KMS キー ARN を入力します。
   - AWS KMS コンソールで新しいカスタマーマネージドキーを作成するには、[KMS キーを作成] を選択します。

7. [Bucket Key] (バケットキー) の [Enable] (有効化) を選択し、 [Save changes] (変更の保存) を選択します。

バケットレベルで S3 バケットキーが有効になったため、このバケットに対してアップロード、変更、またはコピーされたオブジェクトは、デフォルトでこの暗号化設定を継承します。これには、Amazon S3 バッチオペレーションを使用してコピーされたオブジェクトが含まれます。

バッチオペレーションジョブを作成する

1. https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開きます。
2. ナビゲーションペインで、[Batch Operations] (バッチオペレーション) を選択し、[Create Job] (ジョブの作成) を選択します。
3. オブジェクトを保存する [Region] (リージョン) を選択し、マニフェストタイプとして [CSV] を選択します。
4. パスを入力するか、前に S3 Select (または Athena) の結果から作成した CSV マニフェストファイルに移動します。マニフェストにバージョン ID が含まれている場合は、そのボックスを選択します。[Next (次へ)] を選択します。
5. [Copy] (コピー) オペレーションを選択し、コピー先バケットを選択します。サーバー側の暗号化は無効のままにできます。送信先バケットで S3 バケットキーが有効になっている限り、コピーオペレーションは送信先バケットに S3 バケットキーを適用します。
6. (オプション) 必要に応じて、ストレージクラスおよびその他のパラメータを選択します。このステップで指定するパラメータは、マニフェストにリストされているオブジェクトに対して実行されるすべてのオペレーションに適用されます。[次へ] を選択します。
7. サーバー側の暗号化を設定するには、次の手順に従います。

a. [サーバー側の暗号化] で、次のいずれかを選択します。

- Amazon S3 にオブジェクトを格納するときに、バケット設定をデフォルトのサーバー側暗号化のままにするには、[暗号化キーを指定しない] を選択します。送信先バケットで S3 バケットキーが有効になっている限り、コピーオペレーションは送信先バケットに S3 バケットキーを適用します。

> **Note**
>
> 指定された宛先のバケットポリシーで、Amazon S3 に保存する前にオブジェクトを暗号化する必要がある場合は、暗号化キーを指定する必要があります。そうしないと、宛先へのオブジェクトのコピーが失敗します。

- オブジェクトを Amazon S3 に保存する前に暗号化するには、[暗号化キーを指定する] を選択します。

b. [暗号化設定] で [暗号化キーを指定する]] を選択した場合は、[デフォルトの暗号化に送信先バケット設定を使用する] または [デフォルトの暗号化の送信先バケット設定を上書きする]を選択する必要があります。

c. [デフォルトの暗号化に送信先バケット設定を使用する] を選択した場合は、次の暗号化設定を設定する必要があります。

i. [暗号化タイプ] で、[Amazon S3 マネージドキー (SSE-S3)] または [AWS Key Management Service キー (SSE-KMS)] を選択する必要があります。SSE-S3 は、最強のブロック暗号の 1 つである 256 ビットの 高度暗号化規格 (AES-256) を使用して、各オブジェクトを暗号化します。SSE-KMS を使用すると、キーをより細かく制御できます。詳細については、「Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3)」および「AWS KMS キーによるサーバー側の暗号化 (SSE-KMS) の使用」を参照してください。

ii. [AWS Key Management Service キー (SSE-KMS)] を選択した場合は、AWS KMS key で、以下のオプションのいずれかを使用して AWS KMS key を指定できます。

- 使用可能な KMS キーのリストから選択するには、[AWS KMS keys から選択する] を選択し、次に、バケットと同じリージョンの対称暗号化 KMS キーを選択します。AWS マネージドキー (aws/s3) とカスタマーマネージドキーの両方がリストに表示されます。

- KMS キー ARN を入力するには、[AWS KMS キー ARN を入力] を選択し、表示されるフィールドに KMS キー ARN を入力します。
- AWS KMS コンソールで新しいカスタマーマネージドキーを作成するには、[KMS キーを作成] を選択します。

iii. [バケットキー] で [有効化] を選択します。コピーオペレーションでは、送信先バケットに、S3 バケットキーが適用されます。

8. ジョブに説明を付け (またはデフォルトのままにし)、その優先順位レベルを設定し、レポートタイプを選択して、[Path to completion report destination] (完了レポートの送信先へのパス) を指定します。
9. [Permissions] (アクセス権限) セクションで、前に定義したバッチオペレーションの IAM ロールを選択するようにしてください。[Next (次へ)] を選択します。
10. [Review] (確認) で、設定を確認します。変更が必要な場合は、[Previous] (前へ) を選択します。バッチオペレーションの設定を確認したら、[Create job] (ジョブの作成) を選択します。

    詳細については、「S3 バッチオペレーションジョブの作成」を参照してください。

バッチオペレーションジョブを実行する

セットアップウィザードによって、Amazon S3 コンソールの S3 バッチオペレーションセクションに自動的に戻ります。S3 がプロセスを開始すると、新しいジョブが [New] (新規) 状態から [Preparing] (準備中) 状態に遷移します。[Preparing] (準備中) 状態の間、S3 はジョブのマニフェストを読み取り、エラーをチェックし、オブジェクトの数を計算します。

1. 進行状況を確認するには、Amazon S3 コンソールの [Refresh] (更新) ボタンを選択します。マニフェストのサイズによっては、読み取りに数分または数時間かかることがあります。
2. S3 がジョブのマニフェストの読み取りを終了すると、ジョブは [Awaiting your confirmation] (確認待ち) 状態に移行します。ジョブ ID の左にあるオプションボタンを選択し、[Run job] (ジョブの実行) を選択します。
3. ジョブの設定を確認し、右下隅の [Run job] (ジョブの実行) を選択します。

    ジョブの実行が開始したら、[refresh] (更新) ボタンを選択してコンソールのダッシュボードビューで、または特定のジョブを選択して、進行状況を確認できます。
4. ジョブが完了したら、[Successful] (成功) と [Failed] (失敗) のオブジェクト数を表示して、すべてが予期したとおりに実行されたことを確認できます。ジョブレポートを有効にした場合は、ジョブレポートで、失敗したオペレーションの正確な原因を確認します。

これらのステップは、AWS CLI、AWS SDK、または Amazon S3 REST API を使用して実行することもできます。ジョブのステータスと完了レポートの追跡については、ジョブステータスと完了レポートの追跡 を参照してください。

AWS CLI および AWS SDK for Java を使用したタグによるコピーオペレーションの例については、ラベル付けに使用されるジョブタグを使用したバッチ操作ジョブの作成 を参照してください。

AWS Lambda 関数の呼び出し

Amazon S3 バッチオペレーションを使用すると、Amazon S3 のオブジェクトに対して大規模なバッチオペレーションを実行できます。AWS Lambda の呼び出し関数バッチオペレーションは、AWS Lambda 関数を開始し、マニフェストにリストされているオブジェクトに対してカスタムアクションを実行します。このセクションでは、S3 バッチ操作で使用する Lambda 関数とその関数を呼び出すジョブを作成する方法について説明します。S3 バッチ操作ジョブでは、`LambdaInvoke` オペレーションを使用して、マニフェストにリストされているすべてのオブジェクトに対して Lambda 関数を実行します。

Amazon S3 コンソール、AWS Command Line Interface (AWS CLI)、AWS SDK、または Amazon S3 REST API を使用して S3 バッチオペレーションを扱うことができます。Lambda の使用について詳しくは、AWS Lambda 開発者ガイドのAWS Lambda の使用を開始するを参照してください。

以下のセクションでは、S3 バッチ操作で Lambda を使用する方法について説明します。

トピック

- バッチオペレーションで Lambda を使用する
- S3 バッチ操作で使用する Lambda 関数の作成
- Lambda 関数を呼び出す S3 バッチ操作のジョブの作成
- Lambda のマニフェストでのタスクレベルの情報の指定
- S3 バッチ操作のチュートリアル

バッチオペレーションで Lambda を使用する

S3 バッチ操作で AWS Lambda を使用するときは、S3 バッチ操作で使用するための Lambda 関数を新しく作成する必要があります。既存の Amazon S3 のイベントベースの関数を S3 バッチ操作で再利用することはできません。イベント関数はメッセージの受信のみ可能です。メッセージを返すことはできません。S3 バッチ操作で使用する Lambda 関数では、メッセージを受け取って返す必要があ

ります。Amazon S3 のイベントで Lambda を使用する方法について詳しくは、AWS Lambda 開発者ガイドのAWS Lambda を Amazon S3 に使用するを参照してください。

Lambda 関数を呼び出す S3 バッチ操作のジョブを作成します。このジョブは、マニフェストにリストされているすべてのオブジェクトに対して同じ Lambda 関数を実行します。マニフェストのオブジェクトの処理時に使用する Lambda 関数のバージョンは指定できます。S3 バッチ操作では、非修飾 Amazon リソースネーム (ARN)、エイリアス、特定のバージョンがサポートされています。詳しくは、AWS Lambda 開発者ガイドのAWS Lambda 関数のバージョンを参照してください。

S3 バッチ操作のジョブにエイリアスまたは $LATEST 修飾子を使用する関数の ARN を指定し、それらのいずれかが指すバージョンを更新すると、S3 バッチ操作は新しいバージョンの Lambda 関数を呼び出します。これは、大規模なジョブで機能の一部を更新する場合に役立ちます。S3 バッチオペレーションで使用するバージョンを変更したくない場合は、ジョブの作成時に `FunctionARN` パラメータで特定のバージョンを指定します。

1 つの S3 バッチオペレーションを使用する AWS Lambda ジョブで、最大 200 億個のオブジェクトを持つマニフェストをサポートできます。

ディレクトリバケットで Lambda とバッチオペレーションを使用する

ディレクトリバケットは Amazon S3 バケットタイプの1 つであり、一貫して 1 桁ミリ秒のレイテンシーに維持する必要があるワークロードまたはパフォーマンス重視のアプリケーション向けに設計されています。詳細については、「ディレクトリバケット」を参照してください。

バッチオペレーションを使用してディレクトリバケットで動作する Lambda 関数を呼び出すには、独自の要件があります。例えば、更新された JSON スキーマを使用して Lambda リクエストを構築し、ジョブを作成する際に InvocationSchemaVersion 2.0 (1.0 ではない) を指定する必要があります。この更新されたスキーマでは、UserArguments にオプションのキーバリューペアを指定できます。これを使用して、既存の Lambda 関数の特定のパラメータを変更できます。詳細については、「AWS ストレージブログ」の「Automate object processing in Amazon S3 directory buckets with S3 Batch Operations and AWS Lambda」を参照してください。

レスポンスと結果のコード

S3 バッチオペレーションは、それぞれに `TaskID` が関連付けられている 1 つ以上のキーを使用して Lambda 関数を呼び出します。S3 バッチオペレーションには、Lambda 関数からのキーごとの結果コードが必要です。キーごとの結果コードで返されないタスク ID は、リクエストコードで返され、`treatMissingKeysAs` フィールドの結果コードが付与されます。`treatMissingKeysAs` はオプションのリクエストフィールドで、デフォルトは `TemporaryFailure` です。次の表に、`treatMissingKeysAs` フィールドの他の有効な結果コードと値を示します。

Response Code (レスポンスコード)	説明
`Succeeded`	タスクは正常に完了しました。ジョブ完了レポートをリクエストした場合は、タスクの結果の文字列がレポートに含まれます。
`TemporaryFailure`	タスクは一時的に失敗し、ジョブが完了する前に再始動されます。結果の文字列は無視されます。最終的な再処理である場合は、エラーメッセージが最終レポートに含まれます。
`PermanentFailure`	タスクに固定障害が発生しました。ジョブ完了レポートをリクエストした場合、タスクは `Failed` としてマークされ、エラーメッセージの文字列が含まれます。失敗したタスクの結果の文字列は無視されます。

S3 バッチ操作で使用する Lambda 関数の作成

このセクションでは、Lambda 関数で使用する必要のある AWS Identity and Access Management (IAM) アクセス許可の例について説明します。また、S3 バッチ操作で使用する Lambda 関数の例も示します。Lambda 関数を作成したことがない場合は、AWS Lambda 開発者ガイドのチュートリアル: Amazon S3 トリガーを使用して AWS Lambda 関数を呼び出すを参照してください。

S3 バッチ操作で使用するための Lambda 関数を作成する必要があります。既存の Amazon S3 イベントベースの Lambda 関数を再利用することはできません。これは、S3 バッチオペレーションで使用する Lambda 関数では、特別なデータフィールドを受け取って返す必要があるためです。

> **Important**
>
> Java で記述された AWS Lambda 関数は、RequestHandler または RequestStreamHandler ハンドラーインターフェイスのいずれかを受け入れます。ただし、S3 バッチ操作のリクエストとレスポンスの形式をサポートするため、リクエストとレスポンスのカスタムのシリアル化と逆シリアル化のために AWS Lambda は `RequestStreamHandler` インターフェイスを必要とします。このインターフェイスにより、Lambda は Java の `handleRequest` メソッドに InputStream と OutputStream ストリームを渡すことができます。
> S3 バッチ操作で Lambda 関数を使用する場合は、必ず `RequestStreamHandler` インターフェイスを使用してください。`RequestHandler` インターフェイスを使用すると、バッチ

ジョブが失敗し、完了レポートに「Invalid JSON returned in Lambda payload」と表示されます。
詳しくは、AWS Lambda ユーザーガイドのハンドラーのインターフェイスを参照してください。

IAM アクセス許可の例

S3 バッチ操作で Lambda 関数を使用するために必要な IAM アクセス許可の例を以下に示します。

Example - S3 バッチ操作の信頼ポリシー

以下は、バッチ操作の IAM ロールに使用できる信頼ポリシーの例です。この IAM ロールは、ジョブを作成して、バッチ操作に IAM ロールを引き受けるアクセス許可を付与する場合に指定します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "batchoperations.s3.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Example - Lambda の IAM ポリシー

以下は、S3 バッチ操作に Lambda 関数を呼び出して入力のマニフェストを読み取るアクセス許可を与える IAM ポリシーの例です。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "BatchOperationsLambdaPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion",
```

```
                "s3:PutObject",
                "lambda:InvokeFunction"
            ],
            "Resource": "*"
        }
    ]
}
```

リクエストとレスポンスの例

このセクションでは、Lambda 関数のリクエストとレスポンスの例を示します。

Example リクエスト

以下は、Lambda 関数のリクエストの JSON の例です。

```
{
    "invocationSchemaVersion": "1.0",
    "invocationId": "YXNkbGZqYWRmaiBhc2RmdW9hZHNmZGpmaGFzbGtkaGZza2RmaAo",
    "job": {
        "id": "f3cc4f60-61f6-4a2b-8a21-d07600c373ce"
    },
    "tasks": [
        {
            "taskId": "dGFza2lkZ29lc2hlcmUK",
            "s3Key": "customerImage1.jpg",
            "s3VersionId": "1",
            "s3BucketArn": "arn:aws:s3:us-east-1:0123456788:amzn-s3-demo-bucket1"
        }
    ]
}
```

Example レスポンス

以下は、Lambda 関数のレスポンスの JSON の例です。

```
{
  "invocationSchemaVersion": "1.0",
  "treatMissingKeysAs" : "PermanentFailure",
  "invocationId" : "YXNkbGZqYWRmaiBhc2RmdW9hZHNmZGpmaGFzbGtkaGZza2RmaAo",
  "results": [
    {
      "taskId": "dGFza2lkZ29lc2hlcmUK",
      "resultCode": "Succeeded",
```

```
      "resultString": "[\"Mary Major", \"John Stiles\"]"
    }
  ]
}
```

S3 バッチ操作の Lambda 関数の例

次の Python Lambda の例では、バージョン管理されたオブジェクトから削除マーカーを削除します。

例に示すように、S3 バッチ操作のキーは URL エンコードされます。Amazon S3 を他の AWS のサービスとともに使用するには、S3 バッチ操作から渡されたキーを URL デコードすることが重要です。

```
import logging
from urllib import parse
import boto3
from botocore.exceptions import ClientError

logger = logging.getLogger(__name__)
logger.setLevel("INFO")

s3 = boto3.client("s3")


def lambda_handler(event, context):
    """
    Removes a delete marker from the specified versioned object.

    :param event: The S3 batch event that contains the ID of the delete marker
                  to remove.
    :param context: Context about the event.
    :return: A result structure that Amazon S3 uses to interpret the result of the
             operation. When the result code is TemporaryFailure, S3 retries the
             operation.
    """
    # Parse job parameters from Amazon S3 batch operations
    invocation_id = event["invocationId"]
    invocation_schema_version = event["invocationSchemaVersion"]

    results = []
    result_code = None
    result_string = None
```

```
    task = event["tasks"][0]
    task_id = task["taskId"]

    try:
        obj_key = parse.unquote(task["s3Key"], encoding="utf-8")
        obj_version_id = task["s3VersionId"]
        bucket_name = task["s3BucketArn"].split(":")[-1]

        logger.info(
            "Got task: remove delete marker %s from object %s.", obj_version_id,
obj_key
        )

        try:
            # If this call does not raise an error, the object version is not a delete
            # marker and should not be deleted.
            response = s3.head_object(
                Bucket=bucket_name, Key=obj_key, VersionId=obj_version_id
            )
            result_code = "PermanentFailure"
            result_string = (
                f"Object {obj_key}, ID {obj_version_id} is not " f"a delete marker."
            )

            logger.debug(response)
            logger.warning(result_string)
        except ClientError as error:
            delete_marker = error.response["ResponseMetadata"]["HTTPHeaders"].get(
                "x-amz-delete-marker", "false"
            )
            if delete_marker == "true":
                logger.info(
                    "Object %s, version %s is a delete marker.", obj_key,
obj_version_id
                )
                try:
                    s3.delete_object(
                        Bucket=bucket_name, Key=obj_key, VersionId=obj_version_id
                    )
                    result_code = "Succeeded"
                    result_string = (
                        f"Successfully removed delete marker "
                        f"{obj_version_id} from object {obj_key}."
```

```
                    )
                    logger.info(result_string)
                except ClientError as error:
                    # Mark request timeout as a temporary failure so it will be
retried.
                    if error.response["Error"]["Code"] == "RequestTimeout":
                        result_code = "TemporaryFailure"
                        result_string = (
                            f"Attempt to remove delete marker from  "
                            f"object {obj_key} timed out."
                        )
                        logger.info(result_string)
                    else:
                        raise
            else:
                raise ValueError(
                    f"The x-amz-delete-marker header is either not "
                    f"present or is not 'true'."
                )
    except Exception as error:
        # Mark all other exceptions as permanent failures.
        result_code = "PermanentFailure"
        result_string = str(error)
        logger.exception(error)
    finally:
        results.append(
            {
                "taskId": task_id,
                "resultCode": result_code,
                "resultString": result_string,
            }
        )
    return {
        "invocationSchemaVersion": invocation_schema_version,
        "treatMissingKeysAs": "PermanentFailure",
        "invocationId": invocation_id,
        "results": results,
    }
```

Lambda 関数を呼び出す S3 バッチ操作のジョブの作成

Lambda 関数を呼び出す S3 バッチ操作のジョブを作成する場合は、以下を指定する必要があります。

- Lambda 関数の ARN (関数のエイリアスまたは特定のバージョン番号を含む)
- 関数を呼び出すアクセス許可を持つ IAM ロール
- アクションパラメータ `LambdaInvokeFunction`

S3 バッチ操作のジョブの作成の詳細については、「S3 バッチオペレーションジョブの作成」および「S3 バッチ操作でサポートされるオペレーション」を参照してください。

次の例では、AWS CLI を使用して Lambda 関数を呼び出す S3 バッチオペレーションのジョブを作成します。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3control create-job
    --account-id account-id
    --operation  '{"LambdaInvoke": { "FunctionArn": "arn:aws:lambda:region:account-
id:function:LambdaFunctionName" } }'
    --manifest '{"Spec":{"Format":"S3BatchOperations_CSV_20180820","Fields":
["Bucket","Key"]},"Location":{"ObjectArn":"arn:aws:s3:::amzn-s3-demo-manifest-
bucket","ETag":"ManifestETag"}}'
    --report '{"Bucket":"arn:aws:s3:::amzn-s3-demo-
bucket","Format":"Report_CSV_20180820","Enabled":true,"Prefix":"ReportPrefix","ReportScope":"Al
    --priority 2
    --role-arn arn:aws:iam::account-id:role/BatchOperationsRole
    --region region
    --description "Lambda Function"
```

Lambda のマニフェストでのタスクレベルの情報の指定

S3 バッチオペレーションで AWS Lambda 関数を使用する際、操作対象の各タスク/キーに付随する追加データが必要になる場合があります。例えば、ソースオブジェクトキーと新しいオブジェクトキーの両方を提供したい場合があります。Lambda 関数は、元のキーを新しい名前で新しい S3 バケットにコピーできます。デフォルトでは、バッチオペレーションでは、ジョブへの入力マニフェストで移行先バケットとソースキーのリストのみを指定できます。以下の例では、マニフェストにデータを追加して、より複雑な Lambda 関数を実行する方法について説明します。

S3 バッチ操作のマニフェストでキーごとのパラメータを指定して Lambda 関数のコードで使用するには、以下に示すように URL エンコードされた形式の JSON を使用します。key フィールドは、Amazon S3 のオブジェクトのキーのように Lambda 関数に渡されます。ただし、以下の例に示すように、Lambda 関数で他の値や複数のキーを含めるように解釈することができます。

> **Note**
>
> マニフェストの key フィールドの最大文字数は 1,024 文字です。

Example - 「Amazon S3 のキー」を JSON の文字列に置き換える前のマニフェスト

URL エンコードされたバージョンを、S3 バッチ操作に渡す必要があります。

```
amzn-s3-demo-bucket,{"origKey": "object1key", "newKey": "newObject1Key"}
amzn-s3-demo-bucket,{"origKey": "object2key", "newKey": "newObject2Key"}
amzn-s3-demo-bucket,{"origKey": "object3key", "newKey": "newObject3Key"}
```

Example - URL エンコードされたマニフェスト

この URL エンコードされたバージョンを、S3 バッチ操作に渡す必要があります。URL エンコードされていないバージョンは機能しません。

```
amzn-s3-demo-bucket,%7B%22origKey%22%3A%20%22object1key%22%2C%20%22newKey%22%3A
%20%22newObject1Key%22%7D
amzn-s3-demo-bucket,%7B%22origKey%22%3A%20%22object2key%22%2C%20%22newKey%22%3A
%20%22newObject2Key%22%7D
amzn-s3-demo-bucket,%7B%22origKey%22%3A%20%22object3key%22%2C%20%22newKey%22%3A
%20%22newObject3Key%22%7D
```

Example - Lambda 関数とジョブのレポートに結果が書き込まれるマニフェストの形式

この URL エンコードされたマニフェストの例には、解析する次の Lambda 関数のパイプ区切りオブジェクトキーが含まれています。

```
amzn-s3-demo-bucket,object1key%7Clower
amzn-s3-demo-bucket,object2key%7Cupper
amzn-s3-demo-bucket,object3key%7Creverse
amzn-s3-demo-bucket,object4key%7Cdelete
```

この Lambda 関数は、パイプ区切りのタスクをエンコードされた S3 バッチオペレーションのマニフェストに解析する方法を示しています。タスクは、指定されたオブジェクトに適用されているリビジョンオペレーションを示します。

```
import logging
from urllib import parse
import boto3
from botocore.exceptions import ClientError

logger = logging.getLogger(__name__)
logger.setLevel("INFO")

s3 = boto3.resource("s3")


def lambda_handler(event, context):
    """
    Applies the specified revision to the specified object.

    :param event: The Amazon S3 batch event that contains the ID of the object to
                  revise and the revision type to apply.
    :param context: Context about the event.
    :return: A result structure that Amazon S3 uses to interpret the result of the
             operation.
    """
    # Parse job parameters from Amazon S3 batch operations
    invocation_id = event["invocationId"]
    invocation_schema_version = event["invocationSchemaVersion"]

    results = []
    result_code = None
    result_string = None

    task = event["tasks"][0]
    task_id = task["taskId"]
    # The revision type is packed with the object key as a pipe-delimited string.
    obj_key, revision = parse.unquote(task["s3Key"], encoding="utf-8").split("|")
    bucket_name = task["s3BucketArn"].split(":")[-1]

    logger.info("Got task: apply revision %s to %s.", revision, obj_key)

    try:
        stanza_obj = s3.Bucket(bucket_name).Object(obj_key)
```

```
            stanza = stanza_obj.get()["Body"].read().decode("utf-8")
            if revision == "lower":
                stanza = stanza.lower()
            elif revision == "upper":
                stanza = stanza.upper()
            elif revision == "reverse":
                stanza = stanza[::-1]
            elif revision == "delete":
                pass
            else:
                raise TypeError(f"Can't handle revision type '{revision}'.")

            if revision == "delete":
                stanza_obj.delete()
                result_string = f"Deleted stanza {stanza_obj.key}."
            else:
                stanza_obj.put(Body=bytes(stanza, "utf-8"))
                result_string = (
                    f"Applied revision type '{revision}' to " f"stanza {stanza_obj.key}."
                )

            logger.info(result_string)
            result_code = "Succeeded"
        except ClientError as error:
            if error.response["Error"]["Code"] == "NoSuchKey":
                result_code = "Succeeded"
                result_string = (
                    f"Stanza {obj_key} not found, assuming it was deleted "
                    f"in an earlier revision."
                )
                logger.info(result_string)
            else:
                result_code = "PermanentFailure"
                result_string = (
                    f"Got exception when applying revision type '{revision}' "
                    f"to {obj_key}: {error}."
                )
                logger.exception(result_string)
        finally:
            results.append(
                {
                    "taskId": task_id,
                    "resultCode": result_code,
                    "resultString": result_string,
```

```
            }
        )
    return {
        "invocationSchemaVersion": invocation_schema_version,
        "treatMissingKeysAs": "PermanentFailure",
        "invocationId": invocation_id,
        "results": results,
    }
```

S3 バッチ操作のチュートリアル

次のチュートリアルでは、Lambda を使用したいくつかのバッチ操作タスクにおけるエンドツーエンドの一連の手順について説明します。このチュートリアルでは、S3 ソースバケットに保存された動画のバッチトランスコーディング用に Lambda 関数を呼び出すようにバッチオペレーションを設定する方法を学習します。Lambda 関数は AWS Elemental MediaConvert を呼び出して、動画をトランスコードします。

- チュートリアル: S3 バッチオペレーションを使用した動画のバッチトランスコーディング

すべてのオブジェクトタグを置換する

Amazon S3 バッチオペレーションを使用すると、Amazon S3 のオブジェクトに対して大規模なバッチオペレーションを実行できます。[すべてのオブジェクトタグを置換する] オペレーションは、マニフェストにリストされているすべてのオブジェクトのオブジェクトタグを置き換えます。 オブジェクトタグは、オブジェクトのメタデータを保存するために使用できる文字列のキー値ペアです。

[すべてのオブジェクトタグを置換する] ジョブを作成するには、適用するタグのセットを指定します。S3 バッチ操作では、すべてのオブジェクトに同じタグセットが適用されます。指定したタグのセットは、マニフェストのオブジェクトに既に関連付けられているすべてのタグのセットを置き換えます。S3 バッチオペレーションでは、既存のタグを保持したままのオブジェクトへのタグの追加はサポートされていません。

マニフェスト内のオブジェクトがバージョニング対応のバケット内にある場合は、タグセットを適用してすべてのオブジェクトのバージョンを指定することができます。そのためには、マニフェストですべてのオブジェクトにバージョン ID を指定します。オブジェクトのバージョン ID を含めない

場合、S3 バッチオペレーションはすべてのオブジェクトの最新バージョンにタグセットを適用します。バッチ操作マニフェストの詳細については、「マニフェストの指定」をご参照ください。

オブジェクトのタグ付けの詳細については、このガイドの「タグを使用してストレージを分類する」および「Amazon Simple Storage Service API リファレンス」の「PutObjectTagging」、「GetObjectTagging」、「DeleteObjectTagging」を参照してください。

コンソールを使用して [すべてのオブジェクトタグを置換する] ジョブを作成するには、「S3 バッチオペレーションジョブの作成」を参照してください。

制約と制限

バッチオペレーションを使用してオブジェクトタグを置き換える場合、以下の制約と制限が適用されます。

- バッチオペレーションジョブを実行するために指定する AWS Identity and Access Management IAM ロールには、基になる `PutObjectTagging` オペレーションを実行するための許可が必要です。必要なアクセス許可の詳細については、「Amazon Simple Storage Service API リファレンス」の「PutObjectTagging」を参照してください。
- S3 バッチオペレーションは、Amazon S3 の PutObjectTagging オペレーションを使用して、タグをマニフェストの各オブジェクトに適用します。基になるオペレーションに適用されるすべての制約と制限は、S3 バッチ操作ジョブにも適用されます。
- 1 つのすべてのオブジェクトタグの置換ジョブで、最大 200 億個のオブジェクトを持つマニフェストをサポートできます。

すべてのオブジェクトタグを削除する

Amazon S3 バッチオペレーションを使用すると、Amazon S3 のオブジェクトに対して大規模なバッチオペレーションを実行できます。すべてのオブジェクトタグの削除のオペレーションは、マニフェストにリストされているオブジェクトに現在関連付けられているすべての Amazon S3 オブジェクトタグセットを削除します。S3 バッチオペレーションでは、他のタグを維持したままオブジェクトからタグを削除することはできません。

マニフェスト内のオブジェクトがバージョニングされたバケットにある場合は、オブジェクトの特定のバージョンからタグセットを削除できます。これを実行するには、マニフェストですべてのオブジェクトにバージョン ID を指定する必要があります。オブジェクトのバージョン ID を含めない場合、S3 バッチ操作はすべてのオブジェクトの最新バージョンからタグセットを削除します。バッチ操作マニフェストの詳細については、「マニフェストの指定」をご参照ください。

オブジェクトのタグ付けの詳細については、このガイドの「タグを使用してストレージを分類する」および「Amazon Simple Storage Service API リファレンス」の「PutObjectTagging」、「GetObjectTagging」、「DeleteObjectTagging」を参照してください。

> **Warning**
>
> このジョブを実行すると、マニフェストにリストされているすべてのオブジェクトのすべてのオブジェクトタグセットが削除されます。

コンソールを使用して [すべてのオブジェクトタグを削除する] ジョブを作成するには、「S3 バッチオペレーションジョブの作成」を参照してください。

制約と制限

バッチオペレーションを使用してオブジェクトタグを削除する場合、以下の制約と制限が適用されます。

- ジョブを実行するために指定する AWS Identity and Access Management (IAM) ロールには、基になる Amazon S3 の `DeleteObjectTagging` オペレーションを実行するためのアクセス権限が必要です。詳細については、「Amazon Simple Storage Service API リファレンス」の「DeleteObjectTagging」を参照してください。
- S3 バッチオペレーションは、Amazon S3 DeleteObjectTagging オペレーションを使用して、マニフェスト内のすべてのオブジェクトからタグセットを削除します。基になるオペレーションに適用されるすべての制約と制限は、S3 バッチ操作ジョブにも適用されます。
- 1 つのオブジェクト削除タグ付けジョブで、最大 200 億個のオブジェクトを持つマニフェストをサポートできます。

アクセスコントロールリスト (ACL) を置き換える

Amazon S3 バッチオペレーションを使用すると、Amazon S3 のオブジェクトに対して大規模なバッチオペレーションを実行できます。[アクセスコントロールリスト (ACL) を置き換える] オペレーションは、マニフェストにリストされているすべてのオブジェクトのアクセスコントロールリスト (ACL) を置き換えます。ACL を使用すると、オブジェクトにアクセスできる人物およびその人物が実行できるアクションを定義できます。

> **Note**
>
> Amazon S3 の最新のユースケースの大部分では ACL を使用する必要がなくなっています。オブジェクトごとに個別に制御する必要がある通常ではない状況を除き、ACL は無効にしておくことをお勧めします。ACL を無効にすると、誰がオブジェクトをバケットにアップロードしたかに関係なく、ポリシーを使用してバケット内のすべてのオブジェクトへのアクセスを制御できます。詳細については、「オブジェクトの所有権の制御とバケットの ACL の無効化。」を参照してください。

S3 バッチオペレーションでは、ユーザー定義のカスタム ACL と、Amazon S3 で提供されている一連のアクセス許可が事前定義された既定の ACL がサポートされています。

マニフェスト内のオブジェクトがバージョニング対応のバケット内にある場合は、ACL を適用してすべてのオブジェクトのバージョンを指定することができます。そのためには、マニフェストですべてのオブジェクトにバージョン ID を指定します。オブジェクトのバージョン ID を含めない場合、S3 バッチオペレーションはオブジェクトの最新バージョンに ACL を適用します。

Amazon S3 の ACL の詳細については、「アクセスコントロールリスト (ACL) の概要」を参照してください。

S3 ブロックパブリックアクセス

バケット内のすべてのオブジェクトに対するパブリックアクセスを制限する場合は、S3 バッチオペレーションではなく、Amazon S3 パブリックアクセスブロックを使用して ACL を適用することをお勧めします。パブリックアクセスブロックは、素早く効果を発揮する単一の簡単なオペレーションを使用して、バケットごとあるいは全アカウントベースでパブリックアクセスを制限することができます。Amazon S3 パブリックアクセスブロックは、バケットあるいはアカウント内のすべてのオブジェクトに対するパブリックアクセスを制限することが目的の場合には、最適な選択肢となります。S3 バッチオペレーションは、マニフェストのすべてのオブジェクトにカスタム ACL を適用する必要がある場合にのみ使用します。S3 ブロックパブリックアクセスについての詳細は、Amazon S3 ストレージへのパブリックアクセスのブロック を参照してください。

S3 オブジェクトの所有権

マニフェスト内のオブジェクトがバケット内にあり、オブジェクト所有者に [バケット所有者の強制] 設定を使用している場合、[アクセスコントロールリスト (ACL) を置き換える] オペレーションでは、バケット所有者に完全な制御を許可するオブジェクト ACL のみを指定できます。この場合、[アクセスコントロールリスト (ACL) を置き換える] オペレーションは、他の AWS アカウントまたは グルー

プにオブジェクト ACL アクセス許可を付与できません。詳細については、「オブジェクトの所有権の制御とバケットの ACL の無効化。」を参照してください。

制約と制限

バッチオペレーションを使用して ACL を置き換える場合、以下の制約と制限が適用されます。

- [アクセスコントロールリスト (ACL) を置き換える] ジョブを実行するために指定する AWS Identity and Access Management (IAM) ロールには、基になる Amazon S3 `PutObjectAcl` オペレーションを実行するための許可が必要です。必要なアクセス許可の詳細については、Amazon Simple Storage Service API リファレンスの「PutObjectAcl」を参照してください。
- S3 バッチ操作は、Amazon S3 の `PutObjectAcl` オペレーションを使用して、指定した ACL をマニフェストのすべてのオブジェクトに適用します。したがって、基になる `PutObjectAcl` オペレーションに適用されるすべての制約と制限は、S3 バッチオペレーションの [アクセスコントロールリスト (ACL) を置き換える] ジョブにも適用されます。
- 1 つのアクセスコントロールリスト置き換えるジョブで、最大 200 億個のオブジェクトを持つマニフェストをサポートできます。

バッチオペレーションを使ってオブジェクトを復元する

Amazon S3 バッチオペレーションを使用すると、Amazon S3 のオブジェクトに対して大規模なバッチオペレーションを実行できます。Restore オペレーションは、マニフェストにリストされた、アーカイブされた Amazon S3 オブジェクトの復元リクエストを開始します。次のアーカイブされたオブジェクトは、リアルタイムでアクセスする前に、復元される必要があります。

- S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive ストレージクラスにアーカイブされたオブジェクト
- Archive アクセス階層または Deep Archive アクセス階層の S3 Intelligent-Tiering ストレージクラスを介してアーカイブされたオブジェクト

S3 バッチオペレーションジョブで [復元] (S3InitiateRestoreObjectOperation) オペレーションを使用すると、マニフェストで指定されたすべてのオブジェクトの `RestoreObject` リクエストが生成されます。

> **Important**
>
> [復元] ジョブでは、オブジェクトの復元リクエストのみを開始します。S3 バッチ操作では、各オブジェクトに対するリクエストが開始されると、そのオブジェクトのジョブは完了とし

てレポートされます。Amazon S3 では、ジョブを更新したり、オブジェクトが復元されたときに通知したりすることはありません。ただし、S3 イベント通知を使用して、Amazon S3 でオブジェクトが利用可能になったときに通知を受けることはできます。詳細については、「Amazon S3 イベント通知」を参照してください。

[復元] ジョブを作成する場合、次の引数を使用できます。

ExpirationInDays

この引数は、S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive オブジェクトが Amazon S3 で使用できる期間を指定します。S3 Glacier Flexible Retrieval オブジェクトと S3 Glacier Deep Archive オブジェクトをターゲットとする [復元] ジョブには、`ExpirationInDays` を 1 以上に設定する必要があります。

> **Important**
>
> S3 Intelligent-Tiering Archive Access および Deep Archive アクセス階層オブジェクトをターゲットとする [復元] オペレーションの作成時には `ExpirationInDays` を設定しないでください。S3 Intelligent-Tiering Archive Access 階層のオブジェクトは復元の有効期限の対象にならないため、`ExpirationInDays` を指定すると `RestoreObject` リクエストが失敗します。

GlacierJobTier

Amazon S3 では、`EXPEDITED`、`STANDARD`、および `BULK` の 3 つの異なる取得階層のいずれかを使用してオブジェクトを復元できます。ただし、S3 バッチ操作機能は、`STANDARD` および `BULK` の取得階層のみをサポートします。取得階層間の相違点の詳細については、「アーカイブ取得オプションを理解する」を参照してください。

各レベルの料金の詳細については、[Amazon S3 の料金] ページの「リクエストとデータ取り出し」セクションをご参照ください。

S3 Glacier と S3 Intelligent-Tiering からの復元の違い

S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive ストレージクラスからのアーカイブファイルの復元は、Archive アクセス階層または Deep Archive アクセス階層の S3 Intelligent-Tiering ストレージクラスからのファイルの復元とは異なります。

- S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive から復元すると、オブジェクトの一時コピーが作成されます。Amazon S3 は、`ExpirationInDays` 引数で指定した値が経過した後、このコピーを削除します。この一時コピーが削除された後にそのオブジェクトにアクセスするには、追加の復元リクエストを送信する必要があります。
- アーカイブされた S3 Intelligent-Tiering オブジェクトを復元するときは、`ExpirationInDays` 引数を指定しないでください。S3 Intelligent-Tiering Archive アクセス階層または Deep Archive アクセス階層からオブジェクトを復元すると、オブジェクトは S3 Intelligent-Tiering Frequent アクセス階層に戻ります。オブジェクトは、90 日以上連続でアクセスされないと、Archive Access 階層に自動的に移行します。オブジェクトは、180 日以上連続でアクセスされないと、Deep Archive Access 階層に自動的に移行します。
- バッチ操作ジョブは、S3 Glacier Flexible Retrieval および S3 Glacier Deep Archive ストレージクラスオブジェクト、または S3 Intelligent-Tiering Archive Access および Deep Archive Access ストレージ階層オブジェクトのいずれかで操作できます。バッチオペレーションは、同じジョブ内の両方のタイプのアーカイブオブジェクトに対して操作できません。両方のタイプのオブジェクトを復元するには、別個のバッチ操作ジョブを作成する必要があります。

復元の重複

既に復元中のオブジェクトに対して S3InitiateRestoreObjectOperation ジョブを実行しようとすると、S3 バッチオペレーションは次のように処理します。

次のいずれかの条件が true の場合には、オブジェクトに対するこの復元オペレーションは成功します。

- 進行中の復元リクエストと比較して、このジョブの `ExpirationInDays` 値が同じであり、また、`GlacierJobTier` 値が高速であること。
- 以前の復元リクエストが完了済みであり、オブジェクトが現在利用可能であること。この場合、バッチ操作は、復元されたオブジェクトの有効期限を、進行中の復元リクエストで指定された `ExpirationInDays` 値と一致するように更新します。

次のいずれかの条件が true の場合には、オブジェクトに対するこの復元オペレーションは失敗します。

- 進行中の復元リクエストが未完了であり、かつ、このジョブの復元期間 (`ExpirationInDays` 値によって指定) が進行中の復元リクエストで指定される復元期間とは異なること。
- このジョブの復元階層 (`GlacierJobTier` 値によって指定) が進行中の復元リクエストで指定される復元階層と同じであるか、またはより低速であること。

制限

`S3InitiateRestoreObjectOperation` ジョブには次の制限があります。

- アーカイブされたオブジェクトと同じリージョンにジョブを作成する必要があります。
- S3 バッチオペレーションでは、`EXPEDITED` 取得階層はサポートされていません。
- 1 つのバッチオペレーション復元ジョブで、最大 40 億個のオブジェクトを持つマニフェストをサポートできます。

オブジェクトの復元の詳細については、「アーカイブされたオブジェクトの復元」をご参照ください。

S3 オブジェクトロックの保持

Amazon S3 バッチオペレーションを使用すると、Amazon S3 のオブジェクトに対して大規模なバッチオペレーションを実行できます。[Object Lock の保持] オペレーションでは、[ガバナンス] モードまたは [コンプライアンス] モードのいずれかを使用して、オブジェクトの保持日を適用できます。これらのリテンションモードは、さまざまなレベルの保護を適用します。いずれかのリテンションモードを任意のオブジェクトバージョンに適用できます。リーガルホールドなどの保持期間に基づいて、オブジェクトの上書きや削除を防ぎます。Amazon S3 は、オブジェクトのメタデータで指定されている [保持期日] を保存し、その保持期間が経過するまで指定されたバージョンのオブジェクトを保護します。

S3 バッチオペレーションと Object Lock を使用すると、多くの Amazon S3 のオブジェクトの保持期間を一括で管理できます。マニフェストでターゲットオブジェクトのリストを指定し、そのマニフェストをジョブの完了のためにバッチオペレーションに送信します。詳細については、S3 オブジェクトロックの「the section called “保持期間”」を参照してください。

S3 バッチ操作の保持期間の適用ジョブは、完了するか、キャンセルするか、エラー状態になるまで実行されます。S3 バッチオペレーションと S3 Object Lock による保持は、1 回のリクエストで多くのオブジェクトの保持期限を追加、変更、削除する場合に使用することをお勧めします。

バッチ操作は、マニフェストのキーを処理する前に、バケットでオブジェクトロックが有効になっているかどうかを確認します。オペレーションと検証を実行するには、バッチオペレーションがユーザーの代わりに Object Lock を呼び出せるように、AWS Identity and Access Management (IAM) ロールに `s3:GetBucketObjectLockConfiguration` アクセス許可と `s3:PutObjectRetention` アクセス許可が必要です。詳細については、「the section called “オブジェクトロックの考慮事項”」を参照してください。

REST API でこのオペレーションを使用する方法については、「Amazon Simple Storage Service API リファレンス」の「CreateJob」のオペレーションの「S3PutObjectRetention」を参照してください。

AWS Command Line Interface (AWS CLI) でのこのオペレーションの使用例については、「the section called “オブジェクトロック保持でバッチ操作を使用する”」を参照してください。AWS SDK for Java の例については、「the section called “オブジェクトロック保持でバッチ操作を使用する”」を参照してください。

制約と制限

バッチオペレーションを使用して Object Lock の保持期間を適用する場合、以下の制約と制限が適用されます。

- S3 バッチオペレーションでは、バケットレベルでの変更は行われません。
- ジョブを実行するバケットでバージョニングと S3 オブジェクトロックを設定する必要があります。
- マニフェストに登録されているすべてのオブジェクトは同じバケットにあることが必要です。
- マニフェストでオブジェクトのバージョンが明示的に指定されていない限り、オペレーションにはオブジェクトの最新バージョンが使用されます。
- [Object Lock の保持] ジョブを使用するには、IAM ロールに `s3:PutObjectRetention` アクセス許可が必要です。
- ジョブを実行している S3 バケットで Object Lock が有効になっていることを確認するには、`s3:GetBucketObjectLockConfiguration` IAM アクセス許可が必要です。
- オブジェクトの保持期間を延長できるのは、`COMPLIANCE` モードの保持期限が適用されている場合のみであり、短縮することはできません。
- 1 つの S3 Object Lock 保持ジョブで、最大 200 億個のオブジェクトを持つマニフェストをサポートできます。

S3 オブジェクトロックのリーガルホールド

Amazon S3 バッチオペレーションを使用すると、Amazon S3 のオブジェクトに対して大規模なバッチオペレーションを実行できます。[Object Lock のリーガルホールド] オペレーションを使用すると、オブジェクトバージョンにリーガルホールドを適用できます。保持期間の設定と同様に、リーガルホールドは、オブジェクトバージョンが上書きまたは削除されるのを防ぎます。ただし、リーガルホールドには関連する保持期間はなく、削除するまで有効です。

S3 バッチ操作とオブジェクトロックを使用すると、一度に多くの Amazon S3 のオブジェクトをリーガルホールドにすることができます。これを行うには、マニフェストに対象のオブジェクトのリストを指定し、そのリストをバッチオペレーションに渡します。S3 バッチオペレーションの [Object Lock のリーガルホールド] ジョブは、完了するか、キャンセルするか、エラー状態になるまで実行されます。

S3 バッチオペレーションは、マニフェストのオブジェクトを処理する前に、S3 バケットで Object Lock が有効になっているかどうかを確認します。オブジェクトオペレーションとバケットレベルの検証を実行するには、S3 バッチオペレーションに AWS Identity and Access Management (IAM) ロールの `s3:PutObjectLegalHold` と `s3:GetBucketObjectLockConfiguration` が必要です。これらのアクセス許可により、S3 バッチオペレーションはユーザーに代わって S3 Object Lock を呼び出すことができます。

リーガルホールドを削除する S3 バッチオペレーションのジョブを作成するには、リーガルホールドのステータスに `Off` を指定するだけで構いません。詳細については、「the section called “オブジェクトロックの考慮事項”」を参照してください。

Amazon S3 REST API でこのオペレーションを使用する方法については、「Amazon Simple Storage Service API リファレンス」の「CreateJob」のオペレーションの「`S3PutObjectLegalHold`」を参照してください。

このオペレーションの使用例については、「AWS SDK for Java の使用」を参照してください。

制約と制限

バッチオペレーションを使用して Object Lock のリーガルホールドを適用または削除する場合、以下の制約と制限が適用されます。

- S3 バッチオペレーションでは、バケットレベルでの変更は行われません。
- マニフェストに登録されているすべてのオブジェクトは同じバケットにあることが必要です。
- ジョブを実行するバケットでバージョニングと S3 オブジェクトロックを設定する必要があります。
- マニフェストでバージョンが明示的に指定されていない限り、[Object Lock のリーガルホールド] オペレーションにはオブジェクトの最新バージョンが使用されます。
- オブジェクトのリーガルホールドを追加または解除するには、IAM ロールに `s3:PutObjectLegalHold` アクセス許可が必要です。
- ジョブが実行されている S3 バケットで S3 Object Lock が有効になっていることを確認するには、`s3:GetBucketObjectLockConfiguration` IAM アクセス許可が必要です。

- 1 つの S3 Object Lock リーガルホールドジョブで、最大 200 億個のオブジェクトを持つマニフェストをサポートできます。

- オブジェクトのコピー
- AWS Lambda 関数の呼び出し
- すべてのオブジェクトタグを置換する
- すべてのオブジェクトタグを削除する
- アクセスコントロールリスト (ACL) を置き換える
- バッチオペレーションを使ってオブジェクトを復元する
- S3 オブジェクトロックの保持
- S3 オブジェクトロックのリーガルホールド
- バッチレプリケーションを使用した既存のオブジェクトのレプリケーション

S3 バッチ操作ジョブの管理

Amazon S3 は、作成した S3 バッチ操作ジョブを管理するための一連の堅牢なツールを用意しています。このセクションでは、Amazon S3 コンソール、AWS Command Line Interface (AWS CLI)、AWS SDK、または Amazon S3 REST API を使用してジョブを管理および追跡するために使用できるオペレーションについて説明します。

トピック

- S3 バッチオペレーションジョブの管理に Simple Storage Service (Amazon S3) コンソールを使用する
- ジョブのリスト取得
- ジョブの詳細の表示
- ジョブの優先度の割り当て

S3 バッチオペレーションジョブの管理に Simple Storage Service (Amazon S3) コンソールを使用する

コンソールを使用して、S3 バッチオペレーションジョブを管理できます。例えば、以下のことが可能です。

- アクティブなジョブとキュージョブを表示する

- ジョブの優先順位を変更する
- ジョブを確認して実行する
- ジョブのクローンを作成する
- ジョブのキャンセル

S3 コンソールを使用して S3 バッチオペレーションジョブを管理するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[バッチ操作] を選択します。
3. 管理する特定のジョブを選択します。

ジョブのリスト取得

S3 バッチ操作ジョブのリストを取得できます。このリストには、まだ終了していないジョブと 90 日以内に終了したばかりのジョブが含まれます。ジョブリストには、ID、説明、優先度、現在のステータス、および成功したタスクと失敗したタスクの数など、各ジョブに関する情報が含まれています。ジョブのリストをステータスでフィルタリングできます。コンソールからジョブリストを取得するときに、説明または ID でジョブを検索して AWS リージョン 別にフィルタリングすることもできます。

`Active` および `Complete` ジョブのリストを取得する

以下の AWS CLI の例では、`Active` および `Complete` ジョブのリストを取得します。この例を実行するには、*`user input placeholders`* をユーザー自身の情報に置き換えます。

```
aws s3control list-jobs \
    --region us-west-2 \
    --account-id account-id \
    --job-statuses '["Active","Complete"]' \
    --max-results 20
```

詳細と例については、「AWS CLI コマンドリファレンス」で「list-jobs」を参照してください。

ジョブの詳細の表示

ジョブを一覧表示することで取得できるよりも多くの Amazon S3 バッチオペレーションジョブの情報が必要な場合、単一のジョブのすべての詳細を表示できます。まだ終了していないジョブや、過去

90 日以内に終了したジョブの詳細を確認できます。ジョブリストで返される情報に加えて、単一のジョブの詳細には次に示すような他の項目が含まれています。

- オペレーションパラメータ
- マニフェストに関する詳細
- 完了レポートに関する情報 (ジョブの作成時にレポートを設定した場合)
- ジョブの実行に割り当てた AWS Identity and Access Management (IAM) ユーザーロールの Amazon リソースネーム (ARN)

個々のジョブの詳細を表示することで、そのジョブの設定全体にアクセスできます。ジョブの詳細を表示するには、Amazon S3 コンソールまたは AWS Command Line Interface (AWS CLI) を使用します。

Amazon S3 コンソールで S3 バッチオペレーションジョブの説明を取得する

コンソールを使用してバッチオペレーションジョブの説明を表示するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[バッチ操作] を選択します。
3. 詳細を表示する特定のジョブの ID を選択します。

AWS CLI で S3 バッチオペレーションジョブの説明を取得する

次の例では、AWS CLI を使用して S3 バッチオペレーションジョブの説明を取得します。次のコマンド例を使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3control describe-job \
--region us-west-2 \
--account-id account-id \
--job-id 00e123a4-c0d8-41f4-a0eb-b46f9ba5b07c
```

詳細と例については、「AWS CLI コマンドリファレンス」で「describe-job」を参照してください。

ジョブの優先度の割り当て

各 Amazon S3 バッチオペレーションジョブには、数値の優先度 (任意の正の整数) を割り当てることができます。S3 バッチオペレーションは、割り当てられた優先度に従ってジョブの優先順位を決

定します。優先度が高いジョブ (または、優先パラメータの数値が高いジョブ) ほど先に処理されます。優先度は降順に決定されます。たとえば、優先度の値が 10 のジョブキューは、優先度の値が 1 のジョブキューより先にスケジュールされます。

ジョブの実行中にジョブの優先順位を変更できます。また、ジョブの実行中に優先順位が高い新しいジョブを送信すると、優先順位の低いジョブが一時停止して優先順位の高いジョブが実行される可能性があります。

ジョブの優先順位を変更しても、ジョブの処理速度には影響しません。

> **Note**
>
> S3 バッチオペレーションはベストエフォートベースでジョブの優先度を重視します。優先順位の高いジョブは優先順位の低いジョブより優先されるのが一般的ですが、Amazon S3 はジョブの厳密な順序付けを保証しません。

S3 コンソールの使用

Amazon S3 コンソールでジョブの優先度を更新する方法

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[バッチ操作] を選択します。
3. 管理する特定のジョブを選択します。
4. [Actions] (アクション) を選択します。ドロップダウンリストから [Update priority] (更新優先度) を選択します。

AWS CLI を使用する場合

以下の例では、AWS CLI を使用してジョブの優先度を更新します。数値が大きいほど、実行優先度が高くなります。次のコマンド例を使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3control update-job-priority \
    --region us-west-2 \
    --account-id account-id \
    --priority 98 \
    --job-id 00e123a4-c0d8-41f4-a0eb-b46f9ba5b07c
```

AWS SDK for Java を使用する場合

次の例では、AWS SDK for Java を使用して S3 バッチ操作ジョブの優先順位を更新します。

ジョブの優先度の詳細については、「ジョブの優先度の割り当て」を参照してください。

Example

```
package aws.example.s3control;


import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.UpdateJobPriorityRequest;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class UpdateJobPriority {
    public static void main(String[] args) {
        String accountId = "Account ID";
        String jobId = "00e123a4-c0d8-41f4-a0eb-b46f9ba5b07c";

        try {
            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            s3ControlClient.updateJobPriority(new UpdateJobPriorityRequest()
                    .withAccountId(accountId)
                    .withJobId(jobId)
                    .withPriority(98));

        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
```

```
            e.printStackTrace();
        }
    }
}
```

ジョブステータスと完了レポートの追跡

S3 バッチ操作を使用すると、ジョブステータスの表示と更新、通知と口グの追加、ジョブの失敗の追跡、完了レポートの生成を行うことができます。

トピック

- ジョブステータス
- ジョブステータスの更新
- 通知と口グ記録
- ジョブの失敗の追跡
- 完了レポート
- 例: を使用して Amazon EventBridge の S3 バッチ操作ジョブを追跡するAWS CloudTrail
- 例: S3 バッチ操作完了レポート

ジョブステータス

ジョブの作成および実行後、ジョブは一連のステータスを進行します。ステータスとその間のあり得る移行を次の表に示します。

ステータス	説明	Transitions
New	ジョブを作成すると、ジョブは New ステータスから始まります。	Amazon S3 がマニフェストオブジェクトの処理を開始すると、ジョブは自動的に Preparing ステータスになります。
Preparing	Amazon S3 はマニフェストオブジェクトと他のジョブパラメータを処理してセットアップし、ジョブを実行します。	Amazon S3 がマニフェストと他のパラメータの処理を終了すると、ジョブは自動的に Ready ステータスになりま

ステータス	説明	Transitions
		す。その後、ジョブではマニフェストに一覧表示されているオブジェクトにおいて指定されたオペレーションの実行を開始する準備が整います。 ジョブで実行前に確認が必要な場合は (Amazon S3 コンソールを使用してジョブを作成した場合など)、ジョブは `Preparing` から `Suspended` に移行します。ジョブを実行することが確認されるまで、`Suspended` 状態のままになります。
`Suspended`	ジョブには確認が必要ですが、ジョブを実行することをまだ確認していません。Amazon S3 コンソールを使用して作成したジョブのみ確認が必要になります。コンソールを使用して作成したジョブは、`Suspended` 後にすぐ `Preparing` 状態になります。ジョブを実行したいことを確認すると、このジョブは `Ready` になり、`Suspended` 状態に戻ることはありません。	ジョブを実行したいことを確認すると、そのステータスは `Ready` に変更します。

ステータス	説明	Transitions
Ready	Amazon S3 はリクエストしたオブジェクトオペレーションの実行を開始する準備ができました。	Amazon S3 がジョブを開始すると、ジョブは自動的に Active ステータスになります。ジョブが Ready 状態のままになる期間は、優先度の高いジョブをすでに実行中であるかどうか、またそのジョブが完了するまでの時間に応じます。
Active	Amazon S3 はマニフェストで一覧表示されているオブジェクトでリクエストされたオペレーションを実行しています。ジョブが Active の間、Amazon S3 コンソール、あるいは REST API、AWS CLI、または AWS SDK の DescribeJob オペレーションを使用してその進捗状況を監視できます。	ジョブがオブジェクトでオペレーションを実行しなくなると、ジョブは Active 状態ではなくなります。この動作は、ジョブが正常に完了したか失敗した場合などに自動的に起こります。あるいは、ジョブのキャンセルなどのユーザーアクションの結果としても生じます。ジョブが移行する状態は、移行の理由によって異なります。
Pausing	ジョブは別の状態から Paused に移行しています。	Paused ステージが完了すると、ジョブは自動的に Pausing になります。
Paused	ジョブを現在実行中に優先度の高い別のジョブを送信すると、ジョブは Paused になります。	ジョブの実行が完了、失敗、あるいは停止になることを阻止している優先度の高いジョブの後、Paused ジョブは自動的に Active に戻ります。

ステータス	説明	Transitions
Complete	ジョブは、マニフェストのすべてのオブジェクトでリクエストされたオペレーションの実行を終了しました。このオペレーションは、すべてのオブジェクトで成功または失敗することがあります。完了レポートを生成するようにジョブを設定した場合、このレポートはジョブが Complete になるとすぐに利用可能になります。	Complete は終了状態です。ジョブが Complete に達すると、他の状態に移行することはありません。
Cancelling	このジョブは Cancelled に移行しています。	Cancelled ステージが完了すると、ジョブは自動的に Cancelling になります。
Cancelled	ユーザーはジョブのキャンセルをリクエストし、S3 バッチオペレーションはジョブのキャンセルに成功しました。このジョブは、Amazon S3 に新しいリクエストを送信しません。	Cancelled は終了状態です。ジョブが Cancelled に達した後、他の状態には移行しません。
Failing	このジョブは Failed に移行しています。	Failed ステージが完了すると、ジョブは自動的に Failing になります。
Failed	このジョブは失敗し、もう実行されていません。ジョブの失敗に関する詳細については、「ジョブの失敗の追跡」を参照してください。	Failed は終了状態です。ジョブが Failed に達した後、他の状態には移行しません。

ジョブステータスの更新

次の AWS CLI および AWS SDK for Java の例は、バッチオペレーションジョブのステータスを更新します。Amazon S3 コンソールを使用してバッチオペレーションジョブを管理する方法の詳細については、「S3 バッチオペレーションジョブの管理に Simple Storage Service (Amazon S3) コンソールを使用する」を参照してください。

AWS CLI を使用する場合

次のコマンド例を使用する際は、*user input placeholders* をユーザー自身の情報に置き換えます。

- 例えば、--no-confirmation-required のコマンドで create-job パラメータを指定しなかった場合、ジョブのステータスを Ready に設定してジョブを確定するまでこのジョブは停止状態になります。その後、Amazon S3 によってジョブが実行可能になります。

```
aws s3control update-job-status \
    --region us-west-2 \
    --account-id 123456789012 \
    --job-id 00e123a4-c0d8-41f4-a0eb-b46f9ba5b07c \
    --requested-job-status 'Ready'
```

- ジョブステータスを Cancelled に設定して、ジョブをキャンセルします。

```
aws s3control update-job-status \
     --region us-west-2 \
     --account-id 123456789012 \
     --job-id 00e123a4-c0d8-41f4-a0eb-b46f9ba5b07c \
     --status-update-reason "No longer needed" \
     --requested-job-status Cancelled
```

AWS SDK for Java の使用

次の例では、AWS SDK for Java を使用して S3 バッチオペレーションジョブのステータスを更新します。

ジョブのステータスの詳細については、「ジョブステータスと完了レポートの追跡」を参照してください。

Example

```
package aws.example.s3control;


import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.UpdateJobStatusRequest;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class UpdateJobStatus {
    public static void main(String[] args) {
        String accountId = "Account ID";
        String jobId = "00e123a4-c0d8-41f4-a0eb-b46f9ba5b07c";

        try {
            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            s3ControlClient.updateJobStatus(new UpdateJobStatusRequest()
                    .withAccountId(accountId)
                    .withJobId(jobId)
                    .withRequestedJobStatus("Ready"));

        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

通知とログ記録

完了レポートをリクエストすることに加えて、AWS CloudTrail を使用してバッチオペレーションのアクティビティをキャプチャ、確認、および監査することもできます。バッチオペレーションは既存の Amazon S3 API オペレーションを使用してタスクを実行するため、それらのタスクも直接呼び出した場合と同じイベントを出力します。したがって、Amazon S3 で既に使用しているのと同じ通知、ログ記録、および監査ツールとプロセスを使用することで、ジョブの進捗状況とジョブのすべてのタスクを追跡および記録することができます。詳細については、次のセクションの例を参照してください。

> **Note**
>
> バッチオペレーションは、ジョブの実行中に CloudTrail で管理イベントとデータイベントの両方を生成します。これらのイベントの量は、各ジョブのマニフェスト内のキーの数に応じてスケールします。詳細については、「CloudTrail の料金」ページを参照してください。このページには、アカウントで設定した証跡の数に応じて料金がどのように変わるのかを示す例が記載されています。ニーズに合わせてイベントを設定して口グに記録する方法については、AWS CloudTrail ユーザーガイドの最初の証跡の作成を参照してください。

Amazon S3 イベントの詳細については、「Amazon S3 イベント通知」を参照してください。

ジョブの失敗の追跡

指定されたマニフェストを読み取れないなど、S3 バッチ操作が正常に実行できない問題が発生した場合、そのジョブは失敗します。ジョブが失敗すると、1 つ以上の障害コードまたは失敗の理由が生成されます。S3 バッチオペレーションは、ジョブの詳細をリクエストしてそれらを表示できるように、障害コードと理由をジョブとともに保存します。ジョブの完了レポートをリクエストした場合は、そこに障害コードと理由も表示されます。

ジョブが大量の失敗したオペレーションを実行するのを防ぐために、Amazon S3 はすべてのバッチ操作ジョブにタスク失敗のしきい値を設定します。ジョブが 1,000 個以上のタスクを実行すると、Amazon S3 はタスクの失敗率を監視します。いずれかの時点で、失敗率 (実行されたタスクの総数に対する失敗したタスクの数の割合) が 50 パーセントを超えると、そのジョブは失敗します。タスク失敗しきい値を超えたためにジョブが失敗した場合、この失敗の原因を識別できます。たとえば、特定のバケットに存在しないいくつかのオブジェクトを誤ってマニフェストに含めてしまうことがあります。誤りを訂正したら、ジョブを再送信できます。

> **Note**
>
> S3 バッチオペレーションは非同期で動作するため、タスクはマニフェストにリストされているオブジェクトの順序で実行する必要はありません。つまり、どのオブジェクトのタスクが成功して、どれが失敗したかを判断するためにマニフェストの順序を使用することはできません。代わりに、ジョブの完了レポート (リクエストした場合) を調べるか、AWS CloudTrail イベントログを表示して失敗の原因を特定することができます。

完了レポート

ジョブを作成するときに、完了レポートをリクエストできます。S3 バッチオペレーションが少なくとも 1 つのタスクを正常に呼び出す限り、ジョブでタスクの実行が完了した後、失敗したとき、またはキャンセルされたときに、Amazon S3 は完了レポートを生成します。完了レポートに、すべてのタスクを含めるか、失敗したタスクのみを含めるかを設定できます。

完了レポートには、ジョブ設定、ステータス、およびオブジェクトキーとバージョン、ステータス、エラーコード、およびエラーの説明を含む各タスクの情報が含まれます。完了レポートは、追加の設定を必要としない統合形式でタスクの結果を表示する簡単な方法です。完了レポートは、Amazon S3 マネージドキー (SSE-S3) によるサーバー側の暗号化を使用して暗号化されます。完了レポートの例については、「例: S3 バッチ操作完了レポート」を参照してください。

完了レポートを設定していない場合でも、CloudTrail および Amazon CloudWatch を使用して、ジョブとそのタスクをモニタリングして監査できます。詳細については、以下の各トピックを参照してください。

トピック

- 例: を使用して Amazon EventBridge の S3 バッチ操作ジョブを追跡するAWS CloudTrail
- 例: S3 バッチ操作完了レポート

例: を使用して Amazon EventBridge の S3 バッチ操作ジョブを追跡するAWS CloudTrail

Amazon S3 バッチ操作ジョブアクティビティは、 にイベントとして記録されますAWS CloudTrail Amazon EventBridge でカスタムルールを作成し、Amazon Simple Notification Service (Amazon SNS) など、選択したターゲット通知リソースにこれらのイベントを送信できます。

> **Note**
>
> イベントを管理するには、Amazon EventBridge が好ましい方法です。Amazon CloudWatch Events と EventBridge は同じ基盤となるサービスと API ですが、EventBridge はより多くの機能を提供します。CloudWatch または EventBridge のいずれかで行った変更は、各コンソールに表示されます。詳細については、「Amazon EventBridge ユーザーガイドを参照してください。

トラッキングの例

- CloudTrail に記録された S3 バッチ操作イベント
- S3 バッチ操作ジョブイベントを追跡するための EventBridge ルール

CloudTrail に記録された S3 バッチ操作イベント

バッチ操作ジョブが作成されると、CloudTrail に `JobCreated` イベントとして記録されます。ジョブは実行されると、処理中に状態が変わり、他の `JobStatusChanged` イベントが CloudTrail に記録されます。CloudTrail コンソールでこれらのイベントを表示できます。CloudTrail の詳細については、AWS CloudTrail ユーザーガイドを参照してください。

> **Note**
>
> CloudTrail には、S3 バッチ操作ジョブ `status-change` イベントのみが記録されます。

Example — CloudTrail によって記録された S3 バッチオペレーションジョブ完了イベント

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "s3.amazonaws.com"
    },
    "eventTime": "2020-02-05T18:25:30Z",
    "eventSource": "s3.amazonaws.com",
    "eventName": "JobStatusChanged",
    "awsRegion": "us-west-2",
```

```
    "sourceIPAddress": "s3.amazonaws.com",
    "userAgent": "s3.amazonaws.com",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "f907577b-bf3d-4c53-b9ed-8a83a118a554",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "123412341234",
    "serviceEventDetails": {
        "jobId": "d6e58ec4-897a-4b6d-975f-10d7f0fb63ce",
        "jobArn": "arn:aws:s3:us-west-2:181572960644:job/
d6e58ec4-897a-4b6d-975f-10d7f0fb63ce",
        "status": "Complete",
        "jobEventId": "b268784cf0a66749f1a05bce259804f5",
        "failureCodes": [],
        "statusChangeReason": []
    }
}
```

S3 バッチ操作ジョブイベントを追跡するための EventBridge ルール

次の例は、Amazon EventBridge でルールを作成して、AWS CloudTrail によって記録された S3 バッチ操作イベントを任意のターゲットにキャプチャする方法を示しています。

そのためには、「イベントに反応する EventBridge ルールの作成」のすべての手順に従ってルールを作成します。必要に応じて、以下の S3 バッチ操作カスタムイベントパターンポリシーを貼り付け、ターゲットサービスを選択します。

S3 バッチオペレーションカスタムイベントパターンポリシー

```
{
    "source": [
        "aws.s3"
    ],
    "detail-type": [
        "AWS Service Event via CloudTrail"
    ],
    "detail": {
        "eventSource": [
            "s3.amazonaws.com"
        ],
        "eventName": [
            "JobCreated",
```

```
            "JobStatusChanged"
        ]
    }
}
```

以下の例は、EventBridge イベントルールから Amazon Simple Queue Service (Amazon SQS) に送信された 2 つのバッチ操作イベントです。バッチ操作ジョブは処理中にさまざまな状態 (New、Preparing、Active など) に移行するため、ジョブごとに複数のメッセージを受信することになります。

Example — JobCreated サンプルイベント

```
{
    "version": "0",
    "id": "51dc8145-541c-5518-2349-56d7dffdf2d8",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.s3",
    "account": "123456789012",
    "time": "2020-02-27T15:25:49Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "11112223334444",
            "invokedBy": "s3.amazonaws.com"
        },
        "eventTime": "2020-02-27T15:25:49Z",
        "eventSource": "s3.amazonaws.com",
        "eventName": "JobCreated",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "s3.amazonaws.com",
        "userAgent": "s3.amazonaws.com",
        "eventID": "7c38220f-f80b-4239-8b78-2ed867b7d3fa",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "jobId": "e849b567-5232-44be-9a0c-40988f14e80c",
            "jobArn": "arn:aws:s3:us-east-1:181572960644:job/
e849b567-5232-44be-9a0c-40988f14e80c",
            "status": "New",
            "jobEventId": "f177ff24f1f097b69768e327038f30ac",
            "failureCodes": [],
```

```
            "statusChangeReason": []
        }
    }
}
```

Example — JobStatusChanged ジョブ完了イベント

```
{
  "version": "0",
  "id": "c8791abf-2af8-c754-0435-fd869ce25233",
  "detail-type": "AWS Service Event via CloudTrail",
  "source": "aws.s3",
  "account": "123456789012",
  "time": "2020-02-27T15:26:42Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "eventVersion": "1.05",
    "userIdentity": {
      "accountId": "1111222233334444",
      "invokedBy": "s3.amazonaws.com"
    },
    "eventTime": "2020-02-27T15:26:42Z",
    "eventSource": "s3.amazonaws.com",
    "eventName": "JobStatusChanged",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "s3.amazonaws.com",
    "userAgent": "s3.amazonaws.com",
    "eventID": "0238c1f7-c2b0-440b-8dbd-1ed5e5833afb",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "serviceEventDetails": {
      "jobId": "e849b567-5232-44be-9a0c-40988f14e80c",
      "jobArn": "arn:aws:s3:us-east-1:181572960644:job/
e849b567-5232-44be-9a0c-40988f14e80c",
      "status": "Complete",
      "jobEventId": "51f5ac17dba408301d56cd1b2c8d1e9e",
      "failureCodes": [],
      "statusChangeReason": []
    }
  }
}
```

例: S3 バッチ操作完了レポート

S3 バッチ操作ジョブを作成するときに、すべてのタスクまたは失敗したタスクについてのみ完了レポートをリクエストできます。少なくとも 1 つのタスクが正常に呼び出されている限り、S3 バッチ操作は、完了、失敗、またはキャンセルされたジョブに関するレポートを生成します。

完了レポートには、オブジェクトキーの名前とバージョン、ステータス、エラーコード、およびエラーの説明など、各タスクに関する追加情報が含まれています。失敗した各タスクのエラーの説明を使用して、アクセス許可の問題など、ジョブの作成中に発生した問題を診断できます。

> **Note**
>
> 完了レポートは常に、Amazon S3 マネージドキー (SSE-S3) で暗号化されます。

Example — 最上位マニフェストの結果ファイル

次の例に示すように、最上位の `manifest.json` ファイルには、成功した各レポートの場所と (ジョブに失敗があった場合は) 失敗したレポートの場所が含まれています。

```
{
    "Format": "Report_CSV_20180820",
    "ReportCreationDate": "2019-04-05T17:48:39.725Z",
    "Results": [
        {
            "TaskExecutionStatus": "succeeded",
            "Bucket": "my-job-reports",
            "MD5Checksum": "83b1c4cbe93fc893f54053697e10fd6e",
            "Key": "job-f8fb9d89-a3aa-461d-bddc-ea6a1b131955/
results/6217b0fab0de85c408b4be96aeaca9b195a7daa5.csv"
        },
        {
            "TaskExecutionStatus": "failed",
            "Bucket": "my-job-reports",
            "MD5Checksum": "22ee037f3515975f7719699e5c416eaa",
            "Key": "job-f8fb9d89-a3aa-461d-bddc-ea6a1b131955/results/
b2ddad417e94331e9f37b44f1faf8c7ed5873f2e.csv"
        }
    ],
    "ReportSchema": "Bucket, Key, VersionId, TaskStatus, ErrorCode, HTTPStatusCode,
 ResultMessage"
```

```
}
```

Example — 失敗したタスクのレポート

失敗したタスクのレポートには、すべての失敗したタスクに関する以下の情報が含まれています。

- Bucket
- Key
- VersionId
- TaskStatus
- ErrorCode
- HTTPStatusCode
- ResultMessage

次のレポート例は、AWS Lambda 関数がタイムアウトし、失敗が失敗しきい値を超えた場合を示しています。これはその後 PermanentFailure としてマークされました。

```
amzn-s3-demo-bucket1,image_14975,,failed,200,PermanentFailure,"Lambda returned
 function error: {""errorMessage"":""2019-04-05T17:35:21.155Z 2845ca0d-38d9-4c4b-
abcf-379dc749c452 Task timed out after 3.00 seconds""}"
amzn-s3-demo-bucket1,image_15897,,failed,200,PermanentFailure,"Lambda returned
 function error: {""errorMessage"":""2019-04-05T17:35:29.610Z 2d0a330b-de9b-425f-
b511-29232fde5fe4 Task timed out after 3.00 seconds""}"
amzn-s3-demo-bucket1,image_14819,,failed,200,PermanentFailure,"Lambda returned
 function error: {""errorMessage"":""2019-04-05T17:35:22.362Z fcf5efde-74d4-4e6d-b37a-
c7f18827f551 Task timed out after 3.00 seconds""}"
amzn-s3-demo-bucket1,image_15930,,failed,200,PermanentFailure,"Lambda returned
 function error: {""errorMessage"":""2019-04-05T17:35:29.809Z 3dd5b57c-4a4a-48aa-8a35-
cbf027b7957e Task timed out after 3.00 seconds""}"
amzn-s3-demo-bucket1,image_17644,,failed,200,PermanentFailure,"Lambda
 returned function error: {""errorMessage"":""2019-04-05T17:35:46.025Z
 10a764e4-2b26-4d8c-9056-1e1072b4723f Task timed out after 3.00 seconds""}"
amzn-s3-demo-bucket1,image_17398,,failed,200,PermanentFailure,"Lambda returned
 function error: {""errorMessage"":""2019-04-05T17:35:44.661Z 1e306352-4c54-4eba-
aee8-4d02f8c0235c Task timed out after 3.00 seconds""}"
```

Example — 成功したタスクのレポート

成功したタスクのレポートには、完了したタスクに関する以下の情報が含まれています。

- Bucket
- Key
- VersionId
- TaskStatus
- ErrorCode
- HTTPStatusCode
- ResultMessage

次の例では、Lambda 関数は Amazon S3 オブジェクトを別のバケットに正常にコピーしています。返された Amazon S3 レスポンスは S3 バッチ操作に戻され、最終的な完了レポートに書き込まれます。

```
amzn-s3-demo-bucket1,image_17775,,succeeded,200,,"{u'CopySourceVersionId':
 'xVR78haVKlRnurYofbTfYr3ufYbktF8h', u'CopyObjectResult': {u'LastModified':
 datetime.datetime(2019, 4, 5, 17, 35, 39, tzinfo=tzlocal()), u'ETag':
 '""fe66f4390c50f29798f040d7aae72784""'}, 'ResponseMetadata': {'HTTPStatusCode':
 200, 'RetryAttempts': 0, 'HostId': 'nXNaClIMxEJzWNmeMNQV2KpjbaCJLn0OGoXWZpuVOFS/
iQYWxb3QtTvzX9SVfx2lA3oTKLwImKw=', 'RequestId': '3ED5852152014362', 'HTTPHeaders':
 {'content-length': '234', 'x-amz-id-2': 'nXNaClIMxEJzWNmeMNQV2KpjbaCJLn0OGoXWZpuVOFS/
iQYWxb3QtTvzX9SVfx2lA3oTKLwImKw=', 'x-amz-copy-source-version-id':
 'xVR78haVKlRnurYofbTfYr3ufYbktF8h', 'server': 'AmazonS3', 'x-amz-request-id':
 '3ED5852152014362', 'date': 'Fri, 05 Apr 2019 17:35:39 GMT', 'content-type':
 'application/xml'}}}"
amzn-s3-demo-bucket1,image_17763,,succeeded,200,,"{u'CopySourceVersionId':
 '6HjOUSim4Wj6BTcbxToXW44pSZ.40pwq', u'CopyObjectResult': {u'LastModified':
 datetime.datetime(2019, 4, 5, 17, 35, 39, tzinfo=tzlocal()),
 u'ETag': '""fe66f4390c50f29798f040d7aae72784""'}, 'ResponseMetadata':
 {'HTTPStatusCode': 200, 'RetryAttempts': 0, 'HostId': 'GiCZNYr8LHd/
Thyk6beTRP96IGZk2sYxujLe13TuuLpq6U2RD3we0YoluuIdm1PRvkMwnEW1aFc=', 'RequestId':
 '1BC9F5B1B95D7000', 'HTTPHeaders': {'content-length': '234', 'x-amz-id-2':
 'GiCZNYr8LHd/Thyk6beTRP96IGZk2sYxujLe13TuuLpq6U2RD3we0YoluuIdm1PRvkMwnEW1aFc=', 'x-
amz-copy-source-version-id': '6HjOUSim4Wj6BTcbxToXW44pSZ.40pwq', 'server': 'AmazonS3',
 'x-amz-request-id': '1BC9F5B1B95D7000', 'date': 'Fri, 05 Apr 2019 17:35:39 GMT',
 'content-type': 'application/xml'}}}"
amzn-s3-demo-bucket1,image_17860,,succeeded,200,,"{u'CopySourceVersionId':
 'm.MDD0g_QsUnYZ8TBzVFrp.TmjN8PJyX', u'CopyObjectResult': {u'LastModified':
 datetime.datetime(2019, 4, 5, 17, 35, 40, tzinfo=tzlocal()), u'ETag':
 '""fe66f4390c50f29798f040d7aae72784""'}, 'ResponseMetadata': {'HTTPStatusCode':
 200, 'RetryAttempts': 0, 'HostId': 'F9ooZOgpE5g9sNgBZxjdiPHqB4+0DNWgj3qbsir
+sKai4fv7rQEcF2fBN1VeeFc2WH45a9ygb2g=', 'RequestId': '8D9CA56A56813DF3', 'HTTPHeaders':
```

```
 {'content-length': '234', 'x-amz-id-2': 'F9ooZOgpE5g9sNgBZxjdiPHqB4+0DNWgj3qbsir
+sKai4fv7rQEcF2fBN1VeeFc2WH45a9ygb2g=', 'x-amz-copy-source-version-id':
 'm.MDD0g_QsUnYZ8TBzVFrp.TmjN8PJyX', 'server': 'AmazonS3', 'x-amz-request-id':
 '8D9CA56A56813DF3', 'date': 'Fri, 05 Apr 2019 17:35:40 GMT', 'content-type':
 'application/xml'}}}"
```

タグを使用したアクセスのコントロールとジョブのラベル付け

タグを追加することで、S3 バッチ操作ジョブへのラベル付けとアクセスの制御を実行できます。タグを使用して、バッチ操作ジョブの担当者を識別できます。ジョブタグがあることで、ユーザーによるジョブのキャンセル、確認状態にあるジョブの有効化、ジョブの優先度レベルの変更を許可したり制限したりできます。タグをアタッチしてジョブを作成します。作成後にジョブにタグを追加できます。各タグはキーと値のペアであり、ジョブの作成時に追加することも、後で更新することもできます。

> **Warning**
>
> ジョブタグに機密情報や個人データが含まれていないことを確認してください。

以下のタグ付けの例を考えてみます。経理部門にバッチ操作ジョブを作成するとします。`Department` タグに値 `Finance` を割り当ててジョブが作成される場合に、ユーザーに AWS Identity and Access Management の呼び出しを許可する `CreateJob` (IAM) ポリシーを作成できます。さらに、財務部門のメンバーであるすべてのユーザーにそのポリシーをアタッチできます。

この例を進めて、ユーザーに、必要なタグの付いたジョブの優先度を更新することを許可するポリシーや、それらのタグの付いたジョブをキャンセルすることを許可するポリシーを作成できます。詳細については、「the section called “アクセス許可の制御”」を参照してください。

タグは、新しい S3 バッチ操作ジョブの作成時に追加することも、既存のジョブに追加することもできます。

タグには以下の制限があります。

- タグキーが一意である限り、最大 50 個のタグをジョブに関連付けることができます。
- タグキーには最大 128 個の Unicode 文字、タグ値には最大 256 個の Unicode 文字を使用できます。
- キーと値は大文字と小文字が区別されます。

タグの制限の詳細については、AWS Billing and Cost Management ユーザーガイドのユーザー定義タグの制限を参照してください。

S3 バッチ操作ジョブのタグ付けに関連する API オペレーション

Amazon S3 では、S3 バッチ操作ジョブのタグ付けについて次の API オペレーションがサポートされています。

- GetJobTagging – バッチオペレーションジョブに関連付けられたタグセットを返します。
- PutJobTagging – ジョブに関連付けられたタグのセットを置き換えます。この API アクションを使用した S3 バッチ操作ジョブタグの管理には、2 つの異なるシナリオがあります。
  - ジョブにタグがない - ジョブに一連のタグを追加できます (ジョブに以前のタグがない)。
  - ジョブに既存のタグのセットがある - 既存のタグのセットを変更するには、既存のタグのセット全体を置き換えます。または、GetJobTagging により既存のタグのセットを取得し、そのタグのセットに変更を加えて、この API アクションにより既存のタグのセットを、変更したタグのセットに置き換えます。

  > **Note**
  >
  > タグセットを空にしてこのリクエストを送信すると、S3 バッチ操作 によってオブジェクトの既存のタグセットが削除されます。この方法を使用する場合は、階層 1 リクエスト (PUT) に対して料金が発生します。詳細については、「Amazon S3 の料金」を参照してください。
  > バッチ操作ジョブの既存のタグを削除するには、`DeleteJobTagging` アクションをお勧めします。このアクションでは、料金が発生せずに同じ結果が得られるためです。

- DeleteJobTagging - バッチオペレーションジョブに関連付けられたタグセットを削除します。

ラベル付けに使用されるジョブタグを使用したバッチ操作ジョブの作成

タグを追加することで、Amazon S3 バッチオペレーションジョブへのラベル付けとアクセスの制御を実行できます。タグを使用して、バッチ操作ジョブの担当者を識別できます。タグをアタッチしてジョブを作成し、後でジョブにタグを追加できます。詳細については、「the section called “タグの使用”」を参照してください。

AWS CLI の使用

次の AWS CLI の例では、ジョブタグをジョブのラベルとして使用して S3 バッチ操作 S3PutObjectCopy ジョブを作成します。

1. バッチ操作ジョブで実行するアクションまたは OPERATION を選択してから、TargetResource を選択します。

```
read -d '' OPERATION <<EOF
{
  "S3PutObjectCopy": {
    "TargetResource": "arn:aws:s3:::amzn-s3-demo-destination-bucket"
  }
}
EOF
```

2. ジョブに必要なジョブ TAGS を特定します。この場合、2 つのタグ department および FiscalYear を適用し、値 Marketing および 2020 をそれぞれ使用します。

```
read -d '' TAGS <<EOF
[
  {
    "Key": "department",
    "Value": "Marketing"
  },
  {
    "Key": "FiscalYear",
    "Value": "2020"
  }
]
EOF
```

3. バッチ操作ジョブの MANIFEST を指定します。

```
read -d '' MANIFEST <<EOF
{
  "Spec": {
    "Format": "EXAMPLE_S3BatchOperations_CSV_20180820",
    "Fields": [
      "Bucket",
      "Key"
    ]
  },
```

```
  "Location": {
    "ObjectArn": "arn:aws:s3:::amzn-s3-demo-manifest-bucket/example_manifest.csv",
    "ETag": "example-5dc7a8bfb90808fc5d546218"
  }
}
EOF
```

4. バッチ操作ジョブの REPORT を設定します。

```
read -d '' REPORT <<EOF
{
  "Bucket": "arn:aws:s3:::amzn-s3-demo-completion-report-bucket",
  "Format": "Example_Report_CSV_20180820",
  "Enabled": true,
  "Prefix": "reports/copy-with-replace-metadata",
  "ReportScope": "AllTasks"
}
EOF
```

5. create-job アクションを実行し、前のステップで設定した入力を使用してバッチ操作ジョブを作成します。

```
aws \
    s3control create-job \
    --account-id 123456789012 \
    --manifest "${MANIFEST//$'\n'}" \
    --operation "${OPERATION//$'\n'/}" \
    --report "${REPORT//$'\n'}" \
    --priority 10 \
    --role-arn arn:aws:iam::123456789012:role/batch-operations-role \
    --tags "${TAGS//$'\n'/}" \
    --client-request-token "$(uuidgen)" \
    --region us-west-2 \
    --description "Copy with Replace Metadata";
```

AWS SDK for Java の使用

Example

次の例では、AWS SDK for Java を使用して、タグ付き S3 バッチ操作ジョブを作成します。

```
public String createJob(final AWSS3ControlClient awss3ControlClient) {
```

```
    final String manifestObjectArn = "arn:aws:s3:::amzn-s3-demo-manifest-bucket/
manifests/10_manifest.csv";
    final String manifestObjectVersionId = "example-5dc7a8bfb90808fc5d546218";

    final JobManifestLocation manifestLocation = new JobManifestLocation()
            .withObjectArn(manifestObjectArn)
            .withETag(manifestObjectVersionId);

    final JobManifestSpec manifestSpec =
            new
 JobManifestSpec().withFormat(JobManifestFormat.S3InventoryReport_CSV_20161130);

    final JobManifest manifestToPublicApi = new JobManifest()
            .withLocation(manifestLocation)
            .withSpec(manifestSpec);

    final String jobReportBucketArn = "arn:aws:s3:::amzn-s3-demo-completion-report-
bucket";
    final String jobReportPrefix = "example-job-reports";

    final JobReport jobReport = new JobReport()
            .withEnabled(true)
            .withReportScope(JobReportScope.AllTasks)
            .withBucket(jobReportBucketArn)
            .withPrefix(jobReportPrefix)
            .withFormat(JobReportFormat.Report_CSV_20180820);

    final String lambdaFunctionArn = "arn:aws:lambda:us-
west-2:123456789012:function:example-function";

    final JobOperation jobOperation = new JobOperation()
            .withLambdaInvoke(new
 LambdaInvokeOperation().withFunctionArn(lambdaFunctionArn));

    final S3Tag departmentTag = new
 S3Tag().withKey("department").withValue("Marketing");
    final S3Tag fiscalYearTag = new S3Tag().withKey("FiscalYear").withValue("2020");

    final String roleArn = "arn:aws:iam::123456789012:role/example-batch-operations-
role";
    final Boolean requiresConfirmation = true;
    final int priority = 10;

    final CreateJobRequest request = new CreateJobRequest()
```

```
            .withAccountId("123456789012")
            .withDescription("Test lambda job")
            .withManifest(manifestToPublicApi)
            .withOperation(jobOperation)
            .withPriority(priority)
            .withRoleArn(roleArn)
            .withReport(jobReport)
            .withTags(departmentTag, fiscalYearTag)
            .withConfirmationRequired(requiresConfirmation);

    final CreateJobResult result = awss3ControlClient.createJob(request);

    return result.getJobId();
}
```

S3 バッチ操作ジョブからタグを削除

これらの例を使用して、Amazon S3 バッチオペレーションジョブからタグを削除できます。

AWS CLI を使用する場合

次の例では、AWS CLI を使用してバッチ操作ジョブからタグを削除します。

```
aws \
    s3control delete-job-tagging \
    --account-id 123456789012 \
    --job-id Example-e25a-4ed2-8bee-7f8ed7fc2f1c \
    --region us-east-1
```

バッチ操作ジョブのジョブタグを削除する

Example

次の例では、AWS SDK for Java を使用して S3 バッチ操作ジョブのタグを削除します。

```
public void deleteJobTagging(final AWSS3ControlClient awss3ControlClient,
                             final String jobId) {
    final DeleteJobTaggingRequest deleteJobTaggingRequest = new
 DeleteJobTaggingRequest()
            .withJobId(jobId);

    final DeleteJobTaggingResult deleteJobTaggingResult =
                awss3ControlClient.deleteJobTagging(deleteJobTaggingRequest);
```

```
}
```

既存のバッチオペレーションジョブへのジョブタグの追加

PutJobTagging API オペレーションを使用して、既存の Amazon S3 バッチオペレーションジョブにジョブタグを追加できます。詳細については、以下の例を参照してください。

AWS CLI を使用する場合

AWS CLI を使用し、`s3control put-job-tagging` を使用して S3 バッチオペレーションジョブにジョブタグを追加する例を次に示します。例を使用するには、*`user input placeholders`* をユーザー自身の情報に置き換えます。

> **Note**
>
> タグセットを空にしてこのリクエストを送信すると、バッチオペレーション によってオブジェクトの既存のタグセットが削除されます。ただし、この方法を使用する場合は、階層 1 リクエスト (PUT) に対して料金が発生します。詳細については、「Amazon S3 の料金」を参照してください。
> 代わりに、バッチオペレーションジョブの既存のタグを削除するには、DeleteJobTagging オペレーションをお勧めします。このオペレーションでは、料金が発生せずに同じ結果が得られるためです。

1. ジョブに必要なジョブ TAGS を特定します。この場合、2 つのタグ *`department`* および *`FiscalYear`* を適用し、値 *`Marketing`* および *`2020`* をそれぞれ使用します。

   ```
   read -d '' TAGS <<EOF
   [
     {
       "Key": "department",
       "Value": "Marketing"
     },
     {
       "Key": "FiscalYear",
       "Value": "2020"
     }
   ]
   EOF
   ```

2. 次の必須パラメータを使用して、`put-job-tagging` コマンドを実行します。

```
aws \
    s3control put-job-tagging \
    --account-id 123456789012 \
    --tags "${TAGS//$'\n'/}" \
    --job-id Example-e25a-4ed2-8bee-7f8ed7fc2f1c \
    --region us-east-1
```

AWS SDK for Java の使用

Example

次の例では、AWS SDK for Java を使用して S3 バッチオペレーションジョブのタグを配置します。

```
public void putJobTagging(final AWSS3ControlClient awss3ControlClient,
                          final String jobId) {
    final S3Tag departmentTag = new
 S3Tag().withKey("department").withValue("Marketing");
    final S3Tag fiscalYearTag = new S3Tag().withKey("FiscalYear").withValue("2020");

    final PutJobTaggingRequest putJobTaggingRequest = new PutJobTaggingRequest()
            .withJobId(jobId)
            .withTags(departmentTag, fiscalYearTag);

    final PutJobTaggingResult putJobTaggingResult =
 awss3ControlClient.putJobTagging(putJobTaggingRequest);
}
```

S3 バッチ操作ジョブのタグの取得

Amazon S3 バッチオペレーションジョブのタグを取得するには、GetJobTagging API オペレーションを使用できます。詳細については、以下の例を参照してください。

AWS CLI の使用

次の例では、AWS CLI を使用してバッチ操作ジョブのタグを取得します。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws \
    s3control get-job-tagging \
    --account-id 123456789012 \
```

```
    --job-id Example-e25a-4ed2-8bee-7f8ed7fc2f1c \
    --region us-east-1
```

AWS SDK for Java の使用

Example

次の例では、AWS SDK for Java を使用してバッチ操作ジョブのタグを取得します。

```
public List<S3Tag> getJobTagging(final AWSS3ControlClient awss3ControlClient,
                                 final String jobId) {
    final GetJobTaggingRequest getJobTaggingRequest = new GetJobTaggingRequest()
            .withJobId(jobId);

    final GetJobTaggingResult getJobTaggingResult =
            awss3ControlClient.getJobTagging(getJobTaggingRequest);

    final List<S3Tag> tags = getJobTaggingResult.getTags();

    return tags;
}
```

ジョブタグを使用したバッチオペレーションのアクセス許可の制御

Amazon S3 バッチオペレーションジョブの管理に役立つように、ジョブタグを追加できます。ジョブタグを使用すると、バッチ操作ジョブへのアクセスをコントロールし、ジョブの作成時にタグが適用されるようにできます。

バッチ操作ジョブごとに最大 50 個のジョブタグを適用できます。タグを使用することで、ジョブを編集できるユーザーのセットを制限する詳細なポリシーを設定できます。ジョブタグを使用して、ユーザーによるジョブのキャンセル、確認状態にあるジョブの有効化、ジョブの優先度レベルの変更を許可したり制限したりできます。さらに、すべての新しいジョブにタグが適用されるようにし、タグに許可されるキーと値のペアを指定できます。これらのすべての条件を AWS Identity and Access Management IAM ポリシー言語を使用して表現できます。詳細については、「サービス認証リファレンス」の「Actions, resources, and condition keys for Amazon S3」を参照してください。

S3 リソースタイプ別の S3 API オペレーションへのアクセス許可の詳細については、「Amazon S3 API オペレーションに必要なアクセス許可」を参照してください。

以下の例では、S3 バッチ操作ジョブタグを使用して、特定の部門(たとえば、財務またはコンプライアンス部門) 内で実行されるジョブのみを作成および編集するアクセス許可をユーザーに付与する方

法を示しています。QA や本番稼働など、関連する開発のステージに基づいてジョブを割り当てることもできます。

この例では、IAM ポリシーで S3 バッチオペレーションのジョブタグを使用して、部門内で実行されているジョブのみを作成および編集するアクセス権限をユーザーに付与します。QA や本番稼働など、関連する開発のステージに基づいてジョブを割り当てます。

以下の例では、次の部門を使用しています。各部門では、バッチオペレーションをさまざまな方法で使用しています。

- 財務
- コンプライアンス
- ビジネスインテリジェンス
- エンジニアリング

トピック

- ユーザーとリソースへのタグの割り当てによるアクセスのコントロール
- バッチ操作ジョブをステージ別にタグ付けし、ジョブの優先度の制限を強制する

ユーザーとリソースへのタグの割り当てによるアクセスのコントロール

このシナリオでは、管理者は属性ベースのアクセスコントロール (ABAC) を使用しています。ABAC は、ユーザーと AWS リソースの両方にタグを付けることでアクセス許可を定義する IAM 認可戦略です。

ユーザーとジョブには、以下の部門タグのいずれかが割り当てられます。

キー : 値

- `department : Finance`
- `department : Compliance`
- `department : BusinessIntelligence`
- `department : Engineering`

> **Note**
>
> ジョブタグのキーと値は大文字と小文字が区別されます。

ABAC アクセスコントロール戦略を使用して、タグ department=Finance をユーザーと関連付けることで、財務部門のユーザーに対して、部門内で S3 バッチ操作ジョブを作成および管理するアクセス許可を付与します。

さらにマネージドポリシーを IAM ユーザーにアタッチして、社内のすべてのユーザーに、それぞれの部門内での S3 バッチ操作ジョブの作成または変更を許可できます。

この例のポリシーには、3 つのポリシーステートメントが含まれています。

- ポリシーの最初のステートメントでは、ユーザーに対して、ジョブ作成リクエストにそれぞれの部門に一致するジョブタグが含まれている場合に、バッチ操作ジョブの作成を許可しています。これは、"${aws:PrincipalTag/department}" 構文を使用して表現され、ポリシー評価時にユーザーの部門タグに置き換えられます。リクエスト ("aws:RequestTag/department") の部門タグに指定した値がユーザーの部門と一致すると、条件が満たされます。
- ポリシーの 2 番目のステートメントでは、ユーザーに対して、更新対象のジョブがそのユーザーの部門と一致する場合に、ジョブの優先度の変更、ジョブのステータスの更新を許可しています。
- 3 番目のステートメントでは、ユーザーに対して、(1) 部門タグが保持され、(2) 更新対象のジョブが部門内にある限り、PutJobTagging リクエストによりいつでもバッチ操作ジョブのタグを更新することを許可しています。

```
{
      "Version": "2012-10-17",
      "Statement": [
            {
                  "Effect": "Allow",
                  "Action": "s3:CreateJob",
                  "Resource": "*",
                  "Condition": {
                        "StringEquals": {
                              "aws:RequestTag/department": "${aws:PrincipalTag/
department}"
                }
            }
        },
            {
                  "Effect": "Allow",
                  "Action": [
                        "s3:UpdateJobPriority",
                        "s3:UpdateJobStatus"
            ],
```

```
                "Resource": "*",
                "Condition": {
                      "StringEquals": {
                            "aws:ResourceTag/department": "${aws:PrincipalTag/
department}"
                }
            }
        },
            {
                "Effect": "Allow",
                "Action": "s3:PutJobTagging",
                "Resource": "*",
                "Condition": {
                      "StringEquals": {
                            "aws:RequestTag/department": "${aws:PrincipalTag/
department}",
                            "aws:ResourceTag/department": "${aws:PrincipalTag/
department}"
                }
            }
        }
    ]
}
```

バッチ操作ジョブをステージ別にタグ付けし、ジョブの優先度の制限を強制する

すべての S3 バッチ操作ジョブには数値優先順位があり、Amazon S3 がジョブを実行する順序を決定します。この例では、以下のように、ほとんどのユーザーがジョブに割り当てることができる最大優先度を制限し、高い優先度の範囲を特権のあるユーザーの限定セット用に予約します。

- QA ステージの優先度の範囲 (低): 1 ~ 100
- 本番稼働ステージの優先度の範囲 (高): 1 ~ 300

そのためには、ジョブのステージを表す新しいタグのセットを導入します。

キー : 値

- `stage : QA`
- `stage : Production`

部門内での優先度の低いジョブの作成と更新

このポリシーでは、S3 バッチ操作ジョブの作成と更新に対して、部門ベースの制限に加えて 2 つの新しい制限を導入します。

- ジョブにタグ stage=QA が含まれていることを必須とする新しい条件を使用して、ユーザーに、それぞれの部門内でジョブを作成または更新することを許可する。
- ユーザーに、新しい最大優先度 100 までのジョブを作成または更新することを許可する。

```
{
        "Version": "2012-10-17",
        "Statement": [
        {
        "Effect": "Allow",
        "Action": "s3:CreateJob",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:RequestTag/department": "${aws:PrincipalTag/department}",
                "aws:RequestTag/stage": "QA"
            },
            "NumericLessThanEquals": {
                "s3:RequestJobPriority": 100
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": [
            "s3:UpdateJobStatus"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:ResourceTag/department": "${aws:PrincipalTag/department}"
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": "s3:UpdateJobPriority",
        "Resource": "*",
```

```
        "Condition": {
            "StringEquals": {
                "aws:ResourceTag/department": "${aws:PrincipalTag/department}",
                "aws:ResourceTag/stage": "QA"
            },
            "NumericLessThanEquals": {
                "s3:RequestJobPriority": 100
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": "s3:PutJobTagging",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:RequestTag/department" : "${aws:PrincipalTag/department}",
                "aws:ResourceTag/department": "${aws:PrincipalTag/department}",
                "aws:RequestTag/stage": "QA",
                "aws:ResourceTag/stage": "QA"
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": "s3:GetJobTagging",
        "Resource": "*"
    }
    ]
}
```

部門内での優先度の高いジョブの作成と更新

少数のユーザーのみが QA または本番稼働で優先度の高いジョブを作成できる必要があるとします。このニーズに応えるには、前のセクションの優先度の低いポリシーを採用した管理ポリシーを作成します。

このポリシーは以下の処理を実行します。

- タグ stage=QA または stage=Production のいずれかを使用して、ユーザーに、部門内でジョブを作成または更新することを許可する。
- ユーザーに、最大優先度 300 までのジョブを作成または更新することを許可する。

```
{
      "Version": "2012-10-17",
      "Statement": [
          {
                "Effect": "Allow",
                "Action": "s3:CreateJob",
                "Resource": "*",
                "Condition": {
                      "ForAnyValue:StringEquals": {
                            "aws:RequestTag/stage": [
                                  "QA",
                                  "Production"
                    ]
                },
                      "StringEquals": {
                            "aws:RequestTag/department": "${aws:PrincipalTag/
department}"
                },
                      "NumericLessThanEquals": {
                            "s3:RequestJobPriority": 300
                }
            }
        },
          {
                "Effect": "Allow",
                "Action": [
                      "s3:UpdateJobStatus"
            ],
                "Resource": "*",
                "Condition": {
                      "StringEquals": {
                            "aws:ResourceTag/department": "${aws:PrincipalTag/
department}"
                }
            }
        },
          {
                "Effect": "Allow",
                "Action": "s3:UpdateJobPriority",
                "Resource": "*",
                "Condition": {
                      "ForAnyValue:StringEquals": {
                            "aws:ResourceTag/stage": [
```

```
                                    "QA",
                                    "Production"
                    ]
                },
                      "StringEquals": {
                            "aws:ResourceTag/department": "${aws:PrincipalTag/
department}"
                },
                      "NumericLessThanEquals": {
                            "s3:RequestJobPriority": 300
                }
            }
        },
          {
                "Effect": "Allow",
                "Action": "s3:PutJobTagging",
                "Resource": "*",
                "Condition": {
                      "StringEquals": {
                            "aws:RequestTag/department": "${aws:PrincipalTag/
department}",
                            "aws:ResourceTag/department": "${aws:PrincipalTag/
department}"
                },
                      "ForAnyValue:StringEquals": {
                            "aws:RequestTag/stage": [
                                    "QA",
                                    "Production"
                    ],
                            "aws:ResourceTag/stage": [
                                    "QA",
                                    "Production"
                    ]
                }
            }
        }
    ]
}
```

S3 バッチ操作を使用した S3 オブジェクトロックの管理

S3 バッチ操作を使用すると、Amazon S3 のオブジェクトに対して大規模なバッチ操作を実行することができます。S3 バッチ操作では、指定した Amazon S3 のオブジェクトのリストに対して、1 つ

のオペレーションを実行できます。1 つのジョブで、エクサバイトのデータを含む数十億ものオブジェクトに対して、指定されたオペレーションを実行できます。Amazon S3 は、進捗状況の追跡、通知の送信、すべてのアクションの詳細な完了レポートの保存を行い、フルマネージド型の監査可能なサーバーレスエクスペリエンスを提供します。S3 バッチオペレーションは、Amazon S3 コンソール、AWS CLI、AWS SDK、または Amazon S3 REST API を通じて使用できます。

S3 オブジェクトロックを使用すると、オブジェクトバージョンにリーガルホールドを設定することができます。保持期間の設定と同様に、リーガルホールドは、オブジェクトバージョンが上書きまたは削除されるのを防ぎます。ただし、リーガルホールドには関連する保持期間はなく、リーガルホールドが削除されるまで有効です。詳細については、「S3 オブジェクトロックのリーガルホールド」を参照してください。

S3 バッチオペレーションと Object Lock を使用すると、一度に多くの Amazon S3 のオブジェクトをリーガルホールドにすることができます。以下のトピックを参照してください。

トピック

- S3 バッチ操作を使用した S3 オブジェクトロックの有効化
- バッチ操作を使用したオブジェクトロック保持の設定
- S3 オブジェクトロック保持コンプライアンスモードでの S3 バッチ操作の使用
- S3 オブジェクトロック保持ガバナンスモードで S3 バッチ操作を使用する
- S3 バッチオペレーションを使用した S3 Object Lock のリーガルホールドの無効化

S3 バッチ操作を使用した S3 オブジェクトロックの有効化

Amazon S3 バッチオペレーションを S3 Object Lock とともに使用すると、一度に多くの Amazon S3 オブジェクトの保持を管理したり、リーガルホールドを有効にしたりできます。マニフェストでターゲットオブジェクトのリストを指定し、そのマニフェストをジョブの完了のためにバッチ操作に送信します。詳細については、「the section called “オブジェクトロックの保持”」および「the section called “オブジェクトロックのリーガルホールド”」を参照してください。

以下の例では、S3 バッチオペレーションアクセス許可を持つ AWS Identity and Access Management (IAM) ロールを作成し、そのロールのアクセス許可を更新して Object Lock を有効化するジョブを作成する方法を示します。S3 バッチオペレーションジョブのオブジェクトを識別する CSV マニフェストも必要です。詳細については、「the section called “マニフェストの指定”」を参照してください。

次の例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

AWS CLI を使用する場合

1. IAM ロールを作成し、実行する S3 バッチ操作のアクセス許可を割り当てます。

   このステップは、すべての S3 バッチ操作ジョブで必要です。

```
export AWS_PROFILE='aws-user'

read -d '' batch_operations_trust_policy <<EOF
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "batchoperations.s3.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
EOF
aws iam create-role --role-name batch_operations-objectlock \
--assume-role-policy-document "${batch_operations_trust_policy}"
```

2. S3 オブジェクトロックを使用して S3 バッチ操作を実行するように設定します。

   このステップでは、ロールに以下のことを許可します。

   a. バッチ操作を実行するターゲットオブジェクトを含む S3 バケットでオブジェクトロックを実行します。

   b. マニフェスト CSV ファイルとオブジェクトがある S3 バケットを読み取る。

   c. S3 バッチ操作ジョブの結果をレポートバケットに書き込みます。

```
read -d '' batch_operations_permissions <<EOF
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Action": "s3:GetBucketObjectLockConfiguration",
            "Resource": [
                "arn:aws:s3:::{{amzn-s3-demo-manifest-bucket}}"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion",
                "s3:GetBucketLocation"
            ],
            "Resource": [
                "arn:aws:s3:::{{amzn-s3-demo-manifest-bucket}}/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetBucketLocation"
            ],
            "Resource": [
                "arn:aws:s3:::{{amzn-s3-demo-completion-report-bucket}}/*"
            ]
        }
    ]
}
EOF

aws iam put-role-policy --role-name batch_operations-objectlock \
--policy-name object-lock-permissions \
--policy-document "${batch_operations_permissions}"
```

AWS SDK for Java の使用

次の例は、S3 バッチオペレーション許可を持つ IAM ロールを作成し、AWS SDK for Java を使用して Object Lock を有効にするジョブを作成するためにロールの許可を更新する方法を示しています。S3 バッチ操作ジョブのオブジェクトを識別する CSV マニフェストも必要です。詳細については、「the section called “マニフェストの指定”」を参照してください。

以下のステップを実行します。

1. IAM ロールを作成し、実行する S3 バッチ操作のアクセス許可を割り当てます。このステップは、すべての S3 バッチ操作ジョブで必要です。
2. S3 オブジェクトロックを使用して S3 バッチ操作を実行するように設定します。

   ロールに以下のことを許可します。

   1. バッチ操作を実行するターゲットオブジェクトを含む S3 バケットでオブジェクトロックを実行します。
   2. マニフェスト CSV ファイルとオブジェクトがある S3 バケットを読み取る。
   3. S3 バッチ操作ジョブの結果をレポートバケットに書き込みます。

```
public void createObjectLockRole() {
    final String roleName = "batch_operations-object-lock";

    final String trustPolicy = "{" +
            "  \"Version\": \"2012-10-17\", " +
            "  \"Statement\": [ " +
            "    { " +
            "      \"Effect\": \"Allow\", " +
            "      \"Principal\": { " +
            "        \"Service\": [" +
            "          \"batchoperations.s3.amazonaws.com\"" +
            "        ]" +
            "      }, " +
            "      \"Action\": \"sts:AssumeRole\" " +
            "    } " +
            "  ]" +
            "}";

    final String bopsPermissions = "{" +
            "    \"Version\": \"2012-10-17\"," +
            "    \"Statement\": [" +
            "        {" +
            "            \"Effect\": \"Allow\"," +
            "            \"Action\": \"s3:GetBucketObjectLockConfiguration\"," +
            "            \"Resource\": [" +
            "                \"arn:aws:s3:::amzn-s3-demo-manifest-bucket\"" +
            "            ]" +
            "        }," +
```

```
            "        {" +
            "            \"Effect\": \"Allow\"," +
            "            \"Action\": [" +
            "                \"s3:GetObject\"," +
            "                \"s3:GetObjectVersion\"," +
            "                \"s3:GetBucketLocation\"" +
            "            ]," +
            "            \"Resource\": [" +
            "                \"arn:aws:s3:::amzn-s3-demo-manifest-bucket/*\"" +
            "            ]" +
            "        }," +
            "        {" +
            "            \"Effect\": \"Allow\"," +
            "            \"Action\": [" +
            "                \"s3:PutObject\"," +
            "                \"s3:GetBucketLocation\"" +
            "            ]," +
            "            \"Resource\": [" +
            "                \"arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*\""
 +
            "            ]" +
            "        }" +
            "    ]" +
            "}";

    final AmazonIdentityManagement iam =
            AmazonIdentityManagementClientBuilder.defaultClient();

    final CreateRoleRequest createRoleRequest = new CreateRoleRequest()
            .withAssumeRolePolicyDocument(bopsPermissions)
            .withRoleName(roleName);

    final CreateRoleResult createRoleResult = iam.createRole(createRoleRequest);

    final PutRolePolicyRequest putRolePolicyRequest = new PutRolePolicyRequest()
            .withPolicyDocument(bopsPermissions)
            .withPolicyName("batch_operations-permissions")
            .withRoleName(roleName);

    final PutRolePolicyResult putRolePolicyResult =
 iam.putRolePolicy(putRolePolicyRequest);
}
```

バッチ操作を使用したオブジェクトロック保持の設定

Amazon S3 バッチオペレーションと S3 Object Lock を使用すると、多くの Amazon S3 のオブジェクトの保持期間を一括で管理できます。マニフェストでターゲットオブジェクトのリストを指定し、そのマニフェストをジョブの完了のためにバッチ操作に送信します。詳細については、「the section called “オブジェクトロックの保持”」および「the section called “オブジェクトロックのリーガルホールド”」を参照してください。

次の例は、S3 バッチオペレーションのアクセス許可を持つ AWS Identity and Access Management (IAM) ロールを作成し、マニフェストバケット内のオブジェクトで S3 Object Lock 保持を実行できるように、`s3:PutObjectRetention` アクセス許可を含めるようロールアクセス許可を更新する方法を示しています。S3 バッチオペレーションジョブのオブジェクトを識別する CSV マニフェストも必要です。詳細については、「the section called “マニフェストの指定”」を参照してください。

次の例を実行するには、*`user input placeholders`* をユーザー自身の情報に置き換えます。

AWS CLI を使用する場合

次の AWS CLI の例は、バッチオペレーションを使用して、複数のオブジェクトに S3 Object Lock 保持を適用する方法を示しています。

```
export AWS_PROFILE='aws-user'

read -d '' retention_permissions <<EOF
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObjectRetention"
            ],
            "Resource": [
                "arn:aws:s3:::{{amzn-s3-demo-manifest-bucket}}/*"
            ]
        }
    ]
}
EOF

aws iam put-role-policy --role-name batch_operations-objectlock --policy-
name retention-permissions --policy-document "${retention_permissions}"
```

AWS SDK for Java の使用

次の AWS SDK for Java の例は、バッチオペレーションを使用して、複数のオブジェクトに S3 Object Lock 保持を適用する方法を示しています。

```
public void allowPutObjectRetention() {
    final String roleName = "batch_operations-object-lock";

    final String retentionPermissions = "{" +
            "    \"Version\": \"2012-10-17\"," +
            "    \"Statement\": [" +
            "        {" +
            "            \"Effect\": \"Allow\"," +
            "            \"Action\": [" +
            "                \"s3:PutObjectRetention\"" +
            "            ]," +
            "            \"Resource\": [" +
            "                \"arn:aws:s3:::amzn-s3-demo-manifest-bucket*\"" +
            "            ]" +
            "        }" +
            "    ]" +
            "}";

    final AmazonIdentityManagement iam =
            AmazonIdentityManagementClientBuilder.defaultClient();

    final PutRolePolicyRequest putRolePolicyRequest = new PutRolePolicyRequest()
            .withPolicyDocument(retentionPermissions)
            .withPolicyName("retention-permissions")
            .withRoleName(roleName);

    final PutRolePolicyResult putRolePolicyResult =
 iam.putRolePolicy(putRolePolicyRequest);
}
```

S3 オブジェクトロック保持コンプライアンスモードでの S3 バッチ操作の使用

以下の例は、信頼ポリシーを作成し、オブジェクトに S3 バッチ操作と S3 オブジェクトロックの設定アクセス許可を設定する前の例に基づいています。この例では、保持モードを COMPLIANCE に、retain until date を 2025 年 1 月 1 日に設定しています。この例では、マニフェストバケット内のオブジェクトをターゲットとし、指定したレポートバケットに結果を書き込むジョブを作成します。

次の例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

AWS CLI を使用する場合

次の AWS CLI の例は、バッチオペレーションを使用して、複数のオブジェクトに S3 Object Lock 保持コンプライアンスモードを適用する方法を示しています。

Example – 複数のオブジェクトに S3 Object Lock 保持コンプライアンスモードを設定する

```
export AWS_PROFILE='aws-user'
export AWS_DEFAULT_REGION='us-west-2'
export ACCOUNT_ID=123456789012
export ROLE_ARN='arn:aws:iam::123456789012:role/batch_operations-objectlock'

read -d '' OPERATION <<EOF
{
  "S3PutObjectRetention": {
    "Retention": {
      "RetainUntilDate":"2025-01-01T00:00:00",
      "Mode":"COMPLIANCE"
    }
  }
}
EOF

read -d '' MANIFEST <<EOF
{
  "Spec": {
    "Format": "S3BatchOperations_CSV_20180820",
    "Fields": [
      "Bucket",
      "Key"
    ]
  },
  "Location": {
    "ObjectArn": "arn:aws:s3:::amzn-s3-demo-manifest-bucket/compliance-objects-
manifest.csv",
    "ETag": "Your-manifest-ETag"
  }
}
EOF

read -d '' REPORT <<EOF
{
```

```
  "Bucket": "arn:aws:s3:::ReportBucket",
  "Format": "Report_CSV_20180820",
  "Enabled": true,
  "Prefix": "amzn-s3-demo-completion-report-bucket/compliance-objects-batch-
operations",
  "ReportScope": "AllTasks"
}
EOF

aws \
    s3control create-job \
    --account-id "${ACCOUNT_ID}" \
    --manifest "${MANIFEST//$'\n'}" \
    --operation "${OPERATION//$'\n'/}" \
    --report "${REPORT//$'\n'}" \
    --priority 10 \
    --role-arn "${ROLE_ARN}" \
    --client-request-token "$(uuidgen)" \
    --region "${AWS_DEFAULT_REGION}" \
    --description "Set compliance retain-until to 1 Jul 2030";
```

Example – **COMPLIANCE** モードの **retain until date** を 2025 年 1 月 15 日に延長する

以下の例では、COMPLIANCE モードの retain until date を 2025 年 1 月 15 日に延長します。

```
export AWS_PROFILE='aws-user'
export AWS_DEFAULT_REGION='us-west-2'
export ACCOUNT_ID=123456789012
export ROLE_ARN='arn:aws:iam::123456789012:role/batch_operations-objectlock'

read -d '' OPERATION <<EOF
{
  "S3PutObjectRetention": {
    "Retention": {
      "RetainUntilDate":"2025-01-15T00:00:00",
      "Mode":"COMPLIANCE"
    }
  }
}
EOF

read -d '' MANIFEST <<EOF
{
  "Spec": {
```

```
    "Format": "S3BatchOperations_CSV_20180820",
    "Fields": [
      "Bucket",
      "Key"
    ]
  },
  "Location": {
    "ObjectArn": "arn:aws:s3:::amzn-s3-demo-manifest-bucket/compliance-objects-
manifest.csv",
    "ETag": "Your-manifest-ETag"
  }
}
EOF

read -d '' REPORT <<EOF
{
  "Bucket": "arn:aws:s3:::amzn-s3-demo-completion-report-bucket",
  "Format": "Report_CSV_20180820",
  "Enabled": true,
  "Prefix": "reports/compliance-objects-batch_operations",
  "ReportScope": "AllTasks"
}
EOF

aws \
    s3control create-job \
    --account-id "${ACCOUNT_ID}" \
    --manifest "${MANIFEST//$'\n'}" \
    --operation "${OPERATION//$'\n'/}" \
    --report "${REPORT//$'\n'}" \
    --priority 10 \
    --role-arn "${ROLE_ARN}" \
    --client-request-token "$(uuidgen)" \
    --region "${AWS_DEFAULT_REGION}" \
    --description "Extend compliance retention to 15 Jan 2025";
```

AWS SDK for Java の使用

次の AWS SDK for Java の例は、バッチオペレーションを使用して、複数のオブジェクトに S3 Object Lock 保持コンプライアンスモードを適用する方法を示しています。

Example – 保持モードを「COMPLIANCE」に設定して、保持期間を 2025 年 1 月 1 日に設定する

```
public String createComplianceRetentionJob(final AWSS3ControlClient awss3ControlClient)
 throws ParseException {
    final String manifestObjectArn = "arn:aws:s3:::amzn-s3-demo-manifest-bucket/
compliance-objects-manifest.csv";
    final String manifestObjectVersionId = "your-object-version-Id";

    final JobManifestLocation manifestLocation = new JobManifestLocation()
            .withObjectArn(manifestObjectArn)
            .withETag(manifestObjectVersionId);

    final JobManifestSpec manifestSpec =
            new JobManifestSpec()
                    .withFormat(JobManifestFormat.S3BatchOperations_CSV_20180820)
                    .withFields("Bucket", "Key");

    final JobManifest manifestToPublicApi = new JobManifest()
            .withLocation(manifestLocation)
            .withSpec(manifestSpec);

    final String jobReportBucketArn = "arn:aws:s3:::amzn-s3-demo-completion-report-
bucket";
    final String jobReportPrefix = "reports/compliance-objects-bops";

    final JobReport jobReport = new JobReport()
            .withEnabled(true)
            .withReportScope(JobReportScope.AllTasks)
            .withBucket(jobReportBucketArn)
            .withPrefix(jobReportPrefix)
            .withFormat(JobReportFormat.Report_CSV_20180820);

    final SimpleDateFormat format = new SimpleDateFormat("dd/MM/yyyy");
    final Date janFirst = format.parse("01/01/2025");

    final JobOperation jobOperation = new JobOperation()
            .withS3PutObjectRetention(new S3SetObjectRetentionOperation()
                    .withRetention(new S3Retention()
                            .withMode(S3ObjectLockRetentionMode.COMPLIANCE)
                            .withRetainUntilDate(janFirst)));

    final String roleArn = "arn:aws:iam::123456789012:role/batch_operations-object-
lock";
    final Boolean requiresConfirmation = true;
```

```
    final int priority = 10;

    final CreateJobRequest request = new CreateJobRequest()
            .withAccountId("123456789012")
            .withDescription("Set compliance retain-until to 1 Jan 2025")
            .withManifest(manifestToPublicApi)
            .withOperation(jobOperation)
            .withPriority(priority)
            .withRoleArn(roleArn)
            .withReport(jobReport)
            .withConfirmationRequired(requiresConfirmation);

    final CreateJobResult result = awss3ControlClient.createJob(request);

    return result.getJobId();
}
```

Example – **COMPLIANCE** モードを **retain until date** に延長する

以下の例では、COMPLIANCE モードの `retain until date` を 2025 年 1 月 15 日に延長します。

```
public String createExtendComplianceRetentionJob(final AWSS3ControlClient
 awss3ControlClient) throws ParseException {
    final String manifestObjectArn = "arn:aws:s3:::amzn-s3-demo-manifest-bucket/
compliance-objects-manifest.csv";
    final String manifestObjectVersionId = "15ad5ba069e6bbc465c77bf83d541385";

    final JobManifestLocation manifestLocation = new JobManifestLocation()
            .withObjectArn(manifestObjectArn)
            .withETag(manifestObjectVersionId);

    final JobManifestSpec manifestSpec =
            new JobManifestSpec()
                    .withFormat(JobManifestFormat.S3BatchOperations_CSV_20180820)
                    .withFields("Bucket", "Key");

    final JobManifest manifestToPublicApi = new JobManifest()
            .withLocation(manifestLocation)
            .withSpec(manifestSpec);

    final String jobReportBucketArn = "arn:aws:s3:::amzn-s3-demo-completion-report-
bucket";
    final String jobReportPrefix = "reports/compliance-objects-batch_operations";
```

```
    final JobReport jobReport = new JobReport()
            .withEnabled(true)
            .withReportScope(JobReportScope.AllTasks)
            .withBucket(jobReportBucketArn)
            .withPrefix(jobReportPrefix)
            .withFormat(JobReportFormat.Report_CSV_20180820);

    final SimpleDateFormat format = new SimpleDateFormat("dd/MM/yyyy");
    final Date jan15th = format.parse("15/01/2025");

    final JobOperation jobOperation = new JobOperation()
            .withS3PutObjectRetention(new S3SetObjectRetentionOperation()
                    .withRetention(new S3Retention()
                            .withMode(S3ObjectLockRetentionMode.COMPLIANCE)
                            .withRetainUntilDate(jan15th)));

    final String roleArn = "arn:aws:iam::123456789012:role/batch_operations-object-
lock";
    final Boolean requiresConfirmation = true;
    final int priority = 10;

    final CreateJobRequest request = new CreateJobRequest()
            .withAccountId("123456789012")
            .withDescription("Extend compliance retention to 15 Jan 2025")
            .withManifest(manifestToPublicApi)
            .withOperation(jobOperation)
            .withPriority(priority)
            .withRoleArn(roleArn)
            .withReport(jobReport)
            .withConfirmationRequired(requiresConfirmation);

    final CreateJobResult result = awss3ControlClient.createJob(request);

    return result.getJobId();
}
```

S3 オブジェクトロック保持ガバナンスモードで S3 バッチ操作を使用する

次の例は、信頼ポリシーを作成し、S3 バッチ操作と S3 オブジェクトロックの設定アクセス許可を設定する前の例に基づいています。この例は、2025 年 1 月 30 日の `retain until date` で S3 Object Lock 保持ガバナンスを複数のオブジェクトに適用する方法を示しています。また、マニフェストバケットを使用しレポートバケットに結果を書き込むバッチ操作ジョブを作成します。

次の例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

AWS CLI を使用する場合

次の AWS CLI の例は、バッチオペレーションを使用して、複数のオブジェクトに S3 Object Lock 保持ガバナンスモードを適用する方法を示しています。

Example – 2025 年 1 月 30 日まで保持する複数のオブジェクトに S3 Object Lock 保持ガバナンスを適用する

```
export AWS_PROFILE='aws-user'
export AWS_DEFAULT_REGION='us-west-2'
export ACCOUNT_ID=123456789012
export ROLE_ARN='arn:aws:iam::123456789012:role/batch_operations-objectlock'

read -d '' OPERATION <<EOF
{
  "S3PutObjectRetention": {
    "Retention": {
      "RetainUntilDate":"2025-01-30T00:00:00",
      "Mode":"GOVERNANCE"
    }
  }
}
EOF

read -d '' MANIFEST <<EOF
{
  "Spec": {
    "Format": "S3BatchOperations_CSV_20180820",
    "Fields": [
      "Bucket",
      "Key"
    ]
  },
  "Location": {
    "ObjectArn": "arn:aws:s3:::amzn-s3-demo-manifest-bucket/governance-objects-
manifest.csv",
    "ETag": "Your-manifest-ETag"
  }
}
EOF

read -d '' REPORT <<EOF
```

```
{
  "Bucket": "arn:aws:s3:::amzn-s3-demo-completion-report-bucketT",
  "Format": "Report_CSV_20180820",
  "Enabled": true,
  "Prefix": "reports/governance-objects",
  "ReportScope": "AllTasks"
}
EOF

aws \
    s3control create-job \
    --account-id "${ACCOUNT_ID}" \
    --manifest "${MANIFEST//$'\n'}" \
    --operation "${OPERATION//$'\n'/}" \
    --report "${REPORT//$'\n'}" \
    --priority 10 \
    --role-arn "${ROLE_ARN}" \
    --client-request-token "$(uuidgen)" \
    --region "${AWS_DEFAULT_REGION}" \
    --description "Put governance retention";
```

Example – 複数のオブジェクト間での保持ガバナンスのバイパス

次の例は、信頼ポリシーを作成し、S3 バッチ操作と S3 オブジェクトロックの設定アクセス許可を設定する前の例に基づいています。また、複数のオブジェクト間で保持ガバナンスを省略する方法を示し、マニフェストバケットを使用しレポートバケットに結果を書き込むバッチ操作ジョブを作成します。

```
export AWS_PROFILE='aws-user'

read -d '' bypass_governance_permissions <<EOF
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:BypassGovernanceRetention"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
            ]
        }
```

```
    ]
}
EOF

aws iam put-role-policy --role-name batch-operations-objectlock --policy-name bypass-
governance-permissions --policy-document "${bypass_governance_permissions}"

export AWS_PROFILE='aws-user'
export AWS_DEFAULT_REGION='us-west-2'
export ACCOUNT_ID=123456789012
export ROLE_ARN='arn:aws:iam::123456789012:role/batch_operations-objectlock'

read -d '' OPERATION <<EOF
{
  "S3PutObjectRetention": {
    "BypassGovernanceRetention": true,
    "Retention": {
    }
  }
}
EOF

read -d '' MANIFEST <<EOF
{
  "Spec": {
    "Format": "S3BatchOperations_CSV_20180820",
    "Fields": [
      "Bucket",
      "Key"
    ]
  },
  "Location": {
    "ObjectArn": "arn:aws:s3:::amzn-s3-demo-manifest-bucket/governance-objects-
manifest.csv",
    "ETag": "Your-manifest-ETag"
  }
}
EOF

read -d '' REPORT <<EOF
{
  "Bucket": "arn:aws:s3:::amzn-s3-demo-completion-report-bucket",
  "Format": "Report_CSV_20180820",
  "Enabled": true,
```

```
  "Prefix": "reports/batch_operations-governance",
  "ReportScope": "AllTasks"
}
EOF

aws \
    s3control create-job \
    --account-id "${ACCOUNT_ID}" \
    --manifest "${MANIFEST//$'\n'}" \
    --operation "${OPERATION//$'\n'/}" \
    --report "${REPORT//$'\n'}" \
    --priority 10 \
    --role-arn "${ROLE_ARN}" \
    --client-request-token "$(uuidgen)" \
    --region "${AWS_DEFAULT_REGION}" \
    --description "Remove governance retention";
```

AWS SDK for Java の使用

次の例は、信頼ポリシーを作成し、S3 バッチ操作と S3 オブジェクトロックの設定アクセス許可を設定する前の例に基づいています。この例では、`retain until date` を 2025 年 1 月 30 日に設定して、複数のオブジェクトにわたって S3 Object Lock 保持ガバナンスを適用する方法を示します。また、マニフェストバケットを使用して、レポートバケットに結果を書き込むバッチオペレーションジョブを作成します。

Example – 2025 年 1 月 30 日まで保持する複数のオブジェクトに S3 Object Lock 保持ガバナンスを適用する

```
public String createGovernanceRetentionJob(final AWSS3ControlClient awss3ControlClient)
 throws ParseException {
    final String manifestObjectArn = "arn:aws:s3:::amzn-s3-demo-manifest-bucket/
governance-objects-manifest.csv";
    final String manifestObjectVersionId = "15ad5ba069e6bbc465c77bf83d541385";

    final JobManifestLocation manifestLocation = new JobManifestLocation()
            .withObjectArn(manifestObjectArn)
            .withETag(manifestObjectVersionId);

    final JobManifestSpec manifestSpec =
            new JobManifestSpec()
                    .withFormat(JobManifestFormat.S3BatchOperations_CSV_20180820)
                    .withFields("Bucket", "Key");
```

```
    final JobManifest manifestToPublicApi = new JobManifest()
            .withLocation(manifestLocation)
            .withSpec(manifestSpec);

    final String jobReportBucketArn = "arn:aws:s3:::amzn-s3-demo-completion-report-
bucket";
    final String jobReportPrefix = "reports/governance-objects";

    final JobReport jobReport = new JobReport()
            .withEnabled(true)
            .withReportScope(JobReportScope.AllTasks)
            .withBucket(jobReportBucketArn)
            .withPrefix(jobReportPrefix)
            .withFormat(JobReportFormat.Report_CSV_20180820);

    final SimpleDateFormat format = new SimpleDateFormat("dd/MM/yyyy");
    final Date jan30th = format.parse("30/01/2025");

    final JobOperation jobOperation = new JobOperation()
            .withS3PutObjectRetention(new S3SetObjectRetentionOperation()
                    .withRetention(new S3Retention()
                            .withMode(S3ObjectLockRetentionMode.GOVERNANCE)
                            .withRetainUntilDate(jan30th)));

    final String roleArn = "arn:aws:iam::123456789012:role/batch_operations-object-
lock";
    final Boolean requiresConfirmation = true;
    final int priority = 10;

    final CreateJobRequest request = new CreateJobRequest()
            .withAccountId("123456789012")
            .withDescription("Put governance retention")
            .withManifest(manifestToPublicApi)
            .withOperation(jobOperation)
            .withPriority(priority)
            .withRoleArn(roleArn)
            .withReport(jobReport)
            .withConfirmationRequired(requiresConfirmation);

    final CreateJobResult result = awss3ControlClient.createJob(request);

    return result.getJobId();
}
```

Example – 複数のオブジェクト間での保持ガバナンスのバイパス

次の例は、信頼ポリシーを作成し、S3 バッチ操作と S3 オブジェクトロックの設定アクセス許可を設定する前の例に基づいています。この例では、複数のオブジェクト間で保持ガバナンスを省略する方法を示し、マニフェストバケットを使用して、レポートバケットに結果を書き込むバッチオペレーションジョブを作成します。

```
public void allowBypassGovernance() {
    final String roleName = "batch_operations-object-lock";

    final String bypassGovernancePermissions = "{" +
            "    \"Version\": \"2012-10-17\"," +
            "    \"Statement\": [" +
            "        {" +
            "            \"Effect\": \"Allow\"," +
            "            \"Action\": [" +
            "                \"s3:BypassGovernanceRetention\"" +
            "            ]," +
            "            \"Resource\": [" +
            "                \"arn:aws:s3:::amzn-s3-demo-manifest-bucket/*\"" +
            "            ]" +
            "        }" +
            "    ]" +
            "}";

    final AmazonIdentityManagement iam =
            AmazonIdentityManagementClientBuilder.defaultClient();

    final PutRolePolicyRequest putRolePolicyRequest = new PutRolePolicyRequest()
            .withPolicyDocument(bypassGovernancePermissions)
            .withPolicyName("bypass-governance-permissions")
            .withRoleName(roleName);

    final PutRolePolicyResult putRolePolicyResult =
 iam.putRolePolicy(putRolePolicyRequest);
}
public String createRemoveGovernanceRetentionJob(final AWSS3ControlClient
 awss3ControlClient) {
    final String manifestObjectArn = "arn:aws:s3:::amzn-s3-demo-manifest-bucket/
governance-objects-manifest.csv";
    final String manifestObjectVersionId = "15ad5ba069e6bbc465c77bf83d541385";

    final JobManifestLocation manifestLocation = new JobManifestLocation()
```

```
            .withObjectArn(manifestObjectArn)
            .withETag(manifestObjectVersionId);

    final JobManifestSpec manifestSpec =
            new JobManifestSpec()
                    .withFormat(JobManifestFormat.S3BatchOperations_CSV_20180820)
                    .withFields("Bucket", "Key");

    final JobManifest manifestToPublicApi = new JobManifest()
            .withLocation(manifestLocation)
            .withSpec(manifestSpec);

    final String jobReportBucketArn = "arn:aws:s3:::amzn-s3-demo-completion-report-
bucket";
    final String jobReportPrefix = "reports/batch_operations-governance";

    final JobReport jobReport = new JobReport()
            .withEnabled(true)
            .withReportScope(JobReportScope.AllTasks)
            .withBucket(jobReportBucketArn)
            .withPrefix(jobReportPrefix)
            .withFormat(JobReportFormat.Report_CSV_20180820);

    final JobOperation jobOperation = new JobOperation()
            .withS3PutObjectRetention(new S3SetObjectRetentionOperation()
                    .withRetention(new S3Retention()));

    final String roleArn = "arn:aws:iam::123456789012:role/batch_operations-object-
lock";
    final Boolean requiresConfirmation = true;
    final int priority = 10;

    final CreateJobRequest request = new CreateJobRequest()
            .withAccountId("123456789012")
            .withDescription("Remove governance retention")
            .withManifest(manifestToPublicApi)
            .withOperation(jobOperation)
            .withPriority(priority)
            .withRoleArn(roleArn)
            .withReport(jobReport)
            .withConfirmationRequired(requiresConfirmation);

    final CreateJobResult result = awss3ControlClient.createJob(request);
```

```
    return result.getJobId();
}
```

S3 バッチオペレーションを使用した S3 Object Lock のリーガルホールドの無効化

以下の例は、信頼ポリシーを作成し、S3 バッチ操作と S3 オブジェクトロックの設定アクセス許可を設定する前の例に基づいています。この例では、バッチオペレーションを使用して、オブジェクトの Object Lock のリーガルホールドを無効にする方法を示します。

この例ではまず、`s3:PutObjectLegalHold` アクセス許可を付与するようにロールを更新したうえで、マニフェストで指定されたオブジェクトから法的保留をオフにし (削除)、その結果をレポートするバッチ操作ジョブを作成します。

次の例を実行するには、*`user input placeholders`* をユーザー自身の情報に置き換えます。

AWS CLI を使用する場合

次の AWS CLI の例は、バッチオペレーションを使用して、複数のオブジェクト間で S3 Object Lock のリーガルホールドを無効にする方法を示しています。

Example – ロールを更新して **`s3:PutObjectLegalHold`** にアクセス許可を付与する

```
export AWS_PROFILE='aws-user'

read -d '' legal_hold_permissions <<EOF
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObjectLegalHold"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
            ]
        }
    ]

EOF

aws iam put-role-policy --role-name batch_operations-objectlock --policy-name legal-hold-permissions --policy-document "${legal_hold_permissions}"
```

Example – リーガルホールドをオフにする

以下の例では、リーガルホールドをオフにします。

```
export AWS_PROFILE='aws-user'
export AWS_DEFAULT_REGION='us-west-2'
export ACCOUNT_ID=123456789012
export ROLE_ARN='arn:aws:iam::123456789012:role/batch_operations-objectlock'

read -d '' OPERATION <<EOF
{
  "S3PutObjectLegalHold": {
    "LegalHold": {
      "Status":"OFF"
    }
  }
}
EOF

read -d '' MANIFEST <<EOF
{
  "Spec": {
    "Format": "S3BatchOperations_CSV_20180820",
    "Fields": [
      "Bucket",
      "Key"
    ]
  },
  "Location": {
    "ObjectArn": "arn:aws:s3:::amzn-s3-demo-manifest-bucket/legalhold-object-
manifest.csv",
    "ETag": "Your-manifest-ETag"
  }
}
EOF

read -d '' REPORT <<EOF
{
  "Bucket": "arn:aws:s3:::amzn-s3-demo-completion-report-bucket",
  "Format": "Report_CSV_20180820",
  "Enabled": true,
  "Prefix": "reports/legalhold-objects-batch_operations",
  "ReportScope": "AllTasks"
}
```

```
EOF

aws \
    s3control create-job \
    --account-id "${ACCOUNT_ID}" \
    --manifest "${MANIFEST//$'\n'}" \
    --operation "${OPERATION//$'\n'/}" \
    --report "${REPORT//$'\n'}" \
    --priority 10 \
    --role-arn "${ROLE_ARN}" \
    --client-request-token "$(uuidgen)" \
    --region "${AWS_DEFAULT_REGION}" \
    --description "Turn off legal hold";
```

AWS SDK for Java の使用

次の AWS SDK for Java の例は、バッチオペレーションを使用して、複数のオブジェクト間で S3 Object Lock のリーガルホールドを無効にする方法を示しています。

Example – ロールを更新して **s3:PutObjectLegalHold** にアクセス許可を付与する

```
public void allowPutObjectLegalHold() {
    final String roleName = "batch_operations-object-lock";

    final String legalHoldPermissions = "{" +
            "    \"Version\": \"2012-10-17\"," +
            "    \"Statement\": [" +
            "        {" +
            "            \"Effect\": \"Allow\"," +
            "            \"Action\": [" +
            "                \"s3:PutObjectLegalHold\"" +
            "            ]," +
            "            \"Resource\": [" +
            "                \"arn:aws:s3:::amzn-s3-demo-manifest-bucket/*\"" +
            "            ]" +
            "        }" +
            "    ]" +
            "}";

    final AmazonIdentityManagement iam =
            AmazonIdentityManagementClientBuilder.defaultClient();

    final PutRolePolicyRequest putRolePolicyRequest = new PutRolePolicyRequest()
```

```
            .withPolicyDocument(legalHoldPermissions)
            .withPolicyName("legal-hold-permissions")
            .withRoleName(roleName);

    final PutRolePolicyResult putRolePolicyResult =
 iam.putRolePolicy(putRolePolicyRequest);
}
```

Example – リーガルホールドをオフにする

リーガルホールドをオフにする場合は、以下の例を使用します。

```
public String createLegalHoldOffJob(final AWSS3ControlClient awss3ControlClient) {
    final String manifestObjectArn = "arn:aws:s3:::amzn-s3-demo-manifest-bucket/
legalhold-object-manifest.csv";
    final String manifestObjectVersionId = "15ad5ba069e6bbc465c77bf83d541385";

    final JobManifestLocation manifestLocation = new JobManifestLocation()
            .withObjectArn(manifestObjectArn)
            .withETag(manifestObjectVersionId);

    final JobManifestSpec manifestSpec =
            new JobManifestSpec()
                    .withFormat(JobManifestFormat.S3BatchOperations_CSV_20180820)
                    .withFields("Bucket", "Key");

    final JobManifest manifestToPublicApi = new JobManifest()
            .withLocation(manifestLocation)
            .withSpec(manifestSpec);

    final String jobReportBucketArn = "arn:aws:s3:::amzn-s3-demo-completion-report-
bucket";
    final String jobReportPrefix = "reports/legalhold-objects-batch_operations";

    final JobReport jobReport = new JobReport()
            .withEnabled(true)
            .withReportScope(JobReportScope.AllTasks)
            .withBucket(jobReportBucketArn)
            .withPrefix(jobReportPrefix)
            .withFormat(JobReportFormat.Report_CSV_20180820);

    final JobOperation jobOperation = new JobOperation()
            .withS3PutObjectLegalHold(new S3SetObjectLegalHoldOperation()
                    .withLegalHold(new S3ObjectLockLegalHold()
```

```
                            .withStatus(S3ObjectLockLegalHoldStatus.OFF)));

    final String roleArn = "arn:aws:iam::123456789012:role/batch_operations-object-
lock";
    final Boolean requiresConfirmation = true;
    final int priority = 10;

    final CreateJobRequest request = new CreateJobRequest()
            .withAccountId("123456789012")
            .withDescription("Turn off legal hold")
            .withManifest(manifestToPublicApi)
            .withOperation(jobOperation)
            .withPriority(priority)
            .withRoleArn(roleArn)
            .withReport(jobReport)
            .withConfirmationRequired(requiresConfirmation);

    final CreateJobResult result = awss3ControlClient.createJob(request);

    return result.getJobId();
}
```

チュートリアル: S3 バッチオペレーションを使用した動画のバッチトランスコーディング

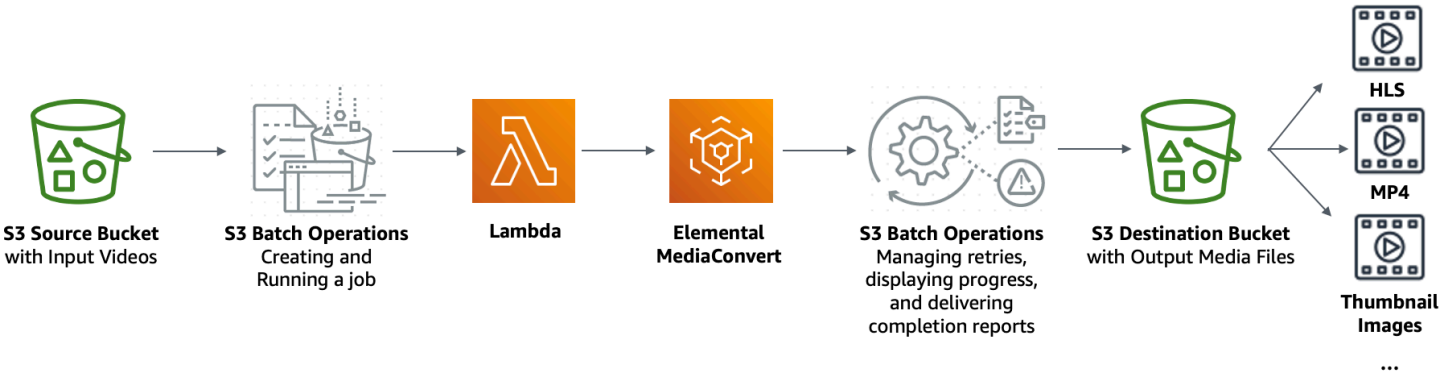
動画消費者は、あらゆる形状、サイズ、ビンテージのデバイスを使用してメディアコンテンツを楽しんでいます。この幅広い一連のデバイスは、コンテンツ作成者やディストリビューターにとって課題となります。動画は、ワンサイズですべてにフィットするフォーマットではなく、幅広いサイズ、フォーマット、ビットレートに変換する必要があります。変換が必要な動画が多数ある場合、この変換タスクはさらに困難になります。

AWS では、以下を実行するスケーラブルな分散アーキテクチャを構築する方法を提供します。

- 入力動画を取り込みます。
- さまざまなデバイスで再生するために動画を処理します。
- トランスコードされたメディアファイルを格納します。
- 需要に合わせて出力メディアファイルを配信します。

Amazon S3 に広範な動画リポジトリを保存している場合は、これらの動画をソース形式から、特定の動画プレーヤーやデバイスに必要なサイズ、解像度、形式の複数のファイルタイプに変換できま

す。具体的には、S3 バッチ操作 は、S3 ソースバケット内の既存の入力動画の AWS Lambda 関数を呼び出すためのソリューションを提供します。次に、Lambda 関数は AWS Elemental MediaConvert を呼び出して、広範な動画トランスコーディングタスクを実行します。変換後の出力メディアファイルは S3 保存先バケットに保存されます。



目的

このチュートリアルでは、S3 送信先バケットに保存された動画のバッチトランスコーディング用に Lambda 関数を呼び出すように S3 バッチ操作を設定する方法を学習します。Lambda 関数は MediaConvert を呼び出して、動画をトランスコードします。S3 ソースバケット内の各動画の出力は、次のとおりです。

- 複数のサイズのデバイスおよびさまざまな帯域幅で再生するための HTTP Live Streaming (HLS) アダプティブビットレートストリーム。
- MP4 動画ファイル
- サムネイル画像は、間隔をおいて収集されます。

トピック

- 前提条件
- ステップ 1: 出力メディアファイルの S3 バケットを作成する。
- ステップ 2: MediaConvert 用に IAM ロールを作成する
- ステップ 3: Lambda 関数の IAM ロールを作成する
- ステップ 4: 動画トランスコーディング用の Lambda 関数の作成
- ステップ 5: S3 ソースバケットの Amazon S3 インベントリを設定する。
- ステップ 6: S3 バッチ操作の IAM ロールを作成する。
- ステップ 7: S3 バッチ操作ジョブを作成して実行する。

- ステップ 8: S3 宛先バケットから出力メディアファイルを確認する。
- ステップ 9: クリーンアップする。
- 次のステップ

前提条件

このチュートリアルを開始する前に、トランスコードされる動画がすでにその中に保存されている Amazon S3 ソースバケットが必要です (例、*amzn-s3-demo-source-bucket*)。

必要に応じて、バケットに別の名前を付けることができます。Amazon S3 のバケット命名規則の詳細については、「汎用バケットの命名規則」を参照してください。

S3 ソースバケットの場合、このバケットのブロックパブリックアクセス設定 に関連する設定をデフォルトに設定したままにします (すべて のパブリックアクセスをブロックする が有効)。詳細については、「汎用バケットの作成」を参照してください。

S3 ソースバケットへの動画のアップロードの詳細については、オブジェクトのアップロード を参照してください。S3 に動画ファイルをアップロードするときは、Amazon S3 Transfer Acceleration を使用して、高速かつ安全なファイル転送を設定します。転送アクセラレーションを使用すると、S3 バケットへの動画のアップロードを高速化して、大きな動画の長距離転送を行うことができます。詳細については、「Amazon S3 Transfer Acceleration を使用した高速かつ安全なファイル転送の設定」を参照してください。

ステップ 1: 出力メディアファイルの S3 バケットを作成する。

このステップでは、変換後の出力メディアファイルを保存するための S3 ソースバケットを作成します。また、Cross Origin Resource Sharing (CORS) 設定を作成して、S3 の送信先バケットに保存されているトランスコードされたメディアファイルへのクロスオリジンアクセスを許可します。

サブステップ

- 出力メディアファイル用のバケットを作成する。
- CORS 設定を S3 出力バケットに追加する

出力メディアファイル用のバケットを作成する。

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。

2. 左側のナビゲーションペインで、[バケット] を選択します。
3. [Create bucket (バケットの作成)] を選択します。
4. Bucket Name に、バケットの名前 (例: *amzn-s3-demo-destination-bucket1*) を入力します。
5. [リージョン] で、バケットを保存する AWS リージョンを選択します。
6. 出力メディアファイルへのパブリックアクセスを確保するには、Block Public Access settings (パブリックアクセスのブロック設定) で、Block all public access (すべてのパブリックアクセスをブロック) をオフにします。

> **Warning**
>
> このステップを完了する前に「Amazon S3 ストレージへのパブリックアクセスのブロック」を読んで、パブリックアクセスを許可することに伴うリスクを理解し、了承します。ブロックパブリックアクセス設定をオフにしてバケットをパブリックにすると、インターネット上の誰でもバケットにアクセスできるようになります。バケットへのすべてのパブリックアクセスをブロックすることをお勧めします。
> ブロックパブリックアクセス設定をクリアしたくない場合は、Amazon CloudFront を使用して、トランスコードされたメディアファイルをビューワー (エンドユーザー) に配信できます。詳細については、「チュートリアル: Amazon S3、Amazon CloudFront、Amazon Route 53 を使用したオンデマンドストリーミング動画のホスティング。」を参照してください。

7. [現在の設定により、このバケットと保存されたオブジェクトがパブリックになる可能性があることを了承します] の横にあるチェックボックスを選択します。
8. 残りの設定はデフォルト値のままにしておきます。
9. [バケットを作成] を選択します。

CORS 設定を S3 出力バケットに追加する

JSON CORS 設定は、特定のドメインにロードされたクライアントウェブアプリケーション (このコンテキストでは動画プレーヤー) が、異なるドメインでトランスコードされた出力メディアファイルを再生する方法を定義します。

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。

3. バケット リストで、先に作成したバケットの名前を選択します(例: *amzn-s3-demo-destination-bucket1*) 。
4. [アクセス許可] タブを選択します。
5. [CORS (クロスオリジンリソース共有)] セクションで、[編集] を選択します。
6. [CORS 設定] テキストボックスで、次に示す CORS 設定をコピーして貼り付けます。

   CORS 設定は、JSON 形式である必要があります。この例では、AllowedOrigins 属性はワイルドカード文字 (*) を使用して、すべてのオリジンを指定します。特定のオリジンがわかっている場合は、AllowedOrigins 属性を特定のプレーヤーの URL に限定します。この属性およびその他の属性の設定の詳細については、「CORS 設定のエレメント」を参照してください。

```
[
    {
        "AllowedOrigins": [
            "*"
        ],
        "AllowedMethods": [
            "GET"
        ],
        "AllowedHeaders": [
            "*"
        ],
        "ExposeHeaders": []

    }
]
```

7. [Save changes] (変更の保存) をクリックします。

ステップ 2: MediaConvert 用に IAM ロールを作成する

AWS Elemental MediaConvert を使用して S3 バケットに保存されている入力動画をトランスコーディングするには、AWS Identity and Access Management (IAM) サービスロールを使用して、S3 ソースバケットおよび宛先バケットから動画ファイルを読み書きするための MediaConvert アクセス許可を付与します。トランスコーディングジョブを実行すると、MediaConvert コンソールはこのロールを使用します。

MediaConvert の IAM ロールを作成するには

1. 選択したロール名を使用して IAM ロールを作成します (例: **`tutorial-mediaconvert-role`**)。このロールを作成するには、「AWS Elemental MediaConvert ユーザーガイド」の「IAM (コンソール) で MediaConvert ロールを作成する」に記載のステップに従ってください。
2. MediaConvert の IAM ロールを作成した後、ロール のリストで、作成した MediaConvert のロールの名前を選択します (例: **`tutorial-mediaconvert-role`**)。
3. 概要 ページで、`arn:aws:iam::` で始まる ロール ARN をコピーし、後で使用できるように ARN を保存します。

   ARN の詳細については、AWS 全般のリファレンスの Amazon リソースネーム (ARN) を参照してください。

ステップ 3: Lambda 関数の IAM ロールを作成する

MediaConvert および S3 バッチ操作で動画をバッチトランスコードするには、これらの 2 つのサービスを接続して動画を変換する Lambda 関数を使用します。この Lambda 関数には、MediaConvert および S3 バッチ操作にアクセスするための許可を Lambda 関数に付与する IAM ロールが必要です。

サブステップ

- Lambda 関数の IAM ロールを作成する
- Lambda 関数の IAM ロールにインラインポリシーを埋め込む

Lambda 関数の IAM ロールを作成する

1. AWS Management Console にサインインして、IAM コンソール https://console.aws.amazon.com/iam/ を開きます。
2. 左側のナビゲーションペインから、[Roles (ロール)] を選択し、[Create role (ロールの作成)] を選択します。
3. AWS サービス ロールの種類を選択し、一般的ユースケース で、Lambda を選択します。
4. [Next: Permissions] (次のステップ: 許可) を選択します。
5. [Attach Permissions policies (許可ポリシーのアタッチ)]ページにあるポリシーのフィルタリング に **`AWSLambdaBasicExecutionRole`** を入力します。管理ポリシー AWSLambdaBasicExecutionRole をこのロールにアタッチして、Amazon CloudWatch Logs へ

の書き込み許可を付与するには、AWSLambdaBasicExecutionRole の横にあるチェックボックスを選択します。

6. [次へ] を選択します。
7. [ロール名] には、「**tutorial-lambda-transcode-role**」と入力します。
8. (オプション) 管理ポリシーにタグを追加します。
9. [ロールの作成] を選択してください。

Lambda 関数の IAM ロールにインラインポリシーを埋め込む

Lambda 関数の実行に必要な MediaConvert リソースに許可を付与するためには、インラインポリシーを使用する必要があります。

1. AWS Management Console にサインインして、IAM コンソール https://console.aws.amazon.com/iam/ を開きます。
2. 左のナビゲーションペインで、[ロール] を選択してください。
3. ロール のリストで、Lambda 関数用に先に作成した IAM ロールの名前を選択します (例、**tutorial-lambda-transcode-role**)。
4. [Permissions] タブを選択します。
5. [Add inline policy] を選択します。
6. [JSON] タブを選択し、以下の JSON ポリシーをコピーペーストします。

   JSON ポリシーでは、`Resource` の例の ARN 値を、ステップ 2 で作成した MediaConvert の IAM ロールのロール ARN に置き換えます (例、**tutorial-mediaconvert-role**)。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "Logging"
        },
        {
```

```
            "Action": [
                "iam:PassRole"
            ],
            "Resource": [
                "arn:aws:iam::111122223333:role/tutorial-mediaconvert-role"
            ],
            "Effect": "Allow",
            "Sid": "PassRole"
        },
        {
            "Action": [
                "mediaconvert:*"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow",
            "Sid": "MediaConvertService"
        },
        {
            "Action": [
                "s3:*"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow",
            "Sid": "S3Service"
        }
    ]
}
```

7. [ポリシーの確認] を選択します。
8. [Name] (名前) に **tutorial-lambda-policy** と入力します。
9. [ポリシーを作成] を選択します。

インラインポリシーを作成すると、Lambda 関数の IAM ロールに自動的に埋め込まれます。

ステップ 4: 動画トランスコーディング用の Lambda 関数の作成

チュートリアルの子のセクションでは、S3 バッチ操作および MediaConvert と統合するには、SDK for Python を使用して Lambda 関数を構築します。S3 ソースバケットにすでに保存されている動画

のトランスコーディングを開始するには、S3 ソースバケット内の各動画に対して Lambda 関数を直接呼び出す S3 バッチ操作ジョブを実行します。次に、Lambda 関数は、各動画のトランスコーディングジョブを MediaConvert に送信します。

サブステップ

- Lambda 関数コードを記述し、デプロイパッケージを作成する
- 実行ロール (コンソール) を使用した Lambda 関数の作成
- .zip ファイルアーカイブを使用して Lambda 関数コードをデプロイし、Lambda 関数を設定します (コンソール)。

Lambda 関数コードを記述し、デプロイパッケージを作成する

1. ローカルマシンで、`batch-transcode` という名前のフォルダを作成します。
2. `batch-transcode` フォルダに、JSON ジョブ設定でファイルを作成します。例えば、このセクションで提供されている設定を使用して、ファイル `job.json` に名前を付けることができます。

   `job.json` ファイルでは、以下を指定します。

   - トランスコードするファイル
   - 入力動画のトランスコード方法
   - 作成したい出力メディアファイル
   - トランスコードされたファイルの名前
   - トランスコードされたファイルを保存する場所
   - 適用する高度な機能など

   このチュートリアルでは、次の `job.json` ファイルを使用して、S3 ソースバケットの各動画に対して次の出力を作成します。

   - 複数のサイズのデバイスおよびさまざまな帯域幅で再生するための HTTP Live Streaming (HLS) アダプティブビットレートストリーム。
   - MP4 動画ファイル
   - 間隔を置いて収集されたサムネイル画像

このサンプル job.json ファイルは、品質が定義された可変ビットレート (QVBR) を使用して動画品質を最適化します。HLS 出力は、Apple に準拠しています (動画からのオーディオの混合、セグメント継続時間 (6 秒)、自動 QVBR により最適化された動画品質)。

ここで提供される設定例を使用しない場合は、ユースケースに基づく job.json 仕様を生成します。出力間で一貫性を保つために、入力ファイルの動画とオーディオの設定が似ていることを確認してください。異なる動画およびオーディオ構成を持つ任意の入力ファイルについては、別のオートメーション (一意の job.json 設定) を作成します。詳細については、「AWS Elemental MediaConvert ユーザーガイド」の「JSON での AWS Elemental MediaConvert ジョブ設定の例」を参照してください。

```
{
  "OutputGroups": [
    {
      "CustomName": "HLS",
      "Name": "Apple HLS",
      "Outputs": [
        {
          "ContainerSettings": {
            "Container": "M3U8",
            "M3u8Settings": {
              "AudioFramesPerPes": 4,
              "PcrControl": "PCR_EVERY_PES_PACKET",
              "PmtPid": 480,
              "PrivateMetadataPid": 503,
              "ProgramNumber": 1,
              "PatInterval": 0,
              "PmtInterval": 0,
              "TimedMetadata": "NONE",
              "VideoPid": 481,
              "AudioPids": [
                482,
                483,
                484,
                485,
                486,
                487,
                488,
                489,
                490,
```

```
                491,
                492
              ]
            }
          },
          "VideoDescription": {
            "Width": 640,
            "ScalingBehavior": "DEFAULT",
            "Height": 360,
            "TimecodeInsertion": "DISABLED",
            "AntiAlias": "ENABLED",
            "Sharpness": 50,
            "CodecSettings": {
              "Codec": "H_264",
              "H264Settings": {
                "InterlaceMode": "PROGRESSIVE",
                "NumberReferenceFrames": 3,
                "Syntax": "DEFAULT",
                "Softness": 0,
                "GopClosedCadence": 1,
                "GopSize": 2,
                "Slices": 1,
                "GopBReference": "DISABLED",
                "MaxBitrate": 1200000,
                "SlowPal": "DISABLED",
                "SpatialAdaptiveQuantization": "ENABLED",
                "TemporalAdaptiveQuantization": "ENABLED",
                "FlickerAdaptiveQuantization": "DISABLED",
                "EntropyEncoding": "CABAC",
                "FramerateControl": "INITIALIZE_FROM_SOURCE",
                "RateControlMode": "QVBR",
                "CodecProfile": "MAIN",
                "Telecine": "NONE",
                "MinIInterval": 0,
                "AdaptiveQuantization": "HIGH",
                "CodecLevel": "AUTO",
                "FieldEncoding": "PAFF",
                "SceneChangeDetect": "TRANSITION_DETECTION",
                "QualityTuningLevel": "SINGLE_PASS_HQ",
                "FramerateConversionAlgorithm": "DUPLICATE_DROP",
                "UnregisteredSeiTimecode": "DISABLED",
                "GopSizeUnits": "SECONDS",
                "ParControl": "INITIALIZE_FROM_SOURCE",
                "NumberBFramesBetweenReferenceFrames": 2,
```

```
                "RepeatPps": "DISABLED"
              }
            },
            "AfdSignaling": "NONE",
            "DropFrameTimecode": "ENABLED",
            "RespondToAfd": "NONE",
            "ColorMetadata": "INSERT"
          },
          "OutputSettings": {
            "HlsSettings": {
              "AudioGroupId": "program_audio",
              "AudioRenditionSets": "program_audio",
              "SegmentModifier": "$dt$",
              "IFrameOnlyManifest": "EXCLUDE"
            }
          },
          "NameModifier": "_360"
        },
        {
          "ContainerSettings": {
            "Container": "M3U8",
            "M3u8Settings": {
              "AudioFramesPerPes": 4,
              "PcrControl": "PCR_EVERY_PES_PACKET",
              "PmtPid": 480,
              "PrivateMetadataPid": 503,
              "ProgramNumber": 1,
              "PatInterval": 0,
              "PmtInterval": 0,
              "TimedMetadata": "NONE",
              "TimedMetadataPid": 502,
              "VideoPid": 481,
              "AudioPids": [
                482,
                483,
                484,
                485,
                486,
                487,
                488,
                489,
                490,
                491,
                492
```

```
            ]
          }
        },
        "VideoDescription": {
          "Width": 960,
          "ScalingBehavior": "DEFAULT",
          "Height": 540,
          "TimecodeInsertion": "DISABLED",
          "AntiAlias": "ENABLED",
          "Sharpness": 50,
          "CodecSettings": {
            "Codec": "H_264",
            "H264Settings": {
              "InterlaceMode": "PROGRESSIVE",
              "NumberReferenceFrames": 3,
              "Syntax": "DEFAULT",
              "Softness": 0,
              "GopClosedCadence": 1,
              "GopSize": 2,
              "Slices": 1,
              "GopBReference": "DISABLED",
              "MaxBitrate": 3500000,
              "SlowPal": "DISABLED",
              "SpatialAdaptiveQuantization": "ENABLED",
              "TemporalAdaptiveQuantization": "ENABLED",
              "FlickerAdaptiveQuantization": "DISABLED",
              "EntropyEncoding": "CABAC",
              "FramerateControl": "INITIALIZE_FROM_SOURCE",
              "RateControlMode": "QVBR",
              "CodecProfile": "MAIN",
              "Telecine": "NONE",
              "MinIInterval": 0,
              "AdaptiveQuantization": "HIGH",
              "CodecLevel": "AUTO",
              "FieldEncoding": "PAFF",
              "SceneChangeDetect": "TRANSITION_DETECTION",
              "QualityTuningLevel": "SINGLE_PASS_HQ",
              "FramerateConversionAlgorithm": "DUPLICATE_DROP",
              "UnregisteredSeiTimecode": "DISABLED",
              "GopSizeUnits": "SECONDS",
              "ParControl": "INITIALIZE_FROM_SOURCE",
              "NumberBFramesBetweenReferenceFrames": 2,
              "RepeatPps": "DISABLED"
            }
```

```
            },
            "AfdSignaling": "NONE",
            "DropFrameTimecode": "ENABLED",
            "RespondToAfd": "NONE",
            "ColorMetadata": "INSERT"
          },
          "OutputSettings": {
            "HlsSettings": {
              "AudioGroupId": "program_audio",
              "AudioRenditionSets": "program_audio",
              "SegmentModifier": "$dt$",
              "IFrameOnlyManifest": "EXCLUDE"
            }
          },
          "NameModifier": "_540"
        },
        {
          "ContainerSettings": {
            "Container": "M3U8",
            "M3u8Settings": {
              "AudioFramesPerPes": 4,
              "PcrControl": "PCR_EVERY_PES_PACKET",
              "PmtPid": 480,
              "PrivateMetadataPid": 503,
              "ProgramNumber": 1,
              "PatInterval": 0,
              "PmtInterval": 0,
              "TimedMetadata": "NONE",
              "VideoPid": 481,
              "AudioPids": [
                482,
                483,
                484,
                485,
                486,
                487,
                488,
                489,
                490,
                491,
                492
              ]
            }
          },
```

```
          "VideoDescription": {
            "Width": 1280,
            "ScalingBehavior": "DEFAULT",
            "Height": 720,
            "TimecodeInsertion": "DISABLED",
            "AntiAlias": "ENABLED",
            "Sharpness": 50,
            "CodecSettings": {
              "Codec": "H_264",
              "H264Settings": {
                "InterlaceMode": "PROGRESSIVE",
                "NumberReferenceFrames": 3,
                "Syntax": "DEFAULT",
                "Softness": 0,
                "GopClosedCadence": 1,
                "GopSize": 2,
                "Slices": 1,
                "GopBReference": "DISABLED",
                "MaxBitrate": 5000000,
                "SlowPal": "DISABLED",
                "SpatialAdaptiveQuantization": "ENABLED",
                "TemporalAdaptiveQuantization": "ENABLED",
                "FlickerAdaptiveQuantization": "DISABLED",
                "EntropyEncoding": "CABAC",
                "FramerateControl": "INITIALIZE_FROM_SOURCE",
                "RateControlMode": "QVBR",
                "CodecProfile": "MAIN",
                "Telecine": "NONE",
                "MinIInterval": 0,
                "AdaptiveQuantization": "HIGH",
                "CodecLevel": "AUTO",
                "FieldEncoding": "PAFF",
                "SceneChangeDetect": "TRANSITION_DETECTION",
                "QualityTuningLevel": "SINGLE_PASS_HQ",
                "FramerateConversionAlgorithm": "DUPLICATE_DROP",
                "UnregisteredSeiTimecode": "DISABLED",
                "GopSizeUnits": "SECONDS",
                "ParControl": "INITIALIZE_FROM_SOURCE",
                "NumberBFramesBetweenReferenceFrames": 2,
                "RepeatPps": "DISABLED"
              }
            },
            "AfdSignaling": "NONE",
            "DropFrameTimecode": "ENABLED",
```

```
            "RespondToAfd": "NONE",
            "ColorMetadata": "INSERT"
          },
          "OutputSettings": {
            "HlsSettings": {
              "AudioGroupId": "program_audio",
              "AudioRenditionSets": "program_audio",
              "SegmentModifier": "$dt$",
              "IFrameOnlyManifest": "EXCLUDE"
            }
          },
          "NameModifier": "_720"
        },
        {
          "ContainerSettings": {
            "Container": "M3U8",
            "M3u8Settings": {}
          },
          "AudioDescriptions": [
            {
              "AudioSourceName": "Audio Selector 1",
              "CodecSettings": {
                "Codec": "AAC",
                "AacSettings": {
                  "Bitrate": 96000,
                  "CodingMode": "CODING_MODE_2_0",
                  "SampleRate": 48000
                }
              }
            }
          ],
          "OutputSettings": {
            "HlsSettings": {
              "AudioGroupId": "program_audio",
              "AudioTrackType": "ALTERNATE_AUDIO_AUTO_SELECT_DEFAULT"
            }
          },
          "NameModifier": "_audio"
        }
      ],
      "OutputGroupSettings": {
        "Type": "HLS_GROUP_SETTINGS",
        "HlsGroupSettings": {
          "ManifestDurationFormat": "INTEGER",
```

```
          "SegmentLength": 6,
          "TimedMetadataId3Period": 10,
          "CaptionLanguageSetting": "OMIT",
          "Destination": "s3://EXAMPLE-BUCKET/HLS/",
          "DestinationSettings": {
            "S3Settings": {
              "AccessControl": {
                "CannedAcl": "PUBLIC_READ"
              }
            }
          },
          "TimedMetadataId3Frame": "PRIV",
          "CodecSpecification": "RFC_4281",
          "OutputSelection": "MANIFESTS_AND_SEGMENTS",
          "ProgramDateTimePeriod": 600,
          "MinSegmentLength": 0,
          "DirectoryStructure": "SINGLE_DIRECTORY",
          "ProgramDateTime": "EXCLUDE",
          "SegmentControl": "SEGMENTED_FILES",
          "ManifestCompression": "NONE",
          "ClientCache": "ENABLED",
          "StreamInfResolution": "INCLUDE"
        }
      }
    },
    {
      "CustomName": "MP4",
      "Name": "File Group",
      "Outputs": [
        {
          "ContainerSettings": {
            "Container": "MP4",
            "Mp4Settings": {
              "CslgAtom": "INCLUDE",
              "FreeSpaceBox": "EXCLUDE",
              "MoovPlacement": "PROGRESSIVE_DOWNLOAD"
            }
          },
          "VideoDescription": {
            "Width": 1280,
            "ScalingBehavior": "DEFAULT",
            "Height": 720,
            "TimecodeInsertion": "DISABLED",
            "AntiAlias": "ENABLED",
```

```
            "Sharpness": 100,
            "CodecSettings": {
              "Codec": "H_264",
              "H264Settings": {
                "InterlaceMode": "PROGRESSIVE",
                "ParNumerator": 1,
                "NumberReferenceFrames": 3,
                "Syntax": "DEFAULT",
                "Softness": 0,
                "GopClosedCadence": 1,
                "HrdBufferInitialFillPercentage": 90,
                "GopSize": 2,
                "Slices": 2,
                "GopBReference": "ENABLED",
                "HrdBufferSize": 10000000,
                "MaxBitrate": 5000000,
                "ParDenominator": 1,
                "EntropyEncoding": "CABAC",
                "RateControlMode": "QVBR",
                "CodecProfile": "HIGH",
                "MinIInterval": 0,
                "AdaptiveQuantization": "AUTO",
                "CodecLevel": "AUTO",
                "FieldEncoding": "PAFF",
                "SceneChangeDetect": "ENABLED",
                "QualityTuningLevel": "SINGLE_PASS_HQ",
                "UnregisteredSeiTimecode": "DISABLED",
                "GopSizeUnits": "SECONDS",
                "ParControl": "SPECIFIED",
                "NumberBFramesBetweenReferenceFrames": 3,
                "RepeatPps": "DISABLED",
                "DynamicSubGop": "ADAPTIVE"
              }
            },
            "AfdSignaling": "NONE",
            "DropFrameTimecode": "ENABLED",
            "RespondToAfd": "NONE",
            "ColorMetadata": "INSERT"
          },
          "AudioDescriptions": [
            {
              "AudioTypeControl": "FOLLOW_INPUT",
              "AudioSourceName": "Audio Selector 1",
              "CodecSettings": {
```

```
                "Codec": "AAC",
                "AacSettings": {
                  "AudioDescriptionBroadcasterMix": "NORMAL",
                  "Bitrate": 160000,
                  "RateControlMode": "CBR",
                  "CodecProfile": "LC",
                  "CodingMode": "CODING_MODE_2_0",
                  "RawFormat": "NONE",
                  "SampleRate": 48000,
                  "Specification": "MPEG4"
                }
              },
              "LanguageCodeControl": "FOLLOW_INPUT",
              "AudioType": 0
            }
          ]
        }
      ],
      "OutputGroupSettings": {
        "Type": "FILE_GROUP_SETTINGS",
        "FileGroupSettings": {
          "Destination": "s3://EXAMPLE-BUCKET/MP4/",
          "DestinationSettings": {
            "S3Settings": {
              "AccessControl": {
                "CannedAcl": "PUBLIC_READ"
              }
            }
          }
        }
      }
    },
    {
      "CustomName": "Thumbnails",
      "Name": "File Group",
      "Outputs": [
        {
          "ContainerSettings": {
            "Container": "RAW"
          },
          "VideoDescription": {
            "Width": 1280,
            "ScalingBehavior": "DEFAULT",
            "Height": 720,
```

```
            "TimecodeInsertion": "DISABLED",
            "AntiAlias": "ENABLED",
            "Sharpness": 50,
            "CodecSettings": {
              "Codec": "FRAME_CAPTURE",
              "FrameCaptureSettings": {
                "FramerateNumerator": 1,
                "FramerateDenominator": 5,
                "MaxCaptures": 500,
                "Quality": 80
              }
            },
            "AfdSignaling": "NONE",
            "DropFrameTimecode": "ENABLED",
            "RespondToAfd": "NONE",
            "ColorMetadata": "INSERT"
          }
        }
      ],
      "OutputGroupSettings": {
        "Type": "FILE_GROUP_SETTINGS",
        "FileGroupSettings": {
          "Destination": "s3://EXAMPLE-BUCKET/Thumbnails/",
          "DestinationSettings": {
            "S3Settings": {
              "AccessControl": {
                "CannedAcl": "PUBLIC_READ"
              }
            }
          }
        }
      }
    }
  ],
  "AdAvailOffset": 0,
  "Inputs": [
    {
      "AudioSelectors": {
        "Audio Selector 1": {
          "Offset": 0,
          "DefaultSelection": "DEFAULT",
          "ProgramSelection": 1
        }
      },
```

```
      "VideoSelector": {
        "ColorSpace": "FOLLOW"
      },
      "FilterEnable": "AUTO",
      "PsiControl": "USE_PSI",
      "FilterStrength": 0,
      "DeblockFilter": "DISABLED",
      "DenoiseFilter": "DISABLED",
      "TimecodeSource": "EMBEDDED",
      "FileInput": "s3://EXAMPLE-INPUT-BUCKET/input.mp4"
    }
  ]
}
```

3. batch-transcode フォルダで、Lambda 関数を使用してファイルを作成します。次の Python の例を使用し、ファイル convert.py に名前を付けます。

   S3 バッチ操作は、特定のタスクデータを Lambda 関数に送信 し、結果データを返します。Lambda 関数のリクエストとレスポンスの例、レスポンスコードと結果コード、S3 バッチ操作の Lambda 関数の例に関する詳細は、「AWS Lambda 関数の呼び出し」を参照してください。

```
import json
import os
from urllib.parse import urlparse
import uuid
import boto3

"""
When you run an S3 Batch Operations job, your job
invokes this Lambda function. Specifically, the Lambda function is
invoked on each video object listed in the manifest that you specify
for the S3 Batch Operations job in Step 5.

Input parameter "event": The S3 Batch Operations event as a request
                         for the Lambda function.

Input parameter "context": Context about the event.

Output: A result structure that Amazon S3 uses to interpret the result
        of the operation. It is a job response returned back to S3 Batch
 Operations.
"""
```

```
def handler(event, context):

    invocation_schema_version = event['invocationSchemaVersion']
    invocation_id = event['invocationId']
    task_id = event['tasks'][0]['taskId']

    source_s3_key = event['tasks'][0]['s3Key']
    source_s3_bucket = event['tasks'][0]['s3BucketArn'].split(':::')[-1]
    source_s3 = 's3://' + source_s3_bucket + '/' + source_s3_key

    result_list = []
    result_code = 'Succeeded'
    result_string = 'The input video object was converted successfully.'

    # The type of output group determines which media players can play
    # the files transcoded by MediaConvert.
    # For more information, see Creating outputs with AWS Elemental MediaConvert.
    output_group_type_dict = {
        'HLS_GROUP_SETTINGS': 'HlsGroupSettings',
        'FILE_GROUP_SETTINGS': 'FileGroupSettings',
        'CMAF_GROUP_SETTINGS': 'CmafGroupSettings',
        'DASH_ISO_GROUP_SETTINGS': 'DashIsoGroupSettings',
        'MS_SMOOTH_GROUP_SETTINGS': 'MsSmoothGroupSettings'
    }

    try:
        job_name = 'Default'
        with open('job.json') as file:
            job_settings = json.load(file)

        job_settings['Inputs'][0]['FileInput'] = source_s3

        # The path of each output video is constructed based on the values of
        # the attributes in each object of OutputGroups in the job.json file.
        destination_s3 = 's3://{0}/{1}/{2}' \
            .format(os.environ['amzn-s3-demo-destination-bucket'],
                    os.path.splitext(os.path.basename(source_s3_key))[0],
                    os.path.splitext(os.path.basename(job_name))[0])

        for output_group in job_settings['OutputGroups']:
            output_group_type = output_group['OutputGroupSettings']['Type']
            if output_group_type in output_group_type_dict.keys():
                output_group_type = output_group_type_dict[output_group_type]
```

```
                output_group['OutputGroupSettings'][output_group_type]
['Destination'] = \
                    "{0}{1}".format(destination_s3,
                                    urlparse(output_group['OutputGroupSettings']
[output_group_type]['Destination']).path)
            else:
                raise ValueError("Exception: Unknown Output Group Type {}."
                                 .format(output_group_type))

        job_metadata_dict = {
            'assetID': str(uuid.uuid4()),
            'application': os.environ['Application'],
            'input': source_s3,
            'settings': job_name
        }

        region = os.environ['AWS_DEFAULT_REGION']
        endpoints = boto3.client('mediaconvert', region_name=region) \
            .describe_endpoints()
        client = boto3.client('mediaconvert', region_name=region,
                              endpoint_url=endpoints['Endpoints'][0]['Url'],
                              verify=False)

        try:
            client.create_job(Role=os.environ['MediaConvertRole'],
                              UserMetadata=job_metadata_dict,
                              Settings=job_settings)
        # You can customize error handling based on different error codes that
        # MediaConvert can return.
        # For more information, see MediaConvert error codes.
        # When the result_code is TemporaryFailure, S3 Batch Operations retries
        # the task before the job is completed. If this is the final retry,
        # the error message is included in the final report.
        except Exception as error:
            result_code = 'TemporaryFailure'
            raise

    except Exception as error:
        if result_code != 'TemporaryFailure':
            result_code = 'PermanentFailure'
        result_string = str(error)

    finally:
        result_list.append({
```

```
            'taskId': task_id,
            'resultCode': result_code,
            'resultString': result_string,
        })

    return {
        'invocationSchemaVersion': invocation_schema_version,
        'treatMissingKeyAs': 'PermanentFailure',
        'invocationId': invocation_id,
        'results': result_list
    }
```

4. ローカルターミナルで、convert.py および lambda.zip という名前の .zip ファイルとして job.json を使用してデプロイパッケージを作成するには、上記で作成した batch-transcode フォルダを開き、次のコマンドを実行します。

   macOS ユーザーの場合は、以下のコマンドを使用します。

   ```
   zip -r lambda.zip convert.py job.json
   ```

   Windows ユーザー の場合は、以下のコマンドを実行します。

   ```
   powershell Compress-Archive convert.py lambda.zip
   ```

   ```
   powershell Compress-Archive -update job.json lambda.zip
   ```

実行ロール (コンソール) を使用した Lambda 関数の作成

1. AWS Lambda コンソールの https://console.aws.amazon.com/lambda/ を開いてください。
2. 左側のナビゲーションペインで、関数 を選択します。
3. 関数の作成 を選択します。
4. Author from scratch を選択します。
5. 基本的な情報 で、以下の作業を行います。

   a. [関数名] に「**tutorial-lambda-convert**」と入力します。

   b. [ランタイム] で [Python 3.13] を選択します。

6. デフォルト実行ロールを変更する を選択し、実行ロール で、既存のロールを使用する を選択します。
7. 既存のロール で、ステップ 3 で Lambda 関数用に作成した IAM ロールの名前を選択します (例、**tutorial-lambda-transcode-role**)。
8. 残りの設定はデフォルトのままにしておきます。
9. 関数の作成 を選択します。

.zip ファイルアーカイブを使用して Lambda 関数コードをデプロイし、Lambda 関数を設定します (コンソール)。

1. 上で作成した Lambda 関数のページの [コードソース] セクション (**tutorial-lambda-convert** など) で、[アップロード元]、[.zip ファイル]の順に選択します。
2. アップロード を選択して、ローカルの `.zip` ファイルを選択します。
3. 前に作成した `lambda.zip` ファイルを選択し、開く を選択します。
4. Save を選択します。
5. ランタイム設定 セクションで、編集 を選択します。
6. Lambda ランタイムに Lambda 関数コード内のどのハンドラメソッドの呼び出しを指示するには、ハンドラー フィールドに **convert.handler** を入力します。

   Python で関数を設定するとき、ハンドラー設定の値は、ファイル名と、ハンドラーモジュールの名前を、ドット (.) で区切ったものになります。例えば、`convert.handler` は、`convert.py` ファイルで定義された `handler` メソッドを呼び出します。
7. Save を選択します。
8. [Lambda 関数] ページで、設定 タブを選択します。設定 タブの左側のナビゲーションペインで、環境変数 を選択し、編集 を選択します。
9. 環境変数の追加 を選択します。次に、次の環境変数ごとにキー および値 を入力します。

   - キー : **DestinationBucket** 値: **amzn-s3-demo-destination-bucket1**

     この値は、ステップ 1 で作成した出力メディアファイルの S3 バケットです。
   - キー : **MediaConvertRole** 値: **arn:aws:iam::*111122223333*:role/tutorial-mediaconvert-role**

     この値は、ステップ 2 で作成した MediaConvert の IAM ロールの ARN です。この ARN を IAM ロールの実際の ARN に置き換えてください。

- キー : **Application** 値: **Batch-Transcoding**

  この値は、アプリケーションの名前です。

10. Save を選択します。
11. (オプション) Configuration (設定) タブの左側のナビゲーションペインの General configuration (一般設定) セクションで、Edit (編集) を選択します。[タイムアウト] フィールドに、**2** 分 **0** 秒と入力します。次に、[保存] を選択します。

    タイムアウトは、Lambda で関数が停止するまでに許可される実行時間の長さです。デフォルト値は 3 秒です。料金は、設定されたメモリの量とコードの実行時間に基づいて請求されます。詳細については、「AWS Lambda 料金表」を参照してください。

ステップ 5: S3 ソースバケットの Amazon S3 インベントリを設定する。

トランスコーディング Lambda 関数をセットアップしたら、S3 バッチ操作ジョブを作成して、一連の動画をトランスコードします。まず、S3 バッチ操作で指定したトランスコーディングアクションを実行する入力動画オブジェクトのリストが必要です。入力動画オブジェクトのリストを取得するには、S3 ソースバケットの S3 インベントリレポートを生成できます (例、*amzn-s3-demo-source-bucket*)。

サブステップ

- 入力動画の S3 インベントリレポート用のバケットを作成して設定する
- S3 動画ソースバケットの Amazon S3 インベントリを設定します。
- S3 動画ソースバケットのインベントリレポートを確認します。

入力動画の S3 インベントリレポート用のバケットを作成して設定する

S3 ソースバケットのオブジェクトをリストする S3 インベントリレポートを保存するには、S3 インベントリ宛先バケットを作成し、そのバケットに対してインベントリファイルを S3 ソースバケットに書き込むようにバケットポリシーを設定します。

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。
3. [Create bucket (バケットの作成)] を選択します。

4. Bucket Name に、バケットの名前 (例: *amzn-s3-demo-destination-bucket2*) を入力します。
5. AWS リージョン で、バケットを保存するAWS リージョン を選択します。

   インベントリ宛先バケットは、S3 インベントリを設定するソースバケットと同じ AWS リージョン である必要があります。インベントリ宛先バケットは、別の AWS アカウント にある場合があります。
6. このバケットのパブリックアクセス設定をブロック で、デフォルト設定 (ブロックすべてパブリックアクセスが有効) のままであることを確認します。
7. 残りの設定はデフォルトのままにしておきます。
8. [バケットを作成] を選択します。
9. [バケット] リストで、作成したばかりのバケットの名前を選択します(例、*amzn-s3-demo-destination-bucket2*) 。
10. S3 インベントリレポートのデータを S3 インベントリ送信先バケットに書き込む許可を Amazon S3 に付与するには、許可 タブを選択します。
11. バケットポリシー セクションまで下にスクロールし、編集 を選択します。バケットポリシーページが開きます。
12. S3 インベントリの許可を付与するには、ポリシー フィールドに、次のバケットポリシーを貼り付けます。

    3 つの例の値を、それぞれ次の値に置き換えます。

    - インベントリレポート (例、*amzn-s3-demo-destination-bucket2*) を保存するために作成したバケットの名前。
    - 入力動画を保存するソースバケットの名前 (例、*amzn-s3-demo-source-bucket*)。
    - S3 動画ソースバケットの作成に使用した AWS アカウント ID (例、*111122223333*)。

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"InventoryAndAnalyticsExamplePolicy",
      "Effect":"Allow",
      "Principal": {"Service": "s3.amazonaws.com"},
      "Action":"s3:PutObject",
      "Resource":["arn:aws:s3:::amzn-s3-demo-destination-bucket2/*"],
```

```
      "Condition": {
          "ArnLike": {
              "aws:SourceArn": "arn:aws:s3:::amzn-s3-demo-source-bucket"
           },
          "StringEquals": {
              "aws:SourceAccount": "111122223333",
              "s3:x-amz-acl": "bucket-owner-full-control"
           }
       }
    }
  ]
}
```

13. [Save changes] (変更の保存) をクリックします。

S3 動画ソースバケットの Amazon S3 インベントリを設定します。

動画オブジェクトとメタデータのフラットファイルリストを生成するには、S3 動画ソースバケットの S3 インベントリを設定する必要があります。これらのスケジュールされたレポートには、バケット内のすべてのオブジェクト、または共有プレフィックスでグループ化されたオブジェクトを含めることができます。このチュートリアルでは、S3 インベントリレポートに S3 ソースバケット内のすべての動画オブジェクトが含まれます。

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。
3. S3 ソースバケットの入力動画の S3 インベントリレポートを設定するには、バケット リストで、S3 ソースバケットの名前を選択します (例、*amzn-s3-demo-source-bucket*)。
4. [管理] タブを選択します。
5. インベントリの設定 セクションを下にスクロールし、インベントリ設定を作成する を選択します。
6. Inventory configuration name (インベントリ設定名) に、名前を入力します (例、**tutorial-inventory-config**)。
7. インベントリの範囲 で、オブジェクトバージョン に対して現在のバージョンのみ を選択し、他のインベントリの範囲 設定をこのチュートリアルのデフォルトに設定したままにします。
8. レポートの詳細 の 宛先バケット で、このアカウント を選択します。

9. 宛先 で S3 を参照 を選択し、インベントリレポートを保存するために先に作成した宛先バケットを選択します (例、*amzn-s3-demo-destination-bucket2*)。次に、パスの選択 を選択します。

   インベントリ宛先バケットは、S3 インベントリを設定するソースバケットと同じ AWS リージョン である必要があります。宛先バケットは、別の AWS アカウント アカウントにある場合があります。

   [送信先] バケットフィールドの下に、Amazon S3 がそのバケットにデータを入れることを許可するために送信先バケットポリシーに追加される [送信先バケットの許可] が追加されます。詳細については、「ターゲットバケットポリシーの作成」を参照してください。
10. 頻度 で、1 日 1 回 を選択します。
11. [Output format] (出力形式) として [CSV] を選択します。
12. Status (ステータス) で、有効 を選択します。
13. サーバー側の暗号化 で、このチュートリアルの 無効 を選択します。

    詳細については、「S3 コンソールを使用したインベントリの設定」および「カスタマーマネージドキーを暗号化に使用するためのアクセス許可を Amazon S3 に付与する」を参照してください。
14. 追加フィールド - オプション セクションで、サイズ、最終更新日時 および ストレージクラス を選択します。
15. [作成] を選択します。

詳細については、「S3 コンソールを使用したインベントリの設定」を参照してください。

S3 動画ソースバケットのインベントリレポートを確認します。

インベントリレポートが発行されると、マニフェストファイルは S3 インベントリ宛先バケットに送信されます。

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。
3. Buckets (バケット) リストで、動画送信先バケットの名前を選択します (例、*amzn-s3-demo-source-bucket*)。
4. [Management (管理)] を選択します。

5. S3 インベントリレポートで S3 バッチ操作ジョブを作成する準備ができているかどうかを確認するには、ステップ 7 の インベントリ設定 で、マニフェストからジョブを作成 ボタンが有効になっているかを確認します。

> **Note**
>
> 最初のレポートが配信されるまでに最大で 48 時間かかることがあります。Create job from manifest (マニフェストからジョブを作成) ボタンが無効になっている場合、最初のインベントリレポートは配信されていません。ステップ 7 で S3 バッチ操作ジョブを作成するには、最初のインベントリレポートが配信され、マニフェストからジョブを作成 ボタンが有効になるまで待つ必要があります。

6. S3 インベントリレポート (`manifest.json`) を確認するには、宛先 列で、インベントリレポートを保存するために先に作成したインベントリ宛先バケットの名前を選択します (例、*amzn-s3-demo-destination-bucket2*)。
7. オブジェクト タブで、S3 ソースバケットの名前を持つ既存のフォルダ (例、*amzn-s3-demo-source-bucket*) を選択します。次に、先にインベントリ設定を作成した際に インベントリの設定名 で入力した名前を選択します (例、**tutorial-inventory-config**)。

   レポートの生成日を名前として含むフォルダのリストを表示できます。
8. 特定の日付の日次 S3 インベントリレポートを確認するには、生成日の名前が付いたフォルダを選択して、`manifest.json` を選択します。
9. 特定の日付のインベントリレポートの詳細を確認するには、manifest.json ページで、Download (ダウンロード) または Open (開く) を選択します。

ステップ 6: S3 バッチ操作の IAM ロールを作成する。

S3 バッチ操作を使用してバッチトランスコーディングを行うには、最初に IAM ロールを作成して、S3 バッチ操作を実行する許可を Amazon S3 に付与する必要があります。

サブステップ

- S3 バッチ操作用の IAM ポリシーを作成する。
- S3 バッチ操作 IAM ロールを作成し、許可ポリシーを割り当てる

S3 バッチ操作用の IAM ポリシーを作成する。

S3 バッチ操作に、入力マニフェストを読み取り、Lambda 関数を呼び出し、S3 バッチ操作ジョブ完了レポートに書き込みを行う許可を与える IAM ポリシーを作成する必要があります。

1. AWS Management Console にサインインして、IAM コンソール https://console.aws.amazon.com/iam/ を開きます。
2. 左のナビゲーションペインの [ポリシー] を選択します。
3. [Create policy (ポリシーの作成)] を選択します。
4. [JSON] タブを選択します。
5. JSON テキストフィールドに、次の JSON ポリシーをコピーして貼り付けます。

   JSON ポリシーで、4 つのサンプル値を次の値に置き換えます。

   - 入力動画を保存するソースバケットの名前 (例、*amzn-s3-demo-source-bucket*)。
   - `manifest.json` ファイル (例、*amzn-s3-demo-destination-bucket2*) を保存するためにステップ 5 で作成したインベントリ送信先バケットの名前。
   - 出力メディアファイルを保存するために ステップ 1 で作成したバケットの名前 (例、*amzn-s3-demo-destination-bucket1*)。このチュートリアルでは、出力メディアファイルの送信先バケットにジョブ完了レポートを配置します。
   - ステップ 4 で作成した Lambda 関数のロール ARN。Lambda 関数のロール ARN を検索してコピーするには、次の操作を行います。
     - 新しいブラウザタブで、https://console.aws.amazon.com/lambda/home#/functions にある Lambda コンソールの 関数 ページを開きます。
     - 関数 のリストから、ステップ 4 で作成した Lambda 関数を選択します (例、**tutorial-lambda-convert**)。
     - [Copy ARN (ARN のコピー)] を選択します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3Get",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
```

```
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-source-bucket/*",
                "arn:aws:s3:::amzn-s3-demo-destination-bucket2/*"
            ]
        },
        {
            "Sid": "S3PutJobCompletionReport",
            "Effect": "Allow",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket1/*"
        },
        {
            "Sid": "S3BatchOperationsInvokeLambda",
            "Effect": "Allow",
            "Action": [
                "lambda:InvokeFunction"
            ],
            "Resource": [
                "arn:aws:lambda:us-west-2:111122223333:function:tutorial-lambda-
convert"
            ]
        }
    ]
}
```

6. [Next: Tags (次へ: タグ)] を選択します。
7. [Next: Review (次へ: レビュー)] を選択します。
8. [名前] フィールドに **tutorial-s3batch-policy** を入力してください。
9. [Create policy (ポリシーの作成)] を選択します。

S3 バッチ操作 IAM ロールを作成し、許可ポリシーを割り当てる

1. AWS Management Console にサインインして、IAM コンソール https://console.aws.amazon.com/iam/ を開きます。
2. 左側のナビゲーションペインから、[Roles (ロール)] を選択し、[Create role (ロールの作成)] を選択します。
3. AWS のサービス ロールタイプを選択し、S3 サービスを選択します。
4. [ユースケースを選択] で、S3 バッチ操作 を選択します。
5. [次へ] を選択します。

6. [アクセス許可をアタッチ] で、事前に作成した IAM ポリシーの名前 (**tutorial-s3batch-policy** など) を検索ボックスに入力し、ポリシーのリストをフィルタリングします。ポリシー名の横にあるチェックボックスを選択します (例、**tutorial-s3batch-policy**)。
7. [次へ] を選択します。
8. [Role name] (ロール名) に**tutorial-s3batch-role**と入力します。
9. [ロールの作成] を選択してください。

   S3 バッチ操作の IAM ロールを作成した後は、次の信頼ポリシーが自動的にロールに添付されます。この信頼ポリシーは、S3 バッチ操作のサービスプリンシパルが IAM ロールを引き受けることを許可します。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"batchoperations.s3.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

ステップ 7: S3 バッチ操作ジョブを作成して実行する。

S3 バッチ操作 ジョブを作成して S3 ソースバケット内の入力動画を処理するには、この特定のジョブのパラメータを指定する必要があります。

> **Note**
>
> S3 バッチ操作ジョブの作成を開始するには、[マニフェストからジョブを作成] ボタンが有効になっていることを確認する必要があります。詳細については、「S3 動画ソースバケットのインベントリレポートを確認します。」を参照してください。マニフェストからジョブを作成 ボタンが無効になっている場合、最初のインベントリレポートは配信されておらず、ボタンが有効になるまで待つ必要があります。ステップ 5 で S3 ソースバケットの Amazon S3

インベントリを設定した後は、最初のインベントリレポートが配信されるまでに最大で 48 時間かかることがあります。

サブステップ

- S3 バッチオペレーションジョブを作成します。
- S3 バッチ操作ジョブを実行して Lambda 関数を呼び出します。
- (オプション) 完了レポートを確認する。
- (オプション) Lambda コンソールで各 Lambda 呼び出しをモニタリングする。
- (オプション)MediaConvert コンソールで各 MediaConvert 動画トランスコーディングジョブを監視する

S3 バッチオペレーションジョブを作成します。

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[バッチ操作] を選択します。
3. [ジョブの作成] を選択します。
4. AWS リージョン については、ジョブを作成する [Region (リージョン)] を選択します。

   このチュートリアルで、S3 バッチ操作ジョブを使用して Lambda 関数を呼び出すには、マニフェストで参照されるオブジェクトがある S3 動画ソースバケットと同じリージョンにジョブを作成する必要があります。
5. マニフェスト セクションで、以下を実行します。

   a. Manifest format (マニフェスト形式) で、S3 inventory report (manifest.json) を選択します。

   b. オブジェクトのマニフェスト については、Browse S3 を選択して、インベントリレポートを保存するために ステップ 5 で作成したバケットを見つけます (例、*amzn-s3-demo-destination-bucket2*)。マニフェストオブジェクト ページで、特定の日付の `manifest.json` ファイルが見つかるまで、オブジェクト名を検索します。このファイルには、バッチトランスコードするすべての動画に関する情報がリストされます。使用する `manifest.json` ファイルを見つけたら、横にあるオプションボタンを選択します。次に、[パスの選択] を選択します。

   c. (オプション) [マニフェストオブジェクトのバージョン ID-オプション] で、最新版以外のバージョンを使用する場合は、マニフェストオブジェクトのバージョン ID を入力します。

6. [次へ] を選択します。
7. Lambda 関数を使用して、選択した `manifest.json` ファイルリストされているすべてのオブジェクトをトランスコードするには、オペレーションタイプ で AWS Lambda 関数を呼び出すを選択します。
8. Lambda 関数の呼び出し ウィンドウで、次を実行します。
   a. Choose from functions in your account (アカウントの関数を選択する) を選択します。
   b. Lambda 関数 で、ステップ 4 で作成した Lambda 関数を選択します (例、**`tutorial-lambda-convert`**)。
   c. Lambda 関数のバージョン で、デフォルト値の $LATEST を維持します。
9. Next を選択します。追加のオプションの設定 ページが開きます。
10. 追加のオプション で、デフォルトの設定を維持します。

    これらのパラメータの詳細については「バッチ操作ジョブのリクエストの要素」を参照してください。
11. 完了レポート セクションの 完了レポートの送信先へのパス で、S3 をブラウズ を選択します。ステップ 1 で出力メディアファイル用に作成したバケットを見つけます (例、*`amzn-s3-demo-destination-bucket1`*)。バケット名の横にあるオプションボタンを選択します。次に、パスの選択 を選択します。

    残りの 完了レポート 設定は、デフォルト値のままにしておきます。レポートの設定の完了に関する詳細については、「バッチ操作ジョブのリクエストの要素」を参照してください。完了レポートには、ジョブの詳細と実行された操作のレコードが保持されます。
12. 許可 で、既存の IAM ロールから選択する を選択します。IAM role (IAM ロール) で、ステップ 6 (例、**`tutorial-s3batch-role`**) で作成した S3 バッチ操作ジョブの IAM ロールを選択します。
13. [次へ] を選択します。
14. Review ページで、設定を確認します。次に、ジョブの作成 を選択します。

    S3 が S3 バッチ操作のジョブのマニフェストの読み取りを終了すると、実行のための確認待ちの ステータス に移行します。ジョブのステータスの更新を表示するには、ページをリフレッシュします。ステータスが 実行のための確認待ち になるまで、ジョブを実行することはできません。

S3 バッチ操作ジョブを実行して Lambda 関数を呼び出します。

バッチ操作ジョブを実行して、動画トランスコーディング用の Lambda 関数を呼び出します。ジョブが失敗した場合は、完了レポートを確認して原因を特定できます。

S3 バッチ操作ジョブを実行するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、バッチ操作 を選択します。
3. ジョブ のリストから、最初の行のジョブの ジョブ ID を選択します。これは、上記で作成した S3 バッチ操作ジョブです。
4. [ジョブの実行] を選択します。
5. ジョブパラメータをもう一度確認し、Total objects listed in manifest (マニフェストにリストされているオブジェクトの総数) の値がマニフェスト内のオブジェクトの数と同じであることを確認します。次に、ジョブの実行 を選択します。

   S3 バッチ操作ジョブページが開きます。
6. ジョブの実行が開始されたら、ジョブページの Status (ステータス) で、Status (ステータス)、% Complete (% 完了)、Total succeeded (rate) (成功合計) (レート)、Total failed (rate) (失敗合計) (レート)、Date terminated (終了日)、Reason for termination (終了理由) など、S3 バッチ操作ジョブの進行状況を確認します。

   S3 バッチ操作ジョブが完了したら、ジョブページのデータを表示して、ジョブが期待どおりに完了したことを確認します。

   1,000 を超える操作が試行された後、失敗が S3 バッチ操作ジョブのオブジェクト操作の 50% を超えると、ジョブは自動的に失敗します。完了レポートを確認して失敗の原因を特定するには、以下のオプション手順を参照してください。

(オプション) 完了レポートを確認する。

完了レポートを使用して、失敗したオブジェクトと失敗の原因を特定できます。

失敗したオブジェクトの詳細について完了レポートを確認するには

1. S3 バッチ操作ジョブのページで、完了レポート までスクロールし、完了レポートの宛先 のリンクを選択します。

S3 出力宛先バケットページが開きます。

2. オブジェクト タブで、上記で作成した S3 バッチ操作ジョブのジョブ ID で終わる名前のフォルダを選択します。
3. results/ (結果/) を選択します。
4. `.csv` ファイルの横にあるチェックボックスを選択します。
5. ジョブレポートを表示するには、[オープン] または [ダウンロード] を選択します。

(オプション) Lambda コンソールで各 Lambda 呼び出しをモニタリングする。

S3 バッチ操作ジョブの実行が開始されると、ジョブは入力動画オブジェクトごとに Lambda 関数の呼び出しを開始します。S3 では、各 Lambda 呼び出しのログを CloudWatch Logs に書き込みます。Lambda コンソールのモニタリングダッシュボードを使用して、Lambda 関数とアプリケーションをモニタリングできます。

1. AWS Lambda コンソールの https://console.aws.amazon.com/lambda/ を開いてください。
2. 左側のナビゲーションペインで、[関数] を選択します。
3. 関数 のリストから、ステップ 4 で作成した Lambda 関数 の名前を選択します (例、**`tutorial-lambda-convert`**)。
4. [Monitor] (モニタリング) タブを選択します。
5. Metrics (メトリクス) で、Lambda 関数のランタイムメトリクスを確認します。
6. Logs (ログ) で、CloudWatch Logs インサイトを使用して各 Lambda 呼び出しのログデータを表示します。

> **Note**
>
> Lambda 関数で S3 バッチ操作を使用する場合、Lambda 関数は各オブジェクトで呼び出されます。S3 バッチ操作ジョブが大きい場合、複数の Lambda 関数を同時に呼び出すことができ、Lambda の同時実行数が急増します。
> 各 AWS アカウント リージョンごとに Lambda 同時実行クォータがあります。詳細については、「AWS Lambda デベロッパーガイド の「AWS Lambda 関数のスケーリング」を参照してください。S3 バッチ操作で Lambda 関数を使用するベストプラクティスは、Lambda 関数自体に同時実行制限を設定することです。同時実行制限を設定することにより、ジョブが Lambda の同時実行数のほとんどを消費したり、アカウント内の

他の機能をスロットリングする可能性がなくなります。詳細については、AWS Lambda デベロッパーガイド の Lambda 予約済同時実行数の管理 を参照してください。

(オプション)MediaConvert コンソールで各 MediaConvert 動画トランスコーディングジョブを監視する

MediaConvert ジョブはメディアファイルの変換作業を行います。S3 バッチ操作ジョブが動画ごとに Lambda 関数を呼び出すと、各 Lambda 呼び出しによって、入力動画ごとに MediaConvert トランスコーディングジョブが作成されます。

1. AWS Management Console にサインインし、MediaConvert コンソール (https://console.aws.amazon.com/mediaconvert/) を開きます。
2. MediaConvert 入門者向けページが表示される場合は、[Get Started] を選択します。
3. ジョブのリストから、各行を表示して、各入力動画のトランスコーディングタスクを監視します。
4. チェックするジョブの行を特定し、ジョブ ID リンクを選択してジョブ詳細ページを開きます。
5. [Job 概要] ページの [出力] で、ブラウザでサポートされている内容に応じて、HLS、MP4、またはサムネイル出力のリンクを選択し、出力メディアファイルの S3 送信先バケットに移動します。
6. S3 出力先バケットの対応するフォルダ(HLS、MP4、またはサムネイル)で、出力メディアファイルオブジェクトの名前を選択します。

   オブジェクトの詳細ページが開きます。
7. [オブジェクトの概要] のオブジェクトの詳細ページで、オブジェクト URL のリンクを選択して、トランスコードされた出力メディアファイルを監視します。

ステップ 8: S3 宛先バケットから出力メディアファイルを確認する。

S3 宛先バケットから出力メディアファイルを確認するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。
3. バケット のリストから、ステップ 1 で作成した出力メディアファイルの S3 宛先バケットの名前を選択します (例、*amzn-s3-demo-destination-bucket1*)。

4. [オブジェクト] タブで、各入力動画には、入力動画の名前を持つフォルダがあります。各フォルダには、入力動画のトランスコードされた出力メディアファイルが含まれています。

   入力動画の出力メディアファイルを確認するには、次の操作を行います。

   a. 確認したい入力動画の名前が入ったフォルダを選択します。
   b. [Default/] フォルダを選択します。
   c. トランスコード形式 (HLS、MP4、またはこのチュートリアルではサムネイル) のフォルダを選択します。
   d. 出力メディアファイルの名前を選択します。
   e. トランスコードされたファイルを見るには、オブジェクト詳細ページで、オブジェクト URL の下のリンクを選択します。

      HLS 形式の出力メディアファイルは、短いセグメントに分割されます。これらの動画を再生するには、互換性のあるプレーヤーに `.m3u8` ファイルのオブジェクト URL を埋め込む必要があります。

ステップ 9: クリーンアップする。

S3 バッチ操作、Lambda、MediaConvert を学習演習としてのみ使用して動画をトランスコードした場合は、割り当てた AWS リ送信先を削除して、料金が発生しないようにします。

サブステップ

- S3 ソースバケットの S3 インベントリ設定を削除する。
- Lambda 関数を削除する
- CloudWatch Logs グループを削除する
- IAM ロールのインラインポリシーとともに IAM ロールを削除する
- カスタマー管理の IAM ポリシーを削除する。
- S3 バケットを空にする
- S3 バケットの削除

S3 ソースバケットの S3 インベントリ設定を削除する。

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。

2. 左側のナビゲーションペインで、[バケット] を選択します。
3. バケット] リストで、送信先バケットの名前を選択します (例、*amzn-s3-demo-source-bucket*)。
4. [管理] タブを選択します。
5. [インベントリ設定] セクションで、ステップ 5 で作成したインベントリ設定の横のオプションボタンを選択します (例、**tutorial-inventory-config**)。
6. [削除]、[確認] の順に選択します。

Lambda 関数を削除する

1. AWS Lambda コンソールの https://console.aws.amazon.com/lambda/ を開いてください。
2. 左側のナビゲーションペインで、[関数] を選択します。
3. ステップ 4 で作成した関数の横にあるチェックボックスを選択します (例、**tutorial-lambda-convert**)。
4. [アクション] を選択し、[削除] を選択します。
5. [関数の削除] ダイアログボックスで、[削除] を選択します。

CloudWatch Logs グループを削除する

1. CloudWatch コンソールの https://console.aws.amazon.com/cloudwatch/ を開いてください。
2. 左のナビゲーションペインで、[ログ] 、[ロググループ] の順に選択します。
3. ステップ 4 で作成した Lambda 関数で終わる名前を持つロググループの横にあるチェックボックスを選択します (例、**tutorial-lambda-convert**)。
4. [アクション] を選択してから、[ロググループの削除] を選択します。
5. [ロググループの削除] ダイアログボックスで、[削除] をクリックします。

IAM ロールのインラインポリシーとともに IAM ロールを削除する

ステップ 2、ステップ 3、およびステップ 6] で作成した IAM ロールを削除するには、次の作業を行います。

1. AWS Management Console にサインインして、IAM コンソール https://console.aws.amazon.com/iam/ を開きます。

2. ナビゲーションペインで、[ロール] を選択し、削除するロール名の隣にあるチェックボックスを選択します。
3. ページの上部で、[削除] を選択します。
4. 確認ダイアログボックスで、プロンプトに基づいてテキスト入力フィールドに必要な応答を入力し、[削除] を選択します。

カスタマー管理の IAM ポリシーを削除する。

ステップ 6 で作成したカスタマー管理の IAM ポリシーを削除するには、次の作業を行います。

1. AWS Management Console にサインインして、IAM コンソール https://console.aws.amazon.com/iam/ を開きます。
2. 左のナビゲーションペインの [ポリシー] を選択します。
3. ステップ 6 で作成したポリシーの横にあるオプションボタンを選択します (例、**tutorial-s3batch-policy**)。検索ボックスを使用して、グループのリストをフィルタリングできます。
4. [アクション] を選択し、[削除] を選択します。
5. テキストフィールドにポリシーの名前を入力して、このポリシーを削除することを確認し、[削除] を選択します。

S3 バケットを空にする

前提条件 、ステップ 1、および ステップ 5 で作成した S3 バケットを空にするには、次の作業を行います。

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。
3. [バケット名] リストで、空にするバケットの名前の横にあるバケットアイコンを選択し、[バケットを空にする] を選択します。
4. [バケットを空にする] ページで、テキストフィールドに **permanently delete** を入力することでバケットを空にすることを確定し、[空にする] を選択します。

S3 バケットの削除

前提条件 、ステップ 1 およびステップ 5 で作成した S3 バケットを削除するには、次の作業を行います。

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。
3. [バケット] リストで、削除するバケット名の横にあるオプションボタンを選択します。
4. [削除] を選択します。
5. [バケットの削除] ページで、テキストフィールドにバケット名を入力することでバケットを削除することを確認し、[バケットを削除] を選択します。

次のステップ

このチュートリアルを完了すると、他の関連するユースケースをさらに詳しく調べることができます。

- Amazon CloudFront を使用して、トランスコードされたメディアファイルを世界中のビューワーにストリーミングできます。詳細については、「チュートリアル: Amazon S3、Amazon CloudFront、Amazon Route 53 を使用したオンデマンドストリーミング動画のホスティング。」を参照してください。
- S3 ソースバケットにアップロードした時点で、動画をトランスコードできます。これを行うには、MediaConvert を使用して S3 の新しいオブジェクトをトランスコードするために、Lambda 関数を自動的に呼び出す Amazon S3 イベントトリガーを設定できます。詳細については、AWS Lambdaデベロッパーガイド のチュートリアル: Amazon S3 トリガーを使用して Lambda 関数を呼び出す を参照してください。

バッチオペレーションのトラブルシューティング

次のトピックは、Amazon S3 バッチオペレーションの実行中に発生する可能性がある問題のトラブルシューティングに役立ちます。

S3 バッチレプリケーションに関する問題のトラブルシューティングについては、「the section called “バッチレプリケーションエラー”」を参照してください。

共通エラー

- アクセス許可の問題があるか、S3 Object Lock 保持モードが有効の場合に、ジョブレポートが配信されない
- 「400 InvalidRequest: Task failed due to missing VersionId」によりオブジェクトが失敗したバッチオペレーション

- ジョブのタグオプションが有効な状態でジョブの失敗を作成する
- マニフェストの読み取り拒否

アクセス許可の問題があるか、S3 Object Lock 保持モードが有効の場合に、ジョブレポートが配信されない

次のエラーは、必要なアクセス許可がないか、配信先のバケットで Object Lock の保持モード (ガバナンスモードまたはコンプライアンスモード) が有効になっている場合に発生します。

エラー: 失敗の理由。ジョブレポートをレポートバケットに書き込めませんでした。権限を確認してください。

AWS Identity and Access Management IAM ロールと信頼ポリシーは、レポートの配信先であるバケットの PUT オブジェクトに対する `s3:PutObject` アクセス許可を S3 バッチオペレーションに付与するように設定する必要があります。必要なアクセス許可がないと、ジョブレポートの配信エラーが発生します。

保持モードが有効な場合、バケットは Write-Once-Read-Many (WORM) で保護されます。Object Lock の保持モードが有効になっている配信先のバケットはサポートされないため、ジョブ完了レポートの配信試行は失敗します。この問題を解決するには、オブジェクトロック保持モードが有効になっていないジョブ完了レポートのレプリケート先バケットを選択します。

「400 InvalidRequest: Task failed due to missing VersionId」によりオブジェクトが失敗したバッチオペレーション

バッチオペレーションジョブがバージョン管理されたバケット内のオブジェクトに対してアクションを実行している場合、マニフェスト内でバージョン ID フィールドが空のオブジェクトがあると、次の例のようなエラーが発生します。

エラー: *`bucket_name,prefix/file_name`*,failed,400,InvalidRequest,Task failed due to missing VersionId

このエラーは、マニフェストのバージョン ID フィールドが `null` リテラル文字列ではなく、空の文字列であるために発生します。

バッチオペレーションは、その特定のオブジェクトでは失敗しますが、ジョブ全体では失敗しません。この問題は、マニフェスト形式がオペレーション中にバージョン ID を使用するように設定されている場合に発生します。バージョン管理されていないジョブでは、各オブジェクトの最新バージョンでのみ動作し、マニフェストのバージョン ID は無視されるため、この問題は発生しません。

この問題を解決するには、空のバージョン ID を null 文字列に変換します。詳細については、「the section called “空のバージョン ID 文字列を NULL 文字列に変換します。”」を参照してください。

ジョブのタグオプションが有効な状態でジョブの失敗を作成する

s3:PutJobTagging 権限がない場合、ジョブのタグオプションを有効にしてバッチオペレーションジョブを作成すると 403 access denied エラーが発生します。

ジョブのタグオプションを有効にしてバッチオペレーションジョブを作成するには、バッチオペレーションジョブを作成する AWS Identity and Access Management (IAM) ユーザーに、s3:PutJobTagging 権限に加えて s3:CreateJob 権限が必要です。

バッチオペレーションに必要なアクセス許可の詳細については、「the section called “アクセス許可の付与”」を参照してください。

マニフェストの読み取り拒否

バッチオペレーションジョブを作成しようとしたときに、バッチオペレーションがマニフェストファイルを読み取れない場合、次のエラーが発生する可能性があります。

AWS CLI

失敗の理由: マニフェストの読み取りは禁止されています: AccessDenied

Amazon S3 コンソール

警告: マニフェストオブジェクトの ETag を取得できません。別のオブジェクトを指定して続行してください。

この問題を解決するには、次の手順を実行します。

- バッチオペレーションジョブの作成に使用した AWS アカウントの IAM ロールに s3:GetObject 権限があることを確認します。アカウントの IAM ロールには、バッチオペレーションがマニフェストファイルの読み取りを許可する s3:GetObject 権限が必要です。

  バッチオペレーションに必要なアクセス許可の詳細については、「the section called “アクセス許可の付与”」を参照してください。
- マニフェストオブジェクトのメタデータに、S3 オブジェクトの所有権とのアクセスの不一致がないか確認します。S3 オブジェクトの所有権の詳細については、「the section called “オブジェクト所有者の管理”」を参照してください。

- マニフェストファイルの暗号化に AWS Key Management Service (AWS KMS) キーが使用されているかどうかを確認してください。

  S3 バッチオペレーションでは、AWS KMS で暗号化された CSV 形式のインベントリレポートがサポートされています。ただし、バッチオペレーションでは、AWS KMS で暗号化された CSV 形式のマニフェストファイルはサポートされていません。詳細については、「Amazon S3 インベントリの設定」および「マニフェストの指定」を参照してください。

Amazon S3 Select で所定のデータをクエリする

> **Important**
>
> 新規のお客様への Amazon S3 Select の提供は終了しました。Amazon S3 Select をご利用の既存のお客様は、今後も通常どおり使用できます。詳細はこちら

Amazon S3 Select では、構造化クエリ言語 (SQL) ステートメントを使用して Amazon S3 オブジェクトのコンテンツをフィルタリングし、必要なデータのサブセットのみ取得できます。Amazon S3 Select を使用してこのデータをフィルタリングする場合、Amazon S3 が転送するデータの量を抑えることで、このデータの取得に必要なコストを削減し、レイテンシーを抑えることができます。

Amazon S3 Select で一度にクエリできるのは、1 つのオブジェクトのみです。CSV、JSON、または Apache Parquet 形式で保存されたオブジェクトのみが対象となります。また、GZIP や BZIP2 で圧縮されたオブジェクト (CSV と JSON 形式のオブジェクトのみ) や、サーバー側で暗号化されたオブジェクトにも使用できます。結果の形式 (CSV または JSON) や、結果のレコードを区切る方法は指定できます。

リクエストで SQL 式を Amazon S3 に渡します。Amazon S3 Select は SQL のサブセットをサポートします。Amazon S3 Select でサポートされている SQL 要素の詳細については、「Amazon S3 Select の SQL リファレンス」を参照してください。

SQL クエリは、Amazon S3 コンソール、AWS Command Line Interface、(AWS CLI)、`SelectObjectContent` REST API オペレーション、または AWS SDK を使用して実行できます。

> **Note**
>
> Amazon S3 コンソールでは、返されるデータの量が 40 MB に制限されます。より多くのデータを取得するには、AWS CLI または API を使用します。

要件と制限

Amazon S3 Select を使用するための要件は以下のとおりです。

- クエリ対象のオブジェクトに対して `s3:GetObject` アクセス許可が必要です。
- クエリ対象のオブジェクトが、お客様が指定したキーによるサーバー側の暗号化 (SSE-C) で暗号化されている場合は、`https` を使用する必要があり、さらにリクエストで暗号化キーを提供する必要があります。

Amazon S3 Select を使用するときは以下の制限が適用されます。

- S3 Select では、リクエストごとにクエリできるのは 1 つのオブジェクトのみです。
- SQL 式の最大長は 256 KB です。
- 入力または結果のレコードの最大長は 1 MB です。
- Amazon S3 Select は JSON 出力形式を使用してネストされたデータのみを出力できます。
- S3 Glacier Flexible Retrieval、S3 Glacier Deep Archive、または Reduced Redundancy Storage (RRS) のストレージクラスに保存されたオブジェクトのクエリはできません。また、S3 Intelligent-Tiering Archive アクセス階層や S3 Intelligent-Tiering Deep Archive アクセス階層に保存されたオブジェクトもクエリできません。ストレージクラスの詳細については、「Amazon S3 ストレージクラスの理解と管理」を参照してください。

Amazon S3 Select を Parquet オブジェクトで使用する場合は、次のとおりの追加の制限が適用されます。

- Amazon S3 Select は、GZIP または Snappy を使用した列指向の圧縮のみをサポートしています。Amazon S3 Select は、Parquet オブジェクトのオブジェクト全体の圧縮はサポートしていません。
- Amazon S3 Select は Parquet 出力をサポートしていません。出力形式として CSV または JSON を指定する必要があります。
- 最大非圧縮の行グループサイズは 512 MB です。

- オブジェクトのスキーマに指定されているデータ型を使用する必要があります。
- 繰り返しフィールドを選択すると、最後の値のみが返されます。

リクエストの構築

リクエストを構築するときは、`InputSerialization` オブジェクトを使用してクエリ対象のオブジェクトの詳細を指定します。`OutputSerialization` オブジェクトを使用して結果を返す方法の詳細を指定します。Amazon S3 でリクエストをフィルタリングできるように、SQL 式を含めることもできます。

Amazon S3 Select リクエストの構築の詳細については、「Amazon Simple Storage Service API リファレンス」の「SelectObjectContent」を参照してください。また、以下のセクションでいずれかの SDK コードサンプルを参照できます。

スキャン範囲を使用したリクエスト

Amazon S3 Select を利用すると、クエリするバイト範囲を指定して、オブジェクトのサブセットをスキャンできます。この機能により、処理を一連の重複していないスキャン範囲の個別の Amazon S3 Select リクエストに分割して、オブジェクト全体のスキャンを並列化できます。

スキャン範囲をレコードの境界に合わせる必要はありません。Amazon S3 Select スキャン範囲リクエストは、指定したバイト範囲全体で実行されます。レコードが指定したスキャン範囲内で開始しても、そのスキャン範囲を超える場合は、クエリによって処理されます。例えば、次に示す Amazon S3 オブジェクトには、一連のレコードが行区切りの CSV 形式で含まれています。

```
A,B
C,D
D,E
E,F
G,H
I,J
```

Amazon S3 Select の `ScanRange` パラメータを使用して、スキャンを 1 (バイト) で開始し、4 (バイト) で終了するとします。この場合、スキャン範囲は「`,`」で開始し、`C` で始まるレコードの最後までスキャンします。スキャン範囲のリクエストは、結果として、レコードの最後までの `C, D` を返します。

Amazon S3 Select のスキャン範囲リクエストは、Parquet、CSV (引用符区切りなし)、JSON オブジェクト (`LINES` モードのみ) をサポートしています。CSV および JSON オブジェクトは非圧縮で

ある必要があります。行ベースの CSV および JSON オブジェクトの場合、スキャン範囲が Amazon S3 Select リクエストの一部として指定されると、スキャン範囲内で開始するすべてのレコードが処理されます。Parquet オブジェクトの場合、リクエストされたスキャン範囲内で開始するすべての行グループが処理されます。

Amazon S3 Select のスキャン範囲リクエストは、AWS CLI、Amazon S3 API、AWS SDK で使用できます。Amazon S3 Select リクエストで、この機能について、ScanRange パラメータを使用できます。詳細については、「Amazon Simple Storage Service API リファレンス」の「SelectObjectContent」を参照してください。

エラー

クエリの実行中に問題が発生すると、Amazon S3 Select からエラーコードおよび関連するエラーメッセージが返されます。エラーコードの一覧とその説明については、Amazon Simple Storage Service API リファレンスのエラーコードページの「SELECT Object Content エラーコードのリスト」セクションを参照してください。

Amazon S3 Select の詳細については、以下のトピックを参照してください。

トピック

- オブジェクトでの Amazon S3 Select の使用例
- Amazon S3 Select の SQL リファレンス

オブジェクトでの Amazon S3 Select の使用例

> **Important**
>
> 新規のお客様への Amazon S3 Select の提供は終了しました。Amazon S3 Select をご利用の既存のお客様は、今後も通常どおり使用できます。詳細はこちら

S3 Select を使用すると、Amazon S3 コンソール、REST API、AWS SDK を使用して単一のオブジェクトのコンテンツを選択できます。

S3 でサポートされている SQL 関数の詳細については、「SQL 関数」を参照してください。

S3 コンソールの使用

Amazon S3 コンソールでオブジェクトからコンテンツを選択するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。
3. コンテンツを選択するオブジェクトが含まれているバケットを選択し、次にオブジェクトの名前を選択します。
4. [オブジェクトアクション] を選択し、[S3 Select を使用したクエリ] を選択します。
5. 入力データの形式に基づいて [入力設定] を行います。
6. 受信する出力の形式に基づいて、[出力設定] を行います。
7. 選択したオブジェクトからレコードを抽出するには、[SQL クエリ] に SELECT SQL コマンドを入力します。SQL コマンドの記述方法の詳細については、「Amazon S3 Select の SQL リファレンス」を参照してください。
8. SQL クエリを入力したら、[SQL クエリを実行] を選択します。次に、[クエリ結果] で SQL クエリの結果を確認できます。

REST API の使用

AWS SDK を使用して、オブジェクトのコンテンツを選択できます。ただし、アプリケーションで必要な場合は、REST リクエストを直接送信できます。リクエストとレスポンスの形式の詳細については、「SelectObjectContent」を参照してください。

AWS SDK の使用

Amazon S3 Select で `selectObjectContent` メソッドを使用してオブジェクトのコンテンツの一部を選択できます。このメソッドが成功すると、SQL 式の結果が返されます。

Java

次の Java コードでは、CSV 形式で保存されているデータを含むオブジェクトに保存されている各レコードの最初の列の値が返ります。また、`Progress` メッセージおよび `Stats` メッセージが返るようリクエストされます。CSV 形式のデータを含む有効なバケット名とオブジェクトを指定する必要があります。

作業サンプルの作成およびテストの手順については、「AWS SDK for Java のデベロッパーガイド」の「使用開始」を参照してください。

```
package com.amazonaws;

import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.CSVInput;
import com.amazonaws.services.s3.model.CSVOutput;
import com.amazonaws.services.s3.model.CompressionType;
import com.amazonaws.services.s3.model.ExpressionType;
import com.amazonaws.services.s3.model.InputSerialization;
import com.amazonaws.services.s3.model.OutputSerialization;
import com.amazonaws.services.s3.model.SelectObjectContentEvent;
import com.amazonaws.services.s3.model.SelectObjectContentEventVisitor;
import com.amazonaws.services.s3.model.SelectObjectContentRequest;
import com.amazonaws.services.s3.model.SelectObjectContentResult;

import java.io.File;
import java.io.FileOutputStream;
import java.io.InputStream;
import java.io.OutputStream;
import java.util.concurrent.atomic.AtomicBoolean;

import static com.amazonaws.util.IOUtils.copy;

/**
 * This example shows how to query data from S3Select and consume the response in
 the form of an
 * InputStream of records and write it to a file.
 */

public class RecordInputStreamExample {

    private static final String BUCKET_NAME = "${my-s3-bucket}";
    private static final String CSV_OBJECT_KEY = "${my-csv-object-key}";
    private static final String S3_SELECT_RESULTS_PATH = "${my-s3-select-results-
path}";
    private static final String QUERY = "select s._1 from S3Object s";

    public static void main(String[] args) throws Exception {
        final AmazonS3 s3Client = AmazonS3ClientBuilder.defaultClient();

        SelectObjectContentRequest request = generateBaseCSVRequest(BUCKET_NAME,
 CSV_OBJECT_KEY, QUERY);
        final AtomicBoolean isResultComplete = new AtomicBoolean(false);
```

```
       try (OutputStream fileOutputStream = new FileOutputStream(new File
(S3_SELECT_RESULTS_PATH));
            SelectObjectContentResult result =
s3Client.selectObjectContent(request)) {
           InputStream resultInputStream =
result.getPayload().getRecordsInputStream(
                   new SelectObjectContentEventVisitor() {
                       @Override
                       public void visit(SelectObjectContentEvent.StatsEvent event)
                       {
                           System.out.println(
                                   "Received Stats, Bytes Scanned: " +
event.getDetails().getBytesScanned()
                                           +  " Bytes Processed: " +
event.getDetails().getBytesProcessed());
                       }

                       /*
                        * An End Event informs that the request has finished
successfully.
                        */
                       @Override
                       public void visit(SelectObjectContentEvent.EndEvent event)
                       {
                           isResultComplete.set(true);
                           System.out.println("Received End Event. Result is
complete.");
                       }
                   }
           );

           copy(resultInputStream, fileOutputStream);
       }

       /*
        * The End Event indicates all matching records have been transmitted.
        * If the End Event is not received, the results may be incomplete.
        */
       if (!isResultComplete.get()) {
           throw new Exception("S3 Select request was incomplete as End Event was
not received.");
       }
   }
```

```
    private static SelectObjectContentRequest generateBaseCSVRequest(String bucket,
String key, String query) {
        SelectObjectContentRequest request = new SelectObjectContentRequest();
        request.setBucketName(bucket);
        request.setKey(key);
        request.setExpression(query);
        request.setExpressionType(ExpressionType.SQL);

        InputSerialization inputSerialization = new InputSerialization();
        inputSerialization.setCsv(new CSVInput());
        inputSerialization.setCompressionType(CompressionType.NONE);
        request.setInputSerialization(inputSerialization);

        OutputSerialization outputSerialization = new OutputSerialization();
        outputSerialization.setCsv(new CSVOutput());
        request.setOutputSerialization(outputSerialization);

        return request;
    }
}
```

JavaScript

AWS SDK for JavaScript と S3 `SelectObjectContent` API オペレーションを使用して Amazon S3 に保存された JSON ファイルと CSV ファイルからレコードを選択する JavaScript の例については、ブログ記事「AWS SDK for JavaScript における Amazon S3 Select のサポートの紹介」を参照してください。

Python

S3 Select を使用してカンマ区切り値 (CSV) ファイルとして Amazon S3 にロードされたデータを検索する SQL クエリの使用に関する Python の例については、ブログ記事「Amazon S3 Select を使用したサーバーまたはデータベースなしのデータのクエリ」を参照してください。

Amazon S3 Select の SQL リファレンス

> **Important**
>
> 新規のお客様への Amazon S3 Select の提供は終了しました。Amazon S3 Select をご利用の既存のお客様は、今後も通常どおり使用できます。詳細はこちら

このリファレンスには、Amazon S3 Select でサポートされる構造化クエリ言語 (SQL) の説明が記載されています。

トピック

- SELECT コマンド
- データ型
- 演算子
- 予約済みキーワード
- SQL 関数

SELECT コマンド

> **Important**
>
> 新規のお客様への Amazon S3 Select の提供は終了しました。Amazon S3 Select をご利用の既存のお客様は、今後も通常どおり使用できます。詳細はこちら

Amazon S3 セレクトは、SELECT SQL コマンドのみをサポートします。次の ANSI スタンダードの句は、SELECT 用にサポートされています。

- SELECT リスト
- FROM 句
- WHERE 句
- LIMIT 句

> **Note**
>
> Amazon S3 Select クエリは、現在サブクエリや結合はサポートしていません。

SELECT のリスト

SELECT リストは、クエリに返させる列、関数、および式を指定します。このリストは、クエリの出力を表しています。

```
SELECT *
SELECT projection1 AS column_alias_1, projection2 AS column_alias_2
```

* (アスタリスク) を使用した最初の SELECT 形式では、WHERE 句を通過したすべての行がそのまま返されます。2 番目の SELECT 形式では、列ごとにユーザー定義の出力スカラー式 ***projection1*** および ***projection2*** を含む行が作成されます。

FROM 句

Amazon S3 Select では、FROM 句の以下の形式がサポートされています。

```
FROM table_name
FROM table_name alias
FROM table_name AS alias
```

FROM 句の各形式で、table_name はクエリの対象となる S3Object です。従来のリレーショナルデータベースから移行したユーザーは、これをテーブルに対する複数のビューを含むデータベーススキーマとして考えることができます。

スタンダード SQL に従って、FROM 句は WHERE 句でフィルタリングされ SELECT リストで射影される行を作成します。

Amazon S3 Select に格納されている JSON オブジェクトでは、次の形式の FROM 句も使用することができます。

```
FROM S3Object[*].path
FROM S3Object[*].path alias
FROM S3Object[*].path AS alias
```

この形式の FROM 句を使用すると、JSON オブジェクト内の配列またはオブジェクトから選択できます。以下のいずれかの形式で path を指定できます。

- 名前 (オブジェクト内): .*name* または ['*name*']
- インデックス (配列内): [*index*]
- ワイルドカード文字 (オブジェクト内): .*
- ワイルドカード文字 (配列内): [*]

Note

- この形式の FROM 句は JSON オブジェクトに対してのみ機能します。
- ワイルドカード文字は常に最低 1 つのレコードを発行します。レコードが一致しない場合、Amazon S3 Select は値 MISSING を発行します。出力のシリアル化中 (クエリの実行の完了後)、Amazon S3 Select は MISSING 値を空のレコードに置き換えます。
- 集約関数 (AVG、COUNT、MAX、MIN、および SUM) は、MISSING 値をスキップします。
- エイリアスを指定せずにワイルドカード文字を使用する場合は、パスの最後の要素を使用して行を参照できます。例えば、クエリ SELECT price FROM S3Object[*].books[*].price を使用して、ブックのリストからすべての価格を選択できます。パスが名前ではなくワイルドカード文字で終わる場合は、値 _1 を使用して行を参照できます。例えば、SELECT price FROM S3Object[*].books[*].price の代わりにクエリ SELECT _1.price FROM S3Object[*].books[*] を使用できます。
- Amazon S3 Select は常に JSON ドキュメントをルートレベルの値の配列として扱います。したがって、クエリ対象の JSON オブジェクトにルート要素が 1 つしかない場合でも、FROM 句は S3Object[*] で始める必要があります。ただし、互換性の理由から、パスを含めない場合、Amazon S3 Select ではワイルドカード文字を省略できます。そのため、完全な句 FROM S3Object は、FROM S3Object[*] as S3Object と同等です。パスを含める場合は、ワイルドカード文字も使用する必要があります。つまり、FROM S3Object と FROM S3Object[*].*path* はどちらも有効な句ですが、FROM S3Object.*path* は有効な句ではありません。

Example

例:

例 1:

この例では、以下のデータセットとクエリを使用した場合の結果を示しています。

```
{ "Rules": [ {"id": "1"}, {"expr": "y > x"}, {"id": "2", "expr": "z = DEBUG"} ]}
{ "created": "June 27", "modified": "July 6" }
```

```
SELECT id FROM S3Object[*].Rules[*].id
```

```
{"id":"1"}
```

```
{}
{"id":"2"}
{}
```

Amazon S3 Select は、以下の理由で次の結果を生成します。

- {"id":"id-1"} — S3Object[0].Rules[0].id は一致を生成しました.
- {} — S3Object[0].Rules[1].id はレコードと一致しなかったため、Amazon S3 Select が MISSING を出力しました。これは、出力のシリアル化中に空のレコードに変更されて返されます。
- {"id":"id-2"} — S3Object[0].Rules[2].id は一致を生成しました。
- {} — S3Object[1] は Rules で一致しなかったため、Amazon S3 Select が MISSING を出力しました。これは、出力のシリアル化中に空のレコードに変更されて返されます。

一致が見つからないときに Amazon S3 Select が空のレコードを返さないようにするには、MISSING という値をテストします。次のクエリは前のクエリと同じ結果を返しますが、空の値は省略されています。

```
SELECT id FROM S3Object[*].Rules[*].id WHERE id IS NOT MISSING
```

```
{"id":"1"}
{"id":"2"}
```

例 2:

この例は、以下のデータセットとクエリを使用した場合の結果を示しています。

```
{ "created": "936864000", "dir_name": "important_docs", "files": [ { "name": "." },
 { "name": ".." }, { "name": ".aws" }, { "name": "downloads" } ], "owner": "Amazon
 S3" }
{ "created": "936864000", "dir_name": "other_docs", "files": [ { "name": "." },
 { "name": ".." }, { "name": "my stuff" }, { "name": "backup" } ], "owner": "User" }
```

```
SELECT d.dir_name, d.files FROM S3Object[*] d
```

```
{"dir_name":"important_docs","files":[{"name":"."},{"name":".."},{"name":".aws"},
{"name":"downloads"}]}
```

```
{"dir_name":"other_docs","files":[{"name":"."},{"name":".."},{"name":"my stuff"},
{"name":"backup"}]}
```

```
SELECT _1.dir_name, _1.owner FROM S3Object[*]
```

```
{"dir_name":"important_docs","owner":"Amazon S3"}
{"dir_name":"other_docs","owner":"User"}
```

WHERE 句

WHERE 句は、この構文に従います。

```
WHERE condition
```

WHERE 句は *condition* に基づいて行をフィルタリングします。condition は、ブール型の結果を持つ式です。condition の結果が TRUE である行のみが結果で返されます。

LIMIT 句

LIMIT 句は、この構文に従います。

```
LIMIT number
```

LIMIT 句により、*number* に基づいてクエリで返されるレコードの数を制限できます。

属性アクセス

SELECT 句および WHERE 句は、クエリ対象のファイルが CSV 形式であるか JSON 形式にあるかによって、以下のセクションのいずれかのメソッドを使用してレコードデータを参照できます。

CSV

- 列番号 – 行の N 番目の列を参照できます。*_N* は列名、N は列位置です。位置カウントは 1 から始まります。たとえば、最初の列名は _1 で、2 番目の列名は _2 です。

  列は *_N* または *alias*.*_N* として参照できます。たとえば、_2 と myAlias._2 はどちらも SELECT リストおよび WHERE 句の列を参照するのに有効な方法です。
- 列ヘッダー – ヘッダー行を持つ CSV 形式のオブジェクトの場合、ヘッダーは SELECT リストおよび WHERE 句で利用できます。特に、従来の SQL では、SELECT および WHERE 句の式内で、*alias*.*column_name* または *column_name* で列を参照できます。

JSON

- ドキュメント – JSON ドキュメントのフィールドは *alias*.*name* としてアクセスできます。ネストされたフィールド (*alias*.*name1*.*name2*.*name3* など) にもアクセスできます。
- リスト – [] 演算子でゼロベースのインデックスを使用して、JSON リストの要素にアクセスできます。例えば、リストの 2 番目の要素に *alias*[1] としてアクセスできます。アクセスするリスト要素とフィールドを組み合わせることができます (例: *alias*.*name1*.*name2*[1].*name3*)。
- 例: この JSON オブジェクトをサンプルデータセットとして考えます。

```
{"name": "Susan Smith",
"org": "engineering",
"projects":
    [
     {"project_name":"project1", "completed":false},
     {"project_name":"project2", "completed":true}
    ]
}
```

例 1:

以下のクエリは次の結果を返します。

```
Select s.name from S3Object s
```

```
{"name":"Susan Smith"}
```

例 2:

以下のクエリは次の結果を返します。

```
Select s.projects[0].project_name from S3Object s
```

```
{"project_name":"project1"}
```

ヘッダーおよび属性名の大文字と小文字の区別

Amazon S3 Select では、二重引用符を使用して、列ヘッダー (CSV オブジェクトの場合) および属性 (JSON オブジェクトの場合) の大文字と小文字を区別することを指定できます。二重引用符がない場合、オブジェクトヘッダーおよび属性の大文字と小文字は区別されません。あいまいな場合はエラーがスローされます。

以下の例は、1) 指定された列ヘッダーを持ち、クエリリクエストに対して `FileHeaderInfo` が `"Use"` に設定されている CSV 形式 の Amazon S3 オブジェクト、または 2) 指定された属性を持つ JSON 形式の Amazon S3 オブジェクトのいずれかです。

例 #1: クエリ対象のオブジェクトには `NAME` というヘッダーまたは属性があります。

- 次の式は、オブジェクトから値を正常に返します。引用符がないため、クエリの大文字と小文字は区別されません。

```
SELECT s.name from S3Object s
```

- 次の式は 400 エラー `MissingHeaderName` を返します。引用符があるため、クエリの大文字と小文字は区別されます。

```
SELECT s."name" from S3Object s
```

例 #2: クエリ対象の Amazon S3 オブジェクトには `NAME` という 1 つのヘッダーまたは属性と、`name` という別のヘッダーまたは属性があります。

- 次の式は 400 エラー `AmbiguousFieldName` を返します。引用符がないため、クエリの大文字と小文字は区別されませんが、2 つの一致があるため、エラーがスローされます。

```
SELECT s.name from S3Object s
```

- 次の式は、オブジェクトから値を正常に返します。引用符があるため、クエリの大文字と小文字が区別されるため、あいまいさはありません。

```
SELECT s."NAME" from S3Object s
```

ユーザー定義の用語としての予約キーワードの使用

Amazon S3 Select には、オブジェクトのコンテンツのクエリに使用する SQL 式を実行するために必要な予約キーワードのセットがあります。予約キーワードには、関数名、データ型、演算子などが含まれます。場合によっては、列ヘッダー (CSV ファイルの場合) や属性 (JSON オブジェクトの場合) などのユーザー定義の用語が、予約キーワードと競合する可能性があります。その場合は、二重引用符を使用して、予約キーワードと競合するユーザー定義の用語を意図的に使用していることを示す必要があります。そうしないと、400 解析エラーが発生します。

予約キーワードの詳細なリストについては、「予約済みキーワード」を参照してください。

次の例は、1) Amazon S3 オブジェクトが CSV 形式で、指定された列ヘッダーを持ち、クエリリクエストに対して `FileHeaderInfo` が `"Use"` に設定されているか、2) Amazon S3 オブジェクトが JSON 形式で、指定された属性を持っています。

例: クエリ対象のオブジェクトに、予約キーワードである `CAST` という名前のヘッダーまたは属性があります。

- 次の式は、オブジェクトから値を正常に返します。クエリで引用符が使用されているため、S3 Select はユーザー定義のヘッダーまたは属性を使用します。

```
SELECT s."CAST" from S3Object s
```

- 次の式は 400 解析エラーを返します。クエリで引用符が使用されていないため、`CAST` は予約キーワードと競合します。

```
SELECT s.CAST from S3Object s
```

スカラー式

`WHERE` 句および `SELECT` リスト内では、スカラー値を返す式である SQL スカラー式を持つことができます。それには以下の形式があります。

- ***literal***

  SQL リテラル。

- ***column_reference***

  形式が *column_name* または *alias*.*column_name* である列への参照。

- ***unary_op expression***

この場合、*unary_op* は SQL 単項演算子です。

- *expression binary_op expression*

  この場合、*binary_op* は SQL 二項演算子です。

- *func_name*

  この場合、*func_name* は、呼び出すスカラー関数の名前です。

- *expression* [NOT] BETWEEN *expression* AND *expression*
- *expression* LIKE *expression* [ESCAPE *expression*]

データ型

> **Important**
>
> 新規のお客様への Amazon S3 Select の提供は終了しました。Amazon S3 Select をご利用の既存のお客様は、今後も通常どおり使用できます。詳細はこちら

Amazon S3 Select は、複数のプリミティブデータ型をサポートします。

データ型変換

一般的なルールは、CAST 関数 (定義されている場合) に従うことです。CAST が定義されていない場合、すべての入力データが文字列として扱われます。その場合、必要に応じて入力データを関連するデータ型にキャストする必要があります。

CAST 関数の詳細については、「CAST」を参照してください。

サポートされているデータ型

Amazon S3 Select では、プリミティブデータ型の以下のセットがサポートされています。

名前	説明	例
bool	ブール値 (TRUE または FALSE)。	FALSE
int, integer	範囲が -9,223,372,036,854,775,808 ~ 9,223,372,036,854,775,807 の 8 バイトの符号付き整数。	100000

名前	説明	例
`string`	UTF8 でエンコードされた可変長文字列。デフォルトの制限は 1 文字です。最大文字数制限は 2,147,483,647 文字です。	`'xyz'`
`float`	8 バイトの浮動小数点数。	`CAST(0.456 AS FLOAT)`
`decimal`, `numeric`	10 を底とする数字、最大精度 38 (有効桁の最大数)、かつ -2^{31} から $2^{31}-1$ までの範囲のスケール (10 を底とするべき指数)。 **Note** Amazon S3 Select では、スケールと精度を同時に指定すると、それらは両方とも無視されます。	`123.456`
`timestamp`	タイムスタンプは特定の時点を表し、常にローカルオフセットを含み、任意の精度が可能です。 テキスト形式では、タイムスタンプは日時形式に関する W3C の注記に従いますが、少なくともまる 1 日の精度でなければ、リテラル `T` で終わる必要があります。小数秒は、精度が少なくとも 1 桁また最大は無制限で許可されています。現地時間オフセットは、UTC からの hour:minute オフセットとして、または UTC の現地時刻を示すリテラル `Z` として表すことができます。ローカルタイムオフセットは、時刻のあるタイムスタンプでは必須であり、日付値では許可されていません。	`CAST('2007-04-05T14:30Z' AS TIMESTAMP)`

サポートされている Parquet 型

Amazon S3 Select では、以下の Parquet 型がサポートされています。

- `DATE`
- `DECIMAL`

- ENUM
- INT(8)
- INT(16)
- INT(32)
- INT(64)
- LIST

> **Note**
>
> LIST Parquet 型の出力に関しては、Amazon S3 Select がサポートしているのは JSON 形式のみです。ただし、単純な値のデータに制限してクエリする場合は、CSV 形式で LIST Parquet 型をクエリすることもできます。

- STRING
- TIMESTAMP のサポートされている精度 (MILLIS/MICROS/NANOS)

> **Note**
>
> INT(96) としてのタイムスタンプの保存は、サポートされていません。INT(64) 型の範囲により、NANOS 単位を使用するタイムスタンプのみが、1677-09-21 00:12:43 から 2262-04-11 23:47:16 までの範囲の値を表すことができます。この範囲外の値は、NANOS 単位で表すことはできません。

Amazon S3 Select でサポートされているデータ型への Parquet 型のマッピング

Parquet タイプ	サポートされているデータ型
DATE	timestamp
DECIMAL	decimal, numeric
ENUM	string

Parquet タイプ	サポートされているデータ型
INT(8)	int, integer
INT(16)	int, integer
INT(32)	int, integer
INT(64)	decimal, numeric
LIST	リスト内の各 Parquet 型は、対応するデータ型にマッピングされます。
STRING	string
TIMESTAMP	timestamp

演算子

> **Important**
>
> 新規のお客様への Amazon S3 Select の提供は終了しました。Amazon S3 Select をご利用の既存のお客様は、今後も通常どおり使用できます。詳細はこちら

Amazon S3 Select は、以下の演算子をサポートしています。

論理演算子

- AND
- NOT
- OR

比較演算子

- <
- >
- <=
- >=
- =
- <>
- !=
- BETWEEN
- IN - 例: `IN ('a', 'b', 'c')`

パターンマッチング演算子

- LIKE
- _ (任意の文字と一致)
- % (任意の一連の文字と一致)

ユニタリー演算子

- IS NULL
- IS NOT NULL

算術演算子

以下に示すとおり、加算、減算、乗算、除算、剰余がサポートされています。

- +
- -
- *
- /
- %

演算子の優先順位

次の表に、演算子の優先順位を高いものから順に示します。

演算子または要素	結合性	必須
-	右	単項マイナス
*, /, %	側の	乗算、除算、剰余
+, -	側の	加算、減算
IN		集合要素関係
BETWEEN		範囲指定
LIKE		文字列パターンマッチング
<>		より小さい、より大きい
=	右	等価、割り当て
NOT	右	論理否定
AND	側の	論理積
OR	側の	論理和

予約済みキーワード

> **Important**
>
> 新規のお客様への Amazon S3 Select の提供は終了しました。Amazon S3 Select をご利用の既存のお客様は、今後も通常どおり使用できます。詳細はこちら

Amazon S3 Select の予約キーワードのリストを以下に示します。これらのキーワードには、オブジェクトのコンテンツをクエリするために使用する SQL 式の実行に必要な関数名、データ型、演算子などが含まれます。

```
absolute
action
add
all
allocate
alter
and
any
are
as
asc
assertion
at
authorization
avg
bag
begin
between
bit
bit_length
blob
bool
boolean
both
by
cascade
cascaded
case
cast
catalog
char
char_length
character
character_length
check
clob
close
coalesce
collate
```

```
collation
column
commit
connect
connection
constraint
constraints
continue
convert
corresponding
count
create
cross
current
current_date
current_time
current_timestamp
current_user
cursor
date
day
deallocate
dec
decimal
declare
default
deferrable
deferred
delete
desc
describe
descriptor
diagnostics
disconnect
distinct
domain
double
drop
else
end
end-exec
escape
except
exception
```

```
exec
execute
exists
external
extract
false
fetch
first
float
for
foreign
found
from
full
get
global
go
goto
grant
group
having
hour
identity
immediate
in
indicator
initially
inner
input
insensitive
insert
int
integer
intersect
interval
into
is
isolation
join
key
language
last
leading
left
```

```
level
like
limit
list
local
lower
match
max
min
minute
missing
module
month
names
national
natural
nchar
next
no
not
null
nullif
numeric
octet_length
of
on
only
open
option
or
order
outer
output
overlaps
pad
partial
pivot
position
precision
prepare
preserve
primary
prior
privileges
```

```
procedure
public
read
real
references
relative
restrict
revoke
right
rollback
rows
schema
scroll
second
section
select
session
session_user
set
sexp
size
smallint
some
space
sql
sqlcode
sqlerror
sqlstate
string
struct
substring
sum
symbol
system_user
table
temporary
then
time
timestamp
timezone_hour
timezone_minute
to
trailing
transaction
```

```
translate
translation
trim
true
tuple
union
unique
unknown
unpivot
update
upper
usage
user
using
value
values
varchar
varying
view
when
whenever
where
with
work
write
year
zone
```

SQL 関数

> **Important**
>
> 新規のお客様への Amazon S3 Select の提供は終了しました。Amazon S3 Select をご利用の既存のお客様は、今後も通常どおり使用できます。詳細はこちら

Amazon S3 Select は、以下の SQL 関数をサポートしています。

トピック

- 集計関数
- 条件関数

- 変換関数
- 日付関数
- 文字列関数

集計関数

> **Important**
>
> 新規のお客様への Amazon S3 Select の提供は終了しました。Amazon S3 Select をご利用の既存のお客様は、今後も通常どおり使用できます。詳細はこちら

Amazon S3 Select では、以下の集計関数がサポートされています。

関数	引数の型	戻り型
AVG(*expression*)	INT, FLOAT, DECIMAL	INT 引数の場合は DECIMAL、浮動小数点の引数の場合は FLOAT。それ以外の場合は、引数のデータ型と同じです。
COUNT	-	INT
MAX(*expression*)	INT, DECIMAL	引数の型と同じです。
MIN(*expression*)	INT, DECIMAL	引数の型と同じです。
SUM(*expression*)	INT, FLOAT, DOUBLE, DECIMAL	INT 引数の場合は INT、浮動小数点

関数	引数の型	戻り型
		の引数の場合は FLOAT。それ以外の場合は、引数のデータ型と同じです。

SUM の例

S3 インベントリレポート内のフォルダの合計オブジェクトサイズを集計するには、SUM 式を使用します。

次の S3 インベントリレポートは GZIP で圧縮された CSV ファイルです。3 つの列があります。

- 最初の列は、S3 インベントリレポートの対象となる S3 バケットの名前 (*DOC-EXAMPLE-BUCKET*) です。
- 2 番目の列は、バケット内のオブジェクトを一意に識別するオブジェクトキー名です。

  最初の行の *example-folder/* 値は、フォルダ *example-folder* 用です。Amazon S3 で、バケットにフォルダを作成すると、S3 は、指定したフォルダ名に設定されたキーを持つ 0 バイトのオブジェクトを作成します。

  2 行目の *example-folder/object1* 値は、*example-folder* フォルダ内のオブジェクト *object1* 用です。

  3 行目の *example-folder/object2* 値は、*example-folder* フォルダ内のオブジェクト *object2* 用です。

  S3 フォルダの詳細については、「フォルダを使用して Amazon S3 コンソールのオブジェクトを整理する」を参照してください。
- 3 番目の列は、バイト単位のオブジェクトサイズです。

```
"DOC-EXAMPLE-BUCKET","example-folder/","0"
"DOC-EXAMPLE-BUCKET","example-folder/object1","2011267"
"DOC-EXAMPLE-BUCKET","example-folder/object2","1570024"
```

SUM 式を使用してフォルダ *example-folder* の合計サイズを計算するには、Amazon S3 Select で SQL クエリを実行します。

```
SELECT SUM(CAST(_3 as INT)) FROM s3object s WHERE _2 LIKE 'example-folder/%' AND _2 !=
 'example-folder/';
```

クエリ結果:

```
3581291
```

条件関数

> **Important**
>
> 新規のお客様への Amazon S3 Select の提供は終了しました。Amazon S3 Select をご利用の既存のお客様は、今後も通常どおり使用できます。詳細はこちら

Amazon S3 Select は、以下の条件関数をサポートしています。

トピック

- CASE
- COALESCE
- NULLIF

CASE

CASE 式は条件関数であり、他の言語で使われている if/then/else ステートメントと似ています。CASE は、複数の条件がある場合に、結果を指定するために使用します。CASE 式には、簡易と検索の 2 種類があります。

簡易 CASE 式では、式は値と比較されます。一致が検出された場合、THEN 句で指定されたアクションが適用されます。一致が検出されない場合、ELSE 句のアクションが適用されます。

検索 CASE 式では、各 CASE がブール式に基づいて評価され、CASE ステートメントが最初の一致する CASE を返します。一致する CASE が WHEN 句で検出されない場合、ELSE 句のアクションが返されます。

構文

> **Note**
>
> 現時点で、Amazon S3 Select は ORDER BY または新しい行を含むクエリサポートしていません。必ず、改行のないクエリを使用してください。

条件の一致に使用する簡易 CASE ステートメントを以下に示します。

```
CASE expression WHEN value THEN result [WHEN...] [ELSE result] END
```

各条件の評価に使用する検索 CASE ステートメントを以下に示します。

```
CASE WHEN boolean condition THEN result [WHEN ...] [ELSE result] END
```

例

> **Note**
>
> Amazon S3 コンソールを使用して以下の例を実行し、CSV ファイルにヘッダー行が含まれている場合は、[CSV データの最初の行を除外する] を選択します。

例 1: 簡易 CASE 式を使用して、クエリの New York City を Big Apple に置き換えます。その他すべての都市名を other に置換します。

```
SELECT venuecity, CASE venuecity WHEN 'New York City' THEN 'Big Apple' ELSE 'other' END
 FROM S3Object;
```

クエリ結果:

```
venuecity        |   case
-----------------+-----------
Los Angeles      | other
New York City    | Big Apple
San Francisco    | other
Baltimore        | other
...
```

例 2: 検索 CASE 式を使用し、それぞれのチケット販売の pricepaid 値に基づいてグループ番号を割り当てます。

```
SELECT pricepaid, CASE WHEN CAST(pricepaid as FLOAT) < 10000 THEN 'group 1' WHEN
 CAST(pricepaid as FLOAT) > 10000 THEN 'group 2' ELSE 'group 3' END FROM S3Object;
```

クエリ結果:

```
pricepaid |  case
-----------+---------
12624.00 | group 2
10000.00 | group 3
10000.00 | group 3
9996.00 | group 1
9988.00 | group 1
...
```

COALESCE

COALESCE は、引数を順に評価し、最初の不明でない値 (最初の非 Null 値または欠落していない値) を返します。この関数は、Null および欠落している値を伝達しません。

構文

```
COALESCE ( expression, expression, ... )
```

パラメータ

expression

関数の対象となる式。

例

```
COALESCE(1)                -- 1
COALESCE(null)             -- null
COALESCE(null, null)       -- null
COALESCE(missing)          -- null
COALESCE(missing, missing) -- null
COALESCE(1, null)          -- 1
COALESCE(null, null, 1)    -- 1
```

```
COALESCE(null, 'string')   -- 'string'
COALESCE(missing, 1)       -- 1
```

NULLIF

2 つの式があり、2 つの式が同じ値に評価される場合、NULLIF は NULL を返し、それ以外の場合、NULLIF は最初の式を評価した結果を返します。

構文

```
NULLIF ( expression1, expression2 )
```

パラメータ

expression1, *expression2*

関数の対象となる式。

例

```
NULLIF(1, 1)             -- null
NULLIF(1, 2)             -- 1
NULLIF(1.0, 1)           -- null
NULLIF(1, '1')           -- 1
NULLIF([1], [1])         -- null
NULLIF(1, NULL)          -- 1
NULLIF(NULL, 1)          -- null
NULLIF(null, null)       -- null
NULLIF(missing, null)    -- null
NULLIF(missing, missing) -- null
```

変換関数

> **Important**
>
> 新規のお客様への Amazon S3 Select の提供は終了しました。Amazon S3 Select をご利用の既存のお客様は、今後も通常どおり使用できます。詳細はこちら

Amazon S3 Select は、次の変換関数をサポートしています。

トピック

- CAST

CAST

CAST 関数は、エンティティ (1 つの値を返す式など) を 1 つの型から別の型へと変換します。

構文

```
CAST ( expression AS data_type )
```

パラメータ

expression

1 つまたは複数の値、演算子、および値を返す SQL 関数の組み合わせです。

data_type

INT のような、式のキャスト先となる対象データ型です。サポートされているデータ型のリストについては、「データ型」を参照してください。

例

```
CAST('2007-04-05T14:30Z' AS TIMESTAMP)
CAST(0.456 AS FLOAT)
```

日付関数

> **Important**
>
> 新規のお客様への Amazon S3 Select の提供は終了しました。Amazon S3 Select をご利用の既存のお客様は、今後も通常どおり使用できます。詳細はこちら

Amazon S3 Select では、以下の日付関数がサポートされています。

トピック

- DATE_ADD
- DATE_DIFF

- EXTRACT
- TO_STRING
- TO_TIMESTAMP
- UTCNOW

DATE_ADD

日付部分、数量、タイムスタンプを指定すると、DATE_ADD は日付部分を数量に応じて変更し、更新されたタイムスタンプを返します。

構文

```
DATE_ADD( date_part, quantity, timestamp )
```

パラメータ

date_part

変更する日付の部分を指定します。これには、次のいずれかを指定できます。

- 年
- か月
- 日
- 時間
- 分
- 秒

quantity

更新されたタイムスタンプ値に適用する値。*quantity* が正の値である場合は、タイムスタンプの date_part に加算し、負の値の場合は減算します。

timestamp

関数の対象となるタイムスタンプ。

例

```
DATE_ADD(year, 5, `2010-01-01T`)                 -- 2015-01-01 (equivalent to
 2015-01-01T)
```

```
DATE_ADD(month, 1, `2010T`)                      -- 2010-02T (result will add precision
 as necessary)
DATE_ADD(month, 13, `2010T`)                     -- 2011-02T
DATE_ADD(day, -1, `2017-01-10T`)                 -- 2017-01-09 (equivalent to
 2017-01-09T)
DATE_ADD(hour, 1, `2017T`)                       -- 2017-01-01T01:00-00:00
DATE_ADD(hour, 1, `2017-01-02T03:04Z`)           -- 2017-01-02T04:04Z
DATE_ADD(minute, 1, `2017-01-02T03:04:05.006Z`) -- 2017-01-02T03:05:05.006Z
DATE_ADD(second, 1, `2017-01-02T03:04:05.006Z`) -- 2017-01-02T03:04:06.006Z
```

DATE_DIFF

日付部分と 2 つの有効なタイムスタンプを指定すると、DATE_DIFF は日付部分の差を返します。戻り値は、*date_part* の値 *timestamp1* が *date_part* の値 *timestamp2* より大きい場合に負の整数となります。戻り値は、*date_part* の値 *timestamp1* が *date_part* の値 *timestamp2* より少ない場合に正の整数となります。

構文

```
DATE_DIFF( date_part, timestamp1, timestamp2 )
```

パラメータ

date_part

比較するタイムスタンプの部分を指定します。date_part の定義については、「DATE_ADD」を参照してください。

timestamp1

比較する最初のタイムスタンプ。

timestamp2

比較する 2 番目のタイムスタンプ。

例

```
DATE_DIFF(year, `2010-01-01T`, `2011-01-01T`)           -- 1
DATE_DIFF(year, `2010T`, `2010-05T`)                    -- 4 (2010T is equivalent to
 2010-01-01T00:00:00.000Z)
DATE_DIFF(month, `2010T`, `2011T`)                      -- 12
DATE_DIFF(month, `2011T`, `2010T`)                      -- -12
```

```
DATE_DIFF(day, `2010-01-01T23:00`, `2010-01-02T01:00`) -- 0 (need to be at least 24h
 apart to be 1 day apart)
```

EXTRACT

日付部分とタイムスタンプを指定すると、EXTRACT はタイムスタンプの日付部分の値を返します。

構文

```
EXTRACT( date_part FROM timestamp )
```

パラメータ

date_part

抽出するタイムスタンプの部分を指定します。これには、次のいずれかを指定できます。

- YEAR
- MONTH
- DAY
- HOUR
- MINUTE
- SECOND
- TIMEZONE_HOUR
- TIMEZONE_MINUTE

timestamp

関数の対象となるタイムスタンプ。

例

```
EXTRACT(YEAR FROM `2010-01-01T`)                              -- 2010
EXTRACT(MONTH FROM `2010T`)                                   -- 1 (equivalent to
 2010-01-01T00:00:00.000Z)
EXTRACT(MONTH FROM `2010-10T`)                                -- 10
EXTRACT(HOUR FROM `2017-01-02T03:04:05+07:08`)                -- 3
EXTRACT(MINUTE FROM `2017-01-02T03:04:05+07:08`)              -- 4
EXTRACT(TIMEZONE_HOUR FROM `2017-01-02T03:04:05+07:08`)       -- 7
EXTRACT(TIMEZONE_MINUTE FROM `2017-01-02T03:04:05+07:08`)     -- 8
```

TO_STRING

タイムスタンプと形式パターンを指定すると、TO_STRING は、指定された形式でタイムスタンプの文字列表現を返します。

構文

```
TO_STRING ( timestamp time_format_pattern )
```

パラメータ

timestamp

関数の対象となるタイムスタンプ。

time_format_pattern

次の特殊文字の解釈を持つ文字列。

形式	例	説明
yy	69	2 桁の年
y	1969	4 桁の年
yyyy	1969	ゼロ詰めの 4 桁の年
M	1	月
MM	01	ゼロ詰めの月
MMM	Jan	月と年の省略名
MMMM	January	完全な年の名前
MMMMM	J	月の最初の文字 (注意: この形式は TO_TIMEST

形式	例	説明
		AMP　関数では使用できません)
d	2	日 (1 ~ 31)
dd	02	ゼロ詰めの日 (01 ~ 31)
a	AM	午前または午後
h	3	時間 (1 ~ 12)
hh	03	ゼロ詰めの時間 (01 ~ 12)
H	3	時間 (0 ~ 23)
HH	03	ゼロ詰めの時間 (00 ~ 23)
m	4	分 (0 ~ 59)
mm	04	ゼロ詰めの分 (00 ~ 59)
s	5	秒 (0 ~ 59)
ss	05	ゼロ詰めの秒 (00 ~ 59)
S	0	1 秒の端数 (精度: 0.1、範囲: 0.0 ~ 0.9)

形式	例	説明
SS	6	1 秒の端数 (精度: 0.01、範囲: 0.0 ~ 0.99)
SSS	60	1 秒の端数 (精度: 0.001、範囲: 0.0 ~ 0.999)
…	…	…
SSSSSSSSS	60000000	1 秒の端数 (最大精度: 1 ナノ秒、範囲: 0.0 ~ 0.999999999)
n	60000000	ナノ秒
X	+07、または Z	時間単位のオフセット。オフセットが 0 の場合は Z
XX 、、または XXXX	+0700 、、または Z	時間および分単位のオフセット。オフセットが 0 の場合は「Z」
XXX 、、または XXXXX	+07:00 、、または Z	時間および分単位のオフセット。オフセットが 0 の場合は Z

形式	例	説明
x	7	オフセット (時間単位)
xx、または xxxx	700	時間および分単位のオフセット
xxx、または xxxxx	+07:00	時間および分単位のオフセット

例

```
TO_STRING(`1969-07-20T20:18Z`,  'MMMM d, y')                    -- "July 20, 1969"
TO_STRING(`1969-07-20T20:18Z`, 'MMM d, yyyy')                   -- "Jul 20, 1969"
TO_STRING(`1969-07-20T20:18Z`, 'M-d-yy')                        -- "7-20-69"
TO_STRING(`1969-07-20T20:18Z`, 'MM-d-y')                        -- "07-20-1969"
TO_STRING(`1969-07-20T20:18Z`, 'MMMM d, y h:m a')               -- "July 20, 1969 8:18
 PM"
TO_STRING(`1969-07-20T20:18Z`, 'y-MM-dd''T''H:m:ssX')           --
 "1969-07-20T20:18:00Z"
TO_STRING(`1969-07-20T20:18+08:00Z`, 'y-MM-dd''T''H:m:ssX')     --
 "1969-07-20T20:18:00Z"
TO_STRING(`1969-07-20T20:18+08:00`, 'y-MM-dd''T''H:m:ssXXXX')   --
 "1969-07-20T20:18:00+0800"
TO_STRING(`1969-07-20T20:18+08:00`, 'y-MM-dd''T''H:m:ssXXXXX')  --
 "1969-07-20T20:18:00+08:00"
```

TO_TIMESTAMP

文字列を指定すると、TO_TIMESTAMP は、それをタイムスタンプに変換します。TO_TIMESTAMP は TO_STRING の逆演算です。

構文

```
TO_TIMESTAMP ( string )
```

パラメータ

string

関数の対象となる文字列。

例

```
TO_TIMESTAMP('2007T')                          -- `2007T`
TO_TIMESTAMP('2007-02-23T12:14:33.079-08:00') -- `2007-02-23T12:14:33.079-08:00`
```

UTCNOW

UTCNOW は、現在の時刻をタイムスタンプとして UTC で返します。

構文

```
UTCNOW()
```

パラメータ

UTCNOW はパラメータを受け取りません。

例

```
UTCNOW() -- 2017-10-13T16:02:11.123Z
```

文字列関数

> **Important**
>
> 新規のお客様への Amazon S3 Select の提供は終了しました。Amazon S3 Select をご利用の既存のお客様は、今後も通常どおり使用できます。詳細はこちら

Amazon S3 Select では、以下の文字列関数がサポートされています。

トピック

- CHAR_LENGTH, CHARACTER_LENGTH

- LOWER
- SUBSTRING
- TRIM
- UPPER

CHAR_LENGTH, CHARACTER_LENGTH

CHAR_LENGTH (または CHARACTER_LENGTH) は、指定された文字列の文字数をカウントします。

> **Note**
>
> CHAR_LENGTH と CHARACTER_LENGTH はシノニムです。

構文

```
CHAR_LENGTH ( string )
```

パラメータ

string

関数の対象となる文字列。

例

```
CHAR_LENGTH('')          -- 0
CHAR_LENGTH('abcdefg')   -- 7
```

LOWER

文字列を指定すると、LOWER はすべての大文字を小文字に変換します。大文字以外の文字は変更されません。

構文

```
LOWER ( string )
```

パラメータ

string

関数の対象となる文字列。

例

```
LOWER('AbCdEfG!@#$') -- 'abcdefg!@#$'
```

SUBSTRING

文字列、起動インデックス、長さ (オプション) を指定すると、SUBSTRING は開始インデックスから文字列の末尾、または指定された長さまでの部分文字列を返します。

> **Note**
>
> 入力文字列の先頭文字は、インデックス位置が 1 になります。
>
> - start が 1 未満で、長さを指定しない場合、インデックス位置は 1 に設定されます。
> - start が 1 未満で、長さを指定した場合、インデックス位置は start + length -1 に設定されます。
> - start + length -1 が 0 未満の場合は、空の文字列が返されます。
> - start + length -1 が 0 以上の場合は、インデックス位置 1 から始まる長さ start + length - 1 の部分文字列が返されます。

構文

```
SUBSTRING( string FROM start [ FOR length ] )
```

パラメータ

string

関数の対象となる文字列。

start

文字列の開始位置。

length

返す部分文字列の長さ。存在しない場合は、文字列の末尾に進みます。

例

```
SUBSTRING("123456789", 0)      -- "123456789"
SUBSTRING("123456789", 1)      -- "123456789"
SUBSTRING("123456789", 2)      -- "23456789"
SUBSTRING("123456789", -4)     -- "123456789"
SUBSTRING("123456789", 0, 999) -- "123456789"
SUBSTRING("123456789", 1, 5)   -- "12345"
```

TRIM

文字列の先頭または末尾の文字を切り捨てます。削除するデフォルトの文字はスペース (' ') です。

構文

```
TRIM ( [[LEADING | TRAILING | BOTH remove_chars] FROM] string )
```

パラメータ

string

関数の対象となる文字列。

LEADING | TRAILING | BOTH

このパラメータは、先頭または末尾の文字、またはその両方を切り捨てるかどうかを指定します。

remove_chars

削除する文字のセット。*remove_chars* は、長さが 1 より大きい文字列とすることができます。この関数は、削除された文字列の先頭または末尾で見つかった *remove_chars* から、任意の文字を含む文字列を返します。

例

```
TRIM('      foobar        ')              -- 'foobar'
```

```
TRIM('      \tfoobar\t         ')            -- '\tfoobar\t'
TRIM(LEADING FROM '       foobar         ')  -- 'foobar         '
TRIM(TRAILING FROM '       foobar         ') -- '       foobar'
TRIM(BOTH FROM '       foobar         ')     -- 'foobar'
TRIM(BOTH '12' FROM '1112211foobar22211122') -- 'foobar'
```

UPPER

文字列を指定すると、UPPER はすべての小文字を大文字に変換します。小文字以外の文字は変更されません。

構文

```
UPPER ( string )
```

パラメータ

string

関数の対象となる文字列。

例

```
UPPER('AbCdEfG!@#$') -- 'ABCDEFG!@#$'
```

ディレクトリバケットの使用

ディレクトリバケットは、汎用バケットのフラットなストレージ構造とは対照的に、データを階層的にディレクトリにまとめます。ディレクトリバケットにはプレフィックスの制限はなく、個々のディレクトリは水平方向にスケールできます。

AWS アカウントごとに最大 100 のディレクトリバケットを作成できます。バケット内に保存できるオブジェクトの数には制限がありません。バケット クォータは、AWS アカウント の各リージョンに適用されます。アプリケーションでこの制限を増やす必要がある場合は、サポート にお問い合わせください。

> **Important**
>
> アベイラビリティゾーンで少なくとも 90 日間リクエストアクティビティがないディレクトリバケットは、非アクティブ状態に移行します。非アクティブ状態の場合、ディレクトリバケットは一時的に読み取りと書き込みが利用できなくなります。非アクティブなバケットには、ストレージ、オブジェクトメタデータ、バケットメタデータがすべて保持されます。非アクティブなバケットには既存のストレージ料金が適用されます。非アクティブなバケットへのアクセスをリクエストすると、バケットは通常数分以内にアクティブな状態に移行します。この移行期間中に読み取りと書き込みを行うと HTTP 503 (Service Unavailable) エラーコードが返されます。これは Local Zones のバケットには適用されません。

Amazon S3 バケットにはいくつかのタイプがあります。バケットを作成する前に、アプリケーションとパフォーマンス要件に最適なバケットタイプを選択していることを確認します。さまざまなバケットタイプとそれぞれの適切なユースケースの詳細については、「バケット」を参照してください。

次のトピックでは、ディレクトリバケットについて説明します。汎用バケットの詳細については、「汎用バケットの概要」を参照してください。

ディレクトリバケットの詳細については、以下のトピックを参照してください。

- ディレクトリバケット名
- ディレクトリ
- キー名
- アクセス管理

ディレクトリバケット名

ディレクトリバケット名は、ユーザーが指定するベース名と、バケットがあるゾーン (アベイラビリティゾーンまたは Local Zone) の ID を示すサフィックスで構成されます。ディレクトリバケット名は次の形式を使用し、ディレクトリバケットの命名規則に従う必要があります。

```
bucket-base-name--zone-id--x-s3
```

例えば、次のディレクトリバケット名にはアベイラビリティーゾーン ID usw2-az1 が含まれています。

```
bucket-base-name--usw2-az1--x-s3
```

詳細については、「ディレクトリバケットの命名規則」を参照してください。

ディレクトリ

ディレクトリバケットは、汎用バケットのフラットなストレージ構造とは対照的に、データを階層的にディレクトリにまとめます。

階層型名前空間では、オブジェクトキーの区切り文字が重要です。ただし、サポートされている唯一の区切り文字はスラッシュ (/) です。ディレクトリは区切り文字の境界で定義されます。例えば、dir1/dir2/file1.txt オブジェクトキーを使用すると、ディレクトリ dir1/ と dir2/ が自動的に作成され、file1.txt オブジェクトが dir1/dir2/file1.txt パス内の /dir2 ディレクトリに追加されます。

ディレクトリバケットインデックスモデルは、ListObjectsV2 API オペレーションに対して並べ替えされていない結果を返します。結果をバケットのサブセクションに限定する必要がある場合は、prefix=dir1/ など、prefix パラメータにサブディレクトリパスを指定できます。

キー名

ディレクトリバケットの場合、複数のオブジェクト キーに共通のサブディレクトリが最初のオブジェクト キーで作成されます。同じサブディレクトリの追加のオブジェクトキーは、以前に作成したサブディレクトリを使用します。このモデルでは、アプリケーションに最適なオブジェクトキーを柔軟に選択でき、疎ディレクトリと密ディレクトリが同等にサポートされます。

アクセス管理

ディレクトリバケットでは、バケットレベルですべての S3 ブロックパブリックアクセス設定がデフォルトで有効になっています。S3 オブジェクト所有者はバケット所有者の強制に設定され、アクセスコントロールリスト (ACL) が無効になっています。上記の設定は変更できません。

デフォルトでは、ユーザーにはディレクトリバケットへのアクセス許可はありません。ディレクトリバケットへのアクセス権限を付与するには、IAM を使用してユーザー、グループ、またはロールを作成し、それらのアイデンティティにアクセス許可をアタッチします。詳細については、「IAM を使用したリージョンエンドポイント API オペレーションの承認」を参照してください。

アクセスポイントを介してディレクトリバケットへのアクセスを制御することもできます。アクセスポイントは、Amazon S3 の共有データセットへの大規模なデータアクセスの管理を簡素化します。アクセスポイントは、アクセスポイントを介して行われたすべてのリクエストに対して個別のアクセス許可とネットワークコントロールを適用するために作成する一意のホスト名です。詳細については、「アクセスポイントを使用したディレクトリバケット内の共有データセットへのアクセスの管理」を参照してください。

ディレクトリバケットのクォータ

クォータ (制限とも呼ばれます) は、AWS アカウントのサービスリソースまたはオペレーションの最大数です。ディレクトリバケットのクォータは次のとおりです。Amazon S3 でのクォータの詳細については、「Amazon S3 クォータ」を参照してください。

名前	デフォルト	引き上げ可能	説明
ディレクトリバケット	各アカウント: 100	あり	アカウントで作成できる Amazon S3 ディレクトリバケットの数。
ディレクトリバケットあたりの読み取り TPS	各ディレクトリバケット: 最大 200,000 読み取り TPS	クォータの引き上げをリクエストするには、サポートまでお問い合わせください。	ディレクトリバケットあたりの 1 秒あたりの GET/HEAD リクエストの数。

名前	デフォルト	引き上げ可能	説明
ディレクトリバケットあたりの書き込み TPS	各ディレクトリバケット: 最大 100,000 書き込み TPS	クォータの引き上げをリクエストするには、サポートまでお問い合わせください。	ディレクトリバケットあたりの 1 秒あたりの PUT/DELETE リクエストの数。

ディレクトリバケットの作成と使用

ディレクトリバケットのオペレーションの詳細については、以降のトピックを参照してください。

- ディレクトリバケットのユースケース
- ディレクトリバケットの違い
- ディレクトリバケットのネットワーク
- ディレクトリバケットの命名規則
- ディレクトリバケットのプロパティの表示
- ディレクトリバケットポリシーの管理
- ディレクトリバケットを空にする
- ディレクトリバケットの削除
- ディレクトリバケットの一覧表示
- ディレクトリバケットにアクセスできるかどうかの判断
- ディレクトリバケットでのオブジェクトの使用
- ディレクトリバケットのセキュリティ
- アクセスポイントを使用したディレクトリバケット内の共有データセットへのアクセスの管理
- ディレクトリバケットのパフォーマンスの最適化
- ディレクトリバケットを使用した開発

ディレクトリバケットのユースケース

ディレクトリバケットは、アベイラビリティーゾーンまたは Local Zone のバケット場所タイプでバケットの作成をサポートしています。

低レイテンシーのユースケースでは、単一のアベイラビリティーゾーンにディレクトリバケットを作成してデータを保存できます。アベイラビリティーゾーンのディレクトリバケットは、S3 Express One Zone ストレージクラスをサポートしています。アプリケーションがパフォーマンスの影響を受けやすく、1 桁ミリ秒の PUT と GET のレイテンシーから利点が得られる場合は、S3 Express One Zone ストレージクラスをお勧めします。アベイラビリティーゾーンでのディレクトリバケットの作成の詳細については、「高性能ワークロード」を参照してください。

データレジデンシーのユースケースでは、単一の AWS 専有ローカルゾーン (DLZ) にディレクトリバケットを作成してデータを保存できます。Local Zones のディレクトリバケットは、S3 One Zone-Infrequent Access (S3 One Zone-IA、Z-IA) ストレージクラスをサポートしています。Local Zones でのディレクトリバケットの作成の詳細については、「データレジデンシーワークロード」を参照してください。

トピック

- 高性能ワークロード
- データレジデンシーワークロード

高性能ワークロード

S3 Express One Zone

Amazon S3 Express One Zone は、高性能ワークロードに使用できます。S3 Express One Zone は、オブジェクトストレージをコンピューティングリソースと同じ場所に配置するオプションを提供し、単一のアベイラビリティーゾーンを選択できる最初の S3 ストレージクラスです。これにより、アクセス速度が最大限に高速化します。S3 Express One Zone のオブジェクトは、アベイラビリティーゾーンにあるディレクトリバケットに保存されます。ディレクトリバケットの詳細については「ディレクトリバケット」を参照してください。

Amazon S3 Express One Zone は、最もレイテンシーの影響を受けやすいアプリケーションに 1 桁のミリ秒単位で一貫したデータアクセスを提供することを目的として構築された、高パフォーマンスのシングルアベイラビリティーゾーンの Amazon S3 ストレージ クラスです。S3 Express One Zone は、現在入手可能なレイテンシーが最も低いクラウドオブジェクトストレージクラスで、データアクセス速度は最大 10 倍速く、リクエストコストは S3 Standard より 50% 低減されます。リクエストが最大で 1 桁速く完了するため、アプリケーションは直ちにメリットを得られます。S3 Express One Zone は、その他の S3 ストレージクラスと同様のパフォーマンス伸縮性を備えています。S3 Express One Zone は、一貫して 1 桁ミリ秒のレイテンシーを必要とするワークロードやパフォーマンス重視のアプリケーションに使用します。

他の Amazon S3 ストレージクラスと同様に、容量やスループットの要件を事前に計画したりプロビジョンしたりする必要はありません。必要に応じてストレージをスケールアップまたはスケールダウンでき、Amazon S3 API を介してデータにアクセスできます。

Amazon S3 Express One Zone ストレージクラスは、単一のアベイラビリティーゾーン内で 99.95% の可用性を実現するように設計されており、Amazon S3 サービスレベル契約に基づいています。S3 Express One Zone では、データは単一のアベイラビリティーゾーン内で冗長的に複数のデバイスに保存されます。S3 Express One Zone は、冗長性の損失を迅速に検出して修復することによって、同時デバイス障害を処理するように設計されています。既存のデバイスに障害が発生した場合、S3 Express One Zone はアベイラビリティーゾーン内の新しいデバイスに自動的にリクエストを移します。この冗長性により、アベイラビリティーゾーン内のデータへのアクセスの中断が回避されます。

S3 Express One Zone は、オブジェクトへのアクセスに必要なレイテンシーを最小限に抑えることが重要なあらゆるアプリケーションに最適です。このようなアプリケーションは、クリエイティブプロフェッショナルがユーザーインターフェイスからコンテンツに迅速にアクセスする必要がある、動画編集のような人間との対話型のワークフローになる可能性があります。S3 Express One Zone は、データに対する応答性の要件が似ている分析や機械学習のワークロード、特に小規模なアクセスやランダムアクセスが多いワークロードにも役立ちます。S3 Express One Zone は、Amazon EMR、Amazon SageMaker、AI、Amazon Athena など、分析や人工知能と機械学習 (AI/ML) のワークロードをサポートするためにその他の AWS のサービスと併用できます。

ディレクトリバケットは、S3 Express One Zone ストレージクラスを使用して、単一のアベイラビリティゾーン内の複数のデバイスにデータを保存しますが、複数のアベイラビリティゾーン間で

データを冗長的に保存することはありません。S3 Express One Zone を使用するためのディレクトリバケットを作成する場合は、パフォーマンスを最適化するために、Amazon EC2、Amazon Elastic Kubernetes Service、または Amazon Elastic Container Service (Amazon ECS) の各コンピューティングインスタンスにローカルな AWS リージョンおよびアベイラビリティーゾーンを指定することをお勧めします。

S3 Express One Zone を使用する場合、ゲートウェイ VPC エンドポイントを使用して、仮想プライベートクラウド (VPC) 内のディレクトリバケットを操作できます。ゲートウェイエンドポイントを使用すると、VPC 用のインターネットゲートウェイや NAT デバイスを必要とせず追加コストあんしで、VPC から S3 Express One Zone にディレクトリバケットにアクセスできます。

汎用バケットやその他のストレージクラスで使用しているのと同じ Amazon S3 の API オペレーションと機能の多くをディレクトリバケットでも使用できます。これには、Mountpoint for Amazon S3、Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3)、AWS Key Management Service (AWS KMS) キーによるサーバー側の暗号化 (SSE-KMS)、S3 バッチオペレーション、S3 ブロックパブリックアクセスなどがあります。Amazon S3 コンソール、AWS Command Line Interface (AWS CLI)、AWS SDK、Amazon S3 REST API を使用して S3 Express One Zone にアクセスすることができます。

S3 Express One Zone の詳細については、次のトピックを参照してください。

- 概要
- S3 Express One Zone の機能
- 関連サービス
- 次のステップ

概要

パフォーマンスを最適化してレイテンシーを低減するために、S3 Express One Zone には次の新しい概念が導入されています。

アベイラビリティーゾーン

Amazon S3 Express One Zone ストレージクラスは、単一のアベイラビリティーゾーン内で 99.95% の可用性を実現するように設計されており、Amazon S3 サービスレベル契約に基づいています。S3 Express One Zone では、データは単一のアベイラビリティーゾーン内で冗長的に複数のデバイスに保存されます。S3 Express One Zone は、冗長性の損失を迅速に検出して修復することによって、同時デバイス障害を処理するように設計されています。既存のデバイスに障害が発生した場合、S3

Express One Zone はアベイラビリティーゾーン内の新しいデバイスに自動的にリクエストを移します。この冗長性により、アベイラビリティーゾーン内のデータへのアクセスの中断が回避されます。

アベイラビリティーゾーンは、AWS リージョン の冗長電源、ネットワーク、および接続を備えた 1 つ以上の個別のデータセンターです。ディレクトリバケットを作成する際は、バケットの配置場所であるアベイラビリティーゾーンと AWS リージョン を選択します。

単一のアベイラビリティーゾーン

ディレクトリバケットを作成する際は、バケットの配置場所であるアベイラビリティーゾーンと AWS リージョン を選択します。

ディレクトリバケットは、パフォーマンス重視のアプリケーションで使用されるように構築された S3 Express One Zone ストレージクラスを使用します。S3 Express One Zone は、オブジェクトストレージをコンピューティングリソースと同じ場所に配置するオプションを提供し、単一のアベイラビリティーゾーンを選択できる最初の S3 ストレージクラスです。これにより、アクセス速度が最大限に高速化します。

S3 Express One Zone を使用すると、データは単一のアベイラビリティーゾーン内の複数のデバイスに冗長的に保存されます。S3 Express One Zone は、単一のアベイラビリティーゾーン内で 99.95% の可用性を実現するように設計されており、Amazon S3 サービスレベル契約に基づいています。詳細については、アベイラビリティーゾーンを参照してください。

エンドポイントとゲートウェイ VPC エンドポイント

ディレクトリバケットのバケット管理 API オペレーションはリージョンエンドポイントを通じて利用でき、リージョンエンドポイント API オペレーションと呼ばれます。リージョンエンドポイント API オペレーションの例には、`CreateBucket`、`DeleteBucket` があります。ディレクトリバケットを作成した後、ゾーンエンドポイント API オペレーションを使用して、ディレクトリバケット内のオブジェクトをアップロードして管理できます。ゾーンエンドポイント API オペレーションは、ゾーンエンドポイントを通じて実行できます。ゾーン別エンドポイント API オペレーションの例には、`PutObject`、`CopyObject` があります。

ゲートウェイ VPC エンドポイントを使用して、VPC から S3 Express One Zone にアクセスできます。ゲートウェイ エンドポイントを作成した後、VPC から S3 Express One Zone を送信先とするトラフィックのルートテーブルにターゲットとして追加できます。Amazon S3 と同様、ゲートウェイエンドポイントの使用に追加料金は発生しません。ゲートウェイ VPC エンドポイントの設定方法の詳細については、「ディレクトリバケットのネットワーク」を参照してください。

セッションベースの承認

S3 Express One Zone では、レイテンシーを最小限に抑えるように最適化された新しいセッションベースのメカニズムを使用して、リクエストを認証および認可します。CreateSession を使用して、バケットへの低レイテンシーアクセスを実現する一時的な認証情報をリクエストできます。このような一時的な認証情報は、特定の S3 ディレクトリバケットに限定されます。セッショントークンはゾーン (オブジェクトレベル) オペレーション (CopyObject を除く) でのみ使用されます。詳細については、「CreateSession を使用したゾーンエンドポイント API オペレーションの承認」を参照してください。

S3 Express One Zone でサポートされている AWS SDK は、ユーザーに代わってセッションの確立と更新を処理します。セッションを保護するため、一時的なセキュリティ認証情報は 5 分後に期限切れになります。AWS SDK をダウンロードしてインストールし、必要な AWS Identity and Access Management (IAM) アクセス許可を設定したら、直ちに API オペレーションの使用を開始できます。

S3 Express One Zone の機能

S3 Express One Zone では、次の S3 の機能が利用できます。サポートされている API とサポートされていない API の全リストについては、「ディレクトリバケットの違い」を参照してください。

アクセス管理とセキュリティ

アクセスを監査および管理するには、以下の機能を使用できます。デフォルトでは、ディレクトリバケットはプライベートであり、アクセスを明示的に許可されているユーザーのみがアクセスできます。バケット、プレフィックス、またはオブジェクトタグレベルでアクセス制御境界を設定できる汎用バケットとは異なり、ディレクトリバケットのアクセス制御境界はバケットレベルでのみ設定されます。詳細については、「IAM を使用したリージョンエンドポイント API オペレーションの承認」を参照してください。

- S3 ブロックパブリックアクセス – すべての S3 ブロックパブリックアクセス設定は、デフォルトでバケットレベルで有効になっています。このデフォルトの設定は変更できません。
- S3 オブジェクト所有権 (デフォルトでバケット所有者の強制) – アクセスコントロールリスト (ACL) はディレクトリバケットではサポートされていません。ディレクトリバケットは、S3 オブジェクト所有権のバケット所有者による強制設定を自動的に使用します。バケット所有者の強制とは、ACL が無効になり、バケット所有者はバケット内のすべてのオブジェクトを自動的に所有し、完全にコントロールできることを意味します。このデフォルトの設定は変更できません。
- AWS Identity and Access Management (IAM) – IAM は、ディレクトリバケットへのアクセスを安全に制御するうえで役立ちます。IAM を使用すると、s3express:CreateSession アクション

を通じてバケット管理 (リージョン) API オペレーションとオブジェクト管理 (ゾーン) API オペレーションへのアクセスを許可できます。詳細については、「IAM を使用したリージョンエンドポイント API オペレーションの承認」を参照してください。オブジェクト管理アクションとは異なり、バケット管理アクションはクロスアカウント間で実行できません。バケット所有者のみが、このようなアクションを実行できます。

- バケットポリシー – IAM ベースのポリシー言語を使用して、ディレクトリバケットのリソースベースのアクセス許可を設定します。IAM を使用して `CreateSession` API オペレーションへのアクセスを制御することもできます。これにより、ゾーン API オペレーションまたはオブジェクト管理 API オペレーションを使用できるようになります。ゾーン API オペレーションに同一アカウントまたはクロスアカウントのアクセス許可を付与することができます。S3 Express One Zone のアクセス許可とポリシーの詳細については、「IAM を使用したリージョンエンドポイント API オペレーションの承認」を参照してください。
- IAM Access Analyzer for S3 – アクセスポリシーを評価してモニタリングし、ポリシーが S3 リソースへの意図したアクセスのみを提供していることを確認します。

ログ記録とモニタリング

S3 Express One Zone は、リソースの使用状況のモニタリングと制御に利用できる次のような S3 ログと監視ツールを使用します。

- Amazon CloudWatch metrics – CloudWatch を使用して AWS リソースとアプリケーションをモニタリングして、パフォーマンスのメトリクスを収集し、追跡します。S3 Express One Zone は、その他の Amazon S3 ストレージクラス (`AWS/S3`) と同じ CloudWatch 名前空間を使用し、`BucketSizeBytes` と `NumberOfObjects` のディレクトリバケットの毎日のストレージメトリクスをサポートします。詳細については、「Amazon CloudWatch によるメトリクスのモニタリング」を参照してください。
- AWS CloudTrail ログ – AWS CloudTrail は、ユーザー、ロール、または AWS のサービス が実行するアクションを記録して、AWS アカウント のオペレーションとリスクの監査、ガバナンス、コンプライアンスの実施に役立つ AWS のサービス です。S3 Express One Zone の場合、CloudTrail はリージョンエンドポイント API オペレーション (`CreateBucket` や `PutBucketPolicy` など) を管理イベントとして、ゾーン API オペレーション(`GetObject` や `PutObject` など) をデータイベントとしてキャプチャします。これらのイベントには、AWS Management Console、AWS Command Line Interface (AWS CLI)、AWS SDK、および AWS API オペレーションで実行されたアクションが含まれます。詳細については、「S3 Express One Zone の AWS CloudTrail による口グ記録」を参照してください。

> **Note**
>
> Amazon S3 サーバーのアクセスログは S3 Express One Zone ではサポートされていません。

オブジェクト管理

オブジェクトストレージを管理するには、Amazon S3 コンソール、AWS SDK、AWS CLI を使用できます。S3 Express One Zone でのオブジェクト管理には次の機能を使用できます。

- S3 バッチオペレーション – バッチオペレーションを使用して、ディレクトリバケット内のオブジェクトに対して一括オペレーションを実行します。例には、Copy、Invoke AWS Lambda 関数などがあります。例えばバッチオペレーションを使用して、ディレクトリバケットと汎用バケット間でオブジェクトをコピーできます。バッチオペレーションを使用すると、AWS SDK または AWS CLI を使用するか、Amazon S3 コンソールで数回クリックするだけで、単一の S3 リクエストで数十億のオブジェクトを大規模に管理できます。
- インポート – ディレクトリバケット作成後、Amazon S3 コンソールのインポート機能を使用してバケットにオブジェクトを追加できます。インポートは、汎用バケットからディレクトリバケットにオブジェクトをコピーするバッチオペレーションジョブを作成するための効率的な方法です。

AWS SDK とクライアントライブラリ

オブジェクトストレージを管理するには、AWS SDK およびクライアントライブラリを使用できます。

- Mountpoint for Amazon S3 – Mountpoint for Amazon S3 は、高スループットのアクセスを実現するとともに、Amazon S3 のデータレイクのコンピューティングコストを削減するオープンソースのファイルクライアントです。Mountpoint for Amazon S3 は、ローカルファイルシステムの API コールを `GET` や `LIST` などの S3 オブジェクト API コールに変換します。ペタバイトのデータを処理できるため、Amazon S3 が提供する伸縮性に優れたスループットを必要とする、読み取り量の多いデータレイクワークロードに最適です。これにより、数千のインスタンスにわたってスケールアップしたりスケールダウンしたりできます。
- S3A – S3Aは Amazon S3 のデータストアにアクセスするための Hadoop と互換性のある推奨インターフェイスです。S3A は Hadoop の S3N ファイルシステムクライアントの後継です。
- PyTorch on AWS — PyTorch on AWS は、機械学習モデルの開発および本番環境へのデプロイを容易にするオープンソースの深層学習フレームワークです。

- AWS SDK – Amazon S3 でのアプリケーション開発には AWS SDK を使用できます。AWS SDK は、基盤となる Amazon S3 REST API をラップして、プログラミング作業を簡素化します。S3 Express One Zone での AWS SDK の使用の詳細については、「the section called “AWS SDK”」を参照してください。

暗号化とデータ保護

S3 Express One Zone 内のオブジェクトは、Amazon S3 マネージドキー (SSE-S3) を使用したサーバー側の暗号化により、自動的に暗号化されます。S3 Express One Zone は、AWS Key Management Service (AWS KMS) キー (SSE-KMS) を使用したサーバー側の暗号化もサポートしています。S3 Express One Zone は、お客様が指定した暗号化キーによるサーバー側の暗号化 (SSE-C) や AWS KMS keys によるデュアルレイヤーのサーバー側の暗号化 (DSSE-KMS) はサポートしていません。詳細については、「データ保護と暗号化」を参照してください。

S3 Express One Zone では、アップロードまたはダウンロード中にデータを検証するために使用されるチェックサムアルゴリズムを選択するオプションが提供されます。CRC32、CRC32C、SHA-1、SHA-256 などのセキュアハッシュアルゴリズム (SHA) や巡回冗長検査 (CRC) データ整合性チェックアルゴリズムのいずれかを選択できます。MD5 ベースのチェックサムは S3 Express One Zone ストレージクラスではサポートされていません。

詳細については、「S3 の追加のチェックサムのベストプラクティス」を参照してください。

AWS Signature Version 4 (SigV4)

S3 Express One Zone は AWS Signature Version 4 (SigV4) を使用します。SigV4 は Amazon S3 に対する HTTP 経由のリクエストを認証するために使用される署名プロトコルです。S3 Express One Zone は AWS Sigv4 を使用してリクエストに署名します。詳細については、Amazon Simple Storage Service API リファレンスの「リクエストの認証 (AWS 署名バージョン 4)」を参照してください。

強力な整合性

S3 Express One Zone は、すべての AWS リージョン のディレクトリバケット内のオブジェクトの PUT と DELETE リクエストに対して、読み取り後書き込みの強力な一貫性を提供します。詳細については、「Amazon S3 のデータ整合性モデル」を参照してください。

関連サービス

S3 Express One Zone AWS のサービス ストレージクラスで次を使用して、特定の低レイテンシーのユースケースをサポートできます。

- Amazon Elastic Compute Cloud (Amazon EC2) – Amazon EC2 は、安全でスケーラブルなコンピューティング容量を AWS クラウド で提供します。Amazon EC2 の使用により、ハードウェアに事前投資する必要がなくなり、アプリケーションをより速く開発およびデプロイできます。Amazon EC2 を使用すると、必要な数 (またはそれ以下) の仮想サーバーの起動、セキュリティおよびネットワーキングの構成、ストレージの管理ができます。
- AWS Lambda – Lambda はサーバーのプロビジョニングや管理を必要とせずにコードを実行できるコンピューティングサービスです。バケットの通知設定を構成し、関数のリソースベースのアクセス許可ポリシーで関数を呼び出すためのアクセス許可を Amazon S3 に付与します。
- Amazon Elastic Kubernetes Service (Amazon EKS) – Amazon EKS は、AWS で独自の Kubernetes コントロールプレーンをインストール、運用、保守する必要がないマネージドサービスです。Kubernetes は、コンテナ化されたアプリケーションの管理、スケーリング、デプロイを自動化するオープンソースシステムです。
- Amazon Elastic Container Service (Amazon ECS) – Amazon ECS は、コンテナ化されたアプリケーションを簡単にデプロイ、管理、スケーリングできる、フルマネージドコンテナオーケストレーションサービスです。
- AWS Key Management Service (AWS KMS) – AWS Key Management Service (AWS KMS) は、データの暗号化に使用する暗号化キーの作成と管理を容易にする AWS マネージドサービスです。AWS KMS で作成した AWS KMS キーは、FIPS 140-2 検証済みハードウェアセキュリティモジュール (HSM) によって保護されます。KMS キーを使用または管理するには、AWS KMS を使用します。
- Amazon Athena – Athena はインタラクティブなクエリサービスで、Amazon S3 内のデータを標準 SQL を使用して直接的に簡単に分析できます。また、Athena を使用すると、リソースの計画、設定、管理を必要とせずに Apache Spark を使用してデータ分析をインタラクティブに実行することもできます。Athena で Apache Spark アプリケーションを実行する場合は、処理用の Spark コードを送信して、結果を直接受け取ります。
- Amazon SageMaker トレーニング – AWS Marketplace の組み込みアルゴリズム、カスタムアルゴリズム、ライブラリ、モデルなど、Amazon SageMaker でモデルをトレーニングするためのオプションを参照します。
- AWS Glue – AWS Glue は、分析を行うユーザーが複数のソースからのデータを簡単に検出、準備、移動、統合できるようにするサーバーレスのデータ統合サービスです。分析用の AWS Glue は、分析、機械学習、アプリケーション開発に使用できます。AWS Glue には、ジョブの作成、実行、ビジネスワークフローの実装のための生産性向上ツールとデータ運用ツールも追加されています。

- Amazon EMR – Amazon EMR は、Apache Hadoop や Apache Spark などのビッグデータフレームワークを AWS で簡単に実行して、膨大な量のデータを処理および分析できるマネージドクラスタープラットフォームです。
- AWS CloudTrail – AWS CloudTrail は、AWS アカウントのリスク監査、ガバナンス、コンプライアンスの活用を支援する AWS のサービスです。ユーザー、ロール、または AWS のサービスによって実行されたアクションは、CloudTrail にイベントとして記録されます。イベントには、AWS マネジメントコンソール、AWS コマンドラインインターフェイス、AWS SDK、API で実行したアクションが含まれます。
- AWS CloudFormation – AWS のリソースのモデリングおよびセットアップに役立つサービスです。リソース管理の時間を減らし、AWS で実行するアプリケーションに注力する時間を増加できます。使用するすべての AWS リソース (Amazon EC2 インスタンスや Amazon RDS DB インスタンスなど) を記述するテンプレートを作成すれば、CloudFormation がお客様に代わってこれらのリソースのプロビジョニングや設定を受け持ちます。AWS リソースを個別に作成、設計して、それぞれの依存関係を考える必要はありません。CloudFormation がこれを処理します。

次のステップ

S3 Express One Zone ストレージクラスとディレクトリバケットの使用の詳細については、次のトピックを参照してください。

- チュートリアル: S3 Express One Zone の使用を開始する
- S3 Express One Zone のアベイラビリティーゾーンとリージョン
- アベイラビリティーゾーンのディレクトリバケットのネットワーク
- アベイラビリティーゾーンでのディレクトリバケットの作成
- アベイラビリティーゾーン内のディレクトリバケット用のリージョンエンドポイントとゾーンエンドポイント
- S3 Express One Zone のパフォーマンスの最適化

チュートリアル: S3 Express One Zone の使用を開始する

Amazon S3 Express One Zone は、オブジェクトストレージをコンピュートリソースと同じ場所に配置するオプションを備えた単一のアベイラビリティーゾーンを選択できる最初の S3 ストレージクラスです。これにより、最高レベルのアクセス速度を実現できます。S3 Express One Zone のデータは、アベイラビリティーゾーン内のディレクトリバケットに保存されます。ディレクトリバケットの詳細については「ディレクトリバケット」を参照してください。

S3 Express One Zone は、リクエストのレイテンシーを最小限に抑えることが不可欠なあらゆるアプリケーションに最適です。このようなアプリケーションは、クリエイティブプロフェッショナルがユーザーインターフェイスからコンテンツに迅速にアクセスする必要がある、動画編集のような人間との対話型のワークフローになる可能性があります。S3 Express One Zone は、データに対する応答性の要件が似ている分析や機械学習のワークロード、特に小規模なアクセスやランダムアクセスが多いワークロードにも役立ちます。分析や人工知能と機械学習 (AI/ML) のワークロードをサポートするために、Amazon EMR、Amazon Athena、AWS Glue データカタログ、Amazon SageMaker モデルトレーニングなどの AWSと併用できます。S3 Express One Zone ストレージクラスとディレクトリバケットは、Amazon S3 コンソール、AWS SDK、AWS コマンドラインインターフェイス (AWS CLI)、Amazon S3 REST API を使って操作できます。詳細については、「S3 Express One Zone とは」および「S3 Express One Zone の違いとは」を参照してください。
これは S3 Express One Zone のワークフロー図です。

目的

このチュートリアルでは、ゲートウェイエンドポイントを作成し、次に IAM ポリシーを作成してアタッチします。その後、ディレクトリバケットを作成し、インポートアクションを使って現在汎用バケットに保存されているオブジェクトをディレクトリバケットに追加します。オブジェクトは手動でディレクトリバケットにアップロードすることもできます。

トピック

- 前提条件
- ステップ 1: S3 Express One Zone ディレクトリバケットに到達するためのゲートウェイ VPC エンドポイントを設定する
- ステップ 2: S3 Express One Zone ディレクトリバケットを作成する
- ステップ 3: S3 Express One Zone ディレクトリバケットへのデータのインポート
- ステップ 4: オブジェクトを S3 Express One Zone ディレクトリバケットに手動でアップロードする
- ステップ 5: S3 Express One Zone ディレクトリバケットを空にする
- ステップ 6: S3 Express One Zone ディレクトリバケットを削除する
- 次のステップ

前提条件

このチュートリアルを開始する前に、適切な許可が付与された AWS Identity and Access Management (IAM) ユーザーとしてサインインできる AWS アカウントが必要です。

サブステップ

- AWS アカウント の作成
- AWS アカウントに IAM ユーザーを作成する (コンソール)
- IAM ポリシーを作成し、IAM ユーザーまたはロールにアタッチする (コンソール)

AWS アカウント の作成

このチュートリアルを完了するには、AWS アカウント が必要です。AWS にサインアップすると、Amazon S3 を含む AWS のすべてのサービスに対して AWS アカウント が自動的にサインアップされます。料金は、使用するサービスの料金のみが請求されます。料金の詳細については、S3 の料金を参照してください。

AWS アカウントに IAM ユーザーを作成する (コンソール)

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に管理するうえで役立つ AWS のサービス です。IAM 管理者は、どのユーザーを認証して (サインイン)、S3 Express One Zone 内のオブジェクトへのアクセスやディレクトリバケットの使用を許可するかを制御します。IAMは追加料金なしでご利用いただけます。

デフォルトでは、ユーザーにはディレクトリバケットにアクセスして S3 Express One Zone オペレーションを実行するアクセス許可はありません。ディレクトリバケットと S3 Express One Zone オペレーションに対するアクセス許可を付与するには、IAM を使用してユーザーまたはロールを作成し、それらのアイデンティティにアクセス許可をアタッチします。IAM ユーザーを作成する方法の詳細については、「IAM ユーザーガイド」の「IAM ユーザーの作成 (コンソール)」を参照してください。IAM ロールを作成する方法の詳細については、「IAM ユーザーガイド」の「IAM ユーザーにアクセス許可を委任するロールの作成」を参照してください。

このチュートリアルでは、わかりやすいように IAM ユーザーを作成して使用します。このチュートリアルを完了したら、忘れずに「IAM ユーザーを削除する」を行います。本番環境で使用する場合は、IAM ユーザーガイドの「IAM でのセキュリティのベストプラクティス」に従うことをお勧めします。ベストプラクティスでは、人間のユーザーと ID プロバイダーとのフェデレーションにより、一時的な認証情報を使用して AWS にアクセスする必要があります。追加のベストプラクティスとして、ワークロードでは一時的な認証情報で IAM ロールを使用し、AWS にアクセス必要があります。AWS IAM Identity Center を使用して一時的な認証情報を持つユーザーを作成する方法については、「AWS IAM Identity Center ユーザーガイド」で開始方法を参照してください。

> **Warning**
>
> IAM ユーザーは長期認証情報を保有するため、セキュリティ上のリスクが生じます。このリスクを軽減するために、これらのユーザーにはタスクの実行に必要な権限のみを付与し、不要になったユーザーを削除することをお勧めします。

IAM ポリシーを作成し、IAM ユーザーまたはロールにアタッチする (コンソール)

デフォルトでは、ユーザーにはディレクトリバケットと S3 Express One Zone オペレーションのためのアクセス許可はありません。ディレクトリバケットへのアクセス権限を付与するには、IAM を使用してユーザー、グループ、またはロールを作成し、それらのアイデンティティにアクセス許可をアタッチします。S3 Express One Zone アクセスのバケットポリシーまたは IAM アイデンティティポリシーに含めることができるリソースは、ディレクトリバケットのみです。

S3 Express One Zone でリージョンエンドポイント API オペレーション (バケットレベルオペレーションまたはコントロールプレーンオペレーション) を使用するには、セッション管理を必要としない IAM 認可モデルを使用します。アクセス許可はアクションごとに個別に付与されます。ゾーンエンドポイント API オペレーション (オブジェクトレベルオペレーションまたはデータプレーンオペレーション) を使用するには、`CreateSession`を使用して、データリクエストの低レイテンシー認可に最適化されたセッションを作成および管理します。ッションントークンを取得して使用するには、アイデンティティベースのポリシーまたはバケットポリシーでディレクトリバケットの `s3express:CreateSession` アクションを許可する必要があります。Amazon S3 コンソール、AWS コマンドラインインターフェイス (AWS CLI)、または AWS SDK を使用して S3 Express One Zone にアクセスしている場合、S3 Express One Zone がユーザーに代わってセッションを作成します。詳細については、「`CreateSession` 認可」および「S3 Express One Zone 向け AWS Identity and Access Management (IAM)」を参照してください。

IAM ポリシーを作成して IAM ユーザー (またはロール) にアタッチする

1. AWS マネジメントコンソールにサインインし、IAM マネジメントコンソールを開きます。
2. ナビゲーションペインで、ポリシー を選択してください。
3. [ポリシーを作成] を選択します。
4. [JSON] を選択します。
5. 次のポリシーをポリシーエディタウィンドウにコピーします。ディレクトリバケットを作成したり、Amazon S3 Express One Zone を使用したりする前に、AWS Identity and Access Management (IAM) ロールまたはユーザーに必要なアクセス許可を付与する必要があります。

このポリシー例では、CreateSession API オペレーション (他のゾーン API オペレーションまたはオブジェクトレベル API オペレーションで使用) とすべてのリージョンエンドポイント (バケットレベル) API オペレーションへのアクセスを許可します。このポリシーでは、すべてのディレクトリバケットでの CreateSession API オペレーションの使用が許可されます。ただし、リージョンエンドポイント API オペレーションは、指定されたディレクトリバケットでの使用のみが許可されます。このポリシーの例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Sid": "AllowAccessRegionalEndpointAPIs",
             "Effect": "Allow",
             "Action": [
                 "s3express:DeleteBucket",
                 "s3express:DeleteBucketPolicy",
                 "s3express:CreateBucket",
                 "s3express:PutBucketPolicy",
                 "s3express:GetBucketPolicy",
                 "s3express:ListAllMyDirectoryBuckets"
             ],

             "Resource": "arn:aws:s3express:region:account_id:bucket/bucket-base-name--zone-id--x-s3/*"
         },
         {
             "Sid": "AllowCreateSession",
             "Effect": "Allow",
             "Action": "s3express:CreateSession",
             "Resource": "*"
         }
     ]
 }
```

6. [次へ] を選択します。
7. ポリシーに名前を付けます。

> **Note**
>
> S3 Express One Zone ではバケットタグはサポートされていません。

8. [Create policy] (ポリシーを作成) を選択します。
9. IAM ポリシーを作成したら、IAM ユーザーにポリシーをアタッチできます。ナビゲーションペインで、ポリシー を選択してください。
10. 検索バーに、ポリシー名を入力します。
11. [アクション] メニューの [アタッチ] を選択します。
12. [Filter by Entity Type] (エンティティタイプでフィルタリング) で、[IAM ユーザー] または [ロール] を選択します。
13. 検索フィールドに、使用するユーザーまたはロールの名前を入力します。
14. [ポリシーをアタッチ] を選択します。

ステップ 1: S3 Express One Zone ディレクトリバケットに到達するためのゲートウェイ VPC エンドポイントを設定する

ゲートウェイ仮想プライベートクラウド (VPC) エンドポイントを通じて、ゾーン API オペレーションとリージョン API オペレーションの両方にアクセスできます。ゲートウェイエンドポイントを設定すると、トラフィックは NAT ゲートウェイを経由せずに S3 Express One Zone に到達できます。S3 Express One Zone の使用時に最適なネットワークパスが提供されるため、ゲートウェイエンドポイントを設定することを強くお勧めします。VPC 用のインターネットゲートウェイや NAT デバイスを必要とせず、追加コストなしで、VPC から S3 Express One Zone ディレクトリバケットにアクセスすることができます。S3 Express One Zone ストレージクラスのオブジェクトとディレクトリバケットに接続するゲートウェイエンドポイントは、次の手順を使用して設定します。

S3 Express One Zone にアクセスするには、標準の Amazon S3 エンドポイントとは異なるリージョンエンドポイントとゾーンエンドポイントを使用します。使用する Amazon S3 API オペレーションに応じて、ゾーンエンドポイントまたはリージョンエンドポイントのいずれかが必要です。エンドポイントタイプ別のサポートされている API オペレーションの完全なリストについては、S3 Express One Zone でサポートされている API オペレーションを参照してください。ゾーンエンドポイントとリージョンエンドポイントの両方にアクセスするには、ゲートウェイ仮想プライベートクラウド (VPC) エンドポイントを介す必要があります。

次の手順を使用して、S3 Express One Zone ストレージクラスのオブジェクトとディレクトリバケットに接続するゲートウェイエンドポイントを作成します。

ゲートウェイ VPC エンドポイントを設定するには

1. https://console.aws.amazon.com/vpc/ で Amazon VPC コンソールを開きます。
2. ナビゲーションペインの [仮想プライベートクラウド] で、[エンドポイント] を選択します。

3. [エンドポイントの作成] を選択します。
4. エンドポイントの名前を作成します。
5. [Service category] (サービスカテゴリ) で、AWS のサービス を選択します。
6. [サービス] で、タイプ = ゲートウェイのフィルターを使って検索し、com.amazonaws.***region***.s3express の隣にあるボタンをクリックします。
7. [VPC] で、エンドポイントを作成する VPC を選択します。
8. [Route tables] (ルートテーブル) で、エンドポイントで使用するルートテーブルを選択します。Amazon VPC は、サービスに送信するトラフィックをエンドポイントネットワークインターフェイスにポイントするルートを自動的に追加します。
9. [ポリシー] では、[フルアクセス] を選択して、VPC エンドポイントのすべてのリソースに対するすべてのプリンシパルによるすべてのオペレーションを許可します。それ以外の場合は、[カスタム] を選択して、プリンシパルが VPC エンドポイントを介してリソースに対してアクションを実行するために必要なアクセス許可を制御する VPC エンドポイントポリシーをアタッチします。
10. [エンドポイントの作成] を選択します。

ゲートウェイエンドポイントを作成した後、リージョン API エンドポイントとゾーン API エンドポイントを使用して、Amazon S3 Express One Zone ストレージクラスのオブジェクトとディレクトリバケットにアクセスできます。

ステップ 2: S3 Express One Zone ディレクトリバケットを作成する

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ページ上部にあるナビゲーションバーで、現在表示されている AWS リージョン の名前をクリックします。次に、バケットを作成するリージョンを選択します。

> **Note**
>
> レイテンシーとコストを最小化するため、さらに規制条件に対応するために、最寄りのリージョンを選択します。明示的に別のリージョンに移動する場合を除き、特定のリージョンに保管されたオブジェクトは、そのリージョンから移動されることはありません。Amazon S3 AWS リージョン のリストについては、「Amazon Web Services 全般のリファレンス」の「AWS のサービス エンドポイント」を参照してください。

3. 左のナビゲーションペインで、[ディレクトリバケット] を選択します。

4. [Create bucket (バケットの作成)] を選択します。[バケットの作成] ページが開きます。
5. [全般設定] で、バケットが作成される AWS リージョン を確認します。

   [バケットタイプ] で [ディレクトリ] を選択します。

   > **Note**
   >
   > - ディレクトリバケットをサポートしていないリージョンを選択した場合、[バケットタイプ] オプションは表示されなくなり、バケットタイプはデフォルトで汎用バケットになります。ディレクトリバケットを作成するには、サポートされているリージョンを選択する必要があります。ディレクトリバケットと Amazon S3 Express One Zone ストレージクラスをサポートするリージョンのリストについては、「the section called “S3 Express One Zone のアベイラビリティーゾーンとリージョン”」を参照してください。
   > - バケット作成後にバケットタイプは変更できません。

   > **Note**
   >
   > このアベイラビリティーゾーンは、バケットの作成後に変更することはできません。

6. [アベイラビリティーゾーン] では、コンピューティングサービスにローカルなアベイラビリティーゾーンを選択します。ディレクトリバケットと S3 Express One Zone ストレージクラスをサポートするアベイラビリティーゾーンのリストについては、「the section called “S3 Express One Zone のアベイラビリティーゾーンとリージョン”」を参照してください。

   [アベイラビリティーゾーン] でチェックボックスをオンにして、アベイラビリティーゾーンに障害が発生した場合に、データが使用できなくなったり、データが失われたりする場合があることに同意します。

   > **Important**
   >
   > ディレクトリバケットは、単一のアベイラビリティーゾーン内の複数のデバイスに保存されますが、ディレクトリバケットはアベイラビリティーゾーン間でデータを冗長に保存することはありません。

7. [バケット名] には、ディレクトリバケット名を入力します。

ディレクトリバケットの命名には、次のルールが適用されます。

- 選択したゾーン (AWS アベイラビリティーゾーンまたは AWS Local Zone) 内で一意である必要があります。
- 名前は、サフィックスを含め 3 文字 (最短) から 63 文字 (最長) の長さでなければなりません。
- 小文字の英文字、数字、およびハイフン (-) で構成されていること。
- 文字や数字で始まり、文字や数字で終わります。
- `--`*`zone-id`*`--x-s3` のサフィックスを含める必要があります。
- バケット名のプレフィックスは `xn--` で始まってはいけません。
- バケット名のプレフィックスは `sthree-` で始まってはいけません。
- バケット名のプレフィックスは `sthree-configurator` で始まってはいけません。
- バケット名のプレフィックスは `amzn-s3-demo-` で始まってはいけません。
- バケット名のサフィックスは `-s3alias` で終わってはいけません。このサフィックスは、アクセスポイントのエイリアス名用に予約されています。詳細については、「汎用バケットのアクセスポイントのエイリアス」を参照してください。
- バケット名のサフィックスは `--ol-s3` で終わってはいけません。このサフィックスは、Object Lambda アクセスポイントのエイリアス名用に予約されています。詳細については、「S3 バケット Object Lambda アクセスポイントでのバケット形式のエイリアスの使用方法」を参照してください。
- バケット名のサフィックスは `.mrap` で終わってはいけません。このサフィックスは、マルチリージョンアクセスポイント名用に予約されています。詳細については、「Amazon S3 マルチリージョンアクセスポイントの命名規則」を参照してください。

コンソールを使用してディレクトリバケットを作成すると、指定したベース名にサフィックスが自動的に追加されます。このサフィックスには、選択したアベイラビリティーゾーンのアベイラビリティーゾーン ID が含まれます。

バケットを作成したら、その名前を変更することはできません。バケットの命名の詳細については、「汎用バケットの命名規則」を参照してください。

> **Important**
>
> バケット名にアカウント番号などの機密情報を含めないでください。バケット名は、バケット内のオブジェクトを参照する URL に表示されます。

8. [オブジェクト所有者] で、[バケット所有者の強制] の設定が自動的に有効になり、アクセスコントロールリスト (ACL) が無効になります。ディレクトリバケットの場合、ACL は有効にできません。

   バケット所有者の強制 (デフォルト) – ACL は無効になり、バケット所有者は汎用バケット内のすべてのオブジェクトを自動的に所有し、完全に制御します。ACL は、S3 汎用バケット内のデータへのアクセス許可に影響を与えなくなりました。このバケットはアクセスコントロールを定義するためだけにポリシーを使用します。

9. [このバケットのブロックパブリックアクセス設定] で、ディレクトリバケットのパブリックアクセスブロック設定がすべて自動的に有効になります。ディレクトリバケットの場合、この設定は変更できません。ブロックパブリックアクセスの詳細については、Amazon S3 ストレージへのパブリックアクセスのブロック を参照してください。

10. デフォルトの暗号化を設定するには、[暗号化タイプ] で次のいずれかを選択します。

    - [Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3)]
    - [AWS Key Management Service キーによるサーバー側の暗号化 (SSE-KMS)]

    Amazon S3 のサーバー側の暗号化を使用してデータを暗号化する方法の詳細については、「データ保護と暗号化」を参照してください。

> **Important**
>
> デフォルト暗号化設定に SSE-KMS オプションを使用する場合、AWS KMS の 1 秒あたりのリクエスト (RPS) 制限が適用されます。AWS KMS クォータの詳細およびクォータの引き上げをリクエストする方法については、「AWS Key Management Service デベロッパーガイド」の「クォータ」を参照してください。
> デフォルト暗号化を有効にする際、バケットポリシーの更新が必要な場合があります。詳細については、「クロスアカウント操作での SSE-KMS 暗号化の使用」を参照してください。

11. [Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3)] を選択した場合は、[バケットキー] の下に [有効] が表示されます。ディレクトリバケットが SSE-S3 でデフォルトの暗号化を使用するように設定すると、S3 バケットキーは常に有効になります。S3 バケットキーは、ディレクトリバケット内の GET および PUT オペレーションで常に有効になっており、無効にすることはできません。SSE-KMS で暗号化されたオブジェクトを、CopyObject、UploadPartCopy、バッチオペレーションの Copy オペレーション、または import ジョブを使用して、汎用バケットからディレクトリバケットへ、ディレクトリバケットから汎用バケットへ、またはディレクトリバケット間でコピーする場合、S3 バケットキーはサポートされません。この場合、KMS で暗号化されたオブジェクトのコピーリクエストが実行されるたびに、Amazon S3 は AWS KMS を呼び出します。

    S3 バケットキーは、Amazon S3 から AWS KMS へのリクエストトラフィックを減らし、暗号化のコストを削減します。詳細については、「Amazon S3 バケットキーを使用した SSE-KMS のコストの削減」を参照してください。

12. [AWS Key Management Service キーによるサーバー側の暗号化 (SSE-KMS)] を選択した場合は、[AWS KMS キー] で次のいずれかの方法で AWS Key Management Service キーを指定するか、新しいキーを作成します。

    - 使用可能な KMS キーのリストから選択するには、[AWS KMS keys から選択する] を選択し、[使用可能な AWS KMS keys] のリストから自分の [KMS キー] を選択します。

      カスタマーマネージドキーのみがこのリストに表示されます。AWS マネージドキー (aws/s3) はディレクトリバケットではサポートされていません。カスタマーマネージドキーの詳細については、AWS Key Management Serviceデベロッパーガイドの「カスタマーキーと AWS キー」を参照してください。
    - KMS キーの ARN またはエイリアスを入力するには、[AWS KMS key ARN を入力] を選択し、[AWS KMS key ARN] に KMS キーの ARN またはエイリアスを入力します。
    - AWS KMS コンソールで新しいカスタマーマネージドキーを作成するには、[KMS キーを作成] を選択します。

      AWS KMS key の作成の詳細については、「AWS Key Management Service デベロッパーガイド」の「キーの作成」を参照してください。

Important

- SSE-KMS 設定では、バケットの存続期間中、ディレクトリバケットごとに 1 つのカスタマーマネージドキーしかサポートできません。AWS マネージドキー (aws/s3) はサポートされていません。また、SSE-KMS のカスタマーマネージドキーを指定した後は、バケットの SSE-KMS 設定のカスタマーマネージドキーを上書きすることはできません。

  バケットの SSE-KMS 設定に指定したカスタマーマネージドキーは、次のように識別できます。

  - `HeadObject` API オペレーションリクエストを実行して、レスポンス内の `x-amz-server-side-encryption-aws-kms-key-id` の値を検索します。

  データに新しいカスタマーマネージドキーを使用するには、新しいカスタマーマネージドキーを使用して既存のオブジェクトを新しいディレクトリバケットにコピーすることをお勧めします。

- バケットと同じ AWS リージョン で使用可能な KMS キーのみを使用できます。Amazon S3 コンソールには、バケットと同じリージョンで最初の 100 個の KMS キーしか表示されません。リストに存在しない KMS キーを使用するには、KMS キー ARN を入力する必要があります。別のアカウントが所有している KMS キーを使用する場合は、まずそのキーを使用するアクセス許可が必要であり、次に KMS キー ARN を入力する必要があります。KMS キーのクロスアカウント権限の詳細については、AWS Key Management Service デベロッパーガイドの「他のアカウントで使用できる KMS キーを作成する」を参照してください。SSE-KMS に関する詳細は、「ディレクトリバケット内の新しいオブジェクトのアップロードに AWS KMS によるサーバー側の暗号化 (SSE-KMS) を指定する」を参照してください。
- ディレクトリバケットでサーバー側の暗号化に AWS KMS key を使用する場合は、対称暗号化 KMS キーを選択する必要があります。Amazon S3 では、対称暗号化 KMS キーのみがサポートされ、非対称暗号化 KMS キーはサポートされません。詳細については、AWS Key Management Service デベロッパーガイドの「Identifying symmetric and asymmetric KMS keys」(対称および非対称 KMS キーの識別) を参照してください。

Amazon S3 での AWS KMS の使用に関する詳細は、「ディレクトリバケットでの AWS KMS キーによるサーバー側の暗号化 (SSE-KMS) の使用」を参照してください。

13. [バケットを作成] を選択します。バケットを作成したら、ファイルやフォルダをバケットに追加できます。詳細については、「the section called “ディレクトリバケットでのオブジェクトの使用”」を参照してください。

ステップ 3: S3 Express One Zone ディレクトリバケットへのデータのインポート

この手順を完了するには、オブジェクトが含まれていて、ディレクトリバケットと同じ AWS リージョンにある汎用バケットが必要です。

Amazon S3 でディレクトリバケットを作成した後、Amazon S3 コンソールでインポートアクションを使用して新しいバケットにデータを入力できます。インポートを使用すると、データをインポートするプレフィックスまたは汎用バケットを選択することで、コピーするすべてのオブジェクトを個々に指定する必要がなくなるため、ディレクトリバケットへのデータのコピーが容易になります。インポートでは、選択したプレフィックスまたは汎用バケット内のオブジェクトをコピーする S3 バッチオペレーションが使用されます。コピーのインポートジョブの進行状況は、S3 バッチオペレーションジョブの詳細ページからモニタリングできます。

インポートアクションを使用するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ページ上部にあるナビゲーションバーで、現在表示されている AWS リージョン の名前をクリックします。次に、ディレクトリバケットがあるアベイラビリティーゾーンに関連付けられたリージョンを選択します。
3. 左のナビゲーションペインで、[ディレクトリバケット] を選択します。
4. オブジェクトをインポートする先のバケットの名前の隣にあるオプションボタンをクリックします。
5. [インポート] を選択します。
6. [ソース] には、インポートするオブジェクトを含む汎用バケット (またはプレフィックスを含むバケットパス) を入力します。リストから既存の汎用バケットを選択するには、[Browse S3] をクリックします。
7. [アクセス許可] セクションで、IAM ロールの自動生成を選択できます。または、リストから IAM ロールを選択するか、IAM ロール ARN を直接入力することもできます。

- Amazon S3 がユーザーに代わって新しい IAM ロールを作成できるようにするには、[新しい IAM ロールを作成] を選択します。

  > **Note**
  >
  > ソースオブジェクトが AWS Key Management Service (AWS KMS) キーを使用したサーバー側の暗号化 (SSE-KMS) で暗号化されている場合は、[新しい IAM ロールを作成] オプションは選択せず、その代わりに、`kms:Decrypt` アクセス許可を持つ既存の IAM ロールを指定します。
  > Amazon S3 は、このアクセス許可を使用してオブジェクトを復号化します。インポート処理中、Amazon S3 は Amazon S3 マネージドキー (SSE-S3) を使用してサーバー側の暗号化 (SSE-S3) でこれらのオブジェクトを再暗号化します。

- リストから既存の IAM ロールを選択するには、[既存の IAM ロールから選択] をクリックします。
- Amazon リソースネーム (ARN) を入力して既存の IAM ロールを指定するには、[IAM ロールの ARN の入力] をクリックして、対応するフィールドに ARN を入力します。

8. [送信先] セクションと [コピーされたオブジェクトの設定] セクションに表示された情報を確認します。[送信先] セクションの情報が適切であれば、[インポート] をクリックしてコピージョブを開始します。

   Amazon S3 コンソールでは、新しいジョブのステータスが [バッチオペレーション] ページに表示されます。ジョブの詳細については、ジョブ名の横にあるオプションボタンを選択して、[アクション] メニューで [詳細を表示] を選択します。オブジェクトのインポート先となるディレクトリバケットを開くには、[インポート先を表示] を選択します。

ステップ 4: オブジェクトを S3 Express One Zone ディレクトリバケットに手動でアップロードする

ディレクトリバケットにオブジェクトを手動でアップロードすることもできます。

オブジェクトを手動でアップロードするには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ページ右上隅にあるナビゲーションバーで、現在表示されている AWS リージョンの名前をクリックします。次に、ディレクトリバケットがあるアベイラビリティーゾーンに関連付けられたリージョンを選択します。

3. 左のナビゲーションペインで、[ディレクトリバケット] を選択します。
4. フォルダまたはファイルをアップロードするバケットの名前を選択します。

> **Note**
>
> このチュートリアルの前のステップで使用したものと同じディレクトリバケットを選択した場合、ディレクトリバケットにはインポートツールでアップロードされたオブジェクトが追加されます。これらのオブジェクトは現在 S3 Express One Zone ストレージクラスに保存されていることに注意してください。

5. [オブジェクト] タブで、[アップロード] を選択します。
6. [アップロード] ページで、以下のいずれかを行います。
   - ファイルとフォルダを点線で示されているアップロードエリアにドラッグアンドドロップします。
   - [ファイルの追加] または [フォルダの追加] を選択し、アップロードするファイルまたはフォルダを選択して [開く] または [アップロード] を選択します。
7. [チェックサム] で、使用する [チェックサム関数] を選択します。

> **Note**
>
> S3 Express One Zone ストレージクラスで最高のパフォーマンスを実現するには、CRC32 と CRC32C を使用することをお勧めします。詳細については、「S3 の追加のチェックサムのベストプラクティス」を参照してください。

   (オプション) サイズが 16 MB 未満の単一のオブジェクトをアップロードする場合は、事前に計算されたチェックサム値を指定することもできます。事前に計算された値を指定すると、Amazon S3 は選択したチェックサム関数を使用して計算した値と比較します。値が一致しない場合、アップロードは開始されません。
8. [アクセス許可] と [プロパティ] セクションのオプションは、自動的にデフォルトに設定され、変更できません。ブロックパブリックアクセスは自動的に有効になり、ディレクトリバケットに対して S3 バージョニングと S3 Object Lock を有効にすることはできません。

   (オプション) オブジェクトにキーと値のペアのメタデータを追加する場合は、[プロパティ] セクションを展開し、[メタデータ]セクションで [メタデータを追加]を選択します。
9. リストされたファイルとフォルダをアップロードするには、[アップロード] を選択します。

Amazon S3 はオブジェクトとフォルダをアップロードします。アップロードが完了すると、[アップロード: ステータス] ページに成功のメッセージが表示されます。

ディレクトリバケットが正常に作成され、オブジェクトがバケットにアップロードされました。

ステップ 5: S3 Express One Zone ディレクトリバケットを空にする

Amazon S3 コンソールを使用して Amazon S3 ディレクトリバケットを空にできます。

ディレクトリバケットを空にするには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ページ右上隅にあるナビゲーションバーで、現在表示されている AWS リージョンの名前をクリックします。次に、ディレクトリバケットがあるアベイラビリティーゾーンに関連付けられたリージョンを選択します。
3. 左のナビゲーションペインで、[ディレクトリバケット] を選択します。
4. 空にするバケットの名前の横にあるオプションボタンを選択し、[空にする] を選択します。
5. [バケットを空にする] ページで、テキストフィールドに **`permanently delete`** を入力することでバケットを空にすることを確定し、[空にする] を選択します。
6. [バケットを空にする: ステータス] ページで、バケットを空にするプロセスの進行状況をモニタリングします。

ステップ 6: S3 Express One Zone ディレクトリバケットを削除する

ディレクトリバケットを空にして進行中のすべてのマルチパートアップロードを中止したら、Amazon S3 コンソールを使用してバケットを削除できます。

ディレクトリバケットを削除するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ページ右上隅にあるナビゲーションバーで、現在表示されている AWS リージョンの名前をクリックします。次に、ディレクトリバケットがあるアベイラビリティーゾーンに関連付けられたリージョンを選択します。
3. 左のナビゲーションペインで、[ディレクトリバケット] を選択します。

4. [ディレクトリバケット] リストで、削除するバケット名の横にあるオプションボタンを選択します。
5. [削除] を選択します。
6. [バケットの削除] ページで、テキストフィールドにバケット名を入力して、バケットの削除を確定します。

> **Important**
>
> ディレクトリバケットを削除すると、元に戻すことはできません。

7. バケットを削除するには、[バケットの削除] をクリックします。

次のステップ

このチュートリアルでは、ディレクトリバケットを作成して、S3 Express One Zone ストレージクラスを使用する方法を学習しました。このチュートリアルを完了すると、S3 Express One Zone ストレージクラスで使用できる関連 AWS サービスについて確認できます。

S3 Express One Zone AWS のサービス ストレージクラスで次を使用して、特定の低レイテンシーのユースケースをサポートできます。

- Amazon Elastic Compute Cloud (Amazon EC2) – Amazon EC2 は、安全でスケーラブルなコンピューティング容量を AWS クラウド で提供します。Amazon EC2 の使用により、ハードウェアに事前投資する必要がなくなり、アプリケーションをより速く開発およびデプロイできます。Amazon EC2 を使用すると、必要な数 (またはそれ以下) の仮想サーバーの起動、セキュリティおよびネットワーキングの構成、ストレージの管理ができます。
- AWS Lambda – Lambda はサーバーのプロビジョニングや管理を必要とせずにコードを実行できるコンピューティングサービスです。バケットの通知設定を構成し、関数のリソースベースのアクセス許可ポリシーで関数を呼び出すためのアクセス許可を Amazon S3 に付与します。
- Amazon Elastic Kubernetes Service (Amazon EKS) は、AWS 上で、独自の Kubernetes コントロールプレーンをインストール、運用、保守する必要がないマネージド型サービスです。Kubernetes は、コンテナ化されたアプリケーションの管理、スケーリング、デプロイを自動化するオープンソースシステムです。
- Amazon Elastic Container Service (Amazon ECS) – Amazon ECS は、コンテナ化されたアプリケーションを簡単にデプロイ、管理、スケーリングできる、フルマネージドコンテナオーケストレーションサービスです。

- Amazon EMR – Amazon EMR は、Apache Hadoop や Apache Spark などのビッグデータフレームワークを AWS で簡単に実行して、膨大な量のデータを処理および分析できるマネージドクラスタープラットフォームです。
- Amazon Athena – Athena はインタラクティブなクエリサービスで、Amazon S3 内のデータを標準 SQL を使用して直接的に簡単に分析できます。また、Athena を使用すると、リソースの計画、設定、管理を必要とせずに Apache Spark を使用してデータ分析をインタラクティブに実行することもできます。Athena で Apache Spark アプリケーションを実行する場合は、処理用の Spark コードを送信して、結果を直接受け取ります。
- AWS Glue データカタログ – AWS Glue は、分析を行うユーザーが複数のソースからのデータを簡単に検出、準備、移動、統合できるようにするサーバーレスのデータ統合サービスです。AWS Glue は分析、機械学習、アプリケーション開発に使用できます。AWSGlue データカタログ は、組織のデータセットに関するメタデータを保存する一元化されたリポジトリです。データソースの場所、スキーマ、およびランタイムメトリクスへのインデックスとして機能します。
- Amazon SageMaker Runtime Model Training – Amazon SageMaker Runtime は、フルマネージド型の機械学習サービスです。SageMaker Runtime では、データサイエンティストやデベロッパーが迅速かつ簡単に機械学習モデルの構築とトレーニングを行うことができ、それらを稼働準備が整ったホストされている環境に直接デプロイできます。

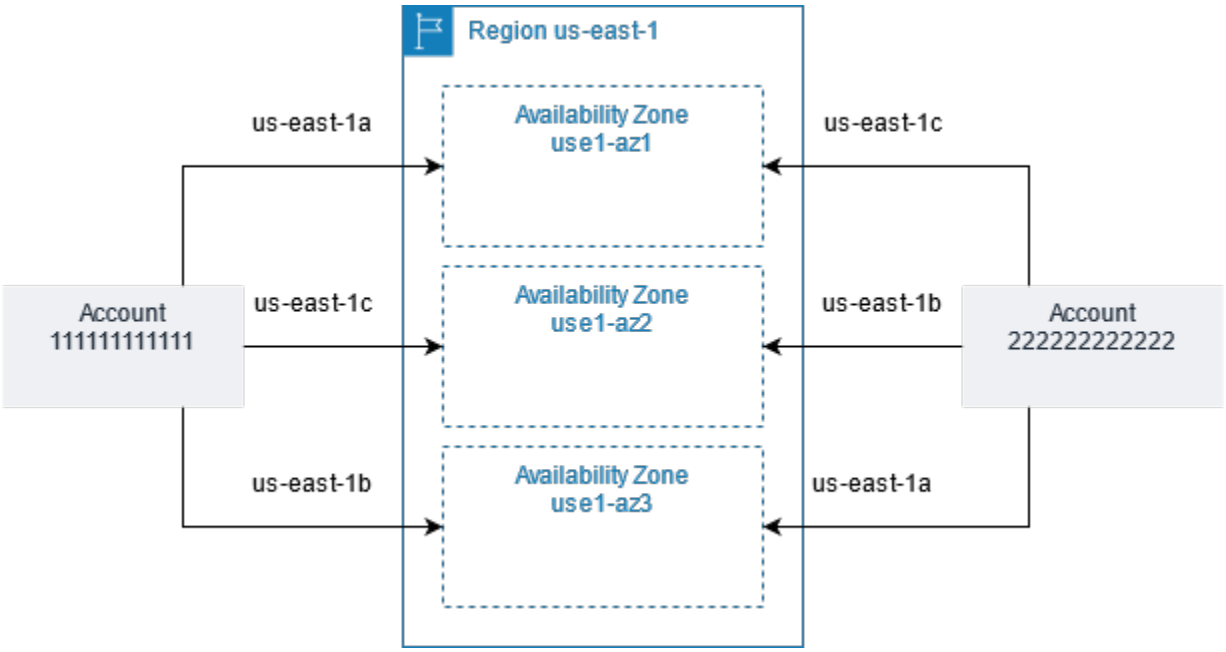
S3 Express One Zone の詳細については、「S3 Express One Zone とは」および「S3 Express One Zone の違いとは」を参照してください。

S3 Express One Zone のアベイラビリティーゾーンとリージョン

アベイラビリティーゾーンは、AWS リージョン の冗長電源、ネットワーク、および接続を備えた 1 つ以上の個別のデータセンターです。低レイテンシーでの取り出しを最適化するために、Amazon S3 Express One Zone ストレージクラスのオブジェクトは、コンピューティングワークロードにローカルにある単一のアベイラビリティーゾーンの S3 ディレクトリバケットに冗長的に保存されます。ディレクトリバケットを作成する際は、バケットの配置場所であるアベイラビリティーゾーンと AWS リージョン を選択します。

AWS は、物理的なアベイラビリティーゾーンを AWS アカウント ごとのアベイラビリティーゾーン名にランダムにマップします。この方法は、各リージョンの最初のアベイラビリティーゾーンにリソースが集中するのではなく、AWS リージョン 内のアベイラビリティーゾーン全体にリソースを分散するのに役立ちます。その結果、AWS アカウント のアベイラビリティーゾーン `us-east-1a` は、別の AWS アカウント の `us-east-1a` と同じ物理的な場所を示さない可能性があります。詳細については、Amazon EC2 ユーザーガイドの「リージョンとアベイラビリティゾーン」を参照してください。

アカウント間でアベイラビリティーゾーンを調整するには、アベイラビリティーゾーンの一意で一貫性のある識別子である AZ ID を使用する必要があります。例えば、`use1-az1` は、`us-east-1` リージョンの AZ ID で、すべての AWS アカウント で同じ物理的な場所になります。次の図は、アベイラビリティーゾーン名がアカウントごとに異なるようにマップされている場合でも、AZ ID がすべてのアカウントで同じであるかどうかを説明しています。



S3 Express One Zone では、データは単一のアベイラビリティーゾーン内で冗長的に複数のデバイスに保存されます。S3 Express One Zone は、単一のアベイラビリティーゾーン内で 99.95% の可用性を実現するように設計されており、Amazon S3 サービスレベル契約に基づいています。詳細については、アベイラビリティーゾーンを参照してください。

次の表は、S3 Express One Zone がサポートするリージョンとアベイラビリティゾーンを示しています。

リージョン名	リージョンコード	アベイラビリティーゾーン ID				
米国東部 (バージニア北部)	`us-east-1`	`use1-az4`				
		`use1-az5`				
		`use1-az6`				

リージョン名	リージョンコード	アベイラビリティーゾーン ID
米国東部 (オハイオ)	us-east-2	use2-az1
		use2-az2
米国西部 (オレゴン)	us-west-2	usw2-az1
		usw2-az3
		usw2-az4
アジアパシフィック (ムンバイ)	ap-south-1	aps1-az1
		aps1-az3
アジアパシフィック (東京)	ap-northeast-1	apne1-az1
		apne1-az4
欧州 (アイルランド)	eu-west-1	euw1-az1
		euw1-az3
欧州 (ストックホルム)	eu-north-1	eun1-az1
		eun1-az2
		eun1-az3

アベイラビリティーゾーンのディレクトリバケットのネットワーク

次のトピックでは、ゲートウェイ VPC エンドポイントを使用して S3 Express One Zone にアクセスするためのネットワーク要件について説明します。

トピック

- アベイラビリティーゾーンのディレクトリバケットのエンドポイント
- VPC ゲートウェイエンドポイントの設定

アベイラビリティーゾーンのディレクトリバケットのエンドポイント

各リージョンとアベイラビリティーゾーンで使用できるリージョン API エンドポイントとゾーン API エンドポイントは、次の表のとおりです。

VPC ゲートウェイエンドポイントの設定

次の手順を使用して、Amazon S3 Express One Zone ストレージクラスのオブジェクトとディレクトリバケットに接続するゲートウェイエンドポイントを作成します。

ゲートウェイ VPC エンドポイントを設定するには

1. Amazon VPC コンソールを開きます。
2. ナビゲーションペインで、[エンドポイント] を選択します。
3. [エンドポイントの作成] を選択します。
4. エンドポイントの名前を作成します。
5. [Service category] (サービスカテゴリ) で、AWS のサービス を選択します。
6. [サービス] では、[Type=Gateway] フィルターを追加して、com.amazonaws.***region***.s3express の隣にあるボタンをクリックします。
7. [VPC] で、エンドポイントを作成する VPC を選択します。
8. [Route tables] (ルートテーブル) で、エンドポイントで使用するルートテーブルを選択します。Amazon VPC は、サービスに送信するトラフィックをエンドポイントネットワークインターフェイスにポイントするルートを自動的に追加します。
9. [ポリシー] では、[フルアクセス] を選択して、VPC エンドポイントのすべてのリソースに対するすべてのプリンシパルによるすべてのオペレーションを許可します。それ以外の場合は、[カスタム] を選択して、プリンシパルが VPC エンドポイントを介してリソースに対してアクションを実行するために必要なアクセス許可を制御する VPC エンドポイントポリシーをアタッチします。
10. (オプション) タグを追加するには、[新しいタグを追加] をクリックして、タグのキーバリューを入力します。
11. [エンドポイントの作成] を選択します。

ゲートウェイエンドポイントを作成した後、リージョン API エンドポイントとゾーン API エンドポイントを使用して、Amazon S3 Express One Zone ストレージクラスのオブジェクトとディレクトリバケットにアクセスできます。

アベイラビリティーゾーンでのディレクトリバケットの作成

Amazon S3 Express One Zone ストレージクラスの使用を開始するには、ディレクトリバケットを使用する必要があります。S3 Express One Zone ストレージクラスを使用するには、ディレクトリバケットを使用する必要があります。S3 Express One Zone ストレージ クラスは、低レイテンシーのユースケースをサポートし、単一のアベイラビリティーゾーン内でより高速なデータ処理を提供します。アプリケーションのパフォーマンスが重視され、1 桁のミリ秒単位の PUT と GET のレイテンシーでの利点が得られる場合は、S3 Express One Zone ストレージクラスを使用できるようにディレクトリバケットを作成することをお勧めします。

Amazon S3 バケットには、汎用バケットとディレクトリバケットの 2 種類があります。アプリケーションとパフォーマンス要件に最適なバケットタイプを選択する必要があります。汎用バケットはオリジナルの S3 バケットタイプです。汎用バケットはほとんどのユースケースとアクセスパターンに推奨されます。S3 Express One Zone を除くすべてのストレージクラスにわたってオブジェクトを保存できます。汎用バケットの詳細については、「汎用バケットの概要」を参照してください。

ディレクトリバケットは、S3 Express One Zone ストレージクラスを使用します。これは、一貫して 1 桁ミリ秒のレイテンシーに維持する必要があるワークロードまたはパフォーマンス重視のアプリケーション向けに設計されています。S3 Express One Zone は、オブジェクトストレージをコンピューティングリソースと同じ場所に配置するオプションを提供し、単一のアベイラビリティーゾーンを選択できる最初の S3 ストレージクラスです。これにより、アクセス速度が最大限に高速化します。ディレクトリバケットを作成する場合、必要に応じて Amazon EC2、Amazon Elastic Kubernetes Service、または Amazon Elastic Container Service (Amazon ECS) コンピュートインスタンスのローカルにある AWS リージョン とアベイラビリティーゾーンを指定して、パフォーマンスを最適化できます。

S3 Express One Zone では、データは単一のアベイラビリティーゾーン内で冗長的に複数のデバイスに保存されます。S3 Express One Zone は、単一のアベイラビリティーゾーン内で 99.95% の可用性を実現するように設計されており、Amazon S3 サービスレベル契約に基づいています。詳細については、アベイラビリティーゾーンを参照してください。

ディレクトリバケットは、汎用バケットのフラットなストレージ構造とは対照的に、データを階層的にディレクトリにまとめます。ディレクトリバケットにはプレフィックスの制限はなく、個々のディレクトリは水平方向にスケールできます。

汎用バケットの詳細については、「ディレクトリバケットの使用」を参照してください。

ディレクトリバケット名

ディレクトリバケット名は次の形式を使用し、ディレクトリバケットの命名規則に従う必要があります。

```
bucket-base-name--zone-id--x-s3
```

例えば、次のディレクトリバケット名にはアベイラビリティーゾーン ID usw2-az1 が含まれています。

```
bucket-base-name--usw2-az1--x-s3
```

ディレクトリバケットの命名規則の詳細については、「ディレクトリバケットの命名規則」を参照してください。

S3 コンソールの使用

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. ページ上部にあるナビゲーションバーで、現在表示されている AWS リージョン の名前をクリックします。次に、バケットを作成するリージョンを選択します。

   > **Note**
   >
   > レイテンシーとコストを最小化するため、さらに規制条件に対応するために、最寄りのリージョンを選択します。明示的に別のリージョンに移動する場合を除き、特定のリージョンに保管されたオブジェクトは、そのリージョンから移動されることはありません。Amazon S3 AWS リージョン のリストについては、「Amazon Web Services 全般のリファレンス」の「AWS のサービス エンドポイント」を参照してください。

3. 左のナビゲーションペインで、[ディレクトリバケット] を選択します。
4. [Create bucket (バケットの作成)] を選択します。[バケットの作成] ページが開きます。
5. [全般設定] で、バケットが作成される AWS リージョン を確認します。

   [バケットタイプ] で [ディレクトリ] を選択します。

   > **Note**
   >
   > - ディレクトリバケットをサポートしていないリージョンを選択した場合、[バケットタイプ] オプションは表示されなくなり、バケットタイプはデフォルトで汎用バケッ

トになります。ディレクトリバケットを作成するには、サポートされているリージョンを選択する必要があります。ディレクトリバケットと Amazon S3 Express One Zone ストレージクラスをサポートするリージョンのリストについては、「the section called “S3 Express One Zone のアベイラビリティーゾーンとリージョン”」を参照してください。

- バケット作成後にバケットタイプは変更できません。

> **Note**
>
> このアベイラビリティーゾーンは、バケットの作成後に変更することはできません。

6. [アベイラビリティーゾーン] では、コンピューティングサービスにローカルなアベイラビリティーゾーンを選択します。ディレクトリバケットと S3 Express One Zone ストレージクラスをサポートするアベイラビリティーゾーンのリストについては、「the section called “S3 Express One Zone のアベイラビリティーゾーンとリージョン”」を参照してください。

   [アベイラビリティーゾーン] でチェックボックスをオンにして、アベイラビリティーゾーンに障害が発生した場合に、データが使用できなくなったり、データが失われたりする場合があることに同意します。

> **Important**
>
> ディレクトリバケットは、単一のアベイラビリティーゾーン内の複数のデバイスに保存されますが、ディレクトリバケットはアベイラビリティーゾーン間でデータを冗長に保存することはありません。

7. [バケット名] には、ディレクトリバケット名を入力します。

   ディレクトリバケットの命名には、次のルールが適用されます。

   - 選択したゾーン (AWS アベイラビリティーゾーンまたは AWS Local Zone) 内で一意である必要があります。
   - 名前は、サフィックスを含め 3 文字 (最短) から 63 文字 (最長) の長さでなければなりません。
   - 小文字の英文字、数字、およびハイフン (-) で構成されていること。
   - 文字や数字で始まり、文字や数字で終わります。

- *--zone-id*--x-s3 のサフィックスを含める必要があります。
- バケット名のプレフィックスは xn-- で始まってはいけません。
- バケット名のプレフィックスは sthree- で始まってはいけません。
- バケット名のプレフィックスは sthree-configurator で始まってはいけません。
- バケット名のプレフィックスは amzn-s3-demo- で始まってはいけません。
- バケット名のサフィックスは -s3alias で終わってはいけません。このサフィックスは、アクセスポイントのエイリアス名用に予約されています。詳細については、「汎用バケットのアクセスポイントのエイリアス」を参照してください。
- バケット名のサフィックスは --ol-s3 で終わってはいけません。このサフィックスは、Object Lambda アクセスポイントのエイリアス名用に予約されています。詳細については、「S3 バケット Object Lambda アクセスポイントでのバケット形式のエイリアスの使用方法」を参照してください。
- バケット名のサフィックスは .mrap で終わってはいけません。このサフィックスは、マルチリージョンアクセスポイント名用に予約されています。詳細については、「Amazon S3 マルチリージョンアクセスポイントの命名規則」を参照してください。

コンソールを使用してディレクトリバケットを作成すると、指定したベース名にサフィックスが自動的に追加されます。このサフィックスには、選択したアベイラビリティーゾーンのアベイラビリティーゾーン ID が含まれます。

バケットを作成したら、その名前を変更することはできません。バケットの命名の詳細については、「汎用バケットの命名規則」を参照してください。

> **Important**
>
> バケット名にアカウント番号などの機密情報を含めないでください。バケット名は、バケット内のオブジェクトを参照する URL に表示されます。

8. [オブジェクト所有者] で、[バケット所有者の強制] の設定が自動的に有効になり、アクセスコントロールリスト (ACL) が無効になります。ディレクトリバケットの場合、ACL は有効にできません。

   バケット所有者の強制 (デフォルト) – ACL は無効になり、バケット所有者は汎用バケット内のすべてのオブジェクトを自動的に所有し、完全に制御します。ACL は、S3 汎用バケット内のデータへのアクセス許可に影響を与えなくなりました。このバケットはアクセスコントロールを定義するためだけにポリシーを使用します。

9. [このバケットのブロックパブリックアクセス設定] で、ディレクトリバケットのパブリックアクセスブロック設定がすべて自動的に有効になります。ディレクトリバケットの場合、この設定は変更できません。ブロックパブリックアクセスの詳細については、Amazon S3 ストレージへのパブリックアクセスのブロック を参照してください。
10. デフォルトの暗号化を設定するには、[暗号化タイプ] で次のいずれかを選択します。

    - [Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3)]
    - [AWS Key Management Service キーによるサーバー側の暗号化 (SSE-KMS)]

    Amazon S3 のサーバー側の暗号化を使用してデータを暗号化する方法の詳細については、「データ保護と暗号化」を参照してください。

    > **Important**
    >
    > デフォルト暗号化設定に SSE-KMS オプションを使用する場合、AWS KMS の 1 秒あたりのリクエスト (RPS) 制限が適用されます。AWS KMS クォータの詳細およびクォータの引き上げをリクエストする方法については、「AWS Key Management Service デベロッパーガイド」の「クォータ」を参照してください。
    > デフォルト暗号化を有効にする際、バケットポリシーの更新が必要な場合があります。詳細については、「クロスアカウント操作での SSE-KMS 暗号化の使用」を参照してください。

11. [Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3)] を選択した場合は、[バケットキー] の下に [有効] が表示されます。ディレクトリバケットが SSE-S3 でデフォルトの暗号化を使用するように設定すると、S3 バケットキーは常に有効になります。S3 バケットキーは、ディレクトリバケット内の GET および PUT オペレーションで常に有効になっており、無効にすることはできません。SSE-KMS で暗号化されたオブジェクトを、CopyObject、UploadPartCopy、バッチオペレーションの Copy オペレーション、または import ジョブを使用して、汎用バケットからディレクトリバケットへ、ディレクトリバケットから汎用バケットへ、またはディレクトリバケット間でコピーする場合、S3 バケットキーはサポートされません。この場合、KMS で暗号化されたオブジェクトのコピーリクエストが実行されるたびに、Amazon S3 は AWS KMS を呼び出します。

    S3 バケットキーは、Amazon S3 から AWS KMS へのリクエストトラフィックを減らし、暗号化のコストを削減します。詳細については、「Amazon S3 バケットキーを使用した SSE-KMS のコストの削減」を参照してください。

12. [AWS Key Management Service キーによるサーバー側の暗号化 (SSE-KMS)] を選択した場合は、[AWS KMS キー] で次のいずれかの方法で AWS Key Management Service キーを指定するか、新しいキーを作成します。

    - 使用可能な KMS キーのリストから選択するには、[AWS KMS keys から選択する] を選択し、[使用可能な AWS KMS keys] のリストから自分の [KMS キー] を選択します。

      カスタマーマネージドキーのみがこのリストに表示されます。AWS マネージドキー (aws/s3) はディレクトリバケットではサポートされていません。カスタマーマネージドキーの詳細については、AWS Key Management Serviceデベロッパーガイドの「カスタマーキーと AWS キー」を参照してください。
    - KMS キーの ARN またはエイリアスを入力するには、[AWS KMS key ARN を入力] を選択し、[AWS KMS key ARN] に KMS キーの ARN またはエイリアスを入力します。
    - AWS KMS コンソールで新しいカスタマーマネージドキーを作成するには、[KMS キーを作成] を選択します。

      AWS KMS key の作成の詳細については、「AWS Key Management Service デベロッパーガイド」の「キーの作成」を参照してください。

    > **Important**
    >
    > - SSE-KMS 設定では、バケットの存続期間中、ディレクトリバケットごとに 1 つのカスタマーマネージドキーしかサポートできません。AWS マネージドキー (aws/s3) はサポートされていません。また、SSE-KMS のカスタマーマネージドキーを指定した後は、バケットの SSE-KMS 設定のカスタマーマネージドキーを上書きすることはできません。
    >
    >   バケットの SSE-KMS 設定に指定したカスタマーマネージドキーは、次のように識別できます。
    >
    >   - `HeadObject` API オペレーションリクエストを実行して、レスポンス内の `x-amz-server-side-encryption-aws-kms-key-id` の値を検索します。
    >
    >   データに新しいカスタマーマネージドキーを使用するには、新しいカスタマーマネージドキーを使用して既存のオブジェクトを新しいディレクトリバケットにコピーすることをお勧めします。
    > - バケットと同じ AWS リージョン で使用可能な KMS キーのみを使用できます。Amazon S3 コンソールには、バケットと同じリージョンで最初の 100 個の KMS

キーしか表示されません。リストに存在しない KMS キーを使用するには、KMS キー ARN を入力する必要があります。別のアカウントが所有している KMS キーを使用する場合は、まずそのキーを使用するアクセス許可が必要であり、次に KMS キー ARN を入力する必要があります。KMS キーのクロスアカウント権限の詳細については、AWS Key Management Service デベロッパーガイドの「他のアカウントで使用できる KMS キーを作成する」を参照してください。SSE-KMS に関する詳細は、「ディレクトリバケット内の新しいオブジェクトのアップロードに AWS KMS によるサーバー側の暗号化 (SSE-KMS) を指定する」を参照してください。

- ディレクトリバケットでサーバー側の暗号化に AWS KMS key を使用する場合は、対称暗号化 KMS キーを選択する必要があります。Amazon S3 では、対称暗号化 KMS キーのみがサポートされ、非対称暗号化 KMS キーはサポートされません。詳細については、AWS Key Management Service デベロッパーガイドの「Identifying symmetric and asymmetric KMS keys」(対称および非対称 KMS キーの識別) を参照してください。

Amazon S3 での AWS KMS の使用に関する詳細は、「ディレクトリバケットでの AWS KMS キーによるサーバー側の暗号化 (SSE-KMS) の使用」を参照してください。

13. [バケットを作成] を選択します。バケットを作成したら、ファイルやフォルダをバケットに追加できます。詳細については、「the section called “ディレクトリバケットでのオブジェクトの使用”」を参照してください。

AWS SDK の使用

SDK for Go

AWS SDK for Go を使用してディレクトリバケットを作成する方法は、次の例のとおりです。

Example

```
var bucket = "..."

func runCreateBucket(c *s3.Client) {
    resp, err := c.CreateBucket(context.Background(), &s3.CreateBucketInput{
        Bucket: &bucket,
        CreateBucketConfiguration: &types.CreateBucketConfiguration{
            Location: &types.LocationInfo{
                Name: aws.String("usw2-az1"),
                Type: types.LocationTypeAvailabilityZone,
```

```
            },
            Bucket: &types.BucketInfo{
                DataRedundancy: types.DataRedundancySingleAvailabilityZone,
                Type:           types.BucketTypeDirectory,
            },
        },
    })
    var terr *types.BucketAlreadyOwnedByYou
    if errors.As(err, &terr) {
        fmt.Printf("BucketAlreadyOwnedByYou: %s\n", aws.ToString(terr.Message))
        fmt.Printf("noop...\n")
        return
    }
    if err != nil {
        log.Fatal(err)
    }

    fmt.Printf("bucket created at %s\n", aws.ToString(resp.Location))
}
```

SDK for Java 2.x

AWS SDK for Java 2.x を使用してディレクトリバケットを作成する方法は、次の例のとおりです。

Example

```
public static void createBucket(S3Client s3Client, String bucketName) {

    //Bucket name format is {base-bucket-name}--{az-id}--x-s3
    //example: doc-example-bucket--usw2-az1--x-s3 is a valid name for a directory
 bucket created in
    //Region us-west-2, Availability Zone 2

    CreateBucketConfiguration bucketConfiguration =
 CreateBucketConfiguration.builder()
             .location(LocationInfo.builder()
                     .type(LocationType.AVAILABILITY_ZONE)
                     .name("usw2-az1").build()) //this must match the Region and
 Availability Zone in your bucket name
             .bucket(BucketInfo.builder()
                    .type(BucketType.DIRECTORY)
                    .dataRedundancy(DataRedundancy.SINGLE_AVAILABILITY_ZONE)
```

```
                    .build()).build();
    try {

             CreateBucketRequest bucketRequest =
 CreateBucketRequest.builder().bucket(bucketName).createBucketConfiguration(bucketConfigurat
             CreateBucketResponse response = s3Client.createBucket(bucketRequest);
             System.out.println(response);
    }

    catch (S3Exception e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
         }
    }
```

AWS SDK for JavaScript

AWS SDK for JavaScript を使用してディレクトリバケットを作成する方法は、次の例のとおりです。

Example

```
// file.mjs, run with Node.js v16 or higher
// To use with the preview build, place this in a folder
// inside the preview build directory, such as /aws-sdk-js-v3/workspace/

import { S3 } from "@aws-sdk/client-s3";

const region = "us-east-1";
const zone = "use1-az4";
const suffix = `${zone}--x-s3`;

const s3 = new S3({ region });

const bucketName = `...--${suffix}`;

const createResponse = await s3.createBucket(
    { Bucket: bucketName,
      CreateBucketConfiguration: {Location: {Type: "AvailabilityZone", Name: zone},
      Bucket: { Type: "Directory", DataRedundancy: "SingleAvailabilityZone" }}
    }
```

```
    );
```

SDK for .NET

SDK for .NET を使用してディレクトリバケットを作成する方法は、次の例のとおりです。

Example

```
using (var amazonS3Client = new AmazonS3Client())
{
    var putBucketResponse = await amazonS3Client.PutBucketAsync(new PutBucketRequest
    {

       BucketName = "DOC-EXAMPLE-BUCKET--usw2-az1--x-s3",
       PutBucketConfiguration = new PutBucketConfiguration
       {
         BucketInfo = new BucketInfo { DataRedundancy =
 DataRedundancy.SingleAvailabilityZone, Type = BucketType.Directory },
         Location = new LocationInfo { Name = "usw2-az1", Type =
 LocationType.AvailabilityZone }
       }
     }).ConfigureAwait(false);
}
```

SDK for PHP

AWS SDK for PHP を使用してディレクトリバケットを作成する方法は、次の例のとおりです。

Example

```
require 'vendor/autoload.php';

$s3Client = new S3Client([

    'region'      => 'us-east-1',
]);


$result = $s3Client->createBucket([
    'Bucket' => 'doc-example-bucket--use1-az4--x-s3',
    'CreateBucketConfiguration' => [
        'Location' => ['Name'=> 'use1-az4', 'Type'=> 'AvailabilityZone'],
```

```
        'Bucket' => ["DataRedundancy" => "SingleAvailabilityZone" ,"Type" =>
 "Directory"]   ],
]);
```

SDK for Python

AWS SDK for Python (Boto3) を使用してディレクトリバケットを作成する方法は、次の例のとおりです。

Example

```
import logging
import boto3
from botocore.exceptions import ClientError

def create_bucket(s3_client, bucket_name, availability_zone):
    '''
    Create a directory bucket in a specified Availability Zone

    :param s3_client: boto3 S3 client
    :param bucket_name: Bucket to create; for example, 'doc-example-bucket--usw2-
az1--x-s3'
    :param availability_zone: String; Availability Zone ID to create the bucket in,
 for example, 'usw2-az1'
    :return: True if bucket is created, else False
    '''

    try:
        bucket_config = {
                'Location': {
                    'Type': 'AvailabilityZone',
                    'Name': availability_zone
                },
                'Bucket': {
                    'Type': 'Directory',
                    'DataRedundancy': 'SingleAvailabilityZone'
                }
            }
        s3_client.create_bucket(
            Bucket = bucket_name,
            CreateBucketConfiguration = bucket_config
        )
    except ClientError as e:
```

```
            logging.error(e)
            return False
    return True


if __name__ == '__main__':
    bucket_name = 'BUCKET_NAME'
    region = 'us-west-2'
    availability_zone = 'usw2-az1'
    s3_client = boto3.client('s3', region_name = region)
    create_bucket(s3_client, bucket_name, availability_zone)
```

SDK for Ruby

AWS SDK for Ruby を使用してディレクトリバケットを作成する方法は、次の例のとおりです。

Example

```
s3 = Aws::S3::Client.new(region:'us-west-2')
s3.create_bucket(
  bucket: "bucket_base_name--az_id--x-s3",
  create_bucket_configuration: {
    location: { name: 'usw2-az1', type: 'AvailabilityZone' },
    bucket: { data_redundancy: 'SingleAvailabilityZone', type: 'Directory' }
  }
)
```

AWS CLI を使用する場合

AWS CLI を使用してディレクトリバケットを作成する方法は、次の例のとおりです。このコマンドを使用する際は、*###############*を独自の情報に置き換えます。

ディレクトリバケットを作成する際は、設定の詳細を指定して、*bucket-base-name*--*zone-id*--x-s3 の命名規則を使用する必要があります。

```
aws s3api create-bucket
--bucket bucket-base-name--zone-id--x-s3
--create-bucket-configuration 'Location={Type=AvailabilityZone,Name=usw2-
az1},Bucket={DataRedundancy=SingleAvailabilityZone,Type=Directory}'
--region us-west-2
```

詳細については、「AWS Command Line Interface」の「create-bucket」を参照してください。

アベイラビリティーゾーン内のディレクトリバケット用のリージョンエンドポイントとゾーンエンドポイント

S3 Express One Zone に保存したオブジェクトやディレクトリバケットにアクセスするには、ゲートウェイ VPC エンドポイントを使用します。ディレクトリバケットでは、リージョン API エンドポイントとゾーン API エンドポイントを使用します。使用する Amazon S3 API オペレーションに応じて、リージョンゾーンエンドポイントまたはゾーンエンドポイントのいずれかが必要です。ゲートウェイエンドポイントは追加料金なしで使用できます。

バケットレベル (またはコントロールプレーン) API オペレーションは、リージョンエンドポイントを通じて利用でき、リージョンエンドポイント API オペレーションと呼ばれます。リージョンエンドポイント API オペレーションの例には、`CreateBucket`、`DeleteBucket` があります。

S3 Express One Zone に保存するディレクトリバケットを作成する場合は、バケットを配置する先のアベイラビリティーゾーンを選択します。ディレクトリバケットにオブジェクトをアップロードして管理するには、ゾーンエンドポイント API オペレーションを使用できます。

オブジェクトレベル (またはデータプレーン) の API オペレーションは、ゾーンエンドポイントを通じて利用でき、ゾーンエンドポイント API オペレーションと呼ばれます。ゾーン別エンドポイント API オペレーションの例には、`CreateSession`、`PutObject` があります。

S3 Express One Zone のパフォーマンスの最適化

Amazon S3 Express One Zone は、最もレイテンシーに敏感なアプリケーションに一貫した 1 桁ミリ秒のデータアクセスを提供することを目的として設計された、高パフォーマンスの単一アベイラビリティーゾーン (AZ) S3 ストレージクラスです。S3 Express One Zone は、単一のアベイラビリティーゾーン内で、Amazon Elastic Compute Cloud、Amazon Elastic Kubernetes Service、Amazon Elastic Container Service などの高パフォーマンスオブジェクトストレージと AWS コンピューティングリソースを同じロケーションに配置するオプションを提供する最初の S3 ストレージクラスです。ストレージとコンピューティングリソースを同じロケーションに配置すると、コンピューティングパフォーマンスとコストが最適化され、データ処理速度が向上します。

S3 Express One Zone は、その他の S3 ストレージ クラスと同様のパフォーマンスの伸縮性を提供します。ただし、最初のバイトの読み取りと書き込みのリクエストのレイテンシは一貫して 1 桁ミリ秒で、S3 Standard よりも最大 10 倍高速です。S3 Express One Zone は、非常に高い集約レベルまでのバーストスループットをサポートするようにゼロから設計されています。S3 Express One Zone ストレージ クラスは、カスタム構築されたアーキテクチャを使用してパフォーマンスを最適化

し、高パフォーマンスハードウェアにデータを保存することで一貫して低いリクエストレイテンシーを実現します。S3 Express One Zone のオブジェクトプロトコルは強化され、認証とメタデータのオーバーヘッドが合理化されています。

レイテンシーをさらに短縮し、1 秒あたり最大 200 万回の読み取りと最大 200,000 回の書き込みをサポートするために、S3 Express One Zone はデータを Amazon S3 ディレクトリバケットに保存します。デフォルトでは、各ディレクトリバケットは、1 秒あたり最大 200,000 回の読み取りと最大 100,000 回の書き込みをサポートします。ワークロードでデフォルトの TPS 制限を超える必要がある場合は、AWS サポートを通じて引き上げをリクエストできます。

1 桁ミリ秒のデータアクセス速度と、1 秒あたりの大量のトランザクションに対応できるディレクトリバケットを実現する高パフォーマンスの専用ハードウェアとソフトウェアの組み合わせにより、S3 Express One Zone はリクエスト集中型のオペレーションに最適な Amazon S3 ストレージクラスとなっています。

後続のトピックでは、S3 Express One Zone ストレージクラスを使用するアプリケーションのパフォーマンスを最適化するためのベストプラクティスのガイドラインと設計パターンについて説明します。

トピック

- S3 Express One Zone のパフォーマンスを最適化するためのベストプラクティス

S3 Express One Zone のパフォーマンスを最適化するためのベストプラクティス

Amazon S3 Express One Zone からオブジェクトをアップロードしたり取得したりするアプリケーションを構築する場合は、パフォーマンスを最適化するためのベストプラクティスガイドラインに従ってください。S3 Express One Zone ストレージクラスを使用するには、S3 ディレクトリバケットを作成する必要があります。S3 Express One Zone ストレージ クラスは、S3 汎用バケットでの使用はサポートされていません。

その他すべての Amazon S3 ストレージクラスと S3 汎用バケットのパフォーマンスガイドラインについては、「設計パターンのベストプラクティス: Amazon S3 のパフォーマンスの最適化」を参照してください。

大規模なワークロードで S3 Express One Zone ストレージクラスとディレクトリバケットを使用して最適なパフォーマンスとスケーラビリティを実現するには、ディレクトリバケットと汎用バケットの動作の違いを理解することが重要です。そこで、アプリケーションをディレクトリバケットの動作に合わせて調整するためのベストプラクティスをご紹介します。

ディレクトリバケットの仕組み

Amazon S3 Express One Zone ストレージクラスは、ディレクトリバケットあたり毎秒最大 2,000,000 件の GET トランザクションと最大 200,000 件の PUT トランザクション (TPS) のワークロードをサポートできます。S3 Express One Zone では、データはアベイラビリティーゾーン内の S3 ディレクトリバケットに保存されます。ディレクトリバケット内のオブジェクトは、フラットな名前空間を持つ S3 汎用バケットとは対照的に、ファイルシステムに似た階層型の名前空間内でアクセス可能です。汎用バケットとは異なり、ディレクトリバケットはキーをプレフィックスではなくディレクトリに階層的に整理します。プレフィックスは、オブジェクトキー名の先頭にある文字列です。プレフィックスを使用してデータを整理し、汎用バケットでフラットオブジェクトストレージアーキテクチャを管理できます。詳細については、「プレフィックスを使用してオブジェクトを整理する」を参照してください。

ディレクトリバケットでは、オブジェクトは階層型の名前空間に整理され、スラッシュ (/) のみが区切り文字としてサポートされます。`dir1/dir2/file1.txt` のようなキーを持つオブジェクトをアップロードすると、Amazon S3 によってディレクトリ `dir1/` と `dir2/` が自動的に作成および管理されます。ディレクトリは `PutObject` または `CreateMultiPartUpload` オペレーション中に作成され、`DeleteObject` または `AbortMultiPartUpload` オペレーション後に空になると自動的に削除されます。ディレクトリ内のオブジェクトとサブディレクトリの数に制限はありません。

オブジェクトがディレクトリバケットにアップロードされたときに作成されるディレクトリは、HTTP `503 (Slow Down)` エラーの可能性を減らすために瞬時にスケールできます。この自動スケーリングにより、アプリケーションは必要に応じてディレクトリ内およびディレクトリ間の読み取り/書き込みリクエストを並列処理できます。S3 Express One Zone の場合、個々のディレクトリはディレクトリバケットの最大リクエストレートをサポートするように設計されています。システムがオブジェクトを自動的に分散して負荷を均等に分散するため、最適なパフォーマンスを実現するためにキープレフィックスをランダム化する必要はありませんが、その結果、キーはディレクトリバケット内で辞書順に格納されません。これは、辞書順に近いキーが同じサーバー上に配置される可能性が高くなる S3 汎用バケットとは対照的です。

ディレクトリバケットオペレーションとディレクトリインタラクションの例の詳細については、「ディレクトリバケットオペレーションとディレクトリインタラクションの例」を参照してください。

ベストプラクティス

ディレクトリバケットのパフォーマンスを最適化し、ワークロードの長期的なスケールアップを支援するためにベストプラクティスに従ってください。

多数のエントリ (オブジェクトまたはサブディレクトリ) を含むディレクトリを使用する

ディレクトリバケットは、すべてのワークロードに対してデフォルトで高いパフォーマンスを提供します。特定のオペレーションでパフォーマンスをさらに最適化するために、より多くのエントリ (オブジェクトまたはサブディレクトリ) をディレクトリに統合すると、レイテンシーが低くなり、リクエストレートが向上します。

- PutObject、DeleteObject、CreateMultiPartUpload、AbortMultiPartUpload などの変異 API オペレーションは、多数の小さなディレクトリではなく、数千のエントリを含む少数の高密度ディレクトリで実装すると、最適なパフォーマンスが得られます。
- ListObjectsV2 オペレーションは、結果ページを生成するためにトラバースする必要があるディレクトリ数が少ないほど、パフォーマンスが向上します。

プレフィックスにエントロピーを使用しない

Amazon S3 オペレーションでは、エントロピーとは、ストレージパーティション間でワークロードを均等に分散するのに役立つプレフィックス命名におけるランダム性を指します。ただし、ディレクトリバケットは内部的に負荷分散を管理するため、パフォーマンスを最大限に高めるためにプレフィックスにエントロピーを使用することは推奨されません。これは、ディレクトリバケットの場合、エントロピーによって既に作成済みのディレクトリが再利用されず、リクエストが遅くなる可能性があるためです。

$HASH/directory/object のようなキーパターンは、多くの中間ディレクトリを作成する可能性があります。次の例では、親が異なるため、すべての job-1 は異なるディレクトリです。ディレクトリはスパースになり、ミューテーションリクエストとリストリクエストは遅くなります。この例では、すべて単一のエントリを持つ中間ディレクトリが 12 個あります。

```
s3://my-bucket/0cc175b9c0f1b6a831c399e269772661/job-1/file1

s3://my-bucket/92eb5ffee6ae2fec3ad71c777531578f/job-1/file2

s3://my-bucket/4a8a08f09d37b73795649038408b5f33/job-1/file3

s3://my-bucket/8277e0910d750195b448797616e091ad/job-1/file4

s3://my-bucket/e1671797c52e15f763380b45e841ec32/job-1/file5

s3://my-bucket/8fa14cdd754f91cc6554c9e71929cce7/job-1/file6
```

代わりに、パフォーマンスを向上させるために、$HASH コンポーネントを削除し、 job-1 を単一のディレクトリにして、ディレクトリの密度を向上させることができます。次の例では、6 つのエントリを持つ単一の中間ディレクトリを使用することで、前の例と比較してパフォーマンスを向上させることができます。

```
s3://my-bucket/job-1/file1

s3://my-bucket/job-1/file2

s3://my-bucket/job-1/file3

s3://my-bucket/job-1/file4

s3://my-bucket/job-1/file5

s3://my-bucket/job-1/file6
```

このパフォーマンス上の利点は、オブジェクトキーが最初に作成され、そのキー名にディレクトリが含まれている場合、そのオブジェクト用のディレクトリが自動的に作成されるためです。同じディレクトリにそれ以降にオブジェクトをアップロードする場合、ディレクトリを作成する必要がないため、既存のディレクトリにオブジェクトをアップロードする際のレイテンシーが軽減されます。

ListObjectsV2 呼び出し中にオブジェクトを論理的にグループ化する必要がない場合は、区切り文字/以外の区切り文字を使用してキーの部分を区切ります。

/ 区切り文字はディレクトリバケットに対して特別に扱われるため、意図的に使用する必要があります。ディレクトリバケットはオブジェクトを辞書順に並べませんが、ディレクトリ内のオブジェクトは引き続き ListObjectsV2 出力でグループ化されます。この機能が不要な場合は、区切り文字として / を別の文字に置き換えて、中間ディレクトリが作成されないようにすることができます。

例えば、以下のキーが YYYY/MM/DD/HH/ というプレフィックスパターンになっているとします。

```
s3://my-bucket/2024/04/00/01/file1

s3://my-bucket/2024/04/00/02/file2

s3://my-bucket/2024/04/00/03/file3

s3://my-bucket/2024/04/01/01/file4

s3://my-bucket/2024/04/01/02/file5
```

```
s3://my-bucket/2024/04/01/03/file6
```

ListObjectsV2 の結果でオブジェクトを時間や日でグループ化する必要はないが、月でグループ化する必要がある場合、YYYY/MM/DD-HH- というキーパターンを使用すると、ディレクトリ数が大幅に減少し、ListObjectsV2 オペレーションのパフォーマンスが向上します。

```
s3://my-bucket/2024/04/00-01-file1

s3://my-bucket/2024/04/00-01-file2

s3://my-bucket/2024/04/00-01-file3

s3://my-bucket/2024/04/01-02-file4

s3://my-bucket/2024/04/01-02-file5

s3://my-bucket/2024/04/01-02-file6
```

可能な場合は、区切りリストオペレーションを使用する

delimiter のない ListObjectsV2 リクエストは、すべてのディレクトリに対して深さ優先の再帰的トラバーサルを実行します。delimiter のある ListObjectsV2 は、prefix パラメータで指定されたディレクトリ内のエントリのみを取得するため、リクエストのレイテンシーが短縮され、1 秒あたりの集計キーが増加します。ディレクトリバケットの場合は、可能な限り区切りリストオペレーションを使用してください。区切りリストを使用することで、ディレクトリへのアクセス回数が減り、1 秒あたりのキー数が増加し、リクエストのレイテンシーが短縮されます。

例えば、ディレクトリバケット内の次のディレクトリとオブジェクトの場合。

```
s3://my-bucket/2024/04/12-01-file1

s3://my-bucket/2024/04/12-01-file2

...

s3://my-bucket/2024/05/12-01-file1

s3://my-bucket/2024/05/12-01-file2

...
```

```
s3://my-bucket/2024/06/12-01-file1

s3://my-bucket/2024/06/12-01-file2

...

s3://my-bucket/2024/07/12-01-file1

s3://my-bucket/2024/07/12-01-file2

...
```

ListObjectsV2 のパフォーマンスを向上させるには、アプリケーションのロジックで許可されている場合は、区切りリストを使用してサブディレクトリとオブジェクトを一覧表示します。例えば、区切りリストオペレーションを実行するには、次のコマンドを実行します。

```
aws s3api list-objects-v2 --bucket my-bucket --prefix '2024/' --delimiter '/'
```

出力はサブディレクトリのリストです。

```
{
    "CommonPrefixes": [
        {
            "Prefix": "2024/04/"
        },
        {
            "Prefix": "2024/05/"
        },
        {
            "Prefix": "2024/06/"
        },
        {
            "Prefix": "2024/07/"
        }
    ]
}
```

各サブディレクトリの一覧表示のパフォーマンスを向上させるには、次の例のようなコマンドを実行します。

コマンド:

```
aws s3api list-objects-v2 --bucket my-bucket --prefix '2024/04' --delimiter '/'
```

出力:

```
{
    "Contents": [
        {
            "Key": "2024/04/12-01-file1"
        },
        {
            "Key": "2024/04/12-01-file2"
        }
    ]
}
```

S3 Express One Zone ストレージと コンピューティングリソースを同じロケーションに配置する

S3 Express One Zone では、各ディレクトリのバケットは、バケットの作成時に選択した単一のアベイラビリティーゾーンに保存されます。まず、コンピュートワークロードまたはリソースにローカルなアベイラビリティーゾーンに新しいディレクトリバケットを作成します。これにより、レイテンシーが非常に低い読み取りと書き込みの利用を直ちに開始できます。ディレクトリバケットは S3 バケットの一種で、コンピューティングとストレージの間のレイテンシーを低減するために AWS リージョン内のアベイラビリティーゾーンを選択できる最初の S3 バケットです。

複数のアベイラビリティーゾーンにわたってディレクトリバケットにアクセスすると、レイテンシーがわずかに増加する可能性があります。パフォーマンスを最適化するには、可能な場合は、同じアベイラビリティーゾーンにある Amazon Elastic Container Service、Amazon Elastic Kubernetes Service、Amazon Elastic Compute Cloud のインスタンスからディレクトリバケットにアクセスすることをお勧めします。

同時接続を使用して、1MB を超えるオブジェクトで高スループットを実現する

ディレクトリバケットに複数のリクエストを同時に発行し、リクエストを別々の接続に分散してアクセス可能な帯域幅を最大化することで、最高のパフォーマンスを実現できます。汎用バケットと同様に、S3 Express One Zone には、バケットへの接続数に制限はありません。同じディレクトリへの同時書き込みが多数発生した場合、個々のディレクトリのパフォーマンスを水平方向かつ自動的にスケールできます。

ディレクトリバケットへの個々の TCP 接続には、1 秒あたりにアップロードまたはダウンロードできるバイト数に対する固定の上限があります。オブジェクトが大きくなると、リクエスト時間はトラ

ンザクション処理ではなくバイトストリーミングによって支配されるようになります。複数の接続を使用して大きなオブジェクトのアップロードまたはダウンロードを並列化することで、エンドツーエンドのレイテンシーを削減できます。Java 2.x SDK を使用する場合は、マルチパートアップロード API オペレーションやバイト範囲フェッチなどのパフォーマンスの向上を利用してデータに並行してアクセスする S3 Transfer Manager の使用を検討する必要があります。

ゲートウェイ VPC エンドポイントを使用する

ゲートウェイエンドポイントは、VPC からディレクトリバケットへの直接接続を提供します。VPC にインターネットゲートウェイや NAT デバイスは必要ありません。パケットがネットワーク上で費やす時間を短縮するには、VPC にディレクトリバケット用のゲートウェイ VPC エンドポイントを設定する必要があります。詳細については、「ディレクトリバケットのネットワーク」を参照してください。

セッション認証を使用し、有効なセッショントークンを再利用する

ディレクトリバケットは、パフォーマンスが重視される API オペレーションのレイテンシーを削減するためのセッショントークン認証メカニズムを提供します。CreateSession を 1 回呼び出すだけでセッショントークンを取得でき、このトークンはその後 5 分間のすべてのリクエストで有効になります。API コールのレイテンシーを最小限に抑えるには、セッショントークンを取得し、そのトークンの有効期間全体にわたって再利用してから更新するようにしてください。

AWS SDK を使用する場合、セッショントークンの更新は SDK によって自動的に処理され、セッションの有効期限が切れたときのサービス中断を回避できます。AWS SDK を使用して CreateSession API オペレーションへのリクエストを開始および管理することをお勧めします。

CreateSession の詳細については、「CreateSession を使用したゾーンエンドポイント API オペレーションの承認」を参照してください。

CRT ベースのクライアントを使用する

AWS Common Runtime (CRT) は、C 言語で記述されたモジュール式で高性能かつ効率的なライブラリのセットで、AWS SDK の基盤として機能します。CRT は、スループットの向上、接続管理の強化、スタートアップタイムの短縮を実現します。CRT は Go を除くすべての AWS SDK で使用できます。

使用する SDK に合わせて CRT を設定する方法の詳細については、「AWS Common Runtime (CRT) libraries」、「Accelerate Amazon S3 throughput with the AWS Common Runtime」、「Introducing CRT-based S3 client and the S3 Transfer Manager in the AWS SDK for Java 2.x」、「Using

S3CrtClient for Amazon S3 operations」、および「Configure AWS CRT-based HTTP clients」を参照してください。

最新バージョンの AWS SDK を使用する

AWS SDK では、Amazon S3 のパフォーマンスの最適化のために推奨されている多くのガイドラインが組み込みでサポートされています。SDK は、アプリケーション内から Amazon S3 を活用するためのシンプルな API を提供し、最新のベストプラクティスに合わせて定期的に更新されます。例えば、SDK は HTTP 503 エラーの後にリクエストを自動的に再試行し、接続レスポンスの遅延を処理します。

Java 2.x SDK を使用している場合は、S3 Transfer Manager の使用を検討する必要があります。S3 Transfer Manager は、必要に応じてバイト範囲リクエストを使用して接続を水平方向に自動的にスケーリングし、1 秒あたり数千件のリクエスト処理を実現します。バイト範囲リクエストは、S3 への同時接続を使用して同じオブジェクト内からさまざまなバイト範囲を取得できるため、パフォーマンスを向上させます。これにより、単一のオブジェクト全体のリクエストに対して高い集約スループットを実現できます。そのため、最新のパフォーマンス最適化機能を利用するには、最新バージョンの AWS SDK を使用することが重要です。

パフォーマンスのトラブルシューティング

レイテンシーの影響を受けやすいアプリケーションに対して、再試行リクエストを設定していますか。

S3 Express One Zone は、追加の調整を必要とせずに一貫したレベルのパフォーマンスを実現できるように設計されています。ただし、タイムアウト値とリトライを積極的に設定すると、レイテンシーとパフォーマンスを一定に維持できます。AWS SDK には、特定のアプリケーションの許容値に調整できる設定可能なタイムアウト値と再試行値があります。

AWS Common Runtime (CRT) ライブラリと最適な Amazon EC2 インスタンスタイプを使用していますか。

多数の読み取りおよび書き込みオペレーションを実行するアプリケーションは、そうでないアプリケーションに比べて、より多くのメモリやコンピューティング容量を必要とする可能性があります。コンピューティングを多用するワークロードのために Amazon EC2 インスタンスを起動する際は、アプリケーションが必要とする量のリソースを持つインスタンスタイプを選択します。S3 Express One Zone の高パフォーマンスストレージは、システムメモリ容量が大きく、高パフォーマンスストレージを活用できるより強力な CPU や GPU を備えた、より大規模で新しいインスタンスタイプと組み合わせるのが理想的です。また、CRT が有効になっている AWS SDK の最新バージョンを使用

することをお勧めします。これにより、読み取りリクエストと書き込みリクエストの並列処理をより高速化できます。

セッションベースの認証に AWS SDK を使用していますか。

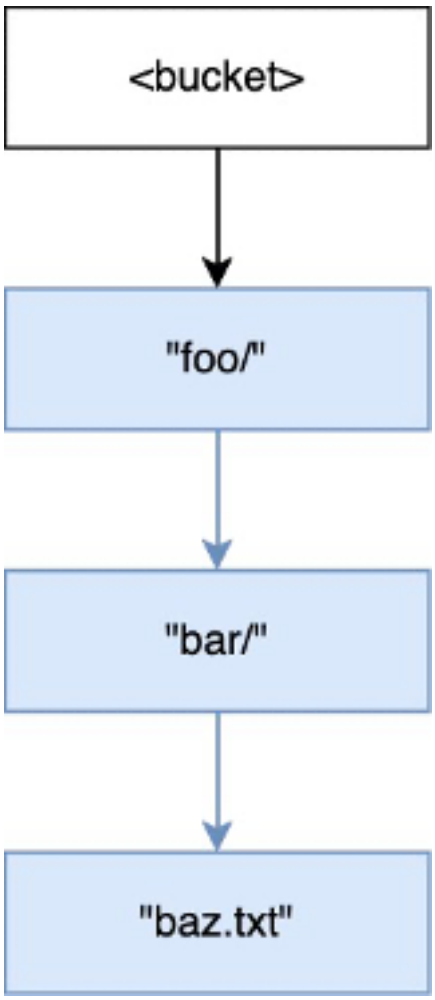
Amazon S3 では、AWS SDK と同じベストプラクティスに従うことで、HTTP REST API リクエストを使用する際のパフォーマンスを最適化することもできます。ただし、S3 Express One Zone で使用されているセッションベースの認可および認証メカニズムの場合、AWS SDK を使用して `CreateSession` およびそのマネージドセッショントークンを管理することを強くお勧めします。AWS SDK は `CreateSession` API オペレーションを使用して、ユーザーに代わってトークンの作成と更新を自動的に行います。`CreateSession` を使用すると、各リクエストを承認するための AWS Identity and Access Management (IAM) へのリクエストごとの往復のレイテンシーを回避できます。

ディレクトリバケットオペレーションとディレクトリインタラクションの例

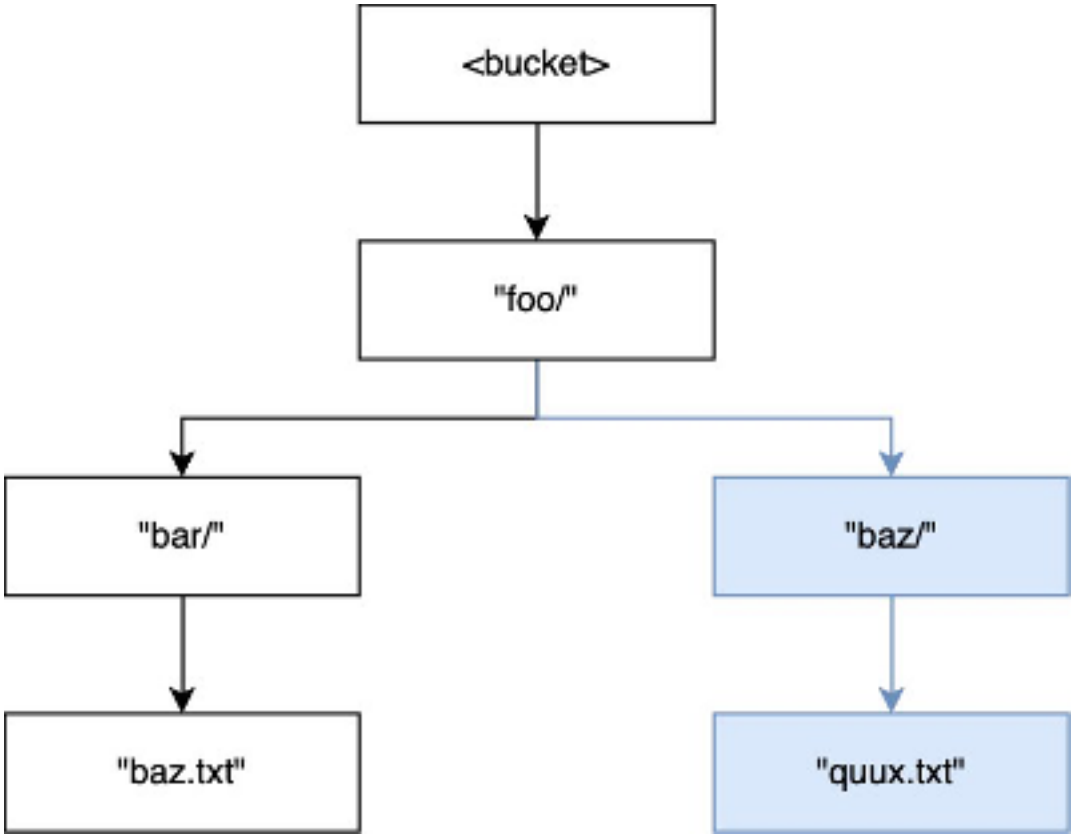
以下に、ディレクトリバケットの仕組みに関する 3 つの例を示します。

例 1: ディレクトリバケットへの S3 **`PutObject`**リクエストがディレクトリとやり取りする方法

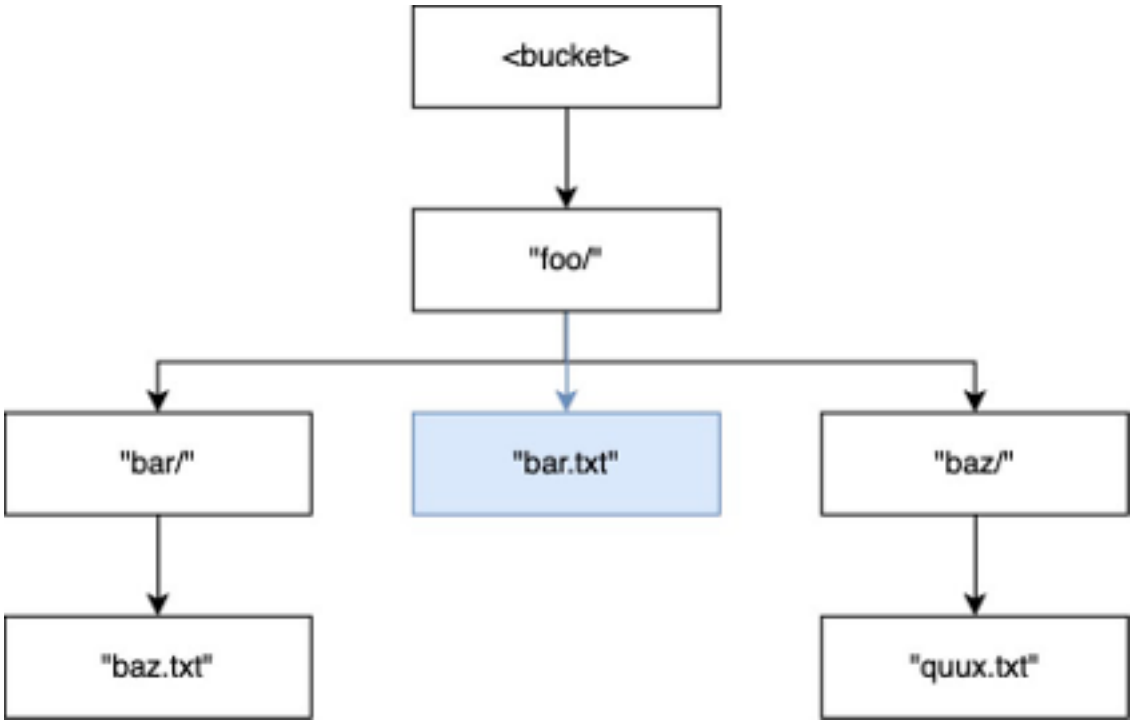
1. 空のバケットで `PUT(<bucket>, "documents/reports/quarterly.txt")` オペレーションが実行されると、バケットのルートにディレクトリ `documents/` が作成され、`documents/` 内にディレクトリ `reports/` が作成され、`reports/` 内にオブジェクト `quarterly.txt` が作成されます。このオペレーションでは、オブジェクトに加えて 2 つのディレクトリが作成されました。



2. 次に、別のオペレーション PUT(<bucket>, "documents/logs/application.txt") が実行されると、 ディレクトリ documents/ は既に存在し、documents/ 内にディレクトリ logs/ が存在しないため新たに作成され、logs/ 内にオブジェクト application.txt が作成されます。このオペレーションでは、オブジェクトに加えて作成されたディレクトリは 1 つだけです。



3. 最後に、PUT(<bucket>, "documents/readme.txt") オペレーションが実行されると、ルート内のディレクトリ documents/ が既に存在し、オブジェクト readme.txt が作成されます。このオペレーションでは、ディレクトリは作成されません。



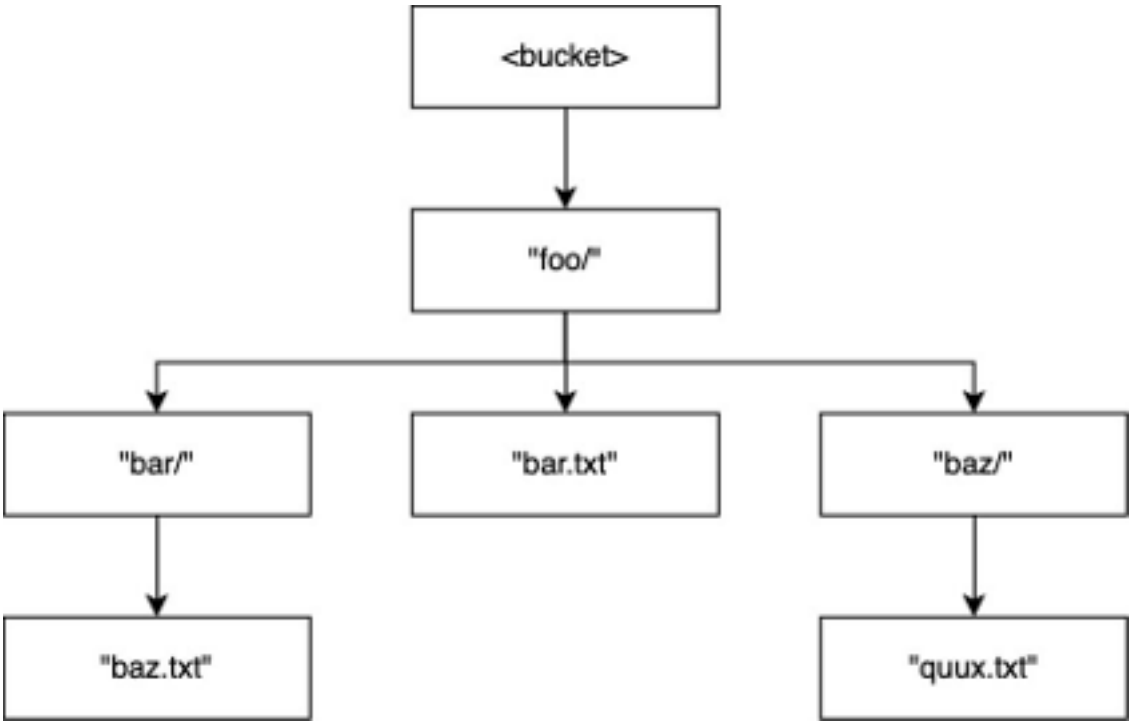
例 2: ディレクトリバケットへの S3 **ListObjectsV2** リクエストがディレクトリとやり取りする方法

区切り文字を指定しない S3 ListObjectsV2 リクエストの場合、バケットは深さ優先方式でトラバースされます。出力は一貫した順序で返されます。ただし、この順序はリクエスト間で同じですが、辞書順ではありません。前の例で作成したバケットとディレクトリの場合:

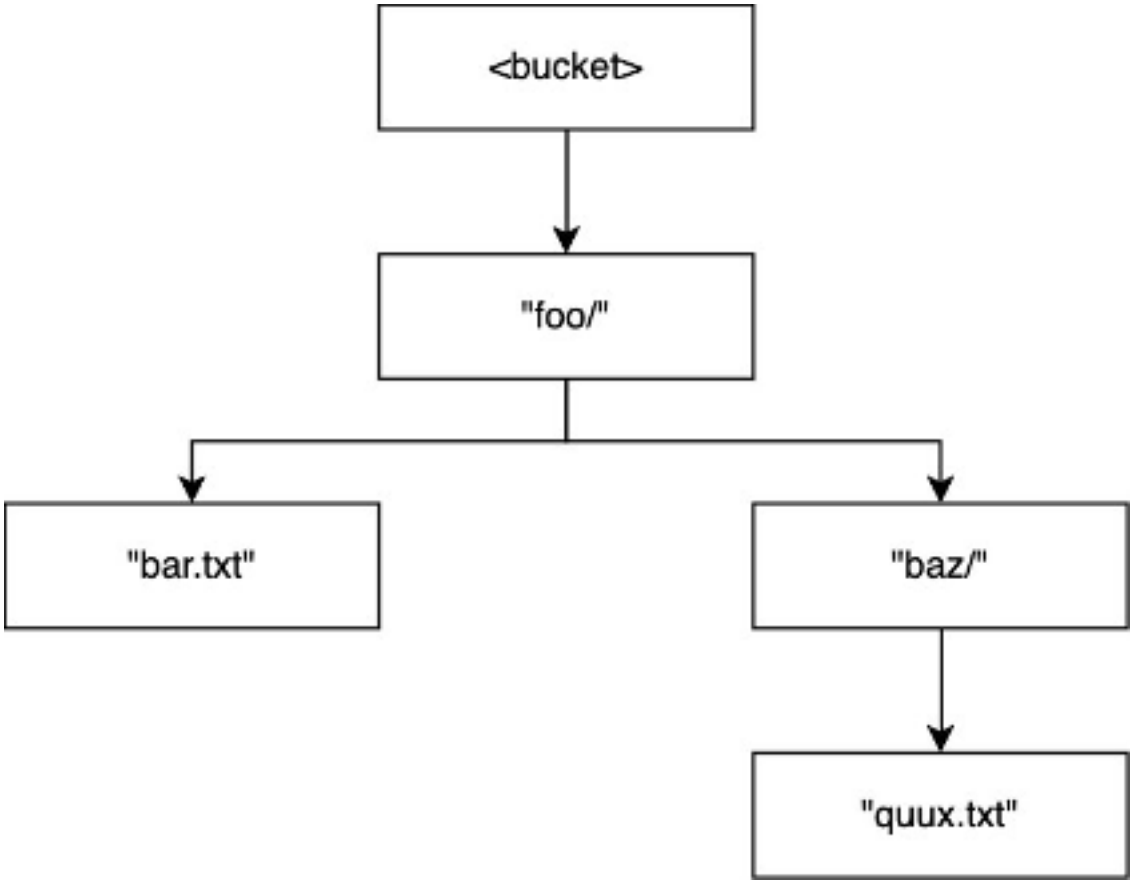
1. LIST(<bucket>) が実行されると、ディレクトリ documents/ に入り、トラバースが開始されます。
2. サブディレクトリ logs/ に入り、トラバースが開始されます。
3. オブジェクト application.txt が logs/ 内に見つかります。
4. logs/ 内にはこれ以上エントリが存在しません。List オペレーションは logs/ を終了し、再び documents/ に入ります。
5. documents/ ディレクトリは引き続きトラバースされ、オブジェクト readme.txt が見つかります。
6. documents/ ディレクトリは引き続きトラバースされ、サブディレクトリ reports/ に入り、トラバースが開始されます。
7. オブジェクト quarterly.txt が reports/ 内に見つかります。
8. reports/ 内にはこれ以上エントリが存在しません。リストは reports/ を出て、再び documents/ に入ります。
9. documents/ 内にはこれ以上のエントリがないので、リストは戻ります。

この例では、logs/ は readme.txt よりも前に順序付けられ、readme.txt は reports/ よりも前に順序付けられています。

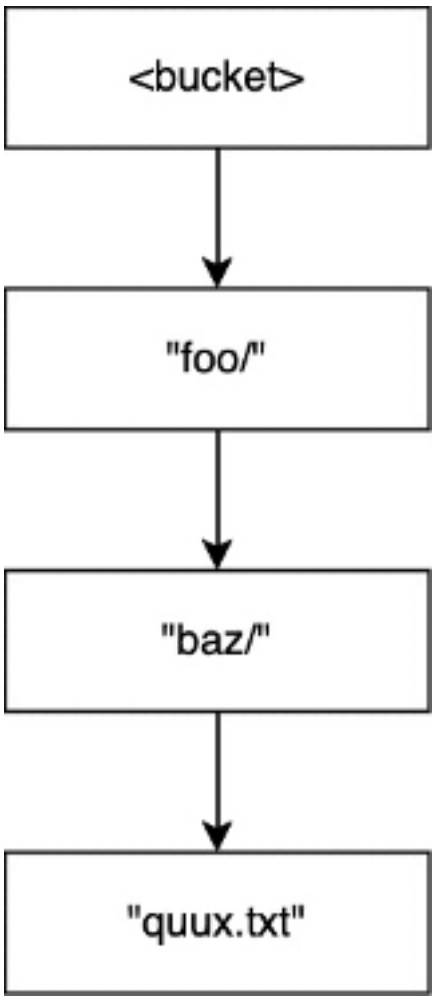
例 3: ディレクトリバケットへの S3 **DeleteObject** リクエストがディレクトリとやり取りする方法



1. 同じバケットで、DELETE(<bucket>, "documents/reports/quarterly.txt") オペレーションを実行すると、オブジェクト quarterly.txt が削除され、ディレクトリ reports/ が空になり、即座に削除されます。documents/ ディレクトリにはディレクトリ logs/ とオブジェクト readme.txt の両方があり、ディレクトリは空ではないため、削除されません。このオペレーションでは、1 つのオブジェクトと 1 つのディレクトリのみが削除されました。



2. DELETE(<bucket>, "documents/readme.txt") オペレーションが実行されると、オブジェクト readme.txt は削除されます。documents/ にはディレクトリ logs/ があり空ではないため、削除されません。このオペレーションでは、ディレクトリは削除されず、オブジェクトのみが削除されます。



3. 最後に、オペレーション DELETE(<bucket>, "documents/logs/application.txt") が実行されると、application.txt は削除され、logs/ が空になり、即座に削除されます。これにより documents/ も空になり、これも即座に削除されます。このオペレーションでは、2 つのディレクトリと 1 つのオブジェクトが削除されます。バケットが空になりました。

データレジデンシーワークロード

AWS 専有ローカルゾーン (専有ローカルゾーン) は、AWS によるフルマネージドの AWS インフラストラクチャの一種で、ユーザーまたはコミュニティ専用に構築され、規制要件に準拠するためにユーザーが指定した場所またはデータセンターに配置されます。専有ローカルゾーンは、AWS Local

Zones (Local Zones) サービスの一種です。詳細については、「AWS 専有ローカルゾーン」を参照してください。

専有ローカルゾーンでは、S3 ディレクトリバケットを作成して特定のデータ境界にデータを保存できるため、データレジデンシーと分離のユースケースをサポートするのに役立ちます。Dedicated Local Zones のディレクトリバケットは、S3 Express One Zone および S3 One Zone-Infrequent Access (S3 One Zone-IA、Z-IA) ストレージクラスをサポートできます。ディレクトリバケットは現在、他の AWS Local Zones ロケーションでは使用できません。

専有ローカルゾーンでは、AWS Management Console、REST API、AWS Command Line Interface (AWS CLI)、および AWS SDK を使用できます。

Local Zones 内のディレクトリバケットのオペレーションの詳細については、以降のトピックを参照してください。

トピック

- Local Zones のディレクトリバケットの概念
- ローカルゾーンのアカウントを有効にする
- VPC からのプライベート接続
- Local Zone でのディレクトリバケットの作成
- Local Zones でのディレクトリバケットの認証と認可

Local Zones のディレクトリバケットの概念

ローカルゾーンでディレクトリバケットを作成する前に、バケットを作成する先のローカルゾーン ID を取得する必要があります。ローカルゾーンに関するすべての情報は、DescribeAvailabilityZones API オペレーションを使用して確認できます。この API オペレーションは、ローカルゾーン ID、親リージョン名、ネットワークボーダーグループ、オプトインステータスなど、ローカルゾーンに関する情報を一覧表示します。ローカルゾーン ID を取得してオプトインしたら、ローカルゾーンでディレクトリバケットを作成できます。ディレクトリバケット名は、ユーザーが指定したベース名、バケットの場所のゾーン ID を含むサフィックス、および `--x-s3` で構成されます。

Local Zone は、Amazon の冗長で非常に広帯域のプライベートネットワークを使用して親リージョンに接続されます。これにより、ローカルゾーンで実行しているアプリケーションは、親リージョン内の他の AWS のサービスに高速、安全、シームレスにアクセスできます。親ゾーン ID は、ローカルゾーンのコントロールプレーンオペレーションを処理するゾーンの ID です。ネットワーク境界グ

ループは、AWS によるパブリック IP アドレスのアドバタイズ元となる一意のグループです。Local Zones、親リージョン、親ゾーン ID の詳細については、「AWS Local Zones User Guide」の「AWS Local Zones concepts」を参照してください。

すべてのディレクトリバケットでは s3express 名前空間を使用します。これは汎用バケットの s3 名前空間とは異なります。ディレクトリバケットの場合、リクエストはリージョンエンドポイントまたはゾーンエンドポイントのいずれかにルーティングされます。AWS Management Console、AWS CLI、または AWS SDK を使用すると、ルーティングは自動的に処理されます。

ほとんどのバケットレベルの API オペレーション (CreateBucket や DeleteBucket など) は、リージョンエンドポイントにルーティングされ、リージョンエンドポイント API オペレーションと呼ばれます。リージョンエンドポイントは s3express-control.ParentRegionCode.amazonaws.com の形式です。すべてのオブジェクトレベルの API オペレーション (PutObject など) と 2 つのバケットレベルの API オペレーション (CreateSession および HeadBucket) はゾーンエンドポイントにルーティングされ、ゾーンエンドポイント API オペレーションと呼ばれます。ゾーンエンドポイントは s3express-LocalZoneID.ParentRegionCode.amazonaws.com の形式です。エンドポイント別の API オペレーションの完全なリストについては、「ディレクトリバケット API オペレーション」を参照してください。

S3 は北京ローカルゾーンで利用できます。

ローカルゾーン ID: cnn1-pkx1-az1

- 親リージョン名: China (Beijing)
- 親リージョンコード: cn-north-1
- 親ゾーン ID: cnn1-az1
- ローカルゾーン名: China (Beijing)
- ローカルゾーンコード: cnn1-pkx1-az1
- ネットワークボーダーグループ: cn-north-1-pkx-1
- バケット ARN の例: arn:aws-cn:s3express:cn-north-1:*123456789012*:bucket/*amzn-s3-demo-bucket*--cnn1-pkx1-az1--x-s3
- リージョンエンドポイント: s3express-control.cn-north-1.amazonaws.com.cn

ゾーンエンドポイント: `s3express-cnn1-pkx1-az1.cn-north-1.amazonaws.com.cn`

ストレージクラス: `S3 One Zone-Infrequent Access (S3 One Zone-IA; Z-IA)`

仮想プライベートクラウド (VPC) から Local Zones のディレクトリバケットにアクセスするには、ゲートウェイ VPC エンドポイントを使用できます。ゲートウェイエンドポイントは追加料金なしで使用できます。Local Zones のディレクトリバケットとオブジェクトにアクセスするためのゲートウェイ VPC エンドポイントを設定するには、「VPC からのプライベート接続」を参照してください。

ローカルゾーンのアカウントを有効にする

次のトピックでは、専有ローカルゾーンでアカウントを有効にする方法について説明します。

Amazon S3 を含む AWS 専有ローカルゾーン (専有ローカルゾーン) のすべてのサービスでは、専有ローカルゾーン内のリソースを作成またはアクセスする前に、管理者が AWS アカウントを有効にする必要があります。DescribeAvailabilityZones API オペレーションを使用して、ローカルゾーンへのアカウント ID アクセスを確認できます。

Amazon S3 のデータをさらに保護するために、デフォルトでは、作成した S3 リソースにのみアクセスできます。Local Zones のバケットでは、すべての S3 ブロックのパブリックアクセス設定がデフォルトで有効になっており、S3 オブジェクトの所有権は [バケット所有者の強制] に設定されています。上記の設定は変更できません。オプションで、Local Zone のネットワーク境界グループ内のみにアクセスを制限するには、IAM ポリシーで条件キー `s3express:AllAccessRestrictedToLocalZoneGroup` を使用できます。詳細については、「Local Zones でのディレクトリバケットの認証と認可」を参照してください。

VPC からのプライベート接続

ゲートウェイエンドポイントを使用して、仮想プライベートクラウド (VPC) から AWS Local Zones (Local Zones) のディレクトリバケットにアクセスできます。VPC 用のインターネットゲートウェイや NAT デバイスは必要なく、追加料金もかかりません。次のトピックでは、VPC と Local Zones のディレクトリバケット間のゲートウェイ VPC エンドポイントの設定について説明します。

ゲートウェイ VPC エンドポイントを設定するには

1. Amazon VPC コンソールを開きます。
2. ナビゲーションペインで、[エンドポイント] を選択します。
3. [エンドポイントの作成] を選択します。

4. エンドポイントの名前を作成します。
5. [Service category] (サービスカテゴリ) で、AWS のサービス を選択します。
6. [サービス] では、[Type=Gateway] フィルターを追加して、com.amazonaws.***region***.s3express の隣にあるボタンをクリックします。
7. [VPC] で、エンドポイントを作成する VPC を選択します。
8. [ルートテーブル] で、エンドポイントで使用する Local Zone のルートテーブルを選択します。エンドポイントが作成されると、このステップで選択したルートテーブルにルートレコードが追加されます。
9. [ポリシー] では、[フルアクセス] を選択して、VPC エンドポイントのすべてのリソースに対するすべてのプリンシパルによるすべてのオペレーションを許可します。それ以外の場合は、[カスタム] を選択して、VPC エンドポイント経由でリソースに対してアクションを実行するためのプリンシパルのアクセス許可を制御する VPC エンドポイントポリシーをアタッチします。
10. (オプション) タグを追加するには、[新しいタグを追加] をクリックして、タグのキーバリューを入力します。
11. [エンドポイントの作成] を選択します。

ゲートウェイ VPC エンドポイントの詳細については、「AWS PrivateLink Guide」の「Gateway endpoints」を参照してください。データレジデンシーのユースケースでは、ゲートウェイ VPC エンドポイントを使用して VPC からのみバケットへのアクセスを有効にすることをお勧めします。アクセスが VPC または VPC エンドポイントに制限されている場合、AWS Management Console、REST API、AWS CLI、および AWS SDK を介してオブジェクトにアクセスできます。

> **Note**
>
> AWS Management Consoleを使用して VPC または VPC エンドポイントへのアクセスを制限するには、AWS Management Console のプライベートアクセスを使用する必要があります。詳細については、「AWS Management Console guide」の「AWS Management Console Private Access」を参照してください。

Local Zone でのディレクトリバケットの作成

専有ローカルゾーンでは、特定のデータ境界にオブジェクトを保存および取得するディレクトリバケットを作成して、データレジデンシーとデータ分離のユースケースに対応できます。S3 ディレクトリバケットは Local Zones でサポートされている唯一のバケットタイプであり、`LocalZone` と

いうバケットの場所タイプが含まれています。ディレクトリバケット名は、指定するベース名と、バケットの場所と `--x-s3` の Zone ID を含むサフィックスで構成されます。Local Zone ID のリストは、DescribeAvailabilityZones API オペレーションを使用して取得できます。詳細については、「ディレクトリバケットの命名規則」を参照してください。

> **Note**
>
> - S3 を含む AWS 専有ローカルゾーン (専有ローカルゾーン) のすべてのサービスでは、専有ローカルゾーン内のリソースを作成またはアクセスする前に、管理者が AWS アカウントを有効にする必要があります。詳細については、「ローカルゾーンのアカウントを有効にする」を参照してください。
> - データレジデンシー要件については、ゲートウェイ VPC エンドポイントからのみバケットへのアクセスを有効にすることをお勧めします。詳細については、「VPC からのプライベート接続」を参照してください。
> - Local Zone のネットワーク境界グループ内のみにアクセスを制限するには、IAM ポリシーで条件キー `s3express:AllAccessRestrictedToLocalZoneGroup` を使用できます。詳細については、「Local Zones でのディレクトリバケットの認証と認可」を参照してください。

以下に、AWS Management Console、AWS CLI、AWS SDK を使用して単一の Local Zone にディレクトリバケットを作成する方法について説明します。

S3 コンソールの使用

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. ページ上部にあるナビゲーションバーで、現在表示されている AWS リージョン の名前をクリックします。次に、ディレクトリバケットの作成先となる Local Zone の親リージョンを選択します。

   > **Note**
   >
   > 親リージョンの詳細については、「Local Zones のディレクトリバケットの概念」を参照してください。

3. 左側のナビゲーションペインで、[バケット] を選択します。

4. [Create bucket (バケットの作成)] を選択します。

   [バケットの作成] ページが開きます。

5. [全般設定] で、バケットが作成される AWS リージョン を確認します。

6. [バケットタイプ] で [ディレクトリ] を選択します。

   > **Note**
   >
   > - ディレクトリバケットをサポートしていないリージョンを選択した場合、バケットタイプはデフォルトで汎用バケットになります。ディレクトリバケットを作成するには、サポートされているリージョンを選択する必要があります。ディレクトリバケットをサポートするリージョンのリストについては、「the section called “ディレクトリバケットのリージョンエンドポイントとゾーンエンドポイント”」を参照してください。
   > - バケット作成後にバケットタイプは変更できません。

7. [バケットの場所] で、使用する Local Zone を選択します。

   > **Note**
   >
   > この Local Zone は、バケットの作成後に変更することはできません。

8. [バケットの場所] でチェックボックスをオンにして、Local Zone に障害が発生した場合に、データが使用できなくなったり、データが失われたりする場合があることに同意します。

   > **Important**
   >
   > ディレクトリバケットは、単一の Local Zone 内の複数のデバイスに保存されますが、ディレクトリバケットは Local Zones 間でデータを冗長に保存することはありません。

9. [バケット名] には、ディレクトリバケット名を入力します。

   ディレクトリバケットの命名規則の詳細については、「汎用バケットの命名規則」を参照してください。コンソールを使用してディレクトリバケットを作成すると、指定したベース名にサフィックスが自動的に追加されます。このサフィックスには、選択した Local Zone の Zone ID が含まれています。

   バケットを作成したら、その名前を変更することはできません。

> **Important**
>
> バケット名にアカウント番号などの機密情報を含めないでください。バケット名は、バケット内のオブジェクトを参照する URL に表示されます。

10. [オブジェクト所有者] で、[バケット所有者の強制] の設定が自動的に有効になり、アクセスコントロールリスト (ACL) が無効になります。ディレクトリバケットの場合、ACL は無効になっており、有効にできません。

    [バケット所有者の強制] 設定を有効にすると、バケット所有者はバケット内のすべてのオブジェクトを自動的に所有し、完全に制御できます。ACL は、S3 バケット内のデータに対するアクセス許可に対して影響を与えません。このバケットはアクセスコントロールを定義するためだけにポリシーを使用します。Amazon S3 の最新のユースケースの大部分では ACL を使用する必要がなくなっています。詳細については、「オブジェクトの所有権の制御とバケットの ACL の無効化。」を参照してください。
11. [このバケットのブロックパブリックアクセス設定] で、ディレクトリバケットのパブリックアクセスブロック設定がすべて自動的に有効になります。ディレクトリバケットの場合、この設定は変更できません。ブロックパブリックアクセスの詳細については、Amazon S3 ストレージへのパブリックアクセスのブロック を参照してください。
12. [デフォルトの暗号化] では、ディレクトリバケットはデフォルトで [Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3)] を使用してデータを暗号化します。[AWS Key Management Service キーによるサーバー側の暗号化 (SSE-KMS)] を使用して、ディレクトリバケット内のデータを暗号化するオプションもあります。
13. [バケットを作成] を選択します。

    バケットを作成したら、ファイルやフォルダをバケットに追加できます。詳細については、「the section called “ディレクトリバケットでのオブジェクトの使用”」を参照してください。

AWS CLI の使用

次の例は、AWS CLI を使用して Local Zone でディレクトリバケットを作成する方法を示しています。このコマンドを使用するには、*###############*を独自の情報に置き換えます。

ディレクトリバケットを作成する際は、設定の詳細を指定して、*bucket-base-name*--*zone-id*--x-s3 の命名規則を使用する必要があります。

```
aws s3api create-bucket
```

```
--bucket bucket-base-name--zone-id--x-s3
--create-bucket-configuration 'Location={Type=LocalZone,Name=local-zone-
id},Bucket={DataRedundancy=SingleLocalZone,Type=Directory}'
--region parent-region-code
```

Local Zone ID と親リージョンコードの詳細については、「Local Zones のディレクトリバケットの概念」を参照してください。AWS CLI コマンドの詳細については、「AWS CLI Command Reference」の「create-bucket」を参照してください。

AWS SDK の使用

SDK for Go

次の例は、AWS SDK for Go を使用して Local Zone でディレクトリバケットを作成する方法を示しています。

Example

```
var bucket = "bucket-base-name--zone-id--x-s3" // The full directory bucket name

func runCreateBucket(c *s3.Client) {
    resp, err := c.CreateBucket(context.Background(), &s3.CreateBucketInput{
        Bucket: &bucket,
        CreateBucketConfiguration: &types.CreateBucketConfiguration{
            Location: &types.LocationInfo{
                Name: aws.String("local-zone-id"),
                Type: types.LocationTypeLocalZone,
            },
            Bucket: &types.BucketInfo{
                DataRedundancy: types.DataRedundancySingleLocalZone,
                Type:           types.BucketTypeDirectory,
            },
        },
    })
    var terr *types.BucketAlreadyOwnedByYou
    if errors.As(err, &terr) {
        fmt.Printf("BucketAlreadyOwnedByYou: %s\n", aws.ToString(terr.Message))
        fmt.Printf("noop...\n") // No operation performed, just printing a message
        return
    }
    if err != nil {
        log.Fatal(err)
    }
```

```
    fmt.Printf("bucket created at %s\n", aws.ToString(resp.Location))
}
```

SDK for Java 2.x

次の例は、AWS SDK for Java 2.x を使用して Local Zone でディレクトリバケットを作成する方法を示しています。

Example

```
public static void createBucket(S3Client s3Client, String bucketName) {

    //Bucket name format is {base-bucket-name}--{local-zone-id}--x-s3
    //example: doc-example-bucket--local-zone-id--x-s3 is a valid name for a
 directory bucket created in a Local Zone.

    CreateBucketConfiguration bucketConfiguration =
 CreateBucketConfiguration.builder()
             .location(LocationInfo.builder()
                     .type(LocationType.LOCAL_ZONE)
                     .name("local-zone-id").build()) //this must match the Local
 Zone ID in your bucket name
             .bucket(BucketInfo.builder()
                    .type(BucketType.DIRECTORY)
                    .dataRedundancy(DataRedundancy.SINGLE_LOCAL_ZONE)
                    .build()).build();
    try {

             CreateBucketRequest bucketRequest =
 CreateBucketRequest.builder().bucket(bucketName).createBucketConfiguration(bucketConfigurat
             CreateBucketResponse response = s3Client.createBucket(bucketRequest);
             System.out.println(response);
    }

    catch (S3Exception e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
         }
    }
```

AWS SDK for JavaScript

次の例は、AWS SDK for JavaScript を使用して Local Zone でディレクトリバケットを作成する方法を示しています。

Example

```
// file.mjs, run with Node.js v16 or higher
// To use with the preview build, place this in a folder
// inside the preview build directory, such as /aws-sdk-js-v3/workspace/

import { S3 } from "@aws-sdk/client-s3";

const region = "parent-region-code";
const zone = "local-zone-id";
const suffix = `${zone}--x-s3`;

const s3 = new S3({ region });

const bucketName = `bucket-base-name--${suffix}`; // Full directory bucket name

const createResponse = await s3.createBucket(
    { Bucket: bucketName,
      CreateBucketConfiguration: {Location: {Type: "LocalZone", Name: "local-zone-
id"},
      Bucket: { Type: "Directory", DataRedundancy: "SingleLocalZone" }}
    }
   );
```

SDK for .NET

次の例は、SDK for .NET を使用して Local Zone でディレクトリバケットを作成する方法を示しています。

Example

```
using (var amazonS3Client = new AmazonS3Client())
{
    var putBucketResponse = await amazonS3Client.PutBucketAsync(new PutBucketRequest
    {

       BucketName = "bucket-base-name--local-zone-id--x-s3",
       PutBucketConfiguration = new PutBucketConfiguration
```

```
        {
          BucketInfo = new BucketInfo { DataRedundancy =
 DataRedundancy.SingleLocalZone, Type = BucketType.Directory },
          Location = new LocationInfo { Name = "local-zone-id", Type =
 LocationType.LocalZone }
        }
      }).ConfigureAwait(false);
}
```

SDK for PHP

次の例は、AWS SDK for PHP を使用して Local Zone でディレクトリバケットを作成する方法を示しています。

Example

```
require 'vendor/autoload.php';

$s3Client = new S3Client([

    'region'      => 'parent-region-code',
]);


$result = $s3Client->createBucket([
    'Bucket' => 'bucket-base-name--local-zone-id--x-s3',
    'CreateBucketConfiguration' => [
        'Location' => ['Name'=> 'local-zone-id', 'Type'=> 'LocalZone'],
        'Bucket' => ["DataRedundancy" => "SingleLocalZone" ,"Type" => "Directory"]
  ],
]);
```

SDK for Python

次の例は、AWS SDK for Python (Boto3) を使用して Local Zone でディレクトリバケットを作成する方法を示しています。

Example

```
import logging
import boto3
from botocore.exceptions import ClientError
```

```
def create_bucket(s3_client, bucket_name, local_zone):
    '''
    Create a directory bucket in a specified Local Zone

    :param s3_client: boto3 S3 client
    :param bucket_name: Bucket to create; for example, 'bucket-base-name--local-
zone-id--x-s3'
    :param local_zone: String; Local Zone ID to create the bucket in
    :return: True if bucket is created, else False
    '''

    try:
        bucket_config = {
                'Location': {
                    'Type': 'LocalZone',
                    'Name': local_zone
                },
                'Bucket': {
                    'Type': 'Directory',
                    'DataRedundancy': 'SingleLocalZone'
                }
            }
        s3_client.create_bucket(
            Bucket = bucket_name,
            CreateBucketConfiguration = bucket_config
        )
    except ClientError as e:
        logging.error(e)
        return False
    return True


if __name__ == '__main__':
    bucket_name = 'BUCKET_NAME'
    region = 'parent-region-code'
    local_zone = 'local-zone-id'
    s3_client = boto3.client('s3', region_name = region)
    create_bucket(s3_client, bucket_name, local_zone)
```

SDK for Ruby

次の例は、AWS SDK for Ruby を使用して Local Zone でディレクトリバケットを作成する方法を示しています。

Example

```
s3 = Aws::S3::Client.new(region:'parent-region-code')
s3.create_bucket(
  bucket: "bucket-base-name--local-zone-id--x-s3",
  create_bucket_configuration: {
    location: { name: 'local-zone-id', type: 'LocalZone' },
    bucket: { data_redundancy: 'SingleLocalZone', type: 'Directory' }
  }
)
```

Local Zones でのディレクトリバケットの認証と認可

Local Zones のディレクトリバケットは、AWS Identity and Access Management (IAM) 認可とセッションベースの認可の両方をサポートしています。ディレクトリバケットの認証と認可についての詳細は、「リクエストの認証と承認」を参照してください。

リソース

ディレクトリバケットの Amazon リソースネーム (ARN) には、s3express 名前空間、AWS 親リージョン、AWS アカウント ID、および Zone ID を含むディレクトリバケット名が含まれます。ディレクトリバケットにアクセスしてアクションを実行するには、次の ARN 形式を使用する必要があります。

```
arn:aws:s3express:region-code:account-id:bucket/bucket-base-name--ZoneID--x-s3
```

Local Zone のディレクトリバケットの場合、Zone ID は Local Zone の ID です。Local Zones 内のディレクトリバケットの詳細については、「Local Zones のディレクトリバケットの概念」を参照してください。ARN の詳細については「IAM ユーザーガイド」の「Amazon リソースネーム (ARN)」を参照してください。リソースの詳細については、「IAM ユーザーガイド」の「IAM JSON ポリシー要素: Resource」を参照してください。

Local Zones のディレクトリバケットの条件キー

Local Zones では、IAM ポリシーのすべての ディレクトリバケットの条件キー を使用できます。さらに、Local Zone のネットワーク境界グループの周囲にデータ境界を作成するには、条件キー s3express:AllAccessRestrictedToLocalZoneGroup を使用して、グループ外からのすべてのリクエストを拒否できます。

次の条件キーを使用すると、IAM ポリシーステートメントが適用される条件をさらに絞り込むことができます。ディレクトリバケットでサポートされている API オペレーション、ポリシーアクション、および条件キーの完全なリストについては、「ディレクトリバケットのポリシーアクション」を参照してください。

> **Note**
>
> 次の条件キーは Local Zones にのみ適用され、アベイラビリティーゾーンと AWS リージョンではサポートされていません。

API オペレーション	ポリシーアクション	説明	条件キー	説明	[Type] (タイプ)
ゾーンエンドポイント API オペレーション	s3express:CreateSession	セッショントークンを作成するアクセス許可を付与します。このセッショントークンは、CreateSession 、HeadBucket 、CopyObject 、PutObject 、GetObject など、すべてのゾーンエンドポイント API オペレーションへのアクセスを許可するために使用されます。	s3express:AllAccessRestrictedToLocalZoneGroup	この条件キーで指定された AWS Local Zone ネットワーク境界グループからリクエストが発信されていない限り、バケットへのすべてのアクセスをフィルタリングします。 値: Local Zone ネットワーク境界グループの値	String

ポリシーの例

定義したデータレジデンシー境界内 (具体的には、同じ AWS リージョンを親とする Local Zones のセットである Local Zone グループ) からのリクエストへのオブジェクトアクセスを制限するには、次のいずれかのポリシーを設定できます。

- サービスコントロールポリシー (SCP)。SCP の詳細については、「AWS Organizations User Guide」の「Service control policies (SCPs)」を参照してください。
- IAM ロールの IAM アイデンティティベースのポリシー。
- VPC エンドポイントポリシー。VPC エンドポイントポリシーの詳細については、「AWS PrivateLink Guide」の「Control access to VPC endpoints using endpoint policies」を参照してください。
- S3 バケットポリシー。

> **Note**
>
> 条件キー `s3express:AllAccessRestrictedToLocalZoneGroup` は、オンプレミス環境からのアクセスをサポートしていません。オンプレミス環境からのアクセスをサポートするには、ソース IP をポリシーに追加する必要があります。詳細については、「IAM ユーザーガイド」の「aws:SourceIp」を参照してください。

Example – SCP ポリシー

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Access-to-specific-LocalZones-only",
            "Effect": "Deny",
            "Action": [
                "s3express:*",
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEqualsIfExists": {
                    "s3express:AllAccessRestrictedToLocalZoneGroup": [
                        "local-zone-network-border-group-value"
                    ]
                }
            }
        }
    ]
}
```

Example – IAM アイデンティティベースのポリシー (IAM ロールにアタッチ)

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Deny",
        "Action": "s3express:CreateSession",
        "Resource": "*",
        "Condition": {
            "StringNotEqualsIfExists": {
                "s3express:AllAccessRestrictedToLocalZoneGroup": [
                    "local-zone-network-border-group-value"
                ]
            }
        }
    }
}
```

Example – VPC エンドポイントポリシー

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Access-to-specific-LocalZones-only",
            "Principal": "*",
            "Action": "s3express:CreateSession",
            "Effect": "Deny",
            "Resource": "*",
            "Condition": {
                 "StringNotEqualsIfExists": {
                     "s3express:AllAccessRestrictedToLocalZoneGroup": [
                         "local-zone-network-border-group-value"
                     ]
                 }
            }
        }
    ]
```

```
}
```

Example - バケットポリシー

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Access-to-specific-LocalZones-only",
            "Principal": "*",
            "Action": "s3express:CreateSession",
            "Effect": "Deny",
            "Resource": "*",
            "Condition": {
                 "StringNotEqualsIfExists": {
                     "s3express:AllAccessRestrictedToLocalZoneGroup": [
                         "local-zone-network-border-group-value"
                     ]
                 }
            }
        }
    ]
}
```

ディレクトリバケットの違い

Amazon S3 を使用する場合、アプリケーションとパフォーマンスの要件に最適なバケットタイプを選択できます。ディレクトリバケットは、低レイテンシーやデータレジデンシーのユースケースに最適なタイプのバケットです。ディレクトリバケットの詳細については、「ディレクトリバケットの使用」を参照してください。

ディレクトリバケットの相違点の詳細については、以下のトピックを参照してください。

トピック

- ディレクトリバケットの違い
- ディレクトリバケットでサポートされている API オペレーション
- ディレクトリバケットでサポートされていない Amazon S3 の機能

ディレクトリバケットの違い

- ディレクトリバケット名
  - ディレクトリバケット名は、ユーザーが指定するベース名と、バケットがあるゾーン (アベイラビリティゾーン) の ID を示すサフィックスで構成されます。ディレクトリバケット名は、次の形式を使用し、ディレクトリバケットの命名規則に従う必要があります。ディレクトリバケット名に関するルールのリストと例については、「ディレクトリバケットの命名規則」を参照してください。
- **ListObjectsV2** の動作
  - ディレクトリバケットの場合、ListObjectsV2 は辞書順 (アルファベット順) にオブジェクトを返すわけではありません。さらに、プレフィックスは区切り文字で終わる必要があり、区切り文字として指定できるのは「/」のみです。
  - ディレクトリバケットの場合、ListObjectsV2 レスポンスには、進行中のマルチパートアップロードにのみ関連するプレフィックスが含まれます。
- 削除動作 – ディレクトリバケット内のオブジェクトを削除すると、Amazon S3 はオブジェクトパス内の空のディレクトリをすべて再帰的に削除します。例えば、オブジェクトキー dir1/dir2/file1.txt を削除した場合、Amazon S3 は file1.txt を削除します。 dir1/ と dir2/ のディレクトリが空で、その他のオブジェクトが含まれていない場合、Amazon S3 はこれらのディレクトリも削除します。
- ETag とチェックサム – ディレクトリバケットのエンティティタグ (ETag) はオブジェクトに一意のランダムな英数字文字列であり、MD5 チェックサムではありません。ディレクトリバケットで追加のチェックサムを使用する方法の詳細については、「S3 の追加のチェックサムのベストプラクティス」を参照してください。
- **DeleteObjects** リクエスト内のオブジェクトキー
  - DeleteObjects リクエストのオブジェクトキーには、空白以外の文字を 1 つ以上含める必要があります。すべての空白文字を含む文字列は DeleteObjects リクエストではサポートされていません。
  - DeleteObjects リクエストのオブジェクトキーには、改行 (\n)、タブ (\t) とキャリッジリターン (\r) 文字を除き、Unicode 制御文字を含めることはできません。
- リージョンエンドポイントとゾーンエンドポイント – ディレクトリバケットのバケット管理 API オペレーションは、リージョンエンドポイントを介して利用可能であり、リージョンエンドポイント API オペレーションと呼ばれます。リージョンエンドポイント API オペレーションの例は、CreateBucket や DeleteBucket です。ディレクトリバケットを作成した後、ゾーンエンドポイント API オペレーションを使用して、ディレクトリバケット内のオブジェ

クトをアップロードして管理できます。ゾーンエンドポイント API オペレーションは、ゾーンエンドポイントを通じて実行できます。ゾーン別エンドポイント API オペレーションの例には、PutObject、CopyObject があります。ディレクトリバケットを使用する場合は、すべてのリクエストでリージョンを指定する必要があります。リージョンエンドポイントの場合は、s3express-control.us-west-2.amazonaws.com などのリージョンを指定します。ゾーンエンドポイントの場合は、s3express-usw2-az1.us-west-2.amazonaws.com など、リージョンとアベイラビリティーゾーンの両方を指定します。詳細については、「ディレクトリバケットのリージョンエンドポイントとゾーンエンドポイント」を参照してください。

- マルチパートアップロード – マルチパートアップロードプロセスを使用して、ディレクトリバケットに保存されている大きなオブジェクトをアップロードおよびコピーできます。ただし、ディレクトリバケットに保存されているオブジェクトでマルチパートアップロードプロセスを使用する場合は、以下のような違いがあります。詳細については、「the section called “ディレクトリバケットでのマルチパートアップロードの使用”」を参照してください。
  - オブジェクトの作成日はマルチパートアップロードの完了日となります。
  - マルチパート番号には連続したパート番号を使用する必要があります。連続しないパーツ番号を使用してマルチパートアップロードリクエストを実行しようとすると、Amazon S3 は HTTP 400 (Bad Request) エラーを生成します。
  - マルチパートアップロードを開始するユーザーは、s3express:CreateSession アクセス許可を通じて明示的に AbortMultipartUpload へのアクセス許可が付与されている場合にのみ、マルチパートアップロードリクエストを中止できます。詳細については、「IAM を使用したリージョンエンドポイント API オペレーションの承認」を参照してください。
- ディレクトリバケットを空にする – AWS Command Line Interface (CLI) による s3 rm コマンド、Mountpoint による delete オペレーション、AWS Management Console による空のバケットオプションボタンでは、ディレクトリバケット内の進行中のマルチパートアップロードを削除できません。こうした進行中のマルチパートアップロードを削除するには、ListMultipartUploads オペレーションを使用してバケット内の進行中のマルチパートアップロードを一覧表示し、AbortMultipartUpload オペレーションを使用して進行中のすべてのマルチパートアップロードを中止します。
- AWS Local Zones – Local Zones は、汎用バケットではなくディレクトリバケットでのみサポートされます。
  - 既存のオブジェクトへのデータの追加は、Local Zones に存在するディレクトリバケットではサポートされていません。アベイラビリティーゾーンに存在するディレクトリバケット内の既存のオブジェクトにのみデータを追加できます。
  - S3 ライフサイクルは、Local Zones のディレクトリバケットではサポートされていません。

ディレクトリバケットでサポートされている API オペレーション

ディレクトリバケットは、リージョン (バケットレベル、またはコントロールプレーン) とゾーン (オブジェクトレベル、またはデータプレーン) の両方のエンドポイント API オペレーションをサポートします。詳細については、「ディレクトリバケットのネットワーク」および「エンドポイントとゲートウェイ VPC エンドポイント」を参照してください。

リージョンエンドポイント API オペレーション

ディレクトリバケット用に、以下のリージョンエンドポイント API オペレーションがサポートされています。

- CreateBucket
- DeleteBucket
- DeleteBucketLifecycle
- DeleteBucketPolicy
- GetBucketPolicy
- GetBucketLifecycleConfiguration
- ListDirectoryBuckets
- PutBucketLifecycleConfiguration
- PutBucketPolicy

ゾーンエンドポイント API オペレーション

ディレクトリバケット用として、以下のゾーンエンドポイント API オペレーションがサポートされています。

- CreateSession
- CopyObject
- DeleteObject
- DeleteObjects
- GetObject
- GetObjectAttributes
- HeadBucket

- HeadObject
- ListObjectsV2
- PutObject
- AbortMultipartUpload
- CompleteMultiPartUpload
- CreateMultipartUpload
- ListMultipartUploads
- ListParts
- UploadPart
- UploadPartCopy
- UploadPartCopy
- PutBucketEncryption
- GetBucketEncryption
- DeleteBucketEncryption

ディレクトリバケットでサポートされていない Amazon S3 の機能

以下の Amazon S3 の機能は、ディレクトリバケットでサポートされていません。

- AWS マネージドポリシー
- S3 向け AWS PrivateLink
- MD5 チェックサム
- 多要素認証 (MFA) Delete
- S3 オブジェクトロック
- リクエスタ支払い
- S3 Access Grants
- S3 アクセスポイント
- バケットのタグ
- Amazon CloudWatch のリクエストメトリクス
- S3 イベント通知
- S3 ライフサイクルの移行アクション

- S3 マルチリージョンアクセスポイント
- S3 Object Lambda アクセスポイント
- S3 バージョニング
- S3 インベントリ
- S3 レプリケーション
- オブジェクトタグ
- S3 Select
- サーバーアクセスログ
- 静的ウェブサイトホスティング
- S3 Storage Lens
- S3 Storage Lens グループ
- S3 Transfer Acceleration
- AWS Key Management Service (AWS KMS) キーによる二層式サーバー側の暗号化 (DSSE-KMS)
- 顧客提供のキーを用いたサーバー側の暗号化 (SSE-C)。
- Amazon S3 コンソールで新しいバケットを作成する際に、既存のバケットの設定をコピーするオプション
- 拡張アクセス拒否 (HTTP `403 Forbidden`) エラーメッセージ

ディレクトリバケットのネットワーク

ディレクトリバケットとその内部のオブジェクトにアクセスするには、標準の Amazon S3 エンドポイントとは異なるリージョン API エンドポイントとゾーン API エンドポイントを使用します。使用する S3 API オペレーションに応じて、ゾーンエンドポイントまたはリージョンエンドポイントのいずれかが必要です。エンドポイント別の API オペレーションの全リストについては、「ディレクトリバケットの違い」を参照してください。

ゲートウェイ仮想プライベートクラウド (VPC) エンドポイントを通じて、ゾーン API オペレーションとリージョン API オペレーションの両方にアクセスできます。

次のトピックでは、ゲートウェイ VPC エンドポイントを使用して S3 Express One Zone にアクセスするためのネットワーク要件について説明します。

トピック

- エンドポイント
- VPC ゲートウェイエンドポイントの設定

エンドポイント

ゲートウェイ VPC エンドポイントを使用して、VPC からディレクトリバケットとその内部のオブジェクトにアクセスできます。ディレクトリバケットでは、リージョン API エンドポイントとゾーン API エンドポイントを使用します。使用する Amazon S3 API オペレーションに応じて、リージョンゾーンエンドポイントまたはゾーンエンドポイントのいずれかが必要です。ゲートウェイエンドポイントは追加料金なしで使用できます。

バケットレベル (またはコントロールプレーン) API オペレーションは、リージョンエンドポイントを通じて利用でき、リージョンエンドポイント API オペレーションと呼ばれます。リージョンエンドポイント API オペレーションの例には、`CreateBucket`、`DeleteBucket` があります。ディレクトリバケットを作成する場合は、ディレクトリバケットを作成する先の単一のゾーン (アベイラビリティーゾーンまたは Local Zone) を選択します。ディレクトリバケットを作成した後、ゾーンエンドポイント API オペレーションを使用して、ディレクトリバケット内のオブジェクトをアップロードして管理できます。

オブジェクトレベル (またはデータプレーン) の API オペレーションは、ゾーンエンドポイントを通じて利用でき、ゾーンエンドポイント API オペレーションと呼ばれます。ゾーン別エンドポイント API オペレーションの例には、`CreateSession`、`PutObject` があります。

アベイラビリティーゾーンのディレクトリバケットをサポートするエンドポイントおよび場所の詳細については、「アベイラビリティーゾーンのディレクトリバケットのエンドポイント」を参照してください。

Local Zones のディレクトリバケットをサポートするエンドポイントおよび場所の詳細については、「ローカルゾーンのアカウントを有効にする」を参照してください。

VPC ゲートウェイエンドポイントの設定

アベイラビリティーゾーンのディレクトリバケットにアクセスするためのゲートウェイ VPC エンドポイントを設定するには、「the section called “VPC ゲートウェイエンドポイントの設定”」を参照してください。

Local Zones のディレクトリバケットにアクセスするためのゲートウェイ VPC エンドポイントを設定するには、「VPC からのプライベート接続」を参照してください。

ディレクトリバケットの命名規則

Amazon S3 でディレクトリバケットを作成する場合、次のバケット命名規則が適用されます。汎用バケットの命名規則の詳細については、「汎用バケットの命名規則」を参照してください。

ディレクトリバケット名は、ユーザーが指定するベース名と、バケットの配置先である AWS ゾーン (アベイラビリティーゾーンまたは Local Zone) の ID と `--x-s3` を含むサフィックスで構成されます。*`zone-id`* は、アベイラビリティーゾーンまたは Local Zone の ID にすることができます。

```
base-name--zoneid--x-s3
```

例えば、次のディレクトリバケット名にはアベイラビリティーゾーン ID `usw2-az1` が含まれています。

```
bucket-base-name--usw2-az1--x-s3
```

> **Note**
>
> コンソールを使用してディレクトリバケットを作成すると、指定したベース名にサフィックスが自動的に追加されます。このサフィックスには、選択したゾーン (アベイラビリティーゾーンまたは Local Zone) の Zone ID が含まれています。
> API を使用してディレクトリバケットを作成する場合は、ゾーン ID を含む完全なサフィックスをリクエストで指定する必要があります。ゾーン ID のリストについては、「エンドポイント」を参照してください。

ディレクトリバケットの命名には、次のルールが適用されます。

- 選択したゾーン (AWS アベイラビリティーゾーンまたは AWS Local Zone) 内で一意である必要があります。
- 名前は、サフィックスを含め 3 文字 (最短) から 63 文字 (最長) の長さでなければなりません。
- 小文字の英文字、数字、およびハイフン (-) で構成されていること。
- 文字や数字で始まり、文字や数字で終わります。
- `--`*`zone-id`*`--x-s3` のサフィックスを含める必要があります。
- バケット名のプレフィックスは `xn--` で始まってはいけません。

- バケット名のプレフィックスは `sthree-` で始まってはいけません。
- バケット名のプレフィックスは `sthree-configurator` で始まってはいけません。
- バケット名のプレフィックスは `amzn-s3-demo-` で始まってはいけません。
- バケット名のサフィックスは `-s3alias` で終わってはいけません。このサフィックスは、アクセスポイントのエイリアス名用に予約されています。詳細については、「汎用バケットのアクセスポイントのエイリアス」を参照してください。
- バケット名のサフィックスは `--ol-s3` で終わってはいけません。このサフィックスは、Object Lambda アクセスポイントのエイリアス名用に予約されています。詳細については、「S3 バケット Object Lambda アクセスポイントでのバケット形式のエイリアスの使用方法」を参照してください。
- バケット名のサフィックスは `.mrap` で終わってはいけません。このサフィックスは、マルチリージョンアクセスポイント名用に予約されています。詳細については、「Amazon S3 マルチリージョンアクセスポイントの命名規則」を参照してください。

ディレクトリバケットのプロパティの表示

Amazon S3 コンソールを使用して、Amazon S3 ディレクトリバケットのプロパティを表示および設定できます。詳細については、「ディレクトリバケットの使用」を参照してください。

S3 コンソールの使用

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 左のナビゲーションペインで、[ディレクトリバケット] を選択します。
3. [ディレクトリバケット] リストで、プロパティを確認するバケットの名前を選択します。
4. [プロパティ] タブを選択します。
5. [プロパティ] タブでは、バケットの次のプロパティを確認できます。

    - [ディレクトリバケットの概要] – バケットの AWS リージョン、ゾーン (アベイラビリティーゾーンまたは Local Zone)、Amazon リソースネーム (ARN)、作成日を確認できます。
    - サーバー側の暗号化設定 – Amazon S3 は、すべての S3 バケットの暗号化の基本レベルとして、Amazon S3 マネージドキー (SSE-S3) を使用したサーバー側の暗号化を適用します。Amazon S3 は、ディスクに保存する前にオブジェクトを暗号化し、ダウンロード時にオブジェクトを復号化します。詳細については、「ディレクトリバケットのデフォルト暗号化の設定とモニタリング」を参照してください。

ディレクトリバケットでサポートされている機能の詳細については、「ディレクトリバケットの作成と使用」を参照してください。

ディレクトリバケットポリシーの管理

Amazon S3 コンソール、AWS SDK、AWS CLI を使用して、Amazon S3 ディレクトリバケットのバケットポリシーを追加、削除、更新、表示できます。詳細については、以下のトピックを参照してください。サポートされている AWS Identity and Access Management (IAM) アクションの詳細については、「IAM を使用したリージョンエンドポイント API オペレーションの承認」を参照してください。ディレクトリバケットのバケット ポリシーの例については、「ディレクトリバケットのバケットポリシーの例」を参照してください。

トピック

- バケットポリシーの追加
- バケットポリシーの表示
- バケットポリシーを削除する

バケットポリシーの追加

バケットポリシーをディレクトリバケットに追加するには、Amazon S3 コンソール、AWS SDK、または AWS CLI を使用できます。

S3 コンソールの使用

バケットポリシーを作成または編集するには

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 左のナビゲーションペインで、[ディレクトリバケット] を選択します。
3. [ディレクトリバケット] リストで、ポリシーを追加するバケットの名前を選択します。
4. [アクセス許可] タブを選択します。
5. [バケットポリシー] で [編集] を選択します。[バケットポリシーを編集] ページが表示されます。
6. ポリシーを自動的に生成するには、[Policy Generator] を選択します。

   [Policy Generator] を選択すると、新しいウィンドウで AWS Policy Generator が開きます。

AWS Policy Generator を使用しない場合は、[ポリシー] セクションで JSON ステートメントを追加または編集できます。

a. [Select Type of Policy] (ポリシーの種類の選択) の [AWS Policy Generator] ページで、[S3 Bucket Policy] (S3 バケットポリシー)を選択します。

b. 提供されたフィールドに情報を入力してステートメントを追加し、ステートメントの追加を選択します。このステップを、追加するステートメントの数だけ繰り返します。ポリシーステートメントの詳細については、IAM ユーザーガイドの IAM JSON ポリシーのエレメントのリファレンスを参照してください。

> **Note**
>
> わかりやすいように、[バケットポリシーの編集] ページでは、現在のバケットの [バケット ARN] (Amazon リソースネーム) が [ポリシー] テキストフィールドの上に表示されます。この ARN をコピーして、AWSポリシージェネレータのステートメントで使用できます。

c. ステートメントの追加が完了したら、ポリシーの生成を選択します。

d. 生成されたポリシーテキストをコピーし、[閉じる] を選択すると、Amazon S3 コンソールのバケットポリシーの編集ページに戻ります。

7. [Policy] (ポリシー) ボックスで、既存のポリシーを編集するか、AWS Policy Generator からバケットポリシーを貼り付けます。ポリシーを保存する前に、セキュリティ警告、エラー、一般的な警告、および提案を解決してください。

> **Note**
>
> バケットポリシーのサイズは 20 KB に制限されています。

8. [Save changes] (変更の保存) を選択すると、[Permissions] (アクセス許可) タブへ戻ります。

AWS SDK の使用

SDK for Java 2.x

Example

`PutBucketPolicy` AWS SDK for Java 2.x

```
public static void setBucketPolicy(S3Client s3Client, String bucketName, String
 policyText) {

      //sample policy text
      /**
       * policy_statement = {
        *         'Version': '2012-10-17',
        *         'Statement': [
        *             {
        *                 'Sid': 'AdminPolicy',
        *                 'Effect': 'Allow',
        *                 'Principal': {
        *                     "AWS": "111122223333"
        *                 },
        *                 'Action': 's3express:*',
        *                 'Resource':
 'arn:aws:s3express:region:111122223333:bucket/bucket-base-name--zone-id--x-s3'
        *             }
        *         ]
        *     }
        */
        System.out.println("Setting policy:");
        System.out.println("----");
        System.out.println(policyText);
        System.out.println("----");
        System.out.format("On Amazon S3 bucket: \"%s\"\n", bucketName);

        try {
            PutBucketPolicyRequest policyReq = PutBucketPolicyRequest.builder()
                    .bucket(bucketName)
                    .policy(policyText)
                    .build();
            s3Client.putBucketPolicy(policyReq);
            System.out.println("Done!");
        }

        catch (S3Exception e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
    }
```

AWS CLI を使用する場合

この例では、AWS CLI を使用してバケットポリシーをディレクトリバケットに追加する方法を示します。このコマンドを使用する際は、*###############*を独自の情報に置き換えます。

```
aws s3api put-bucket-policy --bucket bucket-base-name--zone-id--x-s3 --policy file://
bucket_policy.json
```

bucket_policy.json:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AdminPolicy",
            "Effect": "Allow",
            "Principal": {
                "AWS": "111122223333"
            },
            "Action": "s3express*",
            "Resource": "arn:aws:s3express:us-west-2:111122223333:bucket/amzn-s3-demo-
bucket--usw2-az1--x-s3"
        }
    ]
}
```

詳細については、「AWS Command Line Interface」の「put-bucket-policy」を参照してください。

バケットポリシーの表示

ディレクトリバケットのバケットポリシーを表示するには、次の例を使用します。

AWS CLI を使用する場合

この例では、AWS CLI を使用してディレクトリバケットにアタッチされたバケットポリシーを表示する方法を示します。このコマンドを使用する際は、*###############*を独自の情報に置き換えます。

```
aws s3api get-bucket-policy --bucket bucket-base-name--zone-id--x-s3
```

詳細については、「AWS Command Line Interface」の「get-bucket-policy」を参照してください。

バケットポリシーを削除する

ディレクトリバケットのバケットポリシーを削除するには、次の例を使用します。

AWS SDK の使用

SDK for Java 2.x

Example

DeleteBucketPolicy AWS SDK for Java 2.x

```
public static void deleteBucketPolicy(S3Client s3Client, String bucketName) {
      try {
          DeleteBucketPolicyRequest deleteBucketPolicyRequest =
 DeleteBucketPolicyRequest
                  .builder()
                  .bucket(bucketName)
                  .build()
          s3Client.deleteBucketPolicy(deleteBucketPolicyRequest);
          System.out.println("Successfully deleted bucket policy");
      }

      catch (S3Exception e) {
          System.err.println(e.awsErrorDetails().errorMessage());
          System.exit(1);
      }
```

AWS CLI を使用する場合

この例では、AWS CLI を使用してディレクトリバケットのバケットポリシーを削除する方法を示します。このコマンドを使用する際は、*###############*を独自の情報に置き換えます。

```
aws s3api delete-bucket-policy --bucket bucket-base-name--zone-id--x-s3
```

詳細については、「AWS Command Line Interface」の「delete-bucket-policy」を参照してください。

ディレクトリバケットを空にする

Amazon S3 コンソールを使用してディレクトリバケットを空にできます。汎用バケットの詳細については、「ディレクトリバケットの使用」を参照してください。

ディレクトリバケットを空にする前に、次の点に注意します。

- ディレクトリバケットを空にすると、すべてのオブジェクトが削除されます。ただし、ディレクトリバケットは保持されます。
- ディレクトリバケットを空にすると、空にするアクションを元に戻すことはできません。
- ディレクトリバケットを空にするアクションの進行中にディレクトリバケットに追加されたオブジェクトは削除される可能性があります。

バケットも削除する場合は、次の点に注意してください。

- バケット自体を削除する前に、ディレクトリバケット内のすべてのオブジェクトを削除する必要があります。
- ディレクトリバケット内で進行中のマルチパートアップロードは、バケット自体を削除する前に中止する必要があります。

> **Note**
>
> AWS Command Line Interface (CLI) による `s3 rm` コマンド、Mountpoint による `delete` オペレーション、AWS Management Console による空のバケットオプションボタンでは、ディレクトリバケット内の進行中のマルチパートアップロードを削除できません。こうした進行中のマルチパートアップロードを削除するには、`ListMultipartUploads` オペレーションを使用してバケット内の進行中のマルチパートアップロードを一覧表示し、`AbortMultipartUpload` オペレーションを使用して進行中のすべてのマルチパートアップロードを中止します。

ディレクトリバケットを削除にする方法については、「ディレクトリバケットの削除」を参照してください。進行中のマルチパートアップロードを中止する方法については、「the section called “マルチパートアップロードの中止”」を参照してください。

汎用バケットを空にする方法については、「汎用バケットを空にする」を参照してください。

S3 コンソールの使用

ディレクトリバケットを空にするには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[ディレクトリバケット] を選択します。
3. 空にするバケットの名前の横にあるオプションボタンを選択し、[空にする] を選択します。
4. [バケットを空にする] ページで、テキストフィールドに **`permanently delete`** を入力することでバケットを空にすることを確定し、[空にする] を選択します。
5. [バケットを空にする: ステータス] ページで、バケットを空にするプロセスの進行状況をモニタリングします。

ディレクトリバケットの削除

削除できるのは空の Amazon S3 ディレクトリバケットのみです。ディレクトリバケットを削除する前に、バケット内のすべてのオブジェクトを削除し、進行中のすべてのマルチパートアップロードを中止する必要があります。

ディレクトリバケットがアクセスポイントにアタッチされている場合は、まずアクセスポイントを削除する必要があります。詳細については、「ディレクトリバケットのアクセスポイントを削除する」を参照してください。

ディレクトリバケットを空にする方法については、「ディレクトリバケットを空にする」を参照してください。進行中のマルチパートアップロードを中止する方法については、「the section called “マルチパートアップロードの中止”」を参照してください。

汎用バケットを削除する方法については、「汎用バケットの削除」を参照してください。

S3 コンソールの使用

ディレクトリバケットを空にして進行中のすべてのマルチパートアップロードを中止した後に、バケットを削除できます。

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[ディレクトリバケット] を選択します。

3. [ディレクトリバケット] リストで、削除するバケット名の横にあるオプションボタンを選択します。
4. [削除] を選択します。
5. [バケットの削除] ページで、テキストフィールドにバケット名を入力して、バケットの削除を確定します。

> **Important**
>
> ディレクトリバケットを削除すると、元に戻すことはできません。

6. バケットを削除するには、[バケットの削除] をクリックします。

AWS SDK の使用

次の例では、AWS SDK for Java 2.x と AWS SDK for Python (Boto3) を使用してディレクトリバケットを削除します。

SDK for Java 2.x

Example

```
public static void deleteBucket(S3Client s3Client, String bucketName) {

    try {
        DeleteBucketRequest del = DeleteBucketRequest.builder()
                .bucket(bucketName)
                .build();
        s3Client.deleteBucket(del);
        System.out.println("Bucket " + bucketName + " has been deleted");
    }
    catch (S3Exception e) {
        System.err.println(e.awsErrorDetails().errorMessage());
        System.exit(1);
    }
}
```

SDK for Python

Example

```
import logging
```

```
import boto3
from botocore.exceptions import ClientError

def delete_bucket(s3_client, bucket_name):
    '''
    Delete a directory bucket in a specified Region

    :param s3_client: boto3 S3 client
    :param bucket_name: Bucket to delete; for example, 'doc-example-bucket--usw2-
az1--x-s3'
    :return: True if bucket is deleted, else False
    '''

    try:
        s3_client.delete_bucket(Bucket = bucket_name)
    except ClientError as e:
        logging.error(e)
        return False
    return True

if __name__ == '__main__':
    bucket_name = 'BUCKET_NAME'
    region = 'us-west-2'
    s3_client = boto3.client('s3', region_name = region)
```

AWS CLI を使用する場合

この例では、AWS CLI を使用してディレクトリバケットを削除する方法を示します。このコマンドを使用する際は、*##############*を独自の情報に置き換えます。

```
aws s3api delete-bucket --bucket bucket-base-name--zone-id--x-s3 --region us-west-2
```

詳細については、「AWS Command Line Interface」の「delete-bucket」を参照してください。

ディレクトリバケットの一覧表示

次の例は、AWS Management Console、AWS SDK、AWS CLI を使用してディレクトリバケットを一覧表示する方法を示しています。

S3 コンソールの使用

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. ページ上部にあるナビゲーションバーで、現在表示されている AWS リージョン の名前をクリックします。次に、ディレクトリバケットの一覧を表示するリージョンを選択します。
3. 左のナビゲーションペインで、[ディレクトリバケット] を選択します。ディレクトリバケットの一覧が表示されます。バケット内のオブジェクト、バケットプロパティ、バケットのアクセス許可、メトリクス、バケットに関連付けられたアクセスポイントを表示するか、バケットを管理するには、バケット名を選択します。

AWS SDK の使用

SDK for Java 2.x

Example

次の例では、AWS SDK for Java 2.x を使用してディレクトリバケットを一覧表示します。

```
public static void listBuckets(S3Client s3Client) {
       try {
           ListDirectoryBucketsRequest listDirectoryBucketsRequest =
ListDirectoryBucketsRequest.builder().build();
           ListDirectoryBucketsResponse response =
s3Client.listDirectoryBuckets(listDirectoryBucketsRequest);
           if (response.hasBuckets()) {
               for (Bucket bucket: response.buckets()) {
                   System.out.println(bucket.name());
                   System.out.println(bucket.creationDate());
               }
           }
       }

       catch (S3Exception e) {
           System.err.println(e.awsErrorDetails().errorMessage());
           System.exit(1);
       }
   }
```

SDK for Python

Example

次の例では、AWS SDK for Python (Boto3) を使用してディレクトリバケットを一覧表示します。

```
import logging
import boto3
from botocore.exceptions import ClientError

def list_directory_buckets(s3_client):
'''
Prints a list of all directory buckets in a Region

:param s3_client: boto3 S3 client
:return: True if there are buckets in the Region, else False
'''
try:
    response = s3_client.list_directory_buckets()
    for bucket in response['Buckets']:
        print (bucket['Name'])
except ClientError as e:
    logging.error(e)
    return False
return True


if __name__ == '__main__':
    region = 'us-east-1'
    s3_client = boto3.client('s3', region_name = region)
    list_directory_buckets(s3_client)
```

SDK for .NET

Example

次の例では、AWS SDK for .NET を使用してディレクトリバケットを一覧表示します。

```
var listDirectoryBuckets = await amazonS3Client.ListDirectoryBucketsAsync(new
 ListDirectoryBucketsRequest
{
  MaxDirectoryBuckets = 10
```

```
    }).ConfigureAwait(false);
```

SDK for PHP

Example

次の例では、AWS SDK for PHP を使用してディレクトリバケットを一覧表示します。

```
require 'vendor/autoload.php';

$s3Client = new S3Client([
    'region'      => 'us-east-1',
]);
$result = $s3Client->listDirectoryBuckets();
```

SDK for Ruby

Example

次の例では、AWS SDK for Ruby を使用してディレクトリバケットを一覧表示します。

```
s3 = Aws::S3::Client.new(region:'us-west-1')
s3.list_directory_buckets
```

AWS CLI を使用する場合

次の `list-directory-buckets` コマンド例は、AWS CLI を使用して *us-east-1* リージョン内のディレクトリバケットをリスト表示する方法を示しています。このコマンドを実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3api list-directory-buckets --region us-east-1
```

詳細については、AWS CLI コマンドリファレンスの「list-directory-buckets」を参照してください。

ディレクトリバケットにアクセスできるかどうかの判断

以下の AWS SDK の例は、HeadBucket API オペレーションを使用して、Amazon S3 ディレクトリバケットが存在し、そのバケットにアクセスする許可があるかどうかを調べる方法を示しています。

AWS SDK の使用

次の AWS SDK for Java 2.x の例は、バケットが存在し、そのバケットにアクセスする許可があるかどうかを調べる方法を示しています。

SDK for Java 2.x

Example

AWS SDK for Java 2.x

```
public static void headBucket(S3Client s3Client, String bucketName) {
   try {
        HeadBucketRequest headBucketRequest = HeadBucketRequest
                .builder()
                .bucket(bucketName)
                .build();
        s3Client.headBucket(headBucketRequest);
        System.out.format("Amazon S3 bucket: \"%s\" found.", bucketName);
   }

   catch (S3Exception e) {
       System.err.println(e.awsErrorDetails().errorMessage());
       System.exit(1);
   }
}
```

AWS CLI を使用する場合

次の head-bucket コマンド例は、AWS CLI を使用して、ディレクトリバケットが存在するか、ユーザーにそのディレクトリバケットへのアクセス許可があるかどうかを判断する方法を示しています。このコマンドを実行するには、ユーザー入力プレースホルダーをユーザー自身の情報に置き換えます。

```
aws s3api head-bucket --bucket bucket-base-name--zone-id--x-s3
```

詳細については、AWS CLI コマンドリファレンスの「head-bucket」を参照してください。

ディレクトリバケットでのオブジェクトの使用

Amazon S3 ディレクトリバケット作成後、Amazon S3 コンソール、AWS Command Line Interface (AWS CLI)、AWS SDK を使用してオブジェクトを操作できます。

ディレクトリバケット内のオブジェクトの一括オペレーション、インポート、アップロード、コピー、削除、ダウンロードを実行する方法の詳細については、以下のトピックを参照してください。

トピック

- ディレクトリバケットへのオブジェクトのインポート
- ディレクトリバケットの S3 ライフサイクルの使用
- ディレクトリバケットでのバッチオペレーションの使用
- ディレクトリバケット内のオブジェクトへのデータの追加
- ディレクトリバケットへのオブジェクトのアップロード
- ディレクトリバケットから、またはディレクトリバケットへのオブジェクトのコピー
- ディレクトリバケットのオブジェクトの削除
- ディレクトリバケットからのオブジェクトのダウンロード
- オブジェクトディレクトリバケットを共有するための署名付き URL の生成
- ディレクトリバケットからのオブジェクトメタデータの取得
- ディレクトリバケットからのオブジェクトの一覧表示

ディレクトリバケットへのオブジェクトのインポート

Amazon S3 でディレクトリバケットを作成した後、インポートアクションを使用して新しいバケットにデータを入力できます。インポートは、汎用バケットからディレクトリバケットにオブジェクトをコピーする S3 バッチオペレーションジョブを作成するための効率的な方法です。

> **Note**
>
> インポートジョブには、次の制限が適用されます。
>
> - ソースバケットと送信先バケットの両方が同じ AWS リージョン にあり、同じアカウント内にある必要があります。
> - ソースバケットをディレクトリバケットにすることはできません。

- 5 GB を超えるオブジェクトはサポートされていないため、コピーオペレーションから除外されます。
- Glacier Flexible Retrieval、Glacier Deep Archive、Intelligent-Tiering Archive Access 階層、Intelligent-Tiering Deep Archive 階層などのストレージクラス内のオブジェクトは、インポート前に復元する必要があります。
- MD5 チェックサムアルゴリズムを使用してインポートされたオブジェクトは、CRC32 チェックサムを使用するように変換されます。
- インポートされたオブジェクトは、一般的な目的のバケットで使用されるストレージクラスとは別の料金制の Express One Zone ストレージクラスを使用します。多数のオブジェクトをインポートする場合は、このコストの違いを考慮する必要があります。

インポートジョブを設定する際、既存のオブジェクトのコピー元となるソースバケットまたはプレフィックスを指定します。また、ソースオブジェクトにアクセスするための許可を持つ AWS Identity and Access Management (IAM) ロールも指定します。その後 Amazon S3 は、オブジェクトをコピーして、適切なストレージクラスとチェックサム設定を自動的に適用するバッチオペレーションジョブを開始します。

インポートジョブを設定するには、Amazon S3 コンソールを使用します。

Amazon S3 コンソールの使用

オブジェクトをディレクトリバケットにインポートするには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで [バケット] を選択してから、[ディレクトリバケット] タブをクリックします。オブジェクトをインポートする先のディレクトリバケットの隣にあるオプションボタンをクリックします。
3. [インポート] を選択します。
4. [ソース] には、インポートするオブジェクトを含む汎用バケット (またはプレフィックスを含むバケットパス) を入力します。リストから既存の汎用バケットを選択するには、[Browse S3] をクリックします。
5. [ソースオブジェクトにアクセスおよびコピーするための許可] で、次のいずれかを行い、ソースオブジェクトのインポートに必要なアクセス許可を持つ IAM ロールを指定します。

- Amazon S3 がユーザーに代わって新しい IAM ロールを作成できるようにするには、[新しい IAM ロールを作成] を選択します。
- リストから既存の IAM ロールを選択するには、[既存の IAM ロールから選択] をクリックします。
- Amazon リソースネーム (ARN) を入力して既存の IAM ロールを指定するには、[IAM ロールの ARN の入力] をクリックして、対応するフィールドに ARN を入力します。

6. [送信先] セクションと [コピーされたオブジェクトの設定] セクションに表示された情報を確認します。[送信先] セクションの情報が適切であれば、[インポート] をクリックしてコピージョブを開始します。

   Amazon S3 コンソールでは、新しいジョブのステータスが [バッチオペレーション] ページに表示されます。ジョブの詳細については、ジョブ名の横にあるオプションボタンを選択して、[アクション] メニューで [詳細を表示] を選択します。オブジェクトのインポート先となるディレクトリバケットを開くには、[インポート先を表示] を選択します。

ディレクトリバケットの S3 ライフサイクルの使用

S3 ライフサイクルは、ユーザーに代わって期限切れのオブジェクトを削除することで、S3 Express One Zone のオブジェクトをディレクトリバケットにコスト効率良く保存するのに役立ちます。オブジェクトのライフサイクルを管理するには、ディレクトリバケットの S3 ライフサイクル設定を作成します。S3 ライフサイクル設定は、Amazon S3 がオブジェクトのグループに適用するアクションを定義するルールのセットです。ディレクトリバケットに Amazon S3 ライフサイクル設定をセットアップするには、AWS コマンドラインインターフェイス (AWS CLI)、AWS SDK、Amazon S3 REST API、AWS CloudFormation を使用できます。

S3 ライフサイクル設定では、ルールを使用して、Amazon S3 がオブジェクトに実行するアクションを定義します。ディレクトリバケットに保存されているオブジェクトの場合、古くなったオブジェクトを期限切れにするライフサイクルルールを作成できます。また、ディレクトリバケット内の不完全なマルチパートアップロードを毎日削除するライフサイクルルールを作成することもできます。

ライフサイクル設定をバケットに追加すると、設定ルールは既存のオブジェクトとそれ以降に追加されるオブジェクトの両方に適用されます。例えば、ライフサイクル設定ルールを今日追加し、特定のプレフィックスが付いたオブジェクトを作成から 30 日後に期限切れにするように設定すると、S3 は、30 日を超えた既存のオブジェクトのうち、指定したプレフィックスが付いたものを削除キューに追加します。

ディレクトリバケットの S3 ライフサイクルの違い

ディレクトリバケット内のオブジェクトの場合、オブジェクトを期限切れにし、不完全なマルチパートアップロードを削除するライフサイクルルールを作成できます。ただし、ディレクトリバケットの S3 ライフサイクルは、ストレージクラス間の移行アクションをサポートしていません。

CreateSession

ライフサイクルは、パブリックの `DeleteObject` および `DeleteObjects` API オペレーションを使用して、ディレクトリバケット内のオブジェクトを期限切れにします。これらの API オペレーションを使用するために、S3 ライフサイクルは `CreateSession` API を使用してディレクトリバケット内のオブジェクトにアクセスするための一時的なセキュリティ認証情報を設定します。詳細については、「Amazon S3 API リファレンスの `CreateSession`」を参照してください。

ライフサイクルプリンシパルに対して削除アクセス許可を拒否するアクティブなポリシーがある場合、S3 ライフサイクルがユーザーに代わってオブジェクトを削除することを許可できなくなります。

バケットポリシーを使用して S3 ライフサイクルサービスプリンシパルにアクセス許可を付与する

次のバケットポリシーでは、デフォルトの `ReadWrite` セッションで CreateSession コールを許可するアクセス許可を付与し、ライフサイクルサービスプリンシパルを許可します。

Example – デフォルトの **`ReadWrite`** セッションでの **`CreateSession`** 呼び出しを許可するバケットポリシー

```
{
  "Version":"2008-10-17",
  "Statement":[
     {
        "Effect":"Allow",
        "Principal": {
           "Service":"lifecycle.s3.amazonaws.com"
         },
         "Action":"s3express:CreateSession",
         "Condition": {
            "StringEquals": {
               "s3express:SessionMode": "ReadWrite"
             }
          },
```

```
            "Resource":"arn:aws:s3express:us-east-2:412345678921:bucket/amzn-s3-demo-
bucket--use2-az2--x-s3"
        }
    ]
}
```

ライフサイクルルールのモニタリング

ディレクトリバケットに保存されているオブジェクトの場合、S3 ライフサイクルは AWS CloudTrail 管理とデータイベントのログを生成します。詳細については、「S3 Express One Zone の CloudTrail ログファイルの例」を参照してください。

ライフサイクル設定の作成および S3 ライフサイクル関連の問題のトラブルシューティングの詳細については、以下のトピックを参照してください。

トピック

- ディレクトリバケットのライフサイクル設定の作成と管理
- ディレクトリバケットの S3 ライフサイクルに関する問題のトラブルシューティング

ディレクトリバケットのライフサイクル設定の作成と管理

ディレクトリバケットのライフサイクル設定は、AWS Command Line Interface (AWS CLI)、AWS SDK、REST API を使用して作成できます。

AWS CLI の使用

次の AWS CLI コマンドを使用して、S3 ライフサイクル設定を管理できます。

- `put-bucket-lifecycle-configuration`
- `get-bucket-lifecycle-configuration`
- `delete-bucket-lifecycle`

AWS CLI の設定の手順については、「Amazon S3 API リファレンス」の「AWS CLI を使用した Amazon S3 での開発」を参照してください。

Amazon S3 ライフサイクル設定は XML ファイルである点に注意してください。ただし、AWS CLI を使用する場合、XML 形式を指定することはできません。代わりに JSON 形式を指定する必要があ

ります。XML ライフサイクル設定の例と、AWS CLI コマンドで指定できる同等の JSON の設定は、次のとおりです。

次の AWS CLI の例では、ディレクトリバケットにライフサイクル設定ポリシーを配置します。このポリシーでは、フラグ付きのプレフィックス (myprefix) を持ち、定義されたオブジェクトサイズであるすべてのオブジェクトが 7 日後に期限切れになることを指定します。この例を使用するには、各*##############*を独自の情報に置き換えます。

ライフサイクル設定ポリシーを JSON ファイルに保存します。この例では、ファイルの名前を lifecycle1.json とします。

Example

JSON

```
{
    "Rules": [
        {
        "Expiration": {
            "Days": 7
        },
        "ID": "Lifecycle expiration rule",
        "Filter": {
            "And": {
                "Prefix": "myprefix/",
                "ObjectSizeGreaterThan": 500,
                "ObjectSizeLessThan": 64000
            }
        },
        "Status": "Enabled"
    }
    ]
}
```

put-bucket-lifecycle-configuration CLI コマンドの一部として JSON ファイルを送信します。このコマンドを使用するには、各*##############*を独自の情報に置き換えます。

```
aws s3api put-bucket-lifecycle-configuration --region us-west-2 --profile default
 --bucket amzn-s3-demo-bucket--usw2-az1--x-s3 --lifecycle-configuration file://lc-
policy.json --checksum-algorithm crc32c
```

Example

XML

```
<LifecycleConfiguration>
    <Rule>
        <ID>Lifecycle expiration rule</ID>
        <Filter>
            <And>
                <Prefix>myprefix/</Prefix>
                <ObjectSizeGreaterThan>500</ObjectSizeGreaterThan>
                <ObjectSizeLessThan>64000</ObjectSizeLessThan>
            </And>
        </Filter>
        <Status>Enabled</Status>
        <Expiration>
             <Days>7</Days>
        </Expiration>
    </Rule>
</LifecycleConfiguration>
```

AWS SDK の使用

SDK for Java

Example

```
import
 software.amazon.awssdk.services.s3.model.PutBucketLifecycleConfigurationRequest;
import
 software.amazon.awssdk.services.s3.model.PutBucketLifecycleConfigurationResponse;
import software.amazon.awssdk.services.s3.model.ChecksumAlgorithm;
import software.amazon.awssdk.services.s3.model.BucketLifecycleConfiguration;
import software.amazon.awssdk.services.s3.model.LifecycleRule;
import software.amazon.awssdk.services.s3.model.LifecycleRuleFilter;
import software.amazon.awssdk.services.s3.model.LifecycleExpiration;
import software.amazon.awssdk.services.s3.model.LifecycleRuleAndOperator;
import
 software.amazon.awssdk.services.s3.model.GetBucketLifecycleConfigurationResponse;
import
 software.amazon.awssdk.services.s3.model.GetBucketLifecycleConfigurationRequest;
import software.amazon.awssdk.services.s3.model.DeleteBucketLifecycleRequest;
```

```
import software.amazon.awssdk.services.s3.model.DeleteBucketLifecycleResponse;
import software.amazon.awssdk.services.s3.model.AbortIncompleteMultipartUpload;

// PUT a Lifecycle policy
LifecycleRuleFilter objectExpirationFilter =
 LifecycleRuleFilter.builder().and(LifecycleRuleAndOperator.builder().prefix("dir1/").object
LifecycleRuleFilter mpuExpirationFilter =
 LifecycleRuleFilter.builder().prefix("dir2/").build();

LifecycleRule objectExpirationRule =
 LifecycleRule.builder().id("lc").filter(objectExpirationFilter).status("Enabled").expiratio
                    .days(10)
                    .build())
                .build();
LifecycleRule mpuExpirationRule = LifecycleRule.builder().id("lc-
mpu").filter(mpuExpirationFilter).status("Enabled").abortIncompleteMultipartUpload(AbortInco
                        .daysAfterInitiation(10)
                        .build())
                .build();

PutBucketLifecycleConfigurationRequest putLifecycleRequest =
 PutBucketLifecycleConfigurationRequest.builder()
                .bucket("amzn-s3-demo-bucket--usw2-az1--x-s3")
                .checksumAlgorithm(ChecksumAlgorithm.CRC32)
                .lifecycleConfiguration(
                        BucketLifecycleConfiguration.builder()
                                .rules(objectExpirationRule, mpuExpirationRule)
                                .build()
                ).build();

PutBucketLifecycleConfigurationResponse resp =
 client.putBucketLifecycleConfiguration(putLifecycleRequest);

// GET the Lifecycle policy
GetBucketLifecycleConfigurationResponse getResp =
 client.getBucketLifecycleConfiguration(GetBucketLifecycleConfigurationRequest.builder().buc
s3-demo-bucket--usw2-az1--x-s3").build());

// DELETE the Lifecycle policy
DeleteBucketLifecycleResponse delResp =
 client.deleteBucketLifecycle(DeleteBucketLifecycleRequest.builder().bucket("amzn-
s3-demo-bucket--usw2-az1--x-s3").build());
```

SDK for Go

Example

```
package main

import (
    "context"
    "log"

    "github.com/aws/aws-sdk-go-v2/aws"
    "github.com/aws/aws-sdk-go-v2/config"
    "github.com/aws/aws-sdk-go-v2/service/s3"
    "github.com/aws/aws-sdk-go-v2/service/s3/types"
)
// PUT a Lifecycle policy
func putBucketLifecycleConfiguration(client *s3.Client, bucketName string ) error {
    lifecycleConfig := &s3.PutBucketLifecycleConfigurationInput{
        Bucket: aws.String(bucketName),
        LifecycleConfiguration: &types.BucketLifecycleConfiguration{
            Rules: []types.LifecycleRule{
                {
                    ID:     aws.String("lc"),
                    Filter: &types.LifecycleRuleFilter{
                        And: &types.LifecycleRuleAndOperator{
                            Prefix: aws.String("foo/"),
                            ObjectSizeGreaterThan: aws.Int64(1000000),
                            ObjectSizeLessThan:    aws.Int64(100000000),
                            },
                        },

                    Status: types.ExpirationStatusEnabled,
                    Expiration: &types.LifecycleExpiration{
                        Days: aws.Int32(int32(1)),
                    },
                },
                {
                    ID:     aws.String("abortmpu"),
                    Filter: &types.LifecycleRuleFilter{
                        Prefix: aws.String("bar/"),
                    },
                    Status: types.ExpirationStatusEnabled,
                    AbortIncompleteMultipartUpload:
 &types.AbortIncompleteMultipartUpload{
```

```
                        DaysAfterInitiation: aws.Int32(int32(5)),
                    },
                },
            },
        },
    }
    _, err := client.PutBucketLifecycleConfiguration(context.Background(),
 lifecycleConfig)
    return err
}
// Get the Lifecycle policy
func getBucketLifecycleConfiguration(client *s3.Client, bucketName string) error {
    getLifecycleConfig := &s3.GetBucketLifecycleConfigurationInput{
        Bucket: aws.String(bucketName),
    }

    resp, err := client.GetBucketLifecycleConfiguration(context.Background(),
 getLifecycleConfig)
    if err != nil {
        return err
    }
    return nil
}
// Delete the Lifecycle policy
func deleteBucketLifecycleConfiguration(client *s3.Client, bucketName string) error
 {
    deleteLifecycleConfig := &s3.DeleteBucketLifecycleInput{
        Bucket: aws.String(bucketName),
    }
    _, err := client.DeleteBucketLifecycle(context.Background(),
 deleteLifecycleConfig)
    return err
}
func main() {
    cfg, err := config.LoadDefaultConfig(context.Background(),
 config.WithRegion("us-west-2")) // Specify your region here
    if err != nil {
        log.Fatalf("unable to load SDK config, %v", err)
    }
    s3Client := s3.NewFromConfig(cfg)
    bucketName := "amzn-s3-demo-bucket--usw2-az1--x-s3"
    putBucketLifecycleConfiguration(s3Client, bucketName)
    getBucketLifecycleConfiguration(s3Client, bucketName)
    deleteBucketLifecycleConfiguration(s3Client, bucketName)
```

```
    getBucketLifecycleConfiguration(s3Client, bucketName)
}
```

SDK for .NET

Example

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Collections.Generic;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class LifecycleTest
    {
        private const string bucketName = "amzn-s3-demo-bucket--usw2-az1--x-s3";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 client;
        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            AddUpdateDeleteLifecycleConfigAsync().Wait();
        }

        private static async Task AddUpdateDeleteLifecycleConfigAsync()
        {
            try
            {
                var lifeCycleConfiguration = new LifecycleConfiguration()
                {
                    Rules = new List <LifecycleRule>
                        {
                            new LifecycleRule
                            {
                                 Id = "delete rule",
                                  Filter = new LifecycleFilter()
                                 {
                                     LifecycleFilterPredicate = new
 LifecyclePrefixPredicate()
```

```
                                    {
                                        Prefix = "projectdocs/"
                                    }
                                },
                                Status = LifecycleRuleStatus.Enabled,
                                Expiration = new LifecycleRuleExpiration()
                                {
                                      Days = 10
                                }
                            }
                        }
                };

                // Add the configuration to the bucket.
                await AddExampleLifecycleConfigAsync(client,
lifeCycleConfiguration);

                // Retrieve an existing configuration.
                lifeCycleConfiguration = await RetrieveLifecycleConfigAsync(client);

                // Add a new rule.
                lifeCycleConfiguration.Rules.Add(new LifecycleRule
                {
                    Id = "mpu abort rule",
                    Filter = new LifecycleFilter()
                    {
                        LifecycleFilterPredicate = new LifecyclePrefixPredicate()
                        {
                            Prefix = "YearlyDocuments/"
                        }
                    },
                    Expiration = new LifecycleRuleExpiration()
                    {
                        Days = 10
                    },
                    AbortIncompleteMultipartUpload = new
LifecycleRuleAbortIncompleteMultipartUpload()
                    {
                        DaysAfterInitiation = 10
                    }
                });

                // Add the configuration to the bucket.
```

```
                await AddExampleLifecycleConfigAsync(client,
lifeCycleConfiguration);

                // Verify that there are now two rules.
                lifeCycleConfiguration = await RetrieveLifecycleConfigAsync(client);
                Console.WriteLine("Expected # of rulest=2; found:{0}",
lifeCycleConfiguration.Rules.Count);

                // Delete the configuration.
                await RemoveLifecycleConfigAsync(client);

                // Retrieve a nonexistent configuration.
                lifeCycleConfiguration = await RetrieveLifecycleConfigAsync(client);

            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered ***. Message:'{0}' when writing
an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
writing an object", e.Message);
            }
        }

        static async Task AddExampleLifecycleConfigAsync(IAmazonS3 client,
LifecycleConfiguration configuration)
        {

            PutLifecycleConfigurationRequest request = new
PutLifecycleConfigurationRequest
            {
                BucketName = bucketName,
                Configuration = configuration
            };
            var response = await client.PutLifecycleConfigurationAsync(request);
        }

        static async Task <LifecycleConfiguration>
RetrieveLifecycleConfigAsync(IAmazonS3 client)
        {
```

```
            GetLifecycleConfigurationRequest request = new
 GetLifecycleConfigurationRequest
            {
                BucketName = bucketName
            };
            var response = await client.GetLifecycleConfigurationAsync(request);
            var configuration = response.Configuration;
            return configuration;
        }

        static async Task RemoveLifecycleConfigAsync(IAmazonS3 client)
        {
            DeleteLifecycleConfigurationRequest request = new
 DeleteLifecycleConfigurationRequest
            {
                BucketName = bucketName
            };
            await client.DeleteLifecycleConfigurationAsync(request);
        }
    }
}
```

SDK for Python

Example

```
import boto3

client = boto3.client("s3", region_name="us-west-2")
bucket_name = 'amzn-s3-demo-bucket--usw2-az1--x-s3'

client.put_bucket_lifecycle_configuration(
    Bucket=bucket_name,
    ChecksumAlgorithm='CRC32',
    LifecycleConfiguration={
        'Rules': [
            {
                'ID': 'lc',
                'Filter': {
                    'And': {
                        'Prefix': 'foo/',
                        'ObjectSizeGreaterThan': 1000000,
                        'ObjectSizeLessThan': 100000000,
```

```
                    }
                },
                'Status': 'Enabled',
                'Expiration': {
                    'Days': 1
                }
            },
            {
                'ID': 'abortmpu',
                'Filter': {
                    'Prefix': 'bar/'
                },
                'Status': 'Enabled',
                'AbortIncompleteMultipartUpload': {
                    'DaysAfterInitiation': 5
                }
            }
        ]
    }
)

result = client.get_bucket_lifecycle_configuration(
    Bucket=bucket_name
)

client.delete_bucket_lifecycle(
    Bucket=bucket_name
)
```

ディレクトリバケットの S3 ライフサイクルに関する問題のトラブルシューティング

トピック

- ライフサイクル設定をセットアップしたが、ディレクトリバケット内のオブジェクトの有効期限が切れていない
- ライフサイクルルールによって実行されたアクションをモニタリングするにはどうすればよいですか？

ライフサイクル設定をセットアップしたが、ディレクトリバケット内のオブジェクトの有効期限が切れていない

ディレクトリバケットの S3 ライフサイクルは、パブリック API を使用して S3 Express One Zone のオブジェクトを削除します。オブジェクトレベルのパブリック API を使用するには、`CreateSession` へのアクセスを許可し、オブジェクトを削除するためのアクセス許可を S3 ライフサイクルに付与する必要があります。削除を拒否するアクティブなポリシーがある場合、S3 ライフサイクルがユーザーに代わってオブジェクトを削除することを許可できなくなります。

削除するオブジェクトが確実に期限切れになるように、バケットポリシーを正しく設定することが重要です。AWS CloudTrail で `CreateSession` API 呼び出しに対する `AccessDenied` 証跡を CloudTrail ログでチェックし、アクセスが拒否されたかどうかを確認できます。CloudTrail ログを確認することは、アクセス問題のトラブルシューティングや、アクセス拒否エラーの根本原因の特定に役立ちます。次に、関連するポリシーを更新することで、誤ったアクセスコントロールを修正できます。

バケットポリシーの設定が正しいことを確認しても、問題が発生する場合は、ライフサイクルルールを見直して、適切なオブジェクトのサブセットに適用されていることを確認してください。

ライフサイクルルールによって実行されたアクションをモニタリングするにはどうすればよいですか？

AWS CloudTrail データイベントログを使用して、ディレクトリバケットで S3 ライフサイクルが実行したアクションをモニタリングできます。詳細については、「CloudTrail ログファイルの例」を参照してください。

ディレクトリバケットでのバッチオペレーションの使用

Amazon S3 バッチオペレーションを使用して、S3 バケットに保存されているオブジェクトに対してオペレーションを実行できます。S3 バッチオペレーションの詳細については、「Amazon S3 オブジェクトに対する大規模なバッチオペレーションの実行」を参照してください。

次のトピックでは、ディレクトリバケットで S3 Express One Zone ストレージクラスに保存されているオブジェクトに保存されているオブジェクトに対するバッチオペレーションの実行について説明します。

トピック

- ディレクトリバケットでのバッチオペレーションの使用
- 主な違い

ディレクトリバケットでのバッチオペレーションの使用

ディレクトリバケットに保存されているオブジェクトに対して Copy オペレーションと Invoke AWS Lambda 関数 オペレーションを実行できます。Copy を使用すると、(1 つのディレクトリバケットから別のディレクトリバケットへ、など) 同じタイプのバケット間でオブジェクトをコピーできます。汎用バケットとディレクトリバケットの間でコピーすることもできます。Invoke AWS Lambda 関数を使用すると、Lambda 関数を使用して、定義したコードを使用してディレクトリバケット内のオブジェクトに対してアクションを実行できます。

オブジェクトのコピー

同じバケット タイプ間、またはディレクトリバケットと汎用バケット間でコピーできます。ディレクトリバケットにコピーするときは、このバケットタイプに適した Amazon リソースネーム (ARN) 形式を使用する必要があります。ディレクトリバケットの ARN 形式は `arn:aws:s3express:`*`region`*`:`*`account-id`*`:bucket/`*`bucket-base-name`*`--x-s3` です。

> **Note**
>
> ソースバケットまたは送信先バケットが AWS Local Zone にある場合、異なる AWS リージョン間でのオブジェクトのコピーはサポートされていません。ソースバケットと送信先バケットは、親 AWS リージョンが同じである必要があります。ソースバケットと送信先バケットは、異なるバケットの場所タイプ (アベイラビリティーゾーンまたは Local Zone) にすることができます。

S3 コンソールの Import アクションを使用して、ディレクトリバケットにデータを入力することもできます。インポートは、汎用バケットからディレクトリバケットにオブジェクトをコピーするバッチオペレーションジョブを作成するための効率的な方法です。汎用バケットからディレクトリバケットへのインポートコピージョブの場合、S3 はマニフェストを自動的に生成します。詳細については、「ディレクトリバケットへのオブジェクトのインポート」と「マニフェストの指定」を参照してください。

Lambda 関数の呼び出し (**`LambdaInvoke`**)

バッチオペレーションを使用してディレクトリバケットで動作する Lambda 関数を呼び出すには、独自の要件があります。例えば、v2 JSON 呼び出しスキーマを使用して Lambda リクエストを構築し、ジョブを作成する際に InvocationSchemaVersion 2.0 を指定する必要があります。詳細については、「AWS Lambda 関数の呼び出し」を参照してください。

主な違い

バッチオペレーションを使用して、S3 Express One Zone ストレージクラスを使用するディレクトリバケットに保存されたオブジェクトに対して一括操作を実行する場合の主な相違点は、次の一覧のとおりです。

- ディレクトリバケットでは、SSE-S3 および AWS Key Management Service (AWS KMS) キーによるサーバー側の暗号化 (SSE-KMS) がサポートされています。ディレクトリバケット (送信元または送信先) でお客様が提供するキーを使用したサーバー側の暗号化 (SSE-C) を設定する `CopyObject` リクエストを行うと、HTTP `400 (Bad Request)` エラーの応答が返されます。

  バケットのデフォルト暗号化では、希望する暗号化設定を使用することをお勧めします。また、`CreateSession` リクエストまたは PUT オブジェクトリクエストでは、バケットのデフォルト暗号化を上書きしないことをお勧めします。その後、新しいオブジェクトは必要な暗号化設定で自動的に暗号化されます。ディレクトリバケットの暗号化の上書き動作、および SSE-KMS を使用してディレクトリバケット内の新しいオブジェクトコピーを暗号化する方法の詳細については、「Specifying server-side encryption with AWS KMS for new object uploads」を参照してください。

  S3 バケットキーは、バッチオペレーションの Copy オペレーションを通じて、汎用バケットからディレクトリバケット、ディレクトリバケットから汎用バケット、またはディレクトリバケット間で SSE-KMS で暗号化されたオブジェクトをコピーする場合は、サポートされません。この場合、KMS で暗号化されたオブジェクトに対してコピーリクエストが実行されるたびに、Amazon S3 は AWS KMS を呼び出します。ディレクトリバケットで SSE-KMS を使用する場合の詳細については、「ディレクトリバケットのデフォルト暗号化の設定とモニタリング」および「ディレクトリバケットでの AWS KMS キーによるサーバー側の暗号化 (SSE-KMS) の使用」を参照してください。
- ディレクトリバケット内のオブジェクトにはタグを付けることができません。指定できるのは空のタグセットのみです。デフォルトでは、バッチオペレーションがタグをコピーします。タグ付きのオブジェクトを汎用バケットからディレクトリバケットにコピーすると、`501 (Not Implemented)` の応答が表示されます。
- S3 Express One Zone では、アップロードまたはダウンロード中にデータを検証するために使用されるチェックサムアルゴリズムを選択するオプションが提供されます。CRC32、CRC32、SHA-1、SHA-256 などのセキュアハッシュアルゴリズム (SHA) や巡回冗長検査 (CRC) データ整合性チェックアルゴリズムのいずれかを選択できます。MD5 ベースのチェックサムは S3 Express One Zone ストレージクラスではサポートされていません。

- デフォルトでは、すべての Amazon S3 バケットで S3 オブジェクト所有者の設定がバケット所有者の強制に指定され、アクセスコントロールリスト (ACL) は無効になります。ディレクトリバケットの場合、この設定は変更できません。オブジェクトは、汎用バケットとディレクトリバケットの間でコピーできます。ただし、ディレクトリバケット間のコピーの場合、デフォルト ACL を上書きすることはできません。
- マニフェストの指定方法を問わず、リスト自体は汎用バケットに保存する必要があります。バッチオペレーションでは、既存のマニフェストのディレクトリバケットからのインポート (や生成されたマニフェストのディレクトリバケットへの保存) はできません。ただし、マニフェスト内に記述されたオブジェクトはディレクトリバケットに保存できます。
- バッチオペレーションでは、S3 インベントリレポート内の口ケーションとしてディレクトリバケットを指定することはできません。インベントリレポートはディレクトリバケットをサポートしていません。`ListObjectsV2` API オペレーションを使用してオブジェクトを一覧表示して、ディレクトリバケット内のオブジェクトのマニフェストファイルを作成できます。その後、CSV ファイルにリストを挿入できます。

アクセス権の付与

コピージョブを実行するには、次のアクセス許可が必要です。

- あるディレクトリバケットから別のディレクトリバケットにオブジェクトをコピーするには、`s3express:CreateSession` アクセス許可が必要です。
- ディレクトリバケットから汎用バケットにオブジェクトをコピーするには、コピー先バケットにオブジェクトコピーを書き込む `s3express:CreateSession` アクセス許可と `s3:PutObject` アクセス許可が必要です。
- 汎用バケットからディレクトリバケットにオブジェクトをコピーするには、`s3express:CreateSession` アクセス許可とコピーされるソースオブジェクトを読み取る `s3:GetObject` アクセス許可が必要です。

  詳細については、「Amazon Simple Storage Service API リファレンス」の「CopyObject」を参照してください。
- Lambda 関数を呼び出すには、Lambda 関数に基づいてリソースにアクセス許可を付与する必要があります。必要となるアクセス許可を判断するには、該当する API アクセス許可を確認します。

ディレクトリバケット内のオブジェクトへのデータの追加

ディレクトリバケットの S3 Express One Zone ストレージクラスに保存されている既存のオブジェクトの末尾にデータを追加できます。データが一定期間にわたって継続的に書き込まれる場合や、オブジェクトへの書き込み中にオブジェクトを読み取る必要がある場合は、オブジェクトにデータを追加する機能を利用することをお勧めします。オブジェクトへのデータの追加は、ログファイルに新しいログエントリを追加したり、トランスコードしてストリーミングする動画ファイルに新しい動画セグメントを追加したりするなどのユースケースで一般的です。オブジェクトにデータを追加することで、以前はローカルストレージでデータを結合してから最終的なオブジェクトを Amazon S3 にコピーしていたアプリケーションを簡素化できます。

オブジェクトに追加できるデータの最小サイズ要件はありません。ただし、1 つのリクエストでオブジェクトに追加できるデータの最大サイズは 5 GB です。これは、Amazon S3 API を使用してデータをアップロードする場合の最大リクエストサイズと同じ制限です。

追加オペレーションが成功するたびに、オブジェクトのパートが作成されます。各オブジェクトには最大 10,000 個のパートを含めることができます。つまり、最大 10,000 回、オブジェクトにデータを追加できます。S3 マルチパートアップロードを使用してオブジェクトを作成した場合、アップロードした各パートは合計最大 10,000 個のパートにカウントされます。例えば、マルチパートアップロードで作成した、1,000 個のパートで構成されるオブジェクトには、最大 9,000 回追加できます。

> **Note**
>
> パートの制限に達すると、TooManyParts エラーが発生します。`CopyObject` API を使用してカウントをリセットできます。

オブジェクトに複数のパートを並行してアップロードし、アップロード中はパートを読み取る必要がない場合は、Amazon S3 マルチパートアップロードを使用することをお勧めします。詳細については、「マルチパートアップロードの使用」を参照してください。

オブジェクトへのデータの追加は、S3 Express One Zone ストレージクラスに保存されているディレクトリバケット内のオブジェクトでのみサポートされています。S3 Express One Zone の詳細については、「S3 Express One Zone の使用を開始する」を参照してください。

ディレクトリバケット内のオブジェクトへのデータの追加を開始するには、AWS SDK、AWS CLI、`PutObject` API を使用できます。`PutObject` リクエストを行うときは、`x-amz-write-`

offset-bytes ヘッダーを追加先のオブジェクトのサイズに設定します。PutObject API オペレーションを使用するには、CreateSession API を使用して、ディレクトリバケット内のオブジェクトにアクセスするための一時的なセキュリティ認証情報を確立する必要があります。詳細については、「Amazon S3 API Reference」の「PutObject」と「CreateSession」を参照してください。

追加オペレーションが成功するたびに、PutObject リクエストとして請求が発生します。料金の詳細については、「Amazon S3 pricing」を参照してください。

> **Note**
>
> Mountpoint for Amazon S3 は、1.12 リリース以降、S3 Express One Zone に保存されているオブジェクトへのデータの追加をサポートしています。開始するには、--incremental-upload フラグを設定してオプトインする必要があります。Mountpoint の詳細については、「Mountpoint for Amazon S3 の使用」を参照してください。

追加データのアップロード中に CRC (周期冗長チェック) アルゴリズムを使用する場合は、HeadObject リクエストまたは GetObject リクエストを使用してオブジェクト全体の CRC ベースのチェックサムを取得できます。追加データのアップロード中に SHA-1 または SHA-256 アルゴリズムを使用する場合は、以前の PutObject レスポンスで返された SHA チェックサムを使用して、追加パートのチェックサムを取得して整合性を検証できます。詳細については、「データ保護と暗号化」を参照してください。

AWS CLI、AWS SDK、REST API を使用したオブジェクトへのデータの追加

AWS Command Line Interface (AWS CLI)、AWS SDK、REST API を使用して、オブジェクトにデータを追加できます。

AWS CLI の使用

次の put-object コマンド例は、AWS CLI を使用してオブジェクトにデータを追加する方法を示しています。このコマンドを実行するには、*############*を独自の情報に置き換えます。

```
aws s3api put-object --bucket amzn-s3-demo-bucket--azid--x-s3 --key sampleinput/
file001.bin --body bucket-seed/file001.bin --write-offset-bytes size-of-sampleinput/
file001.bin
```

AWS SDK の使用

SDK for Java

AWS SDK for Java を使用して、オブジェクトにデータを追加できます。

```
var putObjectRequestBuilder = PutObjectRequest.builder()
                                              .key(key)
                                              .bucket(bucketName)
                                              .writeOffsetBytes(9);
var response = s3Client.putObject(putObjectRequestBuilder.build());
```

SDK for Python

```
s3.put_object(Bucket='amzn-s3-demo-bucket--use2-az2--x-s3', Key='2024-11-05-sdk-
test', Body=b'123456789', WriteOffsetBytes=9)
```

REST API の使用

REST リクエストを送信して、オブジェクトにデータを追加できます。詳細については、「PutObject」を参照してください。

ディレクトリバケットへのオブジェクトのアップロード

Amazon S3 ディレクトリバケット作成後、オブジェクトをアップロードできます。次の例は、S3 コンソールと AWS SDK を使用してディレクトリバケットにオブジェクトをアップロードする方法を示しています。S3 Express One Zone を使用したオブジェクトの一括アップロードオペレーションの詳細については、「オブジェクト管理」を参照してください。

S3 コンソールの使用

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 左のナビゲーションペインで、[ディレクトリバケット] を選択します。
3. フォルダまたはファイルをアップロードするバケットの名前を選択します。
4. [オブジェクト] タブで、[アップロード] を選択します。
5. [アップロード] ページで、以下のいずれかを行います。

- ファイルとフォルダを点線で示されているアップロードエリアにドラッグアンドドロップします。
- [ファイルの追加] または [フォルダの追加] を選択し、アップロードするファイルまたはフォルダを選択して [開く] または [アップロード] を選択します。

6. [チェックサム] で、使用する [チェックサム関数] を選択します。

   (オプション) サイズが 16 MB 未満の単一のオブジェクトをアップロードする場合は、事前に計算されたチェックサム値を指定することもできます。事前に計算された値を指定すると、Amazon S3 は選択したチェックサム関数を使用して計算した値と比較します。値が一致しない場合、アップロードは開始されません。

7. [アクセス許可] と [プロパティ] セクションのオプションは、自動的にデフォルトに設定され、変更できません。ブロックパブリックアクセスは自動的に有効になり、ディレクトリバケットに対して S3 バージョニングと S3 Object Lock を有効にすることはできません。

   (オプション) オブジェクトにキーと値のペアのメタデータを追加する場合は、[プロパティ] セクションを展開し、[メタデータ]セクションで [メタデータを追加]を選択します。

8. リストされたファイルとフォルダをアップロードするには、[アップロード] を選択します。

   Amazon S3 はオブジェクトとフォルダをアップロードします。アップロードが完了すると、[アップロード: ステータス] ページに成功のメッセージが表示されます。

AWS SDK の使用

SDK for Java 2.x

Example

```
public static void putObject(S3Client s3Client, String bucketName, String objectKey,
 Path filePath) {
       //Using File Path to avoid loading the whole file into memory
       try {
           PutObjectRequest putObj = PutObjectRequest.builder()
                   .bucket(bucketName)
                   .key(objectKey)
                   //.metadata(metadata)
                   .build();
           s3Client.putObject(putObj, filePath);
           System.out.println("Successfully placed " + objectKey +" into bucket
 "+bucketName);
```

```
        }

        catch (S3Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
}
```

SDK for Python

Example

```
import boto3
import botocore
from botocore.exceptions import ClientError


def put_object(s3_client, bucket_name, key_name, object_bytes):
    """
    Upload data to a directory bucket.
    :param s3_client: The boto3 S3 client
    :param bucket_name: The bucket that will contain the object
    :param key_name: The key of the object to be uploaded
    :param object_bytes: The data to upload
    """
    try:
        response = s3_client.put_object(Bucket=bucket_name, Key=key_name,
                            Body=object_bytes)
        print(f"Upload object '{key_name}' to bucket '{bucket_name}'.")
        return response
    except ClientError:
        print(f"Couldn't upload object '{key_name}' to bucket '{bucket_name}'.")
        raise

def main():
    # Share the client session with functions and objects to benefit from S3 Express
 One Zone auth key
    s3_client = boto3.client('s3')
    # Directory bucket name must end with --zone-id--x-s3
    resp = put_object(s3_client, 'doc-bucket-example--use1-az5--x-s3', 'sample.txt',
 b'Hello, World!')
    print(resp)
```

```
if __name__ == "__main__":
    main()
```

AWS CLI を使用する場合

次の put-object コマンド例は、AWS CLI を使用して Amazon S3 からオブジェクトをアップロードする方法を示しています。このコマンドを実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3api put-object --bucket bucket-base-name--zone-id--x-s3 --key sampleinut/
file001.bin --body bucket-seed/file001.bin
```

詳細については、AWS CLI コマンドリファレンスの「put-object」を参照してください。

トピック

- ディレクトリバケットでのマルチパートアップロードの使用

ディレクトリバケットでのマルチパートアップロードの使用

マルチパートアップロードプロセスを使用すると、単一のオブジェクトをパートのセットとしてアップロードすることができます。各パートは、オブジェクトのデータの連続する部分です。これらのオブジェクトパートは、任意の順序で個別にアップロードできます。いずれかのパートの送信が失敗すると、他のパートに影響を与えることなくそのパートを再送することができます。オブジェクトのすべてのパートがアップロードされたら、Amazon S3 はこれらのパートを組み立ててオブジェクトを作成します。通常、オブジェクトサイズが 100 MB 以上の場合は、単一のオペレーションでオブジェクトをアップロードする代わりに、マルチパートアップロードを使用することを考慮してください。

マルチパートアップロードの使用には、次の利点があります。

- スループットの向上 – パートを並列にアップロードすることで、スループットを向上させることができます。
- ネットワーク問題からの迅速な回復 – パートサイズが小さいほど、ネットワークエラーが原因で失敗したアップロードを再開する際の影響を最小限に抑えることができます。
- オブジェクトのアップロードの一時停止と再開 – オブジェクトの複数のパートを徐々にアップロードできます。マルチパートアップロードをいったん開始すると、終了期限はありません。マルチパートアップロードを明示的に完了または中止する必要があります。

- オブジェクトの最終的なサイズが不明な状態でアップロードを開始 – オブジェクトの作成中でもアップロードを開始できます。

次の方法でマルチパートアップロードを使用することをお勧めします。

- 安定した高帯域幅ネットワーク経由で大きなオブジェクトをアップロードする場合は、複数スレッドのパフォーマンスのためにオブジェクトパートを並行してアップロードすることで、マルチパートアップロードを使用して利用可能な帯域幅を最大限に活用します。
- むらがあるネットワークでアップロードを実行する場合は、マルチパートアップロードを使用して、アップロードの再開を回避することで、ネットワークエラーに対する回復性を高めます。マルチパートアップロードを使用するときには、アップロード中に中断されたパートのアップロードを再試行するだけで済みます。最初からオブジェクトのアップロードを再開する必要はありません。

マルチパートアップロードを使用してディレクトリバケットの Amazon S3 Express One Zone ストレージクラスにオブジェクトをアップロードする場合、マルチパートアップロードプロセスは、マルチパートアップロードを使用して汎用バケットにオブジェクトをアップロードするプロセスと似ています。ただし、重要な相違点がいくつかあります。

マルチパートアップロードを使用して S3 Express One Zone ゾーンにオブジェクトをアップロードする方法の詳細については、以降のトピックを参照してください。

トピック

- マルチパートアップロードのプロセス
- マルチパートアップロードオペレーションを使用したチェックサム
- マルチパートアップロードの同時オペレーション
- マルチパートアップロードと料金
- マルチパートアップロード API オペレーションとアクセス許可
- 例

マルチパートアップロードのプロセス

マルチパートアップロードは次の 3 ステップのプロセスです。

- アップロードを開始します。
- オブジェクトパートをアップロードします。

- すべてのパートをアップロードしたら、マルチパートアップロードを完了します。

Amazon S3 の側では、マルチパートアップロードの完了リクエストを受け取ると同時に、アップロードされたパートからオブジェクトを構築します。構築されたオブジェクトへは、バケット内の他のオブジェクトと同じようにアクセスできます。

マルチパートアップロードの開始

リクエストを送信すると、アップロード ID を含むレスポンスが Amazon S3 から返されます。アップロード ID はマルチパートアップロードの一意の識別子です。パートのアップロード、パートのリスト、アップロードの完了、アップロードの中止を行うときは常に、このアップロード ID を指定する必要があります。

パートのアップロード

パートをアップロードするときは、アップロード ID に加えて、パート番号を指定する必要があります。S3 Express One Zone でマルチパートアップロードを使用する場合、マルチパート番号は連続するパート番号である必要があります。連続しないパート番号を使用してマルチパートアップロードリクエストを実行しようとすると、`HTTP 400 Bad Request` (無効なパート順序) エラーが生成されます。

パート番号によって、アップロードするオブジェクトに含まれるパートとその位置が一意に識別されます。以前にアップロードしたパートと同じパート番号を使って新しいパートをアップロードした場合、以前のパートは上書きされます。

パートをアップロードするたびに、Amazon S3 は エンティティタグ (ETag) ヘッダーを含むレスポンスを返します。パートのアップロードごとに、パート番号と ETag 値を記録する必要があります。すべてのオブジェクトパートアップロードの ETag 値は同じままですが、パートごとに異なるパート番号が割り当てられます。マルチパートアップロードを完了するためには、残りのリクエストにこれらの値を含める必要があります。

Amazon S3 は、S3 バケットにコピーされたすべての新しいオブジェクトを自動的に暗号化します。マルチパートアップロードを実行する際に、リクエストで暗号化情報を指定しないと、アップロードされたパートの暗号化設定は、送信先バケットのデフォルトの暗号化設定に設定されます。Amazon S3 バケットのデフォルトの暗号化設定は常に有効になっており、最低でも Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3) に設定されています。ディレクトリバケットでは、SSE-S3 と AWS KMS キーによるサーバー側の暗号化 (SSE-KMS) がサポートされています。詳細については、「データ保護と暗号化」を参照してください。

マルチパートアップロードの完了

マルチパートアップロードを完了すると、パート番号に基づいて昇順に連結されたオブジェクトが Amazon S3 によって作成されます。完了リクエストが正常に処理されると、個々のパートはなくなります。

「マルチパートアップロードの完了」リクエストには、アップロード ID と、パート番号およびそれに対応する ETag 値の両方のリストが含まれている必要があります。Amazon S3 からのレスポンスには、結合されるオブジェクトデータを一意に識別する ETag が含まれます。この ETag は、オブジェクトデータの MD5 ハッシュであるとは限りません。

マルチパートアップロードのリスト化

特定のマルチパートアップロードのパートや、進行中のすべてのマルチパートアップロードをリスト表示できます。パートのリストオペレーションでは、特定のマルチパートアップロードについて既にアップロードしたパートの情報が返されます。パートのリストリクエストを送信するたびに、指定したマルチパートアップロードのパート情報 (最大で 1,000 個のパート) が Amazon S3 から返されます。マルチパートアップロードに 1,000 を超えるパートが含まれる場合、すべてのパートを取得するにはパートのリストリクエストを追加で送信する必要があります。

返されるパートのリストには、アップロードが完了していないパートは含まれていません。マルチパートアップロードの一覧表示オペレーションを使用すると、進行中のマルチパートアップロードのリストを取得できます。

進行中のマルチパートアップロードとは、開始されているものの、まだ完了または中止されていないアップロードを意味します。各リクエストに最大 1,000 個のマルチパートアップロードが返されます。進行中のマルチパートアップロードが 1,000 個を超える場合、残りのマルチパートアップロードを取得するには、リクエストを追加で送信する必要があります。返されたリストは確認の目的でのみ使用してください。マルチパートアップロードの完了リクエストを送信するときに、このリストの結果を使用しないでください。代わりに、パートのアップロード時に指定したパート番号と、それに対応する、Amazon S3 から返される ETag 値の独自のリストを維持しておいてください。

マルチパートアップロードの一覧の詳細については、「Amazon Simple Storage Service API リファレンス」の「ListParts」を参照してください。

マルチパートアップロードオペレーションを使用したチェックサム

オブジェクトをアップロードする際、オブジェクトの整合性を確認するためのチェックサムアルゴリズムを指定できます。MD5 はディレクトリバケットではサポートされていません。次のセキュア

ハッシュアルゴリズム (SHA) または巡回冗長検査 (CRC) のデータ整合性チェックアルゴリズムのいずれかを指定できます。

- CRC32
- CRC32C
- SHA-1
- SHA-256

`GetObject` または `HeadObject` を使用することで、Amazon S3 REST API または AWS SDK を使用して、個々のパートのチェックサム値を取得できます。まだ処理中のマルチパートアップロードの個々の部分のチェックサム値を取得したい場合は、`ListParts` を使用できます。

> **Important**
>
> 前述のチェックサムアルゴリズムを使用する場合、マルチパートパーツ番号には連続したパーツ番号を使用する必要があります。連続しないパート番号を使用してマルチパートアップロードリクエストを実行しようとすると、Amazon S3 により `HTTP 400 Bad Request` (無効なパート順序) エラーが生成されます。

マルチパートアップロードオブジェクトでのチェックサムの動作の詳細については、「Amazon S3 でのオブジェクトの整合性のチェック」を参照してください。

マルチパートアップロードの同時オペレーション

分散開発環境においては、アプリケーションから同じオブジェクトに対して複数の更新が同時に開始されることもありえます。例えば、アプリケーションが同じオブジェクトキーを使用して複数のマルチパートアップロードを開始する場合があります。そのようなアップロードごとに、アプリケーションからパートのアップロードが行われ、アップロードの完了リクエストが Amazon S3 に送信されて、オブジェクトが作成されます。S3 Express One Zone の場合、オブジェクトの作成時間はマルチパートアップロードの完了日となります。

> **Important**
>
> ディレクトリバケットに保存されているオブジェクトのバージョニングはサポートされていません。

マルチパートアップロードと料金

マルチパートアップロードを開始すると、アップロードを完了または中止するまですべてのパートが Amazon S3 によって保持されます。マルチパートアップロードの実行期間を通して、アップロードとそれに関連するパートのために使用されるすべてのストレージ、帯域幅、リクエストに対して課金が行われます。マルチパートアップロードを中止した場合、Amazon S3 はアップロードしたアーティファクトやアップロードしたすべてのパートを削除するため、これらについて課金されることはなくなります。指定されたストレージクラスに関係なく、不完全なマルチパートアップロードの削除に伴う早期削除料金はありません。料金に関する詳細については、「Amazon S3 の料金」を参照してください。

> **Important**
>
> マルチパートアップロードの完了リクエストの送信が正常に実行されないと、オブジェクトのパーツは組み立てられず、オブジェクトも作成されません。アップロードされたパートに関連のあるすべてのストレージに対して料金が請求されます。そのため、マルチパートアップロードを完了してオブジェクトを作成するか、マルチパートアップロードを停止してアップロードされたパートを削除することが重要です。
> ディレクトリバケットを削除する前に、進行中のすべてのマルチパートアップロードを完了または中止する必要があります。ディレクトリバケットは S3 ライフサイクル設定をサポートしていません。必要に応じて、アクティブなマルチパートアップロードを一覧表示して、アップロードを中止し、バケットを削除できます。

マルチパートアップロード API オペレーションとアクセス許可

ディレクトリバケットのオブジェクト管理 API オペレーションにアクセスできるようにするには、バケットポリシーまたは AWS Identity and Access Management (IAM) ID ベースのポリシーで `s3express:CreateSession` アクセス許可を付与します。

マルチパートアップロードオペレーションを使用するには、必要なアクセス権限を有している必要があります。バケットポリシーまたは IAM ID ベースのポリシーを使用して、これらのオペレーションを実行するアクセス許可を IAM プリンシパルに付与できます。さまざまなマルチパートアップロードオペレーションに必要なアクセス許可の一覧は、次の表のとおりです。

`Initiator` 要素を使用して、マルチパートアップロードの開始点を特定できます。イニシエータが AWS アカウント である場合、このエレメントは `Owner` エレメントと同じ情報を提供します。イニシエータが IAM ユーザーである場合、このエレメントはユーザー ARN と表示名を提供します。

アクション	必要なアクセス許可
マルチパートアップロードの作成	マルチパートアップロードを作成するには、ディレクトリバケットに対して s3express:CreateSession アクションを実行するための許可が必要です。
マルチパートアップロードの開始	マルチパートアップロードを開始するには、ディレクトリバケットに対して s3express:CreateSession アクションを実行するための許可が必要です。
パートのアップロード	パートをアップロードするには、ディレクトリバケットに対して s3express:CreateSession アクションを実行するための許可が必要です。 バケット所有者は、イニシエータがパートをアップロードできるように、ディレクトリバケットに対して s3express:CreateSession アクションを実行するための許可をイニシエータに付与する必要があります。
パートのアップロード (コピー)	パートをアップロードするには、ディレクトリバケットに対して s3express:CreateSession アクションを実行するための許可が必要です。 開始者がオブジェクトのパートをアップロードするには、バケット所有者が、開始者にそのオブジェクトでの s3express:CreateSession アクションの実行を許可する必要があります。
マルチパートアップロードを完了する	マルチパートアップロードを完了するには、ディレクトリバケットで s3express:CreateSession アクションを実行するための許可が必要です。 イニシエータがマルチパートアップロードを実行するには、バケット所有者がイニシエータにオブジェクトに対する s3express:CreateSession アクションの実行を許可する必要があります。
マルチパートアップロードの中止	マルチパートアップロードを中止するには、s3express:CreateSession アクションを実行するための許可が必要です。 イニシエータはマルチパートアップロードを中止できるように、s3express:CreateSession アクションを実行するためのアクセス許可を明示的に付与される必要があります。

アクション	必要なアクセス許可
パートの一覧表示	マルチパートアップロードでパートを一覧表示するには、ディレクトリバケットに対して `s3express:CreateSession` アクションを実行するための許可が必要です。
進行中のマルチパートアップロードの一覧表示	バケットへの進行中のマルチパートアップロードを一覧表示するには、そのバケットに対して `s3:ListBucketMultipartUploads` アクションを実行するための許可が必要です。

マルチパートアップロードに対する API オペレーションサポート

Amazon Simple Storage Service API リファレンスの以下のセクションでは、マルチパートアップロードの Amazon S3 REST API オペレーションについて説明しています。

- CreateMultipartUpload
- UploadPart
- UploadPartCopy
- CompleteMultipartUpload
- AbortMultipartUpload
- ListParts
- ListMultipartUploads

例

マルチパートアップロードを使用してディレクトリバケット内の S3 Express One Zone にオブジェクトをアップロードするには、次の例を参照してください。

トピック

- マルチパートアップロードの作成
- マルチパートアップロードのパートのアップロード
- マルチパートアップロードの完了
- マルチパートアップロードの中止

- マルチパートアップロードのコピーオペレーションの作成
- 進行中のマルチパートアップロードの一覧表示
- マルチパートアップロードパートの一覧表示

マルチパートアップロードの作成

> **Note**
>
> ディレクトリバケットの場合、CreateMultipartUpload オペレーションと UploadPartCopy オペレーションを実行するときに、バケットのデフォルトの暗号化で必要な暗号化設定を使用し、CreateMultipartUpload リクエストで指定したリクエストヘッダーが送信先バケットのデフォルトの暗号化設定と一致する必要があります。

次の例は、マルチパートアップロードの作成方法を示しています。

AWS SDK の使用

SDK for Java 2.x

Example

```
/**
 * This method creates a multipart upload request that generates a unique upload ID
 that is used to track
 * all the upload parts
 *
 * @param s3
 * @param bucketName - for example, 'doc-example-bucket--use1-az4--x-s3'
 * @param key
 * @return
 */
 private static String createMultipartUpload(S3Client s3, String bucketName, String
 key) {

     CreateMultipartUploadRequest createMultipartUploadRequest =
 CreateMultipartUploadRequest.builder()
             .bucket(bucketName)
             .key(key)
             .build();
```

```
    String uploadId = null;

    try {
        CreateMultipartUploadResponse response =
s3.createMultipartUpload(createMultipartUploadRequest);
        uploadId = response.uploadId();
    }
    catch (S3Exception e) {
        System.err.println(e.awsErrorDetails().errorMessage());
        System.exit(1);
    }
    return uploadId;
```

SDK for Python

Example

```
def create_multipart_upload(s3_client, bucket_name, key_name):
    '''
   Create a multipart upload to a directory bucket

   :param s3_client: boto3 S3 client
   :param bucket_name: The destination bucket for the multipart upload
   :param key_name: The key name for the object to be uploaded
   :return: The UploadId for the multipart upload if created successfully, else None
   '''

   try:
        mpu = s3_client.create_multipart_upload(Bucket = bucket_name, Key =
key_name)
        return mpu['UploadId']
    except ClientError as e:
        logging.error(e)
        return None
```

AWS CLI を使用する場合

この例では、AWS CLI を使用してディレクトリバケットへのマルチパートアップロードを作成する方法を示します。このコマンドは、オブジェクト *KEY_NAME* のディレクトリバケット *bucket-base-name*--*zone-id*--x-s3 へのマルチパートアップロードを開始します。このコマンドを使用する際は、*###############*を独自の情報に置き換えます。

```
aws s3api create-multipart-upload --bucket bucket-base-name--zone-id--x-s3 --
key KEY_NAME
```

詳細については、「AWS Command Line Interface」の「create-multipart-upload」を参照してください。

マルチパートアップロードのパートのアップロード

次の例は、マルチパートアップロードの一部をアップロードする方法を示しています。

AWS SDK の使用

SDK for Java 2.x

次の例は、SDK for Java 2.x を使用して、単一のオブジェクトを複数の部分に分割し、それらの部分をディレクトリバケットにアップロードする方法を示しています。

Example

```
/**
 * This method creates part requests and uploads individual parts to S3 and then
 returns all the completed parts
 *
 * @param s3
 * @param bucketName
 * @param key
 * @param uploadId
 * @throws IOException
 */
 private static ListCompletedPartmultipartUpload(S3Client s3, String bucketName,
 String key, String uploadId, String filePath) throws IOException {

        int partNumber = 1;
        ListCompletedPart completedParts = new ArrayList<>();
        ByteBuffer bb = ByteBuffer.allocate(1024 * 1024 * 5); // 5 MB byte buffer

        // read the local file, breakdown into chunks and process
        try (RandomAccessFile file = new RandomAccessFile(filePath, "r")) {
            long fileSize = file.length();
            int position = 0;
            while (position < fileSize) {
                file.seek(position);
```

```
                int read = file.getChannel().read(bb);

                bb.flip(); // Swap position and limit before reading from the
 buffer.
                UploadPartRequest uploadPartRequest = UploadPartRequest.builder()
                        .bucket(bucketName)
                        .key(key)
                        .uploadId(uploadId)
                        .partNumber(partNumber)
                        .build();

                UploadPartResponse partResponse = s3.uploadPart(
                        uploadPartRequest,
                        RequestBody.fromByteBuffer(bb));

                CompletedPart part = CompletedPart.builder()
                        .partNumber(partNumber)
                        .eTag(partResponse.eTag())
                        .build();
                completedParts.add(part);

                bb.clear();
                position += read;
                partNumber++;
            }
        }

        catch (IOException e) {
            throw e;
        }
        return completedParts;
    }
```

SDK for Python

次の例は、SDK for Python を使用して単一のオブジェクトを複数の部分に分割し、それらの部分をディレクトリバケットにアップロードする方法を示しています。

Example

```
def multipart_upload(s3_client, bucket_name, key_name, mpu_id, part_size):
    '''
    Break up a file into multiple parts and upload those parts to a directory bucket
```

```
   :param s3_client: boto3 S3 client
   :param bucket_name: Destination bucket for the multipart upload
   :param key_name: Key name for object to be uploaded and for the local file
that's being uploaded
   :param mpu_id: The UploadId returned from the create_multipart_upload call
   :param part_size: The size parts that the object will be broken into, in bytes.
                     Minimum 5 MiB, Maximum 5 GiB. There is no minimum size for the
last part of your multipart upload.
   :return: part_list for the multipart upload if all parts are uploaded
successfully, else None
   '''

   part_list = []
   try:
       with open(key_name, 'rb') as file:
           part_counter = 1
           while True:
               file_part = file.read(part_size)
               if not len(file_part):
                   break
               upload_part = s3_client.upload_part(
                   Bucket = bucket_name,
                   Key = key_name,
                   UploadId = mpu_id,
                   Body = file_part,
                   PartNumber = part_counter
               )
               part_list.append({'PartNumber': part_counter, 'ETag':
upload_part['ETag']})
               part_counter += 1
   except ClientError as e:
       logging.error(e)
       return None
   return part_list
```

AWS CLI を使用する場合

この例では、AWS CLI を使用して単一のオブジェクトを複数の部分に分割し、それらの部分をディレクトリバケットにアップロードする方法を示しています。このコマンドを使用する際は、`##########`を独自の情報に置き換えます。

```
aws s3api upload-part --bucket bucket-base-name--zone-id--x-s3 --
key KEY_NAME --part-number 1 --body LOCAL_FILE_NAME --upload-id
 "AS_mgt9RaQE9GEaifATue15dAAAAAAAAAAEMAAAAAAAAADQwNzI4MDU0MjUyMBYAAAAAAAAAAA0AAAAAAAAAAH2AfYAA
```

詳細については、「AWS Command Line Interface」の「upload-part」を参照してください。

マルチパートアップロードの完了

次の例は、マルチパートアップロードを完了する方法を示しています。

AWS SDK の使用

SDK for Java 2.x

次の例は、SDK for Java 2.x を使用してマルチパートアップロードを完了する方法を示しています。

Example

```
/**
 * This method completes the multipart upload request by collating all the upload
 parts
 * @param s3
 * @param bucketName - for example, 'doc-example-bucket--usw2-az1--x-s3'
 * @param key
 * @param uploadId
 * @param uploadParts
 */
 private static void completeMultipartUpload(S3Client s3, String bucketName, String
 key, String uploadId, ListCompletedPart uploadParts) {
        CompletedMultipartUpload completedMultipartUpload =
 CompletedMultipartUpload.builder()
                .parts(uploadParts)
                .build();

        CompleteMultipartUploadRequest completeMultipartUploadRequest =
                CompleteMultipartUploadRequest.builder()
                        .bucket(bucketName)
                        .key(key)
                        .uploadId(uploadId)
                        .multipartUpload(completedMultipartUpload)
                        .build();
```

```
        s3.completeMultipartUpload(completeMultipartUploadRequest);
    }

    public static void multipartUploadTest(S3Client s3, String bucketName, String
 key, String localFilePath)  {
        System.out.println("Starting multipart upload for: " + key);
        try {
            String uploadId = createMultipartUpload(s3, bucketName, key);
            System.out.println(uploadId);
            ListCompletedPart parts = multipartUpload(s3, bucketName, key, uploadId,
 localFilePath);
            completeMultipartUpload(s3, bucketName, key, uploadId, parts);
            System.out.println("Multipart upload completed for: " + key);
        }

        catch (Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

SDK for Python

次の例は、SDK for Python を使用してマルチパートアップロードを完了する方法を示しています。

Example

```
def complete_multipart_upload(s3_client, bucket_name, key_name, mpu_id, part_list):
    '''
    Completes a multipart upload to a directory bucket

    :param s3_client: boto3 S3 client
    :param bucket_name: The destination bucket for the multipart upload
    :param key_name: The key name for the object to be uploaded
    :param mpu_id: The UploadId returned from the create_multipart_upload call
    :param part_list: The list of uploaded part numbers with their associated ETags
    :return: True if the multipart upload was completed successfully, else False
    '''

    try:
        s3_client.complete_multipart_upload(
```

```
            Bucket = bucket_name,
            Key = key_name,
            UploadId = mpu_id,
            MultipartUpload = {
                'Parts': part_list
            }
        )
    except ClientError as e:
        logging.error(e)
        return False
    return True

if __name__ == '__main__':
    MB = 1024 ** 2
    region = 'us-west-2'
    bucket_name = 'BUCKET_NAME'
    key_name = 'OBJECT_NAME'
    part_size = 10 * MB
    s3_client = boto3.client('s3', region_name = region)
    mpu_id = create_multipart_upload(s3_client, bucket_name, key_name)
    if mpu_id is not None:
        part_list = multipart_upload(s3_client, bucket_name, key_name, mpu_id,
 part_size)
        if part_list is not None:
            if complete_multipart_upload(s3_client, bucket_name, key_name, mpu_id,
 part_list):
                print (f'{key_name} successfully uploaded through a ultipart upload
 to {bucket_name}')
            else:
                print (f'Could not upload {key_name} hrough a multipart upload to
 {bucket_name}')
```

AWS CLI を使用する場合

この例では、AWS CLI を使用してディレクトリバケットのマルチパートアップロードを完了する方法を示します。このコマンドを使用する際は、*###############*を独自の情報に置き換えます。

```
aws s3api complete-multipart-upload --bucket bucket-base-name--zone-id--x-s3 --
key KEY_NAME --upload-id
 "AS_mgt9RaQE9GEaifATue15dAAAAAAAAAAEMAAAAAAAAADQwNzI4MDU0MjUyMBYAAAAAAAAAAA0AAAAAAAAAAH2AfYAA
 --multipart-upload file://parts.json
```

この例では、完全なファイルに再構成する必要があるマルチパートアップロードの部分を記述した JSON 構造を採用しています。この例では、`file://` プレフィックスを使用して、`parts` という名前のローカルフォルダーにあるファイルから JSON 構造を読み込みます。

parts.json:

```
parts.json
{
  "Parts": [
    {
      "ETag": "6b78c4a64dd641a58dac8d9258b88147",
      "PartNumber": 1
    }
  ]
}
```

詳細については、「AWS Command Line Interface」の「complete-multipart-upload」を参照してください。

マルチパートアップロードの中止

次の例は、マルチパートアップロードを中止する方法を示しています。

AWS SDK の使用

SDK for Java 2.x

次の例は、SDK for Java 2.x を使用してマルチパートアップロードを中止する方法を示しています。

Example

```
public static void abortMultiPartUploads( S3Client s3, String bucketName ) {

         try {
             ListMultipartUploadsRequest listMultipartUploadsRequest =
 ListMultipartUploadsRequest.builder()
                     .bucket(bucketName)
                     .build();

             ListMultipartUploadsResponse response =
 s3.listMultipartUploads(listMultipartUploadsRequest);
```

```
            ListMultipartUpload uploads = response.uploads();

            AbortMultipartUploadRequest abortMultipartUploadRequest;
            for (MultipartUpload upload: uploads) {
                abortMultipartUploadRequest = AbortMultipartUploadRequest.builder()
                        .bucket(bucketName)
                        .key(upload.key())
                        .uploadId(upload.uploadId())
                        .build();

                s3.abortMultipartUpload(abortMultipartUploadRequest);
            }

        }

        catch (S3Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

SDK for Python

次の例は、SDK for Python を使用してマルチパートアップロードを中止する方法を示しています。

Example

```
import logging
import boto3
from botocore.exceptions import ClientError


def abort_multipart_upload(s3_client, bucket_name, key_name, upload_id):
    '''
    Aborts a partial multipart upload in a directory bucket.

    :param s3_client: boto3 S3 client
    :param bucket_name: Bucket where the multipart upload was initiated - for
 example, 'doc-example-bucket--usw2-az1--x-s3'
    :param key_name: Name of the object for which the multipart upload needs to be
 aborted
    :param upload_id: Multipart upload ID for the multipart upload to be aborted
```

```
    :return: True if the multipart upload was successfully aborted, False if not
    '''
    try:
        s3_client.abort_multipart_upload(
            Bucket = bucket_name,
            Key = key_name,
            UploadId = upload_id
        )
    except ClientError as e:
        logging.error(e)
        return False
    return True


if __name__ == '__main__':
    region = 'us-west-2'
    bucket_name = 'BUCKET_NAME'
    key_name = 'KEY_NAME'
        upload_id = 'UPLOAD_ID'
    s3_client = boto3.client('s3', region_name = region)
    if abort_multipart_upload(s3_client, bucket_name, key_name, upload_id):
        print (f'Multipart upload for object {key_name} in {bucket_name} bucket has
 been aborted')
    else:
        print (f'Unable to abort multipart upload for object {key_name} in
 {bucket_name} bucket')
```

AWS CLI を使用する場合

次の例は、AWS CLI を使用してマルチパートアップロードを中止する方法を示しています。このコマンドを使用する際は、*###############*を独自の情報に置き換えます。

```
aws s3api abort-multipart-upload --bucket bucket-base-name--zone-id--x-s3 --
key KEY_NAME --upload-id
 "AS_mgt9RaQE9GEaifATue15dAAAAAAAAAAEMAAAAAAAAADQwNzI4MDU0MjUyMBYAAAAAAAAAAA0AAAAAAAAAAH2AfYAA
MAQAAAAB0OxUFeA7LTbWWFS8WYwhrxDxTIDN-pdEEq_agIHqsbg"
```

詳細については、「AWS Command Line Interface」の「abort-multipart-upload」を参照してください。

マルチパートアップロードのコピーオペレーションの作成

> **Note**
>
> - SSE-KMS を使用してディレクトリバケット内の新しいオブジェクトパーツコピーを暗号化するには、KMS キー (特にカスタマーマネージドキー) を使用してディレクトリバケットのデフォルトの暗号化設定として SSE-KMS を指定する必要があります。AWS マネージドキー (aws/s3) はサポートされていません。SSE-KMS 設定では、バケットの存続期間中、ディレクトリバケットごとに 1 つのカスタマーマネージドキーしかサポートできません。SSE-KMS のカスタマーマネージドキーを指定した後は、バケットの SSE-KMS 設定のカスタマーマネージドキーを上書きすることはできません。UploadPartCopy リクエストヘッダーで SSE-KMS を使用した新しいオブジェクトパートコピーのサーバー側の暗号化設定を指定することはできません。また、CreateMultipartUpload リクエストで指定するリクエストヘッダーは、送信先バケットのデフォルトの暗号化設定と一致する必要があります。
> - SSE-KMS で暗号化されたオブジェクトを UploadPartCopy 経由で汎用バケットからディレクトリバケットにコピーする場合、ディレクトリバケットから汎用バケットにコピーする場合、またはディレクトリバケット間でコピーする場合、S3 バケットキーはサポートされません。この場合、KMS で暗号化されたオブジェクトに対してコピーリクエストが実行されるたびに、Amazon S3 は AWS KMS を呼び出します。

次の例は、マルチパートアップロードを使用して、あるバケットから別のバケットにオブジェクトをコピーする方法を示しています。

AWS SDK の使用

SDK for Java 2.x

次の例は、SDK for Java 2.x を使用して、マルチパートアップロードを使って、あるバケットから別のバケットにオブジェクトをプログラムでコピーする方法を示しています。

Example

```
/**
 * This method creates a multipart upload request that generates a unique upload ID
 that is used to track
 * all the upload parts.
 *
```

```
* @param s3
* @param bucketName
* @param key
* @return
*/
private static String createMultipartUpload(S3Client s3, String bucketName, String
key) {
       CreateMultipartUploadRequest createMultipartUploadRequest =
CreateMultipartUploadRequest.builder()
               .bucket(bucketName)
               .key(key)
               .build();
       String uploadId = null;
       try {
           CreateMultipartUploadResponse response =
s3.createMultipartUpload(createMultipartUploadRequest);
           uploadId = response.uploadId();
       } catch (S3Exception e) {
           System.err.println(e.awsErrorDetails().errorMessage());
           System.exit(1);
       }
       return uploadId;
 }

 /**
  * Creates copy parts based on source object size and copies over individual parts
  *
  * @param s3
  * @param sourceBucket
  * @param sourceKey
  * @param destnBucket
  * @param destnKey
  * @param uploadId
  * @return
  * @throws IOException
  */
   public static ListCompletedPart multipartUploadCopy(S3Client s3, String
sourceBucket, String sourceKey, String destnBucket, String destnKey, String
uploadId) throws IOException {

       // Get the object size to track the end of the copy operation.
       HeadObjectRequest headObjectRequest = HeadObjectRequest
               .builder()
               .bucket(sourceBucket)
```

```
                .key(sourceKey)
                .build();
        HeadObjectResponse response = s3.headObject(headObjectRequest);
        Long objectSize = response.contentLength();

        System.out.println("Source Object size: " + objectSize);

        // Copy the object using 20 MB parts.
        long partSize = 20 * 1024 * 1024;
        long bytePosition = 0;
        int partNum = 1;
        ListCompletedPart completedParts = new ArrayList<>();
        while (bytePosition < objectSize) {
            // The last part might be smaller than partSize, so check to make sure
            // that lastByte isn't beyond the end of the object.
            long lastByte = Math.min(bytePosition + partSize - 1, objectSize - 1);

            System.out.println("part no: " + partNum + ", bytePosition: " +
bytePosition + ", lastByte: " + lastByte);

            // Copy this part.
            UploadPartCopyRequest req = UploadPartCopyRequest.builder()
                    .uploadId(uploadId)
                    .sourceBucket(sourceBucket)
                    .sourceKey(sourceKey)
                    .destinationBucket(destnBucket)
                    .destinationKey(destnKey)
                    .copySourceRange("bytes="+bytePosition+"-"+lastByte)
                    .partNumber(partNum)
                    .build();
            UploadPartCopyResponse res = s3.uploadPartCopy(req);
            CompletedPart part = CompletedPart.builder()
                    .partNumber(partNum)
                    .eTag(res.copyPartResult().eTag())
                    .build();
            completedParts.add(part);
            partNum++;
            bytePosition += partSize;
        }
        return completedParts;
    }
```

```
    public static void multipartCopyUploadTest(S3Client s3, String srcBucket, String
 srcKey, String destnBucket, String destnKey)  {
        System.out.println("Starting multipart copy for: " + srcKey);
        try {
            String uploadId = createMultipartUpload(s3, destnBucket, destnKey);
            System.out.println(uploadId);
            ListCompletedPart parts = multipartUploadCopy(s3, srcBucket,
 srcKey,destnBucket,  destnKey, uploadId);
            completeMultipartUpload(s3, destnBucket, destnKey, uploadId, parts);
            System.out.println("Multipart copy completed for: " + srcKey);
        } catch (Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

SDK for Python

次の例は、SDK for Python を使用して、マルチパートアップロードを使って、あるバケットから別のバケットにオブジェクトをプログラムでコピーする方法を示しています。

Example

```
import logging
import boto3
from botocore.exceptions import ClientError

def head_object(s3_client, bucket_name, key_name):
    '''
    Returns metadata for an object in a directory bucket

    :param s3_client: boto3 S3 client
    :param bucket_name: Bucket that contains the object to query for metadata
    :param key_name: Key name to query for metadata
    :return: Metadata for the specified object if successful, else None
    '''

    try:
        response = s3_client.head_object(
            Bucket = bucket_name,
            Key = key_name
        )
        return response
    except ClientError as e:
```

```
        logging.error(e)
        return None

def create_multipart_upload(s3_client, bucket_name, key_name):
    '''
    Create a multipart upload to a directory bucket

    :param s3_client: boto3 S3 client
    :param bucket_name: Destination bucket for the multipart upload
    :param key_name: Key name of the object to be uploaded
    :return: UploadId for the multipart upload if created successfully, else None
    '''

    try:
        mpu = s3_client.create_multipart_upload(Bucket = bucket_name, Key =
 key_name)
        return mpu['UploadId']
    except ClientError as e:
        logging.error(e)
        return None

def multipart_copy_upload(s3_client, source_bucket_name, key_name,
 target_bucket_name, mpu_id, part_size):
    '''
    Copy an object in a directory bucket to another bucket in multiple parts of a
 specified size

    :param s3_client: boto3 S3 client
    :param source_bucket_name: Bucket where the source object exists
    :param key_name: Key name of the object to be copied
    :param target_bucket_name: Destination bucket for copied object
    :param mpu_id: The UploadId returned from the create_multipart_upload call
    :param part_size: The size parts that the object will be broken into, in bytes.
                      Minimum 5 MiB, Maximum 5 GiB. There is no minimum size for the
 last part of your multipart upload.
    :return: part_list for the multipart copy if all parts are copied successfully,
 else None
    '''

    part_list = []
    copy_source = {
        'Bucket': source_bucket_name,
        'Key': key_name
    }
```

```
    try:
        part_counter = 1
        object_size = head_object(s3_client, source_bucket_name, key_name)
        if object_size is not None:
            object_size = object_size['ContentLength']
        while (part_counter - 1) * part_size <object_size:
            bytes_start = (part_counter - 1) * part_size
            bytes_end = (part_counter * part_size) - 1
            upload_copy_part = s3_client.upload_part_copy (
                Bucket = target_bucket_name,
                CopySource = copy_source,
                CopySourceRange = f'bytes={bytes_start}-{bytes_end}',
                Key = key_name,
                PartNumber = part_counter,
                UploadId = mpu_id
            )
            part_list.append({'PartNumber': part_counter, 'ETag':
 upload_copy_part['CopyPartResult']['ETag']})
            part_counter += 1
    except ClientError as e:
        logging.error(e)
        return None
    return part_list

def complete_multipart_upload(s3_client, bucket_name, key_name, mpu_id, part_list):
    '''
    Completes a multipart upload to a directory bucket

    :param s3_client: boto3 S3 client
    :param bucket_name: Destination bucket for the multipart upload
    :param key_name: Key name of the object to be uploaded
    :param mpu_id: The UploadId returned from the create_multipart_upload call
    :param part_list: List of uploaded part numbers with associated ETags
    :return: True if the multipart upload was completed successfully, else False
    '''

    try:
        s3_client.complete_multipart_upload(
            Bucket = bucket_name,
            Key = key_name,
            UploadId = mpu_id,
            MultipartUpload = {
                'Parts': part_list
            }
```

```
        )
    except ClientError as e:
        logging.error(e)
        return False
    return True

if __name__ == '__main__':
    MB = 1024 ** 2
    region = 'us-west-2'
    source_bucket_name = 'SOURCE_BUCKET_NAME'
    target_bucket_name = 'TARGET_BUCKET_NAME'
    key_name = 'KEY_NAME'
    part_size = 10 * MB
    s3_client = boto3.client('s3', region_name = region)
    mpu_id = create_multipart_upload(s3_client, target_bucket_name, key_name)
    if mpu_id is not None:
        part_list = multipart_copy_upload(s3_client, source_bucket_name, key_name,
 target_bucket_name, mpu_id, part_size)
        if part_list is not None:
            if complete_multipart_upload(s3_client, target_bucket_name, key_name,
 mpu_id, part_list):
                print (f'{key_name} successfully copied through multipart copy from
 {source_bucket_name} to {target_bucket_name}')
            else:
                print (f'Could not copy {key_name} through multipart copy from
 {source_bucket_name} to {target_bucket_name}')
```

AWS CLI を使用する場合

次の例は、AWS CLI を使用して、マルチパートアップロードを使って、あるバケットからあるディレクトリバケットにオブジェクトをプログラムでコピーする方法を示しています。このコマンドを使用する際は、*###############*を独自の情報に置き換えます。

```
aws s3api upload-part-copy --bucket bucket-base-name--zone-id--x-s3 --
key TARGET_KEY_NAME --copy-source SOURCE_BUCKET_NAME/SOURCE_KEY_NAME --part-number 1 --
upload-id
 "AS_mgt9RaQE9GEaifATue15dAAAAAAAAAAEMAAAAAAAAADQwNzI4MDU0MjUyMBYAAAAAAAAAAA0AAAAAAAAAAH2AfYAA
```

詳細については、「AWS Command Line Interface」の「upload-part-copy」を参照してください。

進行中のマルチパートアップロードの一覧表示

ディレクトリバケットへの進行中のマルチパートアップロードをリスト表示するには、AWS SDK または AWS CLI を使用できます。

AWS SDK の使用

SDK for Java 2.x

次の例は、SDK for Java 2.x を使用して、進行中の (不完全な) マルチパートアップロードをリスト表示する方法を示しています。

Example

```
public static void listMultiPartUploads( S3Client s3, String bucketName) {
       try {
           ListMultipartUploadsRequest listMultipartUploadsRequest =
ListMultipartUploadsRequest.builder()
               .bucket(bucketName)
               .build();

           ListMultipartUploadsResponse response =
s3.listMultipartUploads(listMultipartUploadsRequest);
           List MultipartUpload uploads = response.uploads();
           for (MultipartUpload upload: uploads) {
               System.out.println("Upload in progress: Key = \"" + upload.key() +
"\", id = " + upload.uploadId());
           }
     }
     catch (S3Exception e) {
           System.err.println(e.getMessage());
           System.exit(1);
     }
 }
```

SDK for Python

次の例は、SDK for Python を使用して、進行中の (不完全な) マルチパートアップロードをリスト表示する方法を示しています。

Example

```
import logging
```

```
import boto3
from botocore.exceptions import ClientError

def list_multipart_uploads(s3_client, bucket_name):
    '''
    List any incomplete multipart uploads in a directory bucket in e specified gion

    :param s3_client: boto3 S3 client
    :param bucket_name: Bucket to check for incomplete multipart uploads
    :return: List of incomplete multipart uploads if there are any, None if not
    '''

    try:
        response = s3_client.list_multipart_uploads(Bucket = bucket_name)
        if 'Uploads' in response.keys():
            return response['Uploads']
        else:
            return None
    except ClientError as e:
        logging.error(e)

if __name__ == '__main__':
    bucket_name = 'BUCKET_NAME'
    region = 'us-west-2'
    s3_client = boto3.client('s3', region_name = region)
    multipart_uploads = list_multipart_uploads(s3_client, bucket_name)
    if multipart_uploads is not None:
        print (f'There are {len(multipart_uploads)} ncomplete multipart uploads for
 {bucket_name}')
    else:
        print (f'There are no incomplete multipart uploads for {bucket_name}')
```

AWS CLI を使用する場合

次の例は、AWS CLI を使用して、進行中の (不完全な) マルチパートアップロードをリスト表示する方法を示しています。このコマンドを使用する際は、*###############*を独自の情報に置き換えます。

```
aws s3api list-multipart-uploads --bucket bucket-base-name--zone-id--x-s3
```

詳細については、「AWS Command Line Interface」の「list-multipart-uploads」を参照してください。

マルチパートアップロードパートの一覧表示

次の例は、ディレクトリバケットへのマルチパートアップロードの一部をリスト表示する方法を示しています。

AWS SDK の使用

SDK for Java 2.x

次の例は、SDK for Java 2.x を使用して、ディレクトリバケットへのマルチパートアップロードの一部をリスト表示する方法を示しています。

```
public static void listMultiPartUploadsParts( S3Client s3, String bucketName, String
 objKey, String uploadID) {

        try {
            ListPartsRequest listPartsRequest = ListPartsRequest.builder()
                .bucket(bucketName)
                .uploadId(uploadID)
                .key(objKey)
                .build();

            ListPartsResponse response = s3.listParts(listPartsRequest);
            ListPart parts = response.parts();
            for (Part part: parts) {
                System.out.println("Upload in progress: Part number = \"" +
 part.partNumber() + "\", etag = " + part.eTag());
            }

        }

        catch (S3Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }


    }
```

SDK for Python

次の例は、SDK for Python を使用して、ディレクトリバケットへのマルチパートアップロードの一部をリスト表示する方法を示しています。

```
import logging
import boto3
from botocore.exceptions import ClientError

def list_parts(s3_client, bucket_name, key_name, upload_id):
    '''
    Lists the parts that have been uploaded for a specific multipart upload to a
 directory bucket.

    :param s3_client: boto3 S3 client
    :param bucket_name: Bucket that multipart uploads parts have been uploaded to
    :param key_name: Name of the object that has parts uploaded
    :param upload_id: Multipart upload ID that the parts are associated with
    :return: List of parts associated with the specified multipart upload, None if
 there are no parts
    '''
    parts_list = []
    next_part_marker = ''
    continuation_flag = True
    try:
        while continuation_flag:
            if next_part_marker == '':
                response = s3_client.list_parts(
                    Bucket = bucket_name,
                    Key = key_name,
                    UploadId = upload_id
                )
            else:
                response = s3_client.list_parts(
                    Bucket = bucket_name,
                    Key = key_name,
                    UploadId = upload_id,
                    NextPartMarker = next_part_marker
                )
            if 'Parts' in response:
                for part in response['Parts']:
                    parts_list.append(part)
                if response['IsTruncated']:
                    next_part_marker = response['NextPartNumberMarker']
                else:
                    continuation_flag = False
            else:
                continuation_flag = False
```

```
        return parts_list
    except ClientError as e:
        logging.error(e)
        return None

if __name__ == '__main__':
    region = 'us-west-2'
    bucket_name = 'BUCKET_NAME'
    key_name = 'KEY_NAME'
    upload_id = 'UPLOAD_ID'
    s3_client = boto3.client('s3', region_name = region)
    parts_list = list_parts(s3_client, bucket_name, key_name, upload_id)
    if parts_list is not None:
        print (f'{key_name} has {len(parts_list)} parts uploaded to {bucket_name}')
    else:
        print (f'There are no multipart uploads with that upload ID for
 {bucket_name} bucket')
```

AWS CLI を使用する場合

次の例は、AWS CLI を使用して、ディレクトリバケットへのマルチパートアップロードの一部をリスト表示する方法を示しています。このコマンドを使用する際は、*###############*を独自の情報に置き換えます。

```
aws s3api list-parts --bucket bucket-base-name--zone-id--x-s3 --key KEY_NAME --upload-
id
 "AS_mgt9RaQE9GEaifATue15dAAAAAAAAAAEMAAAAAAAAADQwNzI4MDU0MjUyMBYAAAAAAAAAAA0AAAAAAAAAAH2AfYAA
```

詳細については、「AWS Command Line Interface」の「list-parts」を参照してください。

ディレクトリバケットから、またはディレクトリバケットへのオブジェクトのコピー

コピーオペレーションを行うと、Amazon S3 内に既に格納されているオブジェクトのコピーが作成されます。ディレクトリバケットと汎用バケット間でオブジェクトをコピーできます。また、単一のバケット内または同じタイプのバケット間でオブジェクトをコピーすることもできます。例えば、ディレクトリバケットからディレクトリバケットへとオブジェクトをコピーできます。

> **Note**
>
> ソースバケットまたは送信先バケットが AWS Local Zone にある場合、異なる AWS リージョン間でのオブジェクトのコピーはサポートされていません。ソースバケットと送信先バケットは、親 AWS リージョンが同じである必要があります。ソースバケットと送信先バケットは、異なるバケットの場所タイプ (アベイラビリティーゾーンまたは Local Zone) にすることができます。

1 回のアトミックオペレーションでコピーできるオブジェクトのサイズは最大 5 GB です。5 GB を超えるオブジェクトをコピーする場合は、マルチパートアップロード API オペレーションを使用する必要があります。詳細については、「ディレクトリバケットでのマルチパートアップロードの使用」を参照してください。

アクセス許可

これを実行するには、次のアクセス許可が必要です。

- あるディレクトリバケットから別のディレクトリバケットにオブジェクトをコピーするには、`s3express:CreateSession` アクセス許可が必要です。
- ディレクトリバケットから汎用バケットにオブジェクトをコピーするには、コピー先バケットにオブジェクトコピーを書き込む `s3express:CreateSession` アクセス許可と `s3:PutObject` アクセス許可が必要です。
- 汎用バケットからディレクトリバケットにオブジェクトをコピーするには、`s3express:CreateSession` アクセス許可とコピーされるソースオブジェクトを読み取る `s3:GetObject` アクセス許可が必要です。

  詳細については、「Amazon Simple Storage Service API リファレンス」の「CopyObject」を参照してください。

Encryption

Amazon S3 は、S3 バケットにコピーされたすべての新しいオブジェクトを自動的に暗号化します。S3 バケットのデフォルトの暗号化設定は常に有効になっており、最低でも Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3) に設定されています。

ディレクトリバケットでは、SSE-S3 と AWS Key Management Service (AWS KMS) キーによるサーバー側の暗号化 (SSE-KMS) がサポートされています。レプリケート先バケットがディレクトリ

バケットの場合、レプリケート先バケットのデフォルトの暗号化では必要な暗号化設定を使用することをお勧めします。また、バケットのデフォルトの暗号化を上書きしないことをお勧めします。その後、新しいオブジェクトは必要な暗号化設定で自動的に暗号化されます。SSE-KMS で暗号化されたオブジェクトを、CopyObject を使用して、汎用バケットからディレクトリバケットへ、ディレクトリバケットから汎用バケットへ、またはディレクトリバケット間でコピーする場合、S3 バケットキーはサポートされません。この場合、KMS で暗号化されたオブジェクトのコピーリクエストが実行されるたびに、Amazon S3 は AWS KMS を呼び出します。ディレクトリバケットの暗号化の上書き動作の詳細については、「新しいオブジェクトのアップロードに AWS KMS によるサーバー側の暗号化を指定する」を参照してください。

汎用バケットの場合、SSE-S3 (デフォルト)、AWS Key Management Service (AWS KMS) キーを使用したサーバー側の暗号化 (SSE-KMS)、AWS KMS キーを使用した二層式サーバー側の暗号化 (DSSE-KMS)、またはお客様が用意したキーによるサーバー側の暗号化 (SSE-C) を使用できます。

ディレクトリバケットの DSSE-KMS、または SSE-C パラメータをソースまたは送信先として設定するコピーリクエストを実行すると、応答でエラーが返されます。

[タグ]

ディレクトリバケットは タグをサポートしていません。タグ付きのオブジェクトを汎用バケットからディレクトリバケットにコピーすると、HTTP `501 (Not Implemented)` の応答が返されます。詳細については、「Amazon Simple Storage Service API リファレンス」の「CopyObject」を参照してください。

ETag

S3 Express One Zone のエンティティタグ (ETag) はランダムな英数字文字列であり、MD5 チェックサムではありません。オブジェクトの整合性を確保するには、追加のチェックサムを使用します。

追加のチェックサム

S3 Express One Zone では、アップロードまたはダウンロード中にデータを検証するために使用されるチェックサムアルゴリズムを選択するオプションが提供されます。CRC32、CRC32C、SHA-1、SHA-256 などのセキュアハッシュアルゴリズム (SHA) や巡回冗長検査 (CRC) データ整合性チェックアルゴリズムのいずれかを選択できます。MD5 ベースのチェックサムは S3 Express One Zone ストレージクラスではサポートされていません。

詳細については、「S3 の追加のチェックサムのベストプラクティス」を参照してください。

サポートされている機能

S3 Express One Zone でサポートされている Amazon S3 機能については、「ディレクトリバケットの違い」を参照してください。

S3 コンソールの使用 (ディレクトリバケットへのコピー)

> **Note**
>
> コンソールでオブジェクトをディレクトリバケットにコピーする際の制約と制限は次のとおりです。
>
> - Copy アクションは、指定されたフォルダ (プレフィックス) 内のすべてのオブジェクトに適用されます。アクションの進行中にこれらのフォルダに追加されたオブジェクトが影響を受ける可能性があります。
> - お客様が提供する暗号化キー (SSE-C) で暗号化されたオブジェクトは、S3 コンソールを使用してコピーすることはできません。SSE-C で暗号化されたオブジェクトをコピーするには、AWS CLI、AWS SDK、または Amazon S3 REST API を使用します。
> - コピーされたオブジェクトは、元のオブジェクトの Object Lock 設定を保持しません。
> - オブジェクトのコピー元のバケットが S3 オブジェクト所有者にバケット所有者強制設定を使用している場合、オブジェクト ACL は指定された宛先にコピーされません。
> - S3 オブジェクト所有権にバケット所有者強制設定を使用するバケットにオブジェクトをコピーする場合は、ソースバケットでもバケット所有者強制設定が使用されていることを確認するか、他の AWS アカウントおよびグループへのオブジェクト ACL 許可を削除します。
> - 汎用バケットからディレクトリバケットにコピーされたオブジェクトは、オブジェクトタグ、ACLまたは Etag 値を保持しません。チェックサム値はコピーできますが、Etag と同等ではありません。チェックサム値は、追加時と異なる場合があります。
> - ディレクトリバケットにコピーされたすべてのオブジェクトは、S3 オブジェクト所有権のバケット所有者強制設定になります。

汎用バケットまたはディレクトリバケットからディレクトリバケットにオブジェクトをコピーするには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、オブジェクトのコピー元のバケットタイプ:

- 汎用バケットからコピーするには、[汎用バケット] タブをクリックします。
- ディレクトリバケットからコピーするには、[ディレクトリバケット] タブをクリックします。

3. コピーするオブジェクトが含まれる汎用バケットまたはディレクトリバケットを選択します。
4. [オブジェクト] タブを選択します。[オブジェクト] ページで、コピーするオブジェクトの名前の左にあるチェックボックスをオンにします。
5. [Actions (アクション)] メニューで [Copy (コピー)] を選択します。

   [コピー] ページが表示されます。
6. [送信先] で、送信先タイプに [ディレクトリバケット] を選択します。送信先パスを指定するには、[S3 の参照] を選択し、送信先に移動して、送信先の左側にあるオプションボタンを選択します。右下の [Choose destination] (送信先を選択する) を選択します。

   または、送信先パスを入力します。
7. [追加のコピー設定] で、[ソース設定をコピー] するか、[設定を指定しない] か、[設定を指定] するかを選択します。[ソース設定をコピー] がデフォルトのオプションです。ソース設定の属性なしでオブジェクトのみをコピーする場合は、[設定を指定しない] を選択します。サーバー側の暗号化、チェックサム、メタデータの設定を指定するには、[設定を指定] を選択します。
8. 右下の [Copy] (コピー) を選択します。Amazon S3 によってオブジェクトがコピー先にコピーされます。

S3 コンソールの使用 (汎用バケットへのコピー)

> **Note**
>
> コンソールでオブジェクトを汎用バケットにコピーする際の制約と制限は次のとおりです。
>
> - Copy アクションは、指定されたフォルダ (プレフィックス) 内のすべてのオブジェクトに適用されます。アクションの進行中にこれらのフォルダに追加されたオブジェクトが影響を受ける可能性があります。
> - お客様が提供する暗号化キー (SSE-C) で暗号化されたオブジェクトは、S3 コンソールを使用してコピーすることはできません。SSE-C で暗号化されたオブジェクトをコピーするには、AWS CLI、AWS SDK、または Amazon S3 REST API を使用します。
> - コピーされたオブジェクトは、元のオブジェクトの Object Lock 設定を保持しません。
> - オブジェクトのコピー元のバケットが S3 オブジェクト所有者にバケット所有者強制設定を使用している場合、オブジェクト ACL は指定された宛先にコピーされません。

- S3 オブジェクト所有権にバケット所有者強制設定を使用するバケットにオブジェクトをコピーする場合は、ソースバケットでもバケット所有者強制設定が使用されていることを確認するか、他の AWS アカウントおよびグループへのオブジェクト ACL 許可を削除します。

ディレクトリバケットから汎用バケットにオブジェクトをコピーするには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。
3. [ディレクトリバケット] タブをクリックします。
4. コピーするオブジェクトが含まれるディレクトリバケットを選択します。
5. [オブジェクト] タブを選択します。[オブジェクト] ページで、コピーするオブジェクトの名前の左にあるチェックボックスをオンにします。
6. [Actions (アクション)] メニューで [Copy (コピー)] を選択します。
7. [送信先] で、送信先に [汎用バケット] を選択します。送信先パスを指定するには、[S3 の参照] を選択し、送信先に移動して、送信先の左側にあるオプションボタンを選択します。右下の [Choose destination] (送信先を選択する) を選択します。

   または、送信先パスを入力します。
8. [追加のコピー設定] で、[ソース設定をコピー] するか、[設定を指定しない] か、[設定を指定] するかを選択します。[ソース設定をコピー] がデフォルトのオプションです。ソース設定の属性なしでオブジェクトのみをコピーする場合は、[設定を指定しない] を選択します。ストレージクラス、ACL、オブジェクトタグ、メタデータ、サーバー側の暗号化、その他のチェックサムの設定を指定するには、[設定を指定] を選択します。
9. 右下の [Copy] (コピー) を選択します。Amazon S3 によってオブジェクトがコピー先にコピーされます。

AWS SDK の使用

SDK for Java 2.x

Example

```
public static void copyBucketObject (S3Client s3, String sourceBucket, String
objectKey, String targetBucket) {
     CopyObjectRequest copyReq = CopyObjectRequest.builder()
         .sourceBucket(sourceBucket)
         .sourceKey(objectKey)
         .destinationBucket(targetBucket)
         .destinationKey(objectKey)
         .build();
      String temp = "";

      try {
          CopyObjectResponse copyRes = s3.copyObject(copyReq);
          System.out.println("Successfully copied " + objectKey +" from bucket " +
sourceBucket +" into bucket "+targetBucket);
      }

      catch (S3Exception e) {
          System.err.println(e.awsErrorDetails().errorMessage());
          System.exit(1);
      }
}
```

AWS CLI を使用する場合

次の copy-object コマンド例は、AWS CLI を使用して、オブジェクトをあるバケットから別のバケットにコピーする方法を示しています。複数のバケットタイプ間でオブジェクトをコピーできます。このコマンドを実行するには、ユーザー入力プレースホルダーをユーザー自身の情報に置き換えます。

```
aws s3api copy-object --copy-source SOURCE_BUCKET/SOURCE_KEY_NAME --key TARGET_KEY_NAME
 --bucket TARGET_BUCKET_NAME
```

詳細については、AWS CLI コマンドリファレンスの「copy-object」を参照してください。

ディレクトリバケットのオブジェクトの削除

Amazon S3 コンソール、AWS Command Line Interface (AWS CLI)、または AWS SDK を使用して、Amazon S3 ディレクトリバケットからオブジェクトを削除できます。詳細については、「ディレクトリバケットの使用」および「S3 Express One Zone」を参照してください。

Warning

- オブジェクトを削除すると元に戻せません。
- このアクションは、指定されたすべてのオブジェクトを削除します。フォルダを削除する場合は、削除アクションが完了するのを待ってから、フォルダに新しいオブジェクトを追加します。そうしなければ、新しいオブジェクトも削除される可能性があります。

Note

ディレクトリバケットからプログラムを使用して複数のオブジェクトを削除する場合は、次の点に注意してください。

- `DeleteObjects` リクエストのオブジェクトキーには、空白以外の文字を 1 つ以上含める必要があります。空白文字のみを含めることはできません。
- `DeleteObjects` リクエストのオブジェクトキーには、改行 (\n)、タブ (\t)、キャリッジリターン (\r) 文字を除き、Unicode 制御文字を含めることはできません。

S3 コンソールの使用

オブジェクトを削除するには

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 左のナビゲーションペインで、[ディレクトリバケット] を選択します。
3. 削除するオブジェクトが含まれるディレクトリバケットを選択します。
4. [オブジェクト] タブを選択します。[オブジェクト] リストで、削除するオブジェクト (複数選択可) の左にあるチェックボックスをオンにします。
5. [削除] を選択します。

6. [オブジェクトの削除] ページで、テキストボックスに「**permanently delete**」を入力します。
7. [オブジェクトの削除] を選択します。

AWS SDK の使用

SDK for Java 2.x

Example

次の例では、AWS SDK for Java 2.x を使用してディレクトリバケット内のオブジェクトを削除します。

```
static void deleteObject(S3Client s3Client, String bucketName, String objectKey) {



        try {

            DeleteObjectRequest del = DeleteObjectRequest.builder()
                    .bucket(bucketName)
                    .key(objectKey)
                    .build();

            s3Client.deleteObject(del);

            System.out.println("Object " + objectKey + " has been deleted");


        } catch (S3Exception e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }

    }
```

SDK for Python

Example

次の例では、AWS SDK for Python (Boto3) を使用してディレクトリバケット内のオブジェクトを削除します。

```
import logging
import boto3
from botocore.exceptions import ClientError

def delete_objects(s3_client, bucket_name, objects):
    '''
    Delete a list of objects in a directory bucket

    :param s3_client: boto3 S3 client
    :param bucket_name: Bucket that contains objects to be deleted; for example,
 'doc-example-bucket--usw2-az1--x-s3'
    :param objects: List of dictionaries that specify the key names to delete
    :return: Response output, else False
    '''

    try:
        response = s3_client.delete_objects(
            Bucket = bucket_name,
            Delete = {
                'Objects': objects
            }
        )
        return response
    except ClientError as e:
        logging.error(e)
        return False


if __name__ == '__main__':
    region = 'us-west-2'
    bucket_name = 'BUCKET_NAME'
    objects = [
        {
            'Key': '0.txt'
        },
        {
            'Key': '1.txt'
        },
        {
            'Key': '2.txt'
        },
        {
```

```
            'Key': '3.txt'
        },
        {
            'Key': '4.txt'
        }
    ]

    s3_client = boto3.client('s3', region_name = region)
    results = delete_objects(s3_client, bucket_name, objects)
    if results is not None:
        if 'Deleted' in results:
            print (f'Deleted {len(results["Deleted"])} objects from {bucket_name}')
        if 'Errors' in results:
            print (f'Failed to delete {len(results["Errors"])} objects from
{bucket_name}')
```

AWS CLI を使用する場合

次の delete-object コマンド例は、AWS CLI を使用してディレクトリバケットからオブジェクトを削除する方法を示しています。このコマンドを実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3api delete-object --bucket bucket-base-name--zone-id--x-s3 --key KEY_NAME
```

詳細については、AWS CLI コマンドリファレンスの「delete-object」を参照してください。

次の delete-objects コマンド例は、AWS CLI を使用してディレクトリバケットからオブジェクトを削除する方法を示しています。このコマンドを実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

delete.json ファイルは次のとおりです。

```
{
    "Objects": [
        {
            "Key": "0.txt"
        },
        {
            "Key": "1.txt"
        },
```

```
        {
            "Key": "2.txt"
        },
        {
            "Key": "3.txt"
        }
    ]
}
```

以下に delete-objects コマンド例を示します。

```
aws s3api delete-objects --bucket bucket-base-name--zone-id--x-s3 --delete
 file://delete.json
```

詳細については、AWS CLI コマンドリファレンスの「delete-objects」を参照してください。

ディレクトリバケットからのオブジェクトのダウンロード

次のコード例は、GetObject API オペレーションを使用して、Amazon S3 ディレクトリバケット内のオブジェクトからデータを (ダウンロードして) 読み取る方法を示しています。

AWS SDK の使用

SDK for Java 2.x

Example

次のコード例は、AWS SDK for Java 2.x を使用して、ディレクトリバケット内のオブジェクトからデータを読み取る方法を示しています。

```
public static void getObject(S3Client s3Client, String bucketName, String objectKey)
 {
     try {
         GetObjectRequest objectRequest = GetObjectRequest
            .builder()
            .key(objectKey)
            .bucket(bucketName)
            .build();

         ResponseBytes GetObjectResponse objectBytes =
 s3Client.getObjectAsBytes(objectRequest);
         byte[] data = objectBytes.asByteArray();
```

```
         //Print object contents to console
         String s = new String(data, StandardCharsets.UTF_8);
         System.out.println(s);
    }

    catch (S3Exception e) {
        System.err.println(e.awsErrorDetails().errorMessage());
        System.exit(1);
    }
}
```

SDK for Python

Example

次のコード例は、AWS SDK for Python (Boto3) を使用して、ディレクトリバケット内のオブジェクトからデータを読み取る方法を示しています。

```
import boto3
from botocore.exceptions import ClientError
from botocore.response import StreamingBody

def get_object(s3_client: boto3.client, bucket_name: str, key_name: str) ->
 StreamingBody:
    """
    Gets the object.
    :param s3_client:
    :param bucket_name: The bucket that contains the object.
    :param key_name: The key of the object to be downloaded.
    :return: The object data in bytes.
    """
    try:
        response = s3_client.get_object(Bucket=bucket_name, Key=key_name)
        body = response['Body'].read()
        print(f"Got object '{key_name}' from bucket '{bucket_name}'.")
    except ClientError:
        print(f"Couldn't get object '{key_name}' from bucket '{bucket_name}'.")
        raise
    else:
        return body

def main():
    s3_client = boto3.client('s3')
```

```
    resp = get_object(s3_client, 'doc-example-bucket--use1-az4--x-s3', 'sample.txt')
    print(resp)

if __name__ == "__main__":
     main()
```

AWS CLI を使用する場合

次の get-object コマンド例は、AWS CLI を使用して Amazon S3 からオブジェクトをダウンロードする方法を示しています。このコマンドは、ディレクトリバケット *bucket-base-name*--*zone-id*--x-s3 からオブジェクト *KEY_NAME* を取得します。オブジェクトは、*LOCAL_FILE_NAME* という名前のファイルにダウンロードされます。このコマンドを実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3api get-object --bucket bucket-base-name--zone-id--x-s3 --
key KEY_NAME LOCAL_FILE_NAME
```

詳細については、AWS CLI コマンドリファレンスの「get-object」を参照してください。

オブジェクトディレクトリバケットを共有するための署名付き URL の生成

次の例は、Amazon S3 ディレクトリバケットからオブジェクトを共有するための署名付き URL を生成する方法の例を示しています。

AWS CLI を使用する場合

次のコマンド例は、AWS CLI を使用して Amazon S3 からオブジェクトの署名付き URL を生成する方法を示しています。このコマンドは、ディレクトリバケット *bucket-base-name*--*zone-id*--x-s3 からオブジェクト *KEY_NAME* の署名付き URL を生成します。このコマンドを実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3 presign s3://bucket-base-name--zone-id--x-s3/KEY_NAME --expires-in 7200
```

詳細については、AWS CLI コマンドリファレンスの「presign」を参照してください。

ディレクトリバケットからのオブジェクトメタデータの取得

次の AWS SDK と AWS CLI の例は、HeadObject と GetObjectAttributes API オペレーションを使用して、オブジェクト自体は返さずに Amazon S3 ディレクトリバケット内のオブジェクトからメタデータを取得する方法を示しています。

AWS SDK の使用

SDK for Java 2.x

Example

```
public static void headObject(S3Client s3Client, String bucketName, String
 objectKey) {
    try {
        HeadObjectRequest headObjectRequest = HeadObjectRequest
                .builder()
                .bucket(bucketName)
                .key(objectKey)
                .build();
        HeadObjectResponse response = s3Client.headObject(headObjectRequest);
        System.out.format("Amazon S3 object: \"%s\" found in bucket: \"%s\" with
 ETag: \"%s\"", objectKey, bucketName, response.eTag());
    }
    catch (S3Exception e) {
        System.err.println(e.awsErrorDetails().errorMessage());
```

AWS CLI を使用する場合

次の head-object コマンド例は、AWS CLI を使用してオブジェクトからメタデータを取得する方法を示しています。このコマンドを実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3api head-object --bucket bucket-base-name--zone-id--x-s3 --key KEY_NAME
```

詳細については、AWS CLI コマンドリファレンスの「head-object」を参照してください。

次の get-object-attributes コマンド例は、AWS CLI を使用してオブジェクトからメタデータを取得する方法を示しています。このコマンドを実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3api get-object-attributes --bucket bucket-base-name--zone-id--x-s3 --key KEY_NAME
 --object-attributes "StorageClass" "ETag" "ObjectSize"
```

詳細については、AWS CLI コマンドリファレンスの「get-object-attributes」を参照してください。

ディレクトリバケットからのオブジェクトの一覧表示

次のコード例は、ListObjectsV2 API オペレーションを使用して、Amazon S3 ディレクトリバケット内でオブジェクトを一覧表示する方法を示しています。

AWS CLI を使用する場合

次の list-objects-v2 コマンド例は、AWS CLI を使用して Amazon S3 からオブジェクトを一覧表示する方法を示しています。このコマンドは、ディレクトリバケット *bucket-base-name*--*zone-id*--x-s3 からのオブジェクトを一覧表示します。このコマンドを実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3api list-objects-v2 --bucket bucket-base-name--zone-id--x-s3
```

詳細については、AWS CLI コマンドリファレンスの「list-objects-v2」を参照してください。

ディレクトリバケットのセキュリティ

AWS でのクラウドセキュリティは最優先事項です。AWS のユーザーは、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャを利用できます。セキュリティは、AWS とお客様との間での責任共有です。責任共有モデルでは、この責任がクラウドのセキュリティおよびクラウド内のセキュリティとして説明されています。

- クラウドのセキュリティ — AWS は、AWS クラウド で AWS のサービス を実行するインフラストラクチャを保護する責任を負います。また AWS は、お客様が使用するサービスを安全に提供します。AWS Compliance Programs の一環として、サードパーティーの監査人が定期的にセキュリティの有効性をテストおよび検証します。

  コンプライアンスプログラムの詳細については、「AWS のサービス in Scope by Compliance Program」を参照してください。
- クラウド内のセキュリティ — お客様の責任は、使用する AWS のサービス に応じて異なります。また、お客様は、お客様のデータの機密性、企業の要件、および適用可能な法律および規制などの他の要因についても責任を担います。

このドキュメントは、ディレクトリバケットを使用する際に責任共有モデルをどのように適応するかを理解するのに役立ちます。以下のトピックでは、セキュリティとコンプライアンスの目的を満たすようにディレクトリバケットを設定する方法について説明します。また、ディレクトリバケット内の

オブジェクトをモニタリングして保護するのに役立つ他の AWS のサービスを使用する方法についても説明します。

データ保護と暗号化

ディレクトリバケットの暗号化を設定する方法の詳細については、以下のトピックを参照してください。

トピック

- サーバー側の暗号化
- ディレクトリバケットのデフォルト暗号化の設定とモニタリング
- ディレクトリバケットでの AWS KMS キーによるサーバー側の暗号化 (SSE-KMS) の使用
- 転送中の暗号化
- データの削除

サーバー側の暗号化

すべてのディレクトリバケットにはデフォルトで暗号化が設定されており、ディレクトリバケットにアップロードされたすべての新しいオブジェクトは保存時に自動的に暗号化されます。Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3) は、すべてのディレクトリバケットでのデフォルトの暗号化設定です。別の暗号化タイプを指定する場合は、バケットのデフォルトの暗号化設定を設定することで、AWS Key Management Service (AWS KMS) キーによるサーバー側の暗号化 (SSE-KMS) を使用できます。ディレクトリバケットの SSE-KMS の詳細については、「ディレクトリバケットでの AWS KMS キーによるサーバー側の暗号化 (SSE-KMS) の使用」を参照してください。

バケットのデフォルトの暗号化では、必要な暗号化設定を使用することをお勧めします。`CreateSession` リクエストまたは PUT オブジェクトリクエストでは、バケットのデフォルトの暗号化を上書きしないことをお勧めします。その後、新しいオブジェクトは必要な暗号化設定で自動的に暗号化されます。ディレクトリバケットの暗号化の上書き動作の詳細については、「新しいオブジェクトのアップロードに AWS KMS を使用してサーバー側の暗号化を指定する」を参照してください。

ディレクトリバケットを使用する SSE-KMS は、以下の点で汎用バケットの SSE-KMS とは異なります。

- SSE-KMS 設定では、バケットの存続期間中、ディレクトリバケットごとに 1 つのカスタマーマネージドキーしかサポートできません。AWS マネージドキー (`aws/s3`) はサポートされていませ

ん。また、SSE-KMS のカスタマーマネージドキーを指定した後は、バケットの SSE-KMS 設定のカスタマーマネージドキーを上書きすることはできません。

バケットの SSE-KMS 設定に指定したカスタマーマネージドキーは、次のように識別できます。

- `HeadObject` API オペレーションリクエストを実行して、レスポンス内の `x-amz-server-side-encryption-aws-kms-key-id` の値を検索します。

データに新しいカスタマーマネージドキーを使用するには、新しいカスタマーマネージドキーを使用して既存のオブジェクトを新しいディレクトリバケットにコピーすることをお勧めします。

- CopyObject および UploadPartCopy を除くゾーンエンドポイント (オブジェクトレベル) API オペレーションでは、CreateSession を介してリクエストを認証および承認して低レイテンシーを実現します。バケットのデフォルトの暗号化では、必要な暗号化設定を使用することをお勧めします。`CreateSession` リクエストまたは PUT オブジェクトリクエストでは、バケットのデフォルトの暗号化を上書きしないことをお勧めします。その後、新しいオブジェクトは必要な暗号化設定で自動的に暗号化されます。SSE-KMS を使用してディレクトリバケット内の新しいオブジェクトを暗号化するには、KMS キー (特にカスタマーマネージドキー) を使用してディレクトリバケットのデフォルトの暗号化設定として SSE-KMS を指定する必要があります その後、ゾーンエンドポイント API オペレーションのセッションが作成されると、セッション中に新しいオブジェクトが SSE-KMS および S3 バケットキーで自動的に暗号化および復号されます。ディレクトリバケットの暗号化の上書き動作の詳細については、「新しいオブジェクトのアップロードに AWS KMS を使用してサーバー側の暗号化を指定する」を参照してください。

  ゾーンエンドポイント API コール (CopyObject および UploadPartCopy を除く) では、`CreateSession` リクエストの暗号化設定 (`x-amz-server-side-encryption`、`x-amz-server-side-encryption-aws-kms-key-id`、`x-amz-server-side-encryption-context`、`x-amz-server-side-encryption-bucket-key-enabled`) の値を上書きすることはできません。ゾーンエンドポイント API コールでこれらの暗号化設定値を明示的に指定する必要はありません。Amazon S3 は `CreateSession` リクエストの暗号化設定値を使用してディレクトリバケット内の新しいオブジェクトを保護します。

  > **Note**
  >
  > AWS CLI または AWS SDK を使用する場合、セッショントークンは `CreateSession` に対して自動的に更新され、セッションの有効期限が切れたときのサービス中断を回避します。AWS CLI または AWS SDK は、`CreateSession` リクエストにバケットのデフォルトの暗号化設定を使用します。`CreateSession` リクエストの暗号化設定値を上書きすることはサポートされていません。また、ゾーンエンドポイント API コール (CopyObject お

よび UploadPartCopy を除く) では、CreateSession リクエストからの暗号化設定の値を上書きすることはできません。

- CopyObject の場合、SSE-KMS を使用してディレクトリバケット内の新しいオブジェクトコピーを暗号化するには、KMS キー (特にカスタマーマネージドキー) を使用してディレクトリバケットのデフォルトの暗号化設定として SSE-KMS を指定する必要があります。次に、SSE-KMS で新しいオブジェクトコピーにサーバー側の暗号化設定を指定するときは、暗号化キーがディレクトリバケットのデフォルトの暗号化設定に指定したカスタマーマネージドキーと同じであることを確認する必要があります。UploadPartCopy では、SSE-KMS を使用してディレクトリバケット内の新しいオブジェクトパーツコピーを暗号化するには、KMS キー (特にカスタマーマネージドキー) を使用してディレクトリバケットのデフォルトの暗号化設定として SSE-KMS を指定する必要があります。UploadPartCopy リクエストヘッダーで SSE-KMS を使用して新しいオブジェクトパートコピーのサーバー側の暗号化設定を指定することはできません。また、CreateMultipartUpload リクエストで指定する暗号化設定は、送信先バケットのデフォルトの暗号化設定と一致する必要があります。
- S3 バケットキーは、ディレクトリバケット内の GET および PUT オペレーションで常に有効になっており、無効にすることはできません。SSE-KMS で暗号化されたオブジェクトを、CopyObject、UploadPartCopy、バッチオペレーションの Copy オペレーション、または import ジョブを使用して、汎用バケットからディレクトリバケットへ、ディレクトリバケットから汎用バケットへ、またはディレクトリバケット間でコピーする場合、S3 バケットキーはサポートされません。この場合、KMS で暗号化されたオブジェクトのコピーリクエストが実行されるたびに、Amazon S3 は AWS KMS を呼び出します。
- ディレクトリバケットで暗号化に AWS KMS カスタマーマネージドキーを指定する場合は、キー ID またはキー ARN のみを使用します。KMS キーのキーエイリアス形式はサポートされていません。

ディレクトリバケットは、AWS Key Management Service (AWS KMS) キーによる二層式サーバー側の暗号化 (DSSE-KMS) またはお客様が提供する暗号化キーを使用したサーバー側の暗号化 (SSE-C) をサポートしていません。

ディレクトリバケットのデフォルト暗号化の設定とモニタリング

Amazon S3 バケットにはデフォルトで暗号化が有効化されており、新しいオブジェクトは Amazon S3 マネージドキー (SSE-S3) を使用してサーバー側の暗号化により自動的に暗号化されます。この暗号化は Amazon S3 バケット内のすべての新しいオブジェクトに適用され、費用はかかりません。

キーローテーションやアクセスポリシーの付与の管理など、暗号化キーをより細かく制御する必要がある場合は、AWS Key Management Service (AWS KMS) キーによるサーバー側の暗号化 (SSE-KMS) を使用できます。

> **Note**
>
> - バケットのデフォルト暗号化では、必要な暗号化設定を使用することをお勧めします。`CreateSession` リクエストまたは PUT オブジェクトリクエストでは、バケットのデフォルト暗号化を上書きしないことをお勧めします。その後、新しいオブジェクトは必要な暗号化設定で自動的に暗号化されます。ディレクトリバケットでの暗号化の上書き動作の詳細については、「新しいオブジェクトのアップロードに AWS KMS によるサーバー側の暗号化を指定する」を参照してください。
> - SSE-KMS を使用してディレクトリバケット内の新しいオブジェクトを暗号化するには、KMS キー (特にカスタマーマネージドキー) を使用してディレクトリバケットのデフォルトの暗号化設定として SSE-KMS を指定する必要があります。次に、ゾーンエンドポイント API オペレーションのセッションが作成されると、セッション中に新しいオブジェクトが SSE-KMS および S3 バケットキーで自動的に暗号化および復号されます。
> - デフォルトのバケット暗号化を SSE-KMS に設定すると、S3 バケットキーはディレクトリバケット内の `GET` および `PUT` オペレーションで常に有効になり、無効にすることはできません。SSE-KMS で暗号化されたオブジェクトを、CopyObject、UploadPartCopy、バッチオペレーションの Copy オペレーション、または import ジョブを使用して、汎用バケットからディレクトリバケットへ、ディレクトリバケットから汎用バケットへ、またはディレクトリバケット間でコピーする場合、S3 バケットキーはサポートされません。この場合、KMS で暗号化されたオブジェクトのコピーリクエストが実行されるたびに、Amazon S3 は AWS KMS を呼び出します。S3 バケットキーで AWS KMS リクエストコストを削減する方法の詳細については、「Amazon S3 バケットキーを使用した SSE-KMS のコストの削減」を参照してください。
> - ディレクトリバケットで暗号化に AWS KMS カスタマーマネージドキーを指定する場合は、キー ID またはキー ARN のみを使用します。KMS キーのキーエイリアス形式はサポートされていません。
> - AWS KMS キーによる二層式サーバー側の暗号化 (DSSE-KMS) およびお客様が提供する暗号化キーを使用したサーバー側の暗号化 (SSE-C) は、ディレクトリバケットのデフォルトの暗号化ではサポートされません。

デフォルトの暗号化設定の詳細については、「デフォルトの暗号化の設定」を参照してください。

デフォルトの暗号化に必要なアクセス許可の詳細については、『Amazon Simple Storage Service API リファレンス』の「PutBucketEncryption」を参照してください。

Amazon S3 コンソール、AWS SDK、Amazon S3 REST API、および AWS Command Line Interface (AWS CLI) を使用して、Amazon S3 で S3 バケットのデフォルトの暗号化を設定できます。

S3 コンソールの使用

Amazon S3 バケットにデフォルトの暗号化を設定するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。
3. [バケット] リストで、目的のバケットの名前を選択します。
4. [プロパティ] タブを選択します。
5. [サーバー側の暗号化設定] では、ディレクトリバケットは [Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3)] を使用します。
6. [Save changes] (変更の保存) をクリックします。

AWS CLI を使用する場合

以下の例では、SSE-S3 を使用するか、SSE-KMS と S3 バケット キーを使用して、デフォルトの暗号化を設定する方法を示します。

デフォルトの暗号化の詳細については、[Amazon S3 バケット向けのサーバー側のデフォルトの暗号化動作の設定] を参照してください。AWS CLI を使用してデフォルトの暗号化を設定する方法の詳細については、put-bucket-encryption を参照してください。

Example - SSE-S3 を使用したデフォルトの暗号化

この例では、Amazon S3 マネージドキーを使用したデフォルトのバケット暗号化を設定します。このコマンドを使用するには、*###############*を独自の情報に置き換えます。

```
aws s3api put-bucket-encryption --bucket bucket-base-name--zone-id--x-s3 --server-side-encryption-configuration '{
    "Rules": [
        {
            "ApplyServerSideEncryptionByDefault": {
                "SSEAlgorithm": "AES256"
```

```
            }
        }
    ]
}'
```

Example - S3 バケットキーを使用した SSE-KMS でのデフォルトの暗号化

この例では、S3 バケットキーを使用して SSE-KMS でデフォルトのバケット暗号化を設定します。このコマンドを使用するには、*###############*を独自の情報に置き換えます。

```
aws s3api put-bucket-encryption --bucket bucket-base-name--zone-id--x-s3 --server-side-
encryption-configuration '{
    "Rules": [
            {
                "ApplyServerSideEncryptionByDefault": {
                    "SSEAlgorithm": "aws:kms",
                    "KMSMasterKeyID": "KMS-Key-ARN"
                },
                "BucketKeyEnabled": true
            }
        ]
    }'
```

REST API の使用

REST API PutBucketEncryption オペレーションを使用して、デフォルト暗号化を設定し、使用するサーバー側の暗号化のタイプ (SSE-S3 または SSE-KMS) を設定します。

詳細については、「Amazon Simple Storage Service API リファレンス」の「PutBucketEncryption」を参照してください。

AWS SDK の使用

AWS SDK を使用する場合、サーバー側の暗号化に AWS KMS keys を使用するよう Amazon S3 にリクエストできます。次の AWS SDK for Java および .NET の例では、SSE-KMS と S3 バケットキーを使用してディレクトリバケットのデフォルトの暗号化設定を設定します。他の SDK については、AWS デベロッパーセンターのサンプルコードとライブラリを参照してください。

> **Important**
>
> Amazon S3 でサーバー側の暗号化に AWS KMS key を使用する場合は、対称暗号化 KMS キーを選択する必要があります。Amazon S3 は、対称暗号化 KMS キーのみをサポートしま

す。このキーの詳細については、「AWS Key Management Service デベロッパーガイド」の「対称暗号化 KMS キー」を参照してください。

Java

AWS SDK for Java 2.x では、applyServerSideEncryptionByDefault メソッドを使用して、SSE-KMS によるデータ暗号化用にディレクトリバケットのデフォルトの暗号化設定を指定することで、AWS KMS key を使用するように Amazon S3 にリクエストできます。対称暗号化 KMS キーを作成し、それをリクエストで指定します。

```
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.services.s3.model.PutBucketEncryptionRequest;
import software.amazon.awssdk.services.s3.model.ServerSideEncryption;
import software.amazon.awssdk.services.s3.model.ServerSideEncryptionByDefault;
import software.amazon.awssdk.services.s3.model.ServerSideEncryptionConfiguration;
import software.amazon.awssdk.services.s3.model.ServerSideEncryptionRule;

public class Main {
    public static void main(String[] args) {
        S3Client s3 = S3Client.create();
        String bucketName = "bucket-base-name--zoneid--x-s3";
        String kmsKeyId = "your-kms-customer-managed-key-id";

        // AWS managed KMS keys aren't supported. Only customer-managed keys are
 supported.
        ServerSideEncryptionByDefault serverSideEncryptionByDefault =
 ServerSideEncryptionByDefault.builder()
                .sseAlgorithm(ServerSideEncryption.AWS_KMS)
                .kmsMasterKeyID(kmsKeyId)
                .build();

        // The bucketKeyEnabled field is enforced to be true.
        ServerSideEncryptionRule rule = ServerSideEncryptionRule.builder()
                .bucketKeyEnabled(true)
                .applyServerSideEncryptionByDefault(serverSideEncryptionByDefault)
                .build();

        ServerSideEncryptionConfiguration serverSideEncryptionConfiguration =
 ServerSideEncryptionConfiguration.builder()
                .rules(rule)
```

```
                .build();

        PutBucketEncryptionRequest putRequest = PutBucketEncryptionRequest.builder()
                .bucket(bucketName)

 .serverSideEncryptionConfiguration(serverSideEncryptionConfiguration)
                .build();

        s3.putBucketEncryption(putRequest);

    }
}
```

カスタマーマネージドキーの作成の詳細については、「AWS Key Management Service デベロッパーガイド」の「AWS KMS API のプログラミング」を参照してください。

オブジェクトをアップロードするためのコード例については、以下のトピックを参照してください。これらの例を使用するには、コード例を更新し、前出のコード例に示されているように暗号化情報を提供する必要があります。

- 1 つのオペレーションでオブジェクトをアップロードする場合は、ディレクトリバケットへのオブジェクトのアップロード を参照してください。
- マルチパートアップロード API オペレーションについては、「ディレクトリバケットでのマルチパートアップロードの使用」を参照してください。

.NET

AWS SDK for .NET では、`ServerSideEncryptionByDefault` プロパティを使用して、SSE-KMS によるデータ暗号化用にディレクトリバケットのデフォルトの暗号化設定を指定することで、AWS KMS key を使用するように Amazon S3 にリクエストできます。対称暗号化カスタマーマネージドキーを作成し、それをリクエストで指定します。

```
    // Set the bucket server side encryption to use AWSKMS with a customer-managed
 key id.
    // bucketName: Name of the directory bucket. "bucket-base-name--zonsid--x-s3"
    // kmsKeyId: The Id of the customer managed KMS Key. "your-kms-customer-managed-
key-id"
    // Returns True if successful.
```

```
   public static async Task<bool> SetBucketServerSideEncryption(string bucketName,
string kmsKeyId)
   {
       var serverSideEncryptionByDefault = new ServerSideEncryptionConfiguration
       {
           ServerSideEncryptionRules = new List<ServerSideEncryptionRule>
           {
               new ServerSideEncryptionRule
               {
                   ServerSideEncryptionByDefault = new
ServerSideEncryptionByDefault
                   {
                       ServerSideEncryptionAlgorithm =
ServerSideEncryptionMethod.AWSKMS,
                       ServerSideEncryptionKeyManagementServiceKeyId = kmsKeyId
                   }
               }
           }
       };
       try
       {
           var encryptionResponse =await _s3Client.PutBucketEncryptionAsync(new
PutBucketEncryptionRequest
           {
               BucketName = bucketName,
               ServerSideEncryptionConfiguration = serverSideEncryptionByDefault,
           });

           return encryptionResponse.HttpStatusCode == HttpStatusCode.OK;
       }
       catch (AmazonS3Exception ex)
       {
           Console.WriteLine(ex.ErrorCode == "AccessDenied"
               ? $"This account does not have permission to set encryption on
{bucketName}, please try again."
               : $"Unable to set bucket encryption for bucket {bucketName},
{ex.Message}");
       }
       return false;
   }
```

カスタマーマネージドキーの作成の詳細については、「AWS Key Management Service デベロッパーガイド」の「AWS KMS API のプログラミング」を参照してください。

オブジェクトをアップロードするためのコード例については、以下のトピックを参照してください。これらの例を使用するには、コード例を更新し、前出のコード例に示されているように暗号化情報を提供する必要があります。

- 1 つのオペレーションでオブジェクトをアップロードする場合は、ディレクトリバケットへのオブジェクトのアップロード を参照してください。
- マルチパートアップロード API オペレーションについては、「ディレクトリバケットでのマルチパートアップロードの使用」を参照してください。

AWS CloudTrail を使用したディレクトリバケットのデフォルト暗号化のモニタリング

AWS CloudTrail イベントを使用して、Amazon S3 ディレクトリバケットのデフォルトの暗号化設定リクエストを追跡できます。CloudTrail ログでは、以下の API イベント名が使用されます。

- `PutBucketEncryption`
- `GetBucketEncryption`
- `DeleteBucketEncryption`

> **Note**
>
> - EventBridge はディレクトリバケットではサポートされていません。
> - AWS Key Management Service (AWS KMS) キーによる二層式サーバー側の暗号化 (DSSE-KMS) またはお客様が提供する暗号化キーを使用したサーバー側の暗号化 (SSE-C) は、ディレクトリバケットのデフォルトの暗号化ではサポートされません。

AWS CloudTrail を使用したデフォルト暗号化のモニタリングの詳細については、「AWS CloudTrail および Amazon EventBridge によるデフォルト暗号化のモニタリング」を参照してください。

ディレクトリバケットでの AWS KMS キーによるサーバー側の暗号化 (SSE-KMS) の使用

AWS KMS のセキュリティ制御は、暗号化関連のコンプライアンス要件を満たすのに役立ちます。AWS Key Management Service (AWS KMS) キーによるサーバー側の暗号化 (SSE-KMS) を使

用するようにディレクトリバケットを設定し、これらの KMS キーを使用して Amazon S3 ディレクトリバケット内のデータを保護することを選択できます。SSE-KMS に関する詳細は、「AWS KMS キーによるサーバー側の暗号化 (SSE-KMS) の使用」を参照してください。

アクセス許可

AWS KMS key を使用して暗号化されたオブジェクトを Amazon S3 にアップロードまたは Amazon S3 からダウンロードするには、キーに対する `kms:GenerateDataKey` および `kms:Decrypt` の許可が必要です。詳細については、AWS Key Management Service デベロッパーガイドの「キーユーザーが暗号化オペレーションに KMS キーを使用することを許可する」を参照してください。マルチパートアップロードに必要な AWS KMS アクセス許可については、[マルチパートアップロード API とアクセス許可]を参照してください。

SSE-KMS のキーに関する詳細は、「AWS KMS (SSE-KMS) によるサーバー側の暗号化の指定」を参照してください。

トピック

- AWS KMS keys
- クロスアカウント操作での SSE-KMS の使用
- Amazon S3 バケットキー
- SSE-KMS の要求
- 暗号化コンテキスト
- AWS KMS 暗号化されたオブジェクトへのリクエストの送信
- ディレクトリバケットでの SSE-KMS 暗号化の監査
- ディレクトリバケット内の新しいオブジェクトのアップロードに AWS KMS によるサーバー側の暗号化 (SSE-KMS) を指定する

AWS KMS keys

SSE-KMS 設定では、バケットの存続期間中、ディレクトリバケットごとに 1 つのカスタマーマネージドキーしかサポートできません。AWS マネージドキー (`aws/s3`) はサポートされていません。また、SSE-KMS のカスタマーマネージドキーを指定した後は、バケットの SSE-KMS 設定のカスタマーマネージドキーを上書きすることはできません。

バケットの SSE-KMS 設定に指定したカスタマーマネージドキーは、次のように識別できます。

- `HeadObject` API オペレーションリクエストを実行して、レスポンス内の `x-amz-server-side-encryption-aws-kms-key-id` の値を検索します。

データに新しいカスタマーマネージドキーを使用するには、新しいカスタマーマネージドキーを使用して既存のオブジェクトを新しいディレクトリバケットにコピーすることをお勧めします。

ディレクトリバケットで暗号化に AWS KMS カスタマーマネージドキーを指定する場合は、キー ID またはキー ARN のみを使用します。KMS キーのキーエイリアス形式はサポートされていません。

SSE-KMS のキーに関する詳細は、「AWS KMS keys」を参照してください。

クロスアカウント操作での SSE-KMS の使用

ディレクトリバケットのクロスアカウント操作で暗号化を使用する場合は、次の点に注意してください。

- S3 オブジェクトへのクロスアカウントアクセスを許可する場合は、別のアカウントからのアクセスを許可するようにカスタマーマネージドキーのポリシーを設定します。
- カスタマーマネージドキーを指定するには、完全修飾 KMS キー ARN を使用する必要があります。

Amazon S3 バケットキー

S3 バケットキーは、ディレクトリバケット内の GET および PUT オペレーションで常に有効になっており、無効にすることはできません。SSE-KMS で暗号化されたオブジェクトを、CopyObject、UploadPartCopy、バッチオペレーションの Copy オペレーション、または import ジョブを使用して、汎用バケットからディレクトリバケットへ、ディレクトリバケットから汎用バケットへ、またはディレクトリバケット間でコピーする場合、S3 バケットキーはサポートされません。この場合、KMS で暗号化されたオブジェクトのコピーリクエストが実行されるたびに、Amazon S3 は AWS KMS を呼び出します。

CopyObject および UploadPartCopy を除くゾーンエンドポイント (オブジェクトレベル) API オペレーションでは、CreateSession を介してリクエストを認証および承認することで低レイテンシーを実現します。バケットのデフォルトの暗号化では、必要な暗号化設定を使用することをお勧めします。CreateSession リクエストまたは PUT オブジェクトリクエストでは、バケットのデフォルトの暗号化を上書きしないことをお勧めします。その後、新しいオブジェクトは必要な暗号化設定で自動的に暗号化されます。SSE-KMS を使用してディレクトリバケット内の新しいオブジェクトを暗号化するには、KMS キー (特にカスタマーマネージドキー) を使用してディレクトリバケットのデフォルトの暗号化設定として SSE-KMS を指定する必要があります。その後、ゾーンエンドポイント API オペレーションのセッションが作成されると、セッション中に新しいオブジェクトが SSE-KMS および S3 バケットキーで自動的に暗号化および復号されます。ディレクトリバケットの暗号化の上書

き動作の詳細については、「新しいオブジェクトのアップロードに AWS KMS を使用してサーバー側の暗号化を指定する」を参照してください。

S3 バケットキーは Amazon S3 内で期間限定で使用されるため、Amazon S3 で AWS KMS にリクエストを実行し、暗号化オペレーションを完了する必要性が軽減されます。S3 バケットキーの使用の詳細については、「Amazon S3 バケットキー」および「Amazon S3 バケットキーを使用した SSE-KMS のコストの削減」を参照してください。

SSE-KMS の要求

特定のディレクトリバケット内のすべてのオブジェクトの SSE-KMS を要求するには、バケットポリシーを使用できます。例えば、`CreateSession` API オペレーションを使用して新しいオブジェクト (`PutObject`、`CopyObject`、および `CreateMultipartUpload`) をアップロードするアクセス許可を付与する場合、`CreateSession` リクエストに SSE-KMS をリクエストする `x-amz-server-side-encryption-aws-kms-key-id` ヘッダーが含まれていない場合、次のバケットポリシーはすべてのユーザーに対してオブジェクトのアップロードアクセス許可 (`s3express:CreateSession`) を拒否します。

```
{
   "Version":"2012-10-17",
   "Id":"UploadObjectPolicy",
   "Statement":[{
         "Sid":"DenyObjectsThatAreNotSSEKMS",
         "Effect":"Deny",
         "Principal":"*",
         "Action":"s3express:CreateSession",
         "Resource":"arn:aws:s3express:region:account-id:bucket/bucket-base-name--zone-id--x-s3/*",
         "Condition":{
            "Null":{
               "s3express:x-amz-server-side-encryption-aws-kms-key-id":"true"
            }
         }
      }
   ]
}
```

特定の AWS KMS key を使用してバケット内のオブジェクトを暗号化することを要求するには、`s3express:x-amz-server-side-encryption-aws-kms-key-id` 条件キーを使用できます。KMS キーを指定するには、キーの Amazon リソースネーム (ARN)

を `arn:aws:kms:region:acct-id:key/key-id` 形式で使用する必要があります。AWS Identity and Access Management は、`s3express:x-amz-server-side-encryption-aws-kms-key-id` の文字列が存在するかどうかを検証しません。Amazon S3 がオブジェクトの暗号化に使用する AWS KMS キー ID とポリシーの AWS KMS キー ID は一致する必要があります。一致しない場合、Amazon S3 はリクエストを拒否します。

新しいオブジェクトのアップロードに SSE-KMS を使用する方法の詳細については、「ディレクトリバケット内の新しいオブジェクトのアップロードに AWS KMS によるサーバー側の暗号化 (SSE-KMS) を指定する」を参照してください。

ディレクトリバケットの固有条件キーの詳細なリストについては、「IAM を使用したリージョンエンドポイント API オペレーションの承認」を参照してください。

暗号化コンテキスト

ディレクトリバケットの場合、暗号化コンテキストは、データに関する追加のコンテキスト情報が含まれたキーと値のペアのセットです。追加の暗号化コンテキスト値はサポートされていません。暗号化コンテキストの詳細については、「暗号化コンテキスト」を参照してください。

デフォルトでは、ディレクトリバケットで SSE-KMS を使用する場合、Amazon S3 はバケットの Amazon リソースネーム (ARN) を暗号化コンテキストペアとして使用します。

```
arn:aws:s3express:region:account-id:bucket/bucket-base-name--zone-id--x-s3
```

IAM ポリシーまたは AWS KMS キーポリシーで、暗号化コンテキストとしてバケット ARN が使用されていることを確認します。

オプションで、CreateSession などのゾーンエンドポイント API リクエストで `x-amz-server-side-encryption-context` ヘッダーを使用して、明示的な暗号化コンテキストペアを指定できます。このヘッダーの値は、UTF-8 Base64-encoded でエンコードされた JSON の文字列で、暗号化コンテキストをキーと値のペアとして含めます。ディレクトリバケットの場合、暗号化コンテキストはデフォルトの暗号化コンテキストであるバケット Amazon リソースネーム (ARN) と一致する必要があります。また、暗号化コンテキストは暗号化されないため、機密情報を含めないよう注意してください。

暗号化コンテキストを使用して、暗号化オペレーションを識別および分類できます。デフォルトの暗号化コンテキスト ARN 値を使用して、どのディレクトリバケット ARN がどの暗号化キーで使用されたかを確認することで、AWS CloudTrail の関連するリクエストを追跡することもできます。

CloudTrail ログファイルの `requestParameters` フィールドで、ディレクトリバケットで SSE-KMS を使用する場合、暗号化コンテキスト値はバケットの ARN です。

```
"encryptionContext": {
    "aws:s3express:arn": "arn:aws:s3:::arn:aws:s3express:region:account-id:bucket/bucket-base-name--zone-id--x-s3"
}
```

また、ディレクトリバケット内の SSE-KMS によるオブジェクト暗号化の場合、AWS KMS CloudTrail イベントはオブジェクト ARN ではなくバケット ARN をログに記録します。

AWS KMS 暗号化されたオブジェクトへのリクエストの送信

ディレクトリバケットには、HTTPS (TLS) 経由でのみアクセスできます。また、ディレクトリバケットは AWS Signature Version 4 (SigV4) を使用してリクエストに署名します。AWS KMS 暗号化されたオブジェクトのリクエストの送信の詳細については、「AWS KMS 暗号化されたオブジェクトへのリクエストの送信」を参照してください。

オブジェクトで SSE-KMS を使用している場合、`GET` リクエストおよび `HEAD` リクエストに対して暗号化リクエストヘッダーを送信しないでください。そうしないと、HTTP 400 Bad Request エラーが表示されます。

ディレクトリバケットでの SSE-KMS 暗号化の監査

SSE-KMS で暗号化されたデータの AWS KMS キーの使用状況を監査するには、AWS CloudTrail ログを使用します。GenerateDataKey や Decrypt などの暗号化オペレーションに関するインサイトを得ることができます。CloudTrail は、イベント名、ユーザー名、イベントソースなど、検索をフィルタリングするための多数の属性値をサポートしています。

トピック

- ディレクトリバケット内の新しいオブジェクトのアップロードに AWS KMS によるサーバー側の暗号化 (SSE-KMS) を指定する

ディレクトリバケット内の新しいオブジェクトのアップロードに AWS KMS によるサーバー側の暗号化 (SSE-KMS) を指定する

ディレクトリバケットの場合、Amazon S3 マネージドキー (SSE-S3) (デフォルト) を使用したサーバー側の暗号化、AWS Key Management Service (AWS KMS) キーを使用したサーバー側の暗号化 (SSE-KMS) を使用できます。バケットのデフォルトの暗号化では、必要な暗号化設定を使用するこ

とをお勧めします。CreateSession リクエストまたは PUT オブジェクトリクエストでは、バケットのデフォルトの暗号化を上書きしないことをお勧めします。その後、新しいオブジェクトは必要な暗号化設定で自動的に暗号化されます。ディレクトリバケットの暗号化の上書き動作の詳細については、「新しいオブジェクトのアップロードに AWS KMS を使用してサーバー側の暗号化を指定する」を参照してください。

すべての Amazon S3 バケットにはデフォルトで暗号化が設定されており、S3 バケットにアップロードされたすべての新しいオブジェクトは保存時に自動的に暗号化されます。Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3) は、Amazon S3 のすべてのバケットでのデフォルトの暗号化設定です。ディレクトリバケットに別の暗号化タイプを指定する場合は、AWS Key Management Service (AWS KMS) キーによるサーバー側の暗号化 (SSE-KMS) を使用できます。SSE-KMS を使用してディレクトリバケット内の新しいオブジェクトを暗号化するには、KMS キー (特にカスタマーマネージドキー) を使用してディレクトリバケットのデフォルトの暗号化設定として SSE-KMS を指定する必要があります AWS マネージドキー (aws/s3) はサポートされていません。SSE-KMS 設定では、バケットの存続期間中、ディレクトリバケットごとに 1 つのカスタマーマネージドキーしかサポートできません。SSE-KMS のカスタマーマネージドキーを指定した後は、バケットの SSE-KMS 設定のカスタマーマネージドキーを上書きすることはできません。次に、SSE-KMS で新しいオブジェクトにサーバー側の暗号化設定を指定するときは、暗号化キーがディレクトリバケットのデフォルトの暗号化設定に指定したカスタマーマネージドキーと同じであることを確認する必要があります。データに新しいカスタマーマネージドキーを使用するには、新しいカスタマーマネージドキーを使用して既存のオブジェクトを新しいディレクトリバケットにコピーすることをお勧めします。

暗号化は、新しいオブジェクトをアップロードしたり、既存のオブジェクトをコピーしたりするときに適用できます。オブジェクトの暗号化を変更すると、新しいオブジェクトが作成され、古いオブジェクトが置き換えられます。

REST API オペレーション、AWS SDK、および AWS Command Line Interface (AWS CLI) を使用して SSE-KMS を指定できます。

> **Note**
>
> - ディレクトリバケットの場合、暗号化の上書き動作は次のとおりです。
>   - REST API で CreateSession を使用して CopyObject および UploadPartCopy を除くゾーンエンドポイント API リクエストを認証および承認する場合、バケットのデフォルトの暗号化を以前に SSE-KMS で指定した場合にのみ、暗号化設定を SSE-S3 または SSE-KMS に上書きできます。

- AWS CLI または AWS SDK で CreateSession を使用して CopyObject および UploadPartCopy を除くゾーンエンドポイント API リクエストを認証および承認する場合、暗号化設定を上書きすることはできません。
- CopyObject リクエストを行うときは、バケットのデフォルトの暗号化を以前に SSE-KMS で指定した場合にのみ、暗号化設定を SSE-S3 または SSE-KMS に上書きできます。UploadPartCopy リクエストを行う場合、暗号化設定を上書きすることはできません。

- Amazon S3 では、マルチリージョン AWS KMS keys を使用できます。ただし、Amazon S3 では現在、マルチリージョンキーは、単一リージョンキーであるかのように処理され、キーのマルチリージョン特徴は使用しません。詳細については、「AWS Key Management Service デベロッパーガイド」の「マルチリージョンキーを使用する」を参照してください。
- 別のアカウントが所有している KMS キーを使用する場合は、そのキーを使用するアクセス許可が必要です。KMS キーのクロスアカウント権限の詳細については、「AWS Key Management Service デベロッパーガイド」の「他のアカウントで使用できる KMS キーを作成する」を参照してください。

REST API の使用

> **Note**
>
> バケットの存続期間中は、ディレクトリバケットごとに 1 つのカスタマーマネージドキーのみがサポートされます。AWS マネージドキー (aws/s3) はサポートされていません。カスタマーマネージドキーを使用してバケットのデフォルトの暗号化設定として SSE-KMS を指定した後は、バケットの SSE-KMS 設定のカスタマーマネージドキーを変更することはできません。

CopyObject および UploadPartCopy を除くゾーンエンドポイント (オブジェクトレベル) API オペレーションでは、CreateSession を介してリクエストを認証および承認して低レイテンシーを実現します。バケットのデフォルト暗号化では、必要な暗号化設定を使用することをお勧めします。CreateSession リクエストまたは PUT オブジェクトリクエストでは、バケットのデフォルト暗号化を上書きしないことをお勧めします。その後、新しいオブジェクトは必要な暗号化設定で自動的に暗号化されます。SSE-KMS を使用してディレクトリバケット内の新しいオブジェクトを暗号化するには、KMS キー (特にカスタマーマネージドキー) を使用してディレクトリバケットのデフォル

トの暗号化設定として SSE-KMS を指定する必要があります その後、ゾーンエンドポイント API オペレーションのセッションが作成されると、セッション中に新しいオブジェクトが SSE-KMS および S3 バケットキーで自動的に暗号化および復号されます。ディレクトリバケットの暗号化の上書き動作の詳細については、「新しいオブジェクトのアップロードに AWS KMS を使用してサーバー側の暗号化を指定する」を参照してください。

REST API を使用したゾーンエンドポイント API コール (CopyObject および UploadPartCopy を除く) では、`CreateSession` リクエストから暗号化設定 (`x-amz-server-side-encryption`、`x-amz-server-side-encryption-aws-kms-key-id`、`x-amz-server-side-encryption-context`、`x-amz-server-side-encryption-bucket-key-enabled`) の値を上書きすることはできません。ゾーンエンドポイント API コールでこれらの暗号化設定値を明示的に指定する必要はありません。Amazon S3 は `CreateSession` リクエストの暗号化設定値を使用してディレクトリバケット内の新しいオブジェクトを保護します。

> **Note**
>
> AWS CLI または AWS SDK を使用する場合、セッショントークンは `CreateSession` に対して自動的に更新され、セッションの有効期限が切れたときのサービス中断を回避します。AWS CLI または AWS SDK は、`CreateSession` リクエストにバケットのデフォルトの暗号化設定を使用します。`CreateSession` リクエストの暗号化設定値を上書きすることはサポートされていません。また、ゾーンエンドポイント API コール (CopyObject および UploadPartCopyを除く) では、`CreateSession` リクエストからの暗号化設定の値を上書きすることはできません。

CopyObject の場合、SSE-KMS を使用してディレクトリバケット内の新しいオブジェクトコピーを暗号化するには、KMS キー (特にカスタマーマネージドキー) を使用してディレクトリバケットのデフォルトの暗号化設定として SSE-KMS を指定する必要があります。次に、SSE-KMS で新しいオブジェクトコピーにサーバー側の暗号化設定を指定するときは、暗号化キーがディレクトリバケットのデフォルトの暗号化設定に指定したカスタマーマネージドキーと同じであることを確認する必要があります。UploadPartCopy では、SSE-KMS を使用してディレクトリバケット内の新しいオブジェクトパーツコピーを暗号化するには、KMS キー (特にカスタマーマネージドキー) を使用してディレクトリバケットのデフォルトの暗号化設定として SSE-KMS を指定する必要があります。UploadPartCopy リクエストヘッダーで SSE-KMS を使用して新しいオブジェクトパートコピーのサーバー側の暗号化設定を指定することはできません。また、CreateMultipartUpload リクエストで指定する暗号化設定は、送信先バケットのデフォルトの暗号化設定と一致する必要があります。

トピック

- SSE-KMS をサポートする Amazon S3 REST API オペレーション
- 暗号化コンテキスト (x-amz-server-side-encryption-context)
- AWS KMS キー ID (x-amz-server-side-encryption-aws-kms-key-id)
- S3 バケットキー (x-amz-server-side-encryption-aws-bucket-key-enabled)

SSE-KMS をサポートする Amazon S3 REST API オペレーション

ディレクトリバケット内のオブジェクトレベルの REST API オペレーションでは `x-amz-server-side-encryption`、`x-amz-server-side-encryption-aws-kms-key-id`、および `x-amz-server-side-encryption-context` リクエストヘッダーを受け入れます。

- CreateSession – ゾーンエンドポイント (オブジェクトレベル) API オペレーション (CopyObject および UploadPartCopy を除く) を使用する場合、これらのリクエストヘッダーを指定できます。
- PutObject - PUT オペレーションを使用してデータをアップロードするとき、これらのリクエストヘッダーを指定できます。
- CopyObject — オブジェクトをコピーするときには、ソースオブジェクトとターゲットオブジェクトの両方があります。`CopyObject` オペレーションで SSE-KMS ヘッダーを渡す場合は、ターゲットオブジェクトにのみ適用されます。
- CreateMultipartUpload — マルチパートアップロード API オペレーションを使用して大きいオブジェクトをアップロードする場合、これらのヘッダーを指定できます。これらのヘッダーを `CreateMultipartUpload` リクエストで指定します。

次の REST API オペレーションのレスポンスヘッダーは、オブジェクトがサーバー側の暗号化を使用して保存されているときに `x-amz-server-side-encryption` ヘッダーを返します。

- CreateSession
- PutObject
- CopyObject
- POST Object
- CreateMultipartUpload
- UploadPart
- UploadPartCopy
- CompleteMultipartUpload

- GetObject
- HeadObject

> **Important**
>
> - AWS KMS で保護されたオブジェクトに対する GET リクエストと PUT リクエストはすべて、Transport Layer Security (TLS)、または署名バージョン 4 を使用していない場合、失敗します。
> - オブジェクトで SSE-KMS を使用している場合、GET リクエストおよび HEAD リクエストに対して暗号化リクエストヘッダーを送信しないでください。送信すると、HTTP 400 BadRequest エラーが発生します。

暗号化コンテキスト (**x-amz-server-side-encryption-context**)

x-amz-server-side-encryption:aws:kms を指定した場合、Amazon S3 API はオプションで x-amz-server-side-encryption-context ヘッダーの暗号化コンテキストの指定をサポートします。ディレクトリバケットの場合、暗号化コンテキストは、データに関するコンテキスト情報が含まれたキーと値のペアのセットです。値は、デフォルトの暗号化コンテキストであるバケット Amazon リソースネーム (ARN) と一致する必要があります。追加の暗号化コンテキスト値はサポートされていません。

ディレクトリバケットの暗号化コンテキストの詳細については、「暗号化コンテキスト」を参照してください。暗号化コンテキストの一般的な情報については、「AWS Key Management Service デベロッパーガイド」の「AWS Key Management Service Concepts - Encryption context」を参照してください。

AWS KMS キー ID (**x-amz-server-side-encryption-aws-kms-key-id**)

x-amz-server-side-encryption-aws-kms-key-id ヘッダーを使用して、データの保護に使用するカスタマーマネージドキーの ID を指定できます。

SSE-KMS 設定では、バケットの存続期間中、ディレクトリバケットごとに 1 つのカスタマーマネージドキーしかサポートできません。AWS マネージドキー (aws/s3) はサポートされていません。また、SSE-KMS のカスタマーマネージドキーを指定した後は、バケットの SSE-KMS 設定のカスタマーマネージドキーを上書きすることはできません。

バケットの SSE-KMS 設定に指定したカスタマーマネージドキーは、次のように識別できます。

- `HeadObject` API オペレーションリクエストを実行して、レスポンス内の `x-amz-server-side-encryption-aws-kms-key-id` の値を検索します。

データに新しいカスタマーマネージドキーを使用するには、新しいカスタマーマネージドキーを使用して既存のオブジェクトを新しいディレクトリバケットにコピーすることをお勧めします。

ディレクトリバケットの暗号化コンテキストの詳細については、「AWS KMS keys」を参照してください。

S3 バケットキー (**`x-amz-server-side-encryption-aws-bucket-key-enabled`**)

S3 バケットキーは、ディレクトリバケット内の GET および PUT オペレーションで常に有効になっており、無効にすることはできません。SSE-KMS で暗号化されたオブジェクトを、CopyObject、UploadPartCopy、バッチオペレーションの Copy オペレーション、または import ジョブを使用して、汎用バケットからディレクトリバケットへ、ディレクトリバケットから汎用バケットへ、またはディレクトリバケット間でコピーする場合、S3 バケットキーはサポートされません。この場合、KMS で暗号化されたオブジェクトのコピーリクエストが実行されるたびに、Amazon S3 は AWS KMS を呼び出します。ディレクトリバケットでの S3 バケットキーの詳細については、「暗号化コンテキスト」を参照してください。

AWS CLI を使用する場合

> **Note**
>
> `CreateSession` に AWS CLI を使用すると、セッショントークンが自動的に更新され、セッションの有効期限が切れたときにサービスが中断されるのを防ぐことができます。`CreateSession` リクエストの暗号化設定値を上書きすることはサポートされていません。また、ゾーンエンドポイント API コール (CopyObject および UploadPartCopy を除く) では、`CreateSession` リクエストからの暗号化設定の値を上書きすることはできません。SSE-KMS を使用してディレクトリバケット内の新しいオブジェクトを暗号化するには、KMS キー (特にカスタマーマネージドキー) を使用してディレクトリバケットのデフォルトの暗号化設定として SSE-KMS を指定する必要があります その後、ゾーンエンドポイント API オペレーションのセッションが作成されると、セッション中に新しいオブジェクトが SSE-KMS および S3 バケットキーで自動的に暗号化および復号されます。

次の AWS CLI コマンド例を使用する際は、*`user input placeholders`* をユーザー自身の情報に置き換えます。

新しいオブジェクトをアップロードするか、既存のオブジェクトをコピーするときに、AWS KMS キーを使用したサーバー側の暗号化の使用を指定してデータを暗号化できます。これを行うには、put-bucket-encryption コマンドを使用して、ディレクトリバケットのデフォルトの暗号化設定を SSE-KMS (aws:kms) に設定します。具体的には、--server-side-encryption aws:kms ヘッダーをリクエストに追加します。--ssekms-key-id *example-key-id*を使用して、作成したカスタマーマネージド AWS KMS キーを追加します。--server-side-encryption aws:kms を指定する場合は、カスタマーマネージドキーの AWS KMS キー ID を指定する必要があります。ディレクトリバケットは AWS マネージドキーを使用しません。コマンドの例については、AWS CLI を使用する場合 をご参照ください。

次に、次のコマンドを使用して新しいオブジェクトをアップロードすると、Amazon S3 はデフォルトの暗号化にバケット設定を使用して、デフォルトでオブジェクトを暗号化します。

```
aws s3api put-object --bucket bucket-base-name--zone-id--x-s3 --key example-object-key
 --body filepath
```

ゾーンエンドポイント API オペレーションコマンドに -\-bucket-key-enabled を明示的に追加する必要はありません。S3 バケットキーは、ディレクトリバケット内の GET および PUT オペレーションで常に有効になっており、無効にすることはできません。SSE-KMS で暗号化されたオブジェクトを、CopyObject、UploadPartCopy、バッチオペレーションの Copy オペレーション、または import ジョブを使用して、汎用バケットからディレクトリバケットへ、ディレクトリバケットから汎用バケットへ、またはディレクトリバケット間でコピーする場合、S3 バケットキーはサポートされません。この場合、KMS で暗号化されたオブジェクトのコピーリクエストが実行されるたびに、Amazon S3 は AWS KMS を呼び出します。

オブジェクトをレプリケート元バケット (汎用バケットなど) から新しいバケット (ディレクトリバケットなど) にコピーし、レプリケート先オブジェクトに SSE-KMS 暗号化を使用できます。これを行うには、put-bucket-encryption コマンドを使用して、レプリケート先バケット (ディレクトリバケットなど) のデフォルトの暗号化設定を SSE-KMS (aws:kms) に設定します。コマンドの例については、AWS CLI を使用する場合 をご参照ください。次に、次のコマンドを使用してオブジェクトをコピーすると、Amazon S3 はデフォルトの暗号化にバケット設定を使用して、デフォルトでオブジェクトを暗号化します。

```
aws s3api copy-object --copy-source amzn-s3-demo-bucket/example-object-key --
bucket bucket-base-name--zone-id--x-s3 --key example-object-key
```

AWS SDK の使用

AWS SDK を使用する場合、サーバー側の暗号化に AWS KMS keys を使用するよう Amazon S3 にリクエストできます。次の例は、AWS SDK for Java および .NET で SSE-KMS を使用する方法を示しています。他の SDK については、AWS デベロッパーセンターのサンプルコードとライブラリを参照してください。

> **Note**
>
> `CreateSession` に AWS SDK を使用する場合、セッショントークンは自動的に更新され、セッションの有効期限が切れたときのサービス中断を回避します。`CreateSession` リクエストの暗号化設定値を上書きすることはサポートされていません。また、ゾーンエンドポイント API コール (CopyObject および UploadPartCopy を除く) では、`CreateSession` リクエストからの暗号化設定の値を上書きすることはできません。
> SSE-KMS を使用してディレクトリバケット内の新しいオブジェクトを暗号化するには、KMS キー (特にカスタマーマネージドキー) を使用してディレクトリバケットのデフォルトの暗号化設定として SSE-KMS を指定する必要があります その後、ゾーンエンドポイント API オペレーションのセッションが作成されると、セッション中に新しいオブジェクトが SSE-KMS および S3 バケットキーで自動的に暗号化および復号されます。
> AWS SDK を使用してディレクトリバケットのデフォルト暗号化設定を SSE-KMS として設定する方法の詳細については、「AWS SDK の使用」を参照してください。

> **Important**
>
> Amazon S3 でサーバー側の暗号化に AWS KMS key を使用する場合は、対称暗号化 KMS キーを選択する必要があります。Amazon S3 は、対称暗号化 KMS キーのみをサポートします。このキーの詳細については、「AWS Key Management Service デベロッパーガイド」の「対称暗号化 KMS キー」を参照してください。

カスタマーマネージドキーの作成の詳細については、「AWS Key Management Service デベロッパーガイド」の「AWS KMS API のプログラミング」を参照してください。

転送中の暗号化

ディレクトリバケットでは、リージョン API エンドポイントとゾーン API エンドポイントを使用します。使用する Amazon S3 API オペレーションに応じて、リージョンゾーンエンドポイントまたは

ゾーンエンドポイントのいずれかが必要です。ゲートウェイ仮想プライベートクラウド (VPC) エンドポイントを通じて、ゾーン API オペレーションとリージョン API オペレーションにアクセスできます。ゲートウェイエンドポイントは追加料金なしで使用できます。リージョン API エンドポイントとゾーン API エンドポイントの詳細については、「ディレクトリバケットのネットワーク」を参照してください。

データの削除

Amazon S3 コンソール、AWS SDK、AWS Command Line Interface (AWS CLI)、または Amazon S3 REST API を使用して、ディレクトリバケットから 1 つ以上のオブジェクトを直接削除できます。ディレクトリバケット内のすべてのオブジェクトにはストレージ コストが発生するため、不要になったオブジェクトを削除することをお勧めします。

ディレクトリバケットに保存されているオブジェクトを削除すると、削除されるオブジェクト以外のオブジェクトが親ディレクトリに含まれていない場合、親ディレクトリも再帰的に削除されます。

> **Note**
>
> S3 Express One Zone では、多要素認証 (MFA) 削除と S3 バージョニングはサポートされていません。

リクエストの認証と承認

デフォルトでは、ディレクトリバケットはプライベートであり、アクセスを明示的に許可されているユーザーのみがアクセスできます。ディレクトリバケットのアクセスコントロール境界は、バケットレベルでのみ設定されます。対照的に、汎用バケットのアクセス制御境界は、バケット、プレフィックス、またはオブジェクトタグレベルで設定できます。この違いは、S3 Express One Zone アクセスのバケットポリシーまたは IAM アイデンティティポリシーに含めることができるリソースがディレクトリバケットのみであるためです。

Amazon S3 Express One Zone は、AWS Identity and Access Management (AWS IAM) 承認とセッションベースの承認の両方をサポートしています。

- S3 Express One Zone でリージョンエンドポイント API オペレーション (バケットレベル、またはコントロールプレーンのオペレーション) を使用するには、セッション管理を必要としない IAM 認可モデルを使用します。アクセス許可はアクションごとに個別に付与されます。詳細については、「IAM を使用したリージョンエンドポイント API オペレーションの承認」を参照してください。

- ゾーンエンドポイント API オペレーション (オブジェクトレベルまたはデータプレーンオペレーション) を使用するには、CopyObject と HeadBucket を除き、CreateSession API オペレーションを使用して、データリクエストの低レイテンシー承認に最適化されたセッションを作成および管理します。ッションントークンを取得して使用するには、アイデンティティベースのポリシーまたはバケットポリシーでディレクトリバケットの s3express:CreateSession アクションを許可する必要があります。詳細については、「IAM を使用したリージョンエンドポイント API オペレーションの承認」を参照してください。Amazon S3 コンソール、AWS Command Line Interface (AWS CLI)、または AWS SDK を使用して S3 Express One ゾーンにアクセスしている場合、S3 Express One Zone はユーザーに代わってセッションを作成します。

CreateSession API オペレーションでは、新しいセッションベースのメカニズムを使用してリクエストを認証および承認します。CreateSession を使用して、バケットへの低レイテンシーアクセスを実現する一時的な認証情報をリクエストできます。このような一時的な認証情報は、特定のディレクトリバケットに限定されます。

CreateSession を使用するには、最新バージョンの AWS SDK を使用するか AWS Command Line Interface (AWS CLI) を使用することをお勧めします。サポートされている AWS SDK と AWS CLI が、ユーザーに代わってセッションの確立、更新、終了の処理を行います。

セッションントークンはゾーン (オブジェクトレベル) オペレーション (CopyObject と HeadBucket を除く) でのみ使用し、承認関連のレイテンシーをセッション内の多数のリクエストに分散させます。リージョンのエンドポイント API オペレーション (バケットレベルのオペレーション) には IAM 認可を使用しますが、セッションの管理は不要です。詳細については、「IAM を使用したリージョンエンドポイント API オペレーションの承認」および「CreateSession を使用したゾーンエンドポイント API オペレーションの承認」を参照してください。

API オペレーションの認証および承認方法

次の表は、ディレクトリバケット API オペレーションの認証および承認情報の一覧です。この表には、API オペレーションごとに、API オペレーション名、IAM ポリシーアクション、エンドポイントタイプ (リージョンまたはゾーン)、承認メカニズム (IAM またはセッションベース) が表示されています。この表には、クロスアカウントアクセスがサポートされているかどうかも示されています。バケットレベルのアクションへのアクセスは、バケットポリシーではなく、IAM アイデンティティベースのポリシー (ユーザーまたはロール) でのみ付与でます。

API	エンドポイントタイプ	IAM アクション	クロスアカウントアクセス
CreateBucket	リージョン別	s3express:CreateBucket	いいえ
DeleteBucket	リージョン別	s3express:DeleteBucket	いいえ
ListDirectoryBuckets	リージョン別	s3express:ListAllMyDirectoryBuckets	いいえ
PutBucketPolicy	リージョン別	s3express:PutBucketPolicy	いいえ
GetBucketPolicy	リージョン別	s3express:GetBucketPolicy	いいえ
DeleteBucketPolicy	リージョン別	s3express:DeleteBucketPolicy	いいえ
CreateSession	ゾーン別	s3express:CreateSession	はい
CopyObject	ゾーン別	s3express:CreateSession	はい
DeleteObject	ゾーン別	s3express:CreateSession	はい
DeleteObjects	ゾーン別	s3express:CreateSession	はい
HeadObject	ゾーン別	s3express:CreateSession	はい
PutObject	ゾーン別	s3express:CreateSession	はい
GetObjectAttributes	ゾーン別	s3express:CreateSession	はい
ListObjectsV2	ゾーン別	s3express:CreateSession	はい
HeadBucket	ゾーン別	s3express:CreateSession	はい
CreateMultipartUpload	ゾーン別	s3express:CreateSession	はい

API	エンドポイントタイプ	IAM アクション	クロスアカウントアクセス
UploadPart	ゾーン別	s3express:CreateSession	はい
UploadPartCopy	ゾーン別	s3express:CreateSession	はい
CompleteMultipartUpload	ゾーン別	s3express:CreateSession	はい
AbortMultipartUpload	ゾーン別	s3express:CreateSession	はい
ListParts	ゾーン別	s3express:CreateSession	はい
ListMultipartUploads	ゾーン別	s3express:CreateSession	はい
ListAccessPointsForDirectoryBuckets	ゾーン別	s3express:ListAccessPointsForDirectoryBuckets	はい
GetAccessPointScope	ゾーン別	s3express:GetAccessPointScope	はい
PutAccessPointScope	ゾーン別	s3express:PutAccessPointScope	はい
DeleteAccessPointScope	ゾーン別	s3express:DeleteAccessPointScope	はい

トピック

- IAM を使用したリージョンエンドポイント API オペレーションの承認
- CreateSession を使用したゾーンエンドポイント API オペレーションの承認

IAM を使用したリージョンエンドポイント API オペレーションの承認

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に管理するうえで役立つ AWS のサービス です。IAM 管理者は、どのユーザーが認証 (サインイン) して、どのユーザーにリソースの使用を許可する (アクセス許可を持たせる) かを制御します。IAMは追加料金なしでご利用いただけます。

デフォルトでは、ユーザーにはディレクトリバケットと S3 Express One Zone オペレーションのためのアクセス許可はありません。ディレクトリバケットへのアクセス権限を付与するには、IAM を使用してユーザー、グループ、またはロールを作成し、それらのアイデンティティにアクセス許可をアタッチします。IAM の詳細については、「IAM ユーザーガイド」の「IAM でのセキュリティのベストプラクティス」を参照してください。

アクセスを提供するには、ユーザー、グループ、またはロールにアクセス許可を追加します。

- AWS IAM Identity Center 内のユーザーとグループ — アクセス許可セットを作成します。「AWS IAM Identity Center ユーザーガイド」の「権限設定を作成する」の手順に従ってください。
- アイデンティティプロバイダーを介して IAM で管理されているユーザー — ID フェデレーションのロールを作成します。詳細については、「IAM ユーザーガイド」の「サードパーティー ID プロバイダー (フェデレーション) 用のロールの作成」を参照してください。
- IAM ロールとユーザー — ユーザーが引き受けることができるロールを作成します。詳細については、「IAM ユーザーガイド」の「 IAM ユーザーにアクセス許可を委任するロールの作成」を参照してください。

S3 Express One Zone 向けの IAM の詳細については、次のトピックを参照してください。

トピック

- プリンシパル
- リソース
- ディレクトリバケットのアクション
- ディレクトリバケットの条件キー
- ディレクトリバケットの IAM アイデンティティベースのポリシー
- ディレクトリバケットのバケットポリシーの例

プリンシパル

バケットへのアクセスを許可するリソースベースのポリシーを作成する場合は、`Principal` 要素を使用して、そのリソースに対するアクションまたはオペレーションをリクエストできるユーザーまたはアプリケーションを指定する必要があります。ディレクトリバケットポリシーでは、次のプリンシパルを使用できます。

- AWS アカウント。
- IAM ユーザー
- IAM ロール
- フェデレーションユーザー

詳細については、IAM ユーザーガイドPrincipalの を参照してください。

リソース

ディレクトリバケットの Amazon リソースネーム (ARN) には、`s3express` 名前空間、AWS リージョン、AWS アカウント ID、アベイラビリティーゾーン ID を含むディレクトリバケット名が含まれます。ディレクトリバケットにアクセスしてアクションを実行するには、次の ARN 形式を使用する必要があります。

```
arn:aws:s3express:region:account-id:bucket/base-bucket-name--zone-id--x-s3
```

ARN の詳細については、「IAM ユーザーガイド」の「Amazon Resource Names (ARNs)」を参照してください。リソースの詳細については、「IAM ユーザーガイド」の「IAM JSON ポリシー要素: Resource」を参照してください。

ディレクトリバケットのアクション

IAM ポリシーまたはリソースベースのポリシーで、どの S3 on Outposts アクションを許可または拒否するかを定義します。アクションは特定の API オペレーションに対応しています。ディレクトリバケットを使用する場合、S3 Express One Zone 名前空間を使用してアクセス許可を付与できます。この名前空間は `s3express` です。

`s3express:CreateSession` アクセス許可を付与すると、`CreateSession` API オペレーションは ゾーンのエンドポイント API (またはオブジェクトレベル) オペレーションにアクセスする際にセッショントークンを取得できるようになります。このようなセッショントークンは、その他すべ

ての ゾーンのエンドポイント API オペレーションへのアクセスを許可するために使用される認証情報を返します。この結果、IAM ポリシーを使用してゾーンの API オペレーションにアクセス許可を付与する必要がなくなります。代わりに、セッショントークンによりアクセスが実現します。ゾーンエンドポイント API オペレーションとアクセス許可のリストについては、「Authenticating and authorizing requests」を参照してください。

ゾーンとリージョンのエンドポイント API オペレーションの詳細については、「ディレクトリバケットのネットワーク」を参照してください。`CreateSession` API オペレーションの詳細については、「Amazon Simple Storage Service API リファレンス」の「CreateSession」を参照してください。.

IAM ポリシーステートメントの `Action` エレメントでは、以下のアクションを指定できます。ポリシーを使用して、AWS でオペレーションを実行するアクセス許可を付与します。ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、単独のアクションが複数のオペレーションへのアクセスを制御する場合もあります。バケットレベルのアクションへのアクセスは IAM アイデンティティベースのポリシー (ユーザーまたはロール) でのみ付与でき、バケットポリシーでは付与できません。

> **Note**
>
> ディレクトリバケットのアクセスポイントを使用してバケットまたはオブジェクトオペレーションへのアクセスを制御する場合は、次の点に注意してください。
>
> - アクセスポイントを使用してバケットオペレーションへのアクセスを制御する方法については、「ディレクトリバケットのアクセスポイントのポリシーでのバケットオペレーション」を参照してください。
> - アクセスポイントを使用してオブジェクトオペレーションへのアクセスを制御する方法については、「ディレクトリバケットのアクセスポイントのポリシーでのオブジェクトオペレーション」を参照してください。
> - アクセスポイントポリシーの設定方法の詳細については、「ディレクトリバケットのアクセスポイントを使用するための IAM ポリシーの設定」を参照してください。

次の表は、アクションと条件キーを示しています。

アクション	API	説明	アクセスレベル	条件キー
s3express:CreateBucket	CreateBucket	上がらしいバケット作成のための権限	書き込み	s3express:authType s3express:LocationName s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256
s3express:CreateSession	ゾーンエンドポイント API オペレーション	セッショントークンを作成するアクセス許可を付与します。このセッショントークンは、CopyObject 、PutObject 、GetObject 、HeadBucket など、すべてのゾーン (オブジェクトレベル) API オペレーションへのアクセスを許可するために使用します。	書き込み	s3express:authType s3express:SessionMode s3express:ResourceAccount

アクション	API	説明	アクセスレベル	条件キー
				s3express:signatureversion s3express:signatureAge s3express:TlsVersion s3express:x-amz-content-sha256 s3express:x-amz-server-side-encryption s3express:x-amz-server-side-encryption-aws-kms-key-id

アクション	API	説明	アクセスレベル	条件キー
s3express:DeleteBucket	DeleteBucket	URI で指定されたバケットを削除するアクセス許可を付与します。	書き込み	s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256

アクション	API	説明	アクセスレベル	条件キー
s3express:DeleteBucketPolicy	DeleteBucketPolicy	指定されたバケットのポリシーを削除するアクセス許可を付与します。	権限の管理	s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256

アクション	API	説明	アクセスレベル	条件キー
s3express:GetBucketPolicy	GetBucketPolicy	指定されたバケットのポリシーを戻すアクセス許可を付与します。	読み取り	s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256

アクション	API	説明	アクセスレベル	条件キー
s3express:GetEncryptionConfiguration	GetBucketEncryption	ディレクトリバケットにデフォルトの暗号化設定を返すアクセス許可を付与します。	読み取り	s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256

アクション	API	説明	アクセスレベル	条件キー
s3express:ListAllMyDirectoryBuckets	ListDirectoryBuckets	認証されたリクエストの送信者が所有するすべてのディレクトリバケットを一覧表示するアクセス許可を付与します。	リスト	s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256

アクション	API	説明	アクセスレベル	条件キー
s3express:PutBucketPolicy	PutBucketPolicy	バケットのバケットポリシーを追加または置き換えるアクセス許可を付与します。	権限の管理	s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256

アクション	API	説明	アクセスレベル	条件キー
s3express:PutBucketPolicy	PutBucketPolicy	バケットのバケットポリシーを追加または置き換えるアクセス許可を付与します。	権限の管理	s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256

アクション	API	説明	アクセスレベル	条件キー
s3express:PutEncryptionConfiguration	PutBucketEncryption 、または DeleteBucketEncryption	ディレクトリバケットの暗号化設定を設定するアクセス許可を付与します	書き込み	s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256

アクション	API	説明	アクセスレベル	条件キー
s3express:CreateAccessPoint	CreateAccessPoint	ディレクトリバケットに関連付けるアクセスポイントを作成するアクセス許可を付与します。	書き込み	s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:LocationName s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256

アクション	API	説明	アクセスレベル	条件キー
s3express:ListAccessPointsForDirectoryBuckets	ListAccessPointsForDirectoryBuckets	アクセスポイントを一覧表示するアクセス許可を付与します。	リスト	s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256

アクション	API	説明	アクセスレベル	条件キー
s3express:GetAccessPoint	GetAccessPoint	指定したアクセスポイントに関する設定情報を返すアクセス許可を付与します。	読み取り	s3express:DataAccessPointAccount s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256

アクション	API	説明	アクセスレベル	条件キー
s3express:DeleteAccessPoint	DeleteAccessPoint	URI 内の指定したアクセスポイントを削除するアクセス許可を付与します。	書き込み	s3express:DataAccessPointAccount s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256

アクション	API	説明	アクセスレベル	条件キー
s3express:DeleteAccessPointPolicy	DeleteAccessPointPolicy	指定したアクセスポイントのポリシーを削除するアクセスを許可します。	権限の管理	s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256

アクション	API	説明	アクセスレベル	条件キー
s3express:GetAccessPointPolicy	GetAccessPointPolicy	指定したアクセスポイントに関連付けられたアクセスポイントポリシーを返すアクセス許可を付与します。	読み取り	s3express:DataAccessPointAccount s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256

アクション	API	説明	アクセスレベル	条件キー
s3express:PutAccessPointPolicy	PutAccessPointPolicy	指定したアクセスポイントにアクセスポリシーを関連付けるアクセス許可を付与します。	権限の管理	s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256

アクション	API	説明	アクセスレベル	条件キー
s3express:DeleteAccessPointScope	DeleteAccessPointScope	指定したアクセスポイントの範囲の設定を削除するアクセス許可を付与します。	権限の管理	s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256

アクション	API	説明	アクセスレベル	条件キー
s3express:GetAccessPointScope	GetAccessPointScope	指定したアクセスポイントに関連付けられた範囲の設定を返すアクセス許可を付与します。	読み取り	s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256

アクション	API	説明	アクセスレベル	条件キー
s3express:PutAccessPointScope	PutAccessPointScope	アクセスポイントを指定されたアクセスポイントの範囲の設定に関連付けるアクセス許可を付与します。	権限の管理	s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256

ディレクトリバケットの条件キー

IAM ポリシーの Condition 要素で使用できる条件キーは以下のとおりです。これらのキーを使用して、ポリシーステートメントが適用される条件をさらに絞り込むことができます。

条件キー	説明	タイプ
s3express:authType	認証方式でアクセスをフィルタリングします 受信するリクエストが特定の認証方法を使用するように制限するには、このオプションの条件キーを使用します。例えば、この条件キーを使用すると、リクエスト認証のために HTTP Authorization ヘッダーのみの使用を指定できます。 有効な値:REST-HEADER 、REST-QUERY-STRING|	String
s3express:LocationName	CreateBucket API オペレーションへのアクセスを、usw2-az1 などの特定のアベイラビリティーゾーン ID (AZ ID) でフィルタリングします。 値の例: usw2-az1	String
s3express:ResourceAccount	リソース所有者の AWS アカウント ID でアクセスをフィルタリングします 特定の AWS アカウント ID が所有するディレクトリバケットへのユーザー、ロール、またはアプリケーションアクセスを制限するには、aws:ResourceAccount または s3express:ResourceAccount 条件キーを使用できます。この条件キーは、AWS Identity and Access Management (IAM) ID ポリシーまたは仮想プライベートクラウド (VPC) エンドポイントポリシーのいずれかで使用できます。例えば、この条件キーを使用して、VPC 内でユーザーの所有していないバケットにクライアントがアクセスできないように制限できます。 値の例: 111122223333	String

条件キー	説明	タイプ
s3express:SessionMode	CreateSession API オペレーションがリクエストしたアクセス許可でアクセスをフィルタリングします。デフォルトでは、このセッションは ReadWrite です。この条件キーを使用して、ReadOnly アクセスを制限したり、ReadWrite アクセスを明示的に拒否したりできます。詳細については、「Amazon Simple Storage Service API リファレンス」の「ディレクトリバケットのバケットポリシーの例」と「CreateSession」を参照してください。 有効な値:ReadWrite 、ReadOnly|	String
s3express:signatureAge	リクエスト署名の経過時間 (ミリ秒単位) でアクセスをフィルタリングします この条件は、署名付き URL でのみ機能します。 AWS Signature Version 4 では、署名キーは最大 7 日間有効です。したがって、署名の有効期間も最大 7 日間となります。詳細については、「Amazon Simple Storage Service API リファレンス」の「Introduction to Signing Requests」(リクエスト署名の導入) を参照してください。この条件を使用すると、署名の有効期間をさらに制限できます。 値の例: 600000	数値
s3express:signatureversion	認証されたリクエストでサポートされる AWS 署名のバージョンを識別します。リクエストの認証用に Signature Version 4 がサポートされるようになりました。 有効な値: "AWS4-HMAC-SHA256" (Signature Version 4 を識別)	String

条件キー	説明	タイプ
s3express:TlsVersion	クライアントが使用する TLS バージョンでアクセスをフィルタリングします s3:TlsVersion 条件キーを使用して、クライアントが使用する TLS バージョンに基づいてディレクトリバケットへのユーザーまたはアプリケーションのア クセスを制限する IAM ポリシー、仮想プライベートクラウドエンドポイント (VPCE) ポリシー、またはバケットポリシーを作成できます。この条件キーを使用して、最小の TLS バージョンを必要とするポリシーを作成することもできます。 値の例: 1.3	数値

条件キー	説明	タイプ
s3express:x-amz-content-sha256	バケット内の未署名のコンテンツでアクセスをフィルタリングします この条件キーを使用すると、バケット内にある署名されていないコンテンツを許可しません。 Authorization ヘッダーを使用するリクエストに Signature Version 4 を使用する場合、署名計算に x-amz-content-sha256 ヘッダーを追加してから、その値をハッシュペイロードに設定します。 バケットポリシーでこの条件キーを使用すると、ペイロードが署名されていないアップロードを拒否できます。例: • リクエスト認証において、Authorization ヘッダーを使用するアップロードを拒否し、ペイロードには署名しません。詳細については、「Amazon Simple Storage Service API リファレンス」の「Transferring payload in a single chunk」(ペイロードを 1 つのチャンクで転送する) を参照してください。 • 署名付き URL を使用するアップロードを拒否します。署名済み URL は常に UNSIGNED_PAYLOAD を持ちます。詳細については、「Amazon Simple Storage Service API リファレンス」の「Authenticating Requests」(認証リクエスト) 「Authentication methods」(認証メソッド) を参照してください。 有効な値: UNSIGNED-PAYLOAD	String

条件キー	説明	タイプ
s3express:x-amz-server-side-encryption	サーバー側の暗号化でアクセスをフィルタリングします 有効な値:"AES256"、aws:kms|	String
s3express:x-amz-server-side-encryption-aws-kms-key-id	サーバー側の暗号化のための AWS KMS カスタマーマネージド CMK で、アクセスをフィルタリングします 値の例: "arn:aws:kms: *region*:*acct-id*:key/*key-id*"	ARN

ディレクトリバケットの IAM アイデンティティベースのポリシー

ディレクトリバケットを作成する前に、AWS Identity and Access Management (IAM) ロールまたはユーザーに必要なアクセス許可を付与する必要があります。このポリシー例では、CreateSession API オペレーション (ゾーンエンドポイント [オブジェクトレベル] API オペレーションで使用) とすべてのリージョンエンドポイント (バケットレベル) API オペレーションへのアクセスを許可します。このポリシーでは、すべてのディレクトリバケットでの CreateSession API オペレーションの使用が許可されます。ただし、リージョンエンドポイント API オペレーションは、指定されたディレクトリバケットでの使用のみが許可されます。このポリシーの例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Sid": "AllowAccessRegionalEndpointAPIs",
             "Effect": "Allow",
             "Action": [
                 "s3express:DeleteBucket",
                 "s3express:DeleteBucketPolicy",
                 "s3express:CreateBucket",
                 "s3express:PutBucketPolicy",
                 "s3express:GetBucketPolicy",
                 "s3express:ListAllMyDirectoryBuckets"
             ],
```

```
            "Resource": "arn:aws:s3express:region:account_id:bucket/bucket-base-
name--zone-id--x-s3/*"
        },
        {
            "Sid": "AllowCreateSession",
            "Effect": "Allow",
            "Action": "s3express:CreateSession",
            "Resource": "*"
        }
    ]
}
```

ディレクトリバケットのバケットポリシーの例

このセクションでは、ディレクトリバケットポリシーの例を示します。これらのポリシーを使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

次のバケット ポリシーの例では、AWS アカウント ID *111122223333* が、指定されたディレクトリバケットのデフォルト ReadWrite セッションで CreateSession API オペレーションを使用することを許可します。このポリシーは、ゾーンエンドポイント (オブジェクトレベル) の API オペレーションへのアクセスを許可します。

Example – デフォルトの **ReadWrite** セッションでの **CreateSession** 呼び出しを許可するバケットポリシー

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadWriteAccess",
            "Effect": "Allow",
            "Resource": "arn:aws:s3express:us-west-2:account-id:bucket/bucket-base-
name--zone-id--x-s3",
            "Principal": {
                "AWS": [
                    "111122223333"
                ]
            },
            "Action": [
                "s3express:CreateSession"
            ]
```

```
        }
    ]
}
```

Example – **ReadOnly** セッションでの **CreateSession** 呼び出しを許可するバケットポリシー

次のバケットポリシー例では、AWS アカウント ID *111122223333* が CreateSession API オペレーションを使用することを許可しています。このポリシーは、s3express:SessionMode 条件キーと ReadOnly 値を使用して読み取り専用セッションを設定します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadOnlyAccess",
            "Effect": "Allow",
            "Principal": {
                "AWS": "111122223333"
            },
            "Action": "s3express:CreateSession",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "s3express:SessionMode": "ReadOnly"
                }
            }
        }
    ]
}
```

Example — **CreateSession** 呼び出しのためにクロスアカウントアクセスを許可するバケットポリシー

次のバケットポリシーの例では、AWS アカウント ID *111122223333* が、AWS アカウント ID *444455556666* が所有する指定されたディレクトリ バケットに対して CreateSession API オペレーションを使用することを許可します。

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CrossAccount",
            "Effect": "Allow",
            "Principal": {
                "AWS": "111122223333"
            },
            "Action": [
                "s3express:CreateSession"
            ],
            "Resource": "arn:aws:s3express:us-west-2:444455556666:bucket/bucket-base-name--zone-id--x-s3"

        }
    ]
}
```

CreateSession を使用したゾーンエンドポイント API オペレーションの承認

ゾーンエンドポイント API オペレーション (オブジェクトレベルまたはデータプレーンオペレーション) を使用するには (CopyObject と HeadBucket を除く) CreateSession API オペレーションを使用して、データリクエストの低レイテンシー承認に最適化されたセッションを作成および管理します。ッションントークンを取得して使用するには、アイデンティティベースのポリシーまたはバケットポリシーでディレクトリバケットの s3express:CreateSession アクションを許可する必要があります。詳細については、「IAM を使用したリージョンエンドポイント API オペレーションの承認」を参照してください。Amazon S3 コンソール、AWS Command Line Interface (AWS CLI)、または AWS SDK を使用して S3 Express One ゾーンにアクセスしている場合、S3 Express One Zone はユーザーに代わってセッションを作成します。

Amazon S3 REST API を使用する場合、CreateSession API オペレーションを使用して、アクセスキー ID、シークレットアクセスキー、セッショントークン、有効期限を含む一時的なセキュリティ認証情報を取得できます。一時的な認証情報は、IAM ユーザーの認証情報など、長期的なセキュリティ認証情報を使用するのと同じアクセス許可を提供します。ただし、一時的なセキュリティ認証情報にはセッショントークンが含まれている必要があります。

セッションモード

セッションモードはセッションの範囲を定義します。バケットポリシーでは、s3express:SessionMode 条件キーを指定して、ReadWrite セッションや ReadOnly セッ

ションを作成できるユーザーを制御できます。ReadWrite と ReadOnly の詳細については、「Amazon S3 API リファレンス」の「CreateSession の x-amz-create-session-mode パラメータ」を参照してください。バケットポリシー作成の詳細については、「ディレクトリバケットのバケットポリシーの例」を参照してください。

セッショントークン

一時的なセキュリティ認証情報を使用して呼び出しを行う場合、呼び出しにはセッショントークンを含める必要があります。セッショントークンは一時的な認証情報とともに返されます。セッショントークンの範囲はディレクトリバケットに限定され、セキュリティ認証情報が有効で有効期限が切れていないことを確認するために使用されます。セッションを保護するため、一時的なセキュリティ認証情報は 5 分後に期限切れになります。

CopyObject および HeadBucket

一時的なセキュリティ認証情報の範囲は特定のディレクトリバケットに限定され、特定のディレクトリバケットに対するすべてのゾーン (オブジェクトレベル) オペレーション API 呼び出しで自動的に有効になります。その他のゾーンエンドポイント API 操作とは異なり、CopyObject と HeadBucket は CreateSession 認証を使用しません。すべての CopyObject リクエストと HeadBucket リクエストは IAM 認証情報を使用して認証され、署名される必要があります。ただし、その他のゾーンエンドポイント API オペレーションと同様に CopyObject と HeadBucket の s3express:CreateSession による承認が引き続き行われます。

詳細については、「Amazon Simple Storage Service API リファレンス」の「CreateSession」を参照してください。

ディレクトリバケットのセキュリティのベストプラクティス

ディレクトリバケットを使用する際に考慮すべきセキュリティ機能がいくつかあります。以下のベストプラクティスは一般的なガイドラインであり、完全なセキュリティソリューションを提供するものではありません。これらのベストプラクティスは顧客の環境に必ずしも適切または十分でない可能性があるので、処方箋ではなく、あくまで有用な推奨事項とお考えください。

デフォルトのブロックパブリックアクセスとオブジェクト所有権の設定

ディレクトリバケットは S3 ブロックパブリックアクセスと S3 オブジェクト所有権をサポートします。このような S3 機能は、バケットとオブジェクトへのアクセスを監査して管理するために使用されます。

デフォルトでは、ディレクトリバケットのすべてのブロックパブリックアクセス設定が有効になっています。さらに、オブジェクト所有者はバケット所有者の強制に設定されています。これは、アク

セスコントロールリスト (ACL) が無効になっていることを意味します。上記の設定は変更できません。上記の機能の詳細については、「the section called “パブリックアクセスのブロック”」と「the section called “オブジェクト所有者の管理”」を参照してください。

> **Note**
>
> ディレクトリバケットに保存されているオブジェクトへのアクセスは付与できません。アクセスは、ディレクトリバケットにたいしてのみ付与できます。S3 Express One Zone の認可モデルは、Amazon S3 の認可モデルとは異なります。詳細については、「`CreateSession` を使用したゾーンエンドポイント API オペレーションの承認」を参照してください。

認証と認可

ディレクトリバケットの認証と認可のメカニズムは、ゾーンエンドポイント API オペレーションまたはリージョンエンドポイント API オペレーションのどちらにリクエストを行うかに応じて異なります。ゾーン API オペレーションはオブジェクトレベル (データプレーン) のオペレーションです。リージョン API オペレーションはバケットレベル (コントロールプレーン) のオペレーションです。

ゾーンエンドポイント API オペレーションへのリクエストを認証および認可するには、レイテンシーを最小限に抑えるように最適化された新しいセッションベースのメカニズム を使用します。セッションベースの認証では、AWS SDK は `CreateSession` API オペレーション を使用して一時的な認証情報をリクエストします。これにより、ディレクトリバケットに低レイテンシーでアクセスできます。これらの一時認証情報は特定のディレクトリバケットに限定され、5 分後に期限切れになります。このような一時的な認証情報を使用して、ゾーン (オブジェクトレベル) API 呼び出しに署名できます。詳細については、「`CreateSession` を使用したゾーンエンドポイント API オペレーションの承認」を参照してください。

ディレクトリバケット管理用の認証情報を使用したリクエストの署名

認証情報を使用してゾーンエンドポイント (オブジェクトレベル) API リクエストに署名するには、`s3express` をサービス名として、AWS Signature Version 4 を使用します。リクエストに署名する際は、`CreateSession` から返されたシークレットキーを使用し、セッショントークンを `x-amzn-s3session-token header` に渡します。詳細については、「CreateSession」を参照してください。

サポートされている AWS SDK がユーザーに代わって認証情報と署名を管理します。AWS SDK を使用して認証情報を更新し、リクエストに署名することをお勧めします。

IAM 認証情報を使用したリクエストの署名

リージョン (バケットレベル) の API 呼び出しはすべて、一時的なセッション認証情報ではなく AWS Identity and Access Management (IAM) 認証情報で認証および署名される必要があります。IAM 認証情報は IAM アイデンティティのアクセスキー ID とシークレットアクセスキーで構成されます。すべての `CopyObject` リクエストと `HeadBucket` リクエストは IAM 認証情報を使用して認証され、署名される必要があります。

ゾーン (オブジェクトレベル) オペレーション呼び出しのレイテンシーを最小限に抑えるには、`CopyObject` と `HeadBucket` へのリクエストを除き、`CreateSession` を呼び出して取得した認証情報を使用してリクエストに署名することをお勧めします。

AWS CloudTrail を使用する

AWS CloudTrail は、Amazon S3 のユーザー、ロール、または AWS のサービス が実行したアクションの記録を提供します。CloudTrail によって収集されたデータを使用して、以下の情報を判断できます。

- Amazon S3 に対して行われたリクエスト
- リクエストが行われた IP アドレス
- リクエストを行ったユーザー
- リクエストが行われた時間
- リクエストに関するその他の詳細

AWS アカウントのセットアップ時には、CloudTrail 管理イベントはデフォルトで有効になっています。次のリージョンエンドポイント API オペレーション (バケットレベル、またはコントロールプレーンの API オペレーション) が CloudTrail に記録されます。

- CreateBucket
- DeleteBucket
- DeleteBucketPolicy
- PutBucketPolicy
- GetBucketPolicy
- ListDirectoryBuckets
- ListMultipartUploads
- PutBucketEncryption

- GetBucketEncryption
- DeleteBucketEncryption

> **Note**
>
> `ListMultipartUploads` は、ゾーンエンドポイント API オペレーションです。ただし、この API オペレーションは CloudTrail に管理イベントとして記録されます。詳細については、「Amazon Simple Storage Service API リファレンス」の「ListMultipartUploads」を参照してください。

デフォルトでは CloudTrail 証跡はデータイベントを記録しませんが、証跡を設定して、指定したディレクトリバケットのデータイベントを記録したり、ご使用の AWS アカウントですべてのディレクトリバケットのデータイベントを記録したりできます。次のゾーンエンドポイント API オペレーション (オブジェクトレベル、またはデータプレーンの API オペレーション) が CloudTrail に記録されます。

- AbortMultipartUpload
- CompleteMultipartUpload
- CreateSession
- CopyObject
- CreateMultipartUpload
- DeleteObject
- DeleteObjects
- GetObject
- GetObjectAttributes
- HeadBucket
- HeadObject
- ListObjectsV2
- ListParts
- PutObject
- UploadPart
- UploadPartCopy

ディレクトリバケットで AWS CloudTrail を使用する方法の詳細については、「ディレクトリバケットの AWS CloudTrail による口グ記録」を参照してください。

AWS モニタリングツールを使用したモニタリングを実装する

モニタリングは、Amazon S3 および AWS ソリューションの信頼性、セキュリティ、可用性、パフォーマンスを維持する上で重要な工レメントです。AWS では、Amazon S3 およびその他の AWS のサービス をモニタリングするのに役立つツールとサービスを提供しています。例えば、Amazon S3 の Amazon CloudWatch メトリクス、特に `BucketSizeBytes` と `NumberOfObjects` ストレージ メトリクスをモニタリングできます。

ディレクトリバケットに保存されているオブジェクトは、Amazon S3 の `BucketSizeBytes` および `NumberOfObjects` ストレージメトリクスには反映されません。ただし、`BucketSizeBytes` および `NumberOfObjects` ストレージメトリクスはディレクトリバケットでサポートされています。希望するメトリクスを表示するには、`StorageType` ディメンションを指定することで Amazon S3 ストレージクラス間を区別できます。詳細については、「Amazon CloudWatch によるメトリクスのモニタリング」を参照してください。

詳細については、「Amazon CloudWatch によるメトリクスのモニタリング」および「Amazon S3 での口グ記録とモニタリング」を参照してください。

アクセスポイントを使用したディレクトリバケット内の共有データセットへのアクセスの管理

Amazon S3 Access Points は、Amazon S3 の共有データセットへの大規模なデータアクセスの管理を簡素化します。アクセスポイントは、アクセスポイントを介して行われたすべてのリクエストに対して個別のアクセス許可とネットワークコントロールを適用するために作成する一意のホスト名です。バケットごとに数百のアクセスポイントを作成できます。各アクセスポイントには、アプリケーションごとにカスタマイズされた個別の名前とアクセス許可があります。各アクセスポイントには、基になるバケットにアタッチされたバケットポリシーと連動して機能します。

ディレクトリバケットでは、アクセスポイント名は、指定したベース名、ディレクトリバケットの場所のゾーン ID (AWS アベイラビリティゾーンまたはローカルゾーン)、`--xa-s3` で構成されます。例えば、*`accesspointname`*`--`*`zoneID`*`--xa-s3`。アクセスポイントを作成した後は、名前またはゾーン ID を変更することはできません。

ディレクトリバケットのアクセスポイントでは、アクセスポイントの範囲を使用して、特定のプレフィックスまたは API オペレーションへのアクセスを制限できます。任意の量のプレフィックスを

指定できますが、すべてのプレフィックスの文字の合計長は 256 バイト未満である必要があります。

仮想プライベートクラウド (VPC) からのリクエストのみを受け付けるようにアクセスポイントを設定できます。これにより、Amazon S3 データアクセスがプライベートネットワークに制限されます。

このセクションでは、ディレクトリバケットのアクセスポイントを使用する方法について説明します。汎用バケットの詳細については、「ディレクトリバケットの使用」を参照してください。

トピック

- ディレクトリバケットのアクセスポイントの命名規則、制約と制限
- ディレクトリバケットのアクセスポイントの参照
- ディレクトリバケットのアクセスポイントのオブジェクトオペレーション
- ディレクトリバケットのアクセスポイントを使用するための IAM ポリシーの設定
- ディレクトリバケットのアクセスポイントのモニタリングとログ記録
- ディレクトリバケットのアクセスポイントの作成
- ディレクトリバケットのアクセスポイントの管理

ディレクトリバケットのアクセスポイントの命名規則、制約と制限

アクセスポイントは、Amazon S3 の共有データセットへの大規模なデータアクセスの管理を簡素化します。以下のトピックでは、アクセスポイントの命名規則と制限および制約に関する情報を提供します。

トピック

- ディレクトリバケットのアクセスポイントの命名規則
- ディレクトリバケットのアクセスポイントの命名規則、制約と制限

ディレクトリバケットのアクセスポイントの命名規則

アクセスポイントは、バケットと同じゾーンに作成する必要があります。アクセスポイント名は、ゾーン内で一意である必要があります。

アクセスポイント名は DNS に準拠しており、次の条件を満たす必要があります。

- 数字または小文字で始める

- 提供するベース名は、3～50 文字である必要があります。
- 名前をハイフン (-) で開始または終了することはできません。
- 下線 (_)、大文字、スペース、ピリオド (.) は使用しない
- サフィックス *zoneid*--xa--s3 で終わる必要があります。

ディレクトリバケットのアクセスポイントの命名規則、制約と制限

ディレクトリバケットのアクセスポイントには以下の制約と制限があります。

- 各アクセスポイントは、1 つのディレクトリバケットに関連付けられます。作成後のアクセスポイントを別のバケットに関連付けることはできません。ただし、アクセスポイントを削除して、新しいアクセスポイントを同じ名前で作成し、別のバケットに関連付けることはできます。
- アクセスポイントを作成した後、その Virtual Private Cloud (VPC) 設定を変更することはできません。
- アクセスポイントのポリシーのサイズは 20 KB に制限されています。
- アクセスポイントスコーププレフィックスの合計サイズは 256 バイトに制限されています。
- AWS アカウントごと、AWS リージョンごとに最大 10,000 個のアクセスポイントを作成できます。1 つのリージョンで 1 つのアカウントに 10,000 個を超えるアクセスポイントが必要な場合は、サービスクォータの引き上げをリクエストできます。サービスクォータと引き上げリクエストの詳細については、「AWS 全般のリファレンス」の「AWS Service Quotas」を参照してください。
- アクセスポイントは、オブジェクトに対するオペレーションの実行にのみ使用できます。アクセスポイントを使用して、バケットの変更や削除など、Amazon S3 バケットオペレーションを実行することはできません。サポートされているオペレーションの完全なリストについては、「ディレクトリバケットのアクセスポイントのオブジェクトオペレーション」を参照してください。
- アクセスポイントは、名前、アクセスポイントエイリアス、またはvirtual-hosted-style URI で参照できます。ARN でアクセスポイントに対処することはできません。詳細については、「ディレクトリバケットのアクセスポイントの参照」を参照してください。
- アクセスポイントの機能 (`PutAccessPointPolicy` や `GetAccessPointPolicy` など) を制御する API オペレーションでは、アクセスポイントを所有する AWS アカウントを指定する必要があります。
- REST API を使用してアクセスポイントへのリクエストを行う場合は、AWS Signature Version 4 を使用する必要があります。リクエストの認証の詳細については、Amazon Simple Storage Service API リファレンスのリクエストの承認 (AWS Signature Version 4) を参照してください。

- アクセスポイントは HTTPS 経由のリクエストのみをサポートしています。Amazon S3 は、HTTP 経由で行われたすべてのリクエストに対して HTTP リダイレクトで自動的に応答し、リクエストを HTTPS にアップグレードします。
- アクセスポイントは匿名アクセスをサポートしていません。
- 別のアカウントが所有するバケット (クロスアカウントアクセスポイント) へのアクセスポイントを作成する場合、バケット所有者がバケットへのアクセス許可を付与するまで、クロスアカウントアクセスポイントはデータへのアクセスを許可しません。バケット所有者は常にデータを完全に管理できるため、クロスアカウントアクセスポイントからのリクエストを許可するにはバケットポリシーを更新する必要があります。バケットポリシーの例を表示するには、「ディレクトリバケットのアクセスポイントを使用するための IAM ポリシーの設定」を参照してください。

ディレクトリバケットのアクセスポイントの参照

アクセスポイントを作成したら、オブジェクトオペレーションを実行するエンドポイントとして使用できます。ディレクトリバケットのアクセスポイントの場合、アクセスポイントエイリアスはアクセスポイント名と同じです。すべてのデータオペレーションでバケット名の代わりにアクセスポイント名を使用できます。これらのサポートされているオペレーションのリストについては、「ディレクトリバケットのアクセスポイントのオブジェクトオペレーション」を参照してください。

仮想ホスト形式の URI によるアクセスポイントの参照

アクセスポイントでは、仮想ホスト形式のアドレス指定のみがサポートされます。アクセスポイントは、ディレクトリバケットエンドポイントと同じ形式を使用します。詳細については、「ディレクトリバケットのリージョンエンドポイントとゾーンエンドポイント」を参照してください。

S3 アクセスポイントでは、HTTP 経由のアクセスはサポートされていません。アクセスポイントでは HTTPS 経由のセキュアなアクセスのみがサポートされます。

ディレクトリバケットのアクセスポイントのオブジェクトオペレーション

アクセスポイントを使用して、次の S3 データオペレーションを使用してオブジェクトにアクセスできます。

- AbortMultipartUpload
- CompleteMultipartUpload
- CopyObject
- CreateMultipartUpload

- CreateSession
- DeleteObject
- DeleteObjects
- GetObject
- GetObjectAttributes
- HeadBucket
- HeadObject
- ListMultipartUploads
- ListObjectsV2
- ListParts
- PutObject
- UploadPart
- UploadPartCopy

ディレクトリバケットのアクセスポイントを使用するための IAM ポリシーの設定

アクセスポイントは AWS Identity and Access Management (IAM) リソースポリシーをサポートしています。これにより、リソース、ユーザー、その他の条件別にアクセスポイントの使用を制御できます。アプリケーションやユーザーがアクセスポイントを介してオブジェクトにアクセスするには、アクセスポイントと基になるバケットポリシーの両方でリクエストを許可する必要があります。

> **Important**
>
> アクセスポイントをバケットに追加しても、バケット名でアクセスしたときのバケットの動作は変わりません。バケットに対する既存のすべてのオペレーションは、以前と同じように動作します。アクセスポイントポリシーまたはアクセスポイントスコープに含めた制限は、そのアクセスポイントを介したリクエストにのみ適用されます。

IAM リソースポリシーを使用する際、ポリシーを保存する前に、AWS Identity and Access Management Access Analyzer からのセキュリティ警告、エラー、一般的な警告、および提案を解決してください。IAM Access Analyzer は、IAM ポリシーの文法とベストプラクティスに照らしてポリ

シーチェックを行います。これらのチェックにより、機能的でセキュリティのベストプラクティスに準拠したポリシーを作成するのに、役立つ結果とレコメンデーションが示されます。

IAM Access Analyzer を使用したポリシーの検証の詳細については、「IAM ユーザーガイド」の「IAM Access Analyzer のポリシーの検証」を参照してください。IAM Access Analyzer によって返される警告、エラー、および提案のリストを表示するには、「IAM Access Analyzer ポリシーチェックリファレンス」を参照してください。

ディレクトリバケットポリシーのアクセスポイントの例

以下のアクセスポイントポリシーは、ディレクトリバケットへのリクエストを制御する方法を示しています。アクセスポイントポリシーには、バケット ARN またはアクセスポイント ARN が必要です。アクセスポイントのエイリアスは、ポリシーではサポートされていません。アクセスポイント ARN の例を次に示します。

```
arn:aws:s3express:region:account-id:accesspoint/myaccesspoint--zoneID--xa-s3
```

アクセスポイント ARN は、アクセスポイントの詳細で確認できます。詳細については、「ディレクトリバケットのアクセスポイントの詳細を表示する」を参照してください。

> **Note**
>
> アクセスポイントポリシーで付与されるアクセス許可は、基になるバケットでも同じアクセスが許可される場合にのみ有効です。このためには以下の 2 つの方法があります。
>
> 1. (推奨)「アクセスポイントへのアクセスコントロールの委任」の説明に従って、バケットからアクセスポイントにアクセスコントロールを委任します。
> 2. アクセスポイントポリシーに含まれているものと同じアクセス許可を、基になるバケットのポリシーに追加します。

Example 1 – アクセスポイントを VPC ネットワークオリジンに制限するサービスコントロールポリシー

次のサービスコントロールポリシーは、すべての新しいアクセスポイントを 仮想プライベートクラウド (VPC) ネットワークオリジンで作成することを要求します。このポリシーを適用すると、組織内のユーザーは、インターネットからアクセス可能なアクセスポイントを作成できなくなります。

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
        "Effect": "Deny",
        "Action": "s3express:CreateAccessPoint",
        "Resource": "*",
        "Condition": {
            "StringNotEquals": {
                "s3express:AccessPointNetworkOrigin": "VPC"
            }
        }
    }
  ]
}
```

Example 2 – バケットへのアクセスを VPC ネットワークオリジンを持つアクセスポイントに制限するアクセスポイントポリシー

次のアクセスポイントポリシーでは、バケット *amzn-s3-demo-bucket--zoneID--x-s3* へのすべてのアクセスを、VPC ネットワークオリジンを持つアクセスポイントに制限します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Principal": "*",
            "Action": "s3express:CreateSession",
            "Effect": "Deny",
            "Resource": "arn:aws:s3express:region:111122223333:bucket/amzn-s3-demo-
bucket--zoneID--x-s3",
            "Condition": {
                "StringNotEqualsIfExists": {
                    "s3express:AccessPointNetworkOrigin": "VPC"
                }
            }
        }
    ]
}
```

条件キー

ディレクトリバケットのアクセスポイントには、IAM ポリシーでリソースへのアクセスを制御するために使用できる条件キーがあります。以下の条件キーは IAM ポリシーの一部にすぎません。すべてのポリシーの例については、「ディレクトリバケットポリシーのアクセスポイントの例」、「アクセスポイントへのアクセスコントロールの委任」および「クロスアカウントアクセスポイントへのアクセス許可の付与」を参照してください。

s3express:DataAccessPointArn

この例では、アクセスポイントの Amazon リソースネーム (ARN) でアクセスをフィルタリングし、リージョン *region* における AWS アカウント *111122223333* のすべてのアクセスポイントと一致させる方法を示します。

```
"Condition" : {
    "StringLike": {
        "s3express:DataAccessPointArn":
 "arn:aws:s3express:region:111122223333:accesspoint/*"
    }
}
```

s3express:DataAccessPointAccount

この例は、アクセスポイントの所有者のアカウント ID を照合するために使用できる文字列演算子です。次の例では、AWS アカウント *111122223333* が所有するすべてのアクセスポイントを照合します。

```
"Condition" : {
    "StringEquals": {
        "s3express:DataAccessPointAccount": "111122223333"
    }
}
```

s3express:AccessPointNetworkOrigin

この例は、ネットワークオリジン (Internet または VPC) の照合に使用できる文字列演算子です。次の例では、VPC オリジンを持つアクセスポイントのみを照合します。

```
"Condition" : {
    "StringEquals": {
```

```
        "s3express:AccessPointNetworkOrigin": "VPC"
    }
}
```

s3express:Permissions

s3express:Permissions を使用して、アクセスポイントの範囲で特定の API オペレーションへのアクセスを制限できます。以下の API オペレーションがサポートされています。

- PutObject
- GetObject
- DeleteObject
- ListBucket (ListObjectsV2 では必須)
- GetObjectAttributes
- AbortMultipartUpload
- ListBucketMultipartUploads
- ListMultipartUploadParts

> **Note**
>
> 複数値条件キーを使用する場合は、Allow ステートメントで ForAllValues を使用し、Deny ステートメントで ForAnyValue を使用することをお勧めします。詳細については、「IAM ユーザーガイド」の「複数値のコンテキストキー」を参照してください。

Amazon S3 での条件キーの使用についての詳細は、「サービス認可リファレンス」の「Actions, resources, and condition keys for Amazon S3」を参照してください。

S3 リソースタイプ別の S3 API オペレーションへの必須のアクセス許可の詳細については、「Amazon S3 API オペレーションに必要なアクセス許可」を参照してください。

アクセスポイントへのアクセスコントロールの委任

バケットポリシーからアクセスポイントポリシーにアクセス制御を委任できます。以下のバケットポリシーの例では、バケット所有者のアカウントが所有するすべてのアクセスポイントへのフルアクセスを許可しています。ポリシーの適用後、このバケットへのすべてのアクセスは、アクセスポイントポリシーによって制御されます。バケットへの直接アクセスを必要としないすべてのユースケースでは、この方法でバケットを設定することをお勧めします。

Example アクセスコントロールをアクセスポイントに委任するバケットポリシー

```
{
    "Version": "2012-10-17",
    "Statement" : [
    {
        "Effect": "Allow",
        "Principal" : { "AWS": "*" },
        "Action" : "*",
        "Resource" : [ "Bucket ARN",
        "Condition": {
            "StringEquals" : { "s3express:DataAccessPointAccount" : "Bucket owner's
 account ID" }
        }
    }]
}
```

クロスアカウントアクセスポイントへのアクセス許可の付与

別のアカウントが所有するバケットへのアクセスポイントを作成するには、まずバケット名とアカウント所有者 ID を指定してアクセスポイントを作成する必要があります。次に、バケット所有者は、アクセスポイントからのリクエストを許可するようにバケットポリシーを更新する必要があります。アクセスポイントの作成は、アクセスポイントがバケットの内容へのアクセスを提供しないという点で DNS CNAME の作成と似ています。すべてのバケットアクセスはバケットポリシーによって制御されます。次のバケットポリシーの例では、信頼できる AWS アカウント が所有するアクセスポイントからのバケットで、GET および LIST リクエストを許可します。

Bucket ARN は、バケットの ARN に置き換えます。

Example 別の AWS アカウントにアクセス許可を委任するバケットポリシー

```
{
    "Version": "2012-10-17",
    "Statement" : [
    {
        "Effect": "Allow",
        "Principal" : { "AWS": "*" },
        "Action" : "s3express:CreateSession",
        "Resource" : [ "Bucket ARN" ],
        "Condition": {
```

```
            "StringEquals" : {
                "s3express:DataAccessPointAccount": "Access point owner's account ID"
            },
            "ForAllValues:StringEquals": {
                "s3express:Permissions": [
                    "GetObject",
                    "ListBucket"
                ]
            }
        }
    }]
}
```

ディレクトリバケットのアクセスポイントのモニタリングとログ記録

AWS CloudTrail を使用して、アクセスポイントを介して行われたリクエストと、アクセスポイントを管理する API に対するリクエスト (CreateAccessPoint や GetAccessPointPolicy, など) をログに記録します。アクセスポイントを介して行われたリクエストの CloudTrail ログエントリには、ログの resources セクションにアクセスポイント ARN (アクセスポイント名を含む) が含まれます。

例えば、次の設定があるとします。

- リージョン region において my-image.jpg という名前のオブジェクトを含む *amzn-s3-demo-bucket*--*zone-id*--x-s3 という名前のバケット。
- *amzn-s3-demo-bucket*--*zone-id*--x-s3 に関連付けられた my-bucket-ap--zoneID--xa-s3 という名前のアクセスポイント
- 123456789012 の AWS アカウント ID

以下の例は、resources前述の設定の CloudTrail ログエントリの セクションを示しています。

```
"resources": [
        {"type": "AWS::S3Express::Object",

            "ARN": "arn:aws:s3express-region:123456789012:bucket/amzn-s3-demo-
bucket--zone-id--x-s3/my-image.jpg"
        },
        {"accountId": "c",
            "type": "AWS::S3Express::DirectoryBucket",
```

```
            "ARN": "arn:aws::s3express:region:123456789012:bucket/amzn-s3-demo-
bucket--zone-id--x-s3"
        },
        {"accountId": "123456789012",
            "type": "AWS::S3::AccessPoint",
            "ARN": "arn:aws:s3express:region:123456789012:accesspoint/my-bucket-ap--
zoneID--xa-s3"
        }
    ]
```

AWS CloudTrail の詳細については、AWS CloudTrail ユーザーガイド の AWS CloudTrail とは を参照してください。

ディレクトリバケットのアクセスポイントの作成

ディレクトリバケットと同様に、アクセスポイントはアベイラビリティーゾーンまたは専有ローカルゾーンに作成できます。アクセスポイントは、それに関連付けられているディレクトリバケットと同じゾーンに作成する必要があります。

アクセスポイントは、1 つの Amazon S3 ディレクトリバケットにのみ関連付けられます。AWS アカウントでディレクトリバケットを使用する場合は、まずディレクトリバケットを作成する必要があります。ディレクトリバケットの作成の詳細については、「アベイラビリティーゾーンでのディレクトリバケットの作成」または「Local Zone でのディレクトリバケットの作成」を参照してください。

バケット名とバケット所有者のアカウント ID がわかっていれば、別の AWS アカウント のバケットに関連するクロスアカウントアクセスポイントを作成することもできます。ただし、クロスアカウントアクセスポイントを作成しても、バケット所有者からアクセス権が付与されるまで、バケット内のデータへのアクセスは許可されません。バケット所有者は、バケットポリシーを通じて、アクセスポイント所有者のアカウント (お客様のアカウント) にバケットへのアクセス権を付与する必要があります。詳細については、「クロスアカウントアクセスポイントへのアクセス許可の付与」を参照してください。

AWS Management Console、AWS CLI、REST API、または AWS SDK を使用して、任意のディレクトリバケットのアクセスポイントを作成できます。各アクセスポイントは 1 つのディレクトリバケットに関連付けられており、バケットごとに数百のアクセスポイントを作成できます。アクセスポイントを作成するときは、アクセスポイントの名前と関連付けるディレクトリバケットを選択します。アクセスポイント名は、ユーザーが指定したベース名、バケットの場所のゾーン ID を含むサフィックス、および `--xa-s3` で構成されます。例えば、*myaccesspoint*-*zoneID*`--xa-s3` など

です。仮想プライベートクラウド (VPC) を介してアクセスポイントへのアクセスを制限することもできます。次に、ディレクトリバケット名を使用するのと同様に、その名前を使用して、アクセスポイントを介してデータの読み取りと書き込みをすぐに開始できます。

アクセスポイントのスコープを使用すると、アクセスポイントを介したディレクトリバケットへのアクセスを特定のプレフィックスまたは API オペレーションに制限できます。アクセスポイントにスコープを追加しない場合、アクセスポイントを介してアクセスすると、ディレクトリバケット内のすべてのプレフィックスとすべての API オペレーションをバケット内のオブジェクトに対して実行できます。アクセスポイントを作成したら、AWS CLI、AWS SDK、または REST API を使用してスコープを追加、変更、または削除できます。詳細については、「ディレクトリバケットのアクセスポイントの範囲を管理する」を参照してください。

アクセスポイントを作成したら、アクセスポイントの IAM リソースポリシーを設定できます。詳細については、「アクセスポイントポリシーの表示、編集、または削除」を参照してください。

S3 コンソールの使用

> **Note**
>
> ディレクトリバケット画面からディレクトリバケットのアクセスポイントを作成することもできます。この場合、ディレクトリバケット名が提供されるため、アクセスポイントの作成時にバケットを選択する必要はありません。詳細については、「ディレクトリバケットの一覧表示」を参照してください。

ディレクトリバケットのアクセスポイントを作成するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ページ上部にあるナビゲーションバーで、現在表示されている AWS リージョン の名前をクリックします。次に、アクセスポイントを作成するリージョンを選択します。アクセスポイントは、関連付けられたバケットと同じリージョンに作成する必要があります。
3. 左のナビゲーションペインで、[ディレクトリバケットのアクセスポイント] を選択します。
4. [アクセスポイント] ページで、[アクセスポイントの作成] を選択します。
5. 自分のアカウントまたは別のアカウントのディレクトリバケットのアクセスポイントを作成できます。別のアカウントのディレクトリバケットのアクセスポイントを作成するには、次の手順を実行します。

> **Note**
>
> 別の AWS アカウント でバケットを使用している場合は、バケット所有者がアクセスポイントからのリクエストを許可するようにバケットポリシーを更新する必要があります。バケットポリシーの例については、「クロスアカウントアクセスポイントへのアクセス許可の付与」を参照してください。

a. [ディレクトリバケット] フィールドで、[別のアカウントのバケットを指定する] を選択します。

b. [バケット所有者のアカウント ID] フィールドに、バケットを所有する AWS アカウント ID を入力します。

c. [バケット名] フィールドに、ベース名とゾーン ID を含むバケットの名前を入力します。例えば、***bucket-base-name*--*zone-id*--x-s3**。

6. 自分のアカウントでディレクトリバケットのアクセスポイントを作成するには:

a. [ディレクトリバケット] フィールドで、[このアカウントのバケットを選択する] を選択します。

b. [バケット名] フィールドに、ベース名とゾーン ID を含むバケットの名前を入力します。例えば、***bucket-base-name*--*zone-id*--x-s3**。リストからバケットを選択するには、[S3 を参照] を選択し、ディレクトリバケットを選択します。

7. [アクセスポイント名] の [ベース名] フィールドに、アクセスポイントの名前を入力します。ゾーン ID と完全なアクセスポイント名が表示されます。アクセスポイントの名前付けの詳細については、「ディレクトリバケットのアクセスポイントの命名規則」を参照してください。

8. [ネットワークオリジン] で、[仮想プライベートクラウド (VPC)] または [インターネット] のいずれかを選択します。[仮想プライベートクラウド (VPC)] を選択した場合は、[VPC ID] フィールドにアクセスポイントで使用する VPC の ID を入力します。

9. (オプション) [アクセスポイントの範囲] で、このアクセスポイントに範囲を適用するには、[プレフィックスまたはアクセス許可を使用してこのアクセスポイントの範囲を制限する] を選択します。

a. ディレクトリバケット内のプレフィックスへのアクセスを制限するには、[プレフィックス] に 1 つ以上のプレフィックスを入力します。別のプレフィックスを追加するには、[プレフィックスを追加] を選択します。プレフィックスを削除するには、[削除] を選択します。

> **Note**
>
> アクセスポイントのスコープには、プレフィックス全体で合計 512 文字の文字数制限があります。残りの文字数は、[プレフィックスを追加] の下で確認できます。

b. [アクセス許可] で、アクセスポイントが許可する 1 つ以上の API オペレーションを選択します。データオペレーションを削除するには、データオペレーション名の横にある [X] を選択します。

10. アクセスポイントにスコープを適用せず、ディレクトリバケット内のすべてのプレフィックスとアクセスポイントを介したすべての API オペレーションへのアクセスを許可するには、[アクセスポイントの範囲] で、[バケット全体へのアクセスを適用] を選択します。
11. [ディレクトリバケットのアクセスポイントを作成] を選択します。アクセスポイント名とそのその他の情報が、[ディレクトリバケットのアクセスポイント] リストに表示されます。

AWS CLI を使用する場合

次のコマンド例では、アカウント *111122223333* でバケット *amzn-s3-demo-bucket--zone-id--x-s3* のアクセスポイントを *example-ap* という名前で作成します。

```
aws s3control create-access-point --name example-ap--zoneID--xa-s3 --account-
id 111122223333 --bucket amzn-s3-demo-bucket--zone-id--x-s3
```

VPC 経由でアクセスポイントへのアクセスを制限するには、--vpc パラメータと VPC ID を含めます。

```
aws s3control create-access-point --name example-ap--zoneID--xa-s3 --account-
id 111122223333 --bucket amzn-s3-demo-bucket--zone-id--x-s3 --vpc vpc-id
```

クロスアカウントバケットのアクセスポイントを作成するときは、--bucket-account-id パラメータを含めます。次のコマンド例では、AWS アカウント *444455556666* が所有するバケット *amzn-s3-demo-bucket--zone-id--x-s3* のアクセスポイントを AWS アカウント *111122223333* に作成します。

```
aws s3control create-access-point --name example-ap--zoneID--xa-s3 --account-
id 111122223333 --bucket amzn-s3-demo-bucket--zone-id--x-s3 --bucket-account-
id 444455556666
```

詳細および例については、「AWS CLI コマンドリファレンス」の「create-access-point」を参照してください。

REST API の使用

次のコマンド例では、アカウント *111122223333* でバケット *amzn-s3-demo-bucket--zone-id--x-s3* のアクセスポイントを *example-ap* という名前で作成し、VPC *vpc-id* (オプション) を介してアクセスを制限します。

```
PUT /v20180820/accesspoint/example-ap--zoneID--xa-s3 HTTP/1.1
Host: s3express-control.region.amazonaws.com
x-amz-account-id: 111122223333
<?xml version="1.0" encoding="UTF-8"?>
<CreateAccessPointRequest>
   <Bucket>amzn-s3-demo-bucket--zone-id--x-s3s</Bucket>
   <BucketAccountId>111122223333</BucketAccountId>
   <VpcConfiguration>
       <VpcId>vpc-id</VpcId>
   </VpcConfiguration>
</CreateAccessPointRequest>
```

レスポンス:

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<CreateAccessPointResult>
   <AccessPointArn>
       "arn:aws:s3express:region:111122223333:accesspoint/example-ap--zoneID--xa-s3"
   </AccessPointArn>
   <Alias>example-ap--zoneID--xa-s3</Alias>
</CreateAccessPointResult>
```

AWS SDK の使用

AWS SDK を使用してアクセスポイントを作成できます。詳細については、「Amazon Simple Storage Service API Reference」の「list of supported SDKs」を参照してください。

ディレクトリバケットのアクセスポイントの管理

このセクションでは、AWS Command Line Interface、Amazon S3 REST API、または AWS SDK を使用してディレクトリバケットのアクセスポイントを管理する方法について説明します。

トピック

- ディレクトリバケットのアクセスポイントを一覧表示する
- ディレクトリバケットのアクセスポイントの詳細を表示する
- アクセスポイントポリシーの表示、編集、または削除
- ディレクトリバケットのアクセスポイントの範囲を管理する
- ディレクトリバケットのアクセスポイントを削除する

ディレクトリバケットのアクセスポイントを一覧表示する

このセクションでは、AWS Management Console、AWS Command Line Interface (AWS CLI)、REST API、または AWS SDK を使用してディレクトリバケットのアクセスポイントを一覧表示する方法について説明します。

S3 コンソールの使用

AWS アカウント内のすべてのアクセスポイントを一覧表示するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ページ上部にあるナビゲーションバーで、現在表示されている AWS リージョン の名前をクリックします。次に、アクセスポイントをリスト表示するリージョンを選択します。
3. コンソールの左側のナビゲーションペインで、[ディレクトリバケットのアクセスポイント] を選択します。
4. (オプション) アクセスポイントを名前で検索します。選択した AWS リージョンのアクセスポイントのみがここに表示されます。
5. 管理するアクセスポイントの名前を選択します。

AWS CLI を使用する場合

次の `list-access-points-for-directory-buckets` コマンド例は、ディレクトリバケットに関連付けられた、AWS アカウントが所有するアクセスポイントを AWS CLI で一覧表示する方法を示しています。

次のコマンドは、バケット *amzn-s3-demo-bucket--zone-id--x-s3* にアタッチされている、AWS アカウント *111122223333* のアクセスポイントを一覧表示します。

```
aws s3control list-access-points-for-directory-buckets --account-id 111122223333 --
directory-bucket amzn-s3-demo-bucket--zone-id--x-s3
```

詳細と例については、「AWS CLI コマンドリファレンス」の「list-access-points-for-directory-buckets」を参照してください。

REST API の使用

次の例は、REST API を使用してアクセスポイントを一覧表示する方法を示しています。

```
GET /v20180820/directoryaccesspoint?directoryBucket=amzn-s3-demo-bucket--zone-id--x-s3
&maxResults=maxResults HTTP/1.1
Host: s3express-control.region.amazonaws.com
x-amz-account-id: 111122223333
```

Example **`ListAccessPointsForDirectoryBuckets`** レスポンスの

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<ListDirectoryAccessPointsResult>
    <AccessPointList>
        <AccessPoint>
            <AccessPointArn>arn:aws:s3express:region:111122223333:accesspoint/example-
access-point--zoneID--xa-s3</AccessPointArn>
            <Alias>example-access-point--zoneID--xa-s3</Alias>
            <Bucket>amzn-s3-demo-bucket--zone-id--x-s3</Bucket>
            <BucketAccountId>111122223333</BucketAccountId>
            <Name>example-access-point--zoneID--xa-s3</Name>
            <NetworkOrigin>VPC</NetworkOrigin>
```

```
            <VpcConfiguration>
                <VpcId>VPC-1</VpcId>
            </VpcConfiguration>
        </AccessPoint>
    </AccessPointList>
</ListDirectoryAccessPointsResult>
```

AWS SDK の使用

AWS SDK を使用してアクセスポイントを一覧表示できます。詳細については、「Amazon Simple Storage Service API Reference」の「list of supported SDKs」を参照してください。

ディレクトリバケットのアクセスポイントの詳細を表示する

このセクションでは、AWS Management Console、AWS CLI、AWS SDK または REST API を使用してアクセスポイントの詳細を表示する方法について説明します。

S3 コンソールの使用

ディレクトリバケットのアクセスポイントの詳細を表示して、アクセスポイントと関連するディレクトリバケットに関する次の情報を確認します。

- プロパティ:
  - ディレクトリバケット名
  - ディレクトリバケット所有者アカウント ID
  - AWS リージョン
  - ディレクトリバケットのロケーションタイプ
  - ディレクトリバケットのロケーションタイプ名
  - アクセスポイントの作成日
  - ネットワークオリジン
  - VPC ID
  - S3 URI
  - アクセスポイント ARN
  - アクセスポイントエイリアス
- 許可:
  - IAM 外部アクセスアナライザーの検出結果

- アクセスポイントのスコープ
- アクセスポイントポリシー

AWS アカウント内のアクセスポイントの詳細を表示するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ページ上部にあるナビゲーションバーで、現在表示されている AWS リージョン の名前をクリックします。次に、アクセスポイントをリスト表示するリージョンを選択します。
3. コンソールの左側のナビゲーションペインで、[ディレクトリバケットのアクセスポイント] を選択します。
4. (オプション) アクセスポイントを名前で検索します。選択した AWS リージョンのアクセスポイントのみがここに表示されます。
5. 管理するアクセスポイントの名前を選択します。
6. [プロパティ] タブまたは [アクセス許可] タブを選択します。

AWS CLI を使用する場合

次の `get-access-point` コマンド例は、AWS CLI を使用してアクセスポイントの詳細を表示する方法を示しています。

次のコマンドは、AWS アカウント *111122223333* のアクセスポイント *my-access-point--zoneID--xa-s3* の詳細を表示します。

```
aws s3control get-access-point --name my-access-point--zoneID--xa-s3 --account-
id 111122223333
```

Example **`get-access-point`** コマンドの出力例

```
{
    "Name": "example-access-point--zoneID--xa-s3",
    "Bucket": "amzn-s3-demo-bucket--zone-id--x-s3",
    "NetworkOrigin": "Internet",
    "PublicAccessBlockConfiguration": {
        "BlockPublicAcls": true,
```

```
        "IgnorePublicAcls": true,
        "BlockPublicPolicy": true,
        "RestrictPublicBuckets": true
    },
    "CreationDate": "2025-04-23T18:26:22.146000+00:00",
    "Alias": "example-access-point--zoneID--xa-s3",
    "AccessPointArn": "arn:aws:s3express:region:111122223333:accesspoint/example-
access-point--zoneID--xa-s3",
    "BucketAccountId": "296805379465"
}
```

詳細と例については、「AWS CLI コマンドリファレンス」の「get-access-point」を参照してください。

REST API の使用

REST API を使用して、アクセスポイントの詳細を表示できます。詳細については、「Amazon Simple Storage Service API リファレンス」の「GetAccessPoint」を参照してください。

AWS SDK の使用

AWS SDK を使用して、アクセスポイントの詳細を表示できます。詳細については、「Amazon Simple Storage Service API Reference」の「list of supported SDKs」を参照してください。

アクセスポイントポリシーの表示、編集、または削除

AWS Identity and Access Management (IAM) アクセスポイントポリシーを使用して、アクセスポイントにアクセスできるプリンシパルとリソースを制御できます。アクセスポイントの範囲では、アクセスポイントのプレフィックスと API アクセス許可を管理します。アクセスポイントポリシーは、AWS Command Line Interface、REST API、または AWS SDK を使用して作成、編集、削除できます。アクセスポイントの範囲の詳細については、「ディレクトリバケットのアクセスポイントの範囲を管理する」を参照してください。

> **Note**
>
> ディレクトリバケットはセッションベースの認可を使用するため、ポリシーには常に `s3express:CreateSession` アクションを含める必要があります。

S3 コンソールの使用

アクセスポイントポリシーの表示、編集、または削除

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ページ上部にあるナビゲーションバーで、現在表示されている AWS リージョン の名前をクリックします。次に、アクセスポイントをリスト表示するリージョンを選択します。
3. コンソールの左側のナビゲーションペインで、[ディレクトリバケットのアクセスポイント] を選択します。
4. (オプション) アクセスポイントを名前で検索します。選択した AWS リージョンのアクセスポイントのみがここに表示されます。
5. 管理するアクセスポイントの名前を選択します。
6. [アクセス許可] タブを選択します。
7. アクセスポイントポリシーを作成または編集するには、[アクセスポイントポリシー] で [編集] を選択します。ポリシーを編集します。[保存] を選択します。
8. アクセスポイントポリシーを削除するには、[アクセスポイントポリシー] で [削除] を選択します。[アクセスポイントポリシーを削除] ウィンドウで、**`confirm`** と入力し、[削除] を選択します。

AWS CLI を使用する場合

`get-acccess-point-policy`、`put-access-point-policy`、および `delete-access-point-policy` コマンドを使用して、アクセスポイントポリシーを表示、編集、または削除できます。詳細については、AWS CLI コマンドリファレンスの 「get-access-point-policy」、「put-access-point-policy」、または「delete-access-point-policy」を参照してください。

REST API の使用

REST API の `GetAccessPointPolicy`、`DeleteAccessPointPolicy`、`PutAccessPointPolicy` オペレーションを使用して、アクセスポイントポリシーを表示、削除、または編集できます。詳細については、「Amazon Simple Storage Service API リファレンス」の「PutAccessPointPolicy」、「GetAccessPointPolicy」、または「DeleteAccessPointPolicy」を参照してください。

AWS SDK の使用

AWS SDK を使用して、アクセスポイントポリシーを表示、削除、または編集できます。詳細については、「Amazon Simple Storage Service API Reference」の「GetAccessControlPolicy」、「DeleteAccessControlPolicy」、および「PutAccessControlPolicy」でサポートされている SDK のリストを参照してください。

ディレクトリバケットのアクセスポイントの範囲を管理する

このセクションでは、AWS Command Line Interface、REST API、または AWS SDK を使用してディレクトリバケットのアクセスポイントの範囲を表示および変更する方法について説明します。アクセスポイントスコープを使用して、特定のプレフィックスまたは API オペレーションへのアクセスを制限できます。

トピック

- ディレクトリバケットのアクセスポイントの範囲を表示する
- ディレクトリバケットのアクセスポイントの範囲を変更する
- ディレクトリバケットのアクセスポイントの範囲を削除する

ディレクトリバケットのアクセスポイントの範囲を表示する

AWS Management Console、AWS Command Line Interface、REST API、または AWS SDK を使用して、ディレクトリバケットのアクセスポイントの範囲を表示できます。

S3 コンソールの使用

AWS CLI を使用する場合

次の `get-access-point-scope` コマンド例は、AWS CLI を使用してアクセスポイントの範囲を表示する方法を示しています。

次のコマンドは、AWS アカウント *111122223333* のアクセスポイント *my-access-point*--*zoneID*--xa-s3 の範囲を表示します。

```
aws s3control get-access-point-scope --name my-access-point--zoneID--xa-s3 --account-id 111122223333
```

詳細と例については、「AWS CLI コマンドリファレンス」の「get-access-point-scope」を参照してください。

Example **get-access-point-scope** の結果

```
{
    "Scope": {
        "Permissions": [
            "ListBucket",
            "PutObject"
        ]
  "Prefixes": [
            "Prefix": "MyPrefix1*",
            "Prefix": "MyObjectName.csv"
        ]
    }
}
```

REST API の使用

次の GetAccessPointScope リクエスト例は、REST API を使用してアクセスポイントの範囲を表示する方法を示しています。

次のリクエストは、AWS アカウント *111122223333* のアクセスポイント *my-access-point*--*region*-*zoneID*--xa-s3 の範囲を表示します。

```
GET /v20180820/accesspoint/my-access-point--zoneID--xa-s3/scope HTTP/1.1
Host: s3express-control.region.amazonaws.com
x-amz-account-id: 111122223333
```

Example **GetAccessPointScope** の結果

```
      HTTP/1.1 200
      <?xml version="1.0" encoding="UTF-8"?>
      <GetAccessPointScopeResult>
          <Scope>
              <Prefixes>
                  <Prefix>MyPrefix1*</Prefix>
                  <Prefix>MyObjectName.csv</Prefix>
              </Prefixes>
              <Permissions>
```

```
                <Permission>ListBucket</Permission>
                <Permission>PutObject</Permission>
            </Permissions>
            <Scope>
    </GetAccessPointScopeResult>
```

AWS SDK の使用

AWS SDK を使用して、アクセスポイントの範囲を表示できます。詳細については、「Amazon Simple Storage Service API Reference」の「list of supported SDKs」を参照してください。

ディレクトリバケットのアクセスポイントの範囲を変更する

AWS Command Line Interface、REST API、または AWS SDK を使用して、ディレクトリバケットのアクセスポイントの範囲を変更できます。アクセスポイントの範囲は、特定のプレフィックス、API オペレーション、またはその両方の組み合わせへのアクセスを制限するために使用されます。

アクセス許可として、以下の API オペレーションを 1 つ以上含めることができます。

- `PutObject`
- `GetObject`
- `DeleteObject`
- `ListBucket` (`ListObjectsV2` では必須)
- `GetObjectAttributes`
- `AbortMultipartUploads`
- `ListBucketMultipartUploads`
- `ListMultipartUploadParts`

> **Note**
>
> - 任意の量のプレフィックスを指定できますが、すべてのプレフィックスの文字の合計長は 256 バイト未満である必要があります。
> - アクセスポイントのスコープを変更するときは、既存のスコープを置き換えます。

AWS CLI の使用

次の put-access-point-scope コマンド例は、AWS CLI を使用してアクセスポイントの範囲を変更する方法を示しています。

次のコマンドは、AWS アカウント *111122223333* の *my-access-point--zoneID*--xa-s3 のアクセスポイント範囲を変更します。

> **Note**
>
> アスタリスク (*) を使用して、プレフィックスにワイルドカードを使用できます。アスタリスク文字をリテラルとして使用する場合は、エスケープする前にバックスラッシュ (\) を追加します。
> また、すべてのプレフィックスには暗黙的な「*」末尾があります。つまり、プレフィックスを持つすべてのパスが含まれます。

```
aws s3control put-access-point-scope --name my-access-point--zoneID--xa-s3 --account-id 111122223333 --scope Prefixes=string,Permissions=string
```

詳細と例については、「AWS CLI コマンドリファレンス」の「put-access-point-scope」を参照してください。

REST API の使用

次の PutAccessPointScope リクエスト例は、REST API を使用してアクセスポイントの範囲を変更する方法を示しています。

次のリクエストは、AWS アカウント *111122223333* の *my-access-point--zoneID*--xa-s3 のアクセスポイント範囲を変更します。

> **Note**
>
> アスタリスク (*) を使用して、プレフィックスにワイルドカードを使用できます。アスタリスク文字をリテラルとして使用する場合は、エスケープする前にバックスラッシュ (\) を追加します。
> また、すべてのプレフィックスには暗黙的な「*」末尾があります。つまり、プレフィックスを持つすべてのパスが含まれます。

```
PUT /v20180820/accesspoint/my-access-point--zoneID--xa-s3/scope HTTP/1.1
Host: s3express-control.region.amazonaws.com
x-amz-account-id: 111122223333
<?xml version="1.0" encoding="UTF-8"?>
<PutAccessPointScopeRequest>
        <Scope>
            <Prefixes>
                <Prefix>Jane/*</Prefix>
            </Prefixes>
            <Permissions>
                <Permission>PutObject</Permission>
                <Permission>GetObject</Permission>
            </Permissions>
            <Scope>
    </PutAccessPointScopeRequest>
```

AWS SDK の使用

AWS CLI、AWS SDK、または REST API を使用して、アクセスポイントの範囲を変更できます。詳細については、「Amazon Simple Storage Service API Reference」の「list of supported SDKs」を参照してください。

ディレクトリバケットのアクセスポイントの範囲を削除する

AWS Command Line Interface、REST API、または AWS SDK を使用して、ディレクトリバケットのアクセスポイントの範囲を削除できます。

> **Note**
>
> アクセスポイントのスコープを削除すると、すべてのプレフィックスとアクセス許可が削除されます。

AWS CLI を使用する場合

次の `delete-access-point-scope` コマンド例は、AWS CLI を使用してアクセスポイントの範囲を削除する方法を示しています。

次のコマンドは、AWS アカウント *111122223333* のアクセスポイント *my-access-point--zoneID*--xa-s3 の範囲を削除します。

```
aws s3control delete-access-point-scope --name my-access-point--region-zoneID--xa-s3 --
account-id 111122223333
```

詳細と例については、「AWS CLI コマンドリファレンス」の「delete-access-point-scope」を参照してください。

REST API の使用

次のリクエストは、AWS アカウント *111122223333* のアクセスポイント *my-access-point--zoneID*--xa-s3 の範囲を削除します。

```
DELETE /v20180820/accesspoint/my-access-point--zoneID--xa-s3/scope HTTP/1.1
Host: s3express-control.region.amazonaws.com
x-amz-account-id: 111122223333
```

AWS SDK の使用

AWS SDK を使用して、アクセスポイントの範囲を削除できます。詳細については、「Amazon Simple Storage Service API Reference」の「list of supported SDKs」を参照してください。

ディレクトリバケットのアクセスポイントを削除する

このセクションでは、AWS Management Console、AWS Command Line Interface、REST API、または AWS SDK を使用してアクセスポイントを削除する方法について説明します。

> **Note**
>
> アクセスポイントにアタッチされたディレクトリバケットを削除する前に、アクセスポイントを削除する必要があります。

S3 コンソールの使用

AWS アカウント のディレクトリバケットのアクセスポイントを削除するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ページ上部にあるナビゲーションバーで、現在表示されている AWS リージョン の名前をクリックします。次に、アクセスポイントをリスト表示するリージョンを選択します。

3. コンソールの左側のナビゲーションペインで、[ディレクトリバケットのアクセスポイント] を選択します。
4. (オプション) アクセスポイントを名前で検索します。選択した AWS リージョンのアクセスポイントのみがここに表示されます。
5. 削除するアクセスポイントの名前を選択します。
6. [削除] を選択します。
7. 確認のため、**confirm** と入力し、[削除] を選択します。

AWS CLI を使用する場合

次の `delete-access-point` コマンド例は、AWS CLI を使用してアクセスポイントを削除する方法を示しています。

次のコマンドは、AWS アカウント *111122223333* のアクセスポイント *my-access-point--zoneID*--xa-s3 を削除します。

```
aws s3control delete-access-point --name my-access-point--zoneID--xa-s3 --account-
id 111122223333
```

詳細と例については、「AWS CLI コマンドリファレンス」の「delete-access-point」を参照してください。

REST API の使用

REST API を使用してアクセスポイントを削除できます。詳細については、「Amazon Simple Storage Service API リファレンス」の「DeleteAccessPoint」を参照してください。

AWS SDK の使用

AWS SDK を使用してアクセスポイントを削除できます。詳細については、「Amazon Simple Storage Service API Reference」の「list of supported SDKs」を参照してください。

ディレクトリバケットの AWS CloudTrail を使用したログ記録

Amazon S3 は、AWS CloudTrail と統合されています。CloudTrail は、ユーザー、ロール、または AWS サービスによって実行されたアクションのレコードを提供するサービスで、Amazon S3 へのすべての API コールをイベントとしてキャプチャします。CloudTrail で収集された情報を使用して、Amazon S3 に対するリクエスト、リクエスト元の IP アドレス、リクエストの作成日時、その

他の詳細を確認できます。サポートされているイベントアクティビティが Amazon S3 で発生すると、そのアクティビティは CloudTrail イベントに記録されます。AWS CloudTrail 証跡を使用して、ディレクトリバケットの管理イベントとデータイベントを記録できます。詳細については、「AWS CloudTrail ユーザーガイド」の「Amazon S3 CloudTrail イベント」および「AWS CloudTrail とは」を参照してください。

ディレクトリバケットの CloudTrail 管理イベント

デフォルトでは、CloudTrail はディレクトリバケットのバケットレベルのアクションを管理イベントとして記録します。ディレクトリバケットの CloudTrail 管理イベントの `eventsource` は `s3express.amazonaws.com` です。AWS アカウントのセットアップ時には、CloudTrail 管理イベントはデフォルトで有効になっています。次のリージョンエンドポイント API オペレーション (バケットレベル、またはコントロールプレーンの API オペレーション) が CloudTrail に記録されます。

- `CreateBucket`
- `DeleteBucket`
- `DeleteBucketPolicy`
- `PutBucketPolicy`
- `GetBucketPolicy`
- `ListDirectoryBuckets`
- `ListMultipartUploads`
- `GetBucketEncryption`
- `PutBucketEncryption`
- `DeleteBucketEncryption`

> **Note**
>
> `ListMultipartUploads` は、ゾーンエンドポイント API オペレーションです。ただし、この API オペレーションは CloudTrail に管理イベントとして記録されます。詳細については、「Amazon Simple Storage Service API リファレンス」の「`ListMultipartUploads`」を参照してください。

CloudTrail 管理イベントの詳細については、「AWSCloudTrail ユーザーガイド」の「管理イベントのログ記録」を参照してください。

ダイレクトバケットの CloudTrail データイベント

データイベントでは、リソース上またはリソース内で実行されるリソースオペレーション (Amazon S3 オブジェクトの読み取りまたは書き込みなど) についての情報が得られます。これらのイベントは、データプレーンオペレーションとも呼ばれます。データイベントは、多くの場合、高ボリュームのアクティビティです。デフォルトでは、CloudTrail 証跡はデータイベントを記録しませんが、汎用バケットとディレクトリバケットに保存されているオブジェクトのデータイベントを口グに記録するよう証跡を設定できます。詳細については、「コンソールを使用してバケット内のオブジェクトの口グ記録を有効にする」を参照してください。

CloudTrail で証跡のデータイベントを口グに記録する場合、アドバンストイベントセレクタまたはベーシックイベントセレクタのどちらを使用するかを選択できます。ディレクトリバケットに保存されているオブジェクトのデータイベントを口グに記録するには、高度なイベントセレクタを使用する必要があります。高度なリソースセレクタを設定する場合は、リソースタイプとして `AWS::S3Express::Object` を選択または指定します。

次のゾーンエンドポイント API オペレーション (オブジェクトレベル、またはデータプレーンの API オペレーション) が CloudTrail に記録されます。

- `AbortMultipartUpload`
- `CompleteMultipartUpload`
- `CreateSession`
- `CopyObject`
- `CreateMultipartUpload`
- `DeleteObject`
- `DeleteObjects`
- `GetObject`
- `GetObjectAttributes`
- `HeadBucket`
- `HeadObject`
- `ListObjectsV2`
- `ListParts`
- `PutObject`
- `UploadPart`
- `UploadPartCopy`

CloudTrail データイベントの詳細については、「AWS CloudTrail ユーザーガイド」の「データイベントのログ記録」を参照してください。

ディレクトリバケットの CloudTrail イベントの詳細については、以下のトピックを参照してください。

トピック

- ディレクトリバケットの CloudTrail ログファイルの例

ディレクトリバケットの CloudTrail ログファイルの例

CloudTrail ログファイルには、リクエストされた API オペレーション、オペレーションの日時、リクエストパラメーターなどに関する情報が含まれます。このトピックでは、ディレクトリバケットの CloudTrail データイベントと管理イベントの例を示します。

トピック

- ディレクトリバケットの CloudTrail データイベントログファイルの例

ディレクトリバケットの CloudTrail データイベントログファイルの例

以下は、CreateSession を示す CloudTrail ログファイルの例です。

```
    {
        "eventVersion": "1.09",
        "userIdentity": {
          "type": "AssumedRole",
          "principalId": "AROAIDPPEZS35WEXAMPLE:AssumedRoleSessionName",
          "arn": "arn:aws:sts::111122223333assumed-role/RoleToBeAssumed/MySessionName",
          "accountId": "111122223333",
          "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
          "sessionContext": {
            "sessionIssuer": {
              "type": "Role",
              "principalId": "AROAIDPPEZS35WEXAMPLE",
              "arn": "arn:aws:iam::111122223333:role/RoleToBeAssumed",
              "accountId": "111122223333",
              "userName":"RoleToBeAssumed
            },

            "attributes": {
```

```
              "creationDate": "2024-07-02T00:21:16Z",
            "mfaAuthenticated": "false"
            }
          }
        },
        "eventTime": "2024-07-02T00:22:11Z",
        "eventSource": "s3express.amazonaws.com",
        "eventName": "CreateSession",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "72.21.198.68",
        "userAgent": "aws-sdk-java/2.20.160-SNAPSHOT
 Linux/5.10.216-225.855.amzn2.x86_64 OpenJDK_64-Bit_Server_VM/11.0.23+9-LTS
 Java/11.0.23 vendor/Amazon.com_Inc. md/internal exec-env/AWS_Lambda_java11 io/sync
 http/Apache cfg/retry-mode/standard",
        "requestParameters": {
          "bucketName": "bucket-base-name--usw2-az1--x-s3".
            "host": "bucket-base-name--usw2-az1--x-s3.s3express-usw2-az1.us-
west-2.amazonaws.com",
            "x-amz-create-session-mode": "ReadWrite"
        },
        "responseElements": {
            "credentials": {
                "accessKeyId": "AKIAI44QH8DHBEXAMPLE"
                "expiration": ""Mar 20, 2024, 11:16:09 PM",
                "sessionToken": "<session token string>"
           },
        },
        "additionalEventData": {
            "SignatureVersion": "SigV4",
            "cipherSuite": "TLS_AES_128_GCM_SHA256",
            "bytesTransferredIn": 0,
            "AuthenticationMethod": "AuthHeader",
            "xAmzId2": "q6xhNJYmhg",
            "bytesTransferredOut": 1815,
            "availabilityZone": "usw2-az1"
          },
          "requestID": "28d2faaf-3319-4649-998d-EXAMPLE72818",
          "eventID": "694d604a-d190-4470-8dd1-EXAMPLEe20c1",
          "readOnly": true,
          "resources": [
            {
              "type": "AWS::S3Express::Object",
              "ARNPrefix": "arn:aws:s3express:us-west-2:111122223333:bucket-base-name--
usw2-az1--x-s3"
```

```
            },
            {
              "accountId": "111122223333"
              "type": "AWS::S3Express::DirectoryBucket",
              "ARN": "arn:aws:s3express:us-west-2:111122223333:bucket-base-name--usw2-
az1--x-s3"
             }
           ],
           "eventType": "AwsApiCall",
           "managementEvent": false,
           "recipientAccountId": "111122223333",
           "eventCategory": "Data",
           "tlsDetails": {
             "tlsVersion": "TLSv1.3",
             "cipherSuite": "TLS_AES_128_GCM_SHA256",
             "clientProvidedHostHeader": "bucket-base-name--usw2-az1--x-s3.s3express-
usw2-az1.us-west-2.amazonaws.com"
            }
         }
```

ゾーンエンドポイント API オペレーション (オブジェクトレベルまたはデータプレーンオペレーション) を使用するには、CreateSession API オペレーションを使用して、データリクエストの低レイテンシー認可に最適化されたセッションを作成および管理します。CreateSession を使用してログ記録の量を減らすこともできます。セッション中に実行されたゾーン API オペレーションを特定するには、CreateSession ログファイルの responseElements の下にある accessKeyId を、他のゾーン API オペレーションのログファイルの accessKeyId と照合します。詳細については、「CreateSession を使用したゾーンエンドポイント API オペレーションの承認」を参照してください。

以下は、CreateSession によって認証された GetObject API オペレーションを示す CloudTrail ログファイルの例です。

```
    {
        "eventVersion": "1.09",
        "userIdentity": {
          "type": "AssumedRole",
          "principalId": "AROAIDPPEZS35WEXAMPLE:AssumedRoleSessionName",
          "arn": "arn:aws:sts::111122223333assumed-role/RoleToBeAssumed/MySessionName",
          "accountId": "111122223333",
          "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
          "sessionContext": {
            "attributes": {
```

```
              "creationDate": "2024-07-02T00:21:49Z"
            }
          }
        },
        "eventTime": "2024-07-02T00:22:01Z",
        "eventSource": "s3express.amazonaws.com",
        "eventName": "GetObject",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "72.21.198.68",
        "userAgent": "aws-sdk-java/2.25.66 Linux/5.10.216-225.855.amzn2.x86_64
 OpenJDK_64-Bit_Server_VM/17.0.11+9-LTS Java/17.0.11 vendor/Amazon.com_Inc. md/internal
 exec-env/AWS_Lambda_java17 io/sync http/Apache cfg/retry-mode/legacy",
        "requestParameters": {
          "bucketName": "bucket-base-name--usw2-az1--x-s3",
          "x-amz-checksum-mode": "ENABLED",
          "Host": "bucket-base-name--usw2-az1--x-s3.s3express-usw2-az1.us-
west-2.amazonaws.com",
          "key": "test-get-obj-with-checksum"
        },
        "responseElements": null,
        "additionalEventData": {
          "SignatureVersion": "Sigv4",
          "CipherSuite": "TLS_AES_128_GCM_SHA256",
          "bytesTransferredIn": 0,
          "AuthenticationMethod": "AuthHeader",
          "x-amz-id-2": "oOy6w8K7LFsyFN",
          "bytesTransferredOut": 9,
          "availabilityZone": "usw2-az1",
          "sessionModeApplied": "ReadWrite"
         },
          "requestID": "28d2faaf-3319-4649-998d-EXAMPLE72818",
          "eventID": "694d604a-d190-4470-8dd1-EXAMPLEe20c1",
          "readOnly": true,
          "resources": [
            {
              "type": "AWS::S3Express::Object",
              "ARNPrefix": "arn:aws:s3express:us-west-2:111122223333:bucket-base-name--
usw2-az1--x-s3"
            },
            {
              "accountId": "111122223333",
              "type": "AWS::S3Express::DirectoryBucket",
              "ARN": "arn:aws:s3express:us-west-2:111122223333:bucket-base-name--usw2-
az1--x-s3"
```

```
            }
          ],
          "eventType": "AwsApiCall",
          "managementEvent": false,
          "recipientAccountId": "111122223333",
          "eventCategory": "Data",
          "tlsDetails": {
            "tlsVersion": "TLSv1.3",
            "cipherSuite": "TLS_AES_128_GCM_SHA256",
            "clientProvidedHostHeader": "bucket-base-name--usw2-az1--x-s3.s3express-
usw2-az1.us-west-2.amazonaws.com"
          }
        }
```

上記の GetObject ログファイル例にある accessKeyId (AKIAI44QH8DHBEXAMPLE) は、CreateSession ログファイル例の responseElements の下にある accessKeyId と一致しています。accessKeyId の一致は、GetObject オペレーションが実行されたセッションを示します。

次の例は、S3 ライフサイクルで呼び出したディレクトリバケットに対する DeleteObjects アクションを示す CloudTrail ログエントリです。詳細については、「Working with S3 Lifecycle for directory buckets」を参照してください。

```
eventVersion:"1.09",
  userIdentity:{

    type:"AWSService",
    invokedBy:"lifecycle.s3.amazonaws.com"
  },
  eventTime:"2024-09-11T00:55:54Z",
  eventSource:"s3express.amazonaws.com",
  eventName:"DeleteObjects",
  awsRegion:"us-east-2",
  sourceIPAddress:"lifecycle.s3.amazonaws.com",
  userAgent:"gamma.lifecycle.s3.amazonaws.com",
  requestParameters:{

    bucketName:"amzn-s3-demo-bucket--use2-az2--x-s3",
    'x-amz-expected-bucket-owner':"637423581905",
    Host:"amzn-s3-demo-bucket--use2-az2--x-s3.gamma.use2-az2.express.s3.aws.dev",
    delete:"",
    'x-amz-sdk-checksum-algorithm':"CRC32C"
  },
```

```
  responseElements:null,
  additionalEventData:{

    SignatureVersion:"Sigv4",
    CipherSuite:"TLS_AES_128_GCM_SHA256",
    bytesTransferredIn:41903,
    AuthenticationMethod:"AuthHeader",
    'x-amz-id-2':"9H5YWZY0",
    bytesTransferredOut:35316,
    availabilityZone:"use2-az2",
    sessionModeApplied:"ReadWrite"
  },
  requestID:"011eeadd04000191",
  eventID:"d3d8b116-219d-4ee6-a072-5f9950733c74",
  readOnly:false,
  resources:[

    {

      type:"AWS::S3Express::Object",
      ARNPrefix:"arn:aws:s3express:us-east-2:637423581905:bucket/amzn-s3-demo-bucket--
use2-az2--x-s3/"
    },
    {

      accountId:"637423581905",
      type:"AWS::S3Express::DirectoryBucket",
      ARN:"arn:aws:s3express:us-east-2:637423581905:bucket/amzn-s3-demo-bucket--use2-
az2--x-s3"
    }
  ],
  eventType:"AwsApiCall",
  managementEvent:false,
  recipientAccountId:"637423581905",
  sharedEventID:"59f877ac-1dd9-415d-b315-9bb8133289ce",
  eventCategory:"Data"
}
```

次の例は、S3 ライフサイクルで呼び出した CreateSession アクションに対する Access Denied リクエストを示す CloudTrail ログエントリです。詳細については、「CreateSession」を参照してください。

```
{
```

```
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "gamma.lifecycle.s3.amazonaws.com"
    },
    "eventTime": "2024-09-11T18:13:08Z",
    "eventSource": "s3express.amazonaws.com",
    "eventName": "CreateSession",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "gamma.lifecycle.s3.amazonaws.com",
    "userAgent": "gamma.lifecycle.s3.amazonaws.com",
    "errorCode": "AccessDenied",
    "errorMessage": "Access Denied",
    "requestParameters": {
        "bucketName": "amzn-s3-demo-bucket--use2-az2--x-s3",
        "Host": "amzn-s3-demo-bucket--use2-az2--x-s3.gamma.use2-
az2.express.s3.aws.dev",
        "x-amz-create-session-mode": "ReadWrite",
        "x-amz-server-side-encryption": "AES256"
    },
    "responseElements": null,
    "additionalEventData": {
        "SignatureVersion": "Sigv4",
        "CipherSuite": "TLS_AES_128_GCM_SHA256",
        "bytesTransferredIn": 0,
        "AuthenticationMethod": "AuthHeader",
        "x-amz-id-2": "zuDDC1VNbC4LoNwUIc5",
        "bytesTransferredOut": 210,
        "availabilityZone": "use2-az2"
    },
    "requestID": "010932f174000191e24a0",
    "eventID": "dce7cc46-4cd3-46c0-9a47-d1b8b70e301c",
    "readOnly": true,
    "resources": [{
            "type": "AWS::S3Express::Object",
            "ARNPrefix": "arn:aws:s3express:us-east-2:637423581905:bucket/amzn-s3-demo-
bucket--use2-az2--x-s3/"
        },
        {
            "accountId": "637423581905",
            "type": "AWS::S3Express::DirectoryBucket",
            "ARN": "arn:aws:s3express:us-east-2:637423581905:bucket/amzn-s3-demo-
bucket--use2-az2--x-s3"
        }
```

```
    ],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "637423581905",
    "sharedEventID": "da96b5bd-6066-4a8d-ad8d-f7f427ca7d58",
    "eventCategory": "Data"
}
```

ディレクトリバケットのパフォーマンスの最適化

ディレクトリバケットを使用して最高のパフォーマンスを得るには、以下のガイドラインに従うことをお勧めします。

セッションベースの認証を使用する

ディレクトリバケットは、ディレクトリバケットへのリクエストを認証および認可するための新しいセッションベースの認可メカニズムをサポートしています。セッションベースの認証では、AWS SDK は自動的に CreateSession API オペレーションを使用して、ディレクトリバケットへのデータリクエストの低レイテンシー認可に使用できる一時セッショントークンを作成します。

AWS SDK は CreateSession API オペレーションを使用して一時的な認証情報をリクエストし、5 分ごとにユーザーに代わって自動的にトークンを作成して更新します。ディレクトリバケットのパフォーマンスの利点を活用するには、AWS SDK を使用して CreateSession API リクエストを開始および管理することをお勧めします。このセッションベースのモデルの詳細については、「CreateSession を使用したゾーンエンドポイント API オペレーションの承認」を参照してください。

S3 の追加のチェックサムのベストプラクティス

ディレクトリバケットには、アップロードやダウンロード中のデータ検証に使用するチェックサムアルゴリズムを選択するオプションがあります。CRC32、CRC32C、SHA-1、SHA-256 などのセキュアハッシュアルゴリズム (SHA) や巡回冗長検査 (CRC) データ整合性チェックアルゴリズムのいずれかを選択できます。MD5 ベースのチェックサムは S3 Express One Zone ストレージクラスではサポートされていません。

CRC32 は、ディレクトリバケットとの間でデータをやり取りする際に AWS SDK で使用するデフォルトのチェックサムです。ディレクトリバケットで最高のパフォーマンスを得るには、CRC32 と CRC32C を使用することをお勧めします。

最新バージョンの AWS SDK と一般的なランタイムライブラリを使用する

一部の AWS SDK では、S3 クライアントのパフォーマンスをさらに向上させる AWS Common Runtime (CRT) ライブラリも提供しています。このような SDK には AWS SDK for Java 2.x、AWS SDK for C++、AWS SDK for Python (Boto3) があります。CRT ベースの S3 クライアントは、ディレクトリバケットとの間でオブジェクトをやり取りする際に、マルチパートアップロード API オペレーションとバイト範囲フェッチを自動的に使用して水平スケーリング接続を自動化し、パフォーマンスと信頼性を向上させます。

ディレクトリバケットで最高レベルのパフォーマンスを実現するには、CRT ライブラリを含む最新バージョンの AWS SDK を使用するか、AWS Command Line Interface (AWS CLI) を使用することをお勧めします。

ディレクトリバケットを使用した開発

ディレクトリバケットを作成すると、レイテンシーが非常に低い読み取りと書き込みを直ちに開始できます。仮想プライベートクラウド (VPC) を介したエンドポイント接続を使用して、ディレクトリバケットと通信したり、ゾーンとリージョン API オペレーションを使用してオブジェクトとディレクトリバケットを管理したりできます。ディレクトリバケットは、AWS SDK、Amazon S3 コンソール、AWS コマンドラインインターフェイス (AWS CLI)、Amazon S3 REST API で使用できます。

トピック

- ディレクトリバケットのリージョンエンドポイントとゾーンエンドポイント
- S3 コンソール、AWS CLI、AWS SDK を使用したディレクトリバケットの操作
- ディレクトリバケット API オペレーション

ディレクトリバケットのリージョンエンドポイントとゾーンエンドポイント

仮想プライベートクラウド (VPC) からディレクトリバケットのリージョンエンドポイントとゾーンエンドポイントにアクセスするには、ゲートウェイ VPC エンドポイントを使用できます。ゲートウェイエンドポイントを作成したら、VPC からバケットへのトラフィックのターゲットとしてルートテーブルに追加できます。ゲートウェイエンドポイントは追加料金なしで使用できます。ゲートウェイ VPC エンドポイントの設定方法の詳細については、「ディレクトリバケットのネットワーク」を参照してください。

バケットレベル (コントロールプレーン) API オペレーションは、リージョンエンドポイントを通じて利用可能であり、リージョンエンドポイント API オペレーションと呼ばれます。リージョンエンドポイント API オペレーションの例には、`CreateBucket`、`DeleteBucket` があります。

オブジェクトをアップロードおよび管理するには、ゾーン (オブジェクトレベルまたはデータプレーン) エンドポイント API オペレーションを使用します。ゾーンエンドポイント API オペレーションは、ゾーンエンドポイントを通じて実行できます。ゾーン API オペレーションの例には、`PutObject`、`CopyObject` があります。

アベイラビリティーゾーンのディレクトリバケットのリージョンエンドポイントとゾーンエンドポイントの詳細については、「アベイラビリティーゾーン内のディレクトリバケット用のリージョンエンドポイントとゾーンエンドポイント」を参照してください。

Local Zones のディレクトリバケットのリージョンエンドポイントとゾーンエンドポイントの詳細については、「Local Zones のディレクトリバケットの概念」を参照してください。

S3 コンソール、AWS CLI、AWS SDK を使用したディレクトリバケットの操作

AWS SDK、Amazon S3 コンソール、AWS Command Line Interface (AWS CLI)、Amazon S3 REST API を使用して S3 Express One Zone ストレージクラスとディレクトリバケットを操作できます。

S3 コンソール

S3 コンソールを使って使用を開始するには、次の手順に従います。

- アベイラビリティーゾーンでのディレクトリバケットの作成
- ディレクトリバケットを空にする
- ディレクトリバケットの削除

完全なチュートリアルについては、「チュートリアル: S3 Express One Zone の使用を開始する」を参照してください。

AWS SDK

S3 Express One Zone は次の AWS SDK をサポートしています。

- AWS SDK for C++

- AWS SDK for Go v2
- AWS SDK for Java 2.x
- AWS SDK for JavaScript v3
- AWS SDK for .NET
- AWS SDK for PHP
- AWS SDK for Python (Boto3)
- AWS SDK for Ruby
- AWS SDK for Kotlin
- AWS SDK for Rust

S3 Express One Zone を使用する場合は、最新バージョンの AWS SDK を使用することをお勧めします。S3 Express One Zone でサポートされている AWS SDK は、ユーザーに代わってセッションの確立、更新、終了を処理します。つまり、AWS SDK をダウンロードしてインストールし、必要な IAM アクセス許可を設定すると、直ちに API オペレーションを使用開始できます。詳細については、「IAM を使用したリージョンエンドポイント API オペレーションの承認」を参照してください。

AWS SDK のダウンロードやインストールなどの詳細については、「AWS での構築ツール」を参照してください。

AWS SDK の例については、次を参照してください。

- アベイラビリティーゾーンでのディレクトリバケットの作成
- ディレクトリバケットを空にする
- ディレクトリバケットの削除

AWS Command Line Interface (AWS CLI)

AWS Command Line Interface (AWS CLI) を使用してディレクトリ バケットを作成し、S3 Express One Zone でサポートされているリージョンとゾーンのエンドポイント API オペレーションを使用できます。

AWS CLI の使用を開始するには、「AWS CLI コマンドレファレンス」の「AWS CLI の使用を開始する」を参照してください。

> **Note**
>
> ディレクトリバケットで高レベルの aws s3 コマンドを使用するには、AWS CLI を最新バージョンに更新します。AWS CLI のインストールと設定方法の詳細については、「AWS CLIコマンドリファレンス」の「AWS CLI の最新バージョンをインストールまたは更新する」を参照してください。

AWS CLI の例については、次を参照してください。

- アベイラビリティーゾーンでのディレクトリバケットの作成
- ディレクトリバケットを空にする
- ディレクトリバケットの削除

ディレクトリバケット API オペレーション

ディレクトリバケットを管理するには、リージョン (バケットレベルまたはコントロールプレーン) エンドポイント API オペレーションを使用できます。ディレクトリバケット内のオブジェクトを管理するには、ゾーン (オブジェクトレベルまたはデータプレーン) エンドポイント API オペレーションを使用できます。詳細については、「ディレクトリバケットのネットワーク」および「エンドポイントとゲートウェイ VPC エンドポイント」を参照してください。

リージョンエンドポイント API オペレーション

ディレクトリバケット用に、以下のリージョンエンドポイント API オペレーションがサポートされています。

- CreateAccessPoint
- CreateBucket
- DeleteAccessPoint
- DeleteAccessPointPolicy
- DeleteAccessPointScope
- DeleteBucket
- DeleteBucketLifecycle
- DeleteBucketPolicy
- GetAccessPoint

- GetAccessPointPolicy
- GetAccessPointScope
- GetBucketLifecycleConfiguration
- GetBucketPolicy
- ListAccessPointsForDirectoryBuckets
- ListDirectoryBuckets
- PutAccessPointPolicy
- PutAccessPointScope
- PutBucketLifecycleConfiguration
- PutBucketPolicy

ゾーンエンドポイント API オペレーション

ディレクトリバケット用として、以下のゾーンエンドポイント API オペレーションがサポートされています。

- CreateSession
- CopyObject
- DeleteObject
- DeleteObjects
- GetObject
- GetObjectAttributes
- HeadBucket
- HeadObject
- ListObjectsV2
- PutObject
- AbortMultipartUpload
- CompleteMultiPartUpload
- CreateMultipartUpload
- ListMultipartUploads
- ListParts
- UploadPart

- UploadPartCopy
- PutBucketEncryption
- GetBucketEncryption
- DeleteBucketEncryption

Amazon S3 Tables とテーブルバケットの使用

Amazon S3 Tables は、分析ワークロード用に最適化された S3 ストレージを提供し、クエリのパフォーマンスを継続的に向上させ、テーブルのストレージコストを削減するように設計された機能を備えています。S3 テーブルは、毎日の購入トランザクション、ストリーミングセンサーデータ、広告インプレッションなどの表形式データを保存するために専用に構築されています。表形式データは、データベーステーブルのように列と行のデータを表します。

S3 Tables のデータは、新しいバケットタイプ、つまりテーブルをサブリソースとして保存するテーブルバケットに保存されます。テーブルバケットは、Apache Iceberg 形式のテーブルの保存をサポートしています。標準 SQL ステートメントを使用すると、Amazon Athena、Amazon Redshift、Apache Spark などの Iceberg をサポートするクエリエンジンを使用してテーブルをクエリできます。

トピック

- S3 Tables の機能
- 関連サービス
- チュートリアル: S3 Tables の開始方法
- テーブルバケット
- S3 Tables のメンテナンス
- テーブル名前空間
- S3 テーブルバケットのテーブル
- テーブルデータへのアクセス
- S3 Tables AWS リージョン、エンドポイント、および Service Quotas
- S3 Tables のセキュリティ
- S3 Tablesの AWS CloudTrail を使用した口グ記録

S3 Tables の機能

テーブルの専用ストレージ

S3 テーブルバケットは、テーブル用に特別に設計されています。テーブルバケットは、S3 汎用バケットのセルフマネージドテーブルと比較して、1 秒あたりのトランザクション (TPS) が高

く、クエリスループットが向上します。テーブルバケットは、他の Amazon S3 バケットタイプと同じ耐久性、可用性、スケーラビリティを提供します。

Apache Iceberg の組み込みサポート

テーブルバケット内のテーブルは Apache Iceberg 形式で保存されます。Iceberg をサポートするクエリエンジンで標準 SQL を使用してこれらのテーブルをクエリできます。Iceberg には、スキーマ進化やパーティション進化など、クエリパフォーマンスを最適化するためのさまざまな機能があります。

Iceberg を使用すると、クエリを再作成したり、データ構造を再構築したりすることなく、時間の経過とともに進化できるようにデータの整理方法を変更できます。Iceberg は、トランザクションのサポートを通じてデータの一貫性と信頼性を確保するように設計されています。問題を修正したり、タイムトラベルクエリを実行したりするのに役立つように、時間の経過とともにデータがどのように変化するかを追跡し、履歴バージョンにロールバックできます。

自動テーブル最適化

クエリ用テーブルを最適化するために、S3 は圧縮、スナップショット管理、参照されていないファイルの削除などの自動メンテナンスオペレーションを継続的に実行します。これらのオペレーションは、小さなオブジェクトを少数の大きなファイルに圧縮することで、テーブルのパフォーマンスを向上させます。また、メンテナンスオペレーションでは、未使用のオブジェクトをクリーンアップすることでストレージコストを削減できます。この自動メンテナンスにより、手動のテーブルメンテナンスの必要性が減ることで、大規模なデータレイクの運用が効率化されます。テーブルとテーブルバケットごとに、メンテナンス設定をカスタマイズできます。

アクセス管理とセキュリティ

AWS Organizations の AWS Identity and Access Management (IAM) とサービスコントロールポリシーを使用して、テーブルバケットと個々のテーブルの両方のアクセスを管理できます。S3 Tables は、Amazon S3 とは異なるサービス名前空間、つまり s3tables 名前空間を使用します。したがって、S3 Tables サービスとそのリソース専用のポリシーを設計できます。個々のテーブル、テーブル名前空間内のすべてのテーブル、またはテーブルバケット全体へのアクセスを許可するポリシーを設計できます。すべての Amazon S3 ブロックパブリックアクセス設定は、テーブルバケットに対して常に有効になっており、無効にすることはできません。

AWS 分析サービスとの統合

S3 コンソールを使用して、Amazon S3 テーブルバケットが Amazon SageMaker Lakehouse に自動的に統合されるように設定できます。この統合により、AWS 分析サービスが AWS Glue Data Catalog を通じてテーブルデータを自動的に検出してアクセスできるようになります。統合後は、Amazon Athena、Amazon Redshift、QuickSight などの分析サービスを使用して、テー

ブルを操作できます。統合の動作方法の詳細については、「AWS 分析サービスで Amazon S3 Tables を使用する」を参照してください。

関連サービス

特定の分析アプリケーションをサポートするには、S3 Tables で次の AWS のサービスを使用できます。

- Amazon Athena – Athena はインタラクティブなクエリサービスで、Amazon S3 内のデータを標準 SQL を使用して直接分析できます。また、Athena を使用すると、リソースの計画、設定、管理を必要とせずに Apache Spark を使用してデータ分析をインタラクティブに実行することもできます。Athena で Apache Spark アプリケーションを実行する場合は、処理用の Spark コードを送信して、結果を直接受け取ります。
- AWS Glue – AWS Glue は、複数のソースからのデータを検出、準備、移動、統合できるようにするサーバーレスのデータ統合サービスです。分析用の AWS Glue は、分析、機械学習 (ML)、アプリケーション開発に使用できます。AWS Glue には、ジョブの作成、実行、ビジネスワークフローの実装のための生産性向上ツールとデータ運用ツールも追加されています。
- Amazon EMR – Amazon EMR は、Apache Hadoop や Apache Spark などのビッグデータフレームワークを AWS で簡単に実行して、膨大な量のデータを処理および分析できるマネージドクラスタープラットフォームです。
- Amazon Redshift – Amazon Redshift は、クラウド内でのペタバイト規模のデータウェアハウスサービスです。Amazon Redshift Serverless を使用して、プロビジョニングされたデータウェアハウスをすべて設定しなくても、データにアクセスして分析することができます。リソースは自動的にプロビジョニングされて、データウェアハウス容量はインテリジェントにスケーリングされ、要求が厳しく、予測不可能なワークロードであっても高速なパフォーマンスを実現します。データウェアハウスがアイドル状態のときには課金されず、使用した分のみ支払います。Amazon Redshift クエリエディタ v2 またはお好みのビジネスインテリジェンス (BI) ツールで、データをロードしてクエリを直ちに開始することができます。
- QuickSight – QuickSight は、視覚化の構築、アドホック分析の実行、データからのビジネスインサイトの迅速な取得に使用できるビジネス分析サービスです。QuickSight は、QuickSight の超高速、並列、インメモリ、計算エンジン (SPICE) を使用して、AWS データソースをシームレスに検出し、高速で応答性の高いクエリパフォーマンスを提供します。
- AWS Lake Formation – Lake Formation は、データレイクのセットアップ、保護、管理のプロセスを合理化するマネージドサービスです。Lake Formation では、データソースを検出し、そのデータをカタログ化、クレンジング、変換できます。Lake Formation では、Amazon S3 上のデータレ

イクデータと AWS Glue Data Catalog の関連メタデータに対するきめ細かなアクセスコントロールを管理できます。

チュートリアル: S3 Tables の開始方法

このチュートリアルでは、テーブルバケットを作成し、リージョンのテーブルバケットを AWS 分析サービスと統合します。次に、AWS CLI を使用して、テーブルバケットに最初の名前空間とテーブルを作成します。次に、AWS Lake Formation を使用してテーブルに対するアクセス許可を付与し、Athena でテーブルのクエリを開始できるようにします。

> **Tip**
>
> 汎用バケットからテーブルバケットに表形式データを移行する場合のために、AWS Solutions Library にはガイド付きソリューションが用意されています。このソリューションは、AWS Step Functions と Amazon EMR を Apache Spark で使用して、AWS Glue Data Catalog に登録され汎用バケットに保存されている Apache Iceberg および Apache Hive テーブルをテーブルバケットに自動的に移動します。詳細については、AWS Solutions Library で Amazon S3 から S3 Tables への表形式データの移行に関するガイダンスを参照してください。

トピック

- ステップ 1: テーブルバケットを作成し、AWS 分析サービスと統合する
- ステップ 2: テーブル名前空間とテーブルを作成する
- (オプション) ステップ 3: テーブルに対する Lake Formation 許可を付与する
- ステップ 4: Athena で SQL を使用してデータをクエリする

ステップ 1: テーブルバケットを作成し、AWS 分析サービスと統合する

このステップでは、Amazon S3 コンソールを使用して最初のテーブルバケットを作成します。テーブルバケットを作成するその他の方法については、「テーブルバケットの作成」を参照してください。

> **Note**
>
> デフォルトでは、Amazon S3 コンソールはテーブルバケットを Amazon SageMaker Lakehouse と自動的に統合します。これにより、AWS 分析サービスが S3 Tables データを自動的に検出してアクセスできるようになります。AWS Command Line Interface (AWS CLI)、AWS SDK、または REST API を使用して最初のテーブルバケットをプログラムで作成する場合は、AWS 分析サービスの統合を手動で完了する必要があります。詳細については、「AWS 分析サービスで Amazon S3 Tables を使用する」を参照してください。

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ページ上部にあるナビゲーションバーで、現在表示されている AWS リージョン の名前をクリックします。次に、テーブルバケットを作成するリージョンを選択します。
3. 左側のナビゲーションペインで、[テーブルバケット] を選択します。
4. [テーブルバケットを作成] を選択します。
5. [全般設定] で、テーブルバケットの名前を入力します。

   テーブルバケット名には次の条件があります。

   - 現在のリージョンの AWS アカウント内で一意であること。
   - 3 ~ 63 文字で指定する。
   - 小文字、数字、ハイフン (-) のみで構成されていること。
   - 文字や数字で始まり、文字や数字で終わります。

   テーブルバケットを作成した後、その名前を変更することはできません。テーブルバケットを作成した AWS アカウント がその所有者になります。テーブルバケットの命名の詳細については、「テーブルバケットの命名規則」を参照してください。
6. [AWS 分析サービスとの統合] セクションで、[統合を有効にする] チェックボックスがオンになっていることを確認してください。

   コンソールを使用して最初のテーブルバケットを作成するときに [統合を有効にする] が選択されていると、Amazon S3 はテーブルバケットを AWS 分析サービスと統合しようとします。この統合により、AWS 分析サービスを使用して、現在のリージョン内のすべてのテーブルにアクセスできます。詳細については、「AWS 分析サービスで Amazon S3 Tables を使用する」を参照してください。

7. [バケットを作成] を選択します。

ステップ 2: テーブル名前空間とテーブルを作成する

このステップでは、テーブルバケットに名前空間を作成し、その名前空間の下に新しいテーブルを作成します。テーブル名前空間とテーブルはコンソールまたは AWS CLI を使用して作成できます。

> **Important**
>
> テーブルを作成するときは、テーブル名とテーブル定義にすべて小文字を使用してください。例えば、列名がすべて小文字であることを確認します。テーブル名またはテーブル定義に大文字が含まれている場合、テーブルは AWS Lake Formation または AWS Glue Data Catalog ではサポートされていません。この場合、テーブルバケットが AWS 分析サービスと統合されていても、テーブルは Amazon Athena などの AWS 分析サービスに表示されません。
>
> テーブル定義に大文字が含まれている場合、Athena で SELECT クエリを実行すると、次のエラーメッセージが表示されます。「GENERIC_INTERNAL_ERROR: Get table request failed: com.amazonaws.services.glue.model.ValidationException: Unsupported Federation Resource - Invalid table or column names.」

S3 コンソールと Amazon Athena の使用

以下の手順では、Amazon S3 コンソールを使用して Amazon Athena で名前空間とテーブルを作成します。

テーブル名前空間とテーブルを作成するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[テーブルバケット] を選択します。
3. [テーブルバケット] ページで、テーブルを作成するテーブルバケットを選択します。
4. テーブルバケットの詳細ページで、[Athena でテーブルを作成] を選択します。
5. [Athena でテーブルを作成] ダイアログボックスで、[名前空間を作成] を選択し、[名前空間名] フィールドに名前を入力します。名前空間名は 1～255 文字で、テーブルバケット内で一意であることが必要です。有効な文字は a～z、0～9、アンダースコア (_) です。名前空間名の先頭にアンダースコアを使用することはできません。

6. [名前空間の作成] を選択します。
7. [Athena でテーブルを作成] を選択します。
8. Amazon Athena コンソールが開き、Athena クエリエディタが表示されます。クエリエディタには、テーブルの作成に使用できるサンプルクエリが入力されます。クエリを変更して、テーブル名とテーブルに必要な列を指定します。
9. クエリの変更が完了したら、[実行] を選択してテーブルを作成します。

テーブルが作成されると、新しいテーブルの名前が Athena のテーブルのリストに表示されます。Amazon S3 コンソールに戻り、テーブルバケットの詳細ページの [テーブル] リストを更新すると、新しいテーブルが表示されます。

AWS CLI を使用する場合

テーブルバケットに名前空間を作成し、その名前空間の下にスキーマを定義した新しいテーブルを作成するには、次の AWS CLI コマンド例で *user input placeholder* の値を実際の値に置き換えます。

前提条件

- AmazonS3TablesFullAccess ポリシーを IAM ID にアタッチします。
- AWS CLI バージョン 2.23.10 以上をインストールします。詳細については、「AWS Command Line Interface ユーザーガイド」の「AWS CLI の最新バージョンをインストールまたは更新します。」を参照してください。

1. 次のコマンドを実行して、テーブルバケットに新しい名前空間を作成します。

```
aws s3tables create-namespace \
--table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-table-bucket \
--namespace my_namespace
```

   - 次のコマンドを実行して、名前空間が正常に作成されたことを確認します。

```
aws s3tables list-namespaces \
--table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-table-bucket
```

2. 次のコマンドを実行して、テーブルスキーマを定義した新しいテーブルを作成します。

```
aws s3tables create-table --cli-input-json file://mytabledefinition.json
```

mytabledefinition.json ファイルには、次のテーブル定義の例を使用します。

```
{
    "tableBucketARN": "arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-table-bucket",
    "namespace": "my_namespace",
    "name": "my_table",
    "format": "ICEBERG",
    "metadata": {
        "iceberg": {
            "schema": {
                "fields": [
                    {"name": "id", "type": "int","required": true},
                    {"name": "name", "type": "string"},
                    {"name": "value", "type": "int"}
                ]
            }
        }
    }
}
```

(オプション) ステップ 3: テーブルに対する Lake Formation 許可を付与する

このステップでは、新しいテーブルに対する Lake Formation 許可を他の IAM プリンシパルに付与します。これらのアクセス許可により、自分以外のプリンシパルが Athena やその他の AWS 分析サービスを使用してテーブルバケットリソースにアクセスできるようになります。詳細については、「テーブルまたはデータベースに対するアクセス許可の付与」を参照してください。テーブルにアクセスするユーザーが自分だけの場合は、このステップをスキップできます。

1. https://console.aws.amazon.com/lakeformation/ で AWS Lake Formation コンソールを開き、データレイク管理者としてサインインします。データレイク管理者の作成方法の詳細については、「データレイク管理者を作成する」を参照してください。
2. ナビゲーションペインで、[データアクセス許可]、[付与] の順に選択します。

3. [アクセス許可を付与] ページの [プリンシパル] で、[IAM ユーザーとロール] を選択し、テーブルに対するクエリの実行を許可する IAM ユーザーまたはロールを選択します。
4. [LF タグまたはカタログリソース] で、[名前付きのデータカタログリソース] を選択します。
5. アカウント内のすべてのテーブルへのアクセスを許可するか、作成したテーブルバケット内のリソースのみへのアクセスを許可するかに応じて、次のいずれかを実行します。
   - [カタログ] では、テーブルバケットを統合したときに作成したアカウントレベルのカタログを選択します。例えば、*111122223333*:s3tablescatalog。
   - [カタログ] で、テーブルバケットのサブカタログを選択します。例えば、*111122223333*:s3tablescatalog/*amzn-s3-demo-table-bucket*。
6. (オプション) テーブルバケットのサブカタログを選択した場合は、次のいずれかまたは両方を実行します。
   - [データベース] で、作成したテーブルバケットの名前空間を選択します。
   - [テーブル] で、テーブルバケットに作成したテーブルを選択するか、[すべてのテーブル] を選択します。
7. カタログまたはサブカタログのどちらを選択したか、データベースまたはテーブルのどちらを選択したかに応じて、カタログ、データベース、またはテーブルレベルでアクセス許可を設定できます。Lake Formation 許可の詳細については、「AWS Lake Formation デベロッパーガイド」の「Lake Formation 許可の管理」を参照してください。

   次のいずれかを行います：
   - [カタログのアクセス許可] で、[Super] を選択してカタログに対するすべてのアクセス許可を他のプリンシパルに付与するか、[Describe] などのよりきめ細かなアクセス許可を選択します。
   - [データベースのアクセス許可] では、[Super] を選択してデータベースに対するすべてのアクセス許可を他のプリンシパルに付与することはできません。代わりに、[Describe] などのよりきめ細かなアクセス許可を選択します。
   - [テーブルのアクセス許可] で、[Super] を選択してテーブルに対するすべてのアクセス許可を他のプリンシパルに付与するか、[Select] や [Describe] などのよりきめ細かなアクセス許可を選択します。

   > **Note**
   >
   > データカタログリソースに対する Lake Formation のアクセス許可を外部アカウントに付与するか、または別のアカウントの IAM プリンシパルに直接付与する場合、Lake Formation は AWS Resource Access Manager (AWS RAM) サービスを使

用してリソースを共有します。付与対象アカウントが付与する側のアカウントと同じ組織内にある場合、付与対象アカウントはその共有リソースをただちに使用できるようになります。付与対象アカウントが同じ組織内にない場合は、AWS RAM が付与対象アカウントに対して、リソース付与を受け入れる、または拒否するための招待を送信します。その後、共有リソースを利用可能にするために、付与対象アカウントのデータレイク管理者が AWS RAM コンソールまたは AWS CLI を使用して招待を承諾する必要があります。クロスアカウントデータ共有の詳細については、「AWS Lake Formation デベロッパーガイド」の「Lake Formation でのクロスアカウントデータ共有」を参照してください。

8. [Grant] (付与) を選択します。

ステップ 4: Athena で SQL を使用してデータをクエリする

Athena で SQL を使用してテーブルをクエリできます。Athena は S3 Tables に対するデータ定義言語 (DDL)、データ操作言語 (DML)、データクエリ言語 (DQL) クエリをサポートしています。

Athena クエリには、Amazon S3 コンソールまたは Amazon Athena コンソールからアクセスできます。

S3 コンソールと Amazon Athena の使用

以下の手順では、Amazon S3 コンソールを使用して Athena クエリエディタにアクセスし、Amazon Athena でテーブルに対してクエリを実行できるようにします。

テーブルに対してクエリを実行するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[テーブルバケット] を選択します。
3. [テーブルバケット] ページで、クエリを実行するテーブルを含むテーブルバケットを選択します。
4. テーブルバケットの詳細ページで、クエリを実行するテーブルの名前の横にあるオプションボタンを選択します。
5. [Athena でテーブルに対してクエリを実行] を選択します。

6. Amazon Athena コンソールが開き、サンプル SELECT クエリがロードされた状態で Athena クエリエディタが表示されます。必要に応じて、このクエリをユースケースに合わせて変更します。
7. クエリを実行するには、[Run] (実行) を選択します。

Amazon Athena コンソールの使用

テーブルに対してクエリを実行するには

1. https://console.aws.amazon.com/athena/ で Athena コンソールを開きます。
2. テーブルに対してクエリを実行します。以下は、変更できるサンプルクエリです。*user input placeholders* をユーザー自身の情報に必ず置き換えます。

```
SELECT * FROM "s3tablescatalog/amzn-s3-demo-table-bucket"."my_namespace"."my_table"
 LIMIT 10
```

3. クエリを実行するには、[Run] (実行) を選択します。

テーブルバケット

Amazon S3 テーブルバケットは、テーブルを S3 リソースとして作成および保存するために使用できる S3 バケットタイプです。テーブルバケットは、分析ワークロードで使用するためのオブジェクトとして表形式のデータとメタデータを保存するために使用されます。S3 はテーブルバケットのメンテナンスを自動的に実行し、テーブルストレージコストの削減に役立ちます。詳細については、「Amazon S3 テーブルバケットのメンテナンス」を参照してください。

テーブルバケット内に保存されているテーブルを操作するには、テーブルバケットを Apache Iceberg をサポートする分析アプリケーションと統合します。テーブルバケットは、AWS Glue Data Catalog を介して AWS 分析サービスと統合されます。詳細については、「AWS 分析サービスで Amazon S3 Tables を使用する」を参照してください。Amazon S3 Tables Catalog for Apache Iceberg を使用して、オープンソースのクエリエンジンでテーブルを操作することもできます。詳細については、「Amazon S3 Tables Iceberg REST エンドポイントを使用したテーブルへのアクセス」を参照してください。

各テーブルバケットには、一意の Amazon リソースネーム (ARN) とリソースポリシーがアタッチされています。テーブルバケット ARN は次の形式に従います。

```
arn:aws:s3tables:Region:OwnerAccountID:bucket/bucket-name
```

すべてのテーブルバケットとテーブルはプライベートであり、公開することはできません。これらのリソースにアクセスできるのは、明示的にアクセス許可が与えられているユーザーのみです。アクセスを許可するには、テーブルバケットとテーブルには IAM リソースベースのポリシーを使用し、ユーザーとロールには IAM アイデンティティベースのポリシーを使用します。

デフォルトでは、AWS リージョンアカウントの AWS アカウントごとに最大 10 個のテーブルバケットを作成できます。テーブルバケットまたはテーブルのクォータ引き上げをリクエストするには、サポート にお問い合わせください。

Amazon S3 バケットにはいくつかのタイプがあります。バケットを作成する前に、アプリケーションとパフォーマンス要件に最適なバケットタイプを選択していることを確認します。さまざまなバケットタイプとそれぞれの適切なユースケースの詳細については、「バケット」を参照してください。

トピック

- Amazon S3 テーブルバケット、テーブル、および名前空間の命名規則
- テーブルバケットの作成
- テーブルバケットの削除
- Amazon S3 テーブルバケットの詳細の表示
- テーブルバケットポリシーの管理

Amazon S3 テーブルバケット、テーブル、および名前空間の命名規則

テーブルバケットを作成するときは、バケット名と AWS リージョンを選択します。名前は、選択したリージョン内のアカウントに対して一意である必要があります。テーブルバケットを作成した後、バケット名やリージョンを変更することはできません。テーブルバケット名は、特定の命名規則に従う必要があります。テーブルバケットとその中のテーブルと名前空間の命名規則の詳細については、次のトピックを参照してください。

トピック

- テーブルバケットの命名規則
- テーブルと名前空間の命名規則

テーブルバケットの命名規則

Amazon S3 テーブルバケットを作成するときは、テーブルバケット名を指定します。他のバケットタイプと同様に、テーブルバケットの名前を変更することはできません。他のバケットタイプとは異なり、テーブルバケットはグローバル名前空間にないため、アカウント内の各バケット名は現在の AWS リージョン内でのみ一意である必要があります。

汎用バケットの命名規則の詳細については、「汎用バケットの命名規則」を参照してください。ディレクトリバケットの命名規則については、「ディレクトリバケットの命名規則」を参照してください。

テーブルバケットには、次の命名規則が適用されます。

- バケット名は 3～63 文字の長さにする必要があります。
- バケット名は、小文字、数字、およびハイフン (-) のみで構成できます。
- バケット名は、文字または数字で開始および終了する必要があります。
- バケット名にアンダースコア (_) またはピリオド (.) を含めることはできません。
- バケット名は、以下の予約済みプレフィックスで始めることはできません。
  - `xn--`
  - `sthree-`
  - `amzn-s3-demo-`
- バケット名は、以下の予約済みサフィックスで終わることはできません。
  - `-s3alias`
  - `--ol-s3`
  - `--x-s3`
  - `--table-s3`

テーブルと名前空間の命名規則

次の命名規則は、テーブルバケット内のテーブルと名前空間に適用されます。

- 名前の長さは 1～255 文字にする必要があります。
- 名前には小文字、数字、下線 (_) のみを含めることができます。名前空間名の最初と最後にアンダースコアを使用することはできません。
- 名前の最初と最後は、文字または数字にしてください。

- 名前にハイフン (-) またはピリオド (.) を含めることはできません。
- テーブル名は、名前空間内で一意である必要があります。
- 名前空間は、テーブルバケット内で一意である必要があります。
- 名前空間名は、予約済みプレフィックスの aws で始めることはできません。例えば、aws_s3_metadata を名前空間として使用することはできません。aws_s3_metadata はメタデータテーブル用の名前空間として予約されています。詳細については、「S3 メタデータによるデータ検出の高速化」を参照してください。

テーブルバケットの作成

Amazon S3 テーブルバケットは、テーブルを S3 リソースとして作成および保存するために使用できる S3 バケットタイプです。S3 Tables の使用を開始するには、テーブルを保存および管理するためのテーブルバケットを作成します。テーブルバケットを作成するときは、バケット名と AWS リージョン を選択します。テーブルバケット名は、選択したリージョン内のアカウントで一意であることが必要です。テーブルバケットを作成した後、バケット名やリージョンを変更することはできません。テーブルバケットの命名についてさらに詳しくは、「Amazon S3 テーブルバケット、テーブル、および名前空間の命名規則」を参照してください。

テーブルバケットの Amazon リソースネーム (ARN) 形式は次のようになります。

```
arn:aws:s3tables:region:owner-account-id:bucket/bucket-name
```

デフォルトでは、AWS アカウント 内のリージョンごとに最大 10 個のテーブルバケットを作成できます。テーブルバケットまたはテーブルのクォータ引き上げをリクエストするには、サポート にお問い合わせください。

テーブルバケットの作成時に、バケット内に作成するテーブルの暗号化に使用する暗号化タイプを指定できます。バケットの暗号化オプションの詳細については、「the section called “Encryption”」を参照してください。

テーブルバケットを作成するための前提条件

テーブルバケットを作成するには、まず以下の操作を行う必要があります。

- s3tables:CreateTableBucket への AWS Identity and Access Management (IAM) アクセス許可があることを確認します。

> **Note**
>
> デフォルトの暗号化タイプとして SSE-KMS を選択した場合、`s3tables:PutTableBucketEncryption` へのアクセス許可と、選択した AWS KMS キーへの `DescribeKey` アクセス許可が必要です。さらに、使用する AWS KMS キーでは、自動テーブルメンテナンスを実行するアクセス許可を S3 Tables に付与する必要があります。詳細については、S3 Tables の SSE-KMS 暗号化のアクセス許可要件を参照してください。

テーブルバケットを作成するには、Amazon S3 コンソール、Amazon S3 REST API、AWS Command Line Interface (AWS CLI)、または AWS SDK を使用できます。

S3 コンソールの使用

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. ページ上部にあるナビゲーションバーで、現在表示されている AWS リージョン の名前をクリックします。次に、バケットを作成するリージョンを選択します。
3. 左側のナビゲーションペインで、[テーブルバケット] を選択します。
4. [テーブルバケットを作成] を選択して、[テーブルバケットを作成] ページを開きます。
5. [プロパティ] に、テーブルバケットの名前を入力します。

   テーブルバケット名には次の条件があります。

   - 現在のリージョンのアカウント内で一意であること。
   - 3 ~ 63 文字で指定すること
   - 小文字、数字、ハイフン (-) のみで構成されていること。
   - 文字や数字で始まり、文字や数字で終わります。

   バケットを作成したら、その名前を変更することはできません。バケットを作成する AWS アカウント は、そのバケットを所有します。テーブルバケットの命名についてさらに詳しくは、「Amazon S3 テーブルバケット、テーブル、および名前空間の命名規則」を参照してください。
6. テーブルバケットを AWS 分析サービスと統合する場合は、[AWS 分析サービスとの統合] で [統合を有効にする] が選択されていることを確認してください。

> **Note**
>
> コンソールで [統合を有効にする] オプションを選択して最初のテーブルバケットを作成すると、Amazon S3 はテーブルバケットを AWS 分析サービスと自動的に統合しようとします。この統合により、AWS 分析サービスを使用して、現在のリージョン内のすべてのテーブルをクエリできます。詳細については、「AWS 分析サービスで Amazon S3 Tables を使用する」を参照してください。

7. デフォルトの暗号化を設定するには、[暗号化タイプ] で次のいずれかを選択します。

   - [Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3)]
   - [AWS Key Management Service キーによるサーバー側の暗号化 (SSE-KMS)]

   テーブルデータの暗号化オプションの詳細については、「暗号化による S3 テーブルデータの保護」を参照してください。
8. [バケットを作成] を選択します。

AWS CLI を使用する場合

AWS CLI を使用してテーブルバケットを作成する方法は、次の例のとおりです。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3tables create-table-bucket \
    --region us-east-2 \
    --name amzn-s3-demo-bucket1
```

デフォルトでは、S3 テーブルバケットはデフォルトの暗号化設定として SSE-S3 を使用しますが、オプションの `--encryption-configuration` パラメータを使用して別の暗号化タイプを指定することもできます。以下の例は、SSE-KMS 暗号化を使用するバケットを作成する方法を示しています。テーブルバケットの暗号化設定の詳細については、「暗号化による S3 テーブルデータの保護」を参照してください。

```
aws s3tables create-table-bucket \
    --region us-east-2 \
    --name amzn-s3-demo-bucket1
    --encryption-configuration '{
```

```
                    "sseAlgorithm": "aws:kms",
                    "kmsKeyArn":
 "arn:aws:kms:Region:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab" }'
```

テーブルバケットの削除

Amazon S3 API、AWS Command Line Interface、または AWS SDK を使用して、テーブルバケットを削除できます。テーブルバケットを削除する前に、バケット内のすべての名前空間とテーブルを削除する必要があります。

AWS CLI の使用

AWS CLI を使用してテーブルバケットを削除する方法は、次の例のとおりです。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3tables delete-table-bucket \
    --region us-east-2 \
    --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
bucket1
```

Amazon S3 テーブルバケットの詳細の表示

Tables REST API、AWS CLI、または AWS SDK を使用して、Amazon S3 テーブルバケットの詳細をプログラムで表示できます。

AWS CLI の使用

AWS CLI を使用してテーブルバケット詳細を表示する方法は、次の例のとおりです。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3tables get-table-bucket --table-bucket-arn arn:aws:s3tables:us-
east-1:111122223333:bucket/amzn-s3-demo-bucket1
```

テーブルバケットポリシーの管理

Amazon S3 REST API、AWS SDK、AWS Command Line Interface (AWS CLI) を使用して、Amazon S3 テーブルバケットのバケットポリシーを追加、削除、更新、表示できます。詳細については、以下のトピックを参照してください。

詳細については、以下のトピックを参照してください。Amazon S3 Tables でサポートされている AWS Identity and Access Management (IAM) アクションと条件キーの詳細については、「S3 Tables のアクセス管理」を参照してください。ディレクトリバケットのバケットポリシーの例については、「S3 Tables 用のリソースベースのポリシー」を参照してください。

バケットポリシーの追加

バケットポリシーをテーブルバケットに追加するには、次の AWS CLI の例を使用します。

AWS CLI の使用

AWS CLI を使用してテーブルバケットポリシーを作成する方法は、次の例のとおりです。これらのコマンドを使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3tables put-table-bucket-policy \
    --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-bucket1  \
    --resource-policy your-policy-JSON
```

バケットポリシーの表示

テーブルバケットにアタッチされているバケットポリシーを表示するには、次の AWS CLI の例を使用します。

AWS CLI の使用

この例では、AWS CLI を使用してテーブルバケットにアタッチされたバケットポリシーを表示する方法を示します。これらのコマンドを使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3tables get-table-bucket-policy --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-bucket1
```

テーブルバケットポリシーの削除

テーブルバケットにアタッチされているバケットポリシーを削除するには、次の AWS CLI の例を使用します。

AWS CLI の使用

AWS CLI を使用してテーブルバケットポリシーを削除する方法は、次の例のとおりです。これらのコマンドを使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3tables delete-table-bucket-policy --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-bucket1
```

S3 Tables のメンテナンス

Amazon S3 は、S3 Tables またはテーブルバケットのパフォーマンスを向上させるためのメンテナンスを提供します。これらのメンテナンスオプションは、ファイル圧縮、スナップショット管理、および参照されていないファイルの削除です。すべてのオプションはデフォルトで有効になっています。これらのオペレーションは、メンテナンス設定ファイルを使用して編集または無効化できます。

トピック

- S3 Tables メンテナンスジョブのステータス
- Amazon S3 テーブルバケットのメンテナンス
- S3 Tables のメンテナンス
- メンテナンスジョブに関する考慮事項と制限事項

S3 Tables メンテナンスジョブのステータス

S3 Tables メンテナンスジョブは、S3 Tables またはテーブルバケットに対して定期的に実行されます。GetTableMaintenanceJobStatus API を使用して、これらのジョブのステータスをクエリできます。

AWS CLI を使用してメンテナンスジョブのステータスを取得する方法

次の例では、GetTableMaintenanceJobStatus API を使用してメンテナンスジョブのステータスを取得します。

```
aws s3tables get-table-maintenance-job-status \
   --table-bucket-arn="arn:aws:s3tables:arn:aws::111122223333:bucket/amzn-s3-demo-bucket1" \
   --namespace="mynamespace" \
   --name="testtable"
```

詳細については、AWS CLI コマンドリファレンスの「get-table-maintenance-job-status」を参照してください。

S3 Tables メンテナンスジョブは、次の 4 つのステータス間で移行できます。

- `Successful`
- `Failed`
- `Disabled`
- `Not_Yet_Run`

失敗したステータスのジョブには失敗のメッセージが含まれます。次のリストに、考えられる失敗のメッセージを示します。

- テーブルの読み取り中に Iceberg 検証例外が発生しました。テーブルが読み取り可能で、Iceberg 仕様に準拠しており、S3 Tables のエイリアスで始まる S3 パスのみが含まれていることを確認します。
- Iceberg スナップショット管理は現在、ユーザー定義のタグやリファレンスをサポートしていません。
- Iceberg テーブルのメンテナンス設定は、'history.expire.max-snapshot-age-ms' および 'history.expire.min-snapshots-to-keep' テーブルプロパティと互換性がありません。
- Iceberg スナップショット管理と参照されていないファイルの削除は、「gc.enabled」テーブルプロパティが false の場合、サポートされていません。このプロパティが設定されていないか、明示的に true に設定されていることを確認します。
- 古いメタデータのため、コミットに失敗しました。メンテナンスは、次に利用可能な機会に再試行されます。
- テーブルのメンテナンスを実行するためのアクセス権が不十分です。テーブルの暗号化に使用するキーがアクティブであり、存在すること、また S3 サービスプリンシパル `maintenance.s3tables.amazonaws.com` へのアクセスを許可するリソースポリシーがあることを確認します。
- 内部エラー

Amazon S3 テーブルバケットのメンテナンス

Amazon S3 は、テーブルバケットの管理とパフォーマンスを向上させるためのメンテナンスオペレーションを提供します。次のオプションは、すべてのテーブルバケットでデフォルトで有効になっています。このオプションを編集または無効化するには、テーブルバケットのメンテナンス設定ファイルを指定します。

この設定を編集するには、`s3tables:PutTableBucketMaintenanceConfiguration` アクセス許可が必要です。

トピック

- 参照されていないファイルの削除
- 考慮事項と制限事項

参照されていないファイルの削除

参照されていないファイルの削除は、テーブルスナップショットによって参照されていないすべてのオブジェクトを識別して削除します。参照されていないファイル削除ポリシーの一部として、unreferencedDays (デフォルトでは 3 日間) と nonCurrentDays (デフォルトでは 10 日間) の 2 つのプロパティを設定できます。

テーブルで参照されておらず、unreferencedDays プロパティより古いオブジェクトの場合、S3 はオブジェクトを最新ではないものとしてマークします。S3 は、nonCurrentDays プロパティで指定された日数が経過すると、以前のオブジェクトを削除します。

> **Note**
>
> 以前のオブジェクトの削除は永続的であり、これらのオブジェクトを復元する方法はありません。

最新でないとマークされたオブジェクトを表示または復旧するには、AWS サポート に連絡する必要があります。AWS サポート へのお問い合わせの詳細については、AWS サポート ドキュメントの「AWS へのお問い合わせ」を参照してください。

参照されていないファイルの削除では、そのテーブルのみを参照するオブジェクトがテーブルから削除されます。テーブル外でこれらのオブジェクトへの参照が行われても、参照されていないファイルの削除によるオブジェクトの削除は妨げられません。

参照されていないファイルの削除を無効にしても、進行中のジョブは影響を受けません。新しい設定は、設定変更後の次のジョブで有効になります。詳細については、「Amazon S3 の料金」で料金情報を参照してください。

参照されていないファイルの削除は、テーブルバケットレベルでのみ設定できます。この設定は、バケット内のすべてのテーブルに適用されます。

AWS CLI を使用して参照されていないファイルの削除を設定するには

次の例では、PutTableBucketMaintenanceConfiguration API を使用して unreferencedDays を 4 日間に設定し、nonCurrentDays を 10 日間に設定します。

```
aws s3tables put-table-bucket-maintenance-configuration \
   --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
table-bucket \
   --type icebergUnreferencedFileRemoval \
   --value '{"status":"enabled","settings":{"icebergUnreferencedFileRemoval":
{"unreferencedDays":4,"nonCurrentDays":10}}}'
```

詳細については、AWS CLI コマンドリファレンスの「put-table-bucket-maintenance-configuration」を参照してください。

考慮事項と制限事項

参照されていないファイルの削除に関する追加の考慮事項と制限事項の詳細については、「the section called “考慮事項と制限事項”」を参照してください。

S3 Tables のメンテナンス

S3 Tables は、テーブルの管理とパフォーマンスを向上させるためのメンテナンスオペレーションを提供します。次のオプションは、すべてのテーブルでデフォルトで有効になっています。オプションを編集または無効化するには、S3 テーブルのメンテナンス設定ファイルを指定します。

この設定を編集するには、s3tables:GetTableMaintenanceConfiguration および s3tables:PutTableMaintenanceConfiguration アクセス許可が必要です。

トピック

- 圧縮
- スナップショットの管理
- 考慮事項と制限事項

圧縮

圧縮は、小さいオブジェクトを小さいオブジェクトと大きいオブジェクトに組み合わせて、Iceberg クエリのパフォーマンスを向上させます。オブジェクトを組み合わせると、圧縮はテーブル内の行レベル削除の効果も適用します。Amazon S3 は、データアクセスパターンに最適なターゲットファイ

ルサイズ、または指定した値に基づいてテーブルを圧縮します。圧縮されたファイルは、テーブルの最新のスナップショットとして書き込まれます。圧縮はすべてのテーブルでデフォルトで有効になっており、デフォルトのターゲットファイルサイズは 512MB です。

> **Note**
>
> 圧縮は Apache Parquet ファイルタイプでのみサポートされています。

圧縮はテーブルレベルでのみ設定できます。圧縮には追加料金が発生します。詳細については、「Amazon S3 の料金」で料金情報を参照してください。

AWS CLI を使用して圧縮ターゲットファイルサイズを設定するには

次の例では、PutTableMaintenanceConfiguration API を使用してターゲットファイルのサイズを 256MB に変更します。

```
aws s3tables put-table-maintenance-configuration \
   --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
bucket1 \
   --type icebergCompaction \
   --namespace mynamespace \
   --name testtable \
   --value='{"status":"enabled","settings":{"icebergCompaction":
{"targetFileSizeMB":256}}}'
```

詳細については、AWS CLI コマンドリファレンスの「put-table-maintenance-configuration」を参照してください。

AWS CLI を使用して圧縮を無効にするには

次の例では、PutTableMaintenanceConfiguration API を使用して圧縮を無効にします。

```
aws s3tables put-table-maintenance-configuration \
   --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
table-bucket \
   --type icebergCompaction \
   --namespace mynamespace \
   --name testtable \
   --value='{"status":"disabled","settings":{"icebergCompaction":
{"targetFileSizeMB":256}}}'
```

詳細については、AWS CLI コマンドリファレンスの「put-table-maintenance-configuration」を参照してください。

スナップショットの管理

スナップショット管理は、テーブルのアクティブなスナップショットの数を決定します。これは、`MinimumSnapshots` (デフォルトでは 1) と `MaximumSnapshotAge` (デフォルトでは 120 時間) に基づいています。スナップショット管理は、これらの設定に基づいてテーブルスナップショットを有効期限切れにし、削除します。

スナップショットの有効期限が切れると、Amazon S3 はそのスナップショットによってのみ参照されるすべてのオブジェクトを最新でないものとしてマークします。これらの最新でないオブジェクトは、参照されていないファイル削除ポリシーの `NoncurrentDays` プロパティで指定された日数が経過した後に削除されます。

> **Note**
>
> 以前のオブジェクトの削除は永続的であり、これらのオブジェクトを復元する方法はありません。

最新でないとマークされたオブジェクトを表示または復旧するには、AWS サポート に連絡する必要があります。AWS サポート へのお問い合わせの詳細については、AWS サポート ドキュメントの「AWS へのお問い合わせ」を参照してください。

スナップショット管理は、そのテーブルのみを参照して、テーブルから削除するオブジェクトを決定します。テーブル外でこれらのオブジェクトへの参照が行われても、スナップショット管理によるオブジェクトの削除は妨げられません。

> **Note**
>
> スナップショット管理では、ブランチやタグベースの保持を含め、`metadata.json` ファイル内の Iceberg テーブルプロパティとして、または `ALTER TABLE SET TBLPROPERTIES` SQL コマンドを介して設定した保持値はサポートされていません。ブランチまたはタグベースの保持ポリシーを設定する場合、または `PutTableMaintenanceConfiguration` API で設定された値よりも長い保持ポリシーを `metadata.json` ファイルに設定する場合、スナップショット管理は無効になります。このような場合、S3 はスナップショットの有効期限

が切れたり削除されたりしないため、ストレージ料金が発生しないように、スナップショットを手動で削除するか、Iceberg テーブルからプロパティを削除する必要があります。

スナップショット管理は、テーブルレベルでのみ設定できます。詳細については、「Amazon S3 の料金」で料金情報を参照してください。

AWS CLI を使用してスナップショット管理を設定するには

次の例では、PutTableMaintenanceConfiguration API を使用して MinimumSnapshots を 10 に設定し、MaximumSnapshotAgeを 2,500 時間に設定します。

```
aws s3tables put-table-maintenance-configuration \
--table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
table-bucket \
--namespace my_namespace \
--name my_table \
--type icebergSnapshotManagement \
--value '{"status":"enabled","settings":{"icebergSnapshotManagement":
{"minSnapshotsToKeep":10,"maxSnapshotAgeHours":2500}}}'
```

詳細については、AWS CLI コマンドリファレンスの「put-table-maintenance-configuration」を参照してください。

考慮事項と制限事項

圧縮とスナップショット管理に関するその他の考慮事項と制限の詳細については、「the section called “考慮事項と制限事項”」を参照してください。

> **Note**
>
> S3 Tables は、parquet の row-group-default サイズである 128 MB を適用します。

メンテナンスジョブに関する考慮事項と制限事項

Amazon S3 には、S3 テーブルまたはテーブルバケットのパフォーマンスを向上させるためのメンテナンスオペレーションが用意されています。これらのオプションは、ファイル圧縮、スナップショッ

ト管理、および参照されていないファイルの削除です。これらの管理オプションの制限事項と考慮事項を次に示します。

トピック

- 圧縮に関する考慮事項
- スナップショット管理に関する考慮事項
- 参照されていないファイルの削除に関する考慮事項
- S3 テーブルとテーブルバケットのメンテナンスの制限事項

圧縮に関する考慮事項

圧縮には以下の考慮事項が適用されます。圧縮の詳細については、「the section called “テーブルのメンテナンス”」を参照してください。

- 圧縮は Apache Parquet ファイルタイプでのみサポートされています。
- 圧縮は Fixed データ型をサポートしていません。
- 圧縮は圧縮タイプ `brotli`、`lz4` をサポートしていません。

スナップショット管理に関する考慮事項

スナップショット管理には、以下の考慮事項が適用されます。スナップショット管理の詳細については、「the section called “テーブルのメンテナンス”」を参照してください。

- スナップショットは、保持するスナップショットの最小数と指定された保持期間という両方の基準が満たされた場合にのみ保持されます。
- スナップショット管理では、Apache Iceberg から期限切れのスナップショットメタデータを削除し、期限切れのスナップショットのタイムトラベルクエリを防ぎ、オプションで関連するデータファイルを削除します。
- スナップショット管理では、ブランチやタグベースの保持を含め、`metadata.json` ファイル内の Iceberg テーブルプロパティとして、または `ALTER TABLE SET TBLPROPERTIES` SQL コマンドを介して設定した保持値はサポートされていません。ブランチまたはタグベースの保持ポリシーを設定する場合、または `PutTableMaintenanceConfiguration` API で設定された値よりも長い保持ポリシーを `metadata.json` ファイルに設定する場合、スナップショット管理は無効になります。このような場合、S3 はスナップショットの有効期限が切れたり削除されたりしないため、ストレージ料金が発生しないように、スナップショットを手動で削除するか、Iceberg テーブルからプロパティを削除する必要があります。

参照されていないファイルの削除に関する考慮事項

参照されていないファイルの削除には、以下の考慮事項が適用されます。参照されていないファイルの削除の詳細については、「the section called “テーブルバケットのメンテナンス”」を参照してください。

- 参照されていないファイルを削除すると、作成時刻が保持期間より前の場合、Iceberg メタデータによって参照されなくなったデータとメタデータファイルが削除されます。

S3 テーブルとテーブルバケットのメンテナンスの制限事項

メンテナンスオペレーション	プロパティ	テーブルバケットレベルで設定可能か。	テーブルレベルで設定可能か。	デフォルト値	最小値
圧縮	targetFileSizeMB	いいえ	はい	512MB	64MB
スナップショットの管理	minimumSnapshots	いいえ	はい	1	1
スナップショットの管理	maximumSnapshotAge	いいえ	はい	120 時間	1 時間
参照されていないファイルの削除	unreferencedDays	はい	いいえ	3 日	1 日
参照されていないファイルの削除	nonCurrentDays	はい	いいえ	10 日	1 日

> **Note**
>
> S3 Tables は、parquet の row-group-default サイズである 128 MB を適用します。

テーブル名前空間

Amazon S3 テーブルバケット内にテーブルを作成するときは、名前空間と呼ばれる論理グループに整理します。S3 テーブルやテーブルバケットとは異なり、名前空間はリソースではありません。名前空間は、テーブルをスケーラブルに整理および管理するための構成概念です。例えば、会社の人事部門に属するすべてのテーブルを、共通の名前空間値 `hr` でグループ化できます。

特定の名前空間へのアクセスを制御するには、テーブルバケットリソースポリシーを使用できます。詳細については、「the section called “リソースベースのポリシー”」を参照してください。

テーブル名前空間には、次のルールが適用されます。

- 名前空間はそれぞれテーブルバケット内で一意である必要があります。
- テーブルバケットごとに最大 10,000 個の名前空間を作成できます。
- テーブル名はそれぞれ名前空間内で一意である必要があります。
- 各テーブルには、1 レベルの名前空間のみを含めることができます。名前空間はネストできません。
- 各テーブルは 1 つの名前空間に属します。
- 名前空間の間でテーブルを移動できます。

トピック

- ネームスペースの作成
- 名前空間を削除する

ネームスペースの作成

テーブル名前空間は、Amazon S3 テーブルバケット内でテーブルをグループ化するための論理的な構成概念です。各テーブルは 1 つの名前空間に属します。テーブルバケット内にテーブルを作成する前に、テーブルをグループ化するための名前空間を作成する必要があります。名前空間は、Amazon S3 コンソール、AWS Command Line Interface (AWS CLI)、Amazon S3 REST API、AWS SDK、または統合クエリエンジンを使用して作成できます。

名前空間名

名前空間には、次の命名規則が適用されます。

- 名前の長さは 1〜255 文字にする必要があります。
- 名前には小文字、数字、下線 (_) のみを含めることができます。名前空間名の最初と最後にアンダースコアを使用することはできません。
- 名前の最初と最後は、文字または数字にしてください。
- 名前にハイフン (-) またはピリオド (.) を含めることはできません。
- 名前空間は、テーブルバケット内で一意である必要があります。
- 名前空間名は、予約済みプレフィックスの `aws` で始めることはできません。例えば、`aws_s3_metadata` を名前空間として使用することはできません。`aws_s3_metadata` はメタデータテーブル用の名前空間として予約されています。詳細については、「S3 メタデータによるデータ検出の高速化」を参照してください。

有効な名前空間名の詳細については、「テーブルと名前空間の命名規則」を参照してください。

S3 コンソールと Amazon Athena の使用

以下の手順では、「Athena でテーブルを作成する」ワークフローを使用して、Amazon S3 コンソールで名前空間を作成します。Amazon Athena を使用して名前空間にテーブルを作成しない場合は、名前空間の作成後にワークフローをキャンセルできます。

名前空間を作成するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[テーブルバケット] を選択します。
3. [テーブルバケット] ページで、名前空間を作成するバケットを選択します。
4. バケットの詳細ページで、[Athena でテーブルを作成] を選択します。
5. [Athena でテーブルを作成] ダイアログボックスで、[名前空間を作成] を選択した後、[名前空間を作成] を選択します。
6. [名前空間名] フィールドに名前を入力します。名前空間名は 1 ~ 255 文字で、テーブルバケット内で一意であることが必要です。有効な文字は a〜z、0〜9、アンダースコア (_) です。名前空間名の最初と最後にアンダースコアを使用することはできません。
7. [名前空間の作成] を選択します。

8. テーブルも作成する場合は、[Athena でテーブルを作成] を選択します。Athena でテーブルを作成する方法の詳細については、「the section called “S3 コンソールと Amazon Athena の使用”」を参照してください。今すぐテーブルを作成しない場合は、[キャンセル] を選択します。

AWS CLI を使用する場合

この例では、AWS CLI を使用してテーブル名前空間を作成する方法を示します。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3tables create-namespace \
    --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-bucket1 \
    --namespace example_namespace
```

クエリエンジンの使用

Amazon S3 テーブルバケットに接続された Apache Spark セッションに名前空間を作成できます。

この例では、S3 Tables と統合されたクエリエンジンで CREATE ステートメントを使用してテーブルを作成する方法を示します。この例を使用するには、############を独自の情報に置き換えます。

```
spark.sql("CREATE NAMESPACE IF NOT EXISTS s3tablesbucket.my_namespace")
```

名前空間を削除する

Amazon S3 テーブルバケットからテーブル名前空間を削除する前に、名前空間内のすべてのテーブルを削除するか、別の名前空間に移動する必要があります。名前空間は、Amazon S3 REST API、AWS SDK、AWS Command Line Interface (AWS CLI)、または統合クエリエンジンを使用して削除できます。

名前空間の削除に必要なアクセス許可については、「Amazon Simple Storage Service API リファレンス」の「DeleteNamespace」を参照してください。

AWS CLI を使用する場合

この例では、AWS CLI を使用してテーブル名前空間を削除する方法を示します。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3tables delete-namespace \
    --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-bucket1 \
    --namespace example_namespace
```

S3 テーブルバケットのテーブル

S3 テーブルは、基盤となるテーブルデータと関連するメタデータで構成される構造化データセットを表します。このデータは、サブリソースとしてテーブルバケット内に保存されます。テーブルバケット内のすべてのテーブルは、Apache Iceberg テーブル形式で保存されます。Amazon S3 は、自動ファイル圧縮とスナップショット管理を通じてテーブルのメンテナンスを管理します。詳細については、「S3 Tables のメンテナンス」を参照してください。

アカウント内のテーブルを AWS 分析サービスからアクセスできるようにするには、Amazon S3 テーブルバケットを Amazon SageMaker Lakehouse と統合します。この統合により、Amazon Athena や Amazon Redshift などの AWS 分析サービスがテーブルデータを自動的に検出してアクセスできるようになります。

テーブルを作成すると、Amazon S3 はテーブルのウェアハウスの場所を自動的に生成します。これは、テーブルに関連付けられたオブジェクトを保存する一意の S3 の場所です。次の例は、ウェアハウスの場所の形式を示しています。

```
s3://63a8e430-6e0b-46f5-k833abtwr6s8tmtsycedn8s4yc3xhuse1b--table-s3
```

テーブルバケット内で、テーブルを名前空間と呼ばれる論理グループに整理できます。詳細については、「テーブル名前空間」を参照してください。

テーブルの名前は変更できますが、各テーブルには独自の Amazon リソースネーム (ARN) と一意のテーブル ID があります。各テーブルには、リソースポリシーもアタッチされています。このポリシーを使用して、テーブルへのアクセスを管理できます。

テーブル ARN は次の形式を使用します。

```
arn:aws:s3tables:region:owner-account-id:bucket/bucket-name/table/table-id
```

デフォルトでは、テーブルバケットに最大 10,000 個のテーブルを作成できます。テーブルバケットまたはテーブルのクォータ引き上げをリクエストするには、サポート にお問い合わせください。

Amazon S3 は、テーブルバケットで次のタイプのテーブルをサポートしています。

カスタマーテーブル

カスタマーテーブルは、読み書きできるテーブルです。統合されたクエリエンジンを使用して、これらのテーブルからデータを取得できます。S3 API オペレーションまたは統合クエリエンジンを使用して、それらのデータを挿入、更新、または削除できます。

AWS テーブル

AWS テーブルは、ユーザーに代わって AWS のサービスによって生成される読み取り専用テーブルです。これらのテーブルは Amazon S3 によって管理され、Amazon S3 自体の外部にある IAM プリンシパルによって変更することはできません。これらのテーブルから情報を取得することはできますが、その中のデータを変更することはできません。AWS テーブルには S3 メタデータテーブルが含まれており、これには S3 汎用バケット内のオブジェクトからキャプチャされたメタデータが含まれています。詳細については、「S3 メタデータによるデータ検出の高速化」を参照してください。

トピック

- Amazon S3 テーブルの作成
- Amazon S3 テーブルの削除
- テーブルポリシーの管理

Amazon S3 テーブルの作成

Amazon S3 テーブルはテーブルバケットのサブリソースです。テーブルは Apache Iceberg 形式で保存されるため、Apache Iceberg をサポートするクエリエンジンやその他のアプリケーションを使用して操作できます。Amazon S3 は、テーブルを継続的に最適化して、ストレージコストを削減し、分析クエリのパフォーマンスを向上させます。

テーブルを作成すると、Amazon S3 はテーブルのウェアハウスの場所を自動的に生成します。ウェアハウスの場所は、テーブルに関連付けられたオブジェクトを読み書きできる一意の S3 の場所です。次の例は、ウェアハウスの場所の形式を示しています。

```
s3://63a8e430-6e0b-46f5-k833abtwr6s8tmtsycedn8s4yc3xhuse1b--table-s3
```

テーブルの Amazon リソースネーム (ARN) 形式は次のようになります。

```
arn:aws:s3tables:region:owner-account-id:bucket/bucket-name/table/table-id
```

デフォルトでは、テーブルバケットに最大 10,000 個のテーブルを作成できます。テーブルバケットまたはテーブルのクォータ引き上げをリクエストするには、サポート にお問い合わせください。

テーブルを作成するには、Amazon S3 コンソール、Amazon S3 REST API、AWS SDK、AWS Command Line Interface (AWS CLI)、またはテーブルバケットに接続されたクエリエンジンを使用できます。

テーブルの作成時に、テーブルの暗号化設定を指定できます (Athena でテーブルを作成する場合は除きます)。暗号化設定を指定しない場合、テーブルはテーブルバケットのデフォルト設定で暗号化されます。詳細については、「テーブルの暗号化の指定」を参照してください。

テーブルを作成するための前提条件

テーブルを作成するには、まず以下の手順を実行する必要があります。

- テーブルバケットを作成する.
- テーブルバケット内で 名前空間を作成します。。
- `s3tables:CreateTable` および `s3tables:PutTableData` に対する AWS Identity and Access Management (IAM) アクセス許可があることを確認してください。
-

> **Note**
>
> テーブルで SSE-KMS 暗号化を使用する場合は、`s3tables:PutTableEncryption` へのアクセス許可と、選択した AWS KMS キーへの `DescribeKey` アクセス許可が必要です。さらに、使用する AWS KMS キーでは、自動テーブルメンテナンスを実行するアクセス許可を S3 Tables に付与する必要があります。詳細については、S3 Tables の SSE-KMS 暗号化のアクセス許可要件を参照してください。

有効なテーブル名については、「テーブルと名前空間の命名規則」を参照してください。

> **Important**
>
> テーブルを作成するときは、テーブル名とテーブル定義にすべて小文字を使用してください。例えば、列名がすべて小文字であることを確認します。テーブル名またはテーブル定義に大文字が含まれている場合、テーブルは AWS Lake Formation または AWS Glue Data

Catalog ではサポートされていません。この場合、テーブルバケットが AWS 分析サービスと統合されていても、テーブルは Amazon Athena などの AWS 分析サービスに表示されません。
テーブル定義に大文字が含まれている場合、Athena で SELECT クエリを実行すると、次のエラーメッセージが表示されます。「GENERIC_INTERNAL_ERROR: Get table request failed: com.amazonaws.services.glue.model.ValidationException: Unsupported Federation Resource - Invalid table or column names.」

S3 コンソールと Amazon Athena の使用

以下の手順では、Amazon S3 コンソールを使用して、Amazon Athena でテーブルを作成します。テーブルバケット内に名前空間をまだ作成していない場合は、このプロセスの間に作成できます。以下の手順を実行する前に、このリージョンでテーブルバケットを AWS 分析サービスと統合していることを確認してください。詳細については、「the section called “AWS 分析サービスで S3 Tables を使用する”」を参照してください。

> **Note**
>
> Athena を使用して作成したテーブルは、テーブルバケットからデフォルトの暗号化設定を継承します。別の暗号化タイプを使用する場合は、別の方法でテーブルを作成する必要があります。

テーブルを作成するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[テーブルバケット] を選択します。
3. [テーブルバケット] ページで、テーブルを作成するバケットを選択します。
4. バケットの詳細ページで、[Athena でテーブルを作成] を選択します。
5. [Athena でテーブルを作成] ダイアログボックスで、次のいずれかを行います。
   - 新しい名前空間を作成します。[名前空間を作成] を選択し、[名前空間名] フィールドに名前を入力します。名前空間名は 1～255 文字で、テーブルバケット内で一意であることが必要です。有効な文字は a～z、0～9、アンダースコア (_) です。名前空間名の先頭にアンダースコアを使用することはできません。

- [名前空間の作成] を選択します。
- 既存の名前空間を指定します。[このテーブルバケット内の既存の名前空間を指定] を選択します。次に、[既存の名前空間から選択] または [既存の名前空間名を入力] のいずれかを選択します。バケット内に 1,000 個を超える名前空間がある場合、リストに表示されない名前空間名は手動で入力する必要があります。

6. [Athena でテーブルを作成] を選択します。
7. Amazon Athena コンソールが開き、Athena クエリエディタが表示されます。[カタログ] フィールドには、s3tablescatalog/ の後にテーブルバケットの名前が入力されます (s3tablescatalog/***amzn-s3-demo-bucket*** など)。[データベース] フィールドには、以前に作成または選択した名前空間が入力されます。

> **Note**
>
> [カタログ] および [データベース] フィールドにこれらの値が表示されない場合は、このリージョンでテーブルバケットを AWS 分析サービスと統合していることを確認してください。詳細については、「the section called “AWS 分析サービスで S3 Tables を使用する”」を参照してください。

8. クエリエディタには、テーブルの作成に使用できるサンプルクエリが入力されます。クエリを変更して、テーブル名とテーブルに必要な列を指定します。
9. クエリの変更が完了したら、[実行] を選択してテーブルを作成します。

> **Note**
>
> - Athena でクエリを実行しようとしたときに、クエリを実行するためのアクセス許可が不足しており、プリンシパルは指定されたリソースに対する権限を持っていないという内容のエラーが表示される場合は、テーブルに対する必要な Lake Formation 許可が付与されている必要があります。詳細については、「the section called “テーブルまたはデータベースに対するアクセス許可の付与”」を参照してください。
> - Athena でクエリを実行しようとしたときに、Iceberg はリクエストされたリソースにアクセスできないという内容のエラーが表示される場合は、AWS Lake Formation コンソールに移動し、作成したテーブルバケットカタログとデータベース (名前空間) に対するアクセス許可が自分に付与されていることを確認してください。これらのアクセス許可を付与するときは、テーブルを指定しないでください。詳細については、「the section called “テーブルまたはデータベースに対するアクセス許可の付与”」を参照してください。

- Athena で SELECT クエリを実行するときに次のエラーメッセージが表示される場合、このメッセージはテーブル名またはテーブル定義の列名に大文字が含まれていることが原因です。「GENERIC_INTERNAL_ERROR: Get table request failed: com.amazonaws.services.glue.model.ValidationException: Unsupported Federation Resource - Invalid table or column names.」 テーブル名と列名がすべて小文字であることを確認します。

テーブルが作成されると、新しいテーブルの名前が Athena のテーブルのリストに表示されます。Amazon S3 コンソールに戻り、テーブルバケットの詳細ページの [テーブル] リストを更新すると、新しいテーブルが表示されます。

AWS CLI を使用する場合

この例では、スキーマを定義したテーブルを作成し、AWS CLI を使用して JSON でテーブルのメタデータを指定する方法を示しています。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3tables create-table --cli-input-json file://mytabledefinition.json
```

mytabledefinition.json ファイルには、次のテーブル定義の例を使用します。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
{
    "tableBucketARN": "arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
table-bucket",
    "namespace": "your_namespace",
    "name": "example_table",
    "format": "ICEBERG",
    "metadata": {
        "iceberg": {
            "schema": {
                "fields": [
                     {"name": "id", "type": "int","required": true},
                     {"name": "name", "type": "string"},
                     {"name": "value", "type": "int"}
                ]
            }
        }
    }
```

```
}
```

クエリエンジンの使用

テーブルバケットに接続されたサポートされているクエリエンジンで、例えば Amazon EMR 上の Apache Spark セッションで、テーブルを作成できます。

この例では、CREATE ステートメントを使用して Spark でテーブルを作成した後、INSERT ステートメントを使用してテーブルデータを追加するか、既存のファイルからテーブルデータを追加する方法を示します。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
spark.sql(
" CREATE TABLE IF NOT EXISTS s3tablesbucket.example_namespace.`example_table` (
    id INT,
    name STRING,
    value INT
)
USING iceberg "
)
```

テーブルを作成した後、テーブルにデータをロードできます。以下の方法から選択します。

- INSERT ステートメントを使用して、データをテーブルに追加します。

  ```
  spark.sql(
  """
      INSERT INTO s3tablesbucket.my_namespace.my_table
      VALUES
          (1, 'ABC', 100),
          (2, 'XYZ', 200)
  """)
  ```

- 既存のデータファイルを読み込みます。

  1. データを Spark に読み取ります。

     ```
     val data_file_location = "Path such as S3 URI to data file"
     val data_file = spark.read.parquet(data_file_location)
     ```

  2. データを Iceberg テーブルに書き込みます。

```
data_file.writeTo("s3tablesbucket.my_namespace.my_table").using("Iceberg").tableProperty
 ("format-version", "2").createOrReplace()
```

Amazon S3 テーブルの削除

Amazon S3 REST API、AWS SDK、AWS CLI または統合されたクエリエンジンを使用してテーブルを削除できます。

> **Note**
>
> S3 Tables は、purge=false を指定した DROP TABLE オペレーションをサポートしていません。Spark の一部のバージョンでは、DROP TABLE PURGE コマンドの実行時でも常にこのフラグが false に設定されます。DROP TABLE を purge=true にして再試行するか、S3 Tables の DeleteTable REST API を使用してテーブルを削除できます。
> テーブルを削除すると、そのテーブルに関連付けられているオブジェクトは最新ではなくなり、削除されるまでに最大 1 日かかることがあります。

AWS CLI の使用

この例では、AWS CLI を使用してテーブルを削除する方法を示します。このコマンドを使用する際は、*###############*を独自の情報に置き換えます。

```
aws s3tables delete-table \
    --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
table-bucket \
    --namespace example_namespace --name example_table
```

クエリエンジンの使用

Amazon S3 テーブルバケットに接続された Apache Spark セッションでテーブルを削除できます。

この例では、DROP TABLE PURGE コマンドを使用してテーブルを削除する方法を示します。このコマンドを使用する際は、*###############*を独自の情報に置き換えます。

```
spark.sql(
" DROP TABLE [IF EXISTS] s3tablesbucket.example_namespace.example_table PURGE;
```

テーブルポリシーの管理

Amazon S3 REST API、AWS SDK、AWS CLI を使用して、テーブルのテーブルポリシーを追加、削除、更新、表示できます。詳細については、以下のトピックを参照してください。Amazon S3 Tables でサポートされている AWS Identity and Access Management (IAM) アクションと条件キーの詳細については、「S3 Tables のアクセス管理」を参照してください。テーブルポリシーの例については、「S3 Tables 用のリソースベースのポリシー」を参照してください。

テーブルポリシーの追加

テーブルポリシーをテーブルに追加するには、Amazon S3 REST API、AWS SDK、AWS CLI を使用できます。

AWS CLI の使用

この例では、AWS CLI を使用してテーブルポリシーを作成する方法を示します。このコマンドを使用する際は、*###############*を独自の情報に置き換えます。

```
aws s3tables put-table-policy \
    --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-bucket1 \
    --namespace my-namespace \
    --name my-table \
    --resource-policy your-policy-JSON
```

テーブルポリシーの表示

テーブルにアタッチされたバケットポリシーを表示するには、Amazon S3 REST API、AWS SDK、AWS CLI を使用できます。

AWS CLI の使用

この例では、AWS CLI を使用してテーブルにアタッチされたポリシーを表示する方法を示します。このコマンドを使用する際は、*###############*を独自の情報に置き換えます。

```
aws s3tables get-table-policy \
    --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-bucket1/table/tableID \
    --namespace my-namespace \
    --name my-table
```

テーブルポリシーの削除

テーブルにアタッチされたポリシーを削除するには、Amazon S3 REST API、AWS SDK、AWS CLI を使用できます。

AWS CLI の使用

この例では、AWS CLI を使用してテーブルポリシーを削除する方法を示します。このコマンドを使用する際は、*###############*を独自の情報に置き換えます。

```
aws s3tables delete-table-policy \
    --table-ARN arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-bucket1/
table/tableID \
    --namespace your-namespace \
    --name your-table
```

テーブルデータへのアクセス

Amazon S3 テーブルバケット内のテーブルにアクセスする方法は複数あります。Amazon SageMaker Lakehouse を使用してテーブルを AWS 分析サービスと統合するか、Amazon S3 Tables Iceberg REST エンドポイントまたは Amazon S3 Tables Catalog for Apache Iceberg を使用してテーブルに直接アクセスできます。使用するアクセス方法は、カタログの設定、ガバナンスモデル、アクセスコントロールのニーズによって異なります。これらのアクセス方法の概要を次に示します。

Amazon SageMaker Lakehouse の統合

これは、S3 テーブルバケット内のテーブルを操作するために推奨されるアクセス方法です。この統合により、複数の AWS 分析サービス全体で統一されたテーブル管理、一元化されたガバナンス、きめ細かなアクセスコントロールが可能になります。

直接アクセス

AWS Partner Network (APN) カタログ実装、カスタムカタログ実装を使用する必要がある場合、または 1 つのテーブルバケット内のテーブルに対して基本的な読み取り/書き込みオペレーションのみを実行する必要がある場合は、この方法を使用します。

> **Note**
>
> テーブルにアクセスするには、テーブルリソースと S3 Tables アクションへのアクセス権が、ユーザーが使用する IAM ID に必要です。詳細については、「S3 Tables のアクセス管理」を参照してください。

Amazon SageMaker Lakehouse 統合を通じたテーブルへのアクセス

S3 テーブルバケットを Amazon SageMaker Lakehouse と統合して、Amazon Athena、Amazon Redshift、QuickSight などの AWS 分析サービスからテーブルにアクセスできます。Amazon SageMaker Lakehouse は、Amazon S3 データレイクと Amazon Redshift データウェアハウス全体のデータを統合するため、データの 1 つのコピーに対して分析、機械学習 (ML)、生成 AI アプリケーションを構築できます。この統合により、AWS Glue Data Catalog にテーブルリソースが入力され、AWS Lake Formation でこれらのリソースへのアクセスがフェデレーションされます。統合の詳細については、「AWS 分析サービスで Amazon S3 Tables を使用する」を参照してください。

この統合により、AWS Lake Formation を通じたきめ細かなアクセスコントロールが可能になり、セキュリティが向上します。Lake Formation は、独自のアクセス許可モデルと IAM のアクセス許可モデルを組み合わせて、テーブルリソースと基になるデータへのアクセスを制御します。つまり、テーブルへのアクセスリクエストは、IAM と Lake Formation の両方によるアクセス許可チェックに合格する必要があります。詳細については、「AWS Lake Formation デベロッパーガイド」の「Lake Formation 許可の概要」を参照してください。

次の AWS 分析サービスはこの統合を通じてテーブルにアクセスできます。

- Amazon Athena
- Amazon Redshift
- Amazon EMR
- QuickSight
- Amazon Data Firehose

AWS Glue Iceberg REST エンドポイントを使用したテーブルへのアクセス

S3 テーブルバケットが Amazon SageMaker Lakehouse と統合されると、AWS Glue Iceberg REST エンドポイントも使用して、Iceberg をサポートするサードパーティーのクエリエンジンから S3

テーブルに接続することもできます 詳細については、「AWS Glue Iceberg REST エンドポイントを使用した Amazon S3 テーブルへのアクセス」を参照してください。

Spark、PyIceberg、またはその他の Iceberg 互換クライアントからテーブルにアクセスする場合は、AWS Glue Iceberg REST エンドポイントを使用することをお勧めします。

次のクライアントは AWS Glue Iceberg REST エンドポイントを通じてテーブルに直接アクセスできます。

- Spark、PyIceberg などの任意の Iceberg クライアント。

テーブルへの直接アクセス

S3 Tables 管理オペレーションを Apache Iceberg 分析アプリケーションに橋渡しする方法を通じて、オープンソースクエリエンジンからテーブルに直接アクセスできます。直接アクセスには、Amazon S3 Tables Iceberg REST エンドポイントと Amazon S3 Tables Catalog for Apache Iceberg の 2 つの方法があります。REST エンドポイントをお勧めします。

セルフマネージドカタログ実装でテーブルにアクセスする場合、または 1 つのテーブルバケット内のテーブルに対して基本的な読み取り/書き込みオペレーションのみを実行する必要がある場合は、直接アクセスをお勧めします。その他のアクセスシナリオでは、Amazon SageMaker Lakehouse 統合をお勧めします。

テーブルへの直接アクセスは、IAM アイデンティティベースのポリシーか、またはテーブルとテーブルバケットにアタッチされたリソースベースのポリシーを通じて管理されます。テーブルに直接アクセスする場合、テーブルに対する Lake Formation 許可を管理する必要はありません。

Amazon S3 Tables Iceberg REST エンドポイントを通じたテーブルへのアクセス

Amazon S3 Tables Iceberg REST エンドポイントを使用して、HTTP エンドポイントを通じて任意の Iceberg REST 互換クライアントからテーブルに直接アクセスできます。詳細については、「Amazon S3 Tables Iceberg REST エンドポイントを使用したテーブルへのアクセス」を参照してください。

次の AWS 分析サービスとクエリエンジンは、Amazon S3 Tables Iceberg REST エンドポイントを使用してテーブルに直接アクセスできます。

サポートされているクエリエンジン

- Spark、PyIceberg などの任意の Iceberg クライアント。

- Amazon EMR
- AWS Glue ETL

Amazon S3 Tables Catalog for Apache Iceberg を通じたテーブルへの直接アクセス

S3 Tables クライアントカタログを使用することで、Apache Spark のようなクエリエンジンからテーブルに直接アクセスすることもできます。詳細については、「Amazon S3 Tables Catalog for Apache Iceberg を使用した Amazon S3 テーブルへのアクセス」を参照してください。ただし S3 では、言語やエンジン固有のコードを必要とせず、より多くのアプリケーションをサポートしているため、直接アクセスには Amazon S3 Tables Iceberg REST エンドポイントを使用することをお勧めします。

次のクエリエンジンは、クライアントカタログを使用してテーブルに直接アクセスできます。

- Apache Spark

AWS 分析サービスで Amazon S3 Tables を使用する

アカウント内のテーブルを AWS 分析サービスからアクセスできるようにするには、Amazon S3 テーブルバケットを Amazon SageMaker Lakehouse と統合します。この統合により、AWS 分析サービスがテーブルデータを自動的に検出してアクセスできるようになります。この統合を使用して、以下のサービスのテーブルを操作できます。

- Amazon Athena
- Amazon Redshift
- Amazon EMR
- QuickSight
- Amazon Data Firehose

> **Note**
>
> この統合では、AWS Glue および AWS Lake Formation サービスが使用され、AWS Glue リクエストとストレージのコストが発生する可能性があります。詳細については、AWS Glue の料金を参照してください。

S3 テーブルでクエリを実行する場合は、追加料金が適用されます。詳細については、使用しているクエリエンジンの料金情報を参照してください。

統合の仕組み

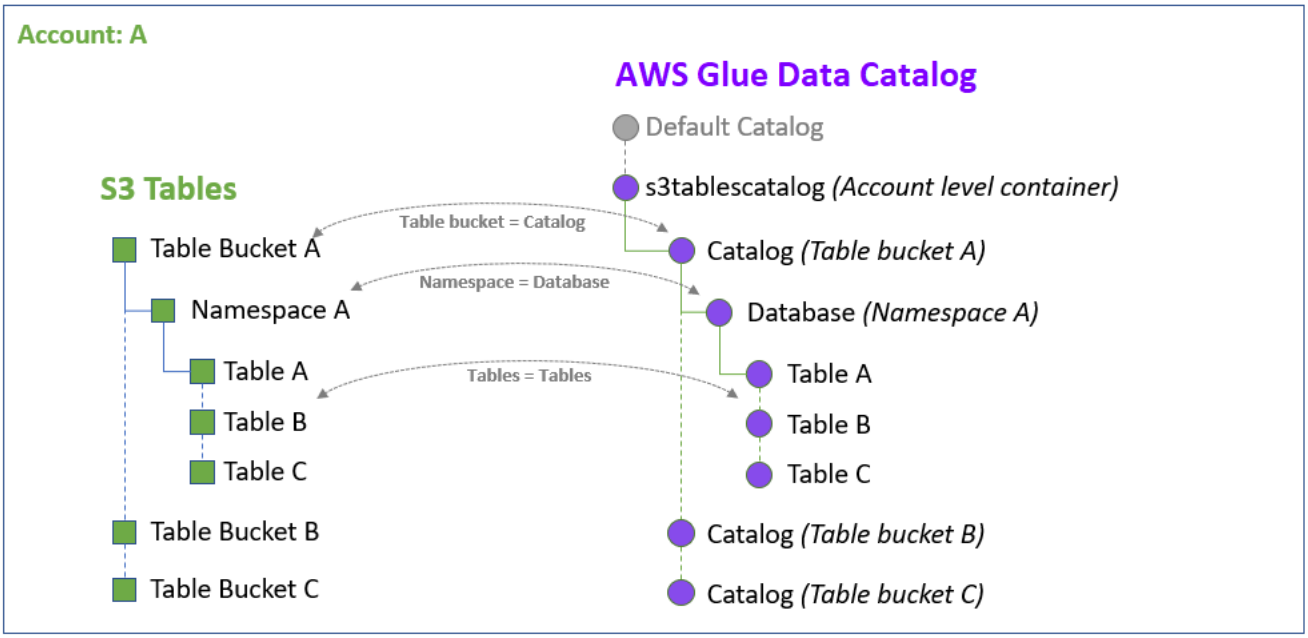
コンソールでテーブルバケットを作成すると、Amazon S3 は次のアクションを開始して、選択したリージョンのテーブルバケットを AWS 分析サービスと統合します。

1. Lake Formation にすべてのテーブルバケットへのアクセスを許可する新しい AWS Identity and Access Management (IAM) サービスロールを作成します。
2. サービスロールを使用して、Lake Formation は現在のリージョンにテーブルバケットを登録します。これにより、Lake Formation は、そのリージョン内のすべての現在および将来のテーブルバケットのアクセス、アクセス許可、ガバナンスを管理できます。
3. `s3tablescatalog` カタログを現在のリージョンの AWS Glue Data Catalog に追加します。`s3tablescatalog` カタログを追加すると、すべてのテーブルバケット、名前空間、テーブルをデータカタログに入力できるようになります。

> **Note**
>
> これらのアクションは Amazon S3 コンソールを通じて自動化されています。この統合をプログラムで実装する場合は、これらの操作をすべて手動で実行する必要があります。

テーブルバケットの統合は AWS リージョンごとに 1 回行います。統合が完了すると、現在および将来のすべてのテーブルバケット、名前空間、およびテーブルが、そのリージョンの AWS Glue Data Catalog に追加されます。

次の図は、`s3tablescatalog` カタログが現在のリージョンのテーブルバケット、名前空間、テーブルをデータカタログ内の対応するオブジェクトとして自動的に入力する方法を示しています。テーブルバケットはサブカタログとして入力されます。テーブルバケット内の名前空間は、それぞれのサブカタログ内のデータベースとして入力されます。テーブルは、それぞれのデータベースにテーブルとして入力されます。



アクセス許可の仕組み

AWS Glue Data Catalog をメタデータストアとして使用するサービス間でテーブルデータを操作できるように、テーブルバケットを AWS 分析サービスと統合することをお勧めします。この統合により、AWS Lake Formation を通じてきめ細かなアクセスコントロールが可能になります。このセキュリティアプローチは、テーブルの操作前に AWS Identity and Access Management (IAM) アクセス許可に加えて、IAM プリンシパルにテーブルに対する Lake Formation 許可を付与する必要があることを意味します。

AWS Lake Formation には、2 つの主な許可タイプがあります。

- メタデータに対するアクセス許可は、データカタログ内でメタデータデータベースとテーブルを作成、読み取り、更新、削除できるかどうかを制御します。
- 基になるデータに対するアクセス許可は、データカタログリソースの参照先となる Amazon S3 の場所にデータを読み書きできるかどうかを制御します。

Lake Formation では、独自のアクセス許可モデルと IAM アクセス許可モデルを組み合わせて使用して、データカタログリソースと基になるデータへのアクセスを制御します。

- データカタログリソースまたは基になるデータへのアクセスリクエストが成功するには、そのリクエストが IAM と Lake Formation の両方によるアクセス許可のチェックに合格する必要があります。

- IAM アクセス許可は Lake Formation へのアクセス、AWS Glue の API とリソースへのアクセスを制御し、Lake Formation 許可はデータカタログリソース、Amazon S3 ロケーション、基になるデータへのアクセスを制御します。

Lake Formation 許可は付与されたリージョン内でのみ適用されます。プリンシパルが Lake Formation 許可を付与されるには、データレイク管理者または必要なアクセス許可を持つ別のプリンシパルによって認可される必要があります。

詳細については、AWS Lake Formation デベロッパーガイドの「Lake Formation 許可の概要」を参照してください。

「the section called “統合の前提条件”」と「the section called “テーブルバケットと AWS 分析サービスの統合”」のステップに従って、AWS Glue Data Catalog とテーブルリソースにアクセスし、AWS 分析サービスを操作するための適切なアクセス許可があることを確認してください。

> **Important**
>
> アカウントで AWS 分析サービスとテーブルバケットの統合を実行したユーザーでない場合は、テーブルに対する必要な Lake Formation 許可が付与されている必要があります。詳細については、「the section called “テーブルまたはデータベースに対するアクセス許可の付与”」を参照してください。

統合の前提条件

テーブルバケットを AWS 分析サービスと統合するには、次の前提条件が必要です。

- テーブルバケットを作成します。
- AWSLakeFormationDataAdmin AWS マネージドポリシーを AWS Identity and Access Management (IAM) プリンシパルにアタッチして、そのユーザーをデータレイク管理者にします。データレイク管理者の作成方法の詳細については、「AWS Lake Formation デベロッパーガイド」の「データレイク管理者を作成する」を参照してください。
- `glue:PassConnection` オペレーションのアクセス許可を IAM プリンシパルに追加します。
- `lakeformation:RegisterResource` および `lakeformation:RegisterResourceWithPrivilegedAccess` オペレーションに対するアクセス許可を IAM プリンシパルに追加します。
- AWS Command Line Interface (AWS CLI) を最新バージョンに更新します。

> **Important**
>
> テーブルを作成するときは、テーブル名とテーブル定義にすべて小文字を使用してください。例えば、列名がすべて小文字であることを確認します。テーブル名またはテーブル定義に大文字が含まれている場合、テーブルは AWS Lake Formation または AWS Glue Data Catalog ではサポートされていません。この場合、テーブルバケットが AWS 分析サービスと統合されていても、テーブルは Amazon Athena などの AWS 分析サービスに表示されません。
>
> テーブル定義に大文字が含まれている場合、Athena で SELECT クエリを実行すると、次のエラーメッセージが表示されます。「GENERIC_INTERNAL_ERROR: Get table request failed: com.amazonaws.services.glue.model.ValidationException: Unsupported Federation Resource - Invalid table or column names.」

テーブルバケットと AWS 分析サービスの統合

この統合は、AWS リージョンごとに 1 回行う必要があります。

> **Important**
>
> AWS 分析サービス統合では、`WithPrivilegedAccess` Lake Formation API オペレーションの `registerResource` オプションを使用して S3 テーブルバケットを登録するようになりました。この統合により、`CreateCatalog` AWS Glue API オペレーションの `AllowFullTableExternalDataAccess` オプションを使用して AWS Glue Data Catalog に `s3tablescatalog` カタログが作成されるようにもなりました。
>
> プレビューリリースで統合を設定した場合は、現在の統合を引き続き使用できます。ただし、更新された統合プロセスではパフォーマンスが向上しているため、移行することをお勧めします。更新された統合に移行するには、「the section called “更新された統合プロセスへの移行”」を参照してください。

S3 コンソールの使用

1. Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 左側のナビゲーションペインで、[テーブルバケット] を選択します。
3. [テーブルバケットを作成] を選択します。

   [テーブルバケットを作成] ページが開きます。

4. テーブルバケット名を入力します。[統合を有効にする] チェックボックスがオンになっていることを確認してください。
5. [テーブルバケットを作成] を選択します。Amazon S3 は、そのリージョンでテーブルバケットを自動的に統合しようとします。

任意のリージョンのテーブルバケットを初めて統合すると、Amazon S3 はユーザーに代わって新しい IAM サービスロールを作成します。このロールにより、Lake Formation はアカウント内のすべてのテーブルバケットにアクセスし、AWS Glue Data Catalog のテーブルへのフェデレーションアクセスが可能になります。

AWS CLI を使用する場合

AWS CLI を使用してテーブルバケットを統合するには

以下の手順は、AWS CLI を使用してテーブルバケットを統合する方法を示しています。これらの手順を使用するには、*user input placeholders* を実際の情報に置き換えます。

1. テーブルバケットを作成します。

```
aws s3tables create-table-bucket \
--region us-east-1 \
--name amzn-s3-demo-table-bucket
```

2. Lake Formation がテーブルリソースにアクセスできるようにする IAM サービスロールを作成します。

   a. 次の信頼ポリシーを含むファイルを Role-Trust-Policy.json という名前で作成します。

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Sid": "LakeFormationDataAccessPolicy",
        "Effect": "Allow",
        "Principal": {
          "Service": "lakeformation.amazonaws.com"
        },
        "Action": [
            "sts:AssumeRole",
            "sts:SetContext",
```

```
            "sts:SetSourceIdentity"
        ],
        "Condition": {
          "StringEquals": {
            "aws:SourceAccount": "111122223333"
          }
        }
      }
    ]
}
```

次のコマンドを使用して IAM サービスロールを作成します。

```
aws iam create-role \
--role-name S3TablesRoleForLakeFormation \
--assume-role-policy-document file://Role-Trust-Policy.json
```

b. 次のポリシーを含むファイルを LF-GluePolicy.json という名前で作成します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "LakeFormationPermissionsForS3ListTableBucket",
            "Effect": "Allow",
            "Action": [
                "s3tables:ListTableBuckets"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "LakeFormationDataAccessPermissionsForS3TableBucket",
            "Effect": "Allow",
            "Action": [
                "s3tables:CreateTableBucket",
                "s3tables:GetTableBucket",
                "s3tables:CreateNamespace",
                "s3tables:GetNamespace",
                "s3tables:ListNamespaces",
                "s3tables:DeleteNamespace",
                "s3tables:DeleteTableBucket",
```

```
                "s3tables:CreateTable",
                "s3tables:DeleteTable",
                "s3tables:GetTable",
                "s3tables:ListTables",
                "s3tables:RenameTable",
                "s3tables:UpdateTableMetadataLocation",
                "s3tables:GetTableMetadataLocation",
                "s3tables:GetTableData",
                "s3tables:PutTableData"
            ],
            "Resource": [
                "arn:aws:s3tables:us-east-1:111122223333:bucket/*"
            ]
        }
    ]
}
```

次のコマンドを使用してポリシーをロールにアタッチします。

```
aws iam put-role-policy \
--role-name S3TablesRoleForLakeFormation  \
--policy-name LakeFormationDataAccessPermissionsForS3TableBucket \
--policy-document file://LF-GluePolicy.json
```

3. 以下を含むファイルを input.json という名前で作成します。

```
{
    "ResourceArn": "arn:aws:s3tables:us-east-1:111122223333:bucket/*",

    "WithFederation": true,
    "RoleArn": "arn:aws:iam::111122223333:role/S3TablesRoleForLakeFormation"
}
```

次のコマンドを使用してテーブルバケットを Lake Formation に登録します。

```
aws lakeformation register-resource \
--region us-east-1 \
--with-privileged-access \
--cli-input-json file://input.json
```

4. 次のカタログを含むファイルを catalog.json という名前で作成します。

```
{
   "Name": "s3tablescatalog",
   "CatalogInput": {
      "FederatedCatalog": {
          "Identifier": "arn:aws:s3tables:us-east-1:111122223333:bucket/*",
          "ConnectionName": "aws:s3tables"
       },
       "CreateDatabaseDefaultPermissions":[],
       "CreateTableDefaultPermissions":[],
       "AllowFullTableExternalDataAccess": "True"
   }
}
```

次のコマンドを使用して s3tablescatalog カタログを作成します。このカタログを作成すると、テーブルバケット、名前空間、テーブルに対応するオブジェクトが AWS Glue Data Catalog に入力されます。

```
aws glue create-catalog \
--region us-east-1 \
--cli-input-json file://catalog.json
```

5. 次のコマンドを使用して、s3tablescatalog カタログが AWS Glue に追加されたことを確認します。

```
aws glue get-catalog --catalog-id s3tablescatalog
```

更新された統合プロセスへの移行

AWS 分析サービス統合プロセスが更新されました。プレビューリリースで統合を設定した場合は、現在の統合を引き続き使用できます。ただし、更新された統合プロセスではパフォーマンスが向上しているため、以下の手順を使用して移行することをお勧めします。移行または統合プロセスの詳細については、「AWS Lake Formation デベロッパーガイド」の「AWS Glue Data Catalog での Amazon S3 Tables カタログの作成」を参照してください。

1. https://console.aws.amazon.com/lakeformation/ で AWS Lake Formation コンソールを開き、データレイク管理者としてサインインします。データレイク管理者の作成方法の詳細については、「AWS Lake Formation デベロッパーガイド」の「データレイク管理者を作成する」を参照してください。

2. 以下の手順で s3tablescatalog カタログを削除します。
   - 左側のナビゲーションペインで、[カタログ] を選択します。
   - [カタログ] リストで s3tablescatalog カタログの横にあるオプションボタンを選択します。Actions メニューで、Delete を選択します。
3. 以下の手順で s3tablescatalog カタログのデータロケーションの登録を解除します。
   - 左側のナビゲーションペインで、[管理] セクションに移動し、[データレイクのロケーション] を選択します。
   - s3tablescatalog データレイクロケーション (s3://tables:*region*:*account-id*:bucket/* など) の横にあるオプションボタンを選択します。
   - [アクション] メニューで、[削除] を選択します。
   - 表示される確認ダイアログボックスで、[削除] を選択します。
4. s3tablescatalog カタログとデータレイクロケーションを削除したので、更新された統合プロセスを使用して、テーブルバケットを AWS 分析サービスと統合する手順に従うことができます。

> **Note**
>
> 統合された AWS 分析サービスで SSE-KMS によって暗号化されたテーブルを使用する場合は、ユーザーが使用するロールに、暗号化オペレーションで AWS KMS キーを使用するアクセス許可が必要です。詳細については、「統合された AWS 分析サービスにおいて暗号化されたテーブルを使用するアクセス許可を IAM プリンシパルに付与する」を参照してください。

次のステップ

- 名前空間を作成します。.
- テーブルの作成.

テーブルの名前空間へのリソースリンクの作成 (Amazon Data Firehose)

テーブルにアクセスするには、Amazon Data Firehose でテーブルの名前空間をターゲットとするリソースリンクが必要です。リソースリンクは、データベースやテーブルなどの別のデータカタログリソースのエイリアスまたはポインタとして機能するデータカタログオブジェクトです。リンクは、作

成されたアカウントまたはリージョンのデータカタログに保存されます。詳細については、「AWS Lake Formation デベロッパーガイド」の「リソースリンクの仕組み」を参照してください。

テーブルバケットを AWS 分析サービスと統合した後、Amazon Data Firehose でテーブルを操作するためのリソースリンクを作成できます。これらのリンクの作成の詳細については、「the section called “Amazon Data Firehose”」を参照してください。

テーブルリソースに対する Lake Formation 許可の付与

テーブルバケットが AWS 分析サービスと統合された後、Lake Formation がテーブルリソースへのアクセスを管理します。Lake Formation は、データカタログリソースのきめ細かなアクセスコントロールを可能にする独自のアクセス許可モデル (Lake Formation 許可) を使用します。Lake Formation は、各 IAM プリンシパル (ユーザーまたはロール) に、Lake Formation が管理するリソースに対してアクションを実行する権限があることを必要とします。詳細については、AWS Lake Formation デベロッパーガイドの「Lake Formation 許可の概要」を参照してください。クロスアカウントデータ共有の詳細については、「AWS Lake Formation デベロッパーガイド」の「Lake Formation でのクロスアカウントデータ共有」を参照してください。

IAM プリンシパルが AWS 分析サービスのテーブルにアクセスする前に、それらのリソースに対する Lake Formation 許可を付与する必要があります。

> **Note**
>
> テーブルバケット統合を実行したユーザーである場合は、テーブルに対する Lake Formation 許可が既に付与されています。テーブルにアクセスする唯一のプリンシパルである場合は、このステップをスキップできます。テーブルに対する Lake Formation 許可を他の IAM プリンシパルに付与するだけで済みます。これにより、クエリを実行するときに他のプリンシパルがテーブルにアクセスできるようになります。詳細については、「テーブルまたはデータベースに対するアクセス許可の付与」を参照してください。

次のサービスでテーブルリソースを他の IAM プリンシパルが操作できるようにするには、テーブルリソースに対する Lake Formation 許可をそれらのプリンシパルに付与する必要があります。

- Amazon Redshift
- Amazon Data Firehose
- Amazon QuickSight
- Amazon Athena

テーブルまたはデータベースに対するアクセス許可の付与

Lake Formation コンソールまたは AWS CLI を通じて、テーブルバケット内のテーブルまたはデータベースに対する Lake Formation 許可をプリンシパルに付与できます。

> **Note**
>
> データカタログリソースに対する Lake Formation のアクセス許可を外部アカウントに付与するか、または別のアカウントの IAM プリンシパルに直接付与する場合、Lake Formation は AWS Resource Access Manager (AWS RAM) サービスを使用してリソースを共有します。付与対象アカウントが付与する側のアカウントと同じ組織内にある場合、付与対象アカウントはその共有リソースをただちに使用できるようになります。付与対象アカウントが同じ組織内にない場合は、AWS RAM が付与対象アカウントに対して、リソース付与を受け入れる、または拒否するための招待を送信します。その後、共有リソースを利用可能にするために、付与対象アカウントのデータレイク管理者が AWS RAM コンソールまたは AWS CLI を使用して招待を承諾する必要があります。クロスアカウントデータ共有の詳細については、「AWS Lake Formation デベロッパーガイド」の「Lake Formation でのクロスアカウントデータ共有」を参照してください。

Console

1. https://console.aws.amazon.com/lakeformation/ で AWS Lake Formation コンソールを開き、データレイク管理者としてサインインします。データレイク管理者の作成方法の詳細については、「AWS Lake Formation デベロッパーガイド」の「データレイク管理者を作成する」を参照してください。
2. ナビゲーションペインで、[データアクセス許可]、[付与] の順に選択します。
3. [アクセス許可の付与] ページの [プリンシパル] で、次のいずれかを実行します。
   - Amazon Athena または Amazon Redshift の場合は、[IAM ユーザーとロール] を選択し、さらにクエリに使用する IAM プリンシパルを選択します。
   - Amazon Data Firehose の場合は、[IAM ユーザーとロール] を選択した後、テーブルへのストリーミング用に作成したサービスロールを選択します。
   - QuickSight の場合は、[SAML ユーザーとグループ] を選択し、QuickSight 管理者ユーザーの Amazon リソースネーム (ARN) を入力します。
4. [LF タグまたはカタログリソース] で、[名前付きのデータカタログリソース] を選択します。

5. [カタログ] で、テーブルバケットを統合したときに作成したサブカタログ (*account-id*:s3tablescatalog/*amzn-s3-demo-bucket* など) を選択します。
6. [データベース] で、作成した S3 テーブルバケット名前空間を選択します。
7. (オプション) [テーブル] で、テーブルバケットに作成した S3 テーブルを選択します。

> **Note**
>
> Athena クエリエディタで新しいテーブルを作成する場合は、テーブルを選択しないでください。

8. 次のいずれかを行います：
   - 前のステップでテーブルを指定した場合は、[テーブルのアクセス許可] で [Super] を選択します。
   - 前のステップでテーブルを指定しなかった場合は、[データベースのアクセス許可] に進みます。クロスアカウントデータ共有の場合は、[Super] を選択して、データベースに対するすべてのアクセス許可を他のプリンシパルに付与することはできません。代わりに、[Describe] などのよりきめ細かなアクセス許可を選択します。
9. [Grant] (付与) を選択します。

CLI

1. 次の AWS CLI コマンドをデータレイク管理者として実行していることを確認してください。詳細については、「AWS Lake Formation デベロッパーガイド」の「データレイク管理者を作成する」を参照してください。
2. 次のコマンドを実行して、S3 テーブルバケットのテーブルに対する Lake Formation 許可を IAM プリンシパルに付与し、テーブルにアクセスします。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws lakeformation grant-permissions \
--region us-east-1 \
--cli-input-json \
'{
    "Principal": {
        "DataLakePrincipalIdentifier": "user or role ARN, for example,
 arn:aws:iam::account-id:role/example-role"
    },
    "Resource": {
```

```
        "Table": {
            "CatalogId": "account-id:s3tablescatalog/amzn-s3-demo-bucket",
            "DatabaseName": "S3 table bucket namespace, for example,
 test_namespace",
            "Name": "S3 table bucket table name, for example test_table"
        }
    },
    "Permissions": [
        "ALL"
    ]
}'
```

AWS Glue Iceberg REST エンドポイントを使用した Amazon S3 テーブルへのアクセス

S3 テーブルバケットが AWS Glue Data Catalog と統合されると、PyIceberg や Spark などの Apache Iceberg 互換クライアントから S3 テーブルに接続するために AWS Glue Iceberg REST エンドポイントを使用できます。AWS Glue Iceberg REST エンドポイントは、Iceberg テーブルを操作するための標準化されたインターフェイスを提供する Iceberg REST Catalog Open API 仕様を実装しています。エンドポイントを使用して S3 テーブルにアクセスするには、IAM ポリシーと AWS Lake Formation 許可を組み合わせてアクセス許可を設定する必要があります。以降のセクションでは、アクセスの設定方法、具体的には、必要な IAM ロールの作成、必要なポリシーの定義、データベースレベルとテーブルレベルの両方のアクセスに対する Lake Formation 許可の設定などについて説明します。

PyIceberg を使用したエンドツーエンドのチュートリアルについては、「AWS Glue Iceberg REST エンドポイントを通じて PyIceberg により Amazon S3 Tables のデータにアクセスする」を参照してください。

前提条件

- テーブルバケットを AWS 分析サービスと統合する
- テーブル名前空間を作成する
- データレイク管理者アカウントへのアクセス権を取得する

クライアント用の IAM ロールを作成する

AWS Glue エンドポイントを通じてテーブルにアクセスするには、AWS Glue および Lake Formation アクションに対するアクセス許可を付与した IAM ロールを作成する必要があります。この手順では、このロールを作成し、そのアクセス許可を設定する方法について説明します。

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. 左のナビゲーションペインの [ポリシー] を選択します。
3. [ポリシーを作成] を選択し、ポリシーエディタで [JSON] を選択します。
4. AWS Glue および Lake Formation アクションへのアクセス許可を付与する次のインラインポリシーを追加します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "glue:GetCatalog",
                "glue:GetDatabase",
                "glue:GetDatabases",
                "glue:GetTable",
                "glue:GetTables",
                "glue:CreateTable",
                "glue:UpdateTable"
            ],
            "Resource": [
                "arn:aws:glue:<region>:<account-id>:catalog",
                "arn:aws:glue:<region>:<account-id>:catalog/s3tablescatalog",
                "arn:aws:glue:<region>:<account-id>:catalog/
s3tablescatalog/<s3_table_bucket_name>",
                "arn:aws:glue:<region>:<account-id>:table/
s3tablescatalog/<s3_table_bucket_name>/<namespace>/*",
                "arn:aws:glue:<region>:<account-id>:database/
s3tablescatalog/<s3_table_bucket_name>/<namespace>"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
```

```
                "lakeformation:GetDataAccess"
            ],
            "Resource": "*"
        }
    ]
}
```

5. ポリシーを作成したら、IAM ロールを作成し、[信頼されたエンティティタイプ] として [カスタム信頼ポリシー] を選択します。
6. [カスタム信頼ポリシー] に以下を入力します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::<accountid>:role/<Admin_role>"
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```

Lake Formation でアクセスを定義する

Lake Formation は、データレイクテーブルに対するきめ細かなアクセスコントロールを提供します。S3 バケットを AWS Glue Data Catalog と統合すると、テーブルは Lake Formation のリソースとして自動的に登録されます。これらのテーブルにアクセスするには、IAM ポリシーのアクセス許可に加えて、特定の Lake Formation 許可を IAM アイデンティティに付与する必要があります。

以下の手順では、Lake Formation のアクセスコントロールを適用して、Iceberg クライアントがテーブルに接続できるようにする方法について説明します。これらのアクセス許可を適用するには、データレイク管理者としてサインインする必要があります。

外部エンジンによるテーブルデータへのアクセスを許可する

Lake Formation では、外部エンジンがデータにアクセスできるように、テーブルへのフルアクセスを有効にする必要があります。これにより、サードパーティーアプリケーションは、リクエストされ

たテーブルに対するフルアクセス許可を付与した IAM ロールを使用する際に、Lake Formation から一時的な認証情報を取得できます。

Lake Formation コンソール (https://console.aws.amazon.com/lakeformation/) を開きます。

1. Lake Formation コンソール (https://console.aws.amazon.com/lakeformation/) を開き、データレイク管理者としてサインインします。
2. ナビゲーションペインの [管理] で、[アプリケーションの統合設定] を選択します。
3. [外部エンジンに、Amazon S3 ロケーション内のデータに対するフルアクセス許可を付与する] を選択します。次に、[保存] を選択します。

テーブルリソースに対する Lake Formation 許可の付与

次に、Iceberg 互換クライアント用に作成した IAM ロールに Lake Formation アクセス許可を付与します。これらのアクセス許可により、ロールは名前空間にテーブルを作成して管理できます。データベースレベルとテーブルレベルの両方のアクセス許可を付与する必要があります。

データベースに対するアクセス許可を付与するには

1. AWS Lake Formation コンソール (https://console.aws.amazon.com/lakeformation/) を開き、データレイク管理者としてサインインします。
2. ナビゲーションペインで、[データアクセス許可]、[付与] の順に選択します。
3. [アクセス許可の付与] ページの [プリンシパル] で、[IAM ユーザーとロール] を選択し、AWS Glue Iceberg REST endpoint アクセス用に作成した IAM ロールを選択します。
4. [LF タグまたはカタログリソース] で、[名前付きのデータカタログリソース] を選択します。
5. [カタログ] で、テーブルバケット用に作成した AWS Glue データカタログを選択します。例えば、`<accoundID>:s3tablescatalog/<table-bucket-name>`。
6. [Database] (データベース) には `mynamespace` を選択します。
7. [テーブルのアクセス許可] で、[テーブルを作成] と [説明] を選択します。
8. [Grant] (付与) を選択します。

テーブルに対するアクセス許可を付与するには

1. AWS Lake Formation コンソール (https://console.aws.amazon.com/lakeformation/) を開き、データレイク管理者としてサインインします。
2. ナビゲーションペインで、[データアクセス許可]、[付与] の順に選択します。

3. [アクセス許可の付与] ページの [プリンシパル] で、[IAM ユーザーとロール] を選択し、AWS Glue Iceberg REST endpoint アクセス用に作成した IAM ロールを選択します。
4. [LF タグまたはカタログリソース] で、[名前付きのデータカタログリソース] を選択します。
5. [カタログ] で、テーブルバケット用に作成した AWS Glue データカタログを選択します。例えば、*<accoundID>*:s3tablescatalog/*<table-bucket-name>*。
6. [データベース] で、作成した S3 テーブルバケット名前空間を選択します。
7. [テーブル]で、[ALL_TABLES] を選択します。
8. [テーブルアクセス許可] で、[Super] を選択します。
9. [Grant] (付与) を選択します。

エンドポイントを使用するための環境を設定する

テーブルへのアクセスに必要な許可を付与した IAM ロールを設定した後、次のコマンドを使用して、AWS CLI をそのロールで設定することで、ローカルマシンから Iceberg クライアントを実行できます。

```
aws sts assume-role --role-arn "arn:aws:iam::<accountid>:role/<glue-irc-role>" --role-session-name <glue-irc-role>
```

AWS Glue REST エンドポイントを通じてテーブルにアクセスするには、Iceberg 互換クライアントでカタログを初期化する必要があります。この初期化では、sigv4 プロパティ、エンドポイント URI、ウェアハウスの場所などのカスタムプロパティを指定する必要があります。これらのプロパティを次のように指定します。

- Sigv4 プロパティ – Sigv4 を有効にする必要があります。署名は glue です。
- ウェアハウスの場所 - テーブルバケットです。次の形式で指定します: *<accountid>*:s3tablescatalog/*<table-bucket-name>*
- エンドポイント URI - リージョン固有のエンドポイントについては、「AWS Glue サービスエンドポイントのリファレンスガイド」を参照してください。

次の例では、pyIceberg カタログを初期化する方法を示しています。

```
rest_catalog = load_catalog(
        s3tablescatalog,
**{
"type": "rest",
```

```
"warehouse": "<accountid>:s3tablescatalog/<table-bucket-name>",
"uri": "https://glue.<region>.amazonaws.com/iceberg",
"rest.sigv4-enabled": "true",
"rest.signing-name": "glue",
"rest.signing-region": region
        }
)
```

AWS GlueIceberg REST エンドポイントの実装の詳細については、「AWS Glue ユーザーガイド」の「AWS Glue Iceberg REST エンドポイントを使用したデータカタログへの接続」を参照してください。

Amazon S3 Tables Iceberg REST エンドポイントを使用したテーブルへのアクセス

Iceberg REST クライアントを Amazon S3 Tables Iceberg REST エンドポイントに接続し、REST API コールを行って、S3 テーブルバケット内のテーブルの作成、更新、またはテーブルに対するクエリの実行ができます。エンドポイントは、Apache Iceberg REST Catalog Open API 仕様で指定された標準化された Iceberg REST API のセットを実装しています。エンドポイントは、Iceberg REST API オペレーションを対応する S3 Tables オペレーションに変換することで機能します。

> **Note**
>
> Amazon S3 Tables Iceberg REST エンドポイントは、AWS Partner Network (APN) カタログ実装またはカスタムカタログ実装のテーブルにアクセスするために使用できます。1 つのテーブルバケットへの基本的な読み取り/書き込みアクセスのみが必要な場合にも使用できます。その他のアクセスシナリオでは、AWS Glue Iceberg REST エンドポイントを使用してテーブルに接続することをお勧めします。これにより、統合されたテーブル管理、一元化されたガバナンス、きめ細かなアクセスコントロールが可能になります。詳細については、「AWS Glue Iceberg REST エンドポイントを使用した Amazon S3 テーブルへのアクセス」を参照してください。

エンドポイントの設定

サービスエンドポイントを使用して Amazon S3 Tables Iceberg REST エンドポイントに接続します。S3 Tables Iceberg REST エンドポイントの形式を次に示します。

```
https://s3tables.<REGION>.amazonaws.com/iceberg
```

リージョン固有のエンドポイントについては、「S3 Tables AWS リージョンとエンドポイント」を参照してください。

カタログ設定プロパティ

Iceberg クライアントを使用して分析エンジンをサービスエンドポイントに接続する場合は、カタログを初期化するときに次の設定プロパティを指定する必要があります。`##########`を実際のリージョンとテーブルバケットの情報に置き換えます。

- エンドポイント URI としてのリージョン固有のエンドポイント: `https://s3tables.<REGION>.amazonaws.com/iceberg`
- ウェアハウスの場所としてのテーブルバケット ARN: `arn:aws:s3tables:<region>:<accountID>:bucket/<bucketname>`
- 認証用の Sigv4 プロパティ。サービスエンドポイントリクエスト用の SigV4 署名: `s3tables`

次の例では、Amazon S3 Tables Iceberg REST エンドポイントを使用するようにさまざまなクライアントを設定する方法を示しています。

PyIceberg

Amazon S3 Tables Iceberg REST エンドポイントを PyIceberg で使用するには、次のアプリケーション設定プロパティを指定します。

```
rest_catalog = load_catalog(
  catalog_name,
  **{
    "type": "rest",
    "warehouse":"arn:aws:s3tables:<Region>:<accountID>:bucket/<bucketname>",
    "uri": "https://s3tables.<Region>.amazonaws.com/iceberg",
    "rest.sigv4-enabled": "true",
    "rest.signing-name": "s3tables",
    "rest.signing-region": "<Region>"
  }
)
```

Apache Spark

Amazon S3 Tables Iceberg REST エンドポイントを Spark で使用するには、次のアプリケーション設定プロパティを指定し、`##########`を実際のリージョンとテーブルバケットの情報に置き換えます。

```
spark-shell \
  --packages "org.apache.iceberg:iceberg-spark-
runtime-3.5_2.12:1.4.1,software.amazon.awssdk:bundle:2.20.160,software.amazon.awssdk:url-
connection-client:2.20.160" \
  --master "local[*]" \
  --conf
 "spark.sql.extensions=org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions"
 \
  --conf "spark.sql.defaultCatalog=spark_catalog" \
   --conf "spark.sql.catalog.spark_catalog=org.apache.iceberg.spark.SparkCatalog" \
  --conf "spark.sql.catalog.spark_catalog.type=rest" \
  --conf "spark.sql.catalog.spark_catalog.uri=https://
s3tables.<Region>.amazonaws.com/iceberg" \
  --conf
 "spark.sql.catalog.spark_catalog.warehouse=arn:aws:s3tables:<Region>:<accountID>:bucket/
<bucketname>" \
  --conf "spark.sql.catalog.spark_catalog.rest.sigv4-enabled=true" \
  --conf "spark.sql.catalog.spark_catalog.rest.signing-name=s3tables" \
  --conf "spark.sql.catalog.spark_catalog.rest.signing-region=<Region>" \
  --conf "spark.sql.catalog.spark_catalog.io-
impl=org.apache.iceberg.aws.s3.S3FileIO" \
  --conf
 "spark.hadoop.fs.s3a.aws.credentials.provider=org.apache.hadoop.fs.s3a.SimpleAWSCredentialP
 \
  --conf "spark.sql.catalog.spark_catalog.rest-metrics-reporting-enabled=false"
```

エンドポイントへのアクセスの認証と承認

S3 Tables サービスエンドポイントへの API リクエストは、AWS Signature Version 4 (SigV4) を使用して認証されます。AWS SigV4 の詳細については、「API リクエストに対する AWS Signature Version 4」を参照してください。

Amazon S3 Tables Iceberg REST エンドポイントリクエストの SigV4 署名: `s3tables`

Amazon S3 Tables Iceberg REST エンドポイントへのリクエストは、REST API オペレーションに対応する `s3tables` IAM アクションを使用して承認されます。これらのアクセス許可は、IAM アイデンティティベースのポリシー、またはテーブルとテーブルバケットにアタッチされたリソースベースのポリシーのいずれかで定義できます。詳細については、「S3 Tables のアクセス管理」を参照してください。

AWS CloudTrail を使用して、REST エンドポイントを通じてテーブルに行われたリクエストを追跡できます。リクエストは、対応する S3 IAM アクションとしてログに記録されます。例えば、LoadTable API により GetTableMetadataLocation オペレーションに対して管理イベントが発生し、GetTableData オペレーションに対してデータイベントが発生します。詳細については、「S3 Tablesの AWS CloudTrail を使用したログ記録」を参照してください。

プレフィックスとパスのパラメータ

Iceberg REST Catalog API のリクエスト URL には、自由形式のプレフィックスが含まれます。例えば、ListNamespaces API コールでは GET/v1/{prefix}/namespaces URL 形式が使用されます。S3 Tables では、REST パス {prefix} は常に URL エンコードされたテーブルバケット ARN です。

例えば、テーブルバケット ARN が arn:aws:s3tables:*us-east-1*:111122223333:bucket/*bucketname* の場合、プレフィックスは arn%3Aaws%3As3tables%3A*us-east-1*%3A*111122223333*%3Abucket%2F*bucketname* となります。

名前空間パスパラメータ

Iceberg REST カタログ API パスの名前空間には、複数のレベルを含めることができます。ただし、S3 Tables は単一レベルの名前空間のみをサポートしています。複数レベルカタログ階層の名前空間にアクセスするには、名前空間を参照するときに、名前空間の上位にある複数レベルカタログに接続できます。これにより、catalog.namespace.table の 3 つの部分で構成される表記をサポートするクエリエンジンが S3 Tables のカタログ階層内のオブジェクトにアクセスできます。複数レベルの名前空間を使用する場合とは異なり、互換性の問題はありません。

サポートされている Iceberg REST API オペレーション

次の表では、サポートされている Iceberg REST API とそれらが S3 テーブルアクションにどのように対応するかを示しています。

Iceberg REST オペレーション	REST パス	S3 Tables IAM アクション	CloudTrail EventName
getConfig	GET /v1/config	s3tables:GetTableBucket	s3tables:GetTableBucket
listNamespaces	GET /v1/{prefix}/namespaces	s3tables:ListNamespaces	s3tables:ListNamespaces

Iceberg REST オペレーション	REST パス	S3 Tables IAM アクション	CloudTrail EventName
createNamespace	POST /v1/{prefix}/namespaces	s3tables:CreateNamespace	s3tables:CreateNamespace
loadNamespaceMetadata	GET /v1/{prefix}/namespaces/{namespace}	s3tables:GetNamespace	s3tables:GetNamespace
dropNamespace	DELETE /v1/{prefix}/namespaces/{namespace}	s3tables:DeleteNamespace	s3tables:DeleteNamespace
listTables	GET /v1/{prefix}/namespaces/{namespace}/tables	s3tables:ListTables	s3tables:ListTables
createTable	POST /v1/{prefix}/namespaces/{namespace}/tables	s3tables:CreateTable , s3tables:PutTableData	s3tables:CreateTable , s3tables:PutObject
loadTable	GET /v1/{prefix}/namespaces/{namespace}/tables/{table}	s3tables:GetTableMetadataLocation , s3tables:GetTableData	s3tables:GetTableMetadataLocation , s3tables:GetObject

Iceberg REST オペレーション	REST パス	S3 Tables IAM アクション	CloudTrail EventName
updateTable	POST /v1/{prefix}/namespaces/{namespace}/tables/{table}	s3tables:UpdateTableMetadataLocation , s3tables:PutTableData , s3tables:GetTableData	s3tables:UpdateTableMetadataLocation , s3tables:PutObject , s3tables:GetObject
dropTable	DELETE /v1/{prefix}/namespaces/{namespace}/tables/{table}	s3tables:DeleteTable	s3tables:DeleteTable
renameTable	POST /v1/{prefix}/tables/rename	s3tables:RenameTable	s3tables:RenameTable
tableExists	HEAD /v1/{prefix}/namespaces/{namespace}/tables/{table}	s3tables:GetTable	s3tables:GetTable
namespaceExists	HEAD /v1/{prefix}/namespaces/{namespace}	s3tables:GetNamespace	s3tables:GetNamespace

考慮事項と制限事項

Amazon S3 Tables Iceberg REST エンドポイントを使用する際の考慮事項と制限事項を次に示します。

考慮事項

- CreateTable API の動作 – このオペレーションでは `stage-create` オプションはサポートされておらず、`400 Bad Request` エラーが発生します。これは、`CREATE TABLE AS SELECT` (CTAS) を使用してクエリ結果からテーブルを作成できないことを意味します。
- DeleteTable API の動作 – パージが有効になっているテーブルのみを削除できます。`purge=false` を使用したテーブルの削除はサポートされておらず、`400 Bad Request` エラーが発生します。Spark の一部のバージョンでは、`DROP TABLE PURGE` コマンドの実行時でも常にこのフラグが false に設定されます。`DROP TABLE PURGE` を試すか、S3 Tables の DeleteTable オペレーションを使用してテーブルを削除できます。
- エンドポイントは標準のテーブルメタデータオペレーションのみをサポートしています。スナップショット管理や圧縮などのテーブルメンテナンスには、S3 Tables のメンテナンス API オペレーションを使用します。詳細については、「S3 Tables のメンテナンス」を参照してください。

制約事項

- 複数レベルの名前空間はサポートされていません。
- OAuth ベースの認証はサポートされていません。
- 名前空間では `owner` プロパティのみがサポートされています。
- Apache Iceberg REST Open API 仕様で定義されているビュー関連の API はサポートされていません。
- 5 MB を超える `metadata.json` ファイルを使用してテーブルに対してオペレーションを実行することはサポートされておらず、`400 Bad Request` エラーが返されます。`metadata.json` ファイルのサイズを制御するには、テーブルメンテナンスオペレーションを使用します。詳細については、「S3 Tables のメンテナンス」を参照してください。

Amazon S3 Tables Catalog for Apache Iceberg を使用した Amazon S3 テーブルへのアクセス

Amazon S3 Tables Catalog for Apache Spark クライアントカタログを使用して、Apache Iceberg のようなオープンソースクエリエンジンから S3 テーブルにアクセスできます。Amazon S3 Tables Catalog for Apache Iceberg は、AWS Labs がホストするオープンソースライブラリです。これは、クエリエンジン内の Apache Iceberg オペレーション (テーブル検出、メタデータの更新、テーブルの追加または削除など) を S3 Tables API オペレーションに変換することで機能します。

Amazon S3 Tables Catalog for Apache Iceberg は、`s3-tables-catalog-for-iceberg.jar` という Maven JAR として配布されています。クライアントカタログ JAR は、AWS Labs GitHub リポジトリから構築するか、Maven からダウンロードできます。テーブルに接続する際、Apache Iceberg 用の Spark セッションを初期化するときに、クライアントカタログ JAR が依存関係として使用されます。

Apache Spark での Amazon S3 Tables Catalog for Apache Iceberg の使用

Spark セッションを初期化するときに、Amazon S3 Tables Catalog for Apache Iceberg クライアントカタログを使用して、オープンソースアプリケーションからテーブルに接続できます。セッション設定で Iceberg と Amazon S3 の依存関係を指定し、テーブルバケットをメタデータウェアハウスとして使用するカスタムカタログを作成します。

前提条件

- テーブルバケットと S3 Tables アクションへのアクセス権を持つ IAM ID。詳細については、「S3 Tables のアクセス管理」を参照してください。

Amazon S3 Tables Catalog for Apache Iceberg を使用して Spark セッションを初期化するには

- 次のコマンドを使用して Spark を初期化します。コマンドを使用するには、Amazon S3 Tables Catalog for Apache Iceberg の*#######*を AWS Labs GitHub リポジトリの最新バージョンに置き換え、*######## ARN* を実際のテーブルバケット ARN に置き換えます。

```
spark-shell \
--packages org.apache.iceberg:iceberg-spark-
runtime-3.5_2.12:1.6.1,software.amazon.s3tables:s3-tables-catalog-for-iceberg-
runtime:0.1.4 \
--conf spark.sql.catalog.s3tablesbucket=org.apache.iceberg.spark.SparkCatalog \
--conf spark.sql.catalog.s3tablesbucket.catalog-
impl=software.amazon.s3tables.iceberg.S3TablesCatalog \
--conf spark.sql.catalog.s3tablesbucket.warehouse=arn:aws:s3tables:us-
east-1:111122223333:bucket/amzn-s3-demo-table-bucket \
--conf
 spark.sql.extensions=org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions
```

Spark SQL を使用した S3 テーブルのクエリ

Spark を使用すると、S3 テーブルで DQL、DML、DDL オペレーションを実行できます。テーブルをクエリするときは、セッションカタログ名を含む完全修飾テーブル名を次のパターンに従って使用します。

CatalogName.*NamespaceName*.*TableName*

次のクエリ例は、S3 テーブルを操作するいくつかの方法を示しています。クエリエンジンでこれらのサンプルクエリを使用するには、*###############*値を実際の値に置き換えます。

Spark を使用してテーブルをクエリするには

- 名前空間を作成します。

```
spark.sql(" CREATE NAMESPACE IF NOT EXISTS s3tablesbucket.my_namespace")
```

- テーブルの作成

```
spark.sql(" CREATE TABLE IF NOT EXISTS s3tablesbucket.my_namespace.`my_table`
( id INT, name STRING, value INT ) USING iceberg ")
```

- テーブルに対してクエリを実行する

```
spark.sql(" SELECT * FROM s3tablesbucket.my_namespace.`my_table` ").show()
```

- テーブルにデータを挿入する

```
spark.sql(
"""
    INSERT INTO s3tablesbucket.my_namespace.my_table
    VALUES
        (1, 'ABC', 100),
        (2, 'XYZ', 200)
""")
```

- テーブルに既存のデータファイルをロードする

  1. データを Spark に読み取ります。

```
val data_file_location = "Path such as S3 URI to data file"
val data_file = spark.read.parquet(data_file_location)
```

2. データを Iceberg テーブルに書き込みます。

```
data_file.writeTo("s3tablesbucket.my_namespace.my_table").using("Iceberg").tableProperty
 ("format-version", "2").createOrReplace()
```

Athena を使用した Amazon S3 テーブルのクエリ

Amazon Athena はインタラクティブなクエリサービスで、Amazon S3 内のデータを標準 SQL を使用して直接分析できます。詳細については、「Amazon Athena ユーザーガイド」の「Amazon Athena とは」を参照してください。

テーブルバケットを AWS 分析サービスと統合した後、Athena で S3 テーブルに対してデータ定義言語 (DDL)、データ操作言語 (DML)、データクエリ言語 (DQL) クエリを実行できます。テーブルバケット内のテーブルに対するクエリの実行方法の詳細については、「Amazon Athena ユーザーガイド」の「S3 テーブルバケットカタログを登録する」を参照してください。

Amazon S3 コンソールから Athena でクエリを実行することもできます。

S3 コンソールと Amazon Athena の使用

以下の手順では、Amazon S3 コンソールを使用して Athena クエリエディタにアクセスし、Amazon Athena でテーブルに対してクエリを実行できるようにします。

> **Note**
>
> 以下の手順を実行する前に、このリージョンでテーブルバケットを AWS 分析サービスと統合していることを確認してください。詳細については、「the section called “AWS 分析サービスで S3 Tables を使用する”」を参照してください。

テーブルに対してクエリを実行するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[テーブルバケット] を選択します。
3. [テーブルバケット] ページで、クエリを実行するテーブルを含むバケットを選択します。
4. バケットの詳細ページで、クエリを実行するテーブルの名前の横にあるオプションボタンを選択します。

5. [Athena でテーブルに対してクエリを実行] を選択します。
6. Amazon Athena コンソールが開き、サンプル SELECT クエリがロードされた状態で Athena クエリエディタが表示されます。必要に応じて、このクエリをユースケースに合わせて変更します。

   クエリエディタで、[カタログ] フィールドに s3tablescatalog/ に続いてテーブルバケットの名前を入力します。例えば、s3tablescatalog/***amzn-s3-demo-bucket*** のようになります。[データベース] フィールドに、テーブルが保存されている名前空間を入力します。

   > **Note**
   >
   > [カタログ] および [データベース] フィールドにこれらの値が表示されない場合は、このリージョンでテーブルバケットを AWS 分析サービスと統合していることを確認してください。詳細については、「the section called “AWS 分析サービスで S3 Tables を使用する”」を参照してください。

7. クエリを実行するには、[Run] (実行) を選択します。

   > **Note**
   >
   > - クエリを実行するためのアクセス許可が不足しているという内容のエラーが表示された場合。Athena でクエリを実行しようとしたときに、プリンシパルは指定されたリソースに対する権限を持っていないという内容のエラーが表示される場合は、テーブルに対する必要な Lake Formation 許可が付与されている必要があります。詳細については、「the section called “テーブルまたはデータベースに対するアクセス許可の付与”」を参照してください。
   > - クエリを実行しようとしたときに、Iceberg はリクエストされたリソースにアクセスできないという内容のエラーが表示される場合は、AWS Lake Formation コンソールに移動し、作成したテーブルバケットカタログとデータベース (名前空間) に対するアクセス許可が自分に付与されていることを確認してください。これらのアクセス許可を付与するときは、テーブルを指定しないでください。詳細については、「the section called “テーブルまたはデータベースに対するアクセス許可の付与”」を参照してください。
   > - Athena で SELECT クエリを実行するときに次のエラーメッセージが表示される場合、このメッセージはテーブル名またはテーブル定義の列名に大文字が含まれていることが原因です。「GENERIC_INTERNAL_ERROR: Get table request failed: com.amazonaws.services.glue.model.ValidationException: Unsupported Federation

Resource - Invalid table or column names.」 テーブル名と列名がすべて小文字であることを確認します。

Amazon Redshift を使用した Amazon S3 テーブルへのアクセス

Amazon Redshift は、高速でフルマネージドのペタバイト規模のデータウェアハウスサービスで、既存のビジネスインテリジェンスツールを使用してすべてのデータを簡単かつコスト効率よく効率的に分析できます。Redshift Serverless を使用すると、プロビジョニングされたデータウェアハウスをすべて設定しなくても、データにアクセスして分析することができます。詳細については、「Amazon Redshift 入門ガイド」の「Amazon Redshift Serverless データウェアハウスの使用を開始」を参照してください。

Amazon Redshift で Amazon S3 テーブルをクエリする

前提条件

- テーブルバケットを AWS 分析サービスと統合します。
  - 名前空間を作成します。.
  - テーブルの作成.
- テーブルリソースに対する Lake Formation 許可の付与.

前提条件を完了したら、次のいずれかの方法で Amazon Redshift を使用してテーブルのクエリを開始できます。

- Amazon Redshift Query Editor V2 を使用する
- SQL クライアントツールを使用して Amazon Redshift データウェアハウスクラスターに接続する
- Amazon Redshift Data API の使用

Amazon EMR を使用した Amazon S3 テーブルへのアクセス

Amazon EMR (旧称 Amazon Elastic MapReduce) は、AWS でビッグデータフレームワーク (Apache Hadoop、Apache Spark、および Apache Spark など) の実行を簡素化して、ビッグデータを処理および分析するマネージドクラスタープラットフォームです。これらのフレームワークと、関連するオープンソースプロジェクトを使用することで、分析用のデータやビジネスインテリジェンスワーク

ロードを処理できます。Amazon EMR は、大量のデータを変換したり、他の AWS データストアやデータベースとの間で出し入れしたりできるようにします。

Amazon EMR の Apache Iceberg クラスターを使用して、Spark セッション内のテーブルバケットに接続することで S3 テーブルを操作できます。Amazon EMR のテーブルバケットに接続するには、AWS Glue Data Catalog を通じて AWS 分析サービスの統合を使用するか、オープンソースの Amazon S3 Tables Catalog for Apache Iceberg クライアントカタログを使用できます。

> **Note**
>
> S3 Tables は Amazon EMR バージョン 7.5 以降でサポートされています。

Amazon EMR Iceberg クラスターでの Spark を使用した S3 テーブルバケットへの接続

この手順では、Apache Iceberg 用に設定された Amazon EMR クラスターをセットアップし、テーブルバケットに接続する Spark セッションを起動します。AWS Glue を通じて AWS 分析サービス統合を使用して設定することも、オープンソースの Amazon S3 Tables Catalog for Apache Iceberg クライアントカタログを使用することもできます。クライアントの詳細については、「Amazon S3 Tables Iceberg REST エンドポイントを使用したテーブルへのアクセス」を参照してください。

次のオプションから、Amazon EMR でテーブルを使用する方法を選択します。

Amazon S3 Tables Catalog for Apache Iceberg

Amazon S3 Tables Catalog for Apache Iceberg を使用して、Amazon EMR で Spark によりテーブルに対してクエリを実行するには、次の前提条件が必要です。

前提条件

- Amazon EMR で使用する IAM ロールに `AmazonS3TablesFullAccess` ポリシーをアタッチします。

Spark を使用してテーブルをクエリするように Amazon EMR クラスターを設定するには

1. 次の設定を使用して、クラスターを作成します。この例を実行するには、*`user input placeholders`* をユーザー自身の情報に置き換えます。

```
aws emr create-cluster --release-label emr-7.5.0 \
```

```
--applications Name=Spark \
--configurations file://configurations.json \
--region us-east-1 \
--name My_Spark_Iceberg_Cluster \
--log-uri s3://amzn-s3-demo-bucket/ \
--instance-type m5.xlarge \
--instance-count 2 \
--service-role EMR_DefaultRole \
--ec2-attributes \

InstanceProfile=EMR_EC2_DefaultRole,SubnetId=subnet-1234567890abcdef0,KeyName=my-key-pair
```

configurations.json:

```
[{
"Classification":"iceberg-defaults",
"Properties":{"iceberg.enabled":"true"}
}]
```

2. SSH を使用して Spark プライマリノードに接続します。
3. テーブルバケットに接続する Iceberg の Spark セッションを初期化するには、次のコマンドを入力します。*user input placeholders* をテーブルバケットの ARN に置き換えます。

```
spark-shell \
--packages software.amazon.s3tables:s3-tables-catalog-for-iceberg-runtime:0.1.3
 \
--conf spark.sql.catalog.s3tablesbucket=org.apache.iceberg.spark.SparkCatalog \
--conf spark.sql.catalog.s3tablesbucket.catalog-
impl=software.amazon.s3tables.iceberg.S3TablesCatalog \
--conf spark.sql.catalog.s3tablesbucket.warehouse=arn:aws:s3tables:us-
east-1:111122223333:bucket/amzn-s3-demo-bucket1 \
--conf spark.sql.defaultCatalog=s3tablesbucket \
--conf
 spark.sql.extensions=org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions
```

4. Spark SQL を使用してテーブルをクエリします。クエリの例については、「the section called “Spark SQL を使用した S3 テーブルのクエリ”」を参照してください。

AWS analytics services integration

AWS 分析サービス統合を使用して、Amazon EMR で Spark によりテーブルをクエリするには、次の前提条件が必要です。

前提条件

- テーブルバケットを AWS 分析サービスと統合します。
- 名前空間へのリソースリンクの作成.
- Amazon EMR のデフォルトのサービスロールを作成します (EMR_DefaultRole_V2)。詳細については、「Amazon EMR のサービスロール (EMR ロール)」を参照してください。
- Amazon EMR (EMR_EC2_DefaultRole) の Amazon EC2 インスタンスプロファイルを作成します。詳細については、「クラスター EC2 インスタンスのサービスロール (EC2 インスタンスプロファイル)」を参照してください。
  - AmazonS3TablesFullAccess ポリシーを EMR_EC2_DefaultRole にアタッチします。

Spark を使用してテーブルをクエリするように Amazon EMR クラスターを設定するには

1. 次の設定を使用して、クラスターを作成します。この例を使用するには、*user input placeholder* の値を実際の情報に置き換えます。

```
aws emr create-cluster --release-label emr-7.5.0 \
--applications Name=Spark \
--configurations file://configurations.json \
--region us-east-1 \
--name My_Spark_Iceberg_Cluster \
--log-uri s3://amzn-s3-demo-bucket/ \
--instance-type m5.xlarge \
--instance-count 2 \
--service-role EMR_DefaultRole \
--ec2-attributes \

InstanceProfile=EMR_EC2_DefaultRole,SubnetId=subnet-1234567890abcdef0,KeyName=my-key-pair
```

configurations.json:

```
[{
"Classification":"iceberg-defaults",
```

```
"Properties":{"iceberg.enabled":"true"}
}]
```

2. SSH を使用して Spark プライマリノードに接続します。
3. 次のコマンドを入力して、テーブルに接続する Iceberg の Spark セッションを初期化します。*user input placeholders* を、ユーザー自身の情報に置き換えます。

```
spark-shell \
--conf
 spark.sql.extensions=org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions
 \
--conf spark.sql.defaultCatalog=s3tables \
--conf spark.sql.catalog.s3tables=org.apache.iceberg.spark.SparkCatalog \
--conf spark.sql.catalog.s3tables.catalog-
impl=org.apache.iceberg.aws.glue.GlueCatalog \
--conf spark.sql.catalog.s3tables.client.region=us-east-1 \
--conf spark.sql.catalog.s3tables.glue.id=111122223333
```

4. Spark SQL を使用してテーブルをクエリします。クエリの例については、「the section called “Spark SQL を使用した S3 テーブルのクエリ”」を参照してください。

> **Note**
>
> Amazon EMR で `DROP TABLE PURGE` コマンドを使用している場合:
>
> - Amazon EMR バージョン 7.5
>
> Spark 設定 `spark.sql.catalog.`*your-catalog-name*`.cache-enabled` を `false` に指定します。この設定が `true` に設定されている場合、テーブルキャッシュがアクティブ化されないように、新しいセッションまたはアプリケーションで コマンドを実行します。
> - Amazon EMR バージョン 7.5 以上
>
> `DROP TABLE` はサポートされていません。S3 Tables の `DeleteTable` REST API を使用してテーブルを削除できます。

QuickSight を使用したテーブルデータの視覚化

QuickSight は、視覚化の構築、アドホック分析の実行、データからのビジネスインサイトの迅速な取得に役立つ高速なビジネス分析サービスです。QuickSight は、QuickSight の超高速、並列、イン

メモリ、計算エンジン (SPICE) を使用して、AWS データソースをシームレスに検出し、組織が数十万のユーザーにスケールするのを可能にし、高速で応答性の高いクエリパフォーマンスを提供します。詳細については、「QuickSight ユーザーガイド」の「QuickSight とは」を参照してください。

テーブルバケットを AWS 分析サービスに統合したら、テーブルからデータセットを作成し、SPICE を使用するか、クエリエンジンから直接 SQL クエリを使用して QuickSight でデータセットを使用できます。QuickSight は、S3 テーブルのデータソースとして Athena をサポートしています。

QuickSight でテーブルにアクセスするためのアクセス許可を設定する

QuickSight で S3 テーブルデータを使用する前に、QuickSight サービスロールと QuickSight 管理者ユーザーにアクセス許可を付与し、アクセスするテーブルへのアクセス許可を Lake Formation を付与する必要があります。

QuickSight サービスロールにアクセス許可を付与する

アカウントで初めて QuickSight を設定する場合、AWS は Athena や Amazon Redshift など、他の AWS のサービスのデータソースにアクセスすることを QuickSight に許可するサービスロールを作成します。デフォルトのロール名は `aws-quicksight-service-role-v0` です。

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. [ロール] を選択し、QuickSight サービスロールを選択します。デフォルト名は `aws-quicksight-service-role-v0` です。
3. [許可を追加] を選択し、続いて [インラインポリシーを作成] を選択します。
4. [JSON] を選択して JSON ポリシーエディタを開き、次のポリシーを追加します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "glue:GetCatalog",
      "Resource": "*"
    }
  ]
}
```

5. [次へ] を選択し、[ポリシー名] を入力して、[ポリシーを作成] を選択します。

QuickSight 管理者ユーザーのアクセス許可を設定するには

1. 次の AWS CLI コマンドを実行して、QuickSight 管理者ユーザーの ARN を見つけます。

```
aws quicksight list-users --aws-account-id 111122223333 --namespace default --
region region
```

2. この ARN へのアクセス許可を Lake Formation に付与します。詳細については、「テーブルリソースに対する Lake Formation 許可の付与」を参照してください。

QuickSight でのテーブルデータの使用

Athena をデータソースとして使用して、テーブルデータに接続できます。

前提条件

- テーブルバケットを AWS 分析サービスと統合します。
  - 名前空間を作成します。.
  - テーブルの作成.
  - QuickSight でテーブルにアクセスするためのアクセス許可を設定する.
- QuickSight にサインアップします。

1. QuickSight アカウント (https://quicksight.aws.amazon.com/) にサインインします。
2. ダッシュボードで、[新しい分析] を選択します。
3. [新しいデータセット] を選択します。
4. [Athena] を選択します。
5. [データソース名] を入力し、[データソースを作成] を選択します。
6. [Use custom SQL (カスタム SQL を使用)] を選択します。[テーブルの選択] ペインからテーブルを選択することはできません。
7. 視覚化する列をキャプチャする Athena SQL クエリを入力し、[クエリの確認] を選択します。例えば、次のクエリを使用してすべての列を選択します。

```
SELECT * FROM "s3tablescatalog/table-bucket-name".namespace.table-name
```

8. [視覚化] を選択してデータを分析し、ダッシュボードの構築を開始します。詳細については、「Visualizing data in QuickSight」および「Exploring interactive dashboards in QuickSight」を参照してください。

Amazon Data Firehose を使用したテーブルへのデータのストリーミング

Amazon Data Firehose は、Amazon S3、Amazon Redshift、Amazon OpenSearch Service、Splunk、Apache Iceberg テーブル、カスタム HTTP エンドポイント、またはサポートされているサードパーティーのサービスプロバイダーが所有する HTTP エンドポイントなどのターゲットにリアルタイムのストリーミングデータを配信するためのフルマネージドサービスです。Amazon Data Firehose を使用すると、アプリケーションを記述したり、リソースを管理したりする必要はありません。Firehose にデータを送信するデータプロデューサーを作成すると、それにより、指定した送信先にデータが自動配信されます。データを配信前に変換するように、Firehose を設定することもできます。Amazon Data Firehose の詳細については、「Amazon Data Firehose とは」を参照してください。

S3 テーブルバケット内のテーブルへの Firehose ストリーミングを設定するには、次の手順に従います。

1. テーブルバケットを AWS 分析サービスと統合します。
2. S3 テーブルにデータを配信するように Firehose を設定します。そのためには、Firehose がテーブルにアクセスできるように AWS Identity and Access Management (IAM) サービスロールを作成します。
3. Firehose サービスロールにテーブルまたはテーブルの名前空間に対する明示的なアクセス許可を付与します。詳細については、「テーブルリソースに対する Lake Formation 許可の付与」を参照してください。
4. テーブルにデータをルーティングする Firehose ストリームを作成します。

Firehose が S3 テーブルを送信先として使用するロールの作成

Firehose には、AWS Glue テーブルにアクセスし、S3 テーブルにデータを書き込むための特定のアクセス許可を持つ IAM サービスロールが必要です。Firehose ストリームを作成する際に、この IAM ロールが必要です。

1. IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. 左のナビゲーションペインの [ポリシー] を選択します。

3. [ポリシーを作成] を選択し、ポリシーエディタで [JSON] を選択します。
4. データカタログ内のすべてのデータベースとテーブルにアクセス許可を付与する次のインラインポリシーを追加します。必要に応じて、特定のテーブルとデータベースにのみ許可を付与できます。このポリシーを使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3TableAccessViaGlueFederation",
      "Effect": "Allow",
      "Action": [
        "glue:GetTable",
        "glue:GetDatabase",
        "glue:UpdateTable"
      ],
      "Resource": [
        "arn:aws:glue:region:account-id:catalog/s3tablescatalog/*",
        "arn:aws:glue:region:account-id:catalog/s3tablescatalog",
        "arn:aws:glue:region:account-id:catalog",
        "arn:aws:glue:region:account-id:database/*",
        "arn:aws:glue:region:account-id:table/*/*"
      ]
    },
    {
      "Sid": "S3DeliveryErrorBucketPermission",
      "Effect": "Allow",
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3:::error delivery bucket",
        "arn:aws:s3:::error delivery bucket/*"
      ]
    },
    {
```

```
      "Sid": "RequiredWhenUsingKinesisDataStreamsAsSource",
      "Effect": "Allow",
      "Action": [
        "kinesis:DescribeStream",
        "kinesis:GetShardIterator",
        "kinesis:GetRecords",
        "kinesis:ListShards"
      ],
      "Resource": "arn:aws:kinesis:region:account-id:stream/stream-name"
    },
    {
      "Sid":
 "RequiredWhenDoingMetadataReadsANDDataAndMetadataWriteViaLakeformation",
      "Effect": "Allow",
      "Action": [
        "lakeformation:GetDataAccess"
      ],
      "Resource": "*"
    },
    {
      "Sid": "RequiredWhenUsingKMSEncryptionForS3ErrorBucketDelivery",
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": [
        "arn:aws:kms:region:account-id:key/KMS-key-id"
      ],
      "Condition": {
        "StringEquals": {
          "kms:ViaService": "s3.region.amazonaws.com"
        },
        "StringLike": {
          "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::error delivery bucket/
prefix*"
        }
      }
    },
    {
      "Sid": "LoggingInCloudWatch",
      "Effect": "Allow",
      "Action": [
        "logs:PutLogEvents"
```

```
      ],
      "Resource": [
        "arn:aws:logs:region:account-id:log-group:log-group-name:log-stream:log-
stream-name"
      ]
    },
    {
      "Sid": "RequiredWhenAttachingLambdaToFirehose",
      "Effect": "Allow",
      "Action": [
        "lambda:InvokeFunction",
        "lambda:GetFunctionConfiguration"
      ],
      "Resource": [
        "arn:aws:lambda:region:account-id:function:function-name:function-version"
      ]
    }
  ]
}
```

このポリシーには、Kinesis Data Streams へのアクセス、Lambda 関数の呼び出し、AWS KMS キーへのアクセスを許可するステートメントが含まれています。これらのリソースを使用しない場合は、それぞれのステートメントを削除できます。

エラーログ記録が有効になっている場合、Firehose はデータ配信エラーを CloudWatch ロググループとストリームにも送信します。このためには、ロググループとログストリーム名を設定する必要があります。ロググループとログストリーム名については、「Monitor Amazon Data Firehose Using CloudWatch Logs」を参照してください。

5. ポリシーを作成したら、[信頼されたエンティティタイプ] として [AWS サービス] を使用して IAM ロールを作成します。
6. [サービスまたはユースケース] で、[Kinesis] を選択します。[ユースケース]で、[Kinesis Firehose] を選択します。
7. [次へ] を選択して、以前に作成したポリシーを選択します。
8. ロールに名前を付けます。ロールの詳細を確認し、[ロールの作成] を選択します。ロールには、以下の信頼ポリシーがあります。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Principal": {
                "Service": [
                    "firehose.amazonaws.com"
                ]
            }
        }
    ]
}
```

S3 テーブルへの Firehose ストリームの設定

次の手順は、コンソールを使用して S3 テーブルにデータを配信するように Firehose ストリームを作成する方法を示しています。S3 テーブルへの Firehose ストリームを設定するには、次の前提条件が必要です。

前提条件

- テーブルバケットを AWS 分析サービスと統合します。
  - 名前空間を作成します。.
  - テーブルの作成.
- Firehose が S3 テーブルにアクセスするためのロールを作成します。
- テーブルにアクセスするために作成した Firehose サービスロールに Lake Formation 許可を付与します。

ストリームを設定するときに Firehose にルーティング情報を提供するには、データベース名とその名前空間内のテーブル名として名前空間を使用します。これらの値は、Firehose ストリーム設定の一意のキーセクションで使用して、データを 1 つのテーブルにルーティングできます。この値を使用して、JSON クエリ式を使用してテーブルにルーティングすることもできます。詳細については、「Route incoming records to a single Iceberg table」を参照してください。

S3 テーブルへの Firehose ストリームを設定するには (コンソール)

1. Firehose コンソール (https://console.aws.amazon.com/firehose/) を開きます。
2. [Firehose ストリームを作成] を選択します。

3. [ソース] で、以下のいずれかのオプションを選択します。
   - Amazon Kinesis Data Streams
   - Amazon MSK
   - ダイレクト PUT
4. [送信先] で、[Apache Iceberg テーブル] を選択します。
5. Firehose ストリーム名を入力します。
6. [ソース設定] を構成します。
7. [送信先の設定] では、自分のアカウントのテーブルにストリーミングする場合は [現在のアカウント] を選択し、別のアカウントのテーブルにストリーミングする場合は [クロスアカウント] を選択します。
   - [現在のアカウント] のテーブルには、[カタログ] ドロップダウンから [S3 Tables カタログ] を選択します。
   - [クロスアカウント] のテーブルには、別のアカウントのストリーミング先のカタログの [カタログ ARN] を入力します。
8. [一意のキー設定]、JSONQuery 式、または Lambda 関数を使用して、データベース名とテーブル名を設定します。詳細については、「Firehose デベロッパーガイド」の「着信レコードを単一の Iceberg テーブルにルーティングする」および「着信レコードを異なる Iceberg テーブルにルーティングする」を参照してください。
9. [バックアップ設定] で、[S3 バックアップバケット] を指定します。
10. [詳細設定] の [既存の IAM ロール] で、Firehose 用に作成した IAM ロールを選択します。
11. [Firehose ストリームを作成] を選択します。

ストリームに対して設定できるその他の設定の詳細については、「Amazon Firehose デベロッパーガイド」の「Firehose ストリームを設定する」を参照してください。

AWS Glue を使用した Amazon S3 テーブルでの ETL ジョブの実行

AWS Glueは、分析を行うユーザーが複数のソースからのデータを簡単に検出、準備、移動、統合できるようにするサーバーレスのデータ統合サービスです。AWS Glue ジョブを使用して抽出、変換、ロード (ETL) パイプラインを実行し、データをデータレイクにロードできます。AWS Glue の詳細については、AWS Glue デベロッパーガイド の「What is AWS Glue?」を参照してください。

AWS Glue ジョブには、ソースデータに接続して処理し、データターゲットに書き出すスクリプトがカプセル化されています。通常、ジョブは、抽出、変換、ロード (ETL) スクリプトを実行します。

ジョブは、Apache Spark ランタイム環境向けに設計されたスクリプトを実行できます。ジョブ実行をモニタリングすると、完了ステータス、継続時間、開始時間などのランタイムメトリクスを知ることができます。

AWS Glue のジョブを使用して S3 テーブルのデータを処理するには、AWS 分析サービスとの統合を通じてテーブルに接続するか、Amazon S3 Tables の Iceberg REST エンドポイントまたは Apache Iceberg の Amazon S3 Tables カタログを使用して直接接続します。このガイドでは、S3 Tables で AWS Glue の使用を開始するための基本的な手順を示します。

トピック

- 前提条件
- テーブルバケットに接続するスクリプトを作成する
- テーブルをクエリする AWS Glue ジョブを作成する

> **Note**
>
> S3 Tables は、AWS Glue バージョン 5.0 以降でサポートされています。

前提条件

AWS Glue ジョブからテーブルに対してクエリを実行する前に、AWS Glue がジョブの実行に使用できる IAM ロールを設定し、ジョブの実行時に AWS Glue がアクセスできる Amazon S3 バケットに Amazon S3 Tables Catalog for Apache Iceberg JAR をアップロードする必要があります。

- テーブルバケットを AWS 分析サービスと統合します。
- AWS Glue 用の IAM ロールを作成します。
  - `AmazonS3TablesFullAccess` 管理ポリシーをロールにアタッチします。
  - `AmazonS3FullAccess` 管理ポリシーをロールにアタッチします。
- (オプション) Apache Iceberg で Amazon S3 Tables カタログを使用する場合は、クライアントカタログ JAR をダウンロードして S3 バケットにアップロードする必要があります。

  カタログ JAR のダウンロード

  1. Maven Central で最新バージョンを検索します。ブラウザまたは次のコマンドを使用して、Maven central から JAR をダウンロードできます。必ず`#######`を最新バージョンに置き換えてください。

```
wget https://repo1.maven.org/maven2/software/amazon/s3tables/s3-tables-catalog-
for-iceberg-runtime/0.1.5/s3-tables-catalog-for-iceberg-runtime-0.1.5.jar
```

2. ダウンロードした JAR を、AWS Glue IAM ロールがアクセスできる S3 バケットにアップロードします。JAR をアップロードするには、次の AWS CLI コマンドを実行します。*#####*を最新バージョンに置き換え、*#####*と*##*を独自のものに置き換えます。

```
aws s3 cp s3-tables-catalog-for-iceberg-runtime-0.1.5.jar s3://amzn-s3-demo-
bucket/jars/
```

テーブルバケットに接続するスクリプトを作成する

AWS Glue ETL ジョブの実行時にテーブルデータにアクセスするには、S3 テーブルバケットに接続する Apache Iceberg の Spark セッションを設定します。既存のスクリプトを変更してテーブルバケットに接続するか、新しいスクリプトを作成できます。AWS Glue スクリプトの作成の詳細については、「AWS Glue デベロッパーガイド」の「チュートリアル: AWS Glue for Spark スクリプトの記述」を参照してください。

次の S3 Tables アクセス方法のいずれかを使用して、テーブルバケットに接続するようにセッションを設定できます。

- S3 Tables と AWS 分析サービスの統合
- Amazon S3 Tables の Iceberg REST エンドポイント
- Apache Iceberg の Amazon S3 Tables カタログ

セットアップ手順と設定例を表示するには、次のアクセス方法から選択します。

AWS analytics services integration

AWS 分析サービス統合を使用して AWS Glue の Spark でテーブルをクエリするための前提条件として、テーブルバケットを AWS 分析サービスと統合する必要があります。

テーブルバケットへの接続は、ジョブの Spark セッションを使用するか、インタラクティブセッションの AWS Glue Studio マジックを使用して設定できます。以下の例を使用するには、*#####*を独自のテーブルバケットの情報に置き換えます。

PySpark スクリプトの使用

PySpark スクリプトで次のコードスニペットを使用して、統合を通じてテーブルバケットに接続するように AWS Glue ジョブを設定します。

```
spark = SparkSession.builder.appName("SparkIcebergSQL") \
    .config("spark.sql.extensions",
 "org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions") \
    .config("spark.sql.defaultCatalog","s3tables") \
    .config("spark.sql.catalog.s3tables",
 "org.apache.iceberg.spark.SparkCatalog") \
    .config("spark.sql.catalog.s3tables.catalog-impl",
 "org.apache.iceberg.aws.glue.GlueCatalog") \
    .config("spark.sql.catalog.s3tables.glue.id",
 "111122223333:s3tablescatalog/amzn-s3-demo-table-bucket") \
    .config("spark.sql.catalog.s3tables.warehouse", "s3://amzn-s3-demo-table-
bucket/warehouse/") \
    .getOrCreate()
```

インタラクティブな AWS Glue セッションの使用

AWS Glue 5.0 でインタラクティブなノートブックセッションを使用する場合は、コードの実行前にセルで %%configure マジックを使用して同じ設定を指定します。

```
%%configure
{"conf":
 "spark.sql.extensions=org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions
 --conf spark.sql.defaultCatalog=s3tables --conf
 spark.sql.catalog.s3tables=org.apache.iceberg.spark.SparkCatalog --conf
 spark.sql.catalog.s3tables.catalog-impl=org.apache.iceberg.aws.glue.GlueCatalog
 --conf spark.sql.catalog.s3tables.glue.id=111122223333:s3tablescatalog/amzn-s3-
demo-table-bucket --conf spark.sql.catalog.s3tables.warehouse=s3://amzn-s3-demo-
table-bucket/warehouse/"}
```

Amazon S3 Tables Iceberg REST endpoint

テーブルバケットへの接続を設定するには、ジョブの Spark セッションを使用するか、インタラクティブセッションの AWS Glue Studio マジックを使用できます。以下の例を使用するには、*########*を独自のテーブルバケットの情報に置き換えます。

PySpark スクリプトの使用

次のコードスニペットを PySpark スクリプトで使用して、エンドポイントを通じてテーブルバケットに接続するように AWS Glue ジョブを設定します。

```
spark = SparkSession.builder.appName("glue-s3-tables-rest") \
    .config("spark.sql.extensions",
 "org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions") \
    .config("spark.sql.defaultCatalog", "s3_rest_catalog") \
    .config("spark.sql.catalog.s3_rest_catalog",
 "org.apache.iceberg.spark.SparkCatalog") \
    .config("spark.sql.catalog.s3_rest_catalog.type", "rest") \
    .config("spark.sql.catalog.s3_rest_catalog.uri", "https://
s3tables.Region.amazonaws.com/iceberg") \
    .config("spark.sql.catalog.s3_rest_catalog.warehouse",
 "arn:aws:s3tables:Region:111122223333:s3tablescatalog/amzn-s3-demo-table-
bucket") \
    .config("spark.sql.catalog.s3_rest_catalog.rest.sigv4-enabled", "true") \
    .config("spark.sql.catalog.s3_rest_catalog.rest.signing-name", "s3tables") \
    .config("spark.sql.catalog.s3_rest_catalog.rest.signing-region", "Region") \
    .config('spark.sql.catalog.s3_rest_catalog.io-
impl','org.apache.iceberg.aws.s3.S3FileIO') \
    .config('spark.sql.catalog.s3_rest_catalog.rest-metrics-reporting-
enabled','false') \
    .getOrCreate()
```

インタラクティブな AWS Glue セッションの使用

AWS Glue 5.0 でインタラクティブなノートブックセッションを使用する場合は、コードの実行前にセルで %%configure マジックを使用して同じ設定を指定します。プレースホルダー値を独自のテーブルバケットの情報に置き換えます。

```
%%configure
{"conf":
 "spark.sql.extensions=org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions
 --conf spark.sql.defaultCatalog=s3_rest_catalog --conf
 spark.sql.catalog.s3_rest_catalog=org.apache.iceberg.spark.SparkCatalog
 --conf spark.sql.catalog.s3_rest_catalog.type=rest --conf
 spark.sql.catalog.s3_rest_catalog.uri=https://s3tables.Region.amazonaws.com/
iceberg --conf
 spark.sql.catalog.s3_rest_catalog.warehouse=arn:aws:s3tables:Region:111122223333:s3table
amzn-s3-demo-table-bucket --conf spark.sql.catalog.s3_rest_catalog.rest.sigv4-
enabled=true --conf spark.sql.catalog.s3_rest_catalog.rest.signing-name=s3tables
```

```
 --conf spark.sql.catalog.s3_rest_catalog.rest.signing-region=Region --conf
 spark.sql.catalog.s3_rest_catalog.io-impl=org.apache.iceberg.aws.s3.S3FileIO --
conf spark.sql.catalog.s3_rest_catalog.rest-metrics-reporting-enabled=false"}
```

Amazon S3 Tables Catalog for Apache Iceberg

Apache Iceberg で Amazon S3 Tables カタログを使用してテーブルに接続するための前提条件として、まず最新のカタログ jar をダウンロードして S3 バケットにアップロードする必要があります。次に、ジョブの作成時に、クライアントカタログ JAR へのパスを特別なパラメータとして追加します。AWS Glue のジョブパラメータの詳細については、「AWS Glue Developer Guide」の「Special parameters used in AWS Glue jobs」を参照してください。

テーブルバケットへの接続を設定するには、ジョブの Spark セッションを使用するか、インタラクティブセッションの AWS Glue Studio マジックを使用できます。以下の例を使用するには、*########*を独自のテーブルバケットの情報に置き換えます。

PySpark スクリプトの使用

次のコードスニペットを PySpark スクリプトで使用して、JAR を通じてテーブルバケットに接続するように AWS Glue ジョブを設定します。プレースホルダー値を独自のテーブルバケットの情報に置き換えます。

```
spark = SparkSession.builder.appName("glue-s3-tables") \
    .config("spark.sql.extensions",
 "org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions") \
    .config("spark.sql.defaultCatalog", "s3tablesbucket") \
    .config("spark.sql.catalog.s3tablesbucket",
 "org.apache.iceberg.spark.SparkCatalog") \
    .config("spark.sql.catalog.s3tablesbucket.catalog-impl",
 "software.amazon.s3tables.iceberg.S3TablesCatalog") \
    .config("spark.sql.catalog.s3tablesbucket.warehouse",
 "arn:aws:s3tables:Region:111122223333:bucket/amzn-s3-demo-table-bucket") \
    .getOrCreate()
```

インタラクティブな AWS Glue セッションの使用

AWS Glue 5.0 でインタラクティブなノートブックセッションを使用する場合は、コードの実行前にセルで %%configure マジックを使用して同じ設定を指定します。プレースホルダー値を独自のテーブルバケットの情報に置き換えます。

```
%%configure
```

```
{"conf":
 "spark.sql.extensions=org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions
 --conf spark.sql.defaultCatalog=s3tablesbucket --conf
 spark.sql.catalog.s3tablesbucket=org.apache.iceberg.spark.SparkCatalog
 --conf spark.sql.catalog.s3tablesbucket.catalog-
impl=software.amazon.s3tables.iceberg.S3TablesCatalog --conf
 spark.sql.catalog.s3tablesbucket.warehouse=arn:aws:s3tables:Region:111122223333:bucket/
amzn-s3-demo-table-bucket", "extra-jars": "s3://amzn-s3-demo-bucket/jars/s3-
tables-catalog-for-iceberg-runtime-0.1.5.jar"}
```

サンプルスクリプト

以下のサンプル PySpark スクリプトは、AWS Glue ジョブで S3 テーブルへのクエリをテストするために使用できます。各スクリプトはテーブルバケットに接続し、新しい名前空間の作成、サンプルテーブルの作成、テーブルへのデータの挿入、テーブルデータの取得を行うためのクエリを実行します。スクリプトを使用するには、*#########*を独自のテーブルバケットの情報に置き換えます。

S3 Tables のアクセス方法に応じて、以下のスクリプトから選択します。

S3 Tables integration with AWS analytics services

```
from pyspark.sql import SparkSession

spark = SparkSession.builder.appName("SparkIcebergSQL") \
    .config("spark.sql.extensions",
 "org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions") \
    .config("spark.sql.defaultCatalog","s3tables")
    .config("spark.sql.catalog.s3tables", "org.apache.iceberg.spark.SparkCatalog") \
    .config("spark.sql.catalog.s3tables.catalog-impl",
 "org.apache.iceberg.aws.glue.GlueCatalog") \
    .config("spark.sql.catalog.s3tables.glue.id",
 "111122223333:s3tablescatalog/amzn-s3-demo-table-bucket") \
    .config("spark.sql.catalog.s3tables.warehouse", "s3://amzn-s3-demo-table-bucket/
bucket/amzn-s3-demo-table-bucket") \
    .getOrCreate()

namespace = "new_namespace"
table = "new_table"

spark.sql("SHOW DATABASES").show()

spark.sql(f"DESCRIBE NAMESPACE {namespace}").show()
```

```
spark.sql(f"""
    CREATE TABLE IF NOT EXISTS {namespace}.{table} (
       id INT,
       name STRING,
       value INT
    )
""")

spark.sql(f"""
    INSERT INTO {namespace}.{table}
    VALUES
       (1, 'ABC', 100),
       (2, 'XYZ', 200)
""")

spark.sql(f"SELECT * FROM {namespace}.{table} LIMIT 10").show()
```

Amazon S3 Tables Iceberg REST endpoint

```
from pyspark.sql import SparkSession

spark = SparkSession.builder.appName("glue-s3-tables-rest") \
    .config("spark.sql.extensions",
 "org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions") \
    .config("spark.sql.defaultCatalog", "s3_rest_catalog") \
    .config("spark.sql.catalog.s3_rest_catalog",
 "org.apache.iceberg.spark.SparkCatalog") \
    .config("spark.sql.catalog.s3_rest_catalog.type", "rest") \
    .config("spark.sql.catalog.s3_rest_catalog.uri", "https://
s3tables.Region.amazonaws.com/iceberg") \
    .config("spark.sql.catalog.s3_rest_catalog.warehouse",
 "arn:aws:s3tables:Region:111122223333:bucket/amzn-s3-demo-table-bucket") \
    .config("spark.sql.catalog.s3_rest_catalog.rest.sigv4-enabled", "true") \
    .config("spark.sql.catalog.s3_rest_catalog.rest.signing-name", "s3tables") \
    .config("spark.sql.catalog.s3_rest_catalog.rest.signing-region", "Region") \
    .config('spark.sql.catalog.s3_rest_catalog.io-
impl','org.apache.iceberg.aws.s3.S3FileIO') \
    .config('spark.sql.catalog.s3_rest_catalog.rest-metrics-reporting-
enabled','false') \
    .getOrCreate()

namespace = "s3_tables_rest_namespace"
```

```
table = "new_table_s3_rest"

spark.sql("SHOW DATABASES").show()

spark.sql(f"DESCRIBE NAMESPACE {namespace}").show()

spark.sql(f"""
    CREATE TABLE IF NOT EXISTS {namespace}.{table} (
       id INT,
       name STRING,
       value INT
    )
""")

spark.sql(f"""
    INSERT INTO {namespace}.{table}
    VALUES
       (1, 'ABC', 100),
       (2, 'XYZ', 200)
""")

spark.sql(f"SELECT * FROM {namespace}.{table} LIMIT 10").show()
```

Amazon S3 Tables Catalog for Apache Iceberg

```
from pyspark.sql import SparkSession

#Spark session configurations
spark = SparkSession.builder.appName("glue-s3-tables") \
    .config("spark.sql.extensions",
 "org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions") \
    .config("spark.sql.defaultCatalog", "s3tablesbucket") \
    .config("spark.sql.catalog.s3tablesbucket",
 "org.apache.iceberg.spark.SparkCatalog") \
    .config("spark.sql.catalog.s3tablesbucket.catalog-impl",
 "software.amazon.s3tables.iceberg.S3TablesCatalog") \
    .config("spark.sql.catalog.s3tablesbucket.warehouse",
 "arn:aws:s3tables:Region:111122223333:bucket/amzn-s3-demo-table-bucket") \
    .getOrCreate()

#Script
```

```
namespace = "new_namespace"
table = "new_table"

spark.sql(f"CREATE NAMESPACE IF NOT EXISTS s3tablesbucket.{namespace}")
spark.sql(f"DESCRIBE NAMESPACE {namespace}").show()

spark.sql(f"""
    CREATE TABLE IF NOT EXISTS {namespace}.{table} (
       id INT,
       name STRING,
       value INT
    )
""")

spark.sql(f"""
    INSERT INTO {namespace}.{table}
    VALUES
       (1, 'ABC', 100),
       (2, 'XYZ', 200)
""")

spark.sql(f"SELECT * FROM {namespace}.{table} LIMIT 10").show()
```

テーブルをクエリする AWS Glue ジョブを作成する

次の手順は、S3 テーブルバケットに接続する AWS Glue ジョブの設定方法を示しています。これを行うには、AWS CLI を使用するか、コンソールで AWS Glue Studio スクリプトエディタを使用します。詳細については、「AWS Glue ユーザーガイド」の「AWS Glue でジョブを作成する」を参照してください。

AWS Glue Studio スクリプトエディタの使用

次の手順は、AWS Glue Studio スクリプトエディタを使用して S3 テーブルをクエリする ETL ジョブを作成する方法を示しています。

前提条件

- 前提条件
- テーブルバケットに接続するスクリプトを作成する

1. https://console.aws.amazon.com/glue/ で AWS Glue コンソール を開きます。

2. ナビゲーションペインで、[ETL ジョブ] を選択します。
3. [スクリプトエディタ] を選択し、[スクリプトのアップロード] を選択し、S3 テーブルをクエリするために作成した PySpark スクリプトをアップロードします。
4. [ジョブの詳細] タブを選択し、[基本プロパティ] に次のように入力します。
   - [名前] で、ジョブの名前を入力します。
   - [IAM ロール] で、作成した AWS Glue ロールを選択します。
5. (オプション) Amazon S3 Tables カタログを Apache Iceberg のアクセス方法として使用する場合は、[詳細プロパティ] を展開し、[依存 JARS パス] に、S3 バケットにアップロードしたクライアントカタログ jar の S3 URI を前提条件として入力します。例: s3://*amzn-s3-demo-bucket1*/*jars*/s3-tables-catalog-for-iceberg-runtime-*0.1.5*.jar
6. [保存] を選択してジョブを作成します。
7. [実行] を選択してジョブを開始し、[実行] タブでジョブのステータスを確認します。

AWS CLI を使用する場合

次の手順は、AWS CLI を使用して S3 テーブルをクエリする ETL ジョブを作成する方法を示しています。コマンドを使用するには、*#########*を独自の値に置き換えます。

前提条件

- 前提条件
- テーブルバケットに接続するスクリプトを作成する、これを S3 バケットにアップロードします。

1. AWS Glue ジョブを作成します。

```
aws glue create-job \
--name etl-tables-job \
--role arn:aws:iam::111122223333:role/AWSGlueServiceRole \
--command '{
    "Name": "glueetl",
    "ScriptLocation": "s3://amzn-s3-demo-bucket1/scripts/glue-etl-query.py",
    "PythonVersion": "3"
}' \
--default-arguments '{
    "--job-language": "python",
    "--class": "GlueApp"
}' \
```

```
--glue-version "5.0"
```

> **Note**
>
> (オプション) Amazon S3 Tables カタログを Apache Iceberg のアクセス方法として使用する場合は、`--extra-jars` パラメータを使用してクライアントカタログ JAR を `--default-arguments` に追加します。パラメータを追加するときに、*##########*は独自のものに置き換えます。
>
> ```
> "--extra-jars": "s3://amzn-s3-demo-bucket/jar-path/s3-tables-catalog-for-iceberg-runtime-0.1.5.jar"
> ```

2. ジョブを開始します。

```
aws glue start-job-run \
--job-name etl-tables-job
```

3. ジョブのステータスを確認するには、前のコマンドの実行 ID をコピーして、次のコマンドに入力します。

```
aws glue get-job-run --job-name etl-tables-job \
--run-id jr_ec9a8a302e71f8483060f87b6c309601ea9ee9c1ffc2db56706dfcceb3d0e1ad
```

S3 Tables AWS リージョン、エンドポイント、および Service Quotas

以下のセクションには、S3 Tables でサポートされている AWS リージョンと Service Quotas が含まれています。

トピック

- S3 Tables AWS リージョンとエンドポイント
- S3 Tables のクォータ

S3 Tables AWS リージョンとエンドポイント

S3 Tables は現在、次の AWS リージョンで利用可能です: AWS のサービスにプログラムで接続するには、エンドポイントを使用します。詳細については、AWS サービスエンドポイントを参照してください。Amazon S3 エンドポイントの詳細については、「Amazon S3 エンドポイント」を参照してください。

リージョン名	リージョン	エンドポイント	プロトコル	署名バージョンのサポート
アフリカ (ケープタウン)	af-south-1	s3tables.af-south-1.amazonaws.com	HTTPS	4
アジアパシフィック (香港)	ap-east-1	s3tables.ap-east-1.amazonaws.com	HTTPS	4
アジアパシフィック (東京)	ap-northeast-1	s3tables.ap-northeast-1.amazonaws.com	HTTPS	4
アジアパシフィック (ソウル)	ap-northeast-2	s3tables.ap-northeast-2.amazonaws.com	HTTPS	4
アジアパシフィック (大阪)	ap-northeast-3	s3tables.ap-northeast-3.amazonaws.com	HTTPS	4
アジアパシフィック (ムンバイ)	ap-south-1	s3tables.ap-south-	HTTPS	4

リージョン名	リージョン	エンドポイント	プロトコル	署名バージョンのサポート
		1.amazonaws.com		
アジアパシフィック (ハイデラバード)	ap-south-2	s3tables.ap-south-2.amazonaws.com	HTTPS	4
アジアパシフィック (シンガポール)	ap-southeast-1	s3tables.ap-southeast-1.amazonaws.com	HTTPS	4
アジアパシフィック (シドニー)	ap-southeast-2	s3tables.ap-southeast-2.amazonaws.com	HTTPS	4
アジアパシフィック (ジャカルタ)	ap-southeast-3	s3tables.ap-southeast-3.amazonaws.com	HTTPS	4
アジアパシフィック (メルボルン)	ap-southeast-4	s3tables.ap-southeast-4.amazonaws.com	HTTPS	4
アジアパシフィック (マレーシア)	ap-southeast-5	s3tables.ap-southeast-5.amazonaws.com	HTTPS	4

リージョン名	リージョン	エンドポイント	プロトコル	署名バージョンのサポート
カナダ (中部)	ca-central-1	s3tables.ca-central-1.amazonaws.com	HTTPS	4
カナダ西部 (カルガリー)	ca-west-1	s3tables.ca-west-1.amazonaws.com	HTTPS	4
欧州 (フランクフルト)	eu-central-1	s3tables.eu-central-1.amazonaws.com	HTTPS	4
欧州 (チューリッヒ)	eu-central-2	s3tables.eu-central-2.amazonaws.com	HTTPS	4
欧州 (ストックホルム)	eu-north-1	s3tables.eu-north-1.amazonaws.com	HTTPS	4
ヨーロッパ (ミラノ)	eu-south-1	s3tables.eu-south-1.amazonaws.com	HTTPS	4
欧州 (スペイン)	eu-south-2	s3tables.eu-south-2.amazonaws.com	HTTPS	4

リージョン名	リージョン	エンドポイント	プロトコル	署名バージョンのサポート
欧州 (アイルランド)	eu-west-1	s3tables.eu-west-1.amazonaws.com	HTTPS	4
欧州 (ロンドン)	eu-west-2	s3tables.eu-west-2.amazonaws.com	HTTPS	4
欧州 (パリ)	eu-west-3	s3tables.eu-west-3.amazonaws.com	HTTPS	4
イスラエル (テルアビブ)	il-central-1	s3tables.il-central-1.amazonaws.com	HTTPS	4
中東 (アラブ首長国連邦)	me-central-1	s3tables.me-central-1.amazonaws.com	HTTPS	4
中東 (バーレーン)	me-south-1	s3tables.me-south-1.amazonaws.com	HTTPS	4
南米 (サンパウロ)	sa-east-1	s3tables.sa-east-1.amazonaws.com	HTTPS	4

リージョン名	リージョン	エンドポイント	プロトコル	署名バージョンのサポート
米国東部 (バージニア北部)	us-east-1	s3tables.us-east-1.amazonaws.com	HTTPS	4
米国東部 (オハイオ)	us-east-2	s3tables.us-east-2.amazonaws.com	HTTPS	4
米国西部 (北カリフォルニア)	us-west-1	s3tables.us-west-1.amazonaws.com	HTTPS	4
米国西部 (オレゴン)	us-west-2	s3tables.us-west-2.amazonaws.com	HTTPS	4

S3 Tables のクォータ

クォータ (制限とも呼ばれます) は、AWS アカウントのサービスリソースまたはオペレーションの最大数です。以下に、S3 Tables リソースのクォータを示します。Amazon S3 クォータの詳細については、「Amazon S3 クォータ」を参照してください。

名前	デフォルト	引き上げ可能	説明
テーブルバケット	10	クォータの引き上げをリクエストするには、サポートにお問い合わせください。	アカウントで AWS リージョンごとに作成できる Amazon S3 テーブルバケットの数

名前	デフォルト	引き上げ可能	説明
名前空間	10,000	クォータの引き上げをリクエストするには、サポートにお問い合わせください。	テーブルバケットごとに作成できる Amazon S3 テーブル名前空間の数。
テーブル	10,000	クォータの引き上げをリクエストするには、サポートにお問い合わせください。	テーブルバケットごとに作成できる Amazon S3 テーブルの数。

S3 Tables のセキュリティ

Amazon S3 には、さまざまなセキュリティ機能とツールが用意されています。以下は、S3 Tables でサポートされている機能とツールのリストです。これらのツールを適切に適用すると、リソースが保護され、目的のユーザーのみがリソースにアクセスできるようにするために役立ちます。

アイデンティティベースのポリシー

アイデンティティベースのポリシーは、IAM ユーザー、グループ、ロールにアタッチされます。アイデンティティベースのポリシーを使用すると、テーブルバケットまたはテーブルへのアクセス許可を IAM アイデンティティに付与できます。デフォルトでは、ユーザーとロールには、テーブルとテーブルバケットを作成および変更するアクセス許可はありません。また、S3 コンソール、AWS CLI、または Amazon S3 REST API を使用してタスクを実行することはできません。アカウント内に IAM ユーザー、グループ、およびロールを作成し、これらにアクセスポリシーをアタッチできます。その後、リソースへのアクセスを許可できます。テーブルバケットとテーブルを作成してアクセスするには、IAM 管理者が AWS Identity and Access Management (IAM) ロールまたはユーザーに必要なアクセス許可を付与する必要があります。詳細については、「Access management for S3 Tables」を参照してください。

リソースベースのポリシー

リソースベースのポリシーをリソースにアタッチします。テーブルバケットとテーブルのリソースベースのポリシーを作成できます。テーブルバケットポリシーを使用して、テーブルバケットと名前空間レベルの API アクセス許可を制御できます。テーブルバケットポリシーを使用して、バケット内の複数のテーブルに対するテーブルレベルの API アクセス許可を制御することもできます。ポリシー定義に応じて、バケットにアタッチされたアクセス許可は、バケット内のすべてのテーブルま

たは特定のテーブルに適用できます。テーブルポリシーを使用して、バケット内の個々のテーブルにテーブルレベルの API アクセス許可を付与することもできます。

S3 Tables は、テーブルバケットオペレーションまたはテーブルオペレーションを実行するリクエストを受け取ると、まずリクエスタに必要なアクセス許可があることを確認します。リクエストを許可するかどうかを決定する際に、関連するすべてのアクセスポリシー、ユーザーポリシー、リソースベースのポリシー (IAM ユーザーポリシー、IAM ロールポリシー、テーブルバケットポリシー、テーブルポリシー) を評価します。テーブルバケットポリシーとテーブルポリシーを使用すると、リソースへのアクセスをパーソナライズして、承認された ID のみがリソースにアクセスしてアクションを実行できるようにすることができます。詳細については、「Access management for S3 Tables」を参照してください。

S3 Tables の AWS Organizations サービスコントロールポリシー (SCP)。

サービスコントロールポリシー (SCP) の Amazon S3 Tables を使用して、組織内のユーザーへのアクセス許可を管理できます。IAM およびリソースポリシーと同様に、すべてのテーブルおよびバケットレベルのアクションは、ポリシーの `s3tables` 名前空間の一部として参照されます。詳細については、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシー (SCPs)」を参照してください。

トピック

- 暗号化による S3 テーブルデータの保護
- S3 Tables のアクセス管理
- S3 Tables の VPC 接続
- S3 Tables のセキュリティに関する考慮事項と制限事項

暗号化による S3 テーブルデータの保護

テーブルバケットでの AWS KMS キーによるサーバー側の暗号化 (SSE-KMS) の使用

トピック

- テーブルとテーブルバケットでの SSE-KMS の仕組み
- テーブルとテーブルバケットでの SSE-KMS の適用とスコープ設定
- テーブルとテーブルバケットの SSE-KMS 暗号化のモニタリングと監査
- S3 Tables の SSE-KMS 暗号化のアクセス許可要件

- テーブルバケットでの AWS KMS キーによるサーバー側の暗号化 (SSE-KMS) の指定

すべてのテーブルバケットには、デフォルトの暗号化設定があり、テーブルは Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3) を使用して自動的に暗号化されます。この暗号化は、S3 テーブルバケット内のすべてのテーブルに適用され、費用はかかりません。

キーローテーションやアクセスポリシー付与を管理するなど、暗号化キーをより細かく制御する必要がある場合は、AWS Key Management Service (AWS KMS) キーによるサーバー側の暗号化 (SSE-KMS) を使用するようにテーブルバケットを設定できます。AWS KMS のセキュリティ制御は、暗号化関連のコンプライアンス要件を満たすのに役立ちます。SSE-KMS に関する詳細は、「AWS KMS キーによるサーバー側の暗号化 (SSE-KMS) の使用」を参照してください。

テーブルとテーブルバケットでの SSE-KMS の仕組み

ディレクトリバケットでの SSE-KMS は、以下の点で汎用バケットでの SSE-KMS とは異なります。

- テーブルバケットと個々のテーブルの暗号化設定を指定できます。
- SSE-KMS では、カスタマーマネージドキーのみを使用できます。AWS マネージドキーはサポートされていません。
- AWS KMS キーにアクセスするには、特定のロールと AWS サービスプリンシパルにアクセス許可を付与する必要があります。詳細については、「S3 Tables の SSE-KMS 暗号化のアクセス許可要件」を参照してください。これには、以下へのアクセスの許可が含まれます。
  - S3 メンテナンスプリンシパル – 暗号化されたテーブルでテーブルメンテナンスを実行
  - S3 Tables 統合ロール – AWS 分析サービスで暗号化されたテーブルを使用
  - クライアントアクセスロール – Apache Iceberg クライアントから暗号化されたテーブルに直接アクセス
  - S3 メタデータプリンシパル – 暗号化された S3 メタデータテーブルを更新
- 暗号化されたテーブルは、テーブルレベルのキーを使用して AWS KMS へのリクエスト数を最小限に抑え、SSE-KMS で暗号化されたテーブルの操作をよりコスト効率の高いものにします。

テーブルバケットの SSE-KMS 暗号化

テーブルバケットを作成するときは、デフォルトの暗号化タイプとして SSE-KMS を選択し、暗号化に使用する特定の KMS キーを指定できます。テーブルバケット内に作成したすべてのテーブルは、テーブルバケットから暗号化設定を自動的に継承します。テーブルバケットのデフォル

トの暗号化設定は、AWS CLI、S3 API、または AWS SDK を使用していつでも変更または削除できます。テーブルバケットの暗号化設定を変更すると、変更後の設定はバケット内に作成した新しいテーブルにのみ適用されます。既存のテーブルの暗号化設定は変更されません。詳細については、「テーブルバケットの暗号化の指定」を参照してください。

テーブルの SSE-KMS 暗号化

バケットのデフォルトの暗号化設定に関係なく、個別のテーブルを別の KMS キーで暗号化することもできます。個別のテーブルの暗号化を設定するには、目的の暗号化キーをテーブルの作成時に指定する必要があります。既存のテーブルの暗号化を変更する場合は、目的のキーを使用してテーブルを作成し、古いテーブルから新しいテーブルにデータをコピーする必要があります。詳細については、「テーブルの暗号化の指定」を参照してください。

AWS KMS 暗号化を使用する場合、S3 Tables は、テーブルレベルの一意のデータキーを自動的に作成して各テーブルに関連する新しいオブジェクトを暗号化します。これらのキーの使用期間は限定され、暗号化オペレーション中の追加の AWS KMS リクエストの必要性を最小限に抑え、暗号化のコストを削減します。これは SSE-KMS の S3 バケットキー に似ています。

テーブルとテーブルバケットでの SSE-KMS の適用とスコープ設定

S3 Tables のリソースベースのポリシー、KMS キーポリシー、IAM アイデンティティベースのポリシー、またはこれらの任意の組み合わせを使用して、S3 テーブルとテーブルバケットでの SSE-KMS の使用を設定できます。テーブルのアイデンティティおよびリソースポリシーの詳細については、「S3 Tables のアクセス管理」を参照してください。キーポリシーの作成方法については、「AWS Key Management Service Developer Guide」の「Key policies」を参照してください。以下の例は、ポリシーを使用して SSE-KMS を適用する方法を示しています。

テーブルバケットポリシーを使用してすべてのテーブルに SSE-KMS を適用する

このテーブルバケットポリシーの例では、ユーザーが特定の AWS KMS キーでテーブルを暗号化しない限り、特定のテーブルバケット内にテーブルを作成できないようにします。このポリシーを使用するには、###############を独自の情報に置き換えます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceKMSEncryption",
      "Effect": "Deny",
      "Principal": "*",
```

```
      "Action": [
        "s3tables:CreateTable"
      ],
      "Resource": [
        "<table-bucket-arn>/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "s3tables:sseAlgorithm": "aws:kms",
          "s3tables:kmsKeyArn": "<kms-key-arn>"
        }
      }
    }
  ]
}
```

IAM ポリシーで SSE-KMS 暗号化を使用するようにユーザーに要求する

この IAM ID ポリシーでは、S3 Tables リソースを作成または設定するときに、特定の AWS KMS キーを暗号化に使用することをユーザーに要求します。このポリシーを使用するには、*##########*を独自の情報に置き換えます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RequireKMSKeyOnTables",
      "Action": [
          "s3tables:CreateTableBucket",
          "s3tables:PutTableBucketEncryption",
          "s3tables:CreateTable"
      ]
      "Effect": "Deny",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
            "s3tables:sseAlgorithm": "aws:kms",
            "s3tables:kmsKeyArn": "<key_arn>"
        }
      }
    }
  ]
}
```

KMS キーポリシーを使用してキーの使用を特定のテーブルバケットに制限する

この KMS キーポリシーの例では、特定のテーブルバケットの暗号化オペレーションにのみキーを使用することを特定のユーザーに許可します。このタイプのポリシーは、クロスアカウントシナリオでキーへのアクセスを制限するのに役立ちます。このポリシーを使用するには、*###############*を独自の情報に置き換えます。

```
{
  "Version": "2012-10-17",
  "Id": "Id",
  "Statement": [
    {
      "Sid": "AllowPermissionsToKMS",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:EncryptionContext:aws:s3:arn": "<table-bucket-arn>/*"
        }
      }
    }
  ]
}
```

テーブルとテーブルバケットの SSE-KMS 暗号化のモニタリングと監査

SSE-KMS で暗号化されたデータの AWS KMS キーの使用状況を監査するには、AWS CloudTrail ログを使用します。`GenerateDataKey` や `Decrypt` などの暗号化オペレーションに関するインサイトを得ることができます。CloudTrail は、イベント名、ユーザー名、イベントソースなど、検索をフィルタリングするための多数の属性値をサポートしています。

CloudTrail イベントを使用して、Amazon S3 のテーブルとテーブルバケットへの暗号化設定リクエストを追跡できます。CloudTrail ログでは、以下の API イベント名が使用されます。

- `s3tables:PutTableBucketEncryption`

- s3tables:GetTableBucketEncryption
- s3tables:DeleteTableBucketEncryption
- s3tables:GetTableEncryption
- s3tables:CreateTable
- s3tables:CreateTableBucket

> **Note**
>
> EventBridge はテーブルバケットではサポートされていません。

S3 Tables の SSE-KMS 暗号化のアクセス許可要件

S3 テーブルバケット内のテーブルで AWS Key Management Service (AWS KMS) キーによるサーバー側の暗号化 (SSE-KMS) を使用する場合は、アカウント内のさまざまな ID にアクセス許可を付与する必要があります。少なくとも、アクセスアイデンティティと S3 Tables メンテナンスプリンシパルには、キーへのアクセス権が必要です。ユースケースに応じて他のアクセス許可が必要になります。

必要なアクセス許可

KMS キーで暗号化されたテーブルにアクセスするには、そのキーに対する以下のアクセス許可が必要です。

- kms:GenerateDataKey
- kms:Decrypt

> **Important**
>
> テーブルで SSE-KMS を使用する場合、Amazon S3 Tables メンテナンスサービスプリンシパル (maintenance.s3tables.amazonaws.com) には、キーへのアクセス許可として kms:GenerateDataKey と kms:Decrypt が必要です。

追加のアクセス許可

ユースケースに応じて、以下の追加のアクセス許可が必要です。

- AWS 分析サービス統合のアクセス許可 – AWS 分析サービスで SSE-KMS で暗号化されたテーブルを使用する場合、統合ロールには KMS キーを使用するアクセス許可が必要です。
- 直接アクセスのアクセス許可 – Amazon S3 Tables の Iceberg REST エンドポイントまたは Apache Iceberg の Amazon S3 Tables カタログなどの方法で SSE-KMS で暗号化されたテーブルを直接使用する場合は、クライアントが使用する IAM ロールにキーへのアクセス許可が必要です。
- S3 メタデータテーブルのアクセス許可 – S3 メタデータテーブルで SSE-KMS 暗号化を使用する場合は、S3 メタデータサービスプリンシパル (`metadata.s3.amazonaws.com`) に KMS キーへのアクセス許可が必要です。これにより、S3 メタデータは暗号化されたテーブルを更新して、最新のデータ変更を反映できます。

> **Note**
>
> クロスアカウント KMS キーの場合、IAM ロールには、キーポリシーでのキーアクセス許可と明示的な認可の両方が必要です。KMS キーのクロスアカウントアクセス許可の詳細については、「AWS Key Management Service Service Developer Guide」の「Allowing external AWS accounts to use a KMS key」を参照してください。

トピック

- S3 Tables メンテナンスサービスプリンシパルに KMS キーへのアクセス許可を付与する
- 統合された AWS 分析サービスにおいて暗号化されたテーブルを使用するアクセス許可を IAM プリンシパルに付与する
- 暗号化されたテーブルを直接使用するアクセス許可を IAM プリンシパルに付与する
- S3 メタデータサービスプリンシパルに KMS キーを使用するアクセス許可を付与する

S3 Tables メンテナンスサービスプリンシパルに KMS キーへのアクセス許可を付与する

このアクセス許可は、SSE-KMS で暗号化されたテーブルを作成して、暗号化されたテーブルに対する圧縮、スナップショット管理、参照されていないファイルの削除などの自動テーブルメンテナンスを許可するために必要です。

> **Note**
>
> SSE-KMS で暗号化されたテーブルの作成をリクエストするたびに、S3 Tables は `maintenance.s3tables.amazonaws.com` プリンシパルが KMS キーにアクセスできるこ

とを確認します。この確認を行うために、テーブルバケットに 0 バイトのオブジェクトが一時的に作成されます。このオブジェクトは、参照されていないファイルの削除メンテナンスオペレーションによって自動的に削除されます。暗号化に指定した KMS キーにメンテナンスアクセス権がない場合、createTable オペレーションは失敗します。

SSE-KMS で暗号化されたテーブルへのメンテナンスアクセスを許可するには、次のキーポリシーの例を使用できます。このポリシーでは、maintenance.s3tables.amazonaws.com サービスプリンシパルに対して、特定のテーブルバケット内のテーブルを暗号化および復号するための特定の KMS キーを使用するアクセス許可が付与されます。ポリシーを使用するには、*##########*を独自の情報に置き換えます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EnableKeyUsage",
            "Effect": "Allow",
            "Principal": {
                "Service": "maintenance.s3tables.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "<kms-key-arn>",
            "Condition": {
                "StringLike": {
                    "kms:EncryptionContext:aws:s3:arn":"<table-or-table-bucket-arn>/*"
                }
            }
        }
    ]
}
```

統合された AWS 分析サービスにおいて暗号化されたテーブルを使用するアクセス許可を IAM プリンシパルに付与する

AWS 分析サービスで S3 テーブルを使用するには、テーブルバケットを Amazon SageMaker Lakehouse と統合します。この統合により、AWS 分析サービスはテーブルデータを自動的に検出

してアクセスできるようになります。統合の詳細については、「AWS 分析サービスで Amazon S3 Tables を使用する」を参照してください。

これらのサービスで SSE-KMS で暗号化されたテーブルを使用する場合、使用するロールには、暗号化オペレーションで AWS KMS キーを使用するアクセス許可が必要です。これらのアクセス許可は、統合中に作成した S3TablesRoleForLakeFormation ロール、または独自の IAM ロールに適用できます。

次のインライン IAM ポリシーの例を使用して、アカウント内の特定の KMS キーを暗号化オペレーションに使用するアクセス許可を S3TablesRoleForLakeFormation サービスロールに付与できます。ポリシーを使用するには、*############*を独自の値に置き換えます。

```
{
  "Sid": "AllowTableRoleAccess",
  "Effect": "Allow",
  "Principal": {
 "AWS": "arn:aws:iam::111122223333:role/service-role/S3TablesRoleForLakeFormation"
  },
  "Action": [
      "kms:GenerateDataKey",
      "kms:Decrypt"
  ],
  "Resource": "<kms-key-arn>"
}
```

暗号化されたテーブルを直接使用するアクセス許可を IAM プリンシパルに付与する

サードパーティーまたは直接アクセス方式を使用して暗号化されたテーブルを使用する場合は、使用するロールに対して KMS キーへのアクセスを許可する必要があります。以下の例は、IAM ポリシーまたは KMS キーポリシーを通じてアクセスを許可する方法を示しています。

IAM policy

このインラインポリシーを IAM ロールにアタッチして、KMS キーへのアクセスを許可します。このポリシーを使用するには、*##########*を独自の KMS キー arn に置き換えます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
        "Effect": "Allow",
        "Action": [
```

```
            "kms:Decrypt",
            "kms:GenerateDataKey"
         ],
        "Resource": "<kms-key-arn>"
        }
    ]
}
```

KMS key policy

このインラインポリシーを KMS キーにアタッチして、指定した AWS KMS ロールに対してキーの使用を許可します。このポリシーを使用するには、############を独自の IAM ロールに置き換えます。

```
{
    "Sid": "Allow use of the key",
    "Effect": "Allow",
    "Principal": {
        "AWS": [
            "arn:aws:iam::<catalog-account-id>:role/<role-name>"
        ]
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey",
    ],
    "Resource": "*"
}
```

S3 メタデータサービスプリンシパルに KMS キーを使用するアクセス許可を付与する

Amazon S3 に対して SSE-KMS で暗号化されたメタデータテーブルを更新し、これらのメタデータテーブルのメンテナンスを実行することを許可するには、次のキーポリシーの例を使用できます。このポリシーでは、metadata.s3.amazonaws.com および maintenance.s3tables.amazonaws.com サービスプリンシパルに対して、特定のキーを使用して特定のテーブルバケット内のテーブルを暗号化および復号することを許可します。ポリシーを使用するには、###############を独自の情報に置き換えます。

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Sid": "EnableKeyUsage",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "maintenance.s3tables.amazonaws.com",
                    "metadata.s3.amazonaws.com"
                ]
            },
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "<kms-key-arn>",
            "Condition": {
                "StringLike ": {
                    "kms:EncryptionContext:aws:s3:arn": "<table-or-table-bucket-arn>/*"
                }
            }
        }
    ]
}
```

テーブルバケットでの AWS KMS キーによるサーバー側の暗号化 (SSE-KMS) の指定

すべての Amazon S3 テーブルバケットにはデフォルトで暗号化が設定され、テーブルバケットに作成したすべての新しいテーブルは保管中に自動的に暗号化されます。Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3) は、すべてのディレクトリバケットのデフォルトの暗号化設定です。別の暗号化タイプを指定する場合は、AWS Key Management Service (AWS KMS) キーによるサーバー側の暗号化 (SSE-KMS) を使用できます。

`CreateTableBucket` または `CreateTable` リクエストで SSE-KMS 暗号化を指定することも、`PutTableBucketEncryption` リクエストでテーブルバケットのデフォルトの暗号化設定を指定することもできます。

> **Important**
>
> SSE-KMS で暗号化したテーブルとテーブルバケットの自動メンテナンスを許可するには、KMS キーを使用するアクセス許可を maintenance.s3tables.amazonaws.com サービスプリンシパルに付与する必要があります。詳細については、「S3 Tables の SSE-KMS 暗号化のアクセス許可要件」を参照してください。

テーブルバケットの暗号化の指定

新しいテーブルバケットを作成するときに、デフォルトの暗号化タイプとして SSE-KMS を指定できます。例については、「テーブルバケットの作成」を参照してください。テーブルバケットを作成したら、REST API オペレーション、AWS SDK、AWS Command Line Interface (AWS CLI) を使用して、デフォルトの暗号化設定として SSE-KMS の使用を指定できます。

> **Note**
>
> デフォルトの暗号化タイプとして SSE-KMS を指定する場合、暗号化に使用するキーは S3 Tables のメンテナンスサービスプリンシパルに対してアクセスを許可する必要があります。メンテナンスサービスプリンシパルにアクセス権がない場合、そのテーブルバケットにテーブルを作成することはできません。詳細については、「S3 Tables メンテナンスサービスプリンシパルに KMS キーへのアクセス許可を付与する」を参照してください。

AWS CLI の使用

次の AWS CLI コマンド例を使用するには、*###############*を独自の情報に置き換えます。

```
aws s3tables put-table-bucket-encryption \
    --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-table-bucket; \
    --encryption-configuration '{
        "sseAlgorithm": "aws:kms",
        "kmsKeyArn": "arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    }' \
    --region us-east-1
```

テーブルバケットのデフォルトの暗号化設定を削除するには、DeleteTableBucketEncryption API オペレーションを使用できます。暗号化設定を削除すると、テーブルバケットに作成した新しいテーブルでは、デフォルトの SSE-S3 暗号化が使用されます。

テーブルの暗号化の指定

SSE-KMS 暗号化は、クエリエンジン、REST API オペレーション、AWS SDK、AWS Command Line Interface (AWS CLI) を使用して新しいテーブルを作成するときに適用できます。テーブルの作成時に指定した暗号化設定は、テーブルバケットのデフォルトの暗号化設定よりも優先されます。

> **Note**
>
> テーブルに SSE-KMS 暗号化を使用する場合、暗号化に使用するキーでは、S3 Tables メンテナンスサービスプリンシパルにアクセスを許可する必要があります。メンテナンスサービスプリンシパルにアクセス権がない場合、テーブルを作成することはできません。詳細については、「S3 Tables メンテナンスサービスプリンシパルに KMS キーへのアクセス許可を付与する」を参照してください。

必要な アクセス許可

暗号化されたテーブルを作成するには、以下のアクセス許可が必要です。

- `s3tables:CreateTable`
- `s3tables:PutTableEncryption`

AWS CLI を使用する場合

次の AWS CLI の例では、基本スキーマを使用して新しいテーブルを作成し、カスタマーマネージド AWS KMS キーを使用してテーブルを暗号化します。このコマンドを使用するには、*##########*を独自の情報に置き換えます。

```
aws s3tables create-table \
  --table-bucket-arn "arn:aws:s3tables:Region:ownerAccountId:bucket/amzn-s3-demo-table-bucket" \
  --namespace "mydataset" \
  --name "orders" \
  --format "ICEBERG" \
  --encryption-configuration '{
    "sseAlgorithm": "aws:kms",
    "kmsKeyArn":
 "arn:aws:kms:Region:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  }' \
  --metadata '{
    "iceberg": {
      "schema": {
        "fields": [
          {
            "name": "order_id",
            "type": "string",
```

```
            "required": true
          },
          {
            "name": "order_date",
            "type": "timestamp",
            "required": true
          },
          {
            "name": "total_amount",
            "type": "decimal(10,2)",
            "required": true
          }
        ]
      }
    }
  }'
```

データ保護とは、転送中 (Amazon S3 とのデータの送受信) と保管中 (Amazon S3 データセンター内のディスクへの保存) のデータを保護することを指します。S3 Tables は、HTTPS 経由で Transport Layer Security (1.2 以降) を使用して、転送中のデータを常に保護します。S3 テーブルバケットに保管中のデータを保護するには、以下のオプションを使用できます。

Amazon S3 マネージドキーを用いたサーバー側の暗号化 (SSE-S3)

すべての Amazon S3 テーブルバケットには、デフォルトで暗号化が設定されます。サーバー側の暗号化のデフォルトのオプションは、Amazon S3 マネージド キー (SSE-S3) を使用しています。この暗号化は、別の暗号化形式を指定しない限り、S3 テーブルバケット内のすべてのテーブルに無料で適用されます。一意のキーで各オブジェクトを暗号化します。追加の保護措置として、SSE-S3 は定期的にローテーションされるルートキーを使ってキーそのものを暗号化します。SSE-S3 は、利用可能な最強のブロック暗号の 1 つである 256 ビットの 高度暗号化規格 (AES-256) を使用して、データを暗号化します。

AWS KMS キーによるサーバー側の暗号化 (SSE-KMS)

AWS Key Management Service (AWS KMS) キーによるサーバー側の暗号化 (SSE-KMS) を使用するようにテーブルバケットまたはテーブルを設定することもできます。AWS KMS のセキュリティ制御は、暗号化関連のコンプライアンス要件を満たすのに役立ちます。SSE-KMS では、以下の操作が可能であり、暗号化キーをより細かく制御できます。

- KMS キーの作成、表示、編集、モニタリング、有効化または無効化、更新、削除のスケジュールを行う。
- KMS キーの使用方法および使用者を制御するポリシーを定義する。

- キーの使用状況を AWS CloudTrail で追跡して、KMS キーが適切に使用されていることを確認する。

S3 Tables は、SSE-KMS でのカスタマーマネージドキーを使用したテーブルの暗号化をサポートしています。AWS マネージドキーはサポートされていません。S3 テーブルとテーブルバケットで SSE-KMS を使用する方法の詳細については、「テーブルバケットでの AWS KMS キーによるサーバー側の暗号化 (SSE-KMS) の使用」を参照してください。

S3 Tables のアクセス管理

S3 Tables リソースには、テーブルバケットとそれらに含まれるテーブルが含まれます。リソースを作成した AWS アカウントのルートユーザー (リソース所有者) と、必要なアクセス許可を持つそのアカウント内の AWS Identity and Access Management (IAM) ユーザーは、作成したリソースにアクセスできます。リソース所有者は、リソースにアクセスできる他のユーザーと、ユーザーがリソースに対して実行できるアクションを指定します。Amazon S3 には、S3 リソースへのアクセスを他のユーザーに許可するために使用できるさまざまなアクセス管理ツールがあります。以下のトピックでは、S3 Tables のリソース、IAM アクション、条件キーの概要について説明します。また、S3 Tables のリソースベースポリシーとアイデンティティベースのポリシーの両方の例も示します。

トピック

- リソース
- S3 Tables のアクション
- S3 Tables の条件キー
- S3 Tables の IAM アイデンティティベースのポリシー
- S3 Tables 用のリソースベースのポリシー
- S3 Tables の AWS マネージドポリシー
- SQL セマンティクスを使用したアクセス権の付与

リソース

S3 Tables リソースには、テーブルバケットとそれらに含まれるテーブルが含まれます。

- テーブルバケット – テーブルバケットは、汎用 S3 バケットのセルフマネージドテーブルと比較して、テーブルとプロバイダーの 1 秒あたりのトランザクション (TPS) が高く、クエリスループットが向上するように特別に設計されています。テーブルバケットは、Amazon S3 汎用バケットと同じ耐久性、可用性、スケーラビリティ、パフォーマンス特性を提供します。

- テーブル – テーブルバケット内のテーブルは Apache Iceberg 形式で保存されます。これらのテーブルは、Iceberg をサポートするクエリエンジンで標準 SQL を使用してクエリできます。

テーブルとテーブルバケットの Amazon リソースネーム (ARN) には、s3tables 名前空間、AWS リージョン、AWS アカウント ID、バケット名が含まれます。テーブルとテーブルバケットにアクセスしてアクションを実行するには、次の ARN 形式を使用する必要があります。

- テーブル ARN 形式:

```
arn:aws:s3tables:us-west-2:111122223333:bucket/amzn-s3-demo-bucket/
table/demo-tableID
```

S3 Tables のアクション

アイデンティティベースのポリシーまたはリソースベースのポリシーで、特定の IAM プリンシパルに対して、どの S3 Tables アクションを許可または拒否するかを定義します。テーブルアクションは、バケットおよびテーブルレベルの API オペレーションに対応しています。すべてのアクションは、一意の IAM 名前空間 s3tables の一部です。

ポリシーでアクションを使用する場合は、通常、同じ名前の API オペレーションまたは CLI コマンドへのアクセスを許可または拒否します。ただし、単独のアクションが複数のオペレーションへのアクセスを制御する場合もあります。例えば、s3tables:GetTableData アクションには、GetObject、ListParts、ListMultiparts API オペレーションのアクセス許可が含まれます。

テーブルバケットでサポートされているアクションは次のとおりです。IAM ポリシーまたはリソースポリシーの Action エレメントでは、以下のアクションを指定できます。

アクション	説明	アクセスレベル	クロスアカウントアクセス
s3tables:CreateTableBucket	新しいバケットを作成するアクセス許可を付与	Write	いいえ

アクション	説明	アクセスレベル	クロスアカウントアクセス
s3tables:GetTableBucket	テーブルバケットARN、テーブルバケット名、作成日を取得するアクセス許可を付与	Write	はい
s3tables:ListTableBuckets	このアカウント内のすべてのテーブルバケットを一覧表示するアクセス許可を付与	Read	いいえ
s3tables:CreateNamespace	テーブルバケットに名前空間を作成するアクセス許可を付与	Read	はい
s3tables:GetNamespace	名前空間の詳細を取得するアクセス許可を付与	Read	はい
s3tables:ListNamespaces	テーブルバケット上のすべての名前空間を一覧表示するアクセス許可を付与	Read	はい

アクション	説明	アクセスレベル	クロスアカウントアクセス
s3tables:DeleteNamespace	テーブルバケット内の名前空間を削除するアクセス許可を付与	Write	はい
s3tables:DeleteTableBucket	バケットを削除するアクセス許可を付与	Write	はい
s3tables:PutTableBucketPolicy	バケットポリシーを追加または置き換えるアクセス許可を付与	Permissions Management	いいえ
s3tables:GetTableBucketPolicy	バケットポリシーを取得するアクセス許可を付与	Read	いいえ
s3tables:DeleteTableBucketPolicy	バケットポリシーを削除するアクセス許可を付与	Permissions Management	いいえ
s3tables:GetTableBucketMaintenanceConfiguration	テーブルバケットのメンテナンス設定を取得するアクセス許可を付与	Read	はい

アクション	説明	アクセスレベル	クロスアカウントアクセス
s3tables:PutTableBucketMaintenanceConfiguration	テーブルバケットのメンテナンス設定を追加または置き換えるアクセス許可を付与	Write	はい
s3tables:PutTableBucketEncryption	テーブルバケットのメンテナンス設定を追加または置換するアクセス許可を付与	Write	いいえ
s3tables:GetTableBucketEncryption	テーブルバケットの暗号化設定を取得するアクセス許可を付与	Read	いいえ
s3tables:DeleteTableBucketEncryption	テーブルバケットの暗号化設定を削除するアクセス許可を付与	Write	いいえ

デーブルでは次のアクションがサポートされています。

アクション	説明	アクセスレベル	クロスアカウントアクセス
s3tables:GetTableMaintenanceConfiguration	テーブルのメンテナンス設定を取得するアクセス許可を付与	Read	はい
s3tables:PutTableMaintenanceConfiguration	テーブルのメンテナンス設定を追加または置き換えるアクセス許可を付与	Write	はい
s3tables:PutTablePolicy	テーブルポリシーを追加または置き換えるアクセス許可を付与	Permissions Management	いいえ
s3tables:GetTablePolicy	テーブルポリシーを取得するアクセス許可を付与	Read	いいえ
s3tables:DeleteTablePolicy	テーブルポリシーを削除するアクセス許可を付与	Permissions management	いいえ
s3tables:CreateTable	テーブルバケットのテーブルを作成するアクセス許可を付与	Write	はい

アクション	説明	アクセスレベル	クロスアカウントアクセス
s3tables:GetTable	テーブル情報を取得するアクセス許可を付与	Read	はい
s3tables:GetTableMetadataLocation	テーブルルートポインタ (メタデータファイル) を取得するアクセス許可を付与	Read	はい
s3tables:ListTables	テーブルバケット内のすべてのテーブルを一覧表示するアクセス許可を付与	Read	はい
s3tables:RenameTable	テーブルの名前を変更するアクセス許可を付与	Write	はい
s3tables:UpdateTableMetadataLocation	テーブルルートポインタ (メタデータファイル) を更新するアクセス許可を付与	Write	はい

アクション	説明	アクセスレベル	クロスアカウントアクセス
s3tables:GetTableData	テーブルバケットに保存されているテーブルメタデータとデータオブジェクトを読み取るアクセス許可を付与	Read	はい
s3tables:PutTableData	テーブルバケットに保存されているテーブルメタデータとデータオブジェクトを書き込むアクセス許可を付与	Write	はい
s3tables:GetTableEncryption	テーブルの暗号化設定を取得するアクセス許可を付与	Write	いいえ
s3tables:PutTableEncryption	テーブルに暗号化を追加するアクセス許可を付与	Write	いいえ

テーブルレベルの読み取りおよび書き込みアクションを実行するために、S3 Tables は GetObject や PutObject などの Amazon S3 API オペレーションをサポートしています。次の表に、オブジェクトレベルのアクションのリストを示します。テーブルに読み取りおよび書き込みアクセス許可を付与する場合は、次のアクションを使用します。

アクション	S3 オブジェクト API		
s3tables:GetTableData	GetObject, ListParts, HeadObject		
s3tables:PutTableData	PutObject, CreateMultipartUpload, CompleteMultipartUpload, UploadPart, AbortMultipartUpload		

例えば、ユーザーが GetTableData アクセス許可を持っている場合、メタデータファイル、マニフェスト、マニフェストリストファイル、parquet データファイルなど、テーブルに関連付けられているすべてのファイルを読み取ることができます。

S3 Tables の条件キー

S3 Tables は、AWS グローバル条件コンテキストキーをサポートしています。

さらに、S3 Tables では、アクセスポリシーで使用できる以下の条件キーを定義します。

条件キー	説明	[Type] (タイプ)	
s3tables:tableName	テーブルバケット内のテーブルの名前でアクセスをフィルタリングします。 s3tables:tableName 条件キーを使用して、この名前条件を満たすテーブルのみにユーザーまたはアプリケーションのアクセスを制限する IAM またはテーブルバケットポリシーを記述できます。 s3tables:tableName 条件キーを使用してアクセスを制御すると、テーブル名の変更がこれらのポリシーに影響を与える可能性があることに	String	

条件キー	説明	[Type] (タイプ)	
	注意してください。 値の例: `"s3tables:tableName":"department*"`		

条件キー	説明	[Type] (タイプ)	
s3tables:namespace	テーブルバケットで作成された名前空間でアクセスをフィルタリングします。 s3tables:namespace 条件キーを使用して、特定の名前空間の一部であるテーブルへのユーザーまたはアプリケーションのアクセスを制限する IAM、テーブル、またはテーブルバケットポリシーを記述できます。値の例: "s3tables:namespace":"hr" s3tables:namespace 条件キーを使用してアクセスを制御すると、名前空間の変更が	String	

条件キー	説明	[Type] (タイプ)	
	これらのポリシーに影響を与える可能性があることに注意してください。		

条件キー	説明	[Type] (タイプ)	
s3tables:SSEAlgorithm	テーブルの暗号化に使用するサーバー側の暗号化アルゴリズムでアクセスをフィルタリングします。 s3tables:SSEAlgorithm 条件キーを使用して、特定の暗号化タイプで暗号化されたテーブルにユーザーまたはアプリケーションのアクセスを制限する IAM、テーブル、またはテーブルバケットポリシーを記述できます。値の例: "s3tables:SSEAlgorithm":"aws:kms" s3tables:SSEAlgorithm 条件	String	

条件キー	説明	[Type] (タイプ)	
	キーを使用してアクセスを制御する場合、暗号化の変更がこれらのポリシーに影響を与える可能性がある点に注意することが重要です。		

条件キー	説明	[Type] (タイプ)	
s3tables:KMSKeyArn	テーブルの暗号化に使用するキーの AWS KMS キー ARN でアクセスをフィルタリングする s3tables:KMSKeyArn 条件キーを使用して、特定の KMS キーで暗号化したテーブルにユーザーまたはアプリケーションのアクセスを制限する IAM、テーブル、またはテーブルバケットポリシーを記述できます。 s3tables:KMSKeyArn 条件キーを使用してアクセスを制御する場合、KMS キーの変更がこれらのポリ	ARN	

条件キー	説明	[Type] (タイプ)	
	シーに影響を与える可能性がある点に注意することが重要です。		

S3 Tables の IAM アイデンティティベースのポリシー

デフォルトでは、ユーザーおよびロールにはテーブルとテーブルバケットを作成または変更するアクセス許可はありません。また、S3 コンソール、AWS Command Line Interface (AWS CLI)、または Amazon S3 REST API を使用してタスクを実行しません。テーブルバケットとテーブルを作成してアクセスするには、AWS Identity and Access Management (IAM) 管理者が IAM ロールまたはユーザーに必要なアクセス許可を付与する必要があります。これらサンプルの JSON ポリシードキュメントを使用して、IAM アイデンティティベースのポリシーを作成する方法については、IAM ユーザーガイドのIAM ポリシーの作成を参照してください。

次のトピックでは、IAM アイデンティティベースのポリシーの例を示します。次のポリシー例を使用する際は、###############を独自の情報に置き換えます。

トピック

- 例 1: テーブルバケットの作成と使用のためのアクセスを許可する
- 例 2: テーブルバケット内のテーブルを作成および使用するためのアクセスを許可する

例 1: テーブルバケットの作成と使用のためのアクセスを許可する

.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "AllowBucketActions",
        "Effect": "Allow",
        "Action": [
            "s3tables:CreateTableBucket",
            "s3tables:PutTableBucketPolicy",
            "s3tables:GetTableBucketPolicy",
            "s3tables:ListTableBuckets",
```

```
            "s3tables:GetTableBucket"
        ],

        "Resource": "arn:aws:s3tables:region:account_id:bucket/*"
    }]
}
```

例 2: テーブルバケット内のテーブルを作成および使用するためのアクセスを許可する

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Sid": "AllowBucketActions",
             "Effect": "Allow",
             "Action": [
                 "s3tables:CreateTable",
                 "s3tables:PutTableData",
                 "s3tables:GetTableData",
                 "s3tables:GetTableMetadataLocation",
                 "s3tables:UpdateTableMetadataLocation",
                 "s3tables:GetNamespace",
                 "s3tables:CreateNamespace"
             ],

             "Resource": [
               "arn:aws:s3tables:region:account_id:bucket/amzn-s3-demo-bucket",
               "arn:aws:s3tables:region:account_id:bucket/amzn-s3-demo-bucket/table/*"
            ]
         }
     ]
 }
```

S3 Tables 用のリソースベースのポリシー

S3 Tables は、テーブルバケットとテーブルへのアクセスを管理するためのリソースベースのポリシー (テーブルバケットポリシーとテーブルポリシー) を提供します。テーブルバケットポリシーを使用して、テーブルバケット、名前空間、またはテーブルレベルで API アクセス許可を付与できます。テーブルバケットにアタッチされたアクセス許可は、ポリシー定義に応じて、バケット内のすべてのテーブルまたはバケット内の特定のテーブルに適用できます。テーブルポリシーを使用して、テーブルレベルでアクセス許可を付与できます。

S3 Tables は、リクエストを受け取ると、まずリクエスタに必要なアクセス許可があることを確認します。リクエストを許可するかどうかを決定する際に、関連するすべてのアクセスポリシー、ユーザーポリシー、リソースベースのポリシー (IAM ユーザーポリシー、IAM ロールポリシー、テーブルバケットポリシー、テーブルポリシー) を評価します。例えば、テーブルバケットポリシーが、バケット内のテーブル (DeleteTable を含む) に対してすべてのアクションを実行するアクセス許可をユーザーに付与しているが、個々のテーブルにすべてのユーザーの DeleteTable アクションを拒否するテーブルポリシーがある場合、そのユーザーはテーブルを削除できません。

次のトピックでは、テーブルおよびテーブルバケットポリシーの例を示します。これらのポリシーを使用するには、###############を独自の情報に置き換えます。

> **Note**
>
> - テーブルを変更するアクセス許可を付与するすべてのポリシーには、GetTableMetadataLocation がテーブルのルートファイルにアクセスするためのアクセス許可を含める必要があります。詳細については、「GetTableMetadataLocation」を参照してください。
> - テーブルで書き込みまたは削除アクティビティを実行するたびに、アクセスポリシーに UpdateTableMetadataLocation へのアクセス許可を含めます。
> - バケットレベルのアクションへのアクセスを管理するにはテーブルバケットポリシーを使用し、テーブルレベルのアクションへのアクセスを管理するにはテーブルポリシーを使用することをお勧めします。複数のテーブルで同じアクセス許可のセットを定義する場合は、テーブルバケットポリシーを使用することをお勧めします。

トピック

- 例 1: テーブルバケットポリシーで、アカウント内のバケットの PutBucketMaintenanceConfiguration へのアクセスを許可する
- 例 2: hr 名前空間に保存されているテーブルへの読み取り (SELECT) アクセスを許可するテーブルバケットポリシー
- 例 3: ユーザーがテーブルを削除できるようにするテーブルポリシー

例 1: テーブルバケットポリシーで、アカウント内のバケットの **PutBucketMaintenanceConfiguration** へのアクセスを許可する

次の例では、テーブルバケットポリシーは、PutBucketMaintenanceConfiguration へのアクセスを許可することで、IAM data steward がアカウント内のすべてのバケットの参照されていないオブジェクトを削除することを許可します。

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Effect": "Allow",
             "Principal": {
               "AWS": "arn:aws:iam::account_id:role/datasteward"
             },
             "Action": ["s3tables:PutTableBucketMaintenanceConfiguration"],
             "Resource":"arn:aws:s3tables:region:account_id:bucket/*"
     }]
 }
```

例 2: **hr** 名前空間に保存されているテーブルへの読み取り (SELECT) アクセスを許可するテーブルバケットポリシー

次の例では、テーブルバケットポリシーは、AWS アカウント ID 123456789012 のユーザーである Jane がテーブルバケットの hr 名前空間に保存されているテーブルにアクセスすることを許可します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:user/Jane"
            },
            "Action": [
                "s3tables:GetTableData",
                "s3tables:GetTableMetadataLocation"
            ],
            "Resource": "arn:aws:s3tables:region:account_id:bucket/amzn-s3-demo-table-
bucket/table/*",
            "Condition": {
```

```
                "StringLike": {"s3tables:namespace": "hr"}
            }
        }
    ]
}
```

例 3: ユーザーがテーブルを削除できるようにするテーブルポリシー

次の例は、IAM ロール `data steward` がテーブルを削除できるようにするテーブルポリシーです。

```
{
     "Version": "2012-10-17",
     "Id": "DeleteTable",
     "Statement": [
      {
       "Effect": "Allow",
       "Principal": {
         "AWS": "arn:aws:iam::account_id:role/datasteward"
        },
        "Action": [
           "s3tables:DeleteTable",
           "s3tables:UpdateTableMetadataLocation",
           "s3tables:PutTableData",
           "s3tables:GetTableMetadataLocation"

        ],
        "Resource":"arn:aws:s3tables:region:account_id:bucket/amzn-s3-demo-bucket1/
table/tableUUID"
     }]
}
```

S3 Tables の AWS マネージドポリシー

AWS マネージドポリシーは、AWS が作成および管理するスタンドアロンポリシーです。AWS マネージドポリシーは、多くの一般的なユースケースに対してアクセス許可を提供するように設計されているため、ユーザー、グループ、ロールへのアクセス権の割り当てを開始できます。

AWS マネージドポリシーは、ご利用の特定のユースケースに対して最小特権のアクセス許可を付与しない場合があることにご注意ください。これは、すべての AWS ユーザーが使用できるようになるのを避けるためです。ユースケースに固有のカスタマー管理ポリシーを定義して、アクセス許可を絞り込むことをお勧めします。

AWS マネージドポリシーで定義されたアクセス許可は変更できません。AWS が AWS マネージドポリシーに定義されている権限を更新すると、更新はポリシーがアタッチされているすべてのプリンシパルアイデンティティ (ユーザー、グループ、ロール) に影響します。新しい AWS のサービス を起動するか、既存のサービスで新しい API オペレーションが使用可能になると、AWS が AWS マネージドポリシーを更新する可能性が最も高くなります。

詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」を参照してください。

AWS マネージドポリシー: AmazonS3TablesFullAccess

AmazonTablesS3FullAccess ポリシーを IAM アイデンティティにアタッチできます。このポリシーは、Amazon S3 Tables への完全なアクセスを可能にするアクセス許可を付与します。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "s3tables:*"
   ],
   "Resource": "*"
  }
 ]
}
```

AWS マネージドポリシー: AmazonS3TablesReadOnlyAccess

AmazonS3TablesReadOnlyAccess ポリシーを IAM アイデンティティにアタッチできます。このポリシーは、Amazon S3 Tables への読み取り専用アクセスを可能にするアクセス許可を付与します。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "s3tables:Get*",
    "s3tables:List*"
   ],
```

```
    "Resource": "*"
   }
  ]
}
```

AWS マネージドポリシーに対する Amazon S3 Tables の更新

Amazon S3 Tables の AWS マネージドポリシーの更新に関する詳細を、S3 Tables がこれらの変更の追跡を開始した以降の分について表示します。

変更	説明	日付
Amazon S3 Tables に AmazonTablesS3FullAccess が追加されました。	S3 Tables に、AmazonTablesS3FullAccess という新しい AWS 管理ポリシーが追加されました。このポリシーは、Amazon S3 Tables への完全なアクセスを可能にするアクセス許可を付与します。	2024 年 12 月 3 日
Amazon S3 Tables に AmazonS3TablesReadOnlyAccess が追加されました。	S3 Tables に、AmazonS3TablesReadOnlyAccess という新しい AWS 管理ポリシーが追加されました。このポリシーは、Amazon S3 Tables への読み取り専用アクセスを可能にするアクセス許可を付与します。	2024 年 12 月 3 日
Amazon S3 Tables で変更の追跡を開始しました。	Amazon S3 Tables が AWS マネージドポリシーの変更の追跡を開始しました。	2024 年 12 月 3 日

SQL セマンティクスを使用したアクセス権の付与

テーブルおよびテーブルバケットポリシーで SQL セマンティクスを使用して、テーブルにアクセス許可を付与できます。使用できる SQL セマンティクスの例

は、CREATE、INSERT、DELETE、UPDATE、ALTER です。次の表は、ユーザーにアクセス許可を付与するために使用できる SQL セマンティクスに関連付けられた API アクションのリストを示しています。

S3 Tables は、SQL セマンティクスを使用したアクセス許可を部分的にサポートしています。例えば、CreateTable API はテーブルバケットに空のテーブルのみを作成します。テーブルスキーマを設定するには、UpdateTableMetadata、PutTableData、GetTableMetadataLocation などの追加のアクセス許可が必要です。これらの追加のアクセス許可は、テーブルに行を挿入するためのアクセス権もユーザーに付与することを意味します。SQL セマンティクスのみに基づいてアクセスを管理する場合は、AWS Lake Formation または S3 Tables と統合されたサードパーティーソリューションを使用することをお勧めします。

テーブルレベルのアクティビティ	IAM アクション		
SELECT	s3tables:GetTableData , s3tables:GetTableMetadataLocation		
CREATE	s3tables:CreateTable , s3tables:UpdateTableMetadataLocation , s3tables:PutTableData , s3tables:GetTableM		

テーブルレベルのアクティビティ	IAM アクション		
	etadataLocation ,		
INSERT	s3tables:UpdateTableMetadataLocation , s3tables:PutTableData , s3tables:GetTableMetadataLocation		
UPDATE	s3tables:UpdateTableMetadataLocation , s3tables:PutTableData , s3tables:GetTableMetadataLocation		

テーブルレベルのアクティビティ	IAM アクション		
ALTER,RENAME	s3tables:UpdateTableMetadataLocation , s3tables:PutTableData , s3tables:GetTableMetadataLocation , s3tables:RenameTable		
DELETE,DROP	s3tables:DeleteTable , s3tables:UpdateTableMetadataLocation , s3tables:PutTableData , s3tables:GetTableMetadataLocation		

S3 Tables の VPC 接続

S3 Tables のすべてのテーブルは Apache Iceberg 形式で、2 種類の S3 オブジェクトで構成されます。これら 2 種類のオブジェクトは、異なる時点でデータファイルに関する情報を追跡するデータとメタデータファイルを保存するデータファイルです。すべてのテーブルバケット、名前空間、テーブルオペレーション (`CreateNamespace`、`CreateTable` など) は S3 Tables エンドポイント (`s3tables.region.amazonaws.com`) を介してルーティングされ、データとメタデータファイルを読み書きするすべてのオブジェクトレベルのオペレーションは引き続き S3 サービスエンドポイント (`s3.region.amazonaws.com`) を介してルーティングされます。

S3 Tables にアクセスするために、Amazon S3は AWS PrivateLink を使用して、ゲートウェイエンドポイントとインターフェイスエンドポイントの 2 つのタイプの VPC エンドポイントをサポートしています。ゲートウェイエンドポイントは、AWS ネットワーク経由で VPC から S3 にアクセスするために、ルートテーブルで指定するゲートウェイです。インターフェイスエンドポイントは、プライベート IP アドレスを使用して、VPC 内、オンプレミス、または VPC ピアリングや AWS Transit Gateway を使用する別の AWS リージョンにある VPC から Amazon S3 にリクエストをルーティングすることにより、ゲートウェイエンドポイントの機能を拡張します。

VPC から S3 Tables にアクセスするには、2 つの VPC エンドポイント (1 つは S3 用、もう 1 つは S3 Tables 用) を作成することをお勧めします。ファイル (オブジェクト) レベルのオペレーションを S3 にルーティングするゲートウェイまたはインターフェイスエンドポイント、およびバケットおよびテーブルレベルのオペレーションを S3 Tables にルーティングするインターフェイスエンドポイントを作成できます。S3 を使用して、ファイルレベルのリクエストに VPC エンドポイントを作成して使用できます。詳細については、「AWS PrivateLink ユーザーガイド」の「Gateway endpoints」を参照してください。

AWS PrivateLink を使用して S3 Tables のエンドポイントを作成および操作する方法の詳細については、以下のトピックを参照してください。VPC インターフェイスエンドポイントを作成するには、AWS PrivateLink ガイドの「VPC エンドポイントの作成」を参照してください。

トピック

- S3 Tables の VPC エンドポイントの作成
- AWS CLI を使用したエンドポイントを介するテーブルバケットとテーブルへのアクセス
- クエリエンジン使用時の VPC ネットワークの設定
- VPC ネットワーク内の S3 Tables へのアクセスの制限

S3 Tables の VPC エンドポイントの作成

VPC エンドポイントを作成すると、S3 Tables はエンドポイント固有の 2 つのタイプの DNS 名 (リージョンおよびゾーン) を生成します。

- リージョン DNS 名は次の形式です。`VPCendpointID.s3tables.AWSregion.vpce.amazonaws.com`。例えば、VPC エンドポイント ID `vpce-1a2b3c4d` の場合、生成される DNS 名は `vpce-1a2b3c4d-5e6f.s3tables.us-east-1.vpce.amazonaws.com` に似ている場合があります。
- ゾーン DNS 名は次の形式です。`VPCendpointID-AvailabilityZone.s3tables.AWSregion.vpce.amazonaws.com`。例えば、VPC エンドポイント ID `vpce-1a2b3c4d-5e6f.` の場合、生成される DNS 名は `vpce-1a2b3c4d-5e6f-us-east-1a.s3tables.us-east-1.vpce.amazonaws.com` に似ている場合があります。

  ゾーン DNS 名にはアベイラビリティーゾーンが含まれます。ゾーン DNS 名は、アーキテクチャがアベイラビリティーゾーンを分離する場合に使用できます。エンドポイント固有の S3 DNS 名は、S3 パブリック DNS ドメインから解決できます。

また、プライベート DNS オプションを使用すると、VPC エンドポイント経由の S3 トラフィックのルーティングが簡単になり、アプリケーションで使用できる最も低コストのネットワークパスを活用できます。プライベート DNS は、S3 Tables のパブリックエンドポイント、例えば `s3tables.region.amazonaws.com` を VPC のプライベート IP にマッピングします。プライベート DNS オプションを使用すると、インターフェイスエンドポイントのエンドポイント固有の DNS 名を使用するように S3 クライアントを更新することなく、Regional S3 トラフィックをルーティングできます。

> **Note**
>
> AWS PrivateLink for Amazon S3 は Amazon S3 デュアルスタックエンドポイントの使用をサポートしていません。詳細については、「Amazon S3 API リファレンス」の「Using Amazon S3 dual-stack endpoints」を参照してください。

AWS CLI を使用したエンドポイントを介するテーブルバケットとテーブルへのアクセス

AWS Command Line Interface (AWS CLI) を使用して、インターフェイスエンドポイントを介してテーブルバケットとテーブルにアクセスできます。AWS CLI を使用すると、aws s3 コマンドは Amazon S3 エンドポイントを介してトラフィックをルーティングします。aws s3tables AWS CLI コマンドは Amazon S3 Tables エンドポイントを使用します。

s3tables VPC エンドポイントの例は、vpce-0123456afghjipljw-nmopsqea.s3tables.region.vpce.amazonaws.com です。

s3tables VPC エンドポイントにはバケット名は含まれません。aws s3tables AWS CLI コマンドを使用して s3tables VPC エンドポイントにアクセスできます。

s3 VPC エンドポイントの例は、amzn-s3-demo-bucket.vpce-0123456afghjipljw-nmopsqea.s3.region.vpce.amazonaws.com です。

aws s3 AWS CLI コマンドを使用して s3 VPC エンドポイントにアクセスできます。

AWS CLI の使用

AWS CLI を使用してインターフェイスエンドポイントを介してテーブルバケットとテーブルにアクセスするには、-region- および --endpoint-url パラメータを使用します。テーブルバケットとテーブルレベルのアクションを実行するには、S3 Tables エンドポイント URL を使用します。オブジェクトレベルのアクションを実行するには、Amazon S3 エンドポイント URL を使用します。

次の例では、*###############*を独自の情報に置き換えます。

[例 1: エンドポイント URL を使用したアカウント内のテーブルバケットのリスト化]

```
aws s3tables list-table-buckets --endpoint https://vpce-0123456afghjipljb-
aac.s3tables.us-east-1.vpce.amazonaws.com –region us-east-1
```

[例 2: エンドポイント URL を使用したバケット内のテーブルのリスト化]

```
aws s3tables list-tables --table-bucket-arn arn:aws:s3tables:us-
east-1:123456789301:bucket/amzn-s3-demo-bucket --endpoint
 https://vpce-0123456afghjipljb-aac.s3tables.us-east-1.vpce.amazonaws.com --region us-
east-1
```

クエリエンジン使用時の VPC ネットワークの設定

クエリエンジンを使用する場合は、次のステップに従って、VPC ネットワークを設定します。

1. 開始するには、VPC を作成または更新します。詳細については、「Create a VPC (VPC を作成する)」を参照してください。
2. S3 Tables にルーティングするテーブルおよびテーブルバケットレベルのオペレーションの場合は、新しいインターフェイスエンドポイントを作成します。詳細については、「インターフェイス VPC エンドポイントを使用して AWS サービスにアクセスする」を参照してください。
3. Amazon S3 にルーティングするすべてのオブジェクトレベルのオペレーションで、ゲートウェイエンドポイントまたはインターフェイスエンドポイントを作成します。ゲートウェイエンドポイントの詳細については、「Create a gateway endpoint」を参照してください。
4. 次に、データリソースを設定し、Amazon EMR クラスターを起動します。詳細については、「Amazon EMR の開始方法」を参照してください。
5. その後、VPC エンドポイントから DNS 名を選択して、追加の設定で Spark アプリケーションを送信できます。例えば、`spark.sql.catalog.ice_catalog.s3tables.endpoint` および `https://interface-endpoint.s3tables.us-east-1.vpce.amazonaws.com` です。詳細については、「Submit work to your Amazon EMR cluster」を参照してください。

VPC ネットワーク内の S3 Tables へのアクセスの制限

リソースベースのポリシーと同様に、テーブルとテーブルバケットへのアクセスを制御するエンドポイントポリシーを VPC エンドポイントにアタッチできます。次の例では、インターフェイスエンドポイントポリシーは特定のテーブルバケットのみへのアクセスを制限します。

```
{
    "Version": "2012-10-17",
    "Id": "Policy141511512309",
    "Statement": [{
        "Sid": "Access-to-specific-bucket-only",
        "Principal": "*",
        "Action": "s3tables:*",
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3tables:region:account_id:bucket/amzn-s3-demo-bucket",
            "arn:aws:s3tables:region:account_id:bucket/amzn-s3-demo-bucket/*"
        ]
    }]
```

```
}
```

S3 Tables のセキュリティに関する考慮事項と制限事項

次のリストでは、S3 Tables でサポートされていない、または制限されているセキュリティおよびアクセスコントロールの機能について説明します。

- パブリックアクセスポリシーはサポートされていません。ユーザーは、バケットポリシーまたはテーブルポリシーを変更して、パブリックアクセスを許可することはできません。
- テーブルに関連付けられたオブジェクトにアクセスするための署名付き URL はサポートされていません。
- タグは、テーブルバケットとテーブルではサポートされていません。したがって、属性ベースのアクセスコントロールとタグベースの割り当てのサポートは利用できません。
- HTTP 経由で行われたリクエストはサポートされていません。Amazon S3 は、HTTP 経由で行われたすべてのリクエストに対して HTTP リダイレクトで自動的に応答し、リクエストを HTTPS にアップグレードします。
- REST API を使用してアクセスポイントへのリクエストを行う場合は、AWS Signature Version 4 を使用する必要があります。
- インターネットプロトコルバージョン 6 (IPv6) を介したリクエストは、テーブルストレージエンドポイントを介したオブジェクトレベルのアクションでのみサポートされ、テーブルレベルおよびバケットレベルのアクションではサポートされません。
- テーブルバケットとテーブルアクセスポリシーのサイズは 20 KB に制限されています。

S3 Tablesの AWS CloudTrail を使用したログ記録

Amazon S3 は、ユーザー、ロール、または AWS のサービスによって実行されたアクションのレコードを提供するサービスである AWS CloudTrail と統合されています。Amazon S3 へのすべての API コールをイベントとしてキャプチャします。CloudTrail で収集された情報を使用して、Amazon S3 に対するリクエスト、リクエスト元の IP アドレス、リクエストの作成日時、その他の詳細を確認できます。サポートされているイベントアクティビティが Amazon S3 で発生すると、そのアクティビティは CloudTrail イベントに記録されます。AWS CloudTrail 証跡を使用して、S3 Tables の管理イベントとデータイベントを記録できます。詳細については、「AWS CloudTrail ユーザーガイド」の「Amazon S3 CloudTrail イベント」および「AWS CloudTrail とは」を参照してください。

S3 Tables の CloudTrail 管理イベント

管理イベントでは、AWS アカウントのリソースで実行される管理オペレーションについての情報が得られます。

CloudTrail は、デフォルトで S3 Tables の管理イベントを ログ記録します。S3 Tables の CloudTrail 管理イベントの `eventsource` は `s3tables.amazonaws.com` です。AWS アカウントのセットアップ時には、CloudTrail 管理イベントはデフォルトで有効になっています。次の管理イベントが CloudTrail に記録されます。

- `CreateNamespace`
- `CreateTable`
- `CreateTableBucket`
- `DeleteNamespace`
- `DeleteTable`
- `DeleteTableBucket`
- `DeleteTableBucketPolicy`
- `DeleteTablePolicy`
- `GetNamespace`
- `GetTable`
- `GetTableBucket`
- `GetTableBucketMaintenanceConfiguration`
- `GetTableBucketPolicy`
- `GetTableMaintenanceConfiguration`
- `GetTableMaintenanceJobStatus`
- `GetTableMetadataLocation`
- `GetTablePolicy`
- `ListNamespaces`
- `ListTableBuckets`
- `ListTables`
- `PutTableBucketMaintenanceConfiguration`
- `PutTableMaintenanceConfiguration`

- PutBucketPolicy
- PutTablePolicy
- RenameTable
- UpdateTableMetadataLocation

CloudTrail 管理イベントの詳細については、「AWS CloudTrail ユーザーガイド」の「管理イベントのログ記録」を参照してください。

S3 Tables の CloudTrail データイベント

データイベントでは、リソース上またはリソース内で実行されるリソースオペレーションについての情報が得られます。デフォルトでは、CloudTrail 証跡はデータイベントを記録しませんが、データイベントをログに記録するよう証跡を設定できます。

CloudTrail で証跡のデータイベントをログに記録する場合、リソースタイプを選択または指定します。S3 Tables には、`AWS::S3Tables::Table` と `AWS::S3Tables::TableBucket` の 2 つのリソースタイプがあります。

次のデータイベントが CloudTrail に記録されます。

- AbortMultipartUpload
- CompleteMultipartUpload
- CreateMultipartUpload
- GetObject
- HeadObject
- ListParts
- PutObject
- UploadPart

CloudTrail データイベントの詳細については、「AWS CloudTrail ユーザーガイド」の「データイベントのログ記録」を参照してください。

S3 Tables の CloudTrail イベントの詳細については、次のトピックを参照してください。

トピック

- S3 Tables の AWS CloudTrail データイベントログファイルの例

S3 Tables の AWS CloudTrail データイベントログファイルの例

AWS CloudTrail ログファイルには、リクエストされた API オペレーション、オペレーションの日時、リクエストパラメータなどに関する情報が含まれます。このトピックでは、S3 Tables の CloudTrail データイベントのログファイルの例を示します。

トピック

- 例 – GetObject データイベントの CloudTrail ログファイル
- 例 – PutObject データイベントの CloudTrail ログファイル

例 – **GetObject** データイベントの CloudTrail ログファイル

以下は、`GetObject` API オペレーションを示す CloudTrail ログファイルの例です。


```
{
    "eventVersion": "1.11",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "123456789012",
      "arn": "arn": "arn:aws:iam::111122223333:user/"myUserName",
      "accountId": "111122223333",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "userName":"myUserName"
    },
    "eventTime": "2024-11-22T17:12:25Z",
    "eventSource": "s3tables.amazonaws.com",
    "eventName": "GetObject",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "[aws-cli/2.18.5]",
    "requestParameters": {
        "Host": "tableWarehouseLocation.s3.us-east-1.amazonaws.com",
        "key": "product-info.json"
    },
    "responseElements":  null,
    "additionalEventData": {
        "SignatureVersion": "SigV4",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "bytesTransferredIn": 0,
        "AuthenticationMethod": "AuthHeader",
        "xAmzId2": "q6xhNJYmhg",
```

```
            "bytesTransferredOut": 28441,

          },
          "requestID": "07D681123BD12AED",
          "eventID": "f2b287f3-0df1-1234-a2f4-c4bdfed47657",
          "readOnly": true,
          "resources": [{
              "accountId": "111122223333",
              "type": "AWS::S3Tables::TableBucket",
               "ARN": "arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
bucket1"
           }, {
              "accountId": "111122223333",
              "type": "AWS::S3Tables::Table",
              "ARN": "arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
bucket/table/111aa1111-22bb-33cc-44dd-5555eee66ffff"

           }],
           "eventType": "AwsApiCall",
           "managementEvent": false,
           "recipientAccountId": "444455556666",
           "eventCategory": "Data",
           "tlsDetails": {
             "tlsVersion": "TLSv1.2",
             "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256"
             "clientProvidedHostHeader": "tableWarehouseLocation.s3.us-
east-1.amazonaws.com"
          }
    }
```

例 – **PutObject** データイベントの CloudTrail ログファイル

以下は、PutObject API オペレーションを示す CloudTrail ログファイルの例です。

```
{
        "eventVersion": "1.11",
        "userIdentity": {
          "type": "IAMUser",
          "principalId": "123456789012",
          "arn": "arn": "arn:aws:iam::444455556666:user/"myUserName",
          "accountId": "444455556666",
          "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
          "userName":"myUserName"
```

```
        },
        "eventTime": "2024-11-22T17:12:25Z",
        "eventSource": "s3tables.amazonaws.com",
        "eventName": "PutObject",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "192.0.2.0",
        "userAgent": "[aws-cli/2.18.5]",
        "requestParameters": {
            "Host": "tableWarehouseLocation.s3.us-east-1.amazonaws.com",
            "key": "product-info.json"
        },
        "responseElements":  {
            "x-amz-server-side-encryption": "AES256",
            "x-amz-version-id": "13zAFMdccAjt3MWd6ehxgCCCDRdkAKDw"
        },
        "additionalEventData": {
            "SignatureVersion": "SigV4",
            "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
            "bytesTransferredIn": 28441,
            "AuthenticationMethod": "AuthHeader",
            "xAmzId2": "q6xhCJYmhg",
            "bytesTransferredOut": 0,

          },
          "requestID": "28d2faaf-1234-4649-997d-EXAMPLE72818",
          "eventID": "694d604a-d190-1234-0dd1-EXAMPLEe20c1",
          "readOnly": false,
          "resources": [{
              "accountId": "444455556666",
              "type": "AWS::S3Tables::TableBucket",
               "ARN": "arn:aws:s3tables:us-east-1444455556666:bucket/amzn-s3-demo-
bucket1"
           }, {
              "accountId": "444455556666",
              "type":  "type": "AWS::S3Tables::Table",
              "ARN": "arn:aws:s3tables:us-east-1:444455556666:bucket/amzn-s3-demo-
bucket1/table/b89ec883-b1d9-4b37-9cd7-b86f590123f4"
           }],
           "eventType": "AwsApiCall",
           "managementEvent": false,
           "recipientAccountId": "111122223333",
           "eventCategory": "Data",
           "tlsDetails": {
             "tlsVersion": "TLSv1.2",
```

```
            "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256"
            "clientProvidedHostHeader": "tableWarehouseLocation.s3.us-
east-1.amazonaws.com"
          }
        }
```

Amazon S3 でのアクセスコントロール

AWS では、リソースはユーザーが操作できるエンティティです。Amazon Simple Storage Service (S3) では、バケットとオブジェクトが元の Amazon S3 リソースです。すべての S3 のお客様のバケットには、オブジェクトが含まれている可能性があります。新機能が S3 に追加され、リソースもさらに追加されましたが、すべてのお客様がこれらの機能固有のリソースを使用しているわけではありません。Amazon S3 リソースの詳細については、「S3 リソース」を参照してください。

デフォルトでは、すべての Amazon S3 リソースはプライベートです。さらにデフォルトでは、リソースを作成した AWS アカウントのルートユーザー (リソース所有者) と、必要なアクセス許可を持つそのアカウント内の IAM ユーザーは、作成したリソースにアクセスできます。リソース所有者は、リソースにアクセスできる他のユーザーと、他のユーザーがリソースに対して実行できるアクションを決定します。S3 には、S3 リソースへのアクセスを他のユーザーに許可するために使用できるさまざまなアクセス管理ツールがあります。

以下のセクションでは、S3 リソースの概要、使用可能な S3 アクセス管理ツール、各アクセス管理ツールの最適なユースケースについて説明します。これらのセクションのリストは、包括的な内容で、すべての S3 リソース、アクセス管理ツール、一般的なアクセス管理のユースケースが含まれることを意図しています。同時に、これらのセクションは、必要な技術的情報へと案内するディレクトリとなるように設計されています。以下のトピックの一部をよく理解している場合は、該当するセクションに進んでください。

S3 リソースタイプ別の S3 API オペレーションへのアクセス許可の詳細については、「Amazon S3 API オペレーションに必要なアクセス許可」を参照してください。

トピック

- S3 リソース
- ID
- アクセス管理ツール
- アクション
- アクセス管理のユースケース
- アクセス管理のトラブルシューティング

S3 リソース

元の Amazon S3 リソースとは、バケットとそれらに含まれるオブジェクトです。S3 に新しい機能が追加されると、新しいリソースも追加されます。以下は、S3 リソースとそれぞれの特徴の完全なリストです。

リソースタイプ	Amazon S3 の特徴	説明
bucket	主要機能	バケット とは、オブジェクトのコンテナのことです。S3 にオブジェクトを保存するには、バケットを作成してから、1 つまたは複数のオブジェクトをバケットにアップロードします。詳細については、「Amazon S3 汎用バケットの作成、設定、操作」を参照してください。
object		オブジェクトには、ファイルと、そのファイルを記述している任意のメタデータを指定できます。オブジェクトがバケットの中にあるときは、オブジェクトを開き、ダウンロードして、移動させます。詳細については、「Amazon S3 オブジェクトの使用」を参照してください。
accesspoint	アクセスポイント	Access Points は、バケットにアタッチされた名前付きのネットワークエンドポイントで、Amazon S3 オブジェクトのオペレーション (GetObject や PutObject など) を実行するために使用できます。各アクセスポイントには、個別の許可とネットワーク制御、および基になるバケットにアタッチされたバケットポリシーと連動して機能するカスタマイズされたアクセスポイントポリシーがあります。仮想プライベートクラウド (VPC) からのリクエストのみを受け入れるように任意のアクセスポイントを設定したり、アクセスポイントごとにカスタムブロックパブリックアクセスを設定したりできます。詳細については、「アクセスポイントを使用した汎用バケット内の共有データセットへのアクセスの管理」を参照してください。

リソースタイプ	Amazon S3 の特徴	説明
`objectlambdaaccesspoint`		Object Lambda アクセスポイントは、Lambda 関数にも関連付けられているバケットのアクセスポイントです。Object Lambda アクセスポイントを使用すると、Amazon S3 `GET`、`LIST`、`HEAD` リクエストに独自のコードを追加して、データがアプリケーションに返されるときにそのデータを変更および処理できます。詳細については、「Object Lambda アクセスポイントの作成」を参照してください。
`multiregionaccesspoint`		マルチリージョン Access Points を使用すると、アプリケーションが複数の AWS リージョンにある Amazon S3 バケットからのリクエストを実行するために使用できるグローバルエンドポイントを作成できます。マルチリージョンアクセスポイントを使用して、単一のリージョンで使用するのと同じシンプルなアーキテクチャでマルチリージョンアプリケーションを構築し、世界中のどこでもこれらのアプリケーションを実行することができます。混雑したパブリックインターネット経由でリクエストを送信する代わりに、マルチリージョンアクセスポイントのグローバルエンドポイントに対して行われたアプリケーションリクエストは、AWS グローバルネットワークを介して最も近い Amazon S3 バケットに自動的にルーティングされます。詳細については、「マルチリージョンアクセスポイントを使用したマルチリージョントラフィックの管理」を参照してください。

リソースタイプ	Amazon S3 の特徴	説明
`job`	S3 バッチオペレーション	ジョブは S3 バッチオペレーション機能のリソースです。S3 バッチオペレーションを使用すると、指定した Amazon S3 のオブジェクトのリストに対して大規模なバッチオペレーションを実行できます。Amazon S3 は、バッチオペレーションジョブの進捗状況の追跡、通知の送信、すべてのアクションの詳細な完了レポートの保存を行い、フルマネージド型の監査可能なサーバーレスエクスペリエンスを提供します。詳細については、「バッチオペレーションでオブジェクトオペレーションを一括で実行する」を参照してください。
`storagelensconfiguration`	S3 Storage Lens	S3 Storage Lens は、組織全体のストレージメトリクスとユーザーデータを収集します。S3 Storage Lens は、組織内の数百または数千のアカウントのオブジェクトストレージの使用状況とアクティビティを 1 つのビューで表示し、複数の集約レベルでインサイトを生成するための詳細情報を提供します。詳細については、「Amazon S3 ストレージレンズを使用してストレージのアクティビティと使用状況を評価する」を参照してください。
`storagelensgroup`		S3 Storage Lens グループは、オブジェクトメタデータに基づくカスタムフィルターを使用してメトリクスを集約します。S3 Storage Lens グループを使用すると、経過時間別のオブジェクトの分布や最も一般的なファイルタイプなど、データの特性を調べることができます。詳細については、「S3 ストレージレンズグループを使用したメトリクスのフィルタリングと集計」を参照してください。

リソースタイプ	Amazon S3 の特徴	説明
accessgrantsinstance	S3 Access Grants	S3 Access Grants インスタンスは、ユーザーが作成した S3 アクセス許可のコンテナです。S3 Access Grants を使用すると、 アカウント内の IAM アイデンティティ、他の アカウントの IAM アイデンティティ (クロスアカウント) 、および社内ディレクトリから AWS IAM Identity Center に追加されたディレクトリアイデンティティの Amazon S3 データへのアクセス許可を作成できます。S3 Access Grants の詳細については、「S3 Access Grants でのアクセス管理」を参照してください。
accessgrantslocation		Access Grants Location は、S3 Access Grants インスタンスに登録するバケット、バケット内のプレフィックス、またはオブジェクトです。S3 Access Grants インスタンス内にロケーションを登録してから、そのロケーションへのアクセス許可を作成する必要があります。次に、S3 Access Grants を使用して、 アカウント内の IAM アイデンティティ、他のアカウントの IAM アイデンティティ (クロスアカウント) 、および社内ディレクトリから AWS IAM Identity Center に追加されたディレクトリアイデンティティのバケット、プレフィックス、またはオブジェクトへのアクセス許可を作成できます。S3 Access Grants の詳細については、「S3 Access Grants でのアクセス管理」を参照してください。
accessgrant		Access Grant は、Amazon S3 データに対する個別のアクセス許可です。S3 Access Grants を使用すると、 アカウント内の IAM アイデンティティ、他の アカウントの IAM アイデンティティ (クロスアカウント) 、および社内ディレクトリから AWS IAM Identity Center に追加されたディレクトリアイデンティティの Amazon S3 データへのアクセス許可を作成できます。S3 Access Grants の詳細については、「S3 Access Grants でのアクセス管理」を参照してください。

バケット

Amazon S3 バケットには、汎用バケットとディレクトリバケットの 2 種類があります。

- 汎用バケット はオリジナルの S3 バケットタイプであり、ほとんどのユースケースやアクセスパターンに推奨されます。汎用バケットでは、S3 Express One Zone 以外のすべてのストレージクラスにオブジェクトを保存することもできます。S3 ストレージクラスの詳細については、「Amazon S3 ストレージクラスの理解と管理」を参照してください。
- ディレクトリバケットは、S3 Express One Zone ストレージクラスのみを使用します。アプリケーションがパフォーマンスの影響を受けやすく、1 桁ミリ秒の PUT と GET のレイテンシーから利点が得られる場合にお勧めします。詳細についてはディレクトリバケットの使用、S3 Express One Zone、およびIAM を使用したリージョンエンドポイント API オペレーションの承認を参照してください。

S3 リソースの分類

Amazon S3 には、S3 リソースを分類および整理する機能が備えられています。リソースの分類は、リソースの整理に役立つだけでなく、これにより、リソースカテゴリに基づいてアクセス管理ルールを設定することもできます。特に、プレフィックスとタグ付けは、アクセス管理のアクセス許可を設定するときに使用する 2 つのストレージ組織機能です。

> **Note**
>
> 以下の情報は、汎用バケットに適用されます。ディレクトリバケットはタグ付けをサポートしておらず、プレフィックスの誓約があります。詳細については、「IAM を使用したリージョンエンドポイント API オペレーションの承認」を参照してください。

- プレフィックス — Amazon S3 のプレフィックスは、S3 バケットに保存されたオブジェクトを整理するために使用されるオブジェクトキー名の先頭にある文字列です。スラッシュ (/) などの区切り文字を使用して、オブジェクトキー名内のプレフィックスの末尾を指定できます。例えば、`engineering/` プレフィックスで始まるオブジェクトキー名や、`marketing/campaigns/` プレフィックスで始まるオブジェクトキー名があるとします。スラッシュ文字 (/) など、プレフィックスの末尾に区切り記号を使用すると、フォルダとファイルの命名規則が工ミュレートされます。ただし、S3 では、プレフィックスはオブジェクトキー名の一部です。汎用 S3 バケットでは、実際のフォルダ階層は存在しません。

Amazon S3 では、プレフィックスを使用してオブジェクトを整理およびグループ化できます。オブジェクトへのアクセスをプレフィックスで管理することもできます。例えば、特定のプレフィックスで始まる名前のオブジェクトへのアクセスのみを制限できます。

詳細については、「プレフィックスを使用してオブジェクトを整理する」を参照してください。S3 コンソールは、フォルダの概念を使用します。これは、汎用バケットでは、基本的にオブジェクトキー名の前に付加されるプレフィックスです。詳細については、「フォルダを使用して Amazon S3 コンソールのオブジェクトを整理する」を参照してください。

- タグ — 各タグは、リソースに割り当てることができるキーと値のペアです。例えば、一部のリソースにタグ `topicCategory=engineering` を付けることができます。タグ付けを使用すると、コスト配分、分類と整理、アクセスコントロールに役立ちます。バケットのタグ付けはコスト配分にのみ使用されます。オブジェクト、S3 Storage Lens、ジョブ、および S3 Access Grants には、整理またはアクセスコントロールの目的でタグ付けできます。S3 Access Grants では、コスト配分にもタグ付けを使用できます。タグを使用してリソースへのアクセスを制御する例として、特定のタグまたはタグの組み合わせを持つオブジェクトのみを共有できます。

  詳細については、IAM ユーザーガイドの「リソースタグを使用した AWS リソースへのアクセスの制御」を参照してください。

ID

Amazon S3 では、リソース所有者は、バケットやオブジェクトなどのリソースを作成した ID です。デフォルトでは、必要なアクセス許可を持つアカウント内でリソースと IAM アイデンティティを作成したアカウントのルートユーザーのみが S3 リソースにアクセスできます。リソース所有者は、他のアイデンティティに S3 リソースへのアクセスを許可できます。

リソースを所有していないアイデンティティは、そのリソースへのアクセスをリクエストできます。リソースに対するリクエストは、認証済みまたは未認証です。認証リクエストには、リクエストの送信元を認証する署名値を含める必要がありますが、未認証のリクエストでは署名は不要です。認証されたユーザーのみにアクセスを許可することをお勧めします。リクエスト認証の詳細については、「Amazon S3 API リファレンス」の「Making requests」を参照してください。

> **Important**
>
> 認証されたリクエストの実行に AWS アカウントのルートユーザー認証情報を使用しないことをお勧めします。代わりに、IAM ロールを作成し、このロールにフルアクセスを許可します。このロールを持つユーザーを管理者ユーザーと呼びます。AWS アカウントのルート

ユーザー認証情報ではなく、管理者ユーザーに割り当てられた認証情報を使用して AWS とやり取りし、バケットの作成、ユーザーの作成、アクセス許可の付与などのタスクを実行できます。詳細については、AWS 全般のリファレンスの「AWS アカウント ルートユーザーの認証情報と IAM ユーザーの認証情報」および 「IAM ユーザーガイド」の「IAM でのセキュリティのベストプラクティス」を参照してください。

Amazon S3 のデータにアクセスするアイデンティティは、次のいずれかになります。

AWS アカウント所有者

リソースを作成した AWS アカウントです。例えば、バケットを作成したアカウントです。このアカウントは リソースを所有しています。詳細については、「AWS アカウントのルートユーザー」を参照してください。

AWS アカウント所有者の同じアカウントの IAM アイデンティティ

S3 アクセスを必要とする新しいチームメンバーのアカウントを設定する場合、AWS アカウント所有者は AWS Identity and Access Management (IAM) を使用してユーザー、グループ、ロールを作成できます。その後、AWS アカウント所有者はこれらの IAM アイデンティティとリソースを共有できます。アカウント所有者は、IAM アイデンティティに付与するアクセス許可を指定することもできます。これにより、共有リソースで実行できるアクションを許可または拒否できます。

IAM アイデンティティを使用すると、共有リソースにアクセスする前にログイン認証情報の入力を要求するなど、機能を強化できます。IAM アイデンティティを使用すると、強力なアイデンティティ基盤をサポートするために、IAM の多要素認証 (MFA) 形式を実装することもできます。IAM のベストプラクティスは、個々のユーザーにアクセス許可を付与するのではなく、アクセス管理用のロールを作成することです。個々のユーザーを適切なロールに割り当てます。詳細については、「IAM のセキュリティのベストプラクティス」を参照してください。

他の AWS アカウント所有者とその IAM アイデンティティ (クロスアカウントアクセス)

AWS アカウント所有者は、他の AWS アカウント所有者、または別の AWS アカウントに属する IAM アイデンティティにリソースへのアクセスを許可することもできます。

Note

アクセス許可の委任 — AWS アカウントがリソースを所有している場合、そのアカウントは別の AWS アカウントにこれらの許可を付与できます。そのアカウントは、それらのアク

セス許可またはそのサブセットを、同じアカウント内のユーザーに委任できます。これはアクセス許可の委任と呼ばれます。ただし、他のアカウントから許可を受け取るアカウントは、別の AWS アカウントに「クロスアカウント」でこれらの許可を委任することはできません。

匿名ユーザー (パブリックアクセス)

AWS アカウント 所有者はリソースを公開できます。リソースを公開すると、リソースが匿名ユーザーと技術的に共有されます。2023 年 4 月以降に作成されたバケットは、この設定を変更しない限り、デフォルトですべてのパブリックアクセスをブロックします。パブリックアクセスをブロックするようにバケットを設定し、認証されたユーザーにのみアクセスを許可することをお勧めします。ブロックパブリックアクセスの詳細については、Amazon S3 ストレージへのパブリックアクセスのブロック を参照してください。

AWS のサービス

リソース所有者は、Amazon S3 リソースへの別の AWS サービスアクセスを許可できます。例えば、ログファイルをバケットに書き込む `s3:PutObject` アクセス許可を AWS CloudTrail サービスに付与できます。詳細については、「AWS サービスへのアクセスの提供」を参照してください。

社内ディレクトリのアイデンティティ

リソース所有者は、S3 Access Grants を使用して、社内ディレクトリのユーザーまたはロールに S3 リソースへのアクセス権を付与できます。AWS IAM Identity Center への社内ディレクトリの追加に関する詳細は、「IAM Identity Center とは何ですか?」を参照してください。

バケットまたはリソース所有者

このようなリソースの所有者は、バケットの作成とオブジェクトのアップロードに使用する AWS アカウントです。バケット所有者は、別の AWS アカウント (または別のアカウントのユーザー) に対して、オブジェクトをアップロードするためのクロスアカウントアクセス許可を付与できます。

バケット所有者が別のアカウントにバケットへのオブジェクトのアップロードを許可すると、バケット所有者はデフォルトで、バケットにアップロードされたすべてのオブジェクトを所有します。ただし、バケット所有者の強制バケット設定とバケット所有者の優先バケット設定の両方がオフになっている場合、オブジェクトをアップロードする AWS アカウントがこれらのオブジェクトを所有し、バケット所有者には別のアカウントが所有するオブジェクトに対するアクセス許可は付与されません。ただし、以下の例外があります。

- バケット所有者が請求の支払いを行う場合、バケット所有者は、オブジェクトの所有者に関係なく、オブジェクトへのアクセスを拒否したり、バケット内のオブジェクトを削除したりすることができます。
- バケット所有者は、オブジェクトの所有者に関係なく、オブジェクトをアーカイブしたり、アーカイブされたオブジェクトを復元したりすることができます。アーカイブはオブジェクトの格納に使用されるストレージクラスを指します。詳細については、「オブジェクトのライフサイクルの管理」を参照してください。

アクセス管理ツール

Amazon S3 には、さまざまなセキュリティ機能とツールが用意されています。以下は、これらの機能とツールの包括的なリストです。これらのアクセス管理ツールがすべて必要なわけではありませんが、Amazon S3 リソースへのアクセスを付与するには、これらのツールを 1 つ以上使用する必要があります。これらのツールを適切に適用すると、データの整合性を維持し、目的のユーザーがリソースにアクセスできるようにするために役立ちます。

最も一般的に使用されるアクセス管理ツールは、アクセスポリシーです。アクセスポリシーは、バケットのバケットポリシーなど、AWS リソースにアタッチされたリソースベースのポリシーに指定できます。アクセスポリシーは、IAM ユーザー、グループ、ロールなどの AWS Identity and Access Management (IAM) アイデンティティにアタッチされたアイデンティティベースのポリシーに指定することもできます。アクセスポリシーを作成して、 AWS アカウントおよび IAM ユーザー、グループ、ロールにアクセス許可を付与し、リソースに対してオペレーションを実行します。例えば、他のアカウントがバケットにオブジェクトをアップロードできるように、別の AWS アカウントに PUT `Object` アクセス許可を付与できます。

アクセスポリシーでは、誰が何にアクセスできるかを記述します。Amazon S3 は、リクエストを受け取ったときにすべてのアクセスポリシーを評価して、リクエストを許可するか拒否するかを判断する必要があります。Amazon S3 がこれらのポリシーを評価する方法の詳細については、Amazon S3 がリクエストを許可する仕組み を参照してください。

Amazon S3 で使用できるアクセス管理ツールを以下に示します。

バケットポリシー

Amazon S3 バケットポリシーは、特定のバケットにアタッチされた JSON 形式の AWS Identity and Access Management (IAM) リソースベースのポリシーです。バケットポリシーを使用すると、バケットおよびバケット内のオブジェクトに対するアクセス許可を、他の AWS アカウントまたは IAM

アイデンティティに付与できます。S3 アクセス管理の多くのユースケースは、バケットポリシーを使用することで要件が満たされます。バケットポリシーを使用すると、承認されたアイデンティティのみがリソースにアクセスしてアクションを実行できるように、バケットアクセスをパーソナライズすることができます。詳細については、「Amazon S3 のバケットポリシー」を参照してください。

以下は、バケットポリシーの例です。JSON ファイルを使用してバケットポリシーを表現します。このポリシーの例では、バケット内のすべてのオブジェクトに IAM ロールの読み取りアクセス許可を付与します。このポリシーには、amzn-s3-demo-bucket1 という名前のバケット内のオブジェクトに対して、s3:GetObject アクション (読み取りアクセス許可) を許可する BucketLevelReadPermissions という名前の 1 個のステートメントがあります。IAM ロールを Principal として指定することで、このポリシーは、このロールを持つすべての IAM ユーザーにアクセス権を付与します。このポリシーの例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid":"BucketLevelReadPermissions",
      "Effect":"Allow",
      "Principal": {
     "AWS": "arn:aws:iam::123456789101:role/s3-role"
      },
      "Action":["s3:GetObject"],
      "Resource":["arn:aws:s3:::amzn-s3-demo-bucket1/*"]
    }]
  }
```

> **Note**
>
> ポリシーを作成するときは、Principal 要素にワイルドカード文字 (*) を使用しないでください。ワイルドカードを使用すると、すべてのユーザーが Amazon S3 リソースにアクセスできるようになります。代わりに、バケットへのアクセスが許可されているユーザーまたはグループを明示的にリストするか、ポリシーで条件句を使用して満たす必要がある条件をリストします。ユーザーまたはグループのアクションにワイルドカード文字を含めるのではなく、該当する場合に特定のアクセス許可を付与します。

ID ベースのポリシー

アイデンティティベースのポリシーまたは IAM ユーザーポリシーは、AWS Identity and Access Management (IAM) ポリシーの一種です。アイデンティティベースのポリシーは、AWSアカウントの IAM ユーザー、グループ、またはロールにアタッチされる JSON 形式のポリシーです。アイデンティティベースのポリシーを使用すると、バケットまたはオブジェクトへのアクセス許可を IAM アイデンティティに付与できます。アカウント内に IAM ユーザー、グループ、およびロールを作成し、これらにアクセスポリシーをアタッチできます。次に、Amazon S3 リソースを含む AWS リソースへのアクセス許可を付与できます。詳細については、「Amazon S3 のアイデンティティベースのポリシー」を参照してください。

以下は、アイデンティティベースポリシーの例です。このポリシーの例では、関連 IAM ロールに、バケットとバケット内のオブジェクトに対して Amazon S3 の 6 つの異なるアクション (アクセス許可) の実行を許可します。このポリシーをアカウントの IAM ロールにアタッチし、そのロールを一部の IAM ユーザーに割り当てると、このロールを持つユーザーは、ポリシーで指定されたリソース (バケット) に対してこれらのアクションを実行できます。このポリシーの例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
{
  "Version": "2012-10-17",
  "Statement": [
  {
    "Sid": "AssignARoleActions",
    "Effect": "Allow",
    "Action": [
   "s3:PutObject",
   "s3:GetObject",
   "s3:ListBucket",
   "s3:DeleteObject",
   "s3:GetBucketLocation"
    ],
    "Resource": [
   "arn:aws:s3:::amzn-s3-demo-bucket1/*",
   "arn:aws:s3:::amzn-s3-demo-bucket1"
    ]
    },
  {
    "Sid": "AssignARoleActions2",
    "Effect": "Allow",
    "Action": "s3:ListAllMyBuckets",
    "Resource": "*"
```

```
  }
  ]
}
```

S3 Access Grants

S3 Access Grants を使用して、Active Directory などの企業 ID ディレクトリ内のアイデンティティと AWS Identity and Access Management (IAM) アイデンティティの両方の Amazon S3 データへのアクセス許可を作成します。S3 Access Grants は、大規模なデータのアクセス許可の管理に役立ちます。さらに、S3 Access Grants は、エンドユーザーアイデンティティと、AWS CloudTrail での S3 データへのアクセスに使用されるアプリケーションをログに記録します。これにより、S3 バケット内のデータへのすべてのアクセスについて、エンドユーザーアイデンティティまで詳細な監査履歴が提供されます。詳細については、「S3 Access Grants でのアクセス管理」を参照してください。

アクセスポイント

Amazon S3 Access Points は、S3 の共有データセットを使用するアプリケーションの大規模なデータアクセスの管理を簡素化します。Access Points は名前付きのネットワークエンドポイントで、バケットにアタッチされます。アクセスポイントを使用すると、オブジェクトのアップロードや取得などの S3 オブジェクトオペレーションを大規模に実行できます。バケットには最大 10,000 個のアクセスポイントをアタッチできます。各アクセスポイントでは、個別のアクセス許可やネットワークコントロールを適用することで、S3 オブジェクトへのアクセスをきめ細かく制御できます。S3 Access Points は、同じアカウントまたは別の信頼されたアカウントのバケットに関連付けることができます。Access Points ポリシーは、基になるバケットポリシーと組み合わせて評価されるリソースベースのポリシーです。詳細については、「アクセスポイントを使用した汎用バケット内の共有データセットへのアクセスの管理」を参照してください。

アクセスコントロールリスト (ACL)

ACL は、アクセス許可の被付与者と付与されるアクセス許可を識別するリストです。ACL は、基本的な読み取り/書き込み許可を他の AWS アカウントに付与します。ACL では、Amazon S3 固有の XML スキーマが使用されます。ACL は、AWS Identity and Access Management (IAM) ポリシーの一種です。オブジェクト ACL は、オブジェクトへのアクセスを管理するために使用され、バケット ACL はバケットへのアクセスを管理するために使用されます。バケットポリシーはバケット全体に対して 1 つですが、オブジェクト ACL は各オブジェクトに対して指定されます。オブジェクトごとに個別にアクセスを制御する必要がある通常ではない状況を除き、ACL は無効にしておくことをお勧めします。ACL の使用方法の詳細については、オブジェクトの所有権の制御とバケットの ACL の無効化。 を参照してください。

> **Warning**
>
> Amazon S3 の最新のユースケースの大部分では ACL を使用する必要がなくなっています。

以下に、バケット ACL の例を示します。この ACL アクセス権限は、フルコントロールのアクセス許可を持つバケット所有者を示します。

```
<?xml version="1.0" encoding="UTF-8"?>
 <AccessControlPolicy xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Owner>
   <ID>Owner-Canonical-User-ID</ID>
   <DisplayName>owner-display-name</DisplayName>
  </Owner>
 <AccessControlList>
  <Grant>
   <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="Canonical
 User">
    <ID>Owner-Canonical-User-ID</ID>
    <DisplayName>display-name</DisplayName>
   </Grantee>
   <Permission>FULL_CONTROL</Permission>
  </Grant>
 </AccessControlList>
</AccessControlPolicy>
```

オブジェクトの所有権

オブジェクトへのアクセスを管理するには、オブジェクトの所有者である必要があります。オブジェクト所有権のバケットレベルの設定を使用すると、バケットにアップロードされたオブジェクトの所有権を制御できます。また、オブジェクト所有権を使用して、ACL を有効にします。デフォルトでは、オブジェクト所有権は [バケット所有者の強制] に設定され、すべての ACL は無効になっています。ACL が無効になっている場合、バケット所有者はバケット内のすべてのオブジェクトを所有し、データへのアクセスの管理のみを行います。アクセスを管理するために、バケット所有者は ACL を除くポリシーまたは別のアクセス管理ツールを使用します。詳細については、「オブジェクトの所有権の制御とバケットの ACL の無効化。」を参照してください。

オブジェクト所有権には、バケットにアップロードされるオブジェクトの所有権を制御し、ACL を無効化または有効化するために使用できる 3 つの設定があります。

ACL を無効化する

- バケット所有者強制 (デフォルト) – ACL は無効になり、バケット所有者はバケット内のすべてのオブジェクトを自動的に所有し、完全に制御します。ACL は、S3 バケット内のデータに対するアクセス許可に対して影響を与えません。このバケットはアクセスコントロールを定義するためだけにポリシーを使用します。

ACL を有効化する

- 希望するバケット所有者 — バケット所有者は、他のアカウントが `bucket-owner-full-control` 既定 ACL でバケットに書き込む新しいオブジェクトを所有し、完全にコントロールできます。
- オブジェクトライター — オブジェクトをアップロードする AWS アカウント は、そのオブジェクトを所有し、そのオブジェクトを完全にコントロールし、ACL を介して他のユーザーにそのオブジェクトへのアクセス権を付与できます。

その他のベストプラクティス

転送中および保管時のデータを保護するために、次のバケット設定とツールを使用することを検討してください。どちらも、データの完全性とアクセシビリティを維持するために重要です。

- パブリックアクセスをブロック — デフォルトのバケットレベルの設定の [パブリックアクセスをブロック] をオフにしないでください。この設定は、デフォルトでデータへのパブリックアクセスをブロックします。ブロックパブリックアクセスの詳細については、Amazon S3 ストレージへのパブリックアクセスのブロック を参照してください。
- S3 バージョニング — データ整合性のために、S3 バージョニングバケット設定を実装できます。この設定では、オブジェクトを上書きするのではなく、更新時にオブジェクトに複数のバージョンを持たせます。S3 バージョニングを使用すると、必要に応じて以前のバージョンを保存、取得、復元できます。S3 バージョニングの詳細については、「S3 バージョニングによる複数のバージョンのオブジェクトの保持」を参照してください。
- S3 Object Lock — S3 Object Lock は、データの整合性を実現するために実装できるもう 1 つの設定です。この機能により、オブジェクトを不変的に保存するための Write-Once-Read-Many (WORM) モデルを実装できます。Object Lock の詳細については、「S3 Object Lock を使用したオブジェクトのロック」を参照してください。
- オブジェクト暗号化 — Amazon S3 には、転送中および保管時のデータを保護するために使用できる、複数のオブジェクト暗号化オプションがあります。サーバー側の暗号化では、オブジェクトを

データセンター内のディスクに保存する前に暗号化し、オブジェクトをダウンロードするときに復号します。リクエストが認証され、お客様がアクセス許可を持っていれば、オブジェクトが暗号化されているかどうかに関係なく同じ方法でアクセスできます。詳細については、「サーバー側の暗号化によるデータの保護」を参照してください。S3 は、新しくアップロードされたオブジェクトをデフォルトで暗号化します。詳細については、「Amazon S3 バケット向けのサーバー側のデフォルトの暗号化動作の設定」を参照してください。クライアント側の暗号化では、Amazon S3 に送信する前にデータを暗号化します。詳細については、「クライアント側の暗号化を使用したデータの保護」を参照してください。

- 署名方法 — 署名バージョン 4 は、HTTP で送信される AWS リクエストに認証情報を追加するプロセスです。セキュリティ対策として、AWS へのほとんどのリクエストは、アクセスキーを使用して署名する必要があります。アクセスキーは、アクセスキー ID とシークレットアクセスキーで構成されます。これらの 2 つのキーは、一般的にセキュリティ認証情報と呼ばれます。詳細については、「リクエストの認証 (AWS 署名バージョン 4)」および「署名バージョン 4 の署名プロセス」を参照してください。

アクション

S3 のアクセス許可および条件キーの完全なリストについては、「サービス認可リファレンス」の「Actions, resources, and condition keys for Amazon S3」を参照してください。

S3 リソースタイプ別の S3 API オペレーションへのアクセス許可の詳細については、「Amazon S3 API オペレーションに必要なアクセス許可」を参照してください。

アクション

Amazon S3 の AWS Identity and Access Management (IAM) アクションは、S3 バケットまたはオブジェクトで実行できるアクションです。これらのアクションをアイデンティティに付与して、S3 リソースに対してアクションを実行できるようにします。S3 アクションの例は、バケット内のオブジェクトを読み取る `s3:GetObject` と、バケットにオブジェクトを書き込む `s3:PutObject` です。

条件キー

アクション以外に、条件が満たされた場合のみのアクセスを許可するように IAM 条件キーが制限されます。条件キーはオプションです。

> **Note**
>
> バケットポリシーなどのリソースベースのアクセスポリシー、またはアイデンティティベースのポリシーでは、以下を指定できます。
>
> - ポリシーステートメントの `Action` 要素内のアクションまたはアクションの配列。
> - ポリシーステートメントの `Effect` 要素で、`Allow` を指定してリストされたアクションを付与するか、`Deny` を指定してリストされたアクションをブロックできます。最小特権の使用をさらに維持するために、アクセスポリシーの `Effect` 要素の `Deny` のステートメントはできるだけ広義に、`Allow` ステートメントはできるだけ狭義にする必要があります。ポリシー条件ステートメントに含まれるアイデンティティに対して、オプトインに関するベストプラクティスを実装するための別の効果的な手段として、「`s3:*`」アクションとペアになった `Deny` 効果があります。
> - ポリシーステートメントの `Condition` 要素の条件キー。

アクセス管理のユースケース

Amazon S3 では、リソース所有者にアクセス権を付与するためのさまざまなツールを提供します。使用する S3 アクセス管理ツールは、共有する S3 リソース、アクセスを許可するアイデンティティ、許可または拒否するアクションによって異なります。S3 アクセス管理ツールの 1 つまたは組み合わせを使用して、S3 リソースへのアクセスを管理できます。

ほとんどの場合、アクセスポリシーを使用すると、アクセス許可を管理できます。アクセスポリシーは、バケットなどのリソース、または別の Amazon S3 リソース (S3 リソース) にアタッチされたリソースベースのポリシーに指定できます。アクセスポリシーは、アカウントの AWS Identity and Access Management (IAM) ユーザー、グループ、ロールにアタッチされたアイデンティティベースのポリシーに指定することもできます。バケットポリシーがユースケースにより適している場合もあります。詳細については、「Amazon S3 のバケットポリシー」を参照してください。または、 AWS Identity and Access Management (IAM) を使用して、AWS アカウント 内に IAM ユーザー、グループ、ロールを作成し、アイデンティティベースのポリシーを介してバケットとオブジェクトへのアクセスを管理できます。詳細については、「Amazon S3 のアイデンティティベースのポリシー」を参照してください。

これらのアクセス管理オプションをナビゲートしやすくするために、Amazon S3 カスタマーの一般的なユースケースと各 S3 アクセス管理ツールの推奨事項を以下に示します。

AWS アカウント所有者が同じアカウント内のユーザーとのみバケットを共有したい

すべてのアクセス管理ツールで、この基本的なユースケースを満たすことができます。このユースケースでは、以下のアクセス管理ツールをお勧めします。

- バケットポリシー – 1 つのバケットまたは少数のバケットへのアクセスを許可する場合、またはバケットのアクセス許可がバケット間で類似している場合は、バケットポリシーを使用します。バケットポリシーでは、バケットごとに 1 つのポリシーを管理します。詳細については、「Amazon S3 のバケットポリシー」を参照してください。
- アイデンティティベースのポリシー – バケットごとにアクセス許可が異なるバケットが多数あり、管理するユーザーロールはわずかの場合は、ユーザー、グループ、またはロールに IAM ポリシーを使用できます。IAM ポリシーは、他の AWS リソースや Amazon S3 リソースへのユーザーアクセスを管理する場合にも適しています。詳細については、「例 1: バケット所有者がユーザーにバケットのアクセス許可を付与する」を参照してください。
- S3 Access Grants – S3 Access Grants を使用すると、S3 バケット、プレフィックス、またはオブジェクトへのアクセスを許可できます。S3 Access Grants では、さまざまなオブジェクトレベルのアクセス許可を大規模に指定できますが、バケットポリシーのサイズは 20 KB に制限されています。詳細については、「S3 Access Grants の開始方法」を参照してください。
- Access Points - バケットにアタッチされる名前付きのネットワークエンドポイントである Access Points を使用できます。バケットには最大 10,000 個のアクセスポイントをアタッチできます。各アクセスポイントでは、個別のアクセス許可やネットワークコントロールを適用することで、S3 オブジェクトへのアクセスをきめ細かく制御できます。詳細については、「アクセスポイントを使用した汎用バケット内の共有データセットへのアクセスの管理」を参照してください。

AWS アカウント所有者が別の AWS アカウントのユーザーとバケットまたはオブジェクトを共有したい (クロスアカウント)

別の AWS アカウントにアクセス許可を付与するには、バケットポリシーまたは次のいずれかの推奨アクセス管理ツールを使用する必要があります。このユースケースでは、アイデンティティベースのアクセスポリシーを使用できません。クロスアカウントアクセスの付与に関する詳細は、「Amazon S3 バケット内のオブジェクトへのクロスアカウントアクセスを提供するには、どうしたらいいですか?」を参照してください。

このユースケースでは、以下のアクセス管理ツールをお勧めします。

- バケットポリシー - バケットポリシーでは、バケットごとに 1 つのポリシーを管理します。詳細については、「Amazon S3 のバケットポリシー」を参照してください。

- S3 Access Grants – S3 Access Grants を使用すると、S3 バケット、プレフィックス、またはオブジェクトへのクロスアカウントアクセスを許可できます。S3 Access Grants を使用すると、さまざまなオブジェクトレベルのアクセス許可を大規模に指定できますが、バケットポリシーのサイズは 20 KB に制限されています。詳細については、「S3 Access Grants の開始方法」を参照してください。
- Access Points - バケットにアタッチされる名前付きのネットワークエンドポイントである Access Points を使用できます。バケットには最大 10,000 個のアクセスポイントをアタッチできます。各アクセスポイントでは、個別のアクセス許可やネットワークコントロールを適用することで、S3 オブジェクトへのアクセスをきめ細かく制御できます。詳細については、「アクセスポイントを使用した汎用バケット内の共有データセットへのアクセスの管理」を参照してください。

AWS アカウント所有者またはバケット所有者が、オブジェクトレベルまたはプレフィックスレベルでアクセス許可を付与する必要があり、これらのアクセス許可がオブジェクトごとまたはプレフィックスごとに異なる。

バケットポリシーでは、例えば、特定のキー名のプレフィックスを共有するバケット内のオブジェクト、または特定のタグを持つオブジェクトへのアクセスを許可できます。例えば、キー名プレフィックス `logs/` で始まるオブジェクトの読み取り権限を付与できます。ただし、アクセス許可がオブジェクトごとに異なる場合、特にバケットポリシーのサイズが 20 KB に制限されているため、バケットポリシーを使用して個々のオブジェクトへのアクセス許可を付与することは実用的でない可能性があります。

このユースケースでは、以下のアクセス管理ツールをお勧めします。

- S3 Access Grants – S3 Access Grants を使用すると、オブジェクトレベルまたはプレフィックスレベルのアクセス許可を管理できます。バケットポリシーとは異なり、S3 Access Grants を使用すると、さまざまなオブジェクトレベルのアクセス許可を大規模に指定できます。バケットポリシーのサイズは 20 KB に制限されています。詳細については、「S3 Access Grants の開始方法」を参照してください。
- Access Points – アクセスポイントを使用すると、オブジェクトレベルまたはプレフィックスレベルのアクセス許可を管理できます。Access Points は名前付きのネットワークエンドポイントで、バケットにアタッチされます。バケットには最大 10,000 個のアクセスポイントをアタッチできます。各アクセスポイントでは、個別のアクセス許可やネットワークコントロールを適用することで、S3 オブジェクトへのアクセスをきめ細かく制御できます。詳細については、「アクセスポイントを使用した汎用バケット内の共有データセットへのアクセスの管理」を参照してください。

- ACL – 特に ACL はオブジェクトごと負荷できる許可数が 100 個に制限されているため、アクセスコントロールリスト (ACL) の使用はお勧めしません。ただし、ACL を有効にした場合、バケット設定で [オブジェクト所有者] を [希望するバケット所有者] と [ACL 有効] に設定します。この設定では、新しいオブジェクトが `bucket-owner-full-control` 既定 ACL はオブジェクトライターではなく、バケット所有者によって自動的に所有されます。次に、XML 形式のアクセスポリシーであるオブジェクト ACL を使用して、他のユーザーにオブジェクトへのアクセスを許可できます。詳細については、「アクセスコントロールリスト (ACL) の概要」を参照してください。

AWS アカウント所有者またはバケット所有者が、特定のアカウント ID のみにバケットアクセスを制限したい

このユースケースでは、以下のアクセス管理ツールをお勧めします。

- バケットポリシー - バケットポリシーでは、バケットごとに 1 つのポリシーを管理します。詳細については、「Amazon S3 のバケットポリシー」を参照してください。
- Access Points – Access Points は名前付きのネットワークエンドポイントで、バケットにアタッチされます。バケットには最大 10,000 個のアクセスポイントをアタッチできます。各アクセスポイントでは、個別のアクセス許可やネットワークコントロールを適用することで、S3 オブジェクトへのアクセスをきめ細かく制御できます。詳細については、「アクセスポイントを使用した汎用バケット内の共有データセットへのアクセスの管理」を参照してください。

AWS アカウント 所有者またはバケット所有者が、データにアクセスするすべてのユーザーまたはアプリケーションに対して個別のエンドポイントを必要としている

このユースケースでは、以下のアクセス管理ツールをお勧めします。

- Access Points – Access Points は名前付きのネットワークエンドポイントで、バケットにアタッチされます。バケットには最大 10,000 個のアクセスポイントをアタッチできます。各アクセスポイントでは、個別のアクセス許可やネットワークコントロールを適用することで、S3 オブジェクトへのアクセスをきめ細かく制御できます。各アクセスポイントは、基になるバケットにアタッチされたバケットポリシーと連動して機能するカスタマイズされたアクセスポイントポリシーを適用します。詳細については、「アクセスポイントを使用した汎用バケット内の共有データセットへのアクセスの管理」を参照してください。

AWS アカウント所有者またはバケット所有者が、S3 の仮想プライベートクラウド (VPC)エンドポイントからのアクセスを管理する必要がある

Amazon S3 の仮想プライベートクラウド (VPC) エンドポイントは、S3 への接続のみを許可する VPC 内の論理エンティティです。このユースケースでは、以下のアクセス管理ツールをお勧めします。

- VPC 設定のバケット – バケットポリシーを使用して、バケットへのアクセスを許可されているユーザーと、バケットがアクセスできる VPC エンドポイントを制御できます。詳細については、「バケットポリシーを使用した VPC エンドポイントからのアクセスコントロール」を参照してください。
- アクセスポイント – アクセスポイントを設定する場合、アクセスポイントポリシーを使用できます。仮想プライベートクラウド (VPC) からのリクエストのみを受け付けるようにアクセスポイントを設定することで、プライベートネットワークへの Amazon S3 データアクセスを制限できます。また、アクセスポイントごとにカスタムのブロックパブリックアクセスを設定することもできます。詳細については、「アクセスポイントを使用した汎用バケット内の共有データセットへのアクセスの管理」を参照してください。

AWS アカウント所有者またはバケット所有者が静的ウェブサイトを公開する必要がある

S3 を使用すると、静的ウェブサイトをホストし、S3 バケットからホストされているウェブサイトのコンテンツを誰でも閲覧できるようになります。

このユースケースでは、以下のアクセス管理ツールをお勧めします。

- Amazon CloudFront – このソリューションでは、バケットのコンテンツへのすべてのパブリックアクセスを継続的にブロックしながら、Amazon S3 静的ウェブサイトをパブリックにホストできます。4 つすべての S3 の [パブリックアクセスをブロック] 設定を有効にしたまま、S3 静的ウェブサイトをホストする場合は、Amazon CloudFront のオリジンアクセスコントロール (OAC) を使用できます。Amazon CloudFront は、セキュアな静的ウェブサイトをセットアップするために必要な機能を提供します。また、このソリューションを使用しない Amazon S3 静的ウェブサイトは、HTTP エンドポイントのみをサポートします。CloudFront は、耐久性に優れた Amazon S3 のあるストレージを使用し、HTTPS などの追加のセキュリティヘッダーを提供します。HTTPS では、通常の HTTP リクエストを暗号化し、一般的なサイバー攻撃から保護することで、セキュリティが強化されます。

詳細については、「Amazon CloudFront デベロッパーガイド」の「安全な静的ウェブサイトの使用開始」を参照してください。

- Amazon S3 バケットをパブリックにアクセス可能にする – パブリックにアクセス可能な静的ウェブサイトとして使用できるようにバケットを設定できます。

  > **Warning**
  >
  > この方法はお勧めしていません。代わりに、Amazon CloudFront の一部として Amazon S3 静的ウェブサイトを使用することをお勧めします。詳細については、前のオプションを参照するか、「安全な静的ウェブサイトの使用開始」を参照してください。

  Amazon CloudFront を使用せずに Amazon S3 静的ウェブサイトを作成するには、まずすべてのパブリックアクセスブロック設定をオフにする必要があります。静的ウェブサイトのバケットポリシーを記述するときは、`ListObject` または `PutObject` アクセス許可ではなく、`s3:GetObject` アクションのみを指定してください。これにより、ユーザーがバケット内のすべてのオブジェクトを表示したり、独自のコンテンツを追加したりできなくなります。詳細については、「ウェブサイトアクセスのアクセス許可の設定」を参照してください。

AWS アカウント所有者またはバケット所有者がバケットのコンテンツを公開したい

新しい Amazon S3 バケットを作成する場合、パブリックアクセスブロック設定はデフォルトで有効になっています。ブロックパブリックアクセスの詳細については、Amazon S3 ストレージへのパブリックアクセスのブロック を参照してください。

バケットへのすべてのパブリックアクセスを許可することはお勧めしません。ただし、特定のユースケースで設定する必要がある場合は、このユースケースで次のアクセス管理ツールを使用することをお勧めします。

- ブロックパブリックアクセス設定を無効にする – バケット所有者は、バケットへの認証されていないリクエストを許可できます。例えば、認証されていない Put Object リクエストは、バケットにパブリックバケットポリシーが適用されている場合や、バケットの ACL でパブリックアクセス許可が付与されている場合は許可されます。認証されていないリクエストはすべて、他の任意の AWS ユーザー、または認証されていない匿名ユーザーによって行われます。このユーザーは、特定の正規ユーザー ID `65a011a29cdf8ec533ec3d1ccaae921c` によって、ACL で表されます。オブジェクトが `WRITE` または `FULL_CONTROL` にアップロードされた場合、特にすべてのユーザーグループまたは匿名ユーザーへのアクセスが許可されます。パブリックバケットポリシーとパ

ブリックアクセスコントロールリスト (ACL) の詳細については、「パブリック」の意味 を参照してください。

AWS アカウント所有者またはバケット所有者がアクセスポリシーのサイズ制限を超えた

バケットポリシーとアイデンティティベースのポリシーには、どちらも 20 KB のサイズ制限があります。アクセス許可の要件が複雑な場合、このサイズ制限を超える可能性があります。

このユースケースでは、以下のアクセス管理ツールをお勧めします。

- Access Points — ユースケースで機能する場合、アクセスポイントを使用します。アクセスポイントでは、各バケットには複数の名前付きネットワークエンドポイントがあり、それぞれに基盤となるバケットポリシーで動作する独自のアクセスポイントポリシーがあります。ただし、アクセスポイントはバケットではなくオブジェクトに対してのみ動作し、クロスリージョンレプリケーションはサポートされていません。詳細については、「アクセスポイントを使用した汎用バケット内の共有データセットへのアクセスの管理」を参照してください。
- S3 Access Grants – S3 Access Grants を使用します。S3 Access Grants は、バケット、プレフィックス、またはオブジェクトへのアクセス権限を付与する非常に多数の許可をサポートしています。詳細については、「S3 Access Grants の開始方法」を参照してください。

AWS アカウント所有者または管理者ロールが、社内ディレクトリ内のユーザーまたはグループにバケット、プレフィックス、またはオブジェクトへの直接アクセスを許可したい

AWS Identity and Access Management (IAM) を介してユーザー、グループ、ロールを管理する代わりに、社内ディレクトリを AWS IAM Identity Center に追加できます。詳細については、「IAM Identity Center とは」を参照してください。

AWS IAM Identity Center に社内ディレクトリを追加したら、以下のアクセス管理ツールを使用して、社内ディレクトリアイデンティティに S3 リソースへのアクセス権を付与することをお勧めします。

- S3 Access Grants – S3 Access Grants を使用します。S3 Access Grants は、社内ディレクトリ内のユーザーまたはロールへのアクセスの付与をサポートしています。詳細については、「S3 Access Grants の開始方法」を参照してください。

AWS アカウント所有者またはバケット所有者が、CloudFront ログを S3 バケットに書き込むためのアクセス権をAWS CloudFront サービスに付与したい

このユースケースでは、以下のアクセス管理ツールをお勧めします。

- バケット ACL – バケット ACL の唯一の推奨されるユースケースは、 Amazon CloudFront `awslogsdelivery` アカウントなどの特定の AWS のサービスに許可を付与することです。ディストリビューションを作成または更新して、CloudFront ロギングを有効にすると、CloudFront はバケット ACL を更新して、バケットにログを書き込むための `awslogsdelivery` 許可を `FULL_CONTROL` アカウントに付与します。詳細については、「Amazon CloudFront デベロッパーガイド」の「標準ログ記録の設定とログファイルへのアクセスに必要なアクセス許可」を参照してください。ログを保存するバケットが S3 オブジェクト所有権のバケット所有者の強制設定を使用して ACL を無効にすると、CloudFront はバケットにログを書き込むことができません。詳細については、「オブジェクトの所有権の制御とバケットの ACL の無効化。」を参照してください。

バケット所有者が、他のユーザーによってバケットに追加されるオブジェクトを完全に制御したい。

バケットポリシー、アクセスポイント、または S3 Access Grants を使用して、バケットにオブジェクトをアップロードするためのアクセス権を他のアカウントに付与できます。バケットへのクロスアカウントアクセスが許可されている場合、バケットにアップロードされたオブジェクトに対して完全なコントロールを維持していることを確認できます。

このユースケースでは、以下のアクセス管理ツールをお勧めします。

- オブジェクト所有者 – バケットレベルの設定 [オブジェクト所有者] をデフォルトの [バケット所有者の強制] 設定のままにします。

アクセス管理のトラブルシューティング

以下のリソースは、S3 アクセス管理に関する問題のトラブルシューティングに役立ちます。

アクセス拒否 (403 Forbidden) エラーのトラブルシューティング

アクセス拒否の問題が発生した場合は、アカウントレベルとバケットレベルの設定を確認してください。また、アクセス権利を付与するために使用するアクセス管理機能をチェックして、ポリシー、設定、または構成が正しいことを確認します。Amazon S3 のアクセス拒否 (403 禁止) エラーの一

般的な原因の詳細については、「Amazon S3 でのアクセス拒否 (403 Forbidden) エラーのトラブルシューティング」を参照してください。

IAM Access Analyzer for S3

どのリソースも公開しない場合、またはリソースへのパブリックアクセスを制限する場合は、IAM Access Analyzer for S3 を使用します。Amazon S3 コンソールで、IAM Access Analyzer for S3 を使用して、パブリックアクセスまたは共有アクセスを許可するバケットアクセスコントロールリスト (ACL)、バケットポリシー、アクセスポイントポリシーを持つすべてのバケットを確認します。IAM Access Analyzer for S3 は、インターネットの任意のユーザーや他の AWS アカウント (組織外の AWS アカウント を含む) にアクセスを許可するように設定されているバケットに関して警告します。パブリックバケットまたは共有バケットごとに、パブリックアクセスや共有アクセスのソースとレベルを報告する結果が送信されます。

IAM Access Analyzer for S3 では、バケットへのすべてのパブリックアクセスを 1 つのアクションでブロックできます。特定のユースケースをサポートするためにパブリックアクセスが必要な場合を除き、バケットへのすべてのパブリックアクセスをブロックすることをお勧めします。すべてのパブリックアクセスをブロックする前に、アプリケーションがパブリックアクセスなしで正常に動作することを確認してください。詳細については、「Amazon S3 ストレージへのパブリックアクセスのブロック」を参照してください。

また、バケットレベルのアクセス許可の設定を参照して、詳細なアクセスレベルを設定することもできます。パブリックアクセスまたは共有アクセスを必要とする特定の検証済みユースケースについては、バケットの調査結果をアーカイブすることで、バケットをパブリックまたは共有とすることを確定して記録できます。これらのバケット設定はいつでも再確認および変更できます。結果は、監査目的で CSV レポートとしてダウンロードすることもできます。

IAM Access Analyzer for S3 は、Amazon S3 コンソールで追加料金なしで使用できます。IAM Access Analyzer for S3 は、AWS Identity and Access Management (IAM) IAM Access Analyzer を利用しています。Amazon S3 コンソールで IAM Access Analyzer for S3 を使用するには、IAM コンソールにアクセスして、IAM Access Analyzer で個別のリージョンごとにアカウントレベルのアナライザーを作成する必要があります。

IAM Access Analyzer for S3 の詳細については、IAM Access Analyzer for S3 を使用したバケットアクセスの確認 を参照してください。

ログ記録とモニタリング

モニタリングは、アクセス障害を簡単にデバッグできるように、Amazon S3 ソリューションの信頼性、可用性、パフォーマンスを維持するうえで重要な部分です。ログ記録により、ユーザーが受け

取ったエラーや、いつどのようなリクエストが行われたかを把握できます。AWS には、Amazon S3 リソースをモニタリングするための以下のようなツールがいくつかあります。

- AWS CloudTrail
- Amazon S3 アクセスログ
- AWS Trusted Advisor
- Amazon CloudWatch

詳細については、「Amazon S3 でのログ記録とモニタリング」を参照してください。

Amazon S3 用 Identity and Access Management

AWS Identity and Access Management (IAM) は管理者が AWS リソースへのアクセスを安全に制御するために役立つ AWS のサービスです。IAM 管理者は、誰が認証 (サインイン) され、Amazon S3 リソースを使用する認可を受ける (許可がある) ことができるかを制御します。IAM は追加費用なしで使用できる AWS のサービスです。

S3 リソースタイプ別の S3 API オペレーションへのアクセス許可の詳細については、「Amazon S3 API オペレーションに必要なアクセス許可」を参照してください。

> **Note**
>
> Amazon S3 Express One Zone ストレージクラスをディレクトリバケットで使用する方法の詳細については、「S3 Express One Zone」と「ディレクトリバケットの使用」を参照してください。

トピック

- 対象者
- アイデンティティによる認証
- ポリシーを使用したアクセス権の管理
- Amazon S3 での IAM の機能
- Amazon S3 がリクエストを許可する仕組み
- Amazon S3 API オペレーションに必要なアクセス許可
- Amazon S3 のポリシーとアクセス許可
- Amazon S3 のバケットポリシー

- Amazon S3 のアイデンティティベースのポリシー
- チュートリアル: ポリシーを使用した Amazon S3 リソースへのアクセスの管理
- Amazon S3 ストレージレンズでのサービスにリンクされたロールの使用
- Amazon S3 アイデンティティとアクセスのトラブルシューティング
- Amazon S3 の AWS マネージドポリシー

対象者

AWS Identity and Access Management (IAM) の使用方法は、Amazon S3 で行う作業に応じて異なります。

サービスユーザー – 業務を行うために Amazon S3 サービスを使用する場合、管理者が必要な認証情報および許可を提供します。業務のために使用する Amazon S3 機能が増えるにつれ、追加の許可が必要な場合があります。アクセスの管理方法を理解すると、管理者に適切なアクセス許可をリクエストするのに役に立ちます。Amazon S3 の機能にアクセスできない場合は、「Amazon S3 アイデンティティとアクセスのトラブルシューティング」を参照してください。

サービス管理者 – 社内の Amazon S3 リソースを担当している場合は、Amazon S3 に対する完全なアクセス権があると思われます。サービスのユーザーがどの Amazon S3 機能やリソースにアクセスするかを決めるのは管理者の仕事です。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を点検して、IAM の基本概念を理解してください。会社が Amazon S3 で IAM を使用する方法の詳細については、「Amazon S3 での IAM の機能」を参照してください。

IAM 管理者 – IAM 管理者には、Amazon S3 へのアクセスを管理するポリシーの作成方法の詳細を理解することが推奨されます。IAM で使用可能な Amazon S3 アイデンティティベースのポリシーの例を確認するには、「Amazon S3 のアイデンティティベースのポリシー」を参照してください。

アイデンティティによる認証

認証とは、アイデンティティ認証情報を使用して AWSにサインインする方法です。ユーザーは、AWS アカウントのルートユーザー、IAM ユーザーとして、または IAM ロールを引き受けることによって、認証される (AWSにサインインする) 必要があります。

ID ソースから提供された認証情報を使用して、フェデレーティッドアイデンティティとして AWS にサインインできます。AWS IAM Identity Centerフェデレーティッドアイデンティティの例としては、(IAM アイデンティティセンター) ユーザー、貴社のシングルサインオン認証、Google または Facebook の認証情報などがあります。フェデレーティッド ID としてサインインする場合、IAM

ロールを使用して、前もって管理者により ID フェデレーションが設定されています。フェデレーションを使用して AWSにアクセスする場合、間接的にロールを引き受けることになります。

ユーザーのタイプに応じて、AWS Management Consoleまたは AWS アクセスポータルにサインインできます。AWS へのサインインの詳細については、「AWS サインイン ユーザーガイド」の「AWS アカウント にサインインする方法」を参照してください。

プログラムを使用して AWS にアクセスする場合、AWSは Software Development Kit (SDK) とコマンドラインインターフェイス (CLI) を提供し、認証情報を使用してリクエストに暗号で署名します。AWS ツールを使用しない場合は、リクエストに自分で署名する必要があります。リクエストに自分で署名する推奨方法の使用については、「IAM ユーザーガイド」の「API リクエストに対する AWS Signature Version 4」を参照してください。

使用する認証方法を問わず、追加セキュリティ情報の提供をリクエストされる場合もあります。例えば、AWS は、アカウントのセキュリティを強化するために多要素認証 (MFA) を使用することをお勧めします。詳細については、「AWS IAM Identity Center ユーザーガイド」の「多要素認証」および「IAM ユーザーガイド」の「IAM の AWS 多要素認証」を参照してください。

AWS アカウント のルートユーザー

AWS アカウント を作成する場合は、このアカウントのすべての AWS のサービス とリソースに対して完全なアクセス権を持つ 1 つのサインインアイデンティティから始めます。このアイデンティティは AWS アカウント ルートユーザーと呼ばれ、アカウントの作成に使用した E メールアドレスとパスワードでサインインすることによってアクセスできます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報は保護し、ルートユーザーでしか実行できないタスクを実行するときに使用します。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、「IAM ユーザーガイド」の「ルートユーザー認証情報が必要なタスク」を参照してください。

フェデレーティッドアイデンティティ

ベストプラクティスとして、管理者アクセスを必要とするユーザーを含む人間のユーザーに対し、ID プロバイダーとのフェデレーションを使用して、一時的な認証情報の使用により、AWS のサービスにアクセスすることを要求します。

フェデレーティッド ID は、エンタープライズユーザーディレクトリ、ウェブ ID プロバイダー、AWS Directory Service、Identity Center ディレクトリのユーザーか、または ID ソースから提供された認証情報を使用して AWS のサービス にアクセスするユーザーです。フェデレーティッド ID が AWS アカウントにアクセスすると、ロールが継承され、ロールは一時的な認証情報を提供します。

アクセスを一元管理する場合は、AWS IAM Identity Centerを使用することをお勧めします。IAM アイデンティティセンター でユーザーとグループを作成するか、すべての AWS アカウント とアプリケーションで使用するために、独自の ID ソースで一連のユーザーとグループに接続して同期することもできます。IAM Identity Center の詳細については、「AWS IAM Identity Centerユーザーガイド」の「What is IAM Identity Center?」(IAM Identity Center とは) を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、1 人のユーザーまたは 1 つのアプリケーションに対して特定の許可を持つ AWS アカウント 内のアイデンティティです。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を保有する IAM ユーザーを作成する代わりに、一時的な認証情報を使用することをお勧めします。ただし、IAM ユーザーでの長期的な認証情報が必要な特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、「IAM ユーザーガイド」の「長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションする」を参照してください。

IAM グループは、IAM ユーザーの集団を指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。例えば、IAMAdmins という名前のグループを設定して、そのグループに IAM リソースを管理する許可を与えることができます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時認証情報が提供されます。詳細については、「IAM ユーザーガイド」の「IAM ユーザーに関するユースケース」を参照してください。

IAM ロール

IAM ロールは、特定の許可を持つ、AWS アカウント内のアイデンティティです。これは IAM ユーザーに似ていますが、特定のユーザーには関連付けられていません。AWS Management Console で IAM ロールを一時的に引き受けるには、ユーザーから IAM ロール に切り替える (コンソール) ことができます。ロールを引き受けるには、AWS CLI または AWS API オペレーションを呼び出すか、カスタム URL を使用します。ロールを使用する方法の詳細については、「IAM ユーザーガイド」の「ロールを引き受けるための各種方法」を参照してください。

IAM ロールと一時的な認証情報は、次の状況で役立ちます:

- フェデレーションユーザーアクセス – フェデレーティッド ID に許可を割り当てるには、ロールを作成してそのロールの許可を定義します。フェデレーティッド ID が認証されると、その ID は

ロールに関連付けられ、ロールで定義されている許可が付与されます。フェデレーションのロールについては、「IAM ユーザーガイド」の「サードパーティー ID プロバイダー (フェデレーション) 用のロールを作成する」を参照してください。IAM Identity Center を使用する場合は、許可セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。アクセス許可セットの詳細については、「AWS IAM Identity Center User Guide」の「Permission sets」を参照してください。

- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。
- クロスアカウントアクセス - IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、一部の AWS のサービス では、(ロールをプロキシとして使用する代わりに) リソースにポリシーを直接アタッチできます。クロスアカウントアクセスにおけるロールとリソースベースのポリシーの違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。
- クロスサービスアクセス権 - 一部の AWS のサービス では、他の AWS のサービス の機能を使用します。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。サービスでは、呼び出し元プリンシパルの許可、サービスロール、またはサービスリンクロールを使用してこれを行う場合があります。
  - 転送アクセスセッション (FAS) – IAM ユーザーまたはロールを使用して AWS でアクションを実行するユーザーは、プリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、AWS のサービスを呼び出すプリンシパルの権限を、AWS のサービスのリクエストと合わせて使用し、ダウンストリームのサービスに対してリクエストを行います。FAS リクエストは、サービスが、完了するために他の AWS のサービス またはリソースとのやりとりを必要とするリクエストを受け取ったときにのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。
  - サービスロール - サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除することができます。詳細については、「IAM ユーザーガイド」の「AWS のサービス に許可を委任するロールを作成する」を参照してください。
  - サービスにリンクされたロール - サービスにリンクされたロールは、AWS のサービス にリンクされたサービスロールの一種です。サービスがロールを引き受け、ユーザーに代わってアクショ

ンを実行できるようになります。サービスにリンクされたロールは、AWS アカウント に表示され、サービスによって所有されます。IAM 管理者は、サービスリンクロールのアクセス許可を表示できますが、編集することはできません。

- Amazon EC2 で実行されているアプリケーション - EC2 インスタンスで実行され、AWS CLI または AWS API リクエストを行っているアプリケーションの一時的な認証情報を管理するには、IAM ロールを使用できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。AWS ロールを EC2 インスタンスに割り当て、そのすべてのアプリケーションで使用できるようにするには、インスタンスに添付されたインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、「IAM ユーザーガイド」の「Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して許可を付与する」を参照してください。

ポリシーを使用したアクセス権の管理

AWS でアクセスを制御するには、ポリシーを作成して AWS ID またはリソースにアタッチします。ポリシーは AWS のオブジェクトであり、アイデンティティやリソースに関連付けて、これらのアクセス許可を定義します。AWS は、プリンシパル (ユーザー、ルートユーザー、またはロールセッション) がリクエストを行うと、これらのポリシーを評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。大半のポリシーは JSON ドキュメントとして AWS に保存されます。JSON ポリシードキュメントの構造と内容の詳細については、「IAM ユーザーガイド」の「JSON ポリシー概要」を参照してください。

管理者は AWS JSON ポリシーを使用して、だれが何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

デフォルトでは、ユーザーやロールに権限はありません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き受けることができます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションの許可を定義します。例えば、`iam:GetRole` アクションを許可するポリシーがあるとします。このポリシーがあるユーザーは、AWS Management Console、AWS CLI、または AWS API からロール情報を取得できます。

アイデンティティベースのポリシー

アイデンティティベースポリシーは、IAM ユーザーグループ、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデン

ティティベースポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」を参照してください。

アイデンティティベースのポリシーは、さらにインラインポリシーまたはマネージドポリシーに分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれます。マネージドポリシーは、AWS アカウント内の複数のユーザー、グループ、およびロールにアタッチできるスタンドアロンポリシーです。マネージドポリシーには、AWS マネージドポリシーとカスタマーマネージドポリシーがあります。マネージドポリシーまたはインラインポリシーのいずれかを選択する方法については、「IAM ユーザーガイド」の「管理ポリシーとインラインポリシーのいずれかを選択する」を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーションユーザー、または AWS のサービス を含めることができます。

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。リソースベースのポリシーでは IAM の AWSマネージドポリシーは使用できません。

アクセスコントロールリスト (ACL)

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための許可を持つかを制御します。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Amazon S3、AWS WAF、および VPC は、ACL をサポートするサービスの例です。ACL の詳細については、「Amazon Simple Storage Service デベロッパーガイド」の「アクセスコントロールリスト (ACL) の概要」を参照してください。

その他のポリシータイプ

AWS では、他の一般的ではないポリシータイプをサポートしています。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- アクセス許可の境界 - アクセス許可の境界は、アイデンティティベースポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる権限の上限を設定する高度な機能です。エンティティにアクセス許可の境界を設定できます。結果として得られる権限は、エンティティのアイデンティティベースポリシーとそのアクセス許可の境界の共通部分になります。`Principal` フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、アクセス許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。アクセス許可の境界の詳細については、「IAM ユーザーガイド」の「IAM エンティティのアクセス許可の境界」を参照してください。
- サービスコントロールポリシー (SCP) - SCP は、AWS Organizations で組織や組織単位 (OU) の最大許可を指定する JSON ポリシーです。AWS Organizations は、お客様が所有する複数の AWS アカウントをグループ化し、一元的に管理するサービスです。組織内のすべての機能を有効にすると、サービスコントロールポリシー (SCP) を一部またはすべてのアカウントに適用できます。SCP はメンバーアカウントのエンティティに対する権限を制限します (各 AWS アカウントのルートユーザー など)。Organizations と SCP の詳細については、「AWS Organizations ユーザーガイド」の「サービスコントロールポリシー (SCP)」を参照してください。
- リソースコントロールポリシー (RCP) – RCP は、所有する各リソースにアタッチされた IAM ポリシーを更新することなく、アカウント内のリソースに利用可能な最大数のアクセス許可を設定するために使用できる JSON ポリシーです。RCP は、メンバーアカウントのリソースの許可を制限し、組織に属するかどうかにかかわらず、AWS アカウントのルートユーザー を含む ID のための有効な許可に影響を及ぼす可能性があります。RCP をサポートする AWS のサービス のリストを含む Organizations と RCP の詳細については、「AWS Organizations ユーザーガイド」の「リソースコントロールポリシー (RCP)」を参照してください。
- セッションポリシー - セッションポリシーは、ロールまたはフェデレーションユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、権限は無効になります。詳細については、「IAM ユーザーガイド」の「セッションポリシー」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される権限を理解するのがさらに難しくなります。複数のポリシータイプが関連するとき、リクエストを許可するかどうかを AWS が決定する方法の詳細については、「IAM ユーザーガイド」の「ポリシーの評価ロジック」を参照してください。

Amazon S3 での IAM の機能

IAM を使用して Amazon S3 へのアクセスを管理する前に、Amazon S3 で利用できる IAM 機能について理解しておく必要があります。

Amazon S3 で使用できる IAM の機能

IAM の機能	Amazon S3 のサポート
アイデンティティベースポリシー	はい
リソースベースのポリシー	はい
ポリシーアクション	はい
ポリシーリソース	はい
ポリシー条件キー (サービス固有)	はい
ACL	はい
ABAC (ポリシー内のタグ)	部分的
一時的な認証情報	あり
転送アクセスセッション (FAS)	あり
サービスロール	はい
サービスリンクロール	部分的

Amazon S3 およびその他の AWS サービスがほとんどの IAM 機能との連携する方法の詳細については、「IAM ユーザーガイド」の「IAM と連携する AWS サービス」を参照してください。

S3 リソースタイプ別の S3 API オペレーションへのアクセス許可の詳細については、「Amazon S3 API オペレーションに必要なアクセス許可」を参照してください。

Amazon S3 のアイデンティティベースのポリシー

アイデンティティベースのポリシーのサポート: あり

アイデンティティベースポリシーは、IAM ユーザーグループ、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。ID ベースのポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」を参照してください。

IAM アイデンティティベースのポリシーでは、許可または拒否するアクションとリソース、およびアクションを許可または拒否する条件を指定できます。プリンシパルは、それが添付されているユーザーまたはロールに適用されるため、アイデンティティベースのポリシーでは指定できません。JSON ポリシーで使用できるすべての要素について学ぶには、「IAM ユーザーガイド」の「IAM JSON ポリシーの要素のリファレンス」を参照してください。

Amazon S3 のアイデンティティベースのポリシー例

Amazon S3 のアイデンティティベースのポリシー例を確認するには、「Amazon S3 のアイデンティティベースのポリシー」を参照してください。

Amazon S3 内のリソースベースのポリシー

リソースベースのポリシーのサポート: あり

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーがアタッチされているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーションユーザー、または AWS のサービス を含めることができます。

クロスアカウントアクセスを有効にするには、全体のアカウント、または別のアカウントの IAM エンティティを、リソースベースのポリシーのプリンシパルとして指定します。リソースベースのポリシーにクロスアカウントのプリンシパルを追加しても、信頼関係は半分しか確立されない点に注意してください。プリンシパルとリソースが異なる AWS アカウント にある場合、信頼できるアカウントの IAM 管理者は、リソースにアクセスするための権限をプリンシパルエンティティ (ユーザーまたはロール) に付与する必要もあります。IAM 管理者は、アイデンティティベースのポリシーをエンティティにアタッチすることで権限を付与します。ただし、リソースベースのポリシーで、同じアカウントのプリンシパルへのアクセス権が付与されている場合は、アイデンティティベースのポリシーをさらに付与する必要はありません。詳細については、「IAM ユーザーガイド」の「IAM でのクロスアカウントリソースアクセス」を参照してください。

Amazon S3 サービスは、バケットポリシー、アクセスポイントポリシー、およびアクセス許可をサポートします。

- バケットポリシーは、Amazon S3 バケットにアタッチされるリソースベースのポリシーです。リソースポリシーは、バケットに対してアクションを実行できるプリンシパルを定義します。
- アクセスポイントポリシーは、基になるバケットポリシーと組み合わせて評価されるリソースベースのポリシーです。
- アクセス許可は、Amazon S3 内のデータへのアクセス許可をプレフィックス、バケット、またはオブジェクトごとに定義するための簡略化されたモデルです。S3 Access Grants の詳細については、「S3 Access Grants でのアクセス管理」を参照してください。

バケットポリシーのプリンシパル

`Principal` エレメントは、リソースへのアクセスを許可または拒否するユーザー、アカウント、サービス、または他のエンティティを指定します。`Principal` を指定する例を以下に示します。詳細については、「IAM ユーザーガイド」の「プリンシパル」を参照してください。

AWS アカウントに許可を付与する

AWS アカウントに許可を付与するには、以下の形式を使用してアカウントを指定します。

```
"AWS":"account-ARN"
```

次に例を示します。

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

```
"Principal":{"AWS":
["arn:aws:iam::AccountID1WithoutHyphens:root","arn:aws:iam::AccountID2WithoutHyphens:root"]}
```

IAM ユーザーにアクセス許可を付与する

アカウントの IAM ユーザーにアクセス許可を付与するには、"AWS":"*user-ARN*" の名前と値のペアを指定する必要があります。

```
"Principal":{"AWS":"arn:aws:iam::account-number-without-hyphens:user/username"}
```

ステップバイステップの手順を説明する詳細な例については、例 1: バケット所有者がユーザーにバケットのアクセス許可を付与する および 例 3: バケット所有者が自分の所有していないオブジェクトに対するアクセス許可を付与する を参照してください。

> **Note**
>
> バケットポリシーを更新した後に IAM ID を削除すると、バケットポリシーのプリンシパル要素には ARN の代わりに一意の ID が表示されます。これらの一意な ID は再利用されることがないため、すべてのポリシーステートメントから一意の ID を持つプリンシパルを安全に削除できます。一意の ID の詳細については、IAM ユーザーガイドの「IAM ID」を参照してください。

匿名アクセス許可を付与する

> **Warning**
>
> Simple Storage Service (Amazon S3) バケットへの匿名アクセスを付与するときは注意が必要です。匿名アクセスを付与すると、世界中のすべてのユーザーがバケットにアクセスできます。種類にかかわらず、S3 バケットへの匿名書き込みアクセスは一切付与しないことを強くお勧めします。

匿名アクセスと呼ばれるアクセス許可を全員に付与するには、`Principal` の値としてワイルドカード (`"*"`) を設定します。例えば、バケットを Web サイトとして設定する場合、以下のように、バケット内のすべてのオブジェクトを公開し、誰でもアクセスできるようにすることができます。

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

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

リソースベースのポリシーで、`"Principal": "*"` 効果と共に `Allow` を使用すると、AWS にサインしていなくても、誰でもリソースにアクセスできるようになります。

リソースベースのポリシーで、`Allow` 効果と共に `"Principal" : { "AWS" : "*" }` を使用すると、同じパーティションのどのアカウントのルートユーザー、IAM ユーザー、引き受けたロールのセッション、フェデレーティッドユーザーでも、リソースにアクセスできるようになります。

匿名ユーザーの場合、これら 2 つの方法は同等です。詳細については、「IAM ユーザーガイド」の「すべてのプリンシパル」を参照してください。

ワイルドカードとして使用して、プリンシパルの名前または ARN の一部に一致させることはできません。

> **Important**
>
> AWS アクセスコントロールポリシーでは、プリンシパル "*" と {"AWS": "*"} は同じように動作します。

リソースのアクセス許可の制限

リソースポリシーを使用して、それ以外の場合は IAM プリンシパルで利用できるリソースへのアクセスを制限することもできます。Deny ステートメントを使用してアクセスを防止します。

次の例では、安全な転送プロトコルが使用されていない場合はアクセスをブロックします。

```
{"Effect": "Deny",
 "Principal": "*",
 "Action": "s3:*",
 "Resource": <bucket ARN>,
 "Condition": {
   "Boolean": { "aws:SecureTransport" : "false"}
 }
}
```

このポリシーでは、この方法を使用して特定のアカウントやプリンシパルのみへのアクセスの拒否を試みるのではなく、"Principal": "*" を使用して、この制限をすべてのユーザーに適用することがベストプラクティスです。

CloudFront の URL を使用したアクセスの要求

Amazon S3 の URL の代わりに CloudFront の URL を使用することで、ユーザーが Amazon S3 のコンテンツのみにアクセスするように制限することができます。これを行うには、CloudFront オリジンアクセスコントロール (OAC) を作成します。その後、S3 データのアクセス許可を変更します。バケットポリシーでは、次のように CloudFront をプリンシパルとして設定できます。

```
"Principal":{"Service":"cloudfront.amazonaws.com"}
```

ポリシーの Condition 要素を使用して、S3 オリジンを含む CloudFront ディストリビューションに代わってリクエストが行われた場合にのみ CloudFront がバケットにアクセスできるようにします。

```
       "Condition": {
          "StringEquals": {
             "AWS:SourceArn":
"arn:aws:cloudfront::111122223333:distribution/CloudFront-distribution-ID"
          }
       }
```

CloudFront URL を使用した S3 アクセスの制限の詳細については、「Amazon CloudFront 開発者ガイド」の「Amazon Simple Storage Service オリジンへのアクセスの制限」を参照してください。Amazon CloudFront を使用する場合のセキュリティとプライバシーのメリットの詳細については、「コンテンツへのセキュアなアクセスとアクセス制限の設定」を参照してください。

Amazon S3 のリソースベースポリシーの例

- Amazon S3 バケットポリシーの例については、「Amazon S3 のバケットポリシー」を参照してください。
- アクセスポイントのポリシーの例については、「汎用バケットのアクセスポイントを使用するための IAM ポリシーの設定」を参照してください。

Amazon S3 のポリシーアクション

ポリシーアクションのサポート:あり

管理者は AWS JSON ポリシーを使用して、だれが何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対して、どのような条件下でアクションを実行できるかということです。

JSON ポリシーの Action 要素にはポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。ポリシーアクションの名前は通常、関連する AWS API オペレーションと同じです。一致する API オペレーションのない許可のみのアクションなど、いくつかの例外があります。また、ポリシーに複数のアクションが必要なオペレーションもあります。これらの追加アクションは依存アクションと呼ばれます。

このアクションは関連付けられたオペレーションを実行するためのアクセス許可を付与するポリシーで使用されます。

以下に、S3 API オペレーションと必要なポリシーアクション間のさまざまなタイプのマッピング関係を示します。

- 同じ名前の 1 対 1 のマッピング。例えば、 PutBucketPolicy API オペレーションを使用するには、s3:PutBucketPolicy ポリシーアクションが必要です。
- 異なる名前の 1 対 1 のマッピング。例えば、 ListObjectsV2 API オペレーションを使用するには、s3:ListBucket ポリシーアクションが必要です。
- 1 対多のマッピング。例えば、HeadObject API オペレーションを使用するには、s3:GetObject が必要です。また、S3 オブジェクトロックを使用し、オブジェクトのリーガルホールドステータスまたは保持設定を取得したい場合は、HeadObject API オペレーションを使用する前に、対応する s3:GetObjectLegalHold または s3:GetObjectRetention ポリシーアクションも必要です。
- 1 対多のマッピング。例えば、ListObjectsV2 または HeadBucket API オペレーションを使用するには、s3:ListBucket ポリシーアクションが必要です。

ポリシーで使用する Amazon S3 アクションの一覧については、「サービス認可リファレンス」の「Amazon S3 で定義されるアクション」を参照してください。Amazon S3 API オペレーションの完全なリストについては、「Amazon Simple Storage Service API リファレンス」の「Amazon S3 API アクション」を参照してください。

S3 リソースタイプ別の S3 API オペレーションへのアクセス許可の詳細については、「Amazon S3 API オペレーションに必要なアクセス許可」を参照してください。

Amazon S3 のポリシーアクションは、アクションの前に次のプレフィックスを使用します。

```
s3
```

単一のステートメントで複数のアクションを指定するには、アクションをカンマで区切ります。

```
"Action": [
      "s3:action1",
      "s3:action2"
         ]
```

バケットオペレーション

バケットオペレーションは、バケットリソースタイプで動作する S3 API オペレーションです。例: `CreateBucket`、`ListObjectsV2`、`PutBucketPolicy`。バケットオペレーションの S3 ポリシーアクションでは、バケットポリシーの `Resource` 要素または IAM アイデンティティベースのポリシーが、次の例形式の S3 バケットタイプの Amazon リソースネーム (ARN) 識別子である必要があります。

```
"Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
```

次のバケットポリシーは、アカウント *12345678901* のユーザー *Akua* に ListObjectsV2 API オペレーションを実行し、S3 バケット内のオブジェクトを一覧表示する `s3:ListBucket` アクセス許可を付与します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow Akua to list objects in the bucket",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::12345678901:user/Akua"
            },
            "Action": [
            "s3:ListBucket"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
        }
    ]
}
```

汎用バケットのアクセスポイントのポリシーでのバケットオペレーション

汎用バケットのアクセスポイントポリシーで付与されるアクセス許可は、基になるバケットで同じアクセス許可が許可される場合にのみ有効です。S3 アクセスポイントを使用する場合は、バケットからアクセスポイントにアクセスコントロールを委任するか、アクセスポイントポリシーで同じアクセス許可を基礎となるバケットのポリシーに追加する必要があります。詳細については、「汎用バケットのアクセスポイントを使用するための IAM ポリシーの設定」を参照してください。アクセスポイントポリシーでは、バケットオペレーションの S3 ポリシーアクションで、次の形式の `Resource` 要素にアクセスポイント ARN を使用する必要があります。

```
"Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-point"
```

次のアクセスポイントポリシーは、*example-access-point* という名前の S3 アクセスポイントを介して ListObjectsV2 API オペレーションを実行する s3:ListBucket アクセス許可をアカウント *12345678901* のユーザー *Akua* に付与します。このアクセス許可により、*Akua* は *example-access-point* に関連付けられているバケット内のオブジェクトを一覧表示できます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow Akua to list objects in the bucket through access point",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::12345678901:user/Akua"
            },
            "Action": [
            "s3:ListBucket"
            ],
            "Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-
point"
        }
    ]
}
```

> **Note**
>
> すべてのバケットオペレーションが汎用バケットのアクセスポイントでサポートされているわけではありません。詳細については、「汎用バケットのアクセスポイントと S3 オペレーションとの互換性」を参照してください。

ディレクトリバケットのアクセスポイントのポリシーでのバケットオペレーション

ディレクトリバケットのアクセスポイントポリシーで付与されるアクセス許可は、基になるバケットで同じアクセス許可が許される場合にのみ有効です。S3 アクセスポイントを使用する場合は、バケットからアクセスポイントにアクセスコントロールを委任するか、アクセスポイントポリシーで同じアクセス許可を基礎となるバケットのポリシーに追加する必要があります。詳細については、「ディレクトリバケットのアクセスポイントを使用するための IAM ポリシーの設定」を参照してく

ださい。アクセスポイントポリシーでは、バケットオペレーションの S3 ポリシーアクションで、次の形式の Resource 要素にアクセスポイント ARN を使用する必要があります。

```
"Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-point--usw2-az1--xa-s3"
```

次のアクセスポイントポリシーは、*example-access-point--usw2-az1--xa-s3* という名前のアクセスポイントを介して ListObjectsV2 API オペレーションを実行する s3:ListBucket アクセス許可をアカウント *12345678901* のユーザー *Akua* に付与します。このアクセス許可により、*Akua* は *example-access-point--usw2-az1--xa-s3* に関連付けられているバケット内のオブジェクトを一覧表示できます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow Akua to list objects in the bucket through access point",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::12345678901:user/Akua"
            },
            "Action": [
            "s3:ListBucket"
            ],
            "Resource": "arn:aws:s3express:us-west-2:123456789012:accesspoint/example-access-point--usw2-az1--xa-s3"
        }
    ]
}
```

> **Note**
>
> すべてのバケットオペレーションがディレクトリバケットのアクセスポイントでサポートされているわけではありません。詳細については、「ディレクトリバケットのアクセスポイントのオブジェクトオペレーション」を参照してください。

オブジェクト操作

オブジェクトオペレーションは、オブジェクトリソースタイプに基づいて実行される S3 API オペレーションです。例: `GetObject`、`PutObject`、`DeleteObject`。オブジェクトオペレーションの S3 ポリシーアクションでは、ポリシーの `Resource` 要素を次の例の形式で S3 オブジェクト ARN にする必要があります。

```
"Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
```

```
"Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/*"
```

> **Note**
>
> 前の例に示すように、オブジェクト ARN にはバケット名の後にスラッシュが含まれている必要があります。

以下のバケットポリシーは、アカウント *12345678901* のユーザー *Akua* に `s3:PutObject` の許可を付与します。このアクセス許可により、*Akua* は PutObject API オペレーションを使用して、*amzn-s3-demo-bucket* という名前の S3 バケットにオブジェクトをアップロードできるようになります。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow Akua to upload objects",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::12345678901:user/Akua"
            },
            "Action": [
            "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
        }
    ]
}
```

アクセスポイントポリシーでのオブジェクトオペレーション

S3 アクセスポイントを使用してオブジェクトオペレーションへのアクセスを制御する場合、アクセスポイントポリシーを使用できます。アクセスポイントポリシーを使用するとき、オブジェクトオペレーションの S3 ポリシーアクションで、arn:aws:s3:*region*:*account-id*:accesspoint/*access-point-name*/object/*resource* 形式の Resource 要素にアクセスポイント ARN を使用する必要があります。アクセスポイントを使用するオブジェクトオペレーションの場合、アクセスポイント ARN 全体の後に /object/ 値を Resource 要素に含める必要があります。次に例を示します。

```
"Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-point/object/
*"
```

```
"Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-point/
object/prefix/*"
```

次のアクセスポイントポリシーは、アカウント *12345678901* のユーザー *Akua* に s3:GetObject アクセス許可を付与します。このアクセス許可により、*Akua* は、アクセスポイントに関連付けられているバケット内のすべてのオブジェクトに対して、*example-access-point* という名前のアクセスポイントを介して GetObject API オペレーションを実行できます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow Akua to get objects through access point",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::12345678901:user/Akua"
            },
            "Action": [
            "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-
point/object/*"
        }
    ]
}
```

> **Note**
>
> すべてのオブジェクトオペレーションがアクセスポイントでサポートされているわけではありません。詳細については、「汎用バケットのアクセスポイントと S3 オペレーションとの互換性」を参照してください。

ディレクトリバケットのアクセスポイントのポリシーでのオブジェクトオペレーション

ディレクトリバケットのアクセスポイントを使用してオブジェクトオペレーションへのアクセスを制御する場合、アクセスポイントポリシーを使用できます。アクセスポイントポリシーを使用するとき、オブジェクトオペレーションの S3 ポリシーアクションで、arn:aws:s3:*region*:*account-id*:accesspoint/*access-point-name*/object/*resource* 形式の Resource 要素にアクセスポイント ARN を使用する必要があります。アクセスポイントを使用するオブジェクトオペレーションの場合、アクセスポイント ARN 全体の後に /object/ 値を Resource 要素に含める必要があります。次に例を示します。

```
"Resource": "arn:aws:s3express:us-west-2:123456789012:accesspoint/example-access-point--usw2-az1--xa-s3/object/*"
```

```
"Resource": "arn:aws:s3express:us-west-2:123456789012:accesspoint/example-access-point--usw2-az1--xa-s3/object/prefix/*"
```

次のアクセスポイントポリシーは、アカウント *12345678901* のユーザー *Akua* に s3:GetObject アクセス許可を付与します。このアクセス許可により、*Akua* は、アクセスポイントに関連付けられているバケット内のすべてのオブジェクトに対して、*example-access-point--usw2-az1--xa-s3* という名前のアクセスポイントを介して GetObject API オペレーションを実行できます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow Akua to get objects through access point",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::12345678901:user/Akua"
            },
            "Action": "s3express:CreateSession","s3:GetObject"
            "Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-point--usw2-az1--xa-s3/object/*"
```

```
        }
    ]
}
```

> **Note**
>
> すべてのオブジェクトオペレーションがディレクトリバケットのアクセスポイントでサポートされているわけではありません。詳細については、「ディレクトリバケットのアクセスポイントのオブジェクトオペレーション」を参照してください。

汎用バケットオペレーションのアクセスポイント

アクセスポイントオペレーションは、accesspoint リソースタイプで動作する S3 API オペレーションです。例: CreateAccessPoint、DeleteAccessPoint、GetAccessPointPolicy。アクセスポイントオペレーションの S3 ポリシーアクションは、バケットポリシーやアクセスポイントポリシーではなく、IAM アイデンティティベースのポリシーでのみ使用できます。アクセスポイントオペレーションでは、Resource 要素を次の例の形式のアクセスポイント ARN にする必要があります。

```
"Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-point"
```

次の IAM アイデンティティベースのポリシーは、*example-access-point* という名前の S3 アクセスポイントで GetAccessPointPolicy API オペレーションを実行する s3:GetAccessPointPolicy アクセス許可を付与します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Grant permission to retrieve the access point policy of access
 point example-access-point",
            "Effect": "Allow",
            "Action": [
            "s3:GetAccessPointPolicy"
            ],
            "Resource": "arn:aws:s3:*:123456789012:accesspoint/example-access-point"
        }
    ]
}
```

アクセスポイントを使用してバケットオペレーションへのアクセスを制御する場合は、「汎用バケットのアクセスポイントのポリシーでのバケットオペレーション」を参照してください。オブジェクトオペレーションへのアクセスを制御するには、「アクセスポイントポリシーでのオブジェクトオペレーション」を参照してください。アクセスポイントポリシーの設定方法の詳細については、「汎用バケットのアクセスポイントを使用するための IAM ポリシーの設定」を参照してください。

ディレクトリバケットオペレーションのアクセスポイント

ディレクトリバケットオペレーションのアクセスポイントは、accesspoint リソースタイプで動作する S3 API オペレーションです。例: CreateAccessPoint、DeleteAccessPoint、GetAccessPointPolicy。アクセスポイントオペレーションの S3 ポリシーアクションは、バケットポリシーやアクセスポイントポリシーではなく、IAM アイデンティティベースのポリシーでのみ使用できます。ディレクトリバケットオペレーションのアクセスポイントでは、Resource 要素を次の例の形式のアクセスポイント ARN にする必要があります。

```
"Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-point--usw2-az1--xa-s3"
```

次の IAM アイデンティティベースのポリシーは、*example-access-point--usw2-az1--xa-s3* という名前のアクセスポイントで GetAccessPointPolicy API オペレーションを実行する s3express:GetAccessPointPolicy アクセス許可を付与します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Grant permission to retrieve the access point policy of access
 point example-access-point--usw2-az1--xa-s3",
            "Effect": "Allow",
            "Action": [
            "s3express:CreateSession","s3express:GetAccessPointPolicy"
            ],
            "Resource": "arn:aws:s3:*:123456789012:accesspoint/example-access-point--
usw2-az1--xa-s3"
        }
    ]
}
```

次の IAM アイデンティティベースのポリシーは、ディレクトリバケットのアクセスポイントを作成する s3express:CreateAccessPoint アクセス許可を付与します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Grant CreateAccessPoint.",
            "Principal": "*",
            "Action": "s3express:CreateSession",
            "s3express:CreateAccessPoint""Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

次の IAM アイデンティティベースのポリシーは、ディレクトリバケットのアクセスポイントのアクセスポイント範囲を作成する s3express:PutAccessPointScope アクセス許可を付与します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Grant PutAccessPointScope",
            "Principal": "*",
            "Action": "s3express:CreateSession",
            "s3express:CreateAccessPoint",
            "S3Express:PutAccessPointScope""Effect": "Allow",
            "Resource": "*",
        }
    ]
}
```

ディレクトリバケットのアクセスポイントを使用してバケットオペレーションへのアクセスを制御する場合は、「ディレクトリバケットのアクセスポイントのポリシーでのバケットオペレーション」を参照してください。オブジェクトオペレーションへのアクセスを制御するには、「ディレクトリバケットのアクセスポイントのポリシーでのオブジェクトオペレーション」を参照してください。ディ

レクトリバケットのアクセスポイントポリシーの設定方法の詳細については、「ディレクトリバケットのアクセスポイントを使用するための IAM ポリシーの設定」を参照してください。

Object Lambda アクセスポイントオペレーション

Amazon S3 Object Lambda を使用すると、Amazon S3 GET、LIST、HEAD リクエストに独自のコードを追加して、データがアプリケーションに返されるときにそのデータを変更および処理できます。Object Lambda アクセスポイントを介したリクエストは、他のアクセスポイントを介したリクエストと同様に行うことができます。詳細については、「S3 Object Lambda を使用したオブジェクトの変換」を参照してください。

Object Lambda アクセスポイントオペレーションのポリシーを設定する方法についての詳細は、「Object Lambda アクセスポイントの IAM ポリシーの設定」を参照してください。

マルチリージョンアクセスポイントオペレーション

マルチリージョンアクセスポイントを使用すると、複数の AWS リージョン にある S3 バケットからのリクエストをアプリケーションが実行するために使用できるグローバルエンドポイントを作成できます。マルチリージョンアクセスポイントを使用して、単一のリージョンで使用するのと同じシンプルなアーキテクチャでマルチリージョンアプリケーションを構築し、世界中のどこでもこれらのアプリケーションを実行することができます。詳細については、「マルチリージョンアクセスポイントを使用したマルチリージョントラフィックの管理」を参照してください。

マルチリージョンアクセスポイントオペレーションのポリシーを設定する方法の詳細については、「マルチリージョンアクセスポイントポリシーの例」を参照してください。

バッチジョブオペレーション

(バッチオペレーション) ジョブオペレーションは、ジョブリソースタイプで動作する S3 API オペレーションです。例えば、DescribeJob と CreateJob です。ジョブオペレーションの S3 ポリシーアクションは、バケットポリシーではなく、IAM アイデンティティベースのポリシーでのみ使用できます。また、ジョブオペレーションでは、IAM アイデンティティベースのポリシーの Resource 要素を次の例の形式の job ARN にする必要があります。

```
"Resource": "arn:aws:s3:*:123456789012:job/*"
```

次の IAM アイデンティティベースのポリシーは、*example-job* という名前の S3 バッチオペレーションジョブに対して DescribeJob API オペレーションを実行する s3:DescribeJob アクセス許可を付与します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow describing the Batch operation job example-job",
            "Effect": "Allow",
            "Action": [
            "s3:DescribeJob"
            ],
            "Resource": "arn:aws:s3:*:123456789012:job/example-job"
        }
    ]
}
```

S3 Storage Lens 設定オペレーション

S3 Storage Lens 設定オペレーションの設定方法の詳細については、「Amazon S3 ストレージレンズアクセス許可の設定」を参照してください。

アカウントオペレーション

アカウントオペレーションは、アカウントレベルで実行される S3 API オペレーションです。例えば、GetPublicAccessBlock (アカウント用) です。アカウントは、Amazon S3 で定義されるリソースタイプではありません。アカウントオペレーションの S3 ポリシーアクションは、バケットポリシーではなく、IAM アイデンティティベースのポリシーでのみ使用できます。また、アカウントオペレーションでは、IAM アイデンティティベースのポリシーの Resource 要素が "*" である必要があります。

次の IAM アイデンティティベースのポリシーは、アカウントレベルの GetPublicAccessBlock API オペレーションを実行し、アカウントレベルのパブリックアクセスブロック設定を取得するために s3:GetAccountPublicAccessBlock アクセス許可を付与します。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"Allow retrieving the account-level Public Access Block settings",
         "Effect":"Allow",
         "Action":[
            "s3:GetAccountPublicAccessBlock"
         ],
         "Resource":[
```

```
            "*"
          ]
        }
    ]
}
```

Amazon S3 のポリシーの例

- Amazon S3 のアイデンティティベースのポリシー例を確認するには、「Amazon S3 のアイデンティティベースのポリシー」を参照してください。
- Amazon S3 のリソースベースのポリシー例を確認するには、「Amazon S3 のバケットポリシー」および「汎用バケットのアクセスポイントを使用するための IAM ポリシーの設定」を参照してください。

Amazon S3 のポリシーリソース

ポリシーリソースのサポート: あり

管理者は AWS JSON ポリシーを使用して、だれが何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

`Resource` JSON ポリシー要素はアクションが適用されるオブジェクトを指定します。ステートメントには`Resource` または `NotResource` 要素を含める必要があります。ベストプラクティスとして、アマゾン リソースネーム (ARN) を使用してリソースを指定します。これは、リソースレベルの許可と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルの権限をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

```
"Resource": "*"
```

一部の Amazon S3 API アクションは複数のリソースをサポートします。例えば、`s3:GetObject` は *`example-resource-1`* と *`example-resource-2`* にアクセスするため、プリンシパルには両方のリソースにアクセスする許可が必要です。1 つのステートメントで複数のリソースを指定するには、次の例に示すように、ARN をカンマで区切ります。

```
"Resource": [
      "example-resource-1",
```

```
        "example-resource-2"
```

Amazon S3 のリソースは、バケット、オブジェクト、アクセスポイント、またはジョブです。ポリシーでは、バケット、オブジェクト、アクセスポイント、またはジョブの Amazon リソースネーム (ARN) を使用してリソースを識別します。

Amazon S3 リソースタイプとその ARN の完全なリストについては、「サービス認可リファレンス」の「Resources defined by Amazon S3」を参照してください。どのアクションで各リソースの ARN を指定できるかについては、「Amazon S3 で定義されるアクション」を参照してください。

S3 リソースタイプ別の S3 API オペレーションへのアクセス許可の詳細については、「Amazon S3 API オペレーションに必要なアクセス許可」を参照してください。

リソース ARN のワイルドカード文字

リソース ARN の一部にワイルドカードを使用できます。ARN セグメント (コロンで区切られている部分) でワイルドカード文字 (* と ?) を使用できます。アスタリスク (*) は 0 個以上の文字の任意の組み合わせを表し、疑問符 (?) は任意の 1 文字を表します。各セグメントで複数の * または ? 文字を使用できます。ただし、ワイルドカード文字はセグメントをまたぐことはできません。

- 以下の ARN は ARN の relative-ID の部分でワイルドカード文字 * を使用して、*amzn-s3-demo-bucket* バケット内のすべてのオブジェクトを識別します。

  ```
  arn:aws:s3:::amzn-s3-demo-bucket/*
  ```

- 次の ARN は * を使用して、S3 のすべてのバケットとオブジェクトを示しています。

  ```
  arn:aws:s3:::*
  ```

- 以下の ARN は、relative-ID の部分で、* および ? の両方のワイルドカード文字を使用します。この ARN により、*amzn-s3-demo-example1bucket*、*amzn-s3-demo-example2bucket*、*amzn-s3-demo-example3bucket* など、バケット内のすべてのオブジェクトを識別します。

  ```
  arn:aws:s3:::amzn-s3-demo-example?bucket/*
  ```

リソース ARN のポリシー変数

Amazon S3 の ARN では、ポリシー変数を使用することもできます。あらかじめ定義されているこれらの変数は、ポリシーの評価時に対応する値で置き換えられます。例えば、バケットをフォルダ

のコレクションとして構成し、ユーザーごとに別のフォルダを使用するとします。フォルダ名はユーザー名と同じです。各ユーザーに自分のフォルダに対するアクセス許可を付与するには、リソース ARN で以下のようにポリシー変数を指定します。

```
arn:aws:s3:::bucket_name/developers/${aws:username}/
```

実行時にポリシーが評価されると、リソース ARN の変数 ${aws:username} には、リクエストを行うユーザーのユーザー名が挿入されます。

Amazon S3 のポリシーの例

- Amazon S3 のアイデンティティベースのポリシー例を確認するには、「Amazon S3 のアイデンティティベースのポリシー」を参照してください。
- Amazon S3 のリソースベースのポリシー例を確認するには、「Amazon S3 のバケットポリシー」および「汎用バケットのアクセスポイントを使用するための IAM ポリシーの設定」を参照してください。

Amazon S3 のポリシー条件キー

サービス固有のポリシー条件キーのサポート: あり

管理者は AWS JSON ポリシーを使用して、だれが何にアクセスできるかを指定できます。つまり、どのプリンシパルがどんなリソースにどんな条件でアクションを実行できるかということです。

Condition 要素 (または Condition ブロック) を使用すると、ステートメントが有効な条件を指定できます。Condition 要素はオプションです。イコールや未満などの 条件演算子 を使用して条件式を作成して、ポリシーの条件とリクエスト内の値を一致させることができます。

1 つのステートメントに複数の Condition 要素を指定する場合、または 1 つの Condition 要素に複数のキーを指定する場合、AWS では AND 論理演算子を使用してそれらを評価します。単一の条件キーに複数の値を指定する場合、AWS では OR 論理演算子を使用して条件を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば IAM ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与することができます。詳細については、「IAM ユーザーガイド」の「IAM ポリシーの要素: 変数およびタグ」を参照してください。

AWS はグローバル条件キーとサービス固有の条件キーをサポートしています。すべての AWS グローバル条件キーを確認するには、IAM ユーザーガイドのAWS グローバル条件コンテキストキーを参照してください。

各 Amazon S3 条件キーは、その条件を設定できる API でサポートされている同じ名前のリクエストヘッダーに対応します。Amazon S3 固有の条件キーでは、同じ名前のリクエストヘッダーの動作が指定されます。例えば、アクセス許可
`s3:GetObjectVersion`
に対して条件付きのアクセス許可を付与する条件キー `s3:VersionId` は、GET Object リクエストで設定する `versionId` クエリパラメータの動作を定義します。

Amazon S3 の条件キーのリストを確認するには、「サービス認可リファレンス」の「Condition keys for Amazon S3」を参照してください。https://docs.aws.amazon.com/service-authorization/latest/reference/list_amazons3.html#amazons3-policy-keysどのアクションおよびリソースで条件キーを使用できるかについては、「Amazon S3 で定義されるアクション」を参照してください。

例: オブジェクトのアップロードを特定のストレージクラスのオブジェクトに制限する

アカウント ID *123456789012* で表されているアカウント A がバケットを所有しているとします。アカウント A の管理者は、アカウント A のユーザーである *Dave* に対して、STANDARD_IA ストレージクラスにオブジェクトが保存されている場合にのみ *Dave* がバケットにオブジェクトをロードすることを許可するとします。オブジェクトのアップロードを特定のストレージクラスに制限するために、アカウント A の管理者は、次のバケットポリシーの例に示すように `s3:x-amz-storage-class` 条件キーを使用できます。

```
{
                "Version": "2012-10-17",
                "Statement": [
                  {
                    "Sid": "statement1",
                    "Effect": "Allow",
                    "Principal": {
                      "AWS": "arn:aws:iam::123456789012:user/Dave"
                    },
                    "Action": "s3:PutObject",
                    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
                    "Condition": {
                      "StringEquals": {
                        "s3:x-amz-storage-class": [
                          "STANDARD_IA"
                        ]
```

```
                    }
                }
            }
        ]
    }
```

この例で、Condition ブロックは指定されたキーと値のペア "s3:x-amz-acl":["public-read"] に適用される StringEquals 条件を指定します。条件の表現に使用できる、事前に定義された一連のキーがあります。この例では、s3:x-amz-acl 条件キーを使用しています。この条件では、public-read の値が指定された x-amz-acl ヘッダーをすべての PutObject リクエストに含めることがユーザーに求められます。

Amazon S3 のポリシーの例

- Amazon S3 のアイデンティティベースのポリシー例を確認するには、「Amazon S3 のアイデンティティベースのポリシー」を参照してください。
- Amazon S3 のリソースベースのポリシー例を確認するには、「Amazon S3 のバケットポリシー」および「汎用バケットのアクセスポイントを使用するための IAM ポリシーの設定」を参照してください。

Amazon S3 での ACL

ACL のサポート: あり

Amazon S3 のアクセスコントロールリスト (ACL) は、どの AWS アカウント がリソースへのアクセス許可を持つかをコントロールします。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

> **Important**
>
> Amazon S3 の最新のユースケースの大部分では ACL を使用する必要がなくなっています。

Amazon S3 での ACL を使用したアクセスコントロールについては、「ACL によるアクセス管理」を参照してください。

Amazon S3 での ABAC

ABAC (ポリシー内のタグ) のサポート: 一部

属性ベースのアクセス制御 (ABAC) は、属性に基づいてアクセス許可を定義する認可戦略です。AWS では、属性はタグと呼ばれます。タグは、IAM エンティティ (ユーザーまたはロール)、および多数の AWS リソースにアタッチできます。エンティティとリソースのタグ付けは、ABAC の最初の手順です。その後、プリンシパルのタグがアクセスしようとしているリソースのタグと一致した場合にオペレーションを許可するように ABAC ポリシーをします。

ABAC は、急成長する環境やポリシー管理が煩雑になる状況で役立ちます。

タグに基づいてアクセスを管理するには、`aws:ResourceTag/key-name`、`aws:RequestTag/key-name`、または `aws:TagKeys` の条件キーを使用して、ポリシーの条件要素でタグ情報を提供します。

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値はありです。サービスが一部のリソースタイプに対してのみ 3 つの条件キーのすべてをサポートする場合、値は「部分的」になります。

ABAC の詳細については、「IAM ユーザーガイド」の「ABAC 認可でアクセス許可を定義する」を参照してください。ABAC をセットアップする手順を説明するチュートリアルについては、「IAM ユーザーガイド」の「属性ベースのアクセスコントロール (ABAC) を使用する」を参照してください。

タグに基づいて S3 バッチオペレーションジョブへのアクセスを制限するためのアイデンティティベースのポリシー例を確認するには、「ジョブタグを使用したバッチオペレーションのアクセス許可の制御」を参照してください。

ABAC とオブジェクトタグ

ABAC ポリシーでは、オブジェクトは `aws:` タグの代わりに `s3:` タグを使用します。オブジェクトタグに基づいてオブジェクトへのアクセスをコントロールするには、以下のタグを使用してポリシーの Condition 要素でタグ情報を指定します。

- `s3:ExistingObjectTag/tag-key`
- `s3:RequestObjectTagKeys`
- `s3:RequestObjectTag/tag-key`

アクセス許可ポリシーの例など、オブジェクトタグを使用したアクセスコントロールについては、「タグ付けとアクセスコントロールポリシー」を参照してください。

Amazon S3 での一時的な認証情報の使用

一時的な認証情報のサポート: あり

AWS のサービスには、一時的な認証情報を使用してサインインしても機能しないものがあります。一時的な認証情報を利用できる AWS のサービス を含めた詳細情報については、「IAM ユーザーガイド」の「IAM と連携する AWS のサービス」を参照してください。

ユーザー名とパスワード以外の方法で AWS Management Console にサインインする場合は、一時的な認証情報を使用していることになります。例えば、会社のシングルサインオン (SSO) リンクを使用して AWS にアクセスすると、そのプロセスは自動的に一時認証情報を作成します。また、ユーザーとしてコンソールにサインインしてからロールを切り替える場合も、一時的な認証情報が自動的に作成されます。ロールの切り替えに関する詳細については、「IAM ユーザーガイド」の「ユーザーから IAM ロールに切り替える (コンソール)」を参照してください。

一時認証情報は、AWS CLI または AWS API を使用して手動で作成できます。作成後、一時認証情報を使用して AWS にアクセスできるようになります。AWSは、長期的なアクセスキーを使用する代わりに、一時認証情報を動的に生成することをお勧めします。詳細については、「IAM の一時的セキュリティ認証情報」を参照してください。

Amazon S3 の転送アクセスセッション

転送アクセスセッション (FAS) のサポート: あり

IAM ユーザーまたはロールを使用して AWS でアクションを実行するユーザーは、プリンシパルとみなされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS は、AWS のサービスを呼び出すプリンシパルの権限を、AWS のサービスのリクエストと合わせて使用し、ダウンストリームのサービスに対してリクエストを行います。FAS リクエストは、サービスが、完了するために他の AWS のサービス またはリソースとのやりとりを必要とするリクエストを受け取ったときにのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

- SSE-KMS を使用してオブジェクトを暗号化した場合、Amazon S3 は FAS を使用してオブジェクトを復号化するための呼び出しを AWS KMS に対して行います。詳細については、「AWS KMS キーによるサーバー側の暗号化 (SSE-KMS) の使用」を参照してください。
- S3 Access Grants も FAS を使用します。特定の ID の S3 データへのアクセス許可を作成すると、被付与者は S3 Access Grants に一時的な認証情報を要求します。S3 Access Grants は、AWS STS からリクエスタの一時的な認証情報を取得し、その認証情報をリクエスタに提供し

ます。詳細については、「S3 Access Grants を介して Amazon S3 データへのアクセスをリクエストする」を参照してください。

Amazon S3 のサービスロール

サービスロールのサポート: あり

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「IAM ユーザーガイド」の「AWS のサービス に許可を委任するロールを作成する」を参照してください。

> **Warning**
>
> サービスロールのアクセス許可を変更すると、Amazon S3 が機能しなくなる可能性があります。サービスロールは、Amazon S3 で指示された場合のみ編集してください。

Amazon S3 のサービスリンクロール

サービスにリンクされたロールをサポート： 一部

サービスにリンクされたロールは、AWS のサービスにリンクされているサービスロールの一種です。サービスがロールを引き受け、ユーザーに代わってアクションを実行できるようになります。サービスにリンクされたロールは、AWS アカウント に表示され、サービスによって所有されます。IAM 管理者は、サービスリンクロールのアクセス許可を表示できますが、編集することはできません。

Amazon S3 では、Amazon S3 Storage Lens 用のサービスにリンクされたロールをサポートしています。Amazon S3 でのサービスリンクロールの作成または管理の詳細については、「Amazon S3 ストレージレンズでのサービスにリンクされたロールの使用」を参照してください。

プリンシパルとしての Amazon S3 サービス

ポリシー内のサービス名	S3 機能	詳細情報
s3.amazonaws.com	S3 レプリケーション	ライブレプリケーションの設定の概要

ポリシー内のサービス名	S3 機能	詳細情報
s3.amazonaws.com	S3 イベント通知	Amazon S3 イベント通知
s3.amazonaws.com	S3 インベントリ	S3 インベントリを使用したデータのカタログ化と分析
access-grants.s3.amazonaws.com	S3 Access Grants	ロケーションを登録する
batchoperations.s3.amazonaws.com	S3 バッチオペレーション	バッチオペレーションに対するアクセス許可の付与
logging.s3.amazonaws.com	S3 サーバーアクセスのログ記録	Amazon S3 サーバーアクセスログを有効にします。
storage-lens.s3.amazonaws.com	S3 Storage Lens	データエクスポートで Amazon S3 Storage Lens のメトリクスを確認する

Amazon S3 がリクエストを許可する仕組み

Amazon S3 は、バケットまたはオブジェクトオペレーションなどのリクエストを受け取ると、まずリクエスタに必要なアクセス許可があることを確認します。Amazon S3 は、関連するすべてのアクセスポリシー、ユーザーポリシー、およびリソースベースのポリシー (バケットポリシー、バケットアクセスコントロールリスト (ACL)、オブジェクト ACL) を評価して、リクエストを許可するかどうかを決めます。

> **Note**
>
> Amazon S3 アクセス許可チェックで有効な許可が見つからなかった場合は、アクセス拒否 (403 Forbidden) アクセス許可拒否エラーが返されます。詳細については、「Amazon S3 でのアクセス拒否 (403 Forbidden) エラーのトラブルシューティング」を参照してください。

Amazon S3 は、リクエストを受け取ると、リクエスタが特定のオペレーションを実行するアクセス許可があるかどうかを確認するため、次の操作を順に実行します。

1. 関連するすべてのアクセスポリシー (ユーザーポリシー、バケットポリシー、および ACL) を実行時に評価ターゲットのポリシーのセットに変換します。
2. 作成したポリシーのセットを次の手順で評価します。各ステップで、Amazon S3 は、コンテキストの権限に基づいて、ポリシーのサブセットを特定のコンテキストで評価します。
   a. ユーザーコンテキスト – ユーザーコンテキストでは、ユーザーが属する親アカウントにコンテキストの権限があります。

      Amazon S3 は、親アカウントが所有するポリシーのサブセットを評価します。このサブセットには、親がユーザーにアタッチするユーザーポリシーが含まれています。親がリクエスト内のリソース (バケットまたはオブジェクト) も所有している場合、Amazon S3 は、対応するリソースポリシー (バケットポリシー、バケット ACL、オブジェクト ACL) も同時に評価します。

      ユーザーは、オペレーションを実行するための親アカウントからのアクセス許可を持つ必要があります。

      このステップは、リクエストが AWS アカウント内のユーザーによって行われた場合にのみ適用されます。リクエストが AWS アカウントのルートユーザー認証情報を使用して行われている場合、Amazon S3 はこのステップをスキップします。

b. バケットコンテキスト – バケットコンテキストでは、Amazon S3 はバケットを所有する AWS アカウント が所有するポリシーを評価します。

   バケットオペレーションに対するリクエストの場合、リクエスタはバケット所有者からのアクセス許可を持つ必要があります。リクエストがオブジェクトをターゲットにしている場合、Amazon S3 は、バケット所有者が所有するすべてのポリシーを評価して、バケット所有者がオブジェクトへのアクセスを明示的に拒否していないかどうかを確認します。明示的な拒否セットが存在する場合、Amazon S3 はリクエストを許可しません。

c. オブジェクトコンテキスト – オブジェクトに対するリクエストの場合、Amazon S3 はオブジェクトの所有者が所有するポリシーのサブセットを評価します。

Amazon S3 がリクエストを承認する方法を示すいくつかのシナリオの例を次に示します。

Example - リクエスタが IAM プリンシパルの場合

リクエスタが IAM プリンシパルの場合、Amazon S3 は、オペレーションを実行するために必要な許可が、プリンシパルが属する親 AWS アカウントよりプリンシパルに付与されているかどうかを判断する必要があります。さらに、リクエストがバケットオペレーション (バケット内容のリストを取得するリクエストなど) の場合、Amazon S3 は、オペレーションを実行するためのアクセス許可をバケット所有者がリクエスタに付与していることを確認する必要があります。IAM プリンシパルがリソースに対して特定のオペレーションを実行するには、そのプリンシパルが属する親 AWS アカウントと、リソースを所有する AWS アカウントの両方からの許可が必要です。

Example - リクエスタが IAM プリンシパルの場合 - リクエストが、バケット所有者が所有していないオブジェクトに対するオペレーションに関連している場合。

バケット所有者が所有していないオブジェクトに対するオペレーションのリクエストの場合は、リクエスタがオブジェクトの所有者からのアクセス許可を持つことの確認に加えて、Amazon S3 はバケットポリシーもチェックして、バケット所有者がオブジェクトに対する明示的な拒否を設定していないことを確認する必要があります。バケット所有者 (請求の支払者) は、オブジェクトの所有者にかかわらず、バケット内のオブジェクトへのアクセスを明示的に拒否できます。また、バケット所有者は、バケット内のすべてのオブジェクトを削除できます。

デフォルトでは、別の AWS アカウントがオブジェクトを S3 汎用バケットにアップロードすると、そのアカウント (オブジェクトライター) がオブジェクトを所有し、そのオブジェクトにアクセスでき、アクセスコントロールリスト (ACL) を介して他のユーザーにそのオブジェクトへのアクセスを許可できます。オブジェクト所有者を使用してこのデフォルト動作を変更することで、ACL を無効

にして、汎用バケット内のすべてのオブジェクトをバケット所有者として自動的に所有できます。その結果、データのアクセスコントロールは、IAM ユーザーポリシー、S3 バケットポリシー、仮想プライベートクラウド (VPC) エンドポイントポリシー、AWS Organizations サービスコントロールポリシー (SCP) などのポリシーに基づいています。詳細については、「オブジェクトの所有権の制御とバケットの ACL の無効化。」を参照してください。

Amazon S3 がアクセスポリシーを評価してバケットオペレーションおよびオブジェクトオペレーションのリクエストを承認または拒否する仕組みについて詳しくは、以下のトピックを参照してください。

トピック

- Amazon S3 がバケットオペレーションのリクエストを承認する仕組み
- Amazon S3 がオブジェクトオペレーションのリクエストを許可する仕組み

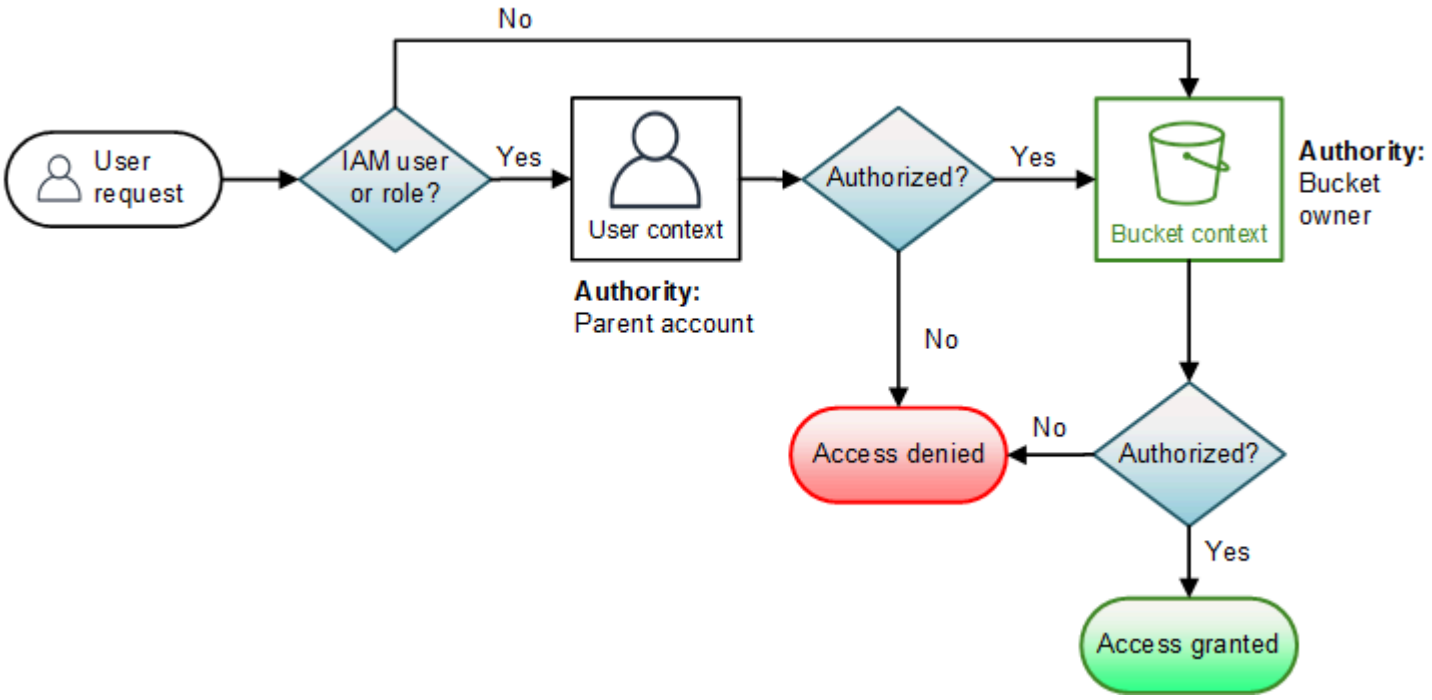
Amazon S3 がバケットオペレーションのリクエストを承認する仕組み

Amazon S3 は、バケットオペレーションのリクエストを受け取ると、関連するすべてのアクセス許可を、実行時に評価する一連のポリシーに変換します。関連するアクセス許可には、リソースベースのアクセス許可 (バケットポリシーやバケットアクセスコントロールリストなど) とユーザーポリシー (リクエストが IAM プリンシパルからの場合) が含まれます。Amazon S3 はその後、作成したポリシーのセットを特定のコンテキスト (ユーザーコンテキストまたはバケットコンテキスト) に従って、一連の手順で評価します。

1. ユーザーコンテキスト – リクエスタが IAM プリンシパルの場合、そのプリンシパルは親 AWS アカウント からアクセス許可を付与されている必要があります。このステップで、Amazon S3 は、親アカウント (コンテキストの権限とも呼ばれる) が所有するポリシーのサブセットを評価します。このポリシーのサブセットには、親アカウントがプリンシパルにアタッチするユーザーポリシーが含まれます。親がリクエスト内のリソース(この場合はバケット)も所有している場合、Amazon S3 は、対応するリソースポリシー(バケットポリシーおよびバケット ACL)も同時に評価します。バケットオペレーションのリクエストが出されるたびに、サーバーアクセスログはリクエスタの正規 ID を記録します。詳細については、サーバーアクセスログによるリクエストのログ記録 を参照してください。
2. バケットコンテキスト – リクエスタは、バケット所有者から特定のバケットオペレーションを実行するためのアクセス許可を付与されている必要があります。このステップで、Amazon S3 は、バケットを所有する AWS アカウントが所有するポリシーのサブセットを評価します。

バケット所有者は、バケットポリシーまたはバケット ACL を使用してアクセス許可を付与できます。バケットを所有している AWS アカウント が IAM プリンシパルの親アカウントでもある場合は、ユーザーポリシーでバケットの許可を設定できます。

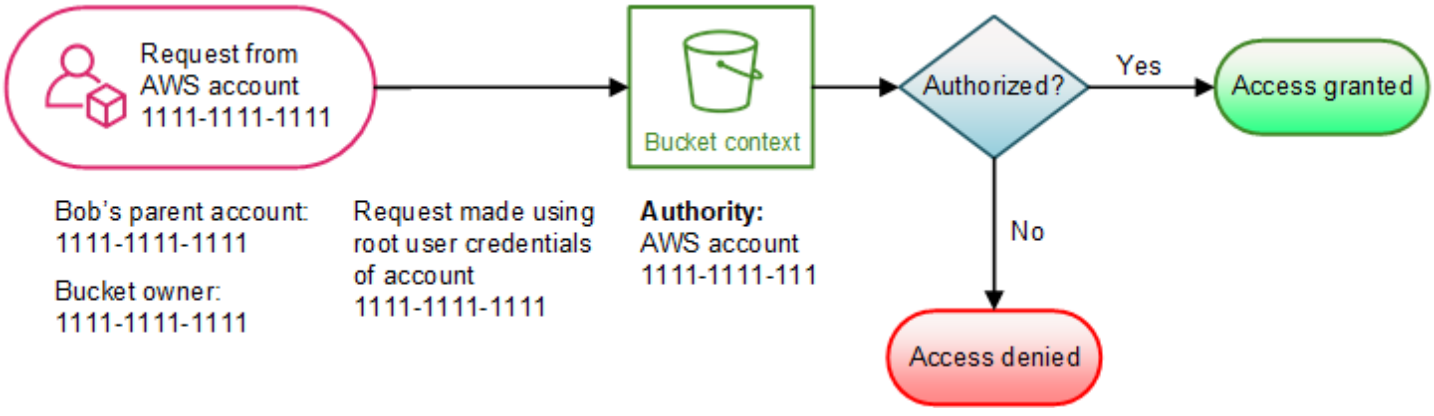
次に示すのは、バケットオペレーションのコンテキストベースの評価を説明するための図です。



次の例は、評価ロジックを示します。

例 1: バケット所有者がリクエストするバケットオペレーション

この例では、バケット所有者が AWS アカウントのルート認証情報を使用してバケットオペレーションへのリクエストを送信します。

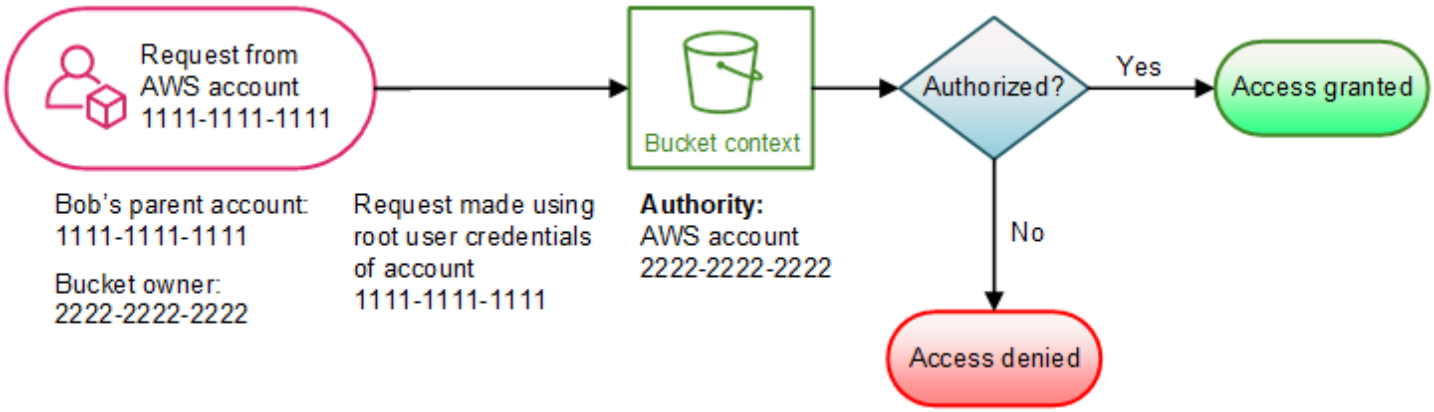


Amazon S3 はコンテキストの評価を次のように実行します。

1. リクエストは AWS アカウントのルートユーザー認証情報を使用して行われるため、ユーザーコンテキストは評価されません。
2. バケットコンテキストでは、Amazon S3 はバケットポリシーを調べて、リクエスタがオペレーションを実行するアクセス許可を持つかどうかを判定します。Amazon S3 はリクエストを許可します。

例 2: バケット所有者でない AWS アカウントがリクエストしたバケットオペレーション

この例では、AWS アカウント 2222-2222-2222 が所有するバケットオペレーションで AWS アカウント 1111-1111-1111 のルートユーザー認証情報を使用してリクエストが行われます。このリクエストに IAM ユーザーは関与していません。

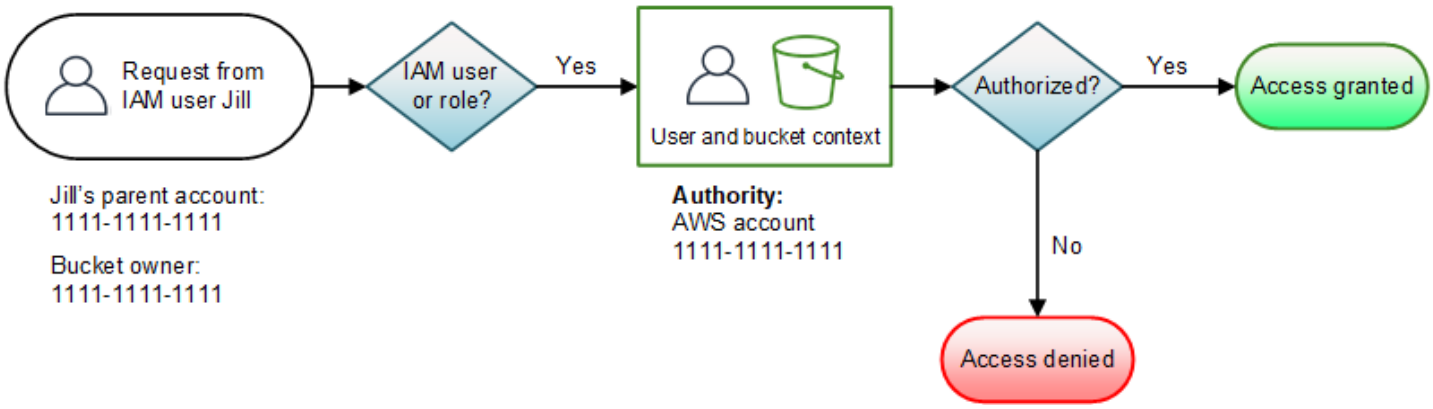


この例では、Amazon S3 は次のようにコンテキストを評価します。

1. リクエストは AWS アカウントのルートユーザー認証情報を使用して行われるため、ユーザーコンテキストは評価されません。
2. バケットコンテキストでは、Amazon S3 はバケットポリシーを調べます。バケット所有者 (AWS アカウント 2222-2222-2222) が、リクエストされたオペレーションを AWS アカウント 1111-1111-1111 に許可していない場合は、Amazon S3 はリクエストを拒否します。それ以外の場合、Amazon S3 はリクエストを許可し、オペレーションを実行します。

例 3: 親 AWS アカウントがバケット所有者でもある IAM プリンシパルがリクエストしたバケットオペレーション

この例では、リクエストを送信したユーザーが AWS アカウント 1111-1111-1111 の IAM ユーザー Jill であり、このアカウントがバケット所有者でもあります。



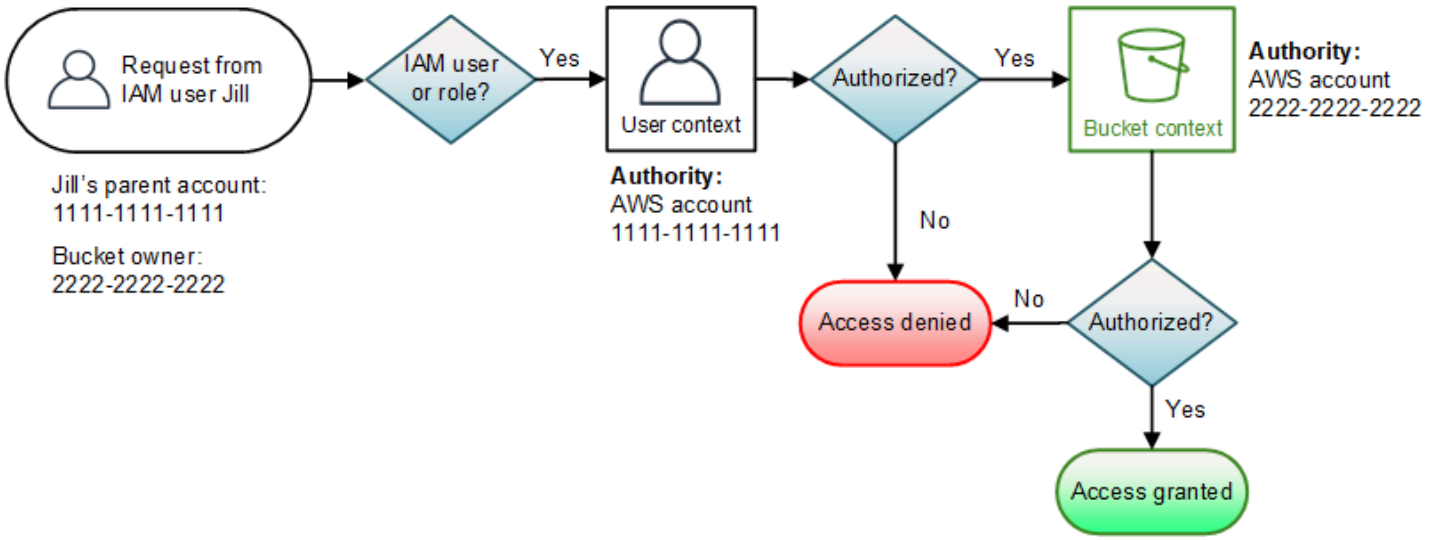
Amazon S3 は次のコンテキスト評価を実行します。

1. リクエストは IAM プリンシパルからであるため、ユーザーコンテキストで、Amazon S3 は親 AWS アカウントに属するすべてのポリシーを評価して、Jill がオペレーションを実行する許可を持っているかどうかを判定します。

   この例では、プリンシパルが属する親 AWS アカウント 1111-1111-1111 は、バケット所有者でもあります。その結果、Amazon S3 は、ユーザーポリシーに加えて、バケットポリシーとバケット ACL も同じコンテキストで評価します。これらが同じアカウントに属するからです。
2. Amazon S3 はバケットポリシーとバケット ACL をユーザーコンテキストの一部として評価したので、バケットコンテキストは評価しません。

例 4: 親 AWS アカウントがバケット所有者でない IAM プリンシパルがリクエストしたバケットオペレーション

この例では、リクエストを送信したのが 1111-1111-1111 を親 AWS アカウント とする IAM ユーザー Jill であり、バケット所有者は別の AWS アカウント 2222-2222-2222 です。



Jill には、親 AWS アカウントとバケット所有者の両方からの許可が必要です。Amazon S3 は次のようにコンテキストを評価します。

1. リクエストは IAM プリンシパルからであるため、Amazon S3 は、アカウントが作成したポリシーを参照してユーザーコンテキストを評価し、Jill に必要なアクセス許可があることを検証します。Jill にアクセス許可がある場合、Amazon S3 はバケットコンテキストの評価に進みます。Jill にアクセス許可がない場合、Amazon S3 はリクエストを拒否します。
2. バケットコンテキストでは、Amazon S3 はバケット所有者の 2222–2222–2222 がリクエストされたオペレーションを実行するアクセス許可を Jill (またはその親 AWS アカウント) に付与していることを確認します。アクセス許可がある場合、Amazon S3 はリクエストを許可し、オペレーションを実行します。アクセス許可がない場合、Amazon S3 はリクエストを拒否します。

Amazon S3 がオブジェクトオペレーションのリクエストを許可する仕組み

Amazon S3 は、オブジェクトオペレーションのリクエストを受け取ると、関連するすべての許可 、リソースベースの許可 (オブジェクトアクセスコントロールリスト (ACL)、バケットポリシー、バケット (ACL) と IAM ユーザーポリシー) を実行時に評価する一連のポリシーに変換します。その後、作成したポリシーのセットを一連の手順で評価します。各ステップでは、ポリシーのサブセットが、ユーザーコンテキスト、バケットコンテキスト、オブジェクトコンテキストの 3 つの固有のコンテキストで評価されます。

1. ユーザーコンテキスト – リクエスタが IAM プリンシパルの場合、そのプリンシパルは親 AWS アカウント からアクセス許可を付与されている必要があります。このステップで、Amazon S3 は、親アカウント (コンテキストの権限とも呼ばれる) が所有するポリシーのサブセットを評価します。このポリシーのサブセットには、親がプリンシパルにアタッチするユーザーポリシー

が含まれます。親がリクエスト内のリソース (バケットまたはオブジェクト) も所有している場合、Amazon S3 は、対応するリソースポリシー (バケットポリシー、バケット ACL、オブジェクト ACL) も同時に評価します。

> **Note**
>
> 親 AWS アカウントがリソース (バケットまたはオブジェクト) を所有している場合、親アカウントは、ユーザーポリシーまたはリソースポリシーを使用して、リソースの許可を IAM プリンシパルに付与できます。

2. バケットコンテキスト – このコンテキストでは、Amazon S3 はバケットを所有する AWS アカウント が所有するポリシーを評価します。

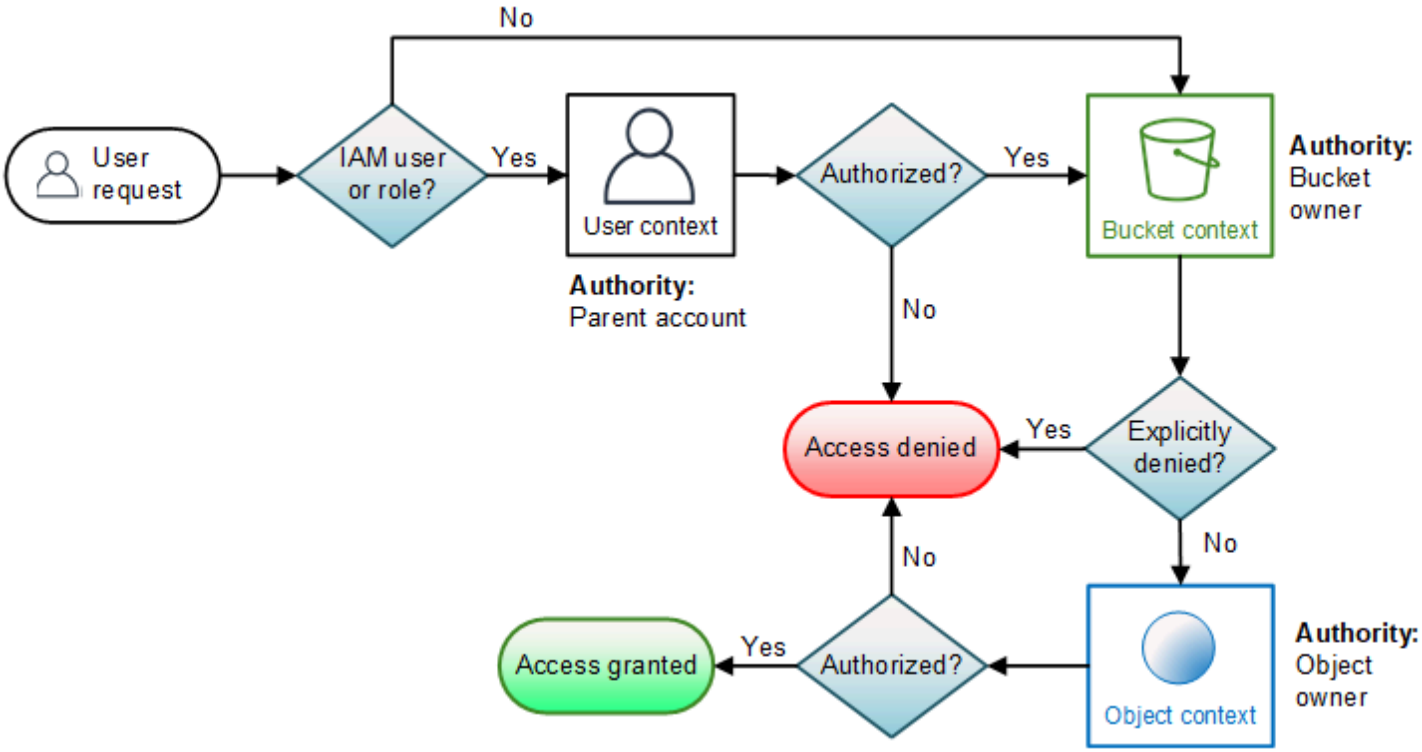
   リクエスト内のオブジェクトを所有する AWS アカウント がバケット所有者と同じでない場合、Amazon S3 はポリシーをチェックして、バケット所有者がオブジェクトへのアクセスを明示的に拒否しているかどうかをチェックします。オブジェクトに対する明示的な拒否セットが存在する場合、Amazon S3 はリクエストを許可しません。

3. オブジェクトコンテキスト – リクエスタは、オブジェクト所有者から特定のオブジェクトオペレーションを実行するためのアクセス許可を付与されている必要があります。このステップで、Amazon S3 はオブジェクト ACL を評価します。

> **Note**
>
> バケットとオブジェクトの所有者が同じ場合、オブジェクトへのアクセスは、バケットコンテキストで評価されるバケットポリシーで許可することができます。所有者が異なる場合、オブジェクトの所有者はオブジェクト ACL を使用してアクセス許可を付与する必要があります。オブジェクトを所有する AWS アカウントが IAM プリンシパルの親アカウントでもある場合は、ユーザーコンテキストで評価されるユーザーポリシーでオブジェクトのアクセス許可を設定できます。これらのアクセスポリシーの各オプションの詳細については、チュートリアル: ポリシーを使用した Amazon S3 リソースへのアクセスの管理 を参照してください。
>
> バケット所有者がバケット内のすべてのオブジェクトを所有し、バケットポリシーまたは IAM ベースのポリシーを使用してこれらのオブジェクトへのアクセスを管理する場合は、オブジェクト所有権にバケット所有者強制設定を適用できます。この設定では、バケット所有者として、バケット内のすべてのオブジェクトを自動的に所有し、完全に制御できます。バケットとオブジェクト ACL は編集できず、アクセスと見なされなくなります。詳

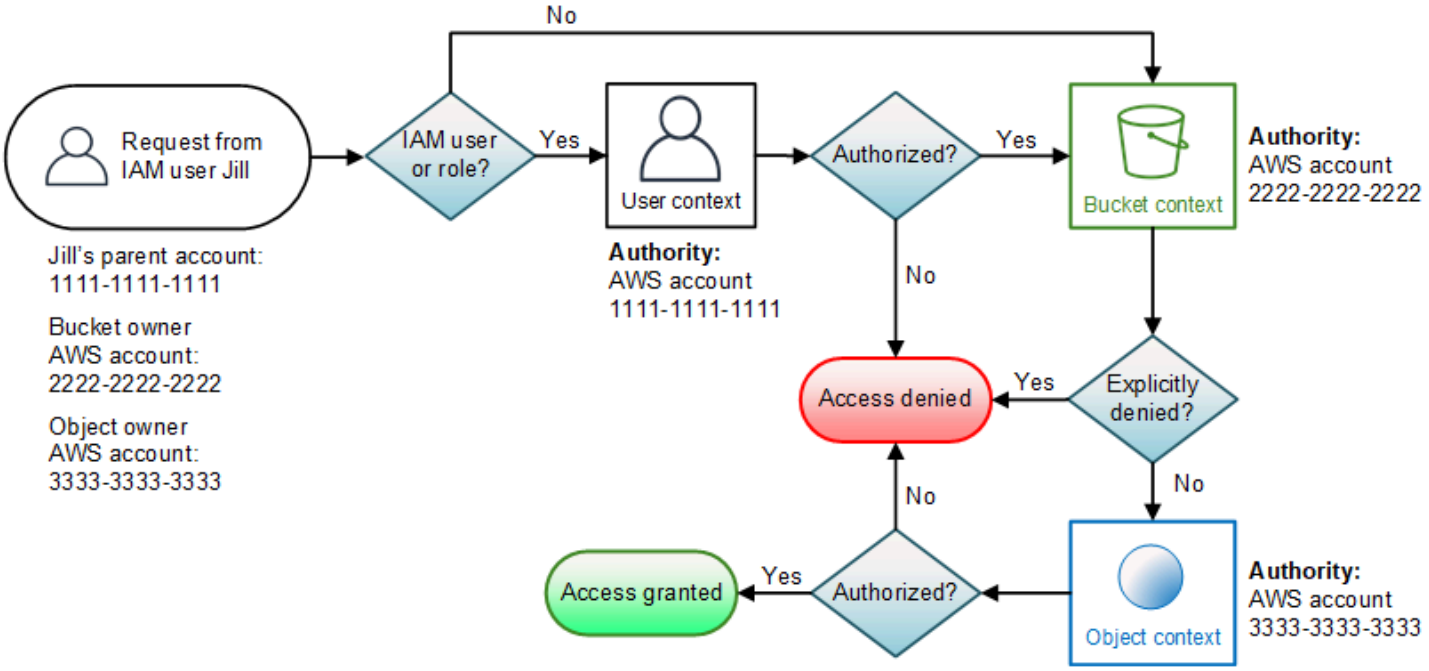
細については、オブジェクトの所有権の制御とバケットの ACL の無効化。 を参照してください。

次に示すのは、オブジェクトオペレーションに対するコンテキストベースの評価の説明です。



オブジェクトオペレーションのリクエストの例

この例では、親 AWS アカウント が 1111-1111-1111 である IAM ユーザー Jill が、GetObject 2222-2222-2222 が所有するバケットにある、AWS アカウント 3333-3333-3333 が所有するオブジェクトに対するオブジェクトオペレーションのリクエスト (AWS アカウント など) を送信します。



Jill には、親 AWS アカウント、バケット所有者、およびオブジェクト所有者からの許可が必要です。Amazon S3 は次のようにコンテキストを評価します。

1. リクエストは IAM プリンシパルからであるため、Amazon S3 は、ユーザーコンテキストを評価して、親 AWS アカウント 1111-1111-1111 がリクエストされたオペレーションを実行するアクセス許可を Jill に付与していることを検証します。アクセス許可がある場合、Amazon S3 はバケットコンテキストを評価します。アクセス許可がない場合、Amazon S3 はリクエストを拒否します。
2. バケットコンテキストでは、バケット所有者の AWS アカウント 2222-2222-2222 がコンテキストの権限です。Amazon S3 は、バケットポリシーを評価して、バケット所有者がオブジェクトへのアクセスを Jill に対して明示的に拒否しているかどうかを判定します。
3. オブジェクトコンテキストでは、コンテキストの権限はオブジェクト所有者の AWS アカウント 3333-3333-3333 です。Amazon S3 は、オブジェクト ACL を評価して、Jill がオブジェクトにアクセスするアクセス許可を持つかどうかを判定します。アクセス許可がある場合、Amazon S3 はリクエストを許可します。

Amazon S3 API オペレーションに必要なアクセス許可

> **Note**
>
> このページでは、汎用バケットの Amazon S3 ポリシーアクションについて説明します。ディレクトリバケットの Amazon S3 ポリシーアクションの詳細については、「ディレクトリバケットのアクション」を参照してください。

S3 API オペレーションを実行するには、適切なアクセス許可が必要です。このページでは、S3 API オペレーションを必要なアクセス許可にマッピングします。S3 API オペレーションを実行するアクセス許可を付与するには、有効なポリシー (S3 バケットポリシーや IAM アイデンティティベースのポリシーなど) を作成し、ポリシーの `Action` 要素で対応するアクションを指定する必要があります。これらのアクションはポリシーアクションと呼ばれます。すべての S3 API オペレーションが 1 つのアクセス許可 (1 つのポリシーアクション) で表されるわけではなく、さまざまな API オペレーションには複数のアクセス許可 (複数のポリシーアクション) が必要です。

ポリシーを作成するときは、対応する Amazon S3 ポリシーアクションに必要な正しいリソースタイプに基づいて、`Resource` 要素を指定する必要があります。このページでは、アクセス許可をリソースタイプ別に S3 API オペレーションに分類します。リソースタイプの詳細については、「サービス認可リファレンス」の「Amazon S3 で定義されるリソースタイプ」を参照してください。Amazon S3 ポリシーアクションの完全なリストとポリシーで使用する条件キーについては、「サービス認可リファレンス」の「Actions, resources, and condition keys for Amazon S3」を参照してください。Amazon S3 API オペレーションの完全なリストについては、「Amazon Simple Storage Service API リファレンス」の「Amazon S3 API アクション」を参照してください。

S3 で HTTP `403 Forbidden` エラーに対処する方法の詳細については、「Amazon S3 でのアクセス拒否 (403 Forbidden) エラーのトラブルシューティング」を参照してください。S3 で使用する IAM 機能の詳細については、「Amazon S3 での IAM の機能」を参照してください。S3 セキュリティのベストプラクティスに関する詳細は、「Amazon S3 のセキュリティのベストプラクティス」を参照してください。

トピック

- バケットオペレーションとアクセス許可
- オブジェクトオペレーションとアクセス許可
- 汎用バケットオペレーションのアクセスポイントとアクセス許可
- Object Lambda アクセスポイントのオペレーションとアクセス許可

- マルチリージョンアクセスポイントとアクセス許可
- バッチジョブのオペレーションとアクセス許可
- S3 ストレージレンズ設定オペレーションとアクセス許可
- S3 ストレージレンズグループのオペレーションとアクセス許可
- S3 Access Grants インスタンスのオペレーションとアクセス許可
- S3 Access Grants ロケーションのオペレーションとアクセス許可
- S3 Access Grants の許可付与オペレーションとアクセス許可
- API オペレーションとアクセス許可

バケットオペレーションとアクセス許可

バケットオペレーションは、バケットリソースタイプで動作する S3 API オペレーションです。バケットポリシーまたは IAM アイデンティティベースのポリシーでバケットオペレーションに S3 ポリシーアクションを指定する必要があります。

ポリシーでは、`Resource` 要素はバケットの Amazon リソースネーム (ARN) である必要があります。`Resource` 要素形式とポリシーの例の詳細については、「バケットオペレーション」を参照してください。

> **Note**
>
> アクセスポイントポリシーのバケットオペレーションにアクセス許可を付与する場合は、次の点に注意してください。
>
> - アクセスポイントポリシーのバケットオペレーションで付与されるアクセス許可は、基になるバケットで同じアクセス許可が許される場合にのみ有効です。アクセスポイントを使用する場合は、バケットからアクセスポイントにアクセスコントロールを委任するか、アクセスポイントポリシーで同じアクセス許可を基礎となるバケットのポリシーに追加する必要があります。
> - バケットオペレーションにアクセス許可を付与するアクセスポイントポリシーでは、`Resource` 要素は `accesspoint` ARN である必要があります。`Resource` 要素形式とポリシーの例の詳細については、「汎用バケットのアクセスポイントのポリシーでのバケットオペレーション」を参照してください。アクセスポイントポリシーの詳細については、「汎用バケットのアクセスポイントを使用するための IAM ポリシーの設定」を参照してください。

- すべてのバケットオペレーションがアクセスポイントでサポートされているわけではありません。詳細については、「汎用バケットのアクセスポイントと S3 オペレーションとの互換性」を参照してください。

以下は、バケットオペレーションと必要なポリシーアクションのマッピングです。

API オペレーション	ポリシーアクション	ポリシーアクションの説明
CreateBucket	(必須) s3:CreateBucket	新しい S3 バケットを作成するのに必要です。
	(条件付きで必須) s3:PutBucketAcl	アクセスコントロールリスト (ACL) を使用して、CreateBucket リクエスト時にバケットに対してアクセス許可を指定する場合に必要です。
	(条件付きで必須) s3:PutBucketObjectLockConfiguration 、s3:PutBucketVersioning	バケットの作成時に Object Lock を有効にする場合は必須です。
	(条件付きで必須) s3:PutBucketOwnershipControls	バケットの作成時に S3 オブジェクトの所有権を指定する場合は必須です。
CreateBucketMetadataTableConfiguration	(必須) s3:CreateBucketMetadataTableConfiguration 、s3tables:CreateNamespace 、s3tables:CreateTable 、s3tables:	汎用バケットでメタデータテーブル設定を作成するために必要です。 メタデータテーブル設定で指定されたテーブルバケットにメタデータテーブルを作成するには、指定された s3tables アクセス許可が必要です。

API オペレーション	ポリシーアクション	ポリシーアクションの説明
	`GetTable` 、`s3tables:PutTablePolicy`	メタデータテーブルをクエリできるようにテーブルバケットを AWS 分析サービスと統合する場合は、追加のアクセス許可が必要です。詳細については、「Integrating Amazon S3 Tables with AWS analytics services」を参照してください。
DeleteBucket	(必須) `s3:DeleteBucket`	S3 バケットを削除するために必要です。
DeleteBucketAnalyticsConfiguration	(必須) `s3:PutAnalyticsConfiguration`	S3 バケットから S3 分析設定を削除するために必要です。
DeleteBucketCors	(必須) `s3:PutBucketCORS`	バケットのクロスオリジンリソース共有 (CORS) 設定を削除するために必要です。
DeleteBucketEncryption	(必須) `s3:PutEncryptionConfiguration`	Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3) は、S3 のバケットでデフォルトの暗号化設定をリセットするために必要です。
DeleteBucketIntelligentTieringConfiguration	(必須) `s3:PutIntelligentTieringConfiguration`	S3 バケットから既存の S3 Intelligent-Tiering 設定を削除するために必要です。
DeleteBucketInventoryConfiguration	(必須) `s3:PutInventoryConfiguration`	S3 バケットから S3 インベントリ設定を削除するために必要です。

API オペレーション	ポリシーアクション	ポリシーアクションの説明
DeleteBucketLifecycle	(必須) s3:PutLifecycleConfiguration	S3 バケットの S3 ライフサイクル設定を削除するために必要です。
DeleteBucketMetadataTableConfiguration	(必須) s3:DeleteBucketMetadataTableConfiguration	汎用バケットからメタデータテーブル設定を削除するために必要です。
DeleteBucketMetricsConfiguration	(必須) s3:PutMetricsConfiguration	Amazon S3 バケットからの Amazon CloudWatch リクエストメトリクスのメトリクス構成を削除するために必要です。
DeleteBucketOwnershipControls	(必須) s3:PutBucketOwnershipControls	S3 バケットのオブジェクト所有権設定を削除するために必要です。削除後、オブジェクト所有権の設定は ObjectWriter になります。
DeleteBucketPolicy	(必須) s3:DeleteBucketPolicy	S3 バケットのポリシーを削除するために必要です。
DeleteBucketReplication	(必須) s3:PutReplicationConfiguration	S3 バケットのレプリケーション設定を削除するために必要です。
DeleteBucketTagging	(必須) s3:PutBucketTagging	S3 バケットからタグを削除するために必要です。
DeleteBucketWebsite	(必須) s3:DeleteBucketWebsite	S3 バケットのウェブサイト設定を削除するために必要です。

API オペレーション	ポリシーアクション	ポリシーアクションの説明
DeletePublicAccessBlock (バケットレベル)	(必須) s3:PutBucketPublicAccessBlock	S3 バケットのブロックパブリックアクセス設定を削除するために必要です。
GetBucketAccelerateConfiguration	(必須) s3:GetAccelerateConfiguration	Accelerate サブリソースを使用してバケット のAmazon S3 Transfer Acceleration 状態 (Enabled または Suspended) を返すために必要です。
GetBucketAcl	(必須) s3:GetBucketAcl	S3 バケットのアクセスコントロールリスト (ACL) を返すために必要です。
GetBucketAnalyticsConfiguration	(必須) s3:GetAnalyticsConfiguration	S3 バケットから分析設定 ID によって識別される分析設定を返すために必要です。
GetBucketCors	(必須) s3:GetBucketCORS	S3 バケットのクロスオリジンリソース共有 (CORS) 設定を返すために必要です。
GetBucketEncryption	(必須) s3:GetEncryptionConfiguration	S3 バケットのデフォルトの暗号化設定を返すために必要です。
GetBucketIntelligentTieringConfiguration	(必須) s3:GetIntelligentTieringConfiguration	S3 バケットの S3 Intelligent-Tiering 設定を取得するために必要です。
GetBucketInventoryConfiguration	(必須) s3:GetInventoryConfiguration	バケットのインベントリ設定 ID で識別されインベントリ設定を返すために必要です。

API オペレーション	ポリシーアクション	ポリシーアクションの説明
GetBucketLifecycle	(必須) s3:GetLifecycleConfiguration	バケットの S3 ライフサイクル設定を返すために必要です。
GetBucketLocation	(必須) s3:GetBucketLocation	S3 バケットが存在する AWS リージョンを返すために必要です。
GetBucketLogging	(必須) s3:GetBucketLogging	S3 バケットのロギングステータスと、ユーザーがそのステータスを表示および変更するアクセス許可を返すために必要です。
GetBucketMetadataTableConfiguration	(必須) s3:GetBucketMetadataTableConfiguration	汎用バケットのメタデータテーブル設定を取得するために必要です。
GetBucketMetricsConfiguration	(必須) s3:GetMetricsConfiguration	メトリクス設定 ID で指定されたメトリクス設定をバケットから取得するために必要です。
GetBucketNotificationConfiguration	(必須) s3:GetBucketNotification	S3 バケットの通知設定を返すために必要です。
GetBucketOwnershipControls	(必須) s3:GetBucketOwnershipControls	S3 バケットのオブジェクト所有権設定を取得するために必要です。
GetBucketPolicy	(必須) s3:GetBucketPolicy	ポリシーを S3 バケットに返すために必要です。

API オペレーション	ポリシーアクション	ポリシーアクションの説明
GetBucketPolicyStatus	(必須) s3:GetBucketPolicyStatus	バケットがパブリックかどうかを示す S3 バケットのポリシーステータスを取得するために必要です。
GetBucketReplication	(必須) s3:GetReplicationConfiguration	S3 バケットのレプリケーション設定を返すために必要です。
GetBucketRequestPayment	(必須) s3:GetBucketRequestPayment	S3 バケットのリクエスト支払い設定を返すために必要です。
GetBucketVersioning	(必須) s3:GetBucketVersioning	S3 バケットのバージョニング状態を返すために必要です。
GetBucketTagging	(必須) s3:GetBucketTagging	S3 バケットに関連付けられているタグセットを返すために必要です。
GetBucketWebsite	(必須) s3:GetBucketWebsite	S3 バケットのウェブサイト設定を返すために必要です。
GetObjectLockConfiguration	(必須) s3:GetBucketObjectLockConfiguration	S3 バケットの Object Lock 設定を取得するために必要です。
GetPublicAccessBlock (バケットレベル)	(必須) s3:GetBucketPublicAccessBlock	S3 バケットのブロックパブリックアクセス設定を取得するために必要です。
HeadBucket	(必須) s3:ListBucket	バケットが存在し、そのバケットにアクセスする許可があるかどうかを判断するために必要です。

API オペレーション	ポリシーアクション	ポリシーアクションの説明
ListBucketAnalyticsConfigurations	(必須) s3:GetAnalyticsConfiguration	S3 バケットの分析設定を一覧表示するために必要です。
ListBucketIntelligentTieringConfigurations	(必須) s3:GetIntelligentTieringConfiguration	S3 バケットの S3 Intelligent-Tiering 設定を一覧表示するために必要です。
ListBucketInventoryConfigurations	(必須) s3:GetInventoryConfiguration	S3 バケットのインベントリ設定のリストを返すために必要です。
ListBucketMetricsConfigurations	(必須) s3:GetMetricsConfiguration	S3 バケットのメトリクス設定を一覧表示するために必要です。
ListObjects	(必須) s3:ListBucket	S3 バケットのオブジェクトの一部またはすべて (最大 1,000) を一覧表示するために必要です。
	(条件付きで必須) s3:GetObjectAcl	オブジェクト所有者情報を表示する場合に必要です。
ListObjectsV2	(必須) s3:ListBucket	S3 バケットのオブジェクトの一部またはすべて (最大 1,000) を一覧表示するために必要です。
	(条件付きで必須) s3:GetObjectAcl	オブジェクト所有者情報を表示する場合に必要です。
ListObjectVersions	(必須) s3:ListBucketVersions	S3 バケット内のすべてのバージョンのオブジェクトに関するメタデータを取得するために必要です。

API オペレーション	ポリシーアクション	ポリシーアクションの説明
PutBucketAccelerateConfiguration	(必須) s3:PutAccelerateConfiguration	既存のバケットの加速設定を指定するために必要です。
PutBucketAcl	(必須) s3:PutBucketAcl	アクセスコントロールリスト (ACL) を使用して、既存のバケットに対するアクセス許可を設定するために必要です。
PutBucketAnalyticsConfiguration	(必須) s3:PutAnalyticsConfiguration	S3 バケットの分析設定を行うために必要です。
PutBucketCors	(必須) s3:PutBucketCORS	S3 バケットのクロスオリジンリソース共有 (CORS) 設定を指定するために必要です。
PutBucketEncryption	(必須) s3:PutEncryptionConfiguration	S3 バケットにデフォルトの暗号化を設定するために必要です。
PutBucketIntelligentTieringConfiguration	(必須) s3:PutIntelligentTieringConfiguration	S3 Intelligent-Tiering 設定を S3 バケットに配置するために必要です。
PutBucketInventoryConfiguration	(必須) s3:PutInventoryConfiguration	S3 バケットにインベントリ設定を追加するために必要です。
PutBucketLifecycle	(必須) s3:PutLifecycleConfiguration	S3 バケットの新しい S3 ライフサイクル設定を作成するか、既存のライフサイクル設定を置き換えるために必要です。

API オペレーション	ポリシーアクション	ポリシーアクションの説明
PutBucketLogging	(必須) s3:PutBucketLogging	S3 バケットのログ記録パラメータを設定し、ログ記録パラメータを表示および変更できるユーザーのアクセス許可を指定するために必要です。
PutBucketMetricsConfiguration	(必須) s3:PutMetricsConfiguration	S3 バケットの Amazon CloudWatch リクエストメトリクスのメトリクス設定を実行または更新するために必要です。
PutBucketNotificationConfiguration	(必須) s3:PutBucketNotification	S3 バケットの指定されたイベントの通知を有効にするために必要です。
PutBucketOwnershipControls	(必須) s3:PutBucketOwnershipControls	S3 バケットのオブジェクト所有権設定を作成または変更するために必要です。
PutBucketPolicy	(必須) s3:PutBucketPolicy	S3 バケットポリシーをバケットに適用するために必要です。
PutBucketReplication	(必須) s3:PutReplicationConfiguration	新しいレプリケーション設定を作成するか、S3 バケットの既存のレプリケーション設定を置き換えるために必要です。
PutBucketRequestPayment	(必須) s3:PutBucketRequestPayment	バケットのリクエスト支払い設定を実行するために必要です。
PutBucketTagging	(必須) s3:PutBucketTagging	S3 バケットにタグのセットを追加するために必要です。

API オペレーション	ポリシーアクション	ポリシーアクションの説明
PutBucketVersioning	(必須) s3:PutBucketVersioning	S3 バケットのバージョニング状態を設定するために必要です。
PutBucketWebsite	(必須) s3:PutBucketWebsite	バケットをウェブサイトとして設定し、ウェブサイトの設定を行うために必要です。
PutObjectLockConfiguration	(必須) s3:PutBucketObjectLockConfiguration	S3 バケットに Object Lock 設定を追加するために必要です。
PutPublicAccessBlock (バケットレベル)	(必須) s3:PutBucketPublicAccessBlock	S3 バケットのブロックパブリックアクセス設定を作成または変更するために必要です。

オブジェクトオペレーションとアクセス許可

オブジェクトオペレーションは、オブジェクトリソースタイプで動作する S3 API オペレーションです。リソースベースのポリシー (バケットポリシー、アクセスポイントポリシー、マルチリージョンアクセスポイントポリシー、VPC エンドポイントポリシーなど) または IAM アイデンティティベースのポリシーでオブジェクトオペレーションに S3 ポリシーアクションを指定する必要があります。

ポリシーでは、Resource 要素はオブジェクト ARN である必要があります。Resource 要素形式とポリシーの例の詳細については、「オブジェクト操作」を参照してください。

> **Note**
>
> - AWS KMS ポリシーアクション (kms:GenerateDataKey および kms:Decrypt) は AWS KMS リソースタイプにのみ適用され、IAM アイデンティティベースのポリシーと AWS KMS リソースベースのポリシー (AWS KMS キーポリシー) で指定する必要があります。S3 バケットポリシーなど、S3 リソースベースのポリシーでは AWS KMS ポリシーアクションを指定できません。

- アクセスポイントを使用してオブジェクトオペレーションへのアクセスを制御する場合、アクセスポイントポリシーを使用できます。アクセスポイントポリシーのオブジェクトオペレーションにアクセス許可を付与するには、次の点に注意してください。
  - オブジェクトオペレーションへのアクセス許可を付与するアクセスポイントポリシーでは、Resource 要素はアクセスポイントを介してアクセスされるオブジェクトの ARN である必要があります。Resource 要素形式とポリシーの例の詳細については、「アクセスポイントポリシーでのオブジェクトオペレーション」を参照してください。
  - すべてのオブジェクトオペレーションがアクセスポイントでサポートされているわけではありません。詳細については、「汎用バケットのアクセスポイントと S3 オペレーションとの互換性」を参照してください。
- すべてのオブジェクトオペレーションがマルチリージョンアクセスポイントでサポートされているわけではありません。詳細については、「S3 オペレーションとマルチリージョンアクセスポイントの互換性」を参照してください。

オブジェクトオペレーションと必要なポリシーアクションのマッピングを次に示します。

API オペレーション	ポリシーアクション	ポリシーアクションの説明
AbortMultipartUpload	(必須) s3:AbortMultipartUpload	マルチパートアップロードを中止するために必要です。
CompleteMultipartUpload	(必須) s3:PutObject	マルチパートアップロードを完了するために必要です。
	(条件付きで必須) kms:Decrypt	AWS KMS カスタマーマネージドキー暗号化オブジェクトのマルチパートアップロードを完了する場合に必要です。
CopyObject	ソースオブジェクトの場合:	ソースオブジェクトの場合:
	(必須) s3:GetObject または s3:GetObjectVersion	• s3:GetObject – リクエストで versionId を指定せずにソースバケットからオブジェクトをコピーする場合に必要です。

API オペレーション	ポリシーアクション	ポリシーアクションの説明
		• s3:GetObjectVersion – リクエストで versionId を指定して、ソースバケットから特定のバージョンのオブジェクトをコピーする場合に必要です。
	(条件付きで必須) kms:Decrypt	ソースバケットから AWS KMS カスタマーマネージドキーで暗号化されたオブジェクトをコピーする場合に必要です。
	送信先オブジェクトの場合:	送信先オブジェクトの場合:
	(必須) s3:PutObject	コピーしたオブジェクトを送信先バケットに配置するために必要です。
	(条件付きで必須) s3:PutObjectAcl	CopyObject リクエストを行うときに、オブジェクトアクセスコントロールリスト (ACL) を持つコピーしたオブジェクトを送信先バケットに配置する場合に必要です。
	(条件付きで必須) s3:PutObjectTagging	CopyObject リクエストを行うときに、オブジェクトのタグが付いたコピーしたオブジェクトを送信先バケットに配置する場合に必要です。

API オペレーション	ポリシーアクション	ポリシーアクションの説明
	(条件付きで必須) kms:GenerateDataKey	コピーしたオブジェクトを AWS KMS カスタマーマネージドキーで暗号化し、送信先バケットに配置する場合に必要です。
	(条件付きで必須) s3:PutObjectRetention	新しいオブジェクトの Object Lock 保持設定を行う場合に必要です。
	(条件付きで必須) s3:PutObjectLegalHold	新しいオブジェクトに Object Lock のリーガルホールドを適用する場合に必要です。
CreateMultipartUpload	(必須) s3:PutObject	マルチパートアップロードを作成するために必要です。
	(条件付きで必須) s3:PutObjectAcl	アップロードしたオブジェクトのオブジェクトアクセスコントロールリスト (ACL) アクセス許可を設定する場合に必要です。
	(条件付きで必須) s3:PutObjectTagging	アップロードしたオブジェクトにオブジェクトのタグ付け (複数可) を追加する場合に必要です。
	(条件付きで必須) kms:GenerateDataKey	マルチパートアップロードを開始するときに、AWS KMS カスタマーマネージドキーを使用してオブジェクトを暗号化する場合に必要です。

API オペレーション	ポリシーアクション	ポリシーアクションの説明
	(条件付きで必須) s3:PutObjectRetention	アップロードしたオブジェクトの Object Lock 保持設定を実行する場合に必要です。
	(条件付きで必須) s3:PutObjectLegalHold	アップロードしたオブジェクトに Object Lock のリーガルホールドを適用する場合に必要です。
DeleteObject	(必須) s3:DeleteObject または s3:DeleteObjectVersion	• s3:DeleteObject – リクエストで versionId を指定せずにオブジェクトを削除する場合に必要です。 • s3:DeleteObjectVersion – リクエストで versionId を指定してオブジェクトの特定のバージョンを削除する場合に必要です。
	(条件付きで必須) s3:BypassGovernanceRetention	Object Lock 保持のガバナンスモードで保護されているオブジェクトを削除する場合に必要です。
DeleteObjects	(必須) s3:DeleteObject または s3:DeleteObjectVersion	• s3:DeleteObject – リクエストで versionId を指定せずにオブジェクトを削除する場合に必要です。 • s3:DeleteObjectVersion – リクエストで versionId を指定してオブジェクトの特定のバージョンを削除する場合に必要です。

API オペレーション	ポリシーアクション	ポリシーアクションの説明
	(条件付きで必須) s3:BypassGovernanceRetention	Object Lock 保持のガバナンスモードで保護されているオブジェクトを削除する場合に必要です。
DeleteObjectTagging	(必須) s3:DeleteObjectTagging または s3:DeleteObjectVersionTagging	• s3:DeleteObjectTagging – リクエストで versionId を指定せずにオブジェクトのタグセット全体を削除する場合に必要です。 • s3:DeleteObjectVersionTagging – リクエストで versionId を指定して、特定のオブジェクトバージョンのタグを削除する場合に必要です。
GetObject	(必須) s3:GetObject または s3:GetObjectVersion	• s3:GetObject – リクエストで versionId を指定せずにオブジェクトを取得する場合に必要です。 • s3:GetObjectVersion – リクエストで versionId を指定して特定のバージョンのオブジェクトを取得する場合に必要です。
	(条件付きで必須) kms:Decrypt	AWS KMS カスタマーマネージドキーで暗号化されたオブジェクトを取得および復号する場合に必要です。

API オペレーション	ポリシーアクション	ポリシーアクションの説明
	(条件付きで必須) s3:GetObjectTagging	GetObject リクエストを行うときにオブジェクトのタグセットを取得する場合に必要です。
	(条件付きで必須) s3:GetObjectLegalHold	オブジェクトの現在の Object Lock のリーガルホールドステータスを取得する場合に必要です。
	(条件付きで必須) s3:GetObjectRetention	オブジェクトの Object Lock 保持設定を取得する場合に必要です。
GetObjectAcl	(必須) s3:GetObjectAcl または s3:GetObjectVersionAcl	• s3:GetObjectAcl – リクエストで versionId を指定せずにオブジェクトのアクセスコントロールリスト (ACL) を取得する場合に必要です。 • s3:GetObjectVersionAcl – リクエストで versionId を指定してオブジェクトのアクセスコントロールリスト (ACL) を取得する場合に必要です。

API オペレーション	ポリシーアクション	ポリシーアクションの説明
GetObjectAttributes	(必須) s3:GetObject または s3:GetObjectVersion	• s3:GetObject – リクエストで versionId を指定せずにオブジェクトに関連する属性を取得する場合に必要です。 • s3:GetObjectVersion – リクエストで versionId を指定して、特定のオブジェクトバージョンに関連する属性を取得する場合に必要です。
	(条件付きで必須) kms:Decrypt	AWS KMS カスタマーマネージドキー暗号化オブジェクトに関連する属性を取得する場合に必要です。
GetObjectLegalHold	(必須) s3:GetObjectLegalHold	オブジェクトの現在の Object Lock のリーガルホールドステータスを取得するために必要です。
GetObjectRetention	(必須) s3:GetObjectRetention	オブジェクトの Object Lock 保持設定を取得するために必要です。

API オペレーション	ポリシーアクション	ポリシーアクションの説明
GetObjectTagging	(必須) s3:GetObjectTagging または s3:GetObjectVersionTagging	• s3:GetObjectTagging – リクエストで versionId を指定せずにオブジェクトのタグセットを取得する場合に必要です。 • s3:GetObjectVersionTagging – リクエストで versionId を指定して、特定のオブジェクトバージョンのタグを取得する場合に必要です。
GetObjectTorrent	(必須) s3:GetObject	オブジェクトの torrent ファイルを返すために必要です。
HeadObject	(必須) s3:GetObject	オブジェクト自体を返さずにオブジェクトからメタデータを取得するために必要です。
	(条件付きで必須) s3:GetObjectLegalHold	オブジェクトの現在の Object Lock のリーガルホールドステータスを取得する場合に必要です。
	(条件付きで必須) s3:GetObjectRetention	オブジェクトの Object Lock 保持設定を取得する場合に必要です。
ListMultipartUploads	(必須) s3:ListBucketMultipartUploads	バケット内の進行中のマルチパートアップロードを一覧表示するために必要です。
ListParts	(必須) s3:ListMultipartUploadParts	特定のマルチパートアップロードでアップロードされている部分を一覧表示するために必要です。

API オペレーション	ポリシーアクション	ポリシーアクションの説明
	(条件付きで必須) kms:Decrypt	AWS KMS カスタマーマネージドキー暗号化マルチパートアップロードの一部を一覧表示する場合に必要です。
PutObject	(必須) s3:PutObject	オブジェクトを配置するために必要です。
	(条件付きで必須) s3:PutObjectAcl	PutObject リクエストを行うときにオブジェクトアクセスコントロールリスト (ACL) を配置する場合に必要です。
	(条件付きで必須) s3:PutObjectTagging	PutObject リクエストを行うときにオブジェクトのタグ付けを行う場合に必要です。
	(条件付きで必須) kms:GenerateDataKey	AWS KMS カスタマーマネージドキーを使用してオブジェクトを暗号化する場合に必要です。
	(条件付きで必須) s3:PutObjectRetention	オブジェクトに Object Lock 保持設定を行う場合に必要です。
	(条件付きで必須) s3:PutObjectLegalHold	指定されたオブジェクトに Object Lock のリーガルホールド設定を適用する場合に必要です。

API オペレーション	ポリシーアクション	ポリシーアクションの説明
PutObjectAcl	(必須) s3:PutObjectAcl または s3:PutObjectVersionAcl	• s3:PutObjectAcl – リクエストで versionId を指定せずに、新規または既存のオブジェクトのアクセスコントロールリスト (ACL) のアクセス許可を設定する場合に必要です。 • s3:PutObjectVersionAcl – リクエストで versionId を指定して、新規または既存のオブジェクトのアクセスコントロールリスト (ACL) アクセス許可を設定する場合に必要です。
PutObjectLegalHold	(必須) s3:PutObjectLegalHold	Object Lock のリーガルホールド設定をオブジェクトに適用するために必要です。
PutObjectRetention	(必須) s3:PutObjectRetention	Object Lock 保持設定をオブジェクトに適用するために必要です。
	(条件付きで必須) s3:BypassGovernanceRetention	Object Lock 保持設定のガバナンスモードをバイパスする場合に必要です。

API オペレーション	ポリシーアクション	ポリシーアクションの説明
PutObjectTagging	(必須) s3:PutObjectTagging または s3:PutObjectVersionTagging	• s3:PutObjectTagging – リクエストで versionId を指定せずに、指定されたタグセットをバケットに既に存在するオブジェクトに設定する場合に必要です。 • s3:PutObjectVersionTagging – リクエストで versionId を指定して、指定されたタグセットをバケットに既に存在するオブジェクトに設定する場合に必要です。
RestoreObject	(必須) s3:RestoreObject	アーカイブしたオブジェクトのコピーを復元するために必要です。
SelectObjectContent	(必須) s3:GetObject	シンプルな構造化クエリ言語 (SQL) ステートメントに基づいて S3 オブジェクトのコンテンツをフィルタリングするために必要です。
	(条件付きで必須) kms:Decrypt	AWS KMS カスタマーマネージドキーで暗号化された S3 オブジェクトのコンテンツをフィルタリングする場合に必要です。
UploadPart	(必須) s3:PutObject	マルチパートアップロードでパートをアップロードするために必要です。

API オペレーション	ポリシーアクション	ポリシーアクションの説明
	(条件付きで必須) kms:GenerateDataKey	アップロードパートを配置し、AWS KMS カスタマーマネージドキーで暗号化する場合に必要です。
UploadPartCopy	ソースオブジェクトの場合:	ソースオブジェクトの場合:
	(必須) s3:GetObject または s3:GetObjectVersion	• s3:GetObject – リクエストで versionId を指定せずにソースバケットからオブジェクトをコピーする場合に必要です。 • s3:GetObjectVersion – リクエストで versionId を指定して、ソースバケットから特定のバージョンのオブジェクトをコピーする場合に必要です。
	(条件付きで必須) kms:Decrypt	ソースバケットから AWS KMS カスタマーマネージドキーで暗号化されたオブジェクトをコピーする場合に必要です。
	送信先のパートの場合:	送信先のパートの場合:
	(必須) s3:PutObject	マルチパートアップロードのパートを送信先バケットにアップロードするために必要です。

API オペレーション	ポリシーアクション	ポリシーアクションの説明
	(条件付きで必須) kms:GenerateDataKey	パートを送信先バケットにアップロードするときに、AWS KMS カスタマーマネージドキーを使用してパートを暗号化する場合に必要です。

汎用バケットオペレーションのアクセスポイントとアクセス許可

アクセスポイントオペレーションは、accesspoint リソースタイプで動作する S3 API オペレーションです。アクセスポイントオペレーションの S3 ポリシーアクションは、バケットポリシーやアクセスポイントポリシーではなく、IAM アイデンティティベースのポリシーで指定する必要があります。

ポリシーでは、Resource 要素は accesspoint ARN である必要があります。Resource 要素形式とポリシーの例の詳細については、「汎用バケットオペレーションのアクセスポイント」を参照してください。

> **Note**
>
> アクセスポイントを使用してバケットまたはオブジェクトオペレーションへのアクセスを制御する場合は、次の点に注意してください。
>
> - アクセスポイントを使用してバケットオペレーションへのアクセスを制御する方法については、「汎用バケットのアクセスポイントのポリシーでのバケットオペレーション」を参照してください。
> - アクセスポイントを使用してオブジェクトオペレーションへのアクセスを制御する方法については、「アクセスポイントポリシーでのオブジェクトオペレーション」を参照してください。
> - アクセスポイントポリシーの設定方法の詳細については、「汎用バケットのアクセスポイントを使用するための IAM ポリシーの設定」を参照してください。

以下は、アクセスポイントオペレーションと必要なポリシーアクションのマッピングです。

API オペレーション	ポリシーアクション	ポリシーアクションの説明
CreateAccessPoint	(必須) s3:CreateAccessPoint	S3 バケットに関連付けられているアクセスポイントを作成するために必要です。
DeleteAccessPoint	(必須) s3:DeleteAccessPoint	アクセスポイントを削除するために必要です。
DeleteAccessPointPolicy	(必須) s3:DeleteAccessPointPolicy	アクセスポイントポリシーを削除するために必要です。
GetAccessPointPolicy	(必須) s3:GetAccessPointPolicy	アクセスポイントポリシーを取得するために必要です。
GetAccessPointPolicyStatus	(必須) s3:GetAccessPointPolicyStatus	指定したアクセスポイントにパブリックアクセスを許可するポリシーが現在あるかどうかに関する情報を取得するために必要です。
PutAccessPointPolicy	(必須) s3:PutAccessPointPolicy	アクセスポイントポリシーを配置するために必要です。

Object Lambda アクセスポイントのオペレーションとアクセス許可

Object Lambda アクセスポイントオペレーションは、objectlambdaaccesspoint リソースタイプで動作する S3 API オペレーションです。Object Lambda アクセスポイントオペレーションのポリシーを設定する方法についての詳細は、「Object Lambda アクセスポイントの IAM ポリシーの設定」を参照してください。

Object Lambda アクセスポイントオペレーションと必要なポリシーアクションのマッピングを次に示します。

API オペレーション	ポリシーアクション	ポリシーアクションの説明
CreateAccessPointForObjectLambda	(必須) s3:CreateAccessPointForObjectLambda	Object Lambda アクセスポイントを作成するために必要です。
DeleteAccessPointForObjectLambda	(必須) s3:DeleteAccessPointForObjectLambda	指定した Object Lambda アクセスポイントを削除するために必要です。
DeleteAccessPointPolicyForObjectLambda	(必須) s3:DeleteAccessPointPolicyForObjectLambda	指定したオブジェクト Lambda アクセスポイントでポリシーを削除するために必要です。
GetAccessPointConfigurationForObjectLambda	(必須) s3:GetAccessPointConfigurationForObjectLambda	Object Lambda アクセスポイントの設定を取得するために必要です。
GetAccessPointForObjectLambda	(必須) s3:GetAccessPointForObjectLambda	Object Lambda アクセスポイントに関する情報を取得するために必要です。
GetAccessPointPolicyForObjectLambda	(必須) s3:GetAccessPointPolicyForObjectLambda	指定した Object Lambda アクセスポイントに関連付けられたアクセスポイントポリシーを返すために必要です。
GetAccessPointPolicyStatusForObjectLambda	(必須) s3:GetAccessPointPolicyStatusForObjectLambda	特定の Object Lambda アクセスポイントポリシーのポリシーステータスを返すために必要です。
PutAccessPointConfigurationForObjectLambda	(必須) s3:PutAccessPointConfigurationForObjectLambda	Object Lambda アクセスポイントの設定に必要です。

API オペレーション	ポリシーアクション	ポリシーアクションの説明
PutAccessPointPolicyForObjectLambda	(必須) s3:PutAccessPointPolicyForObjectLambda	アクセスポリシーを指定した Object Lambda アクセスポイントに関連付けるために必要です。

マルチリージョンアクセスポイントとアクセス許可

マルチリージョンアクセスポイントオペレーションは、multiregionaccesspoint リソースタイプで動作する S3 API オペレーションです。マルチリージョンアクセスポイントオペレーションのポリシーを設定する方法の詳細については、「マルチリージョンアクセスポイントポリシーの例」を参照してください。

以下は、マルチリージョンアクセスポイントオペレーションと必要なポリシーアクションのマッピングです。

API オペレーション	ポリシーアクション	ポリシーアクションの説明
CreateMultiRegionAccessPoint	(必須) s3:CreateMultiRegionAccessPoint	マルチリージョンアクセスポイントを作成し、S3 バケットに関連付けるために必要です。
DeleteMultiRegionAccessPoint	(必須) s3:DeleteMultiRegionAccessPoint	マルチリージョンアクセスポイントを削除するために必要です。
DescribeMultiRegionAccessPointOperation	(必須) s3:DescribeMultiRegionAccessPointOperation	マルチリージョンアクセスポイントを管理するための非同期リクエストのステータスを取得するために必要です。
GetMultiRegionAccessPoint	(必須) s3:GetMultiRegionAccessPoint	指定したマルチリージョンアクセスポイントに関する設定情報を返すために必要です。

API オペレーション	ポリシーアクション	ポリシーアクションの説明
GetMultiRegionAccessPointPolicy	(必須) s3:GetMultiRegionAccessPointPolicy	指定したマルチリージョンアクセスポイントのアクセスコントロールポリシーを返すために必要です。
GetMultiRegionAccessPointPolicyStatus	(必須) s3:GetMultiRegionAccessPointPolicyStatus	指定したマルチリージョンアクセスポイントにパブリックアクセスを許可するアクセスコントロールポリシーが存在するかどうかについて、特定のマルチリージョンアクセスポイントのポリシーステータスを返すために必要です。
GetMultiRegionAccessPointRoutes	(必須) s3:GetMultiRegionAccessPointRoutes	マルチリージョンアクセスポイントのルート設定を返すために必要です。
PutMultiRegionAccessPointPolicy	(必須) s3:PutMultiRegionAccessPointPolicy	指定したマルチリージョンアクセスポイントのアクセスコントロールポリシーを更新するために必要です。
SubmitMultiRegionAccessPointRoutes	(必須) s3:SubmitMultiRegionAccessPointRoutes	マルチリージョンアクセスポイントのルート設定の更新を送信するために必要です。

バッチジョブのオペレーションとアクセス許可

(バッチオペレーション) ジョブオペレーションは、job リソースタイプで動作する S3 API オペレーションです。ジョブオペレーションの S3 ポリシーアクションは、バケットポリシーではなく、IAM アイデンティティベースのポリシーで指定する必要があります。

ポリシーでは、Resource 要素は job ARN である必要があります。Resource 要素形式とポリシーの例の詳細については、「バッチジョブオペレーション」を参照してください。

以下は、バッチジョブオペレーションと必要なポリシーアクションのマッピングです。

API オペレーション	ポリシーアクション	ポリシーアクションの説明
DeleteJobTagging	(必須) s3:DeleteJobTagging	既存の S3 バッチオペレーションジョブからタグを削除するために必要です。
DescribeJob	(必須) s3:DescribeJob	バッチオペレーションジョブの設定パラメータとステータスを取得するために必要です。
GetJobTagging	(必須) s3:GetJobTagging	既存の S3 バッチオペレーションジョブのタグセットを返すために必要です。
PutJobTagging	(必須) s3:PutJobTagging	既存の S3 バッチオペレーションジョブにタグを配置または置換するために必要です。
UpdateJobPriority	(必須) s3:UpdateJobPriority	既存のジョブの優先度を更新するために必要です。
UpdateJobStatus	(必須) s3:UpdateJobStatus	指定したジョブのステータスを更新するために必要です。

S3 ストレージレンズ設定オペレーションとアクセス許可

S3 ストレージレンズオペレーションは、storagelensconfiguration リソースタイプで動作する S3 API オペレーションです。S3 Storage Lens 設定オペレーションの設定方法の詳細については、「Amazon S3 ストレージレンズアクセス許可の設定」を参照してください。

以下は、S3 ストレージレンズの設定オペレーションと必要なポリシーアクションのマッピングです。

API オペレーション	ポリシーアクション	ポリシーアクションの説明
DeleteStorageLensConfiguration	(必須) s3:DeleteStorageLensConfiguration	S3 ストレージレンズ設定を削除するために必要です。
DeleteStorageLensConfigurationTagging	(必須) s3:DeleteStorageLensConfigurationTagging	S3 ストレージレンズ設定タグを削除するために必要です。
GetStorageLensConfiguration	(必須) s3:GetStorageLensConfiguration	S3 ストレージレンズ設定を取得するために必要です。
GetStorageLensConfigurationTagging	(必須) s3:GetStorageLensConfigurationTagging	S3 ストレージレンズ設定のタグを取得するために必要です。
PutStorageLensConfigurationTagging	(必須) s3:PutStorageLensConfigurationTagging	既存の S3 ストレージレンズ設定にタグを配置または置換するために必要です。

S3 ストレージレンズグループのオペレーションとアクセス許可

S3 ストレージレンズグループオペレーションは、storagelensgroup リソースタイプで動作する S3 API オペレーションです。S3 ストレージレンズグループのアクセス許可を設定する方法の詳細については、「Storage Lens グループのアクセス許可。」を参照してください。

以下は、S3 ストレージレンズグループのオペレーションと必要なポリシーアクションのマッピングです。

API オペレーション	ポリシーアクション	ポリシーアクションの説明
DeleteStorageLensGroup	(必須) s3:DeleteStorageLensGroup	既存の S3 ストレージレンズグループを削除するために必要です。

API オペレーション	ポリシーアクション	ポリシーアクションの説明
GetStorageLensGroup	(必須) s3:GetStorageLensGroup	S3 ストレージレンズグループ設定の詳細を取得するために必要です。
UpdateStorageLensGroup	(必須) s3:UpdateStorageLensGroup	既存の S3 ストレージレンズグループを更新するために必要です。
CreateStorageLensGroup	(必須) s3:CreateStorageLensGroup	新しいストレージレンズグループを作成するために必要です。
CreateStorageLensGroup, TagResource	(必須) s3:CreateStorageLensGroup 、s3:TagResource	タグ付きの新しいストレージレンズグループグループを作成するために必要です。
ListStorageLensGroups	(必須) s3:ListStorageLensGroups	ホームリージョンのすべてのストレージレンズグループを一覧表示するために必要です。
ListTagsForResource	(必須) s3:ListTagsForResource	ストレージレンズグループに追加されたタグを一覧表示するために必要です。
TagResource	(必須) s3:TagResource	既存のストレージレンズグループのストレージレンズグループタグを追加または更新するために必要です。
UntagResource	(必須) s3:UntagResource	ストレージレンズグループからタグを削除するために必要です。

S3 Access Grants インスタンスのオペレーションとアクセス許可

S3 Access Grants インスタンスのオペレーションは、accessgrantsinstance リソースタイプに対して実行される S3 API オペレーションです。S3 Access Grants インスタンスは、アクセス許可の論理コンテナです。S3 Access Grants インスタンスの使用の詳細については、「S3 Access Grants インスタンスの使用」を参照してください。

以下は、S3 Access Grants インスタンスの設定オペレーションと必要なポリシーアクションのマッピングです。

API オペレーション	ポリシーアクション	ポリシーアクションの説明
AssociateAccessGrantsIdentityCenter	(必須) s3:AssociateAccessGrantsIdentityCenter	AWS IAM Identity Center インスタンスを S3 Access Grants インスタンスに関連付けるために必要です。これにより、企業 ID ディレクトリ内のユーザーとグループのアクセス許可を作成できるようになります。また、次のアクセス許可も必要です。 sso:CreateApplication 、sso:PutApplicationGrant 、および sso:PutApplicationAuthenticationMethod 。
CreateAccessGrantsInstance	(必須) s3:CreateAccessGrantsInstance	個々のアクセス許可のコンテナである S3 Access Grants インスタンス (accessgrantsinstance リソース) を作成するために必要です。 AWS IAM Identity Center インスタンスを S3 Access Grants インスタンス

API オペレーション	ポリシーアクション	ポリシーアクションの説明
		に関連付けるためには、sso:DescribeInstance 、sso:CreateApplication 、sso:PutApplicationGrant 、sso:PutApplicationAuthenticationMethod のアクセス許可も必要です。
DeleteAccessGrantsInstance	(必須) s3:DeleteAccessGrantsInstance	アカウント内の AWS リージョン から S3 Access Grants インスタンス (accessgrantsinstance リソース) を削除するために必要です。
DeleteAccessGrantsInstanceResourcePolicy	(必須) s3:DeleteAccessGrantsInstanceResourcePolicy	S3 Access Grants インスタンスのリソースポリシーを削除するために必要です。
DissociateAccessGrantsIdentityCenter	(必須) s3:DissociateAccessGrantsIdentityCenter	AWS IAM Identity Center インスタンスと S3 Access Grants インスタンスの関連付けを解除するために必要です。また、次のアクセス許可も必要です。 sso:DeleteApplication
GetAccessGrantsInstance	(必須) s3:GetAccessGrantsInstance	アカウント内の AWS リージョン の S3 Access Grants インスタンスを取得するために必要です。

API オペレーション	ポリシーアクション	ポリシーアクションの説明
GetAccessGrantsInstanceForPrefix	(必須) s3:GetAccessGrantsInstanceForPrefix	特定のプレフィックスを含む S3 Access Grants インスタンスを取得するために必要です。
GetAccessGrantsInstanceResourcePolicy	(必須) s3:GetAccessGrantsInstanceResourcePolicy	S3 Access Grants インスタンスのリソースポリシーを返すために必要です。
ListAccessGrantsInstances	(必須) s3:ListAccessGrantsInstances	アカウント内の S3 Access Grants インスタンスのリストを返すために必要です。
PutAccessGrantsInstanceResourcePolicy	(必須) s3:PutAccessGrantsInstanceResourcePolicy	S3 Access Grants インスタンスのリソースポリシーを更新するために必要です。

S3 Access Grants ロケーションのオペレーションとアクセス許可

S3 Access Grants ロケーションのオペレーションは、accessgrantslocation リソースタイプに対して実行される S3 API オペレーションです。S3 Access Grants ロケーションの使用の詳細については、「S3 Access Grants ロケーションの使用」を参照してください。

以下は、S3 Access Grants ロケーションの設定オペレーションと必要なポリシーアクションのマッピングです。

API オペレーション	ポリシーアクション	ポリシーアクションの説明
CreateAccessGrantsLocation	(必須) s3:CreateAccessGrantsLocation	S3 Access Grants インスタンスにロケーションを登録する (accessgrantslocation リソースを作成する) ために必要です。指定した IAM ロールには、次のアクセス許可も必要です。

API オペレーション	ポリシーアクション	ポリシーアクションの説明
		`iam:PassRole`
DeleteAccessGrantsLocation	(必須) `s3:DeleteAccessGrantsLocation`	S3 Access Grants インスタンスから登録済みの口ケーションを削除するために必要です。
GetAccessGrantsLocation	(必須) `s3:GetAccessGrantsLocation`	S3 Access Grants インスタンスに登録済みの特定の口ケーションの詳細を取得するために必要です。
ListAccessGrantsLocations	(必須) `s3:ListAccessGrantsLocations`	S3 Access Grants インスタンスに登録済みの口ケーションのリストを返すために必要です。
UpdateAccessGrantsLocation	(必須) `s3:UpdateAccessGrantsLocation`	S3 Access Grants インスタンスの登録済み口ケーションの IAM 口ールを更新するために必要です。

S3 Access Grants の許可付与オペレーションとアクセス許可

S3 Access Grants の許可付与オペレーションは、`accessgrant` リソースタイプに対して実行される S3 API オペレーションです。S3 Access Grants の個々の許可付与の使用の詳細については、「S3 Access Grants での許可の使用」を参照してください。

以下は、S3 Access Grants の許可付与の設定オペレーションと必要なポリシーアクションのマッピングです。

API オペレーション	ポリシーアクション	ポリシーアクションの説明
CreateAccessGrant	(必須) `s3:CreateAccessGrant`	S3 Access Grants インスタンスでユーザーまたはグループの個々の許可付与

API オペレーション	ポリシーアクション	ポリシーアクションの説明
		(accessgrant リソース) を作成するために必要です。また、次のアクセス許可も必要です。 任意のディレクトリアイデンティティの場合 — sso:DescribeInstance および sso:DescribeApplication ディレクトリユーザーの場合 — identitystore:DescribeUser
DeleteAccessGrant	(必須) s3:DeleteAccessGrant	S3 Access Grants インスタンスから個々のアクセス許可付与 (accessgrant リソース) を削除するために必要です。
GetAccessGrant	(必須) s3:GetAccessGrant	S3 Access Grants インスタンスの個々のアクセス許可付与の詳細を取得するために必要です。
ListAccessGrants	(必須) s3:ListAccessGrants	S3 Access Grants インスタンスの個々のアクセス許可付与のリストを返すために必要です。
ListCallerAccessGrants	(必須) s3:ListCallerAccessGrants	S3 Access Grants を通じて呼び出し元に Amazon S3 データへのアクセスを許可するアクセス許可付与を一覧表示するために必要です。

API オペレーションとアクセス許可

アカウントオペレーションは、アカウントレベルで実行される S3 API オペレーションです。アカウントは、Amazon S3 で定義されるリソースタイプではありません。アカウントオペレーションの S3 ポリシーアクションは、バケットポリシーではなく、IAM アイデンティティベースのポリシーで指定する必要があります。

ポリシーでは、Resource 要素は "*" である必要があります。ポリシーの例の詳細については、「アカウントオペレーション」を参照してください。

以下は、アカウントオペレーションと必要なポリシーアクションのマッピングです。

API オペレーション	ポリシーアクション	ポリシーアクションの説明
CreateJob	(必須) s3:CreateJob	新しい S3 バッチオペレーションジョブを作成するために必要です。
CreateStorageLensGroup	(必須) s3:CreateStorageLensGroup	新しい S3 ストレージレンズグループを作成し、指定した AWS アカウント ID に関連付けるために必要です。
	(条件付きで必須) s3:TagResource	AWS リソースタグを使用して S3 ストレージレンズグループを作成する場合に必要です。
DeletePublicAccessBlock (アカウントレベル)	(必須) s3:PutAccountPublicAccessBlock	ブロックパブリックアクセス設定を AWS アカウントから削除するために必要です。
GetAccessPoint	(必須) s3:GetAccessPoint	指定したアクセスポイントに関する設定情報を取得するために必要です。
GetAccessPointPolicy (アカウントレベル)	(必須) s3:GetAccountPublicAccessBlock	AWS アカウントのブロックパブリックアクセス設定を取得するために必要です。

API オペレーション	ポリシーアクション	ポリシーアクションの説明
ListAccessPoints	(必須) s3:ListAccessPoints	AWS アカウントが所有する S3 バケットのアクセスポイントを一覧表示するために必要です。
ListAccessPointsForObjectLambda	(必須) s3:ListAccessPointsForObjectLambda	Object Lambda アクセスポイントを一覧表示するために必要です。
ListBuckets	(必須) s3:ListAllMyBuckets	認証されたリクエスト送信者が所有するすべてのバケットのリストを返すために必要です。
ListJobs	(必須) s3:ListJobs	現在のジョブと最近終了したジョブを一覧表示するために必要です。
ListMultiRegionAccessPoints	(必須) s3:ListMultiRegionAccessPoints	指定した AWS アカウントに現在関連付けられているマルチリージョンアクセスポイントのリストを返すために必要です。
ListStorageLensConfigurations	(必須) s3:ListStorageLensConfigurations	AWS アカウントの S3 ストレージレンズ設定のリストを取得するために必要です。
ListStorageLensGroups	(必須) s3:ListStorageLensGroups	指定したホーム AWS リージョン内のすべての S3 ストレージレンズグループを一覧表示するために必要です。

API オペレーション	ポリシーアクション	ポリシーアクションの説明
PutPublicAccessBlock (アカウントレベル)	(必須) s3:PutAccountPublicAccessBlock	AWS アカウントのブロックパブリックアクセス設定を作成または変更するために必要です。
PutStorageLensConfiguration	(必須) s3:PutStorageLensConfiguration	S3 ストレージレンズ設定を配置するために必要です。

Amazon S3 のポリシーとアクセス許可

ここでは、Amazon S3 のバケットポリシーとユーザーポリシーの概要を示し、AWS Identity and Access Management (IAM) ポリシーの基本的な エレメントについて説明します。リストされた各エレメントは、そのエレメントの詳細と使用方法の例にリンクしています。

Amazon S3 アクションの完全なリストについては、「サービス認可リファレンス」の「Actions, resources, and condition keys for Amazon S3」を参照してください。

S3 リソースタイプ別の S3 API オペレーションへのアクセス許可の詳細については、「Amazon S3 API オペレーションに必要なアクセス許可」を参照してください。

基本的に、ポリシーには以下のエレメントが含まれます。

- Resource — ポリシーが適用される Amazon S3 バケット、オブジェクト、アクセスポイント、またはジョブ。バケット、オブジェクト、アクセスポイント、またはジョブの Amazon リソースネーム (ARN) を使用してリソースを識別します。

  バケットレベルのオペレーションの例:

  `"Resource": "arn:aws:s3:::bucket_name"`

  オブジェクトレベルのオペレーションの例:

  - `"Resource": "arn:aws:s3:::bucket_name/*"` (バケットのすべてのオブジェクト)
  - `"Resource": "arn:aws:s3:::bucket_name/prefix/*"` (バケット内の特定のプレフィックスの下にあるオブジェクト)

  詳細については、「Amazon S3 のポリシーリソース」を参照してください。

- Actions – Amazon S3 では、各リソースに対して一連のオペレーションがサポートされています。許可 (または拒否) するリソースのオペレーションは、アクションキーワードを使用して識別します。

  例えば、`s3:ListBucket` アクセス許可は、Amazon S3 の ListObjectsV2 オペレーションの使用をユーザーに許可します (`s3:ListBucket` アクセス許可は、アクション名がオペレーション名に直接マッピングされないケースに該当します)。Amazon S3 アクションの使用に関する詳細については、「Amazon S3 のポリシーアクション」を参照してください。Amazon S3 のアクション一覧については、Amazon Simple Storage Service API リファレンスの「アクション」を参照してください。
- Effect – ユーザーが特定のアクションをリクエストした場合の効力です。`Allow` または `Deny` のいずれかになります。

  リソースへのアクセスを明示的に許可していない場合、アクセスは暗黙的に拒否されます。リソースへのアクセスを明示的に拒否することもできます。別のポリシーでリソースへのアクセスが許可されているユーザーに対して、そのリソースへのアクセスを禁止できます。詳細については、IAM ユーザーガイドの「IAM JSON ポリシーの要素: Effect」を参照してください。
- Principal – ステートメントのアクションやリソースへのアクセスが許可されているアカウントまたはユーザーを指します。バケットポリシーの場合、プリンシパルは、このアクセス許可の被付与者であるユーザー、アカウント、サービス、または他のエンティティです。詳細については、「バケットポリシーのプリンシパル」を参照してください。
- Condition – ポリシーが有効になる条件。Amazon S3 のアクセスポリシーの条件は、AWS 全体のキーと Amazon S3 固有のキーを使用して指定することができます。詳細については、「条件キーを使用したバケットポリシーの例」を参照してください。

以下のバケットポリシーの例は、`Effect`、`Principal`、`Action`、`Resource`の
エレメントを示しています。このポリシーは、アカウント *123456789012* の
ユーザー *Akua* に、*amzn-s3-demo-bucket1* バケットに対する Amazon S3 の
`s3:GetObject`、`s3:GetBucketLocation`、`s3:ListBucket` アクセス許可を付与します。

```
{
    "Version": "2012-10-17",
    "Id": "ExamplePolicy01",
    "Statement": [
        {
            "Sid": "ExampleStatement01",
            "Effect": "Allow",
            "Principal": {
```

```
                "AWS": "arn:aws:iam::123456789012:user/Akua"
            },
            "Action": [
                "s3:GetObject",
                "s3:GetBucketLocation",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket1/*",
                "arn:aws:s3:::amzn-s3-demo-bucket1"
            ]
        }
    ]
}
```

ポリシーの言語の詳細については、「IAM ユーザーガイド」の「IAM でのポリシーとアクセス許可」および「IAM JSON ポリシーリファレンス」を参照してください。

アクセス許可の委任

AWS アカウントがリソースを所有している場合、そのアカウントは別の AWS アカウントにこれらの許可を付与できます。そのアカウントは、それらのアクセス許可またはそのサブセットを、アカウント内のユーザーに委任できます。これはアクセス許可の委任と呼ばれます。ただし、他のアカウントから許可を受け取るアカウントは、別の AWS アカウント にクロスアカウントで許可を委任することはできません。

Amazon S3 のバケットとオブジェクトの所有権

バケットとオブジェクトは Amazon S3 のリソースです。デフォルトでは、リソース所有者のみ、これらのリソースにアクセスできます。リソースの所有者とは、リソースを作成する AWS アカウントを指します。例:

- このようなリソースの所有者は、バケットの作成とオブジェクトのアップロードに使用する AWS アカウントです。
- AWS Identity and Access Management (IAM) ユーザーまたはロールの認証情報を使用してオブジェクトをアップロードする場合、オブジェクトの所有者は、そのユーザーやロールが属する AWS アカウントです。
- バケット所有者は、別の AWS アカウント (または別のアカウントのユーザー) に対して、オブジェクトをアップロードするためのクロスアカウントアクセス許可を付与できます。この場合、オブジェクトをアップロードする AWS アカウントが、それらのオブジェクトを所有します。バケッ

ト所有者には、他のアカウントが所有するオブジェクトに対するアクセス許可はありません。ただし、次のような例外があります。

- バケット所有者が請求の支払いを行う場合、バケット所有者は、オブジェクトの所有者に関係なく、オブジェクトへのアクセスを拒否したり、バケット内のオブジェクトを削除したりすることができます。
- バケット所有者は、オブジェクトの所有者に関係なく、オブジェクトをアーカイブしたり、アーカイブされたオブジェクトを復元したりすることができます。アーカイブはオブジェクトの格納に使用されるストレージクラスを指します。詳細については、オブジェクトのライフサイクルの管理 を参照してください。

所有権とリクエスト認証

バケットに対するリクエストはすべて、認証済みまたは未認証です。認証済みのリクエストには、リクエストの送信元を認証する署名値を含める必要がありますが、未認証のリクエストには含みません。リクエスト認証の詳細については、「Amazon S3 API リファレンス」の「Making requests」を参照してください。

バケット所有者は認証されていないリクエストを許可できます。例えば、認証されていない PutObject リクエストは、バケットにパブリックバケットポリシーが適用されている場合や、バケットの ACL で `All Users` グループまたは匿名ユーザーに `WRITE` または `FULL_CONTROL` のアクセス許可が付与されている場合に許可されます。パブリックバケットポリシーとパブリックアクセスコントロールリスト (ACL) の詳細については、「パブリック」の意味 を参照してください。

認証されていないリクエストはすべて、匿名ユーザーによって行われます。このユーザーは、特定の正規ユーザー ID `65a011a29cdf8ec533ec3d1ccaae921c` によって、ACL で表されます。認証されていないリクエストでオブジェクトがバケットにアップロードされている場合、所有者はその匿名ユーザーです。デフォルトのオブジェクト ACL では、`FULL_CONTROL` がオブジェクトの所有者として匿名ユーザーに付与されます。そのため、Amazon S3 では、認証されていないリクエストによるオブジェクトの取得やその ACL の変更を許可しています。

匿名ユーザーによってオブジェクトが変更されないように、匿名のパブリック書き込みをバケットに許可するバケットポリシーを実装したり、匿名ユーザーにバケットへの書き込みアクセスを許可したりする ACL を使用しないことをお勧めします。この推奨事項を強制的に適用するには、Amazon S3 のパブリックアクセスのブロックを使用します。

パブリックアクセスのブロックの詳細については、Amazon S3 ストレージへのパブリックアクセスのブロック を参照してください。ACL の詳細については、アクセスコントロールリスト (ACL) の概要 を参照してください。

> **Important**
>
> 認証されたリクエストの実行に AWS アカウントのルートユーザー認証情報を使用しないことをお勧めします。代わりに、IAM ロールを作成し、このロールにフルアクセスを許可します。このロールを持つユーザーを管理者ユーザーと呼びます。AWS アカウントのルートユーザー認証情報ではなく、管理者ユーザーに割り当てられた認証情報を使用して AWS とやり取りし、バケットの作成、ユーザーの作成、アクセス許可の付与などのタスクを実行できます。詳細については、「IAM ユーザーガイド」の「AWS セキュリティ認証情報」および「IAM でのセキュリティのベストプラクティス」を参照してください。

Amazon S3 のバケットポリシー

バケットポリシーは、Amazon S3 バケットとその中のオブジェクトへのアクセス許可を付与できるリソースベースのポリシーです。バケット所有者のみが、ポリシーをバケットに関連付けることができます。バケットに添付された許可は、バケット所有者が所有するバケットのすべてのオブジェクトに適用されます。これらの許可は、他の AWS アカウント が所有するオブジェクトには適用されません。

S3 オブジェクト所有権は、Amazon S3 バケットレベルの設定で、バケットにアップロードされたオブジェクトの所有権を制御し、アクセスコントロールリスト (ACL) を有効または無効にするのに使用できます。デフォルトでは、オブジェクト所有権は [バケット所有者の強制] により設定され、すべての ACL は無効になっています。バケット所有者は、バケット内のすべてのオブジェクトを所有し、ポリシーのみを使用してオブジェクトへのアクセスを管理します。

バケットポリシーは、JSON ベースの AWS Identity and Access Management (IAM) ポリシー言語を使用します。バケットポリシーを使用して、バケット内のオブジェクトに対する許可を追加または拒否できます。バケットポリシーは、ポリシーの要素に基づいて、リクエストを許可または拒否します。これらの要素には、リクエスタ、S3 アクション、リソース、およびリクエストの側面または条件 (リクエストの作成に使用された IP アドレスなど) が含まれます。

例えば、次のことを実行するバケットポリシーを作成できます。

- S3 バケットにオブジェクトをアップロードするためのクロスアカウントアクセス許可を付与するクロスアカウントアクセス許可を付与する
- バケット所有者であるユーザーが、アップロードされたオブジェクトを完全に管理できるようにする

詳細については、「Amazon S3 バケットポリシーの例」を参照してください。

> **Important**
>
> バケットポリシーを使用して、S3 ライフサイクルルールによる削除や移行を防ぐことはできません。例えば、バケットポリシーがすべてのプリンシパルのすべてのアクションを拒否する場合でも、S3 ライフサイクル設定は通常どおり機能します。

このセクションのトピックでは、具体例と、S3 コンソールにバケットポリシーを追加する方法について説明します。アイデンティティベースのポリシーについては、「Amazon S3 のアイデンティティベースのポリシー」を参照してください。バケットポリシー言語の詳細については、「Amazon S3 のポリシーとアクセス許可」を参照してください。

S3 リソースタイプ別の S3 API オペレーションへのアクセス許可の詳細については、「Amazon S3 API オペレーションに必要なアクセス許可」を参照してください。

トピック

- Amazon S3 コンソールを使用したバケットポリシーの追加
- バケットポリシーを使用した VPC エンドポイントからのアクセスコントロール
- Amazon S3 バケットポリシーの例
- 条件キーを使用したバケットポリシーの例

Amazon S3 コンソールを使用したバケットポリシーの追加

AWS Policy Generator および Amazon S3 コンソールを使用して、新しいバケットポリシーを追加したり、既存のバケットポリシーを編集したりできます。バケットポリシーはリソースベースの AWS Identity and Access Management (IAM) ポリシーです。バケットポリシーをバケットに追加して、バケットおよびバケット内のオブジェクトに対するアクセス許可を、他の AWS アカウントまたは IAM ユーザーに付与できます。オブジェクトのアクセス許可は、バケット所有者が作成したオブジェクトにのみ適用されます。バケットポリシーの詳細については、「Amazon S3 用 Identity and Access Management」を参照してください。

ポリシーを保存する前に、AWS Identity and Access Management Access Analyzer でセキュリティ警告、エラー、一般的な警告、および提案を解決してください。IAM Access Analyzer は、IAM ポリシーの文法およびベストプラクティス に対してポリシーチェックを行います。これらのチェックにより、機能的でセキュリティのベストプラクティスに準拠したポリシーを作成するのに、役立つ結果

と実行可能なレコメンデーションが示されます。IAM Access Analyzer を使用したポリシーの検証の詳細については、「IAM ユーザーガイド」の「IAM Access Analyzer のポリシーの検証」を参照してください。IAM Access Analyzer によって返される警告、エラー、および提案のリストを表示するには、「IAM Access Analyzer ポリシーチェックリファレンス」を参照してください。

ポリシーのエラーのトラブルシューティングに関するガイダンスについては、「Amazon S3 でのアクセス拒否 (403 Forbidden) エラーのトラブルシューティング」を参照してください。

バケットポリシーを作成または編集するには

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 左のナビゲーションペインで、[汎用バケット] または [ディレクトリバケット] を選択します。
3. バケットのリストで、バケットポリシーを作成するバケットの名前、またはバケットポリシーを編集するバケットの名前を選択します。
4. [アクセス許可] タブを選択します。
5. [バケットポリシー] で [編集] を選択します。[Edit bucket policy] (バケットポリシーを編集) ページが表示されます。
6. [Edit bucket policy] (バケットポリシーを編集) ページで、次の操作を実行します。

   - バケットポリシーの例を表示するには、[ポリシーの例] をクリックします。または、「Amazon S3 ユーザーガイド」の「Amazon S3 バケットポリシーの例」を参照してください。
   - ポリシーを自動的に生成するか、Policy] (ポリシー) セクションで JSON を編集するには、[Policy Generator] を選択します。

   [Policy Generator] を選択すると、AWS Policy Generator が新しいウィンドウで開きます。

   a. [Select Type of Policy] (ポリシーの種類の選択) の [AWS Policy Generator] ページで、[S3 Bucket Policy] (S3 バケットポリシー)を選択します。
   b. 提供されたフィールドに情報を入力してステートメントを追加し、ステートメントの追加を選択します。このステップを、追加するステートメントの数だけ繰り返します。ポリシーステートメントの詳細については、IAM ユーザーガイドの IAM JSON ポリシーのエレメントのリファレンスを参照してください。

> **Note**
>
> わかりやすいように、[バケットポリシーの編集] ページでは、現在のバケットの [バケット ARN] (Amazon リソースネーム) が [ポリシー] テキストフィールドの上に表示されます。この ARN をコピーして、AWSポリシージェネレータのステートメントで使用できます。

c. ステートメントの追加が完了したら、ポリシーの生成を選択します。

d. 生成されたポリシーテキストをコピーし、[閉じる] を選択すると、Amazon S3 コンソールのバケットポリシーの編集ページに戻ります。

7. [Policy] (ポリシー) ボックスで、既存のポリシーを編集するか、AWS Policy Generator からバケットポリシーを貼り付けます。ポリシーを保存する前に、セキュリティ警告、エラー、一般的な警告、および提案を解決してください。

> **Note**
>
> バケットポリシーのサイズは 20 KB に制限されています。

8. (オプション) 新しいポリシーがリソースへのパブリックアクセスおよびクロスアカウントアクセスにどのように影響するかをプレビューするには、[Preview external access] (外部アクセスをプレビュー) を選択します。ポリシーを保存する前に、新しい IAM Access Analyzer の結果が導入されているかどうかや、既存の結果を解決するかどうかを確認できます。アクティブなアナライザーが表示されない場合は、[Go to Access Analyzer] (Access Analyzer に移動) を選択し、[IAM Access Analyzer] でアカウントアナライザーを作成します。詳細については、IAM ユーザーガイドのアクセスのプレビューを参照してください。

9. [Save changes] (変更の保存) を選択すると、[Permissions] (アクセス許可) タブへ戻ります。

バケットポリシーを使用した VPC エンドポイントからのアクセスコントロール

Amazon S3 のバケットポリシーを使用して、特定の仮想プライベートクラウド (VPC) エンドポイントまたは特定の VPC からのバケットへのアクセスを管理できます。このセクションでは、VPC エンドポイントからの Amazon S3 のバケットへのアクセスを管理するために使用できるバケットポリシーの例を示します。VPC エンドポイントの設定方法については、VPC ユーザーガイドの VPC エンドポイントを参照してください。

VPC を使用すると、定義した仮想ネットワーク内で AWS のリソースを起動できます。VPC エンドポイントにより、VPC と他の AWS のサービス 間のプライベート接続を作成できます。このプライベート接続では、インターネットアクセス、仮想プライベートネットワーク (VPN) 接続、NAT インスタンス、または AWS Direct Connect を介した接続は必要ありません。

Amazon S3 の VPC エンドポイントは、Amazon S3 への接続のみを許可する VPC 内の論理エンティティです。VPC エンドポイントはリクエストを Amazon S3 にルーティングし、レスポンスを VPC にルーティングします。VPC エンドポイントはリクエストのルーティング方法のみを変更します。Amazon S3 のパブリックエンドポイントと DNS 名は、VPC エンドポイントでも使用できます。Amazon S3 での VPC エンドポイントの使用の詳細については、「VPC ユーザーガイド」の「Gateway endpoints」および「Gateway endpoints for Amazon S3」を参照してください。

Amazon S3 の VPC エンドポイントは、Amazon S3 のデータへのアクセスを管理する 2 つの方法を提供します。

- 特定の VPC エンドポイントを通じて許可されるリクエスト、ユーザー、またはグループを管理できます。このタイプのアクセス管理については、「VPC ユーザーガイド」の「Controlling access to VPC endpoints using endpoint policies」を参照してください。
- Amazon S3 のバケットポリシーを使用して、バケットへのアクセスを許可する VPC または VPC エンドポイントを管理できます。この種類のバケットポリシーのアクセスコントロールの例については、アクセス制限に関する次のトピックを参照してください。

トピック

- 特定の VPC エンドポイントへのアクセスの制限
- 特定の VPC へのアクセスの制限

> **Important**
>
> このセクションで説明している VPC エンドポイントに Amazon S3 のバケットポリシーを適用すると、バケットへのアクセスが意図せずにブロックされる場合があります。特に VPC エンドポイントからの接続に対するバケットのアクセスを制限することを目的としたバケットのアクセス許可により、バケットへのすべての接続がブロックされる場合があります。この問題を修正する方法については、「AWS サポート 情報センター」の「バケットポリシーの VPC または VPC エンドポイント ID が間違っています。ポリシーを修正してバケットに再度アクセスできるようにするにはどうすればよいですか?」を参照してください。

特定の VPC エンドポイントへのアクセスの制限

以下に、awsexamplebucket1 という特定のバケットに対するアクセスを ID が vpce-1a2b3c4d の VPC エンドポイントからのみに制限する Amazon S3 のバケットポリシーの例を示します。指定されたエンドポイントが使用されていない場合、ポリシーはバケットに対するすべてのアクセスを拒否します。aws:SourceVpce 条件はエンドポイントを指定します。aws:SourceVpce 条件では、VPC エンドポイントの ID のみが必要で、VPC エンドポイントのリソースの Amazon リソースネーム (ARN) は必要ありません。ポリシーで条件を使用する方法の詳細については、条件キーを使用したバケットポリシーの例 を参照してください。

> **Important**
>
> - 次のポリシーの例を使用する前に、VPC エンドポイントの ID をユースケースに応じた値に置き換えてください。そうしないと、バケットにアクセスできません。
> - このポリシーは、コンソールリクエストが指定の VPC エンドポイントを経由していない場合、指定先のバケットへのコンソールアクセスを無効にします。

```
{
   "Version": "2012-10-17",
   "Id": "Policy1415115909152",
   "Statement": [
     {
       "Sid": "Access-to-specific-VPCE-only",
       "Principal": "*",
       "Action": "s3:*",
       "Effect": "Deny",
       "Resource": ["arn:aws:s3:::awsexamplebucket1",
                    "arn:aws:s3:::awsexamplebucket1/*"],
       "Condition": {
         "StringNotEquals": {
           "aws:SourceVpce": "vpce-1a2b3c4d"
         }
       }
     }
   ]
}
```

特定の VPC へのアクセスの制限

aws:SourceVpc 条件を使用して、特定の VPC へのアクセスを制限するバケットポリシーを作成できます。これは、同じ VPC で複数の VPC エンドポイントを設定していて、すべてのエンドポイントで Amazon S3 のバケットへのアクセスを管理したい場合に便利です。以下は、VPC vpc-111bbb22 の外側から awsexamplebucket1 およびそのオブジェクトへのアクセスを拒否するポリシーの例です。指定された VPC が使用されていない場合、ポリシーはバケットに対するすべてのアクセスを拒否します。このステートメントは、バケットへのアクセス許可を付与しません。アクセス許可を付与するには、別の Allow ステートメントを追加する必要があります。vpc-111bbb22 条件キーでは、VPC リソースの ARN は不要で、VPC ID のみが必要です。

> **Important**
>
> - 次のポリシーの例を使用する前に、VPC の ID をユースケースに応じた値に置き換えてください。そうしないと、バケットにアクセスできません。
> - このポリシーは、コンソールリクエストが指定の VPC を経由していない場合、指定先のバケットへのコンソールアクセスを無効にします。

```
{
   "Version": "2012-10-17",
   "Id": "Policy1415115909153",
   "Statement": [
     {
       "Sid": "Access-to-specific-VPC-only",
       "Principal": "*",
       "Action": "s3:*",
       "Effect": "Deny",
       "Resource": ["arn:aws:s3:::awsexamplebucket1",
                    "arn:aws:s3:::awsexamplebucket1/*"],
       "Condition": {
         "StringNotEquals": {
           "aws:SourceVpc": "vpc-111bbb22"
         }
       }
     }
   ]
}
```

特定の IP または VPC に基づいてバケットへのアクセスを制限する方法については、AWS re:Post 情報センターの「特定の VPC エンドポイントまたは IP アドレスのみが Amazon S3 バケットにアクセスできるようにする方法を教えてください」を参照してください。

Amazon S3 バケットポリシーの例

Amazon S3 バケットポリシーを使用すると、バケット内のオブジェクトへのアクセスを保護して、適切な権限を持つユーザーだけがアクセスできるようにすることができます。適切な権限を持たない認証済みユーザーが Amazon S3 リソースにアクセスできないようにすることもできます。

このセクションでは、バケットポリシーの一般的なユースケース例を紹介します。これらのサンプルポリシーは、*amzn-s3-demo-bucket* をリソース値として使用します。これらのポリシーをテストするには、*user input placeholders* をお客様の情報 (バケット名など) と置き換えます。

オブジェクトのセットに対するアクセス許可を付与または拒否するために、Amazon リソースネーム (ARN) やその他の値でワイルドカード文字 (*) を使用できます。例えば、共通のプレフィックスで始まるか、.html などの特定の拡張子で終わるオブジェクトのグループへのアクセスをコントロールできます。

AWS Identity and Access Management (IAM) ポリシー言語については、「Amazon S3 のポリシーとアクセス許可」を参照してください。

S3 リソースタイプ別の S3 API オペレーションへのアクセス許可の詳細については、「Amazon S3 API オペレーションに必要なアクセス許可」を参照してください。

> **Note**
>
> Amazon S3 コンソールを使用して許可をテストするときには、コンソールに必要な `s3:ListAllMyBuckets`、`s3:GetBucketLocation`、`s3:ListBucket` を追加で付与する必要があります。コンソールを使用してユーザーにアクセス許可を付与してテストする例の解説については、「ユーザーポリシーを使用したバケットへのアクセスの制御」を参照してください。

バケットポリシーを作成するためのその他のリソースには、以下が含まれます。

- バケットポリシーの作成時に使用できる IAM ポリシーアクション、リソース、および条件キーの完全なリストについては、「サービス認可リファレンス」の「Actions, resources, and condition keys for Amazon S3」を参照してください。

- S3 リソースタイプ別の S3 API オペレーションへのアクセス許可の詳細については、「Amazon S3 API オペレーションに必要なアクセス許可」を参照してください。
- S3 ポリシーの作成に関するガイダンスについては、「Amazon S3 コンソールを使用したバケットポリシーの追加」を参照してください。
- ポリシーのエラーのトラブルシューティングを行うには、「Amazon S3 でのアクセス拒否 (403 Forbidden) エラーのトラブルシューティング」を参照してください。

ポリシーの追加または更新に問題がある場合は、AWS re:Post 情報センターの「Amazon S3 バケットポリシーを更新しようとする際、『Invalid principal in policy』というエラーが発生する理由を知りたいです」を参照してください。

トピック

- 任意の匿名ユーザーへの読み取り専用アクセス許可の付与
- 暗号化が必要
- 定型の ACL を使ったバケットの管理
- オブジェクトタグ付けによるオブジェクトアクセスの管理
- グローバル条件キーによるオブジェクトアクセスの管理
- HTTP または HTTPS リクエストに基づくアクセス管理
- 特定のフォルダへのユーザーアクセスの管理
- アクセスログへのアクセス管理
- Amazon CloudFront の OAI へのアクセス管理
- Amazon S3 ストレージレンズへのアクセス管理
- S3 インベントリ、S3 分析、および S3 インベントリレポートの権限管理
- MFA が必要
- ユーザーによるオブジェクトの削除を禁止する

任意の匿名ユーザーへの読み取り専用アクセス許可の付与

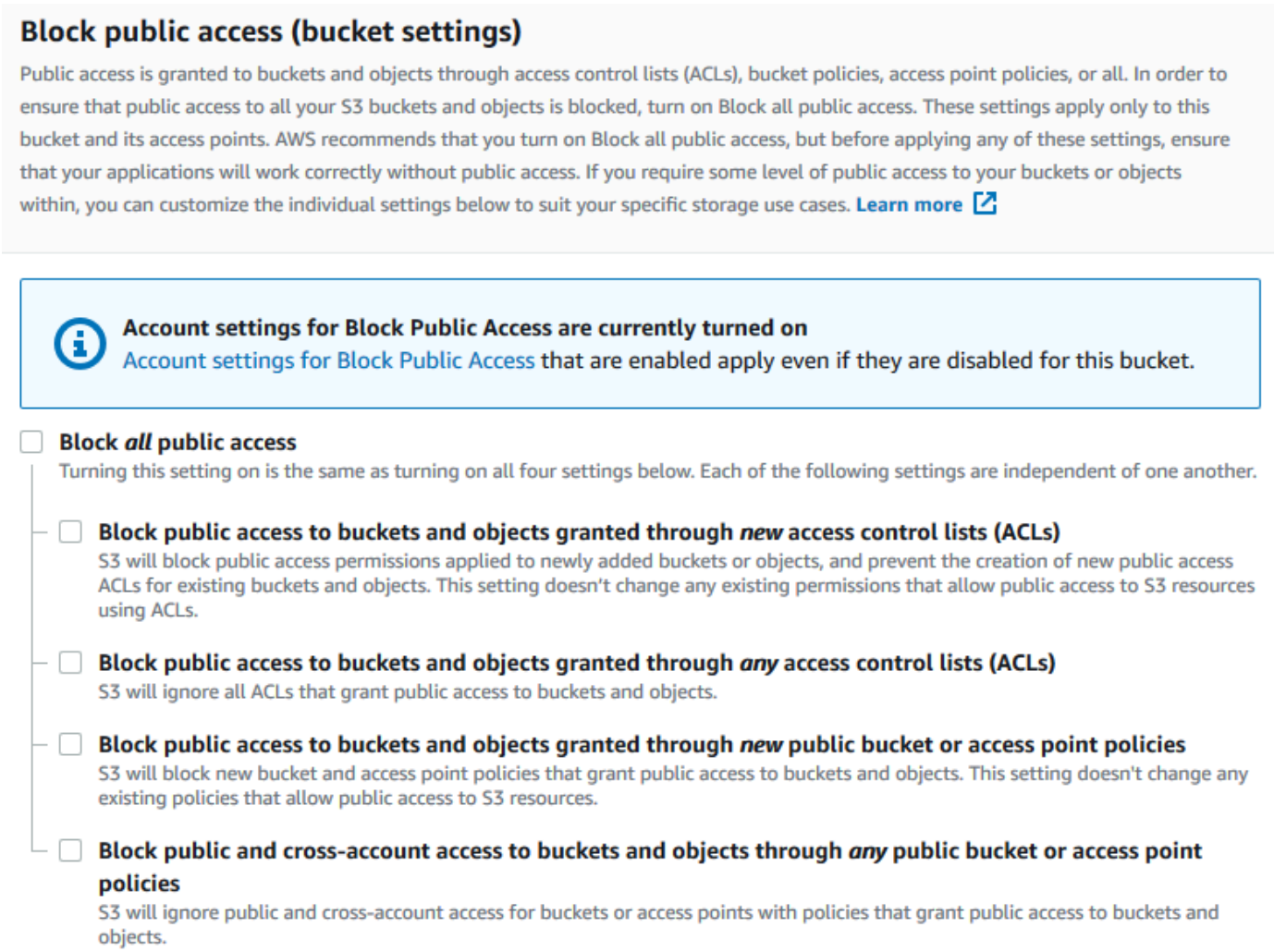
ポリシー設定を使用して、匿名のパブリックユーザーにアクセス許可を付与できます。これは、バケットを静的ウェブサイトとして設定する場合に便利です。匿名のパブリックユーザーにアクセス許可を付与するには、バケットのブロックパブリックアクセス設定を無効にする必要があります。これを行う方法と必要なポリシーの詳細については、「ウェブサイトアクセスのアクセス許可の設定」を参照してください。同じ目的でより制限の厳しいポリシーを設定する方法については、「AWS 情報

センター」の「Amazon S3 バケットの一部のオブジェクトにパブリック読み取りアクセス権を付与するにはどうすればよいですか?」を参照してください。

デフォルトでは、Amazon S3 はアカウントとバケットへのパブリックアクセスをブロックします。バケットを使用して静的ウェブサイトをホストする場合は、以下のステップを使用して、パブリックアクセスブロック設定を編集できます。

> **Warning**
>
> このステップを完了する前に「Amazon S3 ストレージへのパブリックアクセスのブロック」を読んで、パブリックアクセスを許可することに伴うリスクを理解し、了承してください。パブリックアクセスブロック設定をオフにしてバケットをパブリックにすると、インターネット上のだれでもバケットにアクセスできるようになります。バケットへのすべてのパブリックアクセスをブロックすることをお勧めします。

1. https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開きます。
2. 静的ウェブサイトとして設定されたバケットの名前を選択します。
3. [Permissions (アクセス許可)] を選択します。
4. [ブロックパブリックアクセス (バケット設定)] で [編集] を選択します。
5. [Block all public access (すべてのパブリックアクセスをブロックする)] をクリアし、[Save changes (変更の保存)] を選択します。



Amazon S3 で、バケットのブロックパブリックアクセス設定がオフになります。パブリックな静的ウェブサイトを作成するには、バケットポリシーを追加する前に、アカウントのブロックパブリックアクセス設定を編集する必要があります。アカウントのブロックパブリックアクセス設定が現在有効になっている場合は、[ブロックパブリックアクセス (バケット設定)] の下にメモが表示されます。

暗号化が必要

次の例に示すように、AWS Key Management Service (AWS KMS) キーによるサーバー側の暗号化 (SSE-KMS) を要求できます。

バケットに書き込まれるすべてのオブジェクトに SSE-KMS が必要

次のポリシー例では、バケットに書き込まれるすべてのオブジェクトを、AWS Key Management Service (AWS KMS) キーを使用したサーバー側の暗号化 (SSE-KMS) を使用して暗号化することを

要求しています。オブジェクトが SSE-KMS で暗号化されていない場合、リクエストは拒否されます。

```
{
"Version": "2012-10-17",
"Id": "PutObjPolicy",
"Statement": [{
  "Sid": "DenyObjectsThatAreNotSSEKMS",
  "Principal": "*",
  "Effect": "Deny",
  "Action": "s3:PutObject",
  "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
  "Condition": {
    "Null": {
      "s3:x-amz-server-side-encryption-aws-kms-key-id": "true"
    }
  }
}]
}
```

バケットに書き込まれるすべてのオブジェクトに特定の AWS KMS key を使用する SSE-KMS が必要

次のポリシー例では、特定の KMS キー ID を使用して SSE-KMS で暗号化されていないオブジェクトはバケットに書き込まれません。オブジェクトがリクエストごとのヘッダーまたはバケットのデフォルト暗号化を使用して SSE-KMS で暗号化されている場合でも、特定の KMS キーで暗号化されていないオブジェクトはバケットに書き込めません。この例で使用している KMS キー ARN を必ずお客様の KMS キー ARN に置き換えてください。

```
{
"Version": "2012-10-17",
"Id": "PutObjPolicy",
"Statement": [{
  "Sid": "DenyObjectsThatAreNotSSEKMSWithSpecificKey",
  "Principal": "*",
  "Effect": "Deny",
  "Action": "s3:PutObject",
  "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
  "Condition": {
    "ArnNotEqualsIfExists": {
      "s3:x-amz-server-side-encryption-aws-kms-key-id": "arn:aws:kms:us-
east-2:111122223333:key/01234567-89ab-cdef-0123-456789abcdef"
```

```
    }
  }
}]
}
```

定型の ACL を使ったバケットの管理

オブジェクトをアップロードしたり、パブリックアクセス用のオブジェクト ACL を設定したりする権限を複数のアカウントに付与する

以下のユーザーポリシーの例は、複数の AWS アカウント に `s3:PutObject` アクセス許可および `s3:PutObjectAcl` アクセス許可を付与します。また、このポリシーの例では、これらのオペレーションのリクエストには必ず `public-read` という既定のアクセスコントロールリスト (ACL) を含めることが求められています。詳細については、「Amazon S3 のポリシーアクション」および「Amazon S3 のポリシー条件キー」を参照してください。

> **Warning**
>
> `public-read` という既定の ACL を使用すると、バケット内のオブジェクトを世界中の誰でも見ることができます。Amazon S3 のバケットへの匿名アクセスを許可したり、パブリックアクセスブロック設定を無効にしたりする場合は注意が必要です。匿名アクセスを付与すると、世界中のすべてのユーザーがバケットにアクセスできます。静的なウェブサイトのホスティングなどで特に必要な場合を除いて、Amazon S3 のバケットへの匿名アクセスは許可しないことをお勧めします。静的ウェブサイトホスティングのパブリックアクセスをブロックする設定を有効にする場合は、「チュートリアル: Amazon S3 での静的ウェブサイトの設定」を参照してください。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AddPublicReadCannedAcl",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:root",
                    "arn:aws:iam::444455556666:root"
                ]
            },
```

```
            "Action": [
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": [
                        "public-read"
                    ]
                }
            }
        }
    ]
}
```

バケット所有者はフルコントロール権限を持ちながら、オブジェクトをアップロードするためのクロスアカウントアクセス許可を付与する

以下の例は、アップロードされたオブジェクトを完全に制御しながら、別の AWS アカウント がバケットにオブジェクトをアップロードできるようにする方法を示しています。このポリシーでは、特定の AWS アカウント (*111122223333*) に、アップロード時に bucket-owner-full-control の既定 ACL が含まれている場合にのみ、オブジェクトをアップロードする機能が付与されます。ポリシーの StringEquals 条件は、要件を表現する s3:x-amz-acl 条件キーを指定します。詳細については、「Amazon S3 のポリシー条件キー」を参照してください。

```
{
   "Version":"2012-10-17",
   "Statement":[
     {
       "Sid":"PolicyForAllowUploadWithACL",
       "Effect":"Allow",
       "Principal":{"AWS":"111122223333"},
       "Action":"s3:PutObject",
       "Resource":"arn:aws:s3:::amzn-s3-demo-bucket/*",
       "Condition": {
         "StringEquals": {"s3:x-amz-acl":"bucket-owner-full-control"}
       }
     }
   ]
}
```

オブジェクトタグ付けによるオブジェクトアクセスの管理

特定のタグキーと値を持つオブジェクトの読み取り権限のみをユーザーに許可する

以下のアクセス許可ポリシーでは、environment: production タグキーと値を持つオブジェクトのみを読み取れるように制限しています。このポリシーは s3:ExistingObjectTag 条件キーを使用してタグキーと値を指定します。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Principal":{
            "AWS":"arn:aws:iam::111122223333:role/JohnDoe"
         },
         "Effect":"Allow",
         "Action":[
            "s3:GetObject",
            "s3:GetObjectVersion"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket/*",
         "Condition":{
            "StringEquals":{
               "s3:ExistingObjectTag/environment":"production"
            }
         }
      }
   ]
}
```

ユーザーが追加できるオブジェクトタグキーを制限する

次のポリシーの例では、s3:PutObjectTagging アクションを実行するアクセス許可をユーザーに付与します (ユーザーが既存のオブジェクトにタグを追加することができます)。この条件は s3:RequestObjectTagKeys 条件キーを使用して、Owner や CreationDate などの許可されたタグキーを指定します。詳細については、「IAM ユーザーガイド」の「複数のキーの値をテストする条件の作成」を参照してください。

このポリシーは、リクエストで指定されたすべてのタグキーが承認されたタグキーであることを保証します。条件の ForAnyValue 修飾子によって、指定したキーの少なくとも 1 つがリクエストに存在することが保証されます。

```
{
   "Version": "2012-10-17",
  "Statement": [
    {"Principal":{"AWS":[
            "arn:aws:iam::111122223333:role/JohnDoe"
         ]
       },
 "Effect": "Allow",
      "Action": [
        "s3:PutObjectTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ],
      "Condition": {"ForAnyValue:StringEquals": {"s3:RequestObjectTagKeys": [
            "Owner",
            "CreationDate"
          ]
        }
      }
    }
  ]
}
```

ユーザーにオブジェクトタグの追加を許可する場合は特定のタグキーと値が必要

次のポリシーの例では、s3:PutObjectTagging アクションを実行するアクセス許可をユーザーに付与します (ユーザーが既存のオブジェクトにタグを追加することができます)。この条件により、値が *X* に設定された特定のタグキー (*Project* など) をユーザーが含めることが求められます。

```
{
   "Version": "2012-10-17",
  "Statement": [
    {"Principal":{"AWS":[
       "arn:aws:iam::111122223333:user/JohnDoe"
         ]
       },
      "Effect": "Allow",
      "Action": [
        "s3:PutObjectTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
```

```
      ],
      "Condition": {"StringEquals": {"s3:RequestObjectTag/Project": "X"
        }
      }
    }
  ]
}
```

特定のオブジェクトタグキーと値を持つオブジェクトのみを追加することをユーザーに許可する

次のポリシーの例では、s3:PutObject アクションを実行する権限をユーザーに付与して、ユーザーがバケットにオブジェクトを追加できるようにします。ただし、Condition ステートメントは、アップロードされたオブジェクトで使用できるタグキーと値を制限します。この例では、ユーザーがバケットに追加できるのは、値が *Finance* に設定された特定のタグキー (*Department*) を持つオブジェクトだけです。

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Principal":{
            "AWS":[
                 "arn:aws:iam::111122223333:user/JohnDoe"
         ]
        },
        "Effect": "Allow",
        "Action": [
            "s3:PutObject"
        ],
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket/*"
        ],
        "Condition": {
            "StringEquals": {
                "s3:RequestObjectTag/Department": "Finance"
            }
        }
    }]
}
```

グローバル条件キーによるオブジェクトアクセスの管理

グローバル条件キーは、aws プレフィックスが付いた条件キーです。AWS のサービス のサービスは、グローバル条件キーをサポートするか、サービスプレフィックスを含むサービス固有のキーを提供できます。JSON ポリシーの Condition 要素を使用して、リクエストのキーを、ポリシーで指定したキー値と比較できます。

Amazon S3 サーバーアクセスログ配信のみに制限する

次の例のバケットポリシーでは、aws:SourceArn グローバル条件キーを使用して、サービス間リクエストを行っているリソースの Amazon リソースネーム (ARN) を、ポリシーで指定した ARN と比較します。aws:SourceArn 条件キーを使用して、サービス間のトランザクション中に Amazon S3 サービスが混乱した代理として使用されるのを防ぐことができます。Amazon S3 バケットにオブジェクトを追加できるのは Amazon S3 サービスのみです。

この例のバケットポリシーは、ロギングサービスプリンシパル (s3:PutObject) にのみ logging.s3.amazonaws.com 許可を付与します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowPutObjectS3ServerAccessLogsPolicy",
            "Principal": {
                "Service": "logging.s3.amazonaws.com"
            },
            "Effect": "Allow",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket-logs/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111111111111"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:s3:::EXAMPLE-SOURCE-BUCKET"
                }
            }
        },
        {
            "Sid": "RestrictToS3ServerAccessLogs",
            "Effect": "Deny",
            "Principal": "*",
```

```
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket-logs/*",
            "Condition": {
                "ForAllValues:StringNotEquals": {
                    "aws:PrincipalServiceNamesList": "logging.s3.amazonaws.com"
                }
            }
        }
    ]
}
```

自分の組織にのみアクセスを許可

リソースにアクセスするすべての IAM プリンシパルが組織内の AWS アカウント (AWS Organizations管理アカウントを含む) からのアクセスのみに制限する場合は、aws:PrincipalOrgID グローバル条件キーを使用できます。

このタイプのアクセスを許可または制限するには、aws:PrincipalOrgID 条件を定義し、バケットポリシーの組織 ID に値を設定します。組織 ID は、バケットへのアクセスを制御するために使用されます。aws:PrincipalOrgID 条件を使用すると、バケットポリシーのアクセス許可は、組織に追加されるすべての新しいアカウントにも適用されます。

以下は、組織内の特定の IAM プリンシパルにバケットへの直接アクセス許可を付与できるリソースベースのバケットポリシーの例です。バケットポリシーに aws:PrincipalOrgID グローバル条件キーを追加すると、リソースにアクセスするにはプリンシパルアカウントが組織内に存在する必要があります。アクセスを許可するときに誤って間違ったアカウントを指定した場合でも、aws:PrincipalOrgID グローバル条件キーは追加の保護手段として機能します。このグローバルキーをポリシーで使用すると、指定した組織以外のすべてのプリンシパルが、Amazon S3 バケットにアクセスできないようにします。リソースへのアクセス権を取得できるのは、リストにある組織のアカウントのプリンシパルだけです。

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "AllowGetObject",
        "Principal": {
            "AWS": "*"
        },
        "Effect": "Allow",
        "Action": "s3:GetObject",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
```

```
        "Condition": {
            "StringEquals": {
                "aws:PrincipalOrgID": ["o-aa111bb222"]
            }
        }
    }]
}
```

HTTP または HTTPS リクエストに基づくアクセス管理

HTTPS リクエストのみにアクセスを制限

潜在的な攻撃者がネットワークトラフィックを操作するのを防ぎたい場合は、HTTPS (TLS) を使用して暗号化された接続のみを許可し、HTTP リクエストによるバケットへのアクセスを制限できます。リクエストが HTTP か HTTPS かを判断するには、S3 バケットポリシーの aws:SecureTransport グローバル条件キーを使用します。aws:SecureTransport 条件キーは、リクエストが HTTP を使用して送信されたかどうかをチェックします。

リクエストが true を返した場合、リクエストは HTTPS 経由の送信です。リクエストが false を返した場合、リクエストは HTTP 経由の送信です。その後、目的のリクエストスキームに基づいてバケットへのアクセスを許可または拒否することができます。

次の例で、バケットポリシーは HTTP リクエストを明示的に拒否しています。

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "RestrictToTLSRequestsOnly",
        "Action": "s3:*",
        "Effect": "Deny",
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket",
            "arn:aws:s3:::amzn-s3-demo-bucket/*"
        ],
        "Condition": {
            "Bool": {
                "aws:SecureTransport": "false"
            }
        },
        "Principal": "*"
    }]
}
```

特定の HTTP Referer へのアクセスの制限

amzn-s3-demo-bucket というバケットに格納されている写真や動画へのリンクがある *www.example.com* または *example.com* というドメイン名のウェブサイトがあるとします。デフォルトでは、Amazon S3 のすべてのリソースはプライベートであるため、リソースを作成した AWS アカウント のみがアクセスできます。

これらのオブジェクトへのウェブサイトの読み取りアクセスを許可するには、s3:GetObject アクセス許可を条件付きで付与するバケットポリシーを追加する方法があります。条件としては、GET リクエストが特定のウェブページから発生する必要があることを指定します。次のポリシーでは、aws:Referer 条件キー付きの StringLike 条件を使用してリクエストを制限します。

```
{
  "Version":"2012-10-17",
  "Id":"HTTP referer policy example",
  "Statement":[
    {
      "Sid":"Allow only GET requests originating from www.example.com and
 example.com.",
      "Effect":"Allow",
      "Principal":"*",
      "Action":["s3:GetObject","s3:GetObjectVersion"],
      "Resource":"arn:aws:s3:::amzn-s3-demo-bucket/*",
      "Condition":{
        "StringLike":{"aws:Referer":["http://www.example.com/*","http://example.com/
*"]}
      }
    }
  ]
}
```

使用するブラウザのリクエストに HTTP referer ヘッダーが含まれていることを確認します。

> **Warning**
>
> aws:Referer 条件キーを使用するときには、十分な注意が必要です。一般に知られている HTTP 参照子のヘッダー値を含めるのは危険です。認可されていない当事者は、変更されたブラウザまたはカスタムブラウザを使用して任意の aws:Referer 値を提供することができます。したがって、無許可の当事者が AWS リクエストを直接作成できないよう、aws:Referer を使用しないでください。

この aws:Referer 条件キーは、Amazon S3 に保存されているコンテンツなどのデジタルコンテンツが、無許可のサードパーティーサイトで参照されないよう保護する目的でのみ、お客様に提供されています。詳細については、IAM ユーザーガイドaws:Refererの を参照してください。

特定のフォルダへのユーザーアクセスの管理

特定のフォルダへのアクセス許可をユーザーに付与

特定のフォルダへのアクセスをユーザーに許可しようとしているとします。IAM ユーザーと S3 バケットが同じ AWS アカウント に属している場合は、IAM ポリシーを使用してユーザーに特定のバケットフォルダへのアクセス許可を付与できます。このアプローチを使用すると、バケットポリシーを更新してアクセスを付与する必要はありません。複数のユーザーが切り替えることができる IAM ロールに IAM ポリシーを追加できます。

IAM ID と S3 バケットの AWS アカウント が異なる場合は、IAM ポリシーとバケットポリシーの両方でクロスアカウントアクセスを許可する必要があります。クロスアカウントアクセスを付与する方法の詳細については、「バケット所有者がクロスアカウントのバケットのアクセス許可を付与する」を参照してください。

次のバケットポリシーの例では、自分のフォルダ (home/*JohnDoe*/) のみに*JohnDoe* のフルコンソールアクセスを許可しています。home フォルダを作成し、ユーザーに適切なアクセス許可を付与することで、複数のユーザーが 1 つのバケットを共有できます。このポリシーは、次の 3 つの Allow ステートメントで構成されています。

- *AllowRootAndHomeListingOfCompanyBucket*: ユーザー (*JohnDoe*) が *amzn-s3-demo-bucket* バケットのルートレベルと home フォルダ内のオブジェクトを一覧表示できるようにします。このステートメントにより、ユーザーはコンソールを使用してプレフィックス home/ を検索することもできます。
- *AllowListingOfUserFolder*: ユーザー (*JohnDoe*) が home/*JohnDoe*/ フォルダとサブフォルダ内のすべてのオブジェクトを一覧表示できるようにします。
- *AllowAllS3ActionsInUserFolder*: Read、Write、Delete 権限を付与することで、ユーザーが Amazon S3 のすべてのアクションを実行できるようにします。権限はバケット所有者のホームフォルダに限定されます。

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "AllowRootAndHomeListingOfCompanyBucket",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:user/JohnDoe"
                ]
            },
            "Effect": "Allow",
            "Action": ["s3:ListBucket"],
            "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket"],
            "Condition": {
                "StringEquals": {
                    "s3:prefix": ["", "home/", "home/JohnDoe"],
                    "s3:delimiter": ["/"]
                }
            }
        },
        {
            "Sid": "AllowListingOfUserFolder",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:user/JohnDoe"
                ]
            },
            "Action": ["s3:ListBucket"],
            "Effect": "Allow",
            "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket"],
            "Condition": {
                "StringLike": {
                    "s3:prefix": ["home/JohnDoe/*"]
                }
            }
        },
        {
            "Sid": "AllowAllS3ActionsInUserFolder",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:user/JohnDoe"
                ]
            },
            "Action": ["s3:*"],
            "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket/home/JohnDoe/*"]
```

```
        }
    ]
}
```

アクセスログへのアクセス管理

アクセスログを有効にするためのアクセス権限を Application Load Balancer に付与

Application Load Balancer のアクセスログを有効にする場合は、ロードバランサーがログを保存する S3 バケットの名前を指定する必要があります。このバケットは、バケットにアクセスログを書き込む許可を Elastic Load Balancing に付与するアタッチされたポリシーが必要です。

次の例では、バケットポリシーにより、バケットにアクセスログを書き込む許可を Elastic Load Balancing (ELB) に付与しています。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Principal": {
        "AWS": "arn:aws:iam::elb-account-id:root"
      },
      "Effect": "Allow",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/111122223333/*"
    }
  ]
}
```

> **Note**
>
> 必ず、*elb-account-id* を、ご利用の AWS リージョン における Elastic Load Balancing の AWS アカウント ID に置き換えてください。Elastic Load Balancing リージョンのリストについては、「Elastic Load Balancing ユーザーガイド」の「Amazon S3 バケットにポリシーをアタッチする」を参照してください。

ご利用の AWS リージョン がサポートされている Elastic Load Balancing リージョンのリストに表示されない場合は、次のポリシーを使用して、指定されたログ配信サービスにアクセス許可を付与します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
       "Principal": {
         "Service": "logdelivery.elasticloadbalancing.amazonaws.com"
          },
      "Effect": "Allow",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/111122223333/*"
    }
  ]
}
```

次に、必ず Elastic Load Balancing のアクセスログを有効にして設定してください。テストファイルを作成することで、バケットのアクセス許可を確認できます。

Amazon CloudFront の OAI へのアクセス管理

Amazon CloudFront の OAI へのアクセス許可の付与

次のバケットポリシーの例は、CloudFront のオリジンアクセスアイデンティティ (OAI) に S3 のバケット内のすべてのオブジェクトを取得 (読み取り) するアクセス許可を付与します。CloudFront の OAI を使用すると、バケット内のオブジェクトへの CloudFront からのアクセスは許可して、Amazon S3 からの直接アクセスは許可しないようにすることができます。詳細については、「Amazon CloudFront デベロッパーガイド」の「オリジンアクセス ID を使用して Amazon S3 コンテンツへのアクセスを制限する」を参照してください。

次のポリシーは、OAI の ID をポリシーの `Principal` として使用します。S3 のバケットポリシーを使用して CloudFront の OAI にアクセス許可を付与する方法の詳細については、「Amazon CloudFront デベロッパーガイド」の「オリジンアクセスアイデンティティ (OAI) からオリジンアクセスコントロール (OAC) への移行」を参照してください。

この例を使用するには:

- *EH1HDMB1FH2TC* を OAI の ID に置き換えます。OAI の ID を確認するには、CloudFront コンソールのオリジンアクセスアイデンティティページを参照するか、CloudFront API の ListCloudFrontOriginAccessIdentities を使用します。
- *amzn-s3-demo-bucket* をバケットの名前に置き換えます。

```
{
    "Version": "2012-10-17",
    "Id": "PolicyForCloudFrontPrivateContent",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access
 Identity EH1HDMB1FH2TC"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
        }
    ]
}
```

Amazon S3 ストレージレンズへのアクセス管理

Amazon S3 ストレージレンズへのアクセス許可の付与

S3 ストレージレンズはメトリクスを集約し、Amazon S3 コンソールの [Buckets] (バケット) ページの [Account snapshot] (アカウントスナップショット) セクションにこの情報を表示します。S3 Storage Lens は、インサイトと傾向を可視化したり、外れ値にフラグ付けしたり、ストレージコストの最適化やデータ保護のベストプラクティスの適用に関するレコメンデーション事項を受け取ったりするために使用できるインタラクティブダッシュボードも提供します。ダッシュボードには、組織、アカウント、AWS リージョン、ストレージクラス、バケット、プレフィックス、またはストレージレンズのグループレベルでインサイトを生成して可視化できる、ドリルダウンオプションが用意されています。1 日 1 回のメトリクスのエクスポートを CSV 形式または Parquet 形式で S3 バケットに送信することもできます。

S3 ストレージレンズは、収集したストレージ使用量のメトリクスをさらなる分析のため Amazon S3 バケット内にエクスポートできます。S3 Storage Lens がメトリクスのエクスポートを配置するバケットは、送信先バケットとして知られています。S3 Storage Lens のメトリクスエクスポートを設定するとき、ターゲットバケットにバケットポリシーを作成する必要があります。詳細については、「Amazon S3 ストレージレンズを使用してストレージのアクティビティと使用状況を評価する」を参照してください。

次のバケットポリシーの例では、Amazon S3 が送信先バケットにオブジェクトを書き込む (PUT リクエスト) ためのアクセス許可が付与されます。S3 Storage Lens メトリクスのエクスポートを設定するときには、このようなバケットポリシーを送信先バケットに使用します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3StorageLensExamplePolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "storage-lens.s3.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-destination-bucket/destination-prefix/
StorageLens/111122223333/*"
            ],
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceAccount": "111122223333",
                    "aws:SourceArn": "arn:aws:s3:region-code:111122223333:storage-
lens/storage-lens-dashboard-configuration-id"
                }
            }
        }
    ]
}
```

S3 ストレージレンズの組織レベルのメトリクスエクスポートを設定するときには、前述のバケットポリシーの Resource ステートメントに次の変更を加えます。

```
"Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/destination-prefix/
StorageLens/your-organization-id/*",
```

S3 インベントリ、S3 分析、および S3 インベントリレポートの権限管理

S3 インベントリおよび S3 分析に対するアクセス許可の付与

S3 インベントリでは、バケット内のオブジェクトのリストが作成され、S3 分析の工クスポートでは、分析に使用されるデータの出力ファイルが作成されます。インベントリによってオブジェクトがリストされるバケットは、ソースバケットと呼ばれます。インベントリファイルと、分析工クスポートファイルが書き込まれるバケットは、ターゲットバケットと呼ばれます。インベントリまたは分析

のエクスポートを設定する場合、ターゲットバケットにバケットポリシーを作成する必要があります。詳細については、「S3 インベントリを使用したデータのカタログ化と分析」および「Amazon S3 分析 – ストレージクラス分析」を参照してください。

次のバケットポリシーの例では、ソースバケットのアカウントからターゲットバケットにオブジェクトを書き込む (PUT リクエスト) ための Amazon S3 のアクセス許可が付与されます。このようなバケットポリシーは、S3 インベントリと S3 分析エクスポートをセットアップするときに、宛先バケットで使用します。

```
{
      "Version": "2012-10-17",
      "Statement": [
        {
            "Sid": "InventoryAndAnalyticsExamplePolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET/*"
            ],
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:s3:::DOC-EXAMPLE-SOURCE-BUCKET"
                },
                "StringEquals": {
                    "aws:SourceAccount": "111122223333",
                    "s3:x-amz-acl": "bucket-owner-full-control"
                }
            }
        }
    ]
}
```

S3 インベントリレポート設定の作成を制御する

S3 インベントリを使用したデータのカタログ化と分析 は、S3 バケット内のオブジェクトのリストと、各オブジェクトのメタデータを作成します。s3:PutInventoryConfiguration アクセス許可により、ユーザーはデフォルトで使用可能なすべてのオブジェクトメタデータフィールドを含むインベント設定を作成し、インベントリを保存する宛先バケットを指定できます。宛先バケット内のオブジェクトへの読み取りアクセスを持つユーザーは、インベントリレポートで使用可能なすべてのオ

ブジェクトメタデータフィールドにアクセスできます。S3 Inventory で使用できるメタデータフィールドの詳細については、「Amazon S3 インベントリのリスト」を参照してください。

S3 インベントリレポートをユーザーが設定できないようにするには、ユーザーから `s3:PutInventoryConfiguration` アクセス許可を削除します。

S3 インベントリレポート設定の一部のオブジェクトメタデータフィールドはオプションです。つまり、デフォルトで使用できますが、ユーザーに`s3:PutInventoryConfiguration` アクセス許可を付与すると制限できます。`s3:InventoryAccessibleOptionalFields` 条件キーを使用して、ユーザーがこれらのオプションのメタデータフィールドをレポートに含めることができるかどうかを制御できます。S3 インベントリで使用できるオプションのメタデータフィールドのリストについては、「Amazon Simple Storage Service API リファレンス」の「OptionalFields」を参照してください。

特定のオプションのメタデータフィールドを使用してインベントリ設定を作成するアクセス許可をユーザーに付与するには、`s3:InventoryAccessibleOptionalFields` 条件キーを使用してバケットポリシーの条件を絞り込みます。

次のポリシー例では、インベントリ設定を条件付きで作成するアクセス許可をユーザー (*Ana*) に付与します。ポリシーの `ForAllValues:StringEquals`条件は、`s3:InventoryAccessibleOptionalFields`条件キーを使用して、許可される 2 つのオプションのメタデータフィールド、つまり `Size` と `StorageClass` を指定します。したがって、*Ana* がインベントリ設定を作成するとき、含めることができるオプションのメタデータフィールドは `Size` と `StorageClass` のみです。

```
{
 "Id": "InventoryConfigPolicy",
 "Version": "2012-10-17",
 "Statement": [{
   "Sid": "AllowInventoryCreationConditionally",
   "Effect": "Allow",
   "Principal": {
    "AWS": "arn:aws:iam::111122223333:user/Ana"
   },
   "Action":
    "s3:PutInventoryConfiguration",
   "Resource":
    "arn:aws:s3:::DOC-EXAMPLE-SOURCE-BUCKET",
   "Condition": {
    "ForAllValues:StringEquals": {
     "s3:InventoryAccessibleOptionalFields": [
```

```
        "Size",
        "StorageClass"
        ]
      }
    }
   }
 ]
}
```

特定のオプションのメタデータフィールドを含む S3 インベントリレポートをユーザーが設定できないようにするには、レプリケート元バケットのバケットポリシーに明示的な Deny ステートメントを追加します。次のバケットポリシーの例では、オプションの ObjectAccessControlList または ObjectOwner メタデータフィールドを含むインベントリ設定をソースバケット *DOC-EXAMPLE-SOURCE-BUCKET* に作成することをユーザー *Ana* に拒否します。ユーザー*Ana* は、他のオプションのメタデータフィールドを使用してインベントリ設定を作成できます。

```
{
 "Id": "InventoryConfigSomeFields",
 "Version": "2012-10-17",
 "Statement": [{
   "Sid": "AllowInventoryCreation",
   "Effect": "Allow",
   "Principal": {
    "AWS": "arn:aws:iam::111122223333:user/Ana"
   },
   "Action": "s3:PutInventoryConfiguration",
   "Resource":
    "arn:aws:s3:::DOC-EXAMPLE-SOURCE-BUCKET",

  },
  {
   "Sid": "DenyCertainInventoryFieldCreation",
   "Effect": "Deny",
   "Principal": {
    "AWS": "arn:aws:iam::111122223333:user/Ana"
   },
   "Action": "s3:PutInventoryConfiguration",
   "Resource":
     "arn:aws:s3:::DOC-EXAMPLE-SOURCE-BUCKET",
   "Condition": {
    "ForAnyValue:StringEquals": {
     "s3:InventoryAccessibleOptionalFields": [
```

```
        "ObjectOwner",
        "ObjectAccessControlList"
        ]
      }
    }
   }
 ]
}
```

> **Note**
>
> バケットポリシーで s3:InventoryAccessibleOptionalFields 条件キーを使用しても、既存のインベントリ設定に基づくインベントリレポートのデリバリーには影響しません。

> **Important**
>
> 前の例に示すように、Allow 効果で ForAllValues を、または Deny 効果で ForAnyValue を使用することをお勧めします。
> これらの組み合わせは過度に制限され、インベントリ設定の削除がブロックされる可能性があるため、Deny 効果で ForAllValues または Allow 効果で ForAnyValue を使用しないでください。
> ForAllValues および ForAnyValue 条件セット演算子の詳細については、「IAM ユーザーガイド」「複数値のコンテキストキー」を参照してください。

MFA が必要

Amazon S3 は、多エレメント認証 (MFA) で保護された API へのアクセスをサポートしています。この機能により、Amazon S3 のリソースへのアクセスに MFA を強制的に適用することができます。多エレメント認証により、AWS 環境に適用できるセキュリティのレベルが高まります。MFA は、有効な MFA コードを入力して MFA デバイスを物理的に所有していることを証明することがユーザーに要求されるセキュリティ機能です。詳細については、AWS 多エレメント認証 を参照してください。Amazon S3 のリソースにアクセスするすべてのリクエストに対して MFA を要求することができます。

MFA の要件を適用するには、バケットポリシーで aws:MultiFactorAuthAge 条件キーを使用します。IAM ユーザーは、AWS Security Token Service (AWS STS) により発行される一時的な認証情

報を使用して、Amazon S3 のリソースにアクセスできます。AWS STS リクエスト時に、MFA コードを指定します。

Amazon S3 が多要素認証のリクエストを受け取ると、aws:MultiFactorAuthAge 条件キーに一時的な認証情報が作成されてからの時間の数値 (秒) が示されます。リクエストで提供された一時的な認証情報が MFA デバイスを使用して作成されていない場合、このキー値は null (不在) になります。次の例に示すように、バケットポリシーに、この値を確認する条件を追加できます。

このポリシー例は、リクエストが MFA を使用して認証されていない場合、*amzn-s3-demo-bucket* バケットの */taxdocuments* フォルダに対するすべての Amazon S3 オペレーションを拒否します。MFA の詳細については、IAM ユーザーガイドAWSの での多エレメント認証 (MFA) の使用を参照してください。

```
{
    "Version": "2012-10-17",
    "Id": "123",
    "Statement": [
      {
        "Sid": "",
        "Effect": "Deny",
        "Principal": "*",
        "Action": "s3:*",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/taxdocuments/*",
        "Condition": { "Null": { "aws:MultiFactorAuthAge": true }}
      }
    ]
 }
```

aws:MultiFactorAuthAge 条件キー値が null で、リクエスト内の一時的なセキュリティ認証情報が MFA デバイスを使用せずに作成されたことを示している場合、Condition ブロック内の Null 条件の評価は true になります。

次のバケットポリシーは、前述のバケットポリシーの拡張です。次のポリシーには、2 つのポリシーステートメントが含まれています。1 つのステートメントは、バケット (*amzn-s3-demo-bucket*) の s3:GetObject アクセス許可を全員に付与します。もう 1 つのステートメントは、MFA を要求することにより、バケットの *amzn-s3-demo-bucket/taxdocuments* フォルダへのアクセスを制限します。

```
{
    "Version": "2012-10-17",
```

```
    "Id": "123",
    "Statement": [
      {
        "Sid": "",
        "Effect": "Deny",
        "Principal": "*",
        "Action": "s3:*",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/taxdocuments/*",
        "Condition": { "Null": { "aws:MultiFactorAuthAge": true } }
      },
      {
        "Sid": "",
        "Effect": "Allow",
        "Principal": "*",
        "Action": ["s3:GetObject"],
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
      }
    ]
}
```

オプションで、aws:MultiFactorAuthAge キーの有効期間を制限する数値条件を使用することができます。aws:MultiFactorAuthAge キーで指定する期間は、リクエストの認証に使われる一時的セキュリティ認証情報の寿命とは無関係です。

例えば、次のバケットポリシーでは、MFA 認証を要求するほかに、一時セッションが作成されてからの時間もチェックします。このポリシーは、aws:MultiFactorAuthAge キーの値が、一時セッションが 1 時間 (3,600 秒) 以上前に作成されたことを示す場合に、すべてのオペレーションを拒否します。

```
{
    "Version": "2012-10-17",
    "Id": "123",
    "Statement": [
      {
        "Sid": "",
        "Effect": "Deny",
        "Principal": "*",
        "Action": "s3:*",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/taxdocuments/*",
        "Condition": {"Null": {"aws:MultiFactorAuthAge": true }}
      },
      {
        "Sid": "",
```

```
        "Effect": "Deny",
        "Principal": "*",
        "Action": "s3:*",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/taxdocuments/*",
        "Condition": {"NumericGreaterThan": {"aws:MultiFactorAuthAge": 3600 }}
      },
      {
        "Sid": "",
        "Effect": "Allow",
        "Principal": "*",
        "Action": ["s3:GetObject"],
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
      }
    ]
}
```

ユーザーによるオブジェクトの削除を禁止する

デフォルトでは、ユーザーには一切のアクセス許可がありません。ただし、ポリシーを作成する際に、意図しないアクセス許可をユーザーに付与する可能性があります。このようなアクセス許可の抜け穴を防ぐには、明示的な拒否を追加して、より厳格なアクセスポリシーを記述する必要があります。

ユーザーまたはアカウントによるオブジェクトの削除を明示的に防ぐには、バケットポリシーに s3:DeleteObject、s3:DeleteObjectVersion、および s3:PutLifecycleConfiguration のアクションのアクセス許可を追加する必要があります。オブジェクトの削除は、明示的に DELETE Object API オペレーションを呼び出すか、有効期限が過ぎたオブジェクトを Amazon S3 が削除できるようにオブジェクトのライフサイクルを設定 (「オブジェクトのライフサイクルの管理」を参照) することで可能であるため、これらすべてのアクションが必要です。

次の例は、ユーザー *MaryMajor* の DELETE Object アクセス許可を明示的に拒否します。明示的な Deny ステートメントは、付与されている他のどのアクセス許可よりも常に優先されます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "statement1",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/MaryMajor"
      },
```

```
      "Action": [
        "s3:GetObjectVersion",
        "s3:GetBucketAcl"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket1",
   "arn:aws:s3:::amzn-s3-demo-bucket1/*"
      ]
    },
    {
      "Sid": "statement2",
      "Effect": "Deny",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/MaryMajor"
      },
      "Action": [
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket1",
     "arn:aws:s3:::amzn-s3-demo-bucket1/*"
      ]
    }
  ]
}
```

条件キーを使用したバケットポリシーの例

アクセスポリシー言語を使用して、アクセス許可を付与するときに条件を指定できます。オプションの Condition 要素、または Condition ブロックを使用して、ポリシーが有効になるときの条件を指定できます。

オブジェクトおよびバケットオペレーションに Amazon S3 条件キーを使用するポリシーについては、次の例を参照してください。条件キーの詳細については、Amazon S3 のポリシー条件キー を参照してください。Amazon S3 アクションの完全なリストとポリシーで指定できるリソースについては、「サービス認可リファレンス」の「Actions, resources, and condition keys for Amazon S3」を参照してください。

S3 リソースタイプ別の S3 API オペレーションへのアクセス許可の詳細については、「Amazon S3 API オペレーションに必要なアクセス許可」を参照してください。

例: オブジェクトオペレーションで使用できる Amazon S3 の条件キー

以下の例は、オブジェクトオペレーションに Amazon S3 固有の条件キーを使用する方法を示しています。Amazon S3 アクションの完全なリストとポリシーで指定できるリソースについては、「サービス認可リファレンス」の「Actions, resources, and condition keys for Amazon S3」を参照してください。

S3 リソースタイプ別の S3 API オペレーションへのアクセス許可の詳細については、「Amazon S3 API オペレーションに必要なアクセス許可」を参照してください。

ここでは、PutObject オペレーションで条件キーを使用するポリシーの例をいくつか示します。PutObject オペレーションでは、アクセスコントロールリスト (ACL) に固有のヘッダーを使用して、ACL に基づいてアクセス許可を付与することができます。これらの条件キーを使用することで、条件を設定し、ユーザーがオブジェクトをアップロードする場合に特定のアクセス許可を要求することができます。また、PutObjectAcl オペレーションを使用して ACL に基づいてアクセス許可を付与することもできます。詳細については、Amazon S3 Amazon Simple Storage Service API リファレンスの PutObjectAcl を参照してください。ACL の詳細については、アクセスコントロールリスト (ACL) の概要 を参照してください。

トピック

- 例 1: サーバー側の暗号化を使用してオブジェクトを保存するよう要求する s3:PutObject のアクセス許可を付与する
- 例 2: 制限されているコピー元からオブジェクトをコピーする s3:PutObject のアクセス許可を付与する
- 例 3: オブジェクトの特定のバージョンに対するアクセス許可を付与する
- 例 4: オブジェクトタグに基づくアクセス許可の付与
- 例 5: バケット所有者の AWS アカウント ID によるアクセスの制限
- 例 6: 最小の TLS バージョンの要求
- 例 7: Deny ステートメントから特定のプリンシパルを除外する
- 例 8: オブジェクトキー名または ETags に基づいた、クライアントへの条件付きオブジェクトアップロードの強制

例 1: サーバー側の暗号化を使用してオブジェクトを保存するよう要求する **`s3:PutObject`** のアクセス許可を付与する

アカウント A がバケットの所有者であるとします。アカウント管理者がアカウント A のユーザーの Jane にオブジェクトをアップロードするアクセス許可を付与するとします。ただし、Jane が

必ず Amazon S3 マネージドキーを使用したサーバー側の暗号化 (SSE-S3) をリクエストすることを条件とします。この場合、アカウント A の管理者は、以下のように s3:x-amz-server-side-encryption 条件キーを使用することで、この要件を指定できます。次の Condition ブロックのキーと値のペアは、暗号化タイプとして s3:x-amz-server-side-encryption 条件キーと SSE-S3 (AES256) を指定します。

```
"Condition": {
     "StringNotEquals": {
         "s3:x-amz-server-side-encryption": "AES256"
     }}
```

AWS CLI を使用してこのアクセス許可をテストする場合、次の例に示すように、--server-side-encryption パラメータを使用して必要な暗号化を追加する必要があります。このコマンド例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key HappyFace.jpg --body c:
\HappyFace.jpg --server-side-encryption "AES256" --profile AccountAadmin
```

例 2: 制限されているコピー元からオブジェクトをコピーする **s3:PutObject** のアクセス許可を付与する

PUT のオブジェクトリクエストでは、ソースオブジェクトを指定すると、リクエストはコピーオペレーションです (「CopyObject」を参照)。バケット所有者は、これに対応して、ソースに制限が付いているオブジェクトをコピーするためのアクセス許可をユーザーに付与できます。以下に例を示します。

- 指定したソースバケット (例: *amzn-s3-demo-source-bucket*) からのみオブジェクトをコピーすることを許可します。
- 指定したソースバケットから、キー名のプレフィックスが *public/* など特定のプレフィックス (例: *amzn-s3-demo-source-bucket/public/**) で始まるオブジェクトのみコピーすることを許可します。
- ソースバケット (例: *amzn-s3-demo-source-bucket/example.jpg*) から特定のオブジェクトのみをコピーすることを許可します。

次のバケットポリシーでは、ユーザー (*Dave*) に s3:PutObject のアクセス許可が付与されます。このポリシーでは、リクエストに s3:x-amz-copy-source ヘッダーを含め、ヘッダーの値でキー名のプレフィックスに */amzn-s3-demo-source-bucket/public/** を指定している

場合にのみ、オブジェクトをコピーできます。このポリシーの例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
{
    "Version": "2012-10-17",
    "Statement": [
       {
            "Sid": "cross-account permission to user in your own account",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:user/Dave"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
        },
        {
            "Sid": "Deny your user permission to upload object if copy source is not /
bucket/prefix",
            "Effect": "Deny",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:user/Dave"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-source-bucket/*",
            "Condition": {
                "StringNotLike": {
                    "s3:x-amz-copy-source": "amzn-s3-demo-source-bucket/public/*"
                }
            }
        }
    ]
}
```

AWS CLI でポリシーをテストする

AWS CLI の copy-object コマンドを使用して、アクセス許可をテストできます。--copy-source パラメータを追加してソースを指定します。キー名のプレフィックスは、ポリシーで許可されているプレフィックスと一致する必要があります。--profile パラメータを使用して、ユーザー Dave の認証情報を指定します。AWS CLI の設定の詳細については、「Amazon S3 API リファレンス」の「Developing with Amazon S3 using the AWS CLI」を参照してください。

```
aws s3api copy-object --bucket amzn-s3-demo-source-bucket --key HappyFace.jpg
```

```
--copy-source amzn-s3-demo-source-bucket/public/PublicHappyFace1.jpg --
profile AccountADave
```

特定のオブジェクトのみをコピーするアクセス許可を付与する

前述のポリシーでは、StringNotLike 条件を使用しています。次に示すとおり、特定のオブジェクトのみをコピーするアクセス許可を付与するには、条件を StringNotLike から StringNotEquals に変更し、オブジェクトキーを正確に指定する必要があります。このコマンド例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
"Condition": {
       "StringNotEquals": {
           "s3:x-amz-copy-source": "amzn-s3-demo-source-bucket/public/
PublicHappyFace1.jpg"
       }
}
```

例 3: オブジェクトの特定のバージョンに対するアクセス許可を付与する

アカウント A が、バージョニングが有効なバケットを所有しているとします。このバケットには、*HappyFace.jpg* オブジェクトのバージョンが複数含まれています。アカウント A の管理者は、ユーザー *Dave* にオブジェクトの特定のバージョンのみを取得できるアクセス許可を付与したいと考えています。この場合、アカウント管理者は、次に示すように、条件を付けてユーザー *Dave* に s3:GetObjectVersion のアクセス許可を付与できます。Condition ブロックのキーと値のペアは、s3:VersionId 条件キーを指定します。この場合、指定したバージョニングが有効なバケットからオブジェクトを取得するには、*Dave* は正確なオブジェクトバージョン ID を知る必要があります。このポリシーの例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

詳細については、「Amazon Simple Storage Service API リファレンス」の「GetObject」を参照してください。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "statement1",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:user/Dave"
```

```
            },
            "Action": "s3:GetObjectVersion",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/HappyFace.jpg"
        },
        {
            "Sid": "statement2",
            "Effect": "Deny",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:user/Dave"
            },
            "Action": "s3:GetObjectVersion",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/HappyFace.jpg",
            "Condition": {
                "StringNotEquals": {
                    "s3:VersionId": "AaaHbAQitwiL_h47_44lRO2DDfLlBO5e"
                }
            }
        }
    ]
}
```

AWS CLI でポリシーをテストする

このこのポリシーでアクセス許可をテストするには、AWS CLI `get-object` コマンドを実行するときに、特定のオブジェクトバージョンを指定して取得する`--version-id` パラメータを使用します。コマンドは、特定のオブジェクトバージョンを取得し、*`OutputFile.jpg`* ファイルに保存します。

```
aws s3api get-object --bucket amzn-s3-demo-bucket --key HappyFace.jpg OutputFile.jpg --
version-id AaaHbAQitwiL_h47_44lRO2DDfLlBO5e --profile AccountADave
```

例 4: オブジェクトタグに基づくアクセス許可の付与

Amazon S3 のオペレーションでオブジェクトのタグの条件キーを使用する方法の例については、「タグ付けとアクセスコントロールポリシー」を参照してください。

例 5: バケット所有者の AWS アカウント ID によるアクセスの制限

`aws:ResourceAccount` または `s3:ResourceAccount` の条件キーのいずれかを使用して、特定の AWS アカウント ID が所有する Amazon S3 バケットへのユーザー、ロール、またはアプリケーションのアクセスを制限する IAM または仮想プライベートクラウド (VPC) エンドポイントポリシー

を記述できます。これらの条件キーを使用すると、VPC 内のクライアントによる、ユーザーが所有していないバケットへのアクセスを制限できます。

ただし、一部の AWS サービスは AWS マネージドバケットへのアクセスに依存していることに注意してください。したがって、IAM ポリシーで `aws:ResourceAccount` キーまたは `s3:ResourceAccount` キーを使用することは、これらのリソースへのアクセスにも影響する可能性があります。詳細については、以下のリソースを参照してください。

- AWS アカウント ガイドの指定された AWS PrivateLink のバケットへのアクセスの制限
- Amazon ECR ガイドの Amazon ECR が使用するバケットへのアクセスを制限する
- AWS Systems Manager ガイドの AWS が管理する Amazon S3 バケットに必要なアクセスを System Manager に提供する

`aws:ResourceAccount` および `s3:ResourceAccount` 条件キーの詳細と使用方法を示す例については、「AWS ストレージブログ」の「Limit access to Amazon S3 buckets owned by specific AWS アカウント」を参照してください。

例 6: 最小の TLS バージョンの要求

`s3:TlsVersion` 条件キーを使用して、クライアントが使用する TLS バージョンに基づいて Amazon S3 バケットへのユーザーまたはアプリケーションのアクセスを制限する IAM ポリシー、仮想プライベートクラウドエンドポイント (VPCE) ポリシー、またはバケットポリシーを作成できます。この条件キーを使用して、最小の TLS バージョンを必要とするポリシーを記述できます。

> **Note**
>
> AWS のサービスがユーザーに代わって他の AWS のサービスを呼び出す場合 (サービス間呼び出し)、`s3:TlsVersion`、`aws:SecureTransport`、`aws:SourceIp`、および `aws:VpcSourceIp` など、特定のネットワーク固有の認可コンテキストが編集されます。ポリシーで `Deny` ステートメントとともにこれらの条件キーを使用すると、AWS サービスプリンシパルが意図せずブロックされる可能性があります。セキュリティ要件を維持しながら AWS のサービスが適切に動作できるようにするには、値が `false` の `aws:PrincipalIsAWSService` 条件キーを追加して、`Deny` ステートメントからサービスプリンシパルを除外します。例:
>
> ```
> {
>   "Effect": "Deny",
>   "Action": "s3:*",
>   "Resource": "*",
> ```

```
  "Condition": {
    "Bool": {
      "aws:SecureTransport": "false",
      "aws:PrincipalIsAWSService": "false"
    }
  }
}
```

このポリシーは、HTTPS が使用されていない場合に (aws:SecureTransport が false)、AWS 以外のサービスプリンシパルに対してのみ S3 オペレーションへのアクセスを拒否します。これにより、条件付き制限が AWS サービスプリンシパルを除くすべてのプリンシパルに適用されます。

Example

このバケットポリシーの例では、1.2 より前の TLS バージョン (1.1 や 1.0 など) のクライアントによる PutObject リクエストを拒否します。このポリシーの例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket1",
                "arn:aws:s3:::amzn-s3-demo-bucket1/*"
            ],
            "Condition": {
                "NumericLessThan": {
                    "s3:TlsVersion": 1.2
                }
            }
        }
    ]
}
```

Example

このバケットポリシー例では、1.1 よりも高い TLS バージョン (1.2、1.3 以降など) のクライアントによる PutObject リクエストを許可します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket1",
                "arn:aws:s3:::amzn-s3-demo-bucket1/*"
            ],
            "Condition": {
                "NumericGreaterThan": {
                    "s3:TlsVersion": 1.1
                }
            }
        }
    ]
}
```

例 7: **Deny** ステートメントから特定のプリンシパルを除外する

次のバケットポリシーは、アカウント番号 *123456789012* を持つプリンシパルを除き、*amzn-s3-demo-bucket* への s3:GetObject アクセスを拒否します。このポリシーの例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessFromPrincipalNotInSpecificAccount",
      "Principal": {
        "AWS": "*"
      },
      "Action": "s3:GetObject",
```

```
      "Effect": "Deny",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalAccount": [
            "123456789012"
          ]
        }
      }
    }
  ]
}
```

例 8: オブジェクトキー名または ETags に基づいた、クライアントへの条件付きオブジェクトアップロードの強制

条件付き書き込みでは、WRITE リクエストにヘッダーを追加して、S3 オペレーションに前提条件を指定できます。このヘッダーを使用して、条件が満たされないと S3 オペレーションが失敗する条件を指定します。例えば、オブジェクトアップロード時に、バケットに同じキー名を持つオブジェクトが存在しないことを検証することで、既存のデータの上書きを防ぐことができます。または、オブジェクトを書き込む前に、Amazon S3 でオブジェクトのエンティティタグ (ETag) をチェックすることもできます。

バケットポリシーの条件を使用して条件付き書き込みを適用するバケットポリシーの例については、「the section called “条件付き書き込みを強制する”」を参照してください。

例: バケットオペレーションで使用できる Amazon S3 の条件キー

以下のポリシーの例では、バケットオペレーションに Amazon S3 固有の条件キーを使用する方法を示します。

トピック

- 例 1: IP アドレスに対する条件付きの s3:GetObject アクセス許可の付与
- 例 2: 特定のプレフィックスを持つバケット内のオブジェクト一覧の取得
- 例 3: キーの最大数の設定

例 1: IP アドレスに対する条件付きの **s3:GetObject** アクセス許可の付与

リクエストが特定の範囲の IP アドレス (例: *192.0.2.**) から発信された場合は、そのアドレスが除外する IP アドレス (例: *192.0.2.188*) でない限り、s3:GetObject アクションを使用するアクセス許可を認証したユーザーに付与できます。Condition ブロックでは、IpAddress と NotIpAddress は条件であり、それぞれの条件に評価されるキーと値のペアが指定されています。この例の両方のキーと値のペアは、aws:SourceIp AWS 全体キーを使用しています。このポリシーの例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

> **Note**
>
> Condition ブロックで指定されている IPAddress と NotIpAddress のキー値は、RFC 4632 で説明されているように、CIDR 表記を使用しています。詳細については、http://www.rfc-editor.org/rfc/rfc4632.txt を参照してください。

```
{
    "Version": "2012-10-17",
    "Id": "S3PolicyId1",
    "Statement": [
        {
            "Sid": "statement1",
            "Effect": "Allow",
            "Principal": "*",
            "Action":"s3:GetObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition" : {
                "IpAddress" : {
                    "aws:SourceIp": "192.0.2.0/24"
                },
                "NotIpAddress" : {
                    "aws:SourceIp": "192.0.2.188/32"
                }
            }
        }
    ]
}
```

Amazon S3 のポリシーでは、他の AWS 全体の条件キーを使用することもできます。例えば、VPC エンドポイントのバケットポリシーで aws:SourceVpce 条件キーや aws:SourceVpc 条件キーを

指定できます。具体的な例については、「バケットポリシーを使用した VPC エンドポイントからのアクセスコントロール」を参照してください。

> **Note**
>
> 一部の AWS グローバル条件キーでは、特定のリソースタイプのみがサポートされます。そのため、使用するグローバル条件キーとリソースタイプを Amazon S3 がサポートしているかどうか、または代わりに Amazon S3 固有の条件キーを使用する必要があるかどうかを確認してください。Amazon S3 に対してサポートされているリソースタイプと条件キーの完全なリストについては、サービス認可リファレンスの「Actions, resources, and condition keys for Amazon S3」を参照してください。
> S3 リソースタイプ別の S3 API オペレーションへのアクセス許可の詳細については、「Amazon S3 API オペレーションに必要なアクセス許可」を参照してください。

例 2: 特定のプレフィックスを持つバケット内のオブジェクト一覧の取得

`s3:prefix` 条件キーを使用して、ListObjectsV2 API オペレーションを、特定のプレフィックスを持つキー名に制限できます。バケット所有者であれば、条件キーを使用して、ユーザーがバケット内の特定のプレフィックスの内容を一覧表示することを制限できます。`s3:prefix` 条件キーは、バケットのオブジェクトがキー名プレフィックスによって整理されている場合に便利です。

Amazon S3 コンソールでは、キー名のプレフィックスを使用して、フォルダの概念を示します。フォルダの概念をサポートしているはコンソールのみです。Amazon S3 API では、バケットとオブジェクトのみがサポートされています。例えば、キー名が *`public/object1.jpg`* および *`public/object2.jpg`* である 2 つのオブジェクトがある場合、コンソールには *`public`* フォルダ以下のオブジェクトが表示されます。Amazon S3 API では、これらはプレフィックスを持つオブジェクトとして扱われ、フォルダ内のオブジェクトとしては扱われません。プレフィックスと区切り文字を使用してアクセス許可をフィルタリングする方法の詳細については、ユーザーポリシーを使用したバケットへのアクセスの制御 を参照してください。

次のシナリオでは、バケット所有者とユーザーが属する親アカウントは同一です。したがって、バケット所有者は、アクセス許可を付与するためにバケットポリシーまたはユーザーポリシーのどちらも使用できます。`ListObjectsV2` API オペレーションを使用できる条件キーの詳細については、「ListObjectsV2」を参照してください。

> **Note**
>
> バケットがバージョニングに対応している場合、バケット内のオブジェクトのリストを表示するには、以下のポリシーで、s3:ListBucket のアクセス許可ではなく s3:ListBucketVersions のアクセス許可を付与する必要があります。s3:ListBucketVersions アクセス許可は、s3:prefix 条件キーもサポートしています。

ユーザーポリシー

次のユーザーポリシーは、s3:ListBucket のアクセス許可 (「ListObjectsV2」を参照) に、*projects* の値を持つリクエストでプレフィックスを指定する必要がある Condition ステートメントを付与します。このポリシーの例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"statement1",
         "Effect":"Allow",
         "Action": "s3:ListBucket",
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket",
         "Condition" : {
             "StringEquals" : {
                 "s3:prefix": "projects"
             }
          }
       },
      {
         "Sid":"statement2",
         "Effect":"Deny",
         "Action": "s3:ListBucket",
         "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
         "Condition" : {
             "StringNotEquals" : {
                 "s3:prefix": "projects"
             }
          }
       }
```

```
    ]
}
```

Condition ステートメントは、プレフィックスが *projects* のオブジェクトキーのみを一覧表示するようにユーザーを制限します。明示的なDeny ステートメントを追加すると、ユーザーに付与されている他のアクセス許可にかかわらず、他のプレフィックスが付いたキーのリストを求めるユーザーは拒否されます。例えば、以前のユーザーポリシーの更新やバケットポリシーにより、オブジェクトキーのリストを表示するアクセス許可がユーザーに制限なく付与される場合があります。明示的な Deny ステートメントは常に Allow ステートメントを上書きするため、ユーザーが *projects* プレフィックスを持つキー以外のキーを一覧表示しようとすると、リクエストは拒否されます。

バケットポリシー

次の例に示すとおり、上記のユーザーポリシーに Principal 要素を追加して、ユーザーを指定する場合は、バケットポリシーを使用できます。このポリシーの例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"statement1",
         "Effect":"Allow",
         "Principal": {
            "AWS": "arn:aws:iam::123456789012:user/bucket-owner"
         },
         "Action":  "s3:ListBucket",
         "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
         "Condition" : {
             "StringEquals" : {
                 "s3:prefix": "projects"
             }
          }
       },
      {
         "Sid":"statement2",
         "Effect":"Deny",
         "Principal": {
            "AWS": "arn:aws:iam::123456789012:user/bucket-owner"
         },
         "Action": "s3:ListBucket",
         "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
```

```
        "Condition" : {
            "StringNotEquals" : {
                "s3:prefix": "projects"
            }
         }
      }
   ]
}
```

AWS CLI でポリシーをテストする

このポリシーは、次の `list-object` AWS CLI コマンドを使用してテストできます。このコマンドでは、`--profile` パラメータを使用してユーザーの認証情報を指定します。AWS CLI のセットアップと使用の詳細については、「Amazon S3 API リファレンス」の「Developing with Amazon S3 using the AWS CLI」を参照してください。

```
aws s3api list-objects --bucket amzn-s3-demo-bucket --prefix projects --
profile AccountA
```

例 3: キーの最大数の設定

`s3:max-keys` 条件キーを使用すると、リクエスタが ListObjectsV2 または ListObjectVersions リクエストで返すことができるキーの最大数を設定できます。デフォルトでは、API オペレーションは最大 1,000 個のキーを返します。`s3:max-keys` で使用できる数値条件演算子の一覧とその例については、IAM ユーザーガイドの数値条件演算子 を参照してください。

Amazon S3 のアイデンティティベースのポリシー

デフォルトでは、ユーザーとロールには Amazon S3 リソースを作成または変更するアクセス許可がありません。また、AWS Management Console、AWS Command Line Interface (AWS CLI)、または AWS API を使用してタスクを実行することもできません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き継ぐことができます。

これらサンプルの JSON ポリシードキュメントを使用して、IAM アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「IAM ポリシーを作成する (コンソール)」を参照してください。

Amazon S3 が定義するアクションとリソースタイプ (リソースタイプごとの ARN の形式を含む) の詳細については、「サービス認可リファレンス」の「Actions, resources, and condition keys for Amazon S3」を参照してください。

S3 リソースタイプ別の S3 API オペレーションへのアクセス許可の詳細については、「Amazon S3 API オペレーションに必要なアクセス許可」を参照してください。

トピック

- ポリシーに関するベストプラクティス
- ユーザーポリシーを使用したバケットへのアクセスの制御
- Amazon S3 のアイデンティティベースのポリシー例

ポリシーに関するベストプラクティス

アイデンティティベースのポリシーは、あるユーザーがアカウントの Amazon S3 リソースを作成、アクセス、削除できるどうかを決定します。これらのアクションを実行すると、AWS アカウントに料金が発生する可能性があります。アイデンティティベースポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください:

- AWS マネージドポリシーを使用して開始し、最小特権の許可に移行する – ユーザーとワークロードへの許可の付与を開始するには、多くの一般的なユースケースのために許可を付与する AWS マネージドポリシーを使用します。これらは AWS アカウントで使用できます。ユースケース別に AWS カスタマーマネージドポリシーを定義して、マネージドポリシーを絞り込むことをお勧めします。詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」または「ジョブ機能の AWS マネージドポリシー」を参照してください。
- 最小特権を適用する – IAM ポリシーで許可を設定する場合は、タスクの実行に必要な許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、最小特権アクセス許可とも呼ばれています。IAM を使用して許可を適用する方法の詳細については、「IAM ユーザーガイド」の「IAM でのポリシーとアクセス許可」を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する - ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリクエストを SSL を使用して送信するように指定できます。また、AWS CloudFormation などの特定の AWS のサービス を介して使用する場合、条件を使用してサービスアクションへのアクセスを許可することもできます。詳細については、「IAM ユーザーガイド」の「IAM JSON ポリシー要素:条件」を参照してください。
- IAM Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサ

ポートします。詳細については、「IAM ユーザーガイド」の「IAM Access Analyzer でポリシーを検証する」を参照してください。

- 多要素認証 (MFA) を要求する – AWS アカウントで IAM ユーザーまたはルートユーザーを要求するシナリオがある場合は、セキュリティを強化するために MFA をオンにします。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、「IAM ユーザーガイド」の「MFA を使用した安全な API アクセス」を参照してください。

IAM でのベストプラクティスの詳細については、「IAM ユーザーガイド」の「IAM でのセキュリティのベストプラクティス」を参照してください。

ユーザーポリシーを使用したバケットへのアクセスの制御

このチュートリアルでは、Amazon S3 でのユーザーアクセス許可の使用について説明します。この例では、フォルダを含むバケットを作成します。AWS アカウントで AWS Identity and Access Management IAM ユーザーを作成し、作成したユーザーに対して、Amazon S3 バケットおよびバケット内のフォルダへのアクセス許可を段階的に付与します。

トピック

- バケットとフォルダの基本
- チュートリアルの概要
- チュートリアルの準備をする
- ステップ 1: バケットを作成する
- ステップ 2: IAM ユーザーとグループを作成する
- ステップ 3: IAM ユーザーにアクセス許可が付与されていないことを確認する
- ステップ 4: グループレベルのアクセス許可を付与する
- ステップ 5: IAM ユーザーの Alice に特定のアクセス許可を付与する
- ステップ 6: IAM ユーザーの Bob に特定のアクセス許可を付与する
- ステップ 7: Private フォルダをセキュリティで保護する
- ステップ 8: クリーンアップする
- 関連リソース

バケットとフォルダの基本

Amazon S3 のデータモデルはフラットな構造をしています。バケットを作成し、バケットにオブジェクトを保存します。サブバケットやサブフォルダの階層はありませんが、フォルダ階層を エミュレートすることができます。Amazon S3 コンソールなどのツールを使用すると、バケット内の論理フォルダやサブフォルダを表示できます。

companybucket という名前のバケットには、Private、Development、Finance の 3 つのフォルダと s3-dg.pdf オブジェクトが含まれていることがコンソールに表示されます。コンソールでは、フォルダおよびサブフォルダからなる論理的な階層が作成するために、オブジェクト名 (キー) を使用します。次の例を考えます。

- Development フォルダを作成すると、コンソールによって Development/ というキーを持つオブジェクトが作成されます。区切り記号として末尾のスラッシュ (/) が付いている点に注意してください。
- Projects1.xls というオブジェクトを Development フォルダにアップロードすると、コンソールによってそのオブジェクトがアップロードされ、Development/Projects1.xls というキーが設定されます。

  このキーの Development はプレフィックスで、/ は区切り記号です。Amazon S3 API のオペレーションではプレフィックスと区切り記号がサポートされます。例えば、特定のプレフィックスと区切り記号を持つすべてのオブジェクトの一覧を取得できます。コンソールで Development フォルダを開くと、そのフォルダ内のオブジェクトがコンソールに一覧表示されます。次の例では、Development フォルダには 1 つのオブジェクトが含まれています。

  コンソールで Development バケットの companybucket フォルダを表示すると、プレフィックスに Development と区切り文字に / を指定したリクエストが Amazon S3 に送信されます。コンソールのレスポンスは、コンピュータのファイルシステムのフォルダ一覧と似ています。前述の例は、バケット companybucket に Development/Projects1.xls というキーを持つ 1 つのオブジェクトがあることを示しています。

コンソールは、オブジェクトのキーを使用して論理階層を推測しています。Amazon S3 には物理階層はありません。Amazon S3 にはフラットなファイル構造にオブジェクトを含むバケットがあるだけです。Amazon S3 API を使用してオブジェクトを作成すると、オブジェクトのキーを使用して論理階層を表すことができます。オブジェクトの論理階層を作成する場合は、個別のフォルダへのアクセスを管理できます。このチュートリアルで、その方法について説明します。

開始する前に、ルートレベルのバケットの内容の概念を理解する必要があります。companybucket バケットに次のオブジェクトがあるとします。

- Private/privDoc1.txt
- Private/privDoc2.zip
- Development/project1.xls
- Development/project2.xls
- Finance/Tax2011/document1.pdf
- Finance/Tax2011/document2.pdf
- s3-dg.pdf

これらのオブジェクトキーによって、ルートレベルフォルダ Private、Development、および Finance と、ルートレベルオブジェクト s3-dg.pdf を持つ論理階層が作成されます。Amazon S3 コンソールでバケット名を選択すると、ルートレベルの項目が表示されます。コンソールにはトップレベルのプレフィックス (Private/、Development/、Finance/) が表示されます。オブジェクトキー s3-dg.pdf にはプレフィックスがないため、ルートレベル項目として表示されます。

チュートリアルの概要

このチュートリアルでは、3 つのフォルダ (Private、Development、Finance) を含むバケットを作成します。

ユーザーは Alice と Bob の 2 名です。Alice には Development フォルダにのみ、Bob には Finance フォルダにのみアクセスを付与します。Private フォルダの内容は非公開のままにします。このチュートリアルの例では、IAM ユーザー (ユーザー名 Alice と Bob) を作成してアクセスを管理し、必要なアクセス許可を付与します。

IAM では、ユーザーグループを作成して、そのグループのすべてのユーザーに適用するグループレベルのアクセス許可を付与することもできます。これにより、アクセス許可を効果的に管理できます。この演習では、Alice と Bob に共通のアクセス許可が必要です。そのため、Consultants というグループを作成し、Alice と Bob をそのグループに追加します。最初に、グループポリシーをグループに関連付けてアクセス許可を付与します。次に、特定のユーザーにポリシーを関連付けてユーザー固有のアクセス許可を追加します。

> **Note**
>
> このチュートリアルでは、バケット名に companybucket、IAM ユーザーに Alice と Bob、グループ名に Consultants を使用しています。Amazon S3 ではバケット名はグローバルに一意である必要があるため、このバケット名は実際に作成する名前に置き換えてください。

チュートリアルの準備をする

この例では、AWS アカウント 認証情報を使用して、IAM ユーザーを作成します。最初、これらのユーザーにはアクセス許可が何もありません。これらのユーザーに、Amazon S3 の特定のアクションを実行するためのアクセス許可を段階的に付与します。アクセス許可をテストするには、各ユーザーの認証情報を使用してコンソールにサインインします。AWS アカウントの所有者として許可を段階的に付与し、IAM ユーザーとして許可をテストするには、そのたびに異なる認証情報を使用してサインイン/サインアウトする必要があります。これは、1 つのブラウザでテストできますが、2 つのブラウザを使用した方が迅速に処理することができます。一方のブラウザで自分の AWS アカウント 認証情報を使用して AWS Management Console に接続し、もう一方のブラウザで IAM ユーザーの認証情報を使用して接続します。

AWS アカウント 認証情報を使用して AWS Management Console にサインインするには、https://conso4le.aws.amazon.com/ にアクセスします。。IAM ユーザーは、このリンクからはサインインできません。IAM ユーザーは IAM 対応のサインインページを使用する必要があります。アカウント所有者からユーザーにこのリンクを通知します。

IAM の詳細については、IAM ユーザーガイドAWS Management Consoleの へのサインインページを参照してください。

IAM ユーザーにサインインのリンクを提供するには

1. AWS Management Console にサインインして、IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。
2. [Navigation (ナビゲーション)] ペインで、[IAM Dashboard (IAM ダッシュボード)] を選択します。
3. [IAM users sign in link (IAM ユーザーのサインインのリンク)] の URL を書き留めます。このリンクを IAM ユーザーに提供して、IAM ユーザー名とパスワードを使用してコンソールにサインインしてもらいます。

ステップ 1: バケットを作成する

このステップでは、AWS アカウント認証情報を使用して Amazon S3 コンソールにサインインし、バケットの作成、バケットへのフォルダの追加、各フォルダのへの 1 つまたは 2 つのサンプルドキュメントのアップロードを行います。

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. バケットを作成します。

   手順については、汎用バケットの作成 を参照してください。
3. バケットにドキュメントを 1 つアップロードします。

   この演習では、このバケットのルートレベルに `s3-dg.pdf` というドキュメントがあることを前提としています。別のドキュメントをアップロードする場合は、`s3-dg.pdf` をそのドキュメントのファイル名に置き換えてください。
4. 3 つのフォルダ (`Private`、`Finance`、`Development`) をバケットに追加します。

   フォルダを作成するステップバイステップの手順については、Amazon Simple Storage Service ユーザーガイドの フォルダを使用して Amazon S3 コンソールのオブジェクトを整理する を参照してください。
5. 各フォルダにドキュメントを 1 つか 2 つアップロードします。

   この演習では、各フォルダに数個のドキュメントをアップロード済みで、バケットに次のキーを持つオブジェクトが存在することを前提としています。

   - `Private/privDoc1.txt`
   - `Private/privDoc2.zip`
   - `Development/project1.xls`
   - `Development/project2.xls`
   - `Finance/Tax2011/document1.pdf`
   - `Finance/Tax2011/document2.pdf`
   - `s3-dg.pdf`

   手順については、オブジェクトのアップロード を参照してください。

ステップ 2: IAM ユーザーとグループを作成する

IAM コンソールを使用して 2 人の IAM ユーザー (Alice と Bob) を AWS アカウント に追加します。詳細な手順については、「IAM ユーザーガイド」の「AWS アカウント での IAM ユーザーの作成」を参照してください。

また、Consultants という名前の管理グループを作成します。続いて、ユーザーをこのグループに追加します。詳細な手順については、「IAM ユーザーグループの作成」を参照してください。

> **Warning**
>
> ユーザーとグループを追加するときに、これらのユーザーにアクセス許可を付与するポリシーを関連付けないでください。最初の時点では、アクセス許可はこれらのユーザーに付与せず、以降のセクションで段階的に付与します。まず、これらの IAM ユーザーにパスワードを割り当てておく必要があります。それらのユーザー認証情報を使用して Amazon S3 のアクションをテストし、アクセス許可が意図したとおりに機能することを確認します。

新しい IAM ユーザーの作成の各手順については、「IAM ユーザーガイド」の「AWS アカウント での IAM ユーザーの作成」を参照してください。このチュートリアル用にユーザーを作成するときは、[AWS Management Console アクセス] を選択し、[プログラムによるアクセス] を消去します。

管理グループを作成する手順については、IAM ユーザーガイドの最初の IAM 管理者のユーザーおよびグループの作成を参照してください。

ステップ 3: IAM ユーザーにアクセス許可が付与されていないことを確認する

ブラウザを 2 つ使用する場合は、ここで 2 つ目のブラウザからいずれかの IAM ユーザー認証情報を使用して、コンソールにサインインできます。

1. IAM ユーザーのサインインのリンク (「IAM ユーザーにサインインのリンクを提供するには」を参照) から、いずれかの IAM ユーザー認証情報を使用して AWS Management Consoleにサインインします。
2. https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開きます。

   アクセスが拒否されることを示すコンソールメッセージを確認します。

次に、アクセス許可を段階的にユーザーに付与します。最初に、両方のユーザーに必要なアクセス許可を付与するグループポリシーをアタッチします。

ステップ 4: グループレベルのアクセス許可を付与する

ユーザーが次の内容を実行できるようにします。

- 親アカウントが所有するすべてのバケットを表示します。これを行うには、Bob と Alice に `s3:ListAllMyBuckets` アクションのためのアクセス許可が必要です。
- `companybucket` バケット内のルートレベルの項目、フォルダ、およびオブジェクトを一覧表示します。これを行うには、Bob と Alice に `s3:ListBucket` バケットに対する `companybucket` アクションのためのアクセス許可が必要です。

次に、これらのアクセス許可を付与するポリシーを作成し、`Consultants` グループにアタッチします。

ステップ 4.1: すべてのバケットのリストを表示するアクセス許可を付与する

このステップでは、親アカウントが所有するすべてのバケットを表示するのに必要な最小限のアクセス許可をユーザーに付与する管理ポリシーを作成します。そのポリシーを `Consultants` グループにアタッチします。その管理ポリシーをユーザーまたはグループにアタッチしたら、親 AWS アカウントが所有するバケットのリストを取得する許可をそのユーザーまたはグループに付与します。

1. AWS Management Console にサインインして、IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。

   > **Note**
   >
   > ユーザーに許可を付与するため、IAM ユーザーではなく、AWS アカウントの認証情報を使用してサインインします。

2. 管理ポリシーを作成します。

   a. 左側のナビゲーションペインで [ポリシー] を選択し、続いて [ポリシーの作成] を選択します。

   b. [JSON] タブを選択します。

   c. 以下のアクセスポリシーをコピーし、 ポリシーテキストフィールドに貼り付けます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
      "Sid": "AllowGroupToSeeBucketListInTheConsole",
      "Action": ["s3:ListAllMyBuckets"],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::*"]
    }
  ]
}
```

ポリシーは JSON ドキュメントです。そのドキュメントの Statement はオブジェクトの配列であり、各オブジェクトが名前と値のペアを使用してアクセス許可を定義しています。前述のポリシーは、1 つの特定のアクセス許可を定義しています。Action はアクセスの種類を指定します。ポリシーの s3:ListAllMyBuckets は、定義済みの Amazon S3 アクションです。このアクションは Amazon S3 GET サービスオペレーションをターゲットとし、認証された送信者が所有するすべてのバケットの一覧を返します。Effect エレメントの値は、特定のアクセスを許可するかどうかを決定します。

d. [ポリシーの確認] を選択します。次のページで、[AllowGroupToSeeBucketListInTheConsoleName (名前)] フィールドに「」と入力し、[Create policy (ポリシーの作成)] を選択します。

> **Note**
>
> [Summary (概要)] エントリに、このポリシーではどのアクセス許可も付与されないことを示すメッセージが表示されます。このチュートリアルでは、このメッセージを無視しても問題ありません。

3. 作成した AllowGroupToSeeBucketListInTheConsole 管理ポリシーを Consultants グループにアタッチします。

   管理ポリシーのアタッチの各手順については、「IAM ユーザーガイド」の「IAM ID のアクセス許可の追加および削除」を参照してください。

   IAM コンソールで、ポリシードキュメントを IAM ユーザーおよびグループにアタッチします。両方のユーザーがバケットのリストを取得できるように、ポリシーをグループにアタッチします。

4. アクセス許可をテストします。

   a. IAM ユーザーのサインインのリンク (「IAM ユーザーにサインインのリンクを提供するには」を参照) から、いずれかの IAM ユーザー認証情報を使用してコンソールにサインインします。

b. https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開きます。

コンソールにすべてのバケットが表示されますが、バケット内のオブジェクトは表示されません。

ステップ 4.2: バケットのルートレベルの内容をユーザーが表示できるようにする

次に、Consultants グループのすべてのユーザーがルートレベルの companybucket バケット項目を一覧表示できるようにします。Amazon S3 コンソールで会社のバケットを選択すると、そのバケットのルートレベルのアイテムが表示されます。

> **Note**
>
> この例では、companybucket を使用して説明します。作成したバケットの名前を使用する必要があります。

バケット名を選択したときにコンソールから Amazon S3 に送信されるリクエスト、Amazon S3 から返されるレスポンス、コンソールでレスポンスがどのように解釈されるかについて理解するために、さらに詳しくフローを見てみましょう。

バケット名を選択すると、コンソールから Amazon S3 にバケットの GET (ListObjects) のリクエストが送信されます。このリクエストには次のパラメータが含まれます。

- 空の文字列を値に持つ prefix パラメータ。
- delimiter を値に持つ / パラメータ。

リクエストの例を次に示します。

```
GET ?prefix=&delimiter=/ HTTP/1.1
Host: companybucket.s3.amazonaws.com
Date: Wed, 01 Aug  2012 12:00:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:xQE0diMbLRepdf3YB+FIEXAMPLE=
```

Amazon S3 から返されるレスポンスには、次の <ListBucketResult/> エレメントが含まれます。

```
<ListBucketResult xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
```

```
  <Name>companybucket</Name>
  <Prefix></Prefix>
  <Delimiter>/</Delimiter>
   ...
  <Contents>
    <Key>s3-dg.pdf</Key>
    ...
  </Contents>
  <CommonPrefixes>
    <Prefix>Development/</Prefix>
  </CommonPrefixes>
  <CommonPrefixes>
    <Prefix>Finance/</Prefix>
  </CommonPrefixes>
  <CommonPrefixes>
    <Prefix>Private/</Prefix>
  </CommonPrefixes>
</ListBucketResult>
```

キーの s3-dg.pdf オブジェクトには区切り文字のスラッシュ (/) が含まれておらず、このキーは Amazon S3 から <Contents> エレメントで返されています。一方、このバケットの例の他のキーには区切り文字の / が含まれています。Amazon S3 は、キーをグループ化し、<CommonPrefixes>、Development/、および Finance/ のそれぞれのプレフィックス値の Private/ エレメントを返します。このエレメントは、これらのキーの先頭から、指定した / 区切り記号の出現箇所までのサブ文字列です。

コンソールでこの結果が解釈され、ルートレベルの項目が 3 つのフォルダと 1 つのオブジェクトキーとして表示されます。

Bob または Alice が Development フォルダを開くと、コンソールから Amazon S3 にバケットの GET (ListObjects) のリクエストが送信されます。このリクエストの prefix パラメータと delimiter パラメータは、次の値に設定されます。

- 値が prefix の Development/ パラメータ。
- 値が「delimiter」の / パラメータ。

レスポンスでは、指定したプレフィックスで始まるオブジェクトのキーが Amazon S3 から返されます。

```
<ListBucketResult xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
```

```
  <Name>companybucket</Name>
  <Prefix>Development</Prefix>
  <Delimiter>/</Delimiter>
   ...
  <Contents>
    <Key>Project1.xls</Key>
    ...
  </Contents>
  <Contents>
    <Key>Project2.xls</Key>
    ...
  </Contents>
</ListBucketResult>
```

コンソールにオブジェクトキーが表示されます。

ここで、ルートレベルのバケット項目を一覧表示するためのアクセス許可をユーザーに付与する作業に戻ります。バケットの内容を一覧表示するには、ユーザーは s3:ListBucket アクションを呼び出すためのアクセス許可を持っている必要があります。次のポリシーステートメント を参照してください。ルートレベルのコンテンツのみを表示するようにするために、ユーザーがリクエストで prefix に値を指定していないことを条件に追加します。これにより、ユーザーはルートレベルのフォルダをダブルクリックできなくなります。最後に、値が「delimiter」の / パラメータをユーザーリクエストに組み込むようユーザーに義務付けて、フォルダ形式のアクセスを要求する条件を追加します。

```
{
  "Sid": "AllowRootLevelListingOfCompanyBucket",
  "Action": ["s3:ListBucket"],
  "Effect": "Allow",
  "Resource": ["arn:aws:s3:::companybucket"],
  "Condition":{
         "StringEquals":{
             "s3:prefix":[""], "s3:delimiter":["/"]
                       }
              }
}
```

Amazon S3 コンソールでバケットを選択すると、コンソールはまず Get Bucket location リクエストを送信して、バケットがデプロイされている AWS リージョン を確認します。次に、コンソールはリージョン固有のバケットのエンドポイントを使用して、バケットの GET (ListObjects) のリクエストを送信します。結果として、ユーザーがコンソールを使用する場合は、次のポリシーステートメン

トに示すように、s3:GetBucketLocation アクションのためのアクセス許可を付与する必要があります。

```
{
   "Sid": "RequiredByS3Console",
   "Action": ["s3:GetBucketLocation"],
   "Effect": "Allow",
   "Resource": ["arn:aws:s3:::*"]
}
```

ユーザーがルートレベルのバケットの内容を一覧表示できるようにするには

1. AWS Management Console にサインインして、IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。

   IAM ユーザーの認証情報ではなく、AWS アカウントの認証情報を使用してコンソールにサインインします。

2. Consultants グループにアタッチされている既存の AllowGroupToSeeBucketListInTheConsole 管理ポリシーを以下のポリシーに置き換えます。このポリシーでも s3:ListBucket アクションは実行できます。Resource ポリシーの *companybucket* は、自分のバケットの名前に置き換えてください。

   手順については、「IAM ユーザーガイド」の「IAM ポリシーの編集」を参照してください。詳細な手順では、ポリシーがアタッチされているすべてのプリンシパルエンティティに変更を適用するステップに従ってください。

   ```
   {
     "Version": "2012-10-17",
     "Statement": [
        {
          "Sid":
    "AllowGroupToSeeBucketListAndAlsoAllowGetBucketLocationRequiredForListBucket",
          "Action": [ "s3:ListAllMyBuckets", "s3:GetBucketLocation" ],
          "Effect": "Allow",
          "Resource": [ "arn:aws:s3:::*"  ]
        },
        {
          "Sid": "AllowRootLevelListingOfCompanyBucket",
          "Action": ["s3:ListBucket"],
          "Effect": "Allow",
          "Resource": ["arn:aws:s3:::companybucket"],
   ```

```
        "Condition":{
              "StringEquals":{
                    "s3:prefix":[""], "s3:delimiter":["/"]
                          }
                    }
      }
   ]
}
```

3. 更新されたアクセス許可をテストします。

   a. IAM ユーザーのサインインリンク (「IAM ユーザーにサインインのリンクを提供するには」を参照) を使用して AWS Management Consoleにサインインします。

      https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開きます。

   b. 作成したバケットを選択すると、ルートレベルのバケット項目がコンソールに表示されます。バケット内のフォルダを選択しても、フォルダの内容は表示されません。そのためのアクセス許可が付与されていないからです。

このテストは、ユーザーが Amazon S3 コンソールを使用すると成功します。コンソールでバケットを選択すると、コンソールの実装により、空の文字列を値に持つ `prefix` パラメータと、`delimiter` を値に持つ `/` パラメータが送信されるためです。

ステップ 4.3: グループポリシーの概要

追加したグループポリシーによって、IAM ユーザーである Alice と Bob に次の最小限のアクセス許可が付与されます。

- 親アカウントが所有するすべてのバケットを表示します。
- `companybucket` バケット内のルートレベルの項目を表示します。

ただし、ユーザーが実行できる操作はまだ十分ではありません。次のように、ユーザー固有のアクセス許可を付与します。

- `Development` フォルダのオブジェクトの読み書きを Alice に許可します。
- `Finance` フォルダのオブジェクトの読み書きを Alice と Bob に許可します。

ユーザー固有のアクセスを許可するには、グループではなく特定のユーザーにポリシーを関連付けます。次のセクションでは、`Development` フォルダを操作するためのアクセス許可を Alice に付与し

ます。Finance フォルダを操作するための同様のアクセス許可を Bob に付与するステップを繰り返します。

ステップ 5: IAM ユーザーの Alice に特定のアクセス許可を付与する

次に、Development フォルダの内容を表示し、そのフォルダ内のオブジェクトを読み書きできるように、追加のアクセス許可を Alice に付与します。

ステップ 5.1: IAM ユーザーの Alice に Development フォルダの内容を一覧表示するためのアクセス許可を付与する

Alice が Development フォルダの内容を表示できるようにするには、s3:ListBucket バケットに対して companybucket アクションを実行するためのアクセス許可を付与するポリシーをユーザー Alice に適用する必要があります (プレフィックス Development/ がリクエストに含まれていることを前提とします)。このポリシーはユーザー (Alice) にのみ適用するため、インラインポリシーを使用します。インラインポリシーの詳細については、「IAM ユーザーガイド」の「管理ポリシーとインラインポリシー」を参照してください。

1. AWS Management Console にサインインして、IAM コンソール (https://console.aws.amazon.com/iam/) を開きます。

   IAM ユーザーの認証情報ではなく、AWS アカウントの認証情報を使用してコンソールにサインインします。

2. Development フォルダの内容を表示するアクセス許可をユーザー (Alice) に付与するインラインポリシーを作成します。

   a. 左側のナビゲーションペインで、[ユーザー] を選択します。
   b. ユーザー名 [Alice] を選択します。
   c. ユーザーの詳細ページで、[Permissions (アクセス許可)] タブを選択し、[Add inline policy (インラインポリシーの追加)] を選択します。
   d. [JSON] タブを選択します。
   e. 以下のアクセスポリシーをコピーし、ポリシーのテキストフィールドに貼り付けます。

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
      "Sid": "AllowListBucketIfSpecificPrefixIsIncludedInRequest",
      "Action": ["s3:ListBucket"],
```

```
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::companybucket"],
      "Condition":{  "StringLike":{"s3:prefix":["Development/*"] }
       }
    }
  ]
}
```

f. [ポリシーの確認] を選択します。次のページで、[Name (名前)] フィールドに名前を入力し、[Create policy (ポリシーの作成)] を選択します。

3. Alice のアクセス許可の変更をテストします。

a. IAM ユーザーのサインインリンク (「IAM ユーザーにサインインのリンクを提供するには」を参照) を使用して AWS Management Consoleにサインインします。

b. https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開きます。

c. Amazon S3 コンソールで、Alice がバケットの Development/ フォルダ内のオブジェクトを一覧表示できることを確認します。

ユーザーが /Development フォルダ内のオブジェクトを一覧表示するためにそのフォルダを選択すると、Amazon S3 コンソールから Amazon S3 にプレフィックスに ListObjects を指定した /Development のリクエストが送信されます。ユーザーにはプレフィックスに Development と区切り文字に / を指定してオブジェクトを一覧表示するアクセス許可が付与されているため、Amazon S3 からキープレフィックスが Development/ のオブジェクトの一覧が返されてコンソールに表示されます。

ステップ 5.2: IAM ユーザーの Alice に Development フォルダでオブジェクトを取得および作成するためのアクセス許可を付与する

Alice が Development フォルダ内のオブジェクトを読み書きできるようにするには、s3:GetObject および s3:PutObject アクションを呼び出すためのアクセス許可が Alice に必要です。次のポリシーステートメントは、そのアクセス許可を付与します (リクエストに prefix の値を持つ Development/ パラメータが設定されているとします)。

```
{
    "Sid":"AllowUserToReadWriteObjectData",
    "Action":["s3:GetObject", "s3:PutObject"],
    "Effect":"Allow",
    "Resource":["arn:aws:s3:::companybucket/Development/*"]
 }
```

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。

   IAM ユーザーの認証情報ではなく、AWS アカウントの認証情報を使用してコンソールにサインインします。

2. 前のステップで作成したインラインポリシーを編集します。

   a. 左側のナビゲーションペインで、[ユーザー] を選択します。

   b. ユーザー名 [Alice] を選択します。

   c. ユーザーの詳細で、[アクセス許可] タブを選択し、[インラインポリシー] セクションを展開します。

   d. 前のステップで作成したポリシーの名前の横にある [Edit Policy (ポリシーの編集)] をクリックします。

   e. 以下のポリシーをコピーして、 ポリシーテキストフィールドに貼り付け、既存のポリシーと置き換えます。

```
{
     "Version": "2012-10-17",
     "Statement":[
      {
         "Sid":"AllowListBucketIfSpecificPrefixIsIncludedInRequest",
         "Action":["s3:ListBucket"],
         "Effect":"Allow",
         "Resource":["arn:aws:s3:::companybucket"],
         "Condition":{
            "StringLike":{"s3:prefix":["Development/*"]
            }
         }
      },
      {
        "Sid":"AllowUserToReadWriteObjectDataInDevelopmentFolder",
        "Action":["s3:GetObject", "s3:PutObject"],
        "Effect":"Allow",
        "Resource":["arn:aws:s3:::companybucket/Development/*"]
      }
   ]
}
```

3. 更新されたポリシーをテストします。

a. IAM ユーザーのサインインリンク (「IAM ユーザーにサインインのリンクを提供するには」を参照) を使用して AWS Management Consoleにサインインします。

b. https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開きます。

c. Amazon S3 コンソールで、Alice が Development フォルダに対するオブジェクトの追加およびダウンロードを行えるようになったことを確認します。

ステップ 5.3: バケットの他のフォルダへの IAM ユーザーの Alice のアクセス許可を明示的に拒否する

ユーザー Alice が companybucket バケットのルートレベルの内容を表示できるようになったことを確認します。Alice は Development フォルダのオブジェクトを読み書きすることもできます。厳密にアクセス許可を制限したい場合は、バケットの他のフォルダへの Alice のアクセスを明示的に拒否することができます。バケットの他のフォルダへのアクセス許可を Alice に付与する他のポリシー (バケットポリシーまたは ACL) が存在する場合は、この明示的な拒否がそれらのアクセス許可よりも優先されます。

次のステートメントをユーザーの Alice のポリシーに追加すると、Alice が Amazon S3 に送信するすべてのリクエストに prefix パラメータを含めて値を Development/* または空の文字列にすることを要求できます。

```
{
   "Sid": "ExplicitlyDenyAnyRequestsForAllOtherFoldersExceptDevelopment",
   "Action": ["s3:ListBucket"],
   "Effect": "Deny",
   "Resource": ["arn:aws:s3:::companybucket"],
   "Condition":{  "StringNotLike": {"s3:prefix":["Development/*",""] },
                  "Null"         : {"s3:prefix":false }
    }
}
```

Condition ブロックには 2 つの条件式があります。これらの条件式の結果は、論理 AND を使用して結合されます。両方の条件が true の場合、結合された条件の結果は true です。このポリシーの Effect が Deny であるため、Condition が true と評価されると、ユーザーは指定した Action を実行できません。

- Null 条件式により、Alice からのリクエストに prefix パラメータが含まれていることが保証されます。

prefix パラメータはフォルダに類似したアクセスを必要とします。prefix パラメータのないリクエストを送信すると、Amazon S3 によりすべてのオブジェクトキーが返されます。

リクエストに null 値の prefix パラメータが含まれている場合、式の評価結果は true になり、Condition 全体の評価結果が true になります。空の文字列を prefix パラメータの値として許可する必要があります。null 文字列を許可すると、この前の説明に示したコンソールでの操作と同様に、Alice はルートレベルのバケット項目を取得できるようになります。詳細については、ステップ 4.2: バケットのルートレベルの内容をユーザーが表示できるようにする を参照してください。

- 条件式 StringNotLike を使用すると、prefix パラメータの値が指定されていて Development/* でない場合、リクエストは失敗します。

前のセクションの手順に従って、ユーザー Alice 用に作成したインラインポリシーを再び更新します。

以下のポリシーをコピーして、 ポリシーテキストフィールドに貼り付け、既存のポリシーと置き換えます。

```
{
   "Version": "2012-10-17",
   "Statement":[
      {
         "Sid":"AllowListBucketIfSpecificPrefixIsIncludedInRequest",
         "Action":["s3:ListBucket"],
         "Effect":"Allow",
         "Resource":["arn:aws:s3:::companybucket"],
         "Condition":{
            "StringLike":{"s3:prefix":["Development/*"]
            }
         }
      },
      {
        "Sid":"AllowUserToReadWriteObjectDataInDevelopmentFolder",
        "Action":["s3:GetObject", "s3:PutObject"],
        "Effect":"Allow",
        "Resource":["arn:aws:s3:::companybucket/Development/*"]
      },
      {
         "Sid": "ExplicitlyDenyAnyRequestsForAllOtherFoldersExceptDevelopment",
         "Action": ["s3:ListBucket"],
```

```
        "Effect": "Deny",
        "Resource": ["arn:aws:s3:::companybucket"],
        "Condition":{  "StringNotLike": {"s3:prefix":["Development/*",""] },
                       "Null"         : {"s3:prefix":false }
         }
      }
   ]
}
```

ステップ 6: IAM ユーザーの Bob に特定のアクセス許可を付与する

次に、Finance フォルダへのアクセス許可を Bob に付与します。Alice にアクセス許可を付与するときに使用した手順に従います。ただし、Development フォルダは Finance フォルダに置き換えます。手順については、ステップ 5: IAM ユーザーの Alice に特定のアクセス許可を付与する を参照してください。

ステップ 7: Private フォルダをセキュリティで保護する

この例では、ユーザーは 2 名だけです。グループレベルで最小限必要なすべてのアクセス許可を付与し、ユーザーレベルのアクセス許可は、個々のユーザーレベルでアクセスを許可することが必要な場合にのみ付与しました。このようにすると、アクセス許可を管理する手間を最小限に抑えることができます。ユーザー数が増えるに従って、アクセス許可の管理は煩雑になります。例えば、この例のどのユーザーも Private フォルダの内容にアクセスできないようにします。Private フォルダへのアクセス許可を誤って付与しないようにするには、どのような方法があるでしょうか。このフォルダへのアクセスを明示的に拒否するポリシーを追加します。明示的な拒否は他のあらゆるアクセス許可よりも優先されます。

Private フォルダを非公開に保つには、次の 2 つの拒否ステートメントをグループポリシーに追加します。

- 次のステートメントを追加して、Private フォルダのリソースに対するあらゆるアクションを明示的に拒否します (companybucket/Private/*)。

```
{
  "Sid": "ExplictDenyAccessToPrivateFolderToEveryoneInTheGroup",
  "Action": ["s3:*"],
  "Effect": "Deny",
  "Resource":["arn:aws:s3:::companybucket/Private/*"]
}
```

- また、リクエストに Private/ プレフィックスが指定されている場合に、オブジェクトを一覧表示するアクションに必要なアクセス許可を拒否します。コンソールで Bob または Alice が Private フォルダを開くと、このポリシーにより Amazon S3 からエラーレスポンスが返されます。

```
{
  "Sid": "DenyListBucketOnPrivateFolder",
  "Action": ["s3:ListBucket"],
  "Effect": "Deny",
  "Resource": ["arn:aws:s3:::*"],
  "Condition":{
      "StringLike":{"s3:prefix":["Private/"]}
   }
}
```

Consultants グループポリシーを、前述の拒否ステートメントを含む更新したポリシーに置き換えます。更新したポリシーが適用されると、グループ内のどのユーザーも、バケット内の Private フォルダにアクセスできなくなります。

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。

   IAM ユーザーの認証情報ではなく、AWS アカウントの認証情報を使用してコンソールにサインインします。

2. Consultants グループにアタッチされている既存の AllowGroupToSeeBucketListInTheConsole 管理ポリシーを以下のポリシーに置き換えます。ポリシーの *companybucket* は自分のバケットの名前に置き換えてください。

   手順については、「IAM ユーザーガイド」の「カスタマー管理ポリシーの編集 (コンソール)」を参照してください。手順では、ポリシーがアタッチされているすべてのプリンシパルエンティティに変更を適用する指示に従ってください。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid":
 "AllowGroupToSeeBucketListAndAlsoAllowGetBucketLocationRequiredForListBucket",
      "Action": ["s3:ListAllMyBuckets", "s3:GetBucketLocation"],
```

```
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::*"]
    },
    {
      "Sid": "AllowRootLevelListingOfCompanyBucket",
      "Action": ["s3:ListBucket"],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::companybucket"],
      "Condition":{
          "StringEquals":{"s3:prefix":[""]}
       }
    },
    {
      "Sid": "RequireFolderStyleList",
      "Action": ["s3:ListBucket"],
      "Effect": "Deny",
      "Resource": ["arn:aws:s3:::*"],
      "Condition":{
          "StringNotEquals":{"s3:delimiter":"/"}
       }
     },
    {
      "Sid": "ExplictDenyAccessToPrivateFolderToEveryoneInTheGroup",
      "Action": ["s3:*"],
      "Effect": "Deny",
      "Resource":["arn:aws:s3:::companybucket/Private/*"]
    },
    {
      "Sid": "DenyListBucketOnPrivateFolder",
      "Action": ["s3:ListBucket"],
      "Effect": "Deny",
      "Resource": ["arn:aws:s3:::*"],
      "Condition":{
          "StringLike":{"s3:prefix":["Private/"]}
       }
    }
  ]
}
```

ステップ 8: クリーンアップする

クリーンアップするには、IAM コンソールを開き、ユーザーの Alice と Bob を削除します。手順については、「IAM ユーザーガイド」の「IAM ユーザーの削除」を参照してください。

ストレージへの不要な請求を防ぐために、この演習で作成したオブジェクトとバケットも削除してください。

関連リソース

- 「IAM ユーザーガイド」の「IAM ポリシーを管理する」

Amazon S3 のアイデンティティベースのポリシー例

このセクションでは、Amazon S3 へのユーザーアクセスを管理するための AWS Identity and Access Management (IAM) アイデンティティベースポリシーをいくつか示します。バケットポリシー (リソースベースのポリシー) の例については、「Amazon S3 のバケットポリシー」を参照してください。IAM ポリシー言語については、「Amazon S3 のポリシーとアクセス許可」を参照してください。

次のサンプルポリシーは、プログラムで使用する場合に機能します。ただし、Amazon S3 コンソールでこれらを使用するには、コンソールに必要な追加のアクセス許可を付与する必要があります。このようなポリシーの Amazon S3 コンソールでの使用の詳細については、ユーザーポリシーを使用したバケットへのアクセスの制御 を参照してください。

S3 リソースタイプ別の S3 API オペレーションへのアクセス許可の詳細については、「Amazon S3 API オペレーションに必要なアクセス許可」を参照してください。

トピック

- バケット の 1 つへのアクセスを IAM ユーザーに許可する
- バケット内のフォルダへのアクセスを各 IAM ユーザーに許可する
- Amazon S3 で共有フォルダを持つことをグループに許可する
- すべてのユーザーに対し、バケットの特定部分のオブジェクトの読み取りを許可する
- パートナーに対し、バケットの特定部分へのファイルのドロップを許可する
- 特定の AWS アカウント の Amazon S3 バケットへのアクセスを制限する
- 組織単位内の Amazon S3 バケットへのアクセスを制限する
- 組織内の Amazon S3 バケットへのアクセスを制限する

- AWS アカウント に PublicAccessBlock 設定を取得するアクセス許可を付与する
- バケット作成を 1 つのリージョンに制限する

バケット の 1 つへのアクセスを IAM ユーザーに許可する

この例では、AWS アカウントの IAM ユーザーに *amzn-s3-demo-bucket1* という 1 つのバケットに対する許可を付与して、ユーザーがオブジェクトを追加、更新、削除できるようにします。

このポリシーでは、ユーザーに s3:PutObject、s3:GetObject、s3:DeleteObject のアクセス許可を付与するだけでなく、s3:ListAllMyBuckets、s3:GetBucketLocation、および s3:ListBucket のアクセス許可も付与します。これらが、コンソールで必要とされる追加のアクセス許可です。またコンソール内のオブジェクトのコピー、カット、貼り付けを行うためには、s3:PutObjectAcl および s3:GetObjectAcl アクションが必要となります。コンソールを使用してユーザーにアクセス許可を付与してテストする例の解説については、ユーザーポリシーを使用したバケットへのアクセスの制御 を参照してください。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action": "s3:ListAllMyBuckets",
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action":["s3:ListBucket","s3:GetBucketLocation"],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1"
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:PutObjectAcl",
            "s3:GetObject",
            "s3:GetObjectAcl",
            "s3:DeleteObject"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1/*"
      }
   ]
```

```
}
```

バケット内のフォルダへのアクセスを各 IAM ユーザーに許可する

次の例では、Mary と Carlos という 2 人の IAM ユーザーに *amzn-s3-demo-bucket1* というバケットに対するアクセス許可を付与して、この 2 人がオブジェクトを追加、更新、削除できるようにします。ただし、バケット内の単一のプレフィックス (フォルダ) に全ユーザーのアクセスを制限したいとします。フォルダを作成する際、ユーザー名と同じフォルダ名にすることもできます。

```
amzn-s3-demo-bucket1
   Mary/
   Carlos/
```

各ユーザーに本人のフォルダのみへのアクセス権を付与するには、各ユーザー用のポリシーを作成し、個別にアタッチします。例えば、Mary に次のポリシーをアタッチして、*amzn-s3-demo-bucket1*/*Mary* フォルダに対する専用の Amazon S3 のアクセス許可を付与することができます。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:GetObject",
            "s3:GetObjectVersion",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1/Mary/*"
      }
   ]
}
```

その後、ユーザー Carlos に同様のポリシーをアタッチし、Resource 値のフォルダ *Carlos* を指定します。

各ユーザーにポリシーをアタッチするのではなく、ポリシー変数を使用する単一のポリシーを作成し、そのポリシーをグループにアタッチできます。まずグループを作成し、Mary と Carlos をいずれもそのグループに追加する必要があります。次のポリシーの例では、*amzn-s3-demo-bucket1*/${aws:username} フォルダに対する Amazon S3 の一連のアクセス許可を付与しています。ポリ

シーが評価されると、ポリシー変数 ${aws:username} はリクエスタのユーザー名で置き換えられます。例えば、Mary がオブジェクトの PUT リクエストを送信した場合、Mary が *amzn-s3-demo-bucket1*/Mary フォルダにオブジェクトをアップロードする PUT オペレーションのみが許可されます。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:GetObject",
            "s3:GetObjectVersion",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1/${aws:username}/*"
      }
   ]
}
```

> **Note**
>
> ポリシー変数を使用する場合は、2012-10-17 をポリシー内で明示的に指定する必要があります。IAM ポリシー言語のデフォルトバージョンは 2008-10-17 です。このバージョンでは、ポリシー変数をサポートしていません。

Amazon S3 コンソールで前述のポリシーをテストする場合、次のポリシーに示すように、追加のアクセス許可が必要となります。これらのアクセス許可をコンソールで使用する方法については、ユーザーポリシーを使用したバケットへのアクセスの制御 を参照してください。

```
{
 "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AllowGroupToSeeBucketListInTheConsole",
      "Action": [
       "s3:ListAllMyBuckets",
       "s3:GetBucketLocation"
```

```
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*"
    },
    {
      "Sid": "AllowRootLevelListingOfTheBucket",
      "Action": "s3:ListBucket",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1",
      "Condition":{
            "StringEquals":{
                   "s3:prefix":[""], "s3:delimiter":["/"]
                         }
               }
    },
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Action": "s3:ListBucket",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1",
      "Condition":{  "StringLike":{"s3:prefix":["${aws:username}/*"] }
       }
    },
      {
     "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
        "Effect":"Allow",
        "Action":[
           "s3:PutObject",
           "s3:GetObject",
           "s3:GetObjectVersion",
           "s3:DeleteObject",
           "s3:DeleteObjectVersion"
        ],
        "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1/${aws:username}/*"
      }
  ]
}
```

> **Note**
>
> 2012-10-17 バージョンのポリシーでは、ポリシー変数の先頭には $ が付きます。使用するオブジェクトキー (オブジェクト名) に $ が含まれている場合、この構文の変化により衝突が発生します。

この競合を回避するには、$ を使用して ${$} 文字を指定します。例えば、ポリシーにオブジェクトキー my$file を含めるには、my${$}file として指定します。

IAM ユーザー名は人間が読んで理解できるわかりやすい識別子ですが、グローバルで一意である必要はありません。例えば、Carlos が退職して別の Carlos が入社した場合、この別の Carlos が前の Carlos の情報にアクセスできます。

フォルダを作成する際に、ユーザー名の代わりに IAM ユーザー ID を使用することもできます。IAM ユーザー ID はそれぞれ一意であるためです。この場合、${aws:userid} ポリシー変数を使用するように前述のポリシーを修正する必要があります。ユーザー ID の詳細については、「IAM ユーザーガイド」の「IAM 識別子」を参照してください。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:GetObject",
            "s3:GetObjectVersion",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1/home/${aws:userid}/*"
      }
   ]
}
```

バケット内のフォルダへのアクセスを非 IAM ユーザー (モバイルアプリユーザー) に許可する

ユーザーのデータを S3 バケットに保存するモバイルゲームアプリを開発するとします。バケットに各アプリユーザーのフォルダを作成します。また、各ユーザーには本人のフォルダのみにアクセスを制限します。 ただし、ユーザーがアプリをダウンロードしてゲームをプレイし始める前にフォルダを作成することはできません。お客様にはユーザーのユーザー ID がないためです。

この場合、ユーザーには、Login with Amazon、 Facebook、または Google などのパブリックアイデンティプロバイダを使用してアプリにサインインするよう要求できます。ユーザーがこれらのプロバイダの 1 つを使用してアプリにサインインすると、ユーザー ID が設定されるため、お客様はこれを使用して実行時にユーザー固有のフォルダを作成することができます。

これにより、AWS Security Token Service のウェブ認証フェデレーションを使用して、アイデンティティプロバイダからの情報をアプリに組み入れ、各ユーザーの一時的なセキュリティ認証情報を取得することができます。続いて、IAM ポリシーを作成して、アプリがバケットにアクセスできるようにしたり、ユーザー固有のフォルダの作成、データのアップロードなどのオペレーションを実行できるようにすることができます。ウェブ ID フェデレーションの詳細については、IAM ユーザーガイドのウェブ ID フェデレーションについてを参照してください。

Amazon S3 で共有フォルダを持つことをグループに許可する

次のポリシーをグループにアタッチすることで、グループ内の全メンバーに Amazon S3 のフォルダ *amzn-s3-demo-bucket1*/share/marketing へのアクセス権が付与されます。グループメンバーは、この指定のフォルダのオブジェクトに対してのみ、ポリシーに示されている Amazon S3 の特定のアクセス許可を付与されます。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:GetObject",
            "s3:GetObjectVersion",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1/share/marketing/*"
      }
   ]
}
```

すべてのユーザーに対し、バケットの特定部分のオブジェクトの読み取りを許可する

次の例では、*AllUsers* というグループを作成し、AWS アカウントのすべての IAM ユーザーを含めます。次に、GetObject フォルダ内のオブジェクトに対してのみ GetObjectVersion と *amzn-s3-demo-bucket1*/readonly のアクセス権をグループに付与するポリシーをアタッチします。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
```

```
         "Effect":"Allow",
         "Action":[
            "s3:GetObject",
            "s3:GetObjectVersion"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1/readonly/*"
      }
   ]
}
```

パートナーに対し、バケットの特定部分へのファイルのドロップを許可する

次の例では、パートナー会社を表す *AnyCompany* というグループを作成します。パートナー会社でアクセス許可が必要な個人やアプリケーションのために IAM ユーザーを作成し、そのユーザーをグループに入れます。

次に、バケット内の次のフォルダに対する PutObject アクセス権をグループに付与するポリシーをアタッチします。

amzn-s3-demo-bucket1/uploads/anycompany

このバケットに対する他の操作を *AnyCompany* グループに禁止するには、PutObjectで Amazon S3 のリソースに対する AWS アカウント 以外の Amazon S3 のアクションを明示的に拒否するステートメントを追加します。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":"s3:PutObject",
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1/uploads/anycompany/*"
      },
      {
         "Effect":"Deny",
         "Action":"s3:*",
         "NotResource":"arn:aws:s3:::amzn-s3-demo-bucket1/uploads/anycompany/*"
      }
   ]
}
```

特定の AWS アカウント の Amazon S3 バケットへのアクセスを制限する

Amazon S3 プリンシパルが信頼された内のリソースにのみアクセスしていることを確認する場合 AWS アカウントでは、アクセスを制限できます。たとえば、このアイデンティティベースの IAM ポリシーは、Deny 効果を使用して Amazon S3 アクションへのアクセスをブロックします。ただし、アクセスされている Amazon S3 リソースがアカウント *222222222222* 内の場合は除きます。AWS アカウント の IAM プリンシパルがカウント外の Amazon S3 オブジェクトにアクセスすることを防止するには、次の IAM ポリシーをアタッチします。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyS3AccessOutsideMyBoundary",
      "Effect": "Deny",
      "Action": [
        "s3:*"
      ],
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:ResourceAccount": [
            "222222222222"
          ]
        }
      }
    }
  ]
}
```

> **Note**
>
> このポリシーは、アクセス権を付与しないため、既存の IAM アクセスコントロールに置き換わるものではありません。代わりに、このポリシーは、他の IAM ポリシーによって付与されたアクセス権限に関係なく、他の IAM アクセス権限の追加ガードレールとして機能します。

ポリシーのアカウント ID *222222222222* を自身のポリシー AWS アカウント に必ず置き換えます。この制限を維持しながら複数のアカウントにポリシーを適用するには、アカウント ID を

aws:PrincipalAccount 条件キーに置き換えます。この条件では、プリンシパルとリソースが同じアカウントにある必要があります。

組織単位内の Amazon S3 バケットへのアクセスを制限する

AWS Organizations でセットアップされた組織単位 (OU)がある場合、Amazon S3 バケットのアクセスを組織の特定部分に制限することができます。この例では、aws:ResourceOrgPaths キーを使って組織の OU へ Amazon S3 バケットのアクセスを制限します。この例では、OU ID は *ou-acroot-exampleou* です。自身のポリシーでこの値を自身の OU ID に置き換えてください。

```
{
   "Version": "2012-10-17",
   "Statement": [
     {
       "Sid": "AllowS3AccessOutsideMyBoundary",
       "Effect": "Allow",
       "Action": [
         "s3:*"
       ],
       "Resource": "*",
       "Condition": {
         "ForAllValues:StringNotLike": {
           "aws:ResourceOrgPaths": [
             "o-acorg/r-acroot/ou-acroot-exampleou/"
           ]
         }
       }
     }
   ]
 }
```

> **Note**
>
> このポリシーは、アクセス許可を付与しません。代わりに、このポリシーは、他の IAM アクセス権限のバックストップとして機能し、プリンシパルが OU 定義の境界外にある Amazon S3 オブジェクトにアクセスするのを防ぎます。

このポリシーは、アクセスされている Amazon S3 オブジェクトが組織内の *ou-acroot-exampleou* OU 内に存在しない場合、Amazon S3 アクションへのアクセスを拒否します。IAM ポリシー条件は、リストされた OU パスを含めるのに、複数値を持つ条件キー

aws:ResourceOrgPaths を要求します。このポリシーは、ForAllValues:StringNotLike 演算子を使用して aws:ResourceOrgPaths の値をリストされた OU と比較します (大文字と小文字は区別しません)。

組織内の Amazon S3 バケットへのアクセスを制限する

組織内の Amazon S3 オブジェクトへのアクセスを制限するには、組織のルートに IAM ポリシーをアタッチし、組織内のすべてのアカウントに適用します。IAM プリンシパルにこのルールに従うように要求するには、サービスコントロールポリシー (SCP) を使用します。SCP を使用する場合は、組織のルートにポリシーをアタッチする前に、SCP のテストをしっかりと実行してください。

次のポリシー例では、アクセスされている Amazon S3 オブジェクトが、それにアクセスしている IAM プリンシパルと同じ組織内に存在しない限り、Amazon S3 アクションへのアクセスが拒否されます。

```
{
   "Version": "2012-10-17",
   "Statement": [
     {
       "Sid": "DenyS3AccessOutsideMyBoundary",
       "Effect": "Deny",
       "Action": [
         "s3:*"
       ],
       "Resource": "arn:aws:s3:::*/*",
       "Condition": {
         "StringNotEquals": {
           "aws:ResourceOrgID": "${aws:PrincipalOrgID}"
         }
       }
     }
   ]
 }
```

> **Note**
>
> このポリシーは、アクセス許可を付与しません。代わりに、このポリシーは、他の IAM アクセス権限のバックストップとして機能し、プリンシパルが組織外にある Amazon S3 オブジェクトにアクセスするのを防ぎます。このポリシーは、ポリシーが有効になった後に作成される Amazon S3 リソースにも適用されます。

この例の IAM ポリシー条件では、互いに等しい aws:ResourceOrgID および aws:PrincipalOrgID が必要です。この要件では、リクエストを行うプリンシパルとアクセスされるリソースが同じ組織内になければなりません。

AWS アカウント に PublicAccessBlock 設定を取得するアクセス許可を付与する

以下のアイデンティティベースのポリシーの例は、ユーザーに s3:GetAccountPublicAccessBlock のアクセス許可を付与します。これらのアクセス許可については、Resource 値を "*" に設定します。リソース ARN については、「Amazon S3 のポリシーリソース」を参照してください。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"statement1",
         "Effect":"Allow",
         "Action":[
            "s3:GetAccountPublicAccessBlock"
         ],
         "Resource":[
            "*"
         ]
       }
    ]
}
```

バケット作成を 1 つのリージョンに制限する

例えば、AWS アカウント の管理者がユーザー (Dave) に南米 (サンパウロ) リージョンでのみバケットを作成できる許可を付与するとします。アカウント管理者は、以下のように条件を指定して、s3:CreateBucket のアクセス許可を付与する次のユーザーポリシーをアタッチします。Condition ブロックのキーと値のペアは、s3:LocationConstraint キーと、その値として sa-east-1 リージョンを指定します。

> **Note**
>
> この例では、バケット所有者はユーザーの 1 人にアクセス許可を付与するため、バケットポリシーまたはユーザーポリシーのどちらでも使用することができます。この例では、ユーザーポリシーを使用します。

Amazon S3 リージョンのリストについては、AWS 全般のリファレンス の「リージョンとエンドポイント」を参照してください。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"statement1",
         "Effect":"Allow",
         "Action": "s3:CreateBucket",
         "Resource": "arn:aws:s3:::*",
         "Condition": {
             "StringLike": {
                 "s3:LocationConstraint": "sa-east-1"
             }
         }
       }
    ]
}
```

明示的な拒否を追加する

上記のポリシーは、ユーザーが sa-east-1 以外のリージョンでバケットを作成することを制限します。ただし、他の一部のポリシーで、このユーザーに別のリージョンでバケットを作成するアクセス許可を付与する場合があります。例えば、ユーザーがグループに属している場合、グループのアクセス許可内にいるすべてのユーザーが別のリージョンでバケットを作成できるように、ポリシーがアタッチされている場合があります。ユーザーに別のリージョンでバケットを作成するアクセス許可が付与されないように、上記のポリシーに明示的な拒否のステートメントを追加します。

Deny ステートメントは、StringNotLike 条件を使用します。つまり、場所の制約が sa-east-1 でない場合、バケットの作成リクエストは拒否されます。明示的な拒否を使用すれば、どのようなアクセス権限が付与されている場合でも、ユーザーは別のリージョンでバケットを作成できなくなります。次のポリシーには、明示的な拒否ステートメントが含まれています。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"statement1",
         "Effect":"Allow",
         "Action": "s3:CreateBucket",
```

```
          "Resource": "arn:aws:s3:::*",
          "Condition": {
              "StringLike": {
                  "s3:LocationConstraint": "sa-east-1"
              }
          }
        },
       {
          "Sid":"statement2",
          "Effect":"Deny",
          "Action": "s3:CreateBucket",
          "Resource": "arn:aws:s3:::*",
          "Condition": {
              "StringNotLike": {
                  "s3:LocationConstraint": "sa-east-1"
              }
          }
        }
    ]
}
```

AWS CLI でポリシーをテストする

このポリシーは、次の `create-bucket` AWS CLI コマンドを使用してテストできます。この例では、`bucketconfig.txt` ファイルを使用して場所の制約を指定しています。Windows ファイルパスに注目してください。バケットの名前とパスを適切に更新する必要があります。`--profile` パラメータを使用して、ユーザーの認証情報を指定する必要があります。AWS CLI のセットアップと使用の詳細については、「Amazon S3 API リファレンス」の「Developing with Amazon S3 using the AWS CLI」を参照してください。

```
aws s3api create-bucket --bucket examplebucket --profile AccountADave --create-bucket-
configuration file://c:/Users/someUser/bucketconfig.txt
```

`bucketconfig.txt` ファイルは、次のように設定を指定します。

```
{"LocationConstraint": "sa-east-1"}
```

チュートリアル: ポリシーを使用した Amazon S3 リソースへのアクセスの管理

このトピックでは、Amazon S3 リソースへのアクセスの付与について、次の基本的なチュートリアル例を示します。これらの例では、AWS Management Console を使用してリソース (バケット、オブジェクト、ユーザー) を作成し、アクセス許可を付与します。また、これらの例では、コマンドラインツールを使用してアクセス許可を確認する方法を示します。コードを記述する必要はありません。AWS Command Line Interface (AWS CLI) と AWS Tools for Windows PowerShell の両方を使用したコマンドを使用することができます。

- 例 1: バケット所有者がユーザーにバケットのアクセス許可を付与する

  デフォルトでは、使用するアカウントで作成した IAM ユーザーにアクセス許可はありません。この演習では、バケットおよびオブジェクト操作を実行するためのアクセス許可をユーザーに付与します。
- 例 2: バケット所有者がクロスアカウントのバケットのアクセス許可を付与する

  この演習では、バケット所有者 (アカウント A) が別の AWS アカウント (アカウント B) に対してクロスアカウントの許可を付与します。次に、アカウント B でこれらの許可を、そのアカウントのユーザーに委任します。
- オブジェクト所有者とバケット所有者が同じではない場合のオブジェクトのアクセス許可の管理

  このシナリオ例は、バケット所有者が他のユーザーにオブジェクトのアクセス許可を付与しますが、バケット内のすべてのオブジェクトをバケット所有者が所有しているわけではないという場合です。バケット所有者にはどのようなアクセス許可が必要になり、それらのアクセス許可をどのように委任できるのでしょうか。

  バケットを作成する AWS アカウント は、バケット所有者と呼ばれます。この所有者は、オブジェクトをアップロードする許可を他の AWS アカウントに付与することができ、オブジェクトを作成する AWS アカウントがオブジェクトを所有しています。バケット所有者には、他の AWS アカウントで作成されたオブジェクトに対する許可はありません。バケット所有者がオブジェクトへのアクセス権を付与するバケットポリシーを作成する場合、そのポリシーは他のアカウントが所有するオブジェクトには適用されません。

  この場合、オブジェクト所有者は、オブジェクト ACL を使用して、まずバケット所有者にアクセス許可を付与する必要があります。バケット所有者は、以下の例に示すように、これらのオブジェクトの許可を、他のユーザー、自分のアカウントのユーザー、または別の AWS アカウントに委任できます。

- 例 3: バケット所有者が自分の所有していないオブジェクトに対するアクセス許可を付与する

  この演習では、バケット所有者は最初にオブジェクト所有者からアクセス許可を取得します。次に、バケット所有者は、自分のアカウントのユーザーにそのアクセス許可を委任します。

- 例 4 - バケット所有者が所有権のないオブジェクトへのクロスアカウントアクセス許可を付与する

  オブジェクトの所有者からアクセス許可を取得した後も、クロスアカウントの委任がサポートされていないため、バケット所有者は他の AWS アカウント にアクセス許可を委任できません (「アクセス許可の委任」を参照)。代わりに、バケット所有者は、特定のオペレーション (オブジェクトの取得など) を実行する許可を持つ IAM ロールを作成し、別の AWS アカウントがそのロールを引き受けることを許可できます。このロールを引き受けるすべてのユーザーがオブジェクトにアクセスできます。この例では、バケット所有者が IAM ロールを使用してこのクロスアカウントの委任を有効にする方法を示します。

チュートリアル例を実行する前に

これらの例では、AWS Management Console を使用してリソースを作成し、アクセス許可を付与します。許可をテストするために、この例ではコマンドラインツール AWS CLI および AWS Tools for Windows PowerShell を使用するため、コードを書く必要はありません。アクセス許可をテストするには、これらのツールのいずれかをセットアップする必要があります。詳細については、「チュートリアル用のツールのセットアップ」を参照してください。

さらに、これらの例では、リソースの作成時に AWS アカウントのルートユーザー認証情報を使用しません。代わりに、アカウントに、これらのタスクを実行するための管理者ユーザーを作成します。

管理者ユーザーを使用したリソースの作成とアクセス許可の付与について

AWS Identity and Access Management (IAM) では、AWS アカウントのルートユーザー認証情報を使用してリクエストを行わないようお勧めします。代わりに、IAM ユーザーまたはロールを作成してフルアクセスを許可し、そのユーザーまたはロールの認証情報を使用してリクエストを行います。このユーザーを管理者ユーザーまたはロールと呼びます。詳細については、AWS 全般のリファレンスの「AWS アカウントのルートユーザー の認証情報と IAM ID」と IAM ユーザーガイドの「IAM のベストプラクティス」を参照してください。

このセクションのすべてのチュートリアル例では、管理者ユーザーの認証情報を使用します。まだ AWS アカウントの管理者ユーザーを作成していない場合は、トピックでその方法を説明します。

ユーザーの認証情報を使用して AWS Management Console にサインインするには、IAM ユーザーのサインイン URL を使用する必要があります。IAM コンソールは、AWS アカウント にこの URL を提供します。トピックで、この URL を取得する方法を示します。

チュートリアル用のツールのセットアップ

導入例 (チュートリアル: ポリシーを使用した Amazon S3 リソースへのアクセスの管理 を参照) では、AWS Management Console を使用してリソースを作成し、アクセス許可を付与します。許可をテストするために、この例ではコマンドラインツール AWS Command Line Interface (AWS Tools for Windows PowerShell)および AWS CLI を使用するため、コードを書く必要はありません。アクセス許可をテストするには、これらのツールのいずれかをセットアップする必要があります。

AWS CLI をセットアップする方法

1. AWS CLI をダウンロードして設定します。手順については、「AWS Command Line Interface ユーザーガイド」の次のトピックを参照してください。

   AWS Command Line Interface の最新バージョンのインストールまたは更新

   AWS Command Line Interface の開始方法
2. デフォルトのプロファイルを設定します。

   ユーザーの認証情報を AWS CLI 設定ファイルに格納します。AWS アカウントの認証情報を使用して設定ファイルにデフォルトのプロファイルを作成します。AWS CLI 設定ファイルの検索と編集の手順については、「Configuration and credential file settings」を参照してください。

   ```
   [default]
   aws_access_key_id = access key ID
   aws_secret_access_key = secret access key
   region = us-west-2
   ```
3. コマンドプロンプトで以下のコマンドを入力して、セットアップを確認します。これらのコマンドは、いずれも認証情報を明示的に提供しないため、デフォルトプロファイルの認証情報が使用されます。

   - help コマンドを試してみます。

     ```
     aws help
     ```
   - 設定したアカウントのバケットのリストを取得するには、aws s3 ls コマンドを使用します。

```
aws s3 ls
```

このチュートリアルでは、以下の例に示すように、ユーザーを作成し、プロファイルを作成することによってユーザー認証情報を設定ファイルに保存します。これらのプロファイルには、AccountAadmin と AccountBadmin の名前があります。

```
[profile AccountAadmin]
aws_access_key_id = User AccountAadmin access key ID
aws_secret_access_key = User AccountAadmin secret access key
region = us-west-2

[profile AccountBadmin]
aws_access_key_id = Account B access key ID
aws_secret_access_key = Account B secret access key
region = us-east-1
```

これらのユーザー認証情報を使用してコマンドを実行するには、プロファイル名を指定する --profile パラメータを追加します。次の AWS CLI コマンドは、*examplebucket* 内のオブジェクトのリストを取得し、AccountBadmin プロファイルを指定します。

```
aws s3 ls s3://examplebucket --profile AccountBadmin
```

また、コマンドプロンプトから AWS_DEFAULT_PROFILE 環境変数を変更することで、ユーザー認証情報セットをデフォルトプロファイルとして設定できます。これを行うと、--profile パラメータを指定せずに AWS CLI コマンドを実行するたびに、AWS CLI は環境変数でデフォルトプロファイルとして設定したプロファイルを使用します。

```
$ export AWS_DEFAULT_PROFILE=AccountAadmin
```

AWS Tools for Windows PowerShell をセットアップする

1. AWS Tools for Windows PowerShell をダウンロードして設定します。手順については、「AWS Tools for Windows PowerShell ユーザーガイド」の「Installing the AWS Tools for Windows PowerShell」を参照してください。

> **Note**
>
> AWS Tools for Windows PowerShell モジュールをロードするには、PowerShell スクリプトの実行を有効にする必要があります。詳細については、「AWS Tools for Windows PowerShell ユーザーガイド」の「Enable Script Execution」を参照してください。

2. これらのチュートリアルでは、Set-AWSCredentials コマンドを使用して、セッションごとに AWS 認証情報を指定します。このコマンドは永続的なストア (-StoreAs パラメータ) に認証情報を格納します。

```
Set-AWSCredentials -AccessKey AccessKeyID -SecretKey SecretAccessKey -
storeas string
```

3. セットアップを確認します。

   - Amazon S3 オペレーションで使用できるコマンドのリストを取得するには、Get-Command コマンドを実行します。

     ```
     Get-Command -module awspowershell -noun s3* -StoredCredentials string
     ```

   - バケット内のオブジェクトのリストを取得するには、Get-S3Object コマンドを実行します。

     ```
     Get-S3Object -BucketName bucketname -StoredCredentials string
     ```

コマンドのリストについては、「AWS Tools for PowerShell Cmdlet Reference」を参照してください。

これで、チュートリアルを行う準備ができました。各セクションの冒頭に示されているリンクをクリックしてください。

例 1: バケット所有者がユーザーにバケットのアクセス許可を付与する

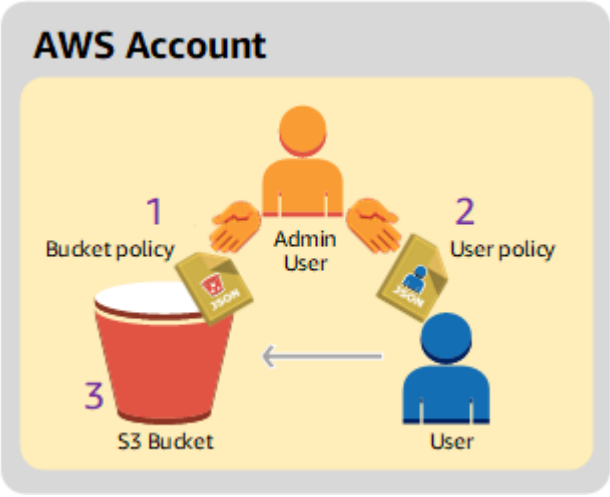
> **Important**
>
> IAM ロールへのアクセス許可の付与は、個別のユーザーへのアクセス許可の付与より優れた方法です。IAM ロールへのアクセス許可の付与方法の詳細については、「クロスアカウントのアクセス許可の理解と IAM ロールの使用」を参照してください。

トピック

- チュートリアルの準備をする
- ステップ 1: アカウント A でリソースを作成して、アクセス許可を付与する
- ステップ 2: アクセス許可をテストする

このチュートリアルでは、AWS アカウント がバケットを所有し、アカウントに IAM ユーザーが含まれています。デフォルトでは、ユーザーにはアクセス許可はありません。何らかのタスクを実行するユーザーには、親アカウントがそのためのアクセス許可をユーザーに付与する必要があります。バケット所有者と親アカウントは同じです。したがって、バケットへの許可をユーザーに付与するには、AWS アカウントは、バケットポリシー、ユーザーポリシー、またはその両方を使用することができます。アカウント所有者は、一部のアクセス許可はバケットポリシーを使用し、他のアクセス許可はユーザーポリシーを使用して付与します。

手順の概要を以下に示します。



1. アカウント管理者は、ユーザーに一連のアクセス許可を付与するバケットポリシーを作成します。

2. アカウント管理者は、ユーザーポリシーをユーザーにアタッチして、追加のアクセス許可を付与します。
3. これによりユーザーは、バケットポリシーとユーザーポリシーの両方を通じて付与されているアクセス許可を使用できます。

この例では、AWS アカウントが必要です。アカウントのルートユーザー認証情報を使用する代わりに、管理者ユーザーを作成します (「管理者ユーザーを使用したリソースの作成とアクセス許可の付与について」を参照してください)。ここ例の AWS アカウント および管理者ユーザーは、次のとおりです。

アカウント ID	アカウントの呼び方	アカウントの管理者ユーザー
1111-1111-1111	アカウント A	AccountAadmin

> **Note**
>
> この例では、管理者ユーザーは AccountAadmin で、アカウント A を参照しており、AccountAdmin ではありません。

ユーザーを作成し、アクセス許可を付与するためのすべてのタスクは、AWS Management Console で実行します。このチュートリアルでは、許可を検証するために、コマンドラインツールの AWS Command Line Interface (AWS CLI) と AWS Tools for Windows PowerShell を使用するので、コードを記述する必要はありません。

チュートリアルの準備をする

1. AWS アカウントが存在し、管理者権限を持つユーザーが存在することを確認します。

   a. 必要な場合、AWS アカウントにサインアップします。このアカウントをアカウント A と呼びます。

      i. https://aws.amazon.com/s3 に移動して、[AWS アカウントの作成] を選択します。

      ii. 画面上の指示に従ってください。

      アカウントがアクティブになり、使用可能な状態になったら、AWS から E メールで通知が届きます。

b. アカウント A に管理者ユーザー **AccountAadmin** を作成します。アカウント A の認証情報を使用して、IAM コンソールにサインインし、次の操作を行います。

i. ユーザー **AccountAadmin** を作成して、ユーザーのセキュリティ認証情報を書き留めます。

手順については、「IAM ユーザーガイド」の「AWS アカウント での IAM ユーザーの作成」を参照してください。

ii. フルアクセスを付与するユーザーポリシーをアタッチして、管理者に AccountAadmin を付与します。

手順については、「IAM ユーザーガイド」の「IAM ポリシーを管理する」を参照してください。

iii. AccountAadmin の IAM ユーザーサインイン URL を書き留めます。この URL は AWS Management Console にサインインする際に使用する必要があります。サインイン URL を見つける方法については、「IAM ユーザーガイド」の「Sign in to the AWS Management Console as an IAM user」を参照してください。URL はアカウントごとにメモしてください。

2. AWS CLI または AWS Tools for Windows PowerShell をセットアップします。管理者ユーザーの認証情報は以下のように保存します。

- AWS CLI を使用する場合は、設定ファイルに `AccountAadmin` プロファイルを作成します。
- AWS Tools for Windows PowerShell を使用する場合は、セッションの認証情報を `AccountAadmin` として保存します。

手順については、「チュートリアル用のツールのセットアップ」を参照してください。

ステップ 1: アカウント A でリソースを作成して、アクセス許可を付与する

アカウント A のユーザー `AccountAadmin` の認証情報と、IAM ユーザー専用のサインイン URL を使用して、AWS Management Consoleにサインインし、次の操作を行います。

1. バケットリソースと IAM ユーザーリソースの作成

a. Amazon S3 コンソールでバケットを作成します。バケットを作成した AWS リージョン を書き留めます。手順については、「汎用バケットの作成」を参照してください。

b. IAM コンソールで次の操作を行います。

i. Dave という名前のユーザーを作成します。

詳細な手順については、「IAM ユーザーガイド」の「IAM ユーザーの作成 (コンソール)」を参照してください。

ii. UserDave 認証情報を書き留めます。

iii. ユーザー Dave の Amazon リソースネーム (ARN) を書き留めます。IAM コンソールでユーザーを選択すると、[概要] タブにユーザー ARN が表示されます。

2. アクセス許可を付与します。

バケット所有者とユーザーが属する親アカウントが同じであるため、AWS アカウントは、バケットポリシー、ユーザーポリシー、またはその両方を使用してユーザーに許可を付与できます。この例では、両方を使用します。オブジェクトの所有者も同じアカウントである場合は、バケット所有者はバケットポリシー (または IAM ポリシー) でオブジェクトのアクセス権を付与することもできます。

a. Amazon S3 コンソールで、次のバケットポリシーを *awsexamplebucket1* にアタッチします。

このポリシーには 2 つのステートメントがあります。

- 最初のステートメントは、バケットオペレーションのアクセス許可 s3:GetBucketLocation と s3:ListBucket を Dave に付与します。
- 2 番目のステートメントは、アクセス許可 s3:GetObject を付与します。アカウント A はオブジェクトの所有者でもあるので、アカウント管理者はアクセス許可 s3:GetObject を付与できます。

Principal ステートメントでは、Dave はユーザー ARN によって識別されます。ポリシーエレメントの詳細については、Amazon S3 のポリシーとアクセス許可 を参照してください。

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "statement1",
         "Effect": "Allow",
         "Principal": {
            "AWS": "arn:aws:iam::AccountA-ID:user/Dave"
```

```
            },
            "Action": [
               "s3:GetBucketLocation",
               "s3:ListBucket"
            ],
            "Resource": [
               "arn:aws:s3:::awsexamplebucket1"
            ]
         },
         {
            "Sid": "statement2",
            "Effect": "Allow",
            "Principal": {
               "AWS": "arn:aws:iam::AccountA-ID:user/Dave"
            },
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
               "arn:aws:s3:::awsexamplebucket1/*"
            ]
         }
   ]
}
```

b. 以下のポリシーを使用して、ユーザー Dave のインラインポリシーを作成します。このポリシーは、s3:PutObject アクセス許可を Dave に付与します。バケット名を指定してポリシーを更新する必要があります。

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "PermissionForObjectOperations",
         "Effect": "Allow",
         "Action": [
            "s3:PutObject"
         ],
         "Resource": [
            "arn:aws:s3:::awsexamplebucket1/*"
         ]
      }
   ]
```

```
}
```

手順については、「IAM ユーザーガイド」の「IAM ポリシーを管理する」を参照してください。コンソールにサインインするには、アカウント A の認証情報を使用する必要があります。

ステップ 2: アクセス許可をテストする

Dave の認証情報を使用して、アクセス許可が機能することを確認します。次の 2 つの手順のいずれかを使用できます。

AWS CLI を使用してアクセス許可をテストする

1. 次の UserDaveAccountA プロファイルを追加して、AWS CLI 設定ファイルを更新します。詳細については、「チュートリアル用のツールのセットアップ」を参照してください。

```
[profile UserDaveAccountA]
aws_access_key_id = access-key
aws_secret_access_key = secret-access-key
region = us-east-1
```

2. Dave がユーザーポリシーで許可されたオペレーションを実行できることを確認します。次の AWS CLI put-object コマンドを使用して、サンプルのオブジェクトをアップロードします。

   アップロードするソースファイルは、コマンドの --body パラメータで指定します。例えば、ファイルが Windows 端末の C: ドライブのルートにある場合、c:\HappyFace.jpg と指定します。--key パラメータは、オブジェクトのキー名を指定します。

```
aws s3api put-object --bucket awsexamplebucket1 --key HappyFace.jpg --
body HappyFace.jpg --profile UserDaveAccountA
```

   次の AWS CLI コマンドを実行して、オブジェクトを取得します。

```
aws s3api get-object --bucket awsexamplebucket1 --key HappyFace.jpg OutputFile.jpg
 --profile UserDaveAccountA
```

AWS Tools for Windows PowerShell を使用してアクセス許可をテストする

1. Dave の認証情報を AccountADave という名前で保存します。次に、この認証情報を使用して、オブジェクトの PUT と GET を実行します。

```
set-awscredentials -AccessKey AccessKeyID -SecretKey SecretAccessKey -storeas
 AccountADave
```

2. 保存したユーザー Dave の認証情報を使用して、AWS Tools for Windows PowerShell `Write-S3Object` コマンドでサンプルオブジェクトをアップロードします。

```
Write-S3Object -bucketname awsexamplebucket1 -key HappyFace.jpg -file HappyFace.jpg
 -StoredCredentials AccountADave
```

先にアップロードしたオブジェクトをダウンロードします。

```
Read-S3Object -bucketname awsexamplebucket1 -key HappyFace.jpg -file Output.jpg -
StoredCredentials AccountADave
```

例 2: バケット所有者がクロスアカウントのバケットのアクセス許可を付与する

> **Important**
>
> アクセス許可は、個々のユーザーではなく、IAM ロールに付与することをお勧めします。これを行う方法については、クロスアカウントのアクセス許可の理解と IAM ロールの使用を参照してください。

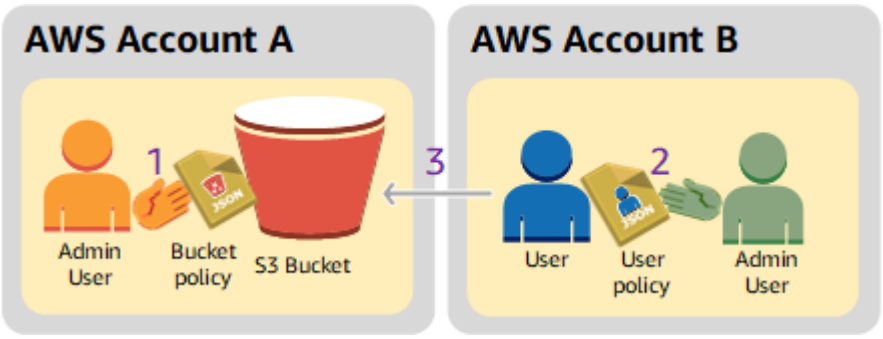
トピック

- チュートリアルの準備をする
- ステップ 1: アカウント A のタスクを実行する
- ステップ 2: アカウント B のタスクを実行する
- ステップ 3: (オプション) 明示的な拒否を試す
- ステップ 4: クリーンアップする

ある AWS アカウント (例えば、アカウント A) で、バケットやオブジェクトなど、そのリソースにアクセスするためのアクセス許可を、別の AWS アカウント (アカウント B) に付与できます。アカウント B では、そのアカウントのユーザーに、付与されたアクセス許可を委任できます。この例のシナリオでは、バケット所有者が、特定のバケットオペレーションを実行するためのクロスアカウントアクセス許可を別のアカウントに付与します。

> **Note**
>
> また、バケットポリシーを使用して、アカウント A から直接アカウント B のユーザーにアクセス許可を付与することもできます。ただし、このユーザーには、アカウント B がアカウント A からアクセス許可を付与されていない場合でも、ユーザーが属している親アカウントであるアカウント B からのアクセス許可が必要です。このユーザーがリソース所有者と親アカウントの両方からのアクセス許可を持っている場合にのみ、ユーザーはリソースにアクセスできます。

この手順の概要を以下に示します。



1. アカウント A の管理者ユーザーは、特定のバケットオペレーションを実行するための、クロスアカウントアクセス許可を付与するバケットポリシーをアカウント B にアタッチします。

   アカウント B の管理者ユーザーは、自動的にこのアクセス許可を継承することに注意してください。
2. アカウント B の管理者ユーザーは、アカウント A から受け取ったアクセス許可を委任するユーザーポリシーをユーザーにアタッチします。
3. アカウント B のユーザーは、アカウント A が所有するバケットのオブジェクトにアクセスすることにより、アクセス許可を確認します。

この例では、2 個のアカウントが必要です。次の表に、これらのアカウントとそれぞれの管理者ユーザーの呼び方を示します。IAM ガイドライン (「管理者ユーザーを使用したリソースの作成とアクセス許可の付与について」を参照) に従い、このチュートリアルではルートユーザー認証情報は使用しません。その代わりに、各アカウントで管理者ユーザーを作成し、その認証情報を使用してリソースを作成し、アクセス許可を付与します。

AWS アカウント ID	アカウントの呼び方	アカウントの管理者ユーザー
1111-1111-1111	アカウント A	AccountAadmin
2222-2222-2222	アカウント B	AccountBadmin

ユーザーを作成し、アクセス許可を付与するためのすべてのタスクは、AWS Management Console で実行します。このチュートリアルでは、許可を検証するために、コマンドラインツールの AWS Command Line Interface (CLI) と AWS Tools for Windows PowerShell を使用するので、コードを記述する必要はありません。

チュートリアルの準備をする

1. 前のセクションの表に示したように、2 個の AWS アカウントがあり、各アカウントに 1 人ずつの管理者ユーザーが存在することを確認します。

   a. 必要な場合、AWS アカウントにサインアップします。

   b. アカウント A の認証情報を使用して、IAM コンソールにサインインし、管理者ユーザーを作成します。

      i. ユーザー **AccountAadmin** を作成して、セキュリティ認証情報を書き留めます。手順については、IAM ユーザーガイドの「AWS アカウントでの IAM ユーザーの作成」を参照してください。

      ii. フルアクセスを付与するユーザーポリシーをアタッチして、管理者に AccountAadmin を付与します。手順については、IAM ユーザーガイドの IAM ポリシーの管理を参照してください。

   c. IAM コンソールの [ダッシュボード] の IAM ユーザーサインイン URL をメモします このアカウントのすべてのユーザーは、AWS Management Console にサインインするときにこの URL を使用する必要があります。

      詳細については、IAM ユーザーガイドのユーザーがお客様のアカウントにサインインする方法 を参照してください。

   d. 前述のステップを、アカウント B の認証情報を使用してもう一度実行し、管理者ユーザー **AccountBadmin** を作成します。

2. AWS Command Line Interface (AWS CLI) または AWS Tools for Windows PowerShell をセットアップします。管理者ユーザーの認証情報は以下のように保存します。

   - AWS CLI を使用する場合は、設定ファイルに `AccountAadmin` と `AccountBadmin` の 2 つのプロファイルを作成します。
   - AWS Tools for Windows PowerShell を使用する場合は、セッションの認証情報を `AccountAadmin` および `AccountBadmin` として保存します。

   手順については、「チュートリアル用のツールのセットアップ」を参照してください。

3. プロファイルとも呼ばれる、管理者ユーザーの認証情報を保存します。入力する各コマンドで認証情報を指定する代わりにプロファイル名を使用できます。詳細については、「チュートリアル用のツールのセットアップ」を参照してください。

a. 2 つのアカウントの管理者ユーザー (AccountAadmin および AccountBadmin) のそれぞれの AWS CLI 認証情報ファイルにプロファイルを追加します。

```
[AccountAadmin]
aws_access_key_id = access-key-ID
aws_secret_access_key = secret-access-key
region = us-east-1

[AccountBadmin]
aws_access_key_id = access-key-ID
aws_secret_access_key = secret-access-key
region = us-east-1
```

b. AWS Tools for Windows PowerShell を使用している場合は、次のコマンドを実行します。

```
set-awscredentials -AccessKey AcctA-access-key-ID -SecretKey AcctA-secret-
access-key -storeas AccountAadmin
set-awscredentials -AccessKey AcctB-access-key-ID -SecretKey AcctB-secret-
access-key -storeas AccountBadmin
```

ステップ 1: アカウント A のタスクを実行する

ステップ 1.1: AWS Management Consoleにサインインする

アカウント A で IAM ユーザーのサインイン URL を使用して、まず AccountAadmin ユーザーとして AWS Management Console にサインインします。このユーザーはバケットを作成し、ポリシーをアタッチします。

ステップ 1.2: バケットを作成する

1. Amazon S3 コンソールでバケットを作成します。この演習では、米国東部 (バージニア北部) AWS リージョン に *amzn-s3-demo-bucket* という名前でバケットを作成することを前提とします。

   手順については、「汎用バケットの作成」を参照してください。

2. サンプルオブジェクトをバケットにアップロードします。

   方法については、ステップ 2: バケットにオブジェクトをアップロードする を参照してください。

ステップ 1.3: クロスアカウントアクセス許可を付与するバケットポリシーをアカウント B にアタッチする

このバケットポリシーは、s3:GetLifecycleConfiguration および s3:ListBucket アクセス許可をアカウント B に付与します。これは、AccountAadmin ユーザーの認証情報を使用してコンソールにサインインしていることを前提としています。

1. 次のバケットポリシーを *amzn-s3-demo-bucket* にアタッチします。このポリシーは、アカウント B に s3:GetLifecycleConfiguration および s3:ListBucket アクションのアクセス許可を付与します。

   手順については、「Amazon S3 コンソールを使用したバケットポリシーの追加」を参照してください。

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Example permissions",
         "Effect": "Allow",
         "Principal": {
            "AWS": "arn:aws:iam::AccountB-ID:root"
         },
         "Action": [
            "s3:GetLifecycleConfiguration",
            "s3:ListBucket"
         ],
         "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket"
         ]
      }
   ]
}
```

2. アカウント B (とその管理ユーザー) がオペレーションを実行できることを確認します。

   - AWS CLI を使用して検証する

```
aws s3 ls s3://amzn-s3-demo-bucket --profile AccountBadmin
aws s3api get-bucket-lifecycle-configuration --bucket amzn-s3-demo-bucket --
profile AccountBadmin
```

- AWS Tools for Windows PowerShell を使用して検証する

```
get-s3object -BucketName amzn-s3-demo-bucket -StoredCredentials AccountBadmin
get-s3bucketlifecycleconfiguration -BucketName amzn-s3-demo-bucket -
StoredCredentials AccountBadmin
```

ステップ 2: アカウント B のタスクを実行する

次に、アカウント B の管理者はユーザー Dave を作成し、アカウント A から受け取ったアクセス許可を委任します。

ステップ 2.1: AWS Management Consoleにサインインする

アカウント B の IAM ユーザーのサインイン URL を使用し、AccountBadmin ユーザーとして AWS Management Console にサインインします。

ステップ 2.2: アカウント B でユーザー Dave を作成する

IAM コンソールで、ユーザー **Dave** を作成します。

手順については、「IAM ユーザーガイド」の「IAM ユーザーの作成 (コンソール)」を参照してください。

ステップ 2.3: ユーザー Dave に許可を委任する

以下のポリシーを使用して、ユーザー Dave のインラインポリシーを作成します。バケット名を指定してポリシーを更新する必要があります。

これは、AccountBadmin ユーザーの認証情報を使用してコンソールにサインインしていることを前提としています。

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Example",
         "Effect": "Allow",
         "Action": [
            "s3:ListBucket"
         ],
```

```
         "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket"
         ]
      }
   ]
}
```

手順については、「IAM ユーザーガイド」の「IAM ポリシーを管理する」を参照してください。

ステップ 2.4: アクセス許可をテストする

これで、アカウント B の Dave はアカウント A が所有する *amzn-s3-demo-bucket* の内容をリストできます。次のいずれかの手順でアクセス許可を確認できます。

AWS CLI を使用してアクセス許可をテストする

1. AWS CLI 設定ファイルに UserDave プロファイルを追加します。設定ファイルの詳細については、チュートリアル用のツールのセットアップ を参照してください。

   ```
   [profile UserDave]
   aws_access_key_id = access-key
   aws_secret_access_key = secret-access-key
   region = us-east-1
   ```

2. コマンドプロンプトで、次の AWS CLI コマンドを入力して、Dave がアカウント A によって所有される *amzn-s3-demo-bucket* からオブジェクトリストを取得できることを検証します。このコマンドでは、UserDave プロファイルを指定していることに注意してください。

   ```
   aws s3 ls s3://amzn-s3-demo-bucket --profile UserDave
   ```

   Dave には他のアクセス許可はありません。したがって、他のオペレーション (次の get-bucket-lifecycle 設定など) を実行しようとすると、Amazon S3 はアクセス許可の拒否を返します。

   ```
   aws s3api get-bucket-lifecycle-configuration --bucket amzn-s3-demo-bucket --profile
    UserDave
   ```

AWS Tools for Windows PowerShell を使用してアクセス許可をテストする

1. Dave の認証情報を AccountBDave という名前で保存します。

```
set-awscredentials -AccessKey AccessKeyID -SecretKey SecretAccessKey -storeas
 AccountBDave
```

2. List Bucket コマンドを試してみます。

```
get-s3object -BucketName amzn-s3-demo-bucket -StoredCredentials AccountBDave
```

Dave には他のアクセス許可はありません。したがって、他のオペレーション (次の get-s3bucketlifecycleconfiguration など) を実行しようとすると、Amazon S3 はアクセス許可の拒否を返します。

```
get-s3bucketlifecycleconfiguration -BucketName amzn-s3-demo-bucket -
StoredCredentials AccountBDave
```

ステップ 3: (オプション) 明示的な拒否を試す

アクセスコントロールリスト (ACL)、バケットポリシー、またはユーザーポリシーを使用して、アクセス許可を付与できます。ただし、バケットポリシーまたはユーザーポリシーによって明示的な拒否が設定されている場合、他のアクセス許可よりも明示的な拒否が優先されます。テストのために、バケットポリシーを更新し、アカウント B の s3:ListBucket アクセス許可を明示的に拒否してみます。このポリシーでは、s3:ListBucket アクセス許可も付与されます。ただし、明示的な拒否が優先され、アカウント B またはアカウント B のユーザーは *amzn-s3-demo-bucket* 内のオブジェクトを一覧表示を行うことはできません。

1. アカウント A のユーザー AccountAadmin の認証情報を使用して、バケットポリシーを次のように置き換えます。

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Example permissions",
         "Effect": "Allow",
         "Principal": {
            "AWS": "arn:aws:iam::AccountB-ID:root"
         },
         "Action": [
            "s3:GetLifecycleConfiguration",
```

```
            "s3:ListBucket"
         ],
         "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket"
         ]
      },
      {
         "Sid": "Deny permission",
         "Effect": "Deny",
         "Principal": {
            "AWS": "arn:aws:iam::AccountB-ID:root"
         },
         "Action": [
            "s3:ListBucket"
         ],
         "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket"
         ]
      }
   ]
}
```

2. ここで AccountBadmin の認証情報を使用してバケットリストを取得しようとすると、アクセスは拒否されます。

   - AWS CLI を使用して、次のコマンドを実行します。

     ```
     aws s3 ls s3://amzn-s3-demo-bucket --profile AccountBadmin
     ```

   - AWS Tools for Windows PowerShell を使用して、次のコマンドを実行します。

     ```
     get-s3object -BucketName amzn-s3-demo-bucket -StoredCredentials AccountBDave
     ```

ステップ 4: クリーンアップする

1. テストが終了したら、次の手順でクリーンアップを行います。

   - アカウント A の認証情報を使用して AWS Management Console (AWS Management Console) にサインインし、次の操作を行います。

- Amazon S3 コンソールで、*amzn-s3-demo-bucket* にアタッチされているバケットポリシーを削除します。バケットの [プロパティ] で、[アクセス許可] セクションのポリシーを削除します。
- バケットをこの演習のために作成した場合は、Amazon S3 コンソールでオブジェクトを削除してから、バケットを削除します。
- IAM コンソールで、AccountAadmin ユーザーを削除します。

2. アカウント B の認証情報を使用して IAM コンソールにサインインします。AccountBadmin ユーザーを削除します。手順については、「IAM ユーザーガイド」の「IAM ユーザーの削除」を参照してください。

例 3: バケット所有者が自分の所有していないオブジェクトに対するアクセス許可を付与する

> **Important**
>
> アクセス許可は、個々のユーザーではなく、IAM ロールに付与することをお勧めします。これを行う方法については、クロスアカウントのアクセス許可の理解と IAM ロールの使用を参照してください。

トピック

- ステップ 0: チュートリアルの準備をする
- ステップ 1: アカウント A のタスクを実行する
- ステップ 2: アカウント B のタスクを実行する
- ステップ 3: アクセス許可をテストする
- ステップ 4: クリーンアップする

この例のシナリオでは、バケット所有者はオブジェクトへのアクセス許可を付与しますが、バケット内のオブジェクトの一部はバケット所有者によって所有されていません。この例では、バケット所有者は、自分のアカウントのユーザーにアクセス許可を付与しようとしています。

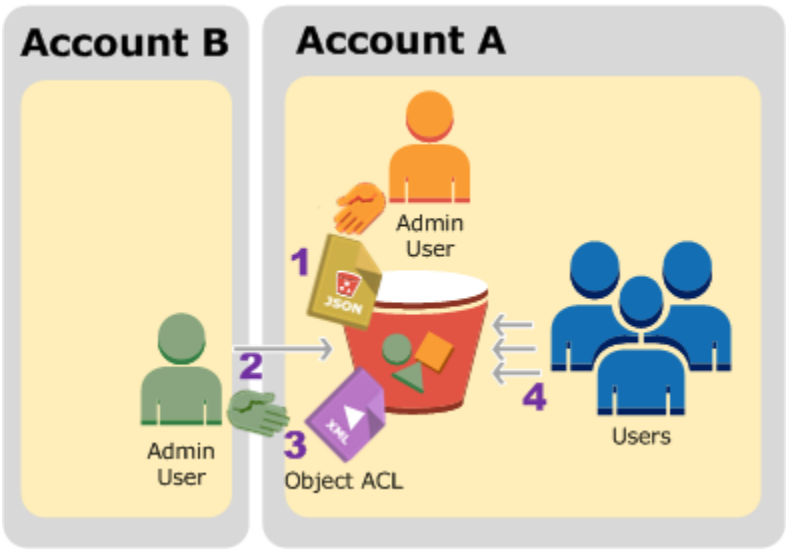
バケット所有者は、他の AWS アカウントにオブジェクトのアップロードを許可できます。デフォルトでは、バケット所有者は別の AWS アカウント によってバケットに書き込まれたオブジェクトを所有しません。オブジェクトは、S3 バケットに書き込むアカウントによって所有されています。バ

ケット所有者がバケット内のオブジェクトを所有していない場合、オブジェクト所有者は最初にオブジェクトのアクセスコントロールリスト (ACL) を使用してバケット所有者に権限を付与する必要があります。その後、バケット所有者は所有していないオブジェクトのアクセス許可を付与できます。詳細については、「Amazon S3 のバケットとオブジェクトの所有権」を参照してください。

バケット所有者がバケットの S3 オブジェクト所有権にバケット所有者強制設定を適用すると、バケット所有者は、別の AWS アカウント によって書き込まれたオブジェクトを含む、バケット内のすべてのオブジェクトを所有します。これにより、オブジェクトがバケット所有者によって所有されていないという問題が解決されます。次に、自分のアカウントまたは他の AWS アカウント アカウントのユーザーにアクセス許可を委任できます。

> **Note**
>
> S3 オブジェクト所有権は、Amazon S3 バケットレベルの設定で、バケットにアップロードされる新しいオブジェクト所有権を制御し、ACL を無効にするのに使用できます。デフォルトでは、オブジェクト所有権はバケット所有者の強制設定に設定され、すべての ACL は無効になります。ACL を無効にすると、バケット所有者はバケット内のすべてのオブジェクトを所有し、アクセス管理ポリシーのみを使用してデータへのアクセスを管理します。
> Amazon S3 の最新のユースケースの大部分では ACL を使用する必要がなくなっています。オブジェクトごとに個別に制御する必要がある通常ではない状況を除き、ACL は無効にしておくことをお勧めします。ACL を無効にすると、誰がオブジェクトをバケットにアップロードしたかに関係なく、ポリシーを使用してバケット内のすべてのオブジェクトへのアクセスを制御できます。詳細については、「オブジェクトの所有権の制御とバケットの ACL の無効化。」を参照してください。

この例では、バケット所有者がオブジェクト所有権のバケット所有者強制設定を適用していないと仮定します。バケット所有者は、自分のアカウントのユーザーに許可を委任します。この手順の概要を以下に示します。



1. アカウント A の管理者ユーザーが、2 つのステートメントを持つバケットポリシーをアタッチします。
   - オブジェクトをアップロードするクロスアカウントアクセスをアカウント B に許可します。
   - 自分のアカウントのユーザーにバケット内のオブジェクトへのアクセスを許可します。
2. アカウント B の管理者ユーザーは、アカウント A が所有するバケットにオブジェクトをアップロードします。
3. アカウント B の管理者は、オブジェクト ACL を更新して、オブジェクトに対するフルコントロールアクセス許可をバケット所有者に付与します。
4. アカウント A のユーザーは、所有者に関わりなくバケット内のオブジェクトにアクセスできることを確認します。

この例では、2 個のアカウントが必要です。次の表に、これらのアカウントの呼び方とそれぞれの管理者ユーザーを示します。このチュートリアルでは、推奨される IAM ガイドラインに従って、アカウントのルートユーザー認証情報を使用しません。詳細については、「管理者ユーザーを使用したリソースの作成とアクセス許可の付与について」を参照してください。その代わりに、各アカウントに管理者を作成し、その認証情報を使用してリソースを作成し、アクセス許可を付与します。

AWS アカウント ID	アカウントの呼び方	アカウントの管理者
1111-1111-1111	アカウント A	AccountAadmin
2222-2222-2222	アカウント B	AccountBadmin

ユーザーを作成し、アクセス許可を付与するためのすべてのタスクは、AWS Management Console で実行します。このチュートリアルでは、許可を検証するために、コマンドラインツールの AWS Command Line Interface (AWS CLI) と AWS Tools for Windows PowerShell を使用するので、コードを記述する必要はありません。

ステップ 0: チュートリアルの準備をする

1. 前のセクションの表に示したように、2 個の AWS アカウントがあり、各アカウントに 1 人ずつの管理者が存在することを確認します。

   a. 必要な場合、AWS アカウントにサインアップします。

   b. アカウント A の認証情報を使用して、IAM コンソールにサインインし、次の操作を行って管理者ユーザーを作成します。

      - ユーザー **AccountAadmin** を作成し、ユーザーのセキュリティ認証情報を書き留めます。ユーザーの追加の詳細については、「IAM ユーザーガイド」の「AWS アカウント での IAM ユーザーの作成」を参照してください。
      - AccountAadmin にフルアクセスを許可するユーザーポリシーをアタッチして、管理者権限を付与します。手順については、「IAM ユーザーガイド」の「IAM ポリシーを管理する」を参照してください。
      - IAM コンソールの [ダッシュボード] で、[IAM ユーザーのサインイン URL] を書き留めます。このアカウントのユーザーは、この URL を使用して AWS Management Console にサインインします。詳細については、IAM ユーザーガイドのユーザーがお客様のアカウントにサインインする方法 を参照してください。

   c. 前述のステップを、アカウント B の認証情報を使用してもう一度実行し、管理者ユーザー **AccountBadmin** を作成します。

2. AWS CLI または Tools for Windows PowerShell をセットアップします。管理者認証情報を必ず次のように保存してください。

   - AWS CLI を使用する場合は、設定ファイルに `AccountAadmin` と `AccountBadmin` の 2 つのプロファイルを作成します。
   - Tools for Windows PowerShell を使用する場合、セッションの認証情報を `AccountAadmin` および `AccountBadmin` として保存します。

   手順については、チュートリアル用のツールのセットアップ を参照してください。

ステップ 1: アカウント A のタスクを実行する

アカウント A に対して、次の手順を実行します。

ステップ 1.1: コンソールにサインインする

アカウント A の IAM ユーザーのサインイン URL を使用して、**AccountAadmin** ユーザーとして AWS Management Console にサインインします。このユーザーはバケットを作成し、ポリシーをアタッチします。

ステップ 1.2: バケットとユーザーを作成し、ユーザーにアクセス許可を付与するバケットポリシーを追加する

1. Amazon S3 コンソールでバケットを作成します。この演習では、米国東部 (バージニア北部) AWS リージョン に *amzn-s3-demo-bucket1* という名前でバケットを作成することを前提とします。

   手順については、「汎用バケットの作成」を参照してください。
2. IAM コンソールで、ユーザー **Dave** を作成します。

   詳細な手順については、「IAM ユーザーガイド」の「IAM ユーザーの作成 (コンソール)」を参照してください。
3. ユーザー Dave の認証情報を書き留めます。
4. Amazon S3 コンソールで、次のバケットポリシーを *amzn-s3-demo-bucket1* バケットにアタッチします。手順については、Amazon S3 コンソールを使用したバケットポリシーの追加 を参照してください。バケットポリシーを追加するには、このステップに従います。アカウント ID を確認する方法については、AWS アカウント ID の検索 を参照してください。

   このポリシーは、アカウント B に s3:PutObject および s3:ListBucket アクセス許可を付与します。このポリシーはまた、ユーザー Dave に s3:GetObject アクセス許可を付与します。

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Statement1",
         "Effect": "Allow",
         "Principal": {
            "AWS": "arn:aws:iam::AccountB-ID:root"
         },
```

```
            "Action": [
               "s3:PutObject",
               "s3:ListBucket"
            ],
            "Resource": [
               "arn:aws:s3:::amzn-s3-demo-bucket1/*",
               "arn:aws:s3:::amzn-s3-demo-bucket1"
            ]
         },
         {
            "Sid": "Statement3",
            "Effect": "Allow",
            "Principal": {
               "AWS": "arn:aws:iam::AccountA-ID:user/Dave"
            },
            "Action": [
               "s3:GetObject"
            ],
            "Resource": [
               "arn:aws:s3:::amzn-s3-demo-bucket1/*"
            ]
         }
      ]
}
```

ステップ 2: アカウント B のタスクを実行する

これでアカウント B はアカウント A のバケットに対するオペレーション実行のアクセス許可を得ましたので、管理者は次の作業を行います。

- アカウント A のバケットにオブジェクトをアップロードします。
- バケット所有者であるアカウント A にそのバケットへのフルコントロールをオブジェクトの ACL で付与します。

AWS CLI を使用する場合

1. `put-object` AWS CLI コマンドを使用して、オブジェクトをアップロードします。アップロードするソースファイルは、コマンドの `--body` パラメータで指定します。例えば、ファイルが Windows 端末の `C:` ドライブにある場合、`c:\HappyFace.jpg` のように指定します。`--key` パラメータは、オブジェクトのキー名を指定します。

```
aws s3api put-object --bucket amzn-s3-demo-bucket1 --key HappyFace.jpg --body
 HappyFace.jpg --profile AccountBadmin
```

2. バケット所有者に対するオブジェクトのフルコントロールの許可をオブジェクト ACL に追加します。正規ユーザー ID を検索する方法については、「AWS Account Management リファレンスガイド」の「AWS アカウント の正規ユーザー ID を検索する」を参照してください。

```
aws s3api put-object-acl --bucket amzn-s3-demo-bucket1 --key HappyFace.jpg --grant-
full-control id="AccountA-CanonicalUserID" --profile AccountBadmin
```

Tools for Windows PowerShell の使用

1. `Write-S3Object` コマンドを使用して、オブジェクトをアップロードします。

```
Write-S3Object -BucketName amzn-s3-demo-bucket1 -key HappyFace.jpg -file
 HappyFace.jpg -StoredCredentials AccountBadmin
```

2. バケット所有者に対するオブジェクトのフルコントロールの許可をオブジェクト ACL に追加します。

```
Set-S3ACL -BucketName amzn-s3-demo-bucket1 -Key HappyFace.jpg -CannedACLName
 "bucket-owner-full-control" -StoredCreden
```

ステップ 3: アクセス許可をテストする

アカウント A のユーザー Dave が、アカウント B が所有するオブジェクトにアクセスできることを確認します。

AWS CLI を使用する場合

1. ユーザー Dave の認証情報を AWS CLI の設定ファイルに追加して、新しいプロファイル UserDaveAccountA を作成します。詳細については、チュートリアル用のツールのセットアップ を参照してください。

```
[profile UserDaveAccountA]
aws_access_key_id = access-key
aws_secret_access_key = secret-access-key
```

```
region = us-east-1
```

2. get-object CLI コマンドを実行して HappyFace.jpg をダウンロードし、ローカルに保存します。--profile パラメータを追加して、ユーザー Dave の認証情報を指定します。

```
aws s3api get-object --bucket amzn-s3-demo-bucket1 --key
 HappyFace.jpg Outputfile.jpg --profile UserDaveAccountA
```

Tools for Windows PowerShell の使用

1. ユーザー Dave の AWS 認証情報を、UserDaveAccountA という名前で永続的ストアに保存します。

```
Set-AWSCredentials -AccessKey UserDave-AccessKey -SecretKey UserDave-
SecretAccessKey -storeas UserDaveAccountA
```

2. Read-S3Object コマンドを実行して HappyFace.jpg オブジェクトをダウンロードし、ローカルに保存します。-StoredCredentials パラメータを追加して、ユーザー Dave の認証情報を指定します。

```
Read-S3Object -BucketName amzn-s3-demo-bucket1 -Key HappyFace.jpg -file
 HappyFace.jpg  -StoredCredentials UserDaveAccountA
```

ステップ 4: クリーンアップする

1. テストが終了したら、次の手順でクリーンアップを行います。

   - アカウント A の認証情報を使用して AWS Management Console にサインインし、次の操作を行います。

     - Amazon S3 コンソールで、*amzn-s3-demo-bucket1* にアタッチされているバケットポリシーを削除します。バケットの [プロパティ] で、[アクセス許可] セクションのポリシーを削除します。
     - バケットをこの演習のために作成した場合は、Amazon S3 コンソールでオブジェクトを削除してから、バケットを削除します。
     - IAM コンソールで、[AccountAadmin] ユーザーを削除します。手順については、「IAM ユーザーガイド」の「IAM ユーザーの削除」を参照してください。

2. アカウント B の認証情報を使用して AWS Management Console にサインインします。IAM コンソールで、ユーザー [AccountBadmin] を削除します。

例 4 - バケット所有者が所有権のないオブジェクトへのクロスアカウントアクセス許可を付与する

トピック

- クロスアカウントのアクセス許可の理解と IAM ロールの使用
- ステップ 0: チュートリアルの準備をする
- ステップ 1: アカウント A のタスクを実行する
- ステップ 2: アカウント B のタスクを実行する
- ステップ 3: アカウント C のタスクを実行する
- ステップ 4: クリーンアップする
- 関連リソース

この例のシナリオでは、バケット所有者が、オブジェクトをアップロードするためのアクセス許可を他の AWS アカウント に付与します。バケットの S3 オブジェクト所有権にバケット所有者強制設定を適用した場合、別の AWS アカウント によって書き込まれたオブジェクトを含む、バケット内のすべてのオブジェクトを所有します。これにより、バケット所有者であるユーザーがオブジェクトを所有していないという問題が解決されます。次に、自分のアカウントまたは他の AWS アカウントアカウントのユーザーにアクセス許可を委任できます。S3 オブジェクト所有権のバケット所有者強制設定が有効になっていないとします。つまり、バケットは、他の AWS アカウントが所有するオブジェクトを含むことができます。

バケット所有者は、オブジェクトの所有者が誰であるかに関係なく、オブジェクトに対するクロスアカウントのアクセス許可を別のアカウントのユーザーに付与しなければならない場合があります。例えば、課金アプリケーションがユーザーとしてオブジェクトのメタデータにアクセスしなければならない場合などです。ここで、主に 2 つの問題が生じます。

- バケット所有者には、他の AWS アカウントで作成されたオブジェクトに対する許可はありません。バケット所有者が、自分が所有していないオブジェクトに対するアクセス許可を付与するには、オブジェクトの所有者 (オブジェクトを作成した) は、最初にバケット所有者にアクセス許可を付与する必要があります。この所有者は、オブジェクトを作成した AWS アカウントです。これで、バケット所有者は、それらのアクセス許可を委任できるようになります。

- バケット所有者は、自分のアカウントのユーザーに許可を委任できます (「例 3: バケット所有者が自分の所有していないオブジェクトに対するアクセス許可を付与する」を参照)。ただし、クロスアカウントの委任はサポートされていないため、バケット所有者アカウントは他の AWS アカウント にアクセス許可を委任できません。

このシナリオでは、バケット所有者はオブジェクトへのアクセス許可を持つ AWS Identity and Access Management (IAM) ロールを作成できます。その後、バケット所有者は別の AWS アカウント にロールを引き受けるアクセス許可を付与して、バケットのオブジェクトへのアクセスを一時的に有効化できます。

> **Note**
>
> S3 オブジェクト所有権は、Amazon S3 バケットレベルの設定で、バケットにアップロードされる新しいオブジェクト所有権を制御し、ACL を無効にするのに使用できます。デフォルトでは、オブジェクト所有権はバケット所有者の強制設定に設定され、すべての ACL は無効になります。ACL を無効にすると、バケット所有者はバケット内のすべてのオブジェクトを所有し、アクセス管理ポリシーのみを使用してデータへのアクセスを管理します。
> Amazon S3 の最新のユースケースの大部分では ACL を使用する必要がなくなっています。オブジェクトごとに個別に制御する必要がある通常ではない状況を除き、ACL は無効にしておくことをお勧めします。ACL を無効にすると、誰がオブジェクトをバケットにアップロードしたかに関係なく、ポリシーを使用してバケット内のすべてのオブジェクトへのアクセスを制御できます。詳細については、「オブジェクトの所有権の制御とバケットの ACL の無効化。」を参照してください。

クロスアカウントのアクセス許可の理解と IAM ロールの使用

IAM ロールは、リソースへのアクセスを委任する、いくつかのシナリオで使用されます。なかでも、クロスアカウントアクセスは重要なシナリオです。この例では、バケット所有者 (アカウント A) は、IAM ロールを使用して、他の AWS アカウント (アカウント C) のユーザーに一時的にオブジェクトへのクロスアカウントの許可を委任します。作成された IAM ロールには、次の 2 つのポリシーがアタッチされています。

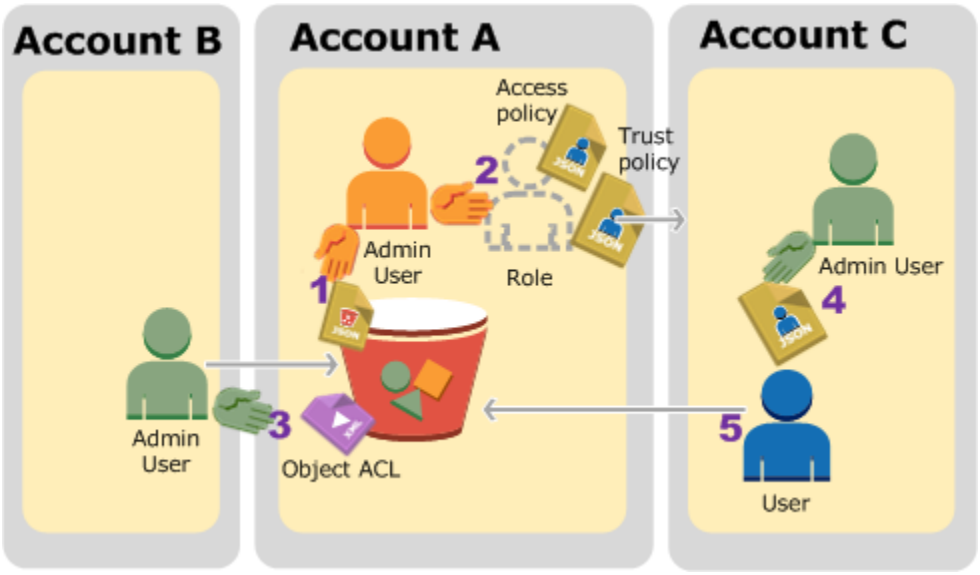
- ロールを引き受ける別の AWS アカウントを指定する信頼ポリシー。
- ロールを引き受けるユーザーに付与されるアクセス許可 (`s3:GetObject` など) を定義するアクセスポリシー。ポリシーで指定できるアクセス許可のリストについては、Amazon S3 のポリシーアクション を参照してください。

信頼ポリシーで指定された AWS アカウントは、アカウントに属するユーザーにロールを引き受ける許可を付与します。ユーザーは、以下の手順でオブジェクトにアクセスします。

- ロールを引き受け、その応答として一時的なセキュリティ認証情報を取得します。
- 一時的なセキュリティ認証情報を使用して、バケットのオブジェクトにアクセスします。

IAM ロールの詳細については、「IAM ユーザーガイド」の「IAM ロール」を参照してください。

この手順の概要を以下に示します。



1. アカウント A の管理者ユーザーは、バケットポリシーをアタッチし、オブジェクトをアップロードする条件付きのアクセス許可をアカウント B に付与します。
2. アカウント A の管理者ユーザーは、IAM ロールを作成し、アカウント C との間に信頼を確立します。これで、アカウント C のユーザーはアカウント A にアクセスできるようになります。ロールにアタッチされたアクセスポリシーは、アカウント C のユーザーがアカウント A にアクセスするときに実行できる操作を制限します。
3. アカウント B の管理者は、アカウント A が所有するバケットにオブジェクトをアップロードし、バケット所有者にフルコントロールのアクセス許可を付与します。
4. アカウント C の管理者は、ユーザーを作成し、ロールを引き受けるためのユーザーポリシーをアタッチします。
5. アカウント C のユーザーが初めてロールを引き受けると、一時的なセキュリティ認証情報が返されます。ユーザーは、この一時的な認証情報を使用して、バケットのオブジェクトにアクセスします。

この例では、3 つのアカウントが必要です。次の表に、これらのアカウントの呼び方とそれぞれの管理者ユーザーを示します。IAM のガイドライン (「管理者ユーザーを使用したリソースの作成とアクセス許可の付与について」を参照) に従い、このチュートリアルでは AWS アカウントのルートユーザーの認証情報を使用しません。その代わりに、各アカウントで管理者ユーザーを作成し、その認証情報を使用してリソースを作成し、アクセス許可を付与します。

AWS アカウント ID	アカウントの呼び方	アカウントの管理者ユーザー
1111-1111-1111	アカウント A	AccountAadmin
2222-2222-2222	アカウント B	AccountBadmin
3333-3333-3333	アカウント C	AccountCadmin

ステップ 0: チュートリアルの準備をする

> **Note**
>
> テキストエディタを開いて、手順を実行しながら、いくつかの情報を書き留めることができます。特に、コンソールに接続する各アカウントのアカウント ID、正規ユーザー ID、IAM ユーザーのサインイン URL、IAM ユーザーとロールの Amazon リソースネーム (ARN) が必要になります。

1. 前のセクションの表に示したように、3 つの AWS アカウント があり、各アカウントに 1 人ずつ管理者ユーザーが存在することを確認します。

   a. 必要に応じて AWS アカウントにサインアップします。ここでは、それぞれのアカウントをアカウント A、アカウント B、アカウント C と呼ぶことにします。

   b. アカウント A の認証情報を使用して、IAM コンソールにサインインし、次の操作を行って管理者ユーザーを作成します。

      - ユーザー **AccountAadmin** を作成して、そのセキュリティ認証情報を書き留めます。ユーザーの追加の詳細については、「IAM ユーザーガイド」の「AWS アカウント での IAM ユーザーの作成」を参照してください。

- フルアクセスを付与するユーザーポリシーをアタッチして、管理者に AccountAadmin を付与します。手順については、「IAM ユーザーガイド」の「IAM ポリシーを管理する」を参照してください。
- IAM コンソールの [ダッシュボード] で、[IAM ユーザーのサインイン URL] を書き留めます。このアカウントのユーザーは、この URL を使用して AWS Management Console にサインインします。詳細については、「IAM ユーザーガイド」の「Sign in to the AWS Management Console as an IAM user」を参照してください。

c. 前述の手順を繰り返し、アカウント B およびアカウント C の管理者ユーザーを作成します。

2. アカウント C で、正規ユーザー ID を書き留めます。

   アカウント A で IAM ロールを作成したら、信頼ポリシーでアカウント C のアカウント ID を指定して、ロールを引き受けるアクセス許可をアカウント C に付与します。アカウント情報は、次の手順で確認できます。

   a. AWS アカウント ID またはアカウントエイリアス、IAM ユーザー名、パスワードを使用して、Amazon S3 コンソールにサインインします。

   b. バケットの詳細を確認する Amazon S3 バケットの名前を選択します。

   c. [Permissions (アクセス許可)] タブを選択してから、[アクセスコントロールリスト] を選択します。

   d. AWS アカウント のアクセスのセッションで、アカウント 列は `c1daexampleaaf850ea79cf0430f33d72579fd1611c97f7ded193374c0b163b6` のような長い識別子です。これが正規ユーザー ID です。

3. バケットポリシーを作成するときは、次の情報が必要になります。これらの値を書き留めます。

   - アカウント A の正規ユーザー ID – アカウント A の管理者がアカウント B の管理者にオブジェクトをアップロードする条件付きのアクセス許可を付与するとき、オブジェクトに対するフルコントロールを取得するアカウント A のユーザーの正規ユーザー ID を指定します。

     > **Note**
     >
     > 正規ユーザー ID は、Amazon S3 固有の概念です。64 文字から成る、難読化されたアカウント ID です。

   - アカウント B 管理者の ユーザー ARN - ユーザー ARN は IAM コンソールにあります。[概要] タブでユーザーを選択し、ユーザーの ARN を見つけます。

バケットポリシーでは、オブジェクトをアップロードするアクセス許可を AccountBadmin に付与し、ARN を使用してユーザーを指定します。ARN 値の例を示します。

```
arn:aws:iam::AccountB-ID:user/AccountBadmin
```

4. AWS Command Line Interface (CLI) または AWS Tools for Windows PowerShell をセットアップします。管理者ユーザーの認証情報は以下のように保存します。

   - AWS CLI を使用する場合は、設定ファイルに AccountAadmin と AccountBadmin のプロファイルを作成します。
   - AWS Tools for Windows PowerShell を使用する場合は、セッションの認証情報を AccountAadmin および AccountBadmin として保存します。

   手順については、「チュートリアル用のツールのセットアップ」を参照してください。

ステップ 1: アカウント A のタスクを実行する

この例では、アカウント A はバケット所有者です。したがって、アカウント A のユーザー AccountAadmin は以下を実行します。

- バケットを作成します。
- オブジェクトをアップロードするアクセス許可をアカウント B の管理者に付与するバケットポリシーをアタッチします。
- バケット内のオブジェクトにアクセスできるように、ロールを引き受けるアクセス許可をアカウント C に付与する IAM ロールを作成します。

ステップ 1.1: AWS Management Consoleにサインインする

アカウント A で IAM ユーザーのサインイン URL を使用して、まず **AccountAadmin** ユーザーとして AWS Management Console にサインインします。このユーザーはバケットを作成し、ポリシーをアタッチします。

ステップ 1.2: バケットを作成してバケットポリシーをアタッチする

Amazon S3 コンソールで、次の操作を行います。

1. バケットを作成します。この演習では、バケットの名前を *amzn-s3-demo-bucket1* とします。

手順については、「汎用バケットの作成」を参照してください。

2. 次のバケットポリシーをアタッチします。このポリシーは、オブジェクトをアップロードする条件付きのアクセス許可をアカウント B の管理者に付与します。

   amzn-s3-demo-bucket1、*AccountB-ID*、*CanonicalUserId-of-AWSaccountA-BucketOwner* に独自の値を指定してポリシーを更新します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "111",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::AccountB-ID:user/AccountBadmin"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*"
        },
        {
            "Sid": "112",
            "Effect": "Deny",
            "Principal": {
                "AWS": "arn:aws:iam::AccountB-ID:user/AccountBadmin"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-grant-full-control": "id=CanonicalUserId-of-
AWSaccountA-BucketOwner"
                }
            }
        }
    ]
}
```

ステップ 1.3: アカウント C にクロスアカウントアクセスを許可する IAM ロールをアカウント A に作成する

IAM コンソールで、アカウント C にロールを引き受けるアクセス許可を付与する IAM ロール (**examplerole**) を作成します。このロールはアカウント A に作成する必要があるため、アカウント A の管理者としてサインインしていることを再度確認してください。

1. ロールを作成する前に、ロールに必要なアクセス許可を定義する管理ポリシーを準備します。後の手順で、このポリシーをロールにアタッチします。

   a. 左側のナビゲーションペインで [ポリシー] を選択し、続いて [ポリシーの作成] を選択します。

   b. [独自のポリシーを作成] の横で、[選択] を選択します。

   c. [Policy Name (ポリシー名)] フィールドに「**access-accountA-bucket** 」と入力します。

   d. 以下のアクセスポリシーをコピーして、[Policy Document (ポリシードキュメント)] フィールドに貼り付けます。このアクセスポリシーは、ロールに `s3:GetObject` のアクセス許可を付与するため、アカウント C のユーザーがこのロールを引き受けると、`s3:GetObject` オペレーションのみを実行できます。

   ```
   {
     "Version": "2012-10-17",
     "Statement": [
       {
         "Effect": "Allow",
         "Action": "s3:GetObject",
         "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*"
       }
     ]
   }
   ```

   e. [ポリシーを作成] を選択します。

   新しいポリシーが管理ポリシーの一覧に表示されます。

2. 左側のナビゲーションペインで、[ロール]、[新しいロールの作成] の順に選択します。

3. [ロールタイプの選択] で [クロスアカウントアクセスのロール] を選択して、[所有する AWS アカウント の間のアクセスの提供] の隣の [選択] ボタンを選択します。

4. アカウント C のアカウント ID を入力します。

このチュートリアルでは、ロールを引き受けるユーザーに多要素認証 (MFA) を必須とする必要がないため、このオプションは選択していない状態のままにしておきます。

5. [次のステップ] を選択して、そのロールに関連するアクセス許可を設定します。
6. 作成した access-accountA-bucket ポリシーの横にあるチェックボックスを選択し、[次のステップ] を選択します。

   [Review] ページが表示されます。このページで作成前のロールの設定を確認できます。このページで注意する重要な項目は、このロールを使用する必要があるユーザーに送信できるリンクです。ユーザーがこのリンクをクリックすると、[ロールの切り替え] ページがすぐに表示されます。このページには、[アカウント ID] と [ロール名] がすでに設定されています。このリンクは、クロスアカウントロールの [ロールの概要] ページで後で確認することもできます。
7. ロール名に「examplerole」と入力し、[次のステップ] を選択します。
8. ロールを確認したら、[ロールの作成] を選択します。

   examplerole ロールがロールの一覧に表示されます。
9. ロール名 examplerole を選択します。
10. [Trust Relationships (信頼関係)] タブを選択します。
11. [ポリシードキュメントの表示] を選択して、表示されている信頼ポリシーが次のポリシーと一致するか確認します。

    次の信頼ポリシーは、アカウント C との信頼を確立し、sts:AssumeRole アクションを許可します。詳細については、AWS Security Token Service API リファレンスの「AssumeRole」を参照してください。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::AccountC-ID:root"
      },
      "Action": "sts:AssumeRole"
    }
  ]
```

```
}
```

12. 作成した examplerole ロールの Amazon リソースネーム (ARN) を書き留めます。

    後の手順で、このロールの引き受けを許可するユーザーポリシーを IAM ユーザーにアタッチしますが、ロールは ARN 値で指定します。

ステップ 2: アカウント B のタスクを実行する

アカウント A が所有するバケットの例では、他のアカウントが所有するオブジェクトが必要です。このステップでは、アカウント B の管理者は、コマンドラインツールを使用してオブジェクトをアップロードします。

- put-object AWS CLI コマンドを使用して、オブジェクトを *amzn-s3-demo-bucket1* にアップロードします。

  ```
  aws s3api put-object --bucket amzn-s3-demo-bucket1 --key HappyFace.jpg --
  body HappyFace.jpg --grant-full-control id="canonicalUserId-ofTheBucketOwner" --
  profile AccountBadmin
  ```

  次の点に注意してください:

  - --Profile パラメータは AccountBadmin のプロファイルを指定しているため、オブジェクトはアカウント B によって所有されます。
  - grant-full-control パラメータは、バケットポリシーに従って、バケット所有者にオブジェクトに対するフルコントロールのアクセス許可を付与します。
  - --body パラメータは、アップロードするソースファイルを指定します。例えば、ファイルが Windows コンピュータの C: ドライブにある場合は、「c:\HappyFace.jpg」と指定します。

ステップ 3: アカウント C のタスクを実行する

これまでの手順で、アカウント A はすでに examplerole ロールを作成し、アカウント C との信頼を確立しています。これにより、アカウント C のユーザーは、アカウント A にアクセスすることができます。このステップでは、アカウント C の管理者がユーザー (Dave) を作成し、アカウント A から取得した sts:AssumeRole のアクセス許可を委任します。examplerole を引き受けた Dave は、一時的にアカウント A へのアクセス権を取得します。アカウント A がロールにアタッチしたア

クセスポリシーは、アカウント A にアクセスする Dave が実行できるアクション (特に *amzn-s3-demo-bucket1* のオブジェクトを取得すること) を制限します。

ステップ 3.1: アカウント C でユーザーを作成し、examplerole を引き受けるアクセス許可を委任する

1. アカウント C で IAM ユーザーのサインイン URL を使用して、まず **AccountCadmin** ユーザーとして AWS Management Console にサインインします。

2. IAM コンソールで、ユーザー Dave を作成します。

   詳細な手順については、「IAM ユーザーガイド」の「AWS Management Console での IAM ユーザーの作成」を参照してください。

3. Dave の認証情報を書き留めます。Dave は、`examplerole` ロールを引き受けるのに、これらの認証情報を必要とします。

4. アカウント A の `sts:AssumeRole` ロールで `examplerole` アクセス許可を Dave に委任する Dave IAM ユーザー用のインラインポリシーを作成します。

   a. 左側のナビゲーションペインで、[ユーザー] を選択します。

   b. ユーザー名 [Dave] を選択します。

   c. ユーザー詳細ページで [Permissions (アクセス許可)] タブを選択し、[Inline Policies (インラインポリシー)] セクションを展開します。

   d. [click here (ここをクリック)] (または [Create User Policy (ユーザーポリシーの作成)]) を選択します。

   e. [Custom Policy] を選択し、[Select] を選択します。

   f. [Policy Name (ポリシー名)] フィールドにポリシーの名前を入力します。

   g. 以下のポリシーをコピーして、[Policy Document (ポリシードキュメント)] フィールドに貼り付けます。

      AccountA-ID を指定してポリシーを更新する必要があります。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["sts:AssumeRole"],
      "Resource": "arn:aws:iam::AccountA-ID:role/examplerole"
```

```
    }
  ]
}
```

h. [ポリシーを適用] を選びます。

5. 別のプロファイル AccountCDave を追加して、Dave の認証情報を AWS CLI の設定ファイルに保存します。

```
[profile AccountCDave]
aws_access_key_id = UserDaveAccessKeyID
aws_secret_access_key = UserDaveSecretAccessKey
region = us-west-2
```

ステップ 3.2: ロール (examplerole) を引き受けてオブジェクトにアクセスする

Dave は、以下の手順でアカウント A が所有するバケットのオブジェクトにアクセスできます。

- Dave は、まず自分の認証情報を使用して、examplerole を引き受けます。一時的な認証情報が返されます。
- この一時的な認証情報を使用して、アカウント A のバケットのオブジェクトにアクセスします。

1. コマンドプロンプトで、AccountCDave プロファイルを使用して、次の AWS CLI assume-role コマンドを実行します。

   examplerole が定義されている *AccountA-ID* を指定して、コマンドの ARN 値を更新する必要があります。

```
aws sts assume-role --role-arn arn:aws:iam::AccountA-ID:role/examplerole --profile
 AccountCDave --role-session-name test
```

   AWS Security Token Service (AWS STS) が一時的なセキュリティ認証情報 (アクセスキー ID、シークレットアクセスキー、およびセッショントークン) を返します。

2. 一時的なセキュリティ認証情報を TempCred プロファイルの AWS CLI 設定ファイルに保存します。

```
[profile TempCred]
aws_access_key_id = temp-access-key-ID
aws_secret_access_key = temp-secret-access-key
```

```
aws_session_token = session-token
region = us-west-2
```

3. コマンドプロンプトで、一時的な認証情報を使用して、次の AWS CLI コマンドを実行してオブジェクトにアクセスします。例えば、コマンドで head-object API を指定すると、HappyFace.jpg オブジェクトのオブジェクトメタデータが取得されます。

```
aws s3api get-object --bucket amzn-s3-demo-bucket1 --
key HappyFace.jpg SaveFileAs.jpg --profile TempCred
```

examplerole にアタッチされているアクセスポリシーでは、アクションが許可されているため、Amazon S3 はリクエストを処理します。バケットの任意のオブジェクトに対して任意のアクションを試してみましょう。

例えば、get-object-acl のアクションを試すと、このロールではそのアクションは許可されていないため、アクセス許可が拒否されます。

```
aws s3api get-object-acl --bucket amzn-s3-demo-bucket1 --key HappyFace.jpg --
profile TempCred
```

この例では、ユーザー Dave がロールを引き受け、一時的な認証情報を使用してオブジェクトにアクセスしました。同様に、アカウント C のアプリケーションが *amzn-s3-demo-bucket1* のオブジェクトにアクセスすることも可能です。アプリケーションが一時的なセキュリティ認証情報を取得すれば、アカウント C はこのアプリケーションに examplerole を引き受けるアクセス許可を委任できます。

ステップ 4: クリーンアップする

1. テストが終了したら、次の手順でクリーンアップを行います。

   - アカウント A の認証情報を使用して AWS Management Console にサインインし、次の操作を行います。

     - Amazon S3 コンソールで、*amzn-s3-demo-bucket1* にアタッチされているバケットポリシーを削除します。バケットの [プロパティ] で、[アクセス許可] セクションのポリシーを削除します。
     - バケットをこの演習のために作成した場合は、Amazon S3 コンソールでオブジェクトを削除してから、バケットを削除します。

- IAM コンソールで、アカウント A で作成した `examplerole` を削除します。詳細な手順については、「IAM ユーザーガイド」の「IAM ユーザーの削除」を参照してください。
- IAM コンソールで、[AccountAadmin] ユーザーを削除します。

2. アカウント B の認証情報を使用して IAM コンソールにサインインします。ユーザー AccountBadmin を削除します。
3. アカウント C の認証情報を使用して IAM コンソールにサインインします。AccountCadmin とユーザー Dave を削除します。

関連リソース

このチュートリアルに関連する詳細については、「IAM ユーザーガイド」の以下のリソースを参照してください。

- IAM ユーザーにアクセス許可を委任するロールの作成
- チュートリアル: IAM ロールを使用した AWS アカウント 全体でのアクセスの委任
- IAM ポリシーを管理する

Amazon S3 ストレージレンズでのサービスにリンクされたロールの使用

Amazon S3 ストレージレンズを使用して AWS Organizations 内のすべてのアカウントでメトリクスを収集および集約するには、最初に組織の管理アカウントにより有効化された、信頼されたアクセスを S3 Storage Lens が持っていることを確認する必要があります。S3 Storage Lens は、サービスリンクロール (SLR) を作成し、そのロールが組織に属する AWS アカウント のリストを取得できるようにします。このアカウントの一覧は、S3 Storage Lens ダッシュボードまたは設定が作成または更新された場合に、すべてのメンバーアカウントの S3 リソースのメトリクスを収集するため S3 Storage Lens によって使用されます。

Amazon S3 ストレージレンズは AWS Identity and Access Management (IAM) サービスにリンクされたロールを使用します。サービスにリンクされたロールは S3 Storage Lens に直接リンクされた一意のタイプの IAM ロールです。サービスにリンクされたロールは、S3 Storage Lens によって事前定義されており、ユーザーの代わりにサービスから他の AWS のサービス を呼び出す必要のある許可がすべて含まれています。

サービスにリンクされたロールを使用すると、必要なアクセス許可を手動で追加する必要がなくなるため、S3 Storage Lens の設定が簡単になります。S3 Storage Lens は、サービスにリンクされたロールのアクセス許可を定義します。特に定義されている場合を除き、S3 Storage Lens のみがその

ロールを引き受けることができます。定義された許可には信頼ポリシーと許可ポリシーが含まれ、その許可ポリシーを他の IAM エンティティにアタッチすることはできません。

関連リソースを削除した後でなければ、このサービスにリンクされたロールを削除することはできません。これにより、リソースにアクセスするためのアクセス許可を不注意で削除することが防止され、S3 Storage Lens リソースは保護されます。

サービスにリンクされたロールをサポートするその他のサービスについては、「IAM と連携する AWS サービス」を参照の上、サービスにリンクされたロール列がはいになっているサービスを検索してください。サービスにリンクされたロールに関するドキュメントをサービスで表示するには、[はい] リンクを選択します。

Amazon S3 ストレージレンズへのサービスにリンクされたロールのアクセス許可

S3 Storage Lens は、AWSServiceRoleForS3StorageLens という名前のサービスにリンクされたロールを使用します。これにより、S3 Storage Lens によって使用または管理される AWS のサービスとリソースにアクセスできます。これにより、S3 Storage Lens は、ユーザーに代わって AWS Organizations のリソースにアクセスできるようになります。

S3 Storage Lens のサービスにリンクされたロールは、組織のストレージ上で次のサービスを信頼します。

- `storage-lens.s3.amazonaws.com`

ロールのアクセス許可ポリシーは、以下のアクションを実行することを S3 Storage Lens に許可します。

- `organizations:DescribeOrganization`

  `organizations:ListAccounts`

  `organizations:ListAWSServiceAccessForOrganization`

  `organizations:ListDelegatedAdministrators`

サービスにリンクされたロールの作成、編集、削除を IAM エンティティ (ユーザー、グループ、ロールなど) に許可するには、アクセス許可を設定する必要があります。詳細については、IAM ユーザーガイドのサービスにリンクされたロールのアクセス許可を参照してください。

S3 Storage Lens へのサービスにリンクされたロールの作成

サービスにリンクされたロールを手動で作成する必要はありません。AWS Organizations 管理アカウントまたは委任された管理者アカウントにサインインしているときに次のいずれかのタスクを完了すると、S3 Storage Lens がサービスにリンクされたロールを作成します。

- Amazon S3 コンソールで、組織用の S3 Storage Lens ダッシュボード設定を作成する。
- REST API、AWS CLI、SDK を使用して組織に S3 Storage Lens 設定を PUT する。

> **Note**
>
> S3 Storage Lens は組織ごとに最大 5 人の委任管理者をサポートします。

このサービスにリンクされたロールを削除した場合、前述のアクションによって必要に応じてロールが再作成されます。

S3 Storage Lens サービスにリンクされたロールのポリシーの例

Example S3 Storage Lens のサービスにリンクされたロールへのアクセス許可ポリシー

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AwsOrgsAccess",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListDelegatedAdministrators"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Amazon S3 ストレージレンズのサービスにリンクされたロールの編集

S3 Storage Lens では、AWSServiceRoleForS3StorageLens サービスリンクロールを編集することはできません。サービスリンクロールを作成すると、多くのエンティティによってロールが参照される可能性があるため、ロール名を変更することはできません。ただし、IAM を使用したロール記述の編集はできます。詳細については、IAM ユーザーガイドのサービスにリンクされたロールの編集を参照してください。

Amazon S3 ストレージレンズのサービスにリンクされたロールの削除

サービスにリンクされたロールが不要になった場合は、そのロールを削除することをお勧めします。そうすることで、使用していないエンティティがアクティブにモニタリングされたり、メンテナンスされたりすることがなくなります。ただし、手動で削除する前に、サービスにリンクされたロールのリソースをクリーンアップする必要があります。

> **Note**
>
> リソースを削除する際に、Amazon S3 ストレージレンズサービスでそのロールが使用されている場合、削除は失敗することがあります。失敗した場合は、数分待ってから再度オペレーションを実行してください。

AWSServiceRoleForS3StorageLens を削除するには、AWS Organizations 管理アカウントまたは委任された管理者アカウントを使用して、すべての AWS リージョン に存在する組織レベルの S3 Storage Lens 設定をすべて削除する必要があります。

リソースは組織レベルの S3 Storage Lens 設定です。S3 Storage Lens を使用してリソースをクリーンアップし、IAM コンソール、CLI、REST API、または AWS SDK を使用してロールを削除します。

REST API、AWS CLI、SDK では、`ListStorageLensConfigurations` を使用して組織が S3 Storage Lens 設定を作成したすべてのリージョンで S3 Storage Lens 設定を見つけることができます。`DeleteStorageLensConfiguration` アクションを使用してこれらの設定を削除し、ロールを削除できるようにします。

> **Note**
>
> サービスにリンクされたロールを削除するには、すべてのリージョンに存在する組織レベルの S3 Storage Lens 設定をすべて削除する必要があります。

AWSServiceRoleForS3StorageLens SLR で使用されている Amazon S3 ストレージレンズリソースを削除するには

1. 組織レベルの設定一覧を取得するには、S3 Storage Lens 設定があるすべてのリージョンで `ListStorageLensConfigurations` を使用する必要があります。この一覧は Amazon S3 コンソールから取得することもできます。
2. これらの設定は、`DeleteStorageLensConfiguration` API コールを呼び出すか Amazon S3 コンソールを使用して、適切なリージョンのエンドポイントから削除する必要があります。

サービスリンクロールを IAM で手動削除するには

設定を削除した後、IAM コンソールから、または IAM API `DeleteServiceLinkedRole` を呼び出すか、AWS CLI もしくは AWS SDK を使用して、AWSServiceRoleForS3StorageLens SLR を削除できます。詳細については、IAM ユーザーガイド のサービスにリンクされたロールの削除を参照してください。

S3 Storage Lens のサービスにリンクされたロールがサポートされるリージョン

S3 Storage Lens は、そのサービスを利用できるすべての AWS リージョンで、サービスにリンクされたロールの使用をサポートします。詳細については、Amazon S3 Regions and Endpoints を参照してください。

Amazon S3 アイデンティティとアクセスのトラブルシューティング

以下の情報を使用して、Amazon S3 と IAM の使用時に発生する可能性がある一般的な問題の診断と修正に役立てます。

トピック

- アクセス拒否エラーが表示された
- Amazon S3 でアクションを実行する権限がありません
- iam:PassRole を実行する権限がありません
- 自分の AWS アカウント 以外のユーザーに Amazon S3 リソースへのアクセスを許可したい
- Amazon S3 でのアクセス拒否 (403 Forbidden) エラーのトラブルシューティング

アクセス拒否エラーが表示された

バケットポリシーまたはアイデンティティベースポリシーのいずれにも、アクセス許可を付与するリクエスタに対する明示的な Deny ステートメントがないことを確認します。

アクセス拒否エラーのトラブルシューティングの詳細については、「Amazon S3 でのアクセス拒否 (403 Forbidden) エラーのトラブルシューティング」を参照してください。

Amazon S3 でアクションを実行する権限がありません

アクションを実行する権限がないというエラーが表示された場合は、そのアクションを実行できるようにポリシーを更新する必要があります。

次のエラー例は、mateojackson IAM ユーザーがコンソールを使用して、ある *my-example-widget* リソースに関する詳細情報を表示しようとしたことを想定して、その際に必要な s3:*GetWidget* アクセス許可を持っていない場合に発生するものです。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 s3:GetWidget on resource: my-example-widget
```

この場合、s3:*GetWidget* アクションを使用して *my-example-widget* リソースへのアクセスを許可するように、mateojackson ユーザーのポリシーを更新する必要があります。

サポートが必要な場合は、AWS 管理者に問い合わせてください。サインイン認証情報を提供した担当者が管理者です。

iam:PassRole を実行する権限がありません

iam:PassRole アクションを実行する権限がないというエラーが表示された場合は、ポリシーを更新して Amazon S3 にロールを渡せるようにする必要があります。

一部の AWS のサービスでは、新しいサービスロールまたはサービスリンクロールを作成せずに、既存のロールをサービスに渡すことが許可されています。そのためには、サービスにロールを渡す権限が必要です。

次のエラー例は、marymajor という IAM ユーザーがコンソールを使用して Amazon S3 でアクションを実行しようとする場合に発生します。ただし、このアクションをサービスが実行するには、サービスロールから付与された権限が必要です。メアリーには、ロールをサービスに渡す許可がありません。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

この場合、Mary のポリシーを更新してメアリーに `iam:PassRole` アクションの実行を許可する必要があります。

サポートが必要な場合は、AWS 管理者に問い合わせてください。サインイン認証情報を提供した担当者が管理者です。

自分の AWS アカウント 以外のユーザーに Amazon S3 リソースへのアクセスを許可したい

他のアカウントのユーザーや組織外の人が、リソースにアクセスするために使用できるロールを作成できます。ロールの引き受けを委託するユーザーを指定できます。リソースベースのポリシーまたはアクセスコントロールリスト (ACL) をサポートするサービスの場合、それらのポリシーを使用して、リソースへのアクセスを付与できます。

詳細については、以下を参照してください。

- Amazon S3 がこれらの機能をサポートしているかどうかを確認するには、「Amazon S3 での IAM の機能」を参照してください。
- 所有している AWS アカウント 全体のリソースへのアクセス権を提供する方法については、「IAM ユーザーガイド」の「所有している別の AWS アカウント へのアクセス権を IAM ユーザーに提供」を参照してください。
- サードパーティーの AWS アカウント にリソースへのアクセス権を提供する方法については、「IAM ユーザーガイド」の「サードパーティーが所有する AWS アカウント へのアクセス権を付与する」を参照してください。
- ID フェデレーションを介してアクセスを提供する方法については、「IAM ユーザーガイド」の「外部で認証されたユーザー (ID フェデレーション) へのアクセスの許可」を参照してください。
- クロスアカウントアクセスにおけるロールとリソースベースのポリシーの使用方法の違いについては、「IAM ユーザーガイド」の「IAM でのクロスアカウントのリソースへのアクセス」を参照してください。

Amazon S3 でのアクセス拒否 (403 Forbidden) エラーのトラブルシューティング

アクセス拒否 (HTTP `403 Forbidden`) エラーは、AWS が認可リクエストを明示的または暗黙的に拒否した場合に表示されます。

- 明示的な拒否は、特定の AWS アクションに対する Deny ステートメントがポリシーに含まれている場合に発生します。
- 該当する Deny ステートメントがなく、該当する Allow ステートメントもない場合に、暗黙的な拒否が発生します。

AWS Identity and Access Management (IAM) ポリシーはデフォルトで IAM プリンシパルを暗黙的に拒否するため、ポリシーではプリンシパルのアクションの実行を明示的に許可する必要があります。それ以外の場合、ポリシーは暗黙的にアクセスを拒否します。詳細については、「IAM ユーザーガイド」の「明示的な拒否と暗黙的な拒否の違い」を参照してください。アクセスリクエストを許可または拒否するかを決定するポリシー評価ロジックの詳細については、「IAM ユーザーガイド」の「ポリシーの評価ロジック」を参照してください。

S3 リソースタイプ別の S3 API オペレーションへのアクセス許可の詳細については、「Amazon S3 API オペレーションに必要なアクセス許可」を参照してください。

以降のトピックでは、Amazon S3 でのアクセス拒否 (403 Forbidden) エラーの最も一般的な原因について説明します。

> **Note**
>
> アクセス拒否 (HTTP 403 Forbidden) エラーの場合、バケット所有者の個別の AWS アカウントまたはバケット所有者の AWS 組織の外部でリクエストが開始された場合、バケット所有者に対する Amazon S3 の料金は発生しません。

トピック

- アクセス拒否メッセージの例とトラブルシューティング方法
- バケットポリシーと IAM ポリシー
- Amazon S3 ACL 設定
- S3 ブロックパブリックアクセス設定
- Amazon S3 の暗号化設定
- S3 オブジェクトロック設定
- VPC エンドポイントポリシー
- AWS Organizations ポリシー
- CloudFront ディストリビューションアクセス

- アクセスポイント設定
- 追加リソース

> **Note**
>
> アクセス許可の問題をトラブルシューティングする場合は、the section called “アクセス拒否メッセージの例とトラブルシューティング方法” セクションから始めて、??? セクションに移動します。「the section called “アクセス許可を確認するためのヒント”」のガイダンスに従う必要もあります。

アクセス拒否メッセージの例とトラブルシューティング方法

Amazon S3 は、同じ AWS アカウント 内のリソースに対して行われたリクエストのアクセス拒否 (HTTP `403 Forbidden`) エラーに追加コンテキストを含めるようになりました。この新しいコンテキストには、アクセスを拒否したポリシーのタイプ、拒否の理由、リソースへのアクセスをリクエストした IAM ユーザーまたはロールに関する情報が含まれます。

この追加のコンテキストは、アクセス問題のトラブルシューティング、アクセス拒否エラーの根本原因の特定、関連するポリシーの更新による誤ったアクセスコントロールの修正に役立ちます。この追加のコンテキストは、AWS CloudTrail ログでも使用できます。AWS GovCloud (US) Regions および中国リージョンを含むすべての AWS リージョンで、同じアカウントリクエストに対する拡張アクセス拒否エラーメッセージが利用可能になりました。

ほとんどのアクセス拒否のエラーメッセージは、`User` *`user-arn`* `is not authorized to perform` *`action`* `on "`*`resource-arn`*`" because` *`context`* の形式です。この例では、*`user-arn`* は、アクセス権がないユーザーの Amazon リソースネーム (ARN)、*`action`* はポリシーが拒否するサービスアクション、*`resource-arn`* はポリシーが対象とするリソースの ARN です。*`context`* フィールドには、ポリシータイプについての追加のコンテキストが表示され、ポリシーがアクセスを拒否した理由が説明されます。

ポリシー内の `Deny` ステートメントで明示的にポリシーがアクセスを拒否した場合、アクセス拒否エラーメッセージには、`with an explicit deny in a` *`type`* `policy` というフレーズが含まれます。ポリシーがアクセスを暗黙的に拒否する場合、アクセス拒否エラーメッセージには、`because no` *`type`* `policy allows the` *`action`* `action` というフレーズが含まれます。

Important

- 拡張アクセス拒否メッセージは、同じアカウントリクエストに対してのみ返されます。クロスアカウントリクエストの場合は、汎用の `Access Denied` メッセージが返されます。

  クロスアカウントアクセスリクエストを許可または拒否するかを決定するポリシー評価ロジックの詳細については、「IAM ユーザーガイド」の「クロスアカウントのポリシーの評価ロジック」を参照してください。クロスアカウントアクセスを許可する方法を説明するチュートリアルについては、「the section called “クロスアカウントアクセス許可の付与”」を参照してください。
- ディレクトリバケットに対するリクエストに関しては、拡張アクセス拒否エラーメッセージは返されません。ディレクトリバケットリクエストの場合は、汎用の `Access Denied` メッセージが返されます。
- ポリシータイプが同じである複数のポリシーが認可リクエストを拒否した場合、アクセスは拒否され、エラーメッセージではポリシーの番号が特定されません。
- 複数のポリシータイプで認可リクエストが拒否された場合、エラーメッセージには、これらのポリシータイプのうち 1 つだけが含まれます。
- 複数の理由でアクセスリクエストが拒否された場合でも、エラーメッセージに含まれるのは、いずれか 1 つの拒否理由のみです。

次の例では、さまざまなタイプのアクセス拒否エラーメッセージの形式と、各タイプのメッセージに関するトラブルシューティング方法を説明しています。

リソースコントロールポリシーによるアクセスの拒否 - 明示的な拒否

1. リソースコントロールポリシー (RCP) 内のアクションの `Deny` ステートメントを確認します。次の例では、`s3:GetObject` がアクションです。
2. `Deny` ステートメントを削除して、RCP を更新してください。詳細については、「AWS Organizations ユーザーガイド」の「Update a resource control policy (RCP)」を参照してください。

```
An error occurred (AccessDenied) when calling the GetObject operation:
User: arn:aws:iam::777788889999:user/MaryMajor is not authorized to perform:
s3:GetObject on resource: "arn:aws:s3:::amzn-s3-demo-bucket1/object-name"
with an explicit deny in a resource control policy
```

サービスコントロールポリシーによるアクセスの拒否 - 暗黙的な拒否

1. サービスコントロールポリシー (SCP) のアクションで、Allow ステートメントが欠けていないかを確認します。次の例では、s3:GetObject がアクションです。
2. Allow ステートメントを追加して、ポリシーを更新してください。詳細については、「AWS Organizations ユーザーガイド」の「SCP の更新」を参照してください。

```
User: arn:aws:iam::777788889999:user/MaryMajor is not authorized to perform:
s3:GetObject because no service control policy allows the s3:GetObject action
```

サービスコントロールポリシーによるアクセスの拒否 - 明示的な拒否

1. サービスコントロールポリシー (SCP) のアクションで、Deny ステートメントを確認します。次の例では、s3:GetObject がアクションです。
2. Deny ステートメントを変更して SCP を更新し、必要なアクセスをユーザーに許可します。これを行う方法の例については、「AWS Organizations ユーザーガイド」の「特定の管理者ロールを除いて、IAM ユーザーとロールが特定の変更を行わないようにする」を参照してください。SCP の更新に関する詳細については、「AWS Organizations ユーザーガイド」の「SCP の更新」を参照してください。

```
User: arn:aws:iam::777788889999:user/MaryMajor is not authorized to perform:
s3:GetObject with an explicit deny in a service control policy
```

VPC エンドポイントポリシーによるアクセスの拒否 – 暗黙的な拒否

1. 仮想プライベートクラウド (VPC) エンドポイントポリシーのアクションで、Allow ステートメントが欠落していないかを確認します。次の例では、s3:GetObject がアクションです。
2. Allow ステートメントを追加して、VPC エンドポイントポリシーを更新します。詳細については、「AWS PrivateLink ガイド」の「VPC エンドポイントポリシーを更新する」を参照してください。

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject because no VPC endpoint policy allows the s3:GetObject action
```

VPC エンドポイントポリシーによるアクセスの拒否 – 明示的拒否

1. 仮想プライベートクラウド (VPC) エンドポイントポリシーのアクションに、明示的な Deny ステートメントがあるかを確認します。次の例では、s3:GetObject がアクションです。
2. Deny ステートメントを変更して VPC エンドポイントポリシーを更新し、ユーザーに必要なアクセスを許可します。例えば、Deny ステートメントを更新して、aws:PrincipalAccount 条件キーと StringNotEquals 条件演算子を使用し、the section called “例 7: Deny ステートメントからプリンシパルを除外する” に示すように、特定のプリンシパルアクセスを許可できます。VPC エンドポイントポリシーの更新の詳細については、「AWS PrivateLink ガイド」の「VPC エンドポイントポリシーの更新」を参照してください。

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject on resource: "arn:aws:s3:::amzn-s3-demo-bucket1/object-name" with
an explicit deny in a VPC endpoint policy
```

アクセス許可の境界によりアクセスの拒否 – 暗黙的な拒否

1. アクセス許可の境界にあるアクションで、Allow ステートメントが欠落してないかを確認してください。次の例では、s3:GetObject がアクションです。
2. IAM ポリシーに Allow ステートメントを追加して、アクセス許可の境界を更新してください。詳細については、「IAM ユーザーガイド」の「IAM エンティティのアクセス許可の境界」と「IAM ポリシーの編集」を参照してください。

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject on resource: "arn:aws:s3:::amzn-s3-demo-bucket1/object-name"
because no permissions boundary allows the s3:GetObject action
```

アクセス許可の境界によりアクセスの拒否 – 明示的拒否

1. アクセス許可の境界にあるアクションで、明示的な Deny ステートメントを確認してください。次の例では、s3:GetObject がアクションです。
2. IAM ポリシーの Deny ステートメントを変更してアクセス許可の境界を更新し、ユーザーに必要なアクセスを許可します。例えば、「IAM ユーザーガイド」の aws:PrincipalAccount に示すように、aws:PrincipalAccount 条件キーと StringNotEquals 条件演算子を使用して、特定のプリンシパルアクセスを許可するように Deny ステートメントを更新できます。詳細について

は、「IAM ユーザーガイド」の「IAM エンティティのアクセス許可の境界」と「IAM ポリシーの編集」を参照してください。

```
User: arn:aws:iam::777788889999:user/MaryMajor is not authorized to perform:
s3:GetObject with an explicit deny in a permissions boundary
```

セッションポリシーによるアクセスの拒否 – 暗黙的な拒否

1. セッションポリシーにあるアクションで、Allow ステートメントが欠落していないかを確認してください。次の例では、s3:GetObject がアクションです。
2. Allow ステートメントを追加して、セッションポリシーを更新してください。詳細については、「IAM ユーザーガイド」の「セッションポリシー」と「IAM ポリシーの編集」を参照してください。

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject because no session policy allows the s3:GetObject action
```

セッションポリシーによるアクセスの拒否 – 明示的拒否

1. セッションポリシーにあるアクションで、明示的な Deny ステートメントがあるのかを確認してください。次の例では、s3:GetObject がアクションです。
2. Deny ステートメントを変更してセッションポリシーを更新し、ユーザーに必要なアクセスを許可します。例えば、Deny ステートメントを更新して、aws:PrincipalAccount 条件キーと StringNotEquals 条件演算子を使用し、the section called “例 7: Deny ステートメントからプリンシパルを除外する” に示すように、特定のプリンシパルアクセスを許可できます。セッションポリシーの更新の詳細については、「IAM ユーザーガイド」の「セッションポリシー」および「IAM ポリシーの編集」を参照してください。

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject on resource: "arn:aws:s3:::amzn-s3-demo-bucket1/object-name" with
an explicit deny in a session policy
```

リソースベースのポリシーによるアクセスの拒否 – 暗黙的な拒否

> **Note**
>
> リソースベースのポリシーとは、バケットポリシーやアクセスポイントポリシーなどのポリシーを指します。

1. リソースベースのポリシーにあるアクションで、Allow ステートメントが欠落してないかを確認してください。IgnorePublicAcls S3 ブロックパブリックアクセス設定が、バケット、アクセスポイント、またはアカウントレベルに適用されているかどうかも確認します。次の例では、s3:GetObject がアクションです。
2. Allow ステートメントを追加して、ポリシーを更新してください。詳細については、「IAM ユーザーガイド」の「リソースベースのポリシー」と「IAM ポリシーの編集」を参照してください。

   バケット、アクセスポイント、またはアカウントの IgnorePublicAcls ブロックパブリックアクセス設定を調整する必要がある場合もあります。詳細については、「the section called “ブロックパブリックアクセス設定によるアクセス拒否”」および「the section called “バケットとアクセスポイントの設定”」を参照してください。

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject because no resource-based policy allows the s3:GetObject action
```

リソースベースのポリシーによるアクセスの拒否 – 明示的拒否

> **Note**
>
> リソースベースのポリシーとは、バケットポリシーやアクセスポイントポリシーなどのポリシーを指します。

1. リソースベースのポリシーにあるアクションで、明示的な Deny ステートメントがあるのかを確認してください。RestrictPublicBuckets S3 ブロックパブリックアクセス設定が、バケット、アクセスポイント、またはアカウントレベルに適用されているかどうかも確認します。次の例では、s3:GetObject がアクションです。
2. Deny ステートメントを変更してポリシーを更新し、ユーザーに必要なアクセスを許可します。例えば、Deny ステートメントを更新して、aws:PrincipalAccount 条件キーと

StringNotEquals 条件演算子を使用し、the section called “例 7: Deny ステートメントからプリンシパルを除外する” に示すように、特定のプリンシパルアクセスを許可できます。リソースベースのポリシーの更新に関する詳細については、「IAM ユーザーガイド」の「リソースベースのポリシー」および「IAM ポリシーの編集」を参照してください。

バケット、アクセスポイント、またはアカウントの RestrictPublicBuckets ブロックパブリックアクセス設定を調整する必要がある場合もあります。詳細については、「the section called “ブロックパブリックアクセス設定によるアクセス拒否”」および「the section called “バケットとアクセスポイントの設定”」を参照してください。

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject on resource: "arn:aws:s3:::amzn-s3-demo-bucket1/object-name" with
an explicit deny in a resource-based policy
```

ID ベースのポリシーによるアクセスの拒否 – 暗黙的な拒否

1. ID にアタッチされた ID ベースのポリシーにあるアクションに対して、Allow ステートメントが欠落していないかを確認してください。次の例のアクションは、ユーザー MaryMajor にアタッチされた s3:GetObject です。
2. Allow ステートメントを追加して、ポリシーを更新してください。詳細については、「IAM ユーザーガイド」の「アイデンティティベースのポリシー」と「IAM ポリシーの編集」を参照してください。

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject because no identity-based policy allows the s3:GetObject action
```

ID ベースのポリシーによるアクセスの拒否 – 明示的拒否

1. ID にアタッチされた ID ベースのポリシーにあるアクションに対して、明示的な Deny ステートメントがあるのかを確認してください。次の例のアクションは、ユーザー MaryMajor にアタッチされた s3:GetObject です。
2. Deny ステートメントを変更してポリシーを更新し、ユーザーに必要なアクセスを許可します。例えば、「IAM ユーザーガイド」の aws:PrincipalAccount に示すように、aws:PrincipalAccount 条件キーと StringNotEquals 条件演算子を使用して、特定のプリンシパルアクセスを許可するように Deny ステートメントを更新できます。詳細について

は、「IAM ユーザーガイド」の「アイデンティティベースのポリシー」と「IAM ポリシーの編集」を参照してください。

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject on resource: "arn:aws:s3:::amzn-s3-demo-bucket1/object-name" with
an explicit deny in an identity-based policy
```

ブロックパブリックアクセス設定によるアクセス拒否

Amazon S3 のパブリックアクセスブロック機能は、Amazon S3 のリソースへのパブリックアクセスの管理に役立つ、アクセスポイント、バケット、アカウントの設定を提供します。Amazon S3 が「パブリック」を定義する方法の詳細については、「「パブリック」の意味」を参照してください。

デフォルトでは、新しいバケット、アクセスポイント、およびオブジェクトはパブリックアクセスを許可しません。ただし、ユーザーはバケットポリシー、アクセスポイントポリシー、IAM ユーザーポリシー、オブジェクトのアクセス許可、またはアクセスコントロールリスト (ACL) を変更することで、パブリックアクセスを許可できます。S3 ブロックパブリックアクセス設定は、このようなポリシー、アクセス許可、ACL を上書きします。2023 年 4 月以降、すべてのブロックパブリックアクセス設定がデフォルトで新しいバケットに対して有効になります。

Amazon S3 はバケットやオブジェクトへのアクセスのリクエストを受け取ると、バケットやバケット所有者のアカウントに適用されているパブリックアクセスブロック設定があるかどうかを確認します。リクエストがアクセスポイントを経由している場合、Amazon S3 はアクセスポイントのパブリックアクセスブロック設定も確認します。リクエストされたアクセスを禁止する既存のパブリックアクセスブロック設定がある場合、Amazon S3 はそのリクエストを拒否します。

Amazon S3 のパブリックアクセスブロックには、4 つの設定があります。これらの設定は、独立しており、任意の組み合わせで使用できます。各設定は、アクセスポイント、バケット、または AWS アカウント全体に適用できます。アクセスポイント、バケット、アカウントのパブリックアクセスブロック設定が異なる場合、Amazon S3 は、アクセスポイント、バケット、アカウントの設定の組み合わせで最も制限が厳しいものを適用します。

Amazon S3 は、パブリックアクセスブロック設定でオペレーションが禁止されているかどうかを評価し、アクセスポイント、バケット、アカウントの設定に違反しているすべてのリクエストを拒否します。

Amazon S3 ブロックパブリックアクセスが提供する 4 つの設定:

- BlockPublicAcls – この設定は、PutBucketAcl、PutObjectAcl、PutObject、CreateBucket、CopyObject、POST Object のリクエストに適用されます。BlockPublicAcls の設定により、次のように動作します。
  - 指定されたアクセスコントロールリスト (ACL) がパブリックである場合、PutBucketAcl と PutObjectAcl の呼び出しは失敗します。
  - リクエストにパブリック ACL が含まれている場合、PutObject の呼び出しは失敗します。
  - この設定がアカウントに適用されている場合、リクエストにパブリック ACL が含まれていると、CreateBucket の呼び出しは失敗し、HTTP 400 (Bad Request) レスポンスが返されます。

  例えば、BlockPublicAcls の設定により CopyObject リクエストのアクセスが拒否されると、次のとおりのメッセージが表示されます。

  ```
  An error occurred (AccessDenied) when calling the CopyObject operation:
  User: arn:aws:sts::123456789012:user/MaryMajor is not authorized to
  perform: s3:CopyObject on resource: "arn:aws:s3:::amzn-s3-demo-bucket1/object-name"
  because public access control lists (ACLs) are blocked by the BlockPublicAcls block
  public access setting.
  ```

- IgnorePublicAcls – IgnorePublicAcls 設定を使用すると、Amazon S3 はバケットとバケット内のすべてのオブジェクトのパブリック ACL を無視します。リクエストの許可がパブリック ACL によってのみ付与されている場合は、IgnorePublicAcls 設定によってリクエストが拒否されます。

  IgnorePublicAcls 設定による拒否は、すべて暗黙的です。例えば、パブリック ACL により、IgnorePublicAcls が GetObject リクエストを拒否すると、次のとおりのメッセージが返されます。

  ```
  User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
  s3:GetObject because no resource-based policy allows the s3:GetObject action
  ```

- BlockPublicPolicy – この設定は、PutBucketPolicy と PutAccessPointPolicy のリクエストに適用されます。

  バケットに対して BlockPublicPolicy を設定すると、指定されたバケットポリシーでパブリックアクセスが許可されている場合、Amazon S3 は PutBucketPolicy への呼び出しを拒否します。この設定により、指定されたポリシーでパブリックアクセスが許可されている場合、Amazon

S3 はバケットの同じアカウントのすべてのアクセスポイントに対する PutAccessPointPolicy への呼び出しも拒否します。

アクセスポイントで BlockPublicPolicy を設定すると、指定されたポリシー (アクセスポイントまたは基盤となるバケットのいずれか) でパブリックアクセスが許可されている場合、Amazon S3 はアクセスポイント経由で行われる PutAccessPointPolicy および PutBucketPolicy への呼び出しを拒否します。

例えば、BlockPublicPolicy の設定が原因で PutBucketPolicy リクエストのアクセスが拒否されると、次のとおりのメッセージが表示されます。

```
An error occurred (AccessDenied) when calling the PutBucketPolicy operation:
User: arn:aws:sts::123456789012:user/MaryMajor is not authorized to
perform: s3:PutBucketPolicy on resource: "arn:aws:s3:::amzn-s3-demo-bucket1/object-
name"
because public policies are blocked by the BlockPublicPolicy block public
access setting.
```

- RestrictPublicBuckets – RestrictPublicBuckets 設定は、パブリックポリシーを持つアクセスポイントまたはバケットへのアクセスを、バケット所有者のアカウントとアクセスポイント所有者のアカウント内の AWS のサービスのプリンシパルと承認済みのユーザーのみに制限します。この設定により、アクセスポイントまたはバケットへのすべてのクロスアカウントアクセスがブロックされます (AWS のサービスのプリンシパルによるアクセスを除く)。ただし、アカウント内のユーザーは引き続きアクセスポイントまたはバケットを管理できます。この設定では、匿名 (または署名なし) のコールもすべて拒否されます。

  RestrictPublicBuckets 設定による拒否は、すべて暗黙的です。例えば、RestrictPublicBuckets がパブリックバケットまたはアクセスポイントポリシーにより GetObject リクエストを拒否した場合、次のメッセージが表示されます。

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject on resource: "arn:aws:s3:::amzn-s3-demo-bucket1/object-name" with
an explicit deny in a resource-based policy
```

これらの設定の詳細については、「the section called “パブリックアクセスブロック設定”」をご参照ください。これらの設定を確認して更新するには、「the section called “パブリックアクセスブロックの設定”」を参照してください。

バケットポリシーと IAM ポリシー

バケットレベルの操作

バケットポリシーが設定されていない場合、バケットはバケット所有者のアカウントの任意の AWS Identity and Access Management (IAM) アイデンティティからのリクエストを暗黙的に許可します。また、バケットは、他の任意のアカウントからの他の IAM ID からのリクエストや、匿名の (署名されていない) リクエストを暗黙的に拒否します。ただし、IAM ユーザーポリシーが設定されていない場合、リクエスタのすべてのリクエストは (AWS アカウントのルートユーザーでない限り) 暗黙的に拒否されます。詳細については、IAM ユーザーガイドの「アカウント内でのリクエストの許可または拒否の決定」を参照してください。

オブジェクトレベルの操作

バケット所有アカウントがオブジェクトを所有している場合、バケットポリシーと IAM ユーザーポリシーは、オブジェクトレベルの操作でもバケットレベルの操作と同じように機能します。例えば、バケットポリシーが設定されていない場合、バケットはバケット所有者のアカウントの任意の IAM アイデンティティからのオブジェクトリクエストを暗黙的に許可します。また、バケットは、他の任意のアカウントの他の IAM ID からのオブジェクトリクエストや、匿名 (署名なし) リクエストを暗黙的に拒否します。ただし、IAM ユーザーポリシーが設定されていない場合、リクエスタのすべてのオブジェクトリクエストは (AWS アカウントのルートユーザーでない限り) 暗黙的に拒否されます。

オブジェクトが外部アカウントによって所有されている場合、オブジェクトへのアクセスはオブジェクトアクセスコントロールリスト (ACL) を通じてのみ許可されます。バケットポリシーと IAM ユーザーポリシーは、引き続きオブジェクトリクエストを拒否するために使用できます。

したがって、バケットポリシーまたは IAM ユーザーポリシーによりアクセス拒否 (403 Forbidden) エラーが発生しないことを確認するには、次の要件が満たされていることを確認します。

- 同じアカウントでアクセスする場合、バケットポリシーまたは IAM ユーザーポリシーのいずれにも、アクセス権限を付与するリクエスタに対する明示的な `Deny` 記述があってはなりません。バケットポリシーと IAM ユーザーポリシーのみを使用してアクセス権限を付与する場合は、これらのポリシーの 1 つに少なくとも 1 つの明示的な `Allow` ステートメントが必要です。
- クロスアカウントアクセスの場合、バケットポリシーまたは IAM ユーザーポリシーのいずれにも、アクセス許可を付与するリクエスタに対する明示的な `Deny` ステートメントを含めることはできません。バケットポリシーと IAM ユーザーポリシーのみを使用してクロスアカウントアクセス許可を付与する場合は、リクエスタのバケットポリシーと IAM ユーザーポリシーの両方に明示的な `Allow` ステートメントが含まれていることを確認します。

> **Note**
>
> バケットポリシーの `Allow` ステートメントは、同じバケット所有アカウントが所有するオブジェクトにのみ適用されます。ただし、バケットポリシーの `Deny` ステートメントは、オブジェクトの所有権に関係なくすべてのオブジェクトに適用されます。

バケットポリシーを確認または編集する方法

> **Note**
>
> バケットポリシーを表示または編集するには、`s3:GetBucketPolicy` アクセス許可が必要です。

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。
3. [バケット] リストで、バケットポリシーを表示または編集するバケットの名前を選択します。
4. [アクセス許可] タブを選択します。
5. [バケットポリシー] で [編集] を選択します。[バケットポリシーを編集] ページが表示されます。

AWS Command Line Interface (AWS CLI) を使用してバケットポリシーを確認または編集するには、get-bucket-policy コマンドを使用します。

> **Note**
>
> バケットポリシーが適正でないためにバケットからロックアウトされた場合は、AWS アカウントのルートユーザー認証情報を使用してAWS Management Consoleにサインインします。バケットへのアクセスを回復するには、必ず AWS アカウントのルートユーザーの認証情報を使用してバケットポリシーを削除します。

アクセス許可を確認するためのヒント

リクエスタが Amazon S3 オペレーションを実行するための適切な権限を持っているかどうかを確認するには、以下を試してください。

- リクエスタを特定します。署名なしのリクエストの場合、IAM ユーザーポリシーのない匿名リクエストです。署名済み URL を使用したリクエストの場合、ユーザーポリシーは、リクエストに署名した IAM ユーザーまたはロールのポリシーと同じになります。
- 正しい IAM ユーザーまたはロールを使用していることを確認します。IAM ユーザーまたはロールを確認するには、AWS Management Console の右上隅を確認するか、aws sts get-caller-identity コマンドを使用することができます。
- IAM ユーザーまたはロールに関連付けられている IAM ポリシーを確認します。次のいずれかの方法を使用します。
  - IAM ポリシーシミュレーターを使用して IAM ポリシーをテストします。
  - さまざまな IAM ポリシータイプを確認します。
- 必要に応じて、IAM ユーザーポリシーを編集します。
- アクセスを明示的に拒否または許可するポリシーについては、以下の例を確認してください。
  - IAM ユーザーポリシーの明示的な許可: IAM: 複数のサービスへのアクセスをプログラムおよびコンソールで許可および拒否
  - バケットポリシーの明示的許可: オブジェクトをアップロードしたり、パブリックアクセス用のオブジェクト ACL を設定したりする権限を複数のアカウントに付与
  - IAM ユーザーポリシーの明示的拒否: AWS: リクエストされた AWS リージョン に基づいてAWS へのアクセスを拒否
  - バケットポリシーの明示的拒否: バケットに書き込まれるすべてのオブジェクトに SSE-KMS が必要

Amazon S3 ACL 設定

ACL 設定を確認するときは、まずオブジェクト所有権の設定を確認して、バケットで ACL が有効になっているかどうかを確認してください。ACL アクセス許可を使用できるのは、アクセス許可を付与するためのみであり、リクエストを拒否するためには使用できないことに注意が必要です。ACL は、バケットポリシーや IAM ユーザーポリシーでの明示的拒否によって拒否されたリクエスタにアクセス権を付与する目的でも使用できません。

オブジェクト所有権設定にバケット所有者強制を設定

バケット所有者強制設定が有効になっている場合、この設定によってバケットとオブジェクトに適用されるすべての ACL が無効になるため、ACL 設定によってアクセス拒否 (403 Forbidden) エラーが発生する可能性はほとんどありません。Amazon S3 バケットのデフォルト (および推奨) 設定は、バケット所有者強制です。

オブジェクト所有権設定にバケット所有者優先またはオブジェクト作成者を設定

ACL 権限は、バケット所有者優先設定またはオブジェクト作成者設定でも引き続き有効です。ACL には、バケット ACL とオブジェクト ACL の 2 種類があります。この 2 種類の ACL の違いについては、「ACL アクセス許可とアクセスポリシーのアクセス許可のマッピング」を参照してください。

拒否されたリクエストのアクションに応じて、以下のようにバケットまたはオブジェクトの ACL 権限を確認してください。

- Amazon S3 が LIST、PUT オブジェクト、GetBucketAcl、または PutBucketAcl リクエストを拒否した場合は、バケットの ACL 権限を確認してください。

> **Note**
>
> バケット ACL 設定では、GET オブジェクトのアクセス許可を付与することはできません。

- Amazon S3 が S3 オブジェクトの GET リクエスト、または PutObjectAcl リクエストを拒否した場合は、そのオブジェクトの ACL 権限を確認してください。

> **Important**
>
> オブジェクトを所有するアカウントがバケットを所有するアカウントと異なる場合、オブジェクトへのアクセスはバケットポリシーによって制御されません。

クロスアカウントによるオブジェクト所有権である場合の、**GET** オブジェクトリクエストによるアクセス拒否 (403 Forbidden) エラーのトラブルシューティング

バケットのオブジェクト所有権設定を確認して、オブジェクト所有者を判断します。オブジェクト ACL へのアクセス権限がある場合は、オブジェクト所有者のアカウントを確認することもできます。(オブジェクト所有者のアカウントを表示するには、Amazon S3 コンソールでオブジェクト ACL 設定を確認します)。または、GetObjectAcl リクエストを実行してオブジェクト所有者の正規 ID を検索し、オブジェクト所有者のアカウントを確認することもできます。デフォルトでは、ACL はオブジェクト所有者のアカウントへの GET リクエストに対する明示的な許可権限を付与します。

オブジェクト所有者がバケット所有者と異なることを確認してから、ユースケースとアクセスレベルに応じて、次のいずれかの方法を選択してアクセス拒否 (403 Forbidden) エラーに対処します。

- ACL を無効にする (推奨) - この方法はすべてのオブジェクトに適用され、バケット所有者が実行できます。この方法では、バケット所有者に所有権が自動的に与えられ、バケット内のすべてのオブジェクトを完全に制御できます。この方法を実行する前に、ACL を無効にする前提条件を確認します。バケット所有者強制 (推奨) モードにバケットを設定する方法については、「既存のバケットでのオブジェクトの所有権の設定」を参照してください。

  > **Important**
  >
  > アクセス拒否 (403 Forbidden) エラーを防ぐには、ACL を無効にする前に、必ず ACL 権限をバケットポリシーに移行してください。詳細については、「ACL 権限からの移行に関するバケットポリシーの例」を参照してください。

- オブジェクト所有者をバケット所有者に変更 - この方法は個々のオブジェクトに適用できますが、オブジェクトの所有権を変更できるのはオブジェクト所有者 (または適切な権限を持つユーザー) のみです。追加の PUT コストが適用される場合があります。(詳細については、「Amazon S3 の料金」を参照してください)。この方法では、バケット所有者にオブジェクトの完全な所有権が付与され、バケット所有者はバケットポリシーを通じてオブジェクトへのアクセスを制御できます。

  オブジェクトの所有権を変更するには、以下のいずれかを実行します。

  - バケット所有者はオブジェクトをコピーしてバケットに戻すことができます。
  - バケットのオブジェクト所有権設定を「バケット所有者優先」に変更できます。バージョニングを無効にすると、バケット内のオブジェクトは上書きされます。バージョニングが有効になっている場合、同じオブジェクトの重複バージョンがバケットに表示され、バケット所有者はライフサイクルルールを期限切れに設定できます。オブジェクト所有権設定を変更する方法については、「既存のバケットでのオブジェクトの所有権の設定」を参照してください。

    > **Note**
    >
    > オブジェクト所有権の設定をバケット所有者優先に更新すると、その設定はバケットにアップロードされた新しいオブジェクトにのみ適用されます。

  - `bucket-owner-full-control` 既定オブジェクト ACL を使用して、オブジェクト所有者にオブジェクトを再度アップロードさせることができます。

    > **Note**
    >
    > クロスアカウントアップロードの場合、バケットポリシーで `bucket-owner-full-control` 既定オブジェクト ACL を要求することもできます。バケットポリシーの例につ

いては、バケット所有者はフルコントロール権限を持ちながら、オブジェクトをアップロードするためのクロスアカウントアクセス許可を付与するを参照してください。

- オブジェクト作成者をオブジェクト所有者のままにする - この方法ではオブジェクトの所有者は変更されませんが、オブジェクトへのアクセス権限を個別に付与できます。オブジェクトへのアクセス権限を付与するには、そのオブジェクトに対する PutObjectAcl 権限が必要です。次に、アクセス拒否 (403 Forbidden) エラーを修正するために、リクエスタをオブジェクトの ACL 内のオブジェクトへのアクセス権限付与者として追加します。詳細については、「ACL の設定」を参照してください。

S3 ブロックパブリックアクセス設定

失敗したリクエストがパブリックアクセスまたはパブリックポリシーに関連している場合は、アカウント、バケット、または S3 アクセスポイントの S3 ブロックパブリックアクセス設定を確認します。S3 パブリックアクセスブロック設定に関連するアクセス拒否エラーのトラブルシューティングの詳細については、「the section called “ブロックパブリックアクセス設定によるアクセス拒否”」を参照してください。

Amazon S3 の暗号化設定

Amazon S3 はバケットのサーバー側暗号化をサポートしています。サーバー側の暗号化とは、データを受信するアプリケーションまたはサービスによって、送信先でデータを暗号化することです。Amazon S3 は、AWS データセンターのディスクに書き込まれるときにデータをオブジェクトレベルで暗号化し、お客様がデータにアクセスするときに復号します。

デフォルトで、Amazon S3 では、Amazon S3 のすべてのバケットに対する基本レベルの暗号化として、Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3) が適用されるようになりました。Amazon S3 では、オブジェクトをアップロードするときにサーバー側を暗号化する方法も指定できます。

バケットのサーバー側暗号化ステータスと暗号化設定を確認する方法

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。
3. [バケット] リストで、暗号化設定を確認するバケットを選択します。
4. [プロパティ] タブを選択します。
5. [デフォルトの暗号化] セクションまでスクロールして、[暗号化タイプ] 設定を表示します。

AWS CLI を使用して暗号化設定を確認するには、get-bucket-encryption コマンドを使用します。

オブジェクトの暗号化状態を確認する方法

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。
3. [バケット] リストで、オブジェクトが含まれるバケットの名前を選択します。
4. [オブジェクト] リストで、暗号化を追加または変更するオブジェクトの名前を選択します。

   オブジェクトの詳細ページが表示されます。
5. [サーバー側の暗号化設定] セクションまでスクロールすると、オブジェクトのサーバー側暗号化設定が表示されます。

AWS CLI を使用してオブジェクト暗号化ステータスを確認するには、head-object コマンドを使用します。

暗号化とアクセス許可の要件

Amazon S3 では 3 種類のサーバー側暗号化がサポートされます。

- Amazon S3 マネージドキーを用いたサーバー側の暗号化 (SSE-S3)
- AWS Key Management Service (AWS KMS) キー (SSE-KMS) によるサーバー側の暗号化
- 顧客提供のキーを用いたサーバー側の暗号化 (SSE-C)。

暗号化設定に基づいて、以下のアクセス許可要件が満たされていることを確認します。

- SSE-S3 - 追加の権限は必要ありません。
- SSE-KMS (カスタマー管理キーを使用) - オブジェクトをアップロードするには、AWS KMS key に `kms:GenerateDataKey` 権限が必要です。オブジェクトをダウンロードしてオブジェクトのマルチパートアップロードを実行するには、KMS キーに `kms:Decrypt` 権限が必要です。
- SSE-KMS (AWS マネージドキー を使用) - リクエスタは `aws/s3` KMS キーを所有しているのと同じアカウントに属している必要があります。また、リクエスタはオブジェクトにアクセスするための正しい Amazon S3 権限を持っている必要があります。
- SSE-C (お客様提供のキーを使用) - 追加の権限は必要ありません。バケットポリシーを設定すると、バケットのオブジェクトに対してお客様が用意した暗号化キーでサーバー側の暗号化をリクエストおよび制限できます。

オブジェクトがカスタマーマネージドキーで暗号化されている場合は、KMS キーポリシーによって kms:GenerateDataKey または kms:Decrypt アクションの実行が許可されていることを確認してください。KMS キーポリシーを確認する手順については、AWS Key Management Service デベロッパーガイドの「キーポリシーの表示」を参照してください。

S3 オブジェクトロック設定

バケットで S3 オブジェクトロックが有効で、オブジェクトが保持期間またはリーガルホールドで保護されている場合、オブジェクトを削除しようとすると Amazon S3 はアクセス拒否 (403 Forbidden) エラーを返します。

バケットでオブジェクトロックが有効になっているかどうかを確認する方法

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。
3. [バケット] リストで、確認するバケットの名前を選択します。
4. [プロパティ] タブを選択します。
5. [オブジェクトロック] セクションまでスクロールします。[オブジェクトロック] 設定が [有効] または [無効] であるかを確認します。

オブジェクトが保持期間またはリーガルホールドで保護されているかを判断するには、オブジェクトのロック情報を参照します。

オブジェクトが保持期間またはリーガルホールドで保護されている場合は、次の点を確認します。

- オブジェクトバージョンがコンプライアンス保存モードで保護されている場合、それを完全に削除する方法はありません。AWS アカウントのルートユーザーを含む、すべてのリクエスタからの永続的な DELETE リクエストは、アクセス拒否 (403 Forbidden) エラーになります。また、コンプライアンス保持モードで保護されているオブジェクトの DELETE リクエストを送信すると、Amazon S3 はそのオブジェクトの削除マーカーを作成することに注意してください。
- オブジェクトバージョンがガバナンス保持モードで保護されていて s3:BypassGovernanceRetention 権限がある場合は、保護をバイパスしてバージョンを完全に削除できます。詳細については、「ガバナンスモードのバイパス」を参照してください。
- オブジェクトバージョンがリーガルホールドで保護されている場合は、永久 DELETE リクエストを実行するとアクセス拒否 (403 Forbidden) エラーが発生する可能性があります。オブジェクトバージョンを永久に削除するには、オブジェクトバージョンのリーガルホールドを解除する必要が

あります。リーガルホールドを解除するには、`s3:PutObjectLegalHold` 許可が必要です。リーガルホールドの解除の詳細については、「オブジェクトロックの設定」を参照してください。

VPC エンドポイントポリシー

仮想プライベートクラウド (VPC) エンドポイントを使用して Amazon S3 にアクセスする場合は、VPC エンドポイントポリシーによって Amazon S3 リソースへのアクセスがブロックされていないことを確認します。デフォルトでは、VPC エンドポイントポリシーは Amazon S3 へのすべてのリクエストを許可します。特定のリクエストを制限するように VPC エンドポイントポリシーを設定することもできます。VPC エンドポイントポリシーを確認する方法については、次のリソースを参照してください。

- the section called “VPC エンドポイントポリシーによるアクセスの拒否 – 暗黙的な拒否”
- the section called “VPC エンドポイントポリシーによるアクセスの拒否 – 明示的拒否”
- 「AWS PrivateLink ガイド」の「エンドポイントポリシーを使用して VPC エンドポイントへのアクセスを制御する」

AWS Organizations ポリシー

あなたの AWS アカウント が組織に所属している場合、AWS Organizations ポリシーによって Amazon S3 リソースへのアクセスがブロックされる場合があります。デフォルトでは、AWS Organizations ポリシーは Amazon S3 へのいずれのリクエストもブロックしません。ただし、AWS Organizations ポリシーが S3 バケットへのアクセスをブロックするように設定されていないことを確認してください。AWS Organizations ポリシーを確認する方法については、以下のリソースを参照してください。

- the section called “サービスコントロールポリシーによるアクセスの拒否 - 暗黙的な拒否”
- the section called “サービスコントロールポリシーによるアクセスの拒否 - 明示的な拒否”
- the section called “リソースコントロールポリシーによるアクセスの拒否 - 明示的な拒否”
- 「AWS Organizations ユーザーガイド」の「すべてのポリシーの一覧表示」

さらに、S3 バケットへのすべてのユーザーのアクセスを拒否するようにメンバーアカウントのバケットポリシーを誤って設定した場合は、IAM でメンバーアカウントの特権セッションを起動することでバケットをロック解除できます。特権セッションを起動すると、誤って設定したバケットポリシーを削除して、バケットへのアクセスを再開できます。詳細については、「AWS Identity and

Access Management ユーザーガイド」の「AWS Organizations メンバーアカウントで特権タスクを実行する」を参照してください

CloudFront ディストリビューションアクセス

CloudFront 経由で S3 静的ウェブサイトにアクセスしようとしたときに「アクセス拒否 (403 Forbidden)」エラーが発生した場合は、次の一般的な問題を確認してください。

- オリジンドメイン名の形式は正しいですか
  - REST API エンドポイントではなく S3 ウェブサイトエンドポイント形式 (bucket-name.s3-website-region.amazonaws.com) を使用していることを確認
  - バケットで静的ウェブサイトホスティングが有効になっていることを確認
- バケットポリシーで CloudFront アクセスが許可されていますか
  - バケットポリシーに CloudFront ディストリビューションのオリジンアクセスアイデンティティ (OAI) またはオリジンアクセスコントロール (OAC) のアクセス許可が含まれていることを確認
  - ポリシーに必要な s3:GetObject アクセス許可が含まれていることを確認

エラーページの設定やプロトコル設定など、その他のトラブルシューティング手順や設定については、AWS re:Post 情報センターの「Amazon S3 ウェブサイトのエンドポイントを CloudFront ディストリビューションのオリジンとして使用すると、"403 access denied" エラーが発生する理由を知りたいです」を参照してください。

> **Note**
>
> このエラーは、S3 に直接アクセスしたときに発生する可能性のある 403 エラーとは異なります。CloudFront 固有の問題については、CloudFront のディストリビューション設定と S3 の設定の両方を確認してください。

アクセスポイント設定

Amazon S3 Access Points 経由でリクエストを行っているときにアクセス拒否 (403 Forbidden) エラーが表示される場合は、次の点を確認する必要がある場合があります。

- アクセスポイントの設定
- アクセスポイントに使用される IAM ユーザーポリシー
- クロスアカウントアクセスポイントの管理または設定に使用されるバケットポリシー

アクセスポイントの設定とポリシー

- アクセスポイントを作成するときに、インターネットまたは VPC をネットワークオリジンとして指定できます。ネットワークオリジンが VPC のみに設定されている場合、Amazon S3 は指定 VPC 以外のアクセスポイントへのリクエストをすべて拒否します。アクセスポイントのネットワークオリジンを確認するには、仮想プライベートクラウドに制限された汎用バケットのアクセスポイントの作成 を参照してください。
- アクセスポイントでは、カスタムのブロックパブリックアクセス設定を構成することもできます。これは、バケットレベルまたはアカウントレベルのブロックパブリックアクセス設定と同様に機能します。カスタムのブロックパブリックアクセス設定を確認する方法は、「汎用バケットのアクセスポイントへのパブリックアクセスの管理」を参照してください。
- アクセスポイントを使用して Amazon S3 へのリクエストを正常に行うには、リクエスタが必要な IAM 権限を持っていることを確認します。詳細については、「汎用バケットのアクセスポイントを使用するための IAM ポリシーの設定」を参照してください。
- リクエストにクロスアカウントアクセスポイントが含まれる場合、バケット所有者がアクセスポイントからのリクエストを許可するようにバケットポリシーを更新済みであることを確認します。詳細については、「クロスアカウントアクセスポイントへのアクセス許可の付与」を参照してください。

このトピックのすべての項目を確認してもアクセス拒否 (403 Forbidden) エラーが解決しない場合は、Amazon S3 リクエスト ID を取得して、追加ガイダンスについて サポート まで問い合わせてください。

追加リソース

アクセス拒否 (403 Forbidden) エラーに関する詳細なガイダンスについては、次のリソースを確認できます。

- AWS re:Post 情報センターの「Amazon S3 での、403 Access Denied エラーをトラブルシューティングする方法を教えてください」。
- AWS re:Post 情報センターの、「Amazon S3 にファイルをアップロードしようとすると「403 禁止」エラーが表示されるのはなぜですか」。
- AWS re:Post 情報センターの、「すべてのリソースが同じ AWS アカウントからのものである場合、Amazon S3 バケットからの 403 アクセス拒否エラーをトラブルシューティングする方法を教えてください」。
- AWS re:Post 情報センターの、「パブリック読み取りアクセス権を持つ Amazon S3 バケットからの 403 アクセス拒否エラーをトラブルシューティングする方法を教えてください」。

- AWS re:Post 情報センターの、「Amazon S3 の署名済み URL でリクエストを行う際の、SignatureDoesNotMatch または 403 Forbidden エラーをトラブルシューティングする方法を教えてください」。
- AWS re:Post 情報センターの、「Amazon S3 バケットで同期コマンドを実行すると、ListObjectsV2 のアクセス拒否エラーが表示されるのはなぜですか」。
- AWS re:Post 情報センターの、「Amazon S3 ウェブサイトのエンドポイントを CloudFront ディストリビューションのオリジンとして使用すると、"403 access denied" エラーが発生する理由を知りたいです」。

Amazon S3 の AWS マネージドポリシー

AWS マネージドポリシーは、AWS が作成および管理するスタンドアロンポリシーです。AWS マネージドポリシーは、多くの一般的ユースケースでアクセス許可を提供するように設計されているため、ユーザー、グループ、ロールへのアクセス許可の割り当てを開始できます。

AWS マネージドポリシーは、ご利用の特定のユースケースに対して最小特権のアクセス許可を付与しない場合があることにご注意ください。これは、すべての AWS ユーザーが使用できるようになるのを避けるためです。ユースケースに固有のカスタマー管理ポリシーを定義して、アクセス許可を絞り込むことをお勧めします。

AWS マネージドポリシーで定義されたアクセス許可は変更できません。AWS が AWS マネージドポリシーに定義されている権限を更新すると、更新はポリシーがアタッチされているすべてのプリンシパルアイデンティティ (ユーザー、グループ、ロール) に影響します。新しい AWS のサービス を起動するか、既存のサービスで新しい API オペレーションが使用可能になると、AWS が AWS マネージドポリシーを更新する可能性が最も高くなります。

詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」を参照してください。

AWS マネージドポリシー: AmazonS3FullAccess

`AmazonS3FullAccess` ポリシーを IAM アイデンティティにアタッチできます。このポリシーは、Amazon S3 への完全なアクセスを可能にする許可を付与します。

このポリシーのアクセス許可を確認するには、「AWS Management Console」の「AmazonS3FullAccess」を参照してください。

AWS マネージドポリシー: AmazonS3ReadOnlyAccess

AmazonS3ReadOnlyAccess ポリシーを IAM アイデンティティにアタッチできます。このポリシーは、Amazon S3 への読み取り専用アクセスを可能にする許可を付与します。

このポリシーのアクセス許可を確認するには、「AWS Management Console」の「AmazonS3ReadOnlyAccess」を参照してください。

AWS マネージドポリシー: AmazonS3ObjectLambdaExecutionRolePolicy

S3 Object Lambda アクセスポイントにリクエストが行われたときに S3 Object Lambda にデータを送信するために必要な許可を AWS Lambda 関数に提供します。また、Amazon CloudWatch Logs に書き込む許可を Lambda に付与します。

このポリシーのアクセス許可を確認するには、「AWS Management Console」の「AmazonS3ObjectLambdaExecutionRolePolicy」を参照してください。

AWS マネージドポリシー: S3UnlockBucketPolicy

S3 バケットへのすべてのユーザーのアクセスを拒否するようにメンバーアカウントのバケットポリシーを誤って設定した場合は、この AWS マネージドポリシー (S3UnlockBucketPolicy) を使用してバケットのロックを解除できます。Amazon S3 バケットへのすべてのプリンシパルのアクセスを拒否するように誤って設定したバケットポリシーを削除する方法の詳細については、「AWS Identity and Access Management ユーザーガイド」の「AWS Organizations メンバーアカウントで特権タスクを実行する」を参照してください。

AWS マネージドポリシーに対する Amazon S3 更新

Amazon S3 の AWS マネージドポリシーの更新に関する詳細を、このサービスがこれらの変更の追跡を開始した以降の分について表示します。

変更	説明	日付
Amazon S3 が S3UnlockBucketPolicy を追加	バケットのロックを解除して、Amazon S3 バケットへのすべてのプリンシパルのアクセスを拒否するように誤って設定したバケットポリシーを削除するために、Amazon S3 は S3UnlockBucketPoli	2024 年 11 月 1 日

変更	説明	日付
	cy という新しい AWS マネージドポリシーを追加しています。	
Amazon S3 が AmazonS3ReadOnlyAccess に記述許可を追加しました	Amazon S3 が s3:Describe* 記述許可を AmazonS3ReadOnlyAccess に追加しました。	2023 年 8 月 11 日
Amazon S3 では、S3 Object Lambda のアクセス許可を AmazonS3FullAccess および AmazonS3ReadOnlyAccess に追加しました。	Amazon S3 は、S3 Object Lambda のアクセス権限を含む AmazonS3FullAccess および AmazonS3ReadOnlyAccess のポリシーを更新しました。	2021 年 9 月 27 日
Amazon S3 が AmazonS3ObjectLambdaExecutionRolePolicy を追加	Amazon S3 は、AmazonS3ObjectLambdaExecutionRolePolicy と呼ばれる新しい AWS マネージドポリシーを追加しました。これは、Lambda 関数に S3 Object Lambda とやり取りして CloudWatch Logs に書き込むための許可を提供します。	2021 年 8 月 18 日
Amazon S3 が変更の追跡を開始	Amazon S3 が AWS マネージドポリシーの変更の追跡を開始しました。	2021 年 8 月 18 日

アクセスポイントを使用した汎用バケット内の共有データセットへのアクセスの管理

汎用バケットの Amazon S3 アクセスポイントは、S3 にデータを保存するあらゆる AWS サービスやお客様のアプリケーションのデータアクセスを簡素化します。アクセスポイントは、汎用バケッ

トにアタッチされた名前付きのネットワークエンドポイントで、S3 オブジェクトのオペレーション (GetObject や PutObject など) を実行するために使用できます。各アクセスポイントには、そのアクセスポイントを介したすべてのリクエストに S3 が適用する個別のアクセス許可とネットワークコントロールがあります。各アクセスポイントは、基になるバケットにアタッチされたバケットポリシーと連動して機能するカスタマイズされたアクセスポイントポリシーを適用します。仮想プライベートクラウド (VPC) からのリクエストのみを受け付けるようにアクセスポイントを設定することで、プライベートネットワークへの Amazon S3 データアクセスを制限できます。また、アクセスポイントごとにカスタムのブロックパブリックアクセスを設定することもできます。

> **Note**
>
> - アクセスポイントは、オブジェクトに対するオペレーションの実行にのみ使用できます。アクセスポイントを使用して、バケットの変更や削除など、他の Amazon S3 オペレーションを実行することはできません。アクセスポイントをサポートする S3 オペレーションの詳細なリストについては、「汎用バケットのアクセスポイントの互換性」を参照してください。
> - アクセスポイントは、AWS の一部のサービスと機能で動作します。たとえば、アクセスポイントを介して動作するようにクロスリージョンレプリケーションを設定することはできません。S3 アクセスポイントと互換性のある AWS のサービスの詳細なリストについては、「汎用バケットのアクセスポイントの互換性」を参照してください。

このセクションのトピックでは、汎用バケットの Amazon S3 アクセスポイントの操作方法について説明します。汎用バケットの操作の詳細については、「汎用バケットの概要」を参照してください。オブジェクトの操作方法の詳細については、Amazon S3 オブジェクトの概要 を参照してください。

トピック

- 汎用バケットのアクセスポイントの命名規則、制約と制限
- ARN、アクセスポイントエイリアス、または仮想ホスト形式の URI を使用した汎用バケットのアクセスポイントの参照
- 汎用バケットのアクセスポイントの互換性
- 汎用バケットのアクセスポイントを使用するための IAM ポリシーの設定
- 汎用バケットのアクセスポイントのモニタリングとログ記録
- 汎用バケットのアクセスポイントの作成
- 汎用バケットの Amazon S3 アクセスポイントの管理

- 汎用バケットでの Amazon S3 アクセスポイントの使用

汎用バケットのアクセスポイントの命名規則、制約と制限

汎用バケットのアクセスポイントは、データの管理を簡単にするためにバケットにアタッチされた、名前付きのネットワークエンドポイントです。アクセスポイントの作成時に、名前と作成先の AWS リージョンを選択します。以下のトピックでは、アクセスポイントの命名規則と制限および制約に関する情報を提供します。

トピック

- 汎用バケットの Amazon S3 アクセスポイントの命名規則
- 汎用バケットのアクセスポイントの命名規則、制約と制限

汎用バケットの Amazon S3 アクセスポイントの命名規則

汎用バケットのアクセスポイント作成時にバケットの名前と作成先の AWS リージョンを選択します。汎用バケットとは異なり、アクセスポイント名は AWS アカウントまたは AWS リージョン間で一意である必要はありません。同じ AWS アカウントが異なる AWS リージョンに同じ名前のアクセスポイントを作成したり、2 つの異なる AWS アカウントが同じアクセスポイント名を使用する場合があります。ただし、単一の AWS リージョン内で、AWS アカウントが同じ名前のアクセスポイントを 2 つ持つことはできません。

> **Note**
>
> アクセスポイント名を公開する場合は、アクセスポイント名に機密情報を含めないでください。アクセスポイント名は、ドメインネームシステム (DNS) と呼ばれるパブリックアクセス可能なデータベースに公開されます。

アクセスポイント名は DNS に準拠しており、次の条件を満たす必要があります。

- 単一の AWS アカウントおよび AWS リージョン内で一意である
- 数字または小文字で始める
- 3 ~ 50 文字の長さにする
- 名前をハイフン (-) で開始または終了することはできません。
- 下線 (_)、大文字、スペース、ピリオド (.) は使用しない

- サフィックス `-s3alias` で終わることはできません。このサフィックスは、アクセスポイントのエイリアス名用に予約されています。詳細については、「汎用バケットのアクセスポイントのエイリアス」を参照してください。

汎用バケットのアクセスポイントの命名規則、制約と制限

汎用バケットの Amazon S3 アクセスポイントには以下の制約と制限があります。

- 各汎用バケットのアクセスポイントは 1 つの汎用バケットにのみ関連付けられます。このバケットは、アクセスポイントの作成時に指定する必要があります。作成後のアクセスポイントを別のバケットに関連付けることはできません。ただし、アクセスポイントを削除して、別のアクセスポイントを同じ名前で作成し、新しいアクセスポイントを別のバケットに関連付けることはできます。
- アクセスポイントを作成した後、その Virtual Private Cloud (VPC) 設定を変更することはできません。
- アクセスポイントのポリシーのサイズは 20 KB に制限されています。
- AWS アカウントごと、AWS リージョンごとに最大 10,000 個のアクセスポイントを作成できます。1 つのリージョンで 1 つのアカウントに 10,000 個を超えるアクセスポイントが必要な場合は、サービスクォータの引き上げをリクエストできます。サービスクォータと引き上げリクエストの詳細については、「AWS 全般のリファレンス」の「AWS Service Quotas」を参照してください。
- アクセスポイントを S3 レプリケーションのレプリケーション先として使用することはできません。レプリケーションの詳細については、「リージョン内およびリージョン間でのオブジェクトのレプリケート」を参照してください。
- Amazon S3 コンソールの 移動オペレーションの移動元または移動先として S3 アクセスポイントのエイリアスを使用することはできません。
- アクセスポイントにアドレス指定できるのは、仮想ホスト形式の URL だけです。仮想ホスティング形式のアドレス指定の詳細については、「Amazon S3 汎用バケットへのアクセス」を参照してください。
- アクセスポイントの機能を制御する API オペレーション (`PutAccessPoint` や `GetAccessPointPolicy` など) は、クロスアカウントコールをサポートしていません。
- REST API を使用してアクセスポイントへのリクエストを行う場合は、AWS Signature Version 4 を使用する必要があります。リクエストの認証の詳細については、Amazon Simple Storage Service API リファレンスのリクエストの承認 (AWS Signature Version 4) を参照してください。

- アクセスポイントは HTTPS 経由のリクエストのみをサポートしています。Amazon S3 は、HTTP 経由で行われたすべてのリクエストに対して HTTP リダイレクトで自動的に応答し、リクエストを HTTPS にアップグレードします。
- アクセスポイントは匿名アクセスをサポートしていません。
- クロスアカウントアクセスポイントは、バケット所有者から権限が付与されるまで、データへのアクセスを許可しません。バケット所有者は常にデータを完全に管理できるため、クロスアカウントアクセスポイントからのリクエストを許可するにはバケットポリシーを更新する必要があります。バケットポリシーの例を表示するには、「汎用バケットのアクセスポイントを使用するための IAM ポリシーの設定」を参照してください。
- 1,000 個以上のアクセスポイントを所有している AWS リージョン では、Amazon S3 コンソールでは、アクセスポイントを名前で検索することはできません。
- Amazon S3 コンソールでクロスアカウントアクセスポイントを表示すると、[アクセス] 列に [不明] と表示されます。Amazon S3 コンソールは、関連するバケットとオブジェクトにパブリックアクセスが許可されているかどうかを判断できません。特定のユースケースでパブリック設定が必要でない限り、ユーザーとバケット所有者は、アクセスポイントとバケットへのすべてのパブリックアクセスをブロックすることをお勧めします。詳細については、「Amazon S3 ストレージへのパブリックアクセスのブロック」を参照してください。

ARN、アクセスポイントエイリアス、または仮想ホスト形式の URI を使用した汎用バケットのアクセスポイントの参照

汎用バケットのアクセスポイントを作成したら、これらのエンドポイントを使用してさまざまなオペレーションを実行できます。汎用バケットのアクセスポイントを参照するときは、Amazon リソースネーム (ARN)、アクセスポイントエイリアス、または仮想ホスト形式の URI を使用できます。

トピック

- 汎用バケットのアクセスポイント ARN
- 汎用バケットのアクセスポイントのエイリアス
- 仮想ホスティング形式の URI

汎用バケットのアクセスポイント ARN

アクセスポイントには Amazon リソースネーム (ARN) があります。汎用バケットのアクセスポイントの ARN は、バケットの ARN と似ていますが、明示的に型指定され、アクセスポイントの AWS リージョンとアクセスポイントの所有者の AWS アカウント ID をエンコードします。ARN の詳細

については、「AWS 全般のリファレンス」の「Amazon リソースネーム (ARN)」を参照してください。

アクセスポイント ARN は、以下の形式を使用します。

```
arn:aws:s3:region:account-id:accesspoint/resource
```

- arn:aws:s3:*us-west-2*:*123456789012*:accesspoint/*test* は、リージョン *us-west-2* でアカウント *123456789012* が所有する *test* と呼ばれるアクセスポイントを表します。
- arn:aws:s3:*us-west-2*:*123456789012*:accesspoint/* は、リージョン *us-west-2* 内のアカウント *123456789012* のすべてのアクセスポイントを表します。

アクセスポイントを介してアクセスされるオブジェクトの ARN は、以下の形式を使用します。

```
arn:aws:s3:region:account-id:accesspoint/access-point-name/object/resource
```

- arn:aws:s3:*us-west-2*:*123456789012*:accesspoint/*test*/object/*unit-01* は、リージョン *us-west-2* でアカウント *123456789012* が所有する、*test* という名前のアクセスポイントを介してアクセスされるオブジェクト *unit-01* を表します。
- arn:aws:s3:*us-west-2*:*123456789012*:accesspoint/*test*/object/* は、リージョン *us-west-2* のアカウント *123456789012* にある、*test* という名前のアクセスポイントのすべてのオブジェクトを表します。
- arn:aws:s3:*us-west-2*:*123456789012*:accesspoint/*test*/object/*unit-01*/*finance*/* は、リージョン *us-west-2* のアカウント *123456789012* にある、*test* という名前のアクセスポイントのプレフィックス *unit-01/finance/* が付いたすべてのオブジェクトを表します。

汎用バケットのアクセスポイントのエイリアス

汎用バケットのアクセスポイントを作成すると、Amazon S3 はデータアクセス用の Amazon S3 バケット名の代わりに使用できるエイリアスを自動的に生成します。このアクセスポイントエイリアスは、アクセスポイントのデータプレーンオペレーションにおいて、Amazon リソースネーム (ARN) の代わりに使用することができます。これらのオペレーションのリストについては、「汎用バケットのアクセスポイントの互換性」を参照してください。

アクセスポイントのエイリアス名は、Amazon S3 バケットと同じ名前空間内に作成されます。このエイリアス名は自動的に生成され、変更できません。アクセスポイントのエイリアス名は、有効な Amazon S3 バケット名のすべての要件を満たしており、次の部分で構成されています。

access point prefix-*metadata*-s3alias

> **Note**
>
> -s3alias サフィックスは、アクセスポイントのエイリアス名用に予約されており、バケット名やアクセスポイント名には使用できません。Amazon S3 バケット命名規則の詳細については、「汎用バケットの命名規則」を参照してください。

汎用バケットのアクセスポイントのエイリアスに関するユースケースと制限事項

汎用バケットのアクセスポイントを採用する場合、大幅なコード変更を必要とせずに、アクセスポイントのエイリアス名を使用できます。

汎用バケットのアクセスポイントを作成すると、次の例に示すように、Amazon S3 によってアクセスポイントのエイリアス名が自動的に生成されます。このコマンドを実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3control create-access-point --bucket amzn-s3-demo-bucket1 --name my-access-point
 --account-id 111122223333
{
    "AccessPointArn": "arn:aws:s3:region:111122223333:accesspoint/my-access-point",
    "Alias": "my-access-point-aqfqprnstn7aefdfbarligizwgyfouse1a-s3alias"
}
```

このアクセスポイントのエイリアス名は、あらゆるデータプレーンオペレーションにおいて、Amazon S3 のバケット名の代わりに使用することができます。これらのオペレーションのリストについては、汎用バケットのアクセスポイントの互換性 を参照してください。

次の get-object コマンドの AWS CLI 例では、バケットのアクセスポイントエイリアスを使用して、指定されたオブジェクトに関する情報を返します。このコマンドを実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3api get-object --bucket my-access-point-aqfqprnstn7aefdfbarligizwgyfouse1a-
s3alias --key dir/my_data.rtf my_data.rtf
```

```
{
    "AcceptRanges": "bytes",
    "LastModified": "2020-01-08T22:16:28+00:00",
    "ContentLength": 910,
    "ETag": "\"00751974dc146b76404bb7290f8f51bb\"",
    "VersionId": "null",
    "ContentType": "text/rtf",
    "Metadata": {}
}
```

アクセスポイントエイリアスの制限

- お客様はエイリアスを設定できません。
- アクセスポイントでは、エイリアスの削除、変更、無効化はできません。
- このアクセスポイントのエイリアス名は、一部のデータプレーンオペレーションにおいて、Amazon S3 のバケット名の代わりに使用することができます。これらのオペレーションのリストについては、汎用バケットのアクセスポイントと S3 オペレーションとの互換性 を参照してください。
- アクセスポイントのエイリアス名は Amazon S3 コントロールプレーンオペレーションに使用することはできません。Amazon S3 コントロールプレーンオペレーションの一覧は、「Amazon Simple Storage Service API リファレンス」の「Amazon S3 コントロール」を参照してください。
- Amazon S3 コンソールの 移動オペレーションの移動元または移動先として S3 アクセスポイントのエイリアスを使用することはできません。
- エイリアスはAWS Identity and Access Management (IAM) ポリシーでは使用できません。
- エイリアスは S3 サーバーアクセスログのログ記録送信先として使用することはできません。
- エイリアスは AWS CloudTrail ログのログ記録送信先として使用することはできません。
- Amazon SageMaker GroundTruth は、アクセスポイントのエイリアスをサポートしていません。

仮想ホスティング形式の URI

汎用バケットのアクセスポイントでは、仮想ホスト形式のアドレス指定のみがサポートされます。仮想ホスティング形式の URI では、アクセスポイント名、AWS アカウント、AWS リージョンは URL のドメイン名の一部です。仮想ホスティングの詳細については、「汎用バケットの仮想ホスティング」を参照してください。

アクセスポイントの仮想ホスト形式の URI は、次の形式を使用します。

```
https://access-point-name-account-id.s3-accesspoint.region.amazonaws.com
```

> **Note**
>
> - アクセスポイント名にダッシュ (-) 文字が含まれている場合は、URL にダッシュを含めて、アカウント ID の前に別のダッシュを挿入します。例えば、リージョン *us-west-2* で アカウント *123456789012* が所有する *finance-docs* という名前のアクセスポイントを使用する場合、適切な URL は `https://finance-docs-123456789012.s3-accesspoint.us-west-2.amazonaws.com` になります。
> - S3 アクセスポイントでは、HTTP 経由のアクセスはサポートされていません。アクセスポイントでは HTTPS 経由のセキュアなアクセスのみがサポートされます。

汎用バケットのアクセスポイントの互換性

汎用バケットのアクセスポイントを介して、次の Amazon S3 API のサブセットを使用してバケットにアクセスできます。以下に示すすべてのオペレーションで、アクセスポイント ARN またはアクセスポイントエイリアスのいずれかを許可できます。

アクセスポイントを使用してオブジェクトにオペレーションを行う例については、「汎用バケットでの Amazon S3 アクセスポイントの使用」を参照してください。

汎用バケットのアクセスポイントと S3 オペレーションとの互換性

S3 オペレーション

- AbortMultipartUpload
- CompleteMultipartUpload
- CopyObject (同じリージョンへのコピーのみ)
- CreateMultipartUpload
- DeleteObject
- DeleteObjects
- DeleteObjectTagging
- GetBucketAcl
- GetBucketCors

- GetBucketLocation
- GetBucketNotificationConfiguration
- GetBucketPolicy
- GetObject
- GetObjectAcl
- GetObjectAttributes
- GetObjectLegalHold
- GetObjectRetention
- GetObjectTagging
- HeadBucket
- HeadObject
- ListMultipartUploads
- ListObjects
- ListObjectsV2
- ListObjectVersions
- ListParts
- Presign
- PutObject
- PutObjectAcl
- PutObjectLegalHold
- PutObjectRetention
- PutObjectTagging
- RestoreObject
- UploadPart
- UploadPartCopy (同じリージョンへのコピーのみ)

汎用バケットのアクセスポイントを使用するための IAM ポリシーの設定

汎用バケットの Amazon S3 アクセスポイントは AWS Identity and Access Management (IAM) リソースポリシーをサポートしています。これにより、リソース、ユーザー、その他の条件別にアクセスポイントの使用を制御できます。アプリケーションやユーザーがアクセスポイントを介してオブ

ジェクトにアクセスできるようにするには、アクセスポイントと基になるバケットの両方でリクエストを許可する必要があります。

> **Important**
>
> S3 アクセスポイントをバケットに追加しても、バケット名や Amazon リソースネーム (ARN) でアクセスしたときのバケットの動作は変わりません。バケットに対する既存のすべてのオペレーションは、以前と同じように動作します。アクセスポイントポリシーに含めた制限は、そのアクセスポイントを介したリクエストにのみ適用されます。

IAM リソースポリシーを使用する際、ポリシーを保存する前に、AWS Identity and Access Management Access Analyzer からのセキュリティ警告、エラー、一般的な警告、および提案を解決してください。IAM Access Analyzer は、IAM ポリシーの文法とベストプラクティスに照らしてポリシーチェックを行います。これらのチェックにより、機能的でセキュリティのベストプラクティスに準拠したポリシーを作成するのに、役立つ結果とレコメンデーションが示されます。

IAM Access Analyzer を使用したポリシーの検証の詳細については、「IAM ユーザーガイド」の「IAM Access Analyzer のポリシーの検証」を参照してください。IAM Access Analyzer によって返される警告、エラー、および提案のリストを表示するには、「IAM Access Analyzer ポリシーチェックリファレンス」を参照してください。

汎用バケットのアクセスポイントのポリシー例

以下の例は、汎用バケットのアクセスポイントを介したリクエストを制御するための IAM ポリシーの作成方法を示しています。

> **Note**
>
> アクセスポイントポリシーで付与されるアクセス許可は、基になるバケットでも同じアクセスが許可される場合にのみ有効です。このためには以下の 2 つの方法があります。
>
> 1. (推奨)「アクセスポイントへのアクセスコントロールの委任」の説明に従って、バケットからアクセスポイントにアクセスコントロールを委任します。
> 2. アクセスポイントポリシーに含まれているものと同じアクセス許可を、基になるバケットのポリシーに追加します。例 1 のアクセスポイントポリシーの例は、必要なアクセスを許可するように基になるバケットポリシーを変更する方法を示しています。

Example 1 - アクセスポイントポリシーによる付与

以下のアクセスポイントポリシーは、アカウント *123456789012* の IAM ユーザー *Jane* に、アカウント *123456789012* のアクセスポイント *my-access-point* を介して、オブジェクト (プレフィックスが *Jane/* であるオブジェクト) を GET および PUT するアクセス許可を付与します。

```
{
    "Version":"2012-10-17",
    "Statement": [
    {
        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::123456789012:user/Jane"
        },
        "Action": ["s3:GetObject", "s3:PutObject"],
        "Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/my-access-point/
object/Jane/*"
    }]
}
```

> **Note**
>
> アクセスポイントポリシーで *Jane* に対して効果的にアクセスを許可するには、基になるバケットでも *Jane* に対して同じアクセスを許可する必要があります。「アクセスポイントへのアクセスコントロールの委任」で説明しているように、バケットからアクセスポイントにアクセスコントロールを委任できます。または、基になるバケットに以下のポリシーを追加して、Jane に必要なアクセス許可を付与できます。Resource エントリはアクセスポイントとバケットのポリシーでは異なります。
>
> ```
> {
>     "Version": "2012-10-17",
>     "Statement": [
>     {
>         "Effect": "Allow",
>         "Principal": {
>             "AWS": "arn:aws:iam::123456789012:user/Jane"
>         },
>         "Action": ["s3:GetObject", "s3:PutObject"],
>         "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/Jane/*"
>     }]
> ```

```
}
```

Example 2 - タグ条件付きのアクセスポイントポリシー

以下のアクセスポイントポリシーは、アカウント *123456789012* の IAM ユーザー *Mateo* に、アカウント *123456789012* のアクセスポイント *my-access-point* を介して、オブジェクト (タグキーが *data*、値が *finance* であるオブジェクト) を GET するアクセス許可を付与します。

```
{
    "Version":"2012-10-17",
    "Statement": [
    {
        "Effect":"Allow",
        "Principal" : {
            "AWS": "arn:aws:iam::123456789012:user/Mateo"
        },
        "Action":"s3:GetObject",
        "Resource" : "arn:aws:s3:us-west-2:123456789012:accesspoint/my-access-point/
object/*",
        "Condition" : {
            "StringEquals": {
                "s3:ExistingObjectTag/data": "finance"
            }
        }
    }]
}
```

Example 3 – バケットのリスト取得を許可するアクセスポイントポリシー

以下のアクセスポイントポリシーでは、アカウント *123456789012* の IAM ユーザー Arnav に、アカウント *123456789012* のアクセスポイント *my-access-point* の基になるバケットに含まれるオブジェクトを表示するアクセス許可を付与します。

```
{
    "Version":"2012-10-17",
    "Statement": [
    {
        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::123456789012:user/Arnav"
        },
```

```
        "Action": "s3:ListBucket",
        "Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/my-access-point"
    }]
}
```

Example 4 – サービスコントロールポリシー

次のサービスコントロールポリシーは、すべての新しいアクセスポイントを 仮想プライベートクラウド (VPC) ネットワークオリジンで作成することを要求します。このポリシーを適用すると、組織内のユーザーは、インターネットからアクセス可能なアクセスポイントを新規に作成できなくなります。

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
        "Effect": "Deny",
        "Action": "s3:CreateAccessPoint",
        "Resource": "*",
        "Condition": {
            "StringNotEquals": {
                "s3:AccessPointNetworkOrigin": "VPC"
            }
        }
    }]
}
```

Example 5 – S3 オペレーションを VPC ネットワークオリジンに制限するバケットポリシー

次のバケットポリシーは、すべての S3 オペレーションからバケット *amzn-s3-demo-bucket* へのアクセスを、VPC をネットワークオリジンとするアクセスポイントに制限します。

> **Important**
>
> この例で示しているようなステートメントを使用する前に、アクセスポイントでサポートされない機能 (クロスリージョンレプリケーションなど) が不要であることを確認してください。

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Effect": "Deny",
            "Principal": "*",
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:BypassGovernanceRetention",
                "s3:DeleteObject",
                "s3:DeleteObjectTagging",
                "s3:DeleteObjectVersion",
                "s3:DeleteObjectVersionTagging",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectLegalHold",
                "s3:GetObjectRetention",
                "s3:GetObjectTagging",
                "s3:GetObjectVersion",
                "s3:GetObjectVersionAcl",
                "s3:GetObjectVersionTagging",
                "s3:ListMultipartUploadParts",
                "s3:PutObject",
                "s3:PutObjectAcl",
                "s3:PutObjectLegalHold",
                "s3:PutObjectRetention",
                "s3:PutObjectTagging",
                "s3:PutObjectVersionAcl",
                "s3:PutObjectVersionTagging",
                "s3:RestoreObject"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "StringNotEquals": {
                    "s3:AccessPointNetworkOrigin": "VPC"
                }
            }
        }
    ]
}
```

条件キー

汎用バケットの S3 アクセスポイントには、IAM ポリシーでリソースへのアクセスを制御するために使用できる条件キーがあります。以下の条件キーは IAM ポリシーの一部にすぎません。すべての

ポリシーの例については、「汎用バケットのアクセスポイントのポリシー例」、「the section called “アクセスポイントへのアクセスコントロールの委任”」および「the section called “クロスアカウントアクセスポイントへのアクセス許可の付与”」を参照してください。

s3:DataAccessPointArn

この例は、アクセスポイントの ARN の照合に使用できる文字列です。次の例では、リージョン *us-west-2* の AWS アカウント *123456789012* のすべてのアクセスポイントを照合します。

```
"Condition" : {
    "StringLike": {
        "s3:DataAccessPointArn": "arn:aws:s3:us-west-2:123456789012:accesspoint/*"
    }
}
```

s3:DataAccessPointAccount

この例は、アクセスポイントの所有者のアカウント ID を照合するために使用できる文字列演算子です。次の例では、AWS アカウント *123456789012* が所有するすべてのアクセスポイントを照合します。

```
"Condition" : {
    "StringEquals": {
        "s3:DataAccessPointAccount": "123456789012"
    }
}
```

s3:AccessPointNetworkOrigin

この例は、ネットワークオリジン (Internet または VPC) の照合に使用できる文字列演算子です。次の例では、VPC オリジンを持つアクセスポイントのみを照合します。

```
"Condition" : {
    "StringEquals": {
        "s3:AccessPointNetworkOrigin": "VPC"
    }
}
```

Amazon S3 での条件キーの使用についての詳細は、「サービス認可リファレンス」の「Actions, resources, and condition keys for Amazon S3」を参照してください。

S3 リソースタイプ別の S3 API オペレーションへのアクセス許可の詳細については、「Amazon S3 API オペレーションに必要なアクセス許可」を参照してください。

アクセスポイントへのアクセスコントロールの委任

バケットのアクセスコントロールをバケットのアクセスポイントに委任できます。以下のバケットポリシーの例では、バケット所有者のアカウントが所有するすべてのアクセスポイントへのフルアクセスを許可しています。したがって、このバケットへのすべてのアクセスは、そのアクセスポイントにアタッチされているポリシーによってコントロールされます。バケットへの直接アクセスを必要としないすべてのユースケースでは、この方法でバケットを設定することをお勧めします。

Example 6 - アクセスコントロールをアクセスポイントに委任するバケットポリシー

```
{
    "Version": "2012-10-17",
    "Statement" : [
    {
        "Effect": "Allow",
        "Principal" : { "AWS": "*" },
        "Action" : "*",
        "Resource" : [ "Bucket ARN", "Bucket ARN/*"],
        "Condition": {
            "StringEquals" : { "s3:DataAccessPointAccount" : "Bucket owner's account
 ID" }
        }
    }]
}
```

クロスアカウントアクセスポイントへのアクセス許可の付与

別のアカウントが所有するバケットへのアクセスポイントを作成するには、まずバケット名とアカウント所有者 ID を指定してアクセスポイントを作成する必要があります。次に、バケット所有者は、アクセスポイントからのリクエストを許可するようにバケットポリシーを更新する必要があります。アクセスポイントの作成は、アクセスポイントがバケットの内容へのアクセスを提供しないという点で DNS CNAME の作成と似ています。すべてのバケットアクセスはバケットポリシーによって制御されます。次のバケットポリシーの例では、信頼できる AWS アカウント が所有するアクセスポイントからのバケットで、GET および LIST リクエストを許可します。

Bucket ARN は、バケットの ARN に置き換えます。

Example 7 — 別の AWS アカウント にアクセス許可を委任するバケットポリシー

```
{
    "Version": "2012-10-17",
    "Statement" : [
    {
        "Effect": "Allow",
        "Principal" : { "AWS": "*" },
        "Action" : ["s3:GetObject","s3:ListBucket"],
        "Resource" : [ "Bucket ARN", "Bucket ARN/*"],
        "Condition": {
            "StringEquals" : { "s3:DataAccessPointAccount" : "Access point owner's
 account ID" }
        }
    }]
}
```

汎用バケットのアクセスポイントのモニタリングとログ記録

Amazon S3 は、汎用バケットのアクセスポイントを介して行われたリクエストと、アクセスポイントを管理する API オペレーションに対するリクエスト (CreateAccessPoint や GetAccessPointPolicy など) をログに記録します。使用パターンをモニタリングおよび管理するために、アクセスポイントの Amazon CloudWatch Logs リクエストメトリクスを設定することもできます。

トピック

- CloudWatch リクエストメトリクス
- リクエストログ

CloudWatch リクエストメトリクス

アクセスポイントを使用しているアプリケーションのパフォーマンスを理解して向上させるために、Amazon S3 リクエストメトリクスで CloudWatch を使用することができます。リクエストメトリクスは、 Amazon S3 リクエストをモニタリングし、オペレーションの問題をすばやく特定して対応するのに役立ちます。

デフォルトでは、 リクエストメトリクスはバケットレベルで利用可能です。ただし、共有プレフィクス、オブジェクトタグ、またはアクセスポイントを使用して、リクエストメトリクスのフィルタを定義できます。アクセスポイントフィルタを作成すると、リクエストメトリクスの設定に、指定し

たアクセスポイントへのリクエストが含まれます。メトリクスの受信、アラームの設定、およびダッシュボードへのアクセスにより、このアクセスポイントで実行されたオペレーションをリアルタイムで表示できます。

コンソールで設定するか、Amazon S3 API を使用して、リクエストメトリクスをオプトインする必要があります。リクエストメトリクスは、処理のレイテンシーの後に 1 分間隔で使用できます。リクエストメトリクスは、CloudWatch カスタムメトリクスと同じ料金レートで請求されます。詳細については、「Amazon CloudWatch の料金」を参照してください。

アクセスポイントでフィルタリングするリクエストメトリクスの設定を作成する方法は、プレフィックス、オブジェクトタグ、またはアクセスポイントでのメトリクス設定の作成 を参照してください。

リクエストログ

サーバーアクセスロギングおよび AWS CloudTrail を使用して、アクセスポイントを介して行われたリクエストと、アクセスポイントを管理する API に対するリクエスト (`CreateAccessPoint` や `GetAccessPointPolicy`, など) を ログに記録します。

アクセスポイントを介して行われたリクエストの CloudTrail ログエントリには、ログの `resources` セクションにアクセスポイント ARN が含まれます。

例えば、次の設定があるとします。

- *`my-image.jpg`* という名前のオブジェクト を含むリージョン *`us-west-2`* の *`amzn-s3-demo-bucket1`* という名前のバケット
- *`amzn-s3-demo-bucket1`* に関連付けられた *`my-bucket-ap`* という名前のアクセスポイント
- *`123456789012`* の AWS アカウント ID

以下の例は、`resources`前述の設定の CloudTrail ログエントリの セクションを示しています。

```
"resources": [
        {"type": "AWS::S3::Object",
            "ARN": "arn:aws:s3:::amzn-s3-demo-bucket1/my-image.jpg"
        },
        {"accountId": "123456789012",
            "type": "AWS::S3::Bucket",
            "ARN": "arn:aws:s3:::amzn-s3-demo-bucket1"
        },
        {"accountId": "123456789012",
```

```
            "type": "AWS::S3::AccessPoint",
            "ARN": "arn:aws:s3:us-west-2:123456789012:accesspoint/my-bucket-ap"
        }
    ]
```

S3 サーバーのアクセスログの詳細については、「サーバーアクセスログによるリクエストのログ記録」を参照してください。AWS CloudTrail の詳細については、AWS CloudTrail ユーザーガイドの AWS CloudTrail とはを参照してください。

汎用バケットのアクセスポイントの作成

汎用バケットの S3 アクセスポイントは、AWS Management Console、AWS Command Line Interface (AWS CLI)、AWS SDK、または Amazon S3 REST API を使用して作成できます。

デフォルトでは、リージョンごとに AWS アカウントあたり最大 10,000 個の汎用バケットのアクセスポイントを作成できます。1 つのリージョンで 1 つのアカウントに 10,000 個を超えるアクセスポイントが必要な場合は、サービスクォータの引き上げをリクエストできます。サービスクォータと引き上げリクエストの詳細については、「AWS 全般のリファレンス」の「AWS Service Quotas」を参照してください。

トピック

- 汎用バケットのアクセスポイントの作成
- 仮想プライベートクラウドに制限された汎用バケットのアクセスポイントの作成
- 汎用バケットのアクセスポイントへのパブリックアクセスの管理

汎用バケットのアクセスポイントの作成

アクセスポイントは、1 つの Amazon S3 汎用バケットにのみ関連付けられます。AWS アカウントでバケットを使用する場合は、まずバケットを作成する必要があります。バケットの作成の詳細については、「Amazon S3 汎用バケットの作成、設定、操作」を参照してください。

バケット名とバケット所有者のアカウント ID がわかっていれば、別の AWS アカウント のバケットに関連するクロスアカウントアクセスポイントを作成することもできます。ただし、クロスアカウントアクセスポイントを作成しても、バケット所有者からアクセス権が付与されるまで、バケット内のデータへのアクセスは許可されません。バケット所有者は、バケットポリシーを通じて、アクセスポイント所有者のアカウント (お客様のアカウント) にバケットへのアクセス権を付与する必要があります。詳細については、「クロスアカウントアクセスポイントへのアクセス許可の付与」を参照してください。

S3 コンソールの使用

アクセスポイントを作成するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ページ上部にあるナビゲーションバーで、現在表示されている AWS リージョン の名前をクリックします。次に、アクセスポイントを作成するリージョンを選択します。アクセスポイントは、関連付けられたバケットと同じリージョンに作成する必要があります。
3. 左のナビゲーションペインで、[アクセスポイント] を選択します。
4. [アクセスポイント] ページで、[アクセスポイントの作成] を選択します。
5. [アクセスポイント名] フィールドに、アクセスポイントの名前を入力します。アクセスポイントの名前付けの詳細については、「汎用バケットの Amazon S3 アクセスポイントの命名規則」を参照してください。
6. [バケット名] には、アクセスポイントで使用する S3 バケットを指定します。

   アカウントのバケットを使用するには、[このアカウント内のバケットを選択] を選択し、バケット名を入力または参照します。

   別の AWS アカウント でバケットを使用するには、[別のアカウントのバケットを指定] を選択し、バケットの AWS アカウント ID と名前を入力します。

   > **Note**
   >
   > 別の AWS アカウント でバケットを使用している場合は、バケット所有者がアクセスポイントからのリクエストを許可するようにバケットポリシーを更新する必要があります。バケットポリシーの例については、「クロスアカウントアクセスポイントへのアクセス許可の付与」を参照してください。

7. [インターネット] または [仮想プライベートクラウド (VPC)] のいずれかの [ネットワークオリジン] を選択します。[仮想プライベートクラウド (VPC)] を選択した場合は、アクセスポイントで使用する [VPC ID] を入力します。

   アクセスポイントのネットワークオリジンの詳細については、「仮想プライベートクラウドに制限された汎用バケットのアクセスポイントの作成」を参照してください。

8. [Block Public Access settings for this Access Point] (このアクセスポイントのパブリックアクセス設定をブロック) で、アクセスポイントに適用するパブリックアクセスブロック設定を選択し

ます。デフォルトでは、新しいアクセスポイントに対してすべてのブロックパブリックアクセス設定が有効になります。これらの設定を特に無効にする必要がある場合を除いて、すべての設定を有効にしておくことをお勧めします。

> **Note**
>
> アクセスポイントの作成後は、アクセスポイントパブリックアクセスのブロック設定を変更できません。

アクセスポイントで Amazon S3 パブリックアクセスブロックを使用することについて詳細は、「汎用バケットのアクセスポイントへのパブリックアクセスの管理」を参照してください。

9. (オプション) [Access Point policy - optional] (アクセスポイントポリシー - オプション) で、アクセスポイントポリシーを指定します。ポリシーを保存する前に、セキュリティ警告、エラー、一般的な警告、および提案を解決してください。アクセスポイントポリシーの指定の詳細については、「汎用バケットのアクセスポイントのポリシー例」を参照してください。
10. [アクセスポイントの作成] を選択します。

AWS CLI を使用する場合

以下の例では、アカウント *111122223333* のバケット *amzn-s3-demo-bucket* に「*example-ap*」という名前のアクセスポイントを作成します。アクセスポイントを作成するには、以下を指定するリクエストを Amazon S3 に送信します。

- アクセスポイント名。命名規則の詳細については、「the section called “汎用バケットの Amazon S3 アクセスポイントの命名規則”」を参照してください。
- アクセスポイントを関連付けるバケットの名前。
- アクセスポイントを所有している AWS アカウントのアカウント ID。

```
aws s3control create-access-point --name example-ap --account-id 111122223333 --
bucket amzn-s3-demo-bucket
```

別の AWS アカウント でバケットを使用してアクセスポイントを作成する場合は、`--bucket-account-id` パラメータを含めてください。次のコマンド例では、AWS アカウント *444455556666* にあるバケット *amzn-s3-demo-bucket2* を使用してAWS アカウント *111122223333* にアクセスポイントを作成します。

```
aws s3control create-access-point --name example-ap --account-id 111122223333 --
bucket amzn-s3-demo-bucket --bucket-account-id 444455556666
```

REST API の使用

REST API を使用してアクセスポイントを作成できます。詳細については、「Amazon Simple Storage Service API リファレンス」の「CreateAccessPoint」を参照してください。

仮想プライベートクラウドに制限された汎用バケットのアクセスポイントの作成

汎用バケットのアクセスポイントを作成するときに、そのアクセスポイントをインターネットからアクセス可能にするか、特定の仮想プライベートクラウド (VPC) からのリクエストにのみアクセスを制限するかを指定できます。インターネットからアクセス可能なアクセスポイントは、`Internet` をネットワークオリジンとすると言います。この種のアクセスポイントは、インターネット上のどこからでも利用できます。ただし、このアクセスポイントや、基となるバケット、関連リソース (リクエストされたオブジェクトなど) に関する他のすべてのアクセス制限に従うことを条件とします。指定された VPC からのみアクセス可能なアクセスポイントは `VPC` をネットワークオリジンとします。Amazon S3 は、アクセスポイントに対するその VPC からのリクエストを除いて、他のすべてのリクエストを拒否します。

> **Important**
>
> アクセスポイントのネットワークオリジンは、アクセスポイントの作成時にのみ指定できます。アクセスポイントの作成後は、そのネットワークオリジンを変更できません。

アクセスポイントを VPC からのアクセスにのみ制限するには、アクセスポイントを作成するリクエストに `VpcConfiguration` パラメータを含めます。`VpcConfiguration` パラメータには、アクセスポイントを使用できるようにする VPC ID を指定します。アクセスポイントを介してリクエストが行われた場合、リクエストは VPC から発信されている必要があり、そうでない場合、Amazon S3 はそれを拒否します。

アクセスポイントのネットワークオリジンを取得するには、AWS CLI、AWS SDK、または REST API を使用します。アクセスポイントに VPC 設定が指定されている場合、そのネットワークオリジンは `VPC` です。それ以外の場合、アクセスポイントのネットワークオリジンは `Internet` です。

Example

例: VPC アクセスに制限されたアクセスポイントを作成する

次の例では、アカウント 123456789012 のバケット *amzn-s3-demo-bucket* に対して vpc-1a2b3c VPC からのアクセスのみを許可する example-vpc-ap という名前のアクセスポイントを作成します。次に、新しいアクセスポイントのネットワークオリジンが VPC であることを確認します。

AWS CLI

```
aws s3control create-access-point --name example-vpc-ap --account-id 123456789012 --
bucket amzn-s3-demo-bucket --vpc-configuration VpcId=vpc-1a2b3c
```

```
aws s3control get-access-point --name example-vpc-ap --account-id 123456789012

{
    "Name": "example-vpc-ap",
    "Bucket": "amzn-s3-demo-bucket",
    "NetworkOrigin": "VPC",
    "VpcConfiguration": {
        "VpcId": "vpc-1a2b3c"
    },
    "PublicAccessBlockConfiguration": {
        "BlockPublicAcls": true,
        "IgnorePublicAcls": true,
        "BlockPublicPolicy": true,
        "RestrictPublicBuckets": true
    },
    "CreationDate": "2019-11-27T00:00:00Z"
}
```

VPC でアクセスポイントを使用するには、VPC エンドポイントのアクセスポリシーを変更する必要があります。VPC エンドポイントは、VPC から Amazon S3 へのトラフィックフローを許可します。これらのエンドポイントには、VPC 内のリソースに対して Amazon S3 とのやり取りを許可する方法を制御するアクセスコントロールポリシーがあります。アクセスポイントを経由した VPC から Amazon S3 へのリクエストが成功するのは、VPC エンドポイントポリシーがアクセスポイントおよび基となるバケットの両方へのアクセスを許可した場合のみです。

> **Note**
>
> VPC 内でのみリソースにアクセスできるようにするには、VPC エンドポイントエンドポイントに対してプライベートホストゾーンを必ず作成してください。プライベートホストゾー

ンを使うには、VPC 設定を変更して、VPC のネットワーク属性 enableDnsHostnames と enableDnsSupport を true に設定してください。

次のポリシーステートメントの例では、awsexamplebucket1 という名前のバケットと example-vpc-ap という名前のアクセスポイントに対する GetObject の呼び出しを許可するように VPC エンドポイントを設定します。

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
        "Principal": "*",
        "Action": [
            "s3:GetObject"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:::awsexamplebucket1/*",
            "arn:aws:s3:us-west-2:123456789012:accesspoint/example-vpc-ap/object/*"
        ]
    }]
}
```

Note

この例の "Resource" 宣言では、Amazon リソースネーム (ARN) を使用してアクセスポイントを指定します。アクセスポイントの ARN の詳細については、「汎用バケットでの Amazon S3 アクセスポイントの使用」を参照してください。

VPC エンドポイントポリシーの詳細については、VPC ユーザーガイドの「Amazon S3 のエンドポイントポリシーの使用」を参照してください。

VPC エンドポイントを使用してアクセスポイントを作成するチュートリアルについては、「Managing Amazon S3 access with VPC endpoints and access points」を参照してください。

汎用バケットのアクセスポイントへのパブリックアクセスの管理

汎用バケットの Amazon S3 アクセスポイントは、アクセスポイントごとに独立したブロックパブリックアクセス設定をサポートしています。アクセスポイントを作成するときに、そのアクセスポイントに適用するパブリックアクセスブロック設定を指定できます。アクセスポイントを経由するすべてのリクエストについて、Amazon S3 は、そのアクセスポイント、基となるバケット、およびバケット所有者のアカウントに関するパブリックアクセスブロック設定を評価します。これらの設定のいずれかで、リクエストをブロックする必要があることが示されると、Amazon S3 はリクエストを拒否します。

S3 のブロックパブリックアクセス機能の詳細については、「Amazon S3 ストレージへのパブリックアクセスのブロック」を参照してください。

> **Important**
>
> - デフォルトでは、アクセスポイントに対してすべてのブロックパブリックアクセス設定が有効になります。アクセスポイントに適用したくない設定がある場合は、明示的に無効にする必要があります。
> - Amazon S3 は、現在、アクセスポイントの作成後におけるアクセスポイントのブロックパブリックアクセス設定の変更をサポートしていません。

Example

例: カスタムのブロックパブリックアクセス設定を使用してアクセスポイントを作成する

この例では、デフォルトではないブロックパブリックアクセス設定を使用して、アカウント 123456789012 のバケット *amzn-s3-demo-bucket* に対して example-ap という名前のアクセスポイントを作成します。次に、新しいアクセスポイントの設定を取得して、ブロックパブリックアクセス設定を確認します。

AWS CLI

```
aws s3control create-access-point --name example-ap --account-id
 123456789012 --bucket amzn-s3-demo-bucket--public-access-block-configuration
 BlockPublicAcls=false,IgnorePublicAcls=false,BlockPublicPolicy=true,RestrictPublicBuckets=t
```

```
aws s3control get-access-point --name example-ap --account-id 123456789012
```

```
{
    "Name": "example-ap",
    "Bucket": "amzn-s3-demo-bucket",
    "NetworkOrigin": "Internet",
    "PublicAccessBlockConfiguration": {
        "BlockPublicAcls": false,
        "IgnorePublicAcls": false,
        "BlockPublicPolicy": true,
        "RestrictPublicBuckets": true
    },
    "CreationDate": "2019-11-27T00:00:00Z"
}
```

汎用バケットの Amazon S3 アクセスポイントの管理

このセクションでは、AWS Management Console、AWS Command Line Interface、または REST API を使用して汎用バケットの Amazon S3 アクセスポイントを管理する方法について説明します。

> **Note**
>
> - 汎用バケットのアクセスポイントは、オブジェクトに対するオペレーションの実行にのみ使用できます。アクセスポイントを使用して、バケットの変更や削除など、他の Amazon S3 オペレーションを実行することはできません。アクセスポイントをサポートする S3 オペレーションの詳細なリストについては、「汎用バケットのアクセスポイントの互換性」を参照してください。
> - 汎用バケットのアクセスポイントは、AWS の一部のサービスと機能で動作します。たとえば、アクセスポイントを介して動作するようにクロスリージョンレプリケーションを設定することはできません。S3 アクセスポイントと互換性のある AWS のサービスの詳細なリストについては、「汎用バケットのアクセスポイントの互換性」を参照してください。

トピック

- 汎用バケットのアクセスポイントを一覧表示する
- 汎用バケットのアクセスポイントの詳細を表示する
- 汎用バケットのアクセスポイントを削除する

汎用バケットのアクセスポイントを一覧表示する

このセクションでは、AWS Management Console、AWS Command Line Interface、または REST API を使用して汎用バケットのアクセスポイントを一覧表示する方法について説明します。

S3 コンソールの使用

AWS アカウント内のすべてのアクセスポイントを一覧表示するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ページ上部にあるナビゲーションバーで、現在表示されている AWS リージョン の名前をクリックします。次に、アクセスポイントをリスト表示するリージョンを選択します。
3. コンソールの左側のナビゲーションペインで、[アクセスポイント] を選択します。
4. (オプション) アクセスポイントを名前で検索します。選択した AWS リージョンのアクセスポイントのみがここに表示されます。
5. 管理または使用するアクセスポイントの名前を選択します。

AWS CLI を使用する場合

次の `list-access-points` コマンド例は、AWS CLI を使用してアクセスポイントを一覧表示する方法を示しています。

次のコマンドは、AWS アカウント *111122223333* のアクセスポイントを一覧表示します。

```
aws s3control list-access-points --account-id 111122223333
```

次のコマンドは、バケット *amzn-s3-demo-bucket* にアタッチされている AWS アカウント *111122223333* のアクセスポイントを一覧表示します。

```
aws s3control list-access-points --account-id 111122223333 --bucket amzn-s3-demo-bucket
```

詳細と例については、「AWS CLI コマンドリファレンス」の「list-access-points」を参照してください。

REST API の使用

REST API を使用してアクセスポイントを一覧表示できます。詳細については、「Amazon Simple Storage Service API リファレンス」の「ListAccessPoints」を参照してください。

汎用バケットのアクセスポイントの詳細を表示する

このセクションでは、AWS Management Console、AWS Command Line Interface、または REST API を使用して汎用バケットのアクセスポイントの詳細を表示する方法について説明します。

S3 コンソールの使用

AWS アカウント内のアクセスポイントの詳細を表示するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ページ上部にあるナビゲーションバーで、現在表示されている AWS リージョン の名前をクリックします。次に、アクセスポイントをリスト表示するリージョンを選択します。
3. コンソールの左側のナビゲーションペインで、[アクセスポイント] を選択します。
4. (オプション) アクセスポイントを名前で検索します。選択した AWS リージョンのアクセスポイントのみがここに表示されます。
5. 管理または使用するアクセスポイントの名前を選択します。
6. [プロパティ] タブを選択すると、選択したアクセスポイントのアクセスポイントバケット、アカウント ID、AWS リージョン、作成日、ネットワークオリジン、S3 URI、ARN、アクセスポイントエイリアスが表示されます。
7. [アクセス許可] タブを選択すると、選択したアクセスポイントの [ブロックパブリックアクセス] 設定とアクセスポイントポリシーが表示されます。

> **Note**
>
> アクセスポイントの作成後は、アクセスポイントの [パブリックアクセスブロック] 設定を変更することはできません。

AWS CLI を使用する場合

次の `get-access-point` コマンド例は、AWS CLI を使用してアクセスポイントの詳細を表示する方法を示しています。

次のコマンドは、AWS アカウント *111122223333* のアクセスポイント *my-access-point* の詳細を一覧表示します。

```
aws s3control get-access-point --name my-access-point --account-id 111122223333
```

出力例:

```
{
    "Name": "my-access-point",
    "Bucket": "amzn-s3-demo-bucket",
    "NetworkOrigin": "Internet",
    "PublicAccessBlockConfiguration": {
        "BlockPublicAcls": true,
        "IgnorePublicAcls": true,
        "BlockPublicPolicy": true,
        "RestrictPublicBuckets": true
    },
    "CreationDate": "2016-08-29T22:57:52Z",
    "Alias": "my-access-point-u1ny6bhm7moymqx8cuon8o1g4mwikuse2a-s3alias",
    "AccessPointArn": "arn:aws:s3:AWS #####:111122223333:accesspoint/my-access-point",
    "Endpoints": {
        "ipv4": "s3-accesspoint.AWS #####.amazonaws.com",
        "fips": "s3-accesspoint-fips.AWS #####.amazonaws.com",
        "fips_dualstack": "s3-accesspoint-fips.dualstack.AWS #####.amazonaws.com",
        "dualstack": "s3-accesspoint.dualstack.AWS #####.amazonaws.com"
    },
    "BucketAccountId": "111122223333"
}
```

詳細と例については、「AWS CLI コマンドリファレンス」の「get-access-point」を参照してください。

REST API の使用

REST API を使用して、アクセスポイントの詳細を表示できます。詳細については、「Amazon Simple Storage Service API リファレンス」の「GetAccessPoint」を参照してください。

汎用バケットのアクセスポイントを削除する

このセクションでは、AWS Management Console、AWS Command Line Interface、または REST API を使用して汎用バケットのアクセスポイントを削除する方法について説明します。

S3 コンソールの使用

AWS アカウント内のアクセスポイントを削除するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ページ上部にあるナビゲーションバーで、現在表示されている AWS リージョン の名前をクリックします。次に、アクセスポイントをリスト表示するリージョンを選択します。
3. コンソールの左側のナビゲーションペインで、[アクセスポイント] を選択します。
4. (オプション) アクセスポイントを名前で検索します。選択した AWS リージョンのアクセスポイントのみがここに表示されます。
5. 管理または使用するアクセスポイントの名前を選択します。
6. [アクセスポイント] ページから、[削除] を選択して、選択したアクセスポイントを削除します。
7. 削除を確認するには、アクセスポイントの名前を入力し、[削除] を選択します。

AWS CLI を使用する場合

次の `delete-access-point` コマンド例は、AWS CLI を使用してアクセスポイントを削除する方法を示しています。

次のコマンドは、AWS アカウント *111122223333* のアクセスポイント *my-access-point* を削除します。

```
aws s3control delete-access-point --name my-access-point --account-id 111122223333
```

詳細と例については、「AWS CLI コマンドリファレンス」の「delete-access-point」を参照してください。

REST API の使用

REST API を使用して、アクセスポイントの詳細を表示できます。詳細については、「Amazon Simple Storage Service API リファレンス」の「DeleteAccessPoint」を参照してください。

汎用バケットでの Amazon S3 アクセスポイントの使用

以下の例は、Amazon S3 の互換性のあるオペレーションで汎用バケットのアクセスポイントを使用する方法を示しています。

> **Note**
>
> S3 は、すべてのアクセスポイントに対してアクセスポイントエイリアスを自動的に生成します。これらのエイリアスは、バケット名を使用してオブジェクトレベルのオペレーションを実行する任意の場所で使用できます。詳細については、「汎用バケットのアクセスポイントのエイリアス」を参照してください。

汎用バケットのアクセスポイントは、オブジェクトに対するオペレーションの実行にのみ使用できます。アクセスポイントを使用して、バケットの変更や削除など、他の Amazon S3 オペレーションを実行することはできません。アクセスポイントをサポートする S3 オペレーションの詳細なリストについては、「汎用バケットのアクセスポイントの互換性」を参照してください。

トピック

- 汎用バケットのアクセスポイントを介してオブジェクトを一覧表示する
- 汎用バケットのアクセスポイントを介してオブジェクトをダウンロードする
- 汎用バケットのアクセスポイントを介してアクセスコントロールリスト (ACL) を設定する
- 汎用バケットのアクセスポイントを介してオブジェクトをアップロードする
- 汎用バケットのアクセスポイントを介してタグセットを追加する
- 汎用バケットのアクセスポイントを介してオブジェクトを削除する

汎用バケットのアクセスポイントを介してオブジェクトを一覧表示する

このセクションでは、AWS Management Console、AWS Command Line Interface、または REST API を使用して汎用バケットのアクセスポイントを介してオブジェクトを一覧表示する方法について説明します。

S3 コンソールの使用

AWS アカウントのアクセスポイント経由でオブジェクトを一覧表示するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ページ上部にあるナビゲーションバーで、現在表示されている AWS リージョン の名前をクリックします。次に、アクセスポイントをリスト表示するリージョンを選択します。
3. コンソールの左側のナビゲーションペインで、[アクセスポイント] を選択します。

4. (オプション) アクセスポイントを名前で検索します。選択した AWS リージョンのアクセスポイントのみがここに表示されます。
5. 管理または使用するアクセスポイントの名前を選択します。
6. [オブジェクト] タブで、アクセスポイント経由でアクセスするオブジェクトの名前を表示できます。アクセスポイントを使用する際は、アクセスポイントのアクセス許可で許可されているオブジェクト操作のみを実行できます。

> **Note**
>
> - コンソールビューには、バケット内のすべてのオブジェクトが常に表示されます。この手順で説明しているようにアクセスポイントを使用すると、これらのオブジェクトに実行できるオペレーションは制限されますが、オブジェクトがバケット内に存在するかどうかの確認は制限されません。
> - AWS Management Consoleでは、仮想プライベートクラウド (VPC) アクセスポイントを使用したバケットリソースへのアクセスはサポートされていません。VPC アクセスポイントからバケットのリソースにアクセスするには、AWS CLI、AWS SDK、または Amazon S3 REST API を使用します。

AWS CLI を使用する場合

次の `list-objects-v2` コマンド例は、AWS CLI を使用してアクセスポイント経由でオブジェクトを一覧表示する方法を示しています。

次のコマンドは、アクセスポイント *my-access-point* を使用して AWS アカウント *111122223333* のオブジェクトを一覧表示します。

```
aws s3api list-objects-v2 --bucket arn:aws:s3:AWS #####:111122223333:accesspoint/my-access-point
```

> **Note**
>
> S3 は、すべてのアクセスポイントに対してアクセスポイントエイリアスを自動的に生成します。これらのエイリアスは、バケット名を使用してオブジェクトレベルのオペレーションを実行する任意の場所で使用できます。詳細については、「汎用バケットのアクセスポイントのエイリアス」を参照してください。

詳細と例については、「AWS CLI コマンドリファレンス」の「list-access-points」を参照してください。

REST API の使用

REST API を使用してアクセスポイントを一覧表示できます。詳細については、「Amazon Simple Storage Service API リファレンス」の「ListObjectsV2」を参照してください。

汎用バケットのアクセスポイントを介してオブジェクトをダウンロードする

このセクションでは、AWS Management Console、AWS Command Line Interface、または REST API を使用して汎用バケットのアクセスポイントを介してオブジェクトをダウンロードする方法について説明します。

S3 コンソールの使用

AWS アカウント内のアクセスポイント経由でオブジェクトをダウンロードするには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ページ上部にあるナビゲーションバーで、現在表示されている AWS リージョン の名前をクリックします。次に、アクセスポイントをリスト表示するリージョンを選択します。
3. コンソールの左側のナビゲーションペインで、[アクセスポイント] を選択します。
4. (オプション) アクセスポイントを名前で検索します。選択した AWS リージョンのアクセスポイントのみがここに表示されます。
5. 管理または使用するアクセスポイントの名前を選択します。
6. [オブジェクト] タブで、ダウンロードするオブジェクトの名前を選択します。
7. [ダウンロード] を選択します。

AWS CLI を使用する場合

次の `get-object` コマンド例は、AWS CLI を使用してアクセスポイント経由でオブジェクトをダウンロードする方法を示しています。

次のコマンドは、アクセスポイント *`my-access-point`* を使用して AWS アカウント *`111122223333`* のオブジェクト `puppy.jpg` をダウンロードします。*`my_downloaded_image.jpg`* など、ダウンロードしたオブジェクトのファイル名である `outfile` を含める必要があります。

```
aws s3api get-object --bucket arn:aws:s3:AWS #####:111122223333:accesspoint/my-access-point --key puppy.jpg my_downloaded_image.jpg
```

> **Note**
>
> S3 は、すべてのアクセスポイントに対してアクセスポイントエイリアスを自動的に生成します。これらのエイリアスは、バケット名を使用してオブジェクトレベルのオペレーションを実行する任意の場所で使用できます。詳細については、「汎用バケットのアクセスポイントのエイリアス」を参照してください。

詳細と例については、「AWS CLI コマンドリファレンス」の「get-object」を参照してください。

REST API の使用

REST API を使用して、アクセスポイントを介してオブジェクトをダウンロードできます。詳細については、「Amazon Simple Storage Service API リファレンス」の「GetObject」を参照してください。

AWS SDK の使用

AWS SDK for Python を使用して、アクセスポイントを介してオブジェクトをダウンロードできます。

Python

次の例では、*my-access-point* という名前のアクセスポイントを使用して、*hello.txt* という名前のファイルが AWS アカウント *111122223333* 用にダウンロードされます。

```
import boto3
s3 = boto3.client('s3')
s3.download_file('arn:aws:s3:us-east-1:111122223333:accesspoint/my-access-point',
 'hello.txt', '/tmp/hello.txt')
```

汎用バケットのアクセスポイントを介してアクセスコントロールリスト (ACL) を設定する

このセクションでは、AWS Management Console、AWS Command Line Interface、または REST API を使用して汎用バケットのアクセスポイント経由で ACL を設定する方法について説明します。ACL の詳細については、「アクセスコントロールリスト (ACL) の概要」を参照してください。

S3 コンソールの使用

AWS アカウント内のアクセスポイント経由で ACL を設定するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ページ上部にあるナビゲーションバーで、現在表示されている AWS リージョン の名前をクリックします。次に、アクセスポイントをリスト表示するリージョンを選択します。
3. コンソールの左側のナビゲーションペインで、[アクセスポイント] を選択します。
4. (オプション) アクセスポイントを名前で検索します。選択した AWS リージョンのアクセスポイントのみがここに表示されます。
5. 管理または使用するアクセスポイントの名前を選択します。
6. [オブジェクト] タブで、ACL を設定するオブジェクトの名前を選択します。
7. [アクセス許可] タブで、[編集] を選択してオブジェクト ACL を設定します。

> **Note**
>
> Amazon S3 は、現在、アクセスポイントの作成後におけるアクセスポイントのブロックパブリックアクセス設定の変更をサポートしていません。

AWS CLI を使用する場合

次の `put-object-acl` コマンド例は、AWS CLI を使用して、ACL を使ってアクセスポイント経由でアクセス許可を設定する方法を示しています。

次のコマンドは、AWS アカウント *111122223333* が所有するアクセスポイント経由で既存のオブジェクト `puppy.jpg` に ACL を適用します。

```
aws s3api put-object-acl --bucket arn:aws:s3:AWS #####:111122223333:accesspoint/my-access-point --key puppy.jpg --acl private
```

> **Note**
>
> S3 は、すべてのアクセスポイントに対してアクセスポイントエイリアスを自動的に生成します。これらのエイリアスは、バケット名を使用してオブジェクトレベルのオペレーションを実行する任意の場所で使用できます。詳細については、「汎用バケットのアクセスポイントのエイリアス」を参照してください。

詳細と例については、「AWS CLI コマンドリファレンス」の「put-object-acl」を参照してください。

REST API の使用

REST API を使用して、ACL を使ってアクセスポイント経由でアクセス許可を設定できます。詳細については、「Amazon Simple Storage Service API リファレンス」の「PutObjectAcl」を参照してください。

汎用バケットのアクセスポイントを介してオブジェクトをアップロードする

このセクションでは、AWS Management Console、AWS Command Line Interface、または REST API を使用して汎用バケットのアクセスポイントを介してオブジェクトをアップロードする方法について説明します。

S3 コンソールの使用

AWS アカウント内のアクセスポイント経由でオブジェクトをアップロードするには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ページ上部にあるナビゲーションバーで、現在表示されている AWS リージョン の名前をクリックします。次に、アクセスポイントをリスト表示するリージョンを選択します。
3. コンソールの左側のナビゲーションペインで、[アクセスポイント] を選択します。
4. (オプション) アクセスポイントを名前で検索します。選択した AWS リージョンのアクセスポイントのみがここに表示されます。
5. 管理または使用するアクセスポイントの名前を選択します。
6. [オブジェクト] タブで、[アップロード] を選択します。
7. アップロードするファイルやフォルダをここにドラッグアンドドロップするか、[ファイルを追加] または [フォルダの追加] を選択します。

> **Note**
>
> Amazon S3 コンソールを使用すると、アップロードできるファイルの最大サイズが 160 GB になります。160 GB を超えるファイルをアップロードするには、AWS Command Line Interface (AWS CLI)、AWS SDK、または Amazon S3 REST API を使用します。

8. アクセスコントロールリストの許可を変更するには、[Permissions] (許可) を選択します。
9. [Access control list (ACL)] (アクセスコントロールリスト (ACL) で、許可を編集します。

   オブジェクトのアクセス許可については、S3 コンソールを使用した、オブジェクトの ACL アクセス権限の設定 を参照してください。アップロードするすべてのファイルについて、オブジェクトの読み取りアクセスをパブリック (世界中のすべてのユーザー) に付与できます。ただし、パブリック読み取りアクセスのデフォルト設定を変更しないことをお勧めします。パブリック読み取りアクセス権限の付与は、バケットがウェブサイトなどに使用されるなど、ユースケースの小さいサブセットに適用されます。オブジェクトをアップロードした後で、オブジェクトの許可をいつでも変更できます。
10. その他の追加プロパティを設定するには、[Properties] (プロパティ) を選択します。
11. [ストレージクラス] で、アップロードするファイルのストレージクラスを選択します。

    ストレージクラスの詳細については、Amazon S3 ストレージクラスの理解と管理 を参照してください。
12. オブジェクトの暗号化設定を更新するには、[Server-side encryption settings] (サーバー側の暗号化設定) で、次の操作を行います。

    a. [Specify an encryption key] (暗号化キーを指定する) を選択します。

    b. [暗号化設定] で、[デフォルトの暗号化にバケット設定を使用する] または [デフォルトの暗号化にバケット設定を上書きする] を選択します。

    c. [デフォルトの暗号化にバケット設定を上書きする] を選択した場合は、次の暗号化設定を設定する必要があります。

       - Amazon S3 管理のキーを使用してアップロードされたファイルを暗号化するには、[Amazon S3 マネージドキー (SSE-S3)] を選択します。

         詳細については、「Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3)」を参照してください。

- AWS Key Management Service (AWS KMS) に保存されているキーを使用してアップロード済みファイルを暗号化するには、AWS Key Management Service キー (SSE-KMS) を選択します。次に、AWS KMS キーについて、以下のいずれかのオプションを選択します。
  - 使用可能な KMS キーのリストから選択するには、[AWS KMS keys から選択する] を選択し、使用可能なキーのリストから自分の KMS キーを選択します。

    AWS マネージドキー (aws/s3) とカスタマーマネージドキーの両方がこのリストに表示されます。カスタマーマネージドキーの詳細については、AWS Key Management Serviceデベロッパーガイドの「カスタマーキーと AWS キー」を参照してください。
  - KMS キー ARN を入力するには、[AWS KMS key ARN を入力] を選択し、表示されるフィールドに KMS キー ARN を入力します。
  - AWS KMS コンソールで新しいカスタマーマネージドキーを作成するには、[KMS キーを作成] を選択します。

    AWS KMS key の作成の詳細については、「AWS Key Management Service デベロッパーガイド」の「キーの作成」を参照してください。

> **Important**
>
> バケットと同じ AWS リージョン で使用可能な KMS キーのみを使用できます。Amazon S3 コンソールには、バケットと同じリージョンで最初の 100 個の KMS キーしか表示されません。リストに存在しない KMS キーを使用するには、KMS キー ARN を入力する必要があります。別のアカウントが所有している KMS キーを使用する場合は、まずそのキーを使用するアクセス許可が必要であり、次に KMS キー ARN を入力する必要があります。
> Amazon S3 では、対称暗号化 KMS キーのみがサポートされ、非対称暗号化 KMS キーはサポートされません。詳細については、AWS Key Management Service デベロッパーガイドの「Identifying symmetric and asymmetric KMS keys」(対称および非対称 KMS キーの識別) を参照してください。

13. 追加のチェックサムを使用するには、[On] (オン) を選択します。次に、[Checksum function] (チェックサム関数) で、使用する関数を選択します。Amazon S3 は、オブジェクト全体を受け取った後、チェックサム値を計算して保存します。[Precalculated value] (事前計算された値) ボックスを使用して、事前計算された値を指定できます。その場合、Amazon S3 は、指定した値と計算した値を比較します。2 つの値が一致しない場合、Amazon S3 はエラーを生成します。

追加のチェックサムを使用すると、データの検証に使用するチェックサムアルゴリズムを指定できます。追加のチェックサムの詳細については、「Amazon S3 でのオブジェクトの整合性のチェック」を参照してください。

14. アップロードするすべてのオブジェクトにタグを追加するには、[Add tag (タグの追加)] を選択します。[キー] フィールドにタグ名を入力します。タグの値を入力します。

    オブジェクトのタグ付けにより、ストレージを分類する方法が提供されます。各タグはキーと値のペアです。キーとタグ値は大文字と小文字が区別されます。オブジェクトごとに最大 10 個のタグを持つことができます。タグキーには最大 128 個の Unicode 文字、タグ値には最大 255 個の Unicode 文字を使用できます。オブジェクトタグの詳細については、タグを使用してストレージを分類するを参照してください。

15. メタデータを追加するには、[Add metadata] (メタデータの追加) を選択します。

    a. [Type] (タイプ) で、[System defined] (システム定義) または [User defined] (ユーザー定義) を選択します。

       システム定義のメタデータの場合は、Content-Type や Content-Disposition などの一般的な HTTP ヘッダーを選択できます。システム定義のメタデータのリストと値を追加できるかどうかについては、システムで定義されたオブジェクトメタデータ を参照してください。プレフィックス `x-amz-meta-` で始まるメタデータはすべてユーザー定義のメタデータとして扱われます。ユーザー定義メタデータはオブジェクトと共に保存され、オブジェクトのダウンロード時に返されます。キーと値の両方が US-ASCII 標準に従っている必要があります。ユーザー定義メタデータのサイズは最大 2 KB です。システム定義メタデータとユーザー定義メタデータの詳細については、オブジェクトメタデータの使用 を参照してください。

    b. [Key] (キー) で、キーを選択します。

    c. キーの値を入力します。

16. オブジェクトをアップロードするには、[Upload] (アップロード) を選択します。

    Amazon S3 はオブジェクトをアップロードします。アップロードが完了すると、[Upload: status] (アップロード: ステータス) ページに成功のメッセージが表示されます。

AWS CLI を使用する場合

次の `put-object` コマンド例は、AWS CLI を使用してアクセスポイント経由でオブジェクトをアップロードする方法を示しています。

次のコマンドは、アクセスポイント *my-access-point* を使用して AWS アカウント *111122223333* のオブジェクト puppy.jpg をアップロードします。

```
aws s3api put-object --bucket arn:aws:s3:AWS #####:111122223333:accesspoint/my-access-point --key puppy.jpg --body puppy.jpg
```

> **Note**
>
> S3 は、すべてのアクセスポイントに対してアクセスポイントエイリアスを自動的に生成します。アクセスポイントエイリアスは、バケット名を使用してオブジェクトレベルのオペレーションを実行する任意の場所で使用できます。詳細については、「汎用バケットのアクセスポイントのエイリアス」を参照してください。

詳細と例については、「AWS CLI コマンドリファレンス」の「put-object」を参照してください。

REST API の使用

REST API を使用して、アクセスポイントを介してオブジェクトをアップロードできます。詳細については、「Amazon Simple Storage Service API リファレンス」の「PutObject」を参照してください。

AWS SDK の使用

AWS SDK for Python を使用して、アクセスポイントを介してオブジェクトをアップロードできます。

Python

次の例では、*my-access-point* という名前のアクセスポイントを使用して、*hello.txt* という名前のファイルが AWS アカウント *111122223333* 用にアップロードされます。

```
import boto3
s3 = boto3.client('s3')
s3.upload_file('/tmp/hello.txt', 'arn:aws:s3:us-east-1:111122223333:accesspoint/my-access-point', 'hello.txt')
```

汎用バケットのアクセスポイントを介してタグセットを追加する

このセクションでは、AWS Management Console、AWS Command Line Interface、または REST API を使用して汎用バケットのアクセスポイントを介してタグセットを追加する方法について説明します。詳細については、「タグを使用してストレージを分類する」を参照してください。

S3 コンソールの使用

AWS アカウント内でのアクセスポイントを使用したタグセットの追加

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ページ上部にあるナビゲーションバーで、現在表示されている AWS リージョン の名前をクリックします。次に、アクセスポイントをリスト表示するリージョンを選択します。
3. コンソールの左側のナビゲーションペインで、[アクセスポイント] を選択します。
4. (オプション) アクセスポイントを名前で検索します。選択した AWS リージョンのアクセスポイントのみがここに表示されます。
5. 管理または使用するアクセスポイントの名前を選択します。
6. [オブジェクト] タブで、タグセットを追加するオブジェクトの名前を選択します。
7. [プロパティ] タブで、[タグ] サブヘッダーを検索して、[編集] を選択します。
8. リストされたオブジェクトを確認し、[タグの追加] を選択します。
9. 各オブジェクトタグはキーと値のペアです。キーと値を入力します。別のタグを追加するには、[タグの追加] を選択します。

   オブジェクトには最大 10 個のタグを入力できます。
10. [Save changes] (変更の保存) をクリックします。

AWS CLI を使用する場合

次の `put-object-tagging` コマンド例は、AWS CLI を使用してアクセスポイント経由でタグセットを追加する方法を示しています。

次のコマンドは、アクセスポイント *`my-access-point`* を使用して既存のオブジェクト `puppy.jpg` のタグセットを追加します。

```
aws s3api put-object-tagging --bucket arn:aws:s3:AWS #####:111122223333:accesspoint/my-access-point --key puppy.jpg --tagging TagSet=[{Key="animal",Value="true"}]
```

> **Note**
>
> S3 は、すべてのアクセスポイントに対してアクセスポイントエイリアスを自動的に生成します。アクセスポイントエイリアスは、バケット名を使用してオブジェクトレベルのオペレーションを実行する任意の場所で使用できます。詳細については、「汎用バケットのアクセスポイントのエイリアス」を参照してください。

詳細と例については、「AWS CLI コマンドリファレンス」の「put-object-tagging」を参照してください。

REST API の使用

REST API を使用して、アクセスポイント経由でオブジェクトにタグセットを追加できます。詳細については、「Amazon Simple Storage Service API リファレンス」の「PutObjectTagging」を参照してください。

汎用バケットのアクセスポイントを介してオブジェクトを削除する

このセクションでは、AWS Management Console、AWS Command Line Interface、または REST API を使用して汎用バケットのアクセスポイントを介してオブジェクトを削除する方法について説明します。

S3 コンソールの使用

AWS アカウント内のアクセスポイント経由でオブジェクトを削除するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ページ上部にあるナビゲーションバーで、現在表示されている AWS リージョン の名前をクリックします。次に、アクセスポイントをリスト表示するリージョンを選択します。
3. コンソールの左側のナビゲーションペインで、[アクセスポイント] を選択します。
4. (オプション) アクセスポイントを名前で検索します。選択した AWS リージョンのアクセスポイントのみがここに表示されます。
5. 管理または使用するアクセスポイントの名前を選択します。
6. [オブジェクト] タブで、削除するオブジェクトの名前を選択します。
7. 削除対象としてリストされているオブジェクトを確認し、確認ボックスに「削除」と入力します。

8. [オブジェクトの削除] を選択します。

AWS CLI を使用する場合

次の `delete-object` コマンド例は、AWS CLI を使用してアクセスポイント経由でオブジェクトを削除する方法を示しています。

次のコマンドは、アクセスポイント *my-access-point* を使用して既存のオブジェクト `puppy.jpg` を削除します。

```
aws s3api delete-object --bucket arn:aws:s3:AWS #####:111122223333:accesspoint/my-access-point --key puppy.jpg
```

> **Note**
>
> S3 は、すべてのアクセスポイントに対してアクセスポイントエイリアスを自動的に生成します。アクセスポイントエイリアスは、バケット名を使用してオブジェクトレベルのオペレーションを実行する任意の場所で使用できます。詳細については、「汎用バケットのアクセスポイントのエイリアス」を参照してください。

詳細と例については、「AWS CLI コマンドリファレンス」の「delete-object」を参照してください。

REST API の使用

REST API を使用して、アクセスポイント経由でオブジェクトを削除できます。詳細については、「Amazon Simple Storage Service API リファレンス」の「DeleteObject」を参照してください。

S3 Access Grants でのアクセス管理

最小特権の原則に従うには、アプリケーション、ペルソナ、グループ、または組織単位に基づいて Amazon S3 データへのきめ細かなアクセスを定義します。アクセスパターンの規模と複雑さに応じて、さまざまなアプローチを使用して Amazon S3 のデータへのきめ細いアクセスを実現できます。

Amazon S3 内の少数から中程度の数のデータセットへのアクセスを AWS Identity and Access Management (IAM) プリンシパルで管理する最も簡単な方法は、IAM アクセス許可ポリシー と S3 バケットポリシー を定義することです。この戦略は、必要なポリシーが S3 バケットポリシー (20 KB)

と IAM ポリシー (5 KB) のポリシーサイズ制限内に収まり、アカウントごとに許可されている IAM プリンシパルの数内である限り有効です。

データセットの数やユースケースの数が増えるにつれて、より多くのポリシースペースが必要になる場合があります。ポリシーステートメントの容量を大幅に増やすには、S3 バケットの追加エンドポイントとして S3 アクセスポイントを使用する方法があります。これは、各アクセスポイントに独自のポリシーを設定できるためです。アカウントにつき AWS リージョン ごとに数千のアクセス ポイントを設定でき、アクセスポイントごとに最大 20 KB のサイズのポリシーを設定できるため、非常にきめ細かいアクセスコントロール パターンを定義できます。S3 Access Points を使用すると、使用可能なポリシースペースの量が増えますが、クライアントが適切なデータセットに適したアクセスポイントを検出するためのメカニズムが必要になります。

3 番目の方法は、IAM セッションブローカーパターンの実装です。このパターンでは、アクセス決定ロジックを実装し、アクセスセッションごとに短期の IAM セッション認証情報を動的に生成します。IAM セッションブローカーの方法の場合、任意の動的なアクセス許可パターンをサポートして、効果的にスケールできる一方、アクセスパターンロジックを構築する必要があります。

このようなアプローチを使用する代わりに、S3 Access Grants を使用して、Amazon S3 データへのアクセスを管理できます。S3 Access Grants は、Amazon S3 内のデータへのアクセス許可をプレフィックス、バケット、またはオブジェクトごとに定義するための簡略化されたモデルを提供します。さらに、S3 Access Grants を使用して IAM プリンシパルにアクセスを付与することも、社内ディレクトリのユーザーまたはグループに直接アクセスを付与することもできます。

Amazon S3 のデータへのアクセス許可は、通常、ユーザーとグループをデータセットにマップすることで定義します。S3 Access Grants を使用して、Amazon S3 バケットとオブジェクト内のユーザーとロールへの S3 プレフィックスごとに直接アクセスマッピングを定義できます。S3 Access Grants のシンプルなアクセススキームを使用すると、読み取り専用、書き込み専用、または読み取り/書き込みのアクセス権限を S3 プレフィックスごとに IAM プリンシパルに付与することも、社内ディレクトリのユーザーまたはグループに直接付与することもできます。このような S3 Access Grants 機能を使用すると、アプリケーションはアプリケーションの現在の認証済みユーザーに代わって Amazon S3 にデータをリクエストできます。

S3 Access Grants を AWS IAM Identity Center の信頼されたアイデンティティプロパゲーション機能と統合すると、アプリケーションは、認証済みの社内ディレクトリユーザーに代わって (S3 Access Grants を含む) AWS のサービス に直接リクエストすることができます。アプリケーションは最初にユーザーを IAM プリンシパルにマッピングする必要がなくなります。さらに、エンドユーザーのアイデンティティが Amazon S3 にまでプロパゲートされるため、どのユーザーがどの S3 オブジェクトにアクセスしたかの監査が簡素化されます。さまざまなユーザーと IAM セッション間の関係性を

再構築する必要がなくなりました。S3 Access Grants と IAM アイデンティティセンターの信頼されたアイデンティティプロパゲーションを連携すると、Amazon S3 の各 AWS CloudTrail データイベントにデータアクセスがどのエンドユーザーの代わりなのかについての直接のリファレンスが含まれます。

信頼された ID の伝播は、接続された AWS のサービス の管理者がサービスデータへのアクセスを許可および監査するために使用できる AWS IAM Identity Center 機能です。このデータへのアクセスは、グループの関連付けなどのユーザー属性に基づいています。信頼された ID の伝播を設定するには、接続された AWS のサービス の管理者と IAM アイデンティティセンターの管理者とのコラボレーションが必要です。詳細については、「Prerequisites and considerations」を参照してください。

S3 Access Grants の詳細については、後続のトピックを参照してください。

トピック

- S3 Access Grants の概念
- S3 Access Grants と社内ディレクトリのアイデンティティ
- S3 Access Grants の開始方法
- S3 Access Grants インスタンスの使用
- S3 Access Grants ロケーションの使用
- S3 Access Grants での許可の使用
- Access Grants を使用した S3 データの取得
- S3 Access は、クロスアカウントアクセスを許可します。
- S3 Access Grants での AWS タグの使用
- S3 Access Grants の制約
- S3 Access Grants の統合

S3 Access Grants の概念

S3 Access Grants のワークフロー

S3 Access Grants のワークフローは次のとおりです。

1. S3 Access Grants インスタンスを作成します。「S3 Access Grants インスタンスの使用」を参照してください。

2. S3 Access Grants インスタンスに、Amazon S3 データ内のロケーションを登録し、これらのロケーションを AWS Identity and Access Management (IAM) ロールにマッピングします。「ロケーションを登録する」を参照してください。
3. 被付与者用の権限を作成し、被付与者に S3 リソースへのアクセス許可を付与します。「S3 Access Grants での許可の使用」を参照してください。
4. 被付与者が S3 Access Grants の一時的な認証情報をリクエストします。「S3 Access Grants を介して Amazon S3 データへのアクセスをリクエストする」を参照してください。
5. 被付与者が、これらの一時的な認証情報を使用して S3 データにアクセスします。「S3 Access Grants が提供する認証情報を使用した S3 データへのアクセス」を参照してください。

詳細については、「S3 Access Grants の開始方法」を参照してください。

S3 Access Grants インスタンス

S3 Access Grants インスタンスは、個々の権限の論理コンテナです。S3 Access Grants インスタンスを作成するときは、AWS リージョンを指定する必要があります。AWS アカウントの AWS リージョンごとに、1 つの S3 Access Grants インスタンスを作成できます。詳細については、「S3 Access Grants インスタンスの使用」を参照してください。

S3 Access Grants を使用して社内ディレクトリ内のユーザーとグループのアイデンティティにアクセス許可を付与する場合は、S3 Access Grants インスタンスを AWS IAM Identity Center インスタンスに関連付ける必要もあります。詳細については、「S3 Access Grants と社内ディレクトリのアイデンティティ」を参照してください。

新規作成された S3 Access Grants インスタンスは空です。インスタンス内で、ロケーションを登録する必要があります。S3 デフォルトパス (`s3://`) 、バケット、またはバケット内のプレフィックスを使用できます。少なくとも 1 つのロケーションを登録したら、この登録したロケーションのデータへのアクセスを許可するアクセス権限を作成できます。

ロケーション

S3 Access Grants のロケーションによって、バケットまたはプレフィックスが AWS Identity and Access Management (IAM) ロールにマッピングされます。S3 Access Grants は、この IAM ロールを引き受けて、その特定のロケーションにアクセスする被付与者に一時的な認証情報を提供します。アクセス権限を作成する前に、まず S3 Access Grants インスタンスに少なくとも 1 つのロケーションを登録する必要があります。

デフォルトのロケーション (`s3://`) を登録し、IAM ロールにマッピングすることをお勧めします。デフォルトの S3 パスのロケーション (`s3://`) を使用すると、アカウントの AWS リージョ

ン内のすべての S3 バケットへのアクセスが カバーされます。アクセス権限を作成するときに、権限の範囲をデフォルトの ロケーション内のバケット、プレフィックス、またはオブジェクトに絞り込むことができます。

より複雑なアクセス管理のユースケースでは、デフォルトの ロケーション以外の登録が必要になる場合があります。例として、次のようなユースケースが挙げられます。

- *amzn-s3-demo-bucket* が S3 Access Grants インスタンスの登録済み ロケーションで、IAM ロールがマッピングされているが、この IAM ロールがバケット内の特定のプレフィックスへのアクセスを拒否されるとします。この場合、IAM ロールがアクセスできないプレフィックスを別の ロケーションとして登録し、その ロケーションを、必要なアクセス権を持つ別の IAM ロールにマッピングできます。
- 仮想プライベートクラウド (VPC) エンドポイント内のユーザーのみにアクセスを制限する権限を作成するとします。この場合、IAM ロールで VPC エンドポイントのみにアクセスを制限するバケットの ロケーションを登録できます。後で、被付与者が S3 Access Grants に認証情報を要求すると、S3 Access Grants は ロケーションの IAM ロールを引き受けて一時的な認証情報を提供します。この認証情報は、呼び出し元が VPC エンドポイント内のユーザーでない限り、特定のバケットへのアクセスを拒否します。こうした拒否のアクセス許可は、権限で指定された通常の READ、WRITE、または READWRITE のアクセス許可に加えて適用されます。

ユースケースで S3 Access Grants インスタンスに複数の ロケーションを登録する必要がある場合は、次のいずれかを登録できます。

- デフォルトの S3 ロケーション (`s3://`)
- 1 つのバケット (*amzn-s3-demo-bucket* など) または複数のバケット
- 1 つのバケットと 1 つのプレフィックス (*amzn-s3-demo-bucket*`/prefix*` など) 、または複数のプレフィックス

S3 Access Grants インスタンスに登録できる ロケーションの最大数については、「S3 Access Grants の制約」を参照してください。S3 Access Grants の ロケーション登録の詳細については「ロケーションを登録する」を参照してください。

S3 Access Grants インスタンスに最初の ロケーションを登録しても、インスタンスに個別のアクセス権限はありません。そのため、S3 データへのアクセスはまだ許可されていません。この時点で、アクセス権限を作成してアクセスを許可できます。権限の作成方法の詳細については、「S3 Access Grants での許可の使用」を参照してください。

権限

S3 Access Grants インスタンス内の個々の「権限」は、特定のアイデンティティ (IAM プリンシパル、社内ディレクトリのユーザーやグループ) に、S3 Access Grants インスタンスに登録された口ケーション内でのアクセスを許可するものです。

権限を作成する際、登録された口ケーション全体へのアクセス許可を付与する必要はありません。口ケーション内で権限のアクセス範囲を絞り込むことができます。登録された口ケーションがデフォルトの S3 パス (s3://) である場合は、バケット、バケット内のプレフィックス、または特定のオブジェクトに権限の範囲を絞り込む必要があります。権限に登録された口ケーションがバケットまたはプレフィックスである場合は、バケットまたはプレフィックス全体へのアクセスを許可することも、オプションで、権限の範囲をプレフィックス、サブプレフィックス、またはオブジェクトに絞り込むこともできます。

権限では、権限のアクセスレベルを READ、WRITE、または READWRITE に設定します。例えば、社内ディレクトリグループ `01234567-89ab-cdef-0123-456789abcdef` にバケット `s3://amzn-s3-demo-bucket/projects/items/*` への READ アクセスを許可する権限があるとします。この場合、そのグループのユーザーには、*amzn-s3-demo-bucket* という名前のバケット内の、プレフィックス `projects/items/` が付いたオブジェクトキー名を持つすべてのオブジェクトへの READ アクセスが付与されます。

S3 Access Grants インスタンスで作成できる権限の最大数については、「S3 Access Grants の制約」を参照してください。権限の作成方法の詳細については、「権限を作成する」を参照してください。

S3 Access Grants の一時的な認証情報

権限を作成すると、権限で指定されたアイデンティティを利用する承認済みアプリケーションは、ジャストインタイムアクセス認証情報をリクエストできるようになります。これを行うために、アプリケーションは GetDataAccess S3 API オペレーションを呼び出します。被付与者は、この API オペレーションを使用して、共有された S3 データへのアクセスをリクエストできます。

S3 Access Grants インスタンスは、`GetDataAccess` リクエストを保持する権限に照会して評価します。リクエスタに一致する権限がある場合、S3 Access Grants は、一致する権限の登録口ケーションに関連付けられた IAM ロールを引き受けます。S3 Access Grants は一時的な認証情報のアクセス許可の範囲を、権限の範囲で指定されている S3 バケット、プレフィックス、またはオブジェクトのみに限定します。

一時アクセス認証情報の有効期限はデフォルトで 1 時間です。ただし、15 分から 12 時間までの任意の値に設定できます。AssumeRole の API リファレンスでセッションの最長時間について確認してください。

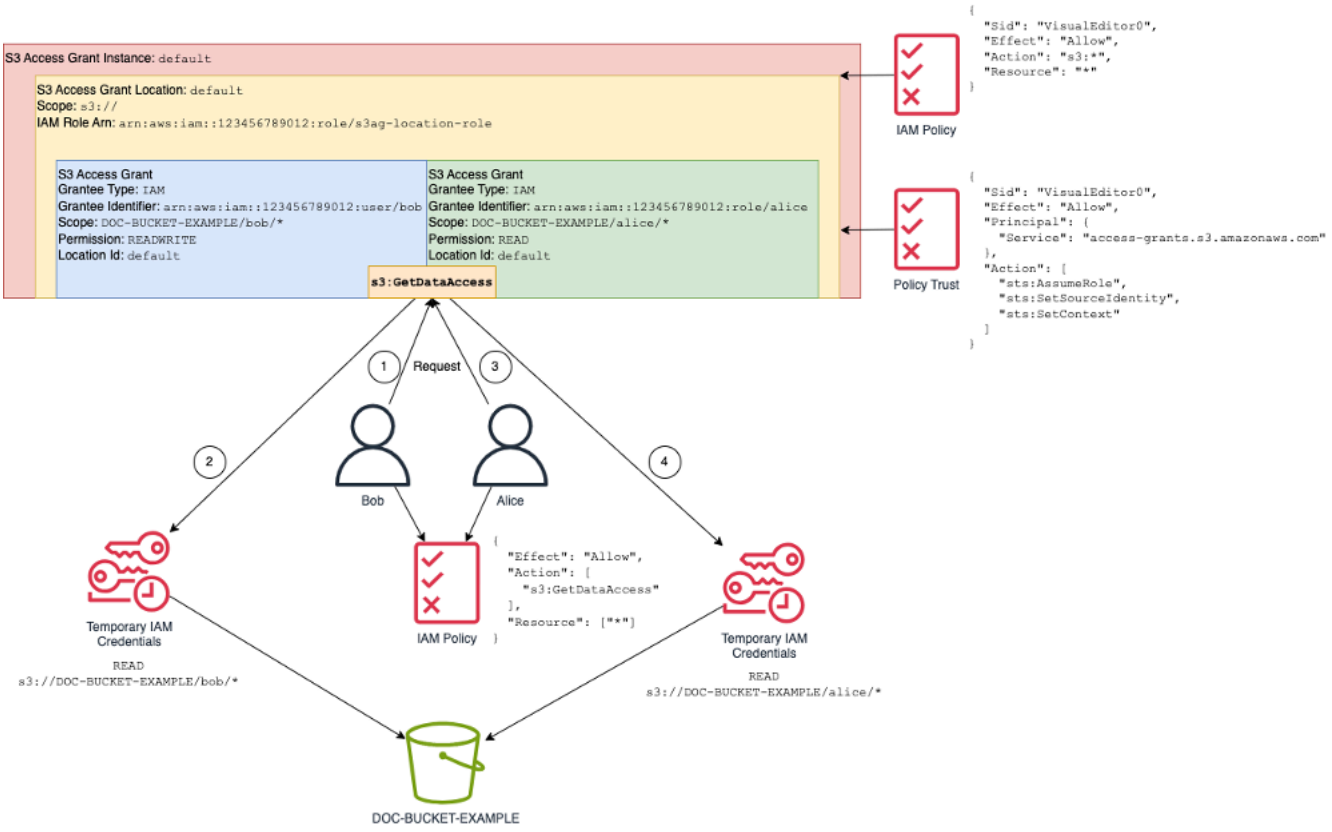
仕組み

次の図では、範囲が s3:// のデフォルトの Amazon S3 ロケーションが IAM ロール s3ag-location-role に登録されています。この IAM ロールには、S3 Access Grants を介して認証情報が取得されると、アカウント内で Amazon S3 アクションを実行するアクセス許可があります。

このロケーションでは、2 人の IAM ユーザーに対して 2 つの個別のアクセス権限が作成されます。IAM ユーザー Bob には、DOC-BUCKET-EXAMPLE バケット内のプレフィックス bob/ への READ と WRITE のアクセス権の両方が付与されます。別の IAM ロールである Alice には、DOC-BUCKET-EXAMPLE バケット内のプレフィックス alice/ への READ アクセス許可のみが付与されます。Bob が DOC-BUCKET-EXAMPLE バケット内のプレフィックス bob/ にアクセスするための権限は青色で定義されています。Alice が DOC-BUCKET-EXAMPLE バケット内のプレフィックス alice/ にアクセスするための権限は緑色で定義されています。

Bob がデータの READ を行う場合、Bob の権限が付与されているロケーションに関連付けられている IAM ロールが S3 Access Grants の GetDataAccess API オペレーションを呼び出します。Bob が s3://DOC-BUCKET-EXAMPLE/bob/* で始まる S3 プレフィックスまたはオブジェクトに対して READ を行おうとすると、GetDataAccess リクエストは s3://DOC-BUCKET-EXAMPLE/bob/* へのアクセス許可がある一時的な IAM セッション認証情報セットを返します。Bob は、権限により許可されているため、s3://DOC-BUCKET-EXAMPLE/bob/* で始まる任意の S3 プレフィックスまたはオブジェクトに対して WRITE を同様に実行できます。

同じように、Alice は、s3://DOC-BUCKET-EXAMPLE/alice/ で始まるすべてに対して READ を実行できます。ただし、s3:// 内のバケット、プレフィックス、オブジェクトに対して WRITE を実行しようとすると、Access Denied (403 Forbidden) エラーが発生します。これは、どのデータに対する WRITE アクセスを Alice に付与する権限がないためです。さらに、Alice が s3://DOC-BUCKET-EXAMPLE/alice/ 外部のデータに対して何らかのアクセスレベル (READ または WRITE) をリクエストしても、同様に Access Denied エラーが表示されます。



このパターンは多数のユーザーとバケットに応じてスケールでき、アクセス許可の管理を簡素化します。個別のユーザーとプレフィックスのアクセス関係を追加または削除するたびに、サイズが大きくなる可能性のある S3 バケットポリシーを編集する代わりに、個別の権限を別々に追加したり削除したりできます。

S3 Access Grants と社内ディレクトリのアイデンティティ

Amazon S3 Access Grants を使用すると、同じ AWS アカウント 内と他のアカウントの両方で、AWS Identity and Access Management (IAM) プリンシパル (ユーザーまたはロール) へのアクセスを許可できます。ただし、多くの場合、データにアクセスするエンティティは社内ディレクトリのエンドユーザーです。IAM プリンシパルにアクセスを付与する代わりに、S3 Access Grants を使用して社内のユーザーやグループに直接アクセスを許可できます。S3 Access Grants を使用すると、社内アプリケーションを介して S3 データにアクセスするために、社内アイデンティティを中間となる IAM プリンシパルにマッピングする必要がなくなります。

エンドユーザーのアイデンティティの使用したデータへのアクセスをサポートするこの新機能は、S3 Access Grants インスタンスを AWS IAM Identity Center インスタンスに関連付けることで実現します。IAM アイデンティティセンターは、標準ベースのアイデンティティプロバイダーをサポートし、S3 Access Grants を含め、エンドユーザーアイデンティティをサポートするあらゆる

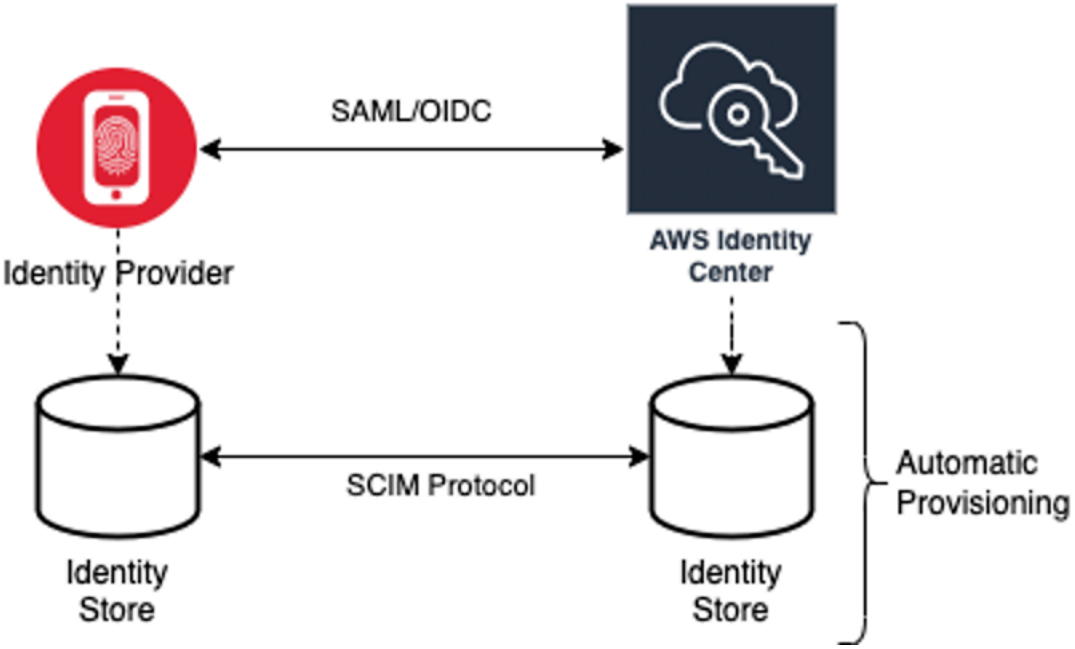
サービスや機能の AWS のハブとなります。IAM アイデンティティセンターは、信頼されているアイデンティティプロパゲーション機能を介して社内アイデンティティの認証をサポートします。詳細については、「アプリケーション間での信頼されたアイデンティティのプロパゲーション」を参照してください。

S3 Access Grants でワークフォースアイデンティティサポートの使用を開始するには、前提条件として、まず IAM アイデンティティセンターで、社内アイデンティティプロバイダーと IAM アイデンティティセンターの間のアイデンティティのプロビジョニングを設定します。IAM アイデンティティセンターは、Okta、Microsoft Entra ID (旧称 Azure Active Directory) などの社内アイデンティティプロバイダー、またはクロスドメインアイデンティティ管理システム (SCIM) プロトコルをサポートするその他の外部アイデンティティプロバイダー (IdP) をサポートしています。IAM アイデンティティセンターを IdP に接続して自動プロビジョニングを有効にすると、IdP のユーザーとグループが IAM アイデンティティセンターのアイデンティティストアに同期されます。このステップが完了すると、IAM アイデンティティセンターにはユーザーとグループに関する独自のビューが表示されるため、S3 Access Grants などのその他の AWS のサービス と機能を使用してユーザーやグループを参照できます。IAM アイデンティティセンターの自動プロビジョニングの設定に関する詳細は、「AWS IAM Identity Center ユーザーガイド」の「自動プロビジョニング」を参照してください。

IAM アイデンティティセンターは、AWS Organizations と統合されているため、各アカウントを手動で設定する必要なく、複数の AWS アカウント にわたるアクセス許可を一元管理できます。通常、組織では、アイデンティティ管理者が組織全体で単一の IAM アイデンティティセンターのインスタンスをアイデンティティ同期の単一ポイントとして、設定します。この IAM アイデンティティセンターのインスタンスは通常、組織内の専用 AWS アカウント インスタンスで実行されます。このような一般的な設定では、組織内のどの AWS アカウント からでも S3 Access Grants のユーザーアイデンティティとグループアイデンティティを参照できます。

ただし、AWS Organizations 管理者が中央の IAM アイデンティティセンターのインスタンスをまだ設定していない場合は、S3 Access Grants インスタンスと同じアカウントにローカルの IAM アイデンティティセンターインスタンスを作成できます。このような設定は、概念実証やローカルの開発環境でのユースケースで一般的です。いずれの場合も、IAM アイデンティティセンターのインスタンスは、関連付けられる S3 Access Grants インスタンスと同じ AWS リージョン に配置する必要があります。

次の図の外部 IdP を使用する IAM アイデンティティセンター設定では、IdP は SCIM で設定され、IdP のアイデンティティストアを IAM アイデンティティセンターのアイデンティティストアと同期します。



社内ディレクトリのアイデンティティを S3 Access Grants で使用するには、次を実行します。

- IAM アイデンティティセンターで 自動プロビジョニング を設定して、IdP からのユーザーとグループの情報を IAM アイデンティティセンターに同期します。
- IAM アイデンティティセンター内の外部アイデンティティソースを信頼できるトークン発行者として設定します。詳細については、「AWS IAM Identity Center ユーザーガイド」の「アプリケーション間での信頼されたアイデンティティのプロパゲーション」を参照してください。
- S3 Access Grants インスタンスを IAM アイデンティティセンターインスタンスに関連付けます。これは、S3 Access Grants インスタンス作成 時に実行できます。S3 Access Grants インスタンスをすでに作成している場合は、「IAM アイデンティティセンターインスタンスの関連付けまたは関連付けを解除します。」を参照してください。

ディレクトリのアイデンティティが S3 データにアクセスする方法

S3 データに社内アプリケーションを介してアクセスする必要がある社内ディレクトリのユーザーがいるとします。例えば、このアプリケーションは、(Okta などの) ユーザー認証を行う外部 IdP と統合されたドキュメントビューアだとします。これらのアプリケーションでのユーザーの認証は、通常、ユーザーのウェブブラウザのリダイレクトによって行われます。ディレクトリ内のユーザーは IAM プリンシパルではないため、アプリケーションには、S3 Access Grants `GetDataAccess` API オペレーションを呼び出し、ユーザーに代わって S3 データへのアクセス認証情報を取得 できる IAM 認証情報が必要です。認証情報を自身で取得する IAM ユーザーやロールとは異なり、アプリ

ケーションには IAM ロールにマップされていないディレクトリユーザーを示す方法が必要です。これにより、ユーザーは S3 Access Grants を通じてデータにアクセスできるようになります。

認証されたディレクトリユーザーから、ディレクトリユーザーに代わって S3 Access Grants へのリクエストを実行できる IAM 呼び出し元へのこの移行は、アプリケーションが IAM アイデンティティセンターの信頼できるトークン発行者機能を通じて行います。アプリケーションは、ディレクトリユーザーを認証すると、(Okta などの) IdP からのアイデンティティトークンを取得し、Okta に従ってディレクトリユーザーを示します。IAM アイデンティティセンターの信頼されたトークン発行者の設定により、アプリケーションはこの Okta トークン (Okta テナントが「信頼できる発行者」として設定されている) を、AWS のサービス 内でディレクトリユーザーを安全に示す IAM アイデンティティセンターの別のアイデンティティトークンと交換できます。その後、データアプリケーションは IAM ロールを引き受け、IAM アイデンティティセンターからのディレクトリユーザーのトークンを追加のコンテキストとして提供します。アプリケーションは、結果として得られる IAM セッションを使用して S3 Access Grants を呼び出すことができます。このトークンは、アプリケーションのアイデンティティ (IAM プリンシパル自体) とディレクトリユーザーのアイデンティティの両方を示します。

この移行の主なステップはトークンの交換です。アプリケーションは IAM アイデンティティセンターの `CreateTokenWithIAM` API オペレーションを呼び出して、このトークン交換を実行します。当然、これもまた AWS API 呼び出しであり、署名には IAM プリンシパルが必要です。このリクエストを行う IAM プリンシパルは、通常、アプリケーションに関連付けられた IAM ロールです。例えば、アプリケーションが Amazon EC2 で実行されている場合、`CreateTokenWithIAM` リクエストは通常、アプリケーションが実行されている EC2 インスタンスに関連付けられている IAM ロールによって実行されます。`CreateTokenWithIAM` 呼び出しが正常に完了すると、新しいアイデンティティトークンが生成され、AWS のサービス 内でそのトークンが認識されます。

アプリケーションがディレクトリユーザーに代わって `GetDataAccess` を呼び出す前の次のステップは、アプリケーションがディレクトリユーザーのアイデンティティを含む IAM セッションを取得することです。アプリケーションは、追加のアイデンティティコンテキストとしてディレクトリユーザーの IAM アイデンティティセンターのトークンも含めた AWS Security Token Service (AWS STS) `AssumeRole` リクエストを使用してこれを実行します。この追加コンテキストにより、IAM アイデンティティセンターはディレクトリユーザーのアイデンティティを次のステップにプロパゲートできるようになります。アプリケーションが引き受ける IAM ロールは、`GetDataAccess` オペレーションを呼び出すために IAM アクセス権限を必要とするロールです。

追加のコンテキストとしてディレクトリユーザーのための IAM アイデンティティセンターのトークンを使用して アイデンティティベアラー IAM ロールを引き受けたため、アプリケーションには、認

証されたディレクトリユーザーに代わって GetDataAccess に署名付きリクエストを行うために必要なものがすべて揃っています。

トークンのプロパゲーションは次のステップに基づいています。

IAM アイデンティティセンターのアプリケーションを作成する

まず、IAM アイデンティティセンターに新しいアプリケーションを作成します。このアプリケーションは、使用できるアプリケーション設定タイプを IAM アイデンティティセンターが識別できるテンプレートを使用します。アプリケーションを作成するコマンドでは、IAM アイデンティティセンターインスタンスの Amazon リソースネーム (ARN)、アプリケーション名、アプリケーションプロバイダー ARN を指定する必要があります。アプリケーションプロバイダーは、アプリケーションが IAM アイデンティティセンターを呼び出すために使用する SAML または OAuth アプリケーションプロバイダーです。

次のコマンド例を使用する際は、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws sso-admin create-application \
 --instance-arn "arn:aws:sso:::instance/ssoins-ssoins-1234567890abcdef" \
 --application-provider-arn "arn:aws:sso::aws:applicationProvider/custom" \
 --name MyDataApplication
```

レスポンス:

```
{
   "ApplicationArn": "arn:aws:sso::123456789012:application/ssoins-
ssoins-1234567890abcdef/apl-abcd1234a1b2c3d"
}
```

信頼できるトークン発行者を作成します。

IAM アイデンティティセンターアプリケーションが完成したところで、次のステップは、IdP IdToken からの値を IAM アイデンティティセンターのトークンと交換するために使用される信頼できるトークン発行者を設定することです。このステップを完了するには、以下の項目が必要です。

- アイデンティティプロバイダーの発行者の URL
- 信頼されたトークン発行者名
- クレーム属性パス
- アイデンティティストア属性パス

- JSON Web Key Set (JWKS) 取り出しオプション

クレーム属性パスは、アイデンティティストア属性へのマッピングに使用されるアイデンティティプロバイダー属性です。通常、クレーム属性パスはユーザーのメールアドレスであるとはいえ、その他の属性を使用してマッピングを実行することもできます。

oidc-configuration.json というファイルを次の内容で作成します。このポリシーを使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
{
  "OidcJwtConfiguration":
     {
      "IssuerUrl": "https://login.microsoftonline.com/a1b2c3d4-abcd-1234-b7d5-
b154440ac123/v2.0",
      "ClaimAttributePath": "preferred_username",
      "IdentityStoreAttributePath": "userName",
      "JwksRetrievalOption": "OPEN_ID_DISCOVERY"
     }
}
```

信頼できるトークン発行者を作成するには、次のコマンドを実行します。このコマンド例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws sso-admin create-trusted-token-issuer \
  --instance-arn "arn:aws:sso:::instance/ssoins-1234567890abcdef" \
  --name MyEntraIDTrustedIssuer \
  --trusted-token-issuer-type OIDC_JWT \
  --trusted-token-issuer-configuration file://./oidc-configuration.json
```

レスポンス

```
{
  "TrustedTokenIssuerArn": "arn:aws:sso::123456789012:trustedTokenIssuer/
ssoins-1234567890abcdef/tti-43b4a822-1234-1234-1234-a1b2c3d41234"
}
```

IAM アイデンティティセンターアプリケーションを信頼できるトークン発行者に接続します。

信頼されたトークン発行者が機能するには、さらにいくつかの設定が必要です。信頼できるトークン発行者が信頼する対象者を設定します。対象者はキーによって識別される IdToken 内部の値で、アイデンティティプロバイダーの設定で確認できます。例:

```
1234973b-abcd-1234-abcd-345c5a9c1234
```

次のコンテンツを含む grant.json という名前のファイルを作成します。このファイルを使用するには、アイデンティティプロバイダーの設定と一致するように対象者を変更し、前のコマンドで返された信頼できるトークン発行者 ARN を指定します。

```
{
   "JwtBearer":
     {
       "AuthorizedTokenIssuers":
         [
           {
             "TrustedTokenIssuerArn": "arn:aws:sso::123456789012:trustedTokenIssuer/
ssoins-1234567890abcdef/tti-43b4a822-1234-1234-1234-a1b2c3d41234",
               "AuthorizedAudiences":
                 [
                   "1234973b-abcd-1234-abcd-345c5a9c1234"
                 ]
            }
         ]
     }
 }
```

次のコマンド例を実行します。このコマンドを使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws sso-admin put-application-grant \
  --application-arn "arn:aws:sso::123456789012:application/ssoins-
ssoins-1234567890abcdef/apl-abcd1234a1b2c3d" \
  --grant-type "urn:ietf:params:oauth:grant-type:jwt-bearer" \
  --grant file://./grant.json \
```

このコマンドは、grant.json ファイル内の対象者を信頼する設定を使用して、信頼されたトークン発行者を設定し、このオーディエンスを、タイプ jwt-bearer のトークンを交換するための最初のステップで作成されたアプリケーションにリンクします。urn:ietf:params:oauth:grant-type:jwt-bearer の文字列は任意の文字列ではありません。これは、OAuth SON Web Token (JWT) アサーションプロファイルに登録されている名前空間です。この名前空間の詳細については、RFC 7523 を参照してください。

次のコマンドを使用して、信頼できるトークン発行者が アイデンティティプロバイダーからの IdToken 値を交換する際にどの範囲を含めるかを設定します。S3 Access Grants の場合、--scope パラメータの値は s3:access_grants:read_write です。

```
aws sso-admin put-application-access-scope \
  --application-arn "arn:aws:sso::111122223333:application/ssoins-
ssoins-111122223333abcdef/apl-abcd1234a1b2c3d" \
  --scope "s3:access_grants:read_write"
```

最後のステップは、リソースポリシーを IAM アイデンティティセンターのアプリケーションにアタッチすることです。このポリシーにより、アプリケーションの IAM ロールが sso-oauth:CreateTokenWithIAM API オペレーションにリクエストを行い、IAM アイデンティティセンター から IdToken 値を受け取ることができるようになります。

次のコンテンツを含む authentication-method.json という名前のファイルを作成します。*123456789012* をアカウント ID に置き換えます。

```
{
   "Iam":
       {
         "ActorPolicy":
             {
                "Version": "2012-10-17",
                    "Statement":
                    [
                        {
                           "Effect": "Allow",
                            "Principal":
                            {
                              "AWS": "arn:aws:iam::123456789012:role/webapp"
                            },
                           "Action": "sso-oauth:CreateTokenWithIAM",
                            "Resource": "*"
                        }
                    ]
                }
            }
        }
```

ポリシーを IAM アイデンティティセンターアプリケーションにアタッチするには、次のコマンドを実行します。

```
aws sso-admin put-application-authentication-method \
   --application-arn "arn:aws:sso::123456789012:application/ssoins-
ssoins-1234567890abcdef/apl-abcd1234a1b2c3d" \
   --authentication-method-type IAM \
   --authentication-method file://./authentication-method.json
```

これで、ウェブアプリケーションを通じてディレクトリユーザーに S3 Access Grants を使用するための設定が完了しました。この設定はアプリケーション内で直接テストすることも、IAM アイデンティティセンターアプリケーションポリシーで許可されている IAM ロールから次のコマンドを使用して CreateTokenWithIAM API オペレーションを呼び出しても行えます。

```
aws sso-oidc create-token-with-iam \
   --client-id "arn:aws:sso::123456789012:application/ssoins-ssoins-1234567890abcdef/
apl-abcd1234a1b2c3d"  \
   --grant-type urn:ietf:params:oauth:grant-type:jwt-bearer \
   --assertion IdToken
```

結果は次のとおりになります。

```
{
    "accessToken": "<suppressed long string to reduce space>",
    "tokenType": "Bearer",
    "expiresIn": 3600,
    "refreshToken": "<suppressed long string to reduce space>",
    "idToken": "<suppressed long string to reduce space>",
    "issuedTokenType": "urn:ietf:params:oauth:token-type:refresh_token",
    "scope": [
      "sts:identity_context",
      "s3:access_grants:read_write",
      "openid",
      "aws"
    ]
}
```

base64 でエンコードされた IdToken 値をデコードすると、JSON 形式のキーバリューペアが表示されます。キー sts:identity_context には、アプリケーションがディレクトリ ユーザーのアイデンティティ情報を含めるために sts:AssumeRole リクエストで送信する必要がある値が含まれています。デコードされた IdToken の例は次のとおりです。

```
{
    "aws:identity_store_id": "d-996773e796",
```

```
    "sts:identity_context": "AQoJb3JpZ2luX2VjEOTtl;<SUPRESSED>",
    "sub": "83d43802-00b1-7054-db02-f1d683aacba5",
    "aws:instance_account": "123456789012",
    "iss": "https://identitycenter.amazonaws.com/ssoins-1234567890abcdef",
    "sts:audit_context": "AQoJb3JpZ2luX2VjEOT<SUPRESSED>==",
    "aws:identity_store_arn": "arn:aws:identitystore::232642235904:identitystore/
d-996773e796",
    "aud": "abcd12344U0gi7n4Yyp0-WV1LWNlbnRyYWwtMQ",
    "aws:instance_arn": "arn:aws:sso:::instance/ssoins-6987d7fb04cf7a51",
    "aws:credential_id": "EXAMPLEHI5glPh40y9TpApJn8...",
    "act": {
       "sub": "arn:aws:sso::232642235904:trustedTokenIssuer/
ssoins-6987d7fb04cf7a51/43b4a822-1020-7053-3631-cb2d3e28d10e"
    },
    "auth_time": "2023-11-01T20:24:28Z",
    "exp": 1698873868,
    "iat": 1698870268
}
```

`sts:identity_context` から値を取得し、この情報を `sts:AssumeRole` 呼び出しで渡すことができます。CLI 出力例は次のとおりです。引き受けるロールは、`s3:GetDataAccess` 呼び出しアクセス許可のある一時的なロールです。

```
aws sts assume-role \
   --role-arn "arn:aws:iam::123456789012:role/temp-role" \
   --role-session-name "TempDirectoryUserRole" \
   --provided-contexts ProviderArn="arn:aws:iam::aws:contextProvider/
IdentityCenter",ContextAssertion="value from sts:identity_context"
```

これで、この呼び出しで受け取った認証情報を使用して `s3:GetDataAccess` API オペレーションを呼び出し、S3 リソースにアクセスできる最終的な認証情報を受け取ることができます。

S3 Access Grants の開始方法

Amazon S3 Access Grants は、S3 データにスケーラブルなアクセスコントロールソリューションを提供する Amazon S3 の機能です。S3 Access Grants は S3 認証情報ベンダーです。つまり、許可のリストとレベルを S3 Access Grants に登録することになります。その後、ユーザーまたはクライアントが S3 データにアクセスする必要が生じると、まず S3 Access Grants に認証情報を要求します。アクセスを許可する対応する権限がある場合、S3 Access Grants は一時的な最小特権のアクセス認証情報を送信します。その後、ユーザーまたはクライアントは S3 Access Grants から提供された認証情報を使用して S3 データにアクセスできます。これを踏まえて、S3 データ要件で複雑ま

たは大規模なアクセス許可設定が必要となる場合は、S3 Access Grants を使用して、ユーザー、グループ、ロール、アプリケーションの S3 データ権限をスケーリングできます。

ほとんどのユースケースでは、AWS Identity and Access Management (IAM) バケットポリシーまたは IAM アイデンティティベースのポリシーを使用して S3 データのアクセスコントロールを管理できます。

ただし、次のような複雑な S3 アクセスコントロール要件がある場合は、S3 Access Grants を使用すると多大な利点が得られます。

- バケットポリシーのサイズ制限である 20 KB に達している場合。
- 分析やビッグデータのために S3 データへのアクセス許可をヒューマンアイデンティティで付与している場合。例えば、Microsoft Entra ID (旧称 Azure Active Directory)、Okta、または Ping など。
- IAM ポリシーを頻繁に更新せずに、クロスアカウントアクセスを提供する必要がある場合。
- データが構造化されておらず、構造化されていない行と列の形式で、オブジェクトレベルの場合。

S3 Access Grants のワークフローは次のとおりです。

ステップ	説明
1	S3 Access Grants インスタンスを作成する 開始するには、個別のアクセス許可を含む S3 Access Grants インスタンスを起動します。
2	ロケーションを登録する 次に、S3 データロケーション (デフォルトの `s3://` など) を登録して、S3 データロケーションへのアクセスを提供する際に S3 Access Grants が引き受けるデフォルトの IAM ロールを指定します。また、特定のバケットまたはプレフィックスにカスタムロケーションを追加し、それらをカスタム IAM ロールにマッピングすることもできます。
3	権限を作成する 個別のアクセス許可権限を作成します。これらのアクセス権限では、登録されている S3 ロケーション、その ロケーション内

ステップ	説明
	のデータアクセス範囲、権限被付与者のアイデンティティ、アクセスレベル (READ、WRITE、またはREADWRITE) を指定します。
4	S3 データへのアクセスをリクエストする ユーザー、アプリケーション、S3 AWS のサービス データへのアクセスには、まずアクセスリクエストを行います。S3 Access Grants が、リクエストを承認すべきかどうかを決定します。アクセスを許可する対応する権限がある場合、S3 Access Grants は、その権限に関連付けられている登録済み口ケーションの IAM ロールを使用して、一時的な認証情報をリクエスタに返送します。
5	S3 データにアクセスする アプリケーションは S3 Access Grants が提供する一時的な認証情報を使用して S3 データにアクセスします。

S3 Access Grants インスタンスの使用

Amazon S3 Access Grants の使用を開始するには、まず S3 Access Grants インスタンスを作成します。作成できるのは、アカウントにつき AWS リージョン ごとに単一の S3 Access Grants インスタンス のみです。S3 Access Grants インスタンスは、登録された口ケーションや権限を含む S3 Access Grants リソースのコンテナとして機能します。

S3 Access Grants を使用すると、AWS Identity and Access Management (IAM) ユーザーとロールに S3 データへのアクセス許可を付与することができます。AWS IAM Identity Center に 社内アイデンティティディレクトリを追加した場合は、社内ディレクトリのこの IAM アイデンティティセンターインスタンスを S3 Access Grants インスタンスに関連付けることができます。その後、社内ユーザーとグループにアクセス権限を作成できます。社内ディレクトリを IAM アイデンティティセンターにまだ追加していない場合は、後で S3 Access Grants インスタンスを IAM アイデンティティセンターインスタンスに関連付けることができます。

トピック

- S3 Access Grants インスタンスを作成する

- S3 Access Grants インスタンスの詳細を取得する
- S3 Access Grants インスタンスを一覧表示する
- IAM アイデンティティセンターインスタンスの関連付けまたは関連付けを解除します。
- S3 Access Grants インスタンスを削除する

S3 Access Grants インスタンスを作成する

Amazon S3 Access Grants の使用を開始するには、まず S3 Access Grants インスタンスを作成します。作成できるのは、アカウントにつき AWS リージョン ごとに単一の S3 Access Grants インスタンス のみです。S3 Access Grants インスタンスは、登録された口ケーションや権限を含む S3 Access Grants リソースのコンテナとして機能します。

S3 Access Grants を使用すると、AWS Identity and Access Management (IAM) ユーザーとロールに S3 データへのアクセス許可を付与することができます。AWS IAM Identity Center に 社内アイデンティティディレクトリを追加した場合は、社内ディレクトリのこの IAM アイデンティティセンターインスタンスを S3 Access Grants インスタンスに関連付けることができます。その後、社内ユーザーとグループにアクセス権限を作成できます。社内ディレクトリを IAM アイデンティティセンターにまだ追加していない場合は、後で S3 Access Grants インスタンスを IAM アイデンティティセンターインスタンスに関連付けることができます。

Amazon S3 コンソール、AWS Command Line Interface、(AWS CLI)、AWS SDK、または Amazon S3 REST API を使用して S3 Storage Lens グループを作成および管理できます。

S3 コンソールの使用

S3 Access Grants を使用して S3 データへのアクセスを許可する前に、まず S3 データと同じ AWS リージョン に S3 Access Grants インスタンスを作成する必要があります。

前提条件

社内ディレクトリのアイデンティティを使用して S3 データへのアクセスを許可する場合は、AWS IAM Identity Center に社内アイデンティティディレクトリを追加します。まだ追加の準備が整っていない場合は、後で S3 Access Grants インスタンスを IAM アイデンティティセンターインスタンスに関連付けることができます。

S3 Access Grants インスタンスを作成するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。

2. ナビゲーションバーで、現在表示されている AWS リージョン の名前をクリックします。次に、切り替え先のリージョンを選択します。
3. 左側のナビゲーションペインで、[Access Grants] を選択します。
4. [S3 Access Grants] ページで、[Create S3 Access Grants instance] をクリックします。

   a. [Access Grants インスタンスをセットアップ] ウィザードの [ステップ 1] で、現在の AWS リージョン でインスタンスを作成することを確認します。S3 データが配置されているのと同じ AWS リージョン であることを確認します。作成できるのは、アカウントにつき AWS リージョン ごとに単一の S3 Access Grants インスタンス です。

   b. (オプション) AWS IAM Identity Center に 社内アイデンティティディレクトリを追加した場合は、社内ディレクトリのこの IAM アイデンティティセンターインスタンスを S3 Access Grants インスタンスに関連付けることができます。

      これを実行するには、[Add IAM Identity Center instance in ***region***] を選択します。次に、IAM アイデンティティセンターインスタンスの Amazon リソースネーム (ARN) を入力します。

      社内ディレクトリを IAM アイデンティティセンターにまだ追加していない場合は、後で S3 Access Grants インスタンスを IAM アイデンティティセンターインスタンスに関連付けることができます。

   c. S3 Access Grants インスタンスを作成するには、[次へ] をクリックします。ロケーションの登録については、「ステップ 2 - ロケーションを登録する」を参照してください。
5. [次へ] または [Create S3 Access Grants instance] が無効になっている場合:

   インスタンスは作成できません

   - 同じ AWS リージョン に S3 Access Grants インスタンスが既にある可能性があります。左側のナビゲーションペインで、[Access Grants] を選択します。[S3 Access Grants] ページで、[S3 Access Grants instance in your account] セクションまで下にスクロールして、インスタンスが既に存在しているかを確認します。
   - S3 Access Grants インスタンスを作成するのに必要な `s3:CreateAccessGrantsInstance` アクセス許可がない可能性があります。アカウント管理者に連絡してください。IAM アイデンティティセンターインスタンスを S3 Access Grants インスタンスに関連付ける場合に必要な追加のアクセス許可については、「CreateAccessGrantsInstance」を参照してください。

AWS CLI を使用する場合

AWS CLI をインストールするには、「AWS Command Line Interface ユーザーガイド」の「AWS CLI をインストールする」を参照してください。

次のコマンド例を使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

Example S3 Access Grants インスタンスを作成する

```
aws s3control create-access-grants-instance \
--account-id 111122223333 \
--region us-east-2
```

レスポンス:

```
{
    "CreatedAt": "2023-05-31T17:54:07.893000+00:00",
    "AccessGrantsInstanceId": "default",
    "AccessGrantsInstanceArn": "arn:aws:s3:us-east-2:111122223333:access-grants/
default"
}
```

REST API の使用

Amazon S3 REST API を使用して S3 Access Grants インスタンスを作成できます。REST API での ACL の管理のサポートの詳細については、「Amazon Simple Storage Service API リファレンス」の次のセクションを参照してください。

- AssociateAccessGrantsIdentityCenter
- CreateAccessGrantsInstance
- DeleteAccessGrantsInstance
- DissociateAccessGrantsIdentityCenter
- GetAccessGrantsInstance
- GetAccessGrantsInstanceForPrefix
- GetAccessGrantsInstanceResourcePolicy
- ListAccessGrantsInstances
- PutAccessGrantsInstanceResourcePolicy

AWS SDK の使用

このセクションでは、AWS SDK を使用して S3 Access Grants インスタンスを作成する方法の例を説明します。

Java

この例では、個別のアクセス許可のコンテナとして機能する S3 Access Grants インスタンスを作成します。作成できるのは、アカウントにつき AWS リージョン ごとに単一の S3 Access Grants インスタンスです。応答には、S3 Access Grants インスタンス用に生成されたインスタンス ID `default` と Amazon リソースネーム (ARN) が含まれます。

Example S3 Access Grants インスタンスリクエストを作成する

```
public void createAccessGrantsInstance() {
CreateAccessGrantsInstanceRequest createRequest =
 CreateAccessGrantsInstanceRequest.builder().accountId("111122223333").build();
CreateAccessGrantsInstanceResponse createResponse =
 s3Control.createAccessGrantsInstance(createRequest);LOGGER.info("CreateAccessGrantsInstance
 " + createResponse);
}
```

レスポンス:

```
CreateAccessGrantsInstanceResponse(
CreatedAt=2023-06-07T01:46:20.507Z,
AccessGrantsInstanceId=default,
AccessGrantsInstanceArn=arn:aws:s3:us-east-2:111122223333:access-grants/default)
```

S3 Access Grants インスタンスの詳細を取得する

特定の AWS リージョン の Amazon S3 Access Grants インスタンスの詳細を取得できます。Amazon S3 コンソール、AWS Command Line Interface、(AWS CLI)、Amazon S3 REST API、AWS SDK を使用して S3 Access Grants インスタンスの詳細を取得できます。

S3 コンソールの使用

S3 Access Grants インスタンスの詳細を取得する方法

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。

2. 左側のナビゲーションペインで、[Access Grants] を選択します。
3. [S3 Access Grants] ページで、取り組む S3 Access Grants インスタンスが含まれるリージョンを選択します。
4. [S3 Access Grants] ページには、S3 Access Grants インスタンスと、アカウントと共有されているクロスアカウントインスタンスが一覧表示されます。インスタンスの詳細を表示するには、[詳細の表示] を選択します。

AWS CLI を使用する場合

AWS CLI をインストールするには、「AWS Command Line Interface ユーザーガイド」の「AWS CLI をインストールする」を参照してください。

次のコマンド例を使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

Example — S3 Access Grants インスタンスの詳細を取得する

```
aws s3control get-access-grants-instance \
 --account-id 111122223333 \
 --region us-east-2
```

レスポンス:

```
{
    "AccessGrantsInstanceArn": "arn:aws:s3:us-east-2: 111122223333:access-grants/
default",
    "AccessGrantsInstanceId": "default",
    "CreatedAt": "2023-05-31T17:54:07.893000+00:00"
}
```

REST API の使用

Amazon REST API での S3 Access Grants インスタンスの管理のサポートの詳細については、「Amazon Simple Storage Service API リファレンス」の次のセクションを参照してください。

- GetAccessGrantsInstance
- GetAccessGrantsInstanceForPrefix

AWS SDK の使用

このセクションでは、AWS SDK を使用して S3 Access Grants インスタンスの詳細を取得する方法の例を説明します。

次の例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

Java

Example – S3 Access Grants インスタンスを取得する

```
public void getAccessGrantsInstance() {
GetAccessGrantsInstanceRequest getRequest = GetAccessGrantsInstanceRequest.builder()
.accountId("111122223333")
.build();
GetAccessGrantsInstanceResponse getResponse =
 s3Control.getAccessGrantsInstance(getRequest);
LOGGER.info("GetAccessGrantsInstanceResponse: " + getResponse);
}
```

レスポンス:

```
GetAccessGrantsInstanceResponse(
AccessGrantsInstanceArn=arn:aws:s3:us-east-2: 111122223333:access-grants/default,
CreatedAt=2023-06-07T01:46:20.507Z)
```

S3 Access Grants インスタンスを一覧表示する

AWS Resource Access Manager (AWS RAM) で共有されたインスタンスなど、S3 Access Grants インスタンスを一覧表示することができます。

Amazon S3 コンソール、AWS Command Line Interface (AWS CLI)、Amazon S3 REST API、AWS SDK を使用することで、S3 Access Grants インスタンスを一覧表示できます。

S3 コンソールの使用

S3 Access Grants インスタンスを一覧表示する方法

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。

2. 左側のナビゲーションペインで、[Access Grants] を選択します。
3. [S3 Access Grants] ページで、取り組む S3 Access Grants インスタンスが含まれるリージョンを選択します。
4. [S3 Access Grants] ページには、S3 Access Grants インスタンスと、アカウントと共有されているクロスアカウントインスタンスが一覧表示されます。インスタンスの詳細を表示するには、[詳細の表示] を選択します。

AWS CLI を使用する場合

AWS CLI をインストールするには、「AWS Command Line Interface ユーザーガイド」の「AWS CLI をインストールする」を参照してください。

次のコマンド例を使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

Example — アカウントのすべての S3 Access Grants インスタンスを一覧表示する

このアクションでは、アカウントのすべての S3 Access Grants インスタンスを一覧表示します。AWS リージョン ごとに単一の S3 Access Grants インスタンスを持つことができます。このアクションでは、アカウントがアクセスできる他のクロスアカウント S3 Access Grants インスタンスも一覧表示されます。

```
aws s3control list-access-grants-instances \
 --account-id 111122223333 \
 --region us-east-2
```

レスポンス:

```
{
    "AccessGrantsInstanceArn": "arn:aws:s3:us-east-2: 111122223333:access-grants/
default",
    "AccessGrantsInstanceId": "default",
    "CreatedAt": "2023-05-31T17:54:07.893000+00:00"
}
```

REST API の使用

Amazon REST API での S3 Access Grants インスタンスの管理のサポートの詳細については、「Amazon Simple Storage Service API リファレンス」の次のセクションを参照してください。

- ListAccessGrantsInstances

AWS SDK の使用

このセクションでは、AWS SDK を使用して S3 Access Grants インスタンスの詳細を取得する方法の例を説明します。

次の例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

Java

Example — アカウントのすべての S3 Access Grants インスタンスを一覧表示する

このアクションでは、アカウントのすべての S3 Access Grants インスタンスを一覧表示します。リージョンごとに単一の S3 Access Grants インスタンスを持つことができます。このアクションでは、アカウントがアクセスできる他のクロスアカウント S3 Access Grants インスタンスも一覧表示されます。

```
public void listAccessGrantsInstances() {
ListAccessGrantsInstancesRequest listRequest =
 ListAccessGrantsInstancesRequest.builder()
.accountId("111122223333")
.build();
ListAccessGrantsInstancesResponse listResponse =
 s3Control.listAccessGrantsInstances(listRequest);
LOGGER.info("ListAccessGrantsInstancesResponse: " + listResponse);
}
```

レスポンス:

```
ListAccessGrantsInstancesResponse(
AccessGrantsInstancesList=[
ListAccessGrantsInstanceEntry(
AccessGrantsInstanceId=default,
AccessGrantsInstanceArn=arn:aws:s3:us-east-2:111122223333:access-grants/default,
CreatedAt=2023-06-07T04:28:11.728Z
)
]
)
```

IAM アイデンティティセンターインスタンスの関連付けまたは関連付けを解除します。

Amazon S3 Access Grants では、企業アイデンティティディレクトリの AWS IAM Identity Center インスタンスを S3 Access Grants インスタンスに関連付けることができます。その後、社内ユーザーとグループ、AWS Identity and Access Management (IAM) ユーザーとロールにアクセス権限を作成できます。

社内ディレクトリのユーザーとグループにアクセス権限を作成する必要がなくなった場合は、IAM アイデンティティセンターインスタンスと S3 Access Grants インスタンスの関連付けを解除できます。

Amazon S3 コンソール、AWS Command Line Interface (AWS CLI)、Amazon S3 REST API、AWS SDK を使用して、IAM アイデンティティセンターインスタンスを関連付けたり、関連付けを解除したりできます。

S3 コンソールの使用

IAM アイデンティティセンターインスタンスを S3 Access Grants インスタンスに関連付ける前に、社内アイデンティティディレクトリを IAM アイデンティティセンターに追加する必要があります。詳細については、「the section called “S3 Access Grants と社内ディレクトリのアイデンティティ”」を参照してください。

IAM アイデンティティセンターインスタンスを S3 アクセス許可インスタンスに関連付けるには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[Access Grants] を選択します。
3. [S3 Access Grants] ページで、取り組む S3 Access Grants インスタンスが含まれるリージョンを選択します。
4. インスタンスの [詳細の表示] をクリックします。
5. 詳細ページの [IAM アイデンティティセンター] セクションで、IAM アイデンティティセンターインスタンスを [追加] するか、既に IAM アイデンティティセンターインスタンスに関連付けられているインスタンスを [登録解除] します。

AWS CLI を使用する場合

AWS CLI をインストールするには、「AWS Command Line Interface ユーザーガイド」の「AWS CLI をインストールする」を参照してください。

次のコマンド例を使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

Example – IAM アイデンティティセンターインスタンスを S3 アクセス許可インスタンスに関連付ける

```
aws s3control associate-access-grants-identity-center \
 --account-id 111122223333 \
 --identity-center-arn arn:aws:sso:::instance/ssoins-1234a567bb89012c \
 --profile access-grants-profile \
 --region eu-central-1

// No response body
```

Example – IAM アイデンティティセンターインスタンスの S3 アクセス許可インスタンスへの関連付けを解除する

```
aws s3control dissociate-access-grants-identity-center \
 --account-id 111122223333 \
 --profile access-grants-profile \
 --region eu-central-1

// No response body
```

REST API の使用

Amazon S3 REST API での IAM アイデンティティセンターと S3 Access Grants 間の関連付けの管理のサポートの詳細については、「Amazon Simple Storage Service API リファレンス」の次のセクションを参照してください。

- AssociateAccessGrantsIdentityCenter
- DissociateAccessGrantsIdentityCenter

S3 Access Grants インスタンスを削除する

削除できるのは、アカウントの AWS リージョン の S3 Access Grants インスタンスです。ただし、S3 Access Grants インスタンスを削除する前に、まず次を完了する必要があります。

- S3 Access Grants インスタンス内の (すべての権限と口ケーションを含む) すべてのリソースを削除します。詳細については、「権限を削除する」と「口ケーションを削除する」を参照してください。
- AWS IAM Identity Center インスタンスを S3 Access Grants インスタンスに関連付けた場合は、IAM アイデンティティセンターインスタンスの関連付けを解除する必要があります。詳細については、「IAM アイデンティティセンターインスタンスの関連付けまたは関連付けの解除」を参照してください。

> **Important**
>
> S3 Access Grants インスタンスの削除は永続的であり、元に戻すことができません。この S3 Access Grants インスタンスの権限を通じてアクセス権を付与されたすべての権限被付与者は、S3 データにアクセスできなくなります。

Amazon S3 コンソール、AWS Command Line Interface、(AWS CLI)、AWS SDK、または Amazon S3 REST API を使用して S3 Storage Lens グループを削除できます。

S3 コンソールの使用

S3 Access Grants インスタンスを削除するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[Access Grants] を選択します。
3. [S3 Access Grants] ページで、取り組む S3 Access Grants インスタンスが含まれるリージョンを選択します。
4. インスタンスの [詳細の表示] をクリックします。
5. インスタンスの詳細ページで、右上隅の [インスタンスを削除] を選択します。
6. 表示されたダイアログボックスで、[削除] を選択します。この操作は元に戻すことができません。

AWS CLI を使用する場合

AWS CLI をインストールするには、「AWS Command Line Interface ユーザーガイド」の「AWS CLI をインストールする」を参照してください。

次のコマンド例を使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

> **Note**
>
> S3 Access Grants インスタンスを削除する前に、まず S3 Access Grants インスタンス内で作成されたすべての権限と口ケーションを削除する必要があります。IAM アイデンティティセンターインスタンスを S3 Access Grants インスタンスに関連付けている場合は、まずその関連付けを解除する必要があります。

Example – S3 Access Grants インスタンスを削除する

```
aws s3control delete-access-grants-instance \
--account-id 111122223333 \
--profile access-grants-profile \
--region us-east-2 \
--endpoint-url https://s3-control.us-east-2.amazonaws.com \

 // No response body
```

REST API の使用

Amazon REST API での S3 Access Grants インスタンスの削除のサポートの詳細については、「Amazon Simple Storage Service API リファレンス」の「DeleteAccessGrantsInstance」を参照してください。

AWS SDK の使用

このセクションでは、AWS SDK を使用して S3 Access Grants インスタンスを作成する方法の例を説明します。

次の例を使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

Java

> **Note**
>
> S3 Access Grants インスタンスを削除する前に、まず S3 Access Grants インスタンス内で作成されたすべての権限と口ケーションを削除する必要があります。IAM アイデンティティセンターインスタンスを S3 Access Grants インスタンスに関連付けている場合は、まずその関連付けを解除する必要があります。

Example – S3 Access Grants インスタンスを削除する

```
public void deleteAccessGrantsInstance() {
DeleteAccessGrantsInstanceRequest deleteRequest =
 DeleteAccessGrantsInstanceRequest.builder()
.accountId("111122223333")
.build();
DeleteAccessGrantsInstanceResponse deleteResponse =
 s3Control.deleteAccessGrantsInstance(deleteRequest);
LOGGER.info("DeleteAccessGrantsInstanceResponse: " + deleteResponse);
}
```

S3 Access Grants 口ケーションの使用

アカウントの AWS リージョンで Amazon S3 Access Grants インスタンスを作成 したら、そのインスタンスに S3 口ケーションを登録できます。S3 Access Grants の口ケーションは、デフォルトの S3 口ケーション (`s3://`) 、バケット、またはプレフィックスを AWS Identity and Access Management (IAM) ロールにマッピングします。S3 Access Grants は、この IAM ロールを引き受けて、その特定の場所にアクセスする被付与者に一時的な認証情報を提供します。アクセス権限を作成する前に、まず S3 Access Grants インスタンスに少なくとも 1 つの口ケーションを登録する必要があります。

口ケーションの登録、口ケーションの詳細の表示、口ケーションの編集、口ケーションの削除を行うことができます。

> **Note**
>
> S3 Access Grants インスタンスに最初の口ケーションを登録しても、インスタンスに個別のアクセス権限はありません。アクセス権限を作成するには、「権限を作成する」を参照してください。

トピック

- 口ケーションを登録する
- 登録済み口ケーションの詳細を表示する
- 登録された口ケーションを更新する
- 登録された口ケーションを削除する

口ケーションを登録する

アカウントの AWS リージョンで Amazon S3 Access Grants インスタンスを作成 したら、そのインスタンスに S3 口ケーションを登録できます。S3 Access Grants の口ケーションは、デフォルトの S3 口ケーション (`s3://`) 、バケット、またはプレフィックスを AWS Identity and Access Management (IAM) ロールにマッピングします。S3 Access Grants は、この IAM ロールを引き受けて、その特定の場所にアクセスする被付与者に一時的な認証情報を提供します。アクセス権限を作成する前に、まず S3 Access Grants インスタンスに少なくとも 1 つの口ケーションを登録する必要があります。

推奨されるユースケース

デフォルトの口ケーション (`s3://`) を登録し、IAM ロールにマッピングすることをお勧めします。デフォルトの S3 パスの口ケーション (`s3://`) を使用すると、アカウントの AWS リージョン内のすべての S3 バケットへのアクセスがカバーされます。アクセス権限を作成するときに、権限の範囲をデフォルトの口ケーション内のバケット、プレフィックス、またはオブジェクトに絞り込むことができます。

アクセス管理が複雑なユースケース

より複雑なアクセス管理のユースケースでは、デフォルトの口ケーション以外の登録が必要になる場合があります。例として、次のようなユースケースが挙げられます。

- *amzn-s3-demo-bucket* が S3 Access Grants インスタンスの登録済み口ケーションで、IAM ロールがマッピングされているが、この IAM ロールがバケット内の特定のプレフィックスへの

アクセスを拒否されるとします。この場合、IAM ロールがアクセスできないプレフィックスを別の ロケーションとして登録し、そのロケーションを、必要なアクセス権を持つ別の IAM ロールにマッピングできます。

- 仮想プライベートクラウド (VPC) エンドポイント内のユーザーのみにアクセスを制限する権限を作成するとします。この場合、IAM ロールで VPC エンドポイントのみにアクセスを制限するバケットのロケーションを登録できます。後で、被付与者が S3 Access Grants に認証情報を要求すると、S3 Access Grants はロケーションの IAM ロールを引き受けて一時的な認証情報を提供します。この認証情報は、呼び出し元が VPC エンドポイント内のユーザーでない限り、特定のバケットへのアクセスを拒否します。こうした拒否のアクセス許可は、権限で指定された通常の READ、WRITE、または READWRITE のアクセス許可に加えて適用されます。

ロケーションを登録するときには、S3 Access Grants が一時的な認証情報を提供したり、特定の権限のアクセス許可の範囲を設定したりするために引き受ける IAM ロールも指定する必要があります。

ユースケースで S3 Access Grants インスタンスに複数のロケーションを登録する必要がある場合は、次のいずれかを登録できます。

S3 URI	IAM ロール	説明
`s3://`	*Default-IAM-role*	デフォルトのロケーション `s3://` には、AWS リージョン 内のすべてのバケットが含まれます。
`s3://`*amzn-s3-demo-bucket1* `/`	*IAM-role-For-bucket*	このロケーションには、指定したバケット内のすべてのオブジェクトが含まれます。
`s3://`*amzn-s3-demo-bucket1* `/`*prefix-name*	*IAM-role-For-prefix*	このロケーションには、指定されたプレフィックスで始まるオブジェクトキー名を持つ、バケット内のすべてのオブジェクトが含まれます。

特定のバケットまたはプレフィックスを登録する前に、次の手順を実行する必要があります。

- アクセスを許可するデータを含むバケットを 1 つまたは複数作成します。これらのバケットは、S3 Access Grants インスタンスと同じ AWS リージョン にある必要があります。詳細については、「バケットの作成」を参照してください。

プレフィックスの追加はオプションの手順です。プレフィックスは、オブジェクトキー名の先頭にある文字列で、これらを使用して、バケット内のオブジェクトを整理したり、アクセスを管理したりできます。バケットにプレフィックスを追加するには、「オブジェクトキー名の作成」を参照してください。

- AWS リージョン内の S3 データにアクセスするためのアクセス権限を持つ IAM ロールを作成します。詳細については、「AWS IAM Identity Centerユーザーガイド」の「IAM ロールの作成」を参照してください。
- IAM ロールの信頼ポリシーで、作成した IAM ロールに対して、S3 Access Grants サービス (`access-grants.s3.amazonaws.com`) のプリンシパルアクセス権を付与します。これを実行するために、次のステートメントを含む JSON ファイルを作成できます。アカウントに信頼ポリシーを追加するには、「カスタム信頼ポリシーを使用したロールの作成」を参照してください。

  TestRolePolicy.json

```
{
  "Version": "2012-10-17",
    "Statement": [
    {
      "Sid": "Stmt1234567891011",
      "Effect": "Allow",
      "Principal": {
        "Service":"access-grants.s3.amazonaws.com"
      },
      "Action": [
        "sts:AssumeRole",
        "sts:SetSourceIdentity"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount":"accountId",
          "aws:SourceArn":"arn:aws:s3:region:accountId:access-grants/default"
        }
      }
    },
    //Optionally, for an IAM Identity Center use case, add:
    {
      "Sid": "Stmt1234567891012",
        "Effect": "Allow",
        "Principal": {
          "Service": "access-grants.s3.amazonaws.com"
```

```
        },
        "Action": "sts:SetContext",
        "Condition":{
          "StringEquals":{
            "aws:SourceAccount":"accountId",
            "aws:SourceArn":"arn:aws:s3:region:accountId:access-grants/default"
          },
          "ForAllValues:ArnEquals": {
            "sts:RequestContextProviders":"arn:aws:iam::aws:contextProvider/
IdentityCenter"
          }
        }
      }
  ]
}
```

- 作成した IAM ロールに Amazon S3 アクセス許可をアタッチする IAM ポリシーを作成します。次の `iam-policy.json` ファイルを例に s h じて、*`user input placeholders`* を実際の情報と置き換えます。

> **Note**
>
> - 次の例では、AWS Key Management Service (AWS KMS) キーによるサーバー側の暗号化を使用してデータを暗号化する場合に、ポリシーに IAM ロールに必要な AWS KMS アクセス許可を含めています。この機能を使用しない場合は、IAM ポリシーからこのようなアクセス許可を削除できます。
> - IAM ロールが S3 データにアクセスするように制限できるのは、S3 Access Grants が認証情報を提供する場合に限られます。この例では、特定の S3 Access Grants インスタンスに `Condition` ステートメントを追加する方法を説明します。この `Condition` を使用するには、`Condition` ステートメント内の S3 Access Grants インスタンス ARN を、`arn:aws:s3:`*`region`*`:`*`accountId`*`:access-grants/default` の形式の S3 Access Grants インスタンス ARN に置き換えます。

iam-policy.json

```
{
   "Version":"2012-10-17",
   "Statement": [
```

```
        {
          "Sid": "ObjectLevelReadPermissions",
          "Effect":"Allow",
          "Action":[
             "s3:GetObject",
             "s3:GetObjectVersion",
             "s3:GetObjectAcl",
             "s3:GetObjectVersionAcl",
             "s3:ListMultipartUploadParts"
          ],
          "Resource":[
             "arn:aws:s3:::*"
          ],
          "Condition":{
             "StringEquals": { "aws:ResourceAccount": "accountId" },
             "ArnEquals": {
                 "s3:AccessGrantsInstanceArn": ["arn:aws:s3:region:accountId:access-
grants/default"]
             }
          }
       },
       {
          "Sid": "ObjectLevelWritePermissions",
          "Effect":"Allow",
          "Action":[
             "s3:PutObject",
             "s3:PutObjectAcl",
             "s3:PutObjectVersionAcl",
             "s3:DeleteObject",
             "s3:DeleteObjectVersion",
             "s3:AbortMultipartUpload"
          ],
          "Resource":[
             "arn:aws:s3:::*"
          ],
          "Condition":{
             "StringEquals": { "aws:ResourceAccount": "accountId" },
             "ArnEquals": {
                 "s3:AccessGrantsInstanceArn": ["arn:aws:s3:AWS ####
#:accountId:access-grants/default"]
             }
          }
       },
       {
```

```
         "Sid": "BucketLevelReadPermissions",
         "Effect":"Allow",
         "Action":[
            "s3:ListBucket"
         ],
         "Resource":[
            "arn:aws:s3:::*"
         ],
         "Condition":{
            "StringEquals": { "aws:ResourceAccount": "accountId" },
            "ArnEquals": {
                "s3:AccessGrantsInstanceArn": ["arn:aws:s3:AWS ####
#:accountId:access-grants/default"]
            }
         }
      },
   //Optionally add the following section if you use SSE-KMS encryption
      {
         "Sid": "KMSPermissions",
         "Effect":"Allow",
         "Action":[
            "kms:Decrypt",
            "kms:GenerateDataKey"
         ],
         "Resource":[
            "*"
         ]
      }
   ]
}
```

Amazon S3 コンソール、AWS Command Line Interface、(AWS CLI)、AWS SDK、または Amazon S3 REST API を使用して S3 Access Grants インスタンスにロケーションを登録できます。

> **Note**
>
> S3 Access Grants インスタンスに最初のロケーションを登録しても、インスタンスに個別のアクセス権限はありません。アクセス権限を作成するには、「権限を作成する」を参照してください。

S3 コンソールの使用

S3 Access Grants を使用して S3 データへのアクセスを許可するには、少なくとも 1 つのロケーションを登録しておく必要があります。

S3 Access Grants インスタンスでロケーションを登録するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[Access Grants] を選択します。
3. [S3 Access Grants] ページで、取り組む S3 Access Grants インスタンスが含まれるリージョンを選択します。

   S3 Access Grants インスタンスを初めて使用する場合は、「Step 1 - S3 Access Grants インスタンスを作成する」を実行し、[Access Grants インスタンスをセットアップ] ウィザードの [ステップ 2] に進んでいる必要があります。S3 Access Grants インスタンスが既にある場合は、[詳細の表示] を選択して、[ロケーション] タブで、[ロケーションを登録] をクリックします。

   a. [ロケーション範囲] では、[Browse S3] をクリックするか、登録先のロケーションへの S3 URI パスを入力します。S3 URI の形式については、ロケーション形式 表を参照してください。URI の入力後、[表示] をクリックして、ロケーションを参照します。
   b. [IAM ロール] で、次のいずれかを選択します。

      - 既存の IAM ロールから選択

        ドロップダウンリストから IAM ロールを選択します。ロールを選択したら、[表示] を選択して、登録するロケーションを管理するのに必要なアクセス許可がこのロールにあることを確認します。具体的には、このロールが S3 Access Grants にアクセス許可 `sts:AssumeRole` と `sts:SetSourceIdentity` を付与していることを確認します。
      - IAM ロールの ARN の入力

        [IAM コンソール] に入ります。IAM ロールの Amazon リソースネーム (ARN) をコピーして、このボックスに貼り付けます。
   c. 終了するには、[次へ] または [ロケーションを登録] を選択します。
4. トラブルシューティング:

   ロケーションを登録できない

   - そのロケーションが既に登録されている可能性があります。

ロケーションを登録する `s3:CreateAccessGrantsLocation` アクセス許可がない可能性があります。アカウント管理者に連絡してください。

AWS CLI を使用する場合

AWS CLI をインストールするには、「AWS Command Line Interface ユーザーガイド」の「AWS CLI をインストールする」を参照してください。

S3 Access Grants インスタンスには`s3://`、デフォルトの場所、またはカスタムロケーションを登録できます。その場所へのプリンシパルアクセス権を持つ IAM ロールを作成し、次に S3 Access Grants にこのロールを引き受ける権限を付与する必要があります。

次のコマンド例を使用する際は、*`user input placeholders`* をユーザー自身の情報に置き換えます。

Example リソースポリシーを作成する

S3 Access Grants が IAM ロールを引き受けることを許可するポリシーを作成します。これを実行するために、次のステートメントを含む JSON ファイルを作成できます。リソースポリシーをアカウントに追加するには、「最初のカスタマー管理ポリシーの作成とアタッチ」を参照してください。

TestRolePolicy.json

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1234567891011",
      "Action": ["sts:AssumeRole", "sts:SetSourceIdentity"],
      "Effect": "Allow",
      "Principal": {"Service":"access-grants.s3.amazonaws.com"}
    }
  ]
}
```

Example ロールを作成する

次の IAM コマンドを実行して、ロールを作成します。

```
aws iam create-role --role-name accessGrantsTestRole \
 --region us-east-2 \
 --assume-role-policy-document file://TestRolePolicy.json
```

create-role コマンドを実行すると、次のとおりポリシーが返されます。

```
{
    "Role": {
        "Path": "/",
        "RoleName": "accessGrantsTestRole",
        "RoleId": "AROASRDGX4WM4GH55GIDA",
        "Arn": "arn:aws:iam::111122223333:role/accessGrantsTestRole",
        "CreateDate": "2023-05-31T18:11:06+00:00",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Sid": "Stmt1685556427189",
                    "Action": [
                        "sts:AssumeRole",
                        "sts:SetSourceIdentity"
                    ],
                    "Effect": "Allow",
                    "Principal": {
                        "Service":"access-grants.s3.amazonaws.com"
                    }
                }
            ]
        }
    }
}
```

Example

Amazon S3 バケットへのアクセス許可を持つ IAM ポリシーを作成します。次の iam-policy.json ファイルを例に s h じて、*user input placeholders* を実際の情報と置き換えます。

> **Note**
>
> AWS Key Management Service (AWS KMS) キーによるサーバー側の暗号化を使用してデータを暗号化する場合、次の例ではポリシーに IAM ロールに必要な AWS KMS アクセス許可

を追加します。この機能を使用しない場合は、IAM ポリシーからこのようなアクセス許可を削除できます。
認証情報が S3 Access Grants によって提供される場合、IAM ロールが S3 内のデータへのアクセスにのみ使用できるようにするために、この例では、S3 Access Grants インスタンス (`s3:AccessGrantsInstance: InstanceArn`) を指定する Condition ステートメントを IAM ポリシーに追加する方法を示します。次のコマンド例を使用する際は、*user input placeholders* をユーザー自身の情報に置き換えます。

iam-policy.json

```
{
   "Version":"2012-10-17",
   "Statement": [
       {
         "Sid": "ObjectLevelReadPermissions",
         "Effect":"Allow",
         "Action":[
            "s3:GetObject",
            "s3:GetObjectVersion",
            "s3:GetObjectAcl",
            "s3:GetObjectVersionAcl",
            "s3:ListMultipartUploadParts"
         ],
         "Resource":[
            "arn:aws:s3:::*"
         ],
         "Condition":{
            "StringEquals": { "aws:ResourceAccount": "accountId" },
            "ArnEquals": {
                "s3:AccessGrantsInstanceArn": ["arn:aws:s3:region:accountId:access-
grants/default"]
            }
        }
      },
      {
         "Sid": "ObjectLevelWritePermissions",
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:PutObjectAcl",
```

```
            "s3:PutObjectVersionAcl",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion",
            "s3:AbortMultipartUpload"
         ],
         "Resource":[
            "arn:aws:s3:::*"
         ],
         "Condition":{
            "StringEquals": { "aws:ResourceAccount": "accountId" },
            "ArnEquals": {
                "s3:AccessGrantsInstanceArn": ["arn:aws:s3:AWS #####:accountId:access-
grants/default"]
            }
         }
      },
      {
         "Sid": "BucketLevelReadPermissions",
         "Effect":"Allow",
         "Action":[
            "s3:ListBucket"
         ],
         "Resource":[
            "arn:aws:s3:::*"
         ],
         "Condition":{
            "StringEquals": { "aws:ResourceAccount": "accountId" },
            "ArnEquals": {
                "s3:AccessGrantsInstanceArn": ["arn:aws:s3:AWS #####:accountId:access-
grants/default"]
            }
         }
      },
      {
         "Sid": "KMSPermissions",
         "Effect":"Allow",
         "Action":[
            "kms:Decrypt",
            "kms:GenerateDataKey"
         ],
         "Resource":[
            "*"
         ]
      }
```

```
    ]
}
```

Example

次のコマンドを実行してください。

```
aws iam put-role-policy \
--role-name accessGrantsTestRole \
--policy-name accessGrantsTestRole \
--policy-document file://iam-policy.json
```

Example デフォルトロケーションを登録します。

```
aws s3control create-access-grants-location \
 --account-id 111122223333 \
 --location-scope s3:// \
 --iam-role-arn arn:aws:iam::111122223333:role/accessGrantsTestRole
```

レスポンス:

```
{"CreatedAt": "2023-05-31T18:23:48.107000+00:00",
    "AccessGrantsLocationId": "default",
    "AccessGrantsLocationArn": "arn:aws:s3:us-east-2:111122223333:access-grants/
default/location/default",
    "LocationScope": "s3://"
    "IAMRoleArn": "arn:aws:iam::111122223333:role/accessGrantsTestRole"
}
```

Example カスタムロケーションを登録する

```
aws s3control create-access-grants-location \
 --account-id 111122223333 \
 --location-scope s3://DOC-BUCKET-EXAMPLE/ \
 --iam-role-arn arn:aws:iam::123456789012:role/accessGrantsTestRole
```

レスポンス:

```
{"CreatedAt": "2023-05-31T18:23:48.107000+00:00",
    "AccessGrantsLocationId": "635f1139-1af2-4e43-8131-a4de006eb456",
    "AccessGrantsLocationArn": "arn:aws:s3:us-east-2: 111122223333:access-grants/
default/location/635f1139-1af2-4e43-8131-a4de006eb888",
```

```
    "LocationScope": "s3://DOC-BUCKET-EXAMPLE/",
    "IAMRoleArn": "arn:aws:iam::111122223333:role/accessGrantsTestRole"
}
```

REST API の使用

Amazon S3 REST API での S3 Access Grants インスタンスの管理のサポートの詳細については、「Amazon Simple Storage Service API リファレンス」の次のセクションを参照してください。

- CreateAccessGrantsLocation
- DeleteAccessGrantsLocation
- GetAccessGrantsLocation
- ListAccessGrantsLocations
- UpdateAccessGrantsLocation

AWS SDK の使用

このセクションでは、AWS SDK を使用してロケーションを登録する方法の例を説明します。

次の例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

Java

S3 Access Grants インスタンスにはs3://、デフォルトの場所、またはカスタムロケーションを登録できます。その場所へのプリンシパルアクセス権を持つ IAM ロールを作成し、次に S3 Access Grants にこのロールを引き受ける権限を付与する必要があります。

次のコマンド例を使用する際は、*user input placeholders* をユーザー自身の情報に置き換えます。

Example デフォルトロケーションを登録する

リクエスト:

```
public void createAccessGrantsLocation() {
CreateAccessGrantsLocationRequest createRequest =
 CreateAccessGrantsLocationRequest.builder()
.accountId("111122223333")
.locationScope("s3://")
.iamRoleArn("arn:aws:iam::123456789012:role/accessGrantsTestRole")
.build();
```

```
CreateAccessGrantsLocationResponse createResponse =
 s3Control.createAccessGrantsLocation(createRequest);
LOGGER.info("CreateAccessGrantsLocationResponse: " + createResponse);
}
```

レスポンス:

```
CreateAccessGrantsLocationResponse(
CreatedAt=2023-06-07T04:35:11.027Z,
AccessGrantsLocationId=default,
AccessGrantsLocationArn=arn:aws:s3:us-east-2:111122223333:access-grants/default/
location/default,
LocationScope=s3://,
IAMRoleArn=arn:aws:iam::111122223333:role/accessGrantsTestRole
)
```

Example カスタムロケーションを登録する

リクエスト:

```
public void createAccessGrantsLocation() {
CreateAccessGrantsLocationRequest createRequest =
 CreateAccessGrantsLocationRequest.builder()
.accountId("111122223333")
.locationScope("s3://DOC-BUCKET-EXAMPLE/")
.iamRoleArn("arn:aws:iam::111122223333:role/accessGrantsTestRole")
.build();
CreateAccessGrantsLocationResponse createResponse =
 s3Control.createAccessGrantsLocation(createRequest);
LOGGER.info("CreateAccessGrantsLocationResponse: " + createResponse);
}
```

レスポンス:

```
CreateAccessGrantsLocationResponse(
CreatedAt=2023-06-07T04:35:10.027Z,
AccessGrantsLocationId=18cfe6fb-eb5a-4ac5-aba9-8d79f04c2012,
AccessGrantsLocationArn=arn:aws:s3:us-east-2:111122223333:access-grants/default/
location/18cfe6fb-eb5a-4ac5-aba9-8d79f04c2666,
LocationScope= s3://test-bucket-access-grants-user123/,
IAMRoleArn=arn:aws:iam::111122223333:role/accessGrantsTestRole
)
```

登録済みロケーションの詳細を表示する

Amazon S3 コンソール、AWS Command Line Interface (AWS CLI)、Amazon S3 REST API、AWS SDK を使用して、S3 Access Grants インスタンスに登録されているロケーションの詳細を取得できます。

S3 コンソールの使用

S3 Access Grants インスタンスに登録済みのロケーションを表示するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[Access Grants] を選択します。
3. [S3 Access Grants] ページで、取り組む S3 Access Grants インスタンスが含まれるリージョンを選択します。
4. インスタンスの [詳細の表示] をクリックします。
5. インスタンスの詳細ページで、[ロケーション] タブをクリックします。
6. 確認する登録済みのロケーションを検索します。登録済みロケーションの一覧にフィルターを適用するには、検索ボックスを使用します。

AWS CLI を使用する場合

AWS CLI をインストールするには、「AWS Command Line Interface ユーザーガイド」の「AWS CLI をインストールする」を参照してください。

次のコマンド例を使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

Example – 登録済みロケーションの詳細を取得する

```
aws s3control get-access-grants-location \
--account-id 111122223333 \
--access-grants-location-id default
```

レスポンス:

```
{
    "CreatedAt": "2023-05-31T18:23:48.107000+00:00",
```

```
    "AccessGrantsLocationId": "default",
    "AccessGrantsLocationArn": "arn:aws:s3:us-east-2:111122223333:access-grants/
default/location/default",
    "IAMRoleArn": "arn:aws:iam::111122223333:role/accessGrantsTestRole"
}
```

Example – S3 Access Grants インスタンスに登録済みの口ケーションをすべて一覧表示する

結果を S3 プレフィックスまたはバケットで限定するには、必要に応じて `--location-scope s3://bucket-and-or-prefix` パラメータを使用できます。

```
aws s3control list-access-grants-locations \
--account-id 111122223333 \
--region us-east-2
```

レスポンス:

```
{"AccessGrantsLocationsList": [
  {
    "CreatedAt": "2023-05-31T18:23:48.107000+00:00",
    "AccessGrantsLocationId": "default",
    "AccessGrantsLocationArn": "arn:aws:s3:us-east-2:111122223333:access-grants/
default/location/default",
    "LocationScope": "s3://"
    "IAMRoleArn": "arn:aws:iam::111122223333:role/accessGrantsTestRole"
     },
  {
    "CreatedAt": "2023-05-31T18:23:48.107000+00:00",
    "AccessGrantsLocationId": "635f1139-1af2-4e43-8131-a4de006eb456",
    "AccessGrantsLocationArn": "arn:aws:s3:us-east-2:111122223333:access-grants/
default/location/635f1139-1af2-4e43-8131-a4de006eb888",
    "LocationScope": "s3://amzn-s3-demo-bucket/prefixA*",
    "IAMRoleArn": "arn:aws:iam::111122223333:role/accessGrantsTestRole"
     }
   ]
  }
```

REST API の使用

Amazon S3 REST API で登録済みの口ケーションの詳細を入手したり、S3 Access Grants インスタンスに登録された口ケーションのすべてを一覧表示する方法の詳細については、「Amazon Simple Storage Service API リファレンス」の次のセクションを参照してください。

- GetAccessGrantsLocation
- ListAccessGrantsLocations

AWS SDK の使用

このセクションでは、AWS SDK を使用して S3 Access Grants インスタンスに登録済みの口ケーションの詳細を取得したり、すべての登録済みの口ケーションを一覧表示する方法の例を説明します。

次の例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

Java

Example – 登録済み口ケーションの詳細を取得する

```
public void getAccessGrantsLocation() {
GetAccessGrantsLocationRequest getAccessGrantsLocationRequest =
 GetAccessGrantsLocationRequest.builder()
.accountId("111122223333")
.accessGrantsLocationId("default")
.build();
GetAccessGrantsLocationResponse getAccessGrantsLocationResponse =
 s3Control.getAccessGrantsLocation(getAccessGrantsLocationRequest);
LOGGER.info("GetAccessGrantsLocationResponse: " + getAccessGrantsLocationResponse);
}
```

レスポンス:

```
GetAccessGrantsLocationResponse(
CreatedAt=2023-06-07T04:35:10.027Z,
AccessGrantsLocationId=default,
AccessGrantsLocationArn=arn:aws:s3:us-east-2:111122223333:access-grants/default/
location/default,
LocationScope= s3://,
IAMRoleArn=arn:aws:iam::111122223333:role/accessGrantsTestRole
)
```

Example – S3 Access Grants インスタンスに登録済みの口ケーションをすべて一覧表示する

結果を S3 プレフィックスまたはバケットで限定するには、必要に応じて `LocationScope` パラメータで `s3://bucket-and-or-prefix` などの S3 URI を使用できます。

```
public void listAccessGrantsLocations() {

ListAccessGrantsLocationsRequest listRequest =
 ListAccessGrantsLocationsRequest.builder()
.accountId("111122223333")
.build();

ListAccessGrantsLocationsResponse listResponse =
 s3Control.listAccessGrantsLocations(listRequest);
LOGGER.info("ListAccessGrantsLocationsResponse: " + listResponse);
}
```

レスポンス:

```
ListAccessGrantsLocationsResponse(
AccessGrantsLocationsList=[
ListAccessGrantsLocationsEntry(
CreatedAt=2023-06-07T04:35:11.027Z,
AccessGrantsLocationId=default,
AccessGrantsLocationArn=arn:aws:s3:us-east-2:111122223333:access-grants/default/
location/default,
LocationScope=s3://,
IAMRoleArn=arn:aws:iam::111122223333:role/accessGrantsTestRole
),
ListAccessGrantsLocationsEntry(
CreatedAt=2023-06-07T04:35:10.027Z,
AccessGrantsLocationId=635f1139-1af2-4e43-8131-a4de006eb456,
AccessGrantsLocationArn=arn:aws:s3:us-east-2:111122223333:access-grants/default/
location/635f1139-1af2-4e43-8131-a4de006eb888,
LocationScope=s3://amzn-s3-demo-bucket/prefixA*,
IAMRoleArn=arn:aws:iam::111122223333:role/accessGrantsTestRole
)
]
)
```

登録されたロケーションを更新する

Amazon S3 Access Grants インスタンスに登録済みのロケーションの AWS Identity and Access Management (IAM) ロールは更新できます。S3 Access Grants にロケーションを登録するために使用する新しい IAM ロールごとに、このロールへの S3 Access Grants サービスプリンシパル (access-grants.s3.amazonaws.com) にアクセス権限を付与する必要があります。これを行うに

は、最初にロケーションを登録 した際に使用したのと同じ信頼ポリシー JSON ファイルに、新しい IAM ロールのエントリを追加します。

Amazon S3 コンソール、AWS Command Line Interface、(AWS CLI)、AWS SDK、または Amazon S3 REST API を使用して S3 Access Grants インスタンスのロケーションを更新できます。

S3 コンソールの使用

Amazon S3 Access Grants インスタンスに登録済みのロケーションの IAM ロールを更新するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[Access Grants] を選択します。
3. [S3 Access Grants] ページで、取り組む S3 Access Grants インスタンスが含まれるリージョンを選択します。
4. インスタンスの [詳細の表示] をクリックします。
5. インスタンスの詳細ページで、[ロケーション] タブをクリックします。
6. 更新するロケーションを検索します。ロケーション一覧にフィルターを適用するには、検索ボックスを使用します。
7. 更新する登録済みのロケーションの隣にあるオプションボタンをクリックします。
8. IAM ロールを更新してから、[変更の保存] をクリックします。

AWS CLI を使用する場合

AWS CLI をインストールするには、「AWS Command Line Interface ユーザーガイド」の「AWS CLI をインストールする」を参照してください。

次のコマンド例を使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

Example – 登録済みロケーションの IAM ロールを更新する

```
aws s3control update-access-grants-location \
--account-id 111122223333 \
--access-grants-location-id 635f1139-1af2-4e43-8131-a4de006eb999 \
--iam-role-arn arn:aws:iam::777788889999:role/accessGrantsTestRole
```

レスポンス:

```
{
    "CreatedAt": "2023-05-31T18:23:48.107000+00:00",
    "AccessGrantsLocationId": "635f1139-1af2-4e43-8131-a4de006eb999",
    "AccessGrantsLocationArn": "arn:aws:s3:us-east-2:777788889999:access-grants/
default/location/635f1139-1af2-4e43-8131-a4de006eb888",
    "LocationScope": "s3://amzn-s3-demo-bucket/prefixB*",
    "IAMRoleArn": "arn:aws:iam::777788889999:role/accessGrantsTestRole"
}
```

REST API の使用

Amazon S3 REST API での S3 Access Grants のロケーション更新のサポートの詳細については、「Amazon Simple Storage Service API リファレンス」の「UpdateAccessGrantsLocation」を参照してください。

AWS SDK の使用

このセクションでは、AWS SDK を使用して登録済みのロケーションを更新する方法の例を説明します。

次の例を使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

Java

Example – 登録済みロケーションのIAM ロールを更新する

```
public void updateAccessGrantsLocation() {
UpdateAccessGrantsLocationRequest updateRequest =
 UpdateAccessGrantsLocationRequest.builder()
.accountId("111122223333")
.accessGrantsLocationId("635f1139-1af2-4e43-8131-a4de006eb999")
.iamRoleArn("arn:aws:iam::777788889999:role/accessGrantsTestRole")
.build();
UpdateAccessGrantsLocationResponse updateResponse =
 s3Control.updateAccessGrantsLocation(updateRequest);
LOGGER.info("UpdateAccessGrantsLocationResponse: " + updateResponse);
}
```

レスポンス:

```
UpdateAccessGrantsLocationResponse(
```

```
CreatedAt=2023-06-07T04:35:10.027Z,
AccessGrantsLocationId=635f1139-1af2-4e43-8131-a4de006eb999,
AccessGrantsLocationArn=arn:aws:s3:us-east-2:777788889999:access-grants/default/
location/635f1139-1af2-4e43-8131-a4de006eb888,
LocationScope=s3://amzn-s3-demo-bucket/prefixB*,
IAMRoleArn=arn:aws:iam::777788889999:role/accessGrantsTestRole
)
```

登録された口ケーションを削除する

S3 Access Grants インスタンスから口ケーション登録を削除することもできます。口ケーションを削除すると、S3 アクセス許可インスタンスから登録が解除されます。

S3 Access Grants インスタンスから口ケーション登録を削除する前に、その口ケーションに関連付けられているすべての権限を削除する必要があります。権限を削除する方法については、「権限を削除する」を参照してください。

Amazon S3 コンソール、AWS Command Line Interface、(AWS CLI)、AWS SDK、または Amazon S3 REST API を使用して S3 Access Grants インスタンスの口ケーションを削除できます。

S3 コンソールの使用

S3 Access Grants インスタンスから口ケーション登録を削除するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[Access Grants] を選択します。
3. [S3 Access Grants] ページで、取り組む S3 Access Grants インスタンスが含まれるリージョンを選択します。
4. インスタンスの [詳細の表示] をクリックします。
5. インスタンスの詳細ページで、[口ケーション] タブをクリックします。
6. 更新する口ケーションを検索します。口ケーション一覧にフィルターを適用するには、検索ボックスを使用します。
7. 削除する登録済みの口ケーションの隣にあるオプションボタンをクリックします。
8. [Deregister] (登録解除) を選択します。
9. この操作は元に戻せないことを警告するダイアログボックスが表示されます。口ケーションを削除するには、[登録解除] を選択します。

AWS CLI を使用する場合

AWS CLI をインストールするには、「AWS Command Line Interface ユーザーガイド」の「AWS CLI をインストールする」を参照してください。

次のコマンド例を使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

Example — ロケーション登録を削除する

```
aws s3control delete-access-grants-location \
--account-id 111122223333 \
--access-grants-location-id  a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
 // No response body
```

REST API の使用

Amazon S3 REST API での S3 Access Grants からのロケーション削除のサポートの詳細については、「Amazon Simple Storage Service API リファレンス」の「DeleteAccessGrantsLocation」を参照してください。

AWS SDK の使用

このセクションでは、AWS SDK を使用してロケーションを削除する方法の例を説明します。

次の例を使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

Java

Example — ロケーション登録を削除する

```
public void deleteAccessGrantsLocation() {
DeleteAccessGrantsLocationRequest deleteRequest =
 DeleteAccessGrantsLocationRequest.builder()
.accountId("111122223333")
.accessGrantsLocationId("a1b2c3d4-5678-90ab-cdef-EXAMPLE11111")
.build();
DeleteAccessGrantsLocationResponse deleteResponse =
 s3Control.deleteAccessGrantsLocation(deleteRequest);
LOGGER.info("DeleteAccessGrantsLocationResponse: " + deleteResponse);
}
```

レスポンス:

```
DeleteAccessGrantsLocationResponse()
```

S3 Access Grants での許可の使用

S3 Access Grants インスタンス内の個々のアクセス「権限」は、AWS Identity and Access Management (IAM) プリンシパルや、社内ディレクトリのユーザーまたはグループといった特定のアイデンティティに、S3 Access Grants インスタンスに登録されたロケーション内でのアクセスを許可するものです。ロケーションによって、バケットまたはプレフィックスが IAM ロールにマッピングされます。S3 Access Grants は、この IAM ロールを引き受けて被付与者に一時的な認証情報を提供します。

Amazon S3 Access Grants インスタンスに少なくとも 1 つのロケーションを登録すると、アクセス権限を作成できます。

被付与者は、IAM ユーザーまたはロール、またはディレクトリユーザーまたはグループにすることができます。ディレクトリユーザーは、S3 Access Grants インスタンスに関連付けられた、社内ディレクトリまたは外部アイデンティティソースのユーザーです。詳細については、「S3 Access Grants と社内ディレクトリのアイデンティティ」を参照してください。IAM アイデンティティセンターから特定のディレクトリユーザーまたはグループに対する権限を作成するには、IAM アイデンティティセンターでそのユーザーを識別するために使用する GUID (例: `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`) を検索します。IAM アイデンティティセンターを使用してユーザー情報を表示する方法については、「AWS IAM Identity Centerユーザーガイド」の「ユーザーとグループの割り当てを表示する」を参照してください。

バケット、プレフィックス、またはオブジェクトへのアクセスを付与できます。Amazon S3 のプレフィックスは、バケット内のオブジェクトを整理するために使用されるオブジェクトキー名の先頭にある文字列です。これには、使用可能な任意の文字列を使用できます。例えば、バケット内の `engineering/` プレフィックスで始まるオブジェクトキー名などです。

トピック

- 権限を作成する
- 権限を表示する
- 権限を削除する

権限を作成する

S3 Access Grants インスタンス内の個々のアクセス「権限」は、AWS Identity and Access Management (IAM) プリンシパルや、社内ディレクトリのユーザーまたはグループといった特定のアイデンティティに、S3 Access Grants インスタンスに登録されたロケーション内でのアクセスを許可するものです。ロケーションによって、バケットまたはプレフィックスが IAM ロールにマッピングされます。S3 Access Grants は、この IAM ロールを引き受けて被付与者に一時的な認証情報を提供します。

Amazon S3 Access Grants インスタンスに少なくとも 1 つのロケーションを登録すると、アクセス権限を作成できます。

被付与者は、IAM ユーザーまたはロール、またはディレクトリユーザーまたはグループにすることができます。ディレクトリユーザーは、S3 Access Grants インスタンスに関連付けられた、社内ディレクトリまたは外部アイデンティティソースのユーザーです。詳細については、「S3 Access Grants と社内ディレクトリのアイデンティティ」を参照してください。IAM アイデンティティセンターから特定のディレクトリユーザーまたはグループに対する権限を作成するには、IAM アイデンティティセンターでそのユーザーを識別するために使用する GUID (例: `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`) を検索します。IAM アイデンティティセンターを使用してユーザー情報を表示する方法については、「AWS IAM Identity Centerユーザーガイド」の「ユーザーとグループの割り当てを表示する」を参照してください。

バケット、プレフィックス、またはオブジェクトへのアクセスを付与できます。Amazon S3 のプレフィックスは、バケット内のオブジェクトを整理するために使用されるオブジェクトキー名の先頭にある文字列です。これには、使用可能な任意の文字列を使用できます。例えば、バケット内の `engineering/` プレフィックスで始まるオブジェクトキー名などです。

サブプレフィックス

登録されたロケーションへのアクセスを許可する場合、`Subprefix` フィールドを使用して、アクセス範囲をロケーション範囲のサブセットに絞り込むことができます。ロケーションとしてデフォルトの S3 パス (`s3://`) を登録した場合は、権限の範囲を絞り込む必要があります。デフォルトのロケーション (`s3://`) に対するアクセス権限は、被付与者が AWS リージョンのすべてのバケットにアクセスできることになるため、作成することはできません。代わりに、権限の範囲を次のいずれかに絞り込む必要があります。

- バケット: `s3://`*`bucket`*`/*`
- バケット内のプレフィックス: `s3://`*`bucket`*`/`*`prefix`*`*`
- プレフィックス内のプレフィックス: `s3://`*`bucket`*`/`*`prefixA`*`/`*`prefixB`*`*`

- オブジェクト: `s3://bucket/object-key-name`

登録済みロケーションがバケットであるアクセス権限を作成する場合、Subprefix フィールドに次のいずれかを渡して、権限の範囲を絞り込むことができます。

- バケット内のプレフィックス: *prefix**
- プレフィックス内のプレフィックス: *prefixA/prefixB**
- オブジェクト: */object-key-name*

権限の作成後、Amazon S3 コンソールに表示される権限の範囲、または API や AWS Command Line Interface (AWS CLI) のレスポンスで返される GrantScope は、ロケーションパスと Subprefix を連結したものになります。この連結されたパスが、アクセスを許可する S3 バケット、プレフィックス、またはオブジェクトに適切にマップされていることを確認します。

> **Note**
>
> - 1 つのオブジェクトにのみアクセスを許可するアクセス権限を作成する必要がある場合は、権限のタイプをオブジェクト用に指定する必要があります。API コールまたは CLI コマンドでこれを行うには、s3PrefixType パラメータに値 Object を渡します。Amazon S3 コンソールで権限を作成する場合は、ロケーションを選択した後、[権限範囲] で [権限範囲がオブジェクト] チェックボックスを選択します。
> - バケットがまだ存在していない場合、そのバケットへの許可は作成できません。ただし、存在しないプレフィックスに対して権限を作成することはできます。
> - S3 Access Grants インスタンスで作成できる権限の最大数については、「S3 Access Grants の制約」を参照してください。

Amazon S3 コンソール、AWS CLI、Amazon S3 REST API、AWS SDK を使用して アクセス権限を作成できます。

S3 コンソールの使用

アクセス権限を作成するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。

2. 左側のナビゲーションペインで、[Access Grants] を選択します。
3. [S3 Access Grants] ページで、取り組む S3 Access Grants インスタンスが含まれるリージョンを選択します。

   S3 Access Grants インスタンスを初めて使用する場合は、「Step 2 - ロケーションを登録する」を実行し、Access Grants インスタンスをセットアップ ウィザードの [ステップ 3] に進んでいる必要があります。S3 Access Grants インスタンスが既にある場合は、[詳細の表示] を選択して、[権限] タブで、[権限を作成] をクリックします。

   a. [権限範囲] セクションで、登録済みのロケーションを選択または入力します。

      デフォルトロケーションの `s3://` を選択した場合は、[サブプレフィックス] ボックスを使用してアクセス権限の範囲を絞り込むことができます。詳細については、「サブプレフィックス」を参照してください。単一のオブジェクトのみへのアクセスを付与するには、[Grant scope is an object] を選択します。

   b. [許可とアクセス] で、[アクセス許可] レベルに [読み取り]、[書き込み]、または両方を選択します。

      次に、[被付与者タイプを選択] をクリックします。社内ディレクトリを IAM アイデンティティセンターに追加して、この IAM アイデンティティセンターインスタンスを S3 Access Grants インスタンスに関連付けた場合は、[IAM アイデンティティセンターからのディレクトリ ID] を選択できます。このオプションを選択した場合は、IAM アイデンティティセンターからユーザーまたはグループのアイデンティティを取得し、このセクションに入力します。

      [被付与者タイプ] が IAM ユーザーまたはロールの場合は、[IAM プリンシパル] を選択します。[IAM プリンシパルタイプ] で [ユーザー] または [ロール] を選択します 次に、[IAM プリンシパルユーザー] で、リストから選択するか、アイデンティティを入力します。

   c. S3 Access Grants 権限を作成するには、[次へ] または [権限を作成] をクリックします。
4. [次へ] または [権限を作成] が無効になっている場合:

   権限が作成できない

   - まず、S3 Access Grants インスタンスで ロケーションを登録 する必要がある場合があります。
   - アクセス権限を作成するのに必要な `s3:CreateAccessGrant` アクセス許可がない可能性があります。アカウント管理者に連絡してください。

AWS CLI を使用する場合

AWS CLI をインストールするには、「AWS Command Line Interface ユーザーガイド」の「AWS CLI をインストールする」を参照してください。

IAM プリンシパルのアクセス許可リクエストを作成する方法と、社内ディレクトリのユーザーまたはグループにアクセス権限リクエストを作成する方法の例は、次のとおりです。

次のコマンド例を使用する際は、*user input placeholders* をユーザー自身の情報に置き換えます。

> **Note**
>
> 単一のオブジェクトのみへのアクセスを許可するアクセス権限を作成する場合は、必要な `--s3-prefix-type Object` パラメータを含めます。

Example IAM プリンシパルのアクセス権限リクエストを作成する

```
aws s3control create-access-grant \
--account-id 111122223333 \
--access-grants-location-id a1b2c3d4-5678-90ab-cdef-EXAMPLE22222 \
--access-grants-location-configuration S3SubPrefix=prefixB* \
--permission READ \
--grantee GranteeType=IAM,GranteeIdentifier=arn:aws:iam::123456789012:user/data-consumer-3
```

Example アクセス権限のレスポンスを作成する

```
{"CreatedAt": "2023-05-31T18:41:34.663000+00:00",
    "AccessGrantId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "AccessGrantArn": "arn:aws:s3:us-east-2:111122223333:access-grants/default/grant/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Grantee": {
        "GranteeType": "IAM",
        "GranteeIdentifier": "arn:aws:iam::111122223333:user/data-consumer-3"
    },
    "AccessGrantsLocationId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "AccessGrantsLocationConfiguration": {
        "S3SubPrefix": "prefixB*"
    },
```

```
    "GrantScope": "s3://DOC-BUCKET-EXAMPLE/prefix*",
    "Permission": "READ"
}
```

ディレクトリユーザーやグループのためのアクセス権限リクエストを作成する

ディレクトリユーザーまたはグループのアクセス許可リクエストを作成するには、まず次のコマンドのいずれかを実行してディレクトリユーザーまたはグループの GUID を取得する必要があります。

Example ディレクトリユーザーやグループの GUID を取得する

IAM アイデンティティセンターユーザーの GUID は、IAM アイデンティティセンターコンソール、AWS CLI、または AWS SDK を使用して検索できます。次のコマンドは、指定した IAM アイデンティティセンターインスタンス内のユーザーを名前とアイデンティティとともに一覧表示します。

```
aws identitystore list-users --identity-store-id d-1a2b3c4d1234
```

このコマンドは、指定した IAM アイデンティティセンターインスタンスのグループを一覧表示します。

```
aws identitystore list-groups --identity-store-id d-1a2b3c4d1234
```

Example ディレクトリユーザーまたはグループのためのアクセス権限を作成する

このコマンドは IAM ユーザーまたはロールの権限の作成と似ています。ただし、被付与者タイプは DIRECTORY_USER または DIRECTORY_GROUP で、被付与者識別子がディレクトリユーザーまたはグループの GUID である点が異なります。

```
aws s3control create-access-grant \
--account-id 123456789012 \
--access-grants-location-id default \
--access-grants-location-configuration S3SubPrefix="amzn-s3-demo-bucket/rafael/*" \
--permission READWRITE \
--grantee GranteeType=DIRECTORY_USER,GranteeIdentifier=83d43802-00b1-7054-db02-
f1d683aacba5 \
```

REST API の使用

REST API でのアクセス権限管理のサポートの詳細については、「Amazon Simple Storage Service API リファレンス」の次のセクションを参照してください。

- CreateAccessGrant
- DeleteAccessGrant
- GetAccessGrant
- ListAccessGrants

AWS SDK の使用

このセクションでは、AWS SDK を使用してアクセス権限を作成する方法の例を説明します。

Java

次のコマンド例を使用する際は、*user input placeholders* をユーザー自身の情報に置き換えます。

> **Note**
>
> 単一のオブジェクトのみへのアクセスを許可するアクセス権限を作成する場合は、必要な `.s3PrefixType(S3PrefixType.Object)` パラメータを含めます。

Example アクセス権限リクエストを作成する

```
public void createAccessGrant() {
CreateAccessGrantRequest createRequest = CreateAccessGrantRequest.builder()
.accountId("111122223333")
.accessGrantsLocationId("a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa")
.permission("READ")
.accessGrantsLocationConfiguration(AccessGrantsLocationConfiguration.builder().s3SubPrefix("
.grantee(Grantee.builder().granteeType("IAM").granteeIdentifier("arn:aws:iam::111122223333:u
data-consumer-3").build())
.build();
CreateAccessGrantResponse createResponse =
 s3Control.createAccessGrant(createRequest);
LOGGER.info("CreateAccessGrantResponse: " + createResponse);
}
```

Example アクセス権限のレスポンスを作成する

```
CreateAccessGrantResponse(
```

```
CreatedAt=2023-06-07T05:20:26.330Z,
AccessGrantId=a1b2c3d4-5678-90ab-cdef-EXAMPLE33333,
AccessGrantArn=arn:aws:s3:us-east-2:444455556666:access-grants/default/grant/
a1b2c3d4-5678-90ab-cdef-EXAMPLE33333,
Grantee=Grantee(
GranteeType=IAM,
GranteeIdentifier=arn:aws:iam::111122223333:user/data-consumer-3
),
AccessGrantsLocationId=a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa,
AccessGrantsLocationConfiguration=AccessGrantsLocationConfiguration(
S3SubPrefix=prefixB*
),
GrantScope=s3://DOC-BUCKET-EXAMPLE/prefixB,
Permission=READ
)
```

権限を表示する

Amazon S3 コンソール、AWS Command Line Interface (AWS CLI)、Amazon S3 REST API、AWS SDK を使用して、S3 Access Grants インスタンスのアクセス権限の詳細を表示できます。

S3 コンソールの使用

アクセス権限の詳細を表示するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[Access Grants] を選択します。
3. [S3 Access Grants] ページで、取り組む S3 Access Grants インスタンスが含まれるリージョンを選択します。
4. インスタンスの [詳細の表示] をクリックします。
5. [詳細] ページで、[権限] タブをクリックします。
6. [権限] セクションで、確認するアクセス権限を検索します。権限一覧にフィルターを適用するには、検索ボックスを使用します。

AWS CLI を使用する場合

AWS CLI をインストールするには、「AWS Command Line Interface ユーザーガイド」の「AWS CLI をインストールする」を参照してください。

次のコマンド例を使用する際は、*user input placeholders* をユーザー自身の情報に置き換えます。

Example — アクセス権限の詳細を取得する

```
aws s3control get-access-grant \
--account-id 111122223333 \
--access-grant-id a1b2c3d4-5678-90ab-cdef-EXAMPLE22222
```

レスポンス:

```
{
    "CreatedAt": "2023-05-31T18:41:34.663000+00:00",
    "AccessGrantId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "AccessGrantArn": "arn:aws:s3:us-east-2:111122223333:access-grants/default/
grant-a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "Grantee": {
        "GranteeType": "IAM",
        "GranteeIdentifier": "arn:aws:iam::111122223333:user/data-consumer-3"
    },
    "Permission": "READ",
    "AccessGrantsLocationId": "12a6710f-5af8-41f5-b035-0bc795bf1a2b",
    "AccessGrantsLocationConfiguration": {
        "S3SubPrefix": "prefixB*"
    },
    "GrantScope": "s3://amzn-s3-demo-bucket/"
}
```

Example – S3 Access Grants インスタンスのアクセス権限をすべて一覧表示する

必要に応じて次のパラメータを使用して、結果を S3 プレフィックスまたは AWS Identity and Access Management (IAM) ID に限定できます。

- サブプレフィックス – `--grant-scope s3://bucket-name/prefix*`
- IAM アイデンティティ – `--grantee-type IAM` と `--grantee-identifier arn:aws:iam::123456789000:role/accessGrantsConsumerRole`

```
aws s3control list-access-grants \
--account-id 111122223333
```

レスポンス:

```
{
    "AccessGrantsList": [{"CreatedAt": "2023-06-14T17:54:46.542000+00:00",
            "AccessGrantId": "dd8dd089-b224-4d82-95f6-975b4185bbaa",
            "AccessGrantArn": "arn:aws:s3:us-east-2:111122223333:access-grants/default/
grant/dd8dd089-b224-4d82-95f6-975b4185bbaa",
            "Grantee": {
                "GranteeType": "IAM",
                "GranteeIdentifier": "arn:aws:iam::111122223333:user/data-consumer-3"
            },
            "Permission": "READ",
            "AccessGrantsLocationId": "23514a34-ea2e-4ddf-b425-d0d4bfcarda1",
            "GrantScope": "s3://amzn-s3-demo-bucket/prefixA*"
        },
        {"CreatedAt": "2023-06-24T17:54:46.542000+00:00",
            "AccessGrantId": "ee8ee089-b224-4d72-85f6-975b4185a1b2",
            "AccessGrantArn": "arn:aws:s3:us-east-2:111122223333:access-grants/default/
grant/ee8ee089-b224-4d72-85f6-975b4185a1b2",
            "Grantee": {
                "GranteeType": "IAM",
                "GranteeIdentifier": "arn:aws:iam::111122223333:user/data-consumer-9"
            },
            "Permission": "READ",
            "AccessGrantsLocationId": "12414a34-ea2e-4ddf-b425-d0d4bfcacao0",
            "GrantScope": "s3://amzn-s3-demo-bucket/prefixB*"
        },

    ]
}
```

REST API の使用

Amazon S3 API オペレーションを使用して、アクセス権限の詳細を表示し、S3 Access Grants インスタンス内のすべてのアクセス権限を一覧表示できます。REST API でのアクセス権限管理のサポートの詳細については、「Amazon Simple Storage Service API リファレンス」の次のセクションを参照してください。

- GetAccessGrant
- ListAccessGrants

AWS SDK の使用

このセクションでは、AWS SDK を使用してアクセス権限の詳細を取得する方法の例を説明します。

次の例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

Java

Example — アクセス権限の詳細を取得する

```
public void getAccessGrant() {
GetAccessGrantRequest getRequest = GetAccessGrantRequest.builder()
.accountId("111122223333")
.accessGrantId("a1b2c3d4-5678-90ab-cdef-EXAMPLE22222")
.build();
GetAccessGrantResponse getResponse = s3Control.getAccessGrant(getRequest);
LOGGER.info("GetAccessGrantResponse: " + getResponse);
}
```

レスポンス:

```
GetAccessGrantResponse(
CreatedAt=2023-06-07T05:20:26.330Z,
AccessGrantId=a1b2c3d4-5678-90ab-cdef-EXAMPLE22222,
AccessGrantArn=arn:aws:s3:us-east-2:111122223333:access-grants/default/
grant-fd3a5086-42f7-4b34-9fad-472e2942c70e,
Grantee=Grantee(
GranteeType=IAM,
GranteeIdentifier=arn:aws:iam::111122223333:user/data-consumer-3
),
Permission=READ,
AccessGrantsLocationId=12a6710f-5af8-41f5-b035-0bc795bf1a2b,
AccessGrantsLocationConfiguration=AccessGrantsLocationConfiguration(
S3SubPrefix=prefixB*
),
GrantScope=s3://amzn-s3-demo-bucket/
)
```

Example – S3 Access Grants インスタンスのアクセス権限をすべて一覧表示する

必要に応じて次のパラメータを使用して、結果を S3 プレフィックスまたは IAM アイデンティティに限定できます。

- 範囲 – GrantScope=s3://*bucket-name/prefix**
- 被付与者 – GranteeType=IAM と GranteeIdentifier= arn:aws:iam::*111122223333*:role/*accessGrantsConsumerRole*

```
public void listAccessGrants() {
ListAccessGrantsRequest listRequest = ListAccessGrantsRequest.builder()
.accountId("111122223333")
.build();
ListAccessGrantsResponse listResponse = s3Control.listAccessGrants(listRequest);
LOGGER.info("ListAccessGrantsResponse: " + listResponse);
}
```

レスポンス:

```
ListAccessGrantsResponse(
AccessGrantsList=[
ListAccessGrantEntry(
CreatedAt=2023-06-14T17:54:46.540z,
AccessGrantId=dd8dd089-b224-4d82-95f6-975b4185bbaa,
AccessGrantArn=arn:aws:s3:us-east-2:111122223333:access-grants/default/
grant/dd8dd089-b224-4d82-95f6-975b4185bbaa,
Grantee=Grantee(
GranteeType=IAM, GranteeIdentifier= arn:aws:iam::111122223333:user/data-consumer-3
),
Permission=READ,
AccessGrantsLocationId=23514a34-ea2e-4ddf-b425-d0d4bfcarda1,
GrantScope=s3://amzn-s3-demo-bucket/prefixA
),
ListAccessGrantEntry(
CreatedAt=2023-06-24T17:54:46.540Z,
AccessGrantId=ee8ee089-b224-4d72-85f6-975b4185a1b2,
AccessGrantArn=arn:aws:s3:us-east-2:111122223333:access-grants/default/
grant/ee8ee089-b224-4d72-85f6-975b4185a1b2,
Grantee=Grantee(
GranteeType=IAM, GranteeIdentifier= arn:aws:iam::111122223333:user/data-consumer-9
),
Permission=READ,
AccessGrantsLocationId=12414a34-ea2e-4ddf-b425-d0d4bfcacao0,
GrantScope=s3://amzn-s3-demo-bucket/prefixB*
)
```

```
]
)
```

権限を削除する

S3 Access Grants インスタンスからアクセス権限を削除することもできます。アクセス権限の削除は元に戻すことができません。アクセス権限を削除すると、被付与者は Amazon S3 データにアクセスできなくなります。

Amazon S3 コンソール、AWS Command Line Interface、(AWS CLI)、AWS SDK、または Amazon S3 REST API を使用してアクセス権限を削除できます。

S3 コンソールの使用

アクセス権限を削除するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[Access Grants] を選択します。
3. [S3 Access Grants] ページで、取り組む S3 Access Grants インスタンスが含まれるリージョンを選択します。
4. インスタンスの [詳細の表示] をクリックします。
5. [詳細] ページで、[権限] タブをクリックします。
6. 削除する権限を検索します。権限を見つけたら、その横にあるラジオボタンをオンにします。
7. [削除] を選択します。この操作は元に戻せないことを警告するダイアログボックスが表示されます。もう一度 [削除] をクリックすると、権限が削除されます。

AWS CLI を使用する場合

AWS CLI をインストールするには、「AWS Command Line Interface ユーザーガイド」の「AWS CLI をインストールする」を参照してください。

次のコマンド例を使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

Example – アクセス権限を削除する

```
aws s3control delete-access-grant \
--account-id 111122223333 \
--access-grant-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111

// No response body
```

REST API の使用

Amazon REST API でのアクセス権限管理のサポートの詳細については、「Amazon Simple Storage Service API リファレンス」の「DeleteAccessGrant」を参照してください。

AWS SDK の使用

このセクションでは、AWS SDK を使用してアクセス権限を削除する方法の例を説明します。次の例を使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

Java

Example – アクセス権限を削除する

```
public void deleteAccessGrant() {
DeleteAccessGrantRequest deleteRequest = DeleteAccessGrantRequest.builder()
.accountId("111122223333")
.accessGrantId("a1b2c3d4-5678-90ab-cdef-EXAMPLE11111")
.build();
DeleteAccessGrantResponse deleteResponse =
 s3Control.deleteAccessGrant(deleteRequest);
LOGGER.info("DeleteAccessGrantResponse: " + deleteResponse);
}
```

レスポンス:

```
DeleteAccessGrantResponse()
```

Access Grants を使用した S3 データの取得

S3 Access Grants を通じて S3 データへのアクセスを許可された被付与者は、S3 Access Grants に一時的な認証情報をリクエストする必要があります。これは、S3 データへのアクセスに使用されま

す。詳細については、「S3 Access Grants を介して Amazon S3 データへのアクセスをリクエストする」を参照してください。次に、被付与者は一時的な認証情報を使用して、S3 データに対して許可される S3 アクションを実行します。詳細については、「S3 Access Grants が提供する認証情報を使用した S3 データへのアクセス」を参照してください。必要に応じて、被付与者は、これらの認証情報をリクエストする前に AWS アカウント のアクセス許可のリストをリクエストできます。詳細については、「発信者のアクセス許可を一覧表示する」を参照してください。

トピック

- S3 Access Grants を介して Amazon S3 データへのアクセスをリクエストする
- S3 Access Grants が提供する認証情報を使用した S3 データへのアクセス
- 発信者のアクセス許可を一覧表示する

S3 Access Grants を介して Amazon S3 データへのアクセスをリクエストする

S3 Access Grants を使用してアクセス許可付与を作成した後、被付与者は、アクセス許可が付与された S3 データにアクセスするための認証情報をリクエストできます。被付与者は AWS Identity and Access Management (IAM) プリンシパル、企業ディレクトリアイデンティティ、または認可されたアプリケーションです。

アプリケーションまたは AWS のサービス は、S3 Access Grants `GetDataAccess` API オペレーションを使用して、被付与者に代わって S3 データへのアクセスを S3 Access Grants にリクエストできます。`GetDataAccess` はまず、この ID にそのデータへのアクセス権が付与されたことを確認します。次に S3 Access Grants は AssumeRole API オペレーションを使用して一時的な認証トークンを取得し、それをリクエスタに送信します。この一時的な認証情報トークンは AWS Security Token Service (AWS STS) トークンです。

`GetDataAccess` リクエストには、一時的な認証情報が適用される S3 `target` データの範囲を指定するパラメータを含める必要があります。この `target` スコープは許可付与のスコープと同一でも、そのスコープのサブセットでもかまいません。ただし、`target` スコープは被付与者の許可付与のスコープ内であることが必要です。このリクエストでは、一時認証情報の権限レベル (`READ`、`WRITE`、`READWRITE`、など) を示す `permission` パラメータも指定する必要があります。

特権

リクエスタは、認証情報リクエストで一時トークンの特権レベルを指定できます。リクエスタはこの `privilege` パラメータを使用して、一時的な認証情報のアクセス範囲を付与範囲内で拡大または縮小できます。`privilege` パラメータのデフォルト値は `Default` であり、返される認証情報のターゲット範囲は元の権限範囲です。`privilege` でこれ以外に指定できる値は、`Minimal` で

す。target 範囲が元の権限範囲から縮小される場合、target 範囲が権限範囲内にある限り、一時的な認証情報は target 範囲と一致するように範囲が再定義されます。

2 つの権限に対する privilege パラメータの効果の詳細は、次のテーブルのとおりです。一方の権限の範囲は、S3://*amzn-s3-demo-bucket1*/bob/*で、*amzn-s3-demo-bucket1* バケットの bob/ プレフィックス全体が含まれます。もう一方の権限の範囲は、S3://*amzn-s3-demo-bucket1*/bob/reports/* で、*amzn-s3-demo-bucket1* バケットの bob/reports/ プレフィックスのみが含まれます。

権限範囲	リクエスト範囲	特権	返される範囲	効果
S3://*amzn-s3-demo-bucket1* /bob/*	*amzn-s3-demo-bucket1* /bob/*	Default	*amzn-s3-demo-bucket1* /bob/*	リクエスタは、*amzn-s3-demo-bucket1* バケット内のプレフィックス *bob/* で始まるキー名を持つすべてのオブジェクトにアクセスできます。
S3://*amzn-s3-demo-bucket1* /bob/*	*amzn-s3-demo-bucket1* /bob/	Minimal	*amzn-s3-demo-bucket1* /bob/	プレフィックス名 bob/ の後にワイルドカードの * 文字がないと、リクエスタがアクセスできるのは、*amzn-s3-demo-bucket1* バケット内のオブジェクト名 bob/ のみです。このようなオブジェクトは通常存在しません。リクエスタは、bob/ プレフィックスで始まるキー名を持つオブジェクトを含め、その他のオブジェクトにはアクセスできません。
S3://*amzn-s3-d*	*amzn-s3-demo-*	Minimal	*amzn-s3-demo-bucket1* /bob/images/*	リクエスタは、*amzn-s3-demo-bucket1* バ

権限範囲	リクエスト範囲	特権	返される範囲	効果
emo-bucket1 /bob/*	*bucket1* /bob/images/*			ケット内のプレフィックス *bob/images/** で始まるキー名を持つすべてのオブジェクトにアクセスできます。
S3://*amzn-s3-demo-bucket1* /bob/reports/*	*amzn-s3-demo-bucket1* /bob/reports/file.txt	Default	*amzn-s3-demo-bucket1* /bob/reports/*	リクエスタは、*amzn-s3-demo-bucket1* バケット内の bob/reports プレフィックスで始まるキー名を持つすべてのオブジェクトにアクセスできます。これは、権限と一致する範囲です。
S3://*amzn-s3-demo-bucket1* /bob/reports/*	*amzn-s3-demo-bucket1* /bob/reports/file.txt	Minimal	*amzn-s3-demo-bucket1* /bob/reports/file.txt	リクエスタは、*amzn-s3-demo-bucket1* バケット内のキー名 bob/reports/file.txt のオブジェクトにのみアクセスできます。リクエスタは、その他のオブジェクトにはアクセスできません。

ディレクトリアイデンティティ

GetDataAccess は、適切な許可付与を照合するときに、リクエストに関連するすべての ID を考慮します。企業ディレクトリアイデンティティの場合、GetDataAccess は、ID 対応セッションに使用される IAM アイデンティティの許可付与も返します。ID 対応セッションの詳細については、「AWS Identity and Access Management ユーザーガイド」の「ID 対応コンソールセッションを使用するアクセス許可の付与」を参照してください。GetDataAccess は、次の表に示すように、最も制限の厳しい許可付与にスコープを絞り込む認証情報を生成します。

IAM アイデンティティの許可付与スコープ	ディレクトリアイデンティティの許可付与スコープ	リクエスト範囲	返される範囲	特権	効果
S3://*amzn-s3-demo-bucket1* / bob/*	*amzn-s3-demo-bucket1* / bob/images/*	S3://*amzn-s3-demo-bucket1* / bob/images/image1.jpeg	S3://*amzn-s3-demo-bucket1* / bob/images/*	Default	リクエスト元は、IAM ロールの許可付与の一環として、プレフィックス bob/ で始まるキー名の付いたすべてのオブジェクトにアクセスできますが、ディレクトリアイデンティティの許可付与の一環として、プレフィックス bob/images/ で制限されます。IAM ロールとディレクトリアイデンティティの両方がリクエストされた範囲 (bob/images/image1.jpeg) へのアクセスを提供しますが、ディレクトリアイデンティティにはより制限の厳しい許可付与があります。したがって、返されるスコープはディレクトリアイデンティティのより制限の厳しい許可付与で絞り込まれます。

IAM アイデンティティの許可付与スコープ	ディレクトリアイデンティティの許可付与スコープ	リクエスト範囲	返される範囲	特権	効果
S3://*amzn-s3-demo-bucket1* / bob/*	*amzn-s3-demo-bucket1* / bob/images/*	S3://*amzn-s3-demo-bucket1* / bob/images/image1.jpeg	S3://*amzn-s3-demo-bucket1* / bob/images/image1.jpeg	Minimal	権限が Minimal に設定されているため、ID がより大きなスコープにアクセスできる場合でも、リクエストされたスコープ bob/images/image1.jpeg のみが返されます。

IAM アイデンティティの許可付与スコープ	ディレクトリアイデンティティの許可付与スコープ	リクエスト範囲	返される範囲	特権	効果
S3://*amzn-s3-demo-bucket1* / bob/images/*	*amzn-s3-demo-bucket1* / bob/*	S3://*amzn-s3-demo-bucket1* / bob/images/image1.jpeg	S3://*amzn-s3-demo-bucket1* / bob/images/*	Default	リクエスト元は、ディレクトリアイデンティティの許可付与の一環として、プレフィックス bob/ で始まるキー名の付いたすべてのオブジェクトにアクセスできますが、IAM ロールの許可付与の一環として、プレフィックス bob/images/ で制限されます。IAM ロールとディレクトリアイデンティティの両方がリクエストされた範囲 (bob/images/image1.jpeg) へのアクセスを提供しますが、IAM ロールにはより制限の厳しい許可付与があります。したがって、返されるスコープは IAM ロールのより制限の厳しい許可付与で絞り込まれます。

IAM アイデンティティの許可付与スコープ	ディレクトリアイデンティティの許可付与スコープ	リクエスト範囲	返される範囲	特権	効果
S3://*amzn-s3-demo-bucket1* / bob/images/*	*amzn-s3-demo-bucket1* / bob/*	S3://*amzn-s3-demo-bucket1* / bob/images/image1.jpeg	S3://*amzn-s3-demo-bucket1* / bob/images/image1.jpeg	Minimal	権限が Minimal に設定されているため、ID がより大きなスコープにアクセスできる場合でも、リクエストされたスコープ bob/images/image1.jpeg のみが返されます。

期間

durationSeconds パラメータでは一時認証情報の有効期間を秒単位で設定します。デフォルト値は 3600 秒 (1 時間) です。リクエスタ (被付与者) は 900 秒 (15 分) から 43200 秒 (12 時間) までの範囲を指定できます。被付与者がこの最大値よりも高い値をリクエストすると、そのリクエストは失敗します。

> **Note**
>
> 一時トークンのリクエストで、ロケーションがオブジェクトの場合は、targetType リクエスト内のパラメータの値を Object に設定します。このパラメータは、ロケーションがオブジェクトで、特権レベルが Minimal の場合にのみ必要です。ロケーションがバケットまたはプレフィックスの場合、このパラメータを指定する必要はありません。

例

AWS Command Line Interface (AWS CLI)、Amazon S3 REST API、AWS SDK を使用して一時的な認証情報をリクエストできます。これらの例を参照してください。

詳細については、「Amazon Simple Storage Service API リファレンス」の「GetDataAccess」を参照してください。

AWS CLI を使用する場合

AWS CLI をインストールするには、「AWS Command Line Interface ユーザーガイド」の「AWS CLI をインストールする」を参照してください。

次のコマンド例を使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

Example 一時認証情報のリクエスト

リクエスト:

```
aws s3control get-data-access \
--account-id 111122223333 \
--target s3://amzn-s3-demo-bucket/prefixA* \
--permission READ \
--privilege Default \
--region us-east-2
```

レスポンス:

```
{
"Credentials": {
"AccessKeyId": "Example-key-id",
"SecretAccessKey": "Example-access-key",
"SessionToken": "Example-session-token",
"Expiration": "2023-06-14T18:56:45+00:00"},
"MatchedGrantTarget": "s3://amzn-s3-demo-bucket/prefixA**",
"Grantee": {
    "GranteeType": "IAM",
    "GranteeIdentifier": "arn:aws:iam::111122223333:role/role-name"
 }
}
```

REST API の使用

Amazon S3 REST API での S3 Access Grants からの一時認証情報のリクエストのサポートの詳細については、「Amazon Simple Storage Service API リファレンス」の「https://docs.aws.amazon.com/AmazonS3/latest/API/API_control_GetDataAccess.html」を参照してください。

AWS SDK の使用

このセクションでは、AWS SDK を使用して被付与者が一時認証情報をリクエストする方法の例を説明します。

Java

次のコード例は、被付与者が S3 データにアクセスするために使用する一時的な認証情報を返します。次のコマンド例を使用する際は、*user input placeholders* をユーザー自身の情報に置き換えます。

Example 一時認証情報を入手する

リクエスト:

```
public void getDataAccess() {
GetDataAccessRequest getDataAccessRequest = GetDataAccessRequest.builder()
.accountId("111122223333")
.permission(Permission.READ)
.privilege(Privilege.MINIMAL)
.target("s3://amzn-s3-demo-bucket/prefixA*")
.build();
GetDataAccessResponse getDataAccessResponse =
 s3Control.getDataAccess(getDataAccessRequest);
LOGGER.info("GetDataAccessResponse: " + getDataAccessResponse);
}
```

レスポンス:

```
GetDataAccessResponse(
Credentials=Credentials(
AccessKeyId="Example-access-key-id",
SecretAccessKey="Example-secret-access-key",
SessionToken="Example-session-token",
Expiration=2023-06-07T06:55:24Z
))
```

S3 Access Grants が提供する認証情報を使用した S3 データへのアクセス

被付与者がアクセス許可を通じて一時的な認証情報を取得 すると、その一時的な認証情報を使用して Amazon S3 API オペレーションを呼び出し、データにアクセスできます。

被付与者は、AWS Command Line Interface (AWS CLI)、AWS SDK、Amazon S3 REST API を使用して、S3 データにアクセスできます。さらに、AWS Python および Java プラグインを使用して S3 Access Grants を呼び出すことができます。

AWS CLI を使用する場合

被付与者は S3 Access Grants から一時的な認証情報を取得したら、その認証情報を使用してプロファイルを設定してデータを取得できます。

AWS CLI をインストールするには、「AWS Command Line Interface ユーザーガイド」の「AWS CLI をインストールする」を参照してください。

次のコマンド例を使用する際は、*user input placeholders* をユーザー自身の情報に置き換えます。

Example – プロファイルを設定する

```
aws configure set aws_access_key_id "$accessKey" --profile access-grants-consumer-access-profile
aws configure set aws_secret_access_key "$secretKey" --profile access-grants-consumer-access-profile
aws configure set aws_session_token "$sessionToken" --profile access-grants-consumer-access-profile
```

次のコマンド例を使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

Example – S3 データを取得する

被付与者は、get-object AWS CLI コマンドを使用して、データにアクセスできます。被付与者は、put-object、ls、その他の S3 AWS CLI コマンドも使用できます。

```
aws s3api get-object \
--bucket amzn-s3-demo-bucket1 \
--key myprefix \
--region us-east-2 \
--profile access-grants-consumer-access-profile
```

AWS SDK の使用

このセクションでは、AWS SDK を使用して S3 データにアクセスする方法の例を説明します。

Java

一時的な認証情報を使用して S3 データを取得する方法の例については、「AWSSDK を使用してオブジェクトを取得する方法」と「AWS SDK for Java 2.x の Amazon S3 コード例」を参照してください。

S3 Access Grants でサポートされている S3 アクション

被付与者は、S3 Access Grants によって提供される一時的な認証情報を使用して、アクセスできる S3 データに対して S3 アクションを実行できます。以下は、被付与者が実行できる S3 アクションのリストです。許可されるアクションは、アクセス許可で付与されるアクセス許可のレベル、`READ`、`WRITE` または `READWRITE` によって異なります。

> **Note**
>
> 以下に示す Amazon S3 アクセス許可に加えて、Amazon S3 は AWS Key Management Service (AWS KMS) Decrypt (`kms:decrypt`) `READ` アクセス許可または AWS KMS GenerateDataKey (`kms:generateDataKey`) `WRITE` アクセス許可を呼び出すことができます。これらのアクセス許可では、AWS KMS キーへの直接アクセスは許可されません。

S3 IAM アクション	API アクションとドキュメント	S3 Access Grants アクセス許可	S3 リソース
`s3:GetObject`	GetObject	`READ`	オブジェクト
`s3:GetObjectVersion`	GetObject	`READ`	オブジェクト
`s3:GetObjectAcl`	GetObjectAcl	`READ`	オブジェクト
`s3:GetObjectVersionAcl`	GetObjectAcl	`READ`	オブジェクト

S3 IAM アクション	API アクションとドキュメント	S3 Access Grants アクセス許可	S3 リソース			
s3:ListMultipartUploads	ListParts	READ	オブジェクト			
s3:PutObject	PutObject、CreateMultipartUpload、UploadPart、UploadPartCopy、CompleteMultipartUpload	WRITE	オブジェクト			
s3:PutObjectAcl	PutObjectAcl	WRITE	オブジェクト			
s3:PutObjectVersionAcl	PutObjectAcl	WRITE	オブジェクト			
s3:DeleteObject	DeleteObject	WRITE	オブジェクト			
s3:DeleteObjectVersion	DeleteObject	WRITE	オブジェクト			
s3:AbortMultipartUpload	AbortMultipartUpload	WRITE	オブジェクト			
s3:ListBucket	HeadBucket、ListObjectsV2、ListObjects	READ	バケット			

S3 IAM アクション	API アクションとドキュメント	S3 Access Grants アクセス許可	S3 リソース			
`s3:ListBucketVersions`	ListObjectVersions	READ	バケット			
`s3:ListBucketMultipartUploads`	ListMultipartUploads	READ	バケット			

発信者のアクセス許可を一覧表示する

S3 データ所有者は、S3 Access Grants を使用して、AWS Identity and Access Management (IAM) ID または AWS IAM Identity Center 企業ディレクトリ ID のアクセス許可を作成できます。IAM アイデンティティと IAM Identity Center ディレクトリ ID は、次に `ListCallerAccessGrants` API を使用して、S3 Access Grants で定義したとおり、アクセスできる Amazon S3 バケット、プレフィックス、およびオブジェクトを一覧表示できます。この API を使用して、IAM またはディレクトリ ID が S3 Access Grants を介してアクセスできるすべての S3 データを検出します。

この機能を使用すると、特定のエンドユーザーがアクセスできるデータを表示するアプリケーションを構築できます。例えば、お客様が S3 バケットにアクセスするために使用するオープンソース UI コンポーネントである AWS Storage Browser for S3 は、この機能を使用して、S3 Access Grants に基づいて Amazon S3 でアクセスできるデータをエンドユーザーに提示します。もう 1 つの例として、Amazon S3 でデータを参照、アップロード、またはダウンロードするためのアプリケーションを構築する場合、この機能を使用して、エンドユーザーが参照できるツリー構造をアプリケーションに構築できます。

> **Note**
>
> 企業ディレクトリアイデンティティの場合、呼び出し元のアクセス許可付与を一覧表示する際に、S3 Access Grants は ID 対応セッションに使用される IAM アイデンティティの許可付与を返します。ID 対応セッションの詳細については、「AWS Identity and Access Management ユーザーガイド」の「ID 対応コンソールセッションを使用するアクセス許可の付与」を参照してください。

IAM アイデンティティまたは社内ディレクトリアイデンティティのいずれかである被付与者が、AWS Command Line Interface (AWS CLI)、Amazon S3 REST API、および AWS SDK を使用することで、付与されたアクセス許可を一覧表示できます。

AWS CLI を使用する場合

AWS CLI をインストールするには、「AWS Command Line Interface ユーザーガイド」の「AWS CLI をインストールする」を参照してください。

次のコマンド例を使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

Example 発信者のアクセス許可を一覧表示する

リクエスト:

```
aws s3control list-caller-access-grants \
--account-id 111122223333 \
--region us-east-2
--max-results 5
```

レスポンス:

```
{
 "NextToken": "6J9S...",
 "CallerAccessGrantsList": [
  {
   "Permission": "READWRITE",
   "GrantScope": "s3://amzn-s3-demo-bucket/prefix1/sub-prefix1/*",
   "ApplicationArn": "NA"
  },
  {
   "Permission": "READWRITE",
   "GrantScope": "s3://amzn-s3-demo-bucket/prefix1/sub-prefix2/*",
   "ApplicationArn": "ALL"
  },
  {
   "Permission": "READWRITE",
   "GrantScope": "s3://amzn-s3-demo-bucket/prefix1/sub-prefix3/*",
   "ApplicationArn": "arn:aws:sso::111122223333:application/ssoins-
ssoins-1234567890abcdef/apl-abcd1234a1b2c3d"
```

```
  }
 ]
}
```

Example バケットに対する発信者のアクセス許可を一覧表示する

grantscope パラメータを使用して結果を絞り込むことができるようになりました。

リクエスト:

```
aws s3control list-caller-access-grants \
--account-id 111122223333 \
--region us-east-2
--grant-scope "s3://amzn-s3-demo-bucket""
--max-results 1000
```

レスポンス:

```
{
 "NextToken": "6J9S...",
 "CallerAccessGrantsList": [
  {
   "Permission": "READ",
   "GrantScope": "s3://amzn-s3-demo-bucket*",
   "ApplicationArn": "ALL"
  },
  {
   "Permission": "READ",
   "GrantScope": "s3://amzn-s3-demo-bucket/prefix1/*",
   "ApplicationArn": "arn:aws:sso::111122223333:application/ssoins-
ssoins-1234567890abcdef/apl-abcd1234a1b2c3d"
  }
 ]
}
```

REST API の使用

API 発信者のアクセス許可リストを取得するための Amazon S3 REST API サポートの詳細については、「Amazon Simple Storage Service API リファレンス」の「ListCallerAccessGrants」を参照してください。

AWS SDK の使用

このセクションでは、AWS SDK を使用して被付与者が一時認証情報をリクエストする方法の例を説明します。

Java

次のコード例は、特定の AWS アカウントの S3 データに対する API 発信者のアクセス許可を返します。次のコマンド例を使用する際は、*user input placeholders* をユーザー自身の情報に置き換えます。

Example 発信者のアクセス許可を一覧表示する

リクエスト:

```
Public void ListCallerAccessGrants() {
 ListCallerAccessGrantsRequest listRequest = ListCallerAccessGrantsRequest.builder()
    .withMaxResults(1000)
    .withGrantScope("s3://")
    .accountId("111122223333");
 ListCallerAccessGrantsResponse listResponse =
 s3control.listCallerAccessGrants(listRequest);
 LOGGER.info("ListCallerAccessGrantsResponse: " + listResponse);
 }
```

レスポンス:

```
ListCallerAccessGrantsResponse(
CallerAccessGrantsList=[
 ListCallerAccessGrantsEntry(
  S3Prefix=s3://amzn-s3-demo-bucket/prefix1/,
  Permission=READ,
  ApplicationArn=ALL
 )
])
```

S3 Access は、クロスアカウントアクセスを許可します。

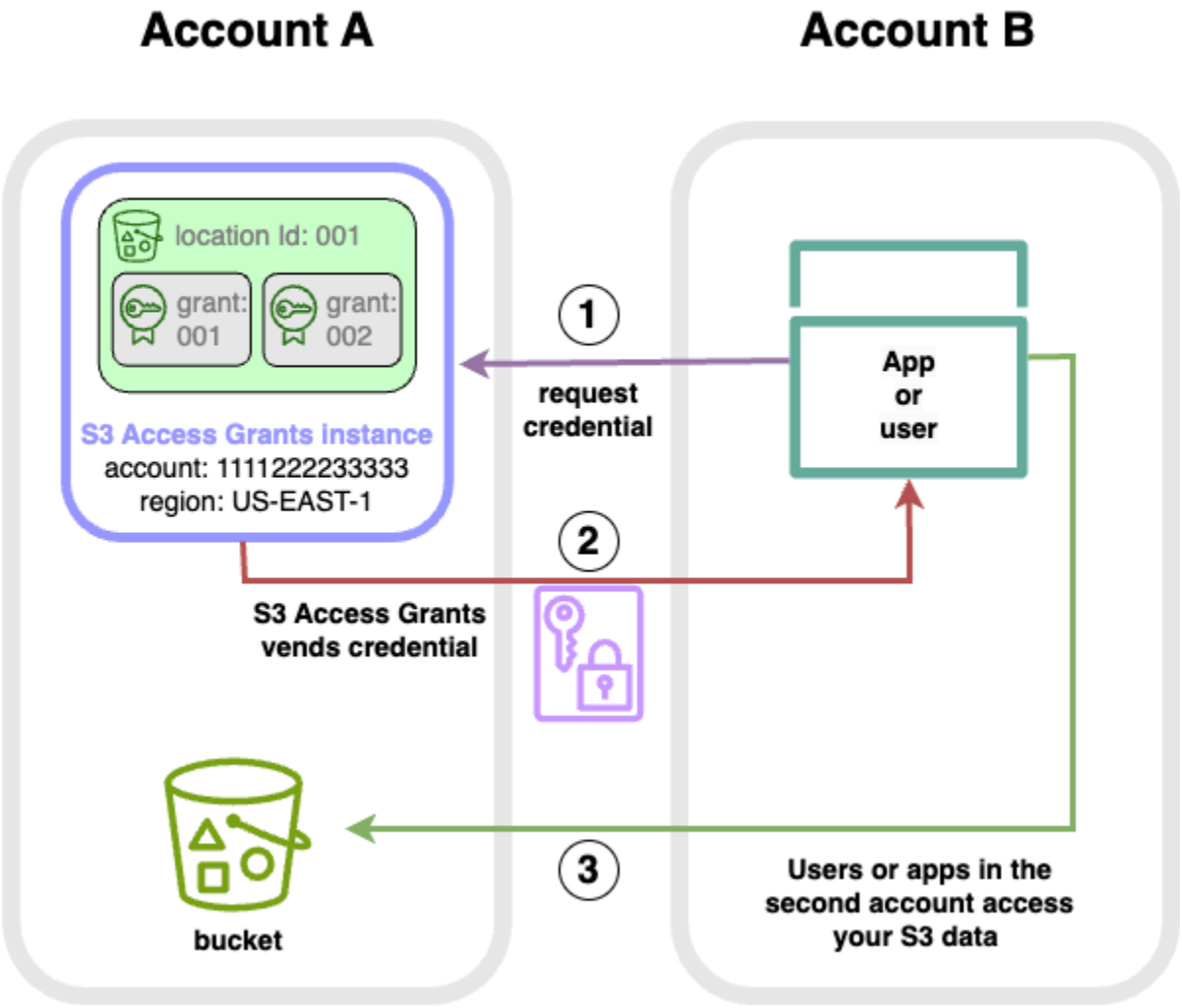
S3 Access Grants を使用すると、Amazon S3 データアクセスを以下に付与できます。

- AWS Identity and Access Management アカウント内の (IAM) アイデンティティ

- 他の AWS アカウントの IAM アイデンティティ
- AWS IAM Identity Center インスタンス内のディレクトリユーザーまたはグループ

まず、他のアカウントでのクロスアカウントアクセスを設定します。これには、リソースポリシーを使用して S3 Access Grants インスタンスへのアクセス許可の付与などがあります。次に、許可を使用して S3 データ (バケット、プレフィックス、オブジェクト) へのアクセス許可を付与します。

クロスアカウントアクセスの設定後、他のアカウントは S3 Access Grants から Amazon S3 データへの一時的なアクセス認証情報をリクエストできるようになります。次の図は、S3 Access Grants によるクロスアカウント S3 アクセスのユーザーフローを説明しています。



1. 2 番目のアカウント (B) のユーザーまたはアプリケーションは、Amazon S3 データが保存されているアカウント (A) の S3 Access Grants インスタンスに認証情報をリクエストします。詳細については、「S3 Access Grants を介して Amazon S3 データへのアクセスをリクエストする」を参照してください。

2. アカウント (A) の S3 Access Grants インスタンスは、2 番目のアカウントに Amazon S3 データへのアクセスを付与する許可がある場合、一時的な認証情報を返します。Access Grants の詳細については、「S3 Access Grants での許可の使用」を参照してください。
3. 2 番目のアカウント (B) のユーザーまたはアプリケーションは、S3 Access Grants が提供する認証情報を使用して、アカウント (A) の S3 データにアクセスします。

S3 Access Grants クロスアカウントアクセスの設定

S3 Access Grants を介してクロスアカウント S3 アクセスを付与するには、次の手順を実行します。

- ステップ 1: S3 データが保存されているアカウント ID 111122223333 など、S3 Access Grants インスタンスをアカウントに設定します。
- ステップ 2: アカウント 111122223333 の S3 Access Grants インスタンスのリソースポリシーを設定して、2 番目のアカウント (アカウント ID 444455556666 など) へのアクセスを許可します。
- ステップ 3: 2 番目のアカウント 444455556666 の IAM プリンシパルの IAM アクセス許可を設定し、アカウント 111122223333 の S3 Access Grants インスタンスに認証情報をリクエストします。
- ステップ 4: 2 番目のアカウント 444455556666 の IAM プリンシパルに 111122223333 アカウント内の S3 データの一部へのアクセスを付与する許可を 111122223333 アカウントに作成します。

ステップ 1: アカウントで S3 Access Grants インスタンスを設定する

Amazon S3 へのアクセスを管理するには、まずアカウント 111122223333 に S3 Access Grants インスタンスが必要です。共有する S3 データが保存されている各 AWS リージョン に S3 Access Grants インスタンスを作成する必要があります。データを複数の AWS リージョン 間で共有する場合は、各 AWS リージョン について、この設定手順を繰り返します。共有する S3 データが保存されている AWS リージョン に S3 Access Grants インスタンスが既にある場合は、次のステップに進みます。S3 Access Grants インスタンスを設定していない場合は、「S3 Access Grants インスタンスの使用」を参照してこのステップを完了します。

ステップ 2: クロスアカウントアクセスを許可するに S3 Access Grants インスタンスを許可するように、S3 Access Grants インスタンスのリソースポリシーを設定する

アカウント 111122223333 でクロスアカウントアクセス用の S3 Access Grants インスタンスを作成したら、アカウント 111122223333 内の S3 Access Grants インスタンスのリソースベースのポリシーを設定して、クロスアカウントアクセスを許可します。S3 Access Grants インスタンス自体は、リソースベースのポリシーをサポートしています。適切なリソースベースのポリシーを施行すると、その他の AWS アカウント の AWS Identity and Access Management (IAM) ユーザーまたはロールに S3 Access Grants インスタンスへのアクセスを付与できます。クロスアカウントアクセスで付与されるのは、次のアクセス許可 (アクション) のみです。

- `s3:GetAccessGrantsInstanceForPrefix` — ユーザー、ロール、またはアプリは、特定のプレフィックスを持つ S3 Access Grants インスタンスを取得できます。
- `s3:ListAccessGrants`
- `s3:ListAccessLocations`
- `s3:ListCallerAccessGrants`
- `s3:GetDataAccess` — ユーザー、ロール、またはアプリは、S3 Access Grants を介して付与されたアクセスに基づいて一時的な認証情報をリクエストできます。これらの認証情報を使用して、アクセスが付与されている S3 データにアクセスする。

このようなアクセス許可のいずれかをリソースポリシーに含めることができます。S3 Access Grants インスタンスのこのリソースポリシーは、通常のリソースベースのポリシーであり、IAM ポリシー言語がサポートするすべてをサポートします。同じポリシーで、例えば `aws:PrincipalArn` 条件を使用して、アカウント 111122223333 の特定の IAM アイデンティティにアクセスを付与することはできるとはいえ、S3 Access Grants ではその必要はありません。代わりに、S3 Access Grants インスタンス内で、自身のアカウントおよびその他のアカウントの個別の IAM アイデンティティに対する付与を作成できます。S3 Access Grants を使用して各アクセス権限を個別に管理することにより、アクセス許可をスケールできます。

AWS Resource Access Manager (AWS RAM) を既に使用している場合は、これを使用して、`s3:AccessGrants` リソースをその他のアカウントや組織内で共有できます。詳細については、「共有 AWS リソースの使用」を参照してください。AWS RAM を使用しない場合は、S3 Access Grants API オペレーションと AWS Command Line Interface (AWS CLI) を使用してリソースポリシーを追加することもできます。

S3 コンソールの使用

`s3:AccessGrants` リソースをその他のアカウントや組織内で共有するには、AWS Resource Access Manager (AWS RAM) コンソールを使用することをお勧めします。S3 Access Grants をクロスアカウントで共有するには、以下を実行します。

S3 Access Grants インスタンスのリソースポリシーを設定するには:

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. AWS リージョン セレクタから AWS リージョン を選択します。
3. 左側のナビゲーションペインで、[Access Grants] を選択します。
4. Access Grants インスタンスページの [このアカウントのインスタンス] セクションで、[インスタンスを共有] をクリックします。これにより、AWS RAM コンソールにリダイレクトされます。
5. [リソース共有を作成] をクリックします。
6. AWS RAM ステップを実行して、リソース共有を作成します。詳細については、「AWS RAM ユーザーガイド」の「リソース共有の作成」を参照してください。

AWS CLI を使用する場合

AWS CLI をインストールするには、「AWS Command Line Interface ユーザーガイド」の「AWS CLI をインストールする」を参照してください。

リソースポリシーは、`put-access-grants-instance-resource-policy` CLI コマンドを使用して追加できます。

アカウント `111122223333` の S3 Access Grants インスタンスへのクロスアカウントアクセスを 2 番目のアカウント `444455556666` に付与する場合、アカウント `111122223333` の S3 Access Grants インスタンスのリソースポリシーは、2 番目のアカウント `444455556666` に次のアクションを実行するアクセス許可を付与する必要があります。

- `s3:ListAccessGrants`
- `s3:ListAccessGrantsLocations`
- `s3:GetDataAccess`
- `s3:GetAccessGrantsInstanceForPrefix`

S3 Access Grants インスタンスのリソースポリシーで、S3 Access Grants インスタンスの ARN を Resource として指定し、2 番目のアカウント 444455556666 を Principal として指定します。次の例を使用する際は、###############を独自の情報に置き換えます。

```
{
"Version": "2012-10-17",
"Statement": [
{
 "Effect": "Allow",
 "Principal": {
 "AWS": "444455556666"
},
 "Action": [
  "s3:ListAccessGrants",
  "s3:ListAccessGrantsLocations",
  "s3:GetDataAccess",
  "s3:GetAccessGrantsInstanceForPrefix"
 ],
 "Resource": "arn:aws:s3:us-east-2:111122223333:access-grants/default"
} ]
}
```

S3 Access Grants インスタンスのリソースポリシーを追加または更新するには、次のコマンドを使用します。次のコマンド例を使用する際は、*user input placeholders* を独自の情報に置き換えます。

Example S3 Access Grants インスタンスのリソースポリシーを追加または更新する

```
aws s3control put-access-grants-instance-resource-policy \
--account-id 111122223333 \
--policy file://resourcePolicy.json \
--region us-east-2
{
 "Policy": "{\n
   \"Version\": \"2012-10-17\",\n
   \"Statement\": [{\n
  \"Effect\": \"Allow\",\n
  \"Principal\": {\n
    \"AWS\": \"444455556666\"\n
  },\n
  \"Action\": [\n
```

```
    \"s3:ListAccessGrants\",\n
    \"s3:ListAccessGrantsLocations\",\n
    \"s3:GetDataAccess\",\n
    \"s3:GetAccessGrantsInstanceForPrefix\",\n
    \"s3:ListCallerAccessGrants"\n
  ],\n
  \"Resource\": \"arn:aws:s3:us-east-2:111122223333:access-grants/default\"\n
    }\n
   ]\n
   }\n",
 "CreatedAt": "2023-06-16T00:07:47.473000+00:00"
}
```

Example S3 Access Grants リソースポリシーを取得する

CLI を使用して、S3 Access Grants インスタンスのリソースポリシーを取得または削除することもできます。

S3 Access Grants リソースポリシーを取得するには、次のサンプルコマンドを使用します。このコマンド例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3control get-access-grants-instance-resource-policy \
--account-id 111122223333 \
--region us-east-2

{
"Policy": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":\"Allow
\",\"Principal\":{\"AWS\":\"arn:aws:iam::111122223333:root\"},\"Action\":
[\"s3:ListAccessGrants\",\"s3:ListAccessGrantsLocations\",\"s3:GetDataAccess\",
\"s3:GetAccessGrantsInstanceForPrefix\",\"s3:ListCallerAccessGrants\"],\"Resource\":
\"arn:aws:
s3:us-east-2:111122223333:access-grants/default\"}]}",
"CreatedAt": "2023-06-16T00:07:47.473000+00:00"
}
```

Example S3 Access Grants リソースポリシーを削除する

S3 Access Grants リソースポリシーを削除するには、次のサンプルコマンドを使用します。このコマンド例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3control delete-access-grants-instance-resource-policy \
--account-id 111122223333 \
--region us-east-2
```

```
// No response body
```

REST API の使用

PutAccessGrantsInstanceResourcePolicy API を使用してリソースポリシーを追加できます。

アカウント 111122223333 の S3 Access Grants インスタンスへのクロスアカウントアクセスを 2 番目のアカウント 444455556666 に付与する場合、アカウント 111122223333 の S3 Access Grants インスタンスのリソースポリシーは、2 番目のアカウント 444455556666 に次のアクションを実行するアクセス許可を付与する必要があります。

- `s3:ListAccessGrants`
- `s3:ListAccessGrantsLocations`
- `s3:GetDataAccess`
- `s3:GetAccessGrantsInstanceForPrefix`

S3 Access Grants インスタンスのリソースポリシーで、S3 Access Grants インスタンスの ARN を `Resource` として指定し、2 番目のアカウント 444455556666 を `Principal` として指定します。次の例を使用する際は、*###############*を独自の情報に置き換えます。

```
{
"Version": "2012-10-17",
"Statement": [
{
 "Effect": "Allow",
 "Principal": {
 "AWS": "444455556666"
},
 "Action": [
  "s3:ListAccessGrants",
  "s3:ListAccessGrantsLocations",
  "s3:GetDataAccess",
  "s3:GetAccessGrantsInstanceForPrefix"
 ],
 "Resource": "arn:aws:s3:us-east-2:111122223333:access-grants/default"
} ]
}
```

その後、PutAccessGrantsInstanceResourcePolicy API を使用して、ポリシーを設定できます。

S3 Access Grants インスタンスのリソースポリシーを更新、取得、または削除するための REST API サポートの詳細については、「Amazon Simple Storage Service API リファレンス」の次のセクションを参照してください。

- PutAccessGrantsInstanceResourcePolicy
- GetAccessGrantsInstanceResourcePolicy
- DeleteAccessGrantsInstanceResourcePolicy

AWS SDK の使用

このセクションでは、S3 アクセス許可リソース ポリシーを設定して 2 番目の AWS アカウントに S3 データの一部へのアクセスを許可する方法の AWS SDK の例を示します。

Java

リソースポリシーを追加、更新、取得、または削除して、S3 Access Grants インスタンスへのクロスアカウントアクセスを管理します。

Example S3 Access Grants インスタンスのリソースポリシーを追加または更新する

アカウント 111122223333 の S3 Access Grants インスタンスへのクロスアカウントアクセスを 2 番目のアカウント 444455556666 に付与する場合、アカウント 111122223333 の S3 Access Grants インスタンスのリソースポリシーは、2 番目のアカウント 444455556666 に次のアクションを実行するアクセス許可を付与する必要があります。

- `s3:ListAccessGrants`
- `s3:ListAccessGrantsLocations`
- `s3:GetDataAccess`
- `s3:GetAccessGrantsInstanceForPrefix`

S3 Access Grants インスタンスのリソースポリシーで、S3 Access Grants インスタンスの ARN を `Resource` として指定し、2 番目のアカウント 444455556666 を `Principal` として指定します。次の例を使用する際は、`###############`を独自の情報に置き換えます。

```
{
"Version": "2012-10-17",
"Statement": [
{
```

```
 "Effect": "Allow",
 "Principal": {
 "AWS": "444455556666"
},
 "Action": [
  "s3:ListAccessGrants",
  "s3:ListAccessGrantsLocations",
  "s3:GetDataAccess",
  "s3:GetAccessGrantsInstanceForPrefix"
 ],
 "Resource": "arn:aws:s3:us-east-2:111122223333:access-grants/default"
} ]
}
```

S3 Access Grants インスタンスのリソースポリシーを追加または更新するには、次のサンプルコードを使用します。

```
public void putAccessGrantsInstanceResourcePolicy() {
 PutAccessGrantsInstanceResourcePolicyRequest putRequest =
 PutAccessGrantsInstanceResourcePolicyRequest.builder()
 .accountId(111122223333)
 .policy(RESOURCE_POLICY)
 .build();
 PutAccessGrantsInstanceResourcePolicyResponse putResponse =
 s3Control.putAccessGrantsInstanceResourcePolicy(putRequest);
 LOGGER.info("PutAccessGrantsInstanceResourcePolicyResponse: " + putResponse);
 }
```

レスポンス:

```
PutAccessGrantsInstanceResourcePolicyResponse(
 Policy={
 "Version": "2012-10-17",
 "Statement": [{
 "Effect": "Allow",
 "Principal": {
 "AWS": "444455556666"
 },
 "Action": [
 "s3:ListAccessGrants",
 "s3:ListAccessGrantsLocations",
 "s3:GetDataAccess",
 "s3:GetAccessGrantsInstanceForPrefix",
```

```
 "s3:ListCallerAccessGrants"
 ],
 "Resource": "arn:aws:s3:us-east-2:111122223333:access-grants/default"
 }]
 }
 )
```

Example S3 Access Grants リソースポリシーを取得する

S3 Access Grants リソースポリシーを取得するには、次のサンプルコマンドを使用します。次のコマンド例を使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
public void getAccessGrantsInstanceResourcePolicy() {
 GetAccessGrantsInstanceResourcePolicyRequest getRequest =
 GetAccessGrantsInstanceResourcePolicyRequest.builder()
 .accountId(111122223333)
 .build();
 GetAccessGrantsInstanceResourcePolicyResponse getResponse =
 s3Control.getAccessGrantsInstanceResourcePolicy(getRequest);
 LOGGER.info("GetAccessGrantsInstanceResourcePolicyResponse: " + getResponse);
 }
```

レスポンス:

```
GetAccessGrantsInstanceResourcePolicyResponse(
 Policy={"Version":"2012-10-17","Statement":[{"Effect":"Allow","Principal":
{"AWS":"arn:aws:iam::444455556666:root"},"Action":
["s3:ListAccessGrants","s3:ListAccessGrantsLocations","s3:GetDataAccess","s3:GetAccessGrants
east-2:111122223333:access-grants/default"}]},
 CreatedAt=2023-06-15T22:54:44.319Z
 )
```

Example S3 Access Grants リソースポリシーを削除する

S3 Access Grants リソースポリシーを削除するには、次のサンプルコマンドを使用します。次のコマンド例を使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
public void deleteAccessGrantsInstanceResourcePolicy() {
 DeleteAccessGrantsInstanceResourcePolicyRequest deleteRequest =
 DeleteAccessGrantsInstanceResourcePolicyRequest.builder()
```

```
.accountId(111122223333)
.build();
DeleteAccessGrantsInstanceResourcePolicyResponse deleteResponse =
s3Control.putAccessGrantsInstanceResourcePolicy(deleteRequest);
LOGGER.info("DeleteAccessGrantsInstanceResourcePolicyResponse: " + deleteResponse);
}
```

レスポンス:

```
DeleteAccessGrantsInstanceResourcePolicyResponse()
```

ステップ 3: 2 番目のアカウントの IAM アイデンティティに、アカウント内の S3 Access Grants インスタンスを呼び出すためのアクセス許可を付与する

Amazon S3 データの所有者がアカウント 111122223333 の S3 Access Grants インスタンスのクロスアカウントポリシーを設定した後、2 番目のアカウント 444455556666 の所有者は、IAM ユーザーまたはロールのアイデンティティベースのポリシーを作成し、S3 Access Grants インスタンスへのアクセスを付与する必要があります。S3 Access Grants インスタンスのリソースポリシーで付与されている内容と付与するアクセス許可に応じて、アイデンティティベースのポリシーに次のアクションを 1 つまたは複数含めます。

- `s3:ListAccessGrants`
- `s3:ListAccessGrantsLocations`
- `s3:GetDataAccess`
- `s3:GetAccessGrantsInstanceForPrefix`
- `s3:ListCallerAccessGrants`

「AWS cross-account access pattern」に従って、2 番目のアカウント 444455556666 の IAM ユーザーまたはロールは、このようなアクセス許可を明示的に 1 つまたは複数持つ必要があります。例えば、IAM ユーザーまたはロールがアカウント 111122223333 内の S3 Access Grants インスタンスを呼び出して認証情報をリクエストできるように、`s3:GetDataAccess` アクセス許可を付与します。

このコマンド例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
{
```

```
 "Version": "2012-10-17",
 "Statement": [
 {
  "Effect": "Allow",
  "Action": [
   "s3:GetDataAccess",
  ],
   "Resource": "arn:aws:s3:us-east-2:111122223333:access-grants/default"
  }
 ]
}
```

IAM アイデンティティベースのポリシーの編集については、「AWS Identity and Access Management ガイド」の「IAM ポリシーの編集」を参照してください。

ステップ 4: アカウントの S3 Access Grants インスタンスで許可を作成して、2 番目のアカウントの IAM アイデンティティに S3 データの一部へのアクセスを許可します。

最後の設定ステップでは、アカウント 111122223333 の S3 Access Grants インスタンスに許可を作成します。これにより、2 番目のアカウント 444455556666 の IAM アイデンティティに、アカウント内の S3 データの一部へのアクセスが付与されます。これを行うには、Amazon S3 コンソール、CLI、API、SDK を使用できます。詳細については、「権限を作成する」を参照してください。

許可では、2 番目のアカウントの IAM アイデンティティの AWS ARN を指定して、アクセスを許可する S3 データの場所 (バケット、プレフィックス、またはオブジェクト) を指定します。この場所は、S3 Access Grants インスタンスに既に登録されている必要があります。詳細については、「ロケーションを登録する」を参照してください。必要に応じて、サブプレフィックスを指定することができます。例えば、アクセスを許可する場所がバケットで、そのバケット内の特定のオブジェクトへのアクセスをさらに制限したい場合は、オブジェクトキー名を `S3SubPrefix` フィールドで渡します。または、キー名が特定のプレフィックス (`2024-03-research-results/` など) で始まるバケット内のオブジェクトへのアクセスを制限したい場合は、`S3SubPrefix=2024-03-research-results/` を渡します。

2 番目のアカウントのアイデンティティに対するアクセス許可を作成するための CLI コマンドの例は、次のとおりです。詳細については「権限を作成する」を参照してください。このコマンド例を実行するには、*`user input placeholders`* をユーザー自身の情報に置き換えます。

```
aws s3control create-access-grant \
```

```
--account-id 111122223333 \
--access-grants-location-id default \
--access-grants-location-configuration S3SubPrefix=prefixA* \
--permission READ \
--grantee GranteeType=IAM,GranteeIdentifier=arn:aws:iam::444455556666:role/data-consumer-1
```

クロスアカウントアクセスを設定したら、2 番目のアカウントのユーザーまたはロールは次を実行できます。

- AWS RAM を介して共有されている S3 Access Grants インスタンスを一覧表示する `ListAccessGrantsInstances` を呼び出します。詳細については、「S3 Access Grants インスタンスの詳細を取得する」を参照してください。
- S3 Access Grants の一時的な認証情報をリクエストします。このようなリクエストを行う方法については、「S3 Access Grants を介して Amazon S3 データへのアクセスをリクエストする」を参照してください。

S3 Access Grants での AWS タグの使用

Amazon S3 Access Grants のタグは、Amazon S3 の オブジェクトタグ と類似の特性を持ちます。各タグはキーバリューのペアです。タグ付けできる S3 Access Grants のリソースは、S3 Access Grants インスタンス、ロケーション、権限 です。

> **Note**
>
> S3 アクセス権限でのタグ付けは、オブジェクトのタグ付けとは異なる API オペレーションを使用します。S3 Access Grants では、TagResource、UntagResource、ListTagsForResource API オペレーションを使用します。リソースは、S3 Access Grants インスタンス、登録済み口ケーション、またはアクセス権限です。

オブジェクトタグ 同様、次の制限が適用されます。

- 新しい S3 Access Grants リソースにタグを追加したり、既存のリソースにタグを追加したりできます。
- 単一のリソースに関連付けることができるのは、最大 10 タグまでです。複数のタグを同じリソースに関連付ける場合は、一意のタグキーが必要となります。

- タグキーには最大 128 個の Unicode 文字、タグ値には最大 256 個の Unicode 文字を使用できます。Amazon S3 オブジェクトタグは、内部的に UTF-16 で表現されます。UTF-16 では、文字は 1 文字または 2 文字分を使用することに注意が必要です。
- キーバリューでは大文字と小文字が区別されます。

タグの制限については、「AWS Billing ユーザーガイド」の「ユーザー定義のタグの制限」を参照してください。

AWS Command Line Interface (AWS CLI)、Amazon S3 REST API、または AWS SDK を使用して S3 Access Grants のリソースにタグ付けできます。

AWS CLI を使用する場合

AWS CLI をインストールするには、「AWS Command Line Interface ユーザーガイド」の「AWS CLI をインストールする」を参照してください。

S3 Access Grants リソースは、作成時または作成後にタグ付けできます。S3 Access Grants のタグ付けまたはタグの削除方法の説明は、次の例のとおりです。登録済みの口ケーションとアクセスグラントに対しても同様のオペレーションを実行できます。

次のコマンド例を使用する際は、*user input placeholders* をユーザー自身の情報に置き換えます。

Example – タグ付けされた S3 Access Grants インスタンスを作成する

```
aws s3control create-access-grants-instance \
 --account-id 111122223333 \
 --profile access-grants-profile \
 --region us-east-2 \
 --tags Key=tagKey1,Value=tagValue1
```

レスポンス:

```
 {
    "CreatedAt": "2023-10-25T01:09:46.719000+00:00",
    "AccessGrantsInstanceId": "default",
    "AccessGrantsInstanceArn": "arn:aws:s3:us-east-2:111122223333:access-grants/
default"
}
```

Example – 既に作成済みの S3 Access Grants インスタンスにタグ付けする

```
aws s3control tag-resource \
--account-id 111122223333 \
--resource-arn "arn:aws:s3:us-east-2:111122223333:access-grants/default" \
--profile access-grants-profile \
--region us-east-2 \
--tags Key=tagKey2,Value=tagValue2
```

Example – S3 Access Grants インスタンスのタグを一覧表示する

```
aws s3control list-tags-for-resource \
--account-id 111122223333 \
--resource-arn "arn:aws:s3:us-east-2:111122223333:access-grants/default" \
--profile access-grants-profile \
--region us-east-2
```

レスポンス:

```
{
    "Tags": [
        {
            "Key": "tagKey1",
            "Value": "tagValue1"
        },
        {
            "Key": "tagKey2",
            "Value": "tagValue2"
        }
    ]
}
```

Example – S3 Access Grants インスタンスのタグ付けを解除する

```
aws s3control untag-resource \
 --account-id 111122223333 \
 --resource-arn "arn:aws:s3:us-east-2:111122223333:access-grants/default" \
 --profile access-grants-profile \
 --region us-east-2 \
 --tag-keys "tagKey2"
```

REST API の使用

Amazon S3 API を使用して、S3 Access Grants インスタンス、登録済みの口ケーション、またはアクセス権限のタグを付けたり、タグを解除したり、タグを一覧表示したりできます。REST API での S3 Access Grants タグ管理のサポートの詳細については、「Amazon Simple Storage Service API リファレンス」の次のセクションを参照してください。

- TagResource
- UntagResource
- ListTagsForResource

S3 Access Grants の制約

S3 Access Grants には、次のとおりの制約があります。

> **Note**
>
> ユースケースがこのような制限を超える場合は、AWS サポート に連絡して制限の引き上げをリクエストしてください。

S3 Access Grants インスタンス

作成できるのは、アカウントにつき AWS リージョン ごとに単一の S3 Access Grants インスタンス です。「S3 Access Grants インスタンスを作成する」を参照してください。

S3 Access Grants 口ケーション

S3 Access Grants インスタンスごとに登録できるのは、1,000 S3 Access Grants 口ケーション です。「S3 Access Grants 口ケーションを登録する」を参照してください。

権限

S3 Access Grants インスタンスごとに作成できるのは、100,000 権限 です。「権限を作成する」を参照してください。

S3 Access Grants の AWS リージョン

S3 Access Grants は現在、次の AWS リージョンで利用できます。

AWS リージョン コード	AWS リージョン 名
us-east-1	米国東部 (バージニア北部)
us-east-2	米国東部 (オハイオ)
us-west-1	米国西部 (北カリフォルニア)
us-west-2	米国西部 (オレゴン)
af-south-1	アフリカ (ケープタウン)
ap-east-1	アジアパシフィック (香港)
ap-northeast-1	アジアパシフィック (東京)
ap-northeast-2	アジアパシフィック (ソウル)
ap-northeast-3	アジアパシフィック (大阪)
ap-south-1	アジアパシフィック (ムンバイ)
ap-south-2	アジアパシフィック (ハイデラバード)
ap-southeast-1	アジアパシフィック (シンガポール)
ap-southeast-2	アジアパシフィック (シドニー)
ap-southeast-3	アジアパシフィック (ジャカルタ)
ap-southeast-4	アジアパシフィック (メルボルン)
ca-central-1	カナダ (中部)
ca-west-1	カナダ西部 (カルガリー)
eu-central-1	欧州 (フランクフルト)
eu-central-2	欧州 (チューリッヒ)
eu-north-1	欧州 (ストックホルム)

AWS リージョン コード	AWS リージョン 名
eu-south-1	欧州 (ミラノ)
eu-south-2	欧州 (スペイン)
eu-west-1	欧州 (アイルランド)
eu-west-2	欧州 (ロンドン)
eu-west-3	欧州 (パリ)
il-central-1	イスラエル (テルアビブ)
me-central-1	中東 (アラブ首長国連邦)
me-south-1	中東 (バーレーン)
sa-east-1	南米 (サンパウロ)
us-gov-east-1	AWS GovCloud (米国東部)
us-gov-west-1	AWS GovCloud (米国西部)

S3 Access Grants の統合

S3 Access Grants は、次の AWS サービスと機能と連携できます。このページは、新しい統合が利用可能になると更新されます。

Amazon Athena

- IAM アイデンティティセンターが有効になっている Athena ワークグループの使用

Amazon EMR

- S3 Access Grants を使用した Amazon EMR クラスターの起動

Amazon EMR on EKS

- S3 Access Grants を使用した Amazon EMR on EKS クラスターの起動

Amazon EMR Serverless アプリケーション

- S3 Access Grants を使用した Amazon EMR Serverless アプリケーションの起動

Amazon Redshift

- Amazon Redshift と Amazon S3 Access Grants の統合

Amazon SageMaker AI Studio

- Amazon S3 Access Grants を Amazon SageMaker AI Studio および SDK for Python (Boto3) プラグインで使用

  SDK for Python (Boto3) プラグインを使用することで、Amazon SageMaker AI Studio ノートブックでの S3 Access Grants の使用がより簡単になります。IAM プリンシパルと AWS IAM Identity Center ディレクトリユーザーのアクセス許可を事前に設定します。Amazon SageMaker AI Studio は ID プロバイダーディレクトリユーザーをネイティブにサポートしていませんが、これらの ID が S3 Access Grants を介して S3 データにアクセスできるようにするプラグインを使用することで、カスタム Python コードを記述できます。データアクセスは、Amazon SageMaker AI ではなくプラグインを使用して行われます。

AWS Glue

- Amazon S3 Access Grants と AWS Glue

AWS IAM Identity Center

- アプリケーション間での信頼されたアイデンティティのプロパゲーション

AWS Transfer Family

- AWS Transfer Family 用に Amazon S3 Access Grants を設定する

Storage Browser for S3

- Storage Browser for S3 を使用した大規模なデータアクセスの管理

オープンソースの Python フレームワーク

- Amazon S3 Access Grants とオープンソースの Python フレームワークの統合

ACL によるアクセス管理

アクセスコントロールリスト (ACL) はリソースベースのオプションの 1 つであり、バケットとオブジェクトへのアクセスを管理するために使用できます。ACL を使用して、基本的な読み取り/書き込

み許可を他の AWS アカウントに付与できます。ACL によるアクセス許可の管理にはいくつかの制限があります。

例えば、アクセス許可を付与できるのは他の AWS アカウント だけで、自分のアカウントのユーザーには付与できません。条件付きアクセス許可を付与することはできず、アクセス許可を明示的に拒否することもできません。ACL が適しているのは、特定のいくつかのシナリオです。例えば、バケット所有者が他の AWS アカウント にオブジェクトのアップロードを許可している場合、これらのオブジェクトへのアクセス許可を管理する方法は、オブジェクトを所有する AWS アカウント によるオブジェクト ACL を使用する以外にありません。

S3 オブジェクト所有権は、Amazon S3 バケットレベルの設定で、バケットにアップロードされる新しいオブジェクト所有権を制御し、ACL を無効にするのに使用できます。デフォルトでは、オブジェクト所有権はバケット所有者の強制設定に設定され、すべての ACL は無効になります。ACL を無効にすると、バケット所有者はバケット内のすべてのオブジェクトを所有し、アクセス管理ポリシーのみを使用してデータへのアクセスを管理します。

Amazon S3 の最新のユースケースの大部分では ACL を使用する必要がなくなっています。オブジェクトごとに個別に制御する必要がある通常ではない状況を除き、ACL は無効にしておくことをお勧めします。ACL を無効にすると、誰がオブジェクトをバケットにアップロードしたかに関係なく、ポリシーを使用してバケット内のすべてのオブジェクトへのアクセスを制御できます。詳細については、「オブジェクトの所有権の制御とバケットの ACL の無効化。」を参照してください。

> **Important**
>
> 汎用バケットで S3 のオブジェクト所有者に [バケット所有者の強制] 設定を使用する場合は、ポリシーを使用して汎用バケットとその中のオブジェクトへのアクセスを許可する必要があります。バケット所有者強制設定が有効になっている場合、アクセスコントロールリスト (ACL) の設定または ACL の更新は失敗し、`AccessControlListNotSupported` エラーコードが返されます。ACL の読み取り要求は引き続きサポートされています。

ACL の詳細については、次のトピックを参照してください。

トピック

- アクセスコントロールリスト (ACL) の概要
- ACL の設定
- ACL のポリシーの例

アクセスコントロールリスト (ACL) の概要

Amazon S3 のアクセスコントロールリスト (ACL) では、バケットとオブジェクトへのアクセスを管理できます。各バケットとオブジェクトには、サブリソースとして ACL がアタッチされています。これにより、アクセスが許可される AWS アカウントまたはグループと、アクセスの種類が定義されます。リソースに対するリクエストを受け取ると、Amazon S3 は該当する ACL を確認して、リクエスタに必要なアクセス許可があることを確かめます。

S3 オブジェクト所有権は、Amazon S3 バケットレベルの設定で、バケットにアップロードされる新しいオブジェクト所有権を制御し、ACL を無効にするのに使用できます。デフォルトでは、オブジェクト所有権はバケット所有者の強制設定に設定され、すべての ACL は無効になります。ACL を無効にすると、バケット所有者はバケット内のすべてのオブジェクトを所有し、アクセス管理ポリシーのみを使用してデータへのアクセスを管理します。

Amazon S3 の最新のユースケースの大部分では ACL を使用する必要がなくなっています。オブジェクトごとに個別に制御する必要がある通常ではない状況を除き、ACL は無効にしておくことをお勧めします。ACL を無効にすると、誰がオブジェクトをバケットにアップロードしたかに関係なく、ポリシーを使用してバケット内のすべてのオブジェクトへのアクセスを制御できます。詳細については、「オブジェクトの所有権の制御とバケットの ACL の無効化。」を参照してください。

> **Important**
>
> 汎用バケットで S3 のオブジェクト所有者に [バケット所有者の強制] 設定を使用する場合は、ポリシーを使用して汎用バケットとその中のオブジェクトへのアクセスを許可する必要があります。バケット所有者強制設定が有効になっている場合、アクセスコントロールリスト (ACL) の設定または ACL の更新は失敗し、`AccessControlListNotSupported` エラーコードが返されます。ACL の読み取り要求は引き続きサポートされています。

バケットまたはオブジェクトを作成すると、Amazon S3 はリソースのフルコントロールをリソースの所有者に付与するデフォルトの ACL を作成します。これを、以下のバケット ACL のサンプルで示します (デフォルトのオブジェクト ACL は同じ構造です)。

Example

```
<?xml version="1.0" encoding="UTF-8"?>
<AccessControlPolicy xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Owner>
    <ID>*** Owner-Canonical-User-ID ***</ID>
    <DisplayName>owner-display-name</DisplayName>
```

```
  </Owner>
  <AccessControlList>
    <Grant>
      <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
               xsi:type="Canonical User">
        <ID>*** Owner-Canonical-User-ID ***</ID>
        <DisplayName>display-name</DisplayName>
      </Grantee>
      <Permission>FULL_CONTROL</Permission>
    </Grant>
  </AccessControlList>
</AccessControlPolicy>
```

サンプル ACL には、Owner の正規ユーザー ID を通じて所有者を識別する AWS アカウント エレメントが含まれています。正規ユーザー ID を見つける手順については、「AWS アカウントの正規ユーザー ID の検索」を参照してください。Grant エレメントは、被付与者 (AWS アカウント またはあらかじめ定義されたグループ) と付与されたアクセス許可を識別します。このデフォルトの ACL には、所有者に対する 1 つの Grant エレメントがあります。Grant エレメントを追加してアクセス許可を付与します。各許可は被付与者とアクセス許可を識別します。

> **Note**
>
> 1 つの ACL には最大 100 個の許可を指定することができます。

トピック

- 被付与者とは
- 付与できるアクセス許可
- 一般的な Amazon S3 リクエストの aclRequired 値
- サンプル ACL
- 既定 ACL

被付与者とは

> **Important**
>
> サポート終了通知: 2025 年 10 月 1 日以降、Amazon S3 は新しい E メール被付与者アクセスコントロールリスト (ACL) の作成のサポートを終了します。この日付より前に作成された E

メール被付与者 ACL は引き続き機能し、AWS マネジメントコンソール、コマンドラインインターフェイス (CLI)、SDK、および REST API から引き続きアクセスできます。ただし、新しい E メール被付与者 ACL は作成できなくなります。
2025 年 7 月 1 日から 2025 年 10 月 1 日の間は、新しい E メール被付与者 ACL を作成しようとすると、Amazon S3 へのリクエストで HTTP 405 エラーの発生率が高くなります。
この変更は、米国東部 (バージニア北部)、米国西部 (北カリフォルニア)、米国西部 (オレゴン)、アジアパシフィック (シンガポール)、アジアパシフィック (シドニー)、アジアパシフィック (東京)、欧州 (アイルランド)、南米 (サンパウロ) の各 AWS リージョンに影響します。

被付与者とは、AWS アカウントまたは事前定義済みのいずれかの Amazon S3 グループです。E メールアドレスまたは正規ユーザー ID を使用して AWS アカウントに許可を付与します。ただし、付与のリクエストでメールアドレスを指定すると、Amazon S3 はそのアカウントの正規ユーザー ID を確認して ACL に追加します。その結果、ACL には AWS アカウントの E メールアドレスではなく、常に AWS アカウントの正規ユーザー ID が含まれます。

アクセス権限を付与する場合は、各被付与者を *type*="*value*" のペアとして指定します。*type* は以下のいずれかです。

- `id` – 指定された値が AWS アカウントの正規ユーザー ID である場合
- `uri` - 事前定義されたグループにアクセス許可を付与する場合
- `emailAddress` – 指定された値が AWS アカウントの E メールアドレスである場合

Important

E メールアドレスを使用した被付与者の指定は、次の AWS リージョンでのみサポートされています。

- 米国東部(バージニア北部)
- 米国西部 (北カリフォルニア)
- 米国西部 (オレゴン)
- アジアパシフィック (シンガポール)
- アジアパシフィック (シドニー)
- アジアパシフィック (東京)
- 欧州 (アイルランド)

- 南米 (サンパウロ)

Amazon S3 でサポートされているリージョンとエンドポイントの一覧については、Amazon Web Services 全般のリファレンス の「リージョンとエンドポイント」を参照してください。

Example 例: E メールアドレス

例えば、次の x-amz-grant-read ヘッダーは、E メールアドレスによって識別される AWS アカウント に、オブジェクトデータとそのメタデータを読み取るアクセス許可を付与します。

```
x-amz-grant-read: emailAddress="xyz@example.com", emailAddress="abc@example.com"
```

Warning

他の AWS アカウントに自分のリソースへのアクセスを許可した場合、その AWS アカウントはアカウント内のユーザーに許可を委任できることに注意してください。これはクロスアカウントアクセスと呼ばれています。クロスアカウントアクセスの使用については、「IAM ユーザーガイド」の「IAM ユーザーにアクセス許可を委任するロールの作成」を参照してください。

AWS アカウントの正規ユーザー ID の検索

正規ユーザー ID は、AWS アカウントに関連付けられています。この ID は、次のような長い文字列です。

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

アカウントの正規ユーザー ID を検索する方法については、「AWS Account Management リファレンスガイド」の「AWS アカウント の正規ユーザー ID を検索する」を参照してください。

また、AWS アカウントがアクセス許可を持つバケットまたはオブジェクトの ACL を読み取って、AWS アカウントの正規ユーザー ID を検索することもできます。許可リクエストによって個別の AWS アカウントに許可が付与された場合、ACL にはアカウントの正規ユーザー ID が含まれた許可エントリが追加されます。

> **Note**
>
> バケットをパブリックにした場合 (非推奨)、認証されていないどのユーザーもバケットにオブジェクトをアップロードできます。これらの匿名ユーザーは AWS アカウントを持っていません。匿名ユーザーがバケットにオブジェクトをアップロードすると、Amazon S3 によって特殊な正規ユーザー ID (65a011a29cdf8ec533ec3d1ccaae921c) がそのオブジェクトの所有者として ACL で追加されます。詳細については、「Amazon S3 のバケットとオブジェクトの所有権」を参照してください。

Amazon S3 の事前定義済みのグループ

Amazon S3 には、事前定義済みの一連のグループがあります。グループにアカウントアクセスを許可するときは、正規ユーザー ID の代わりに Amazon S3 のいずれかの URI を指定します。Amazon S3 には、以下の事前に定義されたグループが用意されています。

- Authenticated Users グループ – `http://acs.amazonaws.com/groups/global/AuthenticatedUsers` で表されます。

  このグループはすべて AWS アカウントを表しています。このグループへのアクセス許可により、AWS アカウント がリソースにアクセスできます。ただし、すべてのリクエストは署名(認証)されている必要があります。

  > **Warning**
  >
  > Authenticated Users グループにアクセスを許可すると、世界中の認証された AWS ユーザーがリソースにアクセスできます。

- All Users グループ – `http://acs.amazonaws.com/groups/global/AllUsers` で表されます。

  このグループへのアクセス許可により、世界中の誰でもリソースにアクセスすることが許可されます。リクエストは署名(認証)済み、または署名なし(匿名)とすることができます。署名なしのリクエストでは、リクエストの Authentication ヘッダーが省略されます。

  > **Warning**
  >
  > All Users グループには、`WRITE`、`WRITE_ACP`、または `FULL_CONTROL` アクセス許可を一切付与しないことを強くお勧めします。例えば、`WRITE` アクセス許可は所有者以外のユー

ザーが既存のオブジェクトを上書きまたは削除することを許可しませんが、WRITE アクセス許可はすべてのユーザーがバケットにオブジェクトを格納することを許可し、この料金はお客様に請求されます。これらのアクセス許可の詳細については、次のセクション 付与できるアクセス許可 を参照してください。

- Log Delivery グループ – http://acs.amazonaws.com/groups/s3/LogDelivery で表されます。

  バケットに対する WRITE アクセス許可により、このグループはサーバーアクセスログ (「サーバーアクセスログによるリクエストのログ記録」を参照) をバケットに書き込むことができます。

> **Note**
>
> ACL を使用する場合、被付与者は AWS アカウントまたは事前定義済みのいずれかの Amazon S3 グループです。被付与者を IAM ユーザーとすることはできません。IAM 内の AWS ユーザーおよびアクセス許可の詳細については、「AWS Identity and Access Management の使用」を参照してください。

付与できるアクセス許可

以下の表に、Amazon S3 の ACL でサポートされている一連のアクセス許可を示します。ACL アクセス許可のセットは、オブジェクト ACL とバケット ACL で同じです。ただし、コンテキスト (バケット ACL かオブジェクト ACL か) に応じて、これらの ACL アクセス許可は特定のバケットまたはオブジェクトオペレーションのためのアクセス許可を付与します。この表では、アクセス許可の一覧と、オブジェクトとバケットにおけるその意味について説明しています。

Amazon S3 コンソールでの ACL アクセス権限の詳細については、「ACL の設定」を参照してください。

アクセス許可	バケット上で付与された場合	オブジェクト上で付与された場合
READ	被付与者がバケット内のオブジェクトをリストすることを許可します	被付与者がオブジェクトデータとそのメタデータを読み込むことを許可します
WRITE	被付与者がバケット内に新しいオブジェクトを作成できるようにします。既存の	該当しません

アクセス許可	バケット上で付与された場合	オブジェクト上で付与された場合
	オブジェクトのバケット所有者およびオブジェクト所有者には、これらのオブジェクトの削除と上書きも許可します。	
READ_ACP	被付与者がバケット ACL を読み込むことを許可します	被付与者がオブジェクト ACL を読み込むことを許可します
WRITE_ACP	被付与者が該当するバケットの ACL を書き込むことを許可します	被付与者が該当するオブジェクトの ACL を書き込むことを許可します
FULL_CONTROL	バケットに対する READ、WRITE、READ_ACP、WRITE_AC のアクセス許可を被付与者に付与します	オブジェクトに対する READ、READ_ACP、WRITE_ACP のアクセス許可を被付与者に付与します

> **Warning**
>
> S3 バケットとオブジェクトにアクセス許可を付与するときは注意が必要です。例えば、あるバケットに対する WRITE のアクセス権を付与すると、被付与者はそのバケットにオブジェクトを作成できます。アクセス許可を付与する前に、「アクセスコントロールリスト (ACL) の概要」セクション全体を読むことを強くお勧めします。

ACL アクセス許可とアクセスポリシーのアクセス許可のマッピング

前の表に示したように、ACL で使用できるアクセス許可のセットは、アクセスポリシーで設定できるアクセス許可に比べると限定されています (「Amazon S3 のポリシーアクション」を参照してください)。これらのアクセス許可はそれぞれ、Amazon S3 の 1 つ以上のオペレーションを許可します。

次の表は、ACL アクセス権限のそれぞれが、対応するアクセスポリシーのアクセス許可にどのようにマッピングされるかを示します。ご覧のように、アクセスポリシーでは ACL よりも多くのアクセス許可が付与されています。ACL は主に、ファイルシステムのアクセス許可と同様に、基本的な読み取り/書き込みアクセス許可を付与するために使用されます。ACL の使用が適している場合の詳細については、Amazon S3 用 Identity and Access Management を参照してください。

Amazon S3 コンソールでの ACL アクセス権限の詳細については、ACL の設定 を参照してください。

ACL アクセス許可	ACL アクセス許可がバケットに付与される場合の、対応するアクセスポリシーのアクセス許可	ACL アクセス許可がオブジェクトに付与される場合の、対応するアクセスポリシーのアクセス許可
READ	s3:ListBucket 、s3:ListBucketVersions 、および s3:ListBucketMultipartUploads	s3:GetObject および s3:GetObjectVersion
WRITE	s3:PutObject バケット所有者は、バケット内の任意のオブジェクトを作成、上書き、削除でき、オブジェクト所有者はそのオブジェクトに対する FULL_CONTROL を有します。 さらに、被付与者がバケット所有者であるときは、バケットの ACL で WRITE アクセス許可を付与すると、そのバケット内の任意のバージョンに対して s3:DeleteObjectVersion アクションを実行できるようになります。	該当しません
READ_ACP	s3:GetBucketAcl	s3:GetObjectAcl および s3:GetObjectVersionAcl
WRITE_ACP	s3:PutBucketAcl	s3:PutObjectAcl および s3:PutObjectVersionAcl
FULL_CONTROL	これは、READ、WRITE、READ_ACP、および WRITE_ACP ACL アクセス許可を付与するのと同等です。したがっ	これは、READ、READ_ACP、および WRITE_ACP ACL アクセス許可を付与するのと同等です。したがって、この ACL アクセス許可は、対応するア

ACL アクセス許可	ACL アクセス許可がバケットに付与される場合の、対応するアクセスポリシーのアクセス許可	ACL アクセス許可がオブジェクトに付与される場合の、対応するアクセスポリシーのアクセス許可
	て、この ACL アクセス許可は、対応するアクセスポリシーのアクセス許可の組み合わせにマッピングされます。	クセスポリシーのアクセス許可の組み合わせにマッピングされます。

条件キー

アクセスポリシー権限を付与する場合、条件キーを使用して、バケットポリシーを使用するオブジェクトの ACL の値を制限できます。以下のコンテキストキーは ACL に対応しています。これらのコンテキストキーを使用して、リクエストで特定の ACL の使用を強制することができます。

- `s3:x-amz-grant-read` - 読み取りアクセスが必要です。
- `s3:x-amz-grant-write` - 書き込みアクセスが必要です。
- `s3:x-amz-grant-read-acp` - バケットの ACL への読み取りアクセスが必要です。
- `s3:x-amz-grant-write-acp` - バケットの ACL への書き込みアクセスが必要です。
- `s3:x-amz-grant-full-control` - フルコントロールが必要です。
- `s3:x-amz-acl` - 既定 ACL が必要です。

ACL 固有のヘッダーを含むポリシーの例については、「バケット所有者にフルコントロールを与えることを条件として s3:PutObject のアクセス許可を付与する」を参照してください。Amazon S3 固有の条件キーの完全なリストについては、「サービス認可リファレンス」の「Actions, resources, and condition keys for Amazon S3」を参照してください。

S3 リソースタイプ別の S3 API オペレーションへのアクセス許可の詳細については、「Amazon S3 API オペレーションに必要なアクセス許可」を参照してください。

一般的な Amazon S3 リクエストの `aclRequired` 値

承認に ACL を必要とした Amazon S3 リクエストを特定するには、Amazon S3 サーバーアクセスログまたは AWS CloudTrail の `aclRequired` 値を使用できます。CloudTrail または Amazon S3 サーバーアクセスログに表示される `aclRequired` 値は、呼び出されたオペレーションと、リクエスター、オブジェクト所有者、バケット所有者に関する特定の情報によって異なります。ACL が不要であったか、`bucket-owner-full-control` の既定 ACL を設定するか、リクエストがバケットポ

リシーで許可されている場合、aclRequired 値の文字列は Amazon S3 サーバーアクセスログでは「-」となり、CloudTrail では存在しません。

以下の表は、さまざまな Amazon S3 API オペレーションに対して CloudTrail または Amazon S3 サーバーアクセスログで期待される aclRequired 値を示しています。この情報から、どの Amazon S3 オペレーションが承認に関して ACL に依存しているかを理解できます。以下の表で、A、B、C は、リクエスター、オブジェクト所有者、バケット所有者と関連する各アカウントを表しています。アスタリスク (*) が付いているエントリは、A、B、C のうち、任意のアカウントを示します。

> **Note**
>
> 次の表の PutObject オペレーションは、特に明記しない限り、ACL を設定しないリクエストを示します。ただし、ACL が bucket-owner-full-control ACL である場合を除きます。aclRequired の値が NULL の場合、aclRequired は AWS CloudTrail ログに存在しないことを示します。

次の表は、CloudTrail の aclRequired 値を示しています。

オペレーション名	リクエスタ	オブジェクト所有者	バケット所有者	バケットポリシーはアクセスを許可する	**aclRequired 値**	理由
GetObject	A	A	A	はい/いいえ	null	同一アカウントアクセス
GetObject	A	B	A	はい/いいえ	null	同一アカウントアクセス (バケット所有者の強制による)
GetObject	A	A	B	はい	null	クロスアカウントア

オペレーション名	リクエスタ	オブジェクト所有者	バケット所有者	バケットポリシーはアクセスを許可する	**aclRequired** 値	理由
						クセスがバケットポリシーで許可される
GetObject	A	A	B	いいえ	はい	クロスアカウントアクセスは ACL に依存する
GetObject	A	A	B	はい	null	クロスアカウントアクセスがバケットポリシーで許可される
GetObject	A	B	B	いいえ	はい	クロスアカウントアクセスは ACL に依存する
GetObject	A	B	C	はい	null	クロスアカウントアクセスがバケットポリシーで許可される

オペレーション名	リクエスタ	オブジェクト所有者	バケット所有者	バケットポリシーはアクセスを許可する	**aclRequired** 値	理由
GetObject	A	B	C	いいえ	はい	クロスアカウントアクセスは ACL に依存する
PutObject	A	該当しない	A	はい/いいえ	null	同一アカウントアクセス
PutObject	A	該当しない	B	はい	null	クロスアカウントアクセスがバケットポリシーで許可される
PutObject	A	該当しない	B	いいえ	はい	クロスアカウントアクセスは ACL に依存する
ACL による PutObject (bucket-owner-full-control を除く)	*	該当しない	*	はい/いいえ	はい	リクエストは ACL を許可する

オペレーション名	リクエスタ	オブジェクト所有者	バケット所有者	バケットポリシーはアクセスを許可する	**aclRequired** 値	理由
ListObjects	A	該当しない	A	はい/いいえ	null	同一アカウントアクセス
ListObjects	A	該当しない	B	はい	null	クロスアカウントアクセスがバケットポリシーで許可される
ListObjects	A	該当しない	B	いいえ	はい	クロスアカウントアクセスは ACL に依存する
DeleteObject	A	該当しない	A	はい/いいえ	null	同一アカウントアクセス
DeleteObject	A	該当しない	B	はい	null	クロスアカウントアクセスがバケットポリシーで許可される
DeleteObject	A	該当しない	B	いいえ	はい	クロスアカウントアクセスは ACL に依存する

オペレーション名	リクエスタ	オブジェクト所有者	バケット所有者	バケットポリシーはアクセスを許可する	**aclRequired** 値	理由
PutObjectAcl	*	*	*	はい/いいえ	はい	リクエストは ACL を許可する
PutBucketAcl	*	該当しない	*	はい/いいえ	はい	リクエストは ACL を許可する

> **Note**
>
> 次の表の REST.PUT.OBJECT オペレーションは、特に明記しない限り、ACL を設定しないリクエストを示します。ただし、ACL が bucket-owner-full-control ACL である場合を除きます。aclRequired 値の文字列「-」は、Amazon S3 サーバーアクセスログの NULL 値を示します。

次の表は、Amazon S3 サーバーアクセスログの aclRequired 値を示しています。

オペレーション名	リクエスタ	オブジェクト所有者	バケット所有者	バケットポリシーはアクセスを許可する	**aclRequired** 値	理由
REST.GET.OBJECT	A	A	A	はい/いいえ	-	同一アカウントアクセス
REST.GET.OBJECT	A	B	A	はい/いいえ	-	同一アカウントアクセス (バケット所有者の

オペレーション名	リクエスタ	オブジェクト所有者	バケット所有者	バケットポリシーはアクセスを許可する	**aclRequired** 値	理由
						強制による)
REST.GET.OBJECT	A	A	B	はい	-	クロスアカウントアクセスがバケットポリシーで許可される
REST.GET.OBJECT	A	A	B	いいえ	はい	クロスアカウントアクセスは ACL に依存する
REST.GET.OBJECT	A	B	B	はい	-	クロスアカウントアクセスがバケットポリシーで許可される
REST.GET.OBJECT	A	B	B	いいえ	はい	クロスアカウントアクセスは ACL に依存する

オペレーション名	リクエスタ	オブジェクト所有者	バケット所有者	バケットポリシーはアクセスを許可する	**aclRequired** 値	理由
REST.GET.OBJECT	A	B	C	はい	-	クロスアカウントアクセスがバケットポリシーで許可される
REST.GET.OBJECT	A	B	C	いいえ	はい	クロスアカウントアクセスは ACL に依存する
REST.PUT.OBJECT	A	該当しない	A	はい/いいえ	-	同一アカウントアクセス
REST.PUT.OBJECT	A	該当しない	B	はい	-	クロスアカウントアクセスがバケットポリシーで許可される
REST.PUT.OBJECT	A	該当しない	B	いいえ	はい	クロスアカウントアクセスは ACL に依存する

オペレーション名	リクエスタ	オブジェクト所有者	バケット所有者	バケットポリシーはアクセスを許可する	**aclRequired** 値	理由
ACL による REST.PUT.OBJECT (bucket-owner-full-control を除く)	*	該当しない	*	はい/いいえ	はい	リクエストは ACL を許可する
REST.GET.BUCKET	A	該当しない	A	はい/いいえ	-	同一アカウントアクセス
REST.GET.BUCKET	A	該当しない	B	はい	-	クロスアカウントアクセスがバケットポリシーで許可される
REST.GET.BUCKET	A	該当しない	B	いいえ	はい	クロスアカウントアクセスは ACL に依存する
REST.DELETE.OBJECT	A	該当しない	A	はい/いいえ	-	同一アカウントアクセス

オペレーション名	リクエスタ	オブジェクト所有者	バケット所有者	バケットポリシーはアクセスを許可する	**aclRequired** 値	理由
REST.DELETE.OBJECT	A	該当しない	B	はい	-	クロスアカウントアクセスがバケットポリシーで許可される
REST.DELETE.OBJECT	A	該当しない	B	いいえ	はい	クロスアカウントアクセスは ACL に依存する
REST.PUT.ACL	*	*	*	はい/いいえ	はい	リクエストは ACL を許可する

サンプル ACL

バケットの以下のサンプル ACL は、リソース所有者と一連の許可を識別します。形式は Amazon S3 REST API の ACL の XML 表現です。バケット所有者はリソースに対する FULL_CONTROL が許可されます。また、この ACL には、正規ユーザー ID で示されている 2 つの AWS アカウントと、前のセクションで説明した事前定義済みの 2 つの Amazon S3 グループに対して、リソースへの許可がどのように付与されるかが示されています。

Example

```
<?xml version="1.0" encoding="UTF-8"?>
<AccessControlPolicy xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Owner>
    <ID>Owner-canonical-user-ID</ID>
    <DisplayName>display-name</DisplayName>
  </Owner>
```

```
  <AccessControlList>
    <Grant>
      <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:type="CanonicalUser">
        <ID>Owner-canonical-user-ID</ID>
        <DisplayName>display-name</DisplayName>
      </Grantee>
      <Permission>FULL_CONTROL</Permission>
    </Grant>

    <Grant>
      <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:type="CanonicalUser">
        <ID>user1-canonical-user-ID</ID>
        <DisplayName>display-name</DisplayName>
      </Grantee>
      <Permission>WRITE</Permission>
    </Grant>

    <Grant>
      <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:type="CanonicalUser">
        <ID>user2-canonical-user-ID</ID>
        <DisplayName>display-name</DisplayName>
      </Grantee>
      <Permission>READ</Permission>
    </Grant>

    <Grant>
      <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="Group">
        <URI>http://acs.amazonaws.com/groups/global/AllUsers</URI>
      </Grantee>
      <Permission>READ</Permission>
    </Grant>
    <Grant>
      <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="Group">
        <URI>http://acs.amazonaws.com/groups/s3/LogDelivery</URI>
      </Grantee>
      <Permission>WRITE</Permission>
    </Grant>

  </AccessControlList>
</AccessControlPolicy>
```

既定 ACL

Amazon S3 では、既定 ACL と呼ばれる事前定義済みの一連の許可がサポートされています。各既定 ACL には、あらかじめ定義された一連の被付与者とアクセス権限が含まれています。以下の表に、一連の既定 ACL と、関連するあらかじめ定義された許可を示します。

既定 ACL	Applies to	ACL に追加されるアクセス許可
`private`	バケットとオブジェクト	所有者は `FULL_CONTROL` を取得します。他のユーザーにはアクセス許可は付与されません (デフォルト)。
`public-read`	バケットとオブジェクト	所有者は `FULL_CONTROL` を取得します。`AllUsers` グループ (被付与者とは を参照) は `READ` アクセス許可を取得します。
`public-read-write`	バケットとオブジェクト	所有者は `FULL_CONTROL` を取得します。`AllUsers` グループは `READ` および `WRITE` アクセス許可を取得します。通常、これをバケットで付与することはお勧めしません。
`aws-exec-read`	バケットとオブジェクト	所有者は `FULL_CONTROL` を取得します。Amazon EC2 には、Amazon S3 から Amazon マシンイメージ (AMI) バンドルを `GET` するための `READ` アクセスが許可されます。
`authenticated-read`	バケットとオブジェクト	所有者は `FULL_CONTROL` を取得します。`AuthenticatedUsers` グループは `READ` アクセス許可を取得します。
`bucket-owner-read`	オブジェクト	オブジェクト所有者は `FULL_CONTROL` を取得します。バケット所有者は `READ` を取得します。バケットの作成時にこの既定 ACL を指定しても、Amazon S3 には無視されます。
`bucket-owner-full-control`	オブジェクト	オブジェクト所有者とバケット所有者はオブジェクトに対する `FULL_CONTROL` を取得します。バケットの作

既定 ACL	Applies to	ACL に追加されるアクセス許可
		成時にこの既定 ACL を指定しても、Amazon S3 には無視されます。
`log-delivery-write`	バケット	`LogDelivery` グループはバケットに対する `WRITE` および `READ_ACP` アクセス許可を取得します。ログの詳細については、サーバーアクセスログによるリクエストのログ記録 を参照してください。

> **Note**
>
> リクエストではこれらの既定 ACL を 1 つのみ指定できます。

`x-amz-acl` リクエストヘッダーを使用して、リクエストに既定 ACL を指定します。Amazon S3 が既定 ACL を含むリクエストを受信すると、あらかじめ定義された許可がリソースの ACL に追加されます。

ACL の設定

このセクションでは、アクセスコントロールリスト (ACL) を使用して S3 バケットとオブジェクトのアクセス許可を管理する方法について説明します。リソース ACL に許可を追加するには、AWS Management Console、AWS Command Line Interface (CLI)、REST API、または AWS SDK を使用します。

バケットに対するアクセス許可とオブジェクトに対するアクセス許可は相互に独立しています。オブジェクトはバケットからアクセス許可を継承しません。例えば、バケットを作成してユーザーに書き込みアクセスを許可した場合、そのユーザーから明示的にアクセスが許可されない限り、そのユーザーのオブジェクトにアクセスできません。

他の AWS アカウント ユーザーまたは事前定義されたグループに許可を与えることができます。アクセス許可が付与されたユーザーまたはグループは、被付与者と呼ばれます。デフォルトでは、バケットを作成した AWS アカウントである所有者が、完全な許可を持っています。

ユーザーまたはグループに付与する各アクセス許可により、バケットに関連付けられたエントリが ACL に追加されます。ACL は、被付与者と付与されたアクセス許可を識別するリストを表示します。

S3 オブジェクト所有権は、Amazon S3 バケットレベルの設定で、バケットにアップロードされる新しいオブジェクト所有権を制御し、ACL を無効にするのに使用できます。デフォルトでは、オブジェクト所有権はバケット所有者の強制設定に設定され、すべての ACL は無効になります。ACL を無効にすると、バケット所有者はバケット内のすべてのオブジェクトを所有し、アクセス管理ポリシーのみを使用してデータへのアクセスを管理します。

Amazon S3 の最新のユースケースの大部分では ACL を使用する必要がなくなっています。オブジェクトごとに個別に制御する必要がある通常ではない状況を除き、ACL は無効にしておくことをお勧めします。ACL を無効にすると、誰がオブジェクトをバケットにアップロードしたかに関係なく、ポリシーを使用してバケット内のすべてのオブジェクトへのアクセスを制御できます。詳細については、「オブジェクトの所有権の制御とバケットの ACL の無効化。」を参照してください。

Important

汎用バケットで S3 のオブジェクト所有者に [バケット所有者の強制] 設定を使用する場合は、ポリシーを使用して汎用バケットとその中のオブジェクトへのアクセスを許可する必要があります。バケット所有者強制設定が有効になっている場合、アクセスコントロールリスト (ACL) の設定または ACL の更新は失敗し、`AccessControlListNotSupported` エラーコードが返されます。ACL の読み取り要求は引き続きサポートされています。

Warning

すべてのユーザー (パブリックアクセス)または認証されたユーザーグループ (すべての AWS 認証ユーザー) のグループへの書き込みアクセスを許可しないことを強くお勧めします。これらのグループに書き込みアクセスを許可した場合の影響の詳細については、Amazon S3 の事前定義済みのグループ を参照してください。

S3 コンソールを使用した、バケットの ACL アクセス権限の設定

コンソールには、重複した被付与者のアクセス権限がまとめて表示されます。ACL の全リストを表示するには、Amazon S3 REST API、AWS CLI、または AWS SDK を使用します。

次の表は、Amazon S3 コンソールでバケットに設定できる ACL アクセス権限を示しています。

バケットの Amazon S3 コンソールの ACL アクセス権限

コンソールのアクセス権限	ACL アクセス許可	アクセス
オブジェクト – リスト	READ	被付与者がバケット内のオブジェクトをリストすることを許可します。
オブジェクト – 書き込み	WRITE	被付与者がバケット内に新しいオブジェクトを作成できるようにします。既存のオブジェクトのバケット所有者およびオブジェクト所有者については、これらのオブジェクトの削除と上書きも許可します。
バケット ACL – 読み取り	READ_ACP	被付与者がバケット ACL を読み込むことを許可します。
バケット ACL – 書き込み	WRITE_ACP	被付与者が該当するバケットの ACL を書き込むことを許可します。
全員 (パブリックアクセス): オブジェクト – リスト	READ	バケット内のオブジェクトに対するパブリック読み取りアクセス権を付与します。リストアクセス権を [Everyone (public access)] (全員 (パブリックアクセス)) に付与すると、世界中のユーザーがバケット内のオブジェクトにアクセスできます。
全員 (パブリックアクセス) : バケット ACL – 読み取り	READ_ACP	バケット ACL のパブリック読み取りアクセス権を付与します。[Everyone (public access)] (全員 (パブリックアクセス)) に読み取りアクセス権を付与すると、世界中のユーザーがバケット ACL にアクセスできます。

ACL アクセス権限の詳細については、アクセスコントロールリスト (ACL) の概要 を参照してください。

> **Important**
>
> 汎用バケットで S3 のオブジェクト所有者に [バケット所有者の強制] 設定を使用する場合は、ポリシーを使用して汎用バケットとその中のオブジェクトへのアクセスを許可する必要

があります。バケット所有者強制設定が有効になっている場合、アクセスコントロールリスト (ACL) の設定または ACL の更新は失敗し、`AccessControlListNotSupported` エラーコードが返されます。ACL の読み取り要求は引き続きサポートされています。

バケットに ACL アクセス許可を設定する

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 左のナビゲーションペインで、[汎用バケット] を選択します。
3. [Buckets (バケット)] リストで、アクセス許可を設定するバケットの名前を選択します。
4. [Permissions] を選択します。
5. [アクセスコントロールリスト] で、[編集] を選択します。

   バケットに対する次の ACL アクセス許可を編集できます。

   オブジェクト

   - List (リスト) – 被付与者がバケット内のオブジェクトをリストすることを許可します
   - Write (書き込み) – 被付与者がバケット内に新しいオブジェクトを作成できるようにします。既存のオブジェクトのバケット所有者およびオブジェクト所有者については、これらのオブジェクトの削除と上書きも許可します。

     S3 コンソールでは、S3 ログデリバリーグループとバケット所有者 (AWS アカウント) にのみ書き込みアクセスを許可できます。他の被付与者には、書き込みアクセスを許可しないことを強くお勧めします。ただし、書き込みアクセスを許可する必要がある場合は、AWS CLI、AWS SDK、または REST API を使用できます。

   バケット ACL

   - Read (読み込み) – 被付与者がバケット ACL を読み込むことを許可します
   - Write (書き込み) – 被付与者が該当するバケットの ACL を書き込むことを許可します
6. バケット所有者の許可を変更するには、バケット所有者 (AWS アカウント)の横で、次の ACL アクセス権限を消去または選択します。

   - [Objects (オブジェクト)] – [List (リスト)] または [Write (書き込み)]
   - [Bucket ACL (バケット ACL)] – [Read (読み取り)] または [Write (書き込み)]

所有者とは、AWS アカウントのルートユーザーであり、AWS Identity and Access Management IAM ユーザーではありません。ルートユーザーの詳細については、IAM ユーザーガイドの「AWS アカウントのルートユーザー」を参照してください。

7. 一般ユーザー (インターネット上のすべてのユーザー) のアクセス許可を付与または取り消すには、[Everyone (public access) (全員 (パブリックアクセス))] の横で、次の ACL アクセス許可をクリアまたは選択します。

   - [Objects (オブジェクト)] – [List (リスト)]
   - [Bucket ACL (バケット ACL)] – [Read (読み取り)]

   > ⚠ Warning
   >
   > [全員] グループに S3 バケットへのパブリックアクセスを付与するときは注意が必要です。このグループにアクセスを付与すると、世界中のすべてのユーザーがバケットにアクセスできます。種類にかかわらず、S3 バケットへのパブリック書き込みアクセスは一切付与しないことを強くお勧めします。

8. AWS アカウント があれば誰でも許可を付与するか取り消すために、認証済みユーザーグループ (AWS アカウント があれば誰でも可) の横で、次の ACL アクセス権限を消去または選択します。

   - [Objects (オブジェクト)] – [List (リスト)]
   - [Bucket ACL (バケット ACL)] – [Read (読み取り)]

9. Amazon S3 がバケットにサーバーアクセスログを書き込むアクセス許可を付与または取り消すには、[S3 log delivery group (S3 ログ配信グループ)] で、次の ACL アクセス許可をクリアまたは選択します。

   - [Objects (オブジェクト)] – [List (リスト)] または [Write (書き込み)]
   - [Bucket ACL (バケット ACL)] – [Read (読み取り)] または [Write (書き込み)]

   バケットがアクセスログを受け取るターゲットバケットとして設定されている場合、バケットのアクセス許可は [ログ配信] グループのバケットへの書き込みアクセスを許可する必要があります。バケット上のサーバアクセスログ記録を有効にすると、Amazon S3 コンソールは、[Log Delivery (ログ配信)] グループにログを受信することを選択したターゲットバケットへの

書き込みアクセス権を付与します。サーバーアクセスログ記録の詳細については、「Amazon S3 サーバーアクセスログを有効にします。」を参照してください。

10. 別の AWS アカウントへの許可を付与するには、次の手順を実行します。

    a. [Add grantee (被付与者の追加)] を選択します。

    b. [Grantee] (被付与者) ボックスに、他の AWS アカウント の正規 ID を入力します。

    c. 次の ACL アクセス許可から選択します。

    - [Objects (オブジェクト)] – [List (リスト)] または [Write (書き込み)]
    - [Bucket ACL (バケット ACL)] – [Read (読み取り)] または [Write (書き込み)]

> ⚠ Warning
>
> 他の AWS アカウントに自分のリソースへのアクセスを許可した場合、その AWS アカウントはアカウント内のユーザーに許可を委任できることに注意してください。これはクロスアカウントアクセスと呼ばれています。クロスアカウントアクセスの使用については、IAM ユーザーガイドのIAM ユーザーにアクセス許可を委任するロールの作成を参照してください。

11. 別の AWS アカウント へのアクセスを削除するには、他の AWS アカウント へのアクセスで、削除を選択します。

12. 変更を保存するには、[変更の保存] を選択します。

S3 コンソールを使用した、オブジェクトの ACL アクセス権限の設定

コンソールには、重複した被付与者のアクセス権限がまとめて表示されます。ACL の全リストを表示するには、Amazon S3 REST API、AWS CLI、または AWS SDK を使用します。次の表に、Amazon S3 コンソールでオブジェクト用に設定できる ACL アクセス権限を示します。

オブジェクト用の Amazon S3 コンソールの ACL アクセス権限

コンソールのアクセス権限	ACL アクセス許可	アクセス
オブジェクト – 読み取り	READ	被付与者がオブジェクトデータとそのメタデータを読み込むことを許可します。

コンソールのアクセス権限	ACL アクセス許可	アクセス
オブジェクト ACL – 読み取り	READ_ACP	被付与者がオブジェクト ACL を読み込むことを許可します。
オブジェクト ACL – 書き込み	WRITE_ACP	被付与者が該当するオブジェクトの ACL を書き込むことを許可します

ACL アクセス権限の詳細については、アクセスコントロールリスト (ACL) の概要 を参照してください。

> **Important**
>
> 汎用バケットで S3 のオブジェクト所有者に [バケット所有者の強制] 設定を使用する場合は、ポリシーを使用して汎用バケットとその中のオブジェクトへのアクセスを許可する必要があります。バケット所有者強制設定が有効になっている場合、アクセスコントロールリスト (ACL) の設定または ACL の更新は失敗し、`AccessControlListNotSupported` エラーコードが返されます。ACL の読み取り要求は引き続きサポートされています。

オブジェクトに ACL アクセス権限を設定する

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. [Buckets] (バケット) リストで、オブジェクトが含まれるバケットの名前を選択します。
3. オブジェクトのリストで、アクセス許可を設定するオブジェクトの名前を選択します。
4. [Permissions] を選択します。
5. [アクセスコントロールリスト (ACL)] で、[編集] を選択します。

   オブジェクトに対する次の ACL アクセス許可を編集できます。

オブジェクト

- Read (読み込み) – 被付与者がオブジェクトデータとそのメタデータを読み込むことを許可します

オブジェクト ACL

- 読み込み (Read) – 被付与者がオブジェクト ACL を読み込むことを許可します
- Write (書き込み) – 被付与者が該当するオブジェクトの ACL を書き込むことを許可します S3 コンソールでは、バケット所有者 (AWS アカウント) にのみ書き込みアクセスを許可できます。他の被付与者には、書き込みアクセスを許可しないことを強くお勧めします。ただし、書き込みアクセスを許可する必要がある場合は、AWS CLI、AWS SDK、または REST API を使用できます。

6. 以下のオブジェクトのアクセス許可を管理できます。

   a. オブジェクト所有者へのアクセス

      所有者とは、AWS アカウントのルートユーザーであり、AWS Identity and Access Management IAM ユーザーではありません。ルートユーザーの詳細については、IAM ユーザーガイドの「AWS アカウントのルートユーザー」を参照してください。

      所有者のオブジェクトアクセス許可を変更するには、オブジェクト所有者へのアクセスで、お客様の AWS アカウント (所有者) を選択します。

      変更するアクセス許可のチェックボックスをオンにして、[保存] を選択します。

   b. その他の AWS アカウントのアクセス

      別の AWS から AWS アカウント ユーザーに許可を与えるには、他の AWS アカウント へのアクセスで、アカウントの追加を選択します。[Enter an ID] (ID の入力) フィールドに、オブジェクトのアクセス許可を付与する AWS ユーザーの正規 ID を入力します。正規 ID の検索に関する詳細は、Amazon Web Services 全般のリファレンス の「AWS アカウント 識別子」を参照してください。最大 99 人のユーザーを追加できます。

      ユーザーに付与するアクセス許可のチェックボックスをオンにして、[保存] を選択します。アクセス許可についての情報を表示するには、ヘルプアイコンを選択します。

c. パブリックアクセス

オブジェクトへのアクセスを一般のユーザー (世界中のすべてのユーザー) に許可するには、[パブリックアクセス] で [全員] を選択します。パブリックアクセス許可を付与すると、世界中の誰でもオブジェクトにアクセスできるようになります。

付与するアクセス許可のチェックボックスをオンにして、[保存] を選択します。

> **Warning**
>
> - [Everyone (全員)] グループに Amazon S3 オブジェクトへの匿名アクセスを付与するときは注意が必要です。このグループにアクセスを付与すると、世界中のすべてのユーザーがオブジェクトにアクセスできます。すべてのユーザーにアクセスを付与する必要がある場合は、[Read objects (オブジェクトの読み取り)] のみのアクセス許可を付与することを強くお勧めします。
> - [全員] グループにオブジェクト書き込み許可は付与しないことを強くお勧めします。付与すると、すべてのユーザーに対して、オブジェクトの ACL アクセス許可を上書きすることが許可されます。

AWS SDK の使用

このセクションでは、バケットやオブジェクトでアクセスコントロールリスト (ACL) の付与を設定する方法の例を示します。

> **Important**
>
> 汎用バケットで S3 のオブジェクト所有者に [バケット所有者の強制] 設定を使用する場合は、ポリシーを使用して汎用バケットとその中のオブジェクトへのアクセスを許可する必要があります。バケット所有者強制設定が有効になっている場合、アクセスコントロールリスト (ACL) の設定または ACL の更新は失敗し、`AccessControlListNotSupported` エラーコードが返されます。ACL の読み取り要求は引き続きサポートされています。

Java

このセクションでは、バケットやオブジェクトでアクセスコントロールリスト (ACL) の付与を設定する方法の例を示します。最初の例では、既定 ACL を使用するバケッ

ト (「既定 ACL」を参照) を作成します。次に、カスタムアクセス許可の付与のリスト を作成して、既定の ACL をカスタム付与を含む ACL で置き換えます。2 番目の例では、AccessControlList.grantPermission( ) メソッドを使用して ACL を変更する方法を示します。

Example バケットを作成し、S3 ログ配信グループにアクセス許可を付与する既定 ACL を指定する

この例では、バケットを作成します。リクエストで既定の ACL を指定し、バケットにログを書き込むアクセス許可をログ配信グループに付与します。

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.*;

import java.io.IOException;
import java.util.ArrayList;

public class CreateBucketWithACL {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String userEmailForReadPermission = "*** user@example.com ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withRegion(clientRegion)
                    .build();

            // Create a bucket with a canned ACL. This ACL will be replaced by the
            // setBucketAcl()
            // calls below. It is included here for demonstration purposes.
            CreateBucketRequest createBucketRequest = new
 CreateBucketRequest(bucketName, clientRegion.getName())
                    .withCannedAcl(CannedAccessControlList.LogDeliveryWrite);
            s3Client.createBucket(createBucketRequest);

            // Create a collection of grants to add to the bucket.
```

```
            ArrayList<Grant> grantCollection = new ArrayList<Grant>();

            // Grant the account owner full control.
            Grant grant1 = new Grant(new
 CanonicalGrantee(s3Client.getS3AccountOwner().getId()),
                    Permission.FullControl);
            grantCollection.add(grant1);

            // Grant the LogDelivery group permission to write to the bucket.
            Grant grant2 = new Grant(GroupGrantee.LogDelivery, Permission.Write);
            grantCollection.add(grant2);

            // Save grants by replacing all current ACL grants with the two we just
 created.
            AccessControlList bucketAcl = new AccessControlList();
            bucketAcl.grantAllPermissions(grantCollection.toArray(new Grant[0]));
            s3Client.setBucketAcl(bucketName, bucketAcl);

            // Retrieve the bucket's ACL, add another grant, and then save the new
 ACL.
            AccessControlList newBucketAcl = s3Client.getBucketAcl(bucketName);
            Grant grant3 = new Grant(new
 EmailAddressGrantee(userEmailForReadPermission), Permission.Read);
            newBucketAcl.grantAllPermissions(grant3);
            s3Client.setBucketAcl(bucketName, newBucketAcl);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Example 既存のオブジェクトの ACL を更新する

この例では、オブジェクトの ACL を更新します。この例では次のタスクを実行しています。

- オブジェクトの ACL を取得する

- すべての既存のアクセス許可を削除して ACL をクリアする
- 2 つのアクセス許可として、所有者へのフルアクセスと、メールアドレスで識別されたユーザーへの WRITE_ACP (付与できるアクセス許可 を参照) を追加する
- ACL をオブジェクトに保存する

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.AccessControlList;
import com.amazonaws.services.s3.model.CanonicalGrantee;
import com.amazonaws.services.s3.model.EmailAddressGrantee;
import com.amazonaws.services.s3.model.Permission;

import java.io.IOException;

public class ModifyACLExistingObject {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String keyName = "*** Key name ***";
        String emailGrantee = "*** user@example.com ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();

            // Get the existing object ACL that we want to modify.
            AccessControlList acl = s3Client.getObjectAcl(bucketName, keyName);

            // Clear the existing list of grants.
            acl.getGrantsAsList().clear();

            // Grant a sample set of permissions, using the existing ACL owner for
 Full
```

```
            // Control permissions.
            acl.grantPermission(new CanonicalGrantee(acl.getOwner().getId()),
 Permission.FullControl);
            acl.grantPermission(new EmailAddressGrantee(emailGrantee),
 Permission.WriteAcp);

            // Save the modified ACL back to the object.
            s3Client.setObjectAcl(bucketName, keyName, acl);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

.NET

Example バケットを作成し、S3 ログ配信グループにアクセス許可を付与する既定 ACL を指定する

この C# の例では、バケットを作成します。リクエストで既定の ACL を指定し、バケットにログを書き込むアクセス許可をログ配信グループに付与します。

コード例を設定および実行する方法の詳細については、「AWS SDK for .NET デベロッパーガイド」の「AWS SDK for .NET の開始方法」 を参照してください。

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class ManagingBucketACLTest
    {
        private const string newBucketName = "*** bucket name ***";
        // Specify your bucket region (an example region is shown).
```

```
        private static readonly RegionEndpoint bucketRegion =
RegionEndpoint.USWest2;
        private static IAmazonS3 client;

        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            CreateBucketUseCannedACLAsync().Wait();
        }

        private static async Task CreateBucketUseCannedACLAsync()
        {
            try
            {
                // Add bucket (specify canned ACL).
                PutBucketRequest putBucketRequest = new PutBucketRequest()
                {
                    BucketName = newBucketName,
                    BucketRegion = S3Region.EUW1, // S3Region.US,
                                                  // Add canned ACL.
                    CannedACL = S3CannedACL.LogDeliveryWrite
                };
                PutBucketResponse putBucketResponse = await
client.PutBucketAsync(putBucketRequest);

                // Retrieve bucket ACL.
                GetACLResponse getACLResponse = await client.GetACLAsync(new
GetACLRequest
                {
                    BucketName = newBucketName
                });
            }
            catch (AmazonS3Exception amazonS3Exception)
            {
                Console.WriteLine("S3 error occurred. Exception: " +
amazonS3Exception.ToString());
            }
            catch (Exception e)
            {
                Console.WriteLine("Exception: " + e.ToString());
            }
        }
    }
```

```
}
```

Example 既存のオブジェクトの ACL を更新する

この C# の例では、既存のオブジェクトで ACL を更新します。この例では次のタスクを実行しています。

- オブジェクトの ACL を取得する。
- すべての既存のアクセス許可を削除して ACL をクリアする。
- 2 つのアクセス許可として、所有者へのフルアクセスと、メールアドレスで識別されたユーザーへの WRITE_ACP を追加する。
- `PutAcl` リクエストを送信して ACL を保存する。

コード例を設定および実行する方法の詳細については、「AWS SDK for .NET デベロッパーガイド」の「AWS SDK for .NET の開始方法」を参照してください。

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Collections.Generic;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class ManagingObjectACLTest
    {
        private const string bucketName = "*** bucket name ***";
        private const string keyName = "*** object key name ***";
        private const string emailAddress = "*** email address ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 client;
        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            TestObjectACLTestAsync().Wait();
        }
        private static async Task TestObjectACLTestAsync()
        {
```

```
            try
            {
                    // Retrieve the ACL for the object.
                    GetACLResponse aclResponse = await client.GetACLAsync(new
GetACLRequest
                    {
                        BucketName = bucketName,
                        Key = keyName
                    });

                    S3AccessControlList acl = aclResponse.AccessControlList;

                    // Retrieve the owner (we use this to re-add permissions after
we clear the ACL).
                    Owner owner = acl.Owner;

                    // Clear existing grants.
                    acl.Grants.Clear();

                    // Add a grant to reset the owner's full permission (the
previous clear statement removed all permissions).
                    S3Grant fullControlGrant = new S3Grant
                    {
                        Grantee = new S3Grantee { CanonicalUser = owner.Id },
                        Permission = S3Permission.FULL_CONTROL

                    };

                    // Describe the grant for the permission using an email address.
                    S3Grant grantUsingEmail = new S3Grant
                    {
                        Grantee = new S3Grantee { EmailAddress = emailAddress },
                        Permission = S3Permission.WRITE_ACP
                    };
                    acl.Grants.AddRange(new List<S3Grant> { fullControlGrant,
grantUsingEmail });

                    // Set a new ACL.
                    PutACLResponse response = await client.PutACLAsync(new
PutACLRequest
                    {
                        BucketName = bucketName,
                        Key = keyName,
                        AccessControlList = acl
```

```
                    });
            }
            catch (AmazonS3Exception amazonS3Exception)
            {
                Console.WriteLine("An AmazonS3Exception was thrown. Exception: " +
 amazonS3Exception.ToString());
            }
            catch (Exception e)
            {
                Console.WriteLine("Exception: " + e.ToString());
            }
        }
    }
}
```

REST API の使用

Amazon S3 API を使用して、バケットまたはオブジェクトの作成時に、ACL を設定できます。Amazon S3 では、既存のバケットまたはオブジェクトに ACL を設定する API も提供します。これらの API は ACL を設定する次のメソッドを提供します。

- リクエストヘッダーを使用した ACL の設定 – リソース (バケットまたはオブジェクト) を作成するリクエストを送るときに、リクエストヘッダーを使用して ACL を設定します。これらのヘッダーを使用して、既定 ACL を指定するか、許可を明示的に指定 (被付与者とアクセス許可を明示的に識別) します。
- リクエストボディを使用した ACL の設定 – 既存のリソースに ACL を設定するリクエストを送信するときに、リクエストのヘッダーまたはボディを使用して ACL を設定できます。

REST API での ACL の管理のサポートの詳細については、Amazon Simple Storage Service API リファレンスの以下のセクションを参照してください。

- GetBucketAcl
- PutBucketAcl
- GetObjecAcl
- PutObjectAcl
- PutObject
- CreateBucket

- CopyObject
- CreateMultipartUpload

> **Important**
>
> 汎用バケットで S3 のオブジェクト所有者に [バケット所有者の強制] 設定を使用する場合は、ポリシーを使用して汎用バケットとその中のオブジェクトへのアクセスを許可する必要があります。バケット所有者強制設定が有効になっている場合、アクセスコントロールリスト (ACL) の設定または ACL の更新は失敗し、`AccessControlListNotSupported` エラーコードが返されます。ACL の読み取り要求は引き続きサポートされています。

アクセスコントロールリスト (ACL) 固有の要求ヘッダー

ヘッダーを使用して、アクセスコントロールリスト (ACL) ベースのアクセス許可を付与できます。デフォルトでは、すべてのオブジェクトがプライベートです。所有者だけがフルアクセスコントロールを持っています。新しいオブジェクトを追加するときに、個々の AWS アカウントに、または Amazon S3 であらかじめ定義されたグループに許可を付与できます。これらのアクセス許可は、オブジェクトのアクセスコントロールリスト (ACL) に追加されます。詳細については、アクセスコントロールリスト (ACL) の概要 を参照してください。

この操作では、次の 2 つの方法のいずれかを使用してアクセス許可を付与できます。

- 既定 ACL (**`x-amz-acl`**) — Amazon S3 は、既定 ACL と呼ばれる、あらかじめ定義された一連の ACL をサポートしています。各既定 ACL には、あらかじめ定義された一連の被付与者とアクセス権限が含まれています。詳細については、既定 ACL を参照してください。
- アクセス許可 — 特定の AWS アカウント またはグループにアクセス許可を明示的に付与するには、次のヘッダーを使用します。各ヘッダーは、Amazon S3 が ACL でサポートする特定のアクセス許可にマッピングされます。詳細については、アクセスコントロールリスト (ACL) の概要 を参照してください。ヘッダーでは、特定のアクセス許可を取得する被付与者のリストを指定します。
  - x-amz-grant-read
  - x-amz-grant-write
  - x-amz-grant-read-acp
  - x-amz-grant-write-acp
  - x-amz-grant-full-control

AWS CLI を使用する場合

AWS CLI を使用した ACL の管理の詳細については、AWS CLI Command Reference の put-bucket-acl を参照してください。

> **Important**
>
> 汎用バケットで S3 のオブジェクト所有者に [バケット所有者の強制] 設定を使用する場合は、ポリシーを使用して汎用バケットとその中のオブジェクトへのアクセスを許可する必要があります。バケット所有者強制設定が有効になっている場合、アクセスコントロールリスト (ACL) の設定または ACL の更新は失敗し、`AccessControlListNotSupported` エラーコードが返されます。ACL の読み取り要求は引き続きサポートされています。

ACL のポリシーの例

バケットポリシーで条件キーを使用して、Amazon S3 へのアクセスをコントロールできます。

トピック

- バケット所有者にフルコントロールを与えることを条件として s3:PutObject のアクセス許可を付与する
- x-amz-acl ヘッダーの条件を使用した s3:PutObject アクセス許可の付与

バケット所有者にフルコントロールを与えることを条件として s3:PutObject のアクセス許可を付与する

PutObject オペレーションでは、アクセスコントロールリスト (ACL) に固有のヘッダーを使用して、ACL に基づいてアクセス許可を付与することができます。バケット所有者は、これらのキーを使用して条件を設定し、ユーザーがオブジェクトをアップロードする場合に特定のアクセス許可を要求することができます。

例えば、アカウント A がバケット所有者であり、アカウント管理者がアカウント B のユーザー Dave に対して、オブジェクトをアップロードするアクセス許可を付与するとします。デフォルトでは、Dave がアップロードするオブジェクトはアカウント B に所有されるため、アカウント A にはそれらのオブジェクトに対するアクセス許可は付与されません。ただし、バケット所有者は請求書を支払うために、Dave がアップロードするオブジェクトに対する完全なアクセス許可を必要としています。この対処方法として、アカウント A の管理者は、明示的に完全なアクセス許可を付与

するか、既定 ACL を使用する ACL 固有のヘッダーをリクエストに含むことを条件として、Dave に s3:PutObject のアクセス許可を付与できます。詳細については、Put Object を参照してください。

x-amz-full-control ヘッダーを必須にする

リクエストで、バケット所有者へのフルコントロールのアクセス許可が含まれる x-amz-full-control ヘッダーを要求できます。以下のバケットポリシーは、s3:PutObject 条件キーを使用して、リクエストに s3:x-amz-grant-full-control ヘッダーを含めることを条件とする x-amz-full-control のアクセス許可をユーザー Dave に付与します。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "statement1",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::AccountB-ID:user/Dave"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::awsexamplebucket1/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-grant-full-control": "id=AccountA-CanonicalUserID"
        }
      }
    }
  ]
}
```

> **Note**
>
> この例では、クロスアカウントのアクセス許可を付与しています。ただし、許可を付与される Dave がバケットを所有している AWS アカウントに属している場合、この条件付き許可は不要になります。これは、ユーザーがアップロードするオブジェクトは Dave が属する親アカウントによって所有されるためです。

明示的な拒否を追加する

前述のバケットポリシーでは、アカウント B のユーザー Dave に条件付きのアクセス許可が付与されます。ただし、このポリシーが有効であっても、Dave が他のポリシーに従って、条件なしで同じアクセス許可を取得する場合があります。例えば、Dave が属するグループに、条件なしで s3:PutObject のアクセス許可が付与される場合があります。このようなアクセス許可の抜け穴を避けるには、明示的な拒否を追加して、より厳格なアクセスポリシーを記述する必要があります。次の例では、バケット所有者に完全なアクセス許可を付与するヘッダーをリクエストに含めない場合、Dave に対してアップロードのアクセス許可を明示的に拒否します。明示的な拒否は、付与されている他のアクセス許可に常に優先されます。以下は、明示的な拒否が追加された、改訂済みアクセスポリシーの例です。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "statement1",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::AccountB-ID:user/AccountBadmin"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::awsexamplebucket1/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-grant-full-control": "id=AccountA-CanonicalUserID"
                }
            }
        },
        {
            "Sid": "statement2",
            "Effect": "Deny",
            "Principal": {
                "AWS": "arn:aws:iam::AccountB-ID:user/AccountBadmin"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::awsexamplebucket1/*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-grant-full-control": "id=AccountA-CanonicalUserID"
                }
            }
        }
    ]
```

```
}
```

AWS CLI でポリシーをテストする

2 つの AWS アカウントがある場合は、AWS Command Line Interface (AWS CLI) を使用してポリシーをテストできます。ポリシーをアタッチしたら、Dave の認証情報を使用し、次の AWS CLI `put-object` コマンドを実行してアクセス許可をテストします。Dave の認証情報は、`--profile` パラメータを追加して指定します。バケット所有者にフルコントロールのアクセス許可を付与するには、`--grant-full-control` パラメータを追加します。AWS CLI のセットアップと使用の詳細については、「Amazon S3 API リファレンス」の「Developing with Amazon S3 using the AWS CLI」を参照してください。

```
aws s3api put-object --bucket examplebucket --key HappyFace.jpg --body c:\HappyFace.jpg
 --grant-full-control id="AccountA-CanonicalUserID" --profile AccountBUserProfile
```

x-amz-acl ヘッダーを必須にする

バケット所有者にフルコントロールのアクセス許可を付与する既定 ACL が指定された `x-amz-acl` ヘッダーを要求できます。リクエストに `x-amz-acl` ヘッダーを含めることを義務付けるには、以下の例のように `Condition` ブロックのキーと値のペアを置き換え、`s3:x-amz-acl` 条件キーを指定します。

```
"Condition": {
    "StringEquals": {
        "s3:x-amz-acl": "bucket-owner-full-control"
    }
}
```

AWS CLI を使用してアクセス許可をテストするには、`--acl` パラメータを指定します。これにより、AWS CLI は送信するリクエストに `x-amz-acl` ヘッダーを追加します。

```
aws s3api put-object --bucket examplebucket --key HappyFace.jpg --body c:\HappyFace.jpg
 --acl "bucket-owner-full-control" --profile AccountBadmin
```

x-amz-acl ヘッダーの条件を使用した s3:PutObject アクセス許可の付与

以下のバケットポリシーは、オブジェクトをパブリックに読み取り可能にする `x-amz-acl` ヘッダーがリクエストに含まれている場合に、2 つの AWS アカウントに `s3:PutObject` の許可を付与し

ます。Condition ブロックでは、StringEquals 条件を使用し、キーと値のペアとして "s3:x-amz-acl":["public-read"] を評価に使用できます。このキーと値のペアで、s3:x-amz-acl は、「s3:」というプレフィックスが示すとおり Amazon S3 固有のキーです。

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
         "Sid":"AddCannedAcl",
            "Effect":"Allow",
         "Principal": {
                "AWS": [
                "arn:aws:iam::Account1-ID:root",
    "arn:aws:iam::Account2-ID:root"
    ]
            },
         "Action":"s3:PutObject",
            "Resource": ["arn:aws:s3:::awsexamplebucket1/*"],
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl":["public-read"]
                }
            }
        }
    ]
}
```

Important

すべての条件が、すべてのアクションに対して意味を成すわけではありません。例えば、Amazon S3 の s3:CreateBucket のアクセス許可を付与するポリシーに条件として s3:LocationConstraint を含めることは理にかなっています。ただし、この条件を s3:GetObject のアクセス許可を付与するポリシーに含めることは意味がありません。Amazon S3 では、このような Amazon S3 固有の条件を含むセマンティックエラーをテストすることができます。ただし、IAM ユーザーまたはロールのポリシーを作成し、意味的に無効な Amazon S3 条件を含めても、IAM は Amazon S3 条件を検証できないため、エラーは報告されません。

Amazon S3 ストレージへのパブリックアクセスのブロック

Amazon S3 のパブリックアクセスブロック機能は、Amazon S3 のリソースへのパブリックアクセスの管理に役立つ、アクセスポイント、バケット、アカウントの設定を提供します。デフォルトでは、新しいバケット、アクセスポイント、およびオブジェクトはパブリックアクセスを許可しません。ただし、ユーザーはバケットポリシー、アクセスポイントポリシー、またはオブジェクトのアクセス許可を変更することで、パブリックアクセスを許可できます。S3 ブロックパブリックアクセス設定は、これらのポリシーやアクセス許可を上書きして、これらのリソースへのパブリックアクセスを制限できるようにします。

S3 のパブリックアクセスブロックでは、アカウント管理者やバケット所有者は Amazon S3 のリソースへのパブリックアクセスを制限する一元的な管理を簡単に設定して、リソースがどのように作成されたかに関係なく強制的に適用することができます。

パブリックブロックアクセスを設定する手順については、パブリックアクセスブロックの設定 を参照してください。

Amazon S3 はバケットやオブジェクトへのアクセスのリクエストを受け取ると、バケットやバケット所有者のアカウントに適用されているパブリックアクセスブロック設定があるかどうかを確認します。リクエストがアクセスポイントを経由している場合、Amazon S3 はアクセスポイントのパブリックアクセスブロック設定も確認します。リクエストされたアクセスを禁止する既存のパブリックアクセスブロック設定がある場合、Amazon S3 はそのリクエストを拒否します。

Amazon S3 のパブリックアクセスブロックには、4 つの設定があります。これらの設定は、独立しており、任意の組み合わせで使用できます。各設定は、アクセスポイント、バケット、または AWS アカウント全体に適用できます。アクセスポイント、バケット、アカウントのパブリックアクセスブロック設定が異なる場合、Amazon S3 は、アクセスポイント、バケット、アカウントの設定の組み合わせで最も制限が厳しいものを適用します。

Amazon S3 は、パブリックアクセスブロック設定でオペレーションが禁止されているかどうかを評価し、アクセスポイント、バケット、アカウントの設定に違反しているすべてのリクエストを拒否します。

> **Important**
>
> パブリックアクセスは、アクセスコントロールリスト (ACL)、アクセスポイントポリシー、バケットポリシー、またはそのすべてからバケットおよびオブジェクトに付与されます。Amazon S3 のすべてのアクセスポイント、バケット、オブジェクトへのパブリックアクセスを確実にブロックするために、アカウントへのパブリックアクセスをブロックする 4 つ

の設定をすべて有効にすることをお勧めします。これらの設定によって、現在および将来のバケットおよびアクセスポイントのパブリックアクセスはすべてブロックされます。
これらの設定を適用する前に、アプリケーションがパブリックアクセスなしで正しく動作することを確認してください。「Amazon S3 を使用して静的ウェブサイトをホスティングする」に示す静的なウェブサイトをホストする場合など、バケットやオブジェクトにある程度のパブリックアクセスが必要な場合は、ストレージのユースケースに合わせて個別に設定をカスタマイズできます。
[パブリックアクセスをブロック] を有効にすると、S3 リソースに直接アタッチされているリソースポリシーやアクセスコントロールリスト (ACL) を通じてパブリックアクセスが付与されるのを防ぐことができるため、リソースを保護できます。パブリックアクセスのブロックを有効にすること以外にも、次のポリシーを慎重に検査して、パブリックアクセスを付与していないことを確認します。

- 関連する AWS プリンシパル (IAM ロールなど) にアタッチされているアイデンティティベースのポリシー
- 関連する AWS リソースにアタッチされたリソースベースのポリシー (AWS Key Management Service (KMS) キーなど)

Note

- パブリックアクセスブロック設定は、アクセスポイント、バケット、AWS アカウントに対してのみ有効にすることができます。Amazon S3 では、オブジェクトごとのパブリックアクセスブロック設定はサポートされていません。
- アカウントにブロックパブリックアクセス設定を適用すると、その設定はすべての AWS リージョンにグローバルに適用されます。設定はすべてのリージョンで即時または同時に有効になるわけではありませんが、最終的にはすべてのリージョンに反映されます。

トピック

- パブリックアクセスブロック設定
- アクセスポイントでのパブリックアクセスブロックオペレーションの実行
- 「パブリック」の意味
- IAM Access Analyzer for S3 を使用したパブリックバケットの確認
- アクセス許可

- パブリックアクセスブロックの設定
- アカウントのパブリックアクセスブロック設定の構成
- S3 バケットへのパブリックアクセスブロック設定の構成

パブリックアクセスブロック設定

S3 のブロックパブリックアクセスには 4 つの設定があります。これらの設定は、個別のアクセスポイント、バケット、または AWS アカウント 全体に任意の組み合わせで適用できます。設定をアカウントに適用すると、その設定はアカウントが所有するすべてのバケットとアクセスポイントに適用されます。同様に、設定をバケットに適用すると、その設定はバケットに関連付けられているすべてのアクセスポイントに適用されます。

次の表に、利用可能な設定が含まれます。

名前	説明
`BlockPublicAcls`	このオプションを TRUE に設定すると、次のように動作します。 • 指定されたアクセスコントロールリスト (ACL) がパブリックである場合、`PutBucketAcl` と `PutObjectAcl` の呼び出しは失敗します。 • リクエストにパブリック ACL が含まれている場合、`PutObject` の呼び出しは失敗します。 • この設定がアカウントに適用されている場合、リクエストにパブリック ACL が含まれていると `PUT Bucket` の呼び出しは失敗します。 この設定が TRUE に設定されている場合、(REST API、AWS CLI、または AWS SDK のいずれを介して行われたかにかかわらず) 指定された操作は失敗します。ただし、バケットとオブジェクトの既存のポリシーと ACL は変更されません。この設定により、パブリックアクセスから保護しながら、バケットとオブジェクトの既存のポリシーと ACL を監査、絞り込み、またはその他の方法で変更することができます。

名前	説明
	Note アクセスポイントには ACL が関連付けられていません。この設定をアクセスポイントに適用すると、基になるバケットへのパススルーとして機能します。この設定がアクセスポイントで有効になっている場合、このアクセスポイントを介したリクエストは、基になるバケットでこの設定が実際に有効になっているかどうかに関係なく、この設定がバケットで有効になっているかのように動作します。
`IgnorePublicAcls`	このオプションを `TRUE` に設定すると、Amazon S3 はバケットとそれに含まれるオブジェクトのすべてのパブリック ACL を無視します。この設定を使用すると、パブリック ACL を含む `PutObject` 呼び出しを許可しながら、ACL によって許可されたパブリックアクセスを安全にブロックできます (`BlockPublicAcls` とは異なり、パブリック ACL を含む `PutObject` 呼び出しを拒否します)。この設定を有効にしても、既存の ACL の永続性には影響せず、新しいパブリック ACL の設定も妨げられません。 **Note** アクセスポイントには ACL が関連付けられていません。この設定をアクセスポイントに適用すると、基になるバケットへのパススルーとして機能します。この設定がアクセスポイントで有効になっている場合、このアクセスポイントを介したリクエストは、基になるバケットでこの設定が実際に有効になっているかどうかに関係なく、この設定がバケットで有効になっているかのように動作します。

名前	説明
BlockPublicPolicy	バケットに対してこのオプションを TRUE に設定すると、指定されたバケットポリシーでパブリックアクセスが許可されている場合、Amazon S3 は PutBucketPolicy への呼び出しを拒否します。バケットに対してこのオプションを TRUE に設定した場合も、Amazon S3 は、指定されたバケットポリシーがパブリックアクセスを許可していれば、Amazon S3 はバケットのすべての同一アカウントアクセスポイントで PutAccessPointPolicy への呼び出しを拒否します。 アクセスポイントでこのオプションを TRUE に設定すると、指定されたポリシー (アクセスポイントまたは基になるバケットのいずれか) でパブリックアクセスが許可されている場合、Amazon S3 はアクセスポイント経由で行われる PutAccessPointPolicy および PutBucketPolicy への呼び出しを拒否します。 この設定を使用することにより、バケットやバケット内のオブジェクトをパブリックに共有することを許可することなく、アクセスポイントとバケットポリシーを管理することをユーザーに許可できます。この設定を有効にしても、既存のアクセスポイントやバケットポリシーには影響しません。 **Important** この設定を効果的に使用するため、アカウントレベルで適用することを推奨します。バケットポリシーでは、ユーザーがバケットのブロックパブリックアクセス設定を変更できます。そのため、バケットポリシーを変更する権限を持つユーザーは、バケットのブロックパブリックアクセス設定を無効にすることを許可するポリシーを挿入できます。この設定が特定のバケットではなくアカウント全体で有効になっている場合、ユーザーがこの設定を無効にするようにバケットポリシーを変更しても、Amazon S3 はパブリックポリシーをブロックします。

名前	説明
RestrictPublicBuckets	このオプションを TRUE に設定すると、パブリックポリシーを持つアクセスポイントやバケットへのアクセスは、バケット所有者のアカウントおよびアクセスポイント所有者のアカウント内の AWS のサービスプリンシパルと承認されたユーザーのみに制限されます。この設定は、アカウント内のユーザーにアクセスポイントやバケットの管理を許可しながら、アクセスポイントやバケットへのすべてのクロスアカウントアクセス (AWS のサービスプリンシパルによるアクセスを除く) をブロックします。 この設定を有効にしても、既存のアクセスポイントポリシーやバケットポリシーには影響しません。ただし、Amazon S3 は、特定のアカウントへのパブリックではない委任を含むパブリックアクセスポイントポリシーやパブリックバケットポリシーから派生したパブリックアクセスやクロスアカウントアクセスをブロックします。

Important

- GetBucketAcl および GetObjectAcl を呼び出すと、指定されたバケットまたはオブジェクトに対して有効なアクセス許可が常に返されます。例えば、パブリックアクセスを許可する ACL がバケットにあり、そのバケットにも IgnorePublicAcls 設定が有効になっているとします。この場合、GetBucketAcl は、バケットに関連付けられている実際の ACL ではなく、Amazon S3 が強制的に適用しているアクセス許可を反映した ACL を返します。
- ブロックパブリックアクセス設定は既存のポリシーまたは ACL を変更しません。そのため、ブロックパブリックアクセス設定を削除しても、パブリックポリシーまたは ACL を持つバケットまたはオブジェクトは再びパブリックにアクセス可能になります。

アクセスポイントでのパブリックアクセスブロックオペレーションの実行

アクセスポイントに対してブロックパブリックアクセスオペレーションを実行するには、AWS CLI サービス s3control を使用します。

> **Important**
>
> アクセスポイントの作成後、アクセスポイントのパブリックアクセスのブロック設定を変更することはできません。アクセスポイントのパブリックアクセスのブロック設定は、アクセスポイントの作成時にのみ指定できます。

「パブリック」の意味

ACL

Amazon S3 は、バケットやオブジェクトの ACL が事前定義済みの `AllUsers` グループまたは `AuthenticatedUsers` グループのメンバーにアクセス許可を付与する場合にパブリックとみなします。事前定義済みのグループの詳細については、Amazon S3 の事前定義済みのグループ を参照してください。

バケットポリシー

バケットポリシーを評価する場合、Amazon S3 はまずポリシーがパブリックであると想定します。その後、ポリシーを評価して非パブリックとしての資格があるかどうかを判断します。非パブリックと見なすには、バケットポリシーで、次のうち 1 つ以上の固定値 (ワイルドカードを含まない値または AWS Identity and Access Managementポリシー変数) にのみアクセスを許可する必要があります。

- AWS プリンシパル、ユーザー、ロール、またはサービスプリンシパル (例: `aws:PrincipalOrgID`)
- `aws:SourceIp` を使用した一連のクラスレスドメイン間ルーティング (CIDR)。CIDR の詳細については、RFC Editor のウェブサイトで RFC 4632 を参照してください。

  > **Note**
  >
  > 非常に広い IP 範囲 (たとえば 0.0.0.0/1) の `aws:SourceIp` 条件キーに基づいてアクセスを許可するバケットポリシーは、「パブリック」と評価されます。これには、IPv4 の場合は /8、IPv6 の場合は /32 よりも広い値が含まれます (RFC1918 のプライベート範囲を除く)。パブリックアクセスのブロックにより、これらの「パブリック」ポリシーが拒否され、これらの「パブリック」ポリシーを既に使用しているバケットへのクロスアカウントアクセスが防止されます。

- `aws:SourceArn`

- aws:SourceVpc
- aws:SourceVpce
- aws:SourceOwner
- aws:SourceAccount
- aws:userid、「AROLEID:*」パターンの外側
- s3:DataAccessPointArn

> **Note**
>
> この値をバケットポリシーで使用すると、アカウント ID が固定されている限り、ポリシーをパブリックにすることなく、アクセスポイント名にワイルドカードを含めることができます。例えば、arn:aws:s3:us-west-2:123456789012:accesspoint/* へのアクセスを許可すると、バケットポリシーをパブリックにすることなく、リージョン 123456789012 のアカウント us-west-2 に関連付けられているすべてのアクセスポイントへのアクセスを許可できます。この動作はアクセスポイントポリシーでは異なります。詳細については、「アクセスポイント」を参照してください。

- s3:DataAccessPointAccount

バケットポリシーの詳細については、Amazon S3 のバケットポリシー を参照してください。

> **Note**
>
> 複数値のコンテキストキーを使用する場合は、ForAllValues または ForAnyValue 集合演算子を使用する必要があります。

Example : パブリックバケットポリシー

これらのルールでは、次のポリシー例はパブリックと見なされます。

```
{
  "Principal": "*",
  "Resource": "*",
  "Action": "s3:PutObject",
  "Effect": "Allow"
 }
```

```
{
  "Principal": "*",
  "Resource": "*",
  "Action": "s3:PutObject",
  "Effect": "Allow",
  "Condition": { "StringLike": {"aws:SourceVpc": "vpc-*"}}
 }
```

これらのポリシーは、固定値を使用して、前述のいずれかの条件キーを含めることによって非パブリックにすることができます。例えば、上記の最後のポリシーは、次のように aws:SourceVpc を固定値に設定することで非パブリックにすることができます。

```
{
  "Principal": "*",
  "Resource": "*",
  "Action": "s3:PutObject",
  "Effect": "Allow",
  "Condition": {"StringEquals": {"aws:SourceVpc": "vpc-91237329"}}
 }
```

Amazon S3 がパブリックと非パブリックの両方のアクセス許可を含むバケットポリシーを評価する方法

この例では、Amazon S3 がパブリックと非パブリックの両方のアクセス許可を含むバケットポリシーを評価する方法を示します。

バケットに一連の固定プリンシパルへのアクセスを許可するポリシーがあるとします。前述のルールの下では、このポリシーはパブリックではありません。したがって、RestrictPublicBuckets 設定を有効にしても、ポリシーは記述どおりに有効になります。これは、RestrictPublicBuckets はパブリックポリシーを持つバケットにのみ適用されるためです。ただし、パブリックステートメントをポリシーに追加すると、RestrictPublicBuckets はバケットに有効になります。これにより、AWS サービスプリンシパルとバケット所有者のアカウントの認証されたユーザーのみがバケットにアクセスできるようになります。

例えば、「アカウント – 1」が所有するバケットに次の内容を含むポリシーがあるとします。

1. AWS CloudTrail (AWS サービスプリンシパル) へのアクセスを許可するステートメント
2. 「アカウント – 2」アカウントへのアクセスを許可するステートメント

3. Condition 制限なしで "Principal": "*" などを指定して、パブリックへのアクセスを許可するステートメント

このポリシーは、3 番目のステートメントのためにパブリックとしての資格があります。このポリシーがあって RestrictPublicBuckets を有効にすると、Amazon S3 は CloudTrail によるアクセスのみを許可します。ステートメント 2 がパブリックでなくても、Amazon S3 は「アカウント – 2」によるアクセスを無効にします。これは、ステートメント 3 がポリシー全体をパブリックにレンダリングするため、RestrictPublicBuckets が適用されるためです。その結果、ポリシーで特定のアカウントのアカウント – 2」にアクセスが委任されていても、Amazon S3 はクロスアカウントアクセスを無効にします。ただし、ポリシーからステートメント 3 を削除した場合、そのポリシーはパブリックとして認められず、RestrictPublicBuckets は適用されなくなります。したがって、RestrictPublicBuckets を有効のままにしていても、「アカウント – 2」はバケットへのアクセスを再取得できます。

アクセスポイント

Amazon S3 がパブリックアクセスブロック設定を評価する方法は、バケットとアクセスポイントで少しだけ異なります。アクセスポイントポリシーがパブリックであることを確認するために Amazon S3 が適用するルールは、通常、アクセスポイントでもバケットと同じですが、次の場合を除きます。

- VPC ネットワークオリジンを持つアクセスポイントは、アクセスポイントポリシーの内容に関係なく、常に非パブリックと見なされます。
- s3:DataAccessPointArn を使用して一連のアクセスポイントへのアクセスを許可するアクセスポイントポリシーは、パブリックと見なされます。この動作は、バケットポリシーとは異なることに注意してください。例えば、s3:DataAccessPointArn と一致する arn:aws:s3:us-west-2:123456789012:accesspoint/* の値へのアクセスを許可するバケットポリシーは、パブリックと見なされません。ただし、アクセスポイントポリシーにおける同じステートメントは、アクセスポイントをパブリックと見なします。

IAM Access Analyzer for S3 を使用したパブリックバケットの確認

IAM Access Analyzer for S3 を使用して、パブリックアクセスを許可するバケットの ACL、バケットポリシー、またはアクセスポイントポリシーを持つバケットを確認できます。IAM Access Analyzer for S3 は、インターネットの任意のユーザーや他の AWS アカウント (組織外の AWS アカウント を含む) にアクセスを許可するように設定されているバケットに関して警告します。パブリックバケッ

トまたは共有バケットごとに、パブリックアクセスや共有アクセスのソースとレベルを報告する結果が送信されます。

IAM Access Analyzer for S3 では、バケットへのすべてのパブリックアクセスをワンクリックでブロックすることができます。また、バケットレベルのアクセス許可の設定を参照して、きめ細かいアクセスレベルを設定することもできます。パブリックアクセスまたは共有アクセスを必要とする特定の検証済みユースケースについては、バケットの調査結果をアーカイブすることで、バケットをパブリックまたは共有とすることを確定して記録できます。

まれに、IAM Access Analyzer for S3 と Amazon S3 パブリックアクセスブロックの評価は、バケットがパブリックかどうかによって異なる場合があります。この動作は、Amazon S3 パブリックアクセスブロックが、パブリックアクセスの評価に加えて、アクションの存在についても検証を実行するために発生します。バケットポリシーに、Amazon S3 でサポートされていないアクション (`s3:NotASupportedAction` など) へのパブリックアクセスを許可する `Action` ステートメントが含まれているとします。この場合、Amazon S3 パブリックアクセスブロックはバケットをパブリックとして評価します。このようなステートメントは、アクションが後でサポートされるときにバケットをパブリックにする可能性があるためです。Amazon S3 パブリックアクセスブロックと IAM Access Analyzer for S3 の評価が異なる場合は、バケットポリシーを確認し、サポートされていないアクションを削除することをお勧めします。

IAM Access Analyzer for S3 の詳細については、IAM Access Analyzer for S3 を使用したバケットアクセスの確認 を参照してください。

アクセス許可

Amazon S3 のパブリックアクセスブロック機能を使用するには、以下のアクセス許可が必要です。

オペレーション	必要なアクセス許可
GET バケットのポリシーステータス	`s3:GetBucketPolicyStatus`
GET バケットのパブリックアクセスのブロック設定	`s3:GetBucketPublicAccessBlock`
PUT バケットのパブリックアクセスのブロック設定	`s3:PutBucketPublicAccessBlock`
DELETE バケットのパブリックアクセスのブロック設定	`s3:PutBucketPublicAccessBlock`

オペレーション	必要なアクセス許可
GET アカウントのパブリックアクセスのブロック設定	s3:GetAccountPublicAccessBlock
PUT アカウントのパブリックアクセスのブロック設定	s3:PutAccountPublicAccessBlock
DELETE アカウントのパブリックアクセスのブロック設定	s3:PutAccountPublicAccessBlock
PUT アクセスポイントのパブリックアクセスのブロック設定	s3:CreateAccessPoint

> **Note**
>
> DELETE オペレーションには、PUT オペレーションと同じアクセス許可が必要です。DELETE オペレーションに対する個別のアクセス許可はありません。

パブリックアクセスブロックの設定

AWS アカウント、Amazon S3 バケット、アクセスポイントのブロックパブリックアクセス設定の詳細については、以下のトピックを参照してください。

- アカウントのパブリックアクセスブロック設定の構成
- S3 バケットへのパブリックアクセスブロック設定の構成
- アクセスポイントでのパブリックアクセスブロックオペレーションの実行

アカウントのパブリックアクセスブロック設定の構成

Amazon S3 のパブリックアクセスブロックは、Amazon S3 のリソースへのパブリックアクセスの管理に役立つ、アクセスポイント、バケット、アカウントの設定を提供します。デフォルトでは、新しいバケット、アクセスポイント、およびオブジェクトはパブリックアクセスを許可しません。

詳細については、「Amazon S3 ストレージへのパブリックアクセスのブロック」を参照してください。

> **Note**
>
> アカウントレベルの設定は、個々のオブジェクトの設定よりも優先されます。パブリックアクセスをブロックするようにアカウントを設定すると、アカウント内の個々のオブジェクトに対して行われたパブリックアクセスの設定が上書きされます。

S3 コンソール、AWS CLI、AWS SDK、および REST API を使用して、アカウント内のすべてのバケットに対して、パブリックアクセスブロック設定を指定できます。詳細については、関連するセクションを参照してください。

バケットのパブリックアクセスブロック設定を構成するには、「S3 バケットへのパブリックアクセスブロック設定の構成」を参照してください。アクセスポイントに関する情報については、「アクセスポイントでのパブリックアクセスブロックオペレーションの実行」を参照してください。

S3 コンソールの使用

Amazon S3 パブリックアクセスブロックを使用して、S3 バケット内のデータへのパブリックアクセスを許可しないようにアプリケーションを設定します。このセクションでは、AWS アカウントのすべての S3 バケットに対するブロックパブリックアクセス設定の編集方法について説明します。パブリックアクセスのブロックの詳細については、Amazon S3 ストレージへのパブリックアクセスのブロック を参照してください。

AWS アカウントのすべての S3 バケットのブロックパブリックアクセス設定を編集するには

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. [Block Public Access settings for this account (このアカウントのブロックパブリックアクセスの設定)] を選択します。
3. [Edit] (編集) を選択して、AWS アカウント のすべてのバケットに対するブロックパブリックアクセス設定を変更します。
4. 変更する設定を選択して、[Save changes (変更の保存)] を選択します。
5. 確認を求められたら、「**`confirm`**」と入力します。次に、[確認] を選択して変更を保存します。

AWS CLI を使用する場合

AWS CLI を介して Amazon S3 のパブリックアクセスブロックを使用することができます。AWS CLI のセットアップおよび使用の詳細については、AWS Command Line Interface とは? を参照してください。

アカウント

アカウントでブロックパブリックアクセス操作を実行するには、AWS CLI サービス `s3control` を使用します。このサービスを使用するアカウントレベルの操作は次のとおりです。

- `PutPublicAccessBlock` (アカウントの場合)
- `GetPublicAccessBlock` (アカウントの場合)
- `DeletePublicAccessBlock` (アカウントの場合)

追加情報と例については、「AWS CLI リファレンス」の「put-public-access-block」を参照してください。

AWS SDK の使用

Java

以下の例は、AWS SDK for Java で Amazon S3 のパブリックアクセスブロックを使用して、Amazon S3 アカウントにパブリックアクセスブロック設定を配置する方法を示しています。

```
AWSS3ControlClientBuilder controlClientBuilder =
 AWSS3ControlClientBuilder.standard();
controlClientBuilder.setRegion(<region>);
controlClientBuilder.setCredentials(<credentials>);

AWSS3Control client = controlClientBuilder.build();
client.putPublicAccessBlock(new PutPublicAccessBlockRequest()
  .withAccountId(<account-id>)
  .withPublicAccessBlockConfiguration(new PublicAccessBlockConfiguration()
    .withIgnorePublicAcls(<value>)
    .withBlockPublicAcls(<value>)
    .withBlockPublicPolicy(<value>)
    .withRestrictPublicBuckets(<value>)));
```

> **Important**
>
> この例は、`AWSS3Control` クライアントクラスを使用するアカウントレベルの操作にのみ関係します。バケットレベルの操作については、前述の例を参照してください。

Other SDKs

その他の AWS SDK の使用については、「Amazon S3 API リファレンス」の「Developing with Amazon S3 using the AWS SDKs」を参照してください。

REST API の使用

REST API での Amazon S3 のパブリックアクセスブロックの使用については、Amazon Simple Storage Service API リファレンスの以下のトピックを参照してください。

- アカウントレベルの操作
  - PutPublicAccessBlock
  - GetPublicAccessBlock
  - DeletePublicAccessBlock

S3 バケットへのパブリックアクセスブロック設定の構成

Amazon S3 のパブリックアクセスブロックは、Amazon S3 のリソースへのパブリックアクセスの管理に役立つ、アクセスポイント、バケット、アカウントの設定を提供します。デフォルトでは、新しいバケット、アクセスポイント、およびオブジェクトはパブリックアクセスを許可しません。

詳細については、「Amazon S3 ストレージへのパブリックアクセスのブロック」を参照してください。

S3 コンソール、AWS CLI、AWS SDK、REST API を使用して、1 つ以上のバケットへのパブリックアクセスを許可できます。また、既にパブリックになっているバケットへのパブリックアクセスをブロックすることもできます。詳細については、関連するセクションを参照してください。

アカウント内のすべてのバケットに対してパブリックアクセスをブロックする設定を構成するには、「アカウントのパブリックアクセスブロック設定の構成」を参照してください。アクセスポイントのパブリックアクセスブロック設定については、「アクセスポイントでのパブリックアクセスブロックオペレーションの実行」を参照してください。

S3 コンソールの使用

Amazon S3 パブリックアクセスブロックを使用して、S3 バケット内のデータへのパブリックアクセスを許可しないようにアプリケーションを設定します。このセクションでは、1 つ以上の S3 バケットに対するブロックパブリックアクセス設定の編集方法について説明します。AWS CLI、AWS SDK、および Amazon S3 REST API を使用したパブリックアクセスのブロックについて詳細は、Amazon S3 ストレージへのパブリックアクセスのブロック を参照してください。

[IAM Access Analyzer] 列の [バケット] リストから、バケットがパブリックにアクセス可能であるかどうかを確認できます。詳細については、「IAM Access Analyzer for S3 を使用したバケットアクセスの確認」を参照してください。

バケットとそのパブリックアクセス設定を一覧表示したときに Error が表示された場合は、必要なアクセス許可がない可能性があります。以下のアクセス許可がユーザーポリシーまたはロールポリシーに追加されていることを確認します。

```
s3:GetAccountPublicAccessBlock
s3:GetBucketPublicAccessBlock
s3:GetBucketPolicyStatus
s3:GetBucketLocation
s3:GetBucketAcl
s3:ListAccessPoints
s3:ListAllMyBuckets
```

まれに、AWS リージョンの停止により、リクエストが失敗することもあります。

単一の S3 バケットをターゲットに Amazon S3 パブリックアクセスブロック設定を編集するには

単一の S3 バケットのパブリックアクセス設定を変更する必要がある場合は、以下の手順に従ってください。

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. [バケット名] リストで、目的のバケットの名前を選択します。
3. [Permissions] を選択します。
4. [ブロックパブリックアクセス (バケット設定)] の横にある [編集] を選択して、バケットのパブリックアクセス設定を変更します。4 つの Amazon S3 パブリックアクセスブロック設定の詳細については、パブリックアクセスブロック設定 を参照してください。
5. 設定を選択してから、[保存] を選択します。

6. 確認を求められたら、「**confirm**」と入力します。次に、[確認] を選択して変更を保存します。

バケットを作成するとき、Amazon S3 パブリックアクセスブロックの設定を変更することもできます。詳細については、「汎用バケットの作成」を参照してください。

AWS CLI の使用

バケットのパブリックアクセスをブロックしたり、パブリックアクセスのブロックを削除するには、AWS CLI サービス `s3api` を使用します。このサービスを使用するバケットレベルの操作は次のとおりです。

- `PutPublicAccessBlock` (バケットの場合)
- `GetPublicAccessBlock` (バケットの場合)
- `DeletePublicAccessBlock` (バケットの場合)
- `GetBucketPolicyStatus`

詳細と例については、「AWS CLI リファレンス」の「put-public-access-block」を参照してください。

AWS SDK の使用

Java

```
AmazonS3 client = AmazonS3ClientBuilder.standard()
   .withCredentials(<credentials>)
   .build();

client.setPublicAccessBlock(new SetPublicAccessBlockRequest()
  .withBucketName(<bucket-name>)
  .withPublicAccessBlockConfiguration(new PublicAccessBlockConfiguration()
    .withBlockPublicAcls(<value>)
    .withIgnorePublicAcls(<value>)
    .withBlockPublicPolicy(<value>)
    .withRestrictPublicBuckets(<value>)));
```

> **Important**
>
> この例は、AmazonS3 クライアントクラスを使用するバケットレベルの操作にのみ関係します。アカウントレベルの操作については、次の例を参照してください。

Other SDKs

その他の AWS SDK の使用については、「Amazon S3 API リファレンス」の「Developing with Amazon S3 using the AWS SDKs」を参照してください。

REST API の使用

REST API での Amazon S3 のパブリックアクセスブロックの使用については、Amazon Simple Storage Service API リファレンスの以下のトピックを参照してください。

- バケットレベルの操作
  - PutPublicAccessBlock
  - GetPublicAccessBlock
  - DeletePublicAccessBlock
  - GetBucketPolicyStatus

IAM Access Analyzer for S3 を使用したバケットアクセスの確認

IAM Access Analyzer for S3 は、インターネットの任意のユーザーや他の AWS アカウント (組織外の AWS アカウントを含む) にアクセスを許可するように設定されている S3 バケットに関して警告します。パブリックバケットまたは共有バケットごとに、パブリックアクセスや共有アクセスのソースとレベルを示す結果が送信されます。例えば、IAM Access Analyzer for S3 は、バケットのアクセスコントロールリスト (ACL)、バケットポリシー、マルチリージョンアクセスポイントポリシー、またはアクセスポイントポリシーを通じて、バケットに読み取りまたは書き込みのアクセス許可が提供されていることを示す場合があります。この情報を用いて、迅速で正確な是正処置を講じ、バケットへのアクセスを意図したとおりに復元できます。

IAM Access Analyzer for S3 でリスクのあるバケットを確認した場合、ワンクリックでバケットへのすべてのパブリックアクセスをブロックできます。特定のユースケースをサポートするためにパブリックアクセスが必要な場合を除き、バケットへのすべてのアクセスをブロックすることをお勧めします。すべてのパブリックアクセスをブロックする前に、アプリケーションがパブリックアクセス

なしで正常に動作することを確認してください。詳細については、Amazon S3 ストレージへのパブリックアクセスのブロック を参照してください。

また、バケットレベルのアクセス許可の設定を参照して、きめ細かいアクセスレベルを設定することもできます。静的なウェブサイトホスティング、パブリックダウンロード、クロスアカウント共有など、パブリックアクセスを必要とする特定の検証済みユースケースについては、バケットの結果をアーカイブすることで、バケットをパブリックまたは共有とすることを確定して記録できます。これらのバケット設定はいつでも再確認および変更できます。結果は、監査目的で CSV レポートとしてダウンロードすることもできます。

IAM Access Analyzer for S3 は、Amazon S3 コンソールで追加料金なしで使用できます。IAM Access Analyzer for S3 は、AWS Identity and Access Management (IAM) IAM Access Analyzer を利用しています。Amazon S3 コンソールで IAM Access Analyzer for S3 を使用するには、IAM コンソールにアクセスして、リージョンごとに IAM Access Analyzer を有効にする必要があります。

IAM Access Analyzer の詳細については、「IAM ユーザーガイド」の「IAM Access Analyzer とは?」を参照してください。IAM Access Analyzer for S3 の詳細については、次のセクションを参照してください。

Important

- IAM Access Analyzer for S3 には、アカウントレベルのアナライザーが必要です。IAM Access Analyzer for S3 を使用するには、IAM Access Analyzer にアクセスして、信頼ゾーンとしてアカウントを持つアナライザーを作成する必要があります。詳細については、IAM ユーザーガイド の「IAM Access Analyzer の有効化」を参照してください。
- IAM Access Analyzer for S3 は、クロスアカウントアクセスポイントにアタッチされているアクセスポイントポリシーを分析しません。この動作は、アクセスポイントとそのポリシーが信頼ゾーン、つまりアカウントの外にあるために発生します。クロスアカウントアクセスポイントへのアクセスを委任するバケットは、バケットまたはアカウントにパブリックアクセスをブロックする `RestrictPublicBuckets` 設定を適用していない場合、[Buckets with public access] (パブリックアクセスのあるバケット) に一覧表示されます。パブリックアクセスをブロックする設定 `RestrictPublicBuckets` を適用すると、そのバケットは、[サードパーティーの AWS アカウント を含む他の AWS アカウント からのアクセスがあるバケット] に表示されます。
- バケットポリシーまたはバケット ACL を追加または変更すると、IAM Access Analyzer は 30 分以内に変更に基づいて結果を生成および更新します。アカウントレベルのブロックパブリックアクセス設定に関連する結果は、設定を変更してから最大 6 時間まで生成また

は更新されない場合があります。マルチリージョンアクセスポイントに関連する調査結果は、マルチリージョンアクセスポイントの作成、削除、またはポリシーの変更後、最大 6 時間は生成または更新できない場合があります。

トピック

- IAM Access Analyzer for S3 はどのような情報を提供しますか？
- IAM Access Analyzer for S3 の有効化
- すべてのパブリックアクセスのブロック
- バケットアクセスの確認と変更
- バケットの結果のアーカイブ
- アーカイブされたバケットの結果の有効化
- 結果の詳細の表示
- IAM Access Analyzer for S3 レポートのダウンロード

IAM Access Analyzer for S3 はどのような情報を提供しますか？

IAM Access Analyzer for S3 は、AWS アカウント 外からアクセスできるバケットに関する結果を提供します。[Buckets with public access (パブリックアクセスを許可するバケット)] に表示されるバケットには、インターネットの任意のユーザーがアクセスできます。IAM Access Analyzer for S3 がパブリックバケットを特定すると、リージョン内のパブリックバケット数を示す警告もページの上部に表示されます。第三者を含む、他の AWS アカウント からアクセスのあるバケット — サード・パーティーを含む AWS アカウントでリスト化したバケットは、組織外のアカウントを含む他の AWS アカウント という条件付きで共有されます。

IAM Access Analyzer for S3 は、バケットごとに次の情報を提供します。

- バケット名
- Access Analyzer によって検出 – IAM Access Analyzer for S3 がパブリックまたは共有バケットアクセスを検出したとき。
- 共有方法 – バケットの共有方法 — バケットポリシー、バケット ACL、マルチリージョンアクセスポイントポリシー、またはアクセスポイントポリシーを通じて。マルチリージョンアクセスポイントおよびクロスアカウントアクセスポイントは、アクセスポイントの下に反映されます。バケットは、ポリシーと ACL の両方を通じて共有できます。バケットアクセスのソースを検索して確認する場合は、この列の情報をまず使用して、迅速で正確な是正措置を実行できます。

- ステータス - バケット結果のステータス。IAM Access Analyzer for S3 には、すべてのパブリックバケットと共有バケットの検出結果が表示されます。
  - アクティブ – 結果は確認されていません。
  - アーカイブ済み – 結果は意図したとおりにレビューおよび確認されています。
  - すべて - パブリックバケット、または他の AWS アカウント (組織外の AWS アカウント を含む) との共有バケットに関するすべての結果。
- アクセスレベル – バケットに付与されているアクセス許可:
  - リスト – リソースを一覧表示します。
  - 読み取り – リソースの内容と属性を読み取ります (ただし、編集しません)。
  - 書き込み – リソースを作成、削除、または変更します。
  - アクセス許可 – リソースに対するアクセス許可を付与または変更します。
  - タグ付け – リソースに関連付けられているタグを更新します。

IAM Access Analyzer for S3 の有効化

IAM Access Analyzer for S3 を使用するには、前提条件に関する以下のステップを完了する必要があります。

1. 必要なアクセス権限を付与します。

   詳細については、IAM ユーザーガイドの「IAM Access Analyzer の使用に必要なアクセス許可」を参照してください。
2. IAM にアクセスして、IAM Access Analyzer を使用するリージョンごとにアカウントレベルのアナライザーを作成します。

   IAM Access Analyzer for S3 には、アカウントレベルのアナライザーが必要です。IAM Access Analyzer for S3 を使用するには、信頼ゾーンとしてアカウントを持つアナライザーを作成する必要があります。詳細については、「IAM ユーザーガイド」の「IAM Access Analyzer の有効化」を参照してください。

すべてのパブリックアクセスのブロック

バケットへのすべてのアクセスをワンクリックでブロックする場合は、IAM Access Analyzer for S3 の [Block all public access] (すべてのパブリックアクセスをブロック) ボタンを使用できます。バケットへのすべてのパブリックアクセスをブロックすると、一切のパブリックアクセスが許可されま

せん。特定の検証済みユースケースをサポートするためにパブリックアクセスが必要な場合を除き、バケットへのすべてのパブリックアクセスをブロックすることをお勧めします。すべてのパブリックアクセスをブロックする前に、アプリケーションがパブリックアクセスなしで正常に動作することを確認してください。

バケットへのすべてのパブリックアクセスをブロックしたくない場合は、Amazon S3 コンソールでブロックパブリックアクセス設定を編集して、バケットへの詳細なアクセスレベルを設定できます。詳細については、「Amazon S3 ストレージへのパブリックアクセスのブロック」を参照してください。

まれに、IAM Access Analyzer for S3 と Amazon S3 パブリックアクセスブロックの評価は、バケットがパブリックかどうかによって異なる場合があります。この動作は、Amazon S3 パブリックアクセスブロックが、パブリックアクセスの評価に加えて、アクションの存在についても検証を実行するために発生します。バケットポリシーに、Amazon S3 でサポートされていないアクション (`s3:NotASupportedAction` など) へのパブリックアクセスを許可する `Action` ステートメントが含まれているとします。この場合、Amazon S3 パブリックアクセスブロックはバケットをパブリックとして評価します。このようなステートメントは、アクションが後でサポートされるときにバケットをパブリックにする可能性があるためです。Amazon S3 パブリックアクセスブロックと IAM Access Analyzer for S3 の評価が異なる場合は、バケットポリシーを確認し、サポートされていないアクションを削除することをお勧めします。

IAM Access Analyzer for S3 を使用してバケットへのすべてのパブリックアクセスをブロックするには

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 左側のナビゲーションペインの [ダッシュボード] で、[Access analyzer for S3 (S3 のアクセスアナライザー)] を選択します。
3. IAM Access Analyzer for S3 で、バケットを選択します。
4. [Block all public access (すべてのパブリックアクセスをブロック)] を選択します。
5. バケットへのすべてのパブリックアクセスをブロックすることを確定するには、[Block all public access (bucket settings) (すべてのパブリックアクセスをブロック (バケット設定))] に「**`confirm`**」と入力します。

   Amazon S3 は、バケットへのすべてのパブリックアクセスをブロックします。バケットの検出結果のステータスが [解決済み] に更新され、バケットが IAM Access Analyzer for S3 のリストから消えます。解決済みのバケットを確認する場合は、IAM コンソールで IAM Access Analyzer を開きます。

バケットアクセスの確認と変更

パブリックアカウントや他の AWS アカウント アカウント (組織外のアカウントを含む) にアクセスを許可しない場合は、バケット ACL、バケットポリシー、マルチリージョンアクセスポイントポリシー、またはアクセスポイントポリシーを変更してバケットへのアクセスを削除できます。[Shared Through] 列には、バケットアクセスのすべてのソース (バケットポリシー、バケット ACL、アクセスポイントポリシー) が表示されます。マルチリージョンアクセスポイントおよびクロスアカウントアクセスポイントは、アクセスポイントの下に反映されます。

バケットポリシー、バケット ACL、マルチリージョンアクセスポイント、またはアクセスポイントポリシーを確認および変更するには

1. https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開きます。
2. ナビゲーションペインで、[S3 用 Access Analyzer] を選択します。
3. パブリックアクセスまたは共有アクセスが、バケットポリシー、バケット ACL、マルチリージョンアクセスポイントポリシー、またはアクセスポイントポリシーを通じて許可されているかどうかを確認するには、[Shared through] 列を調べます。
4. [バケット] で、バケットポリシー、バケット ACL、マルチリージョンアクセスポイントポリシー、またはアクセスポイントポリシーを変更または確認するバケットの名前を選択します。
5. バケット ACL を変更または表示するには

   a. [Permissions] を選択します。

   b. [Access Control List] を選択します。

   c. バケット ACL を確認し、必要に応じて変更します。

      詳細については、ACL の設定 を参照してください。
6. バケットポリシーを変更または確認するには

   a. [Permissions] を選択します。

   b. [バケットポリシー] を選択します。

   c. 必要に応じて、バケットポリシーを確認または変更します。

      詳細については、Amazon S3 コンソールを使用したバケットポリシーの追加 を参照してください。
7. マルチリージョンアクセスポイントポリシーを確認または変更するには

   a. [マルチリージョンアクセスポイント] を選択します。

b. マルチリージョンアクセスポイント名を選択します。

c. 必要に応じて、マルチリージョンアクセスポイントポリシーを確認または変更します。

詳細については、アクセス許可 を参照してください。

8. アクセスポイントポリシーを確認または変更するには

a. [access points] (アクセスポイント) を選択します。

b. アクセスポイント名を選択します。

c. 必要に応じてアクセスを確認または変更します。

詳細については、汎用バケットの Amazon S3 アクセスポイントの管理 を参照してください。

バケット ACL、バケットポリシー、アクセスポイントポリシーを編集または削除してパブリックアクセスまたは共有アクセスを削除すると、バケットの結果のステータスが解決済みに更新されます。解決済みのバケットの検出結果は IAM Access Analyzer for S3 リストから消えますが、IAM Access Analyzer で表示できます。

バケットの結果のアーカイブ

バケットが、特定のユースケース (静的ウェブサイト、パブリックダウンロード、クロスアカウント共有など) をサポートするために、パブリックアカウントや他の AWS アカウント (組織外のアカウントを含む) へのアクセスを許可する場合は、バケットの結果をアーカイブできます。バケットの結果をアーカイブする場合、バケットをパブリックまたは共有にすることを確定して記録します。アーカイブされたバケットの検出結果は IAM Access Analyzer for S3 リストに残るため、どれがパブリックバケットまたは共有バケットであるかを常に把握できます。

IAM Access Analyzer for S3 でバケットの検出結果をアーカイブするには

1. https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開きます。
2. ナビゲーションペインで、[S3 用 Access Analyzer] を選択します。
3. IAM Access Analyzer for S3 で、アクティブなバケットを選択します。
4. このバケットにパブリックアカウントや他の AWS アカウント (組織外のアカウントを含む) からアクセスすることを確定するには、[Archive] (アーカイブ) を選択します。
5. 「**`confirm`**」と入力し、[アーカイブ] を選択します。

アーカイブされたバケットの結果の有効化

結果のアーカイブ後は、いつでも結果に再アクセスし、ステータスをアクティブに戻すことができます。この場合、バケットには別のレビューが必要になります。

アーカイブされたバケットの検出結果を IAM Access Analyzer for S3 でアクティブにするには

1. https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開きます。
2. ナビゲーションペインで、[Access analyzer for S3 (S3 のアクセスアナライザー)] を選択します。
3. アーカイブされたバケットの結果を選択します。
4. [Mark as active (アクティブとしてマーク)] を選択します。

結果の詳細の表示

バケットの詳細情報を表示する必要がある場合は、IAM コンソールの IAM Access Analyzer でバケットの結果の詳細を開くことができます。

IAM Access Analyzer for S3 で検出結果の詳細を表示するには

1. https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開きます。
2. ナビゲーションペインで、[S3 用 Access Analyzer] を選択します。
3. IAM Access Analyzer for S3 で、バケットを選択します。
4. [View details] (詳細を表示する) をクリックします。

   結果の詳細が IAM コンソールの IAM Access Analyzer で開きます。

IAM Access Analyzer for S3 レポートのダウンロード

バケットの結果を CSV レポートとしてダウンロードし、監査目的に使用できます。レポートには、Amazon S3 コンソールの IAM Access Analyzer for S3 に表示される情報と同じ情報が含まれます。

レポートをダウンロードするには

1. https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開きます。

2. 左側のナビゲーションペインで、[Access analyzer for S3 (S3 のアクセスアナライザー)] を選択します。
3. [リージョンフィルタ] で、[リージョン] を選択します。

   IAM Access Analyzer for S3 が更新され、選択したリージョンのバケットが表示されます。
4. [レポートのダウンロード] を選択します。

   CSV レポートが生成され、コンピュータに保存されます。

バケット所有者条件によるバケット所有者の確認

Amazon S3 バケット所有者条件では、S3 オペレーションで使用するバケットが適切な AWS アカウントに属していることを確認します。

ほとんどの S3 オペレーションでは、特定の S3 バケットに対して読み取りまたは書き込みを行います。これらのオペレーションには、オブジェクトのアップロード、コピー、ダウンロード、バケット設定の取得または変更、オブジェクト設定の取得または変更が含まれます。これらのオペレーションを実行するときは、リクエストにバケット名を含めることによって、使用するバケットを指定します。例えば、S3 からオブジェクトを取得するには、バケットの名前と、そのバケットから取得するオブジェクトキーを指定してリクエストを作成します。

Amazon S3 は、名前に基づいてバケットを識別するため、アプリケーションでリクエストに誤ったバケット名を使用した場合、正しくないバケットに対して、誤ってオペレーションが実行される可能性があります。このような状況で意図しないバケットとのやり取りを回避するために、バケット所有者条件を使用できます。バケット所有者条件を使用すると、ターゲットバケット所有者が正しい AWS アカウント であることを確認して、S3 オペレーションの効果が意図どおりになることをさらに保証できます。

トピック

- バケット所有者条件を使用する状況
- バケット所有者の確認
- 例
- 制約と制限

バケット所有者条件を使用する状況

正しいバケット所有者のアカウント ID がわかっていて、サポートされている S3 オペレーションを実行する場合は、バケット所有者条件を使用することをお勧めします。バケット所有者条件は、すべての S3 オブジェクトオペレーションおよびほとんどの S3 バケットオペレーションで使用できます。バケット所有者条件がサポートされない S3 オペレーションのリストについては、制約と制限を参照してください。

バケット所有者条件を使用するメリットを確認するには、AWS の顧客である Bea に関係する次のシナリオを考察してください。

1. Bea は Amazon S3 を使用するアプリケーションを開発しています。開発中、Bea はテスト専用の AWS アカウントを使用して `bea-data-test` という名前のバケットを作成し、アプリケーションで `bea-data-test` にリクエストが実行されるように設定しました。
2. Bea はアプリケーションをデプロイしましたが、本稼働用の AWS アカウントでバケットを使用するようにアプリケーションを再設定するのを忘れました。
3. 本稼働環境では、Bea のアプリケーションが `bea-data-test` にリクエストを行い、その実行に成功しました。その結果、Bea のテストアカウントのバケットに本稼働用データが書き込まれます。

Bea は、バケット所有者条件を使用することで、このような状況を回避できます。バケット所有者条件を使用すると、Bea は正しいバケット所有者の AWS アカウント ID をリクエストに含めることができます。Amazon S3 は、各リクエストを処理する前に、バケット所有者のアカウント ID をチェックします。実際のバケット所有者が正しいバケット所有者と一致しない場合、リクエストは失敗します。

Bea がバケット所有者条件を使用する場合、前述のシナリオで Bea のアプリケーションが誤ってテストバケットに書き込むことにはなりません。その代わりに、ステップ 3 でアプリケーションが行うリクエストは失敗し、`Access Denied` エラーメッセージが表示されます。バケット所有者条件を使用することで、Bea は正しくない AWS アカウント のバケットと誤ってやり取りするリスクを排除できます。

バケット所有者の確認

バケット所有者条件を使用するには、正しいバケット所有者を指定するパラメータをリクエストに含めます。ほとんどの S3 オペレーションに含まれるバケットは 1 つだけであり、バケット所有者条件を使用するために必要になるのは、この 1 つのパラメータのみです。`CopyObject` オペレーション

の場合、この最初のパラメータでは宛先バケットの正しい所有者を指定します。ソースバケットの正しい所有者を指定するには、2 番目のパラメータを含めます。

バケット所有者条件パラメータを含むリクエストを行うと、S3 はリクエストを処理する前に、指定されたパラメータに対してバケット所有者のアカウント ID をチェックします。パラメータがバケット所有者のアカウント ID と一致すると、S3 がリクエストを処理します。パラメータがバケット所有者のアカウント ID と一致しない場合、リクエストは失敗し、`Access Denied` エラーメッセージが表示されます。

バケット所有者条件は、AWS Command Line Interface (AWS CLI)、AWS SDK、および Amazon S3 REST API で使用できます。AWS CLI および Amazon S3 REST API でバケット所有者条件を使用する場合は、次のパラメータ名を使用します。

アクセス方法	コピーオペレーション以外のパラメータ	コピーオペレーションのソースパラメータ	コピーオペレーションの宛先パラメータ
AWS CLI	`--expected-bucket-owner`	`--expected-source-bucket-owner`	`--expected-bucket-owner`
Amazon S3 REST API	`x-amz-expected-bucket-owner` ヘッダー	`x-amz-source-expected-bucket-owner` ヘッダー	`x-amz-expected-bucket-owner` ヘッダー

AWS SDK でバケット所有者条件を使用するために必要なパラメータ名は、言語によって異なります。必要なパラメータを確認するには、使用する言語の SDK ドキュメント を参照してください。SDK ドキュメントには、AWS での構築ツールからアクセスできます。

例

以下の例は、AWS CLI または AWS SDK for Java 2.x を使用してバケット所有者条件を Amazon S3 に実装する方法を示しています。

Example

例: オブジェクトのアップロード

次の例では、バケット所有者条件を使用して S3 バケット *amzn-s3-demo-bucket1* にオブジェクトをアップロードし、*amzn-s3-demo-bucket1* の所有者が AWS アカウント 111122223333 であることを確認します。

AWS CLI

```
aws s3api put-object \
                  --bucket amzn-s3-demo-bucket1 --key exampleobject --
body example_file.txt \
                  --expected-bucket-owner 111122223333
```

AWS SDK for Java 2.x

```
public void putObjectExample() {
    S3Client s3Client = S3Client.create();;
    PutObjectRequest request = PutObjectRequest.builder()
            .bucket("amzn-s3-demo-bucket1")
            .key("exampleobject")
            .expectedBucketOwner("111122223333")
            .build();
    Path path = Paths.get("example_file.txt");
    s3Client.putObject(request, path);
}
```

Example

例: オブジェクトのコピー

次の例では、S3 バケット *amzn-s3-demo-bucket1* から S3 バケット *amzn-s3-demo-bucket2* にオブジェクト object1 をコピーします。この例では、バケット所有者条件を使用し、次の表に従って、バケットを所有するアカウントが正しいことを確認します。

バケット	正しい所有者
amzn-s3-demo-bucket1	111122223333
amzn-s3-demo-bucket2	444455556666

AWS CLI

```
aws s3api copy-object --copy-source amzn-s3-demo-bucket1/object1 \
                            --bucket amzn-s3-demo-bucket2 --key object1copy \
                            --expected-source-bucket-owner 111122223333 --expected-
bucket-owner 444455556666
```

AWS SDK for Java 2.x

```
public void copyObjectExample() {
        S3Client s3Client = S3Client.create();
        CopyObjectRequest request = CopyObjectRequest.builder()
                .copySource("amzn-s3-demo-bucket1/object1")
                .destinationBucket("amzn-s3-demo-bucket2")
                .destinationKey("object1copy")
                .expectedSourceBucketOwner("111122223333")
                .expectedBucketOwner("444455556666")
                .build();
        s3Client.copyObject(request);
    }
```

Example

例: バケットポリシーの取得

次の例では、バケット所有者条件を使用して S3 バケット *amzn-s3-demo-bucket1* のアクセスポリシーを取得し、*amzn-s3-demo-bucket1* の所有者が AWS アカウント 111122223333 であることを確認します。

AWS CLI

```
aws s3api get-bucket-policy --bucket amzn-s3-demo-bucket1 --expected-bucket-
owner 111122223333
```

AWS SDK for Java 2.x

```
public void getBucketPolicyExample() {
    S3Client s3Client = S3Client.create();
    GetBucketPolicyRequest request = GetBucketPolicyRequest.builder()
            .bucket("amzn-s3-demo-bucket1")
```

```
            .expectedBucketOwner("111122223333")
            .build();
    try {
        GetBucketPolicyResponse response = s3Client.getBucketPolicy(request);
    }
    catch (S3Exception e) {
        // The call was transmitted successfully, but Amazon S3 couldn't process
        // it, so it returned an error response.
        e.printStackTrace();
    }
}
```

制約と制限

Amazon S3 バケット所有者条件には、次の制約と制限があります。

- バケット所有者条件パラメータの値は、AWS アカウント ID (12 桁の数値) である必要があります。サービスプリンシパルはサポートされていません。
- バケット所有者条件は、CreateBucket、ListBuckets、または AWS S3 コントロールに含まれるオペレーションでは使用できません。Amazon S3 では、これらのオペレーションに対するリクエストに含まれるバケット所有者条件パラメータがすべて無視されます。
- バケット所有者条件は、検証パラメータで指定されたアカウントがバケットを所有しているかどうかのみを検証します。バケット所有者条件で、バケットの設定はチェックされません。また、バケットの設定が特定の条件を満たしていること、または過去の状態と一致することを保証するものではありません。

オブジェクトの所有権の制御とバケットの ACL の無効化。

S3 オブジェクト所有権は、Amazon S3 バケットレベルの設定で、バケットにアップロードされたオブジェクトの所有権を制御し、アクセスコントロールリスト (ACL) を有効または無効にするのに使用できます。デフォルトでは、オブジェクト所有権は[バケット所有者の強制] 設定に設定され、すべての ACL は無効になっています。ACL が無効になっている場合、バケット所有者はバケット内のすべてのオブジェクトを所有し、アクセス管理ポリシーのみを使用してデータへのアクセスを管理します。

Amazon S3 の最新のユースケースの大部分では ACL を使用する必要がなくなっています。そのため、オブジェクトごとに個別にアクセスを制御する必要がある異常な状況を除き、ACL を無効にしておくことをお勧めします。ACL を無効にすると、バケット内のオブジェクトをアップロードした

ユーザーに関係なく、ポリシーを使用してバケット内のすべてのオブジェクトへのアクセスをより簡単に制御できます。

オブジェクト所有権には、バケットにアップロードされるオブジェクトの所有権を制御し、ACL を無効または有効化するために使用できる 3 つの設定があります。

ACL の無効化

- バケット所有者の強制 (デフォルト) – ACL は無効になり、バケット所有者はバケット内のすべてのオブジェクトを自動的に所有し、完全に制御します。ACL は、S3 バケット内のデータに対するアクセス許可に対して影響を与えません。バケットは、ポリシーを使用してアクセスコントロールを定義します。

ACL の有効化。

- 希望するバケット所有者 — バケット所有者は、他のアカウントが `bucket-owner-full-control` 既定 ACL でバケットに書き込む新しいオブジェクトを所有し、完全にコントロールできます。
- オブジェクトライター — オブジェクトをアップロードする AWS アカウント は、そのオブジェクトを所有し、そのオブジェクトを完全にコントロールし、ACL を介して他のユーザーにそのオブジェクトへのアクセス権を付与できます。

S3 の最近のユースケースの大部分では、[バケット所有者の強制] 設定を適用して ACL を無効なままにし、必要に応じてバケットポリシーを使用して、アカウント外のユーザーとデータを共有することをお勧めします。このアプローチにより、アクセス許可の管理が簡素化されます。新しく作成されたバケットと既存のバケットの両方で ACL を無効にすることができます。新しく作成されたバケットでは、ACL はデフォルトで無効になっています。既存のバケットに既にオブジェクトが含まれている場合、ACL を無効にすると、オブジェクトとバケット ACL はアクセス評価に含まれなくなり、ポリシーに基づいてアクセスが許可または拒否されます。既存のバケットについては、ACL を無効にした後いつでも再度有効化でき、既存のバケットとオブジェクト ACL が復元されます。

ACL を無効にする前に、バケットポリシーを確認して、アカウント外のバケットへのアクセス権を付与するすべての方法をカバーすることを確認することをお勧めします。ACL を無効にすると、バケットは ACL を指定しない PUT リクエスト、またはバケット所有者のフルコントロール ACL (`bucket-owner-full-control` で既定の ACL またはこの ACL と同等の XML で表される形式など) を持つ PUT リクエストのみを受け入れます。バケット所有者のフルコントロール ACL をサポートする既存のアプリケーションには影響はありません。他の ACL (特定の AWS アカウント へのカス

タム許可など) を含む PUT リクエストは失敗し、AccessControlListNotSupported エラーコードを含む 400 エラーを返します。

それとは対照に、[バケット所有者が推奨] で設定されているバケットは、引き続きバケットおよびオブジェクト ACL を受け入れ、遵守します。この設定では、新しいオブジェクトが bucket-owner-full-control 既定 ACL はオブジェクトライターではなく、バケット所有者によって自動的に所有されます。その他のすべての ACL 動作はそのまま残ります。すべての Amazon S3 PUT 操作に bucket-owner-full-control 既定 ACL を含めるように要求するには、この ACL を使用したオブジェクトのアップロードのみを許可するバケットポリシーを追加できます。

どのオブジェクト所有権設定がバケットに適用されているかを確認するには、Amazon S3 ストレージレンズメトリクスを使用できます。S3 ストレージレンズは、オブジェクトストレージの使用状況とアクティビティを組織全体で可視化するために使用できるクラウドストレージ分析機能です。詳細については、「Using S3 Storage Lens to find Object Ownership settings」(S3 ストレージレンズを使用してオブジェクト所有権の設定を検索する) を参照してください。

> **Note**
>
> Amazon S3 Express One Zone ストレージクラスをディレクトリバケットで使用する方法の詳細については、「S3 Express One Zone」と「ディレクトリバケットの使用」を参照してください。

オブジェクトの所有権の設定

この表は、各オブジェクト所有権設定が ACL、オブジェクト、オブジェクト所有権、およびオブジェクトアップロードに与える影響を示しています。

設定	適用先	オブジェクトの所有者への影響	ACL への影響	アップロードを受け付けました
バケット所有者強制 (デフォルト)	既存のオブジェクトと新しいオブジェクト	バケット所有者はすべてのオブジェクトを所有しています。	ACL は無効になり、バケットへのアクセス権限には影響しません。ACL を設定または更新する要求は失	バケット所有者の完全制御 ACL を使用したアップロード、または ACL を指定しないアップロード。

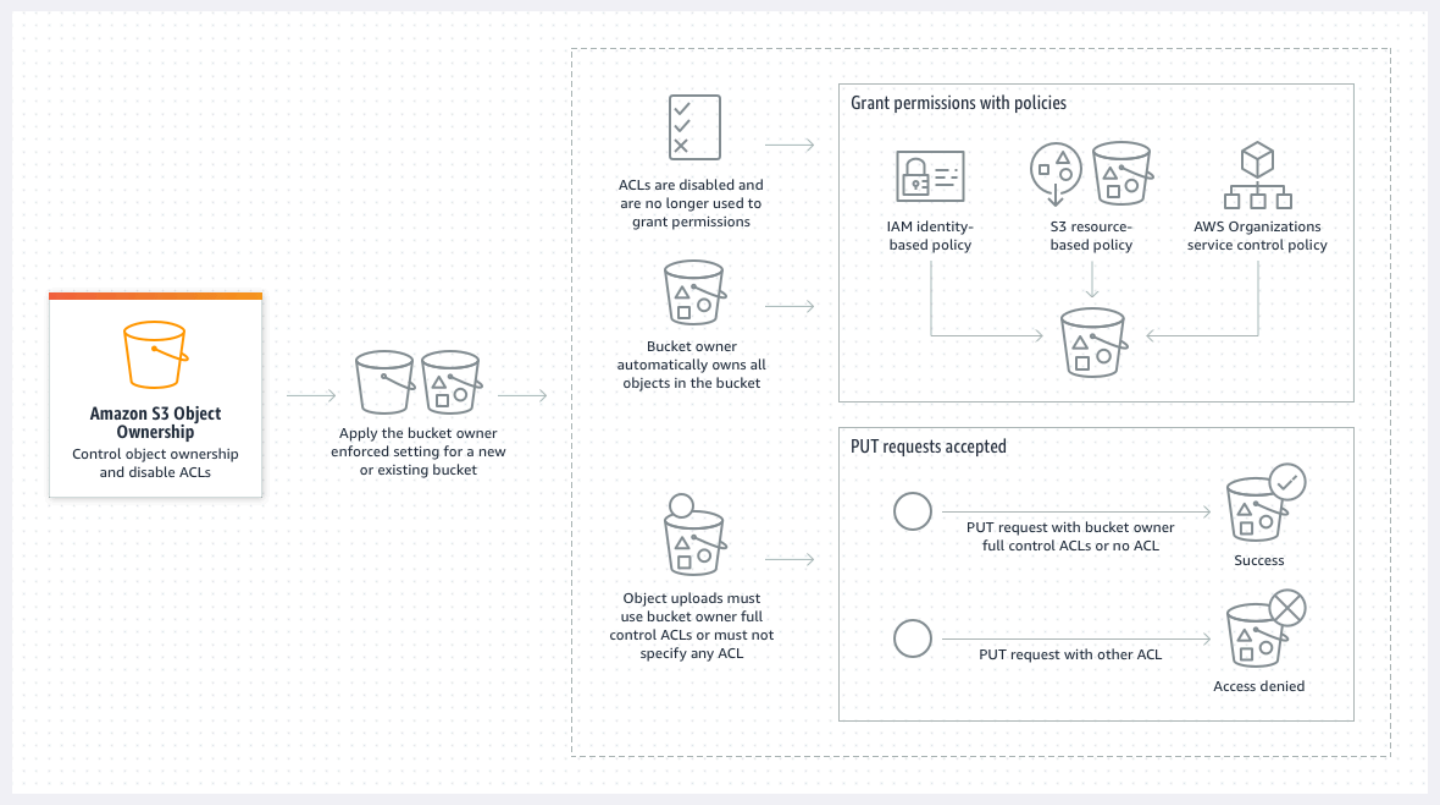
設定	適用先	オブジェクトの所有者への影響	ACL への影響	アップロードを受け付けました
			敗します。ただし、ACL の読み取り要求はサポートされています。 バケット所有者は完全な所有権と制御を有しています。 オブジェクトライターには完全な所有権と制御がなくなりました。	
バケット所有者推奨。	新しいオブジェクト。	オブジェクトのアップロードが `bucket-owner-full-control` 既定 ACL を含む場合、バケット所有者はオブジェクトを所有しています。 他の ACL でアップロードしたオブジェクトは、書き込みアカウントによって所有されます。	ACL は更新でき、許可を付与できます。 オブジェクトのアップロードが `bucket-owner-full-control` 既定 ACL を含む場合、バケット所有者は完全制御アクセスであり、オブジェクトライターは完全制御アクセスではありません。	すべてアップロードします。

設定	適用先	オブジェクトの所有者への影響	ACL への影響	アップロードを受け付けました
オブジェクトライター	新しいオブジェクト	オブジェクトライターがオブジェクトを所有します。	ACL は更新でき、許可を付与できます。 オブジェクトライターは完全制御アクセスを有します。	すべてをアップロード

ACL を無効にして導入された変更

オブジェクト所有権に対して [バケット所有者の強制] 設定を適用すると、ACL は無効になり、追加のアクションを実行せずに、バケット内のすべてのオブジェクトを自動的に所有し、完全に制御できます。[バケット所有者の強制] 設定は、新しく作成されたすべてのバケットでデフォルト設定となっています。[バケット所有者の強制] 設定が適用されると、3 つの変更が表示されます。

- すべてのバケット ACL とオブジェクト ACL が無効になり、バケット所有者としてフルアクセスが付与されます。バケットまたはオブジェクトに対して読み取り ACL リクエストを実行すると、バケット所有者にのみフルアクセスが付与されていることがわかります。
- バケット所有者は、バケット内のすべてのオブジェクトを自動的に所有し、完全に制御できます。
- ACL はバケットへのアクセス許可に影響を与えなくなりました。その結果、データのアクセスコントロールは、AWS Identity and Access Management (IAM) アイデンティティベースのポリシー、Amazon S3 バケットポリシー、VPC エンドポイントポリシー、Organizations サービスコントロールポリシー (SCP)、リソースコントロールポリシー (RCP) などのポリシーに基づいています。



S3 バージョニングを使用する場合、バケット所有者はバケット内のすべてのオブジェクトバージョンを所有し、完全に制御できます。[バケット所有者の強制] 設定を適用しても、オブジェクトの新しいバージョンは追加されません。

新しいオブジェクトをバケットにアップロードできるのは、バケット所有者の完全制御 ACL を使用するか、ACL を指定しない場合のみです。オブジェクトのアップロードは、他の ACL を指定すると失敗します。詳細については、トラブルシューティング を参照してください。

次の AWS Command Line Interface(AWS CLI) を利用した PutObject オペレーションの例には、bucket-owner-full-control 既定 ACL が含まれるため、無効な ACL を持つバケットにオブジェクトをアップロードできます。

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key key-name --body path-to-file --
acl bucket-owner-full-control
```

以下の PutObject オペレーションは ACL を指定しないため、無効な ACL を持つバケットでも成功します。

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key key-name --body path-to-file
```

> **Note**
>
> アップロード後に他の AWS アカウント が、オブジェクトにアクセスする必要がある場合は、バケットポリシーを介してそれらのアカウントに追加のアクセス許可を付与する必要があります。詳細については、チュートリアル: ポリシーを使用した Amazon S3 リソースへのアクセスの管理 を参照してください。

ACL の再有効化

[バケット所有者の強制] 設定から別のオブジェクト所有権設定にいつでも変更することで ACL を再度有効にできます。[バケット所有者の強制] 設定を適用する前に、許可管理のオブジェクト ACL を使用し、これらのオブジェクト ACL アクセス権限をバケットポリシーに移行しなかった場合は、ACL を再度有効にした後に、これらのアクセス許可が復元されます。さらに、[バケット所有者の強制] 設定が適用されている間にバケットに書き込まれたオブジェクトは、バケット所有者によって所有されます。

例えば、[バケット所有者の強制] から [オブジェクトライター] 設定に戻すと、バケット所有者として、他の AWS アカウント が以前に所有していたオブジェクトを所有できなくなり、完全に制御できなくなります。代わりに、アップロードするアカウントがこれらのオブジェクトを再び所有します。他のアカウントが所有するオブジェクトは、許可用の ACL を使用するため、これらのオブジェクトに許可を与えるためポリシーを使用できません。ただし、[バケット所有者の強制] 設定が適用されている間、バケットに書き込まれたオブジェクトは、バケット所有者として引き続き所有されます。ACL を再度有効にしても、これらのオブジェクトはオブジェクトライターによって所有されません。

AWS Management Console、AWS Command Line Interface (CLI)、REST API、または AWS SDK を使用して ACL を有効化および管理する手順については、ACL の設定 を参照してください。

ACL を無効にする前提条件

既存のバケットの ACL を無効にする前に、以下の前提条件を満たしていることを確認してください。

- バケットとオブジェクト ACL を確認し、ACL アクセス権限を移行します。
- 承認に ACL を必要としたリクエストを特定する
- ACL 関連の条件キーを使用するバケットポリシーを確認および更新します。

オブジェクトの所有者許可

バケットのオブジェクト所有権設定を適用、更新、または削除するには、`s3:PutBucketOwnershipControls` 許可が必要です。バケットのオブジェクトの所有権の設定を返すには、`s3:GetBucketOwnershipControls` 許可が必要です。詳細については、バケットの作成時のオブジェクトの所有権の設定。 および S3 バケットのオブジェクト所有権設定の表示 を参照してください。

すべての新しいバケットの ACL を無効にします。

デフォルトでは、新しく作成されたバケットにはすべて[バケット所有者の強制] 設定が適用されており、ACL は無効になっています。ACL は無効にしておくことをお勧めします。原則として、アクセスコントロールには ACL ではなく S3 リソースベースのポリシー (バケットポリシーとアクセスポイントポリシー) または IAM ポリシーを使用することをお勧めします。ポリシーとは、よりシンプルで柔軟なアクセスコントロールのオプションです。バケットポリシーとアクセスポイントポリシーを使用すると、Amazon S3 リソースに対するすべてのリクエストに広く適用されるルールを定義できます。

レプリケーションとオブジェクトの所有権。

S3 レプリケーションを使用し、ソースバケットと宛先バケットが異なる AWS アカウント に所有されている場合、ACL を無効にして (バケット所有者にオブジェクト所有権の設定を適用して)、レプリカの所有権を宛先バケットを所有する AWS アカウント に変更できます。この設定は、`s3:ObjectOwnerOverrideToBucketOwner` 許可の必要なく、既存の所有者のオーバーライド動作を模倣します。[バケット所有者の強制] 設定で宛先バケットにレプリケーションされるすべてのオブジェクトは、宛先バケット所有者によって所有されます。レプリケーション設定の所有者上書きオプションの詳細については、レプリカ所有者の変更 を参照してください。

オブジェクトの所有権の設定

オブジェクト所有権の設定は、S3 コンソール、AWS CLI、AWS SDK、Amazon S3 REST API、または AWS CloudFormation を使用して適用できます。以下の REST API と AWS CLI コマンドは、オブジェクトの所有権をサポートしています。

REST API	AWS CLI	説明
PutBucketOwnershipControls	put-bucket-ownership-controls	既存の S3 バケットのオブジェクト所有権設定を作成または変更します。
CreateBucket	create-bucket	`x-amz-object-ownership` リクエストヘッダーを使用してバケットを作成し、オブジェクトの所有権設定を指定します。
GetBucketOwnershipControls	get-bucket-ownership-controls	Amazon S3 バケットのオブジェクト所有権設定を取り戻します。
DeleteBucketOwnershipControls	delete-bucket-ownership-controls	Amazon S3 バケットのオブジェクトの所有権の設定を削除します。

オブジェクト所有権設定の適用と操作の詳細については、以下のトピックを参照してください。

トピック

- ACL を無効にする前提条件。
- バケットの作成時のオブジェクトの所有権の設定。
- 既存のバケットでのオブジェクトの所有権の設定
- S3 バケットのオブジェクト所有権設定の表示
- すべての新しいバケットの ACL を無効にし、オブジェクト所有権を執行します。
- トラブルシューティング

ACL を無効にする前提条件。

Amazon S3 のバケットアクセスコントロールリスト (ACL) は、S3 バケット内の個々のオブジェクトに対する詳細なアクセス許可を定義し、それらのオブジェクトにアクセスして変更できる AWS アカウントまたはグループを指定できるメカニズムです。Amazon S3 の最新のユースケースの大部分

では ACL を使用する必要がなくなっています。オブジェクトごとに個別に制御する必要がある通常ではない状況を除き、アクセスの管理には AWS Identity and Access Management (IAM) とバケットポリシーを使用し、ACL を無効にしておくことをお勧めします。

バケットで ACL が有効になっている場合は、ACL を無効にする前に、次の前提条件を満たしてください。

トピック

- バケットとオブジェクト ACL を確認し、ACL アクセス権限を移行します。
- 承認に ACL を必要としたリクエストを特定する
- ACL 関連の条件キーを使用するバケットポリシーを確認および更新します。
- ユースケースの例

バケットとオブジェクト ACL を確認し、ACL アクセス権限を移行します。

ACL を無効にすると、バケットおよびオブジェクト ACL によって付与される許可がアクセスに影響しなくなります。ACL を無効にする前に、バケットとオブジェクト ACL を確認します。

IAM ポリシーでは、既存のバケットとオブジェクト ACL にはそれぞれ同等のものが含まれます。次のバケットポリシー例は、バケットおよびオブジェクト ACL の `READ` と `WRITE` の許可は IAM 許可にマッピングされます。各 ACL が IAM アクセス許可に変換される方法の詳細については、ACL アクセス許可とアクセスポリシーのアクセス許可のマッピング を参照してください。

ACL を無効にする前に:

- バケット ACL が AWS アカウント外へのアクセスを許可している場合は、まず、バケット ACL のアクセス許可をバケットポリシーに移行する必要があります。
- 次に、バケット ACL をデフォルトのプライベート ACL にリセットします。
- オブジェクトレベルの ACL アクセス許可を確認し、バケットポリシーに移行することもお勧めします。

バケット ACL がアカウント外の他のユーザーに読み取りまたは書き込みアクセス許可を付与している場合は、ACL を無効にする前に、これらのアクセス許可をバケットポリシーに移行する必要があります。これらのアクセス許可を移行した後、[オブジェクトの所有権] を [バケット所有者強制] 設定にすることができます。アカウントの外部で読み取りまたは書き込みアクセスを許可するバケット ACL を移行しないと、[バケット所有者の強制] 設定を適用するリクエストが失敗し、InvalidBucketAclWithObjectOwnership エラーコードを返します。

バケット ACL が AWS アカウント の外部へのアクセスを許可する場合は、ACL を無効にする前にバケット ACL アクセス権限をバケットポリシーに移行し、バケット ACL をデフォルトのプライベート ACL にリセットする必要があります。移行とリセットを行わない場合、ACL を無効にするために [バケット所有者の強制] 設定を適用するリクエストは失敗し、InvalidBucketAclWithObjectOwnership エラーコードが返されます。また、オブジェクト ACL アクセス権限を確認し、バケットポリシーに移行することをお勧めします。

バケットポリシーへの ACL アクセス権限を確認し、移行するには、以下のトピックを参照してください。

トピック

- バケットポリシーの例
- S3 コンソールを使用した、ACL アクセス権限の確認と移行
- AWS CLI を使用して、ACL アクセス権限を確認して移行します。

バケットポリシーの例

これらのバケットポリシーの例は、READ と WRITE バケット、サードパーティー AWS アカウントの ACL アクセス権限をバケットポリシーに移行およびバケット化およびオブジェクト化する方法を示しています。READ_ACP と WRITE_ACP ACL は、ACL 関連のアクセス許可 (s3:GetBucketAcl、s3:GetObjectAcl、s3:PutBucketAcl、s3:PutObjectAcl) を付与するため、ポリシーとの関連性は低くなります。

Example — バケットの **READ** ACL

バケットの内容の一覧表示を AWS アカウント *111122223333* に許可する READ ACL がバケットにある場合、バケットに対して s3:ListBucket、s3:ListBucketVersions、s3:ListBucketMultipartUploads の各アクセス許可を付与するバケットポリシーを記述できます。

```
{
  "Version": "2012-10-17",
  "Statement": [
   {
    "Sid": "Permission to list the objects in a bucket",
    "Effect": "Allow",
    "Principal": {
     "AWS": [
```

```
      "arn:aws:iam::111122223333:root"
     ]
    },
    "Action": [
     "s3:ListBucket",
     "s3:ListBucketVersions",
     "s3:ListBucketMultipartUploads"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
   }
  ]
 }
```

Example — バケット内の各オブジェクトの **READ** ACL

AWS アカウント *111122223333* にアクセスを許可する READ ACL がバケット内の各オブジェクトにある場合、バケット内の各オブジェクトに対する s3:GetObject アクセス許可と s3:GetObjectVersion アクセス許可をこのアカウントに付与するバケットポリシーを記述できます。

```
{
  "Version": "2012-10-17",
  "Statement": [
   {
    "Sid": "Read permission for every object in a bucket",
    "Effect": "Allow",
    "Principal": {
     "AWS": [
      "arn:aws:iam::111122223333:root"
     ]
    },
    "Action": [
     "s3:GetObject",
     "s3:GetObjectVersion"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
   }
  ]
 }
```

この例のリソースエレメントは、特定のオブジェクトへのアクセスを許可します。

```
"Resource": "arn:aws:s3:::amzn-s3-demo-bucket/OBJECT-KEY"
```

Example — バケットにオブジェクトを書き込むアクセス許可を付与する **WRITE** ACL

バケットへのオブジェクトの書き込み許可を AWS アカウント *111122223333* に付与する WRITE ACL がバケットにある場合は、バケットに s3:PutObject 許可を付与するバケットポリシーを記述できます。

```
{
  "Version": "2012-10-17",
  "Statement": [
   {
    "Sid": "Permission to write objects to a bucket",
    "Effect": "Allow",
    "Principal": {
     "AWS": [
      "arn:aws:iam::111122223333:root"
     ]
    },
    "Action": [
     "s3:PutObject"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
   }
  ]
 }
```

S3 コンソールを使用した、ACL アクセス権限の確認と移行

バケットの ACL アクセス権限を確認する方法

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. [バケット] リストで、バケット名を選択します。
3. [アクセス許可] タブを選択します。
4. アクセスコントロールリスト (ACL) で、バケット ACL アクセス権限を確認します。

オブジェクトの ACL アクセス権限を確認する方法

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. [Buckets] (バケット) リストで、オブジェクトが含まれるバケットの名前を選択します。
3. [オブジェクト] リストで、オブジェクト名を選択します。
4. [アクセス許可] タブを選択します。
5. アクセスコントロールリスト (ACL) で、オブジェクト ACL アクセス権限を確認します。

ACL アクセス権限を移行してバケット ACL を更新します

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. [バケット] リストで、バケット名を選択します。
3. アクセス許可タブの バケットポリシーで 編集をクリックします。
4. ポリシーボックスで、バケットポリシーを追加または更新します。

   バケットポリシーの例ついては、バケットポリシーの例」 と「ユースケースの例 を参照してください。
5. [Save changes] (変更の保存) をクリックします。
6. バケット ACL を更新して、他のグループ、または AWS アカウント への ACL アクセス権限を削除します。
7. オブジェクト所有権にバケット所有者の強制設定を適用します。

AWS CLI を使用して、ACL アクセス権限を確認して移行します。

1. バケットのバケット ACL を返すには、get-bucket-acl AWS CLI コマンドを使用します。

   ```
   aws s3api get-bucket-acl --bucket amzn-s3-demo-bucket
   ```

   例えば、このバケット ACL は WRITE と READ にサードパーティーのアカウントへのアクセスを付与します。この ACL では、サードパーティーアカウントは正規ユーザー ID で識別します。[バケット所有者の強制] 設定を適用して ACL を無効にするには、サードパーティアカウントのこれらの許可をバケットポリシーに移行する必要があります。

```
{
  "Owner": {
   "DisplayName": "DOC-EXAMPLE-ACCOUNT-OWNER",
   "ID": "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID"
  },
  "Grants": [
   {
    "Grantee": {
     "DisplayName": "DOC-EXAMPLE-ACCOUNT-OWNER",
     "ID": "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID",
     "Type": "CanonicalUser"
    },
    "Permission": "FULL_CONTROL"
   },
   {
    "Grantee": {
     "DisplayName": "THIRD-PARTY-EXAMPLE-ACCOUNT",
     "ID":
"72806de9d1ae8b171cca9e2494a8d1335dfced4ThirdPartyAccountCanonicalUserID",
     "Type": "CanonicalUser"
    },
    "Permission": "READ"
   },
   {
    "Grantee": {
     "DisplayName": "THIRD-PARTY-EXAMPLE-ACCOUNT",
     "ID":
"72806de9d1ae8b171cca9e2494a8d1335dfced4ThirdPartyAccountCanonicalUserID",
     "Type": "CanonicalUser"
    },
    "Permission": "WRITE"
   }
  ]
 }
```

その他の ACL の例については、ユースケースの例 を参照してください。

2. バケット ACL アクセス権限をバケットポリシーに移行します。

   この例のバケットポリシーは、サードパーティアカウントの `s3:PutObject` と `s3:ListBucket` アクセス許可を付与します。バケットポリシーでは、サードパーティーアカウントは AWS アカウント ID (*111122223333*)で識別されます。

```
aws s3api put-bucket-policy --bucket amzn-s3-demo-bucket --policy file://
policy.json

 policy.json:
 {
  "Version": "2012-10-17",
  "Statement": [
   {
    "Sid": "PolicyForCrossAccountAllowUpload",
    "Effect": "Allow",
    "Principal": {
     "AWS": [
      "arn:aws:iam::111122223333:root"
     ]
    },
    "Action": [
     "s3:PutObject",
     "s3:ListBucket"
    ],
    "Resource": [
     "arn:aws:s3:::amzn-s3-demo-bucket",
     "arn:aws:s3:::amzn-s3-demo-bucket/*"
   }
  ]
 }
```

バケットポリシーの例については、バケットポリシーの例 と ユースケースの例 を参照してください。

3. 特定のオブジェクトの ACL を返すには、get-object-acl AWS CLI コマンドを使用します。

```
aws s3api get-object-acl --bucket amzn-s3-demo-bucket --key EXAMPLE-OBJECT-KEY
```

4. 必要に応じて、オブジェクト ACL アクセス権限をバケットポリシーに移行します。

   このリソースエレメントの例では、バケットポリシーの特定のオブジェクトへのアクセスを付与します。

```
"Resource": "arn:aws:s3:::amzn-s3-demo-bucket/EXAMPLE-OBJECT-KEY"
```

5. バケットの ACL をデフォルトの ACL にリセットします。

```
aws s3api put-bucket-acl --bucket amzn-s3-demo-bucket --acl private
```

6. オブジェクト所有者に[バケット所有者の強制] 設定を適用します。

承認に ACL を必要としたリクエストを特定する

承認に ACL を必要とした Amazon S3 リクエストを特定するには、Amazon S3 サーバーアクセスログまたは AWS CloudTrail の `aclRequired` 値を使用します。リクエストが承認に ACL を必要としたか、ACL を指定する PUT リクエストがある場合、文字列は `Yes` です。ACL が不要であったか、`bucket-owner-full-control` の既定 ACL を設定するか、リクエストがバケットポリシーで許可されている場合、`aclRequired` 値の文字列は Amazon S3 サーバーアクセスログでは「`-`」となり、CloudTrail では存在しません。期待される `aclRequired` 値の詳細については、「一般的な Amazon S3 リクエストの `aclRequired` 値」を参照してください。

`PutBucketAcl` または `PutObjectAcl` リクエストに ACL ベースのアクセス許可を付与するヘッダーが含まれている場合は、`bucket-owner-full-control` 既定 ACL を除き、ACL を無効にする前にこれらのヘッダーを削除する必要があります。待機しないと、リクエストは失敗します。

承認に ACL を必要としたその他すべてのリクエストについては、これらの ACL アクセス許可をバケットポリシーに移行します。次に、バケット所有者の強制設定を有効にする前に、バケットの ACL をすべて削除します。

> **Note**
>
> オブジェクトの ACL は削除しないでください。削除すると、アクセス許可をオブジェクトの ACL に依存しているアプリケーションはアクセスできなくなります。

承認に ACL を必要としたリクエストがない場合は、ACL の無効化に進むことができます。リクエストの識別方法の詳細については、「Amazon S3 アクセスログを使用したリクエストの識別」と「CloudTrail を使用した Amazon S3 リクエストの識別」を参照してください。

ACL 関連の条件キーを使用するバケットポリシーを確認および更新します。

[バケット所有者の強制] 設定を適用して ACL を無効にすると、リクエストでバケット所有者の完全制御 ACL が使用されているか、ACL が指定されていない場合にのみ、新しいオブジェクトをバケットにアップロードできます。ACL を無効にする前に、ACL 関連の条件キーのバケットポリシーを確認します。

バケットポリシーが ACL 関連の条件キーを使用して、bucket-owner-full-control 既定 ACL (例えば、s3:x-amz-acl) では、バケットポリシーを更新する必要はありません。次のバケットポリシーでは、s3:x-amz-acl S3 の規定 ACL bucket-owner-full-control リクエストを必要とする PutObject を使用します。このポリシーでは、引き続きオブジェクトライターが bucket-owner-full-control 既定 ACL を指定する必要があります。ただし、ACL が無効になっているバケットは引き続きこの ACL を受け入れるため、クライアント側の変更は不要で、リクエストは引き続き成功します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Only allow writes to my bucket with bucket owner full control",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:user/ExampleUser"
                ]
            },
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control"
                }
            }
        }
    ]
}
```

ただし、バケットポリシーで異なる ACL を必要とする ACL 関連の条件キーを使用する場合は、この条件キーを削除する必要があります。この例のバケットポリシーには、 S3 の public-read ACL を PutObject リクエストして、ACL が無効になる前に更新する必要があります。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Only allow writes to my bucket with public read access",
```

```
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:user/ExampleUser"                ]
            },
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "public-read"
                }
            }
        }
    ]
}
```

ユースケースの例

以下の例では、特定のユースケースでの ACL アクセス権限をバケットポリシーに移行する方法を示します。

トピック

- サーバーアクセスのログ記録用の S3 ログ配信グループへのアクセスを付与する
- バケット内のオブジェクトへのパブリック読み取りアクセスを付与します
- S3 バケットへのアクセス権を Amazon ElastiCache (Redis OSS) に付与する

サーバーアクセスのログ記録用の S3 ログ配信グループへのアクセスを付与する

バケット所有者の強制設定を適用してサーバーアクセスログ送信先バケット (別名 ターゲットバケット) の ACL を無効にするには、バケットの S3 ログ配信グループへの ACL アクセス許可をバケットポリシーのログ記録サービスプリンシパル (`logging.s3.amazonaws.com`) に移行する必要があります。ログ配信許可の詳細については、ログ配信許可 を参照してください。

このバケット ACL は、S3 ログ配信グループへの `WRITE` と `READ_ACP` アクセスを許可します。

```
{
    "Owner": {
        "DisplayName": "DOC-EXAMPLE-ACCOUNT-OWNER",
        "ID": "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID"
```

```
    },
    "Grants": [
        {
            "Grantee": {
                "Type": "CanonicalUser",
                "DisplayName": "DOC-EXAMPLE-ACCOUNT-OWNER",
                "ID":
 "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID"
            },
            "Permission": "FULL_CONTROL"
        },
        {
            "Grantee": {
                "Type": "Group",
                "URI": "http://acs.amazonaws.com/groups/s3/LogDelivery"
            },
            "Permission": "WRITE"
        },
        {
            "Grantee": {
                "Type": "Group",
                "URI": "http://acs.amazonaws.com/groups/s3/LogDelivery"
            },
            "Permission": "READ_ACP"
        }
    ]
}
```

S3 ログ配信グループのバケット ACL アクセス権限を、バケットポリシーのロギングサービスプリンシパルに移行します。

1. 次のバケットポリシーをバケットに追加して、例の値を置き換えます。

```
aws s3api put-bucket-policy --bucket amzn-s3-demo-bucket --policy file://
policy.json

policy.json:      {
    {
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3ServerAccessLogsPolicy",
            "Effect": "Allow",
```

```
            "Principal": {
                "Service": "logging.s3.amazonaws.com"
            },
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/EXAMPLE-LOGGING-PREFIX*",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:s3:::SOURCE-BUCKET-NAME"
                },
                "StringEquals": {
                    "aws:SourceAccount": "SOURCE-AWS-ACCOUNT-ID"
                }
            }
        }
    ]
}
```

2. バケットの ACL をデフォルトの ACL にリセットします。

```
aws s3api put-bucket-acl --bucket amzn-s3-demo-bucket --acl private
```

3. オブジェクト所有権のバケット所有者の強制 を送信先バケットに適用します。

バケット内のオブジェクトへのパブリック読み取りアクセスを付与します

オブジェクト ACL がバケット内のすべてのオブジェクトへのパブリック読み取りアクセスを許可する場合、これらの ACL アクセス権限をバケットポリシーに移行できます。

このオブジェクト ACL は、バケット内のオブジェクトへのパブリック読み取りアクセスを許可します。

```
{
    "Owner": {
        "DisplayName": "DOC-EXAMPLE-ACCOUNT-OWNER",
        "ID": "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID"
    },
    "Grants": [
        {
            "Grantee": {
                "DisplayName": "DOC-EXAMPLE-ACCOUNT-OWNER",
```

```
                "ID":
 "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID",
                "Type": "CanonicalUser"
            },
            "Permission": "FULL_CONTROL"
        },
        {
            "Grantee": {
                "Type": "Group",
                "URI": "http://acs.amazonaws.com/groups/global/AllUsers"
            },
            "Permission": "READ"
        }
    ]
}
```

パブリック読み取り ACL アクセス権限をバケットポリシーに移行します。

1. バケット内のすべてのオブジェクトへのパブリック読み取りアクセスを許可するには、例の値を置き換えて、次のバケットポリシーを追加します。

```
aws s3api put-bucket-policy --bucket amzn-s3-demo-bucket --policy
 file://policy.json

policy.json:
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PublicReadGetObject",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        }
    ]
}
```

バケットポリシー内の特定のオブジェクトへのパブリックアクセスを許可するには、Resource エレメントに次の形式を使用します。

```
"Resource": "arn:aws:s3:::amzn-s3-demo-bucket/OBJECT-KEY"
```

特定のプレフィックスを持つすべてのオブジェクトへのパブリックアクセスを許可するには、Resource エレメントに次の形式を使用します。

```
"Resource": "arn:aws:s3:::amzn-s3-demo-bucket/PREFIX/*"
```

2. オブジェクト所有者に[バケット所有者の強制] 設定を適用します。

S3 バケットへのアクセス権を Amazon ElastiCache (Redis OSS) に付与する

S3 バケットに ElastiCache (Redis OSS) のバックアップをエクスポートできます。これにより、ElastiCache の外部からバックアップにアクセスできます。バックアップを S3 バケットにエクスポートするには、スナップショットをバケットにコピーするための ElastiCache 許可を付与する必要があります。バケット ACL で ElastiCache にアクセス許可を付与した場合は、[バケット所有者の強制] 設定を適用して ACL を無効にする前に、これらの許可をバケットポリシーに移行する必要があります。詳細については、Amazon ElastiCache ユーザーガイド の Amazon S3 バケットへの ElastiCache アクセスの許可 を参照してください。

次の例は、ElastiCache に許可を付与するバケット ACL アクセス許可を示しています。

```
{
    "Owner": {
        "DisplayName": "DOC-EXAMPLE-ACCOUNT-OWNER",
        "ID": "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID"
    },
    "Grants": [
        {
            "Grantee": {
                "DisplayName": "DOC-EXAMPLE-ACCOUNT-OWNER",
                "ID":
 "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID",
                "Type": "CanonicalUser"
            },
            "Permission": "FULL_CONTROL"
        },
        {
```

```
            "Grantee": {
                "DisplayName": "aws-scs-s3-readonly",
                "ID":
 "540804c33a284a299d2547575ce1010f2312ef3da9b3a053c8bc45bf233e4353",
                "Type": "CanonicalUser"
            },
            "Permission": "READ"
        },
        {
            "Grantee": {
                "DisplayName": "aws-scs-s3-readonly",
                "ID":
 "540804c33a284a299d2547575ce1010f2312ef3da9b3a053c8bc45bf233e4353",
                "Type": "CanonicalUser"
            },
            "Permission": "WRITE"
        },
        {
            "Grantee": {
                "DisplayName": "aws-scs-s3-readonly",
                "ID":
 "540804c33a284a299d2547575ce1010f2312ef3da9b3a053c8bc45bf233e4353",
                "Type": "CanonicalUser"
            },
            "Permission": "READ_ACP"
        }
    ]
}
```

ElastiCache (Redis OSS) のバケット ACL アクセス許可をバケットポリシーに移行するには

1. 次のバケットポリシーをバケットに追加し、例の値を置き換えます。

```
aws s3api put-bucket-policy --bucket amzn-s3-demo-bucket --policy
 file://policy.json

policy.json:
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt15399483",
            "Effect": "Allow",
```

```
            "Principal": {
                "Service": "Region.elasticache-snapshot.amazonaws.com"
            },
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketAcl",
                "s3:ListMultipartUploadParts",
                "s3:ListBucketMultipartUploads"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        }
    ]
}
```

2. バケットの ACL をデフォルトの ACL にリセットします。

```
aws s3api put-bucket-acl --bucket amzn-s3-demo-bucket --acl private
```

3. オブジェクト所有者に[バケット所有者の強制] 設定を適用します。

バケットの作成時のオブジェクトの所有権の設定。

バケットを作成するときに、S3 オブジェクトの所有権を設定できます。既存のバケットのオブジェクトの所有権を設定するには、既存のバケットでのオブジェクトの所有権の設定 を参照してください。

S3 オブジェクトの所有権は、アクセスコントロールリスト (ACL) を無効化するために使用できる Amazon S3 バケットレベルの設定で、バケット内のすべてのオブジェクトの所有権を取得し、Amazon S3 に保存されているデータのアクセス管理を簡素化します。デフォルトでは、オブジェクト所有者はバケット所有者の強制設定に設定され、新しいバケットの ACL が無効になります。ACL を無効にすると、バケット所有者はバケット内のすべてのオブジェクトを所有し、アクセス管理ポリシーのみを使用してデータへのアクセスを管理します。オブジェクトごとに個別に制御する必要がある通常ではない状況を除き、ACL は無効にしておくことをお勧めします。

オブジェクト所有権には、バケットにアップロードされるオブジェクトの所有権を制御し、ACL を無効または有効化するために使用できる 3 つの設定があります。

ACL の無効化

- バケット所有者の強制 (デフォルト) – ACL は無効になり、バケット所有者はバケット内のすべてのオブジェクトを自動的に所有し、完全に制御します。ACL は、S3 バケット内のデータに対するアクセス許可に対して影響を与えません。バケットは、ポリシーを使用してアクセスコントロールを定義します。

ACL の有効化。

- 希望するバケット所有者 — バケット所有者は、他のアカウントが `bucket-owner-full-control` 既定 ACL でバケットに書き込む新しいオブジェクトを所有し、完全にコントロールできます。
- オブジェクトライター — オブジェクトをアップロードする AWS アカウント は、そのオブジェクトを所有し、そのオブジェクトを完全にコントロールし、ACL を介して他のユーザーにそのオブジェクトへのアクセス権を付与できます。

アクセス許可: [Bucket owner enforced] (バケット所有者の強制) 設定、または [Bucket owner preferred] (バケット所有者の優先) 設定を適用するには、`s3:CreateBucket` および `s3:PutBucketOwnershipControls` のアクセス許可が必要です。オブジェクトライター設定が適用されたバケットを作成する場合、追加の権限は必要ありません。詳細については、「サービス認可リファレンス」の「Actions, resources, and condition keys for Amazon S3」を参照してください。

S3 リソースタイプ別の S3 API オペレーションへのアクセス許可の詳細については、「Amazon S3 API オペレーションに必要なアクセス許可」を参照してください。

> **Important**
>
> Amazon S3 の最新のユースケースの大部分では ACL を使用する必要がなくなり、オブジェクトごとに個別にアクセスを制御する必要がある異常な状況を除き、ACL を無効にすることをお勧めします。オブジェクトの所有権を使用すると ACL を無効にして、アクセスコントロールに関するポリシーに依存できます。ACL を無効にすると、別の AWS アカウントによってアップロードされたオブジェクトを含むバケットを簡単に維持できます。バケット所有者は、バケット内のすべてのオブジェクトを所有し、ポリシーを使用してオブジェクトへのアクセスを管理できます。

S3 コンソールの使用

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. ページ上部にあるナビゲーションバーで、現在表示されている AWS リージョン の名前をクリックします。次に、バケットを作成するリージョンを選択します。

   > **Note**
   >
   > - 一旦バケットを作成したら、そのリージョンを変更することはできません。
   > - レイテンシーとコストを最小化するため、さらに規制条件に対応するために、最寄りのリージョンを選択します。明示的に別のリージョンに移動する場合を除き、特定のリージョンに保管されたオブジェクトは、そのリージョンから移動されることはありません。Amazon S3 AWS リージョン のリストについては、「Amazon Web Services 全般のリファレンス」の「AWS のサービス エンドポイント」を参照してください。

3. 左のナビゲーションペインで、[汎用バケット] を選択します。
4. [Create bucket (バケットの作成)] を選択します。[バケットの作成] ページが開きます。
5. [バケット名] にバケットの名前を入力します。

   バケット名には次の条件があります。

   - パーティション内で一意にする必要があります。パーティションは、リージョンのグループです。AWS には、現在 aws (商用リージョン)、aws-cn (中国リージョン)、および aws-us-gov (AWS GovCloud (US) Regions) の 3 つのパーティションがあります。
   - 3 ~ 63 文字で指定する。
   - 小文字、数字、ピリオド (.)、ハイフン (-) のみで構成されます。互換性を最も高くするには、静的ウェブサイトホスティング専用のバケットを除き、バケット名にピリオド (.) を使用しないことをお勧めします。
   - 文字や数字で始まり、文字や数字で終わります。
   - バケットの命名規則の完全なリストについては、「汎用バケットの命名規則」を参照してください。

> **Important**
>
> - バケットを作成したら、その名前を変更することはできません。
> - バケット名に機密情報を含めないでください。バケット名は、バケット内のオブジェクトを参照する URL に表示されます。

6. (オプション) [全般設定] で、既存のバケットの設定を新しいバケットにコピーすることを選択できます。既存のバケットの設定をコピーしない場合は、次のステップにスキップします。

> **Note**
>
> このオプションの特徴:
>
> - AWS CLI では使用できません。Amazon S3 コンソールでのみ利用できます。
> - バケットポリシーは既存のバケットから新しいバケットにコピーしません。

既存のバケットの設定をコピーするには、[既存のバケットから設定をコピー] で [バケットを選択] をクリックします。[バケットを選択] ウィンドウが開きます。コピーする設定を持つバケットを検索して、[バケットを選択] をクリックします。[バケットを選択] ウィンドウが閉じて、[バケットを作成] ウィンドウが再び開きます。

[既存のバケットから設定をコピー] に、選択したバケットの名前が表示されるようになります。新しいバケットの設定が、選択したバケットの設定と一致するようになりました。コピーした設定を削除する場合は、[デフォルトを復元] を選択します。[バケットを作成] ページで、バケットの残りの設定を確認します。変更しない場合は、最後のステップに進みます。

7. [オブジェクト所有者] で、ACL を無効または有効にし、バケットにアップロードされたオブジェクトの所有権を制御するには、次のいずれかの設定を選択します。

ACL は無効です

- バケット所有者の強制 (デフォルト) – ACL は無効になり、バケット所有者は汎用バケット内のすべてのオブジェクトを自動的に所有し、完全に制御します。ACL は、S3 汎用バケット内のデータへのアクセス許可に影響を与えなくなりました。このバケットはアクセスコントロールを定義するためだけにポリシーを使用します。

デフォルトでは、ACL は無効になっています。Amazon S3 の最新のユースケースの大部分では ACL を使用する必要がなくなっています。オブジェクトごとに個別に制御する必要がある通常ではない状況を除き、ACL は無効にしておくことをお勧めします。詳細については、「オブジェクトの所有権の制御とバケットの ACL の無効化。」を参照してください。

ACL の有効化

- 希望するバケット所有者 — バケット所有者は、他のアカウントが `bucket-owner-full-control` 既定 ACL でバケットに書き込む新しいオブジェクトを所有し、完全にコントロールできます。

  [バケット所有者を推奨] 設定を適用して、すべての Amazon S3 アップロードに `bucket-owner-full-control` 既定 ACL を含めることを要求する場合は、この ACL を使用するオブジェクトアップロードのみを許可するバケットポリシーを追加できます。
- オブジェクトライター — オブジェクトをアップロードする AWS アカウント は、そのオブジェクトを所有し、そのオブジェクトを完全にコントロールし、ACL を介して他のユーザーにそのオブジェクトへのアクセス権を付与できます。

> **Note**
>
> デフォルト設定は [バケット所有者の強制] です。デフォルト設定を適用して ACL を無効のままにするのに必要なのは、`s3:CreateBucket` アクセス許可のみです。ACL を有効にするためには、`s3:PutBucketOwnershipControls` アクセス許可が必要です。

8. [このバケットのパブリックアクセスブロック設定] で、バケットに適用するブロックパブリックアクセス設定を選択します。

   デフォルトでは、4 つすべての [パブリックアクセスをブロック] 設定が有効になっています。特定のユースケースでオフにする必要のある設定が 1 つ以上あることがわかっている場合を除き、すべての設定を有効にしておくことをお勧めします。ブロックパブリックアクセスの詳細については、Amazon S3 ストレージへのパブリックアクセスのブロック を参照してください。

> **Note**
>
> すべての [パブリックアクセスをブロック] 設定を有効にするのに必要なのは、`s3:CreateBucket` アクセス許可のみです。[パブリックアクセスをブロック] 設定をオフにするには、`s3:PutBucketPublicAccessBlock` アクセス許可が必要です。

9. (オプション) [バケットのバージョニング] は、デフォルトで無効になります。バージョニングとは、同じバケット内でオブジェクトの複数のバリアントを保持する手段です。バージョニングを使用して、 バケットに保存されたあらゆるオブジェクトのあらゆるバージョンを保存、取得、復元することができます。バージョニングを使用すれば、意図しないユーザーアクションからもアプリケーション障害からも、より簡単に復旧できます。バージョニングの詳細については、「S3 バージョニングによる複数のバージョンのオブジェクトの保持」を参照してください。

   バケットでバージョニングを有効にするには、[有効化] を選択します。

10. (オプション) [Tags] (タグ) では、バケットにタグを追加することを選択できます。AWS コスト配分では、バケットタグを使用してバケットの使用に対する請求に注釈を付けることができます。タグはキー/値ペアになっており、バケットに割り当てられるラベルを表します。詳細については、「the section called “コスト配分タグの使用”」を参照してください。

    (オプション) タグを追加するには、[キー] を入力してから、オプションの [値] を入力し、[タグの追加] を選択します。

11. [デフォルトの暗号化] を設定するには、[暗号化タイプ] で次のいずれかを選択します。

    - Amazon S3 マネージドキーを用いたサーバー側の暗号化 (SSE-S3)
    - AWS Key Management Service キーによるサーバー側の暗号化 (SSE-KMS)
    - AWS Key Management Service (AWS KMS) キーによる二層式サーバー側の暗号化 (DSSE-KMS)

    > **Important**
    >
    > デフォルト暗号化設定として SSE-KMS または DSSE-KMS オプションを使用する場合、AWS KMS の 1 秒あたりのリクエスト数 (RPS) 制限が適用されます。AWS KMS クォータの詳細およびクォータの引き上げをリクエストする方法については、「AWS Key Management Service デベロッパーガイド」の「クォータ」を参照してください。

バケットと新しいオブジェクトは、暗号化設定の基本レベルとして Amazon S3 マネージドキー (SSE-S3) を使用したサーバー側の暗号化で暗号化されます。デフォルトの暗号化の詳細については、「Amazon S3 バケット向けのサーバー側のデフォルトの暗号化動作の設定」を参照してください。SSE-KMS に関する詳細は、「Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3)」を参照してください。

サーバー側の暗号化を使用してデータを暗号化する方法の詳細については、「the section called "データ暗号化"」を参照してください。

12. Amazon S3 が管理するキー (SSE-S3) によるサーバー側の暗号化または AWS Key Management Service (AWS KMS) キーによる二層式サーバー側の暗号化 (DSSE-KMS) を選択した場合は、次の操作を行います。

    a. [AWS KMS キー] で、次のいずれかの方法で KMS キーを指定します。

    - 使用可能な KMS キーのリストから選択するには、[AWS KMS keys から選択する] を選択し、使用可能なキーのリストから自分の KMS キーを選択します。

      AWS マネージドキー (aws/s3) とカスタマーマネージドキーの両方がこのリストに表示されます。カスタマーマネージドキーの詳細については、AWS Key Management Service デベロッパーガイドの「カスタマーキーと AWS キー」を参照してください。
    - KMS キー ARN を入力するには、[AWS KMS key ARN を入力] を選択し、表示されるフィールドに KMS キー ARN を入力します。
    - AWS KMS コンソールで新しいカスタマーマネージドキーを作成するには、[KMS キーを作成] を選択します。

      AWS KMS key の作成の詳細については、「AWS Key Management Service デベロッパーガイド」の「キーの作成」を参照してください。

> **Important**
>
> バケットと同じ AWS リージョン で使用可能な KMS キーのみを使用できます。Amazon S3 コンソールには、バケットと同じリージョンで最初の 100 個の KMS キーしか表示されません。リストに存在しない KMS キーを使用するには、KMS キー ARN を入力する必要があります。別のアカウントが所有している KMS キーを使用する場合は、まず、そのキーを使用するアクセス許可が必要であり、次に、KMS キー ARN を入力する必要があります。KMS キーのクロスアカウ

ント権限の詳細については、「AWS Key Management Service デベロッパーガイド」の「他のアカウントで使用できる KMS キーを作成する」を参照してください。SSE-KMS に関する詳細は、「AWS KMS (SSE-KMS) によるサーバー側の暗号化の指定」を参照してください。DSSE-KMS に関する詳細については、「the section called "二層式サーバー側の暗号化 (DSSE-KMS) "」を参照してください。Amazon S3 でサーバー側の暗号化に AWS KMS key を使用する場合は、対称暗号化 KMS キーを選択する必要があります。Amazon S3 では、対称暗号化 KMS キーのみがサポートされ、非対称暗号化 KMS キーはサポートされません。詳細については、AWS Key Management Service デベロッパーガイドの「Identifying symmetric and asymmetric KMS keys」(対称および非対称 KMS キーの識別) を参照してください。

b. SSE-KMS でデフォルトの暗号化を使用するようにバケットを設定する場合は、S3 バケットキーを使用することもできます。S3 バケットキーは、Amazon S3 から AWS KMS へのリクエストトラフィックを減らし、暗号化のコストを削減します。詳細については、「Amazon S3 バケットキーを使用した SSE-KMS のコストの削減」を参照してください。S3 バケットキーは DSSE-KMS ではサポートされていません。

   デフォルトでは、S3 バケットキーは Amazon S3 コンソールで有効になっています。コストを削減するには、S3 バケットキーを有効にしておくことをお勧めします。バケットの S3 バケットキーを無効にするには、[バケットキー] で、[無効化] を選択します。

13. (オプション) S3 Object Lock は、新しいオブジェクトが削除または上書きされないように保護するのに役立ちます。詳細については、「S3 Object Lock を使用したオブジェクトのロック」を参照してください。S3 Object Lock を有効にする場合は、次の手順に従います。

    a. [詳細設定] を選択します。

    > **Important**
    >
    > バケットに対して Object Lock を有効にすると、自動でバージョニングも有効になります。バケットを有効にして正常に作成したら、バケットの [プロパティ] タブで Object Lock のデフォルトの保持とリーガルホールドの設定も設定する必要があります。

    b. オブジェクトロックを有効にする場合は、[Enable] (有効化) を選択し、表示される警告を読んだうえで承認します。

> **Note**
>
> Object Lock が有効なバケットを作成するには、s3:CreateBucket、s3:PutBucketVersioning および s3:PutBucketObjectLockConfiguration の許可が必要です。

14. [バケットを作成] を選択します。

AWS CLI を使用する場合

新しいバケットを作成するときにオブジェクトの所有権を設定するには、create-bucket パラメータを指定して AWS CLI と --object-ownership コマンドを使用します。

この例では、AWS CLI を使用して新しいバケットに [バケット所有者の強制] 設定を適用します。

```
aws s3api create-bucket --bucket  amzn-s3-demo-bucket --region us-east-1 --object-
ownership BucketOwnerEnforced
```

> **Important**
>
> AWS CLI を使用してバケットを作成するときにオブジェクト所有権を設定しない場合、デフォルト設定は ObjectWriter (ACL 有効) になります。

AWS SDK for Java の使用

この例では、AWS SDK for Java を使用して新しいバケットの [バケット所有者の強制] 設定を設定します。

```
    // Build the ObjectOwnership for CreateBucket
    CreateBucketRequest createBucketRequest = CreateBucketRequest.builder()
            .bucket(bucketName)
            .objectOwnership(ObjectOwnership.BucketOwnerEnforced)
            .build()

     // Send the request to Amazon S3
     s3client.createBucket(createBucketRequest);
```

AWS CloudFormation の使用

新しいバケットを作成するときに `AWS::S3::Bucket` と AWS CloudFormation リソースを使用してオブジェクトの所有権を設定するには、「AWS CloudFormation ユーザーガイド」の「AWS::S3::Bucket の OwnershipControls」を参照してください。

REST API の使用

S3 オブジェクト所有権に [バケット所有者の強制] 設定を適用するには、`x-amz-object-ownership` リクエストヘッダーを `BucketOwnerEnforced` に設定して `CreateBucket` API オペレーションを使用します。詳細と例については、「Amazon Simple Storage Service API リファレンス」の「CreateBucket」を参照してください。

次のステップ: オブジェクトの所有権にバケット所有者の強制設定またはバケット所有者の優先設定を適用した後、さらに次の手順を実行できます。

- バケット所有者の強制 – IAM または組織ポリシーを使用して、ACL を無効にしてすべての新しいバケットを作成する必要があります。
- バケット所有者推奨 – S3 バケットポリシーを追加して、バケットへのすべてのオブジェクトのアップロードに `bucket-owner-full-control` 規定 ACL を要求します

既存のバケットでのオブジェクトの所有権の設定

既存の S3 バケットで S3 オブジェクトの所有権を設定できます。バケットを作成するときにオブジェクトの所有権を適用するには、バケットの作成時のオブジェクトの所有権の設定。 を参照してください。

S3 オブジェクトの所有権は、アクセスコントロールリスト (ACL) を無効化するために使用できる Amazon S3 バケットレベルの設定で、バケット内のすべてのオブジェクトの所有権を取得し、Amazon S3 に保存されているデータのアクセス管理を簡素化します。デフォルトでは、オブジェクト所有者はバケット所有者の強制設定に設定され、新しいバケットの ACL が無効になります。ACL を無効にすると、バケット所有者はバケット内のすべてのオブジェクトを所有し、アクセス管理ポリシーのみを使用してデータへのアクセスを管理します。オブジェクトごとに個別に制御する必要がある通常ではない状況を除き、ACL は無効にしておくことをお勧めします。

オブジェクト所有権には、バケットにアップロードされるオブジェクトの所有権を制御し、ACL を無効または有効化するために使用できる 3 つの設定があります。

ACL の無効化

- バケット所有者の強制 (デフォルト) – ACL は無効になり、バケット所有者はバケット内のすべてのオブジェクトを自動的に所有し、完全に制御します。ACL は、S3 バケット内のデータに対するアクセス許可に対して影響を与えません。バケットは、ポリシーを使用してアクセスコントロールを定義します。

ACL の有効化。

- 希望するバケット所有者 — バケット所有者は、他のアカウントが `bucket-owner-full-control` 既定 ACL でバケットに書き込む新しいオブジェクトを所有し、完全にコントロールできます。
- オブジェクトライター — オブジェクトをアップロードする AWS アカウント は、そのオブジェクトを所有し、そのオブジェクトを完全にコントロールし、ACL を介して他のユーザーにそのオブジェクトへのアクセス権を付与できます。

前提条件: [バケット所有者の強制] 設定を適用して ACL を無効にする前に、バケット ACL アクセス権限をバケットポリシーに移行し、バケット ACL をデフォルトのプライベート ACL にリセットする必要があります。また、オブジェクト ACL アクセス権限をバケットポリシーに移行し、バケット所有者の完全制御 ACL 以外の ACL を必要とするバケットポリシーを編集することをお勧めします。詳細については、ACL を無効にする前提条件。 を参照してください。

許可: このオペレーションを使用するには、`s3:PutBucketOwnershipControls` 許可が必要です。詳細については、「サービス認可リファレンス」の「Actions, resources, and condition keys for Amazon S3」を参照してください。

S3 リソースタイプ別の S3 API オペレーションへのアクセス許可の詳細については、「Amazon S3 API オペレーションに必要なアクセス許可」を参照してください。

S3 コンソールの使用

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. バケット リストで、S3 オブジェクトの所有者の設定を適用するバケットの名前を選択します。
3. [アクセス許可] タブを選択します。
4. オブジェクトの所有者で [編集] を選択します。

5. オブジェクト所有権は、ACL を無効または有効にして、バケットにアップロードされたオブジェクトの所有権を制御するために、次の設定のいずれか一つを選択します。

   ACL は無効です

   - バケット所有者の強制 - ACL は無効になり、バケット所有者はバケット内のすべてのオブジェクトを自動的に所有し、完全にコントロールできます。ACL は、S3 バケット内のデータに対するアクセス許可に対して影響を与えません。このバケットはアクセスコントロールを定義するためにポリシーを使用します。

     IAM または AWS Organizations ポリシーを使用し、ACL を無効にしてすべての新しいバケットを作成することを要求するには、すべての新しいバケットの ACL を無効にします (バケット所有者の強制) を参照してください。

   ACL の有効化

   - 希望するバケット所有者 — バケット所有者は、他のアカウントが `bucket-owner-full-control` 既定 ACL でバケットに書き込む新しいオブジェクトを所有し、完全にコントロールできます。

     バケット所有者の優先設定を適用して、すべての Amazon S3 アップロードに `bucket-owner-full-control` 既定 ACL を含めることを要求する場合は、この ACL を使用するオブジェクトアップロードのみを許可するバケットポリシーを追加できます。
   - オブジェクトライター (デフォルト) – オブジェクトをアップロードする AWS アカウントは、オブジェクトを所有し、オブジェクトを完全に制御し、ACL を介して他のユーザーにオブジェクトへのアクセスを許可できます。
6. [保存] を選択します。

AWS CLI を使用する場合

既存のバケットにオブジェクトの所有権設定を適用するには、`put-bucket-ownership-controls` パラメータのある `--ownership-controls` コマンドを使用します。所有権の有効な値は `BucketOwnerEnforced`、`BucketOwnerPreferred`、または `ObjectWriter` です。

この例では、AWS CLI を使用して既存のバケットにバケット所有者の強制設定を適用します。

```
aws s3api put-bucket-ownership-controls --bucket amzn-s3-demo-bucket --ownership-controls="Rules=[{ObjectOwnership=BucketOwnerEnforced}]"
```

put-bucket-ownership-controls の詳細については、「AWS Command Line Interface ユーザーガイド」の「put-bucket-ownership-controls」を参照してください。

AWS SDK for Java の使用

この例では、BucketOwnerEnforced を使用して既存のバケットに対してオブジェクト所有権の AWS SDK for Java 設定を適用します。

```
        // Build the ObjectOwnership for BucketOwnerEnforced
        OwnershipControlsRule rule = OwnershipControlsRule.builder()
               .objectOwnership(ObjectOwnership.BucketOwnerEnforced)
               .build();

        OwnershipControls ownershipControls = OwnershipControls.builder()
                  .rules(rule)
                  .build()

         // Build the PutBucketOwnershipControlsRequest
         PutBucketOwnershipControlsRequest putBucketOwnershipControlsRequest =
               PutBucketOwnershipControlsRequest.builder()
                       .bucket(BUCKET_NAME)
                       .ownershipControls(ownershipControls)
                       .build();

         // Send the request to Amazon S3
         s3client.putBucketOwnershipControls(putBucketOwnershipControlsRequest);
```

AWS CloudFormation の使用

既存のバケットにオブジェクト所有者の設定を適用するために AWS CloudFormation を使用するには、「AWS CloudFormation ユーザーガイド」の「AWS::S3::Bucket OwnershipControls」を参照してください。

REST API の使用

REST API を使用して既存の S3 バケットにオブジェクトの所有権設定を適用するには、PutBucketOwnershipControls を使用します。詳細については、「Amazon Simple Storage Service API リファレンス」の「PutBucketOwnershipControls」を参照してください。

次のステップ: オブジェクトの所有権にバケット所有者の強制設定またはバケット所有者の優先設定を適用した後、さらに次の手順を実行できます。

- バケット所有者の強制 – IAM または組織ポリシーを使用して、ACL を無効にしてすべての新しいバケットを作成する必要があります。
- バケット所有者推奨 – S3 バケットポリシーを追加して、バケットへのすべてのオブジェクトのアップロードに bucket-owner-full-control 規定 ACL を要求します

S3 バケットのオブジェクト所有権設定の表示

S3 オブジェクトの所有権は、アクセスコントロールリスト (ACL) を無効化するために使用できる Amazon S3 バケットレベルの設定で、バケット内のすべてのオブジェクトの所有権を取得し、Amazon S3 に保存されているデータのアクセス管理を簡素化します。デフォルトでは、オブジェクト所有者はバケット所有者の強制設定に設定され、新しいバケットの ACL が無効になります。ACL を無効にすると、バケット所有者はバケット内のすべてのオブジェクトを所有し、アクセス管理ポリシーのみを使用してデータへのアクセスを管理します。オブジェクトごとに個別に制御する必要がある通常ではない状況を除き、ACL は無効にしておくことをお勧めします。

オブジェクト所有権には、バケットにアップロードされるオブジェクトの所有権を制御し、ACL を無効または有効化するために使用できる 3 つの設定があります。

ACL の無効化

- バケット所有者の強制 (デフォルト) – ACL は無効になり、バケット所有者はバケット内のすべてのオブジェクトを自動的に所有し、完全に制御します。ACL は、S3 バケット内のデータに対するアクセス許可に対して影響を与えません。バケットは、ポリシーを使用してアクセスコントロールを定義します。

ACL の有効化。

- 希望するバケット所有者 — バケット所有者は、他のアカウントが bucket-owner-full-control 既定 ACL でバケットに書き込む新しいオブジェクトを所有し、完全にコントロールできます。
- オブジェクトライター — オブジェクトをアップロードする AWS アカウント は、そのオブジェクトを所有し、そのオブジェクトを完全にコントロールし、ACL を介して他のユーザーにそのオブジェクトへのアクセス権を付与できます。

Amazon S3 バケットの S3 オブジェクト所有権設定を表示できます。新しいバケットのオブジェクトの所有権を設定するには、バケットの作成時のオブジェクトの所有権の設定。 を参照してくださ

い。既存のバケットのオブジェクトの所有権を設定するには、既存のバケットでのオブジェクトの所有権の設定 を参照してください。

許可: このオペレーションを使用するには、s3:GetBucketOwnershipControls 許可が必要です。詳細については、「サービス認可リファレンス」の「Actions, resources, and condition keys for Amazon S3」を参照してください。

S3 リソースタイプ別の S3 API オペレーションへのアクセス許可の詳細については、「Amazon S3 API オペレーションに必要なアクセス許可」を参照してください。

S3 コンソールの使用

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. バケットリストで、オブジェクト所有権設定を適用するバケットの名前を選択します。
3. [アクセス許可] タブを選択します。
4. オブジェクトの所有権 では、バケットのオブジェクト所有権設定を表示できます。

AWS CLI を使用する場合

S3 バケットの S3 オブジェクト所有権設定を取得するには、get-bucket-ownership-controls AWS CLI コマンドを使用します。

```
aws s3api get-bucket-ownership-controls --bucket amzn-s3-demo-bucket
```

REST API の使用

S3 バケットのオブジェクトの所有権設定を検索するには、GetBucketOwnershipControls API オペレーションを使用します。詳細については、「GetBucketOwnershipControls」を参照してください。

すべての新しいバケットの ACL を無効にし、オブジェクト所有権を執行します。

Amazon S3 バケットで ACL を無効にすることをお勧めします。これを行うには、S3 オブジェクトの所有権に [バケット所有者の強制] 設定を適用します。この設定を適用すると、ACL が無効になり、バケット内のすべてのオブジェクトを自動的に所有し、完全に制御できるようになります。ACL を無効にしてすべての新しいバケットを作成するように要求するには、次のセクションで説明するよ

うに、AWS Identity and Access Management (IAM) ポリシーまたは AWS Organizations サービスコントロールポリシー (SCP) を使用します。

ACL を無効にせずに新しいオブジェクトのオブジェクト所有権を強制するには、バケット所有者の優先設定を適用できます。この設定を適用する場合は、バケットポリシーを更新して、バケットへのすべての PUT リクエストに `bucket-owner-full-control` 既定 ACL を要求することを強くお勧めします。`bucket-owner-full-control` 既定 ACL を他のアカウントのバケットに送信するように、クライアントも更新してください。

トピック

- すべての新しいバケットの ACL を無効にします (バケット所有者の強制)
- Amazon S3 PUT オペレーションで bucket-owner-full-control 既定 ACL を要求する (バケット所有者の優先)

すべての新しいバケットの ACL を無効にします (バケット所有者の強制)

次の例の IAM ポリシーは、[バケット所有者の強制] 設定がオブジェクト所有権に適用されていない限り、特定の IAM ユーザーまたはロールの `s3:CreateBucket` アクセス許可を拒否します。`Condition` ブロック内のキーバリューのペアは、キーには `s3:x-amz-object-ownership` を、値には `BucketOwnerEnforced` 設定を指定します。つまり、IAM ユーザーは、オブジェクト所有権に[バケット所有者の強制] 設定を設定し、ACL を無効にした場合にのみ、バケットを作成できます。このポリシーは、AWS 組織の境界 SCP として使用することもできます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RequireBucketOwnerFullControl",
            "Action": "s3:CreateBucket",
            "Effect": "Deny",
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-object-ownership": "BucketOwnerEnforced"
                }
            }
        }
    ]
}
```

Amazon S3 **PUT** オペレーションで bucket-owner-full-control 既定 ACL を要求する (バケット所有者の優先)

オブジェクト所有権に対するバケット所有者の優先設定を使用すると、バケット所有者は、他のアカウントが bucket-owner-full-control 既定 ACL を使用してバケットに書き込む新しいオブジェクトを所有し、完全に制御できます。ただし、他のアカウントが bucket-owner-full-control 規定 ACL なしでバケットにオブジェクトを書き込む場合、オブジェクトライターは完全制御アクセスを維持します。バケット所有者は、bucket-owner-full-control 既定 ACL を指定した場合にのみ書き込みを許可するバケットポリシーを実装できます。

> **Note**
>
> [バケット所有者の強制] 設定で ACL を無効にすると、バケット所有者として、バケット内のすべてのオブジェクトを自動的に所有し、完全に制御できます。このセクションを使用してバケットポリシーを更新して、バケット所有者にオブジェクトの所有権を適用する必要はありません。

次のバケットポリシーでは、オブジェクトの ACL が bucket-owner-full-control に設定されている場合にのみ、アカウント *111122223333* が *amzn-s3-demo-bucket* にオブジェクトをアップロードできるように指定しています。お客様のアカウントで、*111122223333* を、お客様のバケット名で*amzn-s3-demo-bucket* を置き換えてください。

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Only allow writes to my bucket with bucket owner full control",
         "Effect": "Allow",
         "Principal": {
            "AWS": [
               "arn:aws:iam::111122223333:user/ExampleUser"
            ]
         },
         "Action": [
            "s3:PutObject"
         ],
         "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
         "Condition": {
            "StringEquals": {
```

```
                "s3:x-amz-acl": "bucket-owner-full-control"
            }
        }
    }
  ]
}
```

次に、AWS Command Line Interface (AWS CLI) を使用した `bucket-owner-full-control` 既定 ACL を含むコピーオペレーションの例を示します。

```
aws s3 cp file.txt s3://amzn-s3-demo-bucket --acl bucket-owner-full-control
```

バケットポリシーが有効になった後、クライアントに `bucket-owner-full-control` 既定 ACL が含まれていない場合、オペレーションは失敗し、アップローダーは次のエラーを受け取ります。

PutObject オペレーションを呼び出すときにエラー (AccessDenied) が発生しました: アクセスが拒否されました。

> **Note**
>
> アップロード後にクライアントがオブジェクトにアクセスする必要がある場合は、アップロードアカウントに追加のアクセス権限を付与する必要があります。アカウントにリソースへのアクセス許可を付与する方法については、チュートリアル: ポリシーを使用した Amazon S3 リソースへのアクセスの管理 を参照してください。

トラブルシューティング

S3 オブジェクト所有権のバケット所有者強制設定を適用すると、アクセスコントロールリスト (ACL) が無効になり、バケット所有者として、バケット内のすべてのオブジェクトを自動的に所有することになります。ACL は、バケット内のオブジェクトの許可に影響を与えなくなりました。ポリシーを使用してアクセス許可を付与できます。すべての S3 PUT リクエストは、`bucket-owner-full-control` 既定 ACL を指定するか、ACL を指定しない必要があります。そうしないと失敗します。詳細については、「オブジェクトの所有権の制御とバケットの ACL の無効化。」を参照してください。

無効な ACL が指定されているか、バケット ACL 許可が AWS アカウント の外部へのアクセスを許可している場合、次のエラー応答が表示されることがあります。

AccessControlListNotSupported

オブジェクト所有権に [バケット所有者の強制] 設定を適用すると、ACL は無効になります。ACL の設定または ACL の更新の要求は 400 エラーで失敗し、AccessControlListNotSupported エラーコードを返します。ACL の読み取り要求は引き続きサポートされています。ACL の読み取りリクエストは、バケット所有者の完全制御を示すレスポンスを常に返します。PUT オペレーションでは、バケット所有者の完全制御 ACL を指定するか、ACL を指定しないことが必要です。それ以外の場合、PUT オペレーションは失敗します。

次の `put-object` AWS CLI コマンドの例には、`public-read` 既定 ACL が含まれています。

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key object-key-name --body doc-example-body --acl public-read
```

バケットが [バケット所有者の強制] 設定を使用して ACL を無効にする場合、このオペレーションは失敗し、アップローダーは次のエラーメッセージを受け取ります。

PutObject オペレーションの呼び出し時にエラー (AccessControlListNotSupported) が発生しました。バケットは ACL を許可していません

InvalidBucketAclWithObjectOwnership

[バケット所有者の強制] 設定を適用して ACL を無効にする場合、バケット ACL はバケット所有者にのみ完全制御を与える必要があります。バケット ACL は、外部 AWS アカウント または他のグループへのアクセスを許可できません。例えば、`CreateBucket` リクエストでバケット所有者の強制を設定し、外部 AWS アカウント へのアクセスを提供するバケット ACL を指定した場合、リクエストは 400 エラーで失敗し、InvalidBucketAclWithObjectOwnership エラーコードを返します。同様に、`PutBucketOwnershipControls` リクエストで他のユーザーにアクセス許可を付与するバケット ACL を持つバケットに対してバケット所有者の強制を設定すると、リクエストは失敗します。

Example ：既存のバケット ACL は公開読み取りアクセスを許可します

例えば、既存のバケット ACL がパブリック読み取りアクセスを許可している場合、これらの ACL アクセス許可をバケットポリシーに移行し、バケット ACL をデフォルトのプライベート ACL にリセットするまで、オブジェクト所有権に[バケット所有者の強制] 設定を適用することはできません。詳細については、ACL を無効にする前提条件。 を参照してください。

次のバケット ACL の例は、公開読み取りアクセスを許可します。

```
{
    "Owner": {
        "ID": "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID"
    },
    "Grants": [
        {
            "Grantee": {
                "ID":
 "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID",
                "Type": "CanonicalUser"
            },
            "Permission": "FULL_CONTROL"
        },
        {
            "Grantee": {
                "Type": "Group",
                "URI": "http://acs.amazonaws.com/groups/global/AllUsers"
            },
            "Permission": "READ"
        }
    ]
}
```

次の例の put-bucket-ownership-controls AWS CLI コマンドは、オブジェクト所有権にバケット所有者の強制設定を適用します。

```
aws s3api put-bucket-ownership-controls --bucket amzn-s3-demo-bucket --ownership-
controls Rules=[{ObjectOwnership=BucketOwnerEnforced}]
```

バケット ACL は公開読み取りアクセスを許可するため、リクエストは失敗し、次のエラーコードを返します。

PutBucketOwnershipControls オペレーションを呼び出すときにエラーが発生しました。(InvalidBucketAclWithObjectOwnership): バケットに ObjectOwnership の BucketOwnerEnforced 設定で ACL を設定することはできません

Amazon S3 でのセキュリティ

AWS ではクラウドのセキュリティが最優先事項です。AWS のお客様はセキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャから利点を得られます。

セキュリティはAWS とお客様の間の共有責任です。責任共有モデルでは、この責任がクラウドのセキュリティおよびクラウド内のセキュリティとして説明されています。

クラウドのセキュリティ

AWS は AWS クラウド 内で AWS サービスを実行するインフラストラクチャを保護する責任を担います。また、AWS は、ユーザーが安全に使用できるサービスも提供します。セキュリティの有効性は、AWS コンプライアンスプログラムの一環として、サードパーティーの監査機関によって定期的にテストおよび検証されています。Amazon S3 に適用されるコンプライアンスプログラムについては、AWSコンプライアンスプログラムによるターゲット範囲の のサービスを参照してください。

クラウド内のセキュリティ

お客様の責任は、お客様が使用する AWS のサービスによって決まります。お客様は、データの機密性、組織の要件、および適用法令と規制などのその他要因に対する責任も担います。Amazon S3 において、お客様は以下の事項について責任を負います。

- オブジェクトの所有権 および暗号化 を含むデータの管理。
- アセットの分類。
- IAM ロール およびその他のサービス設定を使用し、適切な権限を適用したデータへのアクセスの管理 。
- AWS CloudTrail または Amazon S3 の Amazon GuardDuty 等のディテクティブコントロールの有効化。

このドキュメントは、Amazon S3 を使用する際に適用される責任共有モデルについての理解の助けとなることを目的としています。以下のトピックでは、セキュリティとコンプライアンスの目的を満たすように Amazon S3 を設定する方法について説明します。また、Amazon S3 のリソースのモニタリングや保護に役立つ AWS の他のサービスを使用する方法についても説明します。

> **Note**
>
> Amazon S3 Express One Zone ストレージクラスをディレクトリバケットで使用する方法の詳細については、「S3 Express One Zone」と「ディレクトリバケットの使用」を参照してください。

トピック

- Amazon S3 のセキュリティのベストプラクティス
- Amazon S3 におけるデータ保護
- 暗号化によるデータの保護
- インターネットトラフィックのプライバシー
- Amazon S3 のコンプライアンス検証
- Amazon S3 の耐障害性
- Amazon S3 のインフラストラクチャセキュリティ
- Amazon S3 での設定と脆弱性の分析
- アクセス管理

Amazon S3 のセキュリティのベストプラクティス

Amazon S3 には、独自のセキュリティポリシーを策定および実装する際に考慮すべきさまざまなセキュリティ機能が用意されています。以下のベストプラクティスは一般的なガイドラインであり、完全なセキュリティソリューションを提供するものではありません。これらのベストプラクティスは顧客の環境に必ずしも適切または十分でない可能性があるので、処方箋ではなく、あくまで有用な推奨事項とお考えください。

トピック

- Amazon S3 のセキュリティベストプラクティス
- Amazon S3 のモニタリングと監査のベストプラクティス
- マネージド AWS セキュリティサービスによるデータセキュリティのモニタリング

Amazon S3 のセキュリティベストプラクティス

以下は、セキュリティ問題の防止に役立つ Amazon S3 でのベストプラクティスです。

アクセスコントロールリスト (ACL) の無効化

S3 オブジェクト所有権は、Amazon S3 バケットレベルの設定で、バケットにアップロードされたオブジェクトの所有権を制御し、ACL を無効または有効にするのに使用できます。デフォルトでは、オブジェクト所有権は[バケット所有者の強制] 設定に設定され、すべての ACL は無効になっています。ACL が無効になっている場合、バケット所有者はバケット内のすべてのオブジェクトを所有し、アクセス管理ポリシーのみを使用してデータへのアクセスを管理します。

Amazon S3 の最近のユースケースの大部分ではアクセスコントロールリスト (ACL) を使用する必要がなくなりました。オブジェクトごとに個別に制御する必要があるまれな状況を除き、ACL を無効にすることをお勧めします。バケットのすべてのオブジェクトの ACL を無効にして、所有権を取得するには、S3 オブジェクト所有権のバケット所有者の強制設定を適用します。ACL を無効にすると、別の AWS アカウント によってアップロードされたオブジェクトを含むバケットを簡単に維持できます。

ACL が無効になっている場合、データのアクセスコントロールは次のようなポリシーに基づきます。

- AWS Identity and Access Management IAM ユーザーポリシー
- S3 バケットポリシー

- 仮想プライベートクラウド (VPC) エンドポイントポリシー
- AWS Organizations サービスコントロールポリシー (SCP)
- AWS Organizations リソースコントロールポリシー (RCP)

ACL の無効化により、アクセス許可の管理と監査が簡素化されます。デフォルトでは、ACL は無効になっています。既存のバケットに対して ACL を無効にすることもできます。既存のバケットに既にオブジェクトが含まれている場合、ACL を無効にすると、オブジェクトとバケット ACL はアクセス評価プロセスの一部ではなくなります。この場合、アクセスはポリシーに基づいて許可または拒否されます。

ACL を無効にする前に、次のことを確認してください。

- バケットポリシーを確認して、アカウント外のバケットへのアクセス権を付与するすべての方法をカバーすることを確認します。
- バケット ACL をデフォルト (バケット所有者にフルコントロール) にリセットします。

ACL を無効にすると、以下の動作が発生します。

- バケットは、ACL を指定しない PUT リクエスト、またはバケット所有者のフルコントロール ACL を含む PUT リクエストのみを受け付けます。これらの ACL には、`bucket-owner-full-control` 既定 ACL または XML で表現された ACL と同等の形式が含まれます。
- バケット所有者の完全制御 ACL をサポートする既存のアプリケーションには影響はありません。
- 他の ACL (例えば、特定 AWS アカウント のへのカスタム許可) を含む PUT 要求は失敗し、`AccessControlListNotSupported` エラーコードとともに HTTPHTTP ステータスコード `400 (Bad Request)` を返します。

詳細については、「オブジェクトの所有権の制御とバケットの ACL の無効化。」を参照してください。

Amazon S3 バケットに正しいポリシーが使用され、バケットが公開されていないことを確認する

インターネット上のだれもが S3 バケットを読み書きできるように明示的にリクエストしない限り、S3 バケットが非公開であることを確認する必要があります。以下に示しているのは、パブリックアクセスをブロックするために実行できるいくつかのステップです。

- S3 パブリックアクセスのブロックを使用します。S3 パブリックアクセスブロックでは、Amazon S3 リソースへのパブリックアクセスを制限する一元管理を簡単に設定することが

できます。これらの一元管理は、リソースの作成方法に関係なく適用されます。詳細については、「Amazon S3 ストレージへのパブリックアクセスのブロック」を参照してください。

- `"Principal": "*"` (事実上「誰でも」という意味) などのワイルドカード ID を許可する Amazon S3 バケットポリシーを特定します。また、ワイルドカードアクション `"*"` (ユーザーが Amazon S3 バケットで任意のアクションを実行できるようにする) ポリシーも探します。
- 同様に、「全員」または「任意の認証済み AWS ユーザー」への読み取り、書き込み、またはフルアクセスを許可する Amazon S3 バケットのアクセスコントロールリスト (ACL) を探します。
- `ListBuckets` API オペレーションを使用して、すべての Amazon S3 バケットをスキャンします。次に、`GetBucketAcl`、`GetBucketWebsite`、`GetBucketPolicy` を使用して、各バケットがアクセスコントロールと設定がコンプライアンス要件を満たしているかどうかを判断します。
- AWS Trusted Advisor を使用して、Amazon S3 の実装を検査します。
- s3-bucket-public-read-prohibited および s3-bucket-public-write-prohibited マネージド AWS Config ルール を使用して、継続的な検出コントロールを実施することを検討します。

詳細については、「Amazon S3 用 Identity and Access Management」を参照してください。

最小特権アクセスの実装

アクセス許可を付与する場合、どのユーザーにどの Amazon S3 リソースに対するアクセス許可を付与するかは、ユーザーが決定します。つまり、該当リソースに対して許可する特定のアクションを有効にするということです。このため、タスクを実行するために必要な許可のみを付与することをお勧めします。最小限の特権アクセスの実装は、セキュリティリスクはもちろん、エラーや悪意ある行動によってもたらされる可能性のある影響を減らす上での基本となります。

以下のツールは、最小限の特権アクセスを実装するために使用できます。

- Amazon S3 のポリシーアクション および IAM エンティティのアクセス許可境界
- Amazon S3 での IAM の機能
- アクセスコントロールリスト (ACL) の概要

上記のメカニズムを採用する場合に何を考慮すべきかに関するガイダンスについては、「Amazon S3 用 Identity and Access Management 」を参照してください。

Amazon S3 アクセスを必要とするアプリケーションと AWS のサービス に IAM ロールを使用する

Amazon EC2 または他の AWS のサービス のアプリケーションが Amazon S3 リソースにアクセスするためには、AWS API リクエストに有効な AWS 認証情報が含まれている必要があります。AWS 認証情報を、アプリケーションまたは Amazon EC2 インスタンスに直接保存しないこ

とをお勧めします。これらは自動的にローテーションされない長期的な認証情報であり、漏洩するとビジネスに大きな影響が及ぶ場合があります。

代わりに、IAM ロールを使用して、Amazon S3 にアクセスする必要があるアプリケーションまたはサービスの一時的な認証情報を管理します。ロールを使用する場合は、Amazon EC2 インスタンスまたは AWS のサービス (AWS Lambda など) に長期の認証情報 (ユーザー名とパスワード、アクセスキーなど) を配布する必要はありません。ロールは、アプリケーションが他の AWS リソースの呼び出しを行うときに使用できる一時的な許可を付与します。

詳細については、IAM ユーザーガイドにある下記のトピックを参照してください。

- IAM ロール
- ロールの一般的なシナリオ: ユーザー、アプリケーション、およびサービス

保管時のデータ暗号化の検討

Amazon S3 で保管時のデータを保護するには、次のようなオプションがあります。

- サーバー側の暗号化 – すべての Amazon S3 バケットにはデフォルトで暗号化が設定されており、S3 バケットにアップロードされたすべての新しいオブジェクトは保存時に自動的に暗号化されます。Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3) は、Amazon S3 のすべてのバケットでのデフォルトの暗号化設定です。別のタイプの暗号化を使用するには、S3 PUT リクエストで使用するサーバー側の暗号化のタイプを指定するか、宛先バケットにデフォルトの暗号化設定を設定できます。

  Amazon S3 には、次のサーバー側の暗号化オプションもあります。

  - AWS Key Management Service (AWS KMS) キー (SSE-KMS) によるサーバー側の暗号化
  - AWS Key Management Service (AWS KMS) キーによる二層式サーバー側の暗号化 (DSSE-KMS)
  - 顧客提供のキーを用いたサーバー側の暗号化 (SSE-C)。

  詳細については、「サーバー側の暗号化によるデータの保護」を参照してください。
- クライアント側の暗号化 – クライアント側でデータを暗号化し、暗号化したデータを Amazon S3 にアップロードします。この場合、暗号化プロセス、暗号化キー、関連ツールはお客様が管理してください。サーバー側の暗号化と同様に、クライアント側の暗号化は、データ自体を保存するメカニズムとは異なるメカニズムで保存されているキーを使用してデータを暗号化することで、リスクを軽減するのに役立ちます。

  Amazon S3 は複数のクライアント側の暗号化オプションを提供します。詳細については、クライアント側の暗号化を使用したデータの保護 を参照してください。

送信時のデータの暗号化を強制する

HTTPS (TLS) を使用すると、潜在的な攻撃者が中間者攻撃または同様の攻撃を使用してネットワークトラフィックを盗聴または操作することを防止できます。Amazon S3 バケットのポリシーで aws:SecureTransport 条件を使用して、HTTPS (TLS) 経由での暗号化された接続のみを許可することをお勧めします。詳細については、S3 バケットポリシーの例「HTTP または HTTPS リクエストに基づくアクセス管理」を参照してください。HTTP リクエストを拒否するだけでなく、Amazon CloudWatch アラームを `tlsDetails.tlsVersion NOT EXISTS` に設定して、コンテンツに HTTP アクセスが試行された場合に警告することをお勧めします。Amazon CloudWatch アラームの設定方法の詳細については、「AWS CloudTrail User Guide」の「Creating CloudWatch alarms for CloudTrail events: examples」と「CloudTrail record contents」を参照してください。

> **Important**
>
> AWS はパブリックに信頼された証明書の固定をサポートしていないため、アプリケーションでは Amazon S3 TLS 証明書を固定しないことをお勧めします。S3 は証明書を自動的に更新し、更新は証明書の有効期限が切れる前に行われます。証明書の更新では、新しいパブリックキーとプライベートキーのペアが生成されます。新しいパブリックキーで最近更新された S3 証明書を固定する場合、アプリケーションが新しい証明書を使用するまで S3 に接続できません。

また、s3-bucket-ssl-requests-only マネージド AWS Config ルールを使用した継続的な検出コントロールの実装を検討してください。

S3 オブジェクトロックの検討

S3 オブジェクトロックでは、Write Once Read Many (WORM) モデルを使用してオブジェクトを保存できます。S3 オブジェクトロックは、データの誤った削除や不適切な削除を防ぐのに役立ちます。例えば、AWS CloudTrail ログを保護するために S3 オブジェクトロックを使用できます。

詳細については、「S3 Object Lock を使用したオブジェクトのロック」を参照してください。

S3 バージョニングの有効化

S3 バージョニングとは、同じバケット内でオブジェクトの複数のバリアントを保持する手段です。バージョニングを使用して、 バケットに保存されたあらゆるオブジェクトのあらゆるバージョンを保存、取得、復元することができます。バージョニングを使用すれば、意図しないユーザーアクションからもアプリケーション障害からも、簡単に復旧できます。

また、s3-bucket-versioning-enabled マネージド AWS Config ルールを使用した継続的な検出コントロールの実装を検討してください。

詳細については、「S3 バージョニングによる複数のバージョンのオブジェクトの保持」を参照してください。

S3 クロスリージョンレプリケーションの検討

Amazon S3 はデフォルトで地理的に異なる複数のアベイラビリティーゾーンにデータを保存しますが、コンプライアンス要件によっては、さらに離れた場所にデータを保存することが要求される場合があります。S3 クロスリージョンレプリケーション (CRR) を使うと、データを遠く離れた AWS リージョン にレプリケートできるため、これらの要件を満たすのに役立ちます。CRR では、異なる AWS リージョンのバケット間でオブジェクトを自動的に非同期コピーできます。詳細については、「リージョン内およびリージョン間でのオブジェクトのレプリケート」を参照してください。

> **Note**
>
> CRR では、ソースとターゲットの両方の S3 バケットでバージョニングが有効になっている必要があります。

また、s3-bucket-replication-enabled マネージド AWS Config ルールを使用した継続的な検出コントロールの実装を検討してください。

Amazon S3 アクセス用の VPC エンドポイントの検討

Amazon S3 の 仮想プライベートクラウド (VPC) エンドポイントは、Amazon S3 への接続のみを許可する VPC 内の論理エンティティです。VPC エンドポイントは、トラフィックがオープンインターネットを通過するのを防ぐのに役立ちます。

Amazon S3 の VPC エンドポイントは、Amazon S3 データへのアクセスを制御するいくつかの方法を提供します。

- S3 バケットポリシーを使用して、特定の VPC エンドポイントを通じて許可されるリクエスト、ユーザー、またはグループを管理できます。
- S3 バケットポリシーを使用して、S3 バケットへのアクセスが可能な VPC または VPC エンドポイントをコントロールできます。
- インターネットゲートウェイのない VPC を使用すると、データの流出を防ぐのに役立ちます。

詳細については、「バケットポリシーを使用した VPC エンドポイントからのアクセスコントロール」を参照してください。

マネージド AWS セキュリティサービスを使用したデータセキュリティの監視

いくつかのマネージド AWS セキュリティサービスは、Amazon S3 データのセキュリティとコンプライアンスのリスクを特定、評価、監視するのに役立ちます。これらのサービスは、こうしたリスクからデータを保護するのにも役立ちます。これらのサービスには、単一の AWS アカウント Amazon S3 リソースから数千のアカウントにまたがる組織向けのリソースに拡張できるように設計された、自動検知、モニタリング、保護機能が含まれます。

詳細については、「マネージド AWS セキュリティサービスによるデータセキュリティのモニタリング」を参照してください。

Amazon S3 のモニタリングと監査のベストプラクティス

以下は、潜在的なセキュリティ上の弱点とインシデントを検出するために役立つ Amazon S3 でのベストプラクティスです。

すべての Amazon S3 バケットを特定して監査

IT アセットの特定はガバナンスとセキュリティの重要な側面です。セキュリティの状態を評価し、潜在的な弱点に対処するには、すべての Amazon S3 リソースが見えていなければなりません。リソースを監査するには、以下を実行することをお勧めします。

- タグエディターを使用してセキュリティまたは監査で注意を要するリソースを識別してタグ付けするには、これらのリソースを検索する必要があるときにそれらのタグを使用します。詳細については、「AWS リソースのタグ付けユーザーガイド」の「タグ付けするリソースの検索」を参照してください。
- S3 インベントリを使用して、ビジネス、コンプライアンス、および規制上のニーズに応じて、オブジェクトのレプリケーションと暗号化のステータスを監査し、レポートします。詳細については、「S3 インベントリを使用したデータのカタログ化と分析」を参照してください。
- Amazon S3 リソースのリソースグループを作成します。詳細については、「AWS Resource Groups ユーザーガイド」の「 リソースグループとは」を参照してください。

AWS モニタリングツールによるモニタリングの実装

モニタリングは、Amazon S3 および AWS ソリューションの信頼性、セキュリティ、可用性、パフォーマンスを維持する上で重要なエレメントです。AWS では、Amazon

S3 およびその他の AWS のサービス をモニタリングするのに役立つツールとサービスを提供しています。例えば、Amazon S3 の Amazon CloudWatch メトリクス (特に、PutRequests、GetRequests、4xxErrors、DeleteRequests) をモニタリングできます。詳細については、「Amazon CloudWatch によるメトリクスのモニタリング」および「Amazon S3 での口グ記録とモニタリング」を参照してください。

別の例については、例: Amazon S3 バケットのアクティビティ を参照してください。この例では、バケットのポリシー、バケットのライフサイクル、またはバケットのレプリケーション設定の PUT または DELETE に対して、あるいはバケット ACL の PUT に対して Amazon S3 API コールが行われたときにトリガーされる CloudWatch アラームを作成する方法について説明します。

Amazon S3 サーバーアクセスログを有効にする

サーバーアクセスのログには、バケットに対するリクエストの詳細が記録されます。サーバーアクセスログは、セキュリティやアクセス監査の参考になることがあり、顧客基盤について知り、Amazon S3 の請求を理解するのに役立ちます。サーバーアクセスログ記録を有効にする手順については、サーバーアクセスログによるリクエストのログ記録 を参照してください。

また、s3-bucket-logging-enabled AWS Config マネージドルールを使用する継続的な検出コントロールの実装を検討してください。

AWS CloudTrail の使用

AWS CloudTrail は、Amazon S3 のユーザー、ロール、または AWS のサービス によって実行されたアクションのレコードを提供します。CloudTrail によって収集されたデータを使用して、以下の情報を判断できます。

- Amazon S3 に対して行われたリクエスト
- リクエストが行われた IP アドレス
- リクエストを行ったユーザー
- リクエストが行われた時間
- リクエストに関するその他の詳細

例えば、データアクセスに影響する PUT アクション (特に PutBucketAcl、PutObjectAcl、PutBucketPolicy および PutBucketWebsite) の CloudTrail エントリを特定できます。

AWS アカウントをセットアップすると、CloudTrail はデフォルトで有効になっています。CloudTrail コンソールで最近のイベントを確認できます。Amazon S3 バケットのアクティビ

ティとイベントの継続的なレコードを作成するには、CloudTrail コンソールで証跡を作成できます。詳細については、「AWS CloudTrail ユーザーガイド」の「データイベントをログ記録する」を参照してください。

証跡を作成する際に、データイベントをログ記録するように CloudTrail を設定できます。データイベントは、リソース上またはリソース内で実行されたリソースオペレーションのレコードです。Amazon S3 では、データイベントは、個々のバケットのオブジェクトレベルの API アクティビティを記録します。CloudTrail は、`GetObject`、`DeleteObject`、`PutObject` などの Amazon S3 オブジェクトレベルの API オペレーションのサブセットをサポートしています。CloudTrail と Amazon S3 との連携の詳細については、AWS CloudTrail を使用した Amazon S3 API コールのログ記録 を参照してください。Amazon S3 コンソールでは、S3 バケットとオブジェクトの CloudTrail イベントログ記録の有効化 に S3 バケットを設定することもできます。

AWS Config に用意されている管理ルール (`cloudtrail-s3-dataevents-enabled`) を使用すると、少なくとも 1 つの CloudTrail 証跡が S3 バケットのデータイベントのログに記録していることを確認できます。詳細については、cloudtrail-s3-dataevents-enabled デベロッパーガイドのAWS Config を参照してください。

AWS Config の有効化

このトピックに示すベストプラクティスのいくつかでは、AWS Config ルールの作成を提案しています。AWS Config では、AWS リソースの設定を評価、監査、診断するのに役立ちます。AWS Config では、リソースの設定をモニタリングし、目的とする安全な設定に対して、記録された設定を評価できます。AWS Config では、次のことを実行できます。

- 設定の変更と AWS リソース間の関係を確認します。
- 詳細なリソース設定履歴の調査
- 内部ガイドラインに指定されている設定に対して全体的なコンプライアンスを決定します。

AWS Config を使用すると、コンプライアンス監査、セキュリティ分析、変更管理、運用上のトラブルシューティングを簡素化できます。詳細については、AWS Config デベロッパーガイドのコンソールを使用した AWS Config の設定 を参照してください。記録するリソースタイプを指定するときは、必ず Amazon S3 リソースを含めてください。

> **Important**
>
> AWS Config マネージドルールは Amazon S3 リソースを評価する際に汎用バケットのみをサポートします。AWS Config ディレクトリバケットの設定変更は記録されません。

詳細については、「AWS Config デベロッパーガイド」の「AWS Config マネージドルール」と「AWS Config マネージドルールリスト」を参照してください。

AWS Config を使用する方法の例については、「AWS セキュリティブログ」の「パブリックアクセスを許可する Amazon S3 バケットを AWS Config でモニタリングおよび応答する方法」を参照してください。

S3 ストレージレンズの使用

S3 ストレージレンズは、オブジェクトストレージの使用状況とアクティビティを組織全体で可視化するために使用できるクラウドストレージ分析機能です。また、S3 Storage Lens は、メトリクスを分析して、ストレージコストを最適化し、データ保護に関するベストプラクティスを適用するために使用できるコンテキストに応じた推奨事項を提供します。

S3 Storage Lens で、組織全体でどれだけのストレージがあるか、または最も急速に成長しているバケットとプレフィックスは何かなどの、要約されたインサイトを生成できます。S3 Storage Lens メトリクスを使用して、コスト最適化の機会を特定し、データ保護とアクセス管理のベストプラクティスを実装し、アプリケーションワークロードのパフォーマンスを向上させることができます。

例えば、S3 ライフサイクルルールがないバケットを特定して、7 日以上経過した不完全なマルチパートアップロードを中止できます。また、S3 レプリケーションや S3 バージョニングの使用など、データ保護のベストプラクティスに従っていないバケットを特定することもできます。詳細については、「Amazon S3 ストレージレンズについて」を参照してください。

AWS セキュリティアドバイザリをモニタリングする

AWS アカウント について Trusted Advisor に投稿されたセキュリティ勧告を定期的に確認することをお勧めします。特に、「オープンアクセス許可」のある Amazon S3 バケットに関する警告を探します。このステップは、describe-trusted-advisor-checks を使用して、プログラムで実行できます。

さらに、各 AWS アカウント に登録されているメインの E メールアドレスを注意してモニタリングしてください。AWS は、この E メールアドレスを使用して、ユーザーに影響を与える可能性のあるセキュリティ問題が発生した場合に連絡します。

広範な影響を与える AWS の運用上の問題は AWS Health Dashboard - Service health に投稿されます。運用上の問題も、AWS Health Dashboard を通じて個々のアカウントに投稿されます。詳細については、AWS Health のドキュメントを参照してください。

マネージド AWS セキュリティサービスによるデータセキュリティのモニタリング

いくつかのマネージド AWS セキュリティサービスは、Amazon S3 データのセキュリティとコンプライアンスのリスクを特定、評価、監視するのに役立ちます。また、こうしたリスクからデータを保護するのにも役立ちます。これらのサービスには、単一の AWS アカウント から数千の AWS アカウント にまたがる組織向けのリソースに拡張できるように設計された、自動検知、モニタリング、保護機能が含まれます。

AWS 検出および対応サービスを使うと、潜在的なセキュリティ設定ミス、脅威、または予期しない動作を特定できるため、環境内の不正または悪意のある可能性があるアクティビティに対して迅速に対応できます。AWS データ保護サービスは、データ、アカウント、ワークロードをモニタリングし、不正アクセスから保護するのに役立ちます。また、Amazon S3 のデータ資産内で個人を特定できる情報 (PII) などの機密データを発見するのにも役立ちます。

データセキュリティとコンプライアンスのリスクを特定して評価するのをサポートするため、マネージド AWS セキュリティサービスでは、検出結果を生成して、Amazon S3 データに関する潜在的なセキュリティイベントや問題を通知します。検出結果には関連する詳細は、インシデント対応のワークフローとポリシーに従ってこれらのリスクを調査、評価、対処するために使用できます。各サービスを使用して、検出結果データに直接アクセスできます。また、セキュリティインシデントやイベント管理システム (SIEM) など、他のアプリケーション、サービス、システムにデータを送信することもできます。

Amazon S3 データのセキュリティをモニタリングするには、これらのマネージド AWS セキュリティサービスの使用を検討してください。

Amazon GuardDuty

Amazon GuardDuty は、悪意のあるアクティビティがないか継続的に AWS アカウント をモニタリングし、詳細なセキュリティ検出結果を提供する脅威検知サービスです。

GuardDuty の S3 保護機能を使用すると、Amazon S3 リソースの AWS CloudTrail 管理イベントとデータイベントを分析するように GuardDuty を設定できます。それにより、GuardDuty は、悪意のあるアクティビティや疑わしいアクティビティについてこれらのイベントをモニタリングします。分析を行い、潜在的なセキュリティリスクを特定するため、GuardDuty は脅威インテリジェンスフィードと機械学習を使用しています。

GuardDuty では、Amazon S3 リソースについてさまざまな種類のアクティビティをモニタリングできます。例えば、Amazon S3 の CloudTrail 管理イベント

には、ListBuckets、DeleteBucket、PutBucketReplication など、バケットレベルのオペレーションが含まれます。Amazon S3 のデータイベントには、GetObject、ListObjects、PutObject などのオブジェクトレベルのオペレーションが含まれます。GuardDuty が異常なアクティビティや潜在的に悪意のあるアクティビティを検出すると、検出結果を生成してユーザーに通知します。

詳細については、「Amazon GuardDuty ユーザーガイド」の「Amazon GuardDuty での Amazon S3 の保護」を参照してください。

Amazon Detective

Amazon Detective は調査プロセスを簡素化し、セキュリティ調査をより迅速かつ効果的に実施できるようにします。Detective が提供する事前に作成されたデータ集計、要約、およびコンテキストは、考えられるセキュリティ問題の性質と範囲を迅速に分析および評価するのに役立ちます。

Detective は、AWS CloudTrail からの API 呼び出しや AWS の Amazon VPC フローログなど、時間ベースのイベントを自動的に抽出します。また、Amazon GuardDuty によって生成された検出結果も取り込みます。次に Detective は、機械学習、統計分析、グラフ理論を使用して、セキュリティ調査をより迅速かつ効率的に行うのに役立つビジュアライゼーションを生成します。

これらのビジュアライゼーションは、リソースの動作と時間の経過に伴うそれらのインタラクションに関するインタラクティブな統合ビューを提供します。この動作グラフを詳しく確認すると、失敗したログオン試行や疑わしい API コールなど、さまざまなアクションを調べることができます。また、これらのアクションが S3 バケットやオブジェクトなどのリソースにどのように影響するかを確認できます。

詳細については、「Amazon Detective 管理ガイド」を参照してください。

IAM Access Analyzer

AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) は、外部エンティティと共有されているリソースを識別するのに役立ちます。また、IAM Access Analyzer を使用して IAM ポリシーをポリシー文法やベストプラクティスに照らして検証し、AWS CloudTrail ログのアクセスアクティビティに基づいて IAM ポリシーを生成することもできます。

IAM Access Analyzer は、ロジックベースの推論を使用して、バケットポリシーなど、AWS 環境内のリソースポリシーを分析します。IAM Access Analyzer for S3 は、インターネットの任意のユーザーや他の AWS アカウント (組織外のアカウントを含む) にアクセスを許可するように S3 バケットが設定された場合、警告します。例えば、IAM Access Analyzer for S3 は、バケットのアクセスコントロールリスト (ACL)、バケットポリシー、マルチリージョンアクセスポイントポリシー、またはアクセスポイントポリシーを通じて、バケットに読み取りまたは書き込みのアク

セス権が提供されていることを報告する場合があります。パブリックバケットまたは共有バケットごとに、パブリックアクセスや共有アクセスのソースとレベルを示す検出結果が送信されます。この情報を用いて、迅速で正確な是正処置を講じ、バケットへのアクセスを意図したとおりに復元できます。

詳細については、「IAM Access Analyzer for S3 を使用したバケットアクセスの確認」を参照してください。

Amazon Macie

Amazon Macie は、機械学習とパターンマッチングを使用して機密データを発見するセキュリティサービスです。Macie はデータセキュリティリスクを可視化し、それらのリスクに対する自動保護を可能にします。Macie を使用すると、Amazon S3 データアセット内の機密データの検出とレポートを自動化して、組織が Amazon S3 に保存しているデータを詳細に把握できます。

Macie を使用して機密データを検出するには、多くの国または地域の機密データタイプの大規模かつ増加しているリストを検出するように設計された組み込み型の基準と手法を使用できます。これらの機密データタイプには、複数の種類の個人を特定できる情報 (PII)、財務データ、認証情報データが含まれます。一致するテキストパターンを定義する正規表現を使用したり、オプションで結果を絞り込む文字シーケンスや近接ルールなど、自分で定義したカスタム基準を使用することもできます。

Macie が S3 オブジェクト内の機密データを検出すると、Macie はセキュリティ上の検出結果を生成して通知します。この検出結果により、影響を受けたオブジェクト、Macie が見つけた機密データの種類と出現回数、および影響を受けた S3 バケットとオブジェクトの調査に役立つ追加情報が得られます。詳細については、「Amazon Macie ユーザーガイド」を参照してください。

AWS Security Hub

AWS Security Hub は、セキュリティのベストプラクティスをチェックし、複数のソースからのアラートと検出結果を 1 つの形式に集約し、自動修復を可能にするセキュリティ体制管理サービスです。

Security Hub は、Amazon Detective、Amazon GuardDuty、IAM Access Analyzer、Amazon Macie などの統合 AWS Partner Network セキュリティソリューションおよび AWS のサービスからセキュリティ検出結果データを収集して提供します。また、AWS ベストプラクティスとサポートされている業界標準に基づいて、継続的な自動セキュリティチェックを実行することによって、独自の検出結果を生成します。

Security Hub はその後、プロバイダー間で結果を関連づけて統合し、最も重要な検出結果を優先化し、処理できるようにします。また、カスタムアクションもサポートされています。カスタム

アクションを使用して、特定クラスの検出結果に対する応答または修復アクションを呼び出すことができます。

Security Hub を使用すると、Amazon S3 リソースのセキュリティとコンプライアンスのステータスを評価できます。これは、個々の AWS リージョン と複数のリージョンで、組織のセキュリティ体制に対するより広範な分析の一部として行うことができます。これには、セキュリティの傾向分析や最も優先度の高いセキュリティ問題の特定が含まれます。また、複数の AWS リージョン からの検出結果を集約したり、1 つのリージョンから集計した検出結果データをモニタリングおよび処理することもできます。

詳細については、「AWS Security Hub ユーザーガイド」の「Amazon Simple Storage Service コントロール」を参照してください。

Amazon S3 におけるデータ保護

Amazon S3 は、ミッションクリティカルで重要なデータストレージのために設計された、高い耐久性を備えたストレージインフラストラクチャです。S3 標準、S3 Intelligent-Tiering、S3 標準 — IA、S3 Glacier インスタント検索、S3 Glacier フレキシブル検索、および S3 Glacier Deep Archive は、AWS リージョン の最低 3 つのアベイラビリティーゾーンにわたって複数のデバイスにオブジェクトを冗長して保存します。アベイラビリティーゾーンは、AWS リージョン の冗長電源、ネットワーク、および接続を備えた 1 つ以上の個別のデータセンターです。アベイラビリティーゾーンは、他のアベイラビリティーゾーンから意味のある距離 (キロメートル) で物理的に分離されていますが、すべてが互いに 100 km (60 マイル)以内にあります。S3 1 ゾーンストレージクラスは、単一のアベイラビリティーゾーン内の複数のデバイスにデータを冗長に保存します。これらのサービスは、失われた冗長性を迅速に検出して修復することにより、同時デバイス障害を処理するように設計されており、また、チェックサムを使用してデータの整合性を定期的に検証します。

Amazon S3 Standard ストレージには以下の特徴があります。

- Amazon S3 サービスレベルアグリーメントに裏づけられています。
- 1 年間に 99.999999999% の耐久性と、99.99% のオブジェクトの可用性を提供するよう設計されています。
- S3 Standard、S3 Intelligent-Tiering、S3 標準 — IA、S3 Glacier インスタント検索、S3 Glacier フレキシブル検索、S3 Glacier Deep Archive は、Amazon S3 アベイラビリティーゾーン全体が失われた場合にデータを維持するように設計されています。

Amazon S3 は、バージョニングを使用してデータ保護を強化しています。バージョニングを使用して、Amazon S3 バケットに格納されたあらゆるオブジェクトのあらゆるバージョンを、格納、取得、復元することができます。バージョニングを使用すれば、意図しないユーザーアクションからもアプリケーション障害からも、簡単に復旧できます。デフォルトでは、リクエストは最も新しく書き込まれたバージョンを取得します。リクエストでオブジェクトのバージョンを指定することにより、古いバージョンのオブジェクトを取得できます。

S3 バージョニングとは別に、Amazon S3 オブジェクトロックと S3 レプリケーションを使用してデータを保護することもできます。詳細については、「Amazon S3 におけるデータ保護」を参照してください。

データ保護目的の場合、AWS アカウント 認証情報を保護して AWS Identity and Access Management で個々のユーザーアカウントをセットアップし、そのユーザーに各自の職務を果たすために必要な許可のみが付与されるようにすることをお勧めします。

コマンドラインインターフェイスまたは API を使用して AWS にアクセスするときに FIPS 140-2 検証済みの暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。使用可能な FIPS エンドポイントの詳細については、連邦情報処理規格 (FIPS) 140-2 を参照してください。

以下のセキュリティのベストプラクティスも Amazon S3 でのデータ保護に対処します。

- Implement server-side encryption
- Enforce encryption of data in transit
- Consider using Macie with Amazon S3
- Identify and audit all your Amazon S3 buckets
- Monitor Amazon Web Services security advisories

暗号化によるデータの保護

> **Important**
>
> Amazon S3 では、Amazon S3 内のすべてのバケットの基本レベルの暗号化として、Amazon S3 が管理するキー (SSE-S3) によるサーバー側の暗号化が適用されるようになりました。2023 年 1 月 5 日以降、Amazon S3 にアップロードされるすべての新しいオブジェクトは、追加費用なしで、パフォーマンスに影響を与えずに自動的に暗号化されます。S3 バケットのデフォルト暗号化設定と新しいオブジェクトのアップロードのための自動暗号化ステータスは、AWS CloudTrail ログ、S3 インベントリ、S3 ストレージレン

ズ、Amazon S3 コンソール、および AWS Command Line Interface と AWS SDK の追加の Amazon S3 API レスポンスヘッダーとして利用できるようになりました。詳細については、「デフォルト暗号化に関するよくある質問」を参照してください。

データ保護とは、転送時 (Amazon S3 との間でデータを送受信するとき)と保存時 (Amazon S3 データセンター内のディスクに格納されているとき) にデータを保護することを指します。Secure Socket Layer/Transport Layer Security (SSL/TLS) またはクライアント側の暗号化を使用して、転送中のデータを保護できます。Amazon S3 で保管時のデータを保護するには、次のようなオプションがあります。

- サーバー側の暗号化 – Amazon S3 は、AWS データセンターのディスクに保存する前にオブジェクトを暗号化し、ダウンロードするときにオブジェクトを復号化します。

  すべての Amazon S3 バケットにはデフォルトで暗号化が設定されており、S3 バケットにアップロードされたすべての新しいオブジェクトは保存時に自動的に暗号化されます。Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3) は、Amazon S3 のすべてのバケットでのデフォルトの暗号化設定です。別のタイプの暗号化を使用するには、S3 PUT リクエストで使用するサーバー側の暗号化のタイプを指定するか、宛先バケットにデフォルトの暗号化設定を更新できます。

  PUT リクエストで別の暗号化タイプを指定する場合は、AWS Key Management Service (AWS KMS) キーによるサーバー側の暗号化 (SSE-KMS)、AWS KMS キーによる二層式サーバー側の暗号化 (DSSE-KMS)、または顧客提供のキーによるサーバー側の暗号化 (SSE-C) を使用できます。宛先バケットに別のデフォルト暗号化設定を設定する場合は、SSE-KMS または DSSE-KMS を使用できます。

  汎用バケットのデフォルトの暗号化設定を変更する方法の詳細については、「デフォルトの暗号化の設定」を参照してください。

  バケットのデフォルトの暗号化設定を SSE-KMS に変更しても、バケット内の既存の Amazon S3 オブジェクトの暗号化タイプは変更されません。デフォルトの暗号化設定を SSE-KMS に更新した後に既存のオブジェクトの暗号化タイプを変更するには、Amazon S3 バッチオペレーションを使用できます。S3 バッチオペレーションにオブジェクトのリストを指定すると、バッチオペレーションが対応する API オペレーションを呼び出します。オブジェクトのコピー アクションを使用して既存のオブジェクトをコピーし、SSE-KMS で暗号化されたオブジェクトと同じバケットに書き戻すことができます。1 つのバッチオペレーションジョブで、数十億ものオブジェクトに対して、指定されたオペレーションを実行できます。詳細については、「バッチオペレーショ

ンでオブジェクトオペレーションを一括で実行する」および AWS Storage Blog の投稿「How to retroactively encrypt existing objects in Amazon S3 using S3 Inventory, Amazon Athena, and S3 Batch Operations」を参照してください。

サーバー側の暗号化の詳細については、「サーバー側の暗号化によるデータの保護」を参照してください。

サーバー側の暗号化を設定するには、以下を参照してください。

- Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3) の指定
- AWS KMS (SSE-KMS) によるサーバー側の暗号化の指定
- the section called “DSSE-KMS の指定”
- お客様が用意したキーによるサーバー側の暗号化 (SSE-C) の指定

- クライアント側の暗号化 – クライアント側でデータを暗号化し、暗号化したデータを Amazon S3 にアップロードします。この場合、暗号化プロセス、暗号化キー、関連ツールはお客様が管理してください。

  クライアント側の暗号化を設定するには、クライアント側の暗号化を使用したデータの保護 を参照してください。

ストレージバイトの何パーセントが暗号化されているかを確認するには、Amazon S3 ストレージレンズメトリクスを使用できます。S3 ストレージレンズは、オブジェクトストレージの使用状況とアクティビティを組織全体で可視化するために使用できるクラウドストレージ分析機能です。詳細については、「S3 Storage Lens を使用したストレージのアクティビティと使用状況の評価」を参照してください。メトリクスの完全なリストについては、「S3 ストレージレンズメトリクスに関する用語集」を参照してください。

サーバー側の暗号化とクライアント側の暗号化の詳細については、以下のトピックを参照してください。

トピック

- サーバー側の暗号化によるデータの保護
- クライアント側の暗号化を使用したデータの保護

サーバー側の暗号化によるデータの保護

> **Important**
>
> Amazon S3 では、Amazon S3 内のすべてのバケットの基本レベルの暗号化として、Amazon S3 が管理するキー (SSE-S3) によるサーバー側の暗号化が適用されるようになりました。2023 年 1 月 5 日以降、Amazon S3 にアップロードされるすべての新しいオブジェクトは、追加費用なしで、パフォーマンスに影響を与えずに自動的に暗号化されます。S3 バケットのデフォルト暗号化設定と新しいオブジェクトのアップロードのための自動暗号化ステータスは、AWS CloudTrail ログ、S3 インベントリ、S3 ストレージレンズ、Amazon S3 コンソール、および AWS Command Line Interface と AWS SDK の追加の Amazon S3 API レスポンスヘッダーとして利用できるようになりました。詳細については、「デフォルト暗号化に関するよくある質問」を参照してください。

サーバー側の暗号化とは、データを受信するアプリケーションまたはサービスによって、送信先でデータを暗号化することです。Amazon S3 は、AWS データセンターのディスクに書き込まれるときにデータをオブジェクトレベルで暗号化し、お客様がデータにアクセスするときに復号します。リクエストが認証され、お客様がアクセス許可を持っていれば、オブジェクトが暗号化されているかどうかに関係なく同じ方法でアクセスできます。例えば、署名付き URL を使用してオブジェクトを共有する場合、その署名付き URL は、オブジェクトが暗号化されているかどうかに関係なく同じように動作します。また、バケット内のオブジェクトを一覧表示すると、リスト API オペレーションは、オブジェクトが暗号化されているかどうかに関係なく、すべてのオブジェクトのリストを返します。

すべての Amazon S3 バケットにはデフォルトで暗号化が設定されており、S3 バケットにアップロードされたすべての新しいオブジェクトは保存時に自動的に暗号化されます。Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3) は、Amazon S3 のすべてのバケットでのデフォルトの暗号化設定です。別のタイプの暗号化を使用するには、S3 PUT リクエストで使用するサーバー側の暗号化のタイプを指定するか、宛先バケットにデフォルトの暗号化設定を更新できます。

PUT リクエストで別の暗号化タイプを指定する場合は、AWS Key Management Service (AWS KMS) キーによるサーバー側の暗号化 (SSE-KMS)、AWS KMS キーによる二層式サーバー側の暗号化 (DSSE-KMS)、または顧客提供のキーによるサーバー側の暗号化 (SSE-C) を使用できます。宛先バケットに別のデフォルト暗号化設定を設定する場合は、SSE-KMS または DSSE-KMS を使用できます。

汎用バケットのデフォルトの暗号化設定を変更する方法の詳細については、「デフォルトの暗号化の設定」を参照してください。

バケットのデフォルトの暗号化設定を SSE-KMS に変更しても、バケット内の既存の Amazon S3 オブジェクトの暗号化タイプは変更されません。デフォルトの暗号化設定を SSE-KMS に更新した後に既存のオブジェクトの暗号化タイプを変更するには、Amazon S3 バッチオペレーションを使用できます。S3 バッチオペレーションにオブジェクトのリストを指定すると、バッチオペレーションが対応する API オペレーションを呼び出します。オブジェクトのコピー アクションを使用して既存のオブジェクトをコピーし、SSE-KMS で暗号化されたオブジェクトと同じバケットに書き戻すことができます。1 つのバッチオペレーションジョブで、数十億ものオブジェクトに対して、指定されたオペレーションを実行できます。詳細については、「バッチオペレーションでオブジェクトオペレーションを一括で実行する」および AWS Storage Blog の投稿「How to retroactively encrypt existing objects in Amazon S3 using S3 Inventory, Amazon Athena, and S3 Batch Operations」を参照してください。

> **Note**
>
> 異なる種類のサーバー側暗号化を同時に同じオブジェクトに適用することはできません。

既存のオブジェクトを暗号化する必要がある場合は、S3 バッチオペレーションと S3 インベントリを使用してください。詳細については、「Encrypting objects with Amazon S3 Batch Operations」(Amazon S3 バッチオペレーションよるオブジェクトの暗号化) および バッチオペレーションでオブジェクトオペレーションを一括で実行する を参照してください。

サーバー側の暗号化には、暗号化キーの管理方法の選択と適用する暗号化レイヤーの数に応じて、相互に排他的な 4 つのオプションがあります。

Amazon S3 マネージドキーを用いたサーバー側の暗号化 (SSE-S3)

すべての Amazon S3 バケットには、デフォルトで暗号化が設定されています。サーバー側の暗号化のデフォルトのオプションは、Amazon S3 マネージド キー (SSE-S3) を使用しています。一意のキーで各オブジェクトを暗号化します。追加の保護措置として、SSE-S3 は定期的にローテーションされるルートキーを使ってキーそのものを暗号化します。SSE-S3 は、利用可能な最強のブロック暗号の 1 つである 256 ビットの 高度暗号化規格 (AES-256) を使用して、データを暗号化します。詳細については、「Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3)」を参照してください。

AWS Key Management Service (AWS KMS) キー (SSE-KMS) によるサーバー側の暗号化

AWS KMS keys (SSE-KMS) によるサーバー側の暗号化は、AWS KMS サービスと Amazon S3 の統合によって提供されます。AWS KMS を使用すると、キーをより細かく制御できます。例えば、個

別のキーを表示し、制御ポリシーを編集して、AWS CloudTrail のキーに従うことができます。さらに、カスタマーマネージドキーを作成および管理したり、ユーザー、サービス、およびリージョンに固有の AWS マネージドキー を使用したりできます。詳細については、「AWS KMS キーによるサーバー側の暗号化 (SSE-KMS) の使用」を参照してください。

AWS Key Management Service (AWS KMS) キーによる二層式サーバー側の暗号化 (DSSE-KMS)

AWS KMS keys による二層式サーバー側の暗号化 (DSSE-KMS) は、SSE-KMS と似ていますが、DSSE-KMS では 1 つのレイヤーの代わりに 2 つの個別のオブジェクトレベルの暗号化レイヤーを適用します。両方の暗号化レイヤーがサーバーサイドでオブジェクトに適用されるため、コンプライアンス要件を満たす暗号化方法を使用しながら、幅広い AWS のサービス とツールを使用して S3 内のデータを分析できます。詳細については、「AWS KMS キーによる二層式サーバー側の暗号化 (DSSE-KMS) の使用」を参照してください。

顧客提供のキーを用いたサーバー側の暗号化 (SSE-C)。

顧客提供キーによるサーバー側の暗号化 (SSE-C) では、お客様が暗号化キーを管理し、Amazon S3 はディスクに書き込む際の暗号化とオブジェクトにアクセスする際の復号を管理します。詳細については、「お客様が指定したキーによるサーバー側の暗号化 (SSE-C) の使用」を参照してください。

Amazon S3 バケット向けのサーバー側のデフォルトの暗号化動作の設定

> **Important**
>
> Amazon S3 では、Amazon S3 内のすべてのバケットの基本レベルの暗号化として、Amazon S3 が管理するキー (SSE-S3) によるサーバー側の暗号化が適用されるようになりました。2023 年 1 月 5 日以降、Amazon S3 にアップロードされるすべての新しいオブジェクトは、追加費用なしで、パフォーマンスに影響を与えずに自動的に暗号化されます。S3 バケットのデフォルト暗号化設定と新しいオブジェクトのアップロードのための自動暗号化ステータスは、AWS CloudTrail ログ、S3 インベントリ、S3 ストレージレンズ、Amazon S3 コンソール、および AWS Command Line Interface と AWS SDK の追加の Amazon S3 API レスポンスヘッダーとして利用できるようになりました。詳細については、「デフォルト暗号化に関するよくある質問」を参照してください。

すべての Amazon S3 バケットにはデフォルトで暗号化が設定されており、オブジェクトは Amazon S3 マネージドキー (SSE-S3) を使用してサーバー側の暗号化により自動的に暗号化されます。この暗号化設定は Amazon S3 バケット内のすべてのオブジェクトに適用されます。

キーローテーションやアクセスポリシーの付与の管理など、キーをより細かく制御する必要がある場合は、AWS Key Management Service (AWS KMS) キーによるサーバー側の暗号化 (SSE-KMS)、または AWS KMS キーによる二層式サーバー側の暗号化 (DSSE-KMS) を使用できます。KMS キーの編集の詳細については、『AWS Key Management Service デベロッパーガイド』の「キーの編集」を参照してください。

> **Note**
>
> 新しいオブジェクトのアップロードを自動的に暗号化するようにバケットを変更しました。以前にデフォルトの暗号化を行わずにバケットを作成した場合、Amazon S3 は SSE-S3 を使用してバケットの暗号化をデフォルトで有効にします。SSE-S3 または SSE-KMS が設定されている既存のバケットについては、デフォルトの暗号化設定は変更されません。SSE-KMS でオブジェクトを暗号化する場合は、バケット設定で暗号化タイプを変更する必要があります。詳細については、「AWS KMS キーによるサーバー側の暗号化 (SSE-KMS) の使用」を参照してください。

SSE-KMS でデフォルトの暗号化を使用するようにバケットを設定する場合、S3 バケットキーを有効にして、Amazon S3 から AWS KMS へのリクエストトラフィックを減らし、暗号化のコストを削減することもできます。詳細については、「Amazon S3 バケットキーを使用した SSE-KMS のコストの削減」を参照してください。

デフォルトの暗号化で SSE-KMS が有効になっているバケットを特定するには、Amazon S3 ストレージレンズメトリクスを使用できます。S3 ストレージレンズは、オブジェクトストレージの使用状況とアクティビティを組織全体で可視化するために使用できるクラウドストレージの分析機能です。詳細については、「Using S3 Storage Lens to protect your data」(S3 ストレージレンズを使用してデータを保護する) を参照してください。

サーバー側の暗号化を使用すると、Amazon S3 はオブジェクトをディスクに保存する前に暗号化し、オブジェクトをダウンロードするときに復号します。サーバー側の暗号化および暗号化キー管理を使用したデータ保護の詳細については、サーバー側の暗号化によるデータの保護 を参照してください。

デフォルトの暗号化に必要なアクセス許可の詳細については、『Amazon Simple Storage Service API リファレンス』の「PutBucketEncryption」を参照してください。

Amazon S3 コンソール、AWS SDK、Amazon S3 REST API、および AWS Command Line Interface (AWS CLI) を使用して、Amazon S3 で S3 バケットのデフォルトの暗号化動作を設定できます。

既存のオブジェクトの暗号化

暗号化されていない既存の Amazon S3 オブジェクトを暗号化するには、Amazon S3 バッチオペレーションを使用します。S3 バッチオペレーションは、操作するオブジェクトのリストとともに提供します。バッチオペレーションは各 API を呼び出して、指定されたオペレーションを実行します。バッチオペレーションのコピーオペレーションを使用して、既存の暗号化されていないオブジェクトをコピーし、同じバケットに新しい暗号化されたオブジェクトを書き込めます。1 つのバッチオペレーションジョブで、数十億ものオブジェクトに対して、指定されたオペレーションを実行できます。詳細については、バッチオペレーションでオブジェクトオペレーションを一括で実行する およびAWS ストレージブログの投稿である Amazon S3 バッチオペレーションによるオブジェクトの暗号化を参照してください。

`CopyObject` API オペレーションまたは `copy-object` AWS CLI コマンドを使用して、既存のオブジェクトを暗号化することもできます。詳細については、AWS ストレージブログの投稿である AWS CLI を使用した既存の Amazon S3 オブジェクトの暗号化を参照してください。

> **Note**
>
> デフォルトの暗号化が SSE-KMS に設定されている Amazon S3 バケットは、the section called “サーバーアクセスのログ記録” の送信先バケットとしては使用できません。サーバーアクセスログの送信先バケットは、デフォルトの暗号化として SSE-S3 のみをサポートしています。

クロスアカウント操作での SSE-KMS 暗号化の使用

クロスアカウント操作で暗号化を使用する場合は、次の点に注意してください。

- AWS KMS key Amazon リソースネーム (ARN) またはエイリアスがリクエスト時またはバケットのデフォルト暗号化設定によって提供されない場合は、AWS マネージドキー (`aws/s3`) が使用されます。
- KMS キーと同じ AWS アカウント の AWS Identity and Access Management (IAM) プリンシパルを使用して S3 オブジェクトをアップロードまたはアクセスする場合は、AWS マネージドキー (`aws/s3`) を使用できます。
- S3 オブジェクトにクロスアカウントアクセスを許可する場合は、カスタマーマネージドキーを使用します。カスタマーマネージドキーのポリシーを設定して、別のアカウントからのアクセスを許可することができます。

- カスタマーマネージド KMS キーを指定している場合、完全修飾 KMS キー ARN を使用することをお勧めします。代わりに KMS キーエイリアスを使用する場合、AWS KMS はリクエスタのアカウント内でキーを解決します。この動作により、バケット所有者ではなく、リクエスタに属する KMS キーでデータが暗号化される可能性があります。
- お客様 (リクエスタ) が `Encrypt` アクセス許可を付与されているキーを指定する必要があります。詳細については、AWS Key Management Service デベロッパーガイドの「キーユーザーが暗号化オペレーションに KMS キーを使用することを許可する」を参照してください。

カスタマーマネージドキーと AWS マネージド KMS キーをどのような場合に使用するかの詳細については、「Amazon S3 にあるオブジェクトの暗号化に AWS マネージドキー、またはカスタマーマネージドキーを使うべきですか」を参照してください。

レプリケーションでのデフォルト暗号化の使用

レプリケーション先バケットのデフォルトの暗号化を有効にすると、以下の暗号化動作が適用されます。

- レプリケート元バケットのオブジェクトが暗号化されていない場合、レプリケート先バケットのレプリカオブジェクトはレプリケート先バケットのデフォルトの暗号化設定を使用して暗号化されます。そのため、レプリケート元のオブジェクトのエンティティタグ (ETag) はレプリカオブジェクトの ETag とは異なります。アプリケーションで ETag を使用している場合は、アプリケーションを更新して、この違いを反映する必要があります。
- レプリケート元バケット内のオブジェクトが Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3)、AWS Key Management Service (AWS KMS) キーによるサーバー側の暗号化 (SSE-KMS)、または AWS KMS キーによる二層式サーバー側の暗号化 (DSSE-KMS) を使用して暗号化されている場合、レプリケート先バケットのレプリカオブジェクトは、レプリケート元オブジェクトと同じタイプの暗号化を使用します。レプリケート先バケットのデフォルトの暗号化設定は使用されません。

SSE-KMS を使用したデフォルト暗号化の使用については、「暗号化オブジェクトのレプリケート」を参照してください。

デフォルトの暗号化で Amazon S3 バケットキーを使用する

新しいオブジェクトで SSE-KMS をデフォルトの暗号化として使用するようにバケットを設定する場合は、S3 バケットキーを設定することもできます。S3 バケットキーは、Amazon S3 から AWS KMS へのトランザクションの数を減らし、SSE-KMS のコストを削減します。

新しいオブジェクトで SSE-KMS の S3 バケットキーを使用するようにバケットを設定すると、AWS KMS によりバケットレベルのキーが生成されます。このキーは、バケット内のオブジェクトの一意のデータキーを作成するために使用されます。この S3 バケットキーは Amazon S3 内で期間限定で使用されるため、Amazon S3 で AWS KMS にリクエストを実行し、暗号化オペレーションを完了する必要性が軽減されます。

S3 バケットキーの使用の詳細については、「Amazon S3 バケットキーの使用」を参照してください。

デフォルトの暗号化の設定

> **Important**
>
> Amazon S3 では、Amazon S3 内のすべてのバケットの基本レベルの暗号化として、Amazon S3 が管理するキー (SSE-S3) によるサーバー側の暗号化が適用されるようになりました。2023 年 1 月 5 日以降、Amazon S3 にアップロードされるすべての新しいオブジェクトは、追加費用なしで、パフォーマンスに影響を与えずに自動的に暗号化されます。S3 バケットのデフォルト暗号化設定と新しいオブジェクトのアップロードのための自動暗号化ステータスは、AWS CloudTrail ログ、S3 インベントリ、S3 ストレージレンズ、Amazon S3 コンソール、および AWS Command Line Interface と AWS SDK の追加の Amazon S3 API レスポンスヘッダーとして利用できるようになりました。詳細については、「デフォルト暗号化に関するよくある質問」を参照してください。

Amazon S3 バケットにはデフォルトで暗号化が有効化されており、新しいオブジェクトは Amazon S3 マネージドキー (SSE-S3) を使用してサーバー側の暗号化により自動的に暗号化されます。この暗号化は Amazon S3 バケット内のすべての新しいオブジェクトに適用され、費用はかかりません。

キーローテーションやアクセスポリシーの付与の管理など、暗号化キーをより細かく制御する必要がある場合は、AWS Key Management Service (AWS KMS) キーによるサーバー側の暗号化 (SSE-KMS)、または AWS KMS キーによる二層式サーバー側の暗号化 (DSSE-KMS) を使用できます。SSE-KMS に関する詳細は、「AWS KMS (SSE-KMS) によるサーバー側の暗号化の指定」を参照してください。DSSE-KMS に関する詳細については、「the section called “二層式サーバー側の暗号化 (DSSE-KMS) ”」を参照してください。

別のアカウントが所有している KMS キーを使用する場合は、そのキーを使用するアクセス許可が必要です。KMS キーのクロスアカウント権限の詳細については、「AWS Key Management Service デベロッパーガイド」の「他のアカウントで使用できる KMS キーを作成する」を参照してください。

デフォルトのバケット暗号化を SSE-KMS に設定すると、S3 バケットキーも設定して、AWS KMS リクエストのコストを削減することができます。詳細については、「Amazon S3 バケットキーを使用した SSE-KMS のコストの削減」を参照してください。

> **Note**
>
> PutBucketEncryption を使用してデフォルトのバケット暗号化を SSE-KMS に設定する場合、KMS キー ID が正しいことを確認する必要があります。Amazon S3 は PutBucketEncryption リクエストで提供された KMS キー ID を検証しません。

S3 バケットのデフォルトの暗号化の使用に追加料金はかかりません。デフォルトの暗号化動作を設定するためのリクエストには、標準 Amazon S3 リクエスト料金がかかります。料金については、「Amazon S3 の料金」を参照してください。SSE-KMS および DSSE-KMS の場合、AWS KMS の料金が適用され、これらは「AWS KMS の料金」に記載されています。

お客様が用意した暗号化キーを使用したサーバー側の暗号化 (SSE-C) はサポートされていません。

Amazon S3 コンソール、AWS SDK、Amazon S3 REST API、および AWS Command Line Interface (AWS CLI) を使用して、Amazon S3 で S3 バケットのデフォルトの暗号化を設定できます。

デフォルトの暗号化を有効にする前に注意する変更

バケットに対してデフォルトの暗号化を有効にした後は、以下の暗号化動作が適用されます。

- デフォルト暗号化が有効にされる前にバケットに存在していたオブジェクトの暗号化は、変更されません。
- デフォルト暗号化を有効にした後、オブジェクトをアップロードするとします。
  - PUT リクエストヘッダーに暗号化情報が含まれていない場合、Amazon S3 はオブジェクトを暗号化するために、バケットのデフォルトの暗号化設定を使用します。
  - PUT リクエストヘッダーに暗号化情報が含まれている場合、Amazon S3 は PUT リクエストの暗号化情報を使用して、オブジェクトを Amazon S3 に保存する前に暗号化します。
- デフォルト暗号化設定として SSE-KMS または DSSE-KMS オプションを使用する場合、AWS KMS の 1 秒あたりのリクエスト数 (RPS) 制限が適用されます。AWS KMS クォータの詳細およびクォータの引き上げをリクエストする方法については、「AWS Key Management Service デベロッパーガイド」の「クォータ」を参照してください。

> **Note**
>
> デフォルトの暗号化が有効になる前にアップロードされたオブジェクトは、暗号化されません。既存のオブジェクトの暗号化の詳細については、「the section called “デフォルトのバケット暗号化の設定”」を参照してください。

S3 コンソールの使用

Amazon S3 バケットにデフォルトの暗号化を設定するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。
3. [バケット] リストで、目的のバケットの名前を選択します。
4. [プロパティ] タブを選択します。
5. [デフォルトの暗号化] で、[編集] を選択します。
6. 暗号化を設定するには、[暗号化タイプ] で次のいずれかを選択します。
   - Amazon S3 マネージドキーを用いたサーバー側の暗号化 (SSE-S3)
   - AWS Key Management Service キーによるサーバー側の暗号化 (SSE-KMS)
   - AWS Key Management Service キーによる二層式サーバー側の暗号化 (DSSE-KMS)

   > **Important**
   >
   > デフォルトの暗号化設定として SSE-KMS または DSSE-KMS オプションを使用する場合、AWS KMS の 1 秒あたりのリクエスト数 (RPS) 制限が適用されます。AWS KMS クォータの詳細およびクォータの引き上げをリクエストする方法については、「AWS Key Management Service デベロッパーガイド」の「クォータ」を参照してください。

   バケットに別のタイプのデフォルト暗号化を指定しない限り、バケットと新しいオブジェクトはデフォルトで SSE-S3 で暗号化されます。デフォルトの暗号化の詳細については、「Amazon S3 バケット向けのサーバー側のデフォルトの暗号化動作の設定」を参照してください。

Amazon S3 のサーバー側の暗号化を使用してデータを暗号化する方法の詳細については、「Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3)」を参照してください。

7. AWS Key Management Service キーによるサーバー側の暗号化 (SSE-KMS) または AWS Key Management Service キーによる二層式サーバー側の暗号化 (DSSE-KMS) を選択した場合は、次の操作を行います。

   a. [AWS KMS キー] で、次のいずれかの方法で KMS キーを指定します。

   - 使用可能な KMS キーのリストから選択するには、[AWS KMS keys から選択する] を選択し、使用可能なキーのリストから自分の KMS キーを選択します。

     AWS マネージドキー (aws/s3) とカスタマーマネージドキーの両方がこのリストに表示されます。カスタマーマネージドキーの詳細については、AWS Key Management Service デベロッパーガイドの「カスタマーキーと AWS キー」を参照してください。
   - KMS キー ARN を入力するには、[AWS KMS key ARN を入力] を選択し、表示されるフィールドに KMS キー ARN を入力します。
   - AWS KMS コンソールで新しいカスタマーマネージドキーを作成するには、[KMS キーを作成] を選択します。

     AWS KMS key の作成の詳細については、「AWS Key Management Service デベロッパーガイド」の「キーの作成」を参照してください。

> **Important**
>
> バケットと同じ AWS リージョン で有効になっている KMS キーのみを使用できます。[Choose from your KMS keys] (KMS キーから選択する) を選択する場合、S3 コンソールにはリージョンごとに 100 個の KMS キーしか表示されません。同じリージョンに 100 個以上の KMS キーがある場合、S3 コンソールには最初の 100 個の KMS キーしか表示されません。コンソールに表示されていない KMS キーを使用するには、[AWS KMS key ARN を入力] を選択し、KMS キー ARN を入力します。Amazon S3 でサーバー側の暗号化に AWS KMS key を使用する場合は、対称暗号化 KMS キーを選択する必要があります。Amazon S3 は、対称暗号化 KMS キーのみをサポートします。これらのキーの詳細については、「AWS Key Management Service デベロッパーガイド」の「対称暗号化 KMS キー」を参照してください。

Amazon S3 における SSE-KMS の使用の詳細については、「AWS KMS キーによるサーバー側の暗号化 (SSE-KMS) の使用」を参照してください。DSSE-KMS の使用の詳細については、「the section called “二層式サーバー側の暗号化 (DSSE-KMS) ”」を参照してください。

b. SSE-KMS でデフォルトの暗号化を使用するようにバケットを設定する場合は、S3 バケットキーを有効にすることもできます。S3 バケットキーは、Amazon S3 から AWS KMS へのリクエストトラフィックを減らし、暗号化のコストを削減します。詳細については、「Amazon S3 バケットキーを使用した SSE-KMS のコストの削減」を参照してください。

S3 バケットキーを使用するには、[バケットキー] で [有効化] を選択します。

> **Note**
>
> S3 バケットキーは DSSE-KMS ではサポートされていません。

8. [Save changes] (変更の保存) をクリックします。

AWS CLI を使用する場合

以下の例では、SSE-S3 を使用するか、SSE-KMS と S3 バケット キーを使用して、デフォルトの暗号化を設定する方法を示します。

デフォルトの暗号化の詳細については、[Amazon S3 バケット向けのサーバー側のデフォルトの暗号化動作の設定] を参照してください。AWS CLI を使用してデフォルトの暗号化を設定する方法の詳細については、put-bucket-encryption を参照してください。

Example - SSE-S3 を使用したデフォルトの暗号化

この例では、Amazon S3 マネージドキーを使用したデフォルトのバケット暗号化を設定します。

```
aws s3api put-bucket-encryption --bucket amzn-s3-demo-bucket --server-side-encryption-
configuration '{
    "Rules": [
        {
            "ApplyServerSideEncryptionByDefault": {
                "SSEAlgorithm": "AES256"
            }
        }
    ]
```

```
}'
```

Example - S3 バケットキーを使用した SSE-KMS でのデフォルトの暗号化

この例では、S3 バケットキーを使用して SSE-KMS でデフォルトのバケット暗号化を設定します。

```
aws s3api put-bucket-encryption --bucket amzn-s3-demo-bucket --server-side-encryption-
configuration '{
    "Rules": [
            {
                "ApplyServerSideEncryptionByDefault": {
                    "SSEAlgorithm": "aws:kms",
                    "KMSMasterKeyID": "KMS-Key-ARN"
                },
                "BucketKeyEnabled": true
            }
        ]
    }'
```

REST API の使用

REST API PutBucketEncryption オペレーションを使用して、デフォルト暗号化を有効にし、使用するサーバー側の暗号化のタイプ (SSE-S3、SSE-KMS、または DSSE-KMS) を設定します。

詳細については、「Amazon Simple Storage Service API リファレンス」の「PutBucketEncryption」を参照してください。

AWS CloudTrail および Amazon EventBridge によるデフォルト暗号化のモニタリング

> **Important**
>
> Amazon S3 では、Amazon S3 内のすべてのバケットの基本レベルの暗号化として、Amazon S3 が管理するキー (SSE-S3) によるサーバー側の暗号化が適用されるようになりました。2023 年 1 月 5 日以降、Amazon S3 にアップロードされるすべての新しいオブジェクトは、追加費用なしで、パフォーマンスに影響を与えずに自動的に暗号化されます。S3 バケットのデフォルト暗号化設定と新しいオブジェクトのアップロードのための自動暗号化ステータスは、AWS CloudTrail ログ、S3 インベントリ、S3 ストレージレンズ、Amazon S3 コンソール、および AWS Command Line Interface と AWS SDK の追加の Amazon S3 API レスポンスヘッダーとして利用できるようになりました。詳細については、「デフォルト暗号化に関するよくある質問」を参照してください。

AWS CloudTrail イベントを使用して、Amazon S3 バケットのデフォルトの暗号化設定リクエストを追跡できます。CloudTrail ログでは、以下の API イベント名が使用されます。

- `PutBucketEncryption`
- `GetBucketEncryption`
- `DeleteBucketEncryption`

これらの API コールの CloudTrail イベントと一致するように EventBridge ルールを作成することもできます。CloudTrail イベントの詳細については、[コンソールを使用してバケット内のオブジェクトのログ記録を有効にする] を参照してください。EventBridge イベントの詳細については、「AWS のサービス からのイベント」を参照してください。

オブジェクトレベルの Amazon S3 アクションに CloudTrail ログを使用して、Amazon S3 への PUT および POST リクエストを追跡できます。これらのアクションを使用すると、受信 PUT リクエストに暗号化ヘッダーがない場合に、デフォルトの暗号化を使用してオブジェクトが暗号化されているかどうかを確認できます。

デフォルトの暗号化設定を使用して Amazon S3 がオブジェクトを暗号化すると、ログには名前と値のペアとして、`"SSEApplied":"Default_SSE_S3"`、`"SSEApplied":"Default_SSE_KMS"`、または `"SSEApplied":"Default_DSSE_KMS"` フィールドの 1 つが含まれます。

PUT の暗号化ヘッダーを使用して Amazon S3 がオブジェクトを暗号化すると、ログには名前と値のペアとして、`"SSEApplied":"SSE_S3"`、`"SSEApplied":"SSE_KMS"`、`"SSEApplied":"DSSE_KMS"`、または `"SSEApplied":"SSE_C"` フィールドの 1 つが含まれます。

マルチパートアップロードについては、この情報は `InitiateMultipartUpload` API リクエストに含まれています。CloudTrail と CloudWatch の併用の詳細については、「Amazon S3 でのログ記録とモニタリング」を参照してください。

デフォルトの暗号化のよくある質問

Amazon S3 では、Amazon S3 内のすべてのバケットの基本レベルの暗号化として、Amazon S3 が管理するキー (SSE-S3) によるサーバー側の暗号化が適用されるようになりました。2023 年 1 月 5 日以降、Amazon S3 にアップロードされるすべての新しいオブジェクトは、追加費用なしで、パフォーマンスに影響を与えずに自動的に暗号化されます。256 ビットの高度暗号化規格 (AES-256) を使用する SSE-S3 は、すべての新しいバケットと、デフォルトの暗号化がまだ設定されていない既存の S3 バケットに自動的に適用されます。S3 バケットのデフォルト暗号化設定と新しいオブ

ジェクトのアップロードのための自動暗号化ステータスは、AWS CloudTrail ログ、S3 インベントリ、S3 ストレージレンズ、Amazon S3 コンソール、および AWS Command Line Interface (AWS CLI) と AWS SDK の追加の Amazon S3 API レスポンスヘッダーとして利用できるようになりました。

以下のセクションでは、この更新に関する質問に答えます。

Amazon S3 は、既にデフォルトの暗号化が設定されている既存のバケットのデフォルトの暗号化設定を変更しますか?

いいえ。SSE-S3 または AWS Key Management Service (AWS KMS) キーを使用したサーバー側の暗号化 (SSE-KMS) が設定されている既存のバケットのデフォルトの暗号化設定は変更されません。バケットのデフォルトの暗号化動作を設定する方法の詳細については、「Amazon S3 バケット向けのサーバー側のデフォルトの暗号化動作の設定」を参照してください。SSE-S3 および SSE-KMS 暗号化設定に関する詳細は、「サーバー側の暗号化によるデータの保護」を参照してください。

デフォルトの暗号化が設定されていない既存のバケットでもデフォルトの暗号化は有効になりますか?

はい。Amazon S3 は、暗号化されていない既存のバケットすべてにデフォルトの暗号化を設定して、これらのバケットにアップロードされる新しいオブジェクトの暗号化の基本レベルとして、S3 マネージドキーによるサーバー側の暗号化 (SSE-S3) を適用するようになりました。既存の暗号化されていないバケットに既に存在するオブジェクトは、自動的に暗号化されません。

新しいオブジェクトアップロードのデフォルトの暗号化ステータスを表示する方法を教えてください。

現在、AWS CloudTrail ログ、S3 インベントリ、S3 ストレージレンズ、Amazon S3 コンソール、および AWS Command Line Interface (AWS CLI) と AWS SDK の追加の Amazon S3 API レスポンスヘッダーで、新しいオブジェクトのアップロードのデフォルトの暗号化ステータスを確認できます。

- CloudTrail イベントを確認するには、「AWS CloudTrail ユーザーガイド」の「CloudTrail コンソールで CloudTrail イベントを表示する」を参照してください。CloudTrail ログは、Amazon S3 への PUT および POST リクエストの API トラッキングを提供します。バケット内のオブジェクトを暗号化するためにデフォルトの暗号化が使用されている場合、PUT および POST API リクエストの CloudTrail ログには、名前と値のペアとして次のフィールドが含まれます。`"SSEApplied":"Default_SSE_S3"`
- S3 インベントリにおける新しいオブジェクトのアップロードの自動暗号化ステータスを確認するには、[Encryption] (暗号化) メタデータフィールドを含むように S3 インベントリレポートを設定

し、レポート内の新しいオブジェクトごとに暗号化ステータスを確認します。詳細については、「Amazon S3 インベントリの設定」を参照してください。

- S3 ストレージレンズにおける新しいオブジェクトのアップロードの自動暗号化ステータスを確認するには、S3 ストレージレンズダッシュボードを設定し、ダッシュボードの [Data protection] (データ保護) カテゴリで、[Encrypted bytes] (暗号化されたバイト数) メトリクスと [Encrypted object count] (暗号化されたオブジェクト数) メトリクスを確認します。詳細については、「S3 コンソールの使用」および「ダッシュボードで S3 Storage Lens のメトリクスを表示する」を参照してください。
- Amazon S3 コンソールでバケットレベルの自動暗号化ステータスを確認するには、Amazon S3 コンソールで Amazon S3 バケットのデフォルトの暗号化を確認します。詳細については、「デフォルトの暗号化の設定」を参照してください。
- 自動暗号化ステータスを AWS Command Line Interface (AWS CLI) および AWS SDK の追加の Amazon S3 API レスポンスヘッダー `x-amz-server-side-encryption` として表示するには、PutObject や GetObject などのオブジェクトアクション API を使用するときにレスポンスヘッダーを確認してください。

この変更を利用するには何をすればよいですか?

既存のアプリケーションに変更を加える必要はありません。すべてのバケットでデフォルトの暗号化が有効になっているため、Amazon S3 にアップロードされたすべての新しいオブジェクトは自動的に暗号化されます。

バケットに書き込まれる新しいオブジェクトの暗号化を無効にすることはできますか?

いいえ。SSE-S3 は、バケットにアップロードされるすべての新しいオブジェクトに適用される新しい基本レベルの暗号化です。新しいオブジェクトアップロードの暗号化を無効にすることはできなくなりました。

私の請求は影響を受けますか?

いいえ。SSE-S3 を使用したデフォルトの暗号化は、追加料金なしで利用できます。通常どおり、ストレージ、リクエスト、その他の S3 機能の料金が請求されます。料金については、「Amazon S3 の料金」を参照してください。

Amazon S3 は、暗号化されていない既存のオブジェクトを暗号化しますか?

いいえ。 2023 年 1 月 5 日以降、Amazon S3 は新しいオブジェクトのアップロードのみを自動的に暗号化します。既存のオブジェクトを暗号化するには、S3 Batch オペレーションを使用してオブ

ジェクトの暗号化されたコピーを作成します。これらの暗号化されたコピーには、既存のオブジェクトデータと名前が保持され、指定した暗号化キーを使用して暗号化されます。詳細については、「AWS ストレージブログ」の「Amazon S3 バッチオペレーションによるオブジェクトの暗号化」を参照してください。

このリリース以前は、バケットの暗号化を有効にしていませんでした。オブジェクトへのアクセス方法を変更する必要がありますか。

いいえ。SSE-S3 を使用したデフォルトの暗号化は、Amazon S3 に書き込まれるときにデータを自動的に暗号化し、お客様がデータにアクセスするときに復号します。自動的に暗号化されたオブジェクトへのアクセス方法に変更はありません。

クライアント側の暗号化オブジェクトにアクセスする方法を変更する必要がありますか。

いいえ。Amazon S3 にアップロードされる前に暗号化されたクライアント側の暗号化されたオブジェクトはすべて、暗号化された暗号文オブジェクトとして Amazon S3 に送られます。これらのオブジェクトには SSE-S3 暗号化レイヤーが追加されます。クライアント側の暗号化オブジェクトを使用するワークロードでは、クライアントサービスや認可設定を変更する必要はありません。

> **Note**
>
> 更新されたバージョンの AWS プロバイダーを使用していない HashiCorp Terraform ユーザーは、お客様定義の暗号化設定なしで新しい S3 バケットを作成した後、予期しないドリフトが発生する可能性があります。このドリフトを避けるには、お使いの Terraform AWS プロバーダーバージョンを次のいずれかのバージョンに更新してください。4.x のいずれかのリリース、3.76.1、2.70.4。

Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3)

> **Important**
>
> Amazon S3 では、Amazon S3 内のすべてのバケットの基本レベルの暗号化として、Amazon S3 が管理するキー (SSE-S3) によるサーバー側の暗号化が適用されるようになりました。2023 年 1 月 5 日以降、Amazon S3 にアップロードされるすべての新しいオブジェクトは、追加費用なしで、パフォーマンスに影響を与えずに自動的に暗号化されます。S3 バケットのデフォルト暗号化設定と新しいオブジェクトのアップロードのための自動暗号化ステータスは、AWS CloudTrail ログ、S3 インベントリ、S3 ストレージレンズ、Amazon S3 コンソール、および AWS Command Line Interface と AWS SDK の追加の

Amazon S3 API レスポンスヘッダーとして利用できるようになりました。詳細については、「デフォルト暗号化に関するよくある質問」を参照してください。

Amazon S3 バケットへの新しいオブジェクトのアップロードはすべて、デフォルトでは Amazon S3 マネージドキーによる暗号化 (SSE-S3) で暗号化されます。

サーバー側の暗号化は、保管中のデータを保護します。Amazon S3 は、一意のキーで各オブジェクトを暗号化します。追加の保護措置として、S3 は定期的にローテーションされるキーを使ってキーそのものを暗号化します。Amazon S3 サーバー側の暗号化では、256 ビットの高度暗号化標準 Galois/Counter Mode (AES-GCM) を使用して、アップロードされたすべてのオブジェクトを暗号化します。

Amazon S3 が管理するキーによるサーバー側の暗号化 (SSE-S3) を使用するために、追加でかかる料金はありません。ただし、デフォルトの暗号化機能を設定するためのリクエストには、標準 Amazon S3 リクエスト料金がかかります。料金については、Amazon S3 の料金を参照してください。

Amazon S3 マネージドキーのみを使用してデータアップロードを暗号化する必要がある場合は、次のバケットポリシーを使用できます。例えば、次のバケットポリシーは、サーバー側の暗号化を要求する `x-amz-server-side-encryption` ヘッダーがリクエストに含まれない限り、オブジェクトをアップロードする許可を拒否します。

```
{
  "Version": "2012-10-17",
  "Id": "PutObjectPolicy",
  "Statement": [
    {
      "Sid": "DenyObjectsThatAreNotSSES3",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
      "Condition": {
        "StringNotEquals": {
          "s3:x-amz-server-side-encryption": "AES256"
        }
      }
    }
   ]
}
```

> **Note**
>
> サーバー側の暗号化では、オブジェクトのメタデータではなく、オブジェクトデータのみが暗号化されます。

サーバー側の暗号化での API サポート

すべての Amazon S3 バケットにはデフォルトで暗号化が設定されており、S3 バケットにアップロードされたすべての新しいオブジェクトは保存時に自動的に暗号化されます。Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3) は、Amazon S3 のすべてのバケットでのデフォルトの暗号化設定です。別のタイプの暗号化を使用するには、S3 PUT リクエストで使用するサーバー側の暗号化のタイプを指定するか、宛先バケットにデフォルトの暗号化設定を更新できます。

PUT リクエストで別の暗号化タイプを指定する場合は、AWS Key Management Service (AWS KMS) キーによるサーバー側の暗号化 (SSE-KMS)、AWS KMS キーによる二層式サーバー側の暗号化 (DSSE-KMS)、または顧客提供のキーによるサーバー側の暗号化 (SSE-C) を使用できます。宛先バケットに別のデフォルト暗号化設定を設定する場合は、SSE-KMS または DSSE-KMS を使用できます。

汎用バケットのデフォルトの暗号化設定を変更する方法の詳細については、「デフォルトの暗号化の設定」を参照してください。

バケットのデフォルトの暗号化設定を SSE-KMS に変更しても、バケット内の既存の Amazon S3 オブジェクトの暗号化タイプは変更されません。デフォルトの暗号化設定を SSE-KMS に更新した後に既存のオブジェクトの暗号化タイプを変更するには、Amazon S3 バッチオペレーションを使用できます。S3 バッチオペレーションにオブジェクトのリストを指定すると、バッチオペレーションが対応する API オペレーションを呼び出します。オブジェクトのコピー アクションを使用して既存のオブジェクトをコピーし、SSE-KMS で暗号化されたオブジェクトと同じバケットに書き戻すことができます。1 つのバッチオペレーションジョブで、数十億ものオブジェクトに対して、指定されたオペレーションを実行できます。詳細については、「バッチオペレーションでオブジェクトオペレーションを一括で実行する」および AWS Storage Blog の投稿「How to retroactively encrypt existing objects in Amazon S3 using S3 Inventory, Amazon Athena, and S3 Batch Operations」を参照してください。

オブジェクト作成の REST API を使用してサーバー側の暗号化を設定するには、`x-amz-server-side-encryption` リクエストヘッダーを提供します。REST API の詳細については、REST API の使用 を参照してください。

以下の Amazon S3 API でこのヘッダーがサポートされています。

- PUT オペレーション – PUT API を使用してデータをアップロードする場合は、リクエストヘッダーを指定します。詳細については、「PutObject」を参照してください。
- マルチパートアップロードの開始 — マルチパートアップロード API オペレーションを使用して大きいオブジェクトをアップロードするときに、開始リクエストでヘッダーを指定します。詳細については、Initiate Multipart Upload を参照してください。
- COPY オペレーション – オブジェクトをコピーする場合、ソースオブジェクトとターゲットオブジェクトがあります。詳細については、PUT Object - Copy を参照してください。

> **Note**
>
> POST オペレーションを使用してオブジェクトをアップロードする場合は、リクエストヘッダーを指定する代わりに、フォームフィールドで同じ情報を指定します。詳細については、POST Object を参照してください。

AWS SDK にも、サーバー側の暗号化を要求するために使用できるラッパー API があります。また、AWS Management Console を使用して、オブジェクトをアップロードしてサーバー側の暗号化を要求することもできます。

詳細については、AWS Key Management Service デベロッパーガイドの「AWS KMS の概念」を参照してください。

トピック

- Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3) の指定

Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3) の指定

すべての Amazon S3 バケットにはデフォルトで暗号化が設定されており、S3 バケットにアップロードされたすべての新しいオブジェクトは保存時に自動的に暗号化されます。Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3) は、Amazon S3 のすべてのバケットでのデフォルトの暗号化設定です。別のタイプの暗号化を使用するには、S3 PUT リクエストで使用するサーバー側の暗号化のタイプを指定するか、宛先バケットにデフォルトの暗号化設定を更新できます。

PUT リクエストで別の暗号化タイプを指定する場合は、AWS Key Management Service (AWS KMS) キーによるサーバー側の暗号化 (SSE-KMS)、AWS KMS キーによる二層式サーバー側の暗号化

(DSSE-KMS)、または顧客提供のキーによるサーバー側の暗号化 (SSE-C) を使用できます。宛先バケットに別のデフォルト暗号化設定を設定する場合は、SSE-KMS または DSSE-KMS を使用できます。

汎用バケットのデフォルトの暗号化設定を変更する方法の詳細については、「デフォルトの暗号化の設定」を参照してください。

バケットのデフォルトの暗号化設定を SSE-KMS に変更しても、バケット内の既存の Amazon S3 オブジェクトの暗号化タイプは変更されません。デフォルトの暗号化設定を SSE-KMS に更新した後に既存のオブジェクトの暗号化タイプを変更するには、Amazon S3 バッチオペレーションを使用できます。S3 バッチオペレーションにオブジェクトのリストを指定すると、バッチオペレーションが対応する API オペレーションを呼び出します。オブジェクトのコピー アクションを使用して既存のオブジェクトをコピーし、SSE-KMS で暗号化されたオブジェクトと同じバケットに書き戻すことができます。1 つのバッチオペレーションジョブで、数十億ものオブジェクトに対して、指定されたオペレーションを実行できます。詳細については、「バッチオペレーションでオブジェクトオペレーションを一括で実行する」および AWS Storage Blog の投稿「How to retroactively encrypt existing objects in Amazon S3 using S3 Inventory, Amazon Athena, and S3 Batch Operations」を参照してください。

S3 コンソール、REST API、AWS SDK、および AWS Command Line Interface (AWS CLI) を使用して SSE-S3 を指定できます。詳細については、「Amazon S3 バケット向けのサーバー側のデフォルトの暗号化動作の設定」を参照してください。

S3 コンソールの使用

このトピックでは、AWS Management Console を使用してオブジェクトの暗号化のタイプを設定または変更する方法について説明します。コンソールを使用してオブジェクトをコピーする場合、Amazon S3 はオブジェクトを現状のままコピーします。つまり、ソースが暗号化されている場合、ターゲットオブジェクトも暗号化されます。コンソールを使用して、オブジェクトの暗号化を追加または変更することもできます。

> **Note**
>
> - オブジェクトが 5 GB 未満の場合は、オブジェクトの暗号化を変更できます。オブジェクトが 5 GB を超える場合は、AWS CLI または AWS SDK を使用してオブジェクトの暗号化を変更する必要があります。
> - オブジェクトの暗号化の変更に必要な追加のアクセス許可のリストについては、「the section called “S3 API オペレーションに必要なアクセス許可”」を参照してください。この

アクセス許可を付与するポリシーの例については、「the section called “アイデンティティベースのポリシーの例”」を参照してください。

- オブジェクトの暗号化を変更すると、新しいオブジェクトが作成され、古いオブジェクトが置き換えられます。S3 バージョニングが有効になっている場合は、オブジェクトの新しいバージョンが作成され、既存のオブジェクトが古いバージョンになります。また、プロパティを変更するロールは、新しいオブジェクト (またはオブジェクトのバージョン) の所有者になります。

オブジェクトの暗号化を変更するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ナビゲーションペインで [バケット] を選択してから、[汎用バケット] タブをクリックします。変更するオブジェクトを含む Amazon S3 バケットまたはフォルダに移動します。
3. 変更するオブジェクトのチェックボックスをオンにします。
4. [アクション] メニューに表示されるオプションのリストから [サーバー側の暗号化を編集] を選択します。
5. [サーバー側の暗号化] セクションまでスクロールします。
6. [暗号化設定] で、[デフォルトの暗号化にバケット設定を使用する] または [デフォルトの暗号化にバケット設定を上書きする] を選択します。
7. [デフォルトの暗号化にバケット設定を上書きする] を選択した場合は、次の暗号化設定を設定します。

   - [暗号化タイプ] で、[Amazon S3 マネージドキーを用いたサーバー側の暗号化 (SSE-S3)] を選択します。SSE-S3 は、最強のブロック暗号の 1 つである 256 ビットの 高度暗号化規格 (AES-256) を使用して、各オブジェクトを暗号化します。詳細については、「Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3)」を参照してください。

8. [追加のコピー設定] で、[ソース設定をコピー] するか、[設定を指定しない] か、[設定を指定] するかを選択します。[ソース設定をコピー] がデフォルトのオプションです。ソース設定の属性なしでオブジェクトのみをコピーする場合は、[設定を指定しない] を選択します。ストレージクラス、ACL、オブジェクトタグ、メタデータ、サーバー側の暗号化、その他のチェックサムの設定を指定するには、[設定を指定] を選択します。
9. [Save changes] (変更の保存) をクリックします。

> **Note**
>
> このアクションは、指定されたすべてのオブジェクトに暗号化を適用します。フォルダを暗号化する場合は、保存オペレーションが完了するのを待ってから、フォルダに新しいオブジェクトを追加します。

REST API の使用

オブジェクト作成時、つまり、新しいオブジェクトをアップロードするときや既存オブジェクトのコピーを作成するときに、リクエストに `x-amz-server-side-encryption` ヘッダーを追加することで、Amazon S3 マネージドキー (SSE-S3) を使用してデータを暗号化するかどうかを指定することができます。ヘッダーの値を、Amazon S3 がサポートする暗号化アルゴリズム `AES256` に設定します。Amazon S3 によりレスポンスヘッダー `x-amz-server-side-encryption` が返されるため、SSE-S3 を使用してオブジェクトが保存されたことを確認できます。

次の REST アップロード API オペレーションは、`x-amz-server-side-encryption` リクエストヘッダーを受け付けます。

- PUT Object
- PUT Object – Copy
- POST Object
- Initiate Multipart Upload

マルチパートアップロード API オペレーションを使用して大容量のオブジェクトをアップロードするときに、`x-amz-server-side-encryption` ヘッダーを Initiate Multipart Upload リクエストに追加することでサーバー側の暗号化を指定することができます。既存のオブジェクトをコピーする際は、コピー元オブジェクトが暗号化されているかどうかに関係なく、明示的にサーバー側の暗号化を要求しない限り、コピー先オブジェクトは暗号化されません。

次の REST API オペレーションのレスポンスヘッダーは、オブジェクトが SSE-S3 を使用して保存されているときに `x-amz-server-side-encryption` ヘッダーを返します。

- PUT Object
- PUT Object – Copy
- POST Object
- Initiate Multipart Upload

- Upload Part
- Upload Part – Copy
- Complete Multipart Upload
- Get Object
- Head Object

> **Note**
>
> オブジェクトで SSE-S3 を使用している場合、または、HTTP ステータスコード 400 (BadRequest) エラーが発生する場合、暗号化リクエストヘッダーを `GET` リクエストおよび `HEAD` リクエストに対して送信しないでください。

AWS SDK の使用

AWS SDK を使用して、Amazon S3 マネージド暗号化キー (SSE-S3) を使用するように Amazon S3 にリクエストできます。このセクションでは、AWS SDK を複数の言語で使用する場合の例を示します。他の SDK については、「サンプルコードとライブラリ」を参照してください。

Java

AWS SDK for Java を使用してオブジェクトをアップロードしたら、SSE-S3 を使用してデータを暗号化します。サーバー側の暗号化を要求するには、`ObjectMetadata` の `PutObjectRequest` プロパティを使用して `x-amz-server-side-encryption` リクエストヘッダーを設定します。`AmazonS3Client` の `putObject()` メソッドを呼び出すと、Amazon S3 はデータを暗号化して保存します。

さらに、マルチパートアップロード API オペレーションを使用して、オブジェクトのアップロード時に、SSE-S3 暗号化をリクエストすることもできます。

- 高レベルマルチパートアップロード API オペレーションを使用するときに、`TransferManager` メソッドを使用して、アップロード時にサーバー側の暗号化をオブジェクトに適用できます。パラメータとして `ObjectMetadata` を受け取る、どのアップロードメソッドを使用してもかまいません。詳細については、「マルチパートアップロードを使用したオブジェクトのアップロード」を参照してください。
- 低レベルマルチパートアップロード API オペレーションを使用する場合は、マルチパートアップロードの開始時にサーバー側の暗号化を指定します。`ObjectMetadata` メソッドを呼び出

して InitiateMultipartUploadRequest.setObjectMetadata() プロパティを追加します。詳細については、AWS SDK の使用 (低レベル API) を参照してください。

オブジェクトの暗号化状態を直接変更することはできません (暗号化されていないオブジェクトの暗号化、または暗号化されたオブジェクトの復号)。オブジェクトの暗号化状態を変更するには、オブジェクトのコピーを作成し、コピーの目的の暗号化状態を指定してから、元のオブジェクトを削除します。Amazon S3 は、明示的にサーバー側の暗号化を要求した場合にのみ、コピーされたオブジェクトを暗号化します。Java API を通じて、コピーされたオブジェクトの暗号化を要求するには、ObjectMetadata プロパティを使用して、CopyObjectRequest でサーバー側の暗号化を指定します。

Example 例

次の例は、AWS SDK for Java を使用してサーバー側の暗号化を設定する方法を示しています。ここでは、以下のタスクの実行方法について説明します。

- SSE-S3 を使用して新しいオブジェクトをアップロードします。
- オブジェクトのコピーを作成して、オブジェクトの暗号化状態を変更する (この例では、以前に暗号化されていないオブジェクトを暗号化する)
- オブジェクトの暗号化状態を確認する

サーバーサイドの暗号化の詳細については、「REST API の使用」を参照してください。作業サンプルの作成およびテストの手順については、「AWS SDK for Java のデベロッパーガイド」の「使用開始」を参照してください。

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.internal.SSEResultBase;
import com.amazonaws.services.s3.model.*;

import java.io.ByteArrayInputStream;

public class SpecifyServerSideEncryption {
```

```
   public static void main(String[] args) {
       Regions clientRegion = Regions.DEFAULT_REGION;
       String bucketName = "*** Bucket name ***";
       String keyNameToEncrypt = "*** Key name for an object to upload and encrypt
***";
       String keyNameToCopyAndEncrypt = "*** Key name for an unencrypted object to
be encrypted by copying ***";
       String copiedObjectKeyName = "*** Key name for the encrypted copy of the
unencrypted object ***";

       try {
           AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                   .withRegion(clientRegion)
                   .withCredentials(new ProfileCredentialsProvider())
                   .build();

           // Upload an object and encrypt it with SSE.
           uploadObjectWithSSEEncryption(s3Client, bucketName, keyNameToEncrypt);

           // Upload a new unencrypted object, then change its encryption state
           // to encrypted by making a copy.
           changeSSEEncryptionStatusByCopying(s3Client,
                   bucketName,
                   keyNameToCopyAndEncrypt,
                   copiedObjectKeyName);
       } catch (AmazonServiceException e) {
           // The call was transmitted successfully, but Amazon S3 couldn't process
           // it, so it returned an error response.
           e.printStackTrace();
       } catch (SdkClientException e) {
           // Amazon S3 couldn't be contacted for a response, or the client
           // couldn't parse the response from Amazon S3.
           e.printStackTrace();
       }
   }

   private static void uploadObjectWithSSEEncryption(AmazonS3 s3Client, String
bucketName, String keyName) {
       String objectContent = "Test object encrypted with SSE";
       byte[] objectBytes = objectContent.getBytes();

       // Specify server-side encryption.
       ObjectMetadata objectMetadata = new ObjectMetadata();
       objectMetadata.setContentLength(objectBytes.length);
```

```
objectMetadata.setSSEAlgorithm(ObjectMetadata.AES_256_SERVER_SIDE_ENCRYPTION);
       PutObjectRequest putRequest = new PutObjectRequest(bucketName,
               keyName,
               new ByteArrayInputStream(objectBytes),
               objectMetadata);

       // Upload the object and check its encryption status.
       PutObjectResult putResult = s3Client.putObject(putRequest);
       System.out.println("Object \"" + keyName + "\" uploaded with SSE.");
       printEncryptionStatus(putResult);
   }

   private static void changeSSEEncryptionStatusByCopying(AmazonS3 s3Client,
           String bucketName,
           String sourceKey,
           String destKey) {
       // Upload a new, unencrypted object.
       PutObjectResult putResult = s3Client.putObject(bucketName, sourceKey,
"Object example to encrypt by copying");
       System.out.println("Unencrypted object \"" + sourceKey + "\" uploaded.");
       printEncryptionStatus(putResult);

       // Make a copy of the object and use server-side encryption when storing the
       // copy.
       CopyObjectRequest request = new CopyObjectRequest(bucketName,
               sourceKey,
               bucketName,
               destKey);
       ObjectMetadata objectMetadata = new ObjectMetadata();

objectMetadata.setSSEAlgorithm(ObjectMetadata.AES_256_SERVER_SIDE_ENCRYPTION);
       request.setNewObjectMetadata(objectMetadata);

       // Perform the copy operation and display the copy's encryption status.
       CopyObjectResult response = s3Client.copyObject(request);
       System.out.println("Object \"" + destKey + "\" uploaded with SSE.");
       printEncryptionStatus(response);

       // Delete the original, unencrypted object, leaving only the encrypted copy
in
       // Amazon S3.
       s3Client.deleteObject(bucketName, sourceKey);
       System.out.println("Unencrypted object \"" + sourceKey + "\" deleted.");
```

```
    }

    private static void printEncryptionStatus(SSEResultBase response) {
        String encryptionStatus = response.getSSEAlgorithm();
        if (encryptionStatus == null) {
            encryptionStatus = "Not encrypted with SSE";
        }
        System.out.println("Object encryption status is: " + encryptionStatus);
    }
}
```

.NET

オブジェクトをアップロードするときに、それを暗号化するように Amazon S3 に指定できます。既存のオブジェクトの暗号化状態を変更するには、オブジェクトのコピーを作成し、コピー元オブジェクトを削除します。デフォルトでは、ターゲットオブジェクトのサーバー側の暗号化を明示的に要求した場合、コピーオペレーションではターゲットのみが暗号化されます。`CopyObjectRequest` で SSE-S3 を指定するには、以下を追加します。

```
ServerSideEncryptionMethod = ServerSideEncryptionMethod.AES256
```

オブジェクトのコピー方法を示す作業サンプルについては、AWS SDK の使用 を参照してください。

次の例では、オブジェクトをアップロードします。このリクエストでは、オブジェクトを暗号化するように Amazon S3 に指定します。次に、オブジェクトのメタデータを取得し、使用された暗号化方法を確認します。コード例を設定および実行する方法の詳細については、「AWS SDK for .NET デベロッパーガイド」の「AWS SDK for .NET の開始方法」 を参照してください。

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class SpecifyServerSideEncryptionTest
    {
        private const string bucketName = "*** bucket name ***";
        private const string keyName = "*** key name for object created ***";
```

```
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
RegionEndpoint.USWest2;
        private static IAmazonS3 client;

        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            WritingAnObjectAsync().Wait();
        }

        static async Task WritingAnObjectAsync()
        {
            try
            {
                var putRequest = new PutObjectRequest
                {
                    BucketName = bucketName,
                    Key = keyName,
                    ContentBody = "sample text",
                    ServerSideEncryptionMethod = ServerSideEncryptionMethod.AES256
                };

                var putResponse = await client.PutObjectAsync(putRequest);

                // Determine the encryption state of an object.
                GetObjectMetadataRequest metadataRequest = new
GetObjectMetadataRequest
                {
                    BucketName = bucketName,
                    Key = keyName
                };
                GetObjectMetadataResponse response = await
client.GetObjectMetadataAsync(metadataRequest);
                ServerSideEncryptionMethod objectEncryption =
response.ServerSideEncryptionMethod;

                Console.WriteLine("Encryption method used: {0}",
objectEncryption.ToString());
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered ***. Message:'{0}' when writing
an object", e.Message);
```

```
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
        }
    }
}
```

PHP

このトピックでは、バージョン 3 の AWS SDK for PHP のクラスを使用して、Amazon S3 にアップロードするオブジェクトに SSE-S3 を追加する方法を示します。AWS SDK for Ruby API の詳細については、AWS SDK for Ruby - バージョン 2 を参照してください。

オブジェクトを Amazon S3 にアップロードするには、Aws\S3\S3Client::putObject() メソッドを使用します。アップロードリクエストに x-amz-server-side-encryption リクエストヘッダーを追加するには、ServerSideEncryption パラメータを指定して AES256 値を設定します。以下に例を示します。サーバー側の暗号化のリクエストについては、REST API の使用 を参照してください。

```
 require 'vendor/autoload.php';

use Aws\S3\S3Client;

$bucket = '*** Your Bucket Name ***';
$keyname = '*** Your Object Key ***';

// $filepath should be an absolute path to a file on disk.
$filepath = '*** Your File Path ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

// Upload a file with server-side encryption.
$result = $s3->putObject([
    'Bucket'               => $bucket,
    'Key'                  => $keyname,
    'SourceFile'           => $filepath,
    'ServerSideEncryption' => 'AES256',
```

```
]);
```

レスポンスとして、Amazon S3 は、x-amz-server-side-encryption ヘッダーを返します。このヘッダーには、オブジェクトのデータの暗号化に使用された暗号化アルゴリズムの値が設定されています。

マルチパートアップロード API オペレーションを使用して大容量のオブジェクトをアップロードする場合、以下のように、アップロードするオブジェクトに対して SSE-S3 を指定できます。

- 低レベルのマルチパートアップロード API オペレーションを使用する場合は、Aws\S3\S3Client::createMultipartUpload() メソッドを呼び出すときにサーバー側の暗号化を指定します。リクエストに x-amz-server-side-encryption ヘッダーを追加する場合は、値 array を使用して ServerSideEncryption パラメータの AES256 キーを指定します。低レベルのマルチパートアップロード API オペレーションの詳細については、「AWS SDK の使用 (低レベル API)」を参照してください。
- 高レベルのマルチパートアップロード API オペレーションを使用する場合は、CreateMultipartUpload API オペレーションの ServerSideEncryption パラメータを使用してサーバー側の暗号化を指定します。高レベルのマルチパートアップロード API オペレーションで setOption() メソッドを使用する例については、「マルチパートアップロードを使用したオブジェクトのアップロード」を参照してください。

以下の PHP コード例に示すように、Aws\S3\S3Client::headObject() メソッドを呼び出し、オブジェクトメタデータを取得して、既存のオブジェクトの暗号化状態を確認できます。

```
 require 'vendor/autoload.php';

use Aws\S3\S3Client;

$bucket = '*** Your Bucket Name ***';
$keyname = '*** Your Object Key ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

// Check which server-side encryption algorithm is used.
$result = $s3->headObject([
    'Bucket' => $bucket,
```

```
    'Key'    => $keyname,
]);
echo $result['ServerSideEncryption'];
```

Aws\S3\S3Client::copyObject() メソッドを使用してオブジェクトのコピーを作成し、コピー元のオブジェクトを削除することで、既存のオブジェクトの暗号化状態を変更できます。デフォルトでは、copyObject() によってコピー先は暗号化されません。ただし、ServerSideEncryption パラメータで AES256 値を使用して、コピー先オブジェクトに対するサーバー側の暗号化を明示的にリクエストした場合は除きます。以下の PHP コード例では、オブジェクトのコピーを作成し、コピー先のオブジェクトにサーバー側の暗号化を追加しています。

```
 require 'vendor/autoload.php';

use Aws\S3\S3Client;

$sourceBucket = '*** Your Source Bucket Name ***';
$sourceKeyname = '*** Your Source Object Key ***';

$targetBucket = '*** Your Target Bucket Name ***';
$targetKeyname = '*** Your Target Object Key ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

// Copy an object and add server-side encryption.
$s3->copyObject([
    'Bucket'               => $targetBucket,
    'Key'                  => $targetKeyname,
    'CopySource'           => "$sourceBucket/$sourceKeyname",
    'ServerSideEncryption' => 'AES256',
]);
```

詳細については、以下の各トピックを参照してください。

- Amazon S3 向け AWS SDK for PHP Aws\S3\S3Client クラスの場合
- AWS SDK for PHP ドキュメント

Ruby

AWS SDK for Ruby を使用してオブジェクトをアップロードするときは、SSE-S3 により保管時にオブジェクトを暗号化して保存することを指定できます。オブジェクトは、読み戻すときに自動的に復号されます。

次の AWS SDK for Ruby バージョン 3 のサンプルは、Amazon S3 にアップロードするファイルを保管時に暗号化するよう指定する方法を示しています。

```
require 'aws-sdk-s3'

# Wraps Amazon S3 object actions.
class ObjectPutSseWrapper
  attr_reader :object

  # @param object [Aws::S3::Object] An existing Amazon S3 object.
  def initialize(object)
    @object = object
  end

  def put_object_encrypted(object_content, encryption)
    @object.put(body: object_content, server_side_encryption: encryption)
    true
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't put your content to #{object.key}. Here's why: #{e.message}"
    false
  end
end

# Example usage:
def run_demo
  bucket_name = "amzn-s3-demo-bucket"
  object_key = "my-encrypted-content"
  object_content = "This is my super-secret content."
  encryption = "AES256"

  wrapper = ObjectPutSseWrapper.new(Aws::S3::Object.new(bucket_name,
 object_content))
  return unless wrapper.put_object_encrypted(object_content, encryption)

  puts "Put your content into #{bucket_name}:#{object_key} and encrypted it with
 #{encryption}."
end
```

```
run_demo if $PROGRAM_NAME == __FILE__
```

次のコード例は、既存のオブジェクトの暗号化状態を判定する方法を示しています。

```
require 'aws-sdk-s3'

# Wraps Amazon S3 object actions.
class ObjectGetEncryptionWrapper
  attr_reader :object

  # @param object [Aws::S3::Object] An existing Amazon S3 object.
  def initialize(object)
    @object = object
  end

  # Gets the object into memory.
  #
  # @return [Aws::S3::Types::GetObjectOutput, nil] The retrieved object data if
 successful; otherwise nil.
  def object
    @object.get
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't get object #{@object.key}. Here's why: #{e.message}"
  end
end

# Example usage:
def run_demo
  bucket_name = "amzn-s3-demo-bucket"
  object_key = "my-object.txt"

  wrapper = ObjectGetEncryptionWrapper.new(Aws::S3::Object.new(bucket_name,
 object_key))
  obj_data = wrapper.get_object
  return unless obj_data

  encryption = obj_data.server_side_encryption.nil? ? 'no' :
 obj_data.server_side_encryption
  puts "Object #{object_key} uses #{encryption} encryption."
end

run_demo if $PROGRAM_NAME == __FILE__
```

Amazon S3 に保存されたオブジェクトにサーバー側の暗号化が使用されていない場合、メソッドは `null` を返します。

既存のオブジェクトの暗号化状態を変更するには、オブジェクトのコピーを作成し、コピー元オブジェクトを削除します。デフォルトでは、明示的にサーバー側の暗号化を要求しない限り、コピーメソッドはターゲットを暗号化しません。ターゲットオブジェクトの暗号化を要求するには、次の Ruby コードの例に示すように、オプションのハッシュ引数に `server_side_encryption` 値を指定します。このコード例は、オブジェクトをコピーし、コピーを SSE-S3 で暗号化する方法を示しています。

```
require 'aws-sdk-s3'

# Wraps Amazon S3 object actions.
class ObjectCopyEncryptWrapper
  attr_reader :source_object

  # @param source_object [Aws::S3::Object] An existing Amazon S3 object. This is
 used as the source object for
  #                                        copy actions.
  def initialize(source_object)
    @source_object = source_object
  end

  # Copy the source object to the specified target bucket, rename it with the target
 key, and encrypt it.
  #
  # @param target_bucket [Aws::S3::Bucket] An existing Amazon S3 bucket where the
 object is copied.
  # @param target_object_key [String] The key to give the copy of the object.
  # @return [Aws::S3::Object, nil] The copied object when successful; otherwise,
 nil.
  def copy_object(target_bucket, target_object_key, encryption)
    @source_object.copy_to(bucket: target_bucket.name, key: target_object_key,
 server_side_encryption: encryption)
    target_bucket.object(target_object_key)
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't copy #{@source_object.key} to #{target_object_key}. Here's why:
 #{e.message}"
  end
end

# Example usage:
def run_demo
```

```
  source_bucket_name = "amzn-s3-demo-bucket1"
  source_key = "my-source-file.txt"
  target_bucket_name = "amzn-s3-demo-bucket2"
  target_key = "my-target-file.txt"
  target_encryption = "AES256"

  source_bucket = Aws::S3::Bucket.new(source_bucket_name)
  wrapper = ObjectCopyEncryptWrapper.new(source_bucket.object(source_key))
  target_bucket = Aws::S3::Bucket.new(target_bucket_name)
  target_object = wrapper.copy_object(target_bucket, target_key, target_encryption)
  return unless target_object

  puts "Copied #{source_key} from #{source_bucket_name} to
 #{target_object.bucket_name}:#{target_object.key} and "\
       "encrypted the target with #{target_object.server_side_encryption}
 encryption."
end

run_demo if $PROGRAM_NAME == __FILE__
```

AWS CLI を使用する場合

AWS CLI を使用してオブジェクトをアップロードするときに SSE-S3 を指定するには、次の例を使用します。

```
aws s3api put-object --bucket amzn-s3-demo-bucket1 --key object-key-name --server-side-encryption AES256  --body file path
```

詳細については、AWS CLI リファレンスの put-object を参照してください。AWS CLI を使用してオブジェクトをコピーするときに SSE-S3 を指定するには、copy-object を参照してください。

AWS CloudFormation の使用

AWS CloudFormation を使用して暗号化を設定する例については、AWS CloudFormation ユーザーガイドの AWS::S3::Bucket ServerSideEncryptionRule トピックの「デフォルト暗号化を備えたバケットの作成」および「AWS KMS サーバー側の暗号化と S3 バケットキーを使用したバケットの作成」の例を参照してください。

AWS KMS キーによるサーバー側の暗号化 (SSE-KMS) の使用

> **Important**
>
> Amazon S3 では、Amazon S3 内のすべてのバケットの基本レベルの暗号化として、Amazon S3 が管理するキー (SSE-S3) によるサーバー側の暗号化が適用されるようになりました。2023 年 1 月 5 日以降、Amazon S3 にアップロードされるすべての新しいオブジェクトは、追加費用なしで、パフォーマンスに影響を与えずに自動的に暗号化されます。S3 バケットのデフォルト暗号化設定と新しいオブジェクトのアップロードのための自動暗号化ステータスは、AWS CloudTrail ログ、S3 インベントリ、S3 ストレージレンズ、Amazon S3 コンソール、および AWS Command Line Interface と AWS SDK の追加の Amazon S3 API レスポンスヘッダーとして利用できるようになりました。詳細については、「デフォルト暗号化に関するよくある質問」を参照してください。

サーバー側の暗号化とは、データを受信するアプリケーションまたはサービスによって、送信先でデータを暗号化することです。

Amazon S3 は、新しいオブジェクトをアップロードするときに、Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3) を自動的に有効にします。

特に指定しない限り、バケットはデフォルトで SSE-S3 を使用してオブジェクトを暗号化します。ただし、代わりにAWS Key Management Service (AWS KMS) キーによるサーバー側の暗号化 (SSE-KMS) を使用するようにバケットを設定することもできます。詳細については、「AWS KMS (SSE-KMS) によるサーバー側の暗号化の指定」を参照してください。

AWS KMS は、安全で可用性の高いハードウェアおよびソフトウェアを結合するサービスであり、クラウド向けに拡張されたキー管理システムを提供します。Amazon S3 は、AWS KMS (SSE-KMS) によるサーバー側の暗号化を使用して、S3 オブジェクトデータを暗号化します。また、オブジェクトに対して SSE-KMS をリクエストすると、オブジェクトのメタデータの一部としての S3 チェックサムが暗号化された形式で保存されます。チェックサムの詳細については、「Amazon S3 でのオブジェクトの整合性のチェック」を参照してください。

KMS キーを使用すると、AWS Management Console または AWS KMS API から AWS KMS を使用して、以下の操作を実行できます。

- KMS キーの作成、表示、編集、監視、有効化または無効化、更新、削除のスケジュールを一元的に行う。

- KMS キーの使用方法および使用者を制御するポリシーを定義する。
- KMS キーの正しい使用状況を監査します。監査は AWS KMS API ではサポートされていますが、AWS KMS コンソールではサポートされていません。

AWS KMS のセキュリティ制御は、暗号化関連のコンプライアンス要件を満たすのに役立ちます。これらの KMS キーを使用して、Amazon S3 バケットのデータを保護できます。S3 バケットで SSE-KMS 暗号化を使用する場合、AWS KMS keys はバケットと同じリージョンに存在する必要があります。

AWS KMS keysを使用するための追加料金はかかります。詳細については、AWS Key Management Service デベロッパーガイドの AWS KMS key の概念およびAWS KMS の料金を参照してください。

IAM ユーザーが KMS で暗号化されたバケットにアクセスできるようにする手順については、「私の Amazon S3 バケットにはカスタムの AWSAWS KMS キーを使用したデフォルト暗号化が設定されています。ユーザーがそのバケットでダウンロードやアップロードを行えるようにするにはどうすればいいですか」を AWS re:Post 情報センターで参照してください。

アクセス許可

AWS KMS キーを使用して、オブジェクトを Amazon S3 に暗号化する `PutObject` リクエストを正常に実行するには、キーに対する `kms:GenerateDataKey` アクセス許可が必要です。AWS KMS key を使用して暗号化されたオブジェクトをダウンロードするには、キーに対して `kms:Decrypt` の許可が必要です。マルチパートアップロードを実行して AWS KMS key でオブジェクトを暗号化するには、キーの `kms:GenerateDataKey` および `kms:Decrypt` アクセス許可が必要です。

> **Important**
>
> KMS キーポリシーで付与されているアクセス権限を慎重に確認します。カスタマーマネージド AWS KMS キーのポリシーのアクセス許可は常に、関連するキーアクションにアクセスする必要がある IAM プリンシパルと AWS サービスのみに限定する必要があります。詳細については、「AWS KMS のキーポリシー」を参照してください。

トピック

- AWS KMS keys
- Amazon S3 バケットキー

- サーバー側の暗号化の要求
- 暗号化コンテキスト
- AWS KMS 暗号化されたオブジェクトへのリクエストの送信
- AWS KMS (SSE-KMS) によるサーバー側の暗号化の指定
- Amazon S3 バケットキーを使用した SSE-KMS のコストの削減

AWS KMS keys

AWS KMS によるサーバー側暗号化 (SSE-KMS) を使用すると、デフォルトの AWS マネージドキーを使用するか、または、作成済みのカスタマーマネージドキーを指定できます。AWS KMS はエンベロープ暗号化をサポートします。S3 は、エンベロープ暗号化の AWS KMS 機能を使用してデータを保護します。エンベロープ暗号化は、データキーでプレーンテキストデータを暗号化してから、そのデータキーを KMS キーで暗号化する手法です。エンベロープ暗号化の仕組みの詳細については、AWS Key Management Service デベロッパーガイドの「エンベロープ暗号化」を参照してください。

カスタマーマネージドキーを指定しない場合、SSE-KMS で暗号化されたオブジェクトをバケットに初めて追加するとき、Amazon S3 によって自動的に AWS アカウント に AWS マネージドキー が作成されます。デフォルトでは、Amazon S3 はこの KMS キーを SSE-KMS に使用します。

> **Note**
>
> SSE-KMS を AWS マネージドキー で使用して暗号化されたオブジェクトは、クロスアカウントで共有できません。SSE-KMS データをアカウント間で共有する必要がある場合は、AWS KMS のカスタマーマネージドキーを使用する必要があります。

SSE-KMS にカスタマーマネージドキーを使用する場合は、SSE-KMS を設定する前に対称暗号化カスタマーマネージドキーを作成します。次に、バケット用に SSE-KMS を設定するときに、既存のカスタマーマネージドキーを指定します。対象暗号化キーの詳細については、「AWS Key Management Service デベロッパーガイド」の「対称暗号化 KMS キー」を参照してください。

カスタマーマネージドキーを独自に作成することで、より柔軟に制御を行えます。例えば、カスタマーマネージドキーを作成、ローテーション、無効化することができます。また、アクセスコントロールを定義し、データを保護するために使用するカスタマーマネージドキーを監査することもできます。カスタマーマネージドキーおよび AWS マネージドキーの詳細については、「AWS Key

Management Service デベロッパーガイド」の「カスタマーキーおよび AWS キー」を参照してください。

> **Note**
>
> 標準の KMS キーとは異なり、外部のキーストアに保存されているカスタマーマネージドキーによるサーバー側の暗号化を使用する場合は、キーマテリアルの可用性と耐久性を確保する責任があります。外部キーストアと、それらによって責任分担モデルがどのように変化するかについての詳細は、「AWS Key Management Service デベロッパーガイド」の「外部キーストア」を参照してください。

クロスアカウント操作での SSE-KMS 暗号化の使用

クロスアカウント操作で暗号化を使用する場合は、次の点に注意してください。

- AWS KMS key Amazon リソースネーム (ARN) またはエイリアスがリクエスト時またはバケットのデフォルト暗号化設定によって提供されない場合は、AWS マネージドキー (`aws/s3`) が使用されます。
- KMS キーと同じ AWS アカウント の AWS Identity and Access Management (IAM) プリンシパルを使用して S3 オブジェクトをアップロードまたはアクセスする場合は、AWS マネージドキー (`aws/s3`) を使用できます。
- S3 オブジェクトにクロスアカウントアクセスを許可する場合は、カスタマーマネージドキーを使用します。カスタマーマネージドキーのポリシーを設定して、別のアカウントからのアクセスを許可することができます。
- カスタマーマネージド KMS キーを指定している場合、完全修飾 KMS キー ARN を使用することをお勧めします。代わりに KMS キーエイリアスを使用する場合、AWS KMS はリクエスタのアカウント内でキーを解決します。この動作により、バケット所有者ではなく、リクエスタに属する KMS キーでデータが暗号化される可能性があります。
- お客様 (リクエスタ) が `Encrypt` アクセス許可を付与されているキーを指定する必要があります。詳細については、AWS Key Management Service デベロッパーガイドの「キーユーザーが暗号化オペレーションに KMS キーを使用することを許可する」を参照してください。

カスタマーマネージドキーと AWS マネージド KMS キーをどのような場合に使用するかの詳細については、「Amazon S3 にあるオブジェクトの暗号化に AWS マネージドキー、またはカスタマーマネージドキーを使うべきですか」を参照してください。

SSE-KMS 暗号化ワークフロー

AWS マネージドキー またはカスタマーマネージドキーを使用してデータの暗号化を選択する場合は、AWS KMS および Amazon S3 は次のエンベロープ暗号化アクションを実行します。

1. Amazon S3 は、プレーンテキストのデータキーおよび指定された KMS キーで暗号化されたキーのコピーをリクエストします。
2. AWS KMS は、データキーを生成し、KMS キーで暗号化して、プレーンテキストデータキーと暗号化されたデータキーの両方を Amazon S3 に送信します。
3. Amazon S3 は、データキーを使用してデータを暗号化し、使用後はメモリからプレーンテキストのキーをできる限り迅速に削除します。
4. Amazon S3 は、暗号化されたデータキーを、暗号化されたデータのメタデータとして保存します。

データの復号をリクエストすると、Amazon S3 と AWS KMS は次のアクションを実行します。

1. `Decrypt` リクエストがあると、Amazon S3 は暗号化されたデータキーを AWS KMS に送信します。
2. AWS KMS は、同じ KMS キーを使用して暗号化データキーを復号し、プレーンテキストのデータキーを Amazon S3 に返します。
3. Amazon S3 は、プレーンテキストデータキーを使用して暗号化されたデータを復号し、できるだけ早くプレーンテキストデータキーをメモリから削除します。

> **Important**
>
> Amazon S3 でサーバー側の暗号化に AWS KMS key を使用する場合は、対称暗号化 KMS キーを選択する必要があります。Amazon S3 は、対称暗号化 KMS キーのみをサポートします。このキーの詳細については、「AWS Key Management Service デベロッパーガイド」の「対称暗号化 KMS キー」を参照してください。

SSE-KMS 暗号化の監査

SSE-KMS を指定するリクエストを識別するには、Amazon S3 ストレージレンズメトリクスの「すべての SSE-KMS リクエスト」と「すべての SSE-KMS リクエストの割合 (%)」メトリクスを使用できます。S3 ストレージレンズは、オブジェクトストレージの使用状況とアクティビティを組織全体

で可視化するために使用できるクラウドストレージ分析機能です。SSE-KMS 対応バケット数と % SSE-KMS 対応バケットを使用して、デフォルトのバケット暗号化 のバケット数 (SSE-KMS) を把握することもできます。詳細については、「S3 Storage Lens を使用したストレージのアクティビティと使用状況の評価」を参照してください。メトリクスの完全なリストについては、「S3 ストレージレンズメトリクスに関する用語集」を参照してください。

SSE-KMS で暗号化されたデータの AWS KMS キーの使用状況を監査するには、AWS CloudTrail ログを使用します。GenerateDataKey や Decrypt などの暗号化オペレーションに関するインサイトを得ることができます。CloudTrail は、イベント名、ユーザー名、イベントソースなど、検索をフィルタリングするための多数の属性値をサポートしています。

Amazon S3 バケットキー

AWS KMS (SSE-KMS) を使用してサーバー側の暗号化を設定する場合、SSE-KMS で S3 バケットキーを使用するようにバケットを設定できます。SSE-KMS でこのバケットレベルのキーを使用すると、Amazon S3 から AWS KMS へのリクエストトラフィックを減らすことにより、AWS KMS のリクエストコストを最大 99% 削減できます。

新しいオブジェクトで SSE-KMS の S3 バケットキーを使用するようにバケットを設定すると、AWS KMS によりバケットレベルのキーが生成されます。このキーは、バケット内のオブジェクトの一意のデータキーを作成するために使用されます。この S3 バケットキーは Amazon S3 内で期間限定で使用されるため、Amazon S3 で AWS KMS にリクエストを実行し、暗号化オペレーションを完了する必要性が軽減されます。S3 バケットキーの使用の詳細については、Amazon S3 バケットキーを使用した SSE-KMS のコストの削減 を参照してください。

サーバー側の暗号化の要求

特定の Amazon S3 バケット内のすべてのオブジェクトのサーバー側の暗号化を要求するには、バケットポリシーを使用できます。例えば、SSE-KMS を使用したサーバー側の暗号化を要求する `x-amz-server-side-encryption-aws-kms-key-id` ヘッダーがリクエストに含まれていない場合、次のバケットポリシーはすべてのユーザーに対し、オブジェクト (`s3:PutObject`) をアップロードするアクセス許可を拒否します。

```
{
   "Version":"2012-10-17",
   "Id":"PutObjectPolicy",
   "Statement":[{
         "Sid":"DenyObjectsThatAreNotSSEKMS",
         "Effect":"Deny",
         "Principal":"*",
```

```
         "Action":"s3:PutObject",
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1/*",
         "Condition":{
            "Null":{
               "s3:x-amz-server-side-encryption-aws-kms-key-id":"true"
            }
         }
      }
   ]
}
```

特定の AWS KMS key を使用してバケット内のオブジェクトを暗号化することを要求するには、`s3:x-amz-server-side-encryption-aws-kms-key-id` 条件キーを使用できます。KMS キーを指定するには、キーの Amazon リソースネーム (ARN) を `arn:aws:kms:region:acct-id:key/key-id` 形式で使用する必要があります。AWS Identity and Access Management は、`s3:x-amz-server-side-encryption-aws-kms-key-id` の文字列が存在するかどうかを検証しません。

> **Note**
>
> オブジェクトをアップロードするときは、`x-amz-server-side-encryption-aws-kms-key-id` ヘッダーを使用して KMS キーを指定するか、デフォルトのバケット暗号化設定を使用できます。PutObject リクエストで `x-amz-server-side-encryption` ヘッダーに `aws:kms` を指定し、`x-amz-server-side-encryption-aws-kms-key-id` ヘッダーを指定しないと、AWS マネージドキーを使用するものと仮定されます。その場合でも、Amazon S3 がオブジェクトの暗号化に使用する AWS KMS キー ID とポリシーの AWS KMS キー ID は一致する必要があります。一致しない場合、Amazon S3 はリクエストを拒否します。

Amazon S3 固有の条件キーの完全なリストについては、「サービス認可リファレンス」の「Condition keys for Amazon S3」を参照してください。

暗号化コンテキスト

暗号化コンテキストは、データに関する追加のコンテキスト情報が含まれたキーと値のペアのセットです。この暗号化コンテキストは暗号化されていません。暗号化オペレーションで暗号化コンテキストを指定すると、Amazon S3 では同じ暗号化コンテキストを復号オペレーションに指定する必要があります。そうでない場合は、復号に失敗します。AWS KMS は、暗号化コンテキストを追加の認証

データ (AAD) として使用し、認証された暗号化をサポートします。暗号化コンテキストの詳細については、「AWS Key Management Service デベロッパーガイド」の「暗号化コンテキスト」を参照してください。

デフォルトでは、Amazon S3 は、オブジェクトまたはバケットの Amazon リソースネーム (ARN) を暗号化コンテキストペアとして使用します。

- S3 バケットキーを有効にせずに SSE-KMS を使用する場合は、オブジェクト ARN を暗号化コンテキストとして使用します。

```
arn:aws:s3:::object_ARN
```

- S3 バケットキーを有効にして SSE-KMS を使用する場合は、暗号化コンテキストとしてバケット ARN を使用します。S3 バケットキーの詳細については、Amazon S3 バケットキーを使用した SSE-KMS のコストの削減 を参照してください。

```
arn:aws:s3:::bucket_ARN
```

s3:PutObject リクエストの `x-amz-server-side-encryption-context` のヘッダーを使って、オプションで追加の暗号化コンテキストペアを指定することができます。しかし、暗号化コンテキストは暗号化されないため、機密情報を含めないでください。Amazon S3 は、この追加のキーペアをデフォルトの暗号化コンテキストとともに保存します。PUT リクエストを処理すると、Amazon S3 は `aws:s3:arn` のデフォルトの暗号化コンテキストを、指定するものに追加します。

暗号化コンテキストを使用して、暗号化オペレーションを識別および分類できます。デフォルトの暗号化コンテキスト ARN 値を使用して、どの Amazon S3 ARN がどの暗号化キーで使用されたかを確認することで、AWS CloudTrail の関連するリクエストを追跡することもできます。

CloudTrail ログファイルの `requestParameters` フィールドでは、暗号化コンテキストは次のようになります。

```
"encryptionContext": {
    "aws:s3:arn": "arn:aws:s3:::amzn-s3-demo-bucket1/file_name"
}
```

SSE-KMS をオプションの S3 バケットキー機能とともに使用すると、暗号化コンテキストの値はバケットの ARN になります。

```
"encryptionContext": {
```

```
    "aws:s3:arn": "arn:aws:s3:::amzn-s3-demo-bucket1"
}
```

AWS KMS 暗号化されたオブジェクトへのリクエストの送信

> **Important**
>
> AWS KMS により暗号化されたオブジェクトに対するすべての GET および PUT リクエストは、Secure Sockets Layer (SSL) または Transport Layer Security (TLS) を使用して生成する必要があります。また、各リクエストは、AWS 署名バージョン 4 (または AWS 署名バージョン 2) のような有効な認証情報を使用して署名する必要もあります。

AWS Signature Version 4 は、HTTP で送信される AWS リクエストに認証情報を追加するプロセスです。セキュリティ対策として、AWS へのほとんどのリクエストは、アクセスキーを使用して署名する必要があります。アクセスキーは、アクセスキー ID とシークレットアクセスキーで構成されます。これらの 2 つのキーは、一般的にセキュリティ認証情報と呼ばれます。詳細については、「リクエストの認証 (AWS 署名バージョン 4)」および「署名バージョン 4 の署名プロセス」を参照してください。

> **Important**
>
> オブジェクトで SSE-KMS を使用している場合、GET リクエストおよび HEAD リクエストに対して暗号化リクエストヘッダーを送信しないでください。そうしないと、HTTP 400 Bad Request エラーが表示されます。

トピック

- AWS KMS (SSE-KMS) によるサーバー側の暗号化の指定
- Amazon S3 バケットキーを使用した SSE-KMS のコストの削減

AWS KMS (SSE-KMS) によるサーバー側の暗号化の指定

すべての Amazon S3 バケットにはデフォルトで暗号化が設定されており、S3 バケットにアップロードされたすべての新しいオブジェクトは保存時に自動的に暗号化されます。Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3) は、Amazon S3 のすべてのバケットでのデフォルトの暗号化設定です。別のタイプの暗号化を使用するには、S3 PUT リクエストで使用するサーバー側の暗号化のタイプを指定するか、宛先バケットにデフォルトの暗号化設定を更新できます。

PUT リクエストで別の暗号化タイプを指定する場合は、AWS Key Management Service (AWS KMS) キーによるサーバー側の暗号化 (SSE-KMS)、AWS KMS キーによる二層式サーバー側の暗号化 (DSSE-KMS)、または顧客提供のキーによるサーバー側の暗号化 (SSE-C) を使用できます。宛先バケットに別のデフォルト暗号化設定を設定する場合は、SSE-KMS または DSSE-KMS を使用できます。

汎用バケットのデフォルトの暗号化設定を変更する方法の詳細については、「デフォルトの暗号化の設定」を参照してください。

バケットのデフォルトの暗号化設定を SSE-KMS に変更しても、バケット内の既存の Amazon S3 オブジェクトの暗号化タイプは変更されません。デフォルトの暗号化設定を SSE-KMS に更新した後に既存のオブジェクトの暗号化タイプを変更するには、Amazon S3 バッチオペレーションを使用できます。S3 バッチオペレーションにオブジェクトのリストを指定すると、バッチオペレーションが対応する API オペレーションを呼び出します。オブジェクトのコピー アクションを使用して既存のオブジェクトをコピーし、SSE-KMS で暗号化されたオブジェクトと同じバケットに書き戻すことができます。1 つのバッチオペレーションジョブで、数十億ものオブジェクトに対して、指定されたオペレーションを実行できます。詳細については、「バッチオペレーションでオブジェクトオペレーションを一括で実行する」および AWS Storage Blog の投稿「How to retroactively encrypt existing objects in Amazon S3 using S3 Inventory, Amazon Athena, and S3 Batch Operations」を参照してください。

Amazon S3 コンソール、REST API オペレーション、AWS SDK、および AWS Command Line Interface (AWS CLI) を使用して SSE-KMS を指定できます。詳細については、以下のトピックを参照してください。

> **Note**
>
> Amazon S3 では、マルチリージョン AWS KMS keys を使用できます。ただし、Amazon S3 では現在、マルチリージョンキーは、単一リージョンキーであるかのように処理され、キーのマルチリージョン特徴は使用しません。詳細については、「AWS Key Management Service デベロッパーガイド」の「Using multi-Region keys」を参照してください。

> **Note**
>
> 別のアカウントが所有している KMS キーを使用する場合は、そのキーを使用するアクセス許可が必要です。KMS キーのクロスアカウント権限の詳細については、AWS Key

Management Service デベロッパーガイドの「他のアカウントで使用できる KMS キーを作成する」を参照してください。

S3 コンソールの使用

このトピックでは、Amazon S3 コンソールを使用して、AWS Key Management Service (AWS KMS) キーによるサーバー側の暗号化 (SSE-KMS) を使用するようにオブジェクトの暗号化のタイプを設定または変更する方法について説明します。

Note

- オブジェクトが 5 GB 未満の場合は、オブジェクトの暗号化を変更できます。オブジェクトが 5 GB を超える場合は、AWS CLI または AWS SDK を使用してオブジェクトの暗号化を変更する必要があります。
- オブジェクトの暗号化の変更に必要な追加のアクセス許可のリストについては、「the section called “S3 API オペレーションに必要なアクセス許可”」を参照してください。このアクセス許可を付与するポリシーの例については、「the section called “アイデンティティベースのポリシーの例”」を参照してください。
- オブジェクトの暗号化を変更すると、新しいオブジェクトが作成され、古いオブジェクトが置き換えられます。S3 バージョニングが有効になっている場合は、オブジェクトの新しいバージョンが作成され、既存のオブジェクトが古いバージョンになります。また、プロパティを変更するロールは、新しいオブジェクト (またはオブジェクトのバージョン) の所有者になります。

オブジェクトの暗号化を追加または変更するには

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. ナビゲーションペインで [バケット] を選択してから、[汎用バケット] タブをクリックします。変更するオブジェクトを含む Amazon S3 バケットまたはフォルダに移動します。
3. 変更するオブジェクトのチェックボックスをオンにします。
4. [アクション] メニューに表示されるオプションのリストから [サーバー側の暗号化を編集] を選択します。
5. [サーバー側の暗号化] セクションまでスクロールします。

6. [暗号化設定] で、[デフォルトの暗号化にバケット設定を使用する] または [デフォルトの暗号化にバケット設定を上書きする] を選択します。

> **Important**
>
> デフォルト暗号化設定に SSE-KMS オプションを使用する場合、AWS KMS の 1 秒あたりのリクエスト (RPS) 制限が適用されます。AWS KMS クォータの詳細およびクォータの引き上げをリクエストする方法については、AWS Key Management Service デベロッパーガイドの「クォータ」を参照してください。

7. [デフォルトの暗号化にバケット設定を上書きする] を選択した場合は、次の暗号化設定を設定します。

   a. [暗号化タイプ] で、[AWS Key Management Service キーによるサーバー側の暗号化 (SSE-KMS)] を選択します。

   b. [AWS KMS キー] で、次のいずれかを実行して KMS キーを選択します。

   - 使用可能な KMS キーのリストから選択するには、[AWS KMS keys から選択する] を選択し、使用可能なキーのリストから自分の KMS キーを選択します。

     AWS マネージドキー (aws/s3) とカスタマーマネージドキーの両方がこのリストに表示されます。カスタマーマネージドキーの詳細については、AWS Key Management Service デベロッパーガイドの「カスタマーキーと AWS キー」を参照してください。

   - KMS キー ARN を入力するには、[AWS KMS key ARN を入力] を選択し、表示されるフィールドに KMS キー ARN を入力します。

   - AWS KMS コンソールで新しいカスタマーマネージドキーを作成するには、[KMS キーを作成] を選択します。

     AWS KMS key の作成の詳細については、「AWS Key Management Service デベロッパーガイド」の「キーの作成」を参照してください。

> **Important**
>
> バケットと同じ AWS リージョン で使用可能な KMS キーのみを使用できます。Amazon S3 コンソールには、バケットと同じリージョンで最初の 100 個の KMS キーしか表示されません。リストに存在しない KMS キーを使用するには、KMS キー ARN を入力する必要があります。別のアカウントが所有している

KMS キーを使用する場合は、まずそのキーを使用するアクセス許可が必要であり、次に KMS キー ARN を入力する必要があります。
Amazon S3 では、対称暗号化 KMS キーのみがサポートされ、非対称暗号化 KMS キーはサポートされません。詳細については、AWS Key Management Service デベロッパーガイドの「Identifying symmetric and asymmetric KMS keys」(対称および非対称 KMS キーの識別) を参照してください。

8. [追加のコピー設定] で、[ソース設定をコピー] するか、[設定を指定しない] か、[設定を指定] するかを選択します。[ソース設定をコピー] がデフォルトのオプションです。ソース設定の属性なしでオブジェクトのみをコピーする場合は、[設定を指定しない] を選択します。ストレージクラス、ACL、オブジェクトタグ、メタデータ、サーバー側の暗号化、その他のチェックサムの設定を指定するには、[設定を指定] を選択します。
9. [Save changes] (変更の保存) をクリックします。

> **Note**
>
> このアクションは、指定されたすべてのオブジェクトに暗号化を適用します。フォルダを暗号化する場合は、保存オペレーションが完了するのを待ってから、フォルダに新しいオブジェクトを追加します。

REST API の使用

オブジェクトを作成するとき (新しいオブジェクトをアップロードするか、既存のオブジェクトをコピーするとき) に、AWS KMS keys (SSE-KMS) を使用したサーバー側の暗号化の使用を指定してデータを暗号化できます。これを行うには、リクエストに `x-amz-server-side-encryption` ヘッダーを追加します。ヘッダーの値を、暗号化アルゴリズム `aws:kms` に設定します。Amazon S3 によりレスポンスヘッダー `x-amz-server-side-encryption` が返されるため、SSE-KMS を使用してオブジェクトが保存されたことを確認できます。

`aws:kms` の値で `x-amz-server-side-encryption` ヘッダーを指定する場合は、次のリクエストヘッダーも使用できます。

- `x-amz-server-side-encryption-aws-kms-key-id`
- `x-amz-server-side-encryption-context`
- `x-amz-server-side-encryption-bucket-key-enabled`

トピック

- SSE-KMS をサポートする Amazon S3 REST API オペレーション
- 暗号化コンテキスト (x-amz-server-side-encryption-context)
- AWS KMS キー ID (x-amz-server-side-encryption-aws-kms-key-id)
- S3 バケットキー (x-amz-server-side-encryption-aws-bucket-key-enabled)

SSE-KMS をサポートする Amazon S3 REST API オペレーション

次の REST API オペレーションでは `x-amz-server-side-encryption`、`x-amz-server-side-encryption-aws-kms-key-id`、および `x-amz-server-side-encryption-context` リクエストヘッダーを受け入れます。

- PutObject - PUT オペレーションを使用してデータをアップロードするとき、これらのリクエストヘッダーを指定できます。
- CopyObject — オブジェクトをコピーするときには、ソースオブジェクトとターゲットオブジェクトの両方があります。CopyObject オペレーションで SSE-KMS ヘッダーを渡す場合は、ターゲットオブジェクトにのみ適用されます。既存のオブジェクトをコピーする際は、コピー元オブジェクトが暗号化されているかどうかに関係なく、明示的にサーバー側の暗号化を要求しない限り、コピー先オブジェクトは暗号化されません。
- POST Object — POST オペレーションを使用してオブジェクトをアップロードするときには、リクエストヘッダーの代わりに、フォームフィールドで同じ情報を指定します。
- CreateMultipartUpload — マルチパートアップロード API オペレーションを使用して大きいオブジェクトをアップロードする場合、これらのヘッダーを指定できます。これらのヘッダーを `CreateMultipartUpload` リクエストで指定します。

次の REST API オペレーションのレスポンスヘッダーは、オブジェクトがサーバー側の暗号化を使用して保存されているときに `x-amz-server-side-encryption` ヘッダーを返します。

- PutObject
- CopyObject
- POST Object
- CreateMultipartUpload
- UploadPart
- UploadPartCopy

- CompleteMultipartUpload
- GetObject
- HeadObject

> **Important**
>
> - AWS KMS で保護されたオブジェクトに対する GET リクエストと PUT リクエストはすべて、Secure Sockets Layer (SSL)、Transport Layer Security (TLS)、または署名バージョン 4 を使用していない場合、失敗します。
> - オブジェクトで SSE-KMS を使用している場合、GET リクエストおよび HEAD リクエストに対して暗号化リクエストヘッダーを送信しないでください。送信すると、HTTP 400 BadRequest エラーが発生します。

暗号化コンテキスト (**x-amz-server-side-encryption-context**)

`x-amz-server-side-encryption:aws:kms` を指定した場合、Amazon S3 API は `x-amz-server-side-encryption-context` ヘッダーの暗号化コンテキストをサポートします。暗号化コンテキストは、データに関する追加のコンテキスト情報が含まれたキーバリューペアのセットです。

Amazon S3 は、オブジェクトまたはバケットの Amazon リソースネーム (ARN) を暗号化コンテキストペアとして自動的に使用します。S3 バケットキーを有効にせずに SSE-KMS を使用する場合は、オブジェクト ARN を暗号化コンテキストとして使用します。例えば、`arn:aws:s3:::`*`object_ARN`* です。ただし、S3 バケットキーを有効にして SSE-KMS を使用する場合は、バケット ARN を暗号化コンテキストに使用します。例えば、`arn:aws:s3:::`*`bucket_ARN`* です。

オプションで、`x-amz-server-side-encryption-context` ヘッダーを使用して、追加の暗号化コンテキストペアを指定することもできます。しかし、暗号化コンテキストは暗号化されないため、機密情報を含めないでください。Amazon S3 は、この追加のキーペアをデフォルトの暗号化コンテキストとともに保存します。

Amazon S3 の暗号化コンテキストの詳細については、「暗号化コンテキスト」を参照してください。暗号化コンテキストの一般的な情報については、「AWS Key Management Service デベロッパーガイド」の「AWS Key Management Service Concepts - Encryption context」を参照してください。

AWS KMS キー ID (**`x-amz-server-side-encryption-aws-kms-key-id`**)

`x-amz-server-side-encryption-aws-kms-key-id` ヘッダーを使用して、データの保護に使用するカスタマーマネージドキーの ID を指定できます。`x-amz-server-side-encryption:aws:kms` ヘッダーを指定しても `x-amz-server-side-encryption-aws-kms-key-id` ヘッダーを指定しない場合、Amazon S3 は AWS マネージドキー (`aws/s3`) を使用してデータを保護します。カスタマーマネージドキーを使用する場合は、カスタマーマネージドキーの `x-amz-server-side-encryption-aws-kms-key-id` ヘッダーを指定する必要があります。

> **Important**
>
> Amazon S3 でサーバー側の暗号化に AWS KMS key を使用する場合は、対称暗号化 KMS キーを選択する必要があります。Amazon S3 は、対称暗号化 KMS キーのみをサポートします。このキーの詳細については、「AWS Key Management Service デベロッパーガイド」の「対称暗号化 KMS キー」を参照してください。

S3 バケットキー (**`x-amz-server-side-encryption-aws-bucket-key-enabled`**)

`x-amz-server-side-encryption-aws-bucket-key-enabled` リクエストヘッダーを使用して、オブジェクトレベルで S3 バケットキーを有効または無効にできます。S3 バケットキーで、Amazon S3 から AWS KMS へのリクエストトラフィックを減らすことにより、AWS KMS リクエストコストを削減できます。詳細については、「Amazon S3 バケットキーを使用した SSE-KMS のコストの削減」を参照してください。

`x-amz-server-side-encryption:aws:kms` ヘッダーを指定しても、`x-amz-server-side-encryption-aws-bucket-key-enabled` は指定しない場合、オブジェクトは送信先バケットの S3 バケットキーの設定を使用して、オブジェクトを暗号化します。詳細については、「オブジェクトレベルで S3 バケットキーを設定する」を参照してください。

AWS CLI の使用

次の AWS CLI コマンド例を使用する際は、*`user input placeholders`* をユーザー自身の情報に置き換えます。

新しいオブジェクトをアップロードするか、既存のオブジェクトをコピーするときに、AWS KMS キーを使用したサーバー側の暗号化の使用を指定してデータを暗号化できます。これを行うには、リクエストに `--server-side-encryption aws:kms` ヘッダーを追加します。`--ssekms-key-id` *`example-key-id`*を使用して、作成したカスタマーマネージド AWS KMS キーを追加します。AWS

KMS キー ID を指定せずに `--server-side-encryption aws:kms` を指定した場合、Amazon S3 は AWS マネージドキーを使用します。

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key example-object-key --server-
side-encryption aws:kms --ssekms-key-id example-key-id --body filepath
```

さらに、`--bucket-key-enabled` または `--no-bucket-key-enabled` を追加することで、PUT または COPY オペレーションで Amazon S3 バケットキーを有効または無効にできます。S3 バケットキーで、Amazon S3 から AWS KMS へのリクエストトラフィックを減らすことにより、AWS KMS リクエストコストを削減できます。詳細については、「Amazon S3 バケットキーを使用した SSE-KMS のコストの削減」を参照してください。

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key example-object-key --server-
side-encryption aws:kms --bucket-key-enabled --body filepath
```

暗号化されていないオブジェクトを元の場所にコピーすることで、SSE-KMS を使用するように暗号化できます。

```
aws s3api copy-object --bucket amzn-s3-demo-bucket --key example-object-key --
body filepath --bucket amzn-s3-demo-bucket --key example-object-key --sse aws:kms --
sse-kms-key-id example-key-id --body filepath
```

AWS SDK の使用

AWS SDK を使用する場合、サーバー側の暗号化に AWS KMS keys を使用するよう Amazon S3 にリクエストできます。次の例は、AWS SDK for Java および .NET で SSE-KMS を使用する方法を示しています。他の SDK については、AWS デベロッパーセンターのサンプルコードとライブラリを参照してください。

> **Important**
>
> Amazon S3 でサーバー側の暗号化に AWS KMS key を使用する場合は、対称暗号化 KMS キーを選択する必要があります。Amazon S3 は、対称暗号化 KMS キーのみをサポートします。このキーの詳細については、「AWS Key Management Service デベロッパーガイド」の「対称暗号化 KMS キー」を参照してください。

CopyObject オペレーション

オブジェクトをコピーする場合は、同じリクエストプロパティ (ServerSideEncryptionMethod および ServerSideEncryptionKeyManagementServiceKeyId) を追加して、AWS KMS key を使用するように Amazon S3 に対してリクエストします。オブジェクトのコピーの詳細については、オブジェクトのコピー、移動、名前の変更 を参照してください。

PUT オペレーション

Java

AWS SDK for Java を使用してオブジェクトをアップロードする場合、次のリクエストのように SSEAwsKeyManagementParams プロパティを追加することによって、AWS KMS key を使用するように Amazon S3 に対してリクエストできます。

```
PutObjectRequest putRequest = new PutObjectRequest(bucketName,
   keyName, file).withSSEAwsKeyManagementParams(new SSEAwsKeyManagementParams());
```

この場合、Amazon S3 は AWS マネージドキー (aws/s3) を使用します。詳細については、「AWS KMS キーによるサーバー側の暗号化 (SSE-KMS) の使用」を参照してください。次の例に示すように、オプションで、対称暗号化 KMS キーを作成し、それをリクエストで指定できます。

```
PutObjectRequest putRequest = new PutObjectRequest(bucketName,
   keyName, file).withSSEAwsKeyManagementParams(new
 SSEAwsKeyManagementParams(keyID));
```

カスタマーマネージドキーの作成の詳細については、「AWS Key Management Service デベロッパーガイド」の「AWS KMS API のプログラミング」を参照してください。

オブジェクトをアップロードするためのコード例については、以下のトピックを参照してください。これらの例を使用するには、コード例を更新し、前出のコード例に示されているように暗号化情報を提供する必要があります。

- 1 つのオペレーションでオブジェクトをアップロードする場合は、オブジェクトのアップロード を参照してください。
- 高レベルまたは低レベルのマルチパートアップロード API オペレーションを使用するマルチパートアップロードについては、「マルチパートアップロードを使用したオブジェクトのアップロード」を参照してください。

.NET

AWS SDK for .NET を使用してオブジェクトをアップロードする場合、次のリクエストのように ServerSideEncryptionMethod プロパティを追加することによって、AWS KMS key を使用するように Amazon S3 に対してリクエストできます。

```
PutObjectRequest putRequest = new PutObjectRequest
 {
     BucketName = amzn-s3-demo-bucket,
     Key = keyName,
     // other properties
     ServerSideEncryptionMethod = ServerSideEncryptionMethod.AWSKMS
 };
```

この場合、Amazon S3 は AWS マネージドキー を使用します。詳細については、「AWS KMS キーによるサーバー側の暗号化 (SSE-KMS) の使用」を参照してください。次の例に示すように、オプションで、独自の対称暗号化カスタマーマネージドキーを作成し、それをリクエストで指定できます。

```
PutObjectRequest putRequest1 = new PutObjectRequest
{
  BucketName = amzn-s3-demo-bucket,
  Key = keyName,
  // other properties
  ServerSideEncryptionMethod = ServerSideEncryptionMethod.AWSKMS,
  ServerSideEncryptionKeyManagementServiceKeyId = keyId
};
```

カスタマーマネージドキーの作成の詳細については、「AWS Key Management Service デベロッパーガイド」の「AWS KMS API のプログラミング」を参照してください。

オブジェクトをアップロードするためのコード例については、以下のトピックを参照してください。これらの例を使用するには、コード例を更新し、前出のコード例に示されているように暗号化情報を提供する必要があります。

- 1 つのオペレーションでオブジェクトをアップロードする場合は、オブジェクトのアップロード を参照してください。
- 高レベルまたは低レベルのマルチパートアップロード API オペレーションを使用するマルチパートアップロードについては、「マルチパートアップロードを使用したオブジェクトのアップロード」を参照してください。

署名付き URL

Java

次の例に示すように、AWS KMS key で暗号化されたオブジェクトの署名付き URL を作成する際には、署名バージョン 4 を明示的に指定する必要があります。

```
ClientConfiguration clientConfiguration = new ClientConfiguration();
clientConfiguration.setSignerOverride("AWSS3V4SignerType");
AmazonS3Client s3client = new AmazonS3Client(
        new ProfileCredentialsProvider(), clientConfiguration);
...
```

コード例については、署名付き URL を使用したオブジェクトの共有 を参照してください。

.NET

次の例に示すように、AWS KMS key で暗号化されたオブジェクトの署名付き URL を作成する際には、署名バージョン 4 を明示的に指定する必要があります。

```
AWSConfigs.S3Config.UseSignatureVersion4 = true;
```

コード例については、署名付き URL を使用したオブジェクトの共有 を参照してください。

Amazon S3 バケットキーを使用した SSE-KMS のコストの削減

Amazon S3 バケットキーは、AWS Key Management Service (AWS KMS) を使用した Amazon S3 サーバー側の暗号化のコストを削減します。SSE-KMS でこのバケットレベルのキーを使用すると、Amazon S3 から AWS KMS へのリクエストトラフィックを減らすことにより、AWS KMS のリクエストコストを最大 99% 削減できます。AWS Management Console を数回クリックするだけで、クライアントアプリケーションの変更はせずにバケットを設定し、新しいオブジェクトで SSE-KMS の暗号化に S3 バケットキーを使用することができます。

> **Note**
>
> S3 バケットキーは、AWS Key Management Service (AWS KMS) キーによる二層式サーバー側の暗号化 (DSSE-KMS) ではサポートされていません。

SSE-KMS の S3 バケットキー

SSE-KMS で暗号化された数百万、数十億のオブジェクトにアクセスするワークロードは、AWS KMS に大量のリクエストを生成します。S3 バケットキーなしで SSE-KMS を使用してデータを保護する場合、Amazon S3 はすべてのオブジェクトに対して個々の AWS KMS データキーを使用します。この場合、KMS で暗号化されたオブジェクトに対してリクエストが実行されるたびに、Amazon S3 は AWS KMS を呼び出します。SSE-KMS の仕組みについては、AWS KMS キーによるサーバー側の暗号化 (SSE-KMS) の使用 を参照してください。

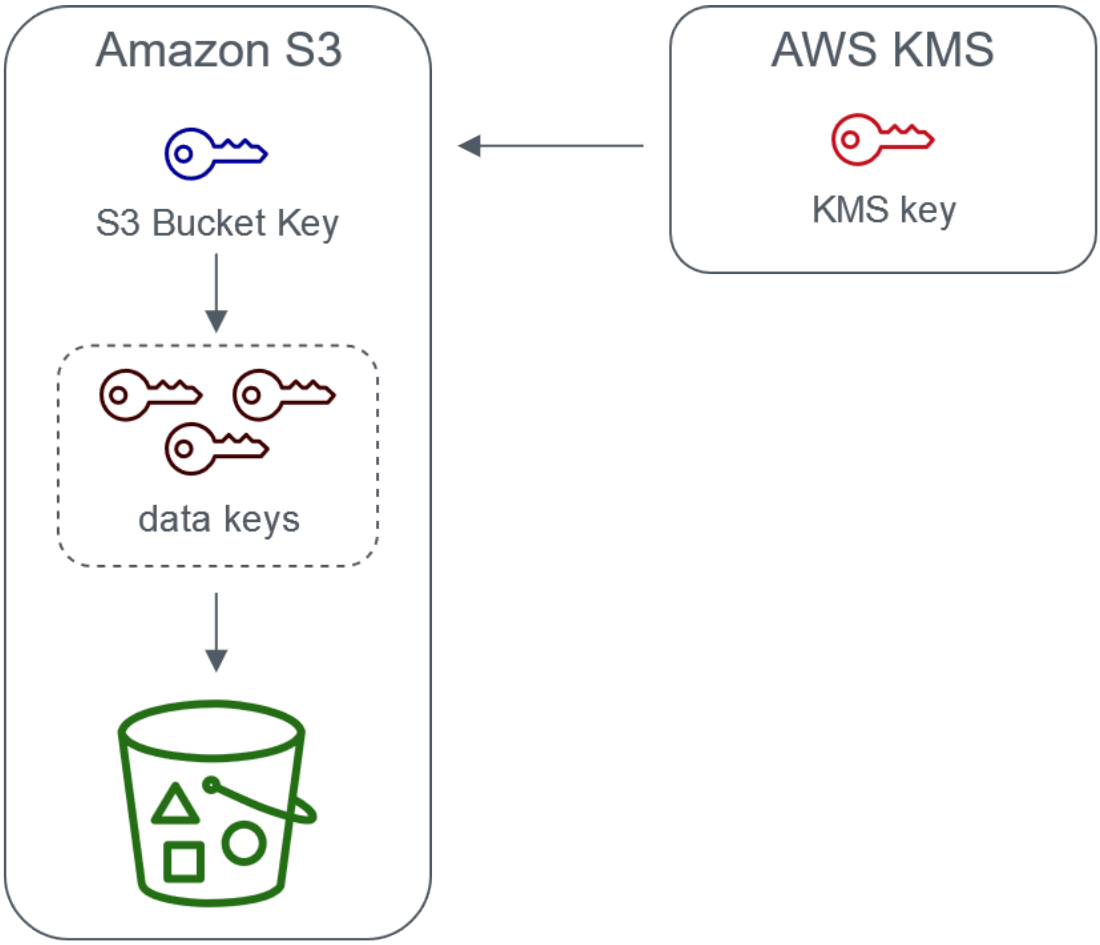
SSE-KMS の S3 バケットキーを使用するようにバケットを設定すると、AWS は AWS KMS から有効期限の短いバケットレベルのキーを生成し、S3 に一時的に保存します。このバケットレベルのキーは、ライフサイクル中に新しいオブジェクトのデータキーを作成します。S3 バケットキーは Amazon S3 内で期間限定で使用されるため、S3 で AWS KMS にリクエストを実行し、暗号化オペレーションを完了する必要性が軽減されます。これにより S3 から AWS KMS へのトラフィックが減少し、これまでと比較してわずかなコストで、Amazon S3 の AWS KMS で暗号化されたオブジェクトにアクセスできるようになります。

固有のバケットレベルのキーはリクエスタごとに少なくとも 1 回フェッチされ、キーへのリクエスターのアクセスが AWS KMS CloudTrail イベントで確実にキャプチャされます。Amazon S3 は、呼び出し元が異なるロールまたはアカウントを使用する場合、または同じロールを異なるスコープポリシーで使用する場合、呼び出し元を異なるリクエスタとして扱います。AWS KMS リクエスト削減数は、リクエスタ数、リクエストパターン、リクエストされたオブジェクトの相対的な経過時間を反映しています。例えば、リクエスタの数が少なく、限られた時間枠で複数のオブジェクトをリクエストして、同じバケットレベルのキーで暗号化した場合、大幅な削減につながります。

> **Note**
>
> S3 バケットキーを使用すると、バケットレベルのキーを使って `Encrypt`、`GenerateDataKey`、`Decrypt` オペレーションの AWS KMS リクエスト数を減らし、AWS KMS リクエストのコストを節約できます。設計上、このバケットレベルのキーを利用する後続のリクエストが AWS KMS API リクエストになったり、AWS KMS キーポリシーに照らしてアクセスが検証されたりすることはありません。

S3 バケットキーを設定する場合、バケット内に既に存在するオブジェクトは S3 バケットキーを使用しません。既存のオブジェクトの S3 バケットキーを設定するには、`CopyObject` オペレーションを使用できます。詳細については、「オブジェクトレベルで S3 バケットキーを設定する」を参照してください。

Amazon S3 は、同じ AWS KMS key で暗号化されるオブジェクトの S3 バケットキーのみを共有します。S3 バケットキーは、AWS KMS によって作成された KMS キー、インポートされたキーマテリアル、およびカスタムキーストア によってバックアップされたキーマテリアルと互換性があります。



Server-side encryption with AWS Key Management service using an S3 Bucket Key

S3 バケットキーの設定

Amazon S3 コンソール、AWS SDK、AWS CLI、または REST API を使用して、新しいオブジェクトで SSE-KMS の S3 バケットキーを使用するようにバケットを設定できます。バケットで S3 バケットキーを有効にすると、別の指定した SSE-KMS キーでアップロードされたオブジェクトは、独自の S3 バケットキーを使用します。S3 バケットキーの設定にかかわらず、リクエストに `true` または `false` の値の付いた `x-amz-server-side-encryption-bucket-key-enabled` ヘッダーを含めると、バケット設定を上書きできます。

S3 バケットキーを使用するようにバケットを設定する前に、「S3 バケットキーを有効にする前に注意するべき変更点」を確認してください。

Amazon S3 コンソールを使用した S3 バケットキーの設定

新しいバケットを作成する際、新しいオブジェクトで SSE-KMS の S3 バケットキーを使用するようにバケットを設定できます。また、バケットプロパティを更新して、新しいオブジェクトで SSE-KMS の S3 バケットキーを使用するように既存のバケットを設定することもできます。

詳細については、新しいオブジェクトで SSE-KMS の S3 バケットキーを使用するようにバケットを設定する を参照してください。

S3 バケットキーに対する REST API、AWS CLI、および AWS SDK のサポート

REST API、AWS CLI、または AWS SDK を使用して、新しいオブジェクトで SSE-KMS の S3 バケットキーを使用するようにバケットを設定できます。オブジェクトレベルで S3 バケットキーを有効にすることもできます。

詳細については次を参照してください:

- オブジェクトレベルで S3 バケットキーを設定する
- 新しいオブジェクトで SSE-KMS の S3 バケットキーを使用するようにバケットを設定する

次の API オペレーションは、SSE-KMS の S3 バケットキーをサポートしています。

- PutBucketEncryption
  - `ServerSideEncryptionRule` は、S3 バケットキーを有効または無効にする `BucketKeyEnabled` パラメータを受け入れます。
- GetBucketEncryption
  - `ServerSideEncryptionRule` は の設定を返します。`BucketKeyEnabled`
- PutObject、CopyObject、CreateMultipartUpload、および POST Object
  - `x-amz-server-side-encryption-bucket-key-enabled` リクエストヘッダーは、オブジェクトレベルで S3 バケットキーを有効または無効にします。
- HeadObject、GetObject、UploadPartCopy、UploadPart、CompleteMultipartUpload
  - `x-amz-server-side-encryption-bucket-key-enabled` レスポンスヘッダーは、オブジェクトに対して S3 バケットキーが有効か無効かを示します。

「AWS CloudFormation」 の使用

AWS CloudFormation では、`AWS::S3::Bucket` のリソースに S3 バケットキーを有効または無効にするために使用できる `BucketKeyEnabled` と呼ばれる暗号化プロパティが含まれています。

詳細については、AWS CloudFormation の使用 を参照してください。

S3 バケットキーを有効にする前に注意するべき変更点

S3 バケットキーを有効にする前に、次の関連する変更点に注意してください。

IAM または AWS KMS キーポリシー

既存の AWS Identity and Access Management (IAM) ポリシーまたは AWS KMS キーポリシーで、オブジェクトの Amazon リソースネーム (ARN) を暗号化コンテキストとして使用し、KMS キーへのアクセスを絞り込んだり制限したりする場合、S3 バケットキーではこれらのポリシーは機能しません。S3 バケットキーは、バケット ARN を暗号化コンテキストとして使用します。S3 バケットキーを有効にする前に、バケット ARN を暗号化コンテキストとして使用するため、IAM ポリシーまたは AWS KMS キーポリシーを更新してください。

暗号化コンテキストと S3 バケットキーの詳細については、「暗号化コンテキスト」を参照してください。

AWS KMS の CloudTrail イベント

S3 バケットキーを有効にすると、オブジェクト ARN の代わりに、AWS KMS CloudTrail イベントがバケット ARN を口グに記録します。さらに、口グに表示される SSE-KMS オブジェクトの KMS CloudTrail イベントが少なくなります。これは、Amazon S3 ではキーマテリアルに時間制限があり、これにより AWS KMS に対するリクエストが減るためです。

レプリケーションでの S3 バケットキーの使用

S3 バケットキーは、同一リージョンレプリケーション (SRR) およびクロスリージョンレプリケーション (CRR) で使用できます。

Amazon S3 では、暗号化されたオブジェクトをレプリケートする場合、通常、レプリケート先バケット内のレプリカオブジェクトの暗号化設定が保持されます。ただし、ソースオブジェクトが暗号化されておらず、レプリケート先バケットがデフォルトの暗号化または S3 バケットキーを使用している場合、Amazon S3 はレプリケート先のバケットの設定でオブジェクトを暗号化します。

以下の例では、S3 バケットキーがレプリケーションでどのように機能するかを示しています。詳細については、「暗号化されたオブジェクトのレプリケート (SSE-S3、SSE-KMS、DSSE-KMS、SSE-C)」を参照してください。

Example 例 1 – ソースオブジェクトで S3 バケットキーを使用し、レプリケート先バケットでデフォルトの暗号化を使用する

ソースオブジェクトでは S3 バケットキーを使用しているが、レプリケート先バケットでは SSE-KMS によるデフォルトの暗号化を使用している場合、レプリカオブジェクトは S3 バケットキーの暗号化設定をレプリケート先バケットに保持します。レプリケート先バケットでは、SSE-KMS によるデフォルトの暗号化が使用されます。

Example 例 2 – ソースオブジェクトが暗号化されておらず、レプリケート先バケットで SSE-KMS の S3 バケットキーを使用する

ソースオブジェクトが暗号化されておらず、レプリケート先のバケットで SSE-KMS の S3 バケットキーを使用する場合、レプリカオブジェクトはレプリケート先バケットで SSE-KMS を使用して、S3 バケットキーで暗号化されます。この結果、ソースオブジェクトの ETag はレプリカオブジェクトの ETag と異なることになります。この違いに対応するには、ETag を使用するアプリケーションを更新する必要があります。

S3 バケットキーの使用

S3 バケットキーの有効化と使用の詳細については、以下のセクションを参照してください。

- 新しいオブジェクトで SSE-KMS の S3 バケットキーを使用するようにバケットを設定する
- オブジェクトレベルで S3 バケットキーを設定する
- S3 バケットキーの設定の表示

新しいオブジェクトで SSE-KMS の S3 バケットキーを使用するようにバケットを設定する

AWS Key Management Service (AWS KMS) キー (SSE-KMS) を使用してサーバー側の暗号化を設定する場合、新しいオブジェクトで SSE-KMS の S3 バケットキーを使用するようにバケットを設定できます。S3 バケットキーは、Amazon S3 から AWS KMS へのリクエストトラフィックを減らし、SSE-KMS におけるコストを削減します。詳細については、「Amazon S3 バケットキーを使用した SSE-KMS のコストの削減」を参照してください。

Amazon S3 コンソール、REST API、AWS SDK、AWS Command Line Interface (AWS CLI)、または AWS CloudFormation を使用して、新しいオブジェクトで SSE-KMS の S3 バケットキーを使用するようにバケットを設定できます。既存のオブジェクトの S3 バケットキーを有効または無効にするには、CopyObject オペレーションを使用できます。詳細については、(オブジェクトレベルで S3 バケットキーを設定する) および (バッチオペレーションを使用して SSE-KMS の S3 バケットキーを有効にする) を参照してください。

レプリケート元バケットまたはレプリケート先バケットで S3 バケットキーを有効にすると、暗号化コンテキストはバケットの Amazon リソースネーム (ARN) になり、オブジェクト ARN にはなりません (例えば、`arn:aws:s3:::bucket_ARN`)。IAM ポリシーを更新して、暗号化コンテキストにバケット ARN を使用する必要があります。詳細については、「S3 バケットキーとレプリケーション」を参照してください。

以下の例では、S3 バケットキーがレプリケーションでどのように機能するかを示しています。詳細については、「暗号化されたオブジェクトのレプリケート (SSE-S3、SSE-KMS、DSSE-KMS、SSE-C)」を参照してください。

前提条件

S3 バケットキーを使用するようにバケットを設定する前に、「S3 バケットキーを有効にする前に注意するべき変更点」を確認してください。

S3 コンソールの使用

S3 コンソールでは、新しいバケットまたは既存のバケットに対して S3 バケットキーを有効または無効にできます。S3 コンソールのオブジェクトは、バケット設定からそれらの S3 バケットキーの設定を継承します。バケットで S3 バケットキーを有効にすると、バケットにアップロードする新しいオブジェクトでは、SSE-KMS に S3 バケット キーが使用されます。

S3 バケットキーが有効になっているバケット内のオブジェクトをアップロード、コピー、または変更する

S3 バケットキーが有効になっているバケットでオブジェクトをアップロード、変更、またはコピーすると、そのオブジェクトの S3 バケットキーの設定がバケット設定に合わせて更新されることがあります。

オブジェクトで既に S3 バケットキーが有効になっている場合、オブジェクトをコピーまたは変更しても、そのオブジェクトの S3 バケットキーの設定は変更されません。ただし、レプリケート先バケットに S3 バケットキーの設定がある状態で S3 バケットキーが有効になっていないオブジェクトを変更またはコピーした場合、オブジェクトはレプリケート先バケットの S3 バケットキーの設定を継承します。例えば、ソースオブジェクトで S3 バケットキーが有効になっていないが、レプリケート先バケットで S3 バケットキーが有効になっている場合、S3 バケットキーは有効になります。

新しいバケットの作成時に S3 バケットキーを有効にするには

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。

3. [Create bucket (バケットの作成)] を選択します。
4. バケット名を入力し、AWS リージョンを選択します。
5. [デフォルトの暗号化] の [暗号化キーの種類] で、[AWS Key Management Service キー (SSE-KMS)] を選択します。
6. [AWS KMS キー] で、次のいずれかを実行して KMS キーを選択します。

   - 使用可能な KMS キーのリストから選択するには、[AWS KMS keys から選択する] を選択し、使用可能なキーのリストから自分の KMS キーを選択します。

     AWS マネージドキー (aws/s3) とカスタマーマネージドキーの両方がこのリストに表示されます。カスタマーマネージドキーの詳細については、AWS Key Management Serviceデベロッパーガイドの「カスタマーキーと AWS キー」を参照してください。
   - KMS キー ARN を入力するには、[AWS KMS key ARN を入力] を選択し、表示されるフィールドに KMS キー ARN を入力します。
   - AWS KMS コンソールで新しいカスタマーマネージドキーを作成するには、[KMS キーを作成] を選択します。

     AWS KMS key の作成の詳細については、「AWS Key Management Service デベロッパーガイド」の「キーの作成」を参照してください。
7. [バケットキー] で [有効化] を選択します。
8. [Create bucket] (バケットの作成) をクリックします。

   Amazon S3 は、S3 バケットキーを有効にしてバケットを作成します。バケットにアップロードする新しいオブジェクトには、S3 バケットキーを使用します。

   S3 バケットキーを無効にするには、前の手順に従い、[無効化] を選択します。

既存のバケットに対して S3 バケットキーを有効にするには

1. Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。
3. [バケット] リストで、S3 バケットキーを有効にするバケットを選択します。
4. [プロパティ] タブを選択します。
5. [デフォルトの暗号化] で、[編集] を選択します。
6. [デフォルトの暗号化] の [暗号化キーの種類] で、[AWS Key Management Service キー (SSE-KMS)] を選択します。

7. [AWS KMS キー] で、次のいずれかを実行して KMS キーを選択します。

   - 使用可能な KMS キーのリストから選択するには、[AWS KMS keys から選択する] を選択し、使用可能なキーのリストから自分の KMS キーを選択します。

     AWS マネージドキー (aws/s3) とカスタマーマネージドキーの両方がこのリストに表示されます。カスタマーマネージドキーの詳細については、AWS Key Management Serviceデベロッパーガイドの「カスタマーキーと AWS キー」を参照してください。
   - KMS キー ARN を入力するには、[AWS KMS key ARN を入力] を選択し、表示されるフィールドに KMS キー ARN を入力します。
   - AWS KMS コンソールで新しいカスタマーマネージドキーを作成するには、[KMS キーを作成] を選択します。

     AWS KMS key の作成の詳細については、「AWS Key Management Service デベロッパーガイド」の「キーの作成」を参照してください。
8. [バケットキー] で [有効化] を選択します。
9. [Save changes] (変更の保存) をクリックします。

   Amazon S3 では、バケットに追加された新しいオブジェクトに対して S3 バケットキーが有効になります。既存のオブジェクトでは S3 バケットキーは使用しません。既存のオブジェクトの S3 バケットキーを設定するには、CopyObject オペレーションを使用できます。詳細については、「オブジェクトレベルで S3 バケットキーを設定する」を参照してください。

   S3 バケットキーを無効にするには、前の手順に従い、[Disable (無効化)] を選択します。

REST API の使用

PutBucketEncryption を使用してバケットの S3 バケットキーを有効または無効にできます。PutBucketEncryption で S3 バケットキーを設定するには、ServerSideEncryptionRule を使用します。これには、SSE-KMS を使用したデフォルトの暗号化が含まれます。また、オプションで、カスタマーマネージドキーの KMS キー ID を指定して、カスタマーマネージドキーを使用することもできます。

詳細と構文の例については、PutBucketEncryption を参照してください。

AWS SDK for Java の使用

次の例では、AWS SDK for Java を使用して、S3 バケットキーと SSE-KMS によるデフォルトのバケット暗号化を有効にします。

Java

```
AmazonS3 s3client = AmazonS3ClientBuilder.standard()
    .withRegion(Regions.DEFAULT_REGION)
    .build();

ServerSideEncryptionByDefault serverSideEncryptionByDefault = new
 ServerSideEncryptionByDefault()
    .withSSEAlgorithm(SSEAlgorithm.KMS);
ServerSideEncryptionRule rule = new ServerSideEncryptionRule()
    .withApplyServerSideEncryptionByDefault(serverSideEncryptionByDefault)
    .withBucketKeyEnabled(true);
ServerSideEncryptionConfiguration serverSideEncryptionConfiguration =
    new ServerSideEncryptionConfiguration().withRules(Collections.singleton(rule));

SetBucketEncryptionRequest setBucketEncryptionRequest = new
 SetBucketEncryptionRequest()
    .withServerSideEncryptionConfiguration(serverSideEncryptionConfiguration)
    .withBucketName(bucketName);

s3client.setBucketEncryption(setBucketEncryptionRequest);
```

AWS CLI を使用する場合

次の例では、AWS CLI を使用して、S3 バケットキーと SSE-KMS によるデフォルトのバケット暗号化を有効にします。*user input placeholders* を、ユーザー自身の情報に置き換えます。

```
aws s3api put-bucket-encryption --bucket amzn-s3-demo-bucket --server-side-encryption-
configuration '{
        "Rules": [
            {
                "ApplyServerSideEncryptionByDefault": {
                    "SSEAlgorithm": "aws:kms",
                    "KMSMasterKeyID": "KMS-Key-ARN"
                },
                "BucketKeyEnabled": true
            }
        ]
    }'
```

AWS CloudFormation の使用

AWS CloudFormation を使用して S3 バケットキーを設定する方法の詳細については、AWS CloudFormation ユーザーガイドの「AWS::S3::Bucket ServerSideEncryptionRule」を参照してください。

オブジェクトレベルで S3 バケットキーを設定する

REST API、AWS SDK、または AWS CLI を使用して PUT オペレーションまたは COPY オペレーションを実行する際、`true` または `false` の値の付いた `x-amz-server-side-encryption-bucket-key-enabled` リスエストヘッダーを追加して、オブジェクトレベルで S3 バケットキーを有効または無効にできます。S3 バケットキーは、Amazon S3 から AWS KMS へのリクエストトラフィックを減らすことにより、AWS Key Management Service (AWS KMS) (SSE-KMS) を使用したサーバー側の暗号化のコストを削減します。詳細については、Amazon S3 バケットキーを使用した SSE-KMS のコストの削減 を参照してください。

PUT オペレーションまたは COPY オペレーションを使用してオブジェクトの S3 バケットキーを設定すると、Amazon S3 では、そのオブジェクトの設定のみが更新されます。レプリケート先バケットの S3 バケットキーの設定は変更されません。KMS で暗号化されたオブジェクトの PUT または COPY リクエストを S3 バケットキーが有効になっているバケットに送信すると、リクエストヘッダーのキーを無効にしない限り、オブジェクトレベルのオペレーションでは自動的に S3 バケットキーが使用されます。オブジェクトに S3 バケットキーを指定しない場合、Amazon S3 ではレプリケート先バケットの S3 バケットキーの設定がオブジェクトに適用されます。

前提条件:

S3 バケットキーを使用するようにオブジェクトを設定する前に、「S3 バケットキーを有効にする前に注意するべき変更点」を確認してください。

トピック

- Amazon S3 バッチオペレーション
- REST API の使用
- AWS SDK Java (PutObject) の使用
- AWS CLI (PutObject) の使用

Amazon S3 バッチオペレーション

既存の Amazon S3 オブジェクトを暗号化するには、Amazon S3 バッチオペレーションを使用します。S3 バッチオペレーションは、操作するオブジェクトのリストとともに提供します。バッチオペレーションは各 API を呼び出して、指定されたオペレーションを実行します。

S3 バッチオペレーションのコピーオペレーションを使用して、既存の暗号化されていないオブジェクトをコピーし、同じバケットに新しい暗号化されたオブジェクトを書き込めます。1 つのバッチオペレーションジョブで、数十億ものオブジェクトに対して、指定されたオペレーションを実行できます。詳細については、バッチオペレーションでオブジェクトオペレーションを一括で実行する および Amazon S3 バッチオペレーションによるオブジェクトの暗号化を参照してください。

REST API の使用

SSE-KMS を使用すると、次の API を使用して、オブジェクトの S3 バケットキーを有効にできます。

- PutObject – オブジェクトをアップロードするときに、`x-amz-server-side-encryption-bucket-key-enabled` リクエストヘッダーを指定して、オブジェクトレベルで S3 バケットキーを有効または無効にできます。
- CopyObject – オブジェクトをコピーして SSE-KMS を設定するときに、`x-amz-server-side-encryption-bucket-key-enabled` リクエストヘッダーを指定して、オブジェクトの S3 バケットキーを有効または無効にできます。
- PostObject – POST オペレーションを使用してオブジェクトをアップロードし、SSE-KMS を設定するとき、`x-amz-server-side-encryption-bucket-key-enabled` フォームフィールドを使用してオブジェクトの S3 バケットキーを有効または無効にできます。
- CreateMultipartUpload – `CreateMultipartUpload` API オペレーションを使用して大きなオブジェクトをアップロードし、SSE-KMS を設定する場合、`x-amz-server-side-encryption-bucket-key-enabled` リクエストヘッダーを使用してオブジェクトの S3 バケットキーを有効または無効にできます。

オブジェクトレベルで S3 バケットキーを有効にするには、`x-amz-server-side-encryption-bucket-key-enabled` リクエストヘッダーを含めます。SSE-KMS および REST API の詳細については、REST API の使用 を参照してください。

AWS SDK Java (PutObject) の使用

次の例を使用して、AWS SDK for Java を使ってオブジェクトレベルで S3 バケットキーを設定できます。

Java

```
AmazonS3 s3client = AmazonS3ClientBuilder.standard()
    .withRegion(Regions.DEFAULT_REGION)
    .build();

String bucketName = "amzn-s3-demo-bucket1";
String keyName = "key name for object";
String contents = "file contents";

PutObjectRequest putObjectRequest = new PutObjectRequest(bucketName, keyName,
 contents)
    .withBucketKeyEnabled(true);

s3client.putObject(putObjectRequest);
```

AWS CLI (PutObject) の使用

次の AWS CLI の例を使用して、PutObject リクエストの一部としてオブジェクトレベルで S3 バケットキーを設定できます。

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key object key name --server-side-
encryption aws:kms --bucket-key-enabled --body filepath
```

S3 バケットキーの設定の表示

Amazon S3 コンソール、REST API、AWS Command Line Interface (AWS CLI)、または AWS SDK を使用して、バケットまたはオブジェクトレベルで S3 バケットキーの設定を表示できます。

S3 バケットキーは、Amazon S3 から AWS KMS へのリクエストトラフィックを減らし、AWS Key Management Service (SSE-KMS) を使用したサーバー側の暗号化のコストを削減します。詳細については、「Amazon S3 バケットキーを使用した SSE-KMS のコストの削減」を参照してください。

バケット設定から S3 バケット キー設定を継承したバケットまたはオブジェクトの S3 バケット キー設定を表示するには、s3:GetEncryptionConfiguration アクションを実行するアクセス許可が必要です。詳細については、Amazon Simple Storage Service API リファレンスの GetBucketEncryption を参照してください。

S3 コンソールの使用

S3 コンソールでは、バケットまたはオブジェクトの S3 バケットキーの設定を表示できます。ソースオブジェクトにすでに S3 バケットキーが設定されていない限り、S3 バケットキーの設定はバケット設定から継承されます。

同じバケット内のオブジェクトとフォルダは、異なる S3 バケットキーの設定を行えます。例えば、REST API を使用してオブジェクトをアップロードし、そのオブジェクトの S3 バケットキーを有効にした場合、レプリケート先バケットで S3 バケットキーが無効になっている場合でも、S3 バケットキーの設定は保持されます。別の例として、既存のバケットに対して S3 バケットキーを有効にした場合、バケット内に既に存在するオブジェクトには S3 バケットキーを使用できません。ただし、新しいオブジェクトでは S3 バケットキーが有効になります。

バケットの S3 バケットキーの設定を表示するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。
3. [バケット] リストで、S3 バケットキーを有効にするバケットを選択します。
4. [プロパティ] を選択します。
5. [Default encryption (デフォルトの暗号化)] セクションの [バケットキー] に、バケットの S3 バケットキーの設定が表示されます。

   S3 バケットキーの設定が表示されない場合は、`s3:GetEncryptionConfiguration` アクションを実行するアクセス許可がない可能性があります。詳細については、「Amazon Simple Storage Service API リファレンス」の「GetBucketEncryption」を参照してください。

オブジェクトの S3 バケットキーの設定を表示するには

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. [バケット] リストで、S3 バケットキーを有効にするバケットを選択します。
3. [オブジェクト] リストで、オブジェクト名を選択します。
4. [詳細] タブの [Server-side encryption settings (サーバー側の暗号化設定)] で、[Edit (編集)] を選択します。

[バケットキー] の下に、オブジェクトの S3 バケットキーの設定が表示されます。この設定を編集することはできません。

AWS CLI を使用する場合

バケットレベルの S3 バケットキーの設定を返すには

この例を実行するには、それぞれの *user input placeholder* をユーザー自身の情報に置き換えます。

```
aws s3api get-bucket-encryption --bucket amzn-s3-demo-bucket1
```

詳細については、AWS CLI コマンドリファレンスの「get-bucket-encryption」を参照してください。

S3 バケットキーのオブジェクトレベルの設定を返すには

この例を実行するには、それぞれの *user input placeholder* をユーザー自身の情報に置き換えます。

```
aws s3api head-object --bucket amzn-s3-demo-bucket1 --key my_images.tar.bz2
```

詳細については、AWS CLI コマンドリファレンスの「head-object」を参照してください。

REST API の使用

バケットレベルの S3 バケットキーの設定を返すには

S3 バケットキーの設定を含むバケットの暗号化情報を返すには、GetBucketEncryption オペレーションを使用します。S3 バケットキーの設定は、BucketKeyEnabled の設定と共に ServerSideEncryptionConfiguration 要素のレスポンス本文に返されます。詳細については、Amazon S3 API リファレンスの GetBucketEncryption を参照してください。

S3 バケットキーのオブジェクトレベルの設定を返すには

オブジェクトの S3 バケットキーのステータスを返すには、HeadObject オペレーションを使用します。HeadObject は、オブジェクトに対して S3 バケットキーが有効か無効かを示す x-amz-server-side-encryption-bucket-key-enabled レスポンスヘッダーを返します。詳細については、Amazon S3 API リファレンス の HeadObject を参照してください。

次の API オペレーションは、オブジェクトに対して S3 バケットキーが設定されている場合、x-amz-server-side-encryption-bucket-key-enabled レスポンスヘッダーも返します。

- PutObject
- PostObject
- CopyObject
- CreateMultipartUpload
- UploadPartCopy
- UploadPart
- CompleteMultipartUpload
- GetObject

AWS KMS キーによる二層式サーバー側の暗号化 (DSSE-KMS) の使用

AWS Key Management Service (AWS KMS) キーによる二層式サーバー側の暗号化 (DSSE-KMS) を使用すると、オブジェクトが Amazon S3 にアップロードされるときに 2 つの暗号化レイヤーが適用されます。DSSE-KMS を使用すると、データに多層暗号化を適用し、暗号化キーを完全に制御する必要があるコンプライアンス基準をより簡単に満たすことができます。

S3 バケットで DSSE-KMS を使用する場合、AWS KMS キーはバケットと同じリージョンに存在する必要があります。また、オブジェクトに対して DSSE-KMS がリクエストされると、オブジェクトのメタデータの一部である S3 チェックサムが暗号化された形式で保存されます。チェックサムの詳細については、「Amazon S3 でのオブジェクトの整合性のチェック」を参照してください。

DSSE-KMS と AWS KMS keys の使用には、追加料金がかかります。DSSE-KMS 料金の詳細については、『AWS Key Management Service デベロッパーガイド』の「AWS KMS key の概念」と「AWS KMS の料金」を参照してください。

> **Note**
>
> S3 バケットキーは DSSE-KMS ではサポートされていません。

AWS KMS keys キーによる二層式サーバー側の暗号化 (DSSE-KMS) の要求

特定の Amazon S3 バケット内のすべてのオブジェクトの二層式サーバー側の暗号化を要求するには、バケットポリシーを使用できます。例えば、DSSE-KMS を使用したサーバー側の暗号化を要求する `x-amz-server-side-encryption` ヘッダーがリクエストに含まれていない場合、次のバケットポリシーはすべてのユーザーに対し、オブジェクト (`s3:PutObject`) をアップロードするアクセス許可を拒否します。

```
{
```

```
            "Version":"2012-10-17",
            "Id":"PutObjectPolicy",
            "Statement":[{
                  "Sid":"DenyUnEncryptedObjectUploads",
                  "Effect":"Deny",
                  "Principal":"*",
                  "Action":"s3:PutObject",
                  "Resource":"arn:aws:s3:::amzn-s3-demo-bucket/*",
                  "Condition":{
                     "StringNotEquals":{
                        "s3:x-amz-server-side-encryption":"aws:kms:dsse"
                     }
                  }
               }
            ]
         }
```

トピック

- AWS KMS キーによる二層式サーバー側の暗号化 (DSSE-KMS) の指定

AWS KMS キーによる二層式サーバー側の暗号化 (DSSE-KMS) の指定

暗号化は、新しいオブジェクトをアップロードしたり、既存のオブジェクトをコピーしたりするときに適用できます。

Amazon S3 コンソール、Amazon S3 REST API、および AWS Command Line Interface (AWS CLI) を使用して、DSSE-KMS を指定できます。詳細については、以下のトピックを参照してください。

> **Note**
>
> Amazon S3 では、マルチリージョン AWS KMS keys を使用できます。ただし、Amazon S3 では現在、マルチリージョンキーは、単一リージョンキーであるかのように処理され、キーのマルチリージョン特徴は使用しません。詳細については、「AWS Key Management Service デベロッパーガイド」の「Using multi-Region keys」を参照してください。

> **Note**
>
> 別のアカウントが所有している KMS キーを使用する場合は、そのキーを使用するアクセス許可が必要です。KMS キーのクロスアカウント権限の詳細については、AWS Key

Management Service デベロッパーガイドの「他のアカウントで使用できる KMS キーを作成する」を参照してください。

S3 コンソールの使用

このセクションでは、Amazon S3 コンソールを使用して、AWS Key Management Service (AWS KMS) キーによる二層式サーバー側の暗号化 (DSSE-KMS) を使用するようにオブジェクトの暗号化のタイプを設定または変更する方法について説明します。

> **Note**
>
> - オブジェクトが 5 GB 未満の場合は、オブジェクトの暗号化を変更できます。オブジェクトが 5 GB を超える場合は、AWS CLI または AWS SDK を使用してオブジェクトの暗号化を変更する必要があります。
> - オブジェクトの暗号化の変更に必要な追加のアクセス許可のリストについては、「the section called “S3 API オペレーションに必要なアクセス許可”」を参照してください。このアクセス許可を付与するポリシーの例については、「the section called “アイデンティティベースのポリシーの例”」を参照してください。
> - オブジェクトの暗号化を変更すると、新しいオブジェクトが作成され、古いオブジェクトが置き換えられます。S3 バージョニングが有効になっている場合は、オブジェクトの新しいバージョンが作成され、既存のオブジェクトが古いバージョンになります。また、プロパティを変更するロールは、新しいオブジェクト (またはオブジェクトのバージョン) の所有者になります。

オブジェクトの暗号化を追加または変更するには

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. ナビゲーションペインで [バケット] を選択してから、[汎用バケット] タブをクリックします。変更するオブジェクトを含む Amazon S3 バケットまたはフォルダに移動します。
3. 変更するオブジェクトのチェックボックスをオンにします。
4. [アクション] メニューに表示されるオプションのリストから [サーバー側の暗号化を編集] を選択します。
5. [サーバー側の暗号化] セクションまでスクロールします。

6. [暗号化設定] で、[デフォルトの暗号化にバケット設定を使用する] または [デフォルトの暗号化にバケット設定を上書きする] を選択します。
7. [デフォルトの暗号化にバケット設定を上書きする] を選択した場合は、次の暗号化設定を設定します。

   a. [暗号化タイプ] で、[AWS Key Management Service キーによる二層式サーバー側の暗号化 (DSSE-KMS)] を選択します。

   b. [AWS KMS キー] で、次のいずれかを実行して KMS キーを選択します。

   - 使用可能な KMS キーのリストから選択するには、[AWS KMS keys から選択する] を選択し、使用可能なキーのリストから自分の KMS キーを選択します。

     AWS マネージドキー (aws/s3) とカスタマーマネージドキーの両方がこのリストに表示されます。カスタマーマネージドキーの詳細については、AWS Key Management Service デベロッパーガイドの「カスタマーキーと AWS キー」を参照してください。
   - KMS キー ARN を入力するには、[AWS KMS key ARN を入力] を選択し、表示されるフィールドに KMS キー ARN を入力します。
   - AWS KMS コンソールで新しいカスタマーマネージドキーを作成するには、[KMS キーを作成] を選択します。

     AWS KMS key の作成の詳細については、「AWS Key Management Service デベロッパーガイド」の「キーの作成」を参照してください。

> **Important**
>
> バケットと同じ AWS リージョン で使用可能な KMS キーのみを使用できます。Amazon S3 コンソールには、バケットと同じリージョンで最初の 100 個の KMS キーしか表示されません。リストに存在しない KMS キーを使用するには、KMS キー ARN を入力する必要があります。別のアカウントが所有している KMS キーを使用する場合は、まず、そのキーを使用するアクセス許可が必要であり、次に、KMS キー ARN を入力する必要があります。
> Amazon S3 では、対称暗号化 KMS キーのみがサポートされ、非対称暗号化 KMS キーはサポートされません。詳細については、『AWS Key Management Service デベロッパーガイド』の「非対称 KMS キーの識別」を参照してください。

8. [バケットキー] で、[無効] を選択します。S3 バケットキーは DSSE-KMS ではサポートされていません。

9. [追加のコピー設定] で、[ソース設定をコピー] するか、[設定を指定しない] か、[設定を指定] するかを選択します。[ソース設定をコピー] がデフォルトのオプションです。ソース設定の属性なしでオブジェクトのみをコピーする場合は、[設定を指定しない] を選択します。ストレージクラス、ACL、オブジェクトタグ、メタデータ、サーバー側の暗号化、その他のチェックサムの設定を指定するには、[設定を指定] を選択します。
10. [Save changes] (変更の保存) をクリックします。

> **Note**
>
> このアクションは、指定されたすべてのオブジェクトに暗号化を適用します。フォルダを暗号化する場合は、保存オペレーションが完了するのを待ってから、フォルダに新しいオブジェクトを追加します。

REST API の使用

オブジェクトを作成するとき (新しいオブジェクトをアップロードするか、既存のオブジェクトをコピーするとき) に、AWS KMS keys による二層式サーバー側の暗号化 (DSSE-KMS) の使用を指定してデータを暗号化できます。これを行うには、リクエストに `x-amz-server-side-encryption` ヘッダーを追加します。ヘッダーの値を、暗号化アルゴリズム `aws:kms:dsse` に設定します。Amazon S3 によりレスポンスヘッダー `x-amz-server-side-encryption` が返されるため、DSSE-KMS 暗号化を使用してオブジェクトが保存されたことを確認できます。

`aws:kms:dsse` の値で `x-amz-server-side-encryption` ヘッダーを指定する場合は、次のリクエストヘッダーも使用できます。

- `x-amz-server-side-encryption-aws-kms-key-id: SSEKMSKeyId`
- `x-amz-server-side-encryption-context: SSEKMSEncryptionContext`

トピック

- DSSE-KMS をサポートする Amazon S3 REST API オペレーション
- 暗号化コンテキスト (x-amz-server-side-encryption-context)
- AWS KMS キー ID (x-amz-server-side-encryption-aws-kms-key-id)

DSSE-KMS をサポートする Amazon S3 REST API オペレーション

次の REST API オペレーションでは `x-amz-server-side-encryption`、`x-amz-server-side-encryption-aws-kms-key-id`、および `x-amz-server-side-encryption-context` リクエストヘッダーを受け入れます。

- PutObject - PUT オペレーションを使用してデータをアップロードするとき、これらのリクエストヘッダーを指定できます。
- CopyObject — オブジェクトをコピーするときには、ソースオブジェクトとターゲットオブジェクトの両方があります。`CopyObject` オペレーションで DSSE-KMS ヘッダーを渡すと、ターゲットオブジェクトにのみ適用されます。既存のオブジェクトをコピーする際は、コピー元オブジェクトが暗号化されているかどうかに関係なく、明示的にサーバー側の暗号化を要求しない限り、コピー先オブジェクトは暗号化されません。
- POST オブジェクト — `POST` オペレーションを使用してオブジェクトをアップロードするときには、リクエストヘッダーの代わりに、フォームフィールドで同じ情報を指定します。
- CreateMultipartUpload - マルチパートアップロードを使用して大きいオブジェクトをアップロードするときには、`CreateMultipartUpload` リクエストでこれらのヘッダーを指定できます。

次の REST API オペレーションのレスポンスヘッダーは、オブジェクトがサーバー側の暗号化を使用して保存されるときに `x-amz-server-side-encryption` ヘッダーを返します。

- PutObject
- CopyObject
- POST オブジェクト
- CreateMultipartUpload
- UploadPart
- UploadPartCopy
- CompleteMultipartUpload
- GetObject
- HeadObject

> **Important**
>
> - AWS KMS で保護されたオブジェクトに対する GET および PUT リクエストはすべて、Secure Sockets Layer (SSL)、Transport Layer Security (TLS)、または署名バージョン 4 を使用していない場合、失敗します。
> - オブジェクトで DSSE-KMS を使用している場合、GET リクエストおよび HEAD リクエストの暗号化リクエストヘッダーを送信しないでください。送信すると、HTTP 400 (Bad Request) エラーが発生します。

暗号化コンテキスト (**x-amz-server-side-encryption-context**)

x-amz-server-side-encryption:aws:kms:dsse を指定した場合、Amazon S3 API は x-amz-server-side-encryption-context ヘッダーの暗号化コンテキストをサポートします。暗号化コンテキストは、データに関する追加のコンテキスト情報が含まれたキーバリューペアのセットです。

Amazon S3 は、オブジェクトの Amazon リソースネーム (ARN) を暗号化コンテキストペア (arn:aws:s3:::*object_ARN* など) として自動的に使用します。

オプションで、x-amz-server-side-encryption-context ヘッダーを使用して、追加の暗号化コンテキストペアを指定することもできます。しかし、暗号化コンテキストは暗号化されないため、機密情報を含めないでください。Amazon S3 は、この追加のキーペアをデフォルトの暗号化コンテキストとともに保存します。

Amazon S3 の暗号化コンテキストの詳細については、「暗号化コンテキスト」を参照してください。暗号化コンテキストの一般的な情報については、「AWS Key Management Service デベロッパーガイド」の「AWS Key Management Service Concepts - Encryption context」を参照してください。

AWS KMS キー ID (**x-amz-server-side-encryption-aws-kms-key-id**)

x-amz-server-side-encryption-aws-kms-key-id ヘッダーを使用して、データの保護に使用するカスタマーマネージドキーの ID を指定できます。x-amz-server-side-encryption:aws:kms:dsse ヘッダーを指定しても x-amz-server-side-encryption-aws-kms-key-id ヘッダーを指定しない場合、Amazon S3 は AWS マネージドキー (aws/s3) を使用してデータを保護します。カスタマーマネージドキーを使用する場合は、カスタマーマネージドキーの x-amz-server-side-encryption-aws-kms-key-id ヘッダーを指定する必要があります。

> **Important**
>
> Amazon S3 でサーバー側の暗号化に AWS KMS key を使用する場合は、対称暗号化 KMS キーを選択する必要があります。Amazon S3 は、対称暗号化 KMS キーのみをサポートします。このキーの詳細については、「AWS Key Management Service デベロッパーガイド」の「対称暗号化 KMS キー」を参照してください。

AWS CLI を使用する場合

新しいオブジェクトをアップロードするか、既存のオブジェクトをコピーするときに、 データの暗号に DSSE-KMS を使用することを指定できます。これを行うには、リクエストに `--server-side-encryption aws:kms:dsse` パラメータを追加します。`--ssekms-key-id` *`example-key-id`* パラメータを使用して、作成したカスタマーマネージド AWS KMS キーを追加します。AWS KMS キー ID を指定せずに `--server-side-encryption aws:kms:dsse` を指定した場合、Amazon S3 は AWS マネージドキー (`aws/s3`) を使用します。

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key example-object-key --server-
side-encryption aws:kms:dsse --ssekms-key-id example-key-id --body filepath
```

暗号化されていないオブジェクトを元の場所にコピーすることで、DSSE-KMS を使用するように暗号化できます。

```
aws s3api copy-object --bucket amzn-s3-demo-bucket --key example-object-key --
body filepath --bucket amzn-s3-demo-bucket --key example-object-key --sse aws:kms:dsse
 --sse-kms-key-id example-key-id --body filepath
```

お客様が指定したキーによるサーバー側の暗号化 (SSE-C) の使用

サーバー側の暗号化は、保管時のデータ保護に関するものです。サーバー側の暗号化では、オブジェクトのメタデータではなく、オブジェクトデータのみが暗号化されます。お客様が用意したキーでのサーバー側の暗号化 (SSE-C) を使用すると、独自の暗号化キーを使用して暗号化されたデータを保存できます。リクエストの一部として用意された暗号化キーで、Amazon S3 は、ディスクに書き込む際のデータ暗号化と、オブジェクトにアクセスする際のデータ復号を管理します。したがって、データの暗号化と復号を実行するコードをお客様が管理する必要はありません。必要なことは、お客様が用意する暗号化キーを管理することだけです。

オブジェクトをアップロードする場合、Amazon S3 はお客様が用意した暗号化キーを使用してデータに AES-256 暗号化を適用します。その後、Amazon S3 はメモリから暗号化キーを削除し

ます。オブジェクトを取得するときは、リクエストの中で同じ暗号化キーを指定する必要があります。Amazon S3 では、最初に指定された暗号化キーが一致することを確認した後、オブジェクトを復号してから、オブジェクトデータを返します。

SSE-C の使用に追加料金はかかりません。ただし、SSE-C を設定および使用するためのリクエストには、標準の Amazon S3 リクエスト料金が発生します。料金については、「Amazon S3 の料金」を参照してください。

> **Note**
>
> Amazon S3 では、お客様が用意した暗号化キーを保存しません。代わりに、以降のリクエストを検証するために、ランダムな SALT 値が付加された暗号化キーの Hash-based Message Authentication Code (HMAC) 値が保存されます。SALT 値が付加された HMAC 値を使用して、暗号化キーの値を求めたり、暗号化されたオブジェクトの内容を復号したりすることはできません。これは、暗号化キーを紛失した場合、オブジェクトが失われることを意味します。

S3 レプリケーションは、SSE-C で暗号化されたオブジェクトをサポートします。暗号化されたオブジェクトのレプリケーションの詳細については、「the section called “暗号化オブジェクトのレプリケート”」を参照してください。

SSE-C の詳細については、以下のトピックを参照してください。

トピック

- SSE-C の概要
- SSE-C の要件と制限
- 署名済み URL および SSE-C
- お客様が用意したキーによるサーバー側の暗号化 (SSE-C) の指定

SSE-C の概要

このセクションでは、SSE-C の概要を示します。SSE-C を使用する際は、以下の考慮事項に注意してください。

- HTTPS を使用する必要があります。

> **Important**
>
> SSE-C を使用する場合、Amazon S3 は HTTP 経由で行われたリクエストをすべて拒否します。セキュリティ上の考慮事項として、誤って HTTP で送信されたキーは漏洩したと見なすことをお勧めします。キーを破棄して、必要に応じて更新してください。

- レスポンスのエンティティタグ (ETag) はオブジェクトデータの MD5 ハッシュではありません。
- 使用した暗号化キーと暗号化したオブジェクトのマッピングは、お客様に管理していただきます。Amazon S3 では暗号化キーを保存しません。どのオブジェクトにどの暗号化キーを使用したかは、お客様が管理してください。
  - バケットのバージョニングが有効になっている場合、この機能を使用してアップロードする各オブジェクトバージョンに、独自の暗号化キーを使用できます。どのオブジェクトバージョンにどの暗号化キーを使用したかは、お客様が管理してください。
  - クライアント側の暗号化キーはお客様が管理するため、キーの更新など、クライアント側での追加の安全対策はお客様に管理していただきます。

> **Warning**
>
> 暗号化キーを紛失した場合、暗号化キーを使用せずにオブジェクトに対して GET リクエストを実行すると失敗し、オブジェクトは失われます。

SSE-C の要件と制限

特定の Amazon S3 バケット内のすべてのオブジェクトの SSE-C を要求するには、バケットポリシーを使用できます。

例えば、次のバケットポリシーは、SSE-C を要求する `x-amz-server-side-encryption-customer-algorithm` ヘッダーを含まないすべてのリクエストに対して、オブジェクトのアップロード (`s3:PutObject`) 許可を拒否します。

```
{
    "Version": "2012-10-17",
    "Id": "PutObjectPolicy",
    "Statement": [
        {
            "Sid": "RequireSSECObjectUploads",
            "Effect": "Deny",
```

```
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "Null": {
                    "s3:x-amz-server-side-encryption-customer-algorithm": "true"
                }
            }
        }
    ]
}
```

特定の Amazon S3 バケット内のすべてのオブジェクトのサーバー側の暗号化を制限する場合も、ポリシーを使用できます。例えば、SSE-C を要求する x-amz-server-side-encryption-customer-algorithm ヘッダーがリクエストに含まれている場合、次のバケットポリシーはすべてのユーザーに対し、オブジェクト (s3:PutObject) をアップロードするアクセス許可を拒否します。

```
{
    "Version": "2012-10-17",
    "Id": "PutObjectPolicy",
    "Statement": [
        {
            "Sid": "RestrictSSECObjectUploads",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "Null": {
                    "s3:x-amz-server-side-encryption-customer-algorithm": "false"
                }
            }
        }
    ]
}
```

Important

バケットポリシーを使用して s3:PutObject に対する SSE-C を要求する場合は、すべてのマルチパートアップロードリクエスト

(CreateMultiPartUpload、UploadPart、CompleteMultipartUpload) に `x-amz-server-side-encryption-customer-algorithm` ヘッダーを含める必要があります。

署名済み URL および SSE-C

新しいオブジェクトのアップロード、既存のオブジェクトやオブジェクトメタデータの取得などのオペレーションに使用できる署名付き URL を生成できます。署名付き URL では、次のように SSE-C がサポートされます。

- 署名付き URL を作成するときに、署名の計算で `x-amz-server-side-encryption-customer-algorithm` ヘッダーを使用してアルゴリズムを指定する必要があります。
- 署名付き URL を使用して新しいオブジェクトをアップロードするとき、既存のオブジェクトを取得するとき、またはオブジェクトメタデータのみを取得するときに、クライアントアプリケーションのリクエストですべての暗号化ヘッダーを指定する必要があります。

> **Note**
>
> SSE-C 以外のオブジェクトでは、署名付き URL を生成し、その URL をブラウザに直接貼り付けることで、データにアクセスできます。
> ただし、これは SSE-C オブジェクトには行えません。署名付き URL に加えて SSE-C オブジェクトに固有の HTTP ヘッダーも含める必要があります。したがって、SSE-C オブジェクトの署名付き URL はプログラムでのみ使用できます。

署名付き URL の詳細については、「the section called “署名付き URL を使用してオブジェクトをダウンロードおよびアップロードする”」を参照してください。

お客様が用意したキーによるサーバー側の暗号化 (SSE-C) の指定

REST API を使用したオブジェクトの作成時に、お客様が用意したキー (SSE-C) を使用してサーバー側の暗号化を指定できます。SSE-C を使用する場合は、次のリクエストヘッダーを使用して暗号化キー情報を指定する必要があります。

名前	説明
`x-amz-server-side-encryption`	暗号化アルゴリズムを指定するには、このヘッダーを使用します。ヘッダーの値は AES256 である必要があります。

名前	説明
`-customer-algorithm`	
`x-amz-server-side-encryption-customer-key`	Amazon S3 でデータを暗号化または復号するために使用する base64 でエンコードされた 256 ビットの暗号化キーを指定するには、このヘッダーを使用します。
`x-amz-server-side-encryption-customer-key-MD5`	RFC 1321 に従って、暗号化キーの base64 エンコードされた 128 ビット MD5 ダイジェストを指定するには、このヘッダーを使用します。Amazon S3 では、このヘッダーを使用してメッセージの整合性を調べて、送信された暗号化キーにエラーがないことを確認します。

AWS SDK ラッパーライブラリを使用して、これらのヘッダーをリクエストに追加できます。必要に応じて、アプリケーションから直接 Amazon S3 REST API を呼び出すことができます。

> **Note**
>
> Amazon S3 コンソールを使用してオブジェクトをアップロードしたり SSE-C をリクエストしたりすることはできません。また、SSE-C を使用して保存されている既存のオブジェクトを更新すること (ストレージクラスの変更やメタデータの追加など) もできません。

REST API の使用

SSE-C をサポートする Amazon S3 REST API

次の Amazon S3 API は、お客様が用意した暗号化キー (SSE-C) を使用したサーバー側の暗号化をサポートします。

- GET オペレーション — GET API (GET Object を参照) を使用してオブジェクトを取得するときに、このリクエストヘッダーを指定できます。
- HEAD オペレーション — HEAD API (HEAD Object を参照) を使用してオブジェクトメタデータを取得するには、これらのリクエストヘッダーを指定できます。
- PUT オペレーション — PUT API (PUT Object を参照) を使用してデータをアップロードするときに、これらのリクエストヘッダーを指定できます。

- マルチパートアップロード — マルチパートアップロード API を使用して大きいオブジェクトをアップロードするときに、これらのヘッダーを指定できます。これらのヘッダーは、開始リクエスト (Initiate Multipart Upload を参照) と、後続の各パートのアップロードリクエスト (Upload Part または Upload Part - Copy を参照) で指定します。各パートのアップロードリクエストでは、暗号化情報がマルチパートアップロードの開始リクエストで指定した情報と同じである必要があります。
- POST オペレーション — POST オペレーションを使用してオブジェクトをアップロードする場合は (POST Object を参照)、リクエストヘッダーの代わりに、フォームフィールドで同じ情報を指定します。
- Copy オペレーション — オブジェクトをコピーする場合 (PUT Object - Copy を参照)、ソースオブジェクトとターゲットオブジェクトがあります。
  - AWS 管理のキーによるサーバー側の暗号化を使用してターゲットオブジェクトを暗号化する場合は、`x-amz-server-side-encryption` リクエストヘッダーを指定する必要があります。
  - SSE-C を使用してターゲットオブジェクトを暗号化する場合は、前の表で説明した 3 つのヘッダーを使用して暗号化情報を指定する必要があります。
  - ソースオブジェクトが SSE-C を使用して暗号化されている場合、Amazon S3 でオブジェクトを復号してコピーできるように、次のヘッダーを使用して暗号化キーの情報を指定する必要があります。

名前	説明
`x-amz-copy-source-server-side-encryption-customer-algorithm`	Amazon S3 でソースオブジェクトを復号するために使用するアルゴリズムを指定するには、このヘッダーを含めます。この値は、AES256 である必要があります。
`x-amz-copy-source-server-side-encryption-customer-key`	Amazon S3 でソースオブジェクトを復号するために使用する base64 でエンコードされた暗号化キーを指定するには、このヘッダーを含めます。この暗号化キーは、Amazon S3 でソースオブジェクトを作成したときに指定したキーであることが必要です。それ以外の場合、Amazon S3 でオブジェクトを復号できません。
`x-amz-copy-source-server-side-encryption`	RFC 1321 に従って、暗号化キーの base64 エンコードされた 128 ビット MD5 ダイジェストを指定するには、このヘッダーを含めます。

名前	説明
`-customer-key-MD5`	

AWS SDK を使用して PUT、GET、Head、および Copy オペレーションの SSE-C を指定する

次の例では、お客様が用意したキーによるサーバー側の暗号化 (SSE-C) をオブジェクト用にリクエストする方法を示します。この例では、次の操作を実行します。各オペレーションでは、SSE-C 関連ヘッダーをリクエストで指定する方法を示します。

- Put object — オブジェクトをアップロードし、顧客が用意した暗号キーによるサーバー側の暗号化をリクエストします。
- Get object — 前のステップでアップロードしたオブジェクトをダウンロードします。リクエストでは、オブジェクトのアップロード時に指定したのと同じ暗号化情報を提供します。Amazon S3 は、オブジェクトを復号して返すために、この情報を必要とします。
- Get object metadata — オブジェクトのメタデータを取得します。オブジェクトの作成時に使用したのと同じ暗号化情報を指定します。
- Copy object — 以前にアップロードしたオブジェクトのコピーを作成します。ソースオブジェクトは SSE-C を使用して保存されるため、コピーリクエストで暗号化情報を指定する必要があります。デフォルトでは、明示的にリクエストした場合に限り、Amazon S3 はオブジェクトのコピーを暗号化します。この例では、オブジェクトの暗号化されたコピーを保存するように Amazon S3 に指示します。

Java

> **Note**
>
> この例では、1 つのオペレーションでオブジェクトをアップロードする方法を示します。マルチパートアップロード API を使用して大きなオブジェクトをアップロードする場合は、この例に示したのと同じ方法で暗号化情報を指定します。AWS SDK for Java を使用するマルチパートアップロードの例については、マルチパートアップロードを使用したオブジェクトのアップロード を参照してください。

必要な暗号化情報を追加するには、リクエストに `SSECustomerKey` を含めます。`SSECustomerKey` クラスの詳細については、REST API」セクションを参照してください。

SSE-C の詳細については、お客様が指定したキーによるサーバー側の暗号化 (SSE-C) の使用 を参照してください。作業サンプルの作成およびテストの手順については、「AWS SDK for Java のデベロッパーガイド」の「使用開始」を参照してください。

Example

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.*;

import javax.crypto.KeyGenerator;
import java.io.BufferedReader;
import java.io.File;
import java.io.IOException;
import java.io.InputStreamReader;
import java.security.NoSuchAlgorithmException;
import java.security.SecureRandom;

public class ServerSideEncryptionUsingClientSideEncryptionKey {
    private static SSECustomerKey SSE_KEY;
    private static AmazonS3 S3_CLIENT;
    private static KeyGenerator KEY_GENERATOR;

    public static void main(String[] args) throws IOException,
 NoSuchAlgorithmException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String keyName = "*** Key name ***";
        String uploadFileName = "*** File path ***";
        String targetKeyName = "*** Target key name ***";

        // Create an encryption key.
        KEY_GENERATOR = KeyGenerator.getInstance("AES");
        KEY_GENERATOR.init(256, new SecureRandom());
        SSE_KEY = new SSECustomerKey(KEY_GENERATOR.generateKey());

        try {
            S3_CLIENT = AmazonS3ClientBuilder.standard()
```

```
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();

            // Upload an object.
            uploadObject(bucketName, keyName, new File(uploadFileName));

            // Download the object.
            downloadObject(bucketName, keyName);

            // Verify that the object is properly encrypted by attempting to
retrieve it
            // using the encryption key.
            retrieveObjectMetadata(bucketName, keyName);

            // Copy the object into a new object that also uses SSE-C.
            copyObject(bucketName, keyName, targetKeyName);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }

    private static void uploadObject(String bucketName, String keyName, File file) {
        PutObjectRequest putRequest = new PutObjectRequest(bucketName, keyName,
file).withSSECustomerKey(SSE_KEY);
        S3_CLIENT.putObject(putRequest);
        System.out.println("Object uploaded");
    }

    private static void downloadObject(String bucketName, String keyName) throws
IOException {
        GetObjectRequest getObjectRequest = new GetObjectRequest(bucketName,
keyName).withSSECustomerKey(SSE_KEY);
        S3Object object = S3_CLIENT.getObject(getObjectRequest);

        System.out.println("Object content: ");
        displayTextInputStream(object.getObjectContent());
    }
```

```
    private static void retrieveObjectMetadata(String bucketName, String keyName) {
        GetObjectMetadataRequest getMetadataRequest = new
 GetObjectMetadataRequest(bucketName, keyName)
                .withSSECustomerKey(SSE_KEY);
        ObjectMetadata objectMetadata =
 S3_CLIENT.getObjectMetadata(getMetadataRequest);
        System.out.println("Metadata retrieved. Object size: " +
 objectMetadata.getContentLength());
    }

    private static void copyObject(String bucketName, String keyName, String
 targetKeyName)
            throws NoSuchAlgorithmException {
        // Create a new encryption key for target so that the target is saved using
        // SSE-C.
        SSECustomerKey newSSEKey = new SSECustomerKey(KEY_GENERATOR.generateKey());

        CopyObjectRequest copyRequest = new CopyObjectRequest(bucketName, keyName,
 bucketName, targetKeyName)
                .withSourceSSECustomerKey(SSE_KEY)
                .withDestinationSSECustomerKey(newSSEKey);

        S3_CLIENT.copyObject(copyRequest);
        System.out.println("Object copied");
    }

    private static void displayTextInputStream(S3ObjectInputStream input) throws
 IOException {
        // Read one line at a time from the input stream and display each line.
        BufferedReader reader = new BufferedReader(new InputStreamReader(input));
        String line;
        while ((line = reader.readLine()) != null) {
            System.out.println(line);
        }
        System.out.println();
    }
}
```

.NET

> **Note**
>
> マルチパートアップロード API を使用した大きなオブジェクトのアップロードの例については、マルチパートアップロードを使用したオブジェクトのアップロード および AWS SDK の使用 (低レベル API) を参照してください。

SSE-C の詳細については、お客様が指定したキーによるサーバー側の暗号化 (SSE-C) の使用 を参照してください。コード例を設定および実行する方法の詳細については、「AWS SDK for .NET デベロッパーガイド」の「AWS SDK for .NET の開始方法」 を参照してください。

Example

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.IO;
using System.Security.Cryptography;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class SSEClientEncryptionKeyObjectOperationsTest
    {
        private const string bucketName = "*** bucket name ***";
        private const string keyName = "*** key name for new object created ***";
        private const string copyTargetKeyName = "*** key name for object copy ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 client;

        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            ObjectOpsUsingClientEncryptionKeyAsync().Wait();
        }
        private static async Task ObjectOpsUsingClientEncryptionKeyAsync()
        {
```

```
            try
            {
                // Create an encryption key.
                Aes aesEncryption = Aes.Create();
                aesEncryption.KeySize = 256;
                aesEncryption.GenerateKey();
                string base64Key = Convert.ToBase64String(aesEncryption.Key);

                // 1. Upload the object.
                PutObjectRequest putObjectRequest = await
UploadObjectAsync(base64Key);
                // 2. Download the object and verify that its contents matches what
you uploaded.
                await DownloadObjectAsync(base64Key, putObjectRequest);
                // 3. Get object metadata and verify that the object uses AES-256
encryption.
                await GetObjectMetadataAsync(base64Key);
                // 4. Copy both the source and target objects using server-side
encryption with
                //    a customer-provided encryption key.
                await CopyObjectAsync(aesEncryption, base64Key);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered ***. Message:'{0}' when writing
an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
writing an object", e.Message);
            }
        }

        private static async Task<PutObjectRequest> UploadObjectAsync(string
base64Key)
        {
            PutObjectRequest putObjectRequest = new PutObjectRequest
            {
                BucketName = bucketName,
                Key = keyName,
                ContentBody = "sample text",
                ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
```

```
                ServerSideEncryptionCustomerProvidedKey = base64Key
            };
            PutObjectResponse putObjectResponse = await
client.PutObjectAsync(putObjectRequest);
            return putObjectRequest;
        }
        private static async Task DownloadObjectAsync(string base64Key,
PutObjectRequest putObjectRequest)
        {
            GetObjectRequest getObjectRequest = new GetObjectRequest
            {
                BucketName = bucketName,
                Key = keyName,
                // Provide encryption information for the object stored in Amazon
S3.
                ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                ServerSideEncryptionCustomerProvidedKey = base64Key
            };

            using (GetObjectResponse getResponse = await
client.GetObjectAsync(getObjectRequest))
            using (StreamReader reader = new
StreamReader(getResponse.ResponseStream))
            {
                string content = reader.ReadToEnd();
                if (String.Compare(putObjectRequest.ContentBody, content) == 0)
                    Console.WriteLine("Object content is same as we uploaded");
                else
                    Console.WriteLine("Error...Object content is not same.");

                if (getResponse.ServerSideEncryptionCustomerMethod ==
ServerSideEncryptionCustomerMethod.AES256)
                    Console.WriteLine("Object encryption method is AES256, same as
we set");
                else
                    Console.WriteLine("Error...Object encryption method is not the
same as AES256 we set");

                // Assert.AreEqual(putObjectRequest.ContentBody, content);
                // Assert.AreEqual(ServerSideEncryptionCustomerMethod.AES256,
getResponse.ServerSideEncryptionCustomerMethod);
            }
        }
```

```
        private static async Task GetObjectMetadataAsync(string base64Key)
        {
            GetObjectMetadataRequest getObjectMetadataRequest = new
GetObjectMetadataRequest
            {
                BucketName = bucketName,
                Key = keyName,

                // The object stored in Amazon S3 is encrypted, so provide the
necessary encryption information.
                ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                ServerSideEncryptionCustomerProvidedKey = base64Key
            };

            GetObjectMetadataResponse getObjectMetadataResponse = await
client.GetObjectMetadataAsync(getObjectMetadataRequest);
            Console.WriteLine("The object metadata show encryption method used is:
{0}", getObjectMetadataResponse.ServerSideEncryptionCustomerMethod);
            // Assert.AreEqual(ServerSideEncryptionCustomerMethod.AES256,
getObjectMetadataResponse.ServerSideEncryptionCustomerMethod);
        }
        private static async Task CopyObjectAsync(Aes aesEncryption, string
base64Key)
        {
            aesEncryption.GenerateKey();
            string copyBase64Key = Convert.ToBase64String(aesEncryption.Key);

            CopyObjectRequest copyRequest = new CopyObjectRequest
            {
                SourceBucket = bucketName,
                SourceKey = keyName,
                DestinationBucket = bucketName,
                DestinationKey = copyTargetKeyName,
                // Information about the source object's encryption.
                CopySourceServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                CopySourceServerSideEncryptionCustomerProvidedKey = base64Key,
                // Information about the target object's encryption.
                ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                ServerSideEncryptionCustomerProvidedKey = copyBase64Key
            };
            await client.CopyObjectAsync(copyRequest);
```

```
        }
    }
}
```

AWS SDK を使用してマルチパートアップロードの SSE-C を指定する

前のセクションの例では、PUT、GET、Head、および COPY オペレーションで、お客様が用意したキーによるサーバー側の暗号化 (SSE-C) をリクエストする方法を示しています。このセクションでは、SSE-C をサポートするその他の Amazon S3 API について説明します。

Java

大きなオブジェクトをアップロードするために、マルチパートアップロード API を使用できます (Amazon S3 でのマルチパートアップロードを使用したオブジェクトのアップロードとコピー を参照)。高レベル API または低レベル API を使用して、大きなオブジェクトをアップロードできます。これらの API は、リクエストでの暗号化関連のヘッダーをサポートします。

- 高レベルの `TransferManager` API を使用する場合は、`PutObjectRequest` で暗号化専用のヘッダーを指定します (「マルチパートアップロードを使用したオブジェクトのアップロード」を参照)。
- 低レベル API を使用する場合は、暗号化関連情報を `InitiateMultipartUploadRequest` で指定し、続けて各 `UploadPartRequest` で同じ暗号化情報を指定します。`CompleteMultipartUploadRequest` で暗号化専用のヘッダーを指定する必要はありません。例については、AWS SDK の使用 (低レベル API) を参照してください。

次の例では、`TransferManager` を使用してオブジェクトを作成し、SSE-C 関連の情報を提供する方法を示します。この例では、次のような処理を実行します。

- `TransferManager.upload()` メソッドを使用してオブジェクトを作成します。`PutObjectRequest` インスタンスで、リクエストする暗号キーの情報を指定します。Amazon S3 は、お客様が用意したキーを使用してオブジェクトを暗号化します。
- `TransferManager.copy()` メソッドを呼び出してオブジェクトのコピーを作成します。この例では、新しい `SSECustomerKey` を使用してオブジェクトのコピーを暗号化するように Amazon S3 に指示します。ソースオブジェクトは SSE-C で暗号化されているため、`CopyObjectRequest` はソースオブジェクトの暗号化キーを提供し、Amazon S3 で復号してからコピーできるようにします。

Example

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.CopyObjectRequest;
import com.amazonaws.services.s3.model.PutObjectRequest;
import com.amazonaws.services.s3.model.SSECustomerKey;
import com.amazonaws.services.s3.transfer.Copy;
import com.amazonaws.services.s3.transfer.TransferManager;
import com.amazonaws.services.s3.transfer.TransferManagerBuilder;
import com.amazonaws.services.s3.transfer.Upload;

import javax.crypto.KeyGenerator;
import java.io.File;
import java.security.SecureRandom;

public class ServerSideEncryptionCopyObjectUsingHLwithSSEC {

    public static void main(String[] args) throws Exception {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String fileToUpload = "*** File path ***";
        String keyName = "*** New object key name ***";
        String targetKeyName = "*** Key name for object copy ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withRegion(clientRegion)
                    .withCredentials(new ProfileCredentialsProvider())
                    .build();
            TransferManager tm = TransferManagerBuilder.standard()
                    .withS3Client(s3Client)
                    .build();

            // Create an object from a file.
            PutObjectRequest putObjectRequest = new PutObjectRequest(bucketName,
 keyName, new File(fileToUpload));

            // Create an encryption key.
```

```
            KeyGenerator keyGenerator = KeyGenerator.getInstance("AES");
            keyGenerator.init(256, new SecureRandom());
            SSECustomerKey sseCustomerEncryptionKey = new
 SSECustomerKey(keyGenerator.generateKey());

            // Upload the object. TransferManager uploads asynchronously, so this
 call
            // returns immediately.
            putObjectRequest.setSSECustomerKey(sseCustomerEncryptionKey);
            Upload upload = tm.upload(putObjectRequest);

            // Optionally, wait for the upload to finish before continuing.
            upload.waitForCompletion();
            System.out.println("Object created.");

            // Copy the object and store the copy using SSE-C with a new key.
            CopyObjectRequest copyObjectRequest = new CopyObjectRequest(bucketName,
 keyName, bucketName, targetKeyName);
            SSECustomerKey sseTargetObjectEncryptionKey = new
 SSECustomerKey(keyGenerator.generateKey());
            copyObjectRequest.setSourceSSECustomerKey(sseCustomerEncryptionKey);

 copyObjectRequest.setDestinationSSECustomerKey(sseTargetObjectEncryptionKey);

            // Copy the object. TransferManager copies asynchronously, so this call
 returns
            // immediately.
            Copy copy = tm.copy(copyObjectRequest);

            // Optionally, wait for the upload to finish before continuing.
            copy.waitForCompletion();
            System.out.println("Copy complete.");
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

.NET

大きなオブジェクトをアップロードするために、マルチパートアップロード API を使用できます (「Amazon S3 でのマルチパートアップロードを使用したオブジェクトのアップロードとコピー」を参照)。AWSSDK for .NET には、大きなオブジェクトをアップロードするため、高レベルおよび低レベルの両方の API が用意されています。これらの API は、リクエストでの暗号化関連のヘッダーをサポートします。

- 高レベルの Transfer-Utility API を使用するときには、次に示すように TransferUtilityUploadRequest で暗号化固有のヘッダーを提供します。コード例については、マルチパートアップロードを使用したオブジェクトのアップロード を参照してください。

```
TransferUtilityUploadRequest request = new TransferUtilityUploadRequest()
{
    FilePath = filePath,
    BucketName = existingBucketName,
    Key = keyName,
    // Provide encryption information.
    ServerSideEncryptionCustomerMethod =
 ServerSideEncryptionCustomerMethod.AES256,
    ServerSideEncryptionCustomerProvidedKey = base64Key,
};
```

- 低レベル API を使用する場合は、マルチパートアップロードの開始リクエストで暗号化関連情報を提供し、以降のパートのアップロードリクエストでは同じ暗号化情報を提供します。マルチパートアップロードの完了リクエストでは、暗号化固有のヘッダーを提供する必要はありません。例については、AWS SDK の使用 (低レベル API) を参照してください。

  既存の大きなオブジェクトをコピーする低レベルのマルチパートアップロードの例を次に示します。この例では、コピーされるオブジェクトは SSE-C を使用して Amazon S3 に保存されており、ターゲットオブジェクトも SSE-C を使用して保存します。例えば、以下を実行します。

  - 暗号化キーと関連情報を提供することによって、マルチパートアップロードのリクエストを開始します。
  - CopyPartRequest でソースオブジェクトとターゲットオブジェクトの暗号化キーを提供します。

- オブジェクトメタデータを取得することによって、コピーされるソースオブジェクトのサイズを取得します。
- 5 MB のパート単位でオブジェクトをアップロードします。

Example

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Collections.Generic;
using System.IO;
using System.Security.Cryptography;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class SSECLowLevelMPUcopyObjectTest
    {
        private const string existingBucketName = "*** bucket name ***";
        private const string sourceKeyName      = "*** source object key name
 ***";
        private const string targetKeyName      = "*** key name for the target
 object ***";
        private const string filePath           = @"*** file path ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;
        static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            CopyObjClientEncryptionKeyAsync().Wait();
        }

        private static async Task CopyObjClientEncryptionKeyAsync()
        {
            Aes aesEncryption = Aes.Create();
            aesEncryption.KeySize = 256;
            aesEncryption.GenerateKey();
            string base64Key = Convert.ToBase64String(aesEncryption.Key);
```

```
            await CreateSampleObjUsingClientEncryptionKeyAsync(base64Key,
s3Client);

            await CopyObjectAsync(s3Client, base64Key);
        }
        private static async Task CopyObjectAsync(IAmazonS3 s3Client, string
base64Key)
        {
            List<CopyPartResponse> uploadResponses = new List<CopyPartResponse>();

            // 1. Initialize.
            InitiateMultipartUploadRequest initiateRequest = new
InitiateMultipartUploadRequest
            {
                BucketName = existingBucketName,
                Key = targetKeyName,
                ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                ServerSideEncryptionCustomerProvidedKey = base64Key,
            };

            InitiateMultipartUploadResponse initResponse =
                await s3Client.InitiateMultipartUploadAsync(initiateRequest);

            // 2. Upload Parts.
            long partSize = 5 * (long)Math.Pow(2, 20); // 5 MB
            long firstByte = 0;
            long lastByte = partSize;

            try
            {
                // First find source object size. Because object is stored
encrypted with
                // customer provided key you need to provide encryption
information in your request.
                GetObjectMetadataRequest getObjectMetadataRequest = new
GetObjectMetadataRequest()
                {
                    BucketName = existingBucketName,
                    Key = sourceKeyName,
                    ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                    ServerSideEncryptionCustomerProvidedKey = base64Key // " *
**source object encryption key ***"
```

```
                };

                GetObjectMetadataResponse getObjectMetadataResponse = await
s3Client.GetObjectMetadataAsync(getObjectMetadataRequest);

                long filePosition = 0;
                for (int i = 1; filePosition <
getObjectMetadataResponse.ContentLength; i++)
                {
                    CopyPartRequest copyPartRequest = new CopyPartRequest
                    {
                        UploadId = initResponse.UploadId,
                        // Source.
                        SourceBucket = existingBucketName,
                        SourceKey = sourceKeyName,
                        // Source object is stored using SSE-C. Provide encryption
information.
                        CopySourceServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                        CopySourceServerSideEncryptionCustomerProvidedKey =
base64Key, //"***source object encryption key ***",
                        FirstByte = firstByte,
                        // If the last part is smaller then our normal part size
then use the remaining size.
                        LastByte = lastByte >
getObjectMetadataResponse.ContentLength ?
                            getObjectMetadataResponse.ContentLength - 1 :
lastByte,

                        // Target.
                        DestinationBucket = existingBucketName,
                        DestinationKey = targetKeyName,
                        PartNumber = i,
                        // Encryption information for the target object.
                        ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                        ServerSideEncryptionCustomerProvidedKey = base64Key
                    };
                    uploadResponses.Add(await
s3Client.CopyPartAsync(copyPartRequest));
                    filePosition += partSize;
                    firstByte += partSize;
                    lastByte += partSize;
                }
```

```
                // Step 3: complete.
                CompleteMultipartUploadRequest completeRequest = new
CompleteMultipartUploadRequest
                {
                    BucketName = existingBucketName,
                    Key = targetKeyName,
                    UploadId = initResponse.UploadId,
                };
                completeRequest.AddPartETags(uploadResponses);

                CompleteMultipartUploadResponse completeUploadResponse =
                    await s3Client.CompleteMultipartUploadAsync(completeRequest);
            }
            catch (Exception exception)
            {
                Console.WriteLine("Exception occurred: {0}", exception.Message);
                AbortMultipartUploadRequest abortMPURequest = new
AbortMultipartUploadRequest
                {
                    BucketName = existingBucketName,
                    Key = targetKeyName,
                    UploadId = initResponse.UploadId
                };
                s3Client.AbortMultipartUpload(abortMPURequest);
            }
        }
        private static async Task
CreateSampleObjUsingClientEncryptionKeyAsync(string base64Key, IAmazonS3
s3Client)
        {
            // List to store upload part responses.
            List<UploadPartResponse> uploadResponses = new
List<UploadPartResponse>();

            // 1. Initialize.
            InitiateMultipartUploadRequest initiateRequest = new
InitiateMultipartUploadRequest
            {
                BucketName = existingBucketName,
                Key = sourceKeyName,
                ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                ServerSideEncryptionCustomerProvidedKey = base64Key
```

```
            };

            InitiateMultipartUploadResponse initResponse =
               await s3Client.InitiateMultipartUploadAsync(initiateRequest);

            // 2. Upload Parts.
            long contentLength = new FileInfo(filePath).Length;
            long partSize = 5 * (long)Math.Pow(2, 20); // 5 MB

            try
            {
                long filePosition = 0;
                for (int i = 1; filePosition < contentLength; i++)
                {
                    UploadPartRequest uploadRequest = new UploadPartRequest
                    {
                        BucketName = existingBucketName,
                        Key = sourceKeyName,
                        UploadId = initResponse.UploadId,
                        PartNumber = i,
                        PartSize = partSize,
                        FilePosition = filePosition,
                        FilePath = filePath,
                        ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                        ServerSideEncryptionCustomerProvidedKey = base64Key
                    };

                    // Upload part and add response to our list.
                    uploadResponses.Add(await
s3Client.UploadPartAsync(uploadRequest));

                    filePosition += partSize;
                }

                // Step 3: complete.
                CompleteMultipartUploadRequest completeRequest = new
CompleteMultipartUploadRequest
                {
                    BucketName = existingBucketName,
                    Key = sourceKeyName,
                    UploadId = initResponse.UploadId,
                    //PartETags = new List<PartETag>(uploadResponses)
```

```
                };
                completeRequest.AddPartETags(uploadResponses);

                CompleteMultipartUploadResponse completeUploadResponse =
                    await s3Client.CompleteMultipartUploadAsync(completeRequest);

            }
            catch (Exception exception)
            {
                Console.WriteLine("Exception occurred: {0}", exception.Message);
                AbortMultipartUploadRequest abortMPURequest = new
 AbortMultipartUploadRequest
                {
                    BucketName = existingBucketName,
                    Key = sourceKeyName,
                    UploadId = initResponse.UploadId
                };
                await s3Client.AbortMultipartUploadAsync(abortMPURequest);
            }
        }
    }
}
```

クライアント側の暗号化を使用したデータの保護

クライアント側の暗号化は、データをローカルで暗号化することで、転送時および保管時のセキュリティを確保するためのものです。Amazon S3 に送信する前にオブジェクトを暗号化するには、Amazon S3 暗号化クライアントを使用します。オブジェクトがこの方法で暗号化されている場合、オブジェクトは AWS を含むサードパーティーに公開されません。Amazon S3 は、すでに暗号化されているオブジェクトを受け取るだけで、オブジェクトの暗号化または復号には関与しません。Amazon S3 暗号化クライアントとサーバー側の暗号化の両方を使用してデータを暗号化できます。暗号化されたオブジェクトを Amazon S3 に送信すると、Amazon S3 はオブジェクトを暗号化されているとは認識せず、一般的なオブジェクトのみを検出します。

Amazon S3 暗号化クライアントは、お客様と Amazon S3 の間の仲介役として機能します。Amazon S3 暗号化クライアントをインスタンス化すると、オブジェクトは、Amazon S3 `PutObject` および `GetObject` リクエストの一部として自動的に暗号化および復号化されます。オブジェクトはすべて、一意のデータキーで暗号化されます。Amazon S3 暗号化クライアントは、ラップキーとして KMS キーを指定した場合でも、バケットキーを使用したり、バケットキーを操作したりしません。

Amazon S3 暗号化クライアント開発者ガイドは、Amazon S3 暗号化クライアントのバージョン 3.0 以降に焦点を当てています。詳細については、Amazon S3 暗号化クライアントデベロッパーガイドの「What is the Amazon S3 Encryption Client?」(Amazon S3 暗号化クライアントとは) を参照してください。

Amazon S3 暗号化クライアントの以前のバージョンの詳細については、プログラミング言語に応じた AWS SDK デベロッパーガイドを参照してください。

- AWS SDK for Java
- AWS SDK for .NET
- AWS SDK for Go
- AWS SDK for PHP
- AWS SDK for Ruby
- AWS SDK for C++

インターネットトラフィックのプライバシー

このトピックでは、Amazon S3 でサービスから他の口ケーションまでの接続を保護する方法について説明します。

サービスとオンプレミスのクライアントおよびアプリケーションとの間のトラフィック

次の接続は、プライベートネットワークと AWS PrivateLink との間の接続を提供する AWS と組み合わせられます。

- AWS Site-to-Site VPN 接続。詳細については、AWS Site-to-Site VPN とは何ですか? を参照してください。
- AWS Direct Connect 接続。詳細については、AWS Direct Connect とは を参照してください。

ネットワークを経由した Amazon S3 へのアクセスは、AWS が発行する API を介して行われます。クライアントは Transport Layer Security (TLS) 1.2 をサポートしている必要があります。TLS 1.3 をお勧めします。クライアントは、Ephemeral Diffie-Hellman (DHE) や Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) などの Perfect Forward Secrecy (PFS) を備えた暗号スイートもサポートする必要があります。これらのモードは、Java 7 以降など、最近のほとんどのシステムでサポートされて

います。また、リクエストには、IAM プリンシパルに関連付けられたアクセスキー ID およびシークレットアクセスキーによる署名が必要です。または、リクエストへの署名のために一時的にセキュリティ認証情報を生成する AWS Security Token Service (STS) を使用することもできます。

同じリージョン内の AWS リソース間のトラフィック

Amazon S3 の 仮想プライベートクラウド (VPC) エンドポイントは、Amazon S3 への接続のみを許可する VPC 内の論理エンティティです。VPC はリクエストを Amazon S3 にルーティングし、レスポンスを VPC にルーティングします。詳細については、VPC ユーザーガイドの VPC エンドポイント を参照してください。VPC エンドポイントから S3 バケットへのアクセスをコントロールするために使用できるバケットポリシーの例については、バケットポリシーを使用した VPC エンドポイントからのアクセスコントロール を参照してください。

AWS PrivateLink for Amazon S3

AWS PrivateLink for Amazon S3 では、Virtual Private Cloud (VPC) でインターフェイス VPC エンドポイント (インターフェイスエンドポイント) をプロビジョニングできます。これらのエンドポイントは、VPN および AWS Direct Connect 経由でオンプレミスにあるアプリケーション、または VPC ピアリング経由で別の AWS リージョン にあるアプリケーションから直接アクセスできます。

インターフェイスエンドポイントは、VPC 内のサブネットからプライベート IP アドレスが割り当てられた 1 つ以上の Elastic Network Interface (ENI) で表されます。インターフェイスエンドポイントを介した Amazon S3 へのリクエストは、Amazon ネットワークに残ります。AWS Direct Connect または AWS Virtual Private Network (AWS VPN) を介して、オンプレミスのアプリケーションから VPC 内のインターフェイスエンドポイントにアクセスすることもできます。VPC をオンプレミスネットワークに接続する方法の詳細については、AWS Direct Connect ユーザーガイドおよび AWS Site-to-Site VPN ユーザーガイドを参照してください。

インターフェイスエンドポイントの一般的な情報については、AWS PrivateLink ガイドのインターフェイス VPC エンドポイント (AWS PrivateLink) を参照してください。

トピック

- Amazon S3 の VPC エンドポイントのタイプ
- AWS PrivateLink for Amazon S3 の制約と制限
- VPC エンドポイントの作成
- Amazon S3 インターフェイスエンドポイントへのアクセス
- プライベート DNS

- S3 インターフェイスエンドポイントからバケット、アクセスポイント、および Amazon S3 コントロール API オペレーションにアクセスする
- オンプレミスの DNS 設定の更新
- Amazon S3 用の VPC エンドポイントポリシーの作成

Amazon S3 の VPC エンドポイントのタイプ

Amazon S3 へのアクセスには、ゲートウェイエンドポイントとインターフェイスエンドポイント (AWS PrivateLink を使用) の 2 つのタイプの VPC エンドポイントを使用できます。ゲートウェイエンドポイントは、AWS ネットワーク経由で VPC から Amazon S3 にアクセスするために、ルートテーブルで指定するゲートウェイです。インターフェイスエンドポイントは、プライベート IP アドレスを使用して、VPC 内、オンプレミス、または VPC ピアリングや AWS リージョン を使用する別の AWS Transit Gateway にある VPC から Amazon S3 にリクエストをルーティングすることにより、ゲートウェイエンドポイントの機能を拡張します。詳細については、「VPC ピア機能とは」および「Transit Gateway vs VPC peering」(Transit Gateway と VPC ピアリング) を参照してください。

インターフェイスエンドポイントは、ゲートウェイエンドポイントと互換性があります。VPC 内に既存のゲートウェイエンドポイントがある場合は、同じ VPC で両方のタイプのエンドポイントを使用できます。

Amazon S3 のゲートウェイエンドポイント	Amazon S3 のインターフェイスエンドポイント
いずれの場合も、ネットワークトラフィックは AWS ネットワーク上に残ります。	
Amazon S3 パブリック IP アドレスを使用する	VPC のプライベート IP アドレスを使用して Amazon S3 にアクセスする
同じ Amazon S3 DNS 名を使用する	エンドポイント固有の Amazon S3 DNS 名を要求する
オンプレミスからのアクセスを許可しない	オンプレミスからのアクセスを許可する
別の AWS リージョン からのアクセスを許可しない	VPC ピアリングまたは AWS Transit Gateway を使用する別の AWS リージョンにある VPC からのアクセスを許可する

Amazon S3 のゲートウェイエンドポイント	Amazon S3 のインターフェイスエンドポイント
課金されない	請求される

ゲートウェイエンドポイントの詳細については、AWS PrivateLink ガイドのゲートウェイ VPC エンドポイントを参照してください。

AWS PrivateLink for Amazon S3 の制約と制限

VPC 制限は、AWS PrivateLink for Amazon S3 に適用されます。詳細については、AWS PrivateLink ガイドの「インターフェイスエンドポイントの考慮事項」と「AWS PrivateLink クォータ」を参照してください。また、以下の制約も適用されます。

AWS PrivateLink for Amazon S3 では、以下はサポートされていません。

- 連邦情報処理規格 (FIPS) エンドポイント
- ウェブサイトエンドポイント
- レガシーグローバルエンドポイント
- S3 ダッシュリージョンのエンドポイント
- デュアルスタックのエンドポイント
- 異なる AWS リージョン のバケット間での CopyObject または UploadPartCopy の使用
- Transport Layer Security (TLS) 1.0
- Transport Layer Security (TLS) 1.1
- Transport Layer Security (TLS) 1.3

VPC エンドポイントの作成

VPC インターフェイスエンドポイントを作成するには、AWS PrivateLink ガイドの「VPC エンドポイントの作成」を参照してください。

Amazon S3 インターフェイスエンドポイントへのアクセス

インターフェイスエンドポイントを作成すると、Amazon S3 はエンドポイント固有の 2 つのタイプの S3 DNS 名 (Regional および zonal) を生成します。

- Regional DNS 名には、一意の VPC エンドポイント ID、サービス識別子、AWS リージョン、およびその名前の vpce.amazonaws.com が含まれます。例えば、VPC エンドポイント ID *vpce-1a2b3c4d* の場合、生成される DNS 名は *vpce-1a2b3c4d-5e6f*.s3.us-east-1.vpce.amazonaws.com に似ている場合があります。
- Zonal DNS 名には、アベイラビリティーゾーンが含まれます (*vpce-1a2b3c4d-5e6f*-**us-east-1a.**s3.us-east-1.vpce.amazonaws.com など)。このオプションは、アーキテクチャがアベイラビリティーゾーンを分離する場合に使用できます。例えば、障害を隔離し、リージョン間のデータ転送コストを削減するために使用できます。

エンドポイント固有の S3 DNS 名は、S3 パブリック DNS ドメインから解決できます。

プライベート DNS

VPC インターフェイスエンドポイント用のプライベート DNS オプションを使用すると、VPC エンドポイント経由の S3 トラフィックのルーティングが簡単になり、アプリケーションで使用できる最も低コストのネットワークパスを活用できます。プライベート DNS オプションを使用すると、インターフェイスエンドポイントのエンドポイント固有の DNS 名を使用するように S3 クライアントを更新したり、DNS インフラストラクチャを管理したりすることなく、Regional S3 トラフィックをルーティングできます。プライベート DNS 名を有効にすると、Regional S3 DNS クエリは次のエンドポイントの AWS PrivateLink のプライベート IP アドレスに解決されます。

- Regional バケットエンドポイント (例: s3.us-east-1.amazonaws.com)
- 制御エンドポイント (例: s3-control.us-east-1.amazonaws.com)
- アクセスポイントエンドポイント (例: s3-accesspoint.us-east-1.amazonaws.com)

AWS PrivateLink for Amazon S3 は Amazon S3 デュアルスタックエンドポイントの使用をサポートしていません。プライベート DNS 名として S3 デュアルスタック DNS 名を使用する場合、IPv6 トラフィックはドロップされるか、仮想プライベートクラウド (VPC) にインターネットゲートウェイがある場合、IPv6 トラフィックは VPC のインターネットゲートウェイ経由でルーティングされます。

VPC にゲートウェイエンドポイントがある場合は、VPC 内リクエストを既存の S3 ゲートウェイエンドポイントに、オンプレミスリクエストをインターフェイスエンドポイントに自動的にルーティングできます。このアプローチでは、VPC 内のトラフィックに課金されないゲートウェイエンドポイントを使用することで、ネットワークコストを最適化できます。オンプレミスアプリケーションは、インバウンドリゾルバーエンドポイントを利用して AWS PrivateLink を使用できます。Amazon は、「Route 53 Resolver」と呼ばれる VPC 用の DNS サーバーを提供しています。インバウンドリゾル

バーエンドポイントは、DNS クエリをオンプレミスネットワークから Route 53 Resolver に転送します。

> **Important**
>
> [インバウンドエンドポイントでのみプライベート DNS を有効にする] を使用するときに最も低コストのネットワークパスを利用するには、ゲートウェイエンドポイントが VPC に存在している必要があります。ゲートウェイエンドポイントが存在すると、[インバウンドエンドポイントでのみプライベート DNS を有効にする] オプションが選択されている場合でも、VPC 内のトラフィックは常に AWS プライベートネットワーク経由でルーティングされます。[インバウンドエンドポイントでのみプライベート DNS を有効にする] オプションが選択されている間は、このゲートウェイエンドポイントを維持する必要があります。ゲートウェイエンドポイントを削除する場合は、まず [インバウンドエンドポイントでのみプライベート DNS を有効にする] をオフにする必要があります。
>
> 既存のインターフェイスエンドポイントを [インバウンドエンドポイントでのみプライベート DNS を有効にする] に更新する場合は、まず VPC に S3 ゲートウェイエンドポイントがあることを確認します。ゲートウェイエンドポイントとプライベート DNS 名の管理の詳細については、AWS PrivateLink ガイドの「ゲートウェイ VPC エンドポイント」と「VPC エンドポイントサービスの DNS 名を管理する」をそれぞれ参照してください。

[インバウンドエンドポイントでのみプライベート DNS を有効にする] オプションは、ゲートウェイエンドポイントをサポートするサービスでのみ使用できます。

[インバウンドエンドポイントでのみプライベート DNS を有効にする] を使用する VPC エンドポイントの作成の詳細については、AWS PrivateLink ガイドのの「VPC エンドポイントの作成」を参照してください。

Amazon VPC コンソールの使用

コンソールには、[DNS 名を有効にする] と [インバウンドエンドポイントに対してのみプライベート DNS を有効にする] の 2 つのオプションがあります。[DNS 名を有効にする] は、AWS PrivateLink でサポートされているオプションです。[DNS 名を有効にする] オプションを使用すると、デフォルトのパブリックエンドポイント DNS 名にリクエストを送信しながら、Amazon S3 への Amazon のプライベート接続を使用できます。このオプションを有効にすると、お客様はアプリケーションで使用できる最も低コストのネットワークパスを利用できます。

Amazon S3 の既存または新しい VPC インターフェイスエンドポイントでプライベート DNS 名を有効にすると、デフォルトで [インバウンドエンドポイントに対してのみプライベート DNS を有効に

する] オプションが選択されます。このオプションを選択すると、アプリケーションはオンプレミストラフィックのインターフェイスエンドポイントのみを使用します。この VPC 内トラフィックは、低コストのゲートウェイエンドポイントを自動的に使用します。または、[インバウンドエンドポイントのみプライベート DNS を有効にする] をオフにして、すべての S3 リクエストをインターフェイスエンドポイントにルーティングすることもできます。

AWS CLI の使用

`PrivateDnsOnlyForInboundResolverEndpoint` の値を指定しない場合は、デフォルトで `true` になります。ただし、VPC は設定を適用する前に、VPC にゲートウェイエンドポイントが存在することを確認します。ゲートウェイエンドポイントが VPC に存在する場合、呼び出しは成功します。そうでない場合は、以下のエラーメッセージが表示されます。

PrivateDnsOnlyForInboundResolverEndpoint を true に設定するには、VPC *vpce_id* にサービスのゲートウェイエンドポイントが必要です。

新しい VPC インターフェイスエンドポイントの場合

`private-dns-enabled` および `dns-options` 属性を使用して、コマンドラインからプライベート DNS を有効にします。`dns-options` 属性の `PrivateDnsOnlyForInboundResolverEndpoint` オプションは `true` に設定する必要があります。*user input placeholders* を、ユーザー自身の情報に置き換えます。

```
aws ec2 create-vpc-endpoint \
--region us-east-1 \
--service-name s3-service-name \
--vpc-id client-vpc-id \
--subnet-ids client-subnet-id \
--vpc-endpoint-type Interface  \
--private-dns-enabled  \
--ip-address-type ip-address-type \
--dns-options PrivateDnsOnlyForInboundResolverEndpoint=true \
--security-group-ids client-sg-id
```

既存の VPC エンドポイントの場合

既存の VPC エンドポイントにプライベート DNS を使用する場合は、以下のコマンド例を使用して、*user input placeholders* を独自の情報に置き換えます。

```
aws ec2 modify-vpc-endpoint \
--region us-east-1 \
--vpc-endpoint-id client-vpc-id \
--private-dns-enabled \
--dns-options PrivateDnsOnlyForInboundResolverEndpoint=false
```

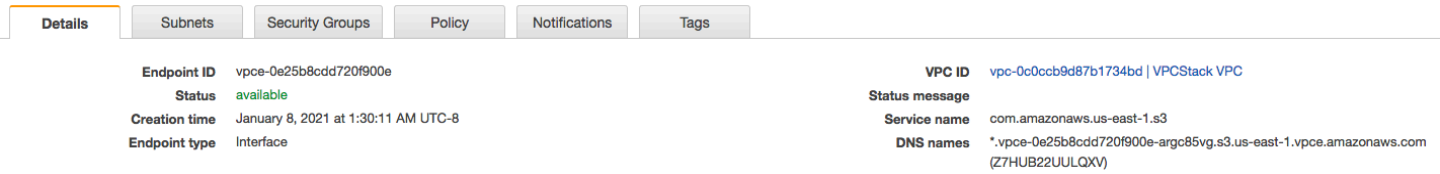
既存の VPC エンドポイントを更新して Inbound Resolver のプライベート DNS のみを有効にする場合は、次の例を使用して、サンプル値を独自の値に置き換えてください。

```
aws ec2 modify-vpc-endpoint \
--region us-east-1 \
--vpc-endpoint-id client-vpc-id \
--private-dns-enabled \
--dns-options PrivateDnsOnlyForInboundResolverEndpoint=true
```

S3 インターフェイスエンドポイントからバケット、アクセスポイント、および Amazon S3 コントロール API オペレーションにアクセスする

AWS CLI または AWS SDK を使用し、S3 インターフェイスエンドポイントを介してバケット、S3 アクセスポイント、および Amazon S3 コントロール API オペレーションにアクセスできます。

次の図は、VPC コンソールの [Details] (詳細) タブを示しています。ここでは、VPC エンドポイントの DNS 名を確認できます。この例では、VPC エンドポイント ID (vpce-id) は `vpce-0e25b8cdd720f900e` で、DNS 名は `*.vpce-0e25b8cdd720f900e-argc85vg.s3.us-east-1.vpce.amazonaws.com` です。



DNS 名を使用してリソースにアクセスする場合は、* を適切な値に置き換えてください。* の代わりに使用する適切な値は次のとおりです。

- bucket
- accesspoint
- control

例えば、バケットにアクセスするには、次のような DNS 名を使用します。

bucket.vpce-0e25b8cdd720f900e-argc85vg.s3.us-east-1.vpce.amazonaws.com

DNS 名を使用してバケット、アクセスポイント、Amazon S3 Control API オペレーションにアクセスする方法の例については、AWS CLI の例 および AWS SDK の例 の以下のセクションを参照してください。

エンドポイント固有の DNS 名の表示方法の詳細については、VPC ユーザーガイドの「Viewing endpoint service private DNS name configuration」(エンドポイントサービスのプライベート DNS 名設定の表示) を参照してください。

AWS CLI の例

AWS CLI コマンドで S3 インターフェイスエンドポイントを介して S3 バケット、S3 アクセスポイント、または Amazon S3 コントロール API 操作にアクセスするには、--region および --endpoint-url パラメータを使用します。

例: エンドポイント URL を使用したバケット内のオブジェクトのリスト化

次の例では、バケット名 *my-bucket*、リージョン *us-east-1*、VPC エンドポイント ID の DNS 名 *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* をユーザー自身の情報に置き換えます。

```
aws s3 ls s3://my-bucket/ --region us-east-1 --endpoint-url
 https://bucket.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com
```

例: エンドポイント URL を使用したアクセスポイントのオブジェクトのリスト化

- 方法 1 — アクセスポイントエンドポイントでアクセスポイントの Amazon リソースネーム (ARN) を使用する

  ARN *us-east-1:123456789012:accesspoint/accesspointexamplename*、リージョン *us-east-1*、VPC エンドポイント ID *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* をユーザー自身の情報に置き換えます。

```
aws s3api list-objects-v2 --bucket arn:aws:s3:us-east-1:123456789012:accesspoint/
accesspointexamplename --region us-east-1 --endpoint-url
 https://accesspoint.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com
```

コマンドを正常に実行できない場合は、AWS CLI を最新バージョンに更新してからやり直してください。更新手順について詳細は、AWS Command Line Interface ユーザーガイドの「AWS CLI の最新バージョンをインストールまたは更新」を参照してください。

- 方法 2 — リージョンバケットエンドポイントでアクセスポイントのエイリアスを使用する

  次の例では、アクセスポイントエイリアス *accesspointexamplename-8tyekmigicmhun8n9kwpfur39dnw4use1a-s3alias*、リージョン *us-east-1*、および VPC エンドポイント ID *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* をユーザー自身の情報に置き換えます。

  ```
  aws s3api list-objects-v2 --
  bucket accesspointexamplename-8tyekmigicmhun8n9kwpfur39dnw4use1a-s3alias
   --region us-east-1 --endpoint-url https://bucket.vpce-1a2b3c4d-5e6f.s3.us-
  east-1.vpce.amazonaws.com
  ```

- 方法 3 — アクセスポイントのエイリアスをアクセスポイントエンドポイントで使用する

  まず、バケットをホスト名の一部として含む S3 エンドポイントを作成するには、`aws s3api` が使用するアドレス指定スタイルを `virtual` に設定します。`AWS configure` の詳細については、AWS Command Line Interface ユーザーガイドの「設定ファイルと認証情報ファイルの設定」を参照してください。

  ```
  aws configure set default.s3.addressing_style virtual
  ```

  次に、次の例では、アクセスポイントのエイリアス *accesspointexamplename-8tyekmigicmhun8n9kwpfur39dnw4use1a-s3alias*、リージョン *us-east-1*、VPC エンドポイント ID *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* をユーザー自身の情報に置き換えます。アクセスポイントエイリアスの詳細については、「汎用バケットのアクセスポイントのエイリアス」を参照してください。

  ```
  aws s3api list-objects-v2 --
  bucket accesspointexamplename-8tyekmigicmhun8n9kwpfur39dnw4use1a-s3alias --
  ```

```
region us-east-1 --endpoint-url https://accesspoint.vpce-1a2b3c4d-5e6f.s3.us-
east-1.vpce.amazonaws.com
```

例: エンドポイント URL を使用して、S3 コントロール API オペレーションでジョブを一覧表示する

次の例では、リージョン *us-east-1*、VPC エンドポイント ID *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com*、およびアカウント ID *12345678* をユーザー自身の情報に置き換えます。

```
aws s3control --region us-east-1 --endpoint-url
 https://control.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com list-jobs --
account-id 12345678
```

AWS SDK の例

AWS SDK を使用する際に S3 インターフェイス エンドポイントを介して S3 バケット、S3 アクセスポイント、または Amazon S3 コントロール API オペレーションにアクセスするには、SDK を最新バージョンに更新します。S3 インターフェイスエンドポイントを介してバケット、アクセスポイント、または S3 コントロール API オペレーションにアクセスするためのエンドポイント URL を使用するようにクライアントを設定します。

SDK for Python (Boto3)

例: エンドポイント URL を使用して S3 バケットにアクセスする

次の例では、リージョン *us-east-1* および VPC エンドポイント ID *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* をユーザー自身の情報に置き換えます。

```
s3_client = session.client(
service_name='s3',
region_name='us-east-1',
endpoint_url='https://bucket.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com'
)
```

例: エンドポイント URL を使用して S3 アクセスポイントにアクセスする

次の例では、リージョン *us-east-1* および VPC エンドポイント ID *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* をユーザー自身の情報に置き換えます。

```
ap_client = session.client(
service_name='s3',
region_name='us-east-1',
endpoint_url='https://accesspoint.vpce-1a2b3c4d-5e6f.s3.us-
east-1.vpce.amazonaws.com'
)
```

例: エンドポイント URL を使用して Amazon S3 コントロール API にアクセスする

次の例では、リージョン *us-east-1* および VPC エンドポイント ID *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* をユーザー自身の情報に置き換えます。

```
control_client = session.client(
service_name='s3control',
region_name='us-east-1',
endpoint_url='https://control.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com'
)
```

SDK for Java 1.x

例: エンドポイント URL を使用して S3 バケットにアクセスする

次の例では、VPC エンドポイント ID *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* をユーザー自身の情報に置き換えます。

```
// bucket client
final AmazonS3 s3 = AmazonS3ClientBuilder.standard().withEndpointConfiguration(
        new AwsClientBuilder.EndpointConfiguration(
                "https://bucket.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com",
                Regions.DEFAULT_REGION.getName()
        )
).build();
List<Bucket> buckets = s3.listBuckets();
```

例: エンドポイント URL を使用して S3 アクセスポイントにアクセスする

次の例では、VPC エンドポイント ID *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* と ARN *us-east-1:123456789012:accesspoint/prod* をユーザー自身の情報に置き換えます。

```
// accesspoint client
```

```
final AmazonS3 s3accesspoint =
 AmazonS3ClientBuilder.standard().withEndpointConfiguration(
        new AwsClientBuilder.EndpointConfiguration(
                "https://accesspoint.vpce-1a2b3c4d-5e6f.s3.us-
east-1.vpce.amazonaws.com",
                Regions.DEFAULT_REGION.getName()
        )
).build();
ObjectListing objects = s3accesspoint.listObjects("arn:aws:s3:us-
east-1:123456789012:accesspoint/prod");
```

例: エンドポイント URL を使用して Amazon S3 コントロール API オペレーションにアクセスする

次の例では、VPC エンドポイント ID *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* をユーザー自身の情報に置き換えます。

```
// control client
final AWSS3Control s3control =
 AWSS3ControlClient.builder().withEndpointConfiguration(
        new AwsClientBuilder.EndpointConfiguration(
                "https://control.vpce-1a2b3c4d-5e6f.s3.us-
east-1.vpce.amazonaws.com",
                Regions.DEFAULT_REGION.getName()
        )
).build();
final ListJobsResult jobs = s3control.listJobs(new ListJobsRequest());
```

SDK for Java 2.x

例: エンドポイント URL を使用して S3 バケットにアクセスする

次の例では、VPC エンドポイント ID *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* とリージョン *Region.US_EAST_1* をユーザー自身の情報に置き換えます。

```
// bucket client
Region region = Region.US_EAST_1;
s3Client = S3Client.builder().region(region)

 .endpointOverride(URI.create("https://bucket.vpce-1a2b3c4d-5e6f.s3.us-
east-1.vpce.amazonaws.com"))
```

```
                    .build()
```

例: エンドポイント URL を使用して S3 アクセスポイントにアクセスする

次の例では、VPC エンドポイント ID *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* とリージョン *Region.US_EAST_1* をユーザー自身の情報に置き換えます。

```
// accesspoint client
Region region = Region.US_EAST_1;
s3Client = S3Client.builder().region(region)

 .endpointOverride(URI.create("https://accesspoint.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com"))
                    .build()
```

例: エンドポイント URL を使用して Amazon S3 コントロール API にアクセスする

次の例では、VPC エンドポイント ID *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* とリージョン *Region.US_EAST_1* をユーザー自身の情報に置き換えます。

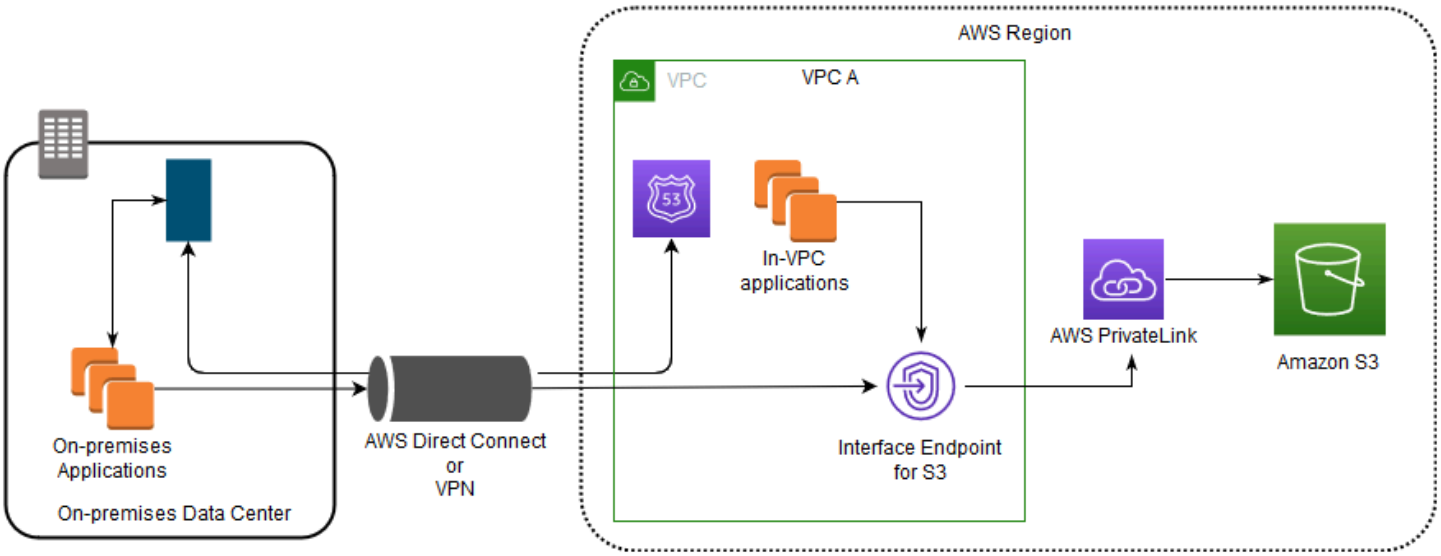
```
// control client
Region region = Region.US_EAST_1;
s3ControlClient = S3ControlClient.builder().region(region)

 .endpointOverride(URI.create("https://control.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com"))
                                  .build()
```

オンプレミスの DNS 設定の更新

エンドポイント固有の DNS 名を使用して Amazon S3 のインターフェイスエンドポイントにアクセスする場合、オンプレミス DNS リゾルバーを更新する必要はありません。パブリック Amazon S3 DNS ドメインからのインターフェイスエンドポイントのプライベート IP アドレスを使用して、エンドポイント固有の DNS 名を解決できます。

Amazon S3 にアクセスするためのインターフェイスエンドポイントの使用 (VPC 内のゲートウェイエンドポイントまたはインターネットゲートウェイの使用なし)

次の図に示すように、VPC 内のインターフェイスエンドポイントは、VPC 内アプリケーションとオンプレミスアプリケーションの両方を Amazon ネットワーク経由で Amazon S3 にルーティングできます。



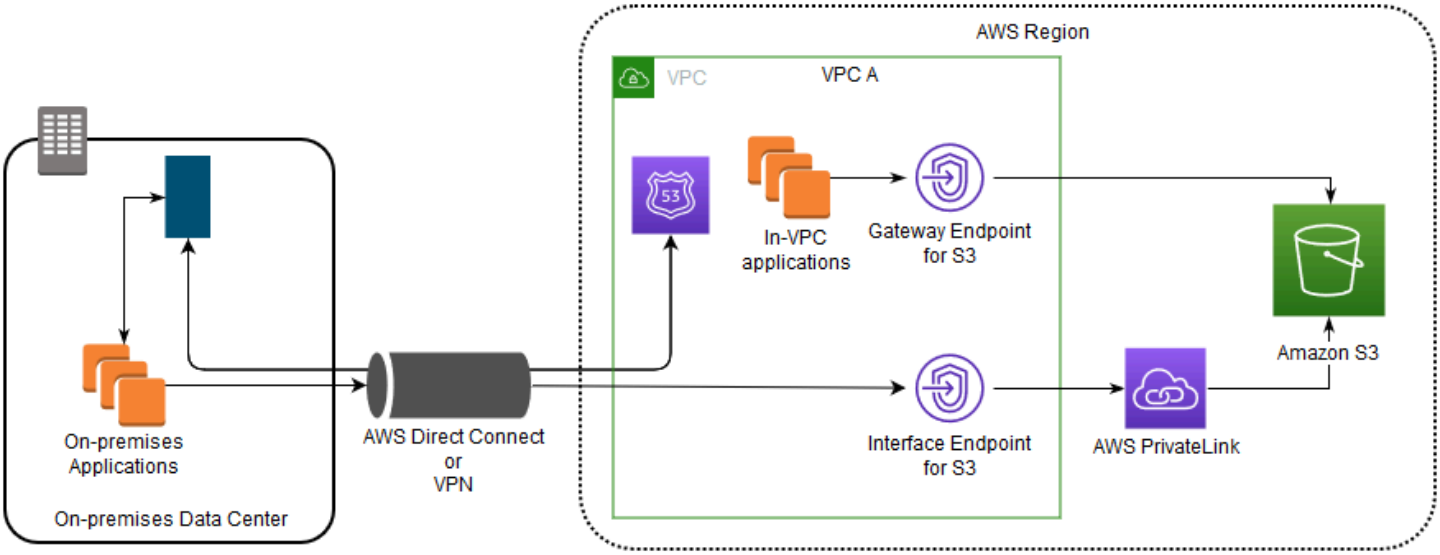
図は、以下を示しています。

- オンプレミスネットワークでは、AWS Direct Connect または AWS VPN を使用して VPC A に接続します。
- オンプレミスと VPC A のアプリケーションでは、エンドポイント固有の DNS 名を使用して S3 インターフェイスエンドポイントを介して Amazon S3 にアクセスします。
- オンプレミスのアプリケーションは、AWS Direct Connect (または AWS VPN) を介して VPC 内のインターフェイスエンドポイントにデータを送信します。AWS PrivateLink は、AWS ネットワークを経由してデータをインターフェイスエンドポイントから Amazon S3 に移動します。
- VPC 内アプリケーションは、インターフェイスエンドポイントにトラフィックの送信も行います。AWS PrivateLink は、AWS ネットワークを経由してデータをインターフェイスエンドポイントから Amazon S3 に移動します。

Amazon S3 にアクセスするための、ゲートウェイエンドポイントとインターフェイスエンドポイントの同じ VPC における併用

次の図に示すように、インターフェイスエンドポイントを作成し、同じ VPC 内に既存のゲートウェイエンドポイントを保持できます。このアプローチにより、VPC 内アプリケーションがゲート

ウェイエンドポイントを介して Amazon S3 に引き続きアクセスすることを許可します。これについての請求はありません。その後、オンプレミスのアプリケーションだけがインターフェイスエンドポイントを使用して Amazon S3 にアクセスします。この方法で Amazon S3 にアクセスするには、Amazon S3 のエンドポイント固有の DNS 名を使用するようにオンプレミスのアプリケーションを更新する必要があります。



この図表は、以下を示すものです：

- オンプレミスのアプリケーションは、エンドポイント固有の DNS 名を使用し、AWS Direct Connect (または AWS VPN) を介して VPC 内のインターフェイスエンドポイントにデータを送信します。AWS PrivateLink は、AWS ネットワークを経由してデータをインターフェイスエンドポイントから Amazon S3 に移動します。
- VPC 内アプリケーションは、デフォルトのリージョンの Amazon S3 名を使用し、AWS ネットワークを介して Amazon S3 に接続するゲートウェイエンドポイントにデータを送信します。

ゲートウェイエンドポイントの詳細については、VPC ユーザーガイドのゲートウェイ VPC エンドポイントを参照してください。

Amazon S3 用の VPC エンドポイントポリシーの作成

VPC エンドポイントに Amazon S3 へのアクセスをコントロールするエンドポイントポリシーをアタッチできます。このポリシーでは、以下の情報を指定します。

- アクションを実行できる AWS Identity and Access Management (IAM) プリンシパル
- 実行可能なアクション
- アクションを実行できるリソース

Amazon S3 バケットポリシーを使用して、バケットポリシーの aws:sourceVpce 条件を使用して、特定の VPC エンドポイントからの特定のバケットへのアクセスを制限することもできます。次の例は、バケットまたはエンドポイントへのアクセスを制限するポリシーを示しています。

トピック

- 例: VPC エンドポイントから特定のバケットへのアクセスの制限
- 例: VPC エンドポイントから特定のアカウントのバケットへのアクセスの制限
- 例: S3 バケットポリシーでの特定の VPC エンドポイントへのアクセスの制限

例: VPC エンドポイントから特定のバケットへのアクセスの制限

特定の Amazon S3 バケットへのアクセスのみを制限するエンドポイントポリシーを作成できます。このタイプのポリシーは、VPC で S3 バケットを使用する他の AWS のサービス がある場合に便利です。次のバケットポリシーは、*amzn-s3-demo-bucket1* へのアクセスのみを制限します。このエンドポイントポリシーを使用するには、*amzn-s3-demo-bucket1* をバケットの名前に置き換えます。

```
{
  "Version": "2012-10-17",
  "Id": "Policy1415115909151",
  "Statement": [
    { "Sid": "Access-to-specific-bucket-only",
      "Principal": "*",
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket1",
                   "arn:aws:s3:::amzn-s3-demo-bucket1/*"]
    }
  ]
}
```

例: VPC エンドポイントから特定のアカウントのバケットへのアクセスの制限

特定の AWS アカウント の S3 バケットへのアクセスのみを制限するエンドポイントポリシーを作成できます。VPC 内のクライアントが所有していないバケットにアクセスできないようにするには、エンドポイント ポリシーで次のステートメントを使用してください。次のステートメント例では、

単一の AWS アカウント、*111122223333* が所有するリソースへのアクセスを制限するポリシーを作成します。

```
{
  "Statement": [
    {
      "Sid": "Access-to-bucket-in-specific-account-only",
      "Principal": "*",
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Effect": "Deny",
      "Resource": "arn:aws:s3:::*",
      "Condition": {
        "StringNotEquals": {
          "aws:ResourceAccount": "111122223333"
        }
      }
    }
  ]
}
```

> **Note**
>
> アクセスされるリソースの AWS アカウント ID を指定するには、IAM ポリシーで `aws:ResourceAccount` キーまたは `s3:ResourceAccount` キーを使用できます。ただし、一部の AWS のサービス は AWS マネージドバケットへのアクセスに依存していることに注意してください。したがって、IAM ポリシーで `aws:ResourceAccount` キーまたは `s3:ResourceAccount` キーを使用することは、これらのリソースへのアクセスにも影響する可能性があります。

例: S3 バケットポリシーでの特定の VPC エンドポイントへのアクセスの制限

例: S3 バケットポリシーでの特定の VPC エンドポイントへのアクセスの制限

次の Amazon S3 バケットポリシーは、VPC エンドポイント *vpce-1a2b3c4d* からのみ、特定のバケット、*amzn-s3-demo-bucket2* へのアクセスを許可します。指定されたエンドポイントを使用していない場合、ポリシーによりバケットへのすべてのアクセスが拒否されます。`aws:sourceVpce` 条件はエンドポイントを指定し、VPC エンドポイントリソースの Amazon

リソースネーム (ARN) を必要とせず、エンドポイント ID のみを指定します。このバケットポリシーを使用するには、*amzn-s3-demo-bucket2* と *vpce-1a2b3c4d* をバケット名とエンドポイントに置き換えてください。

> **Important**
>
> - 次の Amazon S3 バケットポリシーを適用して特定の VPC エンドポイントのみへのアクセスを制限すると、バケットへのアクセスが意図せずにブロックされる場合があります。特に VPC エンドポイントからの接続に対するバケットのアクセスを制限することを目的としたバケットのポリシーにより、バケットへのすべての接続がブロックされる場合があります。この問題を修正する方法については、「バケットポリシーの VPC または VPC エンドポイント ID が間違っています。ポリシーを修正してバケットにアクセスできるようにするにはどうすれば良いですか?」(サポート ナレッジセンター) を参照してください。
> - 次のポリシーの例を使用する前に、VPC エンドポイントの ID をユースケースに応じた値に置き換えてください。そうしないと、バケットにアクセスできません。
> - このポリシーは、コンソールリクエストが指定の VPC エンドポイントを経由していない場合、指定先のバケットへのコンソールアクセスを無効にします。

```
{
  "Version": "2012-10-17",
  "Id": "Policy1415115909152",
  "Statement": [
    { "Sid": "Access-to-specific-VPCE-only",
      "Principal": "*",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket2",
                   "arn:aws:s3:::amzn-s3-demo-bucket2/*"],
      "Condition": {"StringNotEquals": {"aws:sourceVpce": "vpce-1a2b3c4d"}}
    }
  ]
}
```

ポリシーの例については、VPC ユーザーガイドの Amazon S3 のエンドポイントを参照してください。

VPC 接続の詳細については、 ホワイトペーパー Amazon Virtual Private Cloud 接続オプションAWS のネットワークから VPC への接続オプション を参照してください。

Amazon S3 のコンプライアンス検証

Amazon S3 のセキュリティおよびコンプライアンスは、以下を含む複数の AWS コンプライアンスプログラムの一環として、サードパーティーの監査者により評価されます。

- System and Organization Controls (SOC)
- Payment Card Industry Data Security Standard (PCI DSS)
- Federal Risk and Authorization Management Program (FedRAMP)
- Health Insurance Portability and Accountability Act (HIPAA)

AWS は、コンプライアンスプログラムのターゲット範囲内の AWS サービスで、特定のコンプライアンスプログラムのターゲット範囲内における AWS サービス一覧を頻繁に更新しています。

サードパーティーの監査レポートは、AWS Artifact を使用してダウンロードできます。詳細については、AWS Artifact のレポートのダウンロード を参照してください。

AWS コンプライアンスプログラムの詳細については、AWS コンプライアンスプログラム を参照してください。

Amazon S3 を使用する際のお客様のコンプライアンス責任は、組織のデータの機密性や組織のコンプライアンス目的、適用可能な法律、規制によって決定されます。Amazon S3 の使用が HIPAA、PCI、FedRAMP などの標準に準拠していることを前提としている場合、AWS は以下を支援するリソースを提供します。

- セキュリティおよびコンプライアンスのクイックスタートガイドでは、AWS のデプロイメントセキュリティやコンプライアンスに重点を置いたベースライン環境におけるアーキテクチャ上の考慮事項や手順について説明しています。
- HIPAA セキュリティおよびコンプライアンス向けアーキテクチャ設計では、企業が AWS を使用して HIPAA 要件を満たす方法について説明します。
- AWS コンプライアンスリソースを使用すると、業界や地域で使用できるワークブックとガイドとを選択できます。
- AWS Config を使用すると、社内プラクティス、業界ガイドライン、およびに対するリソースの設定の準拠状態を評価できます。
- AWS Security Hub を使用すると、AWS 内のセキュリティ状態を包括的に表示し、セキュリティ業界の標準およびベストプラクティスへの準拠を確認できます。

- S3 Object Lock を使用したオブジェクトのロックを使用すると、特定の種類の帳簿および記録情報に対して、Write Once Read Many (WORM) データストレージの使用を必須とする、金融サービス規制機関 (SEC、FINRA、CFTC など) の技術的要件を満たすことができます。
- S3 インベントリを使用したデータのカタログ化と分析 は、ビジネス、コンプライアンス、規制上のニーズに対応して、オブジェクトのレプリケーションと暗号化のステータスを監査し、レポートするのに役立ちます。

Amazon S3 の耐障害性

AWS グローバルインフラストラクチャは、リージョンおよびアベイラビリティーゾーンを中心に構築されています。AWS リージョンには、低レイテンシー、高スループット、高冗長性のネットワークで接続されている複数の物理的に独立、分離されたアベイラビリティーゾーンがあります。これらのアベイラビリティーゾーンを利用すると、アプリケーションとデータベースを効率的に設計して運用できます。アベイラビリティーゾーンは、従来の単一データセンターのインフラストラクチャや複数データセンターのインフラストラクチャよりも可用性、耐障害性、および拡張性が優れています。特に地理的に離れた場所間でデータをレプリケートする必要がある場合は、リージョン内およびリージョン間でのオブジェクトのレプリケートを使用できます。これにより、さまざまな AWS リージョンにあるバケット間でオブジェクトを自動的に非同期コピーできます。

各 AWS リージョンには、複数のアベイラビリティーゾーンがあります。耐障害性と低レイテンシーのために、同じリージョン内の複数のアベイラビリティーゾーンにアプリケーションをデプロイできます。アベイラビリティーゾーンは高速なプライベート光ファイバーネットワーキングで相互に接続されているため、アプリケーションがアベイラビリティーゾーン間で中断なく自動的にフェイルオーバーできるようなアーキテクチャを簡単に設計できます。

AWS リージョン とアベイラビリティーゾーンの詳細については、AWS グローバルインフラストラクチャ を参照してください。

Amazon S3 では、AWS グローバルインフラストラクチャに加えて、データの耐障害性とバックアップのニーズに対応できるように複数の機能を提供しています。

ライフサイクル設定

ライフサイクル設定は、Amazon S3 がオブジェクトのグループに適用するアクションを定義するルールのセットです。ライフサイクル設定ルールを使用すると、オブジェクトのより安価なストレージクラスへの移行、アーカイブ、削除を Amazon S3 に指定できます。詳細については、オブジェクトのライフサイクルの管理 を参照してください。

バージョニング

バージョニングとは、同じバケット内でオブジェクトの複数のバリアントを保持する手段です。バージョニングを使用して、Amazon S3 バケットに格納されたあらゆるオブジェクトのあらゆるバージョンを、格納、取得、復元することができます。バージョニングを使用すれば、意図しないユーザーアクションからもアプリケーション障害からも、簡単に復旧できます。詳細については、S3 バージョニングによる複数のバージョンのオブジェクトの保持 を参照してください。

S3 オブジェクトロック

S3 オブジェクトロックでは、Write Once Read Many (WORM) モデルを使用してオブジェクトを保存できます。S3 オブジェクトロックを使用すると、オブジェクトが固定期間または無期限に削除または上書きされるのを防止できます。S3 オブジェクトロックを使用して、WORM ストレージを必要とする規制要件を満たしたり、オブジェクトの変更や削除に対する保護レイヤーを追加したりできます。詳細については、S3 Object Lock を使用したオブジェクトのロック を参照してください。

ストレージクラス

Amazon S3 では、ワークロードの要件に応じて、幅広いストレージクラスが提供されています。S3 標準 — IA と S3 1 ゾーン – IA ストレージクラスは、月に約 1 回アクセスし、ミリ秒単位のアクセスが必要になるデータ用に設計されています。S3 Glacier インスタント検索ストレージクラスは、四半期に約 1 回アクセスするミリ秒のアクセスでアクセスされる長期間有効なアーカイブデータ用に設計されています。バックアップなど、即時アクセスを必要としないアーカイブデータについては、S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive ストレージクラスを使用できます。詳細については、Amazon S3 ストレージクラスの理解と管理 を参照してください。

以下のセキュリティのベストプラクティスも耐障害性に対処します。

- Enable versioning
- Consider Amazon S3 cross-region replication
- Identify and audit all your Amazon S3 buckets

Amazon S3 バックアップの暗号化

Amazon S3 を使用してバックアップを保存する場合、バックアップの暗号化は各バケットの設定によって異なります。Amazon S3 により、S3 バケットのデフォルト暗号化の動作を設定できます。バケットにデフォルト暗号化を設定して、バケットに保存される際すべてのオブジェクトが暗号化されるようにします。デフォルト暗号化は、AWS KMS に保存されたキー (SSE-KMS) をサポートしています。詳細については、Amazon S3 バケット向けのサーバー側のデフォルトの暗号化動作の設定 を参照してください。

バージョニングとオブジェクトロックの詳細については、以下のトピックを参照してください。S3 バージョニングによる複数のバージョンのオブジェクトの保持S3 Object Lock を使用したオブジェクトのロック

Amazon S3 のインフラストラクチャセキュリティ

マネージドサービスとして、Amazon S3 は AWS のセキュリティの柱で説明されたグローバルネットワークセキュリティ手順 AWSWell-Architected フレームワークによって保護されます。

ネットワークを経由した Amazon S3 へのアクセスは、AWS が発行する API を介して行われます。クライアントは Transport Layer Security (TLS) 1.2 をサポートしている必要があります。TLS 1.3 もサポートすることをお勧めします (この推奨事項の詳細については、AWS セキュリティブログの「TLS 1.3 による AWS クラウド接続の高速化」を参照してください)。

> **Note**
>
> TLS 1.3 は、Amazon S3 の AWS PrivateLink およびマルチリージョンアクセスポイントを除くすべての S3 エンドポイントでサポートされています。

また、Ephemeral Diffie-Hellman (DHE) や Elliptic Curve Ephemeral Diffie-Hellman (ECDHE) などの Perfect Forward Secrecy (PFS) を使用した暗号スイートもサポートしている必要があります。さらに、AWS Signature V4 または AWS Signature V2 を使用してリクエストに署名する必要があります。そのためには、有効な認証情報を提供する必要があります。

これらの API はネットワークの任意の場所から呼び出すことができます。ただし、Amazon S3 はリソースベースのアクセスポリシーをサポートしており、それらのポリシーには、ソース IP アドレスに基づく制限を含めることができます。Amazon S3 のバケットポリシーを使用して、特定の Virtual Private Cloud (VPC) エンドポイントまたは特定の VPC からのバケットへのアクセスを管理できます。これにより、実質的に AWS ネットワーク内の特定の VPC からのみ特定の Amazon S3 バケットへのネットワークアクセスが分離されます。詳細については、バケットポリシーを使用した VPC エンドポイントからのアクセスコントロール を参照してください。

以下のセキュリティのベストプラクティスも Amazon S3 でのインフラストラクチャのセキュリティに対処します。

- Consider VPC endpoints for Amazon S3 access
- Identify and audit all your Amazon S3 buckets

Amazon S3 での設定と脆弱性の分析

AWS は、ゲストオペレーティングシステム (OS) やデータベースへのパッチ適用、ファイアウォール設定、災害対策などの基本的なセキュリティタスクを処理します。これらの手順は適切な第三者によって確認され、証明されています。詳細については、以下のリソース を参照してください。

- Amazon S3 のコンプライアンス検証
- 責任共有モデル
- Amazon Web Services：セキュリティプロセスの概要

以下のセキュリティのベストプラクティスも Amazon S3 での設定と脆弱性の分析に対処します。

- Identify and audit all your Amazon S3 buckets
- AWS Config の有効化

アクセス管理

Amazon S3 には、さまざまなアクセス管理ツールが用意されています。以下は、これらの機能とツールのリストです。これらのアクセス管理ツールがすべて必要なわけではありませんが、Amazon S3 バケット、オブジェクト、および他の S3 リソース へのアクセスを付与するには、これらのツールを 1 つ以上使用する必要があります。これらのツールを適切に適用すると、データの整合性を維持し、目的のユーザーがリソースにアクセスできるようにするために役立ちます。

最も一般的に使用されるアクセス管理ツールは、アクセスポリシーです。アクセスポリシーは、バケットのバケットポリシーなど、AWS リソースにアタッチされたリソースベースのポリシーに指定できます。アクセスポリシーは、IAM ユーザー、グループ、ロールなどの AWS Identity and Access Management (IAM) アイデンティティにアタッチされたアイデンティティベースのポリシーに指定することもできます。アクセスポリシーでは、誰が何にアクセスできるかを記述します。アクセスポリシーを作成して、 AWS アカウントおよび IAM ユーザー、グループ、ロールにアクセス許可を付与し、リソースに対してオペレーションを実行します。例えば、他のアカウントがバケットにオブジェクトをアップロードできるように、別の AWS アカウントに `PUT Object` アクセス許可を付与できます。

Amazon S3 で使用できるアクセス管理ツールを以下に示します。Amazon S3 アクセスコントロールに関するより包括的なガイドについては、「Amazon S3 でのアクセスコントロール」を参照してください。

バケットポリシー

Amazon S3 バケットポリシーは、特定のバケットにアタッチされた JSON 形式の AWS Identity and Access Management (IAM) リソースベースのポリシーです。バケットポリシーを使用すると、バケットおよびバケット内のオブジェクトに対するアクセス許可を、他の AWS アカウントまたは IAM アイデンティティに付与できます。S3 アクセス管理の多くのユースケースは、バケットポリシーを使用することで要件が満たされます。バケットポリシーを使用すると、承認されたアイデンティティのみがリソースにアクセスしてアクションを実行できるように、バケットアクセスをパーソナライズすることができます。詳細については、「Amazon S3 のバケットポリシー」を参照してください。

ID ベースのポリシー

アイデンティティベースのポリシーまたは IAM ユーザーポリシーは、AWS Identity and Access Management (IAM) ポリシーの一種です。アイデンティティベースのポリシーは、AWSアカウントの IAM ユーザー、グループ、またはロールにアタッチされる JSON 形式のポリシーです。アイデンティティベースのポリシーを使用すると、バケットまたはオブジェクトへのアクセス許可を IAM アイデンティティに付与できます。アカウント内に IAM ユーザー、グループ、およびロールを作成し、これらにアクセスポリシーをアタッチできます。次に、Amazon S3 リソースを含む AWS リソースへのアクセス許可を付与できます。詳細については、「Amazon S3 のアイデンティティベースのポリシー」を参照してください。

S3 Access Grants

S3 Access Grants を使用して、Active Directory などの企業 ID ディレクトリ内のアイデンティティと AWS Identity and Access Management (IAM) アイデンティティの両方の Amazon S3 データへのアクセス許可を作成します。S3 Access Grants は、大規模なデータのアクセス許可の管理に役立ちます。さらに、S3 Access Grants は、エンドユーザーアイデンティティと、AWS CloudTrail での S3 データへのアクセスに使用されるアプリケーションをログに記録します。これにより、S3 バケット内のデータへのすべてのアクセスについて、エンドユーザーアイデンティティまで詳細な監査履歴が提供されます。詳細については、「S3 Access Grants でのアクセス管理」を参照してください。

アクセスポイント

Amazon S3 Access Points は、S3 の共有データセットを使用するアプリケーションの大規模なデータアクセスの管理を簡素化します。Access Points は名前付きのネットワークエンドポイントで、バケットにアタッチされます。アクセスポイントを使用すると、オブジェクトのアップロードや取得などの S3 オブジェクトオペレーションを大規模に実行できます。バケットには最大 10,000 個のアクセスポイントをアタッチできます。各アクセスポイントでは、個別のアクセス許可やネットワークコントロールを適用することで、S3 オブジェクトへのアクセスをきめ細かく制御できます。S3

Access Points は、同じアカウントまたは別の信頼されたアカウントのバケットに関連付けることができます。Access Points ポリシーは、基になるバケットポリシーと組み合わせて評価されるリソースベースのポリシーです。詳細については、「アクセスポイントを使用した汎用バケット内の共有データセットへのアクセスの管理」を参照してください。

アクセスコントロールリスト (ACL)

ACL は、アクセス許可の被付与者と付与されるアクセス許可を識別するリストです。ACL は、基本的な読み取り/書き込み許可を他の AWS アカウントに付与します。ACL では、Amazon S3 固有の XML スキーマが使用されます。ACL は、AWS Identity and Access Management (IAM) ポリシーの一種です。オブジェクト ACL は、オブジェクトへのアクセスを管理するために使用され、バケット ACL はバケットへのアクセスを管理するために使用されます。バケットポリシーはバケット全体に対して 1 つですが、オブジェクト ACL は各オブジェクトに対して指定されます。オブジェクトごとに個別にアクセスを制御する必要がある通常ではない状況を除き、ACL は無効にしておくことをお勧めします。ACL の使用方法の詳細については、オブジェクトの所有権の制御とバケットの ACL の無効化。 を参照してください。

> **Warning**
>
> Amazon S3 の最新のユースケースの大部分では ACL を使用する必要がなくなっています。

オブジェクトの所有権

オブジェクトへのアクセスを管理するには、オブジェクトの所有者である必要があります。オブジェクト所有権のバケットレベルの設定を使用すると、バケットにアップロードされたオブジェクトの所有権を制御できます。また、オブジェクト所有権を使用して、ACL を有効にします。デフォルトでは、オブジェクト所有権は [バケット所有者の強制] に設定され、すべての ACL は無効になっています。ACL が無効になっている場合、バケット所有者はバケット内のすべてのオブジェクトを所有し、データへのアクセスの管理のみを行います。アクセスを管理するために、バケット所有者は ACL を除くポリシーまたは別のアクセス管理ツールを使用します。詳細については、「オブジェクトの所有権の制御とバケットの ACL の無効化。」を参照してください。

Amazon S3 アクセスコントロールに関するより包括的なガイドとその他のベストプラクティスについては、「Amazon S3 でのアクセスコントロール」を参照してください。

Amazon S3 におけるデータ保護

AWS グローバルインフラストラクチャが提供する回復力に加えて、Amazon S3 には、偶発的な削除やリージョンの障害からデータを保護するのに役立つ多くの機能が用意されています。

S3 レプリケーション

ライブレプリケーションを使用すると、Amazon S3 バケット間でオブジェクトを自動で非同期的にコピーできます。オブジェクトのレプリケーション用に設定されたバケットは、同じ AWS アカウント が所有することも、異なるアカウントが所有することもできます。オブジェクトは、単一または複数の送信先バケットにレプリケートできます。送信先バケットは、異なる AWS リージョン でも、ソースバケットと同じリージョン内でも配置することができます。フェイルオーバーコントロールを有効にするには、レプリケーションを双方向に設定して、リージョンの障害発生時にレプリケート元バケットとレプリケート先バケットを同期させることができます。詳細については、「the section called “リージョン内およびリージョン間でのオブジェクトのレプリケート”」を参照してください。

マルチリージョンアクセスポイントとフェイルオーバーコントロール

Amazon S3 マルチリージョンアクセスポイントを使用すると、複数の AWS リージョン にある S3 バケットからのリクエストをアプリケーションが実行するために使用できるグローバルエンドポイントを作成できます。マルチリージョンアクセスポイントを使用して、単一のリージョンで使用するのと同じシンプルなアーキテクチャでマルチリージョンアプリケーションを構築し、世界中のどこでもこれらのアプリケーションを実行することができます。マルチリージョンのアクセスポイントは、輻輳したパブリックインターネット経由でリクエストを送信する代わりに、Amazon S3 へのインターネットベースのリクエストを高速化する組み込みのネットワーク耐障害性を実現します。マルチリージョンアクセスポイントのグローバルエンドポイントに対して行われたアプリケーションリクエストは、AWS Global Accelerator を使用して、AWS グローバルネットワークを介して、アクティブなルーティングステータスを持つ最も近い S3 バケットに自動的にルーティングされます。マルチリージョンアクセスポイントの詳細については、「the section called “マルチリージョントラフィックの管理 ”」を参照してください。

Amazon S3 マルチリージョンアクセスポイントのフェイルオーバーコントロールを使用すると、リージョン別トラフィックが中断してもビジネス継続性を維持できると同時に、アプリケーションをマルチリージョンアーキテクチャにしてコンプライアンスと冗長性のニーズを満たすことができます。リージョン別トラフィックが中断された場合は、マルチリージョンアクセスポイントのフェイルオーバーコントロールを使用して、Amazon S3 マルチリージョンアクセスポイントの

背後にあるどの AWS リージョン がデータアクセスとストレージのリクエストを処理するかを選択できます。

フェイルオーバーをサポートするには、マルチリージョンアクセスポイントをアクティブ/パッシブ構成に設定できます。トラフィックは通常の状態ではアクティブリージョンに流れ、パッシブリージョンはフェイルオーバー用にスタンバイになります。S3 クロスリージョンレプリケーション (CRR) を双方向のレプリケーションルールで有効にしている場合、フェイルオーバー中もバケットを同期された状態にしておくことができます。フェイルオーバーコントロールの詳細については、「the section called “フェイルオーバーの設定”」を参照してください。

S3 バージョニング

バージョニングとは、同じバケット内でオブジェクトの複数のバリアントを保持する手段です。バージョニングを使用して、Amazon S3 バケットに格納されたあらゆるオブジェクトのあらゆるバージョンを、格納、取得、復元することができます。バージョニングを使用すれば、意図しないユーザーアクションからもアプリケーション障害からも、簡単に復旧できます。詳細については、S3 バージョニングによる複数のバージョンのオブジェクトの保持 を参照してください。

S3 オブジェクトロック

S3 オブジェクトロックでは、Write Once Read Many (WORM) モデルを使用してオブジェクトを保存できます。S3 オブジェクトロックを使用すると、オブジェクトが固定期間または無期限に削除または上書きされるのを防止できます。S3 オブジェクトロックを使用して、WORM ストレージを必要とする規制要件を満たしたり、オブジェクトの変更や削除に対する保護レイヤーを追加したりできます。詳細については、「S3 Object Lock を使用したオブジェクトのロック」を参照してください。

AWS Backup

Amazon S3 は、AWS Backup とネイティブに統合されたフルマネージド型のポリシーベースのサービスであるため、バックアップポリシーを一元的に定義して、Amazon S3 内のデータを保護できます。バックアップポリシーを定義し、Amazon S3 リソースをポリシーに割り当てると、AWS Backup は Amazon S3 バックアップの作成を自動化し、バックアッププランで指定した暗号化されたバックアップボールトにバックアップを安全に保存します。詳細については、「the section called “データのバックアップ”」を参照してください。

これらの機能を使用してデータを保護することに関するチュートリアルについては、「チュートリアル: S3 バージョニング、S3 Object Lock、S3 レプリケーションを使用して Amazon S3 上のデータを誤って削除したり、アプリケーションのバグから保護したりする」を参照してください。

> **Important**
>
> 上記の機能を使用してデータを保護するだけでなく、the section called “セキュリティに関するベストプラクティス” の推奨事項を確認することをお勧めします。

トピック

- リージョン内およびリージョン間でのオブジェクトのレプリケート
- マルチリージョンアクセスポイントを使用したマルチリージョントラフィックの管理
- S3 バージョニングによる複数のバージョンのオブジェクトの保持
- S3 Object Lock を使用したオブジェクトのロック
- Amazon S3 データのバックアップ

リージョン内およびリージョン間でのオブジェクトのレプリケート

レプリケーションを使用すると、Amazon S3 バケット間でオブジェクトを自動で非同期的にコピーできます。オブジェクトのレプリケーション用に設定されたバケットは、同じ AWS アカウント が所有することも、異なるアカウントが所有することもできます。オブジェクトは、単一または複数の送信先バケットにレプリケートできます。送信先バケットは、異なる AWS リージョン でも、ソースバケットと同じリージョン内でも配置することができます。

レプリケーションには、ライブレプリケーションとオンデマンドレプリケーションの 2 種類があります。

- ライブレプリケーション – レプリケート元のバケットに書き込まれる際に、新しく作成されたオブジェクトまたは更新されたオブジェクトを自動的にレプリケートするには、ライブレプリケーションを使用します。ライブレプリケーションでは、レプリケーションを設定する前にバケットに存在していたオブジェクトはレプリケートされません。レプリケーションを設定する前に存在していたオブジェクトをレプリケートするには、オンデマンドレプリケーションを使用します。
- オンデマンドレプリケーション — レプリケート元のバケットから 1 つ以上のレプリケート先バケットにオンデマンドで既存のオブジェクトをレプリケートするには、S3 バッチレプリケーションを使用します。既存のオブジェクトのレプリケーションの詳細については、「S3 バッチレプリケーションを使用する状況」を参照してください。

ライブレプリケーションには、クロスリージョンレプリケーション (CRR) と同一リージョンレプリケーション (SRR) の 2 つの形式があります。

- クロスリージョンレプリケーション (CRR) - 異なる AWS リージョン 内の Amazon S3 バケット間でオブジェクトをレプリケートするには、CRR を使用します。CRR の詳細については、「the section called “クロスリージョンレプリケーションを使用する場合”」を参照してください。
- 同一リージョンレプリケーション (SRR) - 同じ AWS リージョン内の Amazon S3 バケット間でオブジェクトをコピーするには、SRR を使用します。SRR の詳細については、「the section called “同一リージョンレプリケーションを使用する時”」を参照してください。

トピック

- レプリケーションを使用する理由
- クロスリージョンレプリケーションを使用する場合
- 同一リージョンレプリケーションを使用する時
- 双方向レプリケーションを使用する場合
- S3 バッチレプリケーションを使用する状況
- ワークロードの要件とライブレプリケーション
- Amazon S3 がレプリケートするもの
- レプリケーションの要件と考慮事項
- ライブレプリケーションの設定の概要
- ライブレプリケーションの管理または一時停止
- バッチレプリケーションを使用した既存のオブジェクトのレプリケーション
- レプリケーションのトラブルシューティング
- メトリクス、イベント通知、ステータスによるレプリケーションのモニタリング

レプリケーションを使用する理由

レプリケーションは、以下の場合に役立ちます。

- メタデータを保持しながらオブジェクトをレプリケートする — レプリケーションを使用すると、元のオブジェクトの作成時刻やバージョン ID などのすべてのメタデータを保持するオブジェクトのコピーを作成できます。この機能は、レプリカがレプリケート元オブジェクトと同じであることを確認する必要がある場合に重要です。
- 別のストレージクラスにオブジェクトをレプリケートする – レプリケーションを使用して、オブジェクトを S3 Glacier Flexible Retrieval、S3 Glacier Deep Archive、またはレプリケート先バケットの別のストレージクラスに直接配置できます。データを同じストレージクラスにレプリケート

し、レプリケート先バケットのライフサイクル設定を使用して、オブジェクトが古くなるにつれてより古いストレージクラスに移動させることもできます。

- オブジェクトのコピーを別の所有権で保持する — レプリケート元オブジェクトの所有者に関係なく、レプリカの所有権をレプリケート先バケット所有者である AWS アカウント に変更するように Simple Storage Service (Amazon S3) に指示できます。これは 所有者オーバーライド オプションと呼ばれます。このオプションを使用すると、オブジェクトのレプリカへのアクセスを制限できます。
- 複数の AWS リージョンに格納されたオブジェクトを保持する – 異なる AWS リージョン間で複数のレプリケート先バケットを設定して、データの保存場所を地理的に異なる場所にします。この機能は、特定のコンプライアンス要件を満たすのに役立つことがあります。
- 15 分以内にオブジェクトをレプリケート — S3 Replication Time Control (S3 RTC) を使用して、予測可能な時間枠内で、同じ AWS リージョンまたは異なるリージョン間でデータをレプリケートできます。S3 RTC は、Simple Storage Service (Amazon S3) 内に保存されている新規オブジェクトの 99.99% を 15 分以内にレプリケートします (サービスレベルアグリーメントに基づく)。詳細については、「the section called “S3 Replication Time Control の有効化”」を参照してください。

> **Note**
>
> S3 RTC はバッチレプリケーションには適用されません。バッチレプリケーションはオンデマンドレプリケーションジョブで、S3 バッチオペレーションで追跡できます。詳細については、「ジョブステータスと完了レポートの追跡」を参照してください。

- バケットの同期、既存オブジェクトのレプリケート、以前に失敗したオブジェクトまたはレプリケートされたオブジェクトのレプリケート - バケットを同期して既存のオブジェクトをレプリケートするには、オンデマンドレプリケーションアクションとしてバッチレプリケーションを使用します。バッチレプリケーション使用時の詳細については、「S3 バッチレプリケーションを使用する状況」を参照してください。
- オブジェクトをレプリケートし、別のAWS リージョン のバケットにフェイルオーバーする - データレプリケーション中にバケット間ですべてのメタデータとオブジェクトを同期させるために、Amazon S3 マルチリージョンアクセスポイントのフェイルオーバーコントロールを構成する前に双方向レプリケーションルールを使用します。双方向のレプリケーションルールにより、トラフィックがフェイルオーバーする S3 バケットにデータが書き込まれると、そのデータがソースバケットにレプリケートされます。

クロスリージョンレプリケーションを使用する場合

異なる AWS リージョン 内の Amazon S3 バケット間でオブジェクトをコピーするには、S3 クロスリージョンレプリケーション (CRR) を使用します。CRR は、次の場合に役立ちます。

- コンプライアンス要件を満たす — Simple Storage Service (Amazon S3) はデフォルトで地理的に離れた複数のアベイラビリティーゾーンにデータを保存しますが、コンプライアンス要件によっては、さらに離れた場所にデータを保存することが要求される場合があります。これらの要件を満たすには、遠く離れた AWS リージョン にデータをレプリケートするクロスリージョンレプリケーションを使用します。
- レイテンシーを最小にする — ユーザーが地理的に離れた 2 つの場所にいる場合、ユーザーにより近い AWS リージョン にオブジェクトのコピーを保持することで、オブジェクトにアクセスする際のレイテンシーを最小にすることができます。
- オペレーション効率を向上する — コンピューティングクラスターが 2 つの異なる AWS リージョン にあり、同じオブジェクトセットを分析している場合、これら 2 つのリージョンにオブジェクトのコピーを保持できます。

同一リージョンレプリケーションを使用する時

同一 AWS リージョン 内の Amazon S3 バケット間でオブジェクトをコピーするには、同一リージョンレプリケーション (SRR) を使用します。SRR は、次の場合に役立ちます。

- ログを 1 つのバケットに集約する — 複数のバケットまたは複数のアカウントにログを保存している場合、ログを 1 つのリージョン内バケットに簡単にレプリケートできます。そうすることで、ログを一箇所でよりシンプルに処理できます。
- 本番稼働用アカウントとテストアカウント間のライブレプリケーションを設定する — お客様またはお客様のユーザーが保持する本稼働用アカウントとテストアカウントで同じデータを使用する場合、オブジェクトメタデータを維持しながら、これらの複数のアカウント間でオブジェクトをレプリケートできます。
- データ主権法に準拠する — データの複数のコピーを特定のリージョン内の複数の異なる AWS アカウントに保存することを義務付けられる場合があります。同一リージョンレプリケーションを使用すると、コンプライアンス規制によりデータを国外に持ち出すことが許可されていない場合に、重要なデータを自動的にレプリケートできます。

双方向レプリケーションを使用する場合

- 複数の AWS リージョン で共有するデータセットを構築する — レプリカ変更の同期により、オブジェクトのアクセスコントロールリスト (ACL)、オブジェクトタグ、またはオブジェクトロックなどのメタデータの変更を、レプリケーションオブジェクトで簡単に複製することができます。この双方向のレプリケーションは、すべてのオブジェクトとオブジェクトメタデータの変更を同期させたい場合に重要です。同一または異なる AWS リージョン にある 2 つ以上のバケット間で双方向レプリケーションを実行する場合、新規または既存のレプリケーションルールでレプリカ変更の同期を有効にすることができます。
- フェイルオーバー中にデータをリージョン間で同期させる — マルチリージョンアクセスポイントから直接 S3 クロスリージョンレプリケーション (CRR) で双方向レプリケーションルールを設定することで、AWS リージョン 間のバケットのデータを同期させることができます。フェイルオーバーを開始するタイミングについて十分な情報に基づいた決定を行うために、S3 レプリケーションメトリクスを有効にして Amazon CloudWatch 内、S3 Replication Time Control (S3 RTC) 内、またはマルチリージョンアクセスポイントからのレプリケーションをモニタリングすることもできます。
- アプリケーションの可用性を高める — リージョンのトラフィックが中断した場合でも、双方向のレプリケーションルールを使用して、データレプリケーション中にすべてのメタデータとオブジェクトをバケット間で同期させることができます。

S3 バッチレプリケーションを使用する状況

バッチレプリケーションは、オンデマンドオプションとして、既存のオブジェクトを異なるバケットにレプリケートします。ライブレプリケーションとは異なり、これらのジョブは必要に応じて実行できます。バッチレプリケーションは、以下の場合に役立ちます。

- 既存のオブジェクトのレプリケーション — バッチレプリケーションを使用して、同じリージョンレプリケーションまたはクロスリージョンレプリケーションが設定される前に、バケットに追加されたオブジェクトをレプリケートできます。
- 以前にレプリケートに失敗したオブジェクトをレプリケートする - バッチレプリケーションジョブをフィルタリングして、レプリケーションステータスが [FAILED] (失敗) のオブジェクトをレプリケートできます。
- すでにレプリケートされたオブジェクトをレプリケートする — データの複数のコピーを別々の AWS アカウントまたは AWS リージョンに保存することを義務付けられる場合があります。バッチレプリケーションでは、新規に追加された宛先に既存のオブジェクトをレプリケートできます。

- レプリケーションルールから作成されたオブジェクトのレプリカをレプリケートする — レプリケーション設定では、レプリケート先バケットにオブジェクトのレプリカが作成されます。オブジェクトのレプリカは、バッチレプリケーションでのみレプリケートできます。

ワークロードの要件とライブレプリケーション

ワークロードの要件に応じて、一部のライブレプリケーションタイプは他のレプリケーションよりもユースケースに適していることがあります。次の表を使用して、使用するレプリケーションのタイプと、ワークロードで S3 Replication Time Control (S3 RTC) を使用するかどうかを判断します。S3 RTC は、Amazon S3 内に保存されている新規オブジェクトの 99.99% を 15 分以内にレプリケートします (サービスレベルアグリーメント (SLA) に基づく)。詳細については、「the section called “S3 Replication Time Control の有効化”」を参照してください。

ワークロードの要件	S3 RTC (15 分の SLA)	クロスリージョンレプリケーション (CRR)	同一リージョンレプリケーション (SRR)
異なる AWS アカウント 間でオブジェクトをレプリケートする	はい	あり	はい
24 ~ 48 時間以内に同じ AWS リージョン 内のオブジェクトをレプリケートする (SLA に基づかない)	いいえ	いいえ	はい
24 ~ 48 時間以内に異なる AWS リージョン 内のオブジェクトをレプリケートする (SLA に基づかない)	いいえ	あり	いいえ
予測可能なレプリケーション時間: SLA に基づき、15 分以内にオブジェクトの	はい	いいえ	いいえ

ワークロードの要件	S3 RTC (15 分の SLA)	クロスリージョンレプリケーション (CRR)	同一リージョンレプリケーション (SRR)
99.9% をレプリケートする			

Amazon S3 がレプリケートするもの

Amazon S3 は、レプリケーションに設定されているバケット内の特定のアイテムのみをレプリケートします。

トピック

- レプリケーション設定でレプリケートされるものは何ですか?
- レプリケーション設定でレプリケートされないものは何ですか?

レプリケーション設定でレプリケートされるものは何ですか?

デフォルトで、Simple Storage Service (Amazon S3) は以下をレプリケートします。

- レプリケーション設定の追加後に作成されたオブジェクト。
- 暗号化されていないオブジェクト
- ユーザー提供のキー (SSE-C) を使用して暗号化されたオブジェクト、Amazon S3 マネージドキー (SSE-S3) の下で保管時に暗号化されたオブジェクト、および AWS Key Management Service (SSE-KMS) に保存されている KMS キーで暗号化されたオブジェクト。詳細については、「the section called “暗号化オブジェクトのレプリケート”」を参照してください。
- レプリケート元オブジェクトからレプリカへのオブジェクトメタデータ。レプリカからレプリケート元オブジェクトへのメタデータのレプリケーションについては、レプリカの変更同期によるメタデータ変更のレプリケートを参照してください。
- バケット所有者がオブジェクトとアクセスコントロールリスト (ACL) の読み取り権限を持つ、レプリケート元バケットのオブジェクトのみをレプリケートします。

  リソース所有者の詳細については「Amazon S3 のバケットとオブジェクトの所有権」を参照してください。

- レプリケート元バケットとレプリケート先バケットが同じアカウントによって所有されていない場合のレプリカの所有権の変更を Amazon S3 に指示しない限り、オブジェクト ACL は更新されます。

  詳細については、「レプリカ所有者の変更」を参照してください。

  Amazon S3 が 2 つの ACL を同期させるまでしばらく時間がかかる可能性があります。オーナーシップのこの変更は、バケットにレプリケーション設定を追加した後に作成されたオブジェクトにのみ適用されます。
- オブジェクトタグ、存在する場合。
- S3 オブジェクトロックの保持情報 (ある場合)。

  Amazon S3 で保持情報が適用されているオブジェクトをレプリケートすると、それらと同じ保持制御がレプリカに適用され、レプリケート先バケットに設定されているデフォルトの保持期間は上書きされます。レプリケート元バケット内のオブジェクトに保持制御が適用されておらず、デフォルトの保持期間が設定されているレプリケート先バケットにレプリケートすると、レプリケート先バケットのデフォルトの保持期間がオブジェクトのレプリカに適用されます。詳細については、「S3 Object Lock を使用したオブジェクトのロック」を参照してください。

削除オペレーションがレプリケーションに与える影響

レプリケート元バケットからオブジェクトを削除すると、デフォルトで次のアクションが実行されます。

- オブジェクトバージョン ID を指定せずに DELETE リクエストを行った場合、Amazon S3 は削除マーカーを追加します。Amazon S3 では、削除マーカーを次のように扱います。
  - 最新バージョンのレプリケーション設定を使用している (すなわち、レプリケーション設定ルールで`Filter`要素を指定している) 場合、Amazon S3 は削除マーカーをレプリケートしません。ただし、タグベース以外のルールには削除マーカーレプリケーションを追加できます。詳細については、「バケット間での削除マーカーのレプリケーション」を参照してください。
  - `Filter`要素を指定しない場合、Amazon S3 はレプリケーション設定がバージョン V1 であるとみなし、ユーザーアクションの結果として生じた削除マーカーをレプリケートします。ただし、ライフサイクルアクションによって Amazon S3 がオブジェクトを削除した場合、削除マーカーはレプリケート先のバケットにはレプリケートされません。
- DELETE リクエストで削除するオブジェクトバージョン ID を指定した場合、Amazon S3 はレプリケート元バケット内のそのオブジェクトバージョンを削除します。しかし、レプリケート先バケット内でその削除をレプリケートすることはありません。これは、レプリケート先バケットからは、

同じオブジェクトバージョンを削除しないことを意味します。これは悪意のある削除からデータを保護します。

レプリケーション設定でレプリケートされないものは何ですか?

デフォルトで、Simple Storage Service (Amazon S3) は以下をレプリケートしません。

- 別のレプリケーションルールによって作成されたレプリカである、レプリケート元バケットのオブジェクト。例えば、バケット A がレプリケート元でバケット B がレプリケート先であるレプリケーションを設定するとします。ここで、バケット B をレプリケート元、バケット C をレプリケート先とする別のレプリケーション設定を追加したとします。この場合、バケット A のオブジェクトのレプリカであるバケット B のオブジェクトは、バケット C にレプリケートされません。

  レプリカであるオブジェクトをレプリケートするには、バッチレプリケーションを使用します。バッチレプリケーションの設定の詳細については、「既存のオブジェクトのレプリケーション」を参照してください。
- 既に別のレプリケート先にレプリケートされている、レプリケート元バケット内のオブジェクト。例えば、既存のレプリケーション設定でレプリケート先バケットを変更した場合、Simple Storage Service (Amazon S3) がそのオブジェクトを再度レプリケートすることはありません。

  以前にレプリケートされたオブジェクトをレプリケートするには、バッチレプリケーションを使用します。バッチレプリケーションの設定の詳細については、「既存のオブジェクトのレプリケーション」を参照してください。
- バッチレプリケーションでは、レプリケート先バケットからオブジェクトのバージョン ID で削除されたオブジェクトの再レプリケーションはサポートされません。これらのオブジェクトを再レプリケートするには、バッチコピージョブを使用してソースオブジェクトを所定の場所でコピーします。これらのオブジェクトを所定の場所でコピーすると、レプリケート元バケットにオブジェクトの新しいバージョンが作成され、レプリケート先へのレプリケーションが自動的に開始されます。バッチコピーの使用方法については、「バッチ操作を使用してオブジェクトをコピーする例」を参照してください。
- デフォルトでは、異なる AWS アカウント からレプリケートする場合、レプリケート元バケットに追加された削除マーカーはレプリケートされません。

  削除マーカーの複製方法については、「バケット間での削除マーカーのレプリケーション」を参照してください。

- S3 Glacier Flexible Retrieval、S3 Glacier Deep Archive、S3 Intelligent-Tiering Archive Access、または S3 Intelligent-Tiering Deep Archive Access のストレージクラスまたはストレージ階層に保存されているオブジェクト。これらのオブジェクトは、復元して別のストレージクラスにコピーするまで複製できません。

  S3 Glacier Flexible Retrieval と S3 Glacier Deep Archive の詳細については、「ほとんどアクセスすることのないオブジェクトのストレージクラス」を参照してください。

  S3 Intelligent-Tiering の詳細については、「Amazon S3 Intelligent-Tiering によるストレージコストの管理」を参照してください。

- バケット所有者が十分な許可を持っていないレプリケート元バケット内のオブジェクト。

  オブジェクト所有者がバケット所有者にアクセス許可を付与する方法の詳細については、「バケット所有者はフルコントロール権限を持ちながら、オブジェクトをアップロードするためのクロスアカウントアクセス許可を付与する」を参照してください。

- バケットレベルのサブリソースの更新

  たとえば、ライフサイクル設定を変更したり、レプリケート元バケットに通知設定を追加した場合、これらの変更はレプリケート先バケットには適用されません。この機能により、レプリケート元バケットとレプリケート先バケットで異なる設定を指定できます。

- ライフサイクル設定によって実行されたアクション。

  たとえば、ライフサイクル設定がレプリケート元バケットでのみ有効である場合、Amazon S3 は失効したオブジェクトに削除マーカーを作成しますが、その削除マーカーはレプリケートされません。同じライフサイクル設定をレプリケート元バケットとレプリケート先バケットの両方に適用する場合は、両方で同じライフサイクル設定を有効にします。ライフサイクル設定についての詳細は、オブジェクトのライフサイクルの管理 を参照してください。

- ライブレプリケーションでタグベースのレプリケーションルールを使用する場合、`PutObject` オペレーションで一致するレプリケーションルールタグを新しいオブジェクトにタグ付けする必要があります。そうしないと、オブジェクトはレプリケートされません。`PutObject` オペレーション後にオブジェクトにタグが付けされると、それらのオブジェクトもレプリケートされません。

  `PutObject` オペレーション後にタグ付けされたオブジェクトをレプリケートするには、S3 バッチレプリケーションを使用する必要があります。バッチレプリケーションの詳細については、「既存のオブジェクトのレプリケーション」を参照してください。

レプリケーションの要件と考慮事項

Amazon S3 レプリケーションでは以下が必要です。

- ソースバケットの所有者は、自分のアカウントに対して送信元と送信先の AWS リージョン を有効にする必要があります。レプリケート先のバケット所有者は、自分のアカウントでレプリケート先リージョンを有効にしておく必要があります。

  AWS リージョンを有効または無効にする方法の詳細については、「AWS アカウント管理 リファレンスガイド」の「アカウントで使用できる AWS リージョンの指定」を参照してください。
- レプリケート元とレプリケート先の両方のバケットで、バージョニングを有効にする必要があります。バージョニングの詳細については、「S3 バージョニングによる複数のバージョンのオブジェクトの保持」を参照してください。
- Amazon S3 には、お客様に代わってレプリケート元バケットから送信先バケットにオブジェクトをレプリケートするためのアクセス許可が必要です。これらのアクセス許可の詳細については、「ライブレプリケーションのアクセス許可の設定」を参照してください。
- ソースバケット所有者がバケット内のオブジェクトを所有していない場合、オブジェクト所有者は、オブジェクトアクセスコントロールリスト (ACL) を使用して、バケット所有者に `READ` 権限と `READ_ACP` 権限を付与する必要があります。詳細については、「アクセスコントロールリスト (ACL) の概要」を参照してください。
- レプリケート元バケットで S3 オブジェクトロックが有効になっている場合は、レプリケート先バケットでも S3 オブジェクトロックが有効になっている必要があります。

  Object Lock が有効になっているバケットでレプリケーションを有効にするには、AWS Command Line Interface、REST API、または AWS SDK を使用する必要があります。一般的な的な情報については、「S3 Object Lock を使用したオブジェクトのロック」を参照してください

> **Note**
>
> レプリケーションを設定するために使用する AWS Identity and Access Management (IAM) ロールで、ソース S3 バケットに対する 2 つの新しいアクセス許可を付与する必要があります。2 つの新しいアクセス許可は `s3:GetObjectRetention` と `s3:GetObjectLegalHold` です。ロールに `s3:Get*` アクセス許可がある場合、そのロールは要件を満たしています。詳細については、「ライブレプリケーションのアクセス許可の設定」を参照してください。

詳細については、「ライブレプリケーションの設定の概要」を参照してください。

異なる AWS アカウント がレプリケート元バケットとレプリケート先バケットを所有するクロスアカウントのシナリオでレプリケーション設定を設定している場合は、次の追加の要件が適用されます。

- レプリケート先バケットの所有者は、バケットポリシーを使用してレプリケート元バケット所有者にオブジェクトをレプリケートするためのアクセス許可を付与する必要があります。詳細については、「レプリケーション元とレプリケーション先のバケットが異なる AWS アカウントによって所有されている場合の許可の付与」を参照してください。
- レプリケート先バケットをリクエスタ支払いバケットとして設定することはできません。詳細については、「ストレージの転送と使用にリクエスタ支払い汎用バケットを使用する」を参照してください。

レプリケーションの考慮事項

レプリケーションを設定する前に、以下を考慮してください。

トピック

- ライフサイクル設定とオブジェクトのレプリカ
- バージョニング設定とレプリケーション設定
- S3 Intelligent-Tiering での S3 レプリケーションの使用
- ログ設定とレプリケーション設定
- CRR とレプリケート先のリージョン
- S3 バッチレプリケーション
- S3 Replication Time Control

ライフサイクル設定とオブジェクトのレプリカ

Amazon S3 がオブジェクトをレプリケートするのにかかる時間は、オブジェクトのサイズによって異なります。大きなオブジェクトの場合、数時間かかることもあります。レプリカがレプリケート先バケットで使用可能になるまでにはしばらく時間がかかります。レプリカの作成には、ソースバケットに対応するオブジェクトを作成するのと同じくらいの時間がかかります。レプリケート先バケットでライフサイクル設定が有効な場合、ライフサイクルルールでは、レプリケート先バケットでレプリカが使用可能になった時間ではなく、オブジェクトの元の作成時間が優先されることに注意してください。

レプリケーション設定では、バケットのバージョニングを有効にする必要があります。バケットのバージョニングを有効にする際、以下の点に注意してください。

- オブジェクトの有効期限ライフサイクル設定がある場合は、バージョニングを有効にした後に NonCurrentVersionExpiration ポリシーを追加して、バージョニングを有効にする前と同じ完全な削除動作を維持する必要があります。
- 移行ライフサイクル設定がある場合は、バージョニングを有効にした後に、NonCurrentVersionTransition ポリシーの追加を検討する必要があります。

バージョニング設定とレプリケーション設定

レプリケート元バケットとレプリケート先バケットはどちらも、バケットにレプリケーションを設定するときに、バージョニングが有効になっている必要があります。レプリケート元バケットとレプリケート先バケットの両方でバージョニングを有効にして、レプリケート元バケットでレプリケーションを設定した後は、次の問題が発生します。

- レプリケート元バケットのバージョニングを無効にしようとすると、Amazon S3 はエラーを返します。レプリケート元バケットのバージョニングを無効にする前に、レプリケーション設定を削除する必要があります。
- レプリケート先バケットのバージョニングを無効にすると、レプリケーションは失敗します。レプリケート元オブジェクトのレプリケーションステータスはFAILEDです。

S3 Intelligent-Tiering での S3 レプリケーションの使用

S3 Intelligent-Tiering は、最もコスト効率の高いアクセス階層にデータを自動的に移動することで、ストレージコストを最適化するように設計されたストレージクラスです。オブジェクトのモニタリングとオートメーションに対して発生する少額の月額料金で、S3 Intelligent-Tiering はアクセスパターンをモニタリングし、あまりアクセスされていないオブジェクトをより低コストのアクセス階層へ自動的に移動させることができます。

S3 バッチレプリケーションを使用して S3 Intelligent-Tiering に保存されたオブジェクトをレプリケートしたり、CopyObject または UploadPartCopy を呼び出したりすると、アクセスが構成されます。これらの場合、コピーやレプリケーションオペレーションのソースオブジェクトは上位の階層に移動されます。

S3 Intelligent-Tiering の詳細については、「Amazon S3 Intelligent-Tiering によるストレージコストの管理」を参照してください。

ログ設定とレプリケーション設定

レプリケーションが有効になっているバケットに Amazon S3 がログを送信している場合、ログオブジェクトをレプリケートします。

サーバーアクセスログまたは AWS CloudTrail ログをレプリケート元やレプリケート先のバケットで有効にすると、Amazon S3 はレプリケーション関連のリクエストをログに含めます。たとえば、Amazon S3 はレプリケートする各オブジェクトをログに記録します。

CRR とレプリケート先のリージョン

異なる AWS リージョン内の S3 バケット間でオブジェクトをコピーするには、Amazon S3 クロスリージョンレプリケーション (CRR) を使用します。レプリケート先バケットのリージョンは、ビジネスニーズまたはコストを考慮して選択することができます。例えば、リージョン間のデータ転送料金は、選択したリージョンによって異なります。

例えば、レプリケート元バケットのリージョンとして米国東部 (バージニア北部) (`us-east-1`) を選択したとします。米国西部 (オレゴン) (`us-west-2`) をレプリケート先バケットのリージョンとして選択した場合、米国東部 (オハイオ) (`us-east-2`) リージョンを選択した場合より多く支払うことになります。料金の詳細については、Amazon S3 の料金の「データ転送の料金」を参照してください。

同一リージョンレプリケーション (SRR) に関連するデータ転送料金はありません。

S3 バッチレプリケーション

バッチレプリケーションの考慮事項については、「S3 バッチレプリケーションに関する考慮事項」を参照してください。

S3 Replication Time Control

S3 Replication Time Control (S3 RTC) のベストプラクティスと考慮事項については、「S3 RTC のベストプラクティスとガイドライン」を参照してください。

ライブレプリケーションの設定の概要

> **Note**
>
> レプリケーションをセットアップする前に存在していたオブジェクトは、自動的にレプリケートされません。つまり、Amazon S3 はオブジェクトをさかのぼってレプリケートすることはしません。レプリケーション設定の前に作成されたオブジェクトをレプリケートするに

は、S3 バッチレプリケーションを使用します。バッチレプリケーション設定については、「既存のオブジェクトのレプリケーション」を参照してください。

ライブレプリケーション (同一リージョンレプリケーション (SRR) またはクロスリージョンレプリケーション (CRR)) を有効にするには、レプリケート元のバケットにレプリケーション設定を追加します。Amazon S3 は、この設定に基づいてオブジェクトをレプリケートします。レプリケーション設定では、以下の項目を指定する必要があります。

- レプリケート先バケット – Simple Storage Service (Amazon S3) でオブジェクトをレプリケートする先のバケット。
- レプリケートするオブジェクト – レプリケート元バケットまたはオブジェクトのサブセット内のすべてのオブジェクトをレプリケートできます。サブセットを特定するには、キー名のプレフィックス、1 つ以上のオブジェクトタグ、またはその両方を設定で指定します。

  たとえば、キー名のプレフィックス `Tax/` の オブジェクトのみをレプリケートするようにレプリケーションルールを設定した場合、Amazon S3 は `Tax/doc1` や `Tax/doc2` などのキーを持つオブジェクトをレプリケートします。しかし、`Legal/doc3` というキーを持つオブジェクトはレプリケートしません。プレフィックスと 1 つ以上のタグの両方を指定した場合、Simple Storage Service (Amazon S3) は特定のキープレフィックスとタグを持つオブジェクトのみをレプリケートします。
- AWS Identity and Access Management (IAM) ロール – Amazon S3 は、ユーザーに代わってオブジェクトをレプリケートするこの IAM ロールを引き受けます。IAM ロールの作成と許可の詳細については、「ライブレプリケーションのアクセス許可の設定」を参照してください。

これらの最小要件に加えて、以下のオプションを選択できます。

- レプリカストレージクラス – デフォルトでは、Simple Storage Service (Amazon S3) はレプリケート元オブジェクトと同じストレージクラスを使用して、オブジェクトのレプリカを保存します。レプリカには別のストレージクラスを指定できます。
- レプリカの所有権 – Simple Storage Service (Amazon S3) は、オブジェクトレプリカが引き続きレプリケート元オブジェクトの所有者によって所有されていると想定します。そのため、オブジェクトをレプリケートするときに、対応するオブジェクトアクセスコントロールリスト (ACL) または S3 オブジェクトの所有権の設定もレプリケートします。レプリケート元とレプリケート先のバケットが異なる AWS アカウントによって所有されている場合、レプリケート先バケットを所有する AWS アカウントにレプリカの所有者を変更するようにレプリケーションを設定できます。詳細については、「the section called “レプリカ所有者の変更”」を参照してください。

Amazon S3 コンソール、AWS Command Line Interface (AWS CLI)、AWS SDK、または Amazon S3 REST APIを使用してレプリケーションを設定できます。レプリケーションの設定方法の詳細なチュートリアルについては、「the section called “レプリケーションのチュートリアル”」を参照してください。

Amazon S3 は、レプリケーションルールの設定をサポートする REST API を提供します。詳細については、Amazon Simple Storage Service API リファレンスの次のトピックを参照してください。

- PutBucketReplication
- GetBucketReplication
- DeleteBucketReplication

トピック

- レプリケーション設定ファイル要素
- ライブレプリケーションのアクセス許可の設定
- ライブレプリケーションの設定例

レプリケーション設定ファイル要素

Amazon S3 はレプリケーション設定を XML 形式で保存します。Amazon S3 REST API を使用してプログラムでレプリケーションを設定する場合は、この XML ファイルでレプリケーション設定のさまざまな要素を指定します。AWS Command Line Interface (AWS CLI) を使用してレプリケーションを設定する場合は、JSON 形式を使用してレプリケーション設定を指定します。JSON の例については、「the section called “レプリケーションのチュートリアル”」のチュートリアルを参照してください。

> **Note**
>
> レプリケーション設定 XML フォーマットの最新バージョンは V2 です。XML V2 レプリケーション設定は、ルールの `<Filter>` 要素と S3 Replication Time Control (S3 RTC) を指定するルールを含むものです。
> レプリケーション設定のバージョンを確認するには、`GetBucketReplication` API オペレーションを使用します。詳細については、「Amazon Simple Storage Service API リファレンス」の「GetBucketReplication」を参照してください。

> Amazon S3 は、後方互換性のために引き続き XML V1 のレプリケーション設定フォーマットをサポートしています。XML V1 のレプリケーション設定フォーマットを使用していた場合、後方互換性については「後方互換性に関する考慮事項」を参照してください。

レプリケーション設定 XML ファイルで、次の例に示すように AWS Identity and Access Management (IAM) ロールと 1 つ以上のルールを指定する必要があります。

```
<ReplicationConfiguration>
    <Role>IAM-role-ARN</Role>
    <Rule>
        ...
    </Rule>
    <Rule>
         ...
    </Rule>
     ...
</ReplicationConfiguration>
```

Amazon S3 はユーザーの許可なしにオブジェクトをレプリケートすることはできません。レプリケーション設定で指定した IAM ロールを使用して Amazon S3 にアクセス許可を付与します。Amazon S3 は、ユーザーに代わってオブジェクトをレプリケートするこの IAM ロールを引き受けます。まずは必要なアクセス許可を IAM ロールに付与する必要があります。これらのアクセス許可の管理の詳細については、「ライブレプリケーションのアクセス許可の設定」を参照してください。

次のシナリオでは、レプリケーション設定にルールを 1 つのみ追加します。

- すべてのオブジェクトをレプリケートします。
- 1 つのオブジェクトのサブセットのみをレプリケートします。ルールにフィルターを追加して、オブジェクトのサブセットを特定します。フィルターでは、ルールが適用されるオブジェクトのサブセットを特定するために、オブジェクトキープレフィックス、タグ、またはその両方の組み合わせを指定します。フィルターは、指定した値と完全に一致するオブジェクトをターゲットにします。

オブジェクトの異なるサブセットをレプリケートする場合は、レプリケーション設定に複数のルールを追加します。各ルールでは、異なるサブセットを選択するフィルターを指定します。例えば、`tax/` または `document/` のいずれかのキープレフィックスを持つオブジェクトをレプリケートするとします。このためには、`tax/` キープレフィックスフィルターを指定するルールと、`document/` キープレフィックスを指定するもう 1 つのルールの 2 つのルールを追加します。オ

ブジェクトキーのプレフィックスの詳細については、「プレフィックスを使用してオブジェクトを整理する」を参照してください。

ここで示している各セクションで、さらに詳しく学習できます。

トピック

- 基本的なルールの設定
- オプション: フィルターの指定
- 追加のレプリケート先の設定
- レプリケーション設定の例
- 後方互換性に関する考慮事項

基本的なルールの設定

各ルールには、そのルールのステータスと優先順位を含める必要があります。また、ルールに削除マーカーをレプリケートするかどうかを指定する必要もあります。

- <Status> 要素は、Enabled または Disabled の値を使用して、ルールが有効か無効かを示します。ルールが無効な場合、Amazon S3 はそのルールで指定されているアクションを実行しません。
- <Priority> 要素は、複数のレプリケーションルールが競合する際に優先するルールを示します。Simple Storage Service (Amazon S3) は、すべてのレプリケーションルールに従ってオブジェクトをレプリケートしようと試みます。ただし、同じレプリケート先バケットを持つルールが 2 つ以上ある場合は、優先度が最も高いルールに従ってオブジェクトがレプリケートされます。数値が大きいほど、優先度が高くなります。
- <DeleteMarkerReplication> 要素は値 Enabled または Disabled を使用して削除マーカーをレプリケートするかどうかを示します。

<Destination> 要素の設定では、Amazon S3 にオブジェクトをレプリケートするレプリケート先バケットの名前を指定する必要があります。

次の例は、V2 ルールの最小要件を示しています。Amazon S3 は、下位互換性のために、引き続き XML V1 形式をサポートしています。 を参照してください。詳細については、「後方互換性に関する考慮事項」を参照してください。

```
...
    <Rule>
```

```
        <ID>Rule-1</ID>
        <Status>Enabled-or-Disabled</Status>
        <Filter>
            <Prefix></Prefix>
        </Filter>
        <Priority>integer</Priority>
        <DeleteMarkerReplication>
           <Status>Enabled-or-Disabled</Status>
        </DeleteMarkerReplication>
        <Destination>
           <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
        </Destination>
    </Rule>
    <Rule>
         ...
    </Rule>
     ...
...
```

他の設定オプションも指定できます。たとえば、コピー元オブジェクトのストレージクラスとは異なるクラスを、オブジェクトレプリカのストレージクラスで使用するように選択できます。

オプション: フィルターの指定

ルールが適用されるオブジェクトのサブセットを選択するには、オプションのフィルタを追加します。オブジェクトキープレフィックス、オブジェクトタグ、またはその両方の組み合わせでフィルターできます。キープレフィックスとオブジェクトタグの両方でフィルターする場合、Simple Storage Service (Amazon S3) は論理 AND 演算子を使用してフィルターを組み合わせます。つまり、このルールは、特定のキープレフィックスと特定のタグの両方を持つオブジェクトのサブセットに適用されます。

オブジェクトのキープレフィックスに基づいたフィルタリング

オブジェクトキープレフィックスに基づくフィルタを使用してルールを指定するには、次の XML を使用します。1 つのルールに指定できるプレフィックスは 1 つだけです。

```
<Rule>
    ...
    <Filter>
        <Prefix>key-prefix</Prefix>
    </Filter>
    ...
```

```
</Rule>
...
```

オブジェクトタグに基づいたフィルタリング

オブジェクトタグに基づくフィルタを使用してルールを指定するには、次の XML を使用します。複数のオブジェクトタグを指定できます。

```
<Rule>
    ...
    <Filter>
        <And>
            <Tag>
                <Key>key1</Key>
                <Value>value1</Value>
            </Tag>
            <Tag>
                <Key>key2</Key>
                <Value>value2</Value>
            </Tag>
             ...
        </And>
    </Filter>
    ...
</Rule>
...
```

キープレフィックスとオブジェクトタグを使用したフィルタリング

キープレフィックスとオブジェクトタグの組み合わせでルールフィルターを指定するには、次の XML を使用します。これらのフィルターは、<And> 親要素でラップします。Amazon S3 は、これらのフィルターを結合する論理 AND オペレーションを実行します。つまり、このルールは、特定のキープレフィックスと特定のタグの両方を持つオブジェクトのサブセットに適用されます。

```
<Rule>
    ...
    <Filter>
        <And>
            <Prefix>key-prefix</Prefix>
            <Tag>
                <Key>key1</Key>
                <Value>value1</Value>
```

```
            </Tag>
            <Tag>
                <Key>key2</Key>
                <Value>value2</Value>
            </Tag>
             ...
    </Filter>
    ...
</Rule>
...
```

> **Note**
>
> - 空の <Filter> 要素を持つルールを指定すると、ルールはバケット内にある全オブジェクトに適用されます。
> - ライブレプリケーションでタグベースのレプリケーションルールを使用する場合、PutObject オペレーションで一致するレプリケーションルールタグを新しいオブジェクトにタグ付けする必要があります。そうしないと、オブジェクトはレプリケートされません。PutObject オペレーション後にオブジェクトにタグが付けされると、それらのオブジェクトもレプリケートされません。
>
> PutObject オペレーション後にタグ付けされたオブジェクトをレプリケートするには、S3 バッチレプリケーションを使用する必要があります。バッチレプリケーションの詳細については、「既存のオブジェクトのレプリケーション」を参照してください。

追加のレプリケート先の設定

レプリケート先設定では、Amazon S3 がオブジェクトをレプリケートするバケットを指定します。1 つのレプリケート元バケットから 1 つまたは複数のレプリケート先バケットに、オブジェクトをレプリケートするように設定できます。

```
...
<Destination>
    <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
</Destination>
...
```

次のオプションを<Destination>要素に追加できます。

トピック

- ストレージクラスを指定する
- 複数の宛先バケットを追加する
- 複数のレプリケート先バケットを持つレプリケーションルールごとに異なるパラメータを指定します。
- レプリカの所有者を変更する
- S3 レプリケーション時間コントロールの有効化
- AWS KMS を使用してサーバー側の暗号化で作成されたオブジェクトをレプリケートする

ストレージクラスを指定する

オブジェクトレプリカのストレージクラスを指定できます。デフォルトでは、Amazon S3 は、レプリケート元オブジェクトのストレージクラスを使用してオブジェクトレプリカを作成します。以下に例を示します。

```
...
<Destination>
       <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
       <StorageClass>storage-class</StorageClass>
</Destination>
...
```

複数の宛先バケットを追加する

次のように、単一のレプリケーション設定に複数のレプリケート先バケットを追加できます。

```
...
<Rule>
    <ID>Rule-1</ID>
    <Status>Enabled-or-Disabled</Status>
    <Priority>integer</Priority>
    <DeleteMarkerReplication>
       <Status>Enabled-or-Disabled</Status>
    </DeleteMarkerReplication>
    <Destination>
       <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket1</Bucket>
    </Destination>
</Rule>
<Rule>
```

```
    <ID>Rule-2</ID>
    <Status>Enabled-or-Disabled</Status>
    <Priority>integer</Priority>
    <DeleteMarkerReplication>
       <Status>Enabled-or-Disabled</Status>
    </DeleteMarkerReplication>
    <Destination>
       <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket2</Bucket>
    </Destination>
</Rule>
...
```

複数のレプリケート先バケットを持つレプリケーションルールごとに異なるパラメータを指定します。

1 つのレプリケーション設定に複数のレプリケート先バケットを追加する場合、次のように、レプリケーションルールごとに異なるパラメータを指定できます。

```
...
<Rule>
    <ID>Rule-1</ID>
    <Status>Enabled-or-Disabled</Status>
    <Priority>integer</Priority>
    <DeleteMarkerReplication>
       <Status>Disabled</Status>
    </DeleteMarkerReplication>
      <Metrics>
    <Status>Enabled</Status>
    <EventThreshold>
      <Minutes>15</Minutes>
    </EventThreshold>
  </Metrics>
    <Destination>
       <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket1</Bucket>
    </Destination>
</Rule>
<Rule>
    <ID>Rule-2</ID>
    <Status>Enabled-or-Disabled</Status>
    <Priority>integer</Priority>
    <DeleteMarkerReplication>
       <Status>Enabled</Status>
    </DeleteMarkerReplication>
```

```
      <Metrics>
    <Status>Enabled</Status>
    <EventThreshold>
      <Minutes>15</Minutes>
    </EventThreshold>
  </Metrics>
  <ReplicationTime>
    <Status>Enabled</Status>
    <Time>
      <Minutes>15</Minutes>
    </Time>
  </ReplicationTime>
    <Destination>
       <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket2</Bucket>
    </Destination>
</Rule>
...
```

レプリカの所有者を変更する

レプリケート元とレプリケート先のバケットが同じアカウントの所有でない場合は、レプリケート先のバケットを所有する AWS アカウント にレプリカの所有権を変更できます。そのためには、<AccessControlTranslation> 要素を追加します。この要素は値 Destination を取ります。

```
...
<Destination>
   <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
   <Account>destination-bucket-owner-account-id</Account>
   <AccessControlTranslation>
       <Owner>Destination</Owner>
   </AccessControlTranslation>
</Destination>
...
```

この要素をレプリケーション設定に <AccessControlTranslation> 要素を追加しない場合は、レプリカはレプリケート元オブジェクトを所有する AWS アカウントの所有になります。詳細については、「レプリカ所有者の変更」を参照してください。

S3 レプリケーション時間コントロールの有効化

S3 Replication Time Control (S3 RTC) はレプリケーション設定で有効にできます。S3 RTC は、ほとんどのオブジェクトを数秒でレプリケートし、オブジェクトの 99.99% を 15 分以内にレプリケートします (サービスレベルアグリーメントに基づく)。

> **Note**
>
> <EventThreshold> と <Time> 要素で受け入れられるのは、<Minutes>15</Minutes> の値のみです。

```
...
<Destination>
  <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
  <Metrics>
    <Status>Enabled</Status>
    <EventThreshold>
      <Minutes>15</Minutes>
    </EventThreshold>
  </Metrics>
  <ReplicationTime>
    <Status>Enabled</Status>
    <Time>
      <Minutes>15</Minutes>
    </Time>
  </ReplicationTime>
</Destination>
...
```

詳細については、「S3 Replication Time Control (S3 RTC)を使用してコンプライアンス要件を満たす」を参照してください。API の例については、「Amazon Simple Storage Service API リファレンス」の「PutBucketReplication」を参照してください。

AWS KMS を使用してサーバー側の暗号化で作成されたオブジェクトをレプリケートする

レプリケート元バケットには、AWS Key Management Service (AWS KMS) (SSE-KMS) キーを使用したサーバー側の暗号化で作成されたオブジェクトが含まれている場合があります。デフォルトでは、Amazon S3 はこれらのオブジェクトをレプリケートしません。オプションで、これらのオブジェクトをレプリケートするように Amazon S3 に指示できます。これを行うには、まず、<SourceSelectionCriteria> 要素を追加することで、この機能を明示的にオプトインしま

す。次に、オブジェクトレプリカの暗号化に使用するための AWS KMS key (レプリケート先バケットの AWS リージョン 用) を入力します。次の例は、これらの要素を指定する方法を示しています。

```
...
<SourceSelectionCriteria>
  <SseKmsEncryptedObjects>
    <Status>Enabled</Status>
  </SseKmsEncryptedObjects>
</SourceSelectionCriteria>
<Destination>
  <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
  <EncryptionConfiguration>
    <ReplicaKmsKeyID>AWS KMS key ID to use for encrypting object replicas</
ReplicaKmsKeyID>
  </EncryptionConfiguration>
</Destination>
...
```

詳細については、「暗号化されたオブジェクトのレプリケート (SSE-S3、SSE-KMS、DSSE-KMS、SSE-C)」を参照してください。

レプリケーション設定の例

開始するには、必要に応じて次のレプリケーション設定例をバケットに追加します。

> **Important**
>
> レプリケーション設定をバケットに追加するには、`iam:PassRole` アクセス許可が必要です。このアクセス許可により、Amazon S3 レプリケーションアクセス許可を付与する IAM ロールを渡すことができます。IAM ロールを指定するには、レプリケーション設定 XML の `<Role>` 要素で使用されている Amazon リソースネーム (ARN) を指定します。詳細については、IAM ユーザーガイドの「AWS のサービス サービスにロールを渡すアクセス権限をユーザーに付与する」を参照してください。

Example 1: ルールが 1 つのレプリケーション設定

次の基本的なレプリケーション設定では 1 つのルールを指定します。このルールは、Amazon S3 が引き受けることができる IAM ロールと、オブジェクトレプリカ用のレプリケート先バケットを指定します。`Enabled` の `<Status>` 要素の値は、ルールが有効であることを示します。

```
<?xml version="1.0" encoding="UTF-8"?>
<ReplicationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Role>arn:aws:iam::account-id:role/role-name</Role>
  <Rule>
    <Status>Enabled</Status>

    <Destination>
      <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
    </Destination>
  </Rule>
</ReplicationConfiguration>
```

レプリケートするオブジェクトのサブセットを選択するために、フィルタを追加できます。次の設定では、フィルタはオブジェクトキープレフィックスを指定します。このルールは、キー名に *Tax/* というプレフィックスが付いているオブジェクトに適用されます。

```
<?xml version="1.0" encoding="UTF-8"?>
<ReplicationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Role>arn:aws:iam::account-id:role/role-name</Role>
  <Rule>
    <Status>Enabled</Status>
    <Priority>1</Priority>
    <DeleteMarkerReplication>
       <Status>string</Status>
    </DeleteMarkerReplication>

    <Filter>
       <Prefix>Tax/</Prefix>
    </Filter>

    <Destination>
       <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
    </Destination>

  </Rule>
</ReplicationConfiguration>
```

<Filter> 要素を指定した場合、<Priority> 要素と <DeleteMarkerReplication> 要素も含める必要があります。この例では、<Priority> 要素に設定した値は、ルールが 1 つしかないため、関係ありません。

次の設定では、フィルタは 1 つのプレフィックスと 2 つのタグを指定します。このルールは、指定されたキープレフィックスとタグを持つオブジェクトのサブセットに適用されます。具体的には、キー名に *Tax/* プレフィックスがあり、2 つの指定されたオブジェクトタグがあるオブジェクトに適用されます。この例では、<Priority> 要素に設定した値は、ルールが 1 つしかないため、関係ありません。

```
<?xml version="1.0" encoding="UTF-8"?>
<ReplicationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Role>arn:aws:iam::account-id:role/role-name</Role>
  <Rule>
    <Status>Enabled</Status>
    <Priority>1</Priority>
    <DeleteMarkerReplication>
       <Status>string</Status>
    </DeleteMarkerReplication>

    <Filter>
        <And>
          <Prefix>Tax/</Prefix>
          <Tag>
             <Tag>
                <Key>tagA</Key>
                <Value>valueA</Value>
             </Tag>
          </Tag>
          <Tag>
             <Tag>
                <Key>tagB</Key>
                <Value>valueB</Value>
             </Tag>
          </Tag>
       </And>

    </Filter>

    <Destination>
        <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
    </Destination>

  </Rule>
</ReplicationConfiguration>
```

オブジェクトレプリカに対し、次のようにストレージクラスを指定できます。

```
<?xml version="1.0" encoding="UTF-8"?>

<ReplicationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Role>arn:aws:iam::account-id:role/role-name</Role>
  <Rule>
    <Status>Enabled</Status>
    <Destination>
       <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
       <StorageClass>storage-class</StorageClass>
    </Destination>
  </Rule>
</ReplicationConfiguration>
```

Amazon S3 がサポートする任意のストレージクラスを指定できます。

Example 2: ルールが 2 つのレプリケーション設定

Example

次のレプリケーション設定では、ルールで以下を指定します。

- 各ルールは異なるキープレフィックスでフィルタリングするため、各ルールはオブジェクトの個別のサブセットに適用されます。例えば、Simple Storage Service (Amazon S3) は、キー名 *Tax/doc1.pdf* と *Project/project1.txt* を持つオブジェクトをレプリケートしますが、キー名 *PersonalDoc/documentA* のオブジェクトはレプリケートされません。
- どちらのルールも <Priority> 要素の値を指定しますが、ルールの優先度は 2 つの異なるオブジェクトセットに適用されるため、関係ありません。次の例は、ルール優先順位が適用されたときに何が起こるかを示しています。
- 2 番目のルールは、オブジェクトレプリカの S3 標準 – IA ストレージクラスを指定します。Amazon S3 は、これらのオブジェクトレプリカに対して指定されたストレージクラスを使用します。

```
<?xml version="1.0" encoding="UTF-8"?>

<ReplicationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Role>arn:aws:iam::account-id:role/role-name</Role>
  <Rule>
```

```
    <Status>Enabled</Status>
    <Priority>1</Priority>
    <DeleteMarkerReplication>
       <Status>string</Status>
    </DeleteMarkerReplication>
    <Filter>
        <Prefix>Tax</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Destination>
      <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
    </Destination>
     ...
  </Rule>
 <Rule>
    <Status>Enabled</Status>
    <Priority>2</Priority>
    <DeleteMarkerReplication>
       <Status>string</Status>
    </DeleteMarkerReplication>
    <Filter>
        <Prefix>Project</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Destination>
      <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
     <StorageClass>STANDARD_IA</StorageClass>
    </Destination>
     ...
  </Rule>


</ReplicationConfiguration>
```

Example 3: プレフィックスが重複している 2 つのルールを使用したレプリケーション設定

この設定では、2 つのルールで、重複するキープレフィックス、*star/* および *starship/* を持つフィルターを指定します。どちらのルールも、キー名が *starship-x* のオブジェクトに適用されます。この場合、Amazon S3 はルールの優先順位を使用して適用するルールを決定します。数値が大きいほど、優先度が高くなります。

```
<ReplicationConfiguration>
```

```
  <Role>arn:aws:iam::account-id:role/role-name</Role>

  <Rule>
    <Status>Enabled</Status>
    <Priority>1</Priority>
    <DeleteMarkerReplication>
       <Status>string</Status>
    </DeleteMarkerReplication>
    <Filter>
        <Prefix>star</Prefix>
    </Filter>
    <Destination>
      <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
    </Destination>
  </Rule>
  <Rule>
    <Status>Enabled</Status>
    <Priority>2</Priority>
    <DeleteMarkerReplication>
       <Status>string</Status>
    </DeleteMarkerReplication>
    <Filter>
        <Prefix>starship</Prefix>
    </Filter>
    <Destination>
      <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
    </Destination>
  </Rule>
</ReplicationConfiguration>
```

Example 4: チュートリアル例

チュートリアルについては、「ライブレプリケーションの設定例」を参照してください。

レプリケーション設定の XML 構造の詳細については、Amazon Simple Storage Service API リファレンスの「PutBucketReplication」を参照してください。

後方互換性に関する考慮事項

レプリケーション設定 XML フォーマットの最新バージョンは V2 です。XML V2 レプリケーション設定は、ルールの `<Filter>` 要素と S3 Replication Time Control (S3 RTC) を指定するルールを含むものです。

レプリケーション設定のバージョンを確認するには、GetBucketReplication API オペレーションを使用します。詳細については、「Amazon Simple Storage Service API リファレンス」の「GetBucketReplication」を参照してください。

Amazon S3 は、後方互換性のために引き続き XML V1 のレプリケーション設定フォーマットをサポートしています。XML V1 のレプリケーション設定フォーマットを使用していた場合は、後方互換性に影響を及ぼす以下の点を考慮してください。

- レプリケーション設定 XML V2 フォーマットでは、ルールに <Filter> 要素が含まれています。<Filter> 要素を使用すると、オブジェクトキープレフィックス、タグ、またはその両方に基づいてオブジェクトフィルタを指定して、ルールが適用されるオブジェクトを範囲指定できます。レプリケーション設定 XML V1 フォーマットは、キープレフィックスのみに基づくフィルタリングをサポートしていました。この場合は、<Prefix> 要素を <Rule> 要素の子要素として直接追加します。以下に例を示します。

```
<?xml version="1.0" encoding="UTF-8"?>
<ReplicationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Role>arn:aws:iam::account-id:role/role-name</Role>
  <Rule>
    <Status>Enabled</Status>
    <Prefix>key-prefix</Prefix>
    <Destination>
       <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
    </Destination>

  </Rule>
</ReplicationConfiguration>
```

- オブジェクトのバージョン ID を指定せずにレプリケート元バケットからオブジェクトを削除すると、Amazon S3 は削除マーカーを追加します。V1 のレプリケーション設定 XML V1 フォーマットを使用した場合、Amazon S3 はユーザーアクションから発生した削除マーカーをレプリケートします。つまり、Amazon S3 はユーザーがオブジェクトを削除した場合にのみ、削除マーカーをレプリケートします。期限切れのオブジェクトが (ライフサイクルアクションの一部として) Amazon S3 によって削除された場合、Amazon S3 は削除マーカーをレプリケートしません。

  レプリケーション設定 XML V2 フォーマットでは、タグベース以外のルールのために削除マーカーレプリケーションを有効にすることができます。詳細については、「バケット間での削除マーカーのレプリケーション」を参照してください。

ライブレプリケーションのアクセス許可の設定

Amazon S3 でライブレプリケーションを設定する場合は、次のように必要なアクセス許可を取得します。

- Simple Storage Service (Amazon S3) は、ユーザーに代わってオブジェクトをレプリケートするための許可を必要とします。AWS Identity and Access Management (IAM) ロールを作成してこれらの許可を付与し、その後、レプリケーション設定でそのロールを指定します。
- レプリケート元バケットとレプリケート先バケットが同じアカウントによって所有されていない場合、レプリケート先バケット所有者は、レプリカを保存するためのアクセス許可をレプリケート元バケット所有者にも付与する必要があります。

トピック

- レプリケーションルールを作成するためのアクセス許可の設定
- IAM ロールの作成
- レプリケーション元とレプリケーション先のバケットが異なる AWS アカウントによって所有されている場合の許可の付与
- レプリカの所有権の変更
- S3 バッチオペレーションに対するアクセス許可の付与

レプリケーションルールを作成するためのアクセス許可の設定

レプリケーションルールの作成に使用する IAM ユーザーまたはロールには、一方向または双方向レプリケーションのレプリケーションルールを作成するためのアクセス許可が必要です。ユーザーまたはロールにこれらのアクセス許可がない場合、レプリケーションルールを作成することはできません。詳細については、「IAM ユーザーガイド」の「IAM アイデンティティ」を参照してください。

ユーザーまたはロールには、次のアクションが必要です。

- `iam:AttachRolePolicy`
- `iam:CreatePolicy`
- `iam:CreateServiceLinkedRole`
- `iam:PassRole`
- `iam:PutRolePolicy`
- `s3:GetBucketVersioning`

- s3:GetObjectVersionAcl
- s3:GetObjectVersionForReplication
- s3:GetReplicationConfiguration
- s3:PutReplicationConfiguration

これらのアクションを含む IAM ポリシーの例を次に示します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetAccessPoint",
                "s3:GetAccountPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:ListAccessPoints",
                "s3:ListAllMyBuckets",
                "s3:PutReplicationConfiguration",
                "s3:GetReplicationConfiguration",
                "s3:GetBucketVersioning",
                "s3:GetObjectVersionForReplication",
                "s3:GetObjectVersionAcl",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetObjectVersion",
                "s3:GetBucketOwnershipControls",
                "s3:PutBucketOwnershipControls",
                "s3:GetObjectLegalHold",
                "s3:GetObjectRetention",
                "s3:GetBucketObjectLockConfiguration"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket1-*",
                "arn:aws:s3:::amzn-s3-demo-bucket2-*/*"
            ]
        },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "s3:List*AccessPoint*",
                "s3:GetMultiRegion*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:Get*",
                "iam:CreateServiceLinkedRole",
                "iam:CreateRole",
                "iam:PassRole"
            ],
            "Resource": "arn:aws:iam::*:role/service-role/s3*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:List*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:AttachRolePolicy",
                "iam:PutRolePolicy",
                "iam:CreatePolicy"
              ],
            "Resource": [
                "arn:aws:iam::*:policy/service-role/s3*",
                "arn:aws:iam::*:role/service-role/s3*"
            ]
        }
    ]
}
```

IAM ロールの作成

デフォルトで、すべての Simple Storage Service (Amazon S3) リソース (バケット、オブジェクト、関連するサブリソース) はプライベートであり、リソース所有者のみがリソースにアクセスできます。Amazon S3 には、ソースバケットからオブジェクトを読み取って、レプリケートするアクセス許可が必要です。IAM ロールを作成してこれらの許可を付与し、レプリケーション設定でそのロールを指定します。

このセクションでは、信頼ポリシーとこの IAM ロールにアタッチされた最低限必要なアクセス許可ポリシーについて説明します。チュートリアル例では、IAM ロールを作成するための手順をステップバイステップで説明しています。詳細については、「ライブレプリケーションの設定例」を参照してください。

信頼ポリシーは、IAM ロールを引き受けることができるプリンシパル ID を識別します。アクセス許可ポリシーは、IAM ロールが実行できるアクション、リソース、および条件を指定します。

- 以下の例は、信頼ポリシーを示しています。ここでは、このロールを引き受けることができる AWS のサービスプリンシパルとして Amazon S3 を特定します。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"s3.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

- 以下の例は、信頼ポリシーを示しています。ここでは、このロールを引き受けることができるプリンシパルとして Amazon S3 および S3 バッチオペレーションを特定します。バッチレプリケーションジョブを作成する場合はこの方法を使用します。詳細については、「新しいレプリケーションルールまたは新しいレプリケート先にバッチレプリケーションジョブを作成する」を参照してください。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
```

```
         "Principal":{
            "Service": [
              "s3.amazonaws.com",
              "batchoperations.s3.amazonaws.com"
           ]
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

IAM ロールの詳細については、IAM ユーザーガイドの IAM ロールを参照してください。

- 以下の例は、アクセス許可ポリシーを示しています。ここでは、ユーザーに代わってレプリケーションタスクを実行する許可を IAM ロールに付与します。Amazon S3 がこのロールを引き受ける場合、このポリシーで指定されたアクセス許可を持つことになります。このポリシーでは、*amzn-s3-demo-source-bucket* はレプリケート元バケットで、*amzn-s3-demo-destination-bucket* はレプリケート先バケットです。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetReplicationConfiguration",
            "s3:ListBucket"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetObjectVersionForReplication",
            "s3:GetObjectVersionAcl",
            "s3:GetObjectVersionTagging"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
         ]
      },
```

```
      {
         "Effect":"Allow",
         "Action":[
            "s3:ReplicateObject",
            "s3:ReplicateDelete",
            "s3:ReplicateTags"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
      }
   ]
}
```

以下のアクセス許可ポリシーは、以下のアクションに対する許可を付与します。

- s3:GetReplicationConfiguration および s3:ListBucket — *amzn-s3-demo-source-bucket* バケットでのこれらのアクションの許可により、Amazon S3 はレプリケーション設定とリストバケットのコンテンツを取得できます。(現在の権限モデルには、s3:ListBucket 削除マーカーにアクセスするために許可が必要です。)
- s3:GetObjectVersionForReplication および s3:GetObjectVersionAcl – すべてのオブジェクトに付与されているこれらのアクションの許可で、Simple Storage Service (Amazon S3) はオブジェクトに関連付けられた特定のオブジェクトバージョンとアクセスコントロールリスト (ACL) を取得することができます。
- s3:ReplicateObject および s3:ReplicateDelete — *amzn-s3-demo-destination-bucket* バケットのオブジェクトに属すこれらのアクションの許可により、Simple Storage Service (Amazon S3) はレプリケート先バケットにオブジェクトまたは削除マーカーをレプリケートできます。削除マーカーの詳細については、「削除オペレーションがレプリケーションに与える影響」を参照してください。

  > **Note**
  >
  > *amzn-s3-demo-destination-bucket* バケット に対する s3:ReplicateObject アクションの許可により、オブジェクトタグや ACL などのメタデータのレプリケーションも許可されます。したがって、s3:ReplicateTags アクションのアクセス許可を明示的に付与する必要はありません。

- s3:GetObjectVersionTagging — *amzn-s3-demo-source-bucket* バケットのオブジェクトに属するこのアクションの許可により、Amazon S3 はレプリケーションのためにオブジェクトタグを読み取ることができるようになります。オブジェクトタグの詳細

については、タグを使用してストレージを分類するを参照してください。Amazon S3 が `s3:GetObjectVersionTagging` アクセス許可を持っていない場合は、オブジェクトはレプリケートされますが、オブジェクトタグはレプリケートされません。

Amazon S3 アクションの一覧については、「サービス認可リファレンス」の「Amazon S3 のアクション、リソース、および条件キー」を参照してください。

S3 リソースタイプ別の S3 API オペレーションへのアクセス許可の詳細については、「Amazon S3 API オペレーションに必要なアクセス許可」を参照してください。

Important

IAM ロールを所有する AWS アカウントは、IAM ロールに付与するアクションの許可を持っている必要があります。
例えば、レプリケート元バケットに別の AWS アカウントが所有するオブジェクトが含まれていたとします。オブジェクトの所有者は、IAM ロールを所有する AWS アカウントに、オブジェクトのアクセスコントロールリスト (ACL) を介して必要な許可を明示的に付与する必要があります。そうでない場合、Amazon S3 はオブジェクトにアクセスできず、オブジェクトのレプリケーションは失敗します。ACL のアクセス許可については、「アクセスコントロールリスト (ACL) の概要」を参照してください。
ここで説明されているアクセス許可は、最小のレプリケーション設定に関連しています。オプションのレプリケーション設定を追加する場合は、追加のアクセス許可を Amazon S3 に付与する必要があります。

- 暗号化されたオブジェクトをレプリケートする場合は、必要な AWS Key Management Service (AWS KMS) キーアクセス許可も付与する必要があります。詳細については、「the section called “暗号化オブジェクトのレプリケート”」を参照してください。
- レプリケーションでオブジェクトロックを使用するには、レプリケーションの設定に使用する AWS Identity and Access Management (IAM) ロールで、ソース S3 バケットに対する 2 つの追加のアクセス許可を付与する必要があります。2 つの新しいアクセス許可とは `s3:GetObjectRetention` と `s3:GetObjectLegalHold` です。ロールに `s3:Get*` アクセス許可がある場合、そのステートメントは要件を満たしています。詳細については、「the section called “S3 レプリケーションでのオブジェクトロックの使用”」を参照してください。

レプリケーション元とレプリケーション先のバケットが異なる AWS アカウントによって所有されている場合の許可の付与

レプリケート元バケットとレプリケート先バケットが同じアカウントによって所有されていない場合、レプリケート先バケット所有者は、次のように、レプリケート元バケット所有者にレプリケーションアクションを実行する許可を付与するバケットポリシーも追加する必要があります。このポリシーの例では、*amzn-s3-demo-destination-bucket* はレプリケーション先バケットです。

Amazon S3 コンソールを使用して、このバケットポリシーを自動的に生成することもできます。詳細については、「レプリケートされたオブジェクトをレプリケート元バケットから受信できるようにする」を参照してください。

> **Note**
>
> ロールの ARN 形式が異なって表示される場合があります。コンソールを使用してロールが作成された場合、ARN 形式は `arn:aws:iam::`*account-ID*`:role/service-role/`*role-name* です。AWS CLI を使用してロールが作成された場合、ARN 形式は `arn:aws:iam::`*account-ID*`:role/`*role-name* です。詳細については、「IAM ユーザーガイド」の「IAM ロール」を参照してください。

```
{
   "Version":"2012-10-17",
   "Id":"PolicyForDestinationBucket",
   "Statement":[
      {
         "Sid":"Permissions on objects",
         "Effect":"Allow",
         "Principal":{
            "AWS":"arn:aws:iam::source-bucket-account-ID:role/service-role/source-account-IAM-role"
         },
         "Action":[
            "s3:ReplicateDelete",
            "s3:ReplicateObject"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
      },
      {
         "Sid":"Permissions on bucket",
         "Effect":"Allow",
```

```
         "Principal":{
            "AWS":"arn:aws:iam::source-bucket-account-ID:role/service-role/source-
account-IAM-role"
         },
         "Action": [
            "s3:List*",
            "s3:GetBucketVersioning",
            "s3:PutBucketVersioning"
         ],
         "Resource":"arn:aws:s3::amzn-s3-demo-destination-bucket"
      }
   ]
}
```

例については、異なるアカウントでのバケットのレプリケーション設定を参照してください。

レプリケート元バケットのオブジェクトがタグ付きの場合は、以下の点に注意してください。

- レプリケート元のバケット所有者が (IAM ロールによって) オブジェクトタグをレプリケートするための s3:GetObjectVersionTagging および s3:ReplicateTags アクションのアクセス許可を Amazon S3 に付与した場合、Amazon S3 はオブジェクトと共にタグをレプリケートします。IAM ロールに関する詳細は、「IAM ロールの作成」を参照してください。
- レプリケート先のバケット所有者は、タグがレプリケートされるのを望まない場合、次のステートメントをレプリケート先のバケットポリシーに追加することで、s3:ReplicateTags アクションのアクセス許可を明示的に拒否できます。このポリシーでは、*amzn-s3-demo-destination-bucket* はレプリケーション先バケットです。

```
...
   "Statement":[
      {
         "Effect":"Deny",
         "Principal":{
            "AWS":"arn:aws:iam::source-bucket-account-id:role/service-role/source-
account-IAM-role"
         },
         "Action":"s3:ReplicateTags",
         "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
      }
   ]
...
```

> **Note**
>
> - 暗号化されたオブジェクトをレプリケートする場合は、必要な AWS Key Management Service (AWS KMS) キーアクセス許可も付与する必要があります。詳細については、「the section called “暗号化オブジェクトのレプリケート”」を参照してください。
> - レプリケーションでオブジェクトロックを使用するには、レプリケーションの設定に使用する AWS Identity and Access Management (IAM) ロールで、ソース S3 バケットに対する 2 つの追加のアクセス許可を付与する必要があります。2 つの新しいアクセス許可とは `s3:GetObjectRetention` と `s3:GetObjectLegalHold` です。ロールに `s3:Get*` アクセス許可がある場合、そのステートメントは要件を満たしています。詳細については、「the section called “S3 レプリケーションでのオブジェクトロックの使用”」を参照してください。

レプリケートされたオブジェクトをレプリケート元バケットから受信できるようにする

上記のポリシーをレプリケート先バケットに手動で追加する代わりに、Amazon S3 コンソールを介して、レプリケート元バケットからレプリケートされたオブジェクトの受信を有効にするために必要なポリシーをすばやく生成できます。

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。
3. バケットリストで、レプリケート先バケットとして使用するバケットを選択します。
4. [Management (管理)] タブを選択し、[Replication rules (レプリケーションルール)] まで下にスクロールします。
5. [Actions] (アクション)で、[Receive replicated objects] (レプリケートされたオブジェクトの受信) を選択します。

   プロンプトに従って、レプリケート元バケットアカウントの AWS アカウント ID を選択し、[ポリシーの生成] を選択します。コンソールにより、Amazon S3 バケットポリシーと KMS キーポリシーが生成されます。
6. このポリシーを既存のバケットポリシーに追加するには、[Apply settings] (設定の適用) を選択するか、または [Copy] (コピー) をクリックして、変更を手動でコピーします。
7. (オプション) AWS KMS ポリシーを AWS Key Management Service コンソール上の必要な KMS キーポリシーへコピーします。

レプリカの所有権の変更

レプリケート元とレプリケート先のバケットが、異なる AWS アカウントによって所有されている場合、レプリケート先バケットを所有する AWS アカウントにレプリカの所有者を変更するように Amazon S3 に指示できます。所有者上書きの詳細については、「レプリカ所有者の変更」を参照してください。

S3 バッチオペレーションに対するアクセス許可の付与

S3 バッチレプリケーションでは、次のオブジェクトをレプリケートできます。

- レプリケーション設定が実行される前に存在していたオブジェクト
- 以前にレプリケートされたオブジェクト
- レプリケーションに失敗したオブジェクト

新しいレプリケーション設定で最初のルールを作成する場合や、Amazon S3 コンソールを介して新しいレプリケート先を既存の設定に追加する場合は、1 回限りのバッチレプリケーションジョブを作成できます。バッチオペレーションジョブを作成して、既存のレプリケーション設定でバッチレプリケーションを開始することもできます。

バッチレプリケーションの IAM ロールとポリシーの例については、「S3 バッチレプリケーション用の IAM ロールの設定」を参照してください。

ライブレプリケーションの設定例

以下の例は、一般的なユースケース用にライブレプリケーションを設定するためのステップバイステップのチュートリアルを示しています。

> **Note**
>
> ライブレプリケーションとは、同一リージョンレプリケーション (SRR) およびクロスリージョンレプリケーション (CRR) を指します。ライブレプリケーションでは、レプリケーションを設定する前にバケットに存在していたオブジェクトはレプリケートされません。レプリケーションを設定する前に存在していたオブジェクトをレプリケートするには、オンデマンドレプリケーションを使用します。バケットを同期して既存のオブジェクトをオンデマンドでレプリケートするには、「既存のオブジェクトのレプリケーション」を参照してください。

これらの例は、Amazon S3 コンソール、AWS Command Line Interface (AWS CLI)、AWS SDK (AWS SDK for Java および AWS SDK for .NET の例を示します) を使用したレプリケーション設定の作成方法を示しています。

AWS CLI のインストールと設定方法の詳細については、「AWS Command Line Interface ユーザーガイド」の次のトピックを参照してください。

- AWS CLI の開始方法
- AWS CLI の設定 - 少なくとも 1 つのプロファイルを設定する必要があります。クロスアカウントのシナリオを学習する場合は、2 つのプロファイルを設定します。

AWS SDK の詳細については、「AWS SDK for Java」および「AWS SDK for .NET」を参照してください。

> **Tip**
>
> ライブレプリケーションを使用してデータをレプリケートする方法の詳細な手順を説明するチュートリアルについては、「Amazon S3 レプリケーションを使用して、AWS リージョン内およびリージョン間でデータをレプリケートする」を参照してください。

トピック

- 同じアカウントでのバケットのレプリケーションの設定
- 異なるアカウントでのバケットのレプリケーション設定
- S3 Replication Time Control (S3 RTC)を使用してコンプライアンス要件を満たす
- 暗号化されたオブジェクトのレプリケート (SSE-S3、SSE-KMS、DSSE-KMS、SSE-C)
- レプリカの変更同期によるメタデータ変更のレプリケート
- バケット間での削除マーカーのレプリケーション

同じアカウントでのバケットのレプリケーションの設定

ライブレプリケーションは、同一または異なる AWS リージョンにある汎用バケット間でオブジェクトを自動的に非同期でコピーする機能です。ライブレプリケーションでは、新しく作成されたオブジェクトおよびオブジェクトの更新が、レプリケート元バケットからレプリケート先バケットにコピーされます。詳細については、「リージョン内およびリージョン間でのオブジェクトのレプリケート」を参照してください。

レプリケーションを設定するときは、レプリケート元バケットにレプリケーションルールを追加します。レプリケーションルールにより、レプリケート元のソースバケットオブジェクトと、レプリケートされたオブジェクトが保存されるレプリケート先バケットが定義されます。ルールを作成して、バケット内のすべてのオブジェクト、または特定のキー名のプレフィックス、1 つ以上のオブジェクトタグ、あるいはその両方を持つオブジェクトのサブセットをレプリケートできます。レプリケート先のバケットはレプリケート元バケットと同じ AWS アカウントにあっても、別のアカウントにあってもかまいません。

削除するオブジェクトバージョンの ID を指定した場合、Amazon S3 はソースバケット内のそのオブジェクトバージョンを削除します。しかし、レプリケート先バケット内でその削除をレプリケートすることはありません。つまり、レプリケート先バケットから同じオブジェクトバージョンを削除しません。これは悪意のある削除からデータを保護します。

バケットにレプリケーションルールを追加すると、ルールはデフォルトで有効になるため、保存するとすぐに動作を開始します。

この例では、同じ AWS アカウントがレプリケート元とレプリケート先のバケットを所有している場合の、ライブレプリケーションのセットアップを行います。Amazon S3 コンソールを使用する例については、AWS Command Line Interface (AWS CLI)、AWS SDK for Java、および AWS SDK for .NET を参照してください。

前提条件

次の手順を使用する前に、ソースバケットと保存先バケットが同じアカウントによって所有されているか異なるアカウントによって所有されているかに応じて、レプリケーションに必要なアクセス許可が設定されていることを確認してください。詳細については、「the section called “アクセス許可のセットアップ”」を参照してください。

Note

- 暗号化されたオブジェクトをレプリケートする場合は、必要な AWS Key Management Service (AWS KMS) キーアクセス許可も付与する必要があります。詳細については、「the section called “暗号化オブジェクトのレプリケート”」を参照してください。
- レプリケーションでオブジェクトロックを使用するには、レプリケーションの設定に使用する AWS Identity and Access Management (IAM) ロールで、ソース S3 バケットに対する 2 つの追加のアクセス許可を付与する必要があります。2 つの新しいアクセス許可とは `s3:GetObjectRetention` と `s3:GetObjectLegalHold` です。ロールに `s3:Get*` アクセス許可がある場合、そのステートメントは要件を満たしています。詳細については、

「the section called “S3 レプリケーションでのオブジェクトロックの使用”」を参照してください。

S3 コンソールの使用

ソースバケットと同じ AWS アカウント に送信先バケットがある場合にレプリケーションルールを設定するには、以下の手順を実行します。

レプリケート先バケットがレプリケート元バケットとは別のアカウントにある場合は、レプリケート先バケットにバケットポリシーを追加して、レプリケート元バケットアカウントの所有者に、レプリケート先バケットのオブジェクトをレプリケートするアクセス許可を付与する必要があります。詳細については、「レプリケーション元とレプリケーション先のバケットが異なる AWS アカウントによって所有されている場合の許可の付与」を参照してください。

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[汎用バケット] を選択します。
3. バケットリストで、目的のバケットの名前を選択します。
4. [管理] タブをクリックし、[レプリケーションルール] までスクロールして、[レプリケーションルールを作成] を選択します。
5. [レプリケーションルールの設定] セクションの、[レプリケーションルール名] で、後でルールを識別しやすいようにルールの名前を入力します。ルール名は必須であり、バケット内で一意である必要があります。
6. [ステータス] では、デフォルトで [有効] が選択されています。有効にされたルールは、保存するとすぐに機能し始めます。ルールを後から有効にする場合は、[無効] を選択します。
7. バケットに既存のレプリケーションルールがある場合は、ルールの優先順位を指定するよう指示されます。ルールの優先順位を指定して、複数のルールの範囲に含まれるオブジェクトによって引き起こされる競合を回避する必要があります。ルールが重複している場合、Amazon S3 はルールの優先度を使用して適用するルールを決定します。数値が大きいほど、優先度が高くなります。ルーティングの優先度の詳細については、「レプリケーション設定ファイル要素」をご覧ください。
8. [ソースバケット] には、レプリケーションソースを設定するための次のオプションがあります。
   - バケット全体をレプリケートするには、[Apply to all objects in the bucket] (バケット内のすべてのオブジェクトに適用) を選択します。

- 同じプレフィックスを持つすべてのオブジェクトをレプリケートするには、[Limit the scope of this rule using one or more filters (1 つまたは複数のフィルターを使用してこのルールの適用範囲を制限します)] を選択します。これにより、指定したプレフィックスで始まる名前を持つすべてのオブジェクトにレプリケーションが制限されます (`pictures` など)。[プレフィックス] ボックスにプレフィックスを入力します。

  > **Note**
  >
  > フォルダの名前をプレフィックスとして入力する場合は、最後の文字に [/] (スラッシュ) を使用する必要があります (例: `pictures/`)。

- 1 つまたは複数のオブジェクトタグを持つすべてのオブジェクトをレプリケートするには、[タグを追加] を選択し、ボックスにキーと値のペアを入力します。別のタグを追加するには、この手順を繰り返します。プレフィックスとタグを組み合わせることができます。オブジェクトタグの詳細については、タグを使用してストレージを分類するを参照してください。

新しいレプリケーション設定 XML スキーマでは、プレフィックスとタグのフィルタリング、およびルールの優先順位付けがサポートされています。新しいスキーマの詳細については、後方互換性に関する考慮事項を参照してください。ユーザーインターフェイスの背後で機能する Amazon S3 API で使用される XML の詳細については、「レプリケーション設定ファイル要素」を参照してください。新しいスキーマは、レプリケーション設定 XML V2 として記述されます。

9. [レプリケート先] で、Amazon S3 がオブジェクトをレプリケートするバケットを選択します。

   > **Note**
   >
   > レプリケート先バケットの数は、特定のパーティション内の AWS リージョンの数に制限されます。パーティションは、リージョンのグループです。AWS には、現在 `aws` (標準リージョン)、`aws-cn` (中国リージョン)、および `aws-us-gov` (AWS GovCloud (US) リージョン) の 3 つのパーティションがあります。レプリケート先バケット制限の増加をリクエストするには、サービスのクォータを使用できます。

   - アカウントのバケットにレプリケートするには、[このアカウントのバケットを選択] をクリックし、レプリケート先バケット名を入力または参照します。

- 別の AWS アカウント のバケットにレプリケートするには、[別のアカウントのバケットを指定] を選択し、レプリケート先バケットのアカウント ID とバケット名を入力します。

  レプリケート先バケットがレプリケート元バケットとは別のアカウントにある場合は、レプリケート先バケットにバケットポリシーを追加して、レプリケート元バケットアカウントの所有者にオブジェクトをレプリケートするアクセス許可を付与する必要があります。詳細については、「レプリケーション元とレプリケーション先のバケットが異なる AWS アカウントによって所有されている場合の許可の付与」を参照してください。

  必要に応じて、レプリケート先バケット内の新しいオブジェクトの所有を標準化するために、[オブジェクト所有者を送信先バケット所有者に変更] を選択します。このオプションの詳細については、「オブジェクトの所有権の制御とバケットの ACL の無効化。」を参照してください。

> **Note**
>
> レプリケート先バケットでバージョニングが有効になっていない場合は、[バージョニングを有効化] ボタンを含む警告が表示されます。バケットでバージョニングを有効にするには、このボタンを選択します。

10. Amazon S3 がユーザーのためにオブジェクトをレプリケートできる AWS Identity and Access Management (IAM) ロールを設定します。

    IAM ロールを設定するには、[IAM ロール] セクションで [IAM ロール] ドロップダウンリストから次のいずれかを選択します。

    - [Create new role (新しいロールの作成)] を選択して、Amazon S3 で新しい IAM ロールが自動的に作成されるようにすることを強くお勧めします。ルールを保存すると、選択したレプリケート元バケットとレプリケート先バケットに一致する IAM ロールに対して新しいポリシーが生成されます。
    - 既存の IAM ロールの使用も選択できます。その場合は、レプリケーションに必要なアクセス許可を Amazon S3 に付与するロールを選択する必要があります。このロールがレプリケーションルールに従うための十分なアクセス許可を Amazon S3 に付与しない場合、レプリケーションは失敗します。

> **Important**
>
> レプリケーションルールをバケットに追加する場合は、Amazon S3 にレプリケーションアクセス許可を付与する IAM ロールを渡すことができる `iam:PassRole` アクセス許可が必要です。詳細については、IAM ユーザーガイドの「AWS のサービス のサービスにロールを渡すアクセス権限をユーザーに付与する」を参照してください。

11. AWS Key Management Service (AWS KMS) キーを使用したサーバー側の暗号化 (SSE-KMS) で暗号化されたソースバケット内のオブジェクトをレプリケートするには、[暗号化] で [AWS KMS で暗号化されたオブジェクトをレプリケート] を選択します。送信先オブジェクト暗号化用の AWS KMS キー には、レプリケーションでの使用を許可しているソースキーが示されています。デフォルトでは、すべてのソース KMS キーが含まれます。KMS キーの選択を絞り込むために、エイリアスまたはキー ID を選択できます。

    選択されていない AWS KMS keys で暗号化されたオブジェクトはレプリケートされません。KMS キーまたは KMS キーのグループが選択されていますが、必要に応じて KMS キーを選択できます。AWS KMS をレプリケーションで使用する方法については、暗号化されたオブジェクトのレプリケート (SSE-S3、SSE-KMS、DSSE-KMS、SSE-C) を参照してください。

    > **Important**
    >
    > AWS KMS で暗号化されたオブジェクトをレプリケートすると、AWS KMS リクエストレートは、ソースリージョンでは倍になり、送信先リージョンでは同じ量だけ増加します。AWS KMS に対するこれらの呼び出しレートの増加は、レプリケーションの送信先リージョンに対して定義した KMS キーを使用してデータが再暗号化された方法によるものです。AWS KMS では、リージョンごとに呼び出しアカウントあたりのリクエストレートが制限されています。制限のデフォルト値については、AWS Key Management Service デベロッパーガイドの「AWS KMS の制限 - 1 秒あたりのリクエスト数: 可変」を参照してください。
    > レプリケーションにおける現在の Amazon S3 PUT オブジェクトリクエストレートが、アカウントでデフォルトで設定されている AWS KMS レート制限の半分を超えている場合は、AWS KMS リクエストレート制限の引き上げをリクエストすることをお勧めします。引き上げをリクエストするには、サポート センターのお問い合わせでケースを作成します。例えば、現在の PUT オブジェクトのリクエストレートが 1 秒あたり 1,000 リクエストであり、オブジェクトの暗号化に AWS KMS を使用しているとします。この場合、レプリケート元リージョンとレプリケート先リージョン (リージョンが異なる場合)

の両方で AWS KMS レート制限を毎秒 2,500 リクエストに引き上げるよう サポート に依頼することをお勧めします。これにより、AWS KMS によるスロットリングがなくなります。
レプリケート元バケットの PUT オブジェクトのリクエストレートを確認するには、Amazon S3 の Amazon CloudWatch リクエストメトリクスの `PutRequests` を確認します。CloudWatch メトリクスの表示方法については、「S3 コンソールの使用」を参照してください

AWS KMS で暗号化されたオブジェクトをレプリケートを選択した場合は、以下の操作を実行します。

- [送信先オブジェクトを暗号化するための AWS KMS key] で、次のいずれかの方法で KMS キーを指定します。
  - 使用可能な KMS キーのリストから選択するには、[AWS KMS keys から選択する] を選択し、使用可能なキーのリストから自分の KMS キーを選択します。

    AWS マネージドキー (`aws/s3`) とカスタマーマネージドキーの両方がこのリストに表示されます。カスタマーマネージドキーの詳細については、AWS Key Management Service デベロッパーガイドの「カスタマーキーと AWS キー」を参照してください。
  - KMS キー Amazon リソースネーム (ARN) を入力するには、[AWS KMS key ARN を入力] を選択し、表示されるフィールドに KMS キー ARN を入力します。これにより、レプリケート先バケットのレプリカが暗号化されます。[IAM コンソール]の [暗号化キー] で、KMS キーの ARN を検索できます。
  - AWS KMS コンソールで新しいカスタマーマネージドキーを作成するには、[KMS キーを作成] を選択します。

    AWS KMS key の作成の詳細については、「AWS Key Management Service デベロッパーガイド」の「キーの作成」を参照してください。

> **Important**
>
> バケットと同じ AWS リージョン で有効になっている KMS キーのみを使用できます。[KMS キーから選択する] を選択する場合、S3 コンソールにはリージョンごとに 100 個の KMS キーしか表示されません。同じリージョンに 100 個以上の KMS キーがある場合、S3 コンソールには最初の 100 個の KMS キーしか表示されませ

ん。コンソールに表示されていない KMS キーを使用するには、[AWS KMS key ARN を入力] を選択し、KMS キー ARN を入力します。
Amazon S3 でサーバー側の暗号化に AWS KMS key を使用する場合は、対称暗号化 KMS キーを選択する必要があります。Amazon S3 では、対称暗号化 KMS キーのみがサポートされ、非対称暗号化 KMS キーはサポートされません。詳細については、AWS Key Management Service デベロッパーガイドの「Identifying symmetric and asymmetric KMS keys」(対称および非対称 KMS キーの識別) を参照してください。

AWS KMS key の作成の詳細については、AWS Key Management Service デベロッパーガイドのキーの作成を参照してください。Amazon S3 での AWS KMS の使用に関する詳細は、「AWS KMS キーによるサーバー側の暗号化 (SSE-KMS) の使用」を参照してください。

12. [レプリケート先ストレージクラス] で、データをレプリケート先の特定のストレージクラスにレプリケートする場合は、[レプリケートされたオブジェクトのストレージクラスを変更] を選択します。次に、レプリケート先のレプリケートされたオブジェクトに使用するストレージクラスを選択します。このオプションを選択しない場合、レプリケートされたオブジェクトのストレージクラスは元のオブジェクトのクラスと同じになります。
13. 追加のレプリケーションオプションを設定する際には、次の追加オプションから選択できます。

    - レプリケーション設定で S3 Replication Time Control (S3 RTC) を有効にする場合は、[レプリケーション時間のコントロール (RTC)] を選択します。このオプションの詳細については、「S3 Replication Time Control (S3 RTC)を使用してコンプライアンス要件を満たす」を参照してください。
    - レプリケーション設定で S3 レプリケーションメトリクスを有効にするには、[Replication metrics and events] (レプリケーションメトリクスとイベント) を選択します。詳細については、「メトリクス、イベント通知、ステータスによるレプリケーションのモニタリング」を参照してください。
    - レプリケーション設定で削除マーカーレプリケーションを有効にする場合は、[削除マーカーのレプリケーション] を選択します。詳細については、「バケット間での削除マーカーのレプリケーション」を参照してください。
    - レプリケーション設定で Amazon S3 レプリカ変更の同期を有効にする場合は、[レプリカ変更の同期] を選択します。詳細については、「レプリカの変更同期によるメタデータ変更のレプリケート」を参照してください。

> **Note**
>
> S3 RTC または S3 レプリケーションメトリクスを使用する場合は、追加料金が適用されます。

14. 終了するには、[Save (保存)] を選択します。
15. ルールを保存したら、ルールを選択して [Edit rule (ルールの編集)] を選択することで、ルールを編集、有効化、無効化、または削除できます。

AWS CLI を使用する場合

レプリケート元バケットとレプリケート先バケットが同じ AWS アカウント によって所有されている場合に、レプリケーションの設定に AWS CLI を使用するには

- レプリケート元バケットとレプリケート先バケットを作成します。
- バケットでのバージョニングを有効化します。
- オブジェクトをレプリケートするための Amazon S3 許可を付与する AWS Identity and Access Management (IAM) ロールを作成します。
- レプリケート元バケットにレプリケーション設定を追加します。

設定を確認するには、テストします。

レプリケート元バケットとレプリケート先バケットが同じ AWS アカウントによって所有されている場合にレプリケーションをセットアップするには

1. AWS CLI の認証情報プロファイルを設定します。この例では、プロファイル名 `acctA` を使用します。名前付きプロファイルの設定と使用に関する詳細については、「AWS Command Line Interface ユーザーガイド」の「設定ファイルと認証情報ファイルの設定」を参照してください。

> **Important**
>
> この例に使用するプロファイルは、必要なアクセス権限を持っている必要があります。たとえば、レプリケーション設定で、Amazon S3 が引き受けることができる IAM ロールを指定します。使用するプロファイルに `iam:PassRole` アクセス権限がある場合のみ実行できます。詳細については、「IAM ユーザーガイド」の「AWS のサービス に

ロールを渡すアクセス権限をユーザーに付与する」を参照してください。管理者の認証情報を使用して名前付きプロファイルを作成すると、すべてのタスクを実行できるようになります。

2. 次の AWS CLI コマンドを使用してレプリケート元バケットを作成し、バージョニングを有効にします。これらのコマンドを使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

   次の create-bucket コマンドは、米国東部 (バージニア北部) (us-east-1) リージョンに *amzn-s3-demo-source-bucket* バケットを作成します。

```
aws s3api create-bucket \
--bucket amzn-s3-demo-source-bucket \
--region us-east-1 \
--profile acctA
```

   次の put-bucket-versioning コマンドは、*amzn-s3-demo-source-bucket* バケットで S3 バージョニングを有効にします。

```
aws s3api put-bucket-versioning \
--bucket amzn-s3-demo-source-bucket \
--versioning-configuration Status=Enabled \
--profile acctA
```

3. 次の AWS CLI コマンドを使用してレプリケート先バケットを作成し、バージョニングを有効にします。これらのコマンドを使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

> **Note**
>
> レプリケーション元とレプリケーション先バケットの両方が同じ AWS アカウントにある場合、レプリケーション設定をセットアップするには、レプリケート元バケットおよびレプリケート先バケットに同じプロファイルを使用します。この例では acctA を使用します。
> 異なる AWS アカウントによってバケットが所有されている場合、レプリケーション設定をテストするには、それぞれのアカウント異なるプロファイルを指定します。例えば、レプリケート先バケットに acctB プロファイルを使用します。

次の create-bucket コマンドは、米国西部 (オレゴン) (us-west-2) リージョンに *amzn-s3-demo-destination-bucket* というレプリケート先バケットを作成します。

```
aws s3api create-bucket \
--bucket amzn-s3-demo-destination-bucket \
--region us-west-2 \
--create-bucket-configuration LocationConstraint=us-west-2 \
--profile acctA
```

次の put-bucket-versioning コマンドは、*amzn-s3-demo-destination-bucket* バケットで S3 バージョニングを有効にします。

```
aws s3api put-bucket-versioning \
--bucket amzn-s3-demo-destination-bucket \
--versioning-configuration Status=Enabled \
--profile acctA
```

4. IAM ロールを作成します。*#######*バケットに後で追加するレプリケーション設定でこのロールを指定します。Amazon S3 は、ユーザーに代わってオブジェクトをレプリケートするこのロールを引き受けます。IAM ロールは 2 つのステップで作成します。

   - ロールを作成します。
   - アクセス権限ポリシーをロールにアタッチします。

   a. IAM ロールを作成します。

      i. 次の信頼ポリシーをコピーして、ローカルコンピュータの現在のディレクトリにある s3-role-trust-policy.json という名前のファイルに保存します。このポリシーは、ロールを引き受けるアクセス許可を Amazon S3 サービスプリンシパルに付与します。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
```

```
            "Service":"s3.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

ii. 次のコマンドを実行して、ロールを作成します。

```
$ aws iam create-role \
--role-name replicationRole \
--assume-role-policy-document file://s3-role-trust-policy.json  \
--profile acctA
```

b. アクセス権限ポリシーをロールにアタッチします。

i. 次のアクセス権限ポリシーをコピーして、ローカルコンピュータの現在のディレクトリにある s3-role-permissions-policy.json という名前のファイルに保存します。このポリシーは、さまざまな Amazon S3 バケットとオブジェクトアクションに対するアクセス許可を付与します。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetObjectVersionForReplication",
            "s3:GetObjectVersionAcl",
            "s3:GetObjectVersionTagging"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:ListBucket",
            "s3:GetReplicationConfiguration"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket"
```

```
            ]
        },
        {
            "Effect":"Allow",
            "Action":[
               "s3:ReplicateObject",
               "s3:ReplicateDelete",
               "s3:ReplicateTags"
            ],
            "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
        }
    ]
}
```

> **Note**
>
> - 暗号化されたオブジェクトをレプリケートする場合は、必要な AWS Key Management Service (AWS KMS) キーアクセス許可も付与する必要があります。詳細については、「the section called “暗号化オブジェクトのレプリケート”」を参照してください。
> - レプリケーションでオブジェクトロックを使用するには、レプリケーションの設定に使用する AWS Identity and Access Management (IAM) ロールで、ソース S3 バケットに対する 2 つの追加のアクセス許可を付与する必要があります。2 つの新しいアクセス許可とは `s3:GetObjectRetention` と `s3:GetObjectLegalHold` です。ロールに `s3:Get*` アクセス許可がある場合、そのステートメントは要件を満たしています。詳細については、「the section called “S3 レプリケーションでのオブジェクトロックの使用”」を参照してください。

ii. ポリシーを作成してロールにアタッチするには、次のコマンドを実行します。*user input placeholders* を、ユーザー自身の情報に置き換えます。

```
$ aws iam put-role-policy \
--role-name replicationRole \
--policy-document file://s3-role-permissions-policy.json \
--policy-name replicationRolePolicy \
--profile acctA
```

5. レプリケート元バケットにレプリケーション設定を追加します。

a. Amazon S3 API はレプリケーション設定を XML で指定する必要がありますが、AWS CLI はレプリケーション設定を JSON で指定する必要があります。以下の JSON を、コンピュータのローカルディレクトリの replication.json というファイルに保存します。

```
{
  "Role": "IAM-role-ARN",
  "Rules": [
    {
      "Status": "Enabled",
      "Priority": 1,
      "DeleteMarkerReplication": { "Status": "Disabled" },
      "Filter" : { "Prefix": "Tax"},
      "Destination": {
        "Bucket": "arn:aws:s3:::amzn-s3-demo-destination-bucket"
      }
    }
  ]
}
```

b. *amzn-s3-demo-destination-bucket* および *IAM-role-ARN* の値を独自の情報に置き換えて JSON を更新します。変更を保存します。

c. 次の put-bucket-replication コマンドを実行して、レプリケート元バケットにレプリケーション設定を追加します。必ずレプリケート元バケット名を指定してください。

```
$ aws s3api put-bucket-replication \
--replication-configuration file://replication.json \
--bucket amzn-s3-demo-source-bucket \
--profile acctA
```

レプリケーション設定を取得するには、get-bucket-replication コマンドを使用します。

```
$ aws s3api get-bucket-replication \
--bucket amzn-s3-demo-source-bucket \
--profile acctA
```

6. 次の手順を実行して、Amazon S3 コンソールでセットアップをテストします。

a. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。

b. 左側のナビゲーションペインで、[バケット] を選択します。[汎用バケット] リストで、レプリケート元バケットの名前を選択します。

c. レプリケート元バケットに *Tax* という名前のフォルダを作成します。

d. レプリケート元バケット内の *Tax* フォルダにサンプルオブジェクトを追加します。

> **Note**
>
> Amazon S3 がオブジェクトをレプリケートするのにかかる時間は、オブジェクトのサイズによって異なります。レプリケーションのステータスを確認する方法については、「レプリケーションステータス情報の取得」を参照してください。

*#######*バケットで、以下の点を確認します。

- Amazon S3 がオブジェクトをレプリケートしたこと。
- オブジェクトがレプリカであること。オブジェクトの [プロパティ] タブで、[オブジェクト管理の概要] セクションまでスクロールします。[管理設定] で、[レプリケーションステータス] の [値] を確認します。この値が `REPLICA` に設定されていることを確認します。
- レプリカがレプリケート元バケットアカウントによって所有されていること。オブジェクトの [アクセス許可] タブで、オブジェクトの所有権を確認できます。

  レプリケート元とレプリケート先のバケットが、異なるアカウントによって所有されている場合、オプションの設定を追加して、レプリカの所有権をレプリケート先バケットに変更するように Amazon S3 に対して指示できます。例については、レプリカの所有者を変更する方法を参照してください。

AWS SDK の使用

以下のコード例を使用して、AWS SDK for Java および AWS SDK for .NET で、レプリケーション設定をバケットにそれぞれ追加します。

> **Note**
>
> - 暗号化されたオブジェクトをレプリケートする場合は、必要な AWS Key Management Service (AWS KMS) キーアクセス許可も付与する必要があります。詳細については、「the section called “暗号化オブジェクトのレプリケート”」を参照してください。

- レプリケーションでオブジェクトロックを使用するには、レプリケーションの設定に使用する AWS Identity and Access Management (IAM) ロールで、ソース S3 バケットに対する 2 つの追加のアクセス許可を付与する必要があります。2 つの新しいアクセス許可とは `s3:GetObjectRetention` と `s3:GetObjectLegalHold` です。ロールに `s3:Get*` アクセス許可がある場合、そのステートメントは要件を満たしています。詳細については、「the section called “S3 レプリケーションでのオブジェクトロックの使用”」を参照してください。

Java

以下の例では、まずバケットにレプリケーション設定を追加した後、その設定を取得して確認します。作業サンプルの作成およびテストの手順については、「AWS SDK for Java デベロッパーガイド」の「使用開始」を参照してください。

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.identitymanagement.AmazonIdentityManagement;
import
 com.amazonaws.services.identitymanagement.AmazonIdentityManagementClientBuilder;
import com.amazonaws.services.identitymanagement.model.CreateRoleRequest;
import com.amazonaws.services.identitymanagement.model.PutRolePolicyRequest;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3Client;
import com.amazonaws.services.s3.model.BucketReplicationConfiguration;
import com.amazonaws.services.s3.model.BucketVersioningConfiguration;
import com.amazonaws.services.s3.model.CreateBucketRequest;
import com.amazonaws.services.s3.model.DeleteMarkerReplication;
import com.amazonaws.services.s3.model.DeleteMarkerReplicationStatus;
import com.amazonaws.services.s3.model.ReplicationDestinationConfig;
import com.amazonaws.services.s3.model.ReplicationRule;
import com.amazonaws.services.s3.model.ReplicationRuleStatus;
import com.amazonaws.services.s3.model.SetBucketVersioningConfigurationRequest;
import com.amazonaws.services.s3.model.StorageClass;
import com.amazonaws.services.s3.model.replication.ReplicationFilter;
import com.amazonaws.services.s3.model.replication.ReplicationFilterPredicate;
import com.amazonaws.services.s3.model.replication.ReplicationPrefixPredicate;
```

```
import java.io.IOException;
import java.util.ArrayList;
import java.util.HashMap;
import java.util.List;
import java.util.Map;

public class CrossRegionReplication {

        public static void main(String[] args) throws IOException {
                Regions clientRegion = Regions.DEFAULT_REGION;
                String accountId = "*** Account ID ***";
                String roleName = "*** Role name ***";
                String sourceBucketName = "*** Source bucket name ***";
                String destBucketName = "*** Destination bucket name ***";
                String prefix = "Tax/";

                String roleARN = String.format("arn:aws:iam::%s:%s", accountId,
 roleName);
                String destinationBucketARN = "arn:aws:s3:::" + destBucketName;

                AmazonS3 s3Client = AmazonS3Client.builder()
                                .withCredentials(new ProfileCredentialsProvider())
                                .withRegion(clientRegion)
                                .build();

                createBucket(s3Client, clientRegion, sourceBucketName);
                createBucket(s3Client, clientRegion, destBucketName);
                assignRole(roleName, clientRegion, sourceBucketName,
 destBucketName);

                try {

                        // Create the replication rule.
                        List<ReplicationFilterPredicate> andOperands = new
 ArrayList<ReplicationFilterPredicate>();
                        andOperands.add(new ReplicationPrefixPredicate(prefix));

                        Map<String, ReplicationRule> replicationRules = new
 HashMap<String, ReplicationRule>();
                        replicationRules.put("ReplicationRule1",
                                        new ReplicationRule()
                                                        .withPriority(0)

 .withStatus(ReplicationRuleStatus.Enabled)
```

```
.withDeleteMarkerReplication(
                                                                    new
DeleteMarkerReplication().withStatus(

   DeleteMarkerReplicationStatus.DISABLED))
                                                        .withFilter(new
ReplicationFilter().withPredicate(
                                                                    new
ReplicationPrefixPredicate(prefix)))
                                                        .withDestinationConfig(new
ReplicationDestinationConfig()

.withBucketARN(destinationBucketARN)

.withStorageClass(StorageClass.Standard)));

                        // Save the replication rule to the source bucket.
                        s3Client.setBucketReplicationConfiguration(sourceBucketName,
                                        new BucketReplicationConfiguration()
                                                        .withRoleARN(roleARN)

.withRules(replicationRules));

                        // Retrieve the replication configuration and verify that
the configuration
                        // matches the rule we just set.
                        BucketReplicationConfiguration replicationConfig = s3Client

.getBucketReplicationConfiguration(sourceBucketName);
                        ReplicationRule rule =
replicationConfig.getRule("ReplicationRule1");
                        System.out.println("Retrieved destination bucket ARN: "
                                        +
rule.getDestinationConfig().getBucketARN());
                        System.out.println("Retrieved priority: " +
rule.getPriority());
                        System.out.println("Retrieved source-bucket replication rule
status: " + rule.getStatus());
                } catch (AmazonServiceException e) {
                        // The call was transmitted successfully, but Amazon S3
couldn't process
                        // it, so it returned an error response.
                        e.printStackTrace();
```

```
                } catch (SdkClientException e) {
                        // Amazon S3 couldn't be contacted for a response, or the
 client
                        // couldn't parse the response from Amazon S3.
                        e.printStackTrace();
                }
        }

        private static void createBucket(AmazonS3 s3Client, Regions region, String
 bucketName) {
                CreateBucketRequest request = new CreateBucketRequest(bucketName,
 region.getName());
                s3Client.createBucket(request);
                BucketVersioningConfiguration configuration = new
 BucketVersioningConfiguration()
                                .withStatus(BucketVersioningConfiguration.ENABLED);

                SetBucketVersioningConfigurationRequest enableVersioningRequest =
 new SetBucketVersioningConfigurationRequest(
                                bucketName, configuration);
                s3Client.setBucketVersioningConfiguration(enableVersioningRequest);

        }

        private static void assignRole(String roleName, Regions region, String
 sourceBucket, String destinationBucket) {
                AmazonIdentityManagement iamClient =
 AmazonIdentityManagementClientBuilder.standard()
                                .withRegion(region)
                                .withCredentials(new ProfileCredentialsProvider())
                                .build();
                StringBuilder trustPolicy = new StringBuilder();
                trustPolicy.append("{\\r\\n   ");
                trustPolicy.append("\\\"Version\\\":\\\"2012-10-17\\\",\\r\\n   ");
                trustPolicy.append("\\\"Statement\\\":[\\r\\n      {\\r\\n
 ");
                trustPolicy.append("\\\"Effect\\\":\\\"Allow\\\",\\r\\n         \\
\"Principal\\\":{\\r\\n            ");
                trustPolicy.append("\\\"Service\\\":\\\"s3.amazonaws.com\\\"\\r\\n
      },\\r\\n         ");
                trustPolicy.append("\\\"Action\\\":\\\"sts:AssumeRole\\\"\\r\\n
  }\\r\\n   ]\\r\\n}");

                CreateRoleRequest createRoleRequest = new CreateRoleRequest()
```

```
                                .withRoleName(roleName)

 .withAssumeRolePolicyDocument(trustPolicy.toString());

                iamClient.createRole(createRoleRequest);

                StringBuilder permissionPolicy = new StringBuilder();
                permissionPolicy.append(
                                "{\\r\\n   \\\"Version\\\":\\\"2012-10-17\\\",\\r\\n
   \\\"Statement\\\":[\\r\\n      {\\r\\n         ");
                permissionPolicy.append(
                                "\\\"Effect\\\":\\\"Allow\\\",\\r\\n         \\
\"Action\\\":[\\r\\n             ");
                permissionPolicy.append("\\\"s3:GetObjectVersionForReplication\\\",\
\r\\n            ");
                permissionPolicy.append(
                                "\\\"s3:GetObjectVersionAcl\\\"\\r\\n         ],\\r\
\n         \\\"Resource\\\":[\\r\\n            ");
                permissionPolicy.append("\\\"arn:aws:s3:::");
                permissionPolicy.append(sourceBucket);
                permissionPolicy.append("/*\\\"\\r\\n         ]\\r\\n      },\\r\\n
     {\\r\\n         ");
                permissionPolicy.append(
                                "\\\"Effect\\\":\\\"Allow\\\",\\r\\n         \\
\"Action\\\":[\\r\\n            ");
                permissionPolicy.append(
                                "\\\"s3:ListBucket\\\",\\r\\n            \\
\"s3:GetReplicationConfiguration\\\"\\r\\n         ");
                permissionPolicy.append("],\\r\\n         \\\"Resource\\\":[\\r\\n
          \\\"arn:aws:s3:::");
                permissionPolicy.append(sourceBucket);
                permissionPolicy.append("\\r\\n         ");
                permissionPolicy
                                .append("]\\r\\n      },\\r\\n      {\\r\\n
 \\\"Effect\\\":\\\"Allow\\\",\\r\\n         ");
                permissionPolicy.append(
                                "\\\"Action\\\":[\\r\\n            \\
\"s3:ReplicateObject\\\",\\r\\n            ");
                permissionPolicy
                                .append("\\\"s3:ReplicateDelete\\\",\\r\\n
  \\\"s3:ReplicateTags\\\",\\r\\n            ");
                permissionPolicy.append("\\\"s3:GetObjectVersionTagging\\\"\\r\\n\\r
\\n         ],\\r\\n         ");
                permissionPolicy.append("\\\"Resource\\\":\\\"arn:aws:s3:::");
```

```
                permissionPolicy.append(destinationBucket);
                permissionPolicy.append("/*\\\"\\r\\n      }\\r\\n   ]\\r\\n}");

                PutRolePolicyRequest putRolePolicyRequest = new
 PutRolePolicyRequest()
                                    .withRoleName(roleName)
                                    .withPolicyDocument(permissionPolicy.toString())
                                    .withPolicyName("crrRolePolicy");

                iamClient.putRolePolicy(putRolePolicyRequest);

        }
}
```

C#

以下の AWS SDK for .NET のコード例では、バケットにレプリケーション設定を追加してから、その設定を取得します。このコードを使用するには、バケットの名前と IAM ロールの Amazon リソースネーム (ARN) を入力します。コード例を設定および実行する方法の詳細については、「AWS SDK for .NET デベロッパーガイド」の「AWS SDK for .NET の開始方法」を参照してください。

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class CrossRegionReplicationTest
    {
        private const string sourceBucket = "*** source bucket ***";
        // Bucket ARN example - arn:aws:s3:::destinationbucket
        private const string destinationBucketArn = "*** destination bucket ARN
 ***";
        private const string roleArn = "*** IAM Role ARN ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint sourceBucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;
        public static void Main()
```

```
        {
            s3Client = new AmazonS3Client(sourceBucketRegion);
            EnableReplicationAsync().Wait();
        }
        static async Task EnableReplicationAsync()
        {
            try
            {
                ReplicationConfiguration replConfig = new ReplicationConfiguration
                {
                    Role = roleArn,
                    Rules =
                        {
                            new ReplicationRule
                            {
                                Prefix = "Tax",
                                Status = ReplicationRuleStatus.Enabled,
                                Destination = new ReplicationDestination
                                {
                                    BucketArn = destinationBucketArn
                                }
                            }
                        }
                };

                PutBucketReplicationRequest putRequest = new
PutBucketReplicationRequest
                {
                    BucketName = sourceBucket,
                    Configuration = replConfig
                };

                PutBucketReplicationResponse putResponse = await
s3Client.PutBucketReplicationAsync(putRequest);

                // Verify configuration by retrieving it.
                await RetrieveReplicationConfigurationAsync(s3Client);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
writing an object", e.Message);
            }
            catch (Exception e)
```

```
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
writing an object", e.Message);
            }
        }
        private static async Task RetrieveReplicationConfigurationAsync(IAmazonS3
client)
        {
            // Retrieve the configuration.
            GetBucketReplicationRequest getRequest = new GetBucketReplicationRequest
            {
                BucketName = sourceBucket
            };
            GetBucketReplicationResponse getResponse = await
client.GetBucketReplicationAsync(getRequest);
            // Print.
            Console.WriteLine("Printing replication configuration information...");
            Console.WriteLine("Role ARN: {0}", getResponse.Configuration.Role);
            foreach (var rule in getResponse.Configuration.Rules)
            {
                Console.WriteLine("ID: {0}", rule.Id);
                Console.WriteLine("Prefix: {0}", rule.Prefix);
                Console.WriteLine("Status: {0}", rule.Status);
            }
        }
    }
}
```

異なるアカウントでのバケットのレプリケーション設定

ライブレプリケーションは、同一または異なる AWS リージョン にあるバケット間でオブジェクトを自動的に非同期でコピーする機能です。ライブレプリケーションでは、新しく作成されたオブジェクトおよびオブジェクトの更新が、レプリケート元バケットからレプリケート先バケットにコピーされます。詳細については、「リージョン内およびリージョン間でのオブジェクトのレプリケート」を参照してください。

レプリケーションを設定するときは、レプリケート元バケットにレプリケーションルールを追加します。レプリケーションルールにより、レプリケート元のソースバケットオブジェクトと、レプリケートされたオブジェクトが保存されるレプリケート先バケットが定義されます。ルールを作成して、バケット内のすべてのオブジェクト、または特定のキー名のプレフィックス、1 つ以上のオブジェクトタグ、あるいはその両方を持つオブジェクトのサブセットをレプリケートできます。レプリケート先

のバケットはレプリケート元バケットと同じ AWS アカウントにあっても、別のアカウントにあってもかまいません。

削除するオブジェクトバージョンの ID を指定した場合、Amazon S3 はソースバケット内のそのオブジェクトバージョンを削除します。しかし、レプリケート先バケット内でその削除をレプリケートすることはありません。つまり、レプリケート先バケットから同じオブジェクトバージョンを削除しません。これは悪意のある削除からデータを保護します。

バケットにレプリケーションルールを追加すると、ルールはデフォルトで有効になるため、保存するとすぐに動作を開始します。

レプリケート元バケットとレプリケート先バケットが異なる AWS アカウントによって所有されている場合のライブレプリケーションの設定は、両方のバケットが同じアカウントによって所有されている場合のレプリケーションの設定と似ています。ただし、クロスアカウントのシナリオでレプリケーションを設定する場合、いくつかの違いがあります。

- レプリケート先バケット所有者は、レプリケート元バケット所有者に、レプリケート先バケットポリシーでオブジェクトをレプリケートするためのアクセス許可を付与する必要があります。
- クロスアカウントのシナリオで AWS Key Management Service (AWS KMS) キー (SSE-KMS) を使用してサーバー側の暗号化で暗号化されたオブジェクトをレプリケートする場合、KMS キーの所有者は、KMS キーを使用するアクセス許可をレプリケート元バケット所有者に付与する必要があります。詳細については、「クロスアカウントシナリオに対する追加のアクセス許可の付与」を参照してください。
- デフォルトでは、レプリケートされたオブジェクトはレプリケート元バケット所有者によって所有されます。クロスアカウントのシナリオでは、レプリケーションを設定してレプリケーションされたオブジェクトの所有権をレプリケート先バケットの所有者に変更できます。詳細については、「レプリカ所有者の変更」を参照してください。

レプリケート元バケットとレプリケート先バケットが異なる AWS アカウントによって所有されている場合にレプリケーションを設定するには

1. この例では、レプリケーション元バケットとレプリケーション先バケットを 2 つの異なる AWS アカウントで作成します。AWS CLI には 2 つの認証情報プロファイルが設定されている必要があります。この例では、これらのプロファイル名に `acctA` と `acctB` を使用します。名前付きプロファイルの設定と使用に関する詳細については、「AWS Command Line Interface ユーザーガイド」の「設定ファイルと認証情報ファイルの設定」を参照してください。
2. 「同じアカウントでのバケットのレプリケーションの設定」の手順に従って、以下の変更を加えます。

- レプリケート元バケットアクティビティ (レプリケート元バケットの作成、バージョニングの有効化、および IAM ロールの作成など) に関連するすべての AWS CLI コマンドには、acctA プロファイルを使用します。acctB プロファイルを使用してレプリケート先バケットを作成します。
- この例で作成したレプリケート元バケット、およびレプリケート先バケットが IAM ロールのアクセス許可ポリシーで指定されていることを確認してください。

3. コンソールで*#######*バケットに次のバケットポリシーを追加して、*#######*バケットの所有者がオブジェクトをレプリケートできるようにします。手順については、「Amazon S3 コンソールを使用したバケットポリシーの追加」を参照してください。必ず、レプリケート元バケット所有者の AWS アカウント ID、IAM ロール名、およびレプリケート先バケット名を指定してポリシーを編集してください。

> **Note**
>
> 次の例を使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。*amzn-s3-demo-destination-bucket* を、レプリケート先のバケットの名前に置き換えます。IAM Amazon リソースネーム (ARN) の *source-bucket-account-ID*:role/service-role/*source-account-IAM-role* を、このレプリケーション設定に使用する IAM ロールに置き換えます。
> IAM サービスロールを手動で作成した場合は、次のポリシー例に示すように、IAM ARN のロールパスを role/service-role/ として設定します。詳細については、「IAM ユーザーガイド」の「IAM ARN」を参照してください。

```
{
   "Version":"2012-10-17",
   "Id":"",
   "Statement":[
      {
         "Sid":"Set-permissions-for-objects",
         "Effect":"Allow",
         "Principal":{
            "AWS":"arn:aws:iam::source-bucket-account-ID:role/service-role/source-account-IAM-role"
         },
         "Action":["s3:ReplicateObject", "s3:ReplicateDelete"],
         "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
      },
```

```
      {
         "Sid":"Set permissions on bucket",
         "Effect":"Allow",
         "Principal":{
            "AWS":"arn:aws:iam::source-bucket-account-ID:role/service-role/source-account-IAM-role"
         },
         "Action":["s3:GetBucketVersioning", "s3:PutBucketVersioning"],
         "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket"
      }
   ]
}
```

4. (オプション) SSE-KMS で暗号化されたオブジェクトをレプリケートする場合、KMS キーの所有者は、KMS キーを使用するアクセス許可をレプリケート元バケット所有者に付与する必要があります。詳細については、「クロスアカウントシナリオに対する追加のアクセス許可の付与」を参照してください。
5. (オプション) レプリケーションでは、デフォルトで、レプリケート元オブジェクトの所有者もレプリカを所有しています。レプリケート元とレプリケート先のバケットが、異なる AWS アカウントによって所有されている場合、レプリケート先バケットを所有する AWS アカウントにレプリカの所有権を変更するためのオプション設定を追加できます。これには、`ObjectOwnerOverrideToBucketOwner` 許可の付与が含まれます。詳細については、「レプリカ所有者の変更」を参照してください。

レプリカ所有者の変更

レプリケーションでは、デフォルトで、レプリケート元オブジェクトの所有者もレプリカを所有しています。しかし、レプリケート元とレプリケート先のバケットが、異なる AWS アカウントによって所有されている場合、レプリカの所有権を変更することができます。例えば、所有権を変更して、オブジェクトレプリカへのアクセスを制限できます。レプリケーション設定では、レプリカの所有権をレプリカ先バケットを所有する AWS アカウントに変更するためのオプションの設定を追加できます。

レプリカ所有者を変更するには、以下を実行します。

- レプリカの所有権を変更するよう Amazon S3 に指示するには、レプリケーション設定に所有者オーバーライドオプションを追加します。
- レプリカの所有権を変更する `s3:ObjectOwnerOverrideToBucketOwner` アクセス許可を Amazon S3 に付与します。

- レプリケート先バケットポリシーに `s3:ObjectOwnerOverrideToBucketOwner` アクセス許可を追加して、レプリカの所有権を変更できるようにします。`s3:ObjectOwnerOverrideToBucketOwner` アクセス許可により、レプリケート先バケットの所有者がオブジェクトレプリカの所有権を受け入れることができるようになります。

詳細については、「the section called “所有権オーバーライドオプションに関する考慮事項”」および「レプリケーション設定への所有者オーバーライドオプションの追加」を参照してください。ステップバイステップの手順を含む実例については、「レプリカの所有者を変更する方法」を参照してください。

> **Important**
>
> 所有者オーバーライドオプションを使用する代わりに、オブジェクト所有権にバケット所有者の強制設定を使用できます。S3 レプリケーションを使用し、レプリケート元バケットとレプリケート先バケットが異なる AWS アカウントによって所有される場合、バケットを使用する場合、レプリケート先バケットのバケット所有者は [オブジェクト所有権] に対するバケット所有者の強制設定を使用して、レプリカの所有権を送信先バケットを所有する AWS アカウントに変更することができます。この設定は、オブジェクトアクセスコントロールリスト (ACL) を無効にします。
>
> このバケット所有者の強制設定は、`s3:ObjectOwnerOverrideToBucketOwner` 許可の必要なく、既存の所有者のオーバーライド動作を模倣します。バケット所有者強制設定で宛先バケットにレプリケーションされるすべてのオブジェクトは、宛先バケット所有者によって所有されます。オブジェクトの所有権の詳細については、「オブジェクトの所有権の制御とバケットの ACL の無効化。」を参照してください。

所有権オーバーライドオプションに関する考慮事項

所有権オーバーライドオプションを設定するときは、次の考慮事項が適用されます。

- デフォルトでは、レプリケート元オブジェクトの所有者がレプリカの所有者となります。Amazon S3 は、オブジェクトバージョンとそれに関連付けられた ACL をレプリケートします。

  レプリケーション設定に所有者オーバーライドオプションを追加すると、Amazon S3 はオブジェクトのバージョンのみをレプリケートし、ACL はレプリケートしません。さらに、Amazon S3 は、以降の変更をレプリケート元オブジェクト ACL にレプリケートしません。Amazon S3 は、完全な制御をレプリケート先バケット所有者に許可する ACL をレプリカに設定します。

- 所有者オーバーライドを有効、または無効にするようにレプリケーション設定を更新すると、以下の挙動が生じます。
  - レプリケーション設定へ所有者オーバーライドオプションを追加する場合。

    Amazon S3 がオブジェクトバージョンをレプリケートすると、レプリケート元オブジェクトに関連付けられている ACL は破棄されます。代わりに、Amazon S3 は完全なコントロールをレプリケート先バケットの所有者に与えるレプリカに設定されます。Amazon S3 は、以降の変更をレプリケート元オブジェクト ACL にレプリケートしません。ただし、この ACL 変更は、所有者オーバーライドオプションを設定する前にレプリケートされたオブジェクトバージョンには適用されません。所有者オーバーライドが設定される前にレプリケートされたレプリケート元オブジェクトの ACL 更新は、レプリケートされ続けます (オブジェクトとそのレプリカの所有者が引き続き同じであるため)。
  - レプリケーション設定から所有者オーバーライドオプションを削除する場合。

    Amazon S3 は、レプリケート元バケットと関連 ACL に表示される新しいオブジェクトを、レプリケート先バケットにレプリケートします。所有者オーバーライドを削除する前にレプリケートされたオブジェクトの場合、Amazon S3 によるオブジェクト所有権の変更が有効なため、Amazon S3 は ACL をレプリケートしません。つまり、所有者オーバーライド設定時にレプリケートされたオブジェクトバージョンに設定された ACL は、引き続きレプリケートされません。

レプリケーション設定への所有者オーバーライドオプションの追加

> **Warning**
>
> 所有者オーバーライドオプションを追加するのは、レプリケーション元バケットとレプリケーション先バケットが異なる AWS アカウントによって所有されている場合のみです。Amazon S3 はバケットが同じアカウントによって所有されているか、異なるアカウントによって所有されているかをチェックしません。両方のバケットが同じ AWS アカウントによって所有されている場合に所有者オーバーライドを追加すると、Amazon S3 は所有者オーバーライドを適用します。このオプションは、レプリケート先バケットの所有者にフルアクセス権を付与し、その後の更新はソースオブジェクトのアクセスコントロールリスト (ACL) にレプリケートされません。レプリカの所有者は、`PutObjectAcl` リクエストを持つレプリカに関連付けられた ACL を直接変更できますが、レプリケーションを通して変更することはできません。

所有者の上書きオプションを指定するには、各Destination要素に次を追加します。

- Amazon S3 にレプリカの所有権を変更するよう指示する AccessControlTranslation 要素
- レプリケート先バケット所有者の AWS アカウントを指定する Account 要素

```
<ReplicationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
    ...
    <Destination>
      ...
      <AccessControlTranslation>
           <Owner>Destination</Owner>
       </AccessControlTranslation>
      <Account>destination-bucket-owner-account-id</Account>
    </Destination>
  </Rule>
</ReplicationConfiguration>
```

次のレプリケーション設定例では、*Tax* キープレフィックスを持つオブジェクトを *amzn-s3-demo-destination-bucket* レプリケート先バケットにレプリケートし、レプリカの所有権を変更するようAmazon S3 に指示します。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
<?xml version="1.0" encoding="UTF-8"?>
<ReplicationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
   <Role>arn:aws:iam::account-id:role/role-name</Role>
   <Rule>
      <ID>Rule-1</ID>
      <Priority>1</Priority>
      <Status>Enabled</Status>
      <DeleteMarkerReplication>
         <Status>Disabled</Status>
      </DeleteMarkerReplication>
      <Filter>
         <Prefix>Tax</Prefix>
      </Filter>
      <Destination>
         <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
         <Account>destination-bucket-owner-account-id</Account>
         <AccessControlTranslation>
            <Owner>Destination</Owner>
         </AccessControlTranslation>
```

```
      </Destination>
   </Rule>
</ReplicationConfiguration>
```

レプリカの所有権を変更するための Amazon S3 アクセス許可の付与

AWS Identity and Access Management IAM ロールに関連付けられているアクセス許可ポリシーに s3:ObjectOwnerOverrideToBucketOwner アクションのアクセス許可を追加することで、Amazon S3 にレプリカの所有権を変更するアクセス許可を付与します。このロールは、Amazon S3 がユーザーに代わってオブジェクトを引き受けてレプリケートすることを可能にする、レプリケーション設定で指定した IAM ロールです。次の例を使用するには、*amzn-s3-demo-destination-bucket* をレプリケート先バケットの名前に置き換えます。

```
...
{
    "Effect":"Allow",
         "Action":[
       "s3:ObjectOwnerOverrideToBucketOwner"
    ],
    "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
}
...
```

レプリケート先バケットポリシーへのレプリカの所有権を変更するアクセス許可の追加

レプリケート先バケットの所有者は、レプリケート元バケットの所有者に、レプリカの所有権を変更するためのアクセス権限を付与する必要があります。レプリケート先バケットの所有者は、レプリケート元バケットの所有者に、s3:ObjectOwnerOverrideToBucketOwner アクションのためのアクセス権限を付与します。このアクセス許可により、レプリケート先バケット所有者はオブジェクトレプリカの所有権を受け入れることができるようになります。次のバケットポリシーステートメントの例は、この操作を行う方法を示しています。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
...
{
    "Sid":"1",
    "Effect":"Allow",
    "Principal":{"AWS":"source-bucket-account-id"},
    "Action":["s3:ObjectOwnerOverrideToBucketOwner"],
    "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
}
```

```
...
```

レプリカの所有者を変更する方法

レプリケーション設定内のレプリケーション元のバケットとレプリケーション先のバケットが異なる AWS アカウントによって所有されている場合、Amazon S3 に対し、レプリカの所有権をレプリケーション先のバケットを所有している AWS アカウントに変更するよう指示できます。次の例は、Amazon S3 コンソール、AWS Command Line Interface (AWS CLI)、および AWS SDK を使用してレプリカの所有権を変更する方法を示しています。

S3 コンソールの使用

手順については、「同じアカウントでのバケットのレプリケーションの設定」を参照してください。このトピックでは、レプリケート元およびレプリケート先バケットが同一の、または異なる AWS アカウントによって所有されている場合にレプリケーション設定を行う手順について説明します。

AWS CLI を使用する場合

次の手順は、AWS CLI を使用してレプリカの所有権を変更する方法を示しています。この手順では、次の操作を行います。

- レプリケート元バケットとレプリケート先バケットを作成します。
- バケットでのバージョニングを有効化します。
- オブジェクトをレプリケートするための Amazon S3 許可を付与する AWS Identity and Access Management (IAM) ロールを作成します。
- レプリケート元バケットにレプリケーション設定を追加します。
- レプリケーション設定で、Amazon S3 にレプリカ所有権の変更を指示します。
- レプリケーション設定をテストします。

レプリケート元とレプリケート先のバケットが、異なる AWS アカウントによって所有されている場合にレプリカの所有権を変更するには (AWS CLI)

この手順の AWS CLI コマンドの例を使用するには、*user input placeholders* を自分の情報に置き換えてください。

1. この例では、レプリケート元およびレプリケート先バケットを 2 つの異なる AWS アカウントで作成します。これらの 2 つのアカウントを使用するには、2 つの名前付きプロファイルで AWS CLI を設定します。この例では、それぞれ *acctA* と *acctB* という名前のプロファイルを使用します。名前付きプロファイルの設定と使用に関する詳細については、「AWS Command Line

Interface ユーザーガイド」の「設定ファイルと認証情報ファイルの設定」を参照してください。

> **Important**
>
> この手順に使用するプロファイルは、必要なアクセス権限を持っている必要があります。たとえば、レプリケーション設定で、Amazon S3 が引き受けることができる IAM ロールを指定します。使用するプロファイルに `iam:PassRole` アクセス権限がある場合のみ実行できます。管理者ユーザーの認証情報を使用して名前付きプロファイルを作成すると、この手順のすべてのタスクを実行できるようになります。詳細については、IAM ユーザーガイドの「AWS のサービス のサービスにロールを渡すアクセス権限をユーザーに付与する」を参照してください。

2. *#######*バケットを作成してバージョニングを有効にします。この例では、米国東部 (バージニア北部) (us-east-1) リージョンに *amzn-s3-demo-source-bucket* というレプリケート元バケットを作成します。

```
aws s3api create-bucket \
--bucket amzn-s3-demo-source-bucket \
--region us-east-1 \
--profile acctA
```

```
aws s3api put-bucket-versioning \
--bucket amzn-s3-demo-source-bucket \
--versioning-configuration Status=Enabled \
--profile acctA
```

3. *#######*バケットを作成してバージョニングを有効にします。この例では、米国西部 (オレゴン) (us-west-2) リージョンに *amzn-s3-demo-destination-bucket* というレプリケート先バケットを作成します。レプリケート元バケットに使用したものとは異なる AWS アカウントプロファイルを使用してください。

```
aws s3api create-bucket \
--bucket amzn-s3-demo-destination-bucket \
--region us-west-2 \
--create-bucket-configuration LocationConstraint=us-west-2 \
--profile acctB
```

```
aws s3api put-bucket-versioning \
```

```
--bucket amzn-s3-demo-destination-bucket \
--versioning-configuration Status=Enabled \
--profile acctB
```

4. *#######*バケットポリシーにアクセス許可を追加して、レプリカの所有権を変更できるようにします。

   a. 次のポリシーを *destination-bucket-policy*.json という名前のファイルに保存します。*user input placeholders* をユーザー自身の情報に必ず置き換えます。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "destination_bucket_policy_sid",
      "Principal": {
        "AWS": "source-bucket-owner-account-id"
      },
      "Action": [
        "s3:ReplicateObject",
        "s3:ReplicateDelete",
        "s3:ObjectOwnerOverrideToBucketOwner",
        "s3:ReplicateTags",
        "s3:GetObjectVersionTagging"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
      ]
    }
  ]
}
```

   b. 次の put-bucket-policy コマンドを使用して、前述のポリシーを送信先バケットに追加します。

```
aws s3api put-bucket-policy --region $ {destination-region} --bucket $ {amzn-
s3-demo-destination-bucket} --policy file://destination_bucket_policy.json
```

5. IAM ロールを作成します。*#######*バケットに後で追加するレプリケーション設定でこのロールを指定します。Amazon S3 は、ユーザーに代わってオブジェクトをレプリケートするこのロールを引き受けます。IAM ロールは 2 つのステップで作成します。

   - ロールを作成します。
   - アクセス権限ポリシーをロールにアタッチします。

   a. IAM ロールを作成します。

      i. 次の信頼ポリシーをコピーして、ローカルコンピュータの現在のディレクトリにある *s3-role-trust-policy*.json という名前のファイルに保存します。このポリシーは、Amazon S3 がロールを引き受けるためのアクセス許可を付与します。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"s3.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

      ii. 次の AWS CLI `create-role` コマンドを実行して、IAM ロールを作成します。

```
$ aws iam create-role \
--role-name replicationRole \
--assume-role-policy-document file://s3-role-trust-policy.json  \
--profile acctA
```

      作成した IAM ロールの Amazon リソースネーム (ARN) を書き留めます。この ARN は、後のステップで必要になります。

   b. アクセス権限ポリシーをロールにアタッチします。

      i. 次のアクセス権限ポリシーをコピーして、ローカルコンピュータの現在のディレクトリにある *s3-role-perm-pol-changeowner*.json という名前のファイルに保存します。このポリシーは、さまざまな Amazon S3 バケットとオブジェクトアクションに対

するアクセス許可を付与します。次の手順では、このポリシーを先ほど作成した IAM ロールにアタッチします。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetObjectVersionForReplication",
            "s3:GetObjectVersionAcl"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:ListBucket",
            "s3:GetReplicationConfiguration"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:ReplicateObject",
            "s3:ReplicateDelete",
            "s3:ObjectOwnerOverrideToBucketOwner",
            "s3:ReplicateTags",
            "s3:GetObjectVersionTagging"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
      }
   ]
}
```

ii. 前述のアクセス許可ポリシーをロールにアタッチするには、次の `put-role-policy` コマンドを実行します。

```
$ aws iam put-role-policy \
--role-name replicationRole \
--policy-document file://s3-role-perm-pol-changeowner.json \
--policy-name replicationRolechangeownerPolicy \
--profile acctA
```

6. レプリケーション設定をレプリケート元バケットに追加します。

   a. AWS CLI では、レプリケーション設定を JSON で指定する必要があります。以下の JSON を、ローカルコンピュータの現在のディレクトリにある、*replication*.json というファイルに保存します。設定では、AccessControlTranslation はレプリカ所有権のレプリケート元バケット所有者からレプリケート先バケット所有者への変更を指定します。

```
{
   "Role":"IAM-role-ARN",
   "Rules":[
      {
         "Status":"Enabled",
         "Priority":1,
         "DeleteMarkerReplication":{
            "Status":"Disabled"
         },
         "Filter":{
         },
         "Status":"Enabled",
         "Destination":{
            "Bucket":"arn:aws:s3:::amzn-s3-demo-destination-bucket",
            "Account":"destination-bucket-owner-account-id",
            "AccessControlTranslation":{
               "Owner":"Destination"
            }
         }
      }
   ]
}
```

   b. レプリケート先バケット名、レプリケート先バケット所有者アカウント ID、および *IAM-role-ARN* の値を指定して JSON を編集します。*IAM-role-ARN* を先ほど作成した IAM ロールの ARN に置き換えます。変更を保存します。

   c. 次のコマンドを実行して、レプリケート元バケットにレプリケーション設定を追加します。

```
$ aws s3api put-bucket-replication \
--replication-configuration file://replication.json \
--bucket amzn-s3-demo-source-bucket \
--profile acctA
```

7. Amazon S3 コンソールでレプリカの所有権を確認して、レプリケーション設定をテストします。

   a. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。

   b. オブジェクトを#######バケットに追加します。レプリケート先バケットにオブジェクトレプリカが含まれていること、およびレプリカの所有権がレプリケート先バケットを所有する AWS アカウントに変更されていることを確認します。

AWS SDK の使用

レプリケーション設定を追加するコード例については、「AWS SDK の使用」を参照してください。レプリケーション設定を適切に変更する必要があります。概念については、「レプリカ所有者の変更」を参照してください。

S3 Replication Time Control (S3 RTC)を使用してコンプライアンス要件を満たす

S3 Replication Time Control (S3 RTC) では、データレプリケーションに関するコンプライアンス要件 (またはビジネス要件) への対応をサポートします。また、Amazon S3 レプリケーション時間を可視化します。S3 RTC は、Amazon S3 にアップロードしたほとんどのオブジェクトを数秒でレプリケートします。99.9% のオブジェクトが 15 分以内にレプリケートされます。

デフォルトでは、S3 RTC にはレプリケーションの進行状況を追跡する 2 つの方法があります。

- S3 レプリケーションメトリクス – S3 レプリケーションメトリクスを使用すると、レプリケーションを保留している S3 API オペレーションの合計数、レプリケーションを保留しているオブジェクトの合計サイズ、およびレプリケート先のリージョンへの最大レプリケーション時間、およびレプリケーションに失敗したオペレーションの合計数をモニタリングできます。次に、個別にレプリケートする各データセットをモニタリングできます。S3 レプリケーションメトリクスは、S3 RTC とは別に有効化することもできます。詳細については、「the section called “S3 レプリケーションメトリクスの使用”」を参照してください。

  S3 Replication Time Control (S3 RTC) が有効なレプリケーションルールは、S3 レプリケーションメトリクスをパブリッシュします。レプリケーションメトリクスは、S3 RTC が有効になってから

15 分以内に使用できます。レプリケーションメトリクスは、Amazon S3 コンソール、Amazon S3 API、AWS SDK、AWS Command Line Interface (AWS CLI)、および Amazon CloudWatch を通じて利用できます。CloudWatch のメトリクスの詳細については、「Amazon CloudWatch によるメトリクスのモニタリング」を参照してください。Amazon S3 コンソールを使用したレプリケーションメトリクスの表示の詳細については、「レプリケーションメトリクスの表示」を参照してください。

S3 レプリケーションメトリクスは、Amazon CloudWatch カスタムメトリクスと同じ料金レートで請求されます。詳細については、「Amazon CloudWatch の料金」を参照してください。

- Amazon S3 イベント通知 – S3 RTC は、オブジェクトレプリケーションが 15 分のしきい値を超えた場合、またはしきい値の後に発生した場合に、バケット所有者に通知する `OperationMissedThreshold` および `OperationReplicatedAfterThreshold` イベントを提供します。S3 RTC を使用すると、まれなケースとして、オブジェクトが 15 分以内にレプリケートされなかったとき、またこれらのオブジェクトが 15 分のしきい値の後にレプリケートされたときに、Amazon S3 イベント通知から通知を受け取ることができます。

  レプリケーションイベントは、S3 RTC が有効になってから 15 分以内に使用できます。Amazon S3 イベント通知は、Amazon SQS、Amazon SNS、または AWS Lambda を通じて利用できます。詳細については、「the section called “レプリケーション失敗イベントの受信”」を参照してください。

S3 RTC のベストプラクティスとガイドライン

S3 Replication Time Control (S3 RTC) を有効にして Amazon S3 にデータをレプリケートする場合は、以下のベストプラクティスガイドラインに従って、ワークロードのレプリケーションパフォーマンスを最適化します。

トピック

- Amazon S3 レプリケーションおよびリクエストレートのパフォーマンスガイドライン
- レプリケーションリクエストレートの見積り
- S3 RTC データ転送レートクォータを超過する場合
- AWS KMS 暗号化オブジェクトのレプリケーションリクエストレート

Amazon S3 レプリケーションおよびリクエストレートのパフォーマンスガイドライン

アプリケーションは、Amazon S3 レプリケーション のストレージをアップロードおよび取得する際に、リクエストパフォーマンスで 1 秒あたり何千ものトランザクションを達成できます。例えば、アプリケーションは S3 バケットでプレフィックスあたり毎秒 3,500 個以上の PUT/COPY/POST/DELETE リクエストまたは 5,500 個以上の GET/HEAD リクエストを処理できます。これには、S3 レプリケーションがユーザーに代わって行うリクエストも含まれます。バケット内のプレフィックスの数に制限はありません。読み取りを並列化することによって読み取りまたは書き込みのパフォーマンスを向上させることができます。例えば、S3 バケットに 10 個のプレフィックスを作成して読み取りを並列化すると、読み取りパフォーマンスを 1 秒あたり 55,000 回の読み取りリクエストにスケールできます。

Amazon S3 は、これらのガイドラインを上回る持続的なリクエストレートや、LIST リクエストで同時実行される持続的なリクエストレートに応じて自動的にスケールします。Amazon S3 が新しいリクエストレートに合わせて最適化を行っている間、最適化が完了するまで一時的に HTTP 503 リクエストレスポンスが送信される場合があります。この動作は、1 秒あたりのリクエスト数が増加したときや、S3 RTC を初めて有効にしたときに発生する場合があります。この間は、レプリケーションのレイテンシーが増加する可能性があります。S3 RTC サービスレベルアグリーメント (SLA) は、1 秒あたりのリクエストに関する Amazon S3 パフォーマンスガイドラインを超えた期間には適用されません。

S3 RTC SLA は、レプリケーションデータ転送速度がデフォルトの 1 Gbps クォータ制限を超えた期間にも適用されません。レプリケーション転送速度が 1 Gbps を超えることが予想される場合は、AWS サポート センターに問い合わせるか、Service Quotas を使用してレプリケーション転送速度クォータの引き上げをリクエストできます。

レプリケーションリクエストレートの見積り

合計リクエストレート (Amazon S3 レプリケーションがユーザーに代わって行うリクエストを含む) は、レプリケート元バケットとレプリケート先バケットの両方で Amazon S3 リクエストレートのガイドライン内に収まる必要があります。レプリケートされたオブジェクトごとに、Amazon S3 レプリケーションがレプリケート元に最大 5 件の GET/HEAD リクエストと 1 件の PUT リクエストを行い、レプリケート先バケットに 1 件の PUT リクエストを行います。

例えば、1 秒あたり 100 個のオブジェクトをレプリケートする場合、Amazon S3 レプリケーションはユーザーに代わって 100 件の PUT リクエストを追加で実行する可能性があります。つまり、レプリケート元 S3 バケットに対して 1 秒あたり合計 200 個の PUT リクエストが実行されることになります。Amazon S3 レプリケーションでは、最大 500 件の GET/HEAD (レプリケートされたオブジェクトごとに 5 件の GET/HEAD リクエスト) を実行する可能性があります。

> **Note**
>
> レプリケートされたオブジェクトごとに 1 つの PUT リクエストに対してのみコストが発生します。詳細については、「Amazon S3 のレプリケーションに関するよくある質問」で料金情報を参照してください。

S3 RTC データ転送レートクォータを超過する場合

S3 RTC のデータ転送速度がデフォルトの 1 Gbps のクォータを超えると予想される場合は、AWS サポート センターに問い合わせるか、Service Quotas を使用して、レプリケーション転送速度クォータの引き上げをリクエストしてください。

AWS KMS 暗号化オブジェクトのレプリケーションリクエストレート

AWS Key Management Service (AWS KMS) キーを使用したサーバー側の暗号化 (SSE-KMS) で暗号化されたオブジェクトをレプリケートする場合、AWS KMS リクエスト/秒のクォータが適用されます。AWS KMS は、リクエストレートが 1 秒あたりのリクエスト数のクォータを超えているために (そうでなければ) 有効なリクエストを拒否することがあります。リクエストがスロットリングされると、AWS KMS は `ThrottlingException` エラーを返します。AWS KMS リクエストレートのクォータは、ユーザーが直接行うリクエストと、ユーザーに代わって Amazon S3 レプリケーションが行うリクエストに適用されます。

例えば、1 秒あたり 1,000 個のオブジェクトをレプリケートする場合、AWS KMS リクエストレートのクォータから 2,000 個のリクエストを差し引くことができます。差し引いた後の 1 秒あたりのリクエストレートを、レプリケーションを除く AWS KMS ワークロードで使用できます。AWS KMSAmazon CloudWatch でリクエストメトリクスを使用して、AWS アカウント の合計 AWS KMS リクエストレートをモニタリングできます。

1 秒あたりの AWS KMS リクエストのクォータ数の増加をリクエストするには、AWS サポート センターに問い合わせるか、Service Quotas を使用します。

S3 レプリケーション時間コントロールの有効化

新しいレプリケーションルールまたは既存のレプリケーションルールで S3 Replication Time Control (S3 RTC) の使用を開始できます。レプリケーションルールを バケット全体に適用するか、特定のプレフィックスやタグを持つオブジェクトに適用するかを選択できます。S3 RTC を有効にすると、レプリケーションルールで S3 レプリケーションメトリクスも有効になります。

S3 RTC は、Amazon S3 コンソール、Amazon S3 API、AWS SDK、AWS Command Line Interface (AWS CLI) を使用して設定することができます。

S3 コンソールの使用

手順については、「同じアカウントでのバケットのレプリケーションの設定」を参照してください。このトピックでは、レプリケート元バケットとレプリケーション先バケットが同じまたは異なる AWS アカウントで所有されている場合に、レプリケーション設定で S3 レプリケーション RTC を有効にする手順について説明します。

AWS CLI を使用する場合

AWS CLI を使用して S3 RTC が有効になったオブジェクトをレプリケートするには、バケットを作成し、バケットのバージョニングを有効にします。さらに、IAM ロールを作成して Amazon S3 にオブジェクトをレプリケートする許可を与え、レプリケート元バケットにレプリケーション設定を追加します。次の例に示すように、レプリケーション設定では S3 RTC が有効になっている必要があります。

AWS CLI を使用してレプリケーション設定を設定する手順については、「同じアカウントでのバケットのレプリケーションの設定」を参照してください。

次のレプリケーション設定例では、レプリケーションルールの `ReplicationTime` と `EventThreshold` の値を有効にして設定します。これらの値を有効にして設定すると、ルールで S3 RTC が有効になります。

```
{
    "Rules": [
        {
            "Status": "Enabled",
            "Filter": {
                "Prefix": "Tax"
            },
            "DeleteMarkerReplication": {
                "Status": "Disabled"
            },
            "Destination": {
                "Bucket": "arn:aws:s3:::amzn-s3-demo-destination-bucket",
                "Metrics": {
                    "Status": "Enabled",
                    "EventThreshold": {
                        "Minutes": 15
                    }
```

```
                },
                "ReplicationTime": {
                    "Status": "Enabled",
                    "Time": {
                        "Minutes": 15
                    }
                }
            },
            "Priority": 1
        }
    ],
    "Role": "IAM-Role-ARN"
}
```

> **Important**
>
> Metrics:EventThreshold:Minutes と ReplicationTime:Time:Minutes に設定できる唯一の有効な値は 15 です。

AWS SDK for Java の使用

有効にした S3 Replication Time Control (S3 RTC) でレプリケーション設定を追加する Java の例は、次のとおりです。

```
import software.amazon.awssdk.auth.credentials.AwsBasicCredentials;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3.model.DeleteMarkerReplication;
import software.amazon.awssdk.services.s3.model.Destination;
import software.amazon.awssdk.services.s3.model.Metrics;
import software.amazon.awssdk.services.s3.model.MetricsStatus;
import software.amazon.awssdk.services.s3.model.PutBucketReplicationRequest;
import software.amazon.awssdk.services.s3.model.ReplicationConfiguration;
import software.amazon.awssdk.services.s3.model.ReplicationRule;
import software.amazon.awssdk.services.s3.model.ReplicationRuleFilter;
import software.amazon.awssdk.services.s3.model.ReplicationTime;
import software.amazon.awssdk.services.s3.model.ReplicationTimeStatus;
import software.amazon.awssdk.services.s3.model.ReplicationTimeValue;

public class Main {

  public static void main(String[] args) {
```

```
    S3Client s3 = S3Client.builder()
      .region(Region.US_EAST_1)
      .credentialsProvider(() -> AwsBasicCredentials.create(
          "AWS_ACCESS_KEY_ID",
          "AWS_SECRET_ACCESS_KEY")
      )
      .build();

    ReplicationConfiguration replicationConfig = ReplicationConfiguration
      .builder()
      .rules(
          ReplicationRule
            .builder()
            .status("Enabled")
            .priority(1)
            .deleteMarkerReplication(
                DeleteMarkerReplication
                    .builder()
                    .status("Disabled")
                    .build()
            )
            .destination(
                Destination
                    .builder()
                    .bucket("destination_bucket_arn")
                    .replicationTime(
                        ReplicationTime.builder().time(
                            ReplicationTimeValue.builder().minutes(15).build()
                        ).status(
                            ReplicationTimeStatus.ENABLED
                        ).build()
                    )
                    .metrics(
                        Metrics.builder().eventThreshold(
                            ReplicationTimeValue.builder().minutes(15).build()
                        ).status(
                            MetricsStatus.ENABLED
                        ).build()
                    )
                    .build()
            )
            .filter(
                ReplicationRuleFilter
                    .builder()
```

```
                    .prefix("testtest")
                    .build()
            )
        .build())
        .role("role_arn")
        .build();

    // Put replication configuration
    PutBucketReplicationRequest putBucketReplicationRequest =
 PutBucketReplicationRequest
      .builder()
      .bucket("source_bucket")
      .replicationConfiguration(replicationConfig)
      .build();

    s3.putBucketReplication(putBucketReplicationRequest);
  }
}
```

暗号化されたオブジェクトのレプリケート (SSE-S3、SSE-KMS、DSSE-KMS、SSE-C)

> **Important**
>
> Amazon S3 では、Amazon S3 内のすべてのバケットの基本レベルの暗号化として、Amazon S3 が管理するキー (SSE-S3) によるサーバー側の暗号化が適用されるようになりました。2023 年 1 月 5 日以降、Amazon S3 にアップロードされるすべての新しいオブジェクトは、追加費用なしで、パフォーマンスに影響を与えずに自動的に暗号化されます。S3 バケットのデフォルト暗号化設定と新しいオブジェクトのアップロードのための自動暗号化ステータスは、AWS CloudTrail ログ、S3 インベントリ、S3 ストレージレンズ、Amazon S3 コンソール、および AWS Command Line Interface と AWS SDK の追加の Amazon S3 API レスポンスヘッダーとして利用できるようになりました。詳細については、「デフォルト暗号化に関するよくある質問」を参照してください。

サーバー側の暗号化を使用して暗号化されているオブジェクトをレプリケートする場合は、いくつかの特別な考慮事項があります。Amazon S3 は、以下の 3 種類のサーバー側の暗号化をサポートしています。

- Amazon S3 マネージドキーを用いたサーバー側の暗号化 (SSE-S3)

- AWS Key Management Service (AWS KMS) キー (SSE-KMS) によるサーバー側の暗号化
- AWS KMS キーによる二層式サーバー側の暗号化 (DSSE-KMS)
- 顧客提供のキーを用いたサーバー側の暗号化 (SSE-C)。

サーバーサイドの暗号化の詳細については、「the section called “サーバー側の暗号化”」を参照してください。

このトピックでは、サーバー側の暗号化を使用して暗号化されているオブジェクトをレプリケートするよう Amazon S3 に指示するために必要なアクセス許可について説明します。このトピックでは、追加できるその他の設定要素や、暗号化されたオブジェクトのレプリケーションに必要なアクセス許可を付与する AWS Identity and Access Management (IAM) ポリシーの例も提供します。

ステップバイステップの手順と例については、「暗号化されたオブジェクトのレプリケーションの有効化」を参照してください。レプリケーション設定の作成については、「リージョン内およびリージョン間でのオブジェクトのレプリケート」を参照してください。

> **Note**
>
> Amazon S3 では、マルチリージョン AWS KMS keys を使用できます。ただし、Amazon S3 では現在、マルチリージョンキーは、単一リージョンキーであるかのように処理され、キーのマルチリージョン特徴は使用しません。詳細については、AWS Key Management Service デベロッパーガイドの「マルチリージョンキーを使用する」を参照してください。

トピック

- バケットのデフォルトの暗号化がレプリケーションに与える影響
- SSE-C で暗号化されたオブジェクトのレプリケーション
- SSE-S3、SSE-KMS、または DSSE-KMS で暗号化されたオブジェクトのレプリケーション
- 暗号化されたオブジェクトのレプリケーションの有効化

バケットのデフォルトの暗号化がレプリケーションに与える影響

レプリケーション先バケットのデフォルトの暗号化を有効にすると、以下の暗号化動作が適用されます。

- レプリケート元バケットのオブジェクトが暗号化されていない場合、レプリケート先バケットのレプリカオブジェクトはレプリケート先バケットのデフォルトの暗号化設定を使用して暗号化されま

す。そのため、レプリケート元のオブジェクトのエンティティタグ (ETag) はレプリカオブジェクトの ETag とは異なります。アプリケーションで ETag を使用している場合は、アプリケーションを更新して、この違いを反映する必要があります。

- レプリケート元バケット内のオブジェクトが Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3)、AWS Key Management Service (AWS KMS) キーによるサーバー側の暗号化 (SSE-KMS)、または AWS KMS キーによる二層式サーバー側の暗号化 (DSSE-KMS) を使用して暗号化されている場合、レプリケート先バケットのレプリカオブジェクトは、レプリケート元オブジェクトと同じタイプの暗号化を使用します。レプリケート先バケットのデフォルトの暗号化設定は使用されません。

SSE-C で暗号化されたオブジェクトのレプリケーション

お客様が指定したキーによるサーバー側の暗号化 (SSE-C) を使用することで、独自の暗号化キーを管理できます。SSE-C ではユーザーがキーを管理し、Amazon S3 は暗号化と復号のプロセスを管理します。ユーザーはリクエストの一部として暗号化キーを指定する必要がありますが、オブジェクトの暗号化または復号を実行するコードを記述する必要はありません。オブジェクトをアップロードすると、Amazon S3 は指定されたキーを使用してオブジェクトを暗号化します。その後、Amazon S3 はそのキーをメモリから削除します。オブジェクトを取得するときは、リクエストの中で同じ暗号化キーを指定する必要があります。詳細については、「the section called “お客様が指定したキーによるサーバー側の暗号化 (SSE-C)”」を参照してください。

S3 レプリケーションは SSE-C で暗号化されたオブジェクトをサポートしています。SSE-C オブジェクトのレプリケーションは、暗号化されていないオブジェクトのレプリケーションを設定するのと同じ方法で、Amazon S3 コンソールまたは AWS SDK で設定できます。レプリケーションに現在必要な権限以外に SSE-C 権限を追加することはできません。

S3 レプリケーションは、新しくアップロードされた SSE-C 暗号化オブジェクトを、S3 レプリケーション設定に従って自動的にレプリケートします (該当する場合)。バケット内の既存のオブジェクトをレプリケートするには、S3 バッチレプリケーションを使用します。オブジェクトのレプリケーションの詳細については、「the section called “ライブレプリケーションの設定”」および「the section called “既存のオブジェクトのレプリケーション”」を参照してください。

SSE-C オブジェクトのレプリケートに追加料金はかかりません。レプリケーション料金の詳細については、「Amazon S3 の料金」を参照してください。

SSE-S3、SSE-KMS、または DSSE-KMS で暗号化されたオブジェクトのレプリケーション

デフォルトでは、Amazon S3 は SSE-KMS または DSSE-KMS で暗号化されたオブジェクトをレプリケートしません。このセクションでは、これらのオブジェクトをレプリケートするよう Amazon S3 に指示するために追加できるその他の設定要素について説明します。

ステップバイステップの手順と例については、「暗号化されたオブジェクトのレプリケーションの有効化」を参照してください。レプリケーション設定の作成については、「リージョン内およびリージョン間でのオブジェクトのレプリケート」を参照してください。

レプリケーション設定の追加情報の指定

レプリケーション設定で、以下を実行してください。

- 次のレプリケーション設定例に示すように、レプリケーション設定の `Destination` 要素に、オブジェクトレプリカを暗号化するために Amazon S3 で使用する対称 AWS KMS カスタマーマネージドキーの ID を追加します。
- KMS キー (SSE-KMS または DSSE-KMS) を使用して暗号化されたオブジェクトのレプリケーションを有効にすることで、明示的にオプトインします。オプトインするには、次のレプリケーション設定例に示すように、`SourceSelectionCriteria` 要素を追加します。

```
<ReplicationConfiguration>
   <Rule>
      ...
      <SourceSelectionCriteria>
         <SseKmsEncryptedObjects>
           <Status>Enabled</Status>
         </SseKmsEncryptedObjects>
      </SourceSelectionCriteria>

      <Destination>
          ...
          <EncryptionConfiguration>
             <ReplicaKmsKeyID>AWS KMS key ARN or Key Alias ARN that's in the same AWS
 ##### as the destination bucket.</ReplicaKmsKeyID>
          </EncryptionConfiguration>
       </Destination>
      ...
   </Rule>
</ReplicationConfiguration>
```

> **Important**
>
> - KMS キーは、レプリケート先バケットと同じ AWS リージョン内で作成されている必要があります。
> - KMS キーは有効 である必要があります。PutBucketReplication API オペレーションは、KMS キーの有効性を確認しません。無効な KMS キーを使用した場合、応答として HTTP 200 OK ステータスコードを受け取りますが、レプリケーションは失敗します。

次の例は、オプションの設定要素が含まれているレプリケーション設定を示します。このレプリケーション設定にはルールが 1 つあります。このルールは、*Tax* キープレフィックスが付いているオブジェクトに適用されます。Amazon S3 は、指定された AWS KMS key ID を使用して、これらのオブジェクトレプリカを暗号化します。

```
<?xml version="1.0" encoding="UTF-8"?>
<ReplicationConfiguration>
   <Role>arn:aws:iam::account-id:role/role-name</Role>
   <Rule>
      <ID>Rule-1</ID>
      <Priority>1</Priority>
      <Status>Enabled</Status>
      <DeleteMarkerReplication>
         <Status>Disabled</Status>
      </DeleteMarkerReplication>
      <Filter>
         <Prefix>Tax</Prefix>
      </Filter>
      <Destination>
         <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
         <EncryptionConfiguration>
            <ReplicaKmsKeyID>AWS KMS key ARN or Key Alias ARN that's in the same AWS ##
### as the destination bucket.</ReplicaKmsKeyID>
         </EncryptionConfiguration>
      </Destination>
      <SourceSelectionCriteria>
         <SseKmsEncryptedObjects>
            <Status>Enabled</Status>
         </SseKmsEncryptedObjects>
      </SourceSelectionCriteria>
   </Rule>
```

```
</ReplicationConfiguration>
```

IAM ロールに対する追加のアクセス許可の付与

SSE-S3、SSE-KMS、または DSSE-KMS を使用して保管時に暗号化されたオブジェクトをレプリケートするには、レプリケーション設定で指定した AWS Identity and Access Management (IAM) ロールに以下の追加のアクセス許可を付与します。IAM ロールに関連付けられているアクセス許可ポリシーを更新してこれらの権限を付与します。

- レプリケート元オブジェクトのための **`s3:GetObjectVersionForReplication`** アクション – このアクションにより、Amazon S3 は、暗号化されていないオブジェクトと、SSE-S3、SSE-KMS、または DSSE-KMS を使用したサーバー側の暗号化で作成されたオブジェクトの両方をレプリケートできるようになります。

  > **Note**
  >
  > `s3:GetObjectVersion` アクションの代わりに `s3:GetObjectVersionForReplication` アクションの使用をお勧めします。`s3:GetObjectVersionForReplication` ではレプリケーションに必要な最小限のアクセス許可のみを Amazon S3 に提供するためです。さらに、`s3:GetObjectVersion` アクションにより、暗号化されていないオブジェクトや SSE-S3 で暗号化されたオブジェクトはレプリケートできますが、KMS キー (SSE-KMS または DSSE-KMS) を使用して暗号化されたオブジェクトをレプリケートすることはできません。

- KMS キーの **`kms:Decrypt`** および **`kms:Encrypt`** AWS KMS アクション
  - レプリケート元オブジェクトの復号に使用された AWS KMS keyに対して `kms:Decrypt` 権限を付与する必要があります。
  - オブジェクトレプリカの暗号化に使用された AWS KMS keyに対して `kms:Encrypt` 許可を付与する必要があります。
- プレーンテキストオブジェクトをレプリケートするための **`kms:GenerateDataKey`** アクション — SSE-KMS または DSSE-KMS 暗号化がデフォルトで有効になっているバケットにプレーンテキストオブジェクトをレプリケートする場合は、レプリケート先の暗号化コンテキストと KMS キーの `kms:GenerateDataKey` アクセス許可を IAM ポリシーに含める必要があります。

AWS KMS 条件キーを使用して、これらの許可を、レプリケート先バケットとオブジェクトのみに制限することをお勧めします。IAM ロールを所有する AWS アカウントには、ポリシーにリストされている KMS キーに対する `kms:Encrypt` アクションおよび `kms:Decrypt` アクションのアクセス許

可が必要です。KMS キーが別の AWS アカウント によって所有されている場合は、KMS キーの所有者が IAM ロールを所有する AWS アカウントにこれらの許可を付与する必要があります。これらの KMS キーへのアクセス管理の詳細については、「AWS Key Management Service デベロッパーガイド」の「AWS KMS での IAM ポリシーの使用」を参照してください。

S3 バケットキーとレプリケーション

S3 バケットキーでレプリケーションを使用するには、オブジェクトレプリカの暗号化に使用する KMS キーの AWS KMS keyポリシーに、呼び出し元のプリンシパルの `kms:Decrypt` 許可を含める必要があります。`kms:Decrypt` の呼び出しでは、S3 バケットキーを使用する前にその整合性を検証します。詳細については、「レプリケーションでの S3 バケットキーの使用」を参照してください。

レプリケート元バケットまたはレプリケート先バケットで S3 バケットキーを有効にすると、暗号化コンテキストはバケットの Amazon リソースネーム (ARN) になり、オブジェクトの ARN (`arn:aws:s3:::`*`bucket_ARN`* など) にはなりません。IAM ポリシーを更新して、暗号化コンテキストにバケット ARN を使用する必要があります。

```
"kms:EncryptionContext:aws:s3:arn": [
"arn:aws:s3:::bucket_ARN"
]
```

詳細については、「暗号化コンテキスト (x-amz-server-side-encryption-context)」(「REST API の使用」セクション) と「S3 バケットキーを有効にする前に注意するべき変更点」を参照してください。

ポリシーの例: レプリケーションに SSE-S3 と SSE-KMS を使用する

次の IAM ポリシーの例は、SSE-S3 と SSE-KMS をレプリケーションで使用するためのステートメントを示しています。

Example – 個別のレプリケート先バケットで SSE-KMS を使用する

次のポリシーの例は、個別のレプリケート先バケットで SSE-KMS を使用するためのステートメントを示しています。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Action": ["kms:Decrypt"],
```

```
        "Effect": "Allow",
        "Condition": {
            "StringLike": {
                "kms:ViaService": "s3.source-bucket-region.amazonaws.com",
                "kms:EncryptionContext:aws:s3:arn": [
                    "arn:aws:s3:::amzn-s3-demo-source-bucket/key-prefix1*"
                ]
            }
         },
         "Resource": [
            "List of AWS KMS key ARNs that are used to encrypt source objects."
         ]
     },
     {
        "Action": ["kms:Encrypt"],
        "Effect": "Allow",
        "Condition": {
           "StringLike": {
              "kms:ViaService": "s3.destination-bucket-1-region.amazonaws.com",
              "kms:EncryptionContext:aws:s3:arn": [
                 "arn:aws:s3:::amzn-s3-demo-destination-bucket1/key-prefix1*"
              ]
        }
        },
        "Resource": [
           "AWS KMS key ARNs (in the same AWS ##### as destination bucket 1). Used to
encrypt object replicas created in destination bucket 1."
        ]
     },
     {
        "Action": ["kms:Encrypt"],
        "Effect": "Allow",
        "Condition": {
           "StringLike": {
              "kms:ViaService": "s3.destination-bucket-2-region.amazonaws.com",
              "kms:EncryptionContext:aws:s3:arn": [
                 "arn:aws:s3:::amzn-s3-demo-destination-bucket2/key-prefix1*"
              ]
        }
        },
        "Resource": [
           "AWS KMS key ARNs (in the same AWS ##### as destination bucket 2). Used to
encrypt object replicas created in destination bucket 2."
        ]
```

```
      }
   ]
}
```

Example - SSE-S3 と SSE-KMS で作成したオブジェクトのレプリケーション

以下は、暗号化されていないオブジェクト、SSE-S3 で作成したオブジェクト、および SSE-KMS で作成したオブジェクトをレプリケートするのに必要な許可を付与する完全な IAM ポリシーを示しています。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetReplicationConfiguration",
            "s3:ListBucket"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetObjectVersionForReplication",
            "s3:GetObjectVersionAcl"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket/key-prefix1*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:ReplicateObject",
            "s3:ReplicateDelete"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/key-prefix1*"
      },
      {
         "Action":[
```

```
            "kms:Decrypt"
         ],
         "Effect":"Allow",
         "Condition":{
            "StringLike":{
               "kms:ViaService":"s3.source-bucket-region.amazonaws.com",
               "kms:EncryptionContext:aws:s3:arn":[
                  "arn:aws:s3:::amzn-s3-demo-source-bucket/key-prefix1*"
               ]
            }
         },
         "Resource":[
           "List of the AWS KMS key ARNs that are used to encrypt source objects."
         ]
      },
      {
         "Action":[
            "kms:Encrypt"
         ],
         "Effect":"Allow",
         "Condition":{
            "StringLike":{
               "kms:ViaService":"s3.destination-bucket-region.amazonaws.com",
               "kms:EncryptionContext:aws:s3:arn":[
                  "arn:aws:s3:::amzn-s3-demo-destination-bucket/prefix1*"
               ]
            }
         },
         "Resource":[
            "AWS KMS key ARNs (in the same AWS ##### as the destination bucket) to use
 for encrypting object replicas"
         ]
      }
   ]
}
```

Example – S3 バケットキーを使用したオブジェクトのレプリケーション

次に示すのは、S3 バケットキーを使用してオブジェクトをレプリケートするのに必要なアクセス許可を付与する完全な IAM ポリシーです。

```
{
   "Version":"2012-10-17",
```

```
    "Statement":[
       {
          "Effect":"Allow",
          "Action":[
             "s3:GetReplicationConfiguration",
             "s3:ListBucket"
          ],
          "Resource":[
             "arn:aws:s3:::amzn-s3-demo-source-bucket"
          ]
       },
       {
          "Effect":"Allow",
          "Action":[
             "s3:GetObjectVersionForReplication",
             "s3:GetObjectVersionAcl"
          ],
          "Resource":[
             "arn:aws:s3:::amzn-s3-demo-source-bucket/key-prefix1*"
          ]
       },
       {
          "Effect":"Allow",
          "Action":[
             "s3:ReplicateObject",
             "s3:ReplicateDelete"
          ],
          "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/key-prefix1*"
       },
       {
          "Action":[
             "kms:Decrypt"
          ],
          "Effect":"Allow",
          "Condition":{
             "StringLike":{
                "kms:ViaService":"s3.source-bucket-region.amazonaws.com",
                "kms:EncryptionContext:aws:s3:arn":[
                   "arn:aws:s3:::amzn-s3-demo-source-bucket"
                ]
             }
          },
          "Resource":[
            "List of the AWS KMS key ARNs that are used to encrypt source objects."
```

```
            ]
        },
        {
            "Action":[
               "kms:Encrypt"
            ],
            "Effect":"Allow",
            "Condition":{
               "StringLike":{
                  "kms:ViaService":"s3.destination-bucket-region.amazonaws.com",
                  "kms:EncryptionContext:aws:s3:arn":[
                     "arn:aws:s3:::amzn-s3-demo-destination-bucket"
                  ]
               }
            },
            "Resource":[
               "AWS KMS key ARNs (in the same AWS ##### as the destination bucket) to use
 for encrypting object replicas"
            ]
        }
    ]
}
```

クロスアカウントシナリオに対する追加のアクセス許可の付与

レプリケート元バケットとレプリケート先バケットが、異なる AWS アカウントによって所有されているクロスアカウントシナリオでは、KMS キーを使用してオブジェクトレプリカを暗号化できます。ただし、KMS キー所有者は、レプリケート元バケットの所有者に KMS キーを使用する許可を付与する必要があります。

> **Note**
>
> SSE-KMS データをクロスアカウントでレプリケートする必要がある場合、レプリケーションルールでは、レプリケート先アカウントの AWS KMS からのカスタマーマネージドキーを指定する必要があります。AWS マネージドキー はクロスアカウントの使用を許可しないため、クロスアカウントレプリケーションの実行には使用できません。

レプリケート元バケット所有者に KMS キー (AWS KMS コンソール) を使用する許可を付与するには

1. AWS Management Console にサインインし、AWS KMS コンソール (https://console.aws.amazon.com/kms) を開きます。

2. AWS リージョン を変更するにはページの右上隅にあるリージョンセレクターを使用します。
3. ユーザーが作成および管理するアカウント内のキーを表示するには、ナビゲーションペインで [Customer managed keys] (カスタマーマネージドキー) を選択します。
4. KMS キーを選択します。
5. [一般設定] セクションで、[キーポリシー] タブを選択します。
6. [別の AWS アカウント] まで下にスクロールします。
7. [別の AWS アカウントを追加] を選択します。

   [別の AWS アカウント]ダイアログボックスが表示されます。
8. ダイアログボックスで、[別の AWS アカウントを追加] を選択します。[arn:aws:iam::] に、レプリケート元バケットのアカウント ID を入力します。
9. [変更の保存] をクリックします。

レプリケート元バケット所有者に KMS キー(AWS CLI) を使用する許可を付与するには

- `put-key-policy` AWS Command Line Interface (AWS CLI) コマンドの詳細については、「AWS CLI コマンドリファレンス」の「put-key-policy」を参照してください。基盤となる `PutKeyPolicy` API オペレーションの詳細については、「AWS Key Management Service API リファレンス」の「PutKeyPolicy」を参照してください。

AWS KMS トランザクションクォータに関する考慮事項

クロスリージョンレプリケーション (CRR) を有効にした後で、AWS KMS 暗号化を使用して多数の新しいオブジェクトを追加すると、スロットリング (HTTP `503 Service Unavailable` エラー) が発生する可能性があります。1 秒あたりの AWS KMS トランザクション数が現在のクォータを超えると、スロットリングが発生します。詳細については、「AWS Key Management Service デベロッパーガイド」の「クォータ」を参照してください。

クォータの引き上げをリクエストするには、Service Quotas を使用してください。詳細については、「Requesting a quota increase」(クォータ引き上げのリクエスト) を参照してください。リージョンの Service Quotas がサポートされていない場合は、AWS サポート ケースを開きます。

暗号化されたオブジェクトのレプリケーションの有効化

デフォルトでは、Amazon S3 は AWS Key Management Service (AWS KMS) キーによるサーバー側の暗号化 (SSE-KMS) または AWS KMS キーによる二層式サーバー側の暗号化 (DSSE-KMS) を使用して暗号化されたオブジェクトをレプリケートしません。SSE-KMS または DSSE-KMS で暗号化さ

れたオブジェクトをレプリケートするには、バケットレプリケーション設定を変更して、Amazon S3 がこれらのオブジェクトをレプリケートするように指示します。この例では、Amazon S3 コンソールと AWS Command Line Interface (AWS CLI) を使用してバケットのレプリケーション設定を変更し、暗号化オブジェクトのレプリケーションを有効にする方法について説明します。

> **Note**
>
> レプリケート元バケットまたはレプリケート先バケットで S3 バケットキーを有効にすると、暗号化コンテキストはバケットの Amazon リソースネーム (ARN) になり、オブジェクトの ARN にはなりません。暗号化コンテキストとしてバケット ARN を使用するには、IAM ポリシーを更新する必要があります。詳細については、「S3 バケットキーとレプリケーション」を参照してください。

> **Note**
>
> Amazon S3 では、マルチリージョン AWS KMS keys を使用できます。ただし、Amazon S3 では現在、マルチリージョンキーは、単一リージョンキーであるかのように処理され、キーのマルチリージョン特徴は使用しません。詳細については、「AWS Key Management Service デベロッパーガイド」の「マルチリージョンキーを使用する」を参照してください。

S3 コンソールの使用

手順については、「同じアカウントでのバケットのレプリケーションの設定」を参照してください。このトピックでは、レプリケート元およびレプリケート先バケットが同一の、または異なる AWS アカウントによって所有されている場合にレプリケーション設定を行う手順について説明します。

AWS CLI を使用する場合

AWS CLI で暗号化されたオブジェクトをレプリケートするには、以下の操作を実行します。

- レプリケート元バケットとレプリケート先バケットを作成して、これらのバケットのバージョニングを有効にします。
- Amazon S3 にオブジェクトをレプリケートするアクセス許可を付与する AWS Identity and Access Management (IAM) サービスロールを作成します。IAM ロールのアクセス許可には、暗号化されたオブジェクトをレプリケートするために必要なアクセス許可が含まれています。

- レプリケート元バケットにレプリケーション設定を追加します。レプリケーション設定は、KMS キーを使用して暗号化されたオブジェクトのレプリケーションに関する情報を提供します。
- レプリケート元バケットに暗号化されたオブジェクトを追加します。
- セットアップをテストして、暗号化されたオブジェクトがレプリケート先バケットにレプリケートされていることを確認します。

このプロセスを以下の手順で説明します。

サーバー側の暗号化されたオブジェクトをレプリケートするには (AWS CLI)

この手順の例を使用するには、*user input placeholders* を自分の情報に置き換えてください。

1. この例では、レプリケート元 (*amzn-s3-demo-source-bucket*) および レプリケート先 (*amzn-s3-demo-destination-bucket*) バケットの両方を同じ AWS アカウントで作成します。AWS CLI の認証情報プロファイルも設定します。この例では、プロファイル名 *acctA* を使用します。

   名前付きプロファイルの設定と使用に関する詳細については、「AWS Command Line Interface ユーザーガイド」の「設定ファイルと認証情報ファイルの設定」を参照してください。

2. 次のコマンドを使用して *amzn-s3-demo-source-bucket* バケットを作成し、バージョニングを有効にします。次の例のコマンドは、*amzn-s3-demo-source-bucket* バケットを米国東部 (バージニア北部) (us-east-1) リージョンに作成します。

   ```
   aws s3api create-bucket \
   --bucket amzn-s3-demo-source-bucket \
   --region us-east-1 \
   --profile acctA
   ```

   ```
   aws s3api put-bucket-versioning \
   --bucket amzn-s3-demo-source-bucket \
   --versioning-configuration Status=Enabled \
   --profile acctA
   ```

3. 次のコマンドを使用して *amzn-s3-demo-destination-bucket* バケットを作成し、バージョニングを有効にします。次のコマンドは、*amzn-s3-demo-destination-bucket* バケットを米国西部 (オレゴン) (us-west-2) リージョンに作成します。

> **Note**
>
> *amzn-s3-demo-source-bucket* と *amzn-s3-demo-destination-bucket* の両方のバケットが同じ AWS アカウント にあるときに、レプリケーション設定をセットアップするには、同じプロファイルを使用します。この例では *acctA* を使用します。バケットが異なる AWS アカウント によって所有されているときに、レプリケーションを設定するには、それぞれに異なるプロファイルを指定します。

```
aws s3api create-bucket \
--bucket amzn-s3-demo-destination-bucket \
--region us-west-2 \
--create-bucket-configuration LocationConstraint=us-west-2 \
--profile acctA
```

```
aws s3api put-bucket-versioning \
--bucket amzn-s3-demo-destination-bucket \
--versioning-configuration Status=Enabled \
--profile acctA
```

4. 次に、IAM サービスロールを作成します。*amzn-s3-demo-source-bucket* バケットに後で追加するレプリケーション設定でこのロールを指定します。Amazon S3 は、ユーザーに代わってオブジェクトをレプリケートするこの ロールを引き受けます。IAM ロールは 2 つのステップで作成します。

   - サービスロールを作成します。
   - アクセス権限ポリシーをロールにアタッチします。

   a. IAM サービスロールを作成するには、以下を実行します。

      i. 次の信頼ポリシーをコピーして、ローカルコンピュータの現在のディレクトリにある *s3-role-trust-policy-kmsobj*.json という名前のファイルに保存します。このポリシーは、ロールを引き受けるサービスプリンシパルアクセス許可を Amazon S3 に付与し、Amazon S3 がユーザーに代わってタスクを実行できるようにします。

```
{
   "Version":"2012-10-17",
```

```
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"s3.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

ii. 次のコマンドを使用して、ロールを作成します。

```
$ aws iam create-role \
--role-name replicationRolekmsobj \
--assume-role-policy-document file://s3-role-trust-policy-kmsobj.json  \
--profile acctA
```

b. 次に、アクセス許可ポリシーをロールにアタッチします。このポリシーは、さまざまな Amazon S3 バケットとオブジェクトアクションに対するアクセス許可を付与します。

i. 次のアクセス権限ポリシーをコピーして、ローカルコンピュータの現在のディレクトリにある *s3-role-permissions-policykmsobj*.json という名前のファイルに保存します。IAM ロールを作成して、後でポリシーをアタッチします。

> **Important**
>
> アクセス許可ポリシーで、*amzn-s3-demo-source-bucket* および *amzn-s3-demo-destination-bucket* バケットの暗号化に使用される AWS KMS キー ID を指定します。*amzn-s3-demo-source-bucket* バケットと *amzn-s3-demo-destination-bucket* バケット用に 2 つの別々の KMS キーを作成する必要があります。AWS KMS keys は、それらが作成された AWS リージョンの外部で共有されることはありません。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Action":[
            "s3:ListBucket",
```

```
            "s3:GetReplicationConfiguration",
            "s3:GetObjectVersionForReplication",
            "s3:GetObjectVersionAcl",
            "s3:GetObjectVersionTagging"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket",
            "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
         ]
      },
      {
         "Action":[
            "s3:ReplicateObject",
            "s3:ReplicateDelete",
            "s3:ReplicateTags"
         ],
         "Effect":"Allow",
         "Condition":{
            "StringLikeIfExists":{
               "s3:x-amz-server-side-encryption":[
                  "aws:kms",
                  "AES256",
                  "aws:kms:dsse"
               ],
               "s3:x-amz-server-side-encryption-aws-kms-key-id":[
                  "AWS KMS key IDs(in ARN format) to use for encrypting
object replicas"
               ]
            }
         },
         "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
      },
      {
         "Action":[
            "kms:Decrypt"
         ],
         "Effect":"Allow",
         "Condition":{
            "StringLike":{
               "kms:ViaService":"s3.us-east-1.amazonaws.com",
               "kms:EncryptionContext:aws:s3:arn":[
                  "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
               ]
```

```
            }
         },
         "Resource":[
            "AWS KMS key IDs(in ARN format) used to encrypt source
 objects."
         ]
      },
      {
         "Action":[
            "kms:Encrypt"
         ],
         "Effect":"Allow",
         "Condition":{
            "StringLike":{
               "kms:ViaService":"s3.us-west-2.amazonaws.com",
               "kms:EncryptionContext:aws:s3:arn":[
                  "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
               ]
            }
         },
         "Resource":[
            "AWS KMS key IDs (in ARN format) to use for encrypting object
 replicas"
         ]
      }
   ]
}
```

ii. ポリシーを作成し、ロールにアタッチします。

```
$ aws iam put-role-policy \
--role-name replicationRolekmsobj \
--policy-document file://s3-role-permissions-policykmsobj.json \
--policy-name replicationRolechangeownerPolicy \
--profile acctA
```

5. 次に、以下のレプリケーション設定を *amzn-s3-demo-source-bucket* バケットに追加します。これは、*Tax/* プレフィックスを持つオブジェクトを *amzn-s3-demo-destination-bucket* バケットにレプリケートするように Amazon S3 に指示します。

> **Important**
>
> レプリケーション設定で、Amazon S3 が引き受けることができる IAM ロールを指定します。ユーザーに iam:PassRole アクセス権限がある場合のみ実行できます。CLI コマンドで指定するプロファイルには、このアクセス許可が必要です。詳細については、IAM ユーザーガイドの「AWS のサービス のサービスにロールを渡すアクセス権限をユーザーに付与する」を参照してください。

```
 <ReplicationConfiguration>
  <Role>IAM-Role-ARN</Role>
  <Rule>
    <Priority>1</Priority>
    <DeleteMarkerReplication>
       <Status>Disabled</Status>
    </DeleteMarkerReplication>
    <Filter>
       <Prefix>Tax</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <SourceSelectionCriteria>
      <SseKmsEncryptedObjects>
        <Status>Enabled</Status>
      </SseKmsEncryptedObjects>
    </SourceSelectionCriteria>
    <Destination>
      <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
      <EncryptionConfiguration>
        <ReplicaKmsKeyID>AWS KMS key IDs to use for encrypting object replicas</
ReplicaKmsKeyID>
      </EncryptionConfiguration>
    </Destination>
  </Rule>
</ReplicationConfiguration>
```

レプリケーション設定を *amzn-s3-demo-source-bucket* バケットに追加するには、以下を実行します。

a. AWS CLI ではレプリケーション設定を JSON 形式で指定する必要があります。以下の JSON を、ローカルコンピュータの現在のディレクトリにあるファイル (*replication*.json) に保存します。

```
{
   "Role":"IAM-Role-ARN",
   "Rules":[
      {
         "Status":"Enabled",
         "Priority":1,
         "DeleteMarkerReplication":{
            "Status":"Disabled"
         },
         "Filter":{
            "Prefix":"Tax"
         },
         "Destination":{
            "Bucket":"arn:aws:s3:::amzn-s3-demo-destination-bucket",
            "EncryptionConfiguration":{
               "ReplicaKmsKeyID":"AWS KMS key IDs (in ARN format) to use for
 encrypting object replicas"
            }
         },
         "SourceSelectionCriteria":{
            "SseKmsEncryptedObjects":{
               "Status":"Enabled"
            }
         }
      }
   ]
}
```

b. JSON を編集して、*amzn-s3-demo-destination-bucket* バケット、*AWS KMS key IDs (in ARN format)*、および *IAM-role-ARN* の値を指定します。変更を保存します。

c. 次のコマンドを使用して、レプリケーション設定を *amzn-s3-demo-source-bucket* バケットに追加します。必ず *amzn-s3-demo-source-bucket* バケット名を指定してください。

```
$ aws s3api put-bucket-replication \
--replication-configuration file://replication.json \
```

```
--bucket amzn-s3-demo-source-bucket \
--profile acctA
```

6. 設定をテストして、暗号化されたオブジェクトがレプリケートされることを確認します。Amazon S3 コンソールで、次の操作を行います。

   a. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。

   b. *amzn-s3-demo-source-bucket* バケットに *Tax* という名前のフォルダを作成します。

   c. サンプルオブジェクトをフォルダに追加します。必ず暗号化オプションを選択し、オブジェクトを暗号化するための KMS キーを指定してください。

   d. *amzn-s3-demo-destination-bucket* バケットにオブジェクトのレプリカが含まれていることと、設定で指定した KMS キーを使用して暗号化されていることを確認します。詳細については、「the section called “レプリケーションステータスの取得”」を参照してください。

AWS SDK の使用

レプリケーション設定を追加するコード例については、「AWS SDK の使用」を参照してください。レプリケーション設定を適切に変更する必要があります。

レプリカの変更同期によるメタデータ変更のレプリケート

Amazon S3 レプリカの変更を同期することで、タグ、アクセスコントロールリスト (ACL)、Object Lock 設定などのオブジェクトメタデータをレプリカとレプリケート元オブジェクト間でレプリケートできます。デフォルトでは、Amazon S3 はレプリケート元オブジェクトからレプリカにのみメタデータをレプリケートします。レプリカの変更同期を有効にすると、Amazon S3 はレプリカコピーに加えられたメタデータの変更をレプリケート元オブジェクトにレプリケートし、レプリケーションを双方向にします。

レプリカ変更の同期の有効化

Amazon S3 レプリカの変更同期は、新規または既存のレプリケーションルールで使用できます。削除マーカーレプリケーションは、バケット全体に適用することも、特定のプレフィックスを持つオブジェクトに適用することもできます。

Amazon S3 コンソールを使用してレプリカ変更の同期を有効にするには、「ライブレプリケーションの設定例」を参照してください。このトピックでは、レプリケート元およびレプリケート先バケッ

トが同じまたは異なる AWS アカウントによって所有されている場合に、レプリケーション設定でレプリカ変更の同期を有効にする手順について説明します。

AWS Command Line Interface (AWS CLI) を使用してレプリカ変更の同期を有効にするには、ReplicaModifications が有効になっているレプリカを含むバケットにレプリケーション設定を追加する必要があります。双方向レプリケーションを設定するには、レプリケート元バケット (*amzn-s3-demo-source-bucket*) から、レプリカを含めるバケット (*amzn-s3-demo-destination-bucket*) に対するレプリケーションルールを作成します。次に、レプリカを含めるバケット (*amzn-s3-demo-destination-bucket*) からレプリケート元バケット (*amzn-s3-demo-source-bucket*) に対するレプリケーションルールを、もう 1 つ作成します。レプリケート元およびレプリケート先バケットは、同一のまたは異なる AWS リージョンに配置することができます。

> **Note**
>
> オブジェクトのアクセスコントロールリスト (ACL)、オブジェクトのタグ、あるいは Object Lock の設定など、レプリカメタデータの変更を複製するには、レプリケート元およびレプリケート先の両方のバケットでレプリカ変更の同期を有効にする必要があります。これらのルールは、すべてのレプリケーションルールと同様に、バケット全体に適用することも、オブジェクトのサブセットをプレフィックスまたはオブジェクトタグでフィルタリングして適用することも可能です。

以下の設定例では、Amazon S3 は *Tax* というプレフィックスのメタデータの変更を *amzn-s3-demo-source-bucket* バケット (このバケットにはレプリケート元オブジェクトを含む) にレプリケートします。

```
{
    "Rules": [
        {
            "Status": "Enabled",
            "Filter": {
                "Prefix": "Tax"
            },
            "SourceSelectionCriteria": {
                "ReplicaModifications":{
                    "Status": "Enabled"
                }
            },
            "Destination": {
```

```
                "Bucket": "arn:aws:s3:::amzn-s3-demo-source-bucket"
            },
            "Priority": 1
        }
    ],
    "Role": "IAM-Role-ARN"
}
```

AWS CLI を使用してレプリケーションルールを作成する手順については、「同じアカウントでのバケットのレプリケーションの設定」を参照してください。

バケット間での削除マーカーのレプリケーション

デフォルトでは、S3 レプリケーションが有効で、レプリケーション元バケットでオブジェクトが削除されると、Amazon S3 はレプリケート元バケットにのみ削除マーカーを追加します。このアクションは、レプリケート先バケット内のデータを偶発的または悪意のある削除から保護するのに役立ちます。削除マーカーレプリケーションが有効になっている場合、これらのマーカーはレプリケート先バケットにコピーされ、Amazon S3 はオブジェクトがレプリケート元バケットとレプリケート先バケットの両方で削除されたように動作します。削除マーカーの動作の詳細については、削除マーカーの使用を参照してください。

> **Note**
>
> - 削除マーカーレプリケーションは、タグベースのレプリケーションルールではサポートされていません。また、削除マーカーレプリケーションは、S3 Replication Time Control (S3 RTC) の使用時に付与される 15 分間のサービスレベルアグリーメント (SLA) に準拠していません。
> - レプリケーション設定の最新 XML バージョンを使用していない場合、削除操作はレプリケーションに異なる影響を与えます。詳細については、「削除オペレーションがレプリケーションに与える影響」を参照してください。
> - 削除マーカーレプリケーションを有効化し、レプリケート元バケットに S3 ライフサイクルの有効期限ルールがある場合、S3 ライフサイクルの有効期限ルールによって追加された削除マーカーはレプリケート先バケットにレプリケートされません。

削除マーカーレプリケーションの有効化

新規または既存のレプリケーションルールで、削除マーカーレプリケーションの使用を開始できます。削除マーカーレプリケーションは、バケット全体に適用することも、特定のプレフィックスを持つオブジェクトに適用することもできます。

Amazon S3 コンソールを使用して削除マーカーレプリケーションを有効にするには、「S3 コンソールの使用」を参照してください。このトピックでは、レプリケート元およびレプリケート先バケットが同じまたは異なる AWS アカウントによって所有されている場合に、レプリケーション設定で削除マーカーレプリケーションを有効にする手順について説明します。

AWS Command Line Interface (AWS CLI) を使用して削除マーカーレプリケーションを有効にするには、次の設定例に示すように、DeleteMarkerReplication が有効になっているレプリケート元バケットにレプリケーション設定を追加する必要があります。

次のレプリケーション設定例では、*Tax* というプレフィクスの下にあるオブジェクトのレプリケート先バケットである *amzn-s3-demo-destination-bucket* に、削除マーカーがレプリケートされます。

```
{
    "Rules": [
        {
            "Status": "Enabled",
            "Filter": {
                "Prefix": "Tax"
            },
            "DeleteMarkerReplication": {
                "Status": "Enabled"
            },
            "Destination": {
                "Bucket": "arn:aws:s3:::amzn-s3-demo-destination-bucket"
            },
            "Priority": 1
        }
    ],
    "Role": "IAM-Role-ARN"
}
```

AWS CLI を使用してレプリケーションルールを作成する手順については、「同じアカウントでのバケットのレプリケーションの設定」を参照してください。

ライブレプリケーションの管理または一時停止

ライブレプリケーションは、同一または異なる AWS リージョン にあるバケット間でオブジェクトを自動的に非同期でコピーする機能です。レプリケーションを設定すると、Amazon S3 は新しく作成されたオブジェクトと更新されたオブジェクトをレプリケート元バケットから指定された 1 つ以上のレプリケート先バケットにレプリケートします。

レプリケーションルールは、Amazon S3 コンソールを使用してレプリケート元のバケットに追加できます。レプリケーションルールにより、レプリケート元のソースバケットオブジェクトと、レプリケートされたオブジェクトが保存されるレプリケート先バケットが定義されます。レプリケーションの詳細については、「リージョン内およびリージョン間でのオブジェクトのレプリケート」を参照してください。

Amazon S3 コンソールの [レプリケーション] ページで、レプリケーションルールを管理できます。レプリケーションルールは、追加、表示、編集、有効化、無効化、削除できます。また、レプリケーションルールの優先度を変更することもできます。バケットへのレプリケーションルールの追加については、「S3 コンソールの使用」を参照してください。

Amazon S3 コンソールを使用してバケットのレプリケーションルールを管理するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。
3. [汎用バケット] タブで、バケットの名前を選択します。
4. [管理] タブを選択して、[レプリケーションルール] まで下にスクロールします。
5. レプリケーションルールは、以下の方法で変更することができます。
   - レプリケーションルールを有効化または無効化するには、ルールの左側にあるオプションボタンを選択します。[アクション] メニューで、[ルールの有効化] または [ルールの無効化] を選択します。[アクション] メニューでは、バケットのすべてのルールを無効化、有効化、削除することもできます。

> **Note**
>
> レプリケーションルールを無効化し、後でルールを再度有効化した場合、ルールの無効化中にレプリケートされなかった新規または変更されたオブジェクトは、ルールを再度有効にしても自動的にレプリケートされません。これらのオブジェクトをレプリケートするには、S3 バッチレプリケーションを使用する必要があります。詳

細については、「the section called “既存のオブジェクトのレプリケーション”」を参照してください。

- ルールの優先度を変更するには、ルールの左側にあるオプションボタンを選択して、[ルールの編集] を選択します。

  ルールの優先順位を指定して、複数のルールの範囲に含まれるオブジェクトによって引き起こされる競合を回避します。ルールが重複している場合、Amazon S3 はルールの優先度を使用して適用するルールを決定します。数値が大きいほど、優先度が高くなります。ルーティングの優先度の詳細については、「レプリケーション設定ファイル要素」をご覧ください。

レプリケーションの一時停止または停止

レプリケーションを一時停止し、後で自動的に再開するには、AWS Fault Injection Service の `aws:s3:bucket-pause-replication` アクションを使用できます。詳細については、「AWS Fault Injection Service ユーザーガイド」の「aws:s3:bucket-pause-replication」および「Pause S3 Replication」を参照してください。

Amazon S3 でレプリケーションを停止するには、レプリケーションルールを無効化することをお勧めします。レプリケーションルールを無効化し、後でルールを再度有効化した場合、ルールの無効化中にレプリケートされなかった新規または変更されたオブジェクトは、ルールを再度有効にしても自動的にレプリケートされません。これらのオブジェクトをレプリケートするには、S3 バッチレプリケーションを使用する必要があります。詳細については、「the section called “既存のオブジェクトのレプリケーション”」を参照してください。

AWS Identity and Access Management (IAM) ロール、AWS Key Management Service (AWS KMS) アクセス許可、または必要なアクセス許可を Amazon S3 に付与するバケットポリシーアクセス許可を削除すると、レプリケーションは停止します。ただし、レプリケーションが失敗するため、これらのアプローチはお勧めしません。Amazon S3 は、影響を受けるオブジェクトのレプリケーションステータスを `FAILED` として報告します。アクセス許可が後で復元された場合、`FAILED` とマークされたオブジェクトは自動的にレプリケートされません。これらのオブジェクトをレプリケートするには、S3 バッチレプリケーションを使用する必要があります。

バッチレプリケーションを使用した既存のオブジェクトのレプリケーション

S3 バッチレプリケーションは、Amazon S3 バケット間で新しいオブジェクトを継続的かつ自動的にレプリケートするライブレプリケーションとは異なります。代わりに、S3 バッチレプリケーションは既存のオブジェクトでオンデマンドで実行されます。S3 バッチレプリケーションを使用して、次のタイプのオブジェクトをレプリケートできます。

- レプリケーション設定が実行される前に存在していたオブジェクト
- 以前にレプリケートされたオブジェクト
- レプリケーションに失敗したオブジェクト

バッチオペレーションジョブを使用して、これらのオブジェクトをオンデマンドでレプリケートできます。

バッチレプリケーションを開始するには、次の操作を行います。

- 新しいレプリケーションルールまたはレプリケート先のバッチレプリケーションを開始する — 1 回限りのバッチレプリケーションジョブは、新しいレプリケーション設定で最初のルールを作成する場合や、Amazon S3 を介して既存の設定に新しいレプリケート先バケットを追加する場合に作成できます。
- 既存のレプリケーション設定のバッチレプリケーションを開始する — S3 バッチオペレーションを使用して、Amazon S3 コンソール、AWS Command Line Interface (AWS CLI)、AWS SDK、または Amazon S3 REST API を介し、新しいバッチレプリケーションジョブを作成できます。

バッチレプリケーションジョブが終了すると、完了レポートが表示されます。このレポートを使用してジョブを検査する方法の詳細については、「ジョブステータスと完了レポートの追跡」を参照してください。

S3 バッチレプリケーションに関する考慮事項

S3 バッチレプリケーションを使用する前に、次の考慮事項のリストを確認してください。

- レプリケート元バケットには既存のレプリケーション設定が必要です。レプリケーションを有効にするには、「ライブレプリケーションの設定の概要」と「ライブレプリケーションの設定例」を参照してください。

- バケットで S3 ライフサイクルが設定されている場合は、バッチレプリケーションジョブがアクティブな際には、ライフサイクルルールを無効にすることをお勧めします。これは、レプリケート元バケットとレプリケート先バケットの間で等価性を確保するのに役立ちます。これを行わない場合、これらのバケットが分岐し、レプリケート先バケットがレプリケート元バケットの完全なレプリカではなくなる可能性があります。たとえば、次のシナリオを考えてみます。
  - レプリケート元バケットには、オブジェクトとそのオブジェクトの削除マーカーの複数のバージョンがあります。
  - レプリケート元とレプリケート先のバケットには、期限切れの削除マーカーを削除するライフサイクル設定が設定されています。

  このシナリオでは、バッチレプリケーションにより、オブジェクトのバージョンがレプリケートされる前に、レプリケート先バケットに削除マーカーがレプリケートされることがあります。その場合、オブジェクトのバージョンがレプリケートされる前に、ライフサイクル設定で削除マーカーの有効期限が切れ、削除マーカーがレプリケート先バケットから削除される可能性があります。
- バッチオペレーションジョブを実行するために指定する AWS Identity and Access Management IAM ロールには、基になるバッチレプリケーションを実行する権限が必要です。IAM ロールの作成の詳細については、「S3 バッチレプリケーション用の IAM ロールの設定」を参照してください。
- バッチレプリケーションには、Amazon S3 で生成できるマニフェストが必要です。生成されたマニフェストは、レプリケーション元バケットと同じ AWS リージョンに保存されている必要があります。マニフェストを生成しない場合は、レプリケートするオブジェクトを含む Amazon S3 インベントリレポートまたは CSV ファイルを指定できます。詳細については、「the section called “バッチレプリケーションジョブのマニフェストの指定”」を参照してください。
- バッチレプリケーションでは、レプリケート先バケットからオブジェクトのバージョン ID を指定することで削除されたオブジェクトの再レプリケーションはサポートされません。これらのオブジェクトを再レプリケートするには、バッチコピージョブを使用してソースオブジェクトを所定の場所でコピーします。これらのオブジェクトを所定の場所でコピーすると、レプリケート元バケットにオブジェクトの新しいバージョンが作成され、レプリケート先バケットへのレプリケーションが自動的に開始されます。レプリケート先バケットを削除して再作成しても、レプリケーションは開始されません。

  バッチコピーの詳細については、「バッチ操作を使用してオブジェクトをコピーする例」を参照してください。
- レプリケート元バケットでレプリケーションルールを使用している場合は、レプリケーション設定を更新して、レプリケーションルールにアタッチされている IAM ロールに、オブジェクトをレプ

リケートするための適切な権限を付与してください。この IAM ロールには、ソースバケットとレプリケート先バケットの両方でレプリケーションを実行する権限が必要です。

- 短期間に同じバケットに対して複数のバッチレプリケーションジョブを送信すると、Amazon S3 はそれらのジョブを同時に実行します。
- 2 つの異なるバケットに対して複数の Batch レプリケーションジョブを送信する場合、Amazon S3 がすべてのジョブを同時に実行するわけではないことに注意してください。アカウントで一度に実行できるバッチレプリケーションジョブの数を超えると、Amazon S3 は優先度の低いジョブを一時停止して優先度の高いジョブを処理します。優先度の高いジョブが完了すると、一時停止していたジョブは再びアクティブになります。
- バッチオペレーションは、S3 Glacier Flexible Retrieval ストレージクラスと S3 Glacier Deep Archive ストレージクラスに保存されたオブジェクトに対してはサポートされていません。
- アーカイブアクセスまたはディープアーカイブアクセスのストレージ階層に保存されている S3 Intelligent-Tiering オブジェクトのバッチレプリケーションを行うには、まず復元リクエストを開始し、オブジェクトが高頻度アクセス階層に移動されるまで待つ必要があります。
- 1 つのバッチレプリケーションジョブで、最大 200 億個のオブジェクトを持つマニフェストをサポートできます。

バッチレプリケーションジョブのマニフェストの指定

マニフェストは、Amazon S3 が動作するオブジェクトキーを含む Amazon S3 オブジェクトです。バッチレプリケーションジョブを作成する場合は、ユーザー生成のマニフェストを指定するか、レプリケーション設定に基づいて Amazon S3 でマニフェストを生成させる必要があります。

ユーザーが作成したマニフェストを提供する場合は、Amazon S3 インベントリレポートまたは CSV ファイルの形式である必要があります。マニフェスト内のオブジェクトがバージョニング対応のバケット内にある場合は、そのオブジェクトのバージョン ID を指定する必要があります。マニフェストで指定されたバージョン ID を持つオブジェクトのみがレプリケートされます。マニフェストの指定の詳細については、「マニフェストの指定」を参照してください。

Amazon S3 がユーザーに代わってマニフェストファイルを生成するように選択した場合、リストされるオブジェクトでは、レプリケート元バケットのレプリケーション設定と同じレプリケート元バケット、プレフィックス、タグを使用します。生成されたマニフェストでは、Amazon S3 はオブジェクトの適格なバージョンをすべてレプリケートします。

> **Note**
>
> Amazon S3 によるマニフェストの生成を選択する場合は、マニフェストがレプリケーション元バケットと同じ AWS リージョンに保存されている必要があります。

バッチレプリケーションジョブのフィルター

バッチレプリケーションジョブを作成するときに、オプションで、オブジェクトの作成日やレプリケーションステータスなどの追加のフィルターを指定して、ジョブのスコープを縮小できます。

オブジェクトのレプリケーションは、`ObjectReplicationStatuses` 値を基に、以下の値を 1 つ以上指定することでフィルターできます。

- `"NONE"` - Simple Storage Service (Amazon S3) がこれまでオブジェクトのレプリケートを試みたことがないことを示します。
- `"FAILED"` - Amazon S3 が以前にオブジェクトのレプリケートを試みたがオブジェクトのレプリケーションに失敗したことを示します。
- `"COMPLETED"` - Simple Storage Service (Amazon S3) が以前にオブジェクトを正常にレプリケートしたことを示します。
- `"REPLICA"` - このオブジェクトが Amazon S3 が別のレプリケート元バケットからレプリケートしたレプリカであることを示します。

レプリケーションステータスの詳細については、「レプリケーションステータス情報の取得」を参照してください。

バッチレプリケーションジョブをフィルターしない場合、バッチオペレーションは、デフォルトでレプリケートされない特定のオブジェクトを除き、レプリケーション設定のルールに一致するマニフェスト内のすべてのオブジェクト (`ObjectReplicationStatus` に関係なく) のレプリケーションを試みます。詳細については、the section called “レプリケーション設定でレプリケートされないものは何ですか?”を参照してください。

目標によっては、以下の 1 つまたは複数の値に `ObjectReplicationStatuses` を設定する場合があります。

- レプリケートされたことがない既存のオブジェクトのみをレプリケートするには、`"NONE"` のみを含めます。

- 以前にレプリケートに失敗したオブジェクトのレプリケートのみを再試行するには、"FAILED" のみを含めます。
- 既存のオブジェクトをレプリケートし、以前にレプリケートに失敗したオブジェクトのレプリケーションを再試行するには、"NONE" と "FAILED" の両方を含めます。
- 別のレプリケート先にレプリケートされたオブジェクトをレプリケート先バケットにバックフィルするには、"COMPLETED" を含めます。
- 以前にレプリケートオブジェクトをレプリケートするには、"REPLICA" を含めます。

バッチレプリケーション完了レポート

バッチレプリケーションジョブを作成するときに、CSV 完了レポートをリクエストできます。このレポートには、オブジェクト、レプリケーションの成功コードまたは失敗コード、出力、および説明が表示されます。ジョブの追跡と完了レポートの追跡については、「完了レポート」を参照してください。

レプリケーション失敗コードのリストと説明については、「Amazon S3 レプリケーションの失敗の理由」を参照してください。

バッチレプリケーションのトラブルシューティングについては、「バッチレプリケーションエラー」を参照してください。

バッチレプリケーションの使用開始

バッチレプリケーションの使用方法の詳細については、「チュートリアル: S3 バッチレプリケーションによる Amazon S3 バケット内の既存のオブジェクトのレプリケーション」を参照してください。

S3 バッチレプリケーション用の IAM ロールの設定

Amazon S3 バッチレプリケーションはバッチオペレーションジョブの一種であるため、AWS Identity and Access Management (IAM) ロールを作成し、ユーザーに代わってアクションを実行するためのバッチオペレーション許可を付与する必要があります。また、バッチレプリケーション IAM ポリシーをバッチオペレーション IAM ロールにアタッチする必要があります。

次の手順を使用して、バッチレプリケーションジョブを開始するバッチオペレーションの許可を与えるポリシーと IAM ロールを作成します。

バッチレプリケーションのポリシーを作成するには

1. AWS Management Console にサインインして、IAM コンソール https://console.aws.amazon.com/iam/ を開きます。
2. [アクセス管理] で、[ポリシー] を選択します。
3. [Create policy] (ポリシーの作成) を選択します。
4. [アクセス許可の指定] ページで、[JSON] を選択します。
5. マニフェストが Amazon S3 によって生成されるか、独自のマニフェストを提供するかに応じて、次のいずれかのポリシーを挿入します。マニフェストの詳細については、「バッチレプリケーションジョブのマニフェストの指定」を参照してください。

   これらのポリシーを使用する前に、次のポリシーの *user input placeholders* をレプリケーション元バケット、マニフェストバケット、および完了レポートバケットの名前に置き換えます。

   > **Note**
   >
   > バッチレプリケーションの IAM ロールには、マニフェストを生成するか提供するかに応じて異なるアクセス許可が必要です。そのため、次の例から適切なポリシーを選択してください。

   AmazonS3 で生成されたマニフェストを使用して保存する場合のポリシー

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Action":[
            "s3:InitiateReplication"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
         ]
      },
      {
         "Action":[
            "s3:GetReplicationConfiguration",
```

```
            "s3:PutInventoryConfiguration"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket"
         ]
      },
      {
         "Action":[
            "s3:GetObject",
            "s3:GetObjectVersion"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:PutObject"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*",
            "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
         ]
      }
   ]
}
```

ユーザー指定のマニフェストを使用する場合のポリシー

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Action":[
            "s3:InitiateReplication"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
         ]
```

```
      },
            {
         "Action":[
            "s3:GetObject",
            "s3:GetObjectVersion"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:PutObject"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
         ]
      }
   ]
}
```

6. [次へ] を選択します。
7. ポリシーの名前を指定し、[ポリシーの作成] を選択します。

バッチレプリケーションの IAM ロールを作成するには

1. AWS Management Console にサインインして、IAM コンソール https://console.aws.amazon.com/iam/ を開きます。
2. [Access management] (アクセス管理) で、[Roles] (ロール) を選択します。
3. [ロールの作成] を選択してください。
4. 信頼されたエンティティの種類に、[AWS のサービス] を選択します。[ユースケース] セクションで、サービスとして [S3]、ユースケースとして [S3 バッチオペレーション] を選択します。
5. [次へ] を選択します。[アクセス許可を追加] ページが表示されます。検索ボックスで、前述の手順で作成したポリシーを検索します。ポリシー名の横にあるチェックボックスにチェックを入れてから、[次へ] を選択します。
6. [名前、確認および作成] ページで、IAM ロールに名前を指定します。

7. [ステップ 1: 信頼 ID] セクションで、IAM ロールが次の信頼ポリシーを使用していることを確認します。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"batchoperations.s3.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

8. [ステップ 2: アクセス許可を追加する] セクションで、IAM ロールが前に作成したポリシーを使用していることを確認します。
9. [ロールの作成] を選択してください。

新しいレプリケーションルールまたは新しいレプリケート先にバッチレプリケーションジョブを作成する

Amazon S3 では、ライブレプリケーションは、レプリケーション設定を作成する前にレプリケート元バケットに既に存在していたオブジェクトをレプリケートしません。ライブレプリケーションは、レプリケーション設定の作成後にバケットに書き込まれた新しいオブジェクトと更新されたオブジェクトのみを自動的にレプリケートします。既存のオブジェクトをレプリケートするには、S3 バッチレプリケーションを使用して、これらのオブジェクトをオンデマンドでレプリケートできます。

新しいライブレプリケーション設定で最初のルールを作成する場合、または Amazon S3 コンソールを介して新しいレプリケート先バケットを既存のレプリケーション設定に追加する場合は、オプションでバッチレプリケーションジョブを作成できます。このバッチレプリケーションジョブを使用して、レプリケート元バケット内の既存のオブジェクトをレプリケート先バケットにレプリケートできます。

既存の設定に対して、新しいレプリケート先バケットを追加せずにバッチレプリケーションを使用するには、「既存のレプリケーションルールのバッチレプリケーションジョブを作成する」を参照してください。

前提条件

バッチオペレーションジョブを作成する前に、バッチオペレーション AWS Identity and Access Management (IAM) ロールを作成し、ユーザーに代わってアクションを実行するための Amazon S3 許可を付与する必要があります。詳細については、「S3 バッチレプリケーション用の IAM ロールの設定」を参照してください。

Amazon S3 コンソールを介して新しいレプリケーションルールまたはレプリケート先にバッチレプリケーションを使用する

新しいレプリケーション設定で最初のルールを作成する場合、または Amazon S3 コンソールを介して新しいレプリケート先バケットを既存の設定に追加する場合は、バッチレプリケーションジョブを作成してレプリケート元バケットで既存のオブジェクトをレプリケートできます。

レプリケーション設定を作成または更新するときにバッチレプリケーションジョブを作成するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。
3. [汎用バケット] リストで、レプリケートするオブジェクトが含まれるバケットの名前を選択します。
4. 新しいレプリケーションルールを作成するか、既存のルールを編集するには、[管理] を選択し、下へスクロールして [レプリケーションルール] を選択します。
   - 新しいレプリケーションルールを作成するには、[レプリケーションルールの作成] を選択します。ベーシックレプリケーションルールのセットアップ方法の例については、「ライブレプリケーションの設定例」を参照してください。
   - 既存のバックアップルールを編集するには、ルール名の隣にあるオプションボタンを選択してから、[編集] を選択します。
5. 新しいレプリケーションルールを作成するか、既存のレプリケーションルールのレプリケーション先を編集して、[保存] を選択します。

   新しいレプリケーション設定で最初のルールを作成した後、または既存の設定を編集して新しいレプリケート先を追加すると、[Replicate existing objects?] (既存のオブジェクトをレプリケーションしますか?) ダイアログが表示され、バッチレプリケーションジョブを作成するオプションが表示されます。
6. このジョブを今すぐ作成して実行する場合は、[はい、既存のオブジェクトをレプリケートする] を選択します。

バッチレプリケーションジョブを後で作成するには、[いいえ、既存のオブジェクトをレプリケートしない を選択します。

7. [はい、既存のオブジェクトをレプリケートする] を選択すると、[バッチオペレーションの作成ジョブ] ページが表示されます。S3 バッチレプリケーションジョブには、次の設定があります。

ジョブ実行オプション

S3 バッチレプリケーションジョブをすぐに実行する場合は、[準備ができたジョブを自動的に実行] を選択します。後でジョブを実行する場合は、[ジョブの準備ができるまで実行を待機] 選択します。

> **Note**
>
> [準備ができたジョブを自動的に実行] を選択すると、バッチオペレーションマニフェストを作成および保存することはできません。バッチオペレーションマニフェストを保存するには、[ジョブの準備ができるまで実行を待機] を選択します。

バッチオペレーションマニフェスト

[ジョブの準備ができるまで実行を待機] を選択した場合、[バッチオペレーションマニフェスト] セクションが表示されます。マニフェストとは、指定されたアクションを実行するすべてのオブジェクトのリストです。マニフェストを保存することもできます。S3 インベントリファイルと同様に、マニフェストは CSV ファイルとして保存され、バケットに保存されます。バッチオペレーションマニフェストの詳細については、「マニフェストの指定」を参照してください。

完了レポート

S3 バッチオペレーションは、マニフェストで指定された各オブジェクトに対して 1 つのタスクを実行します。完了レポートは、追加の設定を必要としない統合形式でタスクの結果を表示する簡単な方法です。すべてのタスクまたは失敗したタスクについてのみ完了レポートをリクエストできます。完了レポートの詳細については、「完了レポート」を参照してください。

アクセス許可

レプリケーション失敗の最も一般的な原因の 1 つは、提供されている AWS Identity and Access Management (IAM) ロールの権限が不十分であることです。このロールの作成の詳細については、「S3 バッチレプリケーション用の IAM ロールの設定」を参照してください。バッチレプリケーションに必要なアクセス許可を持つ IAM ロールを作成または選択します。

8. [保存] を選択します。

既存のレプリケーションルールのバッチレプリケーションジョブを作成する

Amazon S3 では、ライブレプリケーションは、レプリケーション設定を作成する前にレプリケート元バケットに既に存在していたオブジェクトをレプリケートしません。ライブレプリケーションは、レプリケーション設定の作成後にバケットに書き込まれた新しいオブジェクトと更新されたオブジェクトのみを自動的にレプリケートします。既存のオブジェクトをレプリケートするには、S3 バッチレプリケーションを使用して、これらのオブジェクトをオンデマンドでレプリケートできます。

AWS SDK、AWS Command Line Interface (AWS CLI)、Simple Storage Service (Amazon S3) コンソールを使用して、既存のレプリケーション設定に S3 バッチレプリケーションを設定できます。バッチレプリケーションの概要については、「バッチレプリケーションを使用した既存のオブジェクトのレプリケーション」を参照してください。

バッチレプリケーションジョブが終了すると、完了レポートが表示されます。レポートを使用してジョブを検査する方法の詳細については、「ジョブステータスと完了レポートの追跡」を参照してください。

前提条件

バッチオペレーションジョブを作成する前に、バッチオペレーション AWS Identity and Access Management (IAM) ロールを作成し、ユーザーに代わってアクションを実行するための Amazon S3 許可を付与する必要があります。詳細については、「S3 バッチレプリケーション用の IAM ロールの設定」を参照してください。

S3 コンソールの使用

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 左のナビゲーションペインで、[バッチ操作] を選択します。
3. [ジョブの作成] を選択します。

4. [AWS リージョン] セクションに、ジョブを作成するリージョンが表示されていることを確認します。
5. [マニフェスト] セクションで、使用するマニフェスト形式を指定します。マニフェストとは、指定されたアクションを実行するすべてのオブジェクトのリストです。バッチオペレーションマニフェストの詳細については、「マニフェストの指定」を参照してください。

   - マニフェストの準備ができている場合は、S3 インベントリレポート manifest.jsonまたはCSV。マニフェストがバージョニングされたバケットにある場合は、マニフェストのバージョン ID を指定できます。バージョン ID を指定しない場合、バッチオペレーションはマニフェストの最新バージョンを使用します。マニフェストの作成の詳細については、「マニフェストの指定」を参照してください。

     > **Note**
     >
     > マニフェスト内のオブジェクトがバージョニング対応のバケット内にある場合は、そのオブジェクトのバージョン ID を指定する必要があります。詳細については、「マニフェストの指定」を参照してください。

   - レプリケーション構成に基づいてマニフェストを作成するには、[Create manifest using S3 Replication configuration] (S3 レプリケーション設定を使用してマニフェストを作成する) を選択します。レプリケーション設定のレプリケート元バケットを選択します。
6. (オプション) [S3 レプリケーション設定を使用してマニフェストを作成する] を選択した場合は、オブジェクト作成日やレプリケーションステータスなどの追加のフィルターを含めることができます。レプリケーションステータスによるフィルター方法の例については、「バッチレプリケーションジョブのマニフェストの指定」を参照してください。
7. (オプション) [S3 レプリケーション設定を使用してマニフェストを作成する] を選択した場合は、生成されたマニフェストを保存できます。マニフェストを保存するには、[バッチオペレーションマニフェストを保存] を選択します。次に、マニフェストのレプリケート先バケットを指定し、マニフェストを暗号化するかどうかを選択します。

   > **Note**
   >
   > 生成されたマニフェストは、レプリケーション元バケットと同じ AWS リージョンに保存されている必要があります。

8. [次へ] を選択します。
9. [オペレーション] ページで、[レプリケート] を選択し、[次へ] を選択します。

10. (オプション) [Description] (説明) に入力します。
11. 必要に応じて、ジョブの [Priority] (優先度) を調整します。番号が高いほど、優先順位が高いことを表します。Simple Storage Service (Amazon S3) は、優先度の低いジョブの前に優先度の高いジョブを実行しようとします。ジョブの優先度の詳細については、「ジョブの優先度の割り当て」を参照してください。
12. (オプション) 完了レポートを生成します。このレポートを生成するには [完了レポートを生成] を選択します。

    完了レポートを生成する場合は、[Failed tasks only] (失敗したタスクのみ) または [All tasks] (すべてのタスク) をレポートするかを選択肢、レポートのレプリケート先バケットを指定する必要があります。
13. [アクセス許可] セクションで、バッチレプリケーションに必要なアクセス許可を持つ IAM ロールが選択されていることを確認してください。レプリケーション失敗の最も一般的な原因の 1 つは、提供されている (IAM) ロールのアクセス許可が不十分であることです。このロールの作成の詳細については、「S3 バッチレプリケーション用の IAM ロールの設定」を参照してください。
14. (オプション) バッチレプリケーションジョブにジョブタグを追加します。
15. [次へ] を選択します。
16. ジョブの設定を確認し、[ジョブの作成] を選択します。

S3 マニフェストとともに、AWS CLI を使用する

次の `create-job` コマンド例では、S3 が AWS アカウント *111122223333* に生成したマニフェストを使用して S3 バッチレプリケーションジョブを作成します。この例では、既存のオブジェクトと以前にレプリケートに失敗したオブジェクトをレプリケートします。レプリケーションステータスによるフィルタリングの詳細については、「バッチレプリケーションジョブのマニフェストの指定」を参照してください。

このコマンドを使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。IAM ロール `role/`*batch-Replication-IAM-policy* を、以前に作成した IAM ロールに置き換えます。詳細については、「S3 バッチレプリケーション用の IAM ロールの設定」を参照してください。

```
aws s3control create-job --account-id 111122223333 \
--operation '{"S3ReplicateObject":{}}' \
--report '{"Bucket":"arn:aws:s3:::amzn-s3-demo-completion-report-bucket",\
```

```
"Prefix":"batch-replication-report", \
"Format":"Report_CSV_20180820","Enabled":true,"ReportScope":"AllTasks"}' \
--manifest-generator '{"S3JobManifestGenerator": {"ExpectedBucketOwner":
 "111122223333", \
"SourceBucket": "arn:aws:s3:::amzn-s3-demo-source-bucket", \
"EnableManifestOutput": false, "Filter": {"EligibleForReplication": true, \
"ObjectReplicationStatuses": ["NONE","FAILED"]}}}' \
--priority 1 \
--role-arn arn:aws:iam::111122223333:role/batch-Replication-IAM-policy \
--no-confirmation-required \
--region source-bucket-region
```

> **Note**
>
> ジョブは、レプリケーション元バケットと同じ AWS リージョンから開始する必要があります。

バッチレプリケーションジョブを正常に開始すると、応答としてジョブ ID を受け取ります。次の describe-job コマンドを使用して、このジョブをモニタリングできます。このコマンドを使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3control describe-job --account-id 111122223333 --job-id job-id --region source-
bucket-region
```

ユーザー提供のマニフェストとともに AWS CLI を使用する

次の例では、AWS アカウント *111122223333* のユーザー定義のマニフェストを使用して S3 バッチレプリケーションジョブを作成します。マニフェスト内のオブジェクトがバージョニング対応のバケット内にある場合は、そのオブジェクトのバージョン ID を指定する必要があります。マニフェストで指定されたバージョン ID を持つオブジェクトのみがレプリケートされます。マニフェストの作成の詳細については、「マニフェストの指定」を参照してください。

このコマンドを使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。IAM ロール role/*batch-Replication-IAM-policy* を、以前に作成した IAM ロールに置き換えます。詳細については、「S3 バッチレプリケーション用の IAM ロールの設定」を参照してください。

```
aws s3control create-job --account-id 111122223333 \
```

```
--operation '{"S3ReplicateObject":{}}' \
--report '{"Bucket":"arn:aws:s3:::amzn-s3-demo-completion-report-bucket",\
"Prefix":"batch-replication-report", \
"Format":"Report_CSV_20180820","Enabled":true,"ReportScope":"AllTasks"}' \
--manifest '{"Spec":{"Format":"S3BatchOperations_CSV_20180820",\
"Fields":["Bucket","Key","VersionId"]},\
"Location":{"ObjectArn":"arn:aws:s3:::amzn-s3-demo-manifest-bucket/manifest.csv",\
"ETag":"Manifest Etag"}}' \
--priority 1 \
--role-arn arn:aws:iam::111122223333:role/batch-Replication-IAM-policy \
--no-confirmation-required \
--region source-bucket-region
```

> **Note**
>
> ジョブは、レプリケーション元バケットと同じ AWS リージョンから開始する必要があります。

バッチレプリケーションジョブを正常に開始すると、応答としてジョブ ID を受け取ります。次の describe-job コマンドを使用して、このジョブをモニタリングできます。

```
aws s3control describe-job --account-id 111122223333 --job-id job-id --region source-bucket-region
```

レプリケーションのトラブルシューティング

このセクションでは、Amazon S3 レプリケーションのトラブルシューティングのヒントと S3 バッチレプリケーションエラーに関する情報を一覧で示します。

トピック

- S3 レプリケーションのトラブルシューティングのヒント
- バッチレプリケーションエラー

S3 レプリケーションのトラブルシューティングのヒント

レプリケーションを設定した後にオブジェクトレプリカがレプリケート先バケットに表示されない場合は、これらのトラブルシューティングのヒントを使用して問題を特定し、修正してください。

- 大部分のオブジェクトは、15 分以内にレプリケートされます。Amazon S3 がオブジェクトをレプリケートするために要する時間は、さまざまな要因に依存します (レプリケート元とレプリケート先のリージョンペア、オブジェクトのサイズなど)。大きなオブジェクトの場合は、レプリケーションには最大で数時間かかることもあります。レプリケート時間を可視化するには、S3 Replication Time Control (S3 RTC) を使用できます。

  レプリケートされているオブジェクトが大きい場合は、レプリケート先バケットに表示されるかどうかを確認する前に、少しの間待機してください。また、レプリケート先オブジェクトのレプリケーションの状態を確認できます。オブジェクトのレプリケーションステータスが PENDING の場合は、Amazon S3 がレプリケーションを完了していません。オブジェクトのレプリケーションの状態が FAILED の場合は、レプリケート元バケットのレプリケーション設定を確認してください。

  さらに、レプリケーション中の失敗についての情報を受信するには、Amazon S3 イベント通知レプリケーションを設定することで失敗イベントを受信できます。詳細については、「Amazon S3 イベント通知によるレプリケーション失敗イベントの受信」を参照してください。
- オブジェクトのレプリケーションの状態を確認するには、HeadObject API オペレーションを呼び出します。HeadObject API オペレーションは、PENDING、COMPLETED、または FAILED で、オブジェクトのレプリケーションの状態を返します。HeadObject API コールへの応答では、レプリケーションの状態が x-amz-replication-status ヘッダーで返されます。

  > **Note**
  >
  > HeadObject を実行するには、リクエストするオブジェクトへの読み取りアクセス権が必要です。HEAD リクエストには、GET リクエストと同じオプションがあり、GET オペレーションは実行されません。例えば、AWS Command Line Interface (AWS CLI) を使用して HeadObject リクエストを実行するには、次のコマンドを実行します。*user input placeholders* を、ユーザー自身の情報に置き換えます。
  >
  > ```
  > aws s3api head-object --bucket amzn-s3-demo-source-bucket --key index.html
  > ```
- HeadObject が FAILED のレプリケーション状態のオブジェクトを返した場合、S3 バッチレプリケーションを使用して、失敗したオブジェクトをレプリケートできます。詳細については、「the section called “既存のオブジェクトのレプリケーション”」を参照してください。また、失敗したオブジェクトをレプリケート元バケットに再アップロードできます。これにより、新しいオブジェクトに対するレプリケーションが開始されます。
- レプリケート元バケットのレプリケーション設定について、以下を確認します。

  - レプリケート先バケットの Amazon リソースネーム (ARN) が正しい。
  - キー名のプレフィックスが正しい。たとえば、Tax というプレフィックスが付いたオブジェクトをレプリケートする設定にした場合、Tax/document1 や Tax/document2 のようなキー名のオブジェクトのみがレプリケートされます。キー名が "document3" のオブジェクトはレプリケートされません。
  - レプリケーションルールの状態は Enabled です。
- レプリケーション設定で、どのバケットでもバージョニングが一時停止されていないことを確認します。レプリケート元とレプリケート先の両方のバケットで、バージョニングを有効にする必要があります。
- レプリケーションルールが [オブジェクト所有権をレプリケート先バケット所有者に変更] に設定されている場合、レプリケーションに使用する AWS Identity and Access Management (IAM) ロールに s3:ObjectOwnerOverrideToBucketOwner 権限が必要です。この権限はリソース (この場合はレプリケート先バケット) に付与されます。例えば、次の Resource ステートメントは、レプリケート先バケットにこの権限を付与する方法を示しています。

```
{
  "Effect":"Allow",
  "Action":[
    "s3:ObjectOwnerOverrideToBucketOwner"
  ],
  "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
}
```

- レプリケート先バケットを他のアカウントが所有している場合、レプリケート先バケットの所有者は、レプリケート先バケットポリシーにより、レプリケート元バケットの所有者に対しても s3:ObjectOwnerOverrideToBucketOwner 権限を付与する必要があります。次の例のバケットポリシーを使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
{
  "Version": "2012-10-17",
  "Id": "Policy1644945280205",
  "Statement": [
    {
      "Sid": "Stmt1644945277847",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789101:role/s3-replication-role"
      },
```

```
      "Action": [
        "s3:ReplicateObject",
        "s3:ReplicateTags",
        "s3:ObjectOwnerOverrideToBucketOwner"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    }
  ]
}
```

> **Note**
>
> レプリケート先バケットのオブジェクト所有権設定に [バケット所有者の強制] が含まれている場合は、レプリケーションルールの [オブジェクト所有権をレプリケート先バケット所有者に変更] 設定を更新する必要はありません。オブジェクトの所有権の変更はデフォルトで行われます。レプリカの所有権の変更の詳細については、「レプリカ所有者の変更」を参照してください。

- レプリケート元バケットとレプリケート先バケットが異なる AWS アカウントによって所有されているクロスアカウントシナリオでレプリケーション設定を行っている場合、レプリケート先バケットをリクエスタ支払いバケットに設定することはできません。詳細については、「ストレージの転送と使用にリクエスタ支払い汎用バケットを使用する」を参照してください。
- バケットのレプリケート先オブジェクトが AWS Key Management Service (AWS KMS) キーを使用したサーバー側暗号化 (SSE-KMS) を使用して暗号化されている場合、AWS KMS で暗号化されたオブジェクトが含まれるようにレプリケーションルールを設定する必要があります。Amazon S3 コンソールの暗号化設定で、必ず [AWS KMS で暗号化されたオブジェクトをレプリケートする] を選択してください。次に、レプリケート先オブジェクトを暗号化するための AWS KMS キーを選択します。

> **Note**
>
> レプリケート先バケットが別のアカウントにある場合は、レプリケート先アカウントが所有する AWS KMS カスタマーマネージドキーを指定します。デフォルトの Amazon S3 マネージドキー (aws/s3) は使用しないでください。デフォルトのキーを使用すると、レプリケート元アカウントが所有する Amazon S3 マネージドキーでオブジェクトが暗号化され、オブジェクトが別のアカウントと共有されるのを防ぎます。その結果、レプリケート先アカウントはレプリケート先バケット内のオブジェクトにアクセスできなくなります。

レプリケート先アカウントに属する AWS KMS キーを使用してレプリケート先オブジェクトを暗号化するには、レプリケート先アカウントによって KMS キーポリシーのレプリケーションロールに kms:GenerateDataKey および kms:Encrypt 権限を付与する必要があります。次の例のステートメントを KMS キーポリシーで使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
{
    "Sid": "AllowS3ReplicationSourceRoleToUseTheKey",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::123456789101:role/s3-replication-role"
    },
    "Action": ["kms:GenerateDataKey", "kms:Encrypt"],
    "Resource": "*"
}
```

AWS KMS キーポリシーの Resource ステートメントにアスタリスク (*) を使用すると、そのポリシーは KMS キーの使用権限をレプリケーションロールのみに付与します。このポリシーでは、レプリケーションロールの権限の昇格は許可していません。

デフォルトでは、KMS キーポリシーによって、キーに対するすべての権限をルートユーザーに付与します。この権限は、同じアカウントの他のユーザーに委任できます。ソース KMS キーポリシーに Deny ステートメントがない限り、IAM ポリシーを使用してレプリケーションロールにソース KMS キーへのアクセス権限を付与するだけで十分です。

> **Note**
>
> 特定の CIDR 範囲、仮想プライベートクラウド (VPC) エンドポイント、S3 アクセスポイントへのアクセスを制限する KMS キーポリシーにより、レプリケーションが失敗する可能性があります。

レプリケート元またはレプリケート先の KMS キーのいずれかが、暗号化コンテキストに基づいてアクセス権限を付与する場合は、Amazon S3 バケットキーがバケットに対して有効になっていることを確認します。バケットで S3 バケットキーが有効になっている場合、暗号化コンテキストは次のようなバケットレベルのリソースである必要があります。

```
"kms:EncryptionContext:arn:aws:arn": [
     "arn:aws:s3:::amzn-s3-demo-source-bucket"
     ]
"kms:EncryptionContext:arn:aws:arn": [
     "arn:aws:s3:::amzn-s3-demo-destination-bucket"
     ]
```

KMS キーポリシーによって付与されるアクセス権限に加えて、レプリケート元アカウントは、レプリケーションロールの IAM ポリシーに次の最小限必要なアクセス権限を追加する必要があります。

```
{
    "Effect": "Allow",
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
    ],
    "Resource": [
        "Source-KMS-Key-ARN"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "kms:GenerateDataKey",
        "kms:Encrypt"
    ],
    "Resource": [
        "Destination-KMS-Key-ARN"
    ]
}
```

AWS KMS で暗号化されたオブジェクトをレプリケートする方法の詳細については、「暗号化オブジェクトのレプリケート」を参照してください。

- レプリケート先バケットが他の AWS アカウントによって所有されている場合、バケット所有者が、レプリケート元バケットの所有者に対してオブジェクトのレプリケーションを許可するバケットポリシーをレプリケート先バケットに設定していることを確認します。例については、異なるアカウントでのバケットのレプリケーション設定を参照してください。

- レプリケーションでオブジェクトロックを使用するには、レプリケーションの設定に使用する AWS Identity and Access Management (IAM) ロールで、ソース S3 バケットに対する 2 つの追加のアクセス許可を付与する必要があります。2 つの新しいアクセス許可とは `s3:GetObjectRetention` と `s3:GetObjectLegalHold` です。ロールに `s3:Get*` アクセス許可がある場合、そのステートメントは要件を満たしています。詳細については、「the section called “S3 レプリケーションでのオブジェクトロックの使用”」を参照してください。
- 権限を検証してもオブジェクトがレプリケートされない場合は、次の場所に明示的な Deny ステートメントがないかを確認してください。
  - レプリケート先またはレプリケート先バケットポリシーにおける Deny ステートメント。バケットポリシーで次のいずれかのアクションでレプリケーションのロールへのアクセスを拒否した場合、レプリケーションは失敗します。

    レプリケート元のバケット

    ```
            "s3:GetReplicationConfiguration",
            "s3:ListBucket",
            "s3:GetObjectVersionForReplication",
            "s3:GetObjectVersionAcl",
            "s3:GetObjectVersionTagging"
    ```

    レプリケート先バケット:

    ```
            "s3:ReplicateObject",
            "s3:ReplicateDelete",
            "s3:ReplicateTags"
    ```

  - IAM ロールにアタッチされた Deny ステートメントまたはアクセス許可の境界により、レプリケーションが失敗する可能性があります。
  - レプリケート元アカウントまたはレプリケート先アカウントのいずれかにアタッチされた AWS Organizations サービスコントロールポリシー (SCP) の Deny ステートメントが原因で、レプリケーションが失敗する可能性があります。
  - レプリケート元バケットまたはレプリケート先バケットのいずれかにアタッチされた AWS Organizations リソースコントロールポリシー (RCP) の Deny ステートメントが原因で、レプリケーションが失敗する場合があります。
- レプリケート先バケットにオブジェクトのレプリカが表示されない場合、次の問題でレプリケーションを妨げている可能性があります。

  - レプリケート元バケットのオブジェクト自体が別のレプリケーション設定によって作成されたレプリカである場合、Amazon S3 はそのオブジェクトをレプリケートしません。例えば、バケット A からバケット B へ、バケット B からバケット C へのレプリケーション設定を設定した場合、Amazon S3 はバケット B にあるオブジェクトレプリカをバケット C へレプリケートしません。
  - レプリケート元バケット所有者は、オブジェクトをアップロードするための許可を他の AWS アカウントに付与できます。デフォルトでは、レプリケート元バケット所有者は、他のアカウントによって作成されたオブジェクトに対するアクセス許可を持ちません。レプリケーション設定では、レプリケート元バケット所有者がアクセス許可を持つオブジェクトのみがレプリケートされます。この問題を回避するために、レプリケート元バケット所有者は、条件付きでオブジェクトを作成するための他の AWS アカウントアクセス許可を付与し、それらのオブジェクトに対する明示的なアクセス許可を要求することができます。ポリシーの例については[バケット所有者はフルコントロール権限を持ちながら、オブジェクトをアップロードするためのクロスアカウントアクセス許可を付与する]を参照してください。

- レプリケーション設定に、特定のタグを持つオブジェクトのサブセットをレプリケートするためのルールを追加するとします。この場合、Amazon S3 がオブジェクトをレプリケートするには、オブジェクトの作成時に特定のタグキーと値を割り当てる必要があります。まず、オブジェクトを作成して、それから既存のオブジェクトにタグを追加した場合、Amazon S3 はそのオブジェクトをレプリケートしません。
- Amazon S3 イベント通知を使用すると、オブジェクトがレプリケート先の AWS リージョンにレプリケートされない場合に通知します。Amazon S3 イベント通知は、Amazon Simple Queue Service (Amazon SQS)、Amazon Simple Notification Service (Amazon SNS)、または AWS Lambda を通じて使用できます。詳細については、「[Amazon S3 イベント通知によるレプリケーション失敗イベントの受信]」を参照してください。

  また、Amazon S3 イベント通知を使用して、レプリケーションの失敗の理由を確認できます。失敗理由のリストを確認するには、「[Amazon S3 レプリケーションの失敗の理由]」を参照してください。

バッチレプリケーションエラー

レプリケート先バケットにレプリケートされないオブジェクトをトラブルシューティングするには、バケット、レプリケーションロール、バッチレプリケーションジョブの作成に使用した IAM ロールのさまざまなタイプのアクセス許可を確認します。また、ブロックパブリックアクセス設定とバケットの S3 オブジェクトの所有権設定を必ず確認してください。

バッチオペレーションの使用に関するトラブルシューティングのその他のヒントについては、「the section called “バッチオペレーションのトラブルシューティング”」を参照してください。

レプリケーションを設定していて、オブジェクトがレプリケートされていない場合は、AWS re:Post ナレッジセンターの「バケット間のレプリケーションを設定したにもかかわらず、Amazon S3 オブジェクトがレプリケートされない理由を知りたいです。」を参照してください。

バッチレプリケーションの使用中に、次のいずれかのエラーが発生する可能性があります。

- マニフェストの生成で、フィルター条件に一致するキーが見つかりませんでした。

  このエラーは、以下のいずれかの原因で発生することがあります。

  - レプリケート元バケット内のオブジェクトが S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive のストレージクラスに保存されている場合。

    これらのオブジェクトでバッチレプリケーションを使用するには、まず、バッチオペレーションジョブで [復元] (`S3InitiateRestoreObjectOperation`) オペレーションを使用して、オブジェクトを S3 標準ストレージクラスに復元します。詳細については、「アーカイブされたオブジェクトの復元」および「オブジェクトの復元 (バッチオペレーション)」を参照してください。オブジェクトの復元後、バッチレプリケーションジョブを使用してオブジェクトをレプリケートできます。

  - 指定したフィルター条件がソースバケット内の有効なオブジェクトと一致しない場合。

    フィルター条件を確認して修正します。例えば、バッチレプリケーションルールにおいて、フィルター条件によってレプリケート元バケット内でプレフィックス `Tax/` を持つすべてのオブジェクトを検索するとします。プレフィックス名が誤って入力され、スラッシュが末尾だけでなく先頭と末尾の両方にある場合 (`/Tax/`)、S3 オブジェクトは見つかりません。このエラーを解決するには、レプリケーションルールのプレフィックスを `/Tax/` から `Tax/` に修正します。

- バッチオペレーションの状態は失敗です。理由: ジョブレポートをレポートバケットに書き込めませんでした。

  このエラーは、バッチオペレーションジョブに使用される IAM ロールが、ジョブの作成時に指定された場所に完了レポートを保存できない場合に発生します。このエラーを解決するには、バッチオペレーションの完了レポートを保存するバケットの `s3:PutObject` アクセス許可が IAM ロールにあることを確認します。レプリケート元バケットとは異なるバケットにレポートを配信することをお勧めします。

  このエラーの解決に関するその他のヒントについては、「the section called “アクセス許可の問題があるか、保持モードが有効の場合に、ジョブレポートが配信されない”」を参照してください。

- バッチオペレーションが失敗しました。失敗合計は 0 ではありません。

  このエラーは、実行中のバッチレプリケーションジョブにオブジェクト権限が不十分という問題がある場合に発生します。バッチレプリケーションジョブにレプリケーションルールを使用している場合は、レプリケーションに使用する IAM ロールに、レプリケート元またはレプリケート先のバケットのオブジェクトにアクセスする適切な権限があることを確認します。また、バッチレプリケーション完了レポートで、特定の Amazon S3 レプリケーション失敗の理由を確認できます。
- バッチジョブは正常に実行されましたが、レプリケート先バケットに必要なオブジェクトの数が一致しません。

  このエラーは、バッチレプリケーションジョブで提供されたマニフェストにリストアップされているオブジェクトと、ジョブの作成時に選択したフィルターが一致しない場合に発生します。また、レプリケート元バケット内のオブジェクトがどのレプリケーションルールにも一致せず、生成されたマニフェストに含まれていない場合にもこのメッセージが表示されることがあります。

バッチオペレーションの失敗は、既存のレプリケーション設定に新しいレプリケーションルールを追加した後に発生します

バッチオペレーションは、レプリケート元バケットのレプリケーション設定のすべてのルールに対して、既存オブジェクトのレプリケーションを実行しようとします。既存のレプリケーションルールのいずれかに問題があると、失敗が発生する可能性があります。

バッチオペレーションジョブの完了レポートには、ジョブの失敗理由が説明されています。一般的なエラーのリストについては、「Amazon S3 レプリケーションの失敗の理由」を参照してください。

メトリクス、イベント通知、ステータスによるレプリケーションのモニタリング

以下のメカニズムを使用して、ライブレプリケーション設定と S3 バッチレプリケーションジョブをモニタリングできます。

- S3 レプリケーションメトリクス – S3 レプリケーションメトリクスを有効にすると、Amazon CloudWatch は、保留中のバイト数、保留中のオペレーション、レプリケーションレイテンシーをレプリケーションルールレベルで追跡するために使用できるメトリクスを出力します。S3 レプリケーションメトリクスは、Amazon S3 コンソールと Amazon CloudWatch コンソールから表示できます。Amazon S3 コンソールでは、ソースバケットの [メトリクス] タブでこれらのメトリクスを表示できます。S3 レプリケーションメトリクスの詳細については、「the section called “S3 レプリケーションメトリクスの使用”」を参照してください。

- S3 ストレージレンズメトリクス – S3 レプリケーションメトリクスに加えて、S3 ストレージレンズダッシュボードが提供するレプリケーション関連のデータ保護メトリクスを使用できます。例えば、S3 ストレージレンズの無料のメトリクスを使用すると、ソースバケットからレプリケートされた総バイト数や、ソースバケットからレプリケートされたオブジェクトの数などのメトリクスを表示できます。

  レプリケーションインスタンス全体を監査するには、S3 ストレージレンズで高度なメトリクスを有効にします。S3 ストレージレンズの高度なメトリクスを使用すると、無効なレプリケーション先を持つレプリケーションルールの数など、さまざまなタイプのレプリケーションルールの数を確認できます。

  S3 ストレージレンズでのレプリケーションメトリクスの使用の詳細については、「the section called “S3 ストレージレンズでのレプリケーションメトリクスの表示”」を参照してください。

- S3 イベント通知 – S3 イベント通知は、オブジェクトが宛先の AWS リージョンにレプリケートされない場合や、オブジェクトが特定のしきい値内にレプリケートされない場合に、インスタンスのオブジェクトレベルで通知できます。S3 イベント通知には、`s3:Replication:OperationFailedReplication`、`s3:Replication:OperationMissedThr` および `s3:Replication:OperationNotTracked` のレプリケーションイベントタイプが用意されています。

  Amazon S3 イベントは、Amazon Simple Queue Service (Amazon SQS)、Amazon Simple Notification Service (Amazon SNS)、または AWS Lambda を通じて使用できます。詳細については、「the section called “レプリケーション失敗イベントの受信”」を参照してください。

- レプリケーションステータス値 – オブジェクトのレプリケーションステータスを取得することもできます。レプリケーションステータスは、レプリケートされているオブジェクトの現在の状態を判断するのに役立ちます。レプリケート元オブジェクトのレプリケーションステータスは、`PENDING`、`COMPLETED`または`FAILED`のいずれかを返します。レプリカのレプリケーションステータスが`REPLICA`に返されます。

  S3 バッチレプリケーションジョブを作成するときにも、レプリケーションステータス値を使用することもできます。例えば、これらのステータス値を使用して、レプリケートされたことがない、またはレプリケーションに失敗したオブジェクトをレプリケートできます。

  オブジェクトのレプリケーションステータスの取得の詳細については、「the section called “レプリケーションステータスの取得”」を参照してください。バッチレプリケーションでこれらの値を使用する方法の詳細については、「the section called “バッチレプリケーションジョブのフィルター”」を参照してください。

トピック

- S3 レプリケーションメトリクスの使用
- S3 ストレージレンズでのレプリケーションメトリクスの表示
- Amazon S3 イベント通知によるレプリケーション失敗イベントの受信
- レプリケーションステータス情報の取得

S3 レプリケーションメトリクスの使用

S3 レプリケーションメトリクス は、レプリケーション設定のレプリケーションルールの詳細なメトリクスを提供します。レプリケーションメトリクスを使って、保留中のバイト数、保留中のオペレーション、レプリケーションに失敗したオペレーション、レプリケーションのレイテンシーを追跡すると、レプリケーションの進行状況を 1 分単位でモニタリングできます。

> **Note**
>
> - S3 レプリケーションメトリクスは、Amazon CloudWatch カスタムメトリクスと同じ料金レートで請求されます。詳細については、「Amazon CloudWatch の料金」を参照してください。
> - S3 レプリケーション時間コントロールを使用している場合、Amazon CloudWatch は、各レプリケーションルールで S3 RTC を有効にしてから 15 分後にレプリケーションメトリクスのレポートを開始します。

S3 Replication Time Control (S3 RTC) を有効にすると、S3 レプリケーションメトリクスが自動的にオンになります。ルールを作成または編集するときに、S3 RTC とは独立して S3 レプリケーションメトリクスを有効にすることもできます。S3 RTC には、サービスレベルアグリーメント (SLA) やしきい値の欠落に関する通知など、その他の機能が含まれています。詳細については、「S3 Replication Time Control (S3 RTC)を使用してコンプライアンス要件を満たす」を参照してください。

S3 レプリケーションメトリクスが有効になっている場合、Amazon S3 は次のメトリクスを Amazon CloudWatch に発行します。CloudWatch メトリクスは、ベストエフォートで配信されます。

メトリクス名	メトリクスの説明	このメトリクスはどのオブジェクトに適用されますか。	このメトリクスはどのリージョンで発行されていますか。	レプリケート先バケットが削除された場合でも、このメトリクスは発行されますか。	レプリケーションが行われない場合、このメトリクスは引き続き発行されますか。
レプリケーション保留中のバイト数	特定のレプリケーションルールについて、レプリケーションが保留中のオブジェクトの合計バイト数。	このメトリクスは、S3 クロスリージョンレプリケーション (S3 CRR) または S3 同一リージョンレプリケーション (S3 SRR) でレプリケートされた新しいオブジェクトにのみ適用されます。	このメトリクスは、レプリケート先バケットのリージョンで発行されます。	いいえ	はい
レプリケーションレイテンシー	特定のレプリケーションルールについて、レプリケート先バケットがレプリケート元バケットより遅れる最大秒数。	このメトリクスは、S3 CRR または S3 SRR でレプリケートされた新しいオブジェクトにのみ適用されます。	このメトリクスは、レプリケート先バケットのリージョンで発行されます。	いいえ	はい
レプリケーション保留	特定のレプリケーショ	このメトリクスは、S3	このメトリクスは、レプリ	いいえ	はい

メトリクス名	メトリクスの説明	このメトリクスはどのオブジェクトに適用されますか。	このメトリクスはどのリージョンで発行されていますか。	レプリケート先バケットが削除された場合でも、このメトリクスは発行されますか。	レプリケーションが行われない場合、このメトリクスは引き続き発行されますか。
中のオペレーション	ンルールについて、レプリケーションが保留中のオペレーションの数。このメトリクスは、オブジェクト、削除マーカー、タグ、アクセスコントロールリスト (ACL)、S3 オブジェクトロックに関連するオペレーションを追跡します。	CRR または S3 SRR でレプリケートされた新しいオブジェクトにのみ適用されます。	ケート先バケットのリージョンで発行されます。		

メトリクス名	メトリクスの説明	このメトリクスはどのオブジェクトに適用されますか。	このメトリクスはどのリージョンで発行されていますか。	レプリケート先バケットが削除された場合でも、このメトリクスは発行されますか。	レプリケーションが行われない場合、このメトリクスは引き続き発行されますか。
オペレーション失敗レプリケーション	特定のレプリケーションルールについて、レプリケーションに失敗したオペレーションの数。このメトリクスは、オブジェクト、削除マーカー、タグ、アクセスコントロールリスト (ACL)、Object Lockに関連するオペレーションを追跡します。 [レプリケーションに失敗したオペレーション] は、S3 レプリケーションの失敗を 1 分間隔で集計して追跡しま	このメトリクスは S3 CRR または S3 SRR でレプリケートされる新しいオブジェクトと、S3 バッチレプリケーションでレプリケートされる既存のオブジェクトの両方に適用されます。 **Note** S3 バッチレプリケーションジョブがまった	このメトリクスは、ソースバケットのリージョンで公開されます。	はい	いいえ

メトリクス名	メトリクスの説明	このメトリクスはどのオブジェクトに適用されますか。	このメトリクスはどのリージョンで発行されていますか。	レプリケート先バケットが削除された場合でも、このメトリクスは発行されますか。	レプリケーションが行われない場合、このメトリクスは引き続き発行されますか。
	す。レプリケーションに失敗した特定のオブジェクトとその失敗理由を特定するには、Amazon S3 イベント通知で `OperationFailedReplication` イベントをサブスクライブしてください。詳細については、「Amazon S3 イベント通知によるレプリケーション失敗イベントの受信」を参照してください。	く実行されなかった場合、メトリクスは Amazon CloudWatch に送信されません。例えば、S3 Batch レプリケーションジョブを実行するため			

メトリクス名	メトリクスの説明	このメトリクスはどのオブジェクトに適用されますか。	このメトリクスはどのリージョンで発行されていますか。	レプリケート先バケットが削除された場合でも、このメトリクスは発行されますか。	レプリケーションが行われない場合、このメトリクスは引き続き発行されますか。
		に必要なアクセス許可がない場合、またはレプリケーション設定のタグまたはプレフィックスが一致しない場合、ジョブは実行			

メトリクス名	メトリクスの説明	このメトリクスはどのオブジェクトに適用されますか。	このメトリクスはどのリージョンで発行されていますか。	レプリケート先バケットが削除された場合でも、このメトリクスは発行されますか。	レプリケーションが行われない場合、このメトリクスは引き続き発行されますか。
		されません。			

CloudWatch でこれらのメトリクスを利用する方法については、「the section called “CloudWatch の S3 レプリケーションメトリクス”」を参照してください。

S3 レプリケーションメトリクスの有効化

S3 レプリケーションメトリクスは、新規または既存のレプリケーションルールを使用して開始できます。レプリケーションルールの作成方法の詳細については、「同じアカウントでのバケットのレプリケーションの設定」を参照してください。レプリケーションルールを S3 バケット全体に適用するか、特定のプレフィックスやタグを持つ Amazon S3 オブジェクトに適用するかを選択できます。

このトピックでは、ソースバケットとレプリケーション先バケットが同じまたは異なる AWS アカウント で所有されている場合に、レプリケーション設定で S3 レプリケーションメトリクスを有効にする手順について説明します。

AWS Command Line Interface (AWS CLI) を使用してレプリケーションメトリクスを有効にするには、`Metrics` が有効になっているレプリケート元バケットにレプリケーション設定を追加する必要があります。この設定例では、*`Tax`* というプレフィックスの下にあるオブジェクトがレプリケート先バケットである *`amzn-s3-demo-bucket`* にレプリケートされて、それらのオブジェクトのメトリクスが生成されます。

```
{
    "Rules": [
        {
            "Status": "Enabled",
            "Filter": {
                "Prefix": "Tax"
```

```
            },
            "Destination": {
                "Bucket": "arn:aws:s3:::amzn-s3-demo-bucket",
                "Metrics": {
                    "Status": "Enabled"
                }
            },
            "Priority": 1
        }
    ],
    "Role": "IAM-Role-ARN"
}
```

レプリケーションメトリクスの表示

S3 レプリケーションメトリクスは、Amazon S3 コンソールのソース汎用バケットの [メトリクス] タブで表示できます。これらの Amazon CloudWatch メトリクスは、Amazon CloudWatch コンソールでも使用できます。S3 レプリケーションメトリクスを有効にすると、Amazon CloudWatch は、保留中のバイト数、保留中のオペレーション、レプリケーションレイテンシーをレプリケーションルールレベルで追跡するために使用できるメトリクスを出力します。

Amazon S3 コンソールまたは Amazon S3 REST API を使用して S3 Replication Time Control (S3 RTC) でレプリケーションを有効にすると、S3 レプリケーションメトリクスが自動的にオンになります。ルールを作成または編集するときに、S3 RTC とは独立して S3 レプリケーションメトリクスを有効にすることもできます。

S3 レプリケーション時間コントロールを使用している場合、Amazon CloudWatch は、各レプリケーションルールで S3 RTC を有効にしてから 15 分後にレプリケーションメトリクスのレポートを開始します。詳細については、「S3 レプリケーションメトリクスの使用」を参照してください。

レプリケーションメトリクスは、レプリケーション設定のルール ID を追跡します。レプリケーションルール ID は、プレフィックス、タグ、またはその両方の組み合わせに固有です。

Amazon S3 の CloudWatch メトリクスの詳細については、「Amazon CloudWatch によるメトリクスのモニタリング」を参照してください。

前提条件

S3 レプリケーションメトリクスが有効になっているレプリケーションルールを作成します。詳細については、「the section called “レプリケーションメトリクスの有効化”」を参照してください。

レプリケート元バケットの [メトリクス] タブで S3 レプリケーションメトリクスを表示するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[汎用バケット] を選択します。
3. バケットリストで、レプリケーションメトリクスを取得するオブジェクトが含まれているソースバケットの名前を選択します。
4. [メトリクス] タブをクリックします。
5. [レプリケーションメトリクス] で、メトリクスを表示するレプリケーションルールを選択します。
6. [Display charts (チャートの表示)] を選択します。

   Amazon S3 には、選択したルールの [レプリケーションレイテンシー]、[レプリケーション保留中のバイト数]、[レプリケーションを保留中のオペをレーション]、および [レプリケーションに失敗したオペレーション] のグラフが表示されます。

S3 ストレージレンズでのレプリケーションメトリクスの表示

S3 レプリケーションメトリクスに加えて、S3 ストレージレンズが提供するレプリケーション関連のデータ保護メトリクスを使用できます。S3 ストレージレンズは、オブジェクトストレージの使用状況とアクティビティを組織全体で可視化するために使用できるクラウドストレージの分析機能です。詳細については、「Using S3 Storage Lens to protect your data」(S3 ストレージレンズを使用してデータを保護する) を参照してください。

S3 ストレージレンズには、無料のメトリクスと、追加料金でアップグレードできるアドバンストメトリクスとレコメンデーションの 2 つの階層のメトリクスがあります。アドバンストメトリクスとレコメンデーションをご利用になれば、ストレージに関するインサイトが得られる追加のメトリクスや機能にアクセスできます。S3 Storage Lens の料金の詳細については、「Amazon S3 の料金」を参照してください。

S3 ストレージレンズで無料のメトリクスを使用すると、ソースバケットからレプリケートされた総バイト数や、ソースバケットからレプリケートされたオブジェクトの数などのメトリクスを表示できます。

レプリケーションインスタンス全体を監査するには、S3 ストレージレンズで高度なメトリクスを有効にします。S3 ストレージレンズの高度なメトリクスを使用すると、無効なレプリケーション先を持つレプリケーションルールの数など、さまざまなタイプのレプリケーションルールの数を確認できます。

各階層にあるレプリケーションメトリクスを含む S3 ストレージレンズメトリクスの完全なリストについては、「S3 ストレージレンズのメトリクスに関する用語集」を参照してください。

前提条件

ライブレプリケーション設定または S3 バッチレプリケーションジョブを作成します。

Amazon S3 ストレージレンズでレプリケーションメトリクスを表示するには

1. S3 ストレージレンズダッシュボードを作成します。手順については、「the section called “S3 コンソールの使用”」を参照してください。
2. (オプション) ダッシュボードの設定中に、すべての S3 ストレージレンズレプリケーションメトリクスを表示するには、[高度なメトリクスとレコメンデーション] を選択し、[高度なデータ保護メトリクス] を選択します。メトリクスの完全なリストについては、「Amazon S3 Storage Lens のメトリクスに関する用語集」を参照してください。

   高度なメトリクスとレコメンデーションを有効にすると、レプリケーション設定に関する詳細なインサイトを得ることができます。例えば、S3 ストレージレンズのレプリケーションルール数メトリクスを使用して、レプリケーション用に設定されているバケットに関する詳細な情報を取得できます。この情報には、バケット内とリージョン内およびバケット間とリージョン間のレプリケーションルールが含まれます。詳細については、「the section called “各バケットのレプリケーションルールの総数を数える”」を参照してください。
3. ダッシュボードを作成したら、ダッシュボードを開き、[バケット] タブを選択します。
4. [Buckets] (バケット) セクションまで下にスクロールします。[Metrics categories] (メトリクスのカテゴリ) で、[Data protection] (データ保護) を選択します。次に、[Summary] (概要) を選択解除します。
5. [バケット] リストをフィルタリングしてレプリケーションメトリクスのみを表示するには、設定アイコン
   ( )
   を選択します。
6. レプリケーションメトリクスだけが選択された状態になるまで、他のすべてのデータ保護メトリクスを選択解除します。
7. (オプション) [Page size] (ページサイズ) で、リストに表示するバケットの数を選択します。
8. [続行] をクリックしてください。

Amazon S3 イベント通知によるレプリケーション失敗イベントの受信

レプリケーション設定で S3 レプリケーションメトリクスを有効にしている場合は、Amazon S3 イベント通知を設定して、オブジェクトが宛先 AWS リージョンにレプリケートされない場合に通知を受けることができます。レプリケーション設定で S3 Replication Time Control (S3 RTC) を有効にしている場合、レプリケーションの 15 分間の S3 RTC しきい値内にオブジェクトがレプリケートされない場合にも通知を受け取ることができます。

次の Replication イベントタイプを使用すると、保留中のバイト数、保留中のオペレーション、およびレプリケーションのレイテンシーを追跡すると、レプリケーションイベントの進行状況を 1 分単位でモニタリングできます。S3 レプリケーションメトリクスの詳細については、「S3 レプリケーションメトリクスの使用」を参照してください。

- -s3:Replication:OperationFailedReplicationイベントタイプは、レプリケーションのターゲットであったオブジェクトがレプリケートに失敗したときに通知を受け取ります。
- s3:Replication:OperationMissedThreshold イベントタイプは、S3 RTC を使用するレプリケーションの対象であったオブジェクトがレプリケーションの 15 分の閾値を超えたときに通知します。
- s3:Replication:OperationReplicatedAfterThreshold イベントタイプは、S3 RTC を使用するレプリケーションの対象であったオブジェクトが 15 分の閾値を超えてレプリケートされたときに通知します。
- s3:Replication:OperationNotTracked イベントタイプは、ライブレプリケーションの対象であったオブジェクト (同一リージョンレプリケーション [SRR] またはクロスリージョンレプリケーション [CRR]) がレプリケーションメトリクスによって追跡されなくなったときに通知します。

サポートされているすべてのレプリケーションイベントタイプの詳細な説明については、「the section called “SQS、SNS、および Lambda でサポートされているイベントタイプ”」を参照してください。

S3 イベント通知によってキャプチャされた失敗コードのリストについては、「Amazon S3 レプリケーションの失敗の理由」を参照してください。

S3 イベント通知は、Amazon Simple Queue Service (Amazon SQS)、Amazon Simple Notification Service (Amazon SNS)、または AWS Lambda を使用して受信できます。詳細については、「the section called “Amazon S3 イベント通知”」を参照してください。

Amazon S3 イベント通知を設定する手順については、Enabling event notifications を参照してください。

> **Note**
>
> イベント通知を有効にするだけでなく、S3 レプリケーションメトリクスも有効にしてください。詳細については、「the section called “レプリケーションメトリクスの有効化”」を参照してください。

次は Amazon S3 が s3:Replication:OperationFailedReplication イベントを発行するために送信するメッセージの例です。詳細については、「the section called “イベントメッセージの構造”」を参照してください。


```
{
  "Records": [
    {
      "eventVersion": "2.2",
      "eventSource": "aws:s3",
      "awsRegion": "us-east-1",
      "eventTime": "2024-09-05T21:04:32.527Z",
      "eventName": "Replication:OperationFailedReplication",
      "userIdentity": {
        "principalId": "s3.amazonaws.com"
      },
      "requestParameters": {
        "sourceIPAddress": "s3.amazonaws.com"
      },
      "responseElements": {
        "x-amz-request-id": "123bf045-2b4b-4ca8-a211-c34a63c59426",
        "x-amz-id-2":
 "12VAWNDIHnwJsRhTccqQTeAPoXQmRt22KkewMV8G3XZihAuf9CLDdmkApgZzudaIe2KlLfDqGS0="
      },
      "s3": {
        "s3SchemaVersion": "1.0",
        "configurationId": "ReplicationEventName",
        "bucket": {
          "name": "amzn-s3-demo-bucket1",
          "ownerIdentity": {
            "principalId": "111122223333"
          },
          "arn": "arn:aws:s3:::amzn-s3-demo-bucket1"
```

```
        },
        "object": {
          "key": "replication-object-put-test.png",
          "size": 520080,
          "eTag": "e12345ca7e88a38428305d3ff7fcb99f",
          "versionId": "abcdeH0Xp66ep__QDjR76LK7Gc9X4wKO",
          "sequencer": "0066DA1CBF104C0D51"
        }
      },
      "replicationEventData": {
        "replicationRuleId": "notification-test-replication-rule",
        "destinationBucket": "arn:aws:s3:::amzn-s3-demo-bucket2",
        "s3Operation": "OBJECT_PUT",
        "requestTime": "2024-09-05T21:03:59.168Z",
        "failureReason": "AssumeRoleNotPermitted"
      }
    }
  ]
}
```

Amazon S3 レプリケーションの失敗の理由

次の表は、Amazon S3 レプリケーションが失敗した理由を示しています。Amazon S3 イベント通知で `s3:Replication:OperationFailedReplication` イベントを受信し、`failureReason` 値を見ると、これらの理由を確認できます。

失敗の理由は、S3 バッチレプリケーション完了レポートでも確認できます。詳細については、「バッチレプリケーション完了レポート」を参照してください。

レプリケーションの失敗の理由	説明
`AssumeRoleNotPermitted`	Amazon S3 は、レプリケーション設定またはバッチオペレーションジョブで指定された AWS Identity and Access Management (IAM) ロールを引き受けることができません。
`DstBucketInvalidRegion`	宛先バケットがバッチオペレーションジョブで指定されたのと同じ AWS リージョンにありません。このエラーはバッチレプリケーションに固有のものです。

レプリケーションの失敗の理由	説明
DstBucketNotFound	Amazon S3 は、レプリケーション設定で指定されたレプリケート先バケットを見つけることができません。
DstBucketObjectLockConfigMissing	オブジェクトロックが有効になっているレプリケート元バケットからオブジェクトをレプリケートするには、レプリケート先バケットでもオブジェクトロックが有効になっている必要があります。このエラーは、レプリケート先バケットでオブジェクトロックが有効になっていない可能性があることを示しています。詳細については、「オブジェクトロックの考慮事項」を参照してください。
DstBucketUnversioned	S3 レプリケート先バケットでバージョニングが有効になっていません。S3 レプリケーションでオブジェクトをレプリケートするには、レプリケート先バケットのバージョニングを有効にします。
DstDelObjNotPermitted	Amazon S3 は、レプリケート先バケットに削除マーカーをレプリケートできません。レプリケート先バケットに対する s3:ReplicateDelete 権限がない可能性があります。
DstKmsKeyInvalidState	レプリケート先バケットの AWS Key Management Service (AWS KMS) キーが無効な状態です。必要な AWS KMS キーを確認して有効にします。AWS KMS キーの管理について詳しくは、AWS Key Management Service デベロッパーガイドの「AWS KMS キーのキーステータス」を参照してください。

レプリケーションの失敗の理由	説明
DstKmsKeyNotFound	レプリケーション設定でレプリケート先バケットに設定されている AWS KMS キーは存在しません。
DstMultipartCompleteNotPermitted	Amazon S3 は、レプリケート先バケットでオブジェクトのマルチパートアップロードを完了できません。レプリケート先バケットに対する s3:ReplicateObject 権限がない可能性があります。
DstMultipartInitNotPermitted	Amazon S3 は、レプリケート先バケットへのオブジェクトのマルチパートアップロードを開始できません。レプリケート先バケットに対する s3:ReplicateObject 権限がない可能性があります。
DstMultipartUploadNotPermitted	Amazon S3 は、レプリケート先バケットにマルチパートアップロードオブジェクトをアップロードできません。レプリケート先バケットに対する s3:ReplicateObject 権限がない可能性があります。
DstObjectHardDeleted	S3 バッチレプリケーションでは、レプリケート先バケットからオブジェクトのバージョン ID で削除されたオブジェクトの再レプリケーションはサポートされません。このエラーはバッチレプリケーションに固有のものです。
DstPutAclNotPermitted	Amazon S3 は、レプリケート先バケットにオブジェクトアクセスコントロールリスト (ACL) をレプリケートできません。レプリケート先バケットに対する s3:ReplicateObject 権限がない可能性があります。

レプリケーションの失敗の理由	説明
DstPutLegalHoldNotPermitted	イミュータブルなオブジェクトをレプリケートしている際は、Amazon S3 ではレプリケート先オブジェクトに Object Lock のリーガルホールドを設定できません。レプリケート先バケットに対する s3:PutObjectLegalHold 権限がない可能性があります。詳細については、「リーガルホールド」を参照してください。
DstPutObjectNotPermitted	Amazon S3 は、レプリケート先バケットにオブジェクトをレプリケートできません。これは、レプリケート先バケットに必要なアクセス許可 (s3:ReplicateObject または s3:ObjectOwnerOverrideToBucketOwner アクセス許可) がない場合、または AWS KMS キーポリシーによってソースのレプリケーションロールが宛先バケットで AWS KMS キー (kms:Decrypt および kms:GenerateDataKey* アクション) を使用することが許可されていない場合に発生する可能性があります。
DstPutRetentionNotPermitted	イミュータブルなオブジェクトをレプリケートしている際は、Amazon S3 では送信先オブジェクトに保持期間を設定することができません。レプリケート先バケットに対する s3:PutObjectRetention 権限がない可能性があります。
DstPutTaggingNotPermitted	Amazon S3 は、レプリケート先バケットにオブジェクトタグをレプリケートできません。レプリケート先バケットに対する s3:ReplicateObject 権限がない可能性があります。

レプリケーションの失敗の理由	説明
DstVersionNotFound	Amazon S3 は、メタデータをレプリケートする必要があるレプリケート先バケットで必要なオブジェクトバージョンを見つけることができません。
InitiateReplicationNotPermitted	Amazon S3 は、オブジェクトのレプリケーションを開始できません。バッチオペレーションジョブに対する s3:InitiateReplication 権限がない可能性があります。このエラーはバッチレプリケーションに固有のものです。
SrcBucketInvalidRegion	レプリケート元バケットがバッチオペレーションジョブで指定されたのと同じ AWS リージョンにありません。このエラーはバッチレプリケーションに固有のものです。
SrcBucketNotFound	Amazon S3 はレプリケート元バケットを見つけることができません。
SrcBucketReplicationConfigMissing	Amazon S3 はソースバケットのレプリケーション設定を見つけることができませんでした。

レプリケーションの失敗の理由	説明
SrcGetAclNotPermitted	Amazon S3 は、レプリケート元バケットにあるオブジェクトにアクセスしてレプリケートを行うことができません。レプリケート元バケットオブジェクトに対する s3:GetObjectVersionAcl 権限がない可能性があります。 ソースバケットのオブジェクトは、バケット所有者が所有している必要があります。ACL が有効になっている場合は、[オブジェクト所有権] が [希望するバケット所有者] または [オブジェクトライター] に設定されているかどうかを確認してください。オブジェクト所有権が [希望するバケット所有者] に設定されている場合、バケット所有者がオブジェクト所有者になるためには、ソースバケットオブジェクトに bucket-owner-full-control ACL が必要です。ソースアカウントは、オブジェクト所有権を [バケット所有者の強制] に設定して、ACL を無効にすることで、バケット内のすべてのオブジェクトの所有権を取得できます。
SrcGetLegalHoldNotPermitted	Amazon S3 は S3 オブジェクトロックのリーガルホールド情報にアクセスできません。
SrcGetObjectNotPermitted	Amazon S3 は、レプリケート元バケットにあるオブジェクトにアクセスしてレプリケートを行うことができません。レプリケート元バケットに対する s3:GetObjectVersionForReplication 権限がない可能性があります。
SrcGetRetentionNotPermitted	Amazon S3 は S3 オブジェクトロックの保持期間情報にアクセスできません。

レプリケーションの失敗の理由	説明
SrcGetTaggingNotPermitted	Amazon S3 はレプリケート元バケットのオブジェクトタグ情報にアクセスできません。レプリケート元バケットに対する s3:GetObjectVersionTagging 権限がない可能性があります。
SrcHeadObjectNotPermitted	Amazon S3 はレプリケート元バケットからオブジェクトメタデータを取得できません。レプリケート元バケットに対する s3:GetObjectVersionForReplication 権限がない可能性があります。
SrcKeyNotFound	Amazon S3 は、レプリケートするソースオブジェクトキーを見つけることができません。ソースオブジェクトはレプリケーションが完了する前に削除された可能性があります。
SrcKmsKeyInvalidState	レプリケート元バケットの AWS KMS キーは有効な状態ではありません。必要な AWS KMS キーを確認して有効にします。AWS KMS キーの管理について詳しくは、AWS Key Management Service デベロッパーガイドの「AWS KMS キーのキーステータス」を参照してください。
SrcObjectNotEligible	一部のオブジェクトはレプリケーションの対象外です。これは、オブジェクトのストレージクラスが原因であるか、オブジェクトタグがレプリケーション構成と一致しないことが原因である可能性があります。
SrcObjectNotFound	ソースオブジェクトが存在しません。

レプリケーションの失敗の理由	説明
SrcReplicationNotPending	Amazon S3 はすでにこのオブジェクトをレプリケートしています。このオブジェクトはもう保留中レプリケーションではなくなっています。
SrcVersionNotFound	Amazon S3 は、レプリケートするソースオブジェクトバージョンを見つけることができません。ソースオブジェクトバージョンはレプリケーションが完了する前に削除された可能性があります。

関連トピック

ライブレプリケーションのアクセス許可の設定

レプリケーションのトラブルシューティング

レプリケーションステータス情報の取得

レプリケーションステータスは、レプリケートされるオブジェクトの現在の状態を判断するのに役立ちます。レプリケート元オブジェクトのレプリケーションステータスは、 PENDING、COMPLETEDまたはFAILEDのいずれかを返します。レプリカのレプリケーションステータスがREPLICAに返されます。

S3 バッチレプリケーションジョブを作成するときにも、レプリケーションステータス値を使用することもできます。例えば、これらのステータス値を使用して、レプリケートされたことがない、またはレプリケーションに失敗したオブジェクトをレプリケートできます。バッチレプリケーションでこれらの値を使用する方法の詳細については、「the section called “バッチレプリケーションジョブでのレプリケーションステータス情報の使用”」を参照してください。

トピック

- レプリケーションステータスの概要
- 複数のレプリケート先バケットにレプリケートする場合のレプリケーションステータス
- Amazon S3 レプリカ変更の同期が有効になっている場合のレプリケーションステータス
- バッチレプリケーションジョブでのレプリケーションステータス情報の使用
- レプリケーションステータスの検索

レプリケーションステータスの概要

レプリケーションには、レプリケーションを設定するレプリケート元バケットと、Amazon S3 がオブジェクトをレプリケートする 1 つ以上のレプリケート先バケットがあります。これらのバケットからオブジェクト (GetObject を使用) またはオブジェクトメタデータ (HeadObject を使用) をリクエストすると、Amazon S3 はレスポンスとして x-amz-replication-status ヘッダーを返します。

- レプリケート元バケットのオブジェクトをリクエストする場合、リクエストしたオブジェクトがレプリケーション対象であると、Amazon S3 は x-amz-replication-status ヘッダーを返します。

  たとえば、レプリケーション設定でオブジェクトプレフィックス TaxDocs を指定して、キー名のプレフィックス TaxDocs が付いたオブジェクトのみをレプリケートするように Amazon S3 に指示しているとします。このキー名のプレフィックスを持つ、アップロードしたすべてのオブジェクト (TaxDocs/document1.pdf など) がレプリケートされます。このキー名のプレフィックスが付いたオブジェクトのリクエストでは、Amazon S3 が、オブジェクトのレプリケーション状態が PENDING、COMPLETED、または FAILED の値のいずれかの x-amz-replication-status ヘッダーを返します。

  > **Note**
  >
  > オブジェクトをアップロードした後で、オブジェクトのレプリケーションに失敗した場合、レプリケーションを再試行できません。オブジェクトを再度アップロードするか、S3 バッチレプリケーションを使用して失敗したオブジェクトをレプリケートする必要があります。バッチレプリケーションの使用の詳細については、「the section called “既存のオブジェクトのレプリケーション”」を参照してください。
  > レプリケーションロールの許可、AWS Key Management Service (AWS KMS) 許可、またはバケットの許可がないなどの問題がある場合、オブジェクトは FAILED ステータスに移行します。バケットやリージョンが使用できないなどの一時的な障害が発生した場合、レプリケーションのステータスは FAILED にはならず、PENDING のままになります。リソースがオンラインに戻ると、Amazon S3 はこれらのオブジェクトのレプリケーションを再開します。

- レプリケート先バケットからオブジェクトをリクエストした場合、リクエストされたオブジェクトが Amazon S3 によって作成されたレプリカであるときに、Amazon S3 は値がREPLICAであるx-amz-replication-statusヘッダーを返します。

> **Note**
>
> レプリケーションが有効になっているレプリケート元バケットからオブジェクトを削除する前に、削除する前にオブジェクトのレプリケーションステータスをチェックして、そのオブジェクトがレプリケートされていることを確認します。
> レプリケート元バケットで S3 ライフサイクル設定が有効である場合、Amazon S3 は、オブジェクトのステータスが COMPLETED または FAILED になるまでライフサイクルアクションを停止します。

複数のレプリケート先バケットにレプリケートする場合のレプリケーションステータス

オブジェクトを複数のレプリケート先バケットにレプリケートした場合、x-amz-replication-statusヘッダーの動作はそれぞれ異なります。レプリケート元オブジェクトのヘッダーは、すべてのレプリケート先へのレプリケーションが成功した場合のみ、COMPLETED の値を返します。すべてのレプリケート先に対してレプリケーションが完了するまで、ヘッダーはPENDINGの値のままになります。1 つ以上のレプリケート先がレプリケーションに失敗すると、ヘッダーはFAILEDを返します。

Amazon S3 レプリカ変更の同期が有効になっている場合のレプリケーションステータス

レプリケーションルールが Amazon S3 レプリカの変更を有効にすると、レプリカは REPLICA 以外のステータスをレポートできます。メタデータの変更がレプリケート中の場合は、x-amz-replication-status ヘッダーは PENDING を返します。レプリカ変更の同期がメタデータのレプリケートに失敗した場合、ヘッダーは FAILED を返します。メタデータが正しくレプリケートされると、レプリカはヘッダー REPLICA を返します。

バッチレプリケーションジョブでのレプリケーションステータス情報の使用

バッチレプリケーションジョブを作成するときに、オプションで、オブジェクトの作成日やレプリケーションステータスなどの追加のフィルターを指定して、ジョブのスコープを縮小できます。

オブジェクトのレプリケーションは、ObjectReplicationStatuses 値を基に、以下の値を 1 つ以上指定することでフィルターできます。

- "NONE" - Simple Storage Service (Amazon S3) がこれまでオブジェクトのレプリケートを試みたことがないことを示します。
- "FAILED" - Amazon S3 が以前にオブジェクトのレプリケートを試みたがオブジェクトのレプリケーションに失敗したことを示します。

- "COMPLETED" - Simple Storage Service (Amazon S3) が以前にオブジェクトを正常にレプリケートしたことを示します。
- "REPLICA" - Amazon S3 が別のソースからレプリケートしたレプリカオブジェクトであることを示します。

バッチレプリケーションでこれらのレプリケーションステータス値を使用する方法の詳細については、「the section called “バッチレプリケーションジョブのフィルター”」を参照してください。

レプリケーションステータスの検索

バケット内のオブジェクトのレプリケーションステータスを取得するには、Amazon S3 インベントリツールを使用できます。Amazon S3 は、インベントリ設定で指定したレプリケート先バケットに CSV ファイルを送信します。Amazon Athena を使用して、インベントリレポートのレプリケーションステータスをクエリすることもできます。Amazon S3 インベントリのさらなる詳細については、S3 インベントリを使用したデータのカタログ化と分析 を参照してください。

オブジェクトのレプリケーションステータスは、Amazon S3 コンソール、AWS Command Line Interface (AWS CLI)、または AWS SDK で確認できます。

S3 コンソールの使用

S3 コンソールでは、オブジェクトの詳細ページで、オブジェクトのレプリケーションステータスを確認できます。

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。
3. [汎用バケット] リストで、レプリケーションソースバケットの名前を選択します。
4. [オブジェクト] リストで、オブジェクト名を選択します。オブジェクトの詳細ページが表示されます。
5. [プロパティ] タブで、[オブジェクト管理の概要] セクションまでスクロールします。[管理設定] で、[レプリケーションステータス] の [値] を確認します。

AWS CLI を使用する場合

次の例に示すように、AWS Command Line Interface (AWS CLI) `head-object` コマンドを使用して、オブジェクトのメタデータを取得します。*`amzn-s3-demo-source-bucket1`* をレプリケー

ションソースバケットの名前に置き換え、その他の *user input placeholders* を独自の情報に置き換えます。

```
aws s3api head-object --bucket amzn-s3-demo-source-bucket1 --key object-key --version-
id object-version-id
```

このコマンドは、以下のレスポンス例に示すように、ReplicationStatus を含むオブジェクトメタデータを返します。

```
{
   "AcceptRanges":"bytes",
   "ContentType":"image/jpeg",
   "LastModified":"Mon, 23 Mar 2015 21:02:29 GMT",
   "ContentLength":3191,
   "ReplicationStatus":"COMPLETED",
   "VersionId":"jfnW.HIMOfYiD_9rGbSkmroXsFj3fqZ.",
   "ETag":"\"6805f2cfc46c0f04559748bb039d69ae\"",
   "Metadata":{

   }
}
```

AWS SDK の使用

次のコードフラグメントは、それぞれ AWS SDK for Java および AWS SDK for .NET を使用してレプリケーションステータスを取得します。

Java

```
GetObjectMetadataRequest metadataRequest = new GetObjectMetadataRequest(bucketName,
 key);
ObjectMetadata metadata = s3Client.getObjectMetadata(metadataRequest);

System.out.println("Replication Status : " +
 metadata.getRawMetadataValue(Headers.OBJECT_REPLICATION_STATUS));
```

.NET

```
GetObjectMetadataRequest getmetadataRequest = new GetObjectMetadataRequest
    {
         BucketName = sourceBucket,
```

```
        Key        = objectKey
    };

GetObjectMetadataResponse getmetadataResponse =
 client.GetObjectMetadata(getmetadataRequest);
Console.WriteLine("Object replication status: {0}",
 getmetadataResponse.ReplicationStatus);
```

マルチリージョンアクセスポイントを使用したマルチリージョントラフィックの管理

Amazon S3 マルチリージョンアクセスポイントを使用すると、複数の AWS リージョンにある S3 バケットからのリクエストをアプリケーションが実行するために使用できるグローバルエンドポイントを作成できます。マルチリージョンアクセスポイントを使用して、単一のリージョンで使用するのと同じシンプルなアーキテクチャでマルチリージョンアプリケーションを構築し、世界中のどこでもこれらのアプリケーションを実行することができます。マルチリージョンのアクセスポイントは、輻輳したパブリックインターネット経由でリクエストを送信する代わりに、Amazon S3 へのインターネットベースのリクエストを高速化する組み込みのネットワーク耐障害性を実現します。マルチリージョンアクセスポイントのグローバルエンドポイントに対して行われたアプリケーションリクエストは、AWS Global Accelerator を使用して、AWS グローバルネットワークを介して、アクティブなルーティングステータスを持つ最も近い S3 バケットに自動的にルーティングされます。

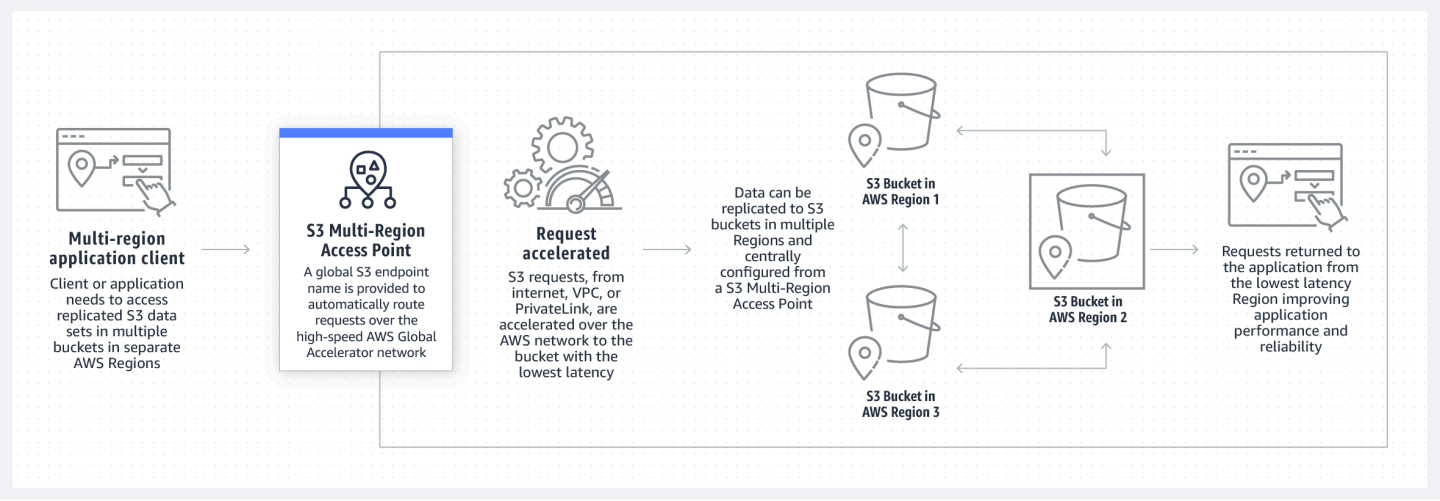
リージョントラフィックの中断が発生した場合は、マルチリージョンアクセスポイントのフェイルオーバーコントロールを使用して、S3 データリクエストトラフィックを AWS リージョン間でシフトし、S3 トラフィックを中断から数分以内にリダイレクトできます。また、中断に対してアプリケーションの耐障害性をテストして、アプリケーションのフェイルオーバーとディザスタリカバリシミュレーションを実行することもできます。VPC の外部から S3 へのリクエストに接続して高速化する必要がある場合は、Amazon S3 マルチリージョンアクセスポイントを使用してアプリケーションとネットワークアーキテクチャを簡素化できます。マルチリージョンアクセスポイントリクエストは AWS グローバルネットワーク経由でルーティングされ、パブリックインターネットを経由することなく、AWS リージョン内の S3 に戻ります。その結果、可用性の高いアプリケーションを構築できます。

マルチリージョンアクセスポイントを作成および設定するときは、そのマルチリージョンアクセスポイントを介して提供されるデータを保存する AWS リージョンのセットを指定します。指定されたマルチリージョンアクセスポイントエンドポイント名を使用してクライアントを接続できます。クライアント接続を確立したら、マルチリージョンアクセスポイントリクエストをルーティングする既存ま

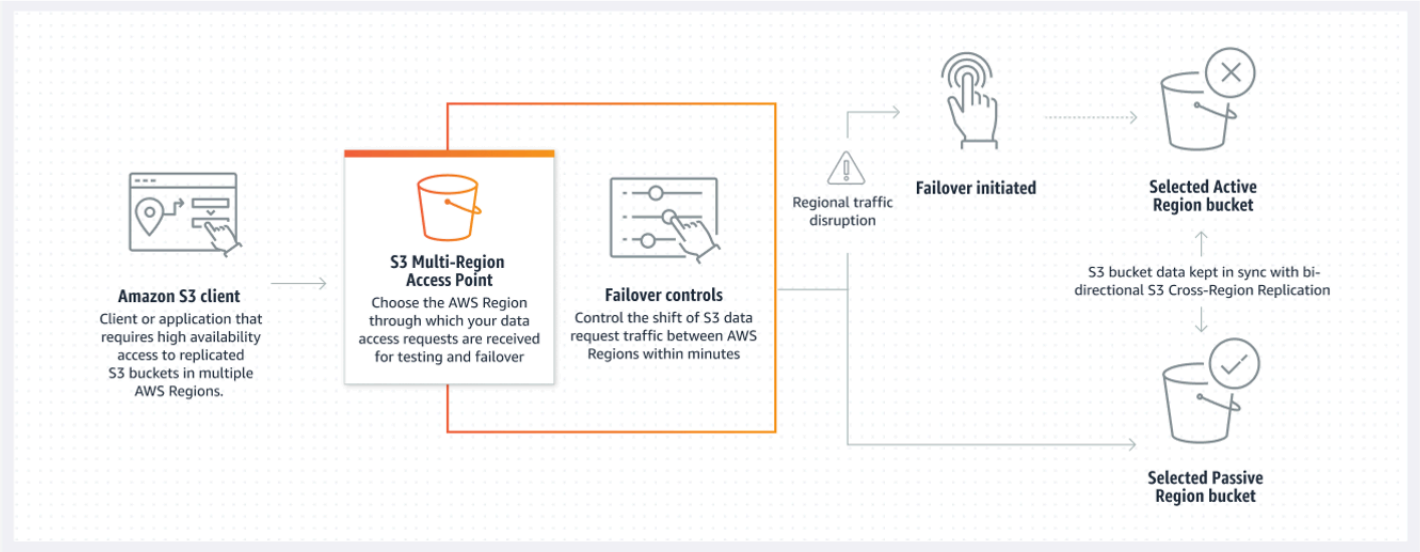
たは新しいバケットを選択できます。その後、S3 クロスリージョンレプリケーション (CRR) ルールを使用して、それらのリージョンのバケット間でデータを同期します。

マルチリージョンアクセスポイントを設定した後、マルチリージョンアクセスポイントグローバルエンドポイントを介してデータを要求または書き込みできます。Amazon S3 は、最も近い利用可能なリージョンからレプリケートされたデータセットへのリクエストを自動的に処理します。AWS Management Console 内では、マルチリージョンアクセスポイントリクエストに関連する基盤となるレプリケーショントポロジーとレプリケーションメトリクスを表示することもできます。これにより、マルチリージョンアプリケーションのストレージの構築、管理、モニタリングがさらに容易になります。または、Amazon CloudFront を使用して S3 マルチリージョンアクセスポイントの作成と設定を自動化することもできます。

次のイメージは、アクティブ-アクティブ構成の Amazon S3 マルチリージョンアクセスポイントを図で示したものです。この図は、Amazon S3 リクエストが最も近いアクティブな AWS リージョンに自動的にルーティングされる様子を示しています。



次のイメージは、アクティブ/パッシブ構成の Amazon S3 マルチリージョンアクセスポイントを図で示したものです。この図は、Amazon S3 データアクセストラフィックを制御してアクティブ-パッシブの AWS リージョン 間でフェイルオーバーする方法を示しています。



マルチリージョンアクセスポイントの使用方法の詳細については、「チュートリアル: Amazon S3 マルチリージョンアクセスポイントの使用の開始方法」を参照してください。

トピック

- マルチリージョンアクセスポイントの作成
- AWS PrivateLink で使用するマルチリージョンアクセスポイントの設定
- マルチリージョンアクセスポイントを使用したリクエスト

マルチリージョンアクセスポイントの作成

Amazon S3 でマルチリージョンアクセスポイントを作成するには、以下の作業を行います。

- マルチリージョンアクセスポイントの名前を指定します。
- マルチリージョンアクセスポイントのリクエストを処理するそれぞれの AWS リージョン でバケットを 1 つ選択します。
- マルチリージョンアクセスポイントに Amazon S3 パブリックアクセスブロックを設定します。

このすべての情報は、Amazon S3 が非同期で処理する作成リクエストで提供します。Amazon S3 は、非同期作成リクエストのステータスをモニタリングするために使用できるトークンを提供しています。

ポリシーを保存する前に、AWS Identity and Access Management Access Analyzer でセキュリティ警告、エラー、一般的な警告、および提案を解決してください。IAM Access Analyzer は、IAM ポ

リシーの文法およびベストプラクティス に対してポリシーチェックを行います。これらのチェックにより、機能的でセキュリティのベストプラクティスに準拠したポリシーを作成するのに、役立つ結果と実行可能なレコメンデーションが示されます。IAM Access Analyzer を使用したポリシーの検証の詳細については、IAM ユーザーガイドの IAM Access Analyzer のポリシーの検証を参照してください。IAM Access Analyzer によって返される警告、エラー、および提案のリストを表示するには、IAM Access Analyzer ポリシーチェックリファレンスを参照してください。

API を使用する場合、マルチリージョンアクセスポイントの作成リクエストは非同期です。マルチリージョンアクセスポイントを作成するリクエストを送信すると、Amazon S3 はリクエストを同期的に承認します。次に、作成リクエストの進行状況を追跡するために使用できるトークンをすぐに返します。マルチリージョンアクセスポイントを作成および管理するための非同期要リクエストの追跡の詳細については、「マルチリージョンアクセスポイントでのサポートされている API オペレーションの使用」を参照してください。

マルチリージョンアクセスポイントを作成すると、そのアクセスコントロールポリシーを作成できます。それぞれのマルチリージョンアクセスポイントには、ポリシーを関連付けることができます。マルチリージョンアクセスポイントポリシーは、リソース、ユーザー、またはその他の条件別にマルチリージョンアクセスポイントの使用を制限するために使用できるリソースベースのポリシーです。

> **Note**
>
> アプリケーションまたはユーザーがマルチリージョンアクセスポイントを介してオブジェクトにアクセスできるようにするには、次の両方のポリシーでリクエストを許可する必要があります。
>
> - マルチリージョンアクセスポイントのアクセスポリシー
> - オブジェクトを含む基になるバケットのアクセスポリシー
>
> 2 つのポリシーが異なる場合は、より制限の厳しいポリシーが優先されます。
> マルチリージョンアクセスポイントのアクセス許可管理を簡素化するために、バケットからマルチリージョンアクセスポイントにアクセスコントロールを委任できます。詳細については、「the section called “マルチリージョンアクセスポイントポリシーの例”」を参照してください。

マルチリージョンアクセスポイントでバケットを使用しても、既存のバケット名または Amazon リソースネーム (ARN) を使用してバケットにアクセスする場合のバケットの動作は変わりません。バケットに対する既存のすべてのオペレーションは、以前と同じように動作します。マルチリージョン

アクセスポイントポリシーに含めた制限は、そのマルチリージョンアクセスポイントを介したリクエストにのみ適用されます。

マルチリージョンアクセスポイントのポリシーは、作成後に更新できますが、ポリシーを削除することはできません。ただし、マルチリージョンアクセスポイントポリシーを更新して、すべてのアクセス許可を拒否することができます。

トピック

- Amazon S3 マルチリージョンアクセスポイントの命名規則
- Amazon S3 マルチリージョンアクセスポイントのバケットを選択するためのルール
- Amazon S3 マルチリージョンアクセスポイントを作成する
- Amazon S3 のマルチリージョンアクセスポイントを使用したパブリックアクセスのブロック
- Amazon S3 マルチリージョンアクセスポイントの設定の詳細を表示する
- マルチリージョンアクセスポイントの削除

Amazon S3 マルチリージョンアクセスポイントの命名規則

マルチリージョンアクセスポイントを作成するときは、名前を付けます。これは、選択した文字列です。マルチリージョンアクセスポイントの作成後は名前を変更できません。名前は、AWS アカウント で一意であり、マルチリージョンアクセスポイントの制約および制限事項 に記載されている命名要件に準拠している必要があります。マルチリージョンアクセスポイントを識別しやすくするために、自分にとって意味のある名前、組織にとって意味のある名前、またはシナリオを反映した名前を使用します。

この名前は、`GetMultiRegionAccessPoint` および `PutMultiRegionAccessPointPolicy` などのマルチリージョンアクセスポイント管理オペレーションを呼び出す際に使用します。この名前は、マルチリージョンアクセスポイントへのリクエストの送信には使用されないため、マルチリージョンアクセスポイントを使用してリクエストを行うクライアントに対して公開する必要はありません。

Amazon S3 がマルチリージョンアクセスポイントを作成すると、自動的にエイリアスが割り当てられます。このエイリアスは、`.mrap` で終わる一意の英数字文字列です。エイリアスは、マルチリージョンアクセスポイントのホスト名と Amazon リソースネーム (ARN) を構築するために使用されます。また、完全修飾名は、マルチリージョンアクセスポイントのエイリアスにも基づいています。

マルチリージョンアクセスポイントの名前をエイリアスから特定することはできません。そのため、イリアスを公開しても、マルチリージョンアクセスポイントの名前、目的、所有者を公開する危険性

はありません。Amazon S3 は、新しいマルチリージョンアクセスポイントごとにエイリアスを選択し、エイリアスを変更することはできません。マルチリージョンアクセスポイントのアドレス指定方法の詳細については、「マルチリージョンアクセスポイントを使用したリクエスト」を参照してください。

マルチリージョンアクセスポイントのエイリアスは、時間が経過しても一意であり、マルチリージョンアクセスポイントの名前や構成には基づいていません。マルチリージョンアクセスポイントを作成し、それを削除し、同じ名前と構成で別のものを作成した場合、2 番目のマルチリージョンアクセスポイントのエイリアスは最初のものと異なります。新しいマルチリージョンアクセスポイントは、以前のマルチリージョンアクセスポイントと同じエイリアスを持つことはできません。

Amazon S3 マルチリージョンアクセスポイントのバケットを選択するためのルール

それぞれのマルチリージョンアクセスポイントは、リクエストを処理するリージョンに関連付けられています。マルチリージョンアクセスポイントは、それぞれのリージョンの 1 つのバケットだけに関連付けられる必要があります。マルチリージョンアクセスポイントを作成するために、リクエストで各バケットの名前を指定します。マルチリージョンアクセスポイントをサポートするバケットは、マルチリージョンアクセスポイントを所有している同じ AWS アカウント にあることも、他の AWS アカウント にあることもできます。

1 つのバケットを複数のマルチリージョンアクセスポイントで使用できます。

> **Important**
>
> - マルチリージョンアクセスポイントに関連付けられるバケットは、作成時にのみ指定できます。作成後は、マルチリージョンアクセスポイント設定からバケットを追加、変更、または削除することはできません。バケットを変更するには、マルチリージョンアクセスポイント全体を削除し、新しいリージョンアクセスポイントを作成する必要があります。
> - マルチリージョンアクセスポイントの一部であるバケットは削除できません。マルチリージョンアクセスポイントに添付されたバケットを削除する場合は、まずマルチリージョンアクセスポイントを削除します。
> - 別のアカウントが所有しているバケットをマルチリージョンアクセスポイントに追加する場合、バケット所有者は、バケットポリシーを更新して、マルチリージョンアクセスポイントにアクセス許可を付与する必要もあります。そうしない場合、マルチリージョンアクセスポイントはそのバケットからデータを取得できません。このようなアクセスを許可する方法を示すポリシーの例については、「マルチリージョンアクセスポイントポリシーの例」を参照してください。

- すべてのリージョンがマルチリージョンアクセスポイントをサポートしているわけではありません。サポートされているリージョンのリストを確認するには、「マルチリージョンアクセスポイントの制約および制限事項」を参照してください。

バケット間でデータを同期するレプリケーションルールを作成できます。これらのルールを使用すると、ソースバケットからコピー先バケットにデータを自動的にコピーできます。バケットをマルチリージョンアクセスポイントに接続しても、レプリケーションの動作には影響しません。マルチリージョンアクセスポイントを使用したレプリケーションの設定については、後のセクションで説明します。

Important

マルチリージョンアクセスポイントにリクエストを行うと、マルチリージョンアクセスポイントは、マルチリージョンアクセスポイント内のバケットのデータコンテンツを認識しません。そのため、リクエストを受け取ったバケットには、リクエストされたデータが含まれていない可能性があります。マルチリージョンアクセスポイントに関連付けられた Amazon S3 バケットに一貫性のあるデータセットを作成するには、S3 クロスリージョンレプリケーション (CRR) を設定することをお勧めします。詳細については、「マルチリージョンアクセスポイントで使用するためのレプリケーションの設定」を参照してください。

Amazon S3 マルチリージョンアクセスポイントを作成する

以下の例では、Amazon S3 コンソールを使用してマルチリージョンアクセスポイントを作成する方法を示しています。

S3 コンソールの使用

マルチリージョンアクセスポイントを作成するには

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. ナビゲーションペインで、[Multi-Region Access Points] (マルチリージョンアクセスポイント) を選択します。
3. [マルチリージョンアクセスポイントの作成] を選択して、マルチリージョンアクセスポイントの作成を開始します。

4. [マルチリージョンアクセスポイント] ページの [マルチリージョンアクセスポイント名] フィールドに、マルチリージョンアクセスポイントの名前を入力します。
5. このマルチリージョンアクセスポイントに関連付けるバケットを選択します。自分のアカウントにあるバケットを選択することも、他のアカウントからバケットを選択することもできます。

> **Note**
>
> 自分のアカウントまたは他のアカウントから、少なくとも 1 つのバケットを追加する必要があります。また、マルチリージョンアクセスポイントは、AWS リージョン ごとに 1 つのバケットしかサポートしないことにも注意してください。したがって、同じリージョンから 2 つのバケットを追加することはできません。デフォルトで無効になっている AWS リージョン はサポートされません。

- アカウントにあるバケットを追加するには、[バケットの追加] を選択します。アカウント内のすべてのバケットのリストを表示します。バケットを名前で検索するか、バケット名をアルファベット順に並べ替えることができます。
- 別のアカウントからバケットを追加するには、[他のアカウントからバケットを追加] を選択します。他のアカウントでバケットを検索したり参照したりすることはできないため、正確なバケット名とAWS アカウント ID がわかっていることを確認してください。

> **Note**
>
> 有効なAWS アカウント ID とバケット名を入力する必要があります。また、バケットはサポートされているリージョンにある必要があり、ない場合は、マルチリージョンアクセスポイントを作成しようとするとエラーが発生します。マルチリージョンアクセスポイントをサポートするリージョンのリストについては、「マルチリージョンアクセスポイントの制約および制限事項」を参照してください。

6. (オプション) 追加したバケットを削除する必要がある場合は、[削除] を選択します。

> **Note**
>
> 作成が完了した後に、このマルチリージョンアクセスポイントのバケットを追加したり削除したりすることはできません。

7. [このマルチリージョンアクセスポイントのパブリックアクセス設定をブロック] で、マルチリージョンアクセスポイントに適用するブロックパブリックアクセス設定を選択します。デフォルトでは、新しいマルチリージョンアクセスポイントに対してすべてのブロックパブリックアクセス設定が有効になります。これらの設定を特に無効にする必要がある場合を除いて、すべての設定を有効にしておくことをお勧めします。

> **Note**
>
> マルチリージョンアクセスポイントを作成した後に、マルチリージョンアクセスポイントのブロックパブリックアクセス設定を変更することはできません。したがって、パブリックアクセスをブロックする場合は、マルチリージョンアクセスポイントを作成する前に、パブリックアクセスがなくてもアプリケーションが正しく動作することを確認してください。

8. [マルチリージョンアクセスポイントの作成] を選択します。

> **Important**
>
> 別のアカウントが所有しているバケットをマルチリージョンアクセスポイントに追加する場合、バケット所有者は、バケットポリシーを更新して、マルチリージョンアクセスポイントにアクセス許可を付与する必要もあります。そうしない場合、マルチリージョンアクセスポイントはそのバケットからデータを取得できません。このようなアクセスを許可する方法を示すポリシーの例については、「マルチリージョンアクセスポイントポリシーの例」を参照してください。

AWS CLI の使用

AWS CLI を使用して、マルチリージョンアクセスポイントを作成できます。マルチリージョンアクセスポイントを作成するときは、それがサポートするすべてのバケットを提供する必要があります。マルチリージョンアクセスポイントを作成した後に、マルチリージョンアクセスポイントにバケットを追加することはできません。

次の例では、AWS CLI を使用して、2 つのバケットを持つマルチリージョンアクセスポイントを作成します。このコマンドの例を実行するには、*`user input placeholders`* をユーザー自身の情報に置き換えます。

```
aws s3control create-multi-region-access-point --account-id 111122223333 --details '{
```

```
        "Name": "simple-multiregionaccesspoint-with-two-regions",
        "PublicAccessBlock": {
            "BlockPublicAcls": true,
            "IgnorePublicAcls": true,
            "BlockPublicPolicy": true,
            "RestrictPublicBuckets": true
        },
        "Regions": [
            { "Bucket": "amzn-s3-demo-bucket1" },
            { "Bucket": "amzn-s3-demo-bucket2" }
        ]
    }' --region us-west-2
```

Amazon S3 のマルチリージョンアクセスポイントを使用したパブリックアクセスのブロック

それぞれのマルチリージョンアクセスポイントには、Amazon S3 パブリックアクセスブロックの個別の設定があります。これらの設定は、マルチリージョンアクセスポイントと基となるバケットを所有する AWS アカウント のブロックパブリックアクセス設定と連動して機能します。

Amazon S3 がリクエストを承認すると、これらの設定の最も制限の厳しい組み合わせが適用されます。これらのリソース (マルチリージョンアクセスポイント所有者アカウント、基となるバケット、またはバケット所有者アカウント) のブロックパブリックアクセス設定が、リクエストされたアクションまたはリソースへのアクセスをブロックすると、Amazon S3 はリクエストを拒否します。

これらの設定を特に無効にする必要がある場合を除いては、すべての設定を有効にしておくことをお勧めします。デフォルトでは、マルチリージョンアクセスポイントに対してすべてのブロックパブリックアクセス設定が有効になります。ブロックパブリックアクセスが有効になっている場合、マルチリージョンアクセスポイントはインターネットベースのリクエストを受け付けることができません。

> **Important**
>
> マルチリージョンアクセスポイントを作成した後にブロックパブリックアクセス設定を変更することはできません。

Amazon S3 のブロックパブリックアクセスの詳細については、「Amazon S3 ストレージへのパブリックアクセスのブロック」を参照してください。

Amazon S3 マルチリージョンアクセスポイントの設定の詳細を表示する

以下の例では、Amazon S3 コンソールを使用してマルチリージョンアクセスポイントの設定の詳細を表示する方法を示しています。

S3 コンソールの使用

マルチリージョンアクセスポイントを作成するには

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. ナビゲーションペインで、[Multi-Region Access Points] (マルチリージョンアクセスポイント) を選択します。
3. 設定の詳細を表示するマルチリージョンアクセスポイントの名前を選択します。

   - [プロパティ] タブには、マルチリージョンアクセスポイントに関連付けられているすべてのバケット、作成日、Amazon リソースネーム (ARN)、およびエイリアスが表示されます。AWS アカウント ID 列には、マルチリージョンアクセスポイントに関連付けられている外部アカウントが所有するバケットもすべて表示されます。
   - [アクセス許可] タブには、このマルチリージョンアクセスポイントに関連付けられたバケットに適用されるブロックパブリックアクセス設定が表示されます。マルチリージョンアクセスポイントを作成している場合は、マルチリージョンアクセスポイントのポリシーを表示することもできます。[アクセス許可] ページの [情報] アラートには、このマルチリージョンアクセスポイントの [パブリックアクセスはブロックされています] 設定が有効になっているすべてのバケット (自分のアカウントと他のアカウント内) も一覧表示されます。
   - [レプリケーションとフェイルオーバー] タブには、マルチリージョンアクセスポイントに関連付けられているバケットと、バケットが置かれているリージョンのマップビューが表示されます。データを取得するアクセス許可のない別のアカウントのバケットがある場合、そのリージョンはレプリケーションの概要マップ上で赤くマークされ、レプリケーションステータスの取得中にエラーが発生した AWS リージョン であることを示します。

     > **Note**
     >
     > 外部アカウントのバケットからレプリケーションステータス情報を取得するには、バケット所有者がバケットポリシーで `s3:GetBucketReplication` アクセス許可を付与する必要があります。

このタブには、マルチリージョンアクセスポイントで使用されているリージョンのレプリケーションメトリクス、レプリケーションルール、フェイルオーバーステータスも表示されます。

AWS CLI の使用

AWS CLI を使用して、マルチリージョンアクセスポイントの設定の詳細を表示できます。

次の AWS CLI の例では、現在のマルチリージョンアクセスポイント設定を取得します。このコマンドの例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3control get-multi-region-access-point --account-id 111122223333 --name amzn-s3-demo-bucket
```

マルチリージョンアクセスポイントの削除

次の手順では、Amazon S3 コンソールを使用してマルチリージョンアクセスポイントを削除する方法を説明します。

マルチリージョンアクセスポイントを削除しても、マルチリージョンアクセスポイントに関連付けられたバケットは削除されず、マルチリージョンアクセスポイント自体だけが削除されます。

S3 コンソールの使用

マルチリージョンアクセスポイントを削除するには

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. ナビゲーションペインで、[Multi-Region Access Points] (マルチリージョンアクセスポイント) を選択します。
3. マルチリージョンアクセスポイントの名前の横にあるオプションボタンを選択します。
4. [削除] を選択します。
5. [マルチリージョンアクセスポイントの削除] ダイアログボックスで、削除する AWS バケットの名前を入力します。

> **Note**
>
> 有効なバケット名を入力していることを確認してください。有効ではない場合、[削除] ボタンが無効になります。

6. [削除] を選択して、マルチリージョンアクセスポイントの削除を確認します。

AWS CLI の使用

AWS CLI を使用して、マルチリージョンアクセスポイントを削除できます。このアクションでは、マルチリージョンアクセスポイントに関連付けられたバケットは削除されず、マルチリージョンアクセスポイント自体だけが削除されます。このコマンドの例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3control delete-multi-region-access-point --account-id 123456789012 --details
 Name=example-multi-region-access-point-name
```

AWS PrivateLink で使用するマルチリージョンアクセスポイントの設定

マルチリージョンアクセスポイントを使用して、AWS リージョン 間で Amazon S3 リクエストトラフィックのルーティングを行うことができます。各マルチリージョンアクセスポイントのグローバルエンドポイントは、複数の送信元からの Amazon S3 データリクエストトラフィックをルーティングします。個別のエンドポイントで複雑なネットワーク設定を構築する必要はありません。これらのデータリクエストトラフィックソースには以下が含まれます。

- 仮想プライベートクラウド (VPC) から発信されるトラフィック
- AWS PrivateLink を経由する、オンプレミスのデータセンターからのトラフィック
- パブリックインターネットからのトラフィック

S3 マルチリージョンアクセスポイントへの AWS PrivateLink 接続を確立すると、シンプルなネットワークアーキテクチャと設定を使用して、AWS に、またはプライベート接続を経由して複数の AWS リージョン に、S3 リクエストをルーティングできます。AWS PrivateLink を使用する場合、VPC ピアリング接続を設定する必要はありません。

トピック

- AWS PrivateLink で使用するマルチリージョンアクセスポイントの設定

- VPC エンドポイントからマルチリージョンアクセスポイントへのアクセスを削除する

AWS PrivateLink で使用するマルチリージョンアクセスポイントの設定

AWS PrivateLink は、Virtual Private Cloud (VPC) 内のプライベート IP アドレスを使用して Amazon S3 にプライベート接続できます。VPC 内で 1 つ以上のインターフェイスエンドポイントをプロビジョニングして、Amazon S3 マルチリージョンアクセスポイントに接続できます。

AWS Management Console、AWS CLI、または AWS SDK によって、マルチリージョンアクセスポイントの com.amazonaws.s3-global.accesspoint エンドポイントを作成することができます。マルチリージョンアクセスポイントのインターフェイスエンドポイントを設定する方法の詳細については、VPC ユーザーガイドの「インターフェイス VPC エンドポイント」を参照してください。

インターフェイスエンドポイント経由でマルチリージョンアクセスポイントにリクエストを送信するには、次の手順に従って VPC とマルチリージョンアクセスポイントを設定します。

AWS PrivateLink で使用するマルチリージョンアクセスポイントを設定するには

1. マルチリージョンアクセスポイントに接続できる適切な VPC エンドポイントを作成するか、所有します。VPC エンドポイントの作成の詳細については、VPC ユーザーガイドの「インターフェイス VPC エンドポイント」を参照してください。

   > **Important**
   >
   > 必ず com.amazonaws.s3-global.acesspoint エンドポイントを作成してください。他のエンドポイントタイプでは、マルチリージョンアクセスポイントにアクセスできません。

   この VPC エンドポイントが作成されると、エンドポイントに対してプライベート DNS が有効になっている場合、VPC 内のすべてのマルチリージョンアクセスポイントリクエストはこのエンドポイントを経由します。これはデフォルトで有効になっています。
2. マルチリージョンアクセスポイントポリシーが VPC エンドポイントからの接続をサポートしていない場合は、更新する必要があります。
3. 個々のバケットポリシーで、マルチリージョンアクセスポイントのユーザーへのアクセスが許可されていることを確認します。

マルチリージョンアクセスポイントは、リクエスト自体を満たすのではなく、バケットにリクエストをルーティングすることによって機能することに注意してください。リクエストの発信者は、マルチ

リージョンアクセスポイントに対する許可を持ち、マルチリージョンアクセスポイント内の個々のバケットへのアクセスが許可されている必要があることを覚えておくことが重要です。そうしないと、リクエストは、発信者がリクエストを実行するための許可を持たないバケットにルーティングされる可能性があります。マルチリージョンアクセスポイントと関連付けられているバケットは、同じまたは別の AWS アカウントに所有されることができます。ただし、許可が正しく設定されていれば、異なるアカウントの VPC でマルチリージョンアクセスポイントを使用できます。

このため、VPC エンドポイントポリシーでは、マルチリージョンアクセスポイントと、リクエストを処理できるようにする基盤となる各バケットの両方へのアクセスを許可する必要があります。例えば、エイリアス mfzwi23gnjvgw.mrap を持つマルチリージョンアクセスポイントがあるとします。バケット amzn-s3-demo-bucket1 および amzn-s3-demo-bucket2 によって支えられており、すべて AWS アカウント 123456789012 が所有しています。この場合、以下の VPC エンドポイントでは、mfzwi23gnjvgw.mrap に対して行われた VPC からの GetObject リクエストを、いずれかのバッキングバケットで実行できます。

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
        "Sid": "Read-buckets-and-MRAP-VPCE-policy",
        "Principal": "*",
        "Action": [
            "s3:GetObject"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket1/*",
            "arn:aws:s3:::amzn-s3-demo-bucket2/*",
            "arn:aws:s3::123456789012:accesspoint/mfzwi23gnjvgw.mrap/object/*"
        ]
    }]
}
```

前述したように、マルチリージョンアクセスポイントポリシーが VPC エンドポイント経由のアクセスをサポートするように設定されていることも確認する必要があります。アクセスをリクエストしている VPC エンドポイントを指定する必要はありません。次のサンプルポリシーは、GetObject リクエストにマルチリージョンアクセスポイントを使用しようとしているリクエスターにアクセスを許可します。

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
    {
        "Sid": "Open-read-MRAP-policy",
        "Effect": "Allow",
        "Principal": "*",
        "Action": [
            "s3:GetObject"
          ],
        "Resource": "arn:aws:s3::123456789012:accesspoint/mfzwi23gnjvgw.mrap/object/*"
    }]
}
```

もちろん、個々のバケットには、VPC エンドポイントを介して送信されたリクエストからのアクセスをサポートするポリシーが必要です。以下のポリシーの例では、VPC エンドポイントを介して行われたリクエストを含む匿名ユーザーに読み取りアクセス許可が付与されます。

```
{
    "Version":"2012-10-17",
   "Statement": [
   {
       "Sid": "Public-read",
       "Effect":"Allow",
       "Principal": "*",
       "Action": "s3:GetObject",
       "Resource": [
           "arn:aws:s3:::amzn-s3-demo-bucket1",
           "arn:aws:s3:::amzn-s3-demo-bucket2/*"]
    }]
}
```

VPC エンドポイントポリシーの編集については、「VPC ユーザーガイド」の「VPC エンドポイントによるサービスへのアクセスのコントロール」を参照してください。

VPC エンドポイントからマルチリージョンアクセスポイントへのアクセスを削除する

マルチリージョンアクセスポイントを所有しており、インターフェイスエンドポイントからそのアクセス権を削除する場合は、マルチリージョンアクセスポイントに新しいアクセスポリシーを提供して、VPC エンドポイントを経由するリクエストへのアクセスを防止する必要があります。ただし、マルチリージョンアクセスポイントのバケットが VPC エンドポイント経由のリクエストをサポートしている場合、これらのリクエストは引き続きサポートされます。このサポートを禁止する場合は、

バケットのポリシーも更新しなければなりません。マルチリージョンアクセスポイントに新しいアクセスポリシーを指定すると、マルチリージョンアクセスポイントへのアクセスだけが禁止され、基になるバケットへのアクセスは禁止されません。

> **Note**
>
> マルチリージョンアクセスポイントのアクセスポリシーを削除することはできません。マルチリージョンアクセスポイントへのアクセスを削除するには、変更したアクセスで新しいアクセスポリシーを提供する必要があります。

マルチリージョンアクセスポイントのアクセスポリシーを更新する代わりに、バケットポリシーを更新して、VPC エンドポイントを使用したリクエストを防ぐことができます。この場合、ユーザーは VPC エンドポイント経由でマルチリージョンアクセスポイントにアクセスできます。ただし、マルチリージョンアクセスポイントリクエストが、バケットポリシーがアクセスを禁止するバケットにルーティングされると、リクエストによりエラーメッセージが生成されます。

マルチリージョンアクセスポイントを使用したリクエスト

他のリソースと同様に、Amazon S3 マルチリージョンアクセスポイントには、Amazon リソースネーム (ARN) があります。これらの ARN を使用することで、AWS Command Line Interface (AWS CLI)、AWS SDK、または Amazon S3 API を使用してマルチリージョンのアクセスポイントにリクエストを指示できます。これらの ARN を使用して、アクセスコントロールポリシーでマルチリージョンアクセスポイントを識別することもできます。マルチリージョンアクセスポイント ARN にマルチリージョンアクセスポイントの名前が含まれたり、公開されたりすることはありません。ARN の詳細については、「AWS 全般のリファレンス」の「Amazon リソースネーム (ARN)」を参照してください。

> **Note**
>
> マルチリージョンアクセスポイントのエイリアスと ARN は互換的に使用できません。

マルチリージョンアクセスポイント ARN は、以下の形式を使用します。

`arn:aws:s3::`*`account-id`*`:accesspoint/`*`MultiRegionAccessPoint_alias`*

以下に、マルチリージョンアクセスポイント ARN の例をいくつか示します。

- arn:aws:s3::123456789012:accesspoint/mfzwi23gnjvgw.mrap は、AWS アカウント 123456789012 が所有する、エイリアス mfzwi23gnjvgw.mrap を持つマルチリージョンアクセスポイントを表します。
- arn:aws:s3::123456789012:accesspoint/* は、アカウント 123456789012 内のすべてのマルチリージョンアクセスポイントを表します。この ARN は、アカウント 123456789012 のすべてのマルチリージョンアクセスポイントと一致しますが、ARN に AWS リージョン が含まれていないため、リージョンの Amazon S3 Access Points とは一致しません。これとは対照的に、ARN arn:aws:s3:us-west-2:123456789012:accesspoint/* は、リージョン us-west-2 にあるアカウント 123456789012 のすべてのリージョンの Amazon S3 Access Points とは一致しますが、マルチリージョンアクセスポイントとは一致しません。

マルチリージョンアクセスポイントを介してアクセスされるオブジェクトの ARN は、以下の形式を使用します。

arn:aws:s3::*account_id*:accesspoint/*MultiRegionAccessPoint_alias*//*key*

マルチリージョンアクセスポイント ARN と同様に、マルチリージョンアクセスポイントを介してアクセスされるオブジェクトの ARN には AWS リージョン は含まれません。次に例を示します。

- arn:aws:s3::123456789012:accesspoint/mfzwi23gnjvgw.mrap//-01 は、アカウント 123456789012 が所有する、エイリアス mfzwi23gnjvgw.mrap を持つマルチリージョンアクセスポイントを通じてアクセスされる、-01 を表します。
- arn:aws:s3::123456789012:accesspoint/mfzwi23gnjvgw.mrap//* は、アカウント 123456789012 で、エイリアス mfzwi23gnjvgw.mrap を持ち、マルチリージョンアクセスポイントを通じてアクセスできるすべてのオブジェクトを表します。
- arn:aws:s3::123456789012:accesspoint/mfzwi23gnjvgw.mrap//-01/finance/* は、アカウント 123456789012 で、エイリアス mfzwi23gnjvgw.mrap を持ち、マルチリージョンアクセスポイントの -01/finance/ でアクセスできるすべてのオブジェクトを表します。

マルチリージョンアクセスポイントのホスト名

マルチリージョンアクセスポイントのホスト名を使用して、マルチリージョンアクセスポイントを介して Amazon S3 のデータにアクセスできます。パブリックインターネットからこのホスト名にリクエストを送信できます。マルチリージョンアクセスポイントに 1 つ以上のインターネットゲートウェイを設定している場合は、仮想プライベートクラウド (VPC) からこのホスト名にリクエストを送信することもできます。マルチリージョンアクセスポイントで使用する VPC インターフェイスエ

ンドポイントの作成の詳細については、「AWS PrivateLink で使用するマルチリージョンアクセスポイントの設定」を参照してください。

また、VPC エンドポイントを使用して VPC からマルチリージョンアクセスポイント経由でリクエストを行うには、AWS PrivateLink を使用することができます。AWS PrivateLink を使用してマルチリージョンアクセスポイントへのリクエストを行う場合、*region*.vpce.amazonaws.com で終わるエンドポイント固有のリージョンのドメインネームシステム (DNS) を直接使用することはできません。このホスト名には証明書が関連付けられていないため、直接使用することはできません。ただし、引き続き、VPC エンドポイントのパブリックドメインネームシステム (DNS) 名を CNAME または ALIAS ターゲットとして使用することはできます。あるいは、エンドポイントでプライベートドメインネームシステム (DNS) を有効にし、このセクションで説明されているように、標準のマルチリージョンアクセスポイント *MultiRegionAccessPoint_alias*.accesspoint.s3-global.amazonaws.com ドメインネームシステム (DNS) 名を使用することもできます。

マルチリージョンアクセスポイント経由で API for Amazon S3 データオペレーション (例えば GetObject) にリクエストする場合、リクエストのホスト名は次のようになります。

MultiRegionAccessPoint_alias.accesspoint.s3-global.amazonaws.com

例えば、エイリアス mfzwi23gnjvgw.mrap を持つマルチリージョンアクセスポイントを介して GetObject リクエストを行うには、ホスト名 mfzwi23gnjvgw.mrap.accesspoint.s3-global.amazonaws.com に対してクエストを行います。ホスト名の s3-global 部分は、このホスト名が特定のリージョン用ではないことを示しています。

マルチリージョンアクセスポイントを使用したリクエストの作成は、単一リージョンアクセスポイントを使用したリクエストの作成と似ています。ただし、以下の違いを考慮する必要があります。

- マルチリージョンアクセスポイント ARN に AWS リージョン は含まれません。フォーマット arn:aws:s3::*account-id*:accesspoint/*MultiRegionAccessPoint_alias* に従います。
- API オペレーションを介して行われたリクエスト (これらのリクエストに ARN を使用する必要はありません) では、マルチリージョンアクセスポイントは異なるエンドポイントスキームを使用します。スキームは *MultiRegionAccessPoint_alias*.accesspoint.s3-global.amazonaws.com です。例えば、mfzwi23gnjvgw.mrap.accesspoint.s3-global.amazonaws.com です。単一リージョンアクセスポイントとの相違点に注意してください。
  - マルチリージョンアクセスポイントのホスト名は、マルチリージョンアクセスポイント名ではなく、エイリアスを使用します。

  - マルチリージョンアクセスポイントのホスト名には、所有者の AWS アカウント ID は含まれません。
  - マルチリージョンアクセスポイントのホスト名には、AWS リージョン は含まれません。
  - マルチリージョンアクセスポイントのホスト名には、`s3.amazonaws.com` の代わりに `s3-global.amazonaws.com` が含まれます。
- マルチリージョンアクセスポイントのリクエストは、署名バージョン 4A (SigV4A) を使用して署名する必要があります。AWS SDK を使用時する場合、SDK は Sigv4 を SigV4A に自動的に変換します。そのため、ご使用の AWS SDK が、グローバル AWS リージョン リクエストの署名に使用される署名実装として SigV4AA をサポートしていることを確認してください。SigV4A の詳細については、「AWS 全般のリファレンス」の「AWS API リクエストの署名」を参照してください。

マルチリージョンアクセスポイントと Amazon S3 Transfer Acceleration

Amazon S3 Transfer Acceleration は、バケットへの高速データ転送を実現する機能です。Transfer Acceleration は個々のバケットレベルで設定されます。Transfer Acceleration の詳細については、「Amazon S3 Transfer Acceleration を使用した高速かつ安全なファイル転送の設定」を参照してください。

マルチリージョンアクセスポイントは、Transfer Acceleration と同様の高速転送メカニズムを使用して、大きなオブジェクトを AWS ネットワークで送信します。このため、マルチリージョンアクセスポイント経由でリクエストを送信する場合、Transfer Acceleration を使用する必要はありません。この転送パフォーマンスの向上は、マルチリージョンアクセスポイントに自動的に組み込まれます。

トピック

- アクセス許可
- マルチリージョンアクセスポイントの制約および制限事項
- マルチリージョンアクセスポイントリクエストのルーティング
- Amazon S3 マルチリージョンアクセスポイントフェイルオーバーコントロール
- マルチリージョンアクセスポイントで使用するためのレプリケーションの設定
- マルチリージョンアクセスポイントでのサポートされている API オペレーションの使用
- マルチリージョンアクセスポイントから基盤となるリソースへのリクエストのモニタリングとログ記録

アクセス許可

Amazon S3 マルチリージョンアクセスポイントは、複数の AWS リージョン の Amazon S3 バケットへのデータアクセスを簡素化します。マルチリージョンアクセスポイントは、Amazon S3 のデータアクセスオブジェクトのオペレーション (`GetObject` や `PutObject` など) を実行するために使用できる名前付きのグローバルエンドポイントです。各マルチリージョンアクセスポイントは、グローバルエンドポイントを介したすべてのリクエストについて、個別のアクセス許可とネットワークコントロールを設定できます。

各マルチリージョンアクセスポイントは、基になるバケットにアタッチされたバケットポリシーと連動して機能するカスタマイズされたアクセスポリシーを適用することもできます。クロスアカウントリクエストが成功するには、次のポリシーでオペレーションが許可されている必要があります。

- マルチリージョンアクセスポイントポリシー
- 基になる AWS Identity and Access Management (IAM) ポリシー
- 基になるバケットポリシー (リクエストのルーティング先)

> **Note**
>
> 同じアカウントリクエストの場合、適切なアクセス許可を付与する基盤となる IAM ポリシーのみが必要です。

マルチリージョンアクセスポイントポリシーは、特定の IAM ユーザーまたはグループからのリクエストのみを受け入れるように設定できます。これを行う方法の例については、「the section called “マルチリージョンアクセスポイントポリシーの例”」の例 2 を参照してください。Virtual Private Cloud (VPC) からのリクエストだけを受け入れるようにマルチリージョンアクセスポイントポリシーを設定することで、プライベートネットワークへの Amazon S3 データアクセスを制限できます。

例えば、次のようになります。`AppDataReader` というユーザーを AWS アカウントで使用して、マルチリージョンアクセスポイントを介して `GetObject` リクエストを行うとします。リクエストが拒否されないようにするために、マルチリージョンアクセスポイントと、マルチリージョンアクセスポイントの基盤となる各バケットによって `AppDataReader` ユーザーに `s3:GetObject` 許可を付与する必要があります。`AppDataReader` は、この許可を付与しないバケットからデータを取得できません。

> **Important**
>
> バケットのアクセスコントロールをマルチリージョンアクセスポイントポリシーに委任しても、バケット名または Amazon リソースネーム (ARN) を使用してバケットに直接アクセスする場合のバケットの動作は変わりません。バケットに対して直接行われるすべてのオペレーションは、以前と同じように動作します。マルチリージョンアクセスポイントポリシーに含めた制限は、そのマルチリージョンアクセスポイントを介したリクエストにのみ適用されます。

マルチリージョンアクセスポイントへのパブリックアクセスの管理

マルチリージョンアクセスポイントは、 マルチリージョンアクセスポイントごとに独立したブロックパブリックアクセス設定をサポートしています。 マルチリージョンアクセスポイントを作成するときに、その マルチリージョンアクセスポイントに適用するブロックパブリックアクセス設定を指定できます。

> **Note**
>
> マルチリージョンアクセスポイントの個別のパブリックアクセスをブロックする設定が無効になっていても、(自分のアカウントの) [このアカウントのブロックパブリックアクセス設定] または [外部バケットのブロックパブリック設定] は引き続き適用されます。

マルチリージョンアクセスポイントを介して行われたリクエストについて、Amazon S3 は以下に対するブロックパブリックアクセス設定を評価します。

- マルチリージョンアクセスポイント
- 基になるバケット (外部バケットを含む)
- マルチリージョンアクセスポイントを所有するアカウント
- 基になるバケットを所有するアカウント (外部アカウントを含む)

これらの設定のいずれかで、リクエストをブロックする必要があることが示されると、Amazon S3 はリクエストを拒否します。Amazon S3 ブロックパブリックアクセス機能の詳細については、「Amazon S3 ストレージへのパブリックアクセスのブロック」を参照してください。

> **Important**
>
> デフォルトでは、マルチリージョンアクセスポイントに対してすべてのブロックパブリックアクセス設定が有効になります。 マルチリージョンアクセスポイントに適用したくない設定がある場合は、明示的に無効にする必要があります。
> マルチリージョンアクセスポイントを作成した後にブロックパブリックアクセス設定を変更することはできません。

マルチリージョンアクセスポイントのパブリックアクセスブロック設定の表示

マルチリージョンアクセスポイントのパブリックアクセスブロック設定を表示するには

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. ナビゲーションペインで、[Multi-Region Access Points] (マルチリージョンアクセスポイント) を選択します。
3. 確認するマルチリージョンアクセスポイントの名前を選択します。
4. [アクセス許可] タブを選択します。
5. [Block Public Access settings for this Multi-Region Access Point] (このマルチリージョンアクセスポイントのパブリックアクセス設定をブロック) で、マルチリージョンアクセスポイントのブロックパブリックアクセス設定を確認します。

> **Note**
>
> マルチリージョンアクセスポイントを作成した後、ブロックパブリックアクセス設定を編集することはできません。したがって、パブリックアクセスをブロックする場合は、マルチリージョンアクセスポイントを作成する前に、パブリックアクセスがなくてもアプリケーションが正しく動作することを確認してください。

マルチリージョンアクセスポイントポリシーの使用

次のマルチリージョンアクセスポイントポリシーの例では、IAM ユーザーに対して、マルチリージョンアクセスポイントのファイルを一覧表示およびダウンロードするアクセス権限を付与しています。このポリシーの例を実行するには、*`user input placeholders`* をユーザー自身の情報に置き換えます。

```
 {
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "AWS":"arn:aws:iam::123456789012:user/JohnDoe"
         },
         "Action":[
            "s3:ListBucket",
            "s3:GetObject"
         ],
         "Resource":[
            "arn:aws:s3::111122223333:accesspoint/MultiRegionAccessPoint_alias",
            "arn:aws:s3::111122223333:accesspoint/MultiRegionAccessPoint_alias/object/
*"
         ]
      }
   ]
}
```

AWS Command Line Interface (AWS CLI) を使用して、マルチリージョンアクセスポイントポリシーを指定されたマルチリージョンアクセスポイントに関連付けるには、次の put-multi-region-access-point-policy コマンドを使用します。このコマンドの例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。各マルチリージョンアクセスポイントに設定できるポリシーは 1 つだけなので、put-multi-region-access-point-policy アクションをリクエストすると、指定されたマルチリージョンアクセスポイントに関連付けられている既存のポリシーがすべて置き換えられます。

AWS CLI

```
aws s3control put-multi-region-access-point-policy
--account-id 111122223333
--details { "Name": "amzn-s3-demo-bucket-MultiRegionAccessPoint",
 "Policy": "{ \"Version\": \"2012-10-17\", \"Statement\": { \"Effect\":
 \"Allow\", \"Principal\": { \"AWS\": \"arn:aws:iam::111122223333:root
\" }, \"Action\": [\"s3:ListBucket\", \"s3:GetObject\"], \"Resource\":
 [ \"arn:aws:s3::111122223333:accesspoint/MultiRegionAccessPoint_alias",
 \"arn:aws:s3::111122223333:accesspoint/MultiRegionAccessPoint_alias/object/*
\" ] } }" }
```

前のオペレーションの結果をクエリするには、次のコマンドを使用します。

AWS CLI

```
aws s3control describe-multi-region-access-point-operation
--account-id 111122223333
--request-token-arn requestArn
```

マルチリージョンアクセスポイントポリシーを取得するには、次のコマンドを使用します。

AWS CLI

```
aws s3control get-multi-region-access-point-policy
--account-id 111122223333
--name=amzn-s3-demo-bucket-MultiRegionAccessPoint
```

マルチリージョンアクセスポイントポリシーの編集

マルチリージョンアクセスポイントポリシー (JSON で記述) は、このマルチリージョンアクセスポイントで使用する Amazon S3 バケットへのストレージアクセスを提供します。特定のプリンシパルがマルチリージョンアクセスポイントでさまざまなアクションを実行することを許可または拒否できます。リクエストがマルチリージョンアクセスポイントを介してバケットにルーティングされると、マルチリージョンアクセスポイントとバケットの両方のアクセスポリシーが適用されます。より制限の厳しいアクセスポリシーが常に優先されます。

> **Note**
>
> バケットに他のアカウントが所有するオブジェクトが含まれている場合、マルチリージョンアクセスポイントのポリシーは他の AWS アカウント が所有するオブジェクトには適用されません。

マルチリージョンアクセスポイントポリシーを適用した後、ポリシーを削除することはできません。ポリシーを編集するか、既存のポリシーを上書きする新しいポリシーを作成することができます。

マルチリージョンアクセスポイントポリシーを編集するには

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. ナビゲーションペインで、[Multi-Region Access Points] (マルチリージョンアクセスポイント) を選択します。
3. ポリシーを編集するマルチリージョンアクセスポイントの名前を選択します。
4. [アクセス許可] タブを選択します。
5. [Multi-Region Access Point policy] (マルチリージョンアクセスポイントポリシー) セクションまでスクロールします。[Edit] (編集) を選択し、ポリシーを更新します。
6. [Edit Multi-Region Access Point policy] (マルチリージョンアクセスポイントポリシーの編集) ページが表示されます。ポリシーをテキストフィールドに直接入力するか、[Add statement] (ステートメントの追加) を選択してドロップダウンリストからポリシーの要素を選択できます。

> **Note**
>
> コンソールに、マルチリージョンアクセスポイントの Amazon リソースネーム (ARN) が自動的に表示されます。これをポリシーで使用できます。マルチリージョンアクセスポイントポリシーの例については、「the section called “マルチリージョンアクセスポイントポリシーの例”」を参照してください。

マルチリージョンアクセスポイントポリシーの例

Amazon S3 マルチリージョンアクセスポイントは、AWS Identity and Access Management (IAM) リソースポリシーをサポートします。これらのポリシーを使用して、リソース、ユーザー、その他の条件別にマルチリージョンアクセスポイントの使用を制御することができます。アプリケーションやユーザーがマルチリージョンアクセスポイントを介してオブジェクトにアクセスできるようにするには、マルチリージョンアクセスポイントと基になるバケットの両方が同じアクセスを許可している必要があります。

マルチリージョンアクセスポイントと基になるバケットの両方に同じアクセスを許可するには、次のいずれかを実行します。

- (推奨) Amazon S3 マルチリージョンアクセスポイントを使用する際のアクセスコントロールを簡素化するには、Amazon S3 バケットのアクセスコントロールをマルチリージョンアクセスポイントに委任します。これを行う方法の例については、このセクションの例 1 を参照してください。
- マルチリージョンアクセスポイントポリシーに含まれているものと同じアクセス許可を、基になるバケットのポリシーに追加します。

> **Important**
>
> バケットのアクセスコントロールをマルチリージョンアクセスポイントポリシーに委任しても、バケット名または Amazon リソースネーム (ARN) を使用してバケットに直接アクセスする場合のバケットの動作は変わりません。バケットに対して直接行われるすべてのオペレーションは、以前と同じように動作します。マルチリージョンアクセスポイントポリシーに含めた制限は、そのマルチリージョンアクセスポイントを介したリクエストにのみ適用されます。

Example 1 - (同じアカウントまたはクロスアカウントの) バケットポリシーで特定のマルチリージョンアクセスポイントへのアクセスを委任する

以下のバケットポリシーの例では、特定のマルチリージョンアクセスポイントにフルバケットアクセスを付与しています。したがって、このバケットへのすべてのアクセスは、そのマルチリージョンアクセスポイントに添付されているポリシーによってコントロールされます。バケットへの直接アクセスを必要としないすべてのユースケースでは、この方法でバケットを設定することをお勧めします。このバケットポリシー構造は、同じアカウントまたは別のアカウントのマルチリージョンアクセスポイントに使用できます。

```
{
    "Version": "2012-10-17",
    "Statement" : [
    {
        "Effect": "Allow",
        "Principal" : { "AWS": "*" },
        "Action" : "*",
        "Resource" : [ "Bucket ARN", "Bucket ARN/*"],
        "Condition": {
            "StringEquals" : { "s3:DataAccessPointArn" : "MultiRegionAccessPoint_ARN" }
        }
    }]
}
```

> **Note**
>
> アクセス権を付与する複数のマルチリージョンアクセスポイントがある場合は、必ず個々のマルチリージョンアクセスポイントを一覧表示してください。

Example 2 – マルチリージョンアクセスポイントポリシーでマルチリージョンアクセスポイントにアカウントアクセスを付与する

以下のマルチリージョンアクセスポイントポリシーでは、*MultiRegionAccessPoint_ARN* によって定義されたマルチリージョンアクセスポイントに含まれるオブジェクトを表示および読み取る *123456789012* アクセス許可をアカウントに付与します。

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
       "Effect": "Allow",
       "Principal": {
          "AWS":"arn:aws:iam::123456789012:user/JohnDoe"
       },
       "Action":[
          "s3:ListBucket",
          "s3:GetObject"
       ],
       "Resource":[
          "MultiRegionAccessPoint_ARN",
          "MultiRegionAccessPoint_ARN/object/*"
       ]
     }
  ]
}
```

Example 3 – バケットのリスト取得を許可するマルチリージョンアクセスポイントポリシー

以下のマルチリージョンアクセスポイントポリシーでは、*MultiRegionAccessPoint_ARN* によって定義されたマルチリージョンアクセスポイントに含まれるオブジェクトを表示する *123456789012* アクセス許可をアカウントに付与します。

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
       "Effect": "Allow",
       "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/JohnDoe"
        },
        "Action": "s3:ListBucket",
```

```
            "Resource": "MultiRegionAccessPoint_ARN"
        }
    ]
}
```

マルチリージョンアクセスポイントの制約および制限事項

Amazon S3 のマルチリージョンアクセスポイントには以下の制約と制限事項があります。

- マルチリージョンアクセスポイント名:
  - 1 つの AWS アカウント内で一意である
  - 数字または小文字で始める
  - 3 ~ 50 文字の長さにする
  - 名前をハイフン (-) で開始または終了することはできません。
  - 下線 (_)、大文字、ピリオド (.) は使用しない
  - 作成後は編集できない
- マルチリージョンアクセスポイントのエイリアスは Amazon S3 によって生成され、編集や再利用はできません。
- ゲートウェイエンドポイントを使用して、マルチリージョンアクセスポイントを介してデータにアクセスすることはできません。ただし、インターフェイスエンドポイントを使用して、マルチリージョンアクセスポイントを介してデータにアクセスすることはできます。AWS PrivateLink を使用するには、VPC エンドポイントを作成する必要があります。詳細については、「AWS PrivateLink で使用するマルチリージョンアクセスポイントの設定」を参照してください。
- Amazon CloudFront でマルチリージョンアクセスポイントを使用するには、マルチリージョンアクセスポイントを `Custom Origin` ディストリビューションタイプとして設定する必要があります。さまざまなオリジンタイプの詳細については、「CloudFront ディストリビューションでのさまざまなオリジンの使用」を参照してください。Amazon CloudFront でのマルチリージョンアクセスポイントの使用については、AWS ストレージブログの「Building an active-active, proximity-based application across multiple Regions」を参照してください。
- マルチリージョンアクセスポイントの最小要件 :
  - Transport Layer Security (TLS) v1.2

> **Note**
>
> Transport Layer Security (TLS) v1.3 はサポートされていません。

- 署名バージョン 4 (SigV4A)

  マルチリージョンアクセスポイントは、署名バージョン 4A をサポートします。このバージョンの SigV4 では、複数の AWS リージョン についてリクエストに署名できます。この機能は、いくつかのリージョンのいずれかからデータにアクセスする可能性がある API 操作に役立ちます。AWS SDK を使用する場合、認証情報を提供すると、マルチリージョンアクセスポイントへのリクエストでは、追加の設定なしで署名バージョン 4A が使用されます。必ず SigV4A アルゴリズムと AWS SDK との互換性を確認してください。SigV4A の詳細については、「AWS 全般のリファレンス」の「AWS API リクエストの署名」を参照してください。

  > **Note**
  >
  > 例えば AWS Identity and Access Management IAM ロールを使用する場合など、一時的なセキュリティ認証情報で SigV4A を使用するには、必ずリージョン AWS Security Token Service (AWS STS) でエンドポイントから一時的認証情報を要求してください。グローバル AWS STS エンドポイント (`sts.amazonaws.com`) から一時的な認証情報をリクエストする場合は、まず、グローバルエンドポイントに対するセッショントークンのリージョンの互換性をすべての AWS リージョンで有効に設定する必要があります。詳細については、IAM ユーザーガイドの 「AWS リージョン での AWS STS の管理」を参照してください。

- マルチリージョンアクセスポイントは、匿名リクエストをサポートしていません。
- マルチリージョンアクセスポイントの制限事項 :
  - IPv6 はサポートされていません。
  - Amazon S3 on Outposts バケットはサポートされていません。
  - マルチリージョンアクセスポイントは、マルチリージョンアクセスポイント ARN を使用する場合に限り、マルチリージョンアクセスポイントを宛先とするコピー操作をサポートします。
  - S3 バッチオペレーション機能はサポートされていません。
- 一部の AWS SDK はサポートされていません。マルチリージョンアクセスポイントでどの AWS SDK がサポートされているかを確認するには、「AWS SDK との互換性」を参照してください。
- マルチリージョンアクセスポイントの Service Quotas は、以下のとおりです。
  - アカウントごとに、最大 100 のマルチリージョンアクセスポイントです。
  - 1 つのマルチリージョンアクセスポイントには、17 リージョンの制約があります。
- マルチリージョンアクセスポイントの作成後は、マルチリージョンアクセスポイント設定でのバケットの追加、変更、または削除はできません。バケットを変更するには、マルチリージョンアク

セスポイント全体を削除し、新しいリージョンアクセスポイントを作成する必要があります。マルチリージョンアクセスポイントのクロスアカウントバケットが削除された場合、このバケットを再接続する唯一の方法は、そのアカウントで同じ名前とリージョンを使用してバケットを再作成することです。

- マルチリージョンアクセスポイントで使用されている (同じアカウントにある) 基になるバケットは、マルチリージョンアクセスポイントを削除した後でのみ削除できます。
- マルチリージョンアクセスポイントの作成または保守のすべてのコントロールプレーンリクエストは、US West (Oregon) リージョンにルーティングされる必要があります。マルチリージョンアクセスポイントのデータプレーンリクエストでは、リージョンを指定する必要はありません。
- マルチリージョンアクセスポイントのフェイルオーバーコントロールプレーンの場合、リクエストは次の 5 つのサポートされているリージョンのいずれかにルーティングされる必要があります。
  - US East (N. Virginia)
  - US West (Oregon)
  - Asia Pacific (Sydney)
  - Asia Pacific (Tokyo)
  - Europe (Ireland)
- マルチリージョンアクセスポイントは、以下の AWS リージョン のバケットのみをサポートします。
  - US East (N. Virginia)
  - US East (Ohio)
  - US West (N. California)
  - US West (Oregon)
  - Asia Pacific (Mumbai)
  - Asia Pacific (Osaka)
  - Asia Pacific (Seoul)
  - Asia Pacific (Singapore)
  - Asia Pacific (Sydney)
  - Asia Pacific (Tokyo)
  - Canada (Central)
  - Europe (Frankfurt)
  - Europe (Ireland)
  - Europe (London)

- Europe (Paris)
- Europe (Stockholm)
- South America (São Paulo)

マルチリージョンアクセスポイントリクエストのルーティング

マルチリージョンアクセスポイントを介してリクエストを行うと、Amazon S3 は、マルチリージョンアクセスポイントに関連付けられたバケットのうち、どのバケットが最も近くにあるかを決定します。Amazon S3 は、リクエストをそのバケットに送信します。これは、配置されている AWS リージョンに関わりません。

マルチリージョンアクセスポイントが最も近くにあるバケットにリクエストをルーティングすると、Amazon S3 はリクエストをそのバケットに直接送信したかのように処理します。マルチリージョンアクセスポイントは、Amazon S3 バケットのデータコンテンツを認識しません。そのため、リクエストを受け取ったバケットには、リクエストされたデータが含まれていない可能性があります。マルチリージョンアクセスポイントに関連付けられた Amazon S3 バケットに一貫性のあるデータセットを作成するには、S3 クロスリージョンレプリケーション (CRR) を設定できます。その後、どのバケットも リクエストを正常に処理します。

Amazon S3 は、次のルールに従って、マルチリージョンアクセスポイントリクエストを送信します。

- Amazon S3 は、近接の度合いに応じてリクエストが実行されるように最適化します。マルチリージョンアクセスポイントでサポートされているバケットを調べて、最も近いバケットにリクエストをリレーします。
- リクエストが既存のリソース (例えば、`GetObject`) を指定しても、Amazon S3 は、リクエストを実行するときにオブジェクトの名前を考慮しません。つまり、マルチリージョンアクセスポイントの 1 つのバケットにオブジェクトが存在する場合でも、リクエストはそのオブジェクトを含まないバケットにルーティングできるということです。この状況では、クライアント に 404 エラーメッセージが返されます。

  404 エラーを避けるには、バケットに S3 クロスリージョンレプリケーション (CRR) を設定することをお勧めします。レプリケーションにより、目的のオブジェクトがマルチリージョンアクセスポイントのバケットには存在するが、リクエストがルーティングされた特定のバケットに存在しない場合に発生する可能性のある問題を解決できます。レプリケーション設定については、「マルチリージョンアクセスポイントで使用するためのレプリケーションの設定」を参照してください。

必要な特定のオブジェクトを使用してリクエストが確実に受理されるようにするには、バケットのバージョニングを有効にし、リクエストにバージョン ID を含めることもお勧めします。このアプローチにより、探しているオブジェクトの正しいバージョンを確実に取得できます。バージョニングを有効にしたバケットでは、誤って上書きしても、オブジェクトを復旧できます。詳細については、「S3 バケットでのバージョニングの使用」を参照してください。

- リクエストがリソースを作成するものである場合 (例えば、PutObject または CreateMultipartUpload)、Amazon S3 は最も近いバケットを使用してリクエストを実行します。例えば、世界中のどこからでも動画のアップロードをサポートしたい動画会社があるとします。ユーザーが PUT リクエストをマルチリージョンアクセスポイントに送信すると、オブジェクトは最も近くにあるバケットに配置されます。アップロードした動画を世界中の他のユーザーが最短のレイテンシーでダウンロードできるようにするには、CRR と双方向レプリケーションを使用できます。CRR を双方向レプリケーションと使用すると、マルチリージョンアクセスポイントに関連付けられたすべてのバケットのコンテンツを同期された状態に維持します。マルチリージョンアクセスポイントでのレプリケーションの使用の詳細については、「マルチリージョンアクセスポイントで使用するためのレプリケーションの設定」を参照してください。

Amazon S3 マルチリージョンアクセスポイントフェイルオーバーコントロール

Amazon S3 マルチリージョンアクセスポイントのフェイルオーバーコントロールを使用すると、リージョン別トラフィックが中断してもビジネス継続性を維持できると同時に、アプリケーションをマルチリージョンアーキテクチャにしてコンプライアンスと冗長性のニーズを満たすことができます。リージョン別トラフィックが中断された場合は、マルチリージョンアクセスポイントのフェイルオーバーコントロールを使用して、Amazon S3 マルチリージョンアクセスポイントの背後にあるどの AWS リージョン がデータアクセスとストレージのリクエストを処理するかを選択できます。

フェイルオーバーをサポートするには、マルチリージョンアクセスポイントをアクティブ/パッシブ構成に設定できます。トラフィックは通常の状態ではアクティブリージョンに流れ、パッシブリージョンはフェイルオーバー用にスタンバイになります。

例えば、選択した AWS リージョン へのフェイルオーバーを行うには、プライマリ (アクティブ) リージョンからのトラフィックをセカンダリ (パッシブ) リージョンに移行します。このようなアクティブ/パッシブ構成では、一方のバケットはアクティブでトラフィックを受け入れますが、もう一方のバケットはパッシブでトラフィックを受け入れません。パッシブバケットは災害対策に使用されます。フェイルオーバーを開始すると、すべてのトラフィック (GET や PUT リクエストなど) はアクティブ状態 (1 つのリージョン内) のバケットに送られ、パッシブ状態のバケット (別のリージョン内) から離れます。

S3 クロスリージョンレプリケーション (CRR) を双方向のレプリケーションルールで有効にしている場合、フェイルオーバー中もバケットを同期された状態にしておくことができます。さらに、アクティブ/アクティブ設定で CRR を有効にしている場合、Amazon S3 マルチリージョンアクセスポイントは、最も近いバケットの場所からデータを取得できるため、アプリケーションのパフォーマンスが向上します。

AWS リージョン サポート

Amazon S3 マルチリージョンアクセスポイントのフェイルオーバーコントロールにより、S3 バケットはマルチリージョンアクセスポイントがサポートされている 17 リージョンのいずれにも存在することができます。フェイルオーバーは、任意の 2 つのリージョンで一度に開始できます。

> **Note**
>
> フェイルオーバーは一度に 2 つのリージョン間でのみ開始されますが、マルチリージョンアクセスポイントでは、同時に複数のリージョンのルーティングステータスを個別に更新できます。

以下のトピックでは、Amazon S3 マルチリージョンアクセスポイントフェイルオーバーコントロールの使用方法と管理方法について説明します。

トピック

- Amazon S3 マルチリージョンアクセスポイントルーティング状態
- Amazon S3 マルチリージョンアクセスポイントアクセスポイントフェイルオーバーコントロールの使用
- Amazon S3 マルチリージョンアクセスポイントフェイルオーバーコントロールのエラー

Amazon S3 マルチリージョンアクセスポイントルーティング状態

Amazon S3 マルチリージョンアクセスポイントのフェイルオーバー設定は、マルチリージョンアクセスポイントで使用される AWS リージョン のルーティングステータスを決定します。Amazon S3 マルチリージョンアクセスポイントは、アクティブ/アクティブ状態またはアクティブ/パッシブ状態に設定できます。

- アクティブ/アクティブ — アクティブ/アクティブ設定では、すべてのリクエストはマルチリージョンアクセスポイントの最も近い AWS リージョン に自動的に送信されます。マルチリージョンアクセスポイントをアクティブ/アクティブ状態に設定すると、すべてのリージョンがトラ

フィックを受信できます。アクティブ/アクティブ設定でトラフィックの中断が発生した場合、ネットワークトラフィックはアクティブリージョンのいずれかに自動的にリダイレクトされます。

- アクティブ/パッシブ — アクティブ/パッシブ設定では、マルチリージョンアクセスポイントのアクティブリージョンはトラフィックを受信し、パッシブリージョンはトラフィックを受信しません。災害がある状況で S3 フェイルオーバーコントロールを使用してフェイルオーバーを開始する場合は、災害対策計画のテストと実行中に、マルチリージョンアクセスポイントをアクティブ/パッシブ設定にセットアップします。

Amazon S3 マルチリージョンアクセスポイントアクセスポイントフェイルオーバーコントロールの使用

このセクションでは、AWS Management Console を使用して、Amazon S3 マルチリージョンアクセスポイントフェイルオーバーコントロールを管理および使用する方法について説明します。

AWS Management Console のマルチリージョンアクセスポイントの詳細ページの [Failover configuration] (フェイルオーバーの設定) セクションには、[Edit routing status] (ルーティングステータスの編集) と[Failover] (フェイルオーバー) の 2 つのフェイルオーバーコントロールがあります。これらのコントロールは以下のように使用できます。

- [Edit routing status] (ルーティングステータスの編集) — [Edit routing status] (ルーティングステータスの編集) を選択すると、マルチリージョンアクセスポイントの 1 回のリクエストで最大 17 の AWS リージョン ルーティングステータスを手動で編集できます。[Edit routing status] (ルーティングステータスの編集) は次の目的で使用できます。
  - マルチリージョンアクセスポイントの 1 つ以上のリージョンのルーティングステータスを設定または編集する
  - 2 つのリージョンをアクティブ/パッシブ状態に設定してマルチリージョンアクセスポイントのフェイルオーバー設定を作成する
  - リージョンを手動でフェイルオーバーする
  - リージョン間でトラフィックを手動で切り替える
- [Failover] (フェイルオーバー) — [Failover] (フェイルオーバー) を選択してフェイルオーバーを開始すると、既にアクティブ/パッシブ状態に設定されている 2 つのリージョンのルーティングステータスが更新されるだけです。[Failover] (フェイルオーバー) を選択して開始したフェイルオーバー中に、2 つのリージョン間のルーティングステータスが自動的に切り替わります。

マルチリージョンアクセスポイントの、リージョンのルーティングステータスの編集

マルチリージョンアクセスポイントの詳細ページの [Failover configuration] (フェイルオーバー設定) セクションで [Edit routing status] (ルーティングステータスの編集) を選択すると、マルチリージョンアクセスポイントの 1 回のリクエストで最大 17 AWS リージョン のルーティングステータスを手動で更新できます。ただし、[Failover] (フェイルオーバー) を選択してフェイルオーバーを開始すると、既にアクティブ/パッシブ状態に設定されている 2 つのリージョンのルーティングステータスのみが更新されます。[Failover] (フェイルオーバー) を選択して開始したフェイルオーバーの間、2 つのリージョン間のルーティングステータスが自動的に切り替わります。

[Edit routing status] (ルーティングステータスの編集) (以下の手順で説明) は、次の目的で使用できます。

- マルチリージョンアクセスポイントの 1 つ以上のリージョンのルーティングステータスを設定または編集する
- 2 つのリージョンをアクティブ/パッシブ状態に設定してマルチリージョンアクセスポイントのフェイルオーバー設定を作成する
- リージョンを手動でフェイルオーバーする
- リージョン間でトラフィックを手動で切り替える

S3 コンソールの使用

マルチリージョンアクセスポイントのリージョンのルーティングステータスを更新するには

1. AWS マネジメントコンソールにサインインします。
2. https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開きます。
3. ナビゲーションペインで、[Multi-Region Access Points] (マルチリージョンアクセスポイント) を選択します。
4. 更新するマルチリージョンアクセスポイントを選択します。
5. [Replication and failover] (レプリケーションとフェイルオーバー) タブを選択します。
6. ルーティングステータスを編集するリージョンを 1 つ以上選択します。

> **Note**
>
> フェイルオーバーを開始するには、マルチリージョンアクセスポイントで少なくとも 1 つの AWS リージョン を [Active] (アクティブ) に、1 つのリージョンを [Passive] (パッシブ) に指定する必要があります。

7. [Edit routing status] (ルーティングステータスの編集) を選択します。
8. 表示されるダイアログボックスで、各リージョンの [Routing status] (ルーティングステータス) として [Active] (アクティブ) または [Passive] (パッシブ) を選択します。

   アクティブな状態では、トラフィックがリージョンにルーティングされます。パッシブな状態では、トラフィックがリージョンに誘導されなくなります。

   マルチリージョンアクセスポイントのフェイルオーバー設定を作成する場合、またはフェイルオーバーを開始する場合は、マルチリージョンアクセスポイントで少なくとも 1 つの AWS リージョン を [Active] (アクティブ) に、1 つのリージョンを [Passive] (パッシブ) に指定する必要があります。
9. [Save routing status] (ルーティングステータスを保存) を選択します。トラフィックがリダイレクトされるまでに約 2 分かかります。

マルチリージョンアクセスポイントの AWS リージョン のルーティングステータスを送信すると、ルーティングステータスの変更を検証できます。これらの変更を検証するには、Amazon CloudWatch の https://console.aws.amazon.com/cloudwatch/ にアクセスして、アクティブリージョンとパッシブリージョン間の Amazon S3 データリクエストトラフィック (GET および PUT リクエストなど) のシフトをモニタリングします。フェイルオーバー中に既存の接続は終了しません。既存の接続は、成功または失敗のステータスに達するまで継続されます。

AWS CLI の使用

> **Note**
>
> マルチリージョンアクセスポイント AWS CLI のルーティングコマンドは、次の 5 つのリージョンのいずれかに対して実行できます。
>
> - `ap-southeast-2`
> - `ap-northeast-1`
> - `us-east-1`

- us-west-2
- eu-west-1

次のコマンド例では、現在のマルチリージョンアクセスポイントのルート設定を更新します。バケットのアクティブまたはパッシブステータスを更新するには、TrafficDialPercentage の値をアクティブの場合は 100 に、パッシブの場合は 0 に設定します。この例では、*amzn-s3-demo-bucket1* がアクティブに設定され、*amzn-s3-demo-bucket2* がパッシブに設定されています。このコマンド例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3control submit-multi-region-access-point-routes
--region ap-southeast-2
--account-id 123456789012
--mrap MultiRegionAccessPoint_ARN
--route-updates Bucket=amzn-s3-demo-bucket1,TrafficDialPercentage=100
                Bucket=amzn-s3-demo-bucket2
,TrafficDialPercentage=0
```

次のコマンド例では、更新されたマルチリージョンアクセスポイントのルーティング設定を取得します。このコマンド例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3control get-multi-region-access-point-routes
--region eu-west-1
--account-id 123456789012
--mrap MultiRegionAccessPoint_ARN
```

フェイルオーバーの開始

マルチリージョンアクセスポイントの詳細ページの [Failover configuration] (フェイルオーバー設定) セクションで [Failover] (フェイルオーバー) を選択してフェイルオーバーを開始すると、Amazon S3 リクエストトラフィックは自動的に代替の AWS リージョン に移行されます。フェイルオーバープロセスは 2 分以内に完了します。

フェイルオーバーは、(マルチリージョンアクセスポイントがサポートされている 17 のリージョンのうち) 任意の 2 つの AWS リージョン で一度に開始できます。その後、フェイルオーバーイベントが AWS CloudTrail に口グインされます。フェイルオーバーが完了すると、Amazon S3 トラフィック

と、Amazon CloudWatch の新しいアクティブリージョンへのトラフィックルーティングの更新をモニタリングできます。

> **Important**
>
> データレプリケーション中にすべてのメタデータとオブジェクトをバケット間で同期させるには、フェイルオーバーコントロールを設定する前に、双方向のレプリケーションルールを作成し、レプリカ変更の同期を有効にすることをお勧めします。
> 双方向のレプリケーションルールにより、トラフィックがフェイルオーバーする Amazon S3 バケットにデータが書き込まれると、そのデータがソースバケットにレプリケートされます。レプリカ変更の同期により、双方向のレプリケーション中にオブジェクトメタデータもバケット間で確実に同期されます。
> フェイルオーバーをサポートするレプリケーションの設定については、「the section called "バケットレプリケーション"」を参照してください。

レプリケートされたバケット間のフェイルオーバーを開始するには

1. AWS マネジメントコンソールにサインインします。
2. https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開きます。
3. 左のナビゲーションペインで、[Multi-Region Access Points] (マルチリージョンアクセスポイント) を選択します。
4. フェイルオーバーを開始するために使用する、マルチリージョンアクセスポイントを選択します。
5. [Replication and failover] (レプリケーションとフェイルオーバー) タブを選択します。
6. [Failover configuration] (フェイルオーバー設定) セクションまでスクロールして、AWS リージョン を 2 つ選択します。

   > **Note**
   >
   > フェイルオーバーを開始するには、マルチリージョンアクセスポイントで少なくとも 1 つの AWS リージョン を [Active] (アクティブ) に、1 つのリージョンを [Passive] (パッシブ) に指定する必要があります。アクティブな状態では、トラフィックがリージョンに誘導されます。パッシブな状態では、トラフィックがリージョンへ誘導されなくなります。

7. [フェイルオーバー] を選択します。

8. ダイアログボックスで、再度 [Failover] (フェイルオーバー) を選択して、フェイルオーバープロセスを開始します。このプロセス中に、2 つのリージョンのルーティングステータスが自動的に切り替わります。新しいトラフィックはすべてアクティブになったリージョンに誘導され、トラフィックはパッシブになったリージョンへ誘導されなくなります。トラフィックがリダイレクトされるまでに約 2 分かかります。

   フェイルオーバープロセスを開始すると、トラフィックの変化を検証できます。これらの変更を検証するには、Amazon CloudWatch の https://console.aws.amazon.com/cloudwatch/ にアクセスして、アクティブリージョンとパッシブリージョン間の Amazon S3 データリクエストトラフィック (GET および PUT リクエストなど) のシフトをモニタリングします。フェイルオーバー中に既存の接続は終了しません。既存の接続は、成功または失敗のステータスになるまで継続されます。

Amazon S3 マルチリージョンアクセスポイントアクセスポイントルーティングコントロールを表示する

S3 コンソールの使用

Amazon S3 マルチリージョンアクセスポイントのルーティングコントロールを表示するには

1. AWS マネジメントコンソールにサインインします。
2. https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開きます。
3. 左のナビゲーションペインで、[Multi-Region Access Points] (マルチリージョンアクセスポイント) を選択します。
4. 確認するマルチリージョンアクセスポイントを選択します。
5. [Replication and failover] (レプリケーションとフェイルオーバー) タブを選択します。このページには、マルチリージョンアクセスポイントのルーティング設定の詳細と概要、関連するレプリケーションルール、およびレプリケーションメトリクスが表示されます。リージョンのルーティングステータスは、[Failover configuration] (フェイルオーバー設定) セクションで確認できます。

AWS CLI の使用

次の例の AWS CLI コマンドでは、指定されたリージョンの、現在のマルチリージョンアクセスポイントのルート設定 を取得します。このコマンドの例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3control get-multi-region-access-point-routes
--region eu-west-1
--account-id 123456789012
--mrap MultiRegionAccessPoint_ARN
```

> **Note**
>
> このコマンドは、次の 5 つのリージョンに対してのみ実行できます。
>
> - ap-southeast-2
> - ap-northeast-1
> - us-east-1
> - us-west-2
> - eu-west-1

Amazon S3 マルチリージョンアクセスポイントフェイルオーバーコントロールのエラー

マルチリージョンアクセスポイントのフェイルオーバー設定を更新すると、次のいずれかのエラーが発生する可能性があります。

- HTTP 400 Bad Request: このエラーは、フェイルオーバー設定の更新中に無効なマルチリージョンアクセスポイント ARN を入力した場合に発生する可能性があります。マルチリージョンアクセスポイント ARN は、マルチリージョンアクセスポイントポリシーを確認することで確認できます。マルチリージョンアクセスポイントポリシーを確認または更新するには、「マルチリージョンアクセスポイントポリシーの編集」を参照してください。このエラーは、Amazon S3 マルチリージョンアクセスポイントのフェイルオーバーコントロールの更新中に空の文字列またはランダムな文字列を使用した場合にも発生する可能性があります。必ずマルチリージョンアクセスポイント ARN 形式を使用してください。

  ```
  arn:aws:s3::account-id:accesspoint/MultiRegionAccessPoint_alias
  ```

- HTTP 503 Slow Down: このエラーは、短期間に送信するリクエストが多すぎる場合に発生します。拒否されたリクエストはエラーになります。
- HTTP 409 Conflict: このエラーは、2 つ以上の同時ルート設定更新リクエストが 1 つのマルチリージョンアクセスポイントを対象としている場合に発生します。最初のリクエストは成功しますが、他のリクエストはエラーで失敗します。

- HTTP 405 Method Not Allowed: このエラーは、フェイルオーバーの開始時に AWS リージョン が 1 つしかないマルチリージョンアクセスポイントを選択した場合に発生します。フェイルオーバーを開始する前に、2 つのリージョンを選択する必要があります。それ以外の場合は、エラーが返ります。

マルチリージョンアクセスポイントで使用するためのレプリケーションの設定

マルチリージョンアクセスポイントエンドポイントに対してリクエストを行うと、Amazon S3 は、最も近接したバケットにリクエストを自動的にルーティングします。この決定を行う際には、Amazon S3 ではリクエストの内容は考慮されません。オブジェクトの GET へのリクエストを行う場合、リクエストが、このオブジェクトのコピーを持たないバケットにルーティングされる可能性もあります。その場合は、HTTP ステータスコード 404 (見つかりません) エラーが表示されます。マルチリージョンアクセスポイントのリクエストルーティングの詳細については、「the section called “リクエストルーティング”」を参照してください。

リクエストを受け取るバケットに関係なく、マルチリージョンアクセスポイントでオブジェクトを取得できるようにするには、Amazon S3 クロスリージョンレプリケーションを設定する必要があります。

例えば、3 つのバケットを持つマルチリージョンアクセスポイントについて考えてみましょう。

- オブジェクト my-image.jpg を含む、リージョン US West (Oregon) の *amzn-s3-demo-bucket1* という名前のバケット
- オブジェクト my-image.jpg を含む、リージョン Asia Pacific (Mumbai) の *amzn-s3-demo-bucket2* という名前のバケット
- オブジェクトmy-image.jpg を含まないリージョン Europe (Frankfurt) の *amzn-s3-demo-bucket* という名前のバケット

このような状況では、オブジェクト my-image.jpg に対して GetObject リクエストを行った場合、そのリクエストの成功は、どのバケットがリクエストを受け取ったかによって異なります。Amazon S3 はリクエストの内容を考慮しないため、バケットが最も近接していると応答する場合、GetObject リクエストを *amzn-s3-demo-bucket* バケットにルーティングします。オブジェクトがマルチリージョンアクセスポイントのバケット内にある場合でも、リクエストを受け取った個々のバケットにオブジェクトが含まれていないため、404 Not Found エラーが発生します。

クロスリージョンレプリケーション (CRR) を有効にすると、この結果を回避できます。適切なレプリケーションルールを使用すると、my-image.jpg オブジェクトは *amzn-s3-demo-bucket* バ

ケットにコピーされます。そのため、Amazon S3 がリクエストをそのバケットにルーティングすれば、オブジェクトを取得できるようになります。

レプリケーションは、マルチリージョンアクセスポイントに割り当てられているバケットでは通常どおりに機能します。Amazon S3 は、マルチリージョンアクセスポイントにあるバケットに対して特別なレプリケーション処理を実行しません。バケットでレプリケーションを設定する方法については、「ライブレプリケーションの設定の概要」を参照してください。

マルチリージョンアクセスポイントでのレプリケーションの使用に関する推奨事項

マルチリージョンアクセスポイントでの操作時にレプリケーションパフォーマンスを最大限に高めたい場合は、次のことをお勧めします。

- S3 Replication Time Control (S3 RTC) を設定します。S3 RTC を使用して、予測可能な時間枠内で異なるリージョン間でデータをレプリケートできます。S3 RTC は、Simple Storage Service (Amazon S3) 内に保存されている新規オブジェクトの 99.99% を 15 分以内にレプリケートします (サービスレベルアグリーメントに基づく)。詳細については、「the section called “S3 Replication Time Control の有効化”」を参照してください。S3 RTC を使用するための追加料金はかかります。詳細については、「Amazon S3 の料金」を参照してください。
- また、双方向レプリケーションを有効にして、マルチリージョンアクセスポイントを介してバケットが更新されるときにバケットの同期を維持することをサポートします。詳細については、「the section called “マルチリージョンアクセスポイント用の双方向レプリケーションルールを作成する”」を参照してください。
- クロスアカウントのマルチリージョンアクセスポイントを作成して、AWS アカウント データを別のバケットに複製します。このアプローチでは、アカウントレベルで分離できるため、ソースバケット以外のさまざまなリージョンのさまざまなアカウントからデータにアクセスして、データを複製できます。クロスアカウントのマルチリージョンアクセスポイントの設定には、追加費用はかかりません。バケットの所有者であっても、マルチリージョンアクセスポイントを所有していない場合、データ転送とリクエストの費用のみがかかります。マルチリージョンアクセスポイントの所有者の場合は、データルーティングとインターネットアクセラレーションの費用がかかります。詳細については、「Amazon S3 の料金」を参照してください。
- 各レプリケーションルールでレプリカ変更同期を有効にすると、オブジェクトへのメタデータの変更も同期されます。詳細については、「レプリカ変更の同期の有効化する」を参照してください。
- Amazon CloudWatch メトリクスを有効にして、レプリケーションイベントをモニタリングします。CloudWatch メトリクス料金が適用されます。詳細については、「Amazon CloudWatch の料金」を参照してください。

トピック

- マルチリージョンアクセスポイント用の一方向レプリケーションルールを作成する
- マルチリージョンアクセスポイント用の双方向レプリケーションルールを作成する
- マルチリージョンアクセスポイント用のレプリケーションルールを表示する

マルチリージョンアクセスポイント用の一方向レプリケーションルールを作成する

レプリケーションルールでは、異なるバケット間でオブジェクトを自動的に非同期コピーできます。一方向レプリケーションルールを使用すると、1 つの AWS リージョン のソースバケットから別のリージョンの送信先バケットにデータを完全に、確実にレプリケートできます。一方向レプリケーションを設定する場合は、レプリケート元バケット (*amzn-s3-demo-bucket*) からレプリケート先バケット (*amzn-s3-demo-bucket*) へのレプリケーションルールが作成されます。これらの一方向レプリケーションルールは、すべてのレプリケーションルールと同様に、Amazon S3 バケット全体に適用することも、オブジェクトのサブセットをプレフィックスまたはオブジェクトタグでフィルタリングして適用することも可能です。

> **Important**
>
> ユーザーがレプリケート先バケット内のオブジェクトのみを使用する場合は、一方向レプリケーションを使用することをお勧めします。ユーザーがレプリケート先バケットのオブジェクトをアップロードまたは変更する場合は、双方向レプリケーションを使用してすべてのバケットを同期させてください。また、マルチリージョンアクセスポイントをフェイルオーバーに使用する場合は、双方向レプリケーションをお勧めします。双方向レプリケーションを設定するには、「the section called “マルチリージョンアクセスポイント用の双方向レプリケーションルールを作成する”」を参照してください。

マルチリージョンアクセスポイント用の一方向レプリケーションルールを作成するには

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. ナビゲーションペインで、[Multi-Region Access Points] (マルチリージョンアクセスポイント) を選択します。
3. マルチリージョンアクセスポイント名を選択します。
4. [Replication and failove] (レプリケーションとフェイルオーバー) タブを選択します。

5. [Replication rules] (レプリケーションルール) セクションまでスクロールして、[Create replication rules] (レプリケーションルールの作成) を選択します。レプリケーションルールを作成するための十分なアクセス権限があることを確認してください。権限がないと、バージョニングが無効になります。

   > **Note**
   >
   > レプリケーションルールは、自分が所有するアカウントのバケットに対してのみ作成できます。外部バケットのレプリケーションルールを作成するには、バケットの所有者がそれらのバケットのレプリケーションルールを作成する必要があります。

6. [レプリケーションルールの作成] ページで、[1 つ以上のレプリケート元バケットから 1 つ以上のレプリケート先バケットにオブジェクトをレプリケート] テンプレートを選択します。

   > **Important**
   >
   > このテンプレートを使用してレプリケーションルールを作成すると、バケットに既に割り当てられている既存のレプリケーションルールが置き換えられます。
   > 既存のレプリケーションルールを置き換える代わりに追加または変更するには、コンソールで各バケットの [Management] (管理) タブに移動し、[Replication rules] (レプリケーションルール) セクションでルールを編集します。AWS CLI (SDK)、または REST API を使用して、既存のレプリケーションルールを追加または変更することもできます。詳細については、「レプリケーション設定ファイル要素」を参照してください。

7. [送信元と送信先] セクションの [レプリケート元バケット] で、オブジェクトのレプリケート元となるバケットを 1 つ以上選択します。レプリケーション用に選択したすべてのバケット (レプリケート元とレプリケート先) では S3 バージョニングが有効になっている必要があり、各バケットは異なる AWS リージョン に配置されている必要があります。オブジェクトのバージョニングを管理する方法の詳細については、「S3 バケットでのバージョニングの使用」を参照してください。

   [レプリケート先バケット] セクションで、オブジェクトのレプリケート先となるバケットを 1 つ以上選択します。

8. [Replication rule configuration] (レプリケーションルール設定) セクションで、作成時にレプリケーションルールを[Enabled] (有効) にするか [Disabled] (無効) にするかを選択します。

> **Note**
>
> [Replication rule name] (レプリケーションルール名) ボックスに名前を入力することはできません。レプリケーションルール名は、レプリケーションルールを作成したときの構成に基づいて生成されます。

9. [Scope] (スコープ) セクションで、レプリケーションに適したスコープを選択します。

   - バケット全体をレプリケートするには、[Apply to all objects in the bucket] (バケット内のすべてのオブジェクトに適用) を選択します。
   - バケットのオブジェクトのサブセットをレプリケートするには、[Limit the scope of this rule using one or more filters] (1 つまたは複数のフィルターを使用してこのルールの適用範囲を制限します) を選択します。

     プレフィックス、オブジェクトタグ、またはその両方の組み合わせでフィルターできます。

     - 同じ文字列で始まる名前 (`pictures` など) をもつすべてのオブジェクトにレプリケーションを制限するには、[Prefix] (プレフィクス) ボックスにプレフィックスを入力します。

       フォルダの名前をプレフィックスとして入力する場合は、/ (スラッシュ) などの区切り文字を使用して、階層のレベルを示す必要があります (例:`pictures/`)。プレフィックスの詳細については、「プレフィックスを使用してオブジェクトを整理する」を参照してください。
     - 1 つまたは複数のオブジェクトタグを持つすべてのオブジェクトをレプリケートするには、[Add tag] (タグを追加) を選択し、ボックスにキーと値のペアを入力します。別のタグを追加するには、この手順を繰り返します。オブジェクトタグの詳細については、タグを使用してストレージを分類するを参照してください。

10. [Additional replication options] (その他のレプリケーションオプション) セクションまでスクロールして、適用するレプリケーションオプションを選択します。

> **Note**
>
> 以下のオプションの適用をお勧めします。
>
> - S3 Replication Time Control (S3 RTC) – 予測可能な時間枠内で異なるリージョン間でデータをレプリケートするには、S3 Replication Time Control (S3 RTC) を使用します。S3 RTC は、Simple Storage Service (Amazon S3) 内に保存されている新規オブジェクトの 99.99% を 15 分以内にレプリケートします (サービスレベルアグリーメン

トに基づく)。詳細については、「the section called “S3 Replication Time Control の有効化”」を参照してください。

- レプリケーションメトリクスと通知 – Amazon CloudWatch メトリクスを有効にして、レプリケーションイベントをモニタリングできます。
- 削除マーカーのレプリケーション — S3 の削除オペレーションによって作成された削除マーカーがレプリケートされます。ライフサイクルルールによって作成された削除マーカーはレプリケートされません。詳細については、「バケット間での削除マーカーのレプリケーション」を参照してください。

S3 RTC と CloudWatch のレプリケーションメトリクスと通知には追加料金がかかります。詳細については、「Amazon S3 の料金」および「Amazon CloudWatch の料金」を参照してください。

11. 既存のレプリケーションルールを置き換える新しいレプリケーションルールを作成する場合は、[Create replication rules] (レプリケーションルールを作成) を選択すると、既存のレプリケーションルールが上書きされることに同意します。
12. [レプリケーションルールの作成] を選択し、新しい一方向レプリケーションルールを作成して保存します。

マルチリージョンアクセスポイント用の双方向レプリケーションルールを作成する

レプリケーションルールでは、異なるバケット間でオブジェクトを自動的に非同期コピーできます。双方向レプリケーションルールは、異なる AWS リージョン にあるデータが複数のバケット間で完全に同期されることを保証します。双方向レプリケーションを設定する場合、レプリケート元バケット (DOC-EXAMPLE-BUCKET-1) から、レプリカが含まれているバケット (DOC-EXAMPLE-BUCKET-2) に対するレプリケーションルールを作成します。次に、レプリカを含むバケット (DOC-EXAMPLE-BUCKET-2) からレプリケート元バケット (DOC-EXAMPLE-BUCKET-1) に対する 2 つ目のレプリケーションルールを作成します。

これらの双方向レプリケーションルールは、すべてのレプリケーションルールと同様に、Amazon S3 バケット全体に適用することも、オブジェクトのサブセットをプレフィックスまたはオブジェクトタグでフィルタリングして適用することも可能です。各レプリケーションルールでレプリカ変更同期を有効にすると、オブジェクトへのメタデータの変更も同期されます。Amazon S3 コンソール、AWS CLI、AWS SDK、Amazon S3 REST API、または AWS CloudFormation を使用して、レプリカ変更の同期を有効にすることができます。

Amazon CloudWatch のオブジェクトとオブジェクトメタデータのレプリケーションの進行状況をモニタリングするには、S3 レプリケーションメトリクスと通知を有効にします。詳細については、「レプリケーションメトリクスと Amazon S3 イベント通知による、進捗状況のモニタリング」を参照してください。

マルチリージョンアクセスポイント用の双方向レプリケーションルールを作成するには

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. ナビゲーションペインで、[Multi-Region Access Points] (マルチリージョンアクセスポイント) を選択します。
3. 更新するマルチリージョンアクセスポイントの名前を選択します。
4. [Replication and failove] (レプリケーションとフェイルオーバー) タブを選択します。
5. [Replication rules] (レプリケーションルール) セクションまでスクロールして、[Create replication rules] (レプリケーションルールの作成) を選択します。
6. [Create replication rules] (レプリケーションルールの作成) ページで、[Replicate objects among all specified buckets] (指定されたすべてのバケット間でオブジェクトをレプリケート) テンプレートを選択します。[Replicate objects among all specified buckets] (指定されたすべてのバケット間でオブジェクトをレプリケート) テンプレートは、バケットの双方向レプリケーション (フェイルオーバー機能付き) を設定します。

   > **Important**
   >
   > このテンプレートを使用してレプリケーションルールを作成すると、バケットに既に割り当てられている既存のレプリケーションルールが置き換えられます。
   > 既存のレプリケーションルールを置き換える代わりに追加または変更するには、コンソールで各バケットの [Management] (管理) タブに移動し、[Replication rules] (レプリケーションルール) セクションでルールを編集します。AWS CLI、AWS SDK、または Amazon S3 REST API を使用して既存のレプリケーションルールを追加または変更することもできます。詳細については、「レプリケーション設定ファイル要素」を参照してください。

7. [Buckets] (バケット) セクションで、オブジェクトの複製元となるバケットを少なくとも 2 つ選択します。レプリケーション用に選択したすべてのバケットで S3 バージョニングが有効になっている必要があり、各バケットは異なる AWS リージョン にある必要があります。オブジェク

トのバージョニングを管理する方法の詳細については、「S3 バケットでのバージョニングの使用」を参照してください。

> **Note**
>
> レプリケーションを確立するために必要な読み取り権限とレプリケート権限があることを確認してください。権限がないと、エラーが発生します。詳細については、「IAM ロールの作成」を参照してください。

8. [Replication rule configuration] (レプリケーションルール設定) セクションで、作成時にレプリケーションルールを[Enabled] (有効) にするか [Disabled] (無効) にするかを選択します。

> **Note**
>
> [Replication rule name] (レプリケーションルール名) ボックスに名前を入力することはできません。レプリケーションルール名は、レプリケーションルールを作成したときの構成に基づいて生成されます。

9. [Scope] (スコープ) セクションで、レプリケーションに適したスコープを選択します。

   - バケット全体をレプリケートするには、[Apply to all objects in the bucket] (バケット内のすべてのオブジェクトに適用) を選択します。
   - バケットのオブジェクトのサブセットをレプリケートするには、[Limit the scope of this rule using one or more filters] (1 つまたは複数のフィルターを使用してこのルールの適用範囲を制限します) を選択します。

     プレフィックス、オブジェクトタグ、またはその両方の組み合わせでフィルターできます。

     - 同じ文字列で始まる名前 (`pictures` など) をもつすべてのオブジェクトにレプリケーションを制限するには、[Prefix] (プレフィクス) ボックスにプレフィックスを入力します。

       フォルダの名前をプレフィックスとして入力する場合は、最後の文字に / (スラッシュ) を使用する必要があります (例: `pictures/`)。
     - 1 つまたは複数のオブジェクトタグを持つすべてのオブジェクトをレプリケートするには、[Add tag] (タグを追加) を選択し、ボックスにキーと値のペアを入力します。別のタグを追加するには、この手順を繰り返します。オブジェクトタグの詳細については、タグを使用してストレージを分類するを参照してください。

10. [Additional replication options] (その他のレプリケーションオプション) セクションまでスクロールして、適用するレプリケーションオプションを選択します。

> **Note**
>
> 特にマルチリージョンアクセスポイントをフェイルオーバーをサポートするように設定する場合は、次のオプションを適用することをお勧めします。
>
> - S3 Replication Time Control (S3 RTC) – 予測可能な時間枠内で異なるリージョン間でデータをレプリケートするには、S3 Replication Time Control (S3 RTC) を使用します。S3 RTC は、Simple Storage Service (Amazon S3) 内に保存されている新規オブジェクトの 99.99% を 15 分以内にレプリケートします (サービスレベルアグリーメントに基づく)。詳細については、「the section called “S3 Replication Time Control の有効化”」を参照してください。
> - レプリケーションメトリクスと通知 – Amazon CloudWatch メトリクスを有効にして、レプリケーションイベントをモニタリングできます。
> - 削除マーカーのレプリケーション — S3 の削除オペレーションによって作成された削除マーカーがレプリケートされます。ライフサイクルルールによって作成された削除マーカーはレプリケートされません。詳細については、「バケット間での削除マーカーのレプリケーション」を参照してください。
> - レプリカ変更同期 – 各レプリケーションルールでレプリカ変更同期を有効にすると、オブジェクトへのメタデータの変更も同期されます。詳細については、「レプリカ変更の同期の有効化する」を参照してください。
>
> S3 RTC と CloudWatch のレプリケーションメトリクスと通知には追加料金がかかります。詳細については、「Amazon S3 の料金」および「Amazon CloudWatch の料金」を参照してください。

11. 既存のレプリケーションルールを置き換える新しいレプリケーションルールを作成する場合は、[Create replication rules] (レプリケーションルールを作成) を選択すると、既存のレプリケーションルールが上書きされることに同意します。
12. [Create replication rules] (レプリケーションルールを作成) を選択し、新しい双方向レプリケーションルールを作成して保存します。

マルチリージョンアクセスポイント用のレプリケーションルールを表示する

マルチリージョンアクセスポイントでは、一方向レプリケーションルールまたは双方向レプリケーションルールを設定できます。レプリケーションルールの管理方法の詳細については、「Amazon S3 コンソールを使用したレプリケーションルールの管理」を参照してください。

マルチリージョンアクセスポイント用のレプリケーションルールを表示するには

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. ナビゲーションペインで、[Multi-Region Access Points] (マルチリージョンアクセスポイント) を選択します。
3. マルチリージョンアクセスポイント名を選択します。
4. [Replication and failover] (レプリケーションとフェイルオーバー) タブを選択します。
5. [レプリケーションルール] セクションまで、下にスクロールします。このセクションには、マルチリージョンアクセスポイント用に作成されたすべてのレプリケーションルールが一覧表示されます。

> **Note**
>
> 別のアカウントから、このマルチリージョンアクセスポイントにバケットを追加した場合、そのバケットのレプリケーションルールを表示するにはバケット所有者からの `s3:GetBucketReplication` 権限が必要です。

マルチリージョンアクセスポイントでのサポートされている API オペレーションの使用

Amazon S3 は、マルチリージョンアクセスポイントを管理するための一連オペレーションを提供します。Amazon S3 は、これらのオペレーションの一部を同期的に処理し、一部を非同期的に処理します。非同期オペレーションを呼び出すと、Amazon S3 は最初にリクエストされたオペレーションを同期的に承認します。承認が成功すると、リクエストされたオペレーションの進行状況と結果を追跡するために使用できるトークンが Amazon S3 から返されます。

> **Note**
>
> Amazon S3 コンソールを介して実行されるリクエストは常に同期されます。コンソールは、リクエストが完了するまで待機してから、別のリクエストを送信できるようにします。

コンソールを使用するか、AWS CLI、AWS SDK、または REST API で `DescribeMultiRegionAccessPointOperation` を使用して、非同期オペレーションの現在のステータスと結果を表示できます。Amazon S3 は、非同期オペレーションへの応答で追跡用トークンを提供します。その追跡用トークンを、`DescribeMultiRegionAccessPointOperation` への引数として含めます。追跡用トークンを含めると、Amazon S3 はその後、エラーや関連するリソース情報を含む、指定されたオペレーションの現在のステータスと結果を返します。Amazon S3 は `DescribeMultiRegionAccessPointOperation` オペレーションを同期的に実行します。

マルチリージョンアクセスポイントの作成または保守のすべてのコントロールプレーンリクエストは、`US West (Oregon)` リージョンにルーティングされる必要があります。マルチリージョンアクセスポイントのデータプレーンリクエストでは、リージョンを指定する必要はありません。マルチリージョンアクセスポイントのフェイルオーバーコントロールプレーンの場合、リクエストは 5 つのサポートされているリージョンのいずれかにルーティングされる必要があります。マルチリージョンアクセスポイントのサポートされているリージョンの詳細については、「マルチリージョンアクセスポイントの制約および制限事項」を参照してください。

さらに、`s3:ListAllMyBuckets` アクセス許可を、ユーザー、ロール、またはマルチリージョンアクセスポイントを管理するためのリクエストを作成する他の AWS Identity and Access Management (IAM) エンティティに付与します。

以下の例は、Amazon S3 の互換性のあるオペレーションでマルチリージョンアクセスポイントを使用する方法を示しています。

トピック

- マルチリージョンアクセスポイントと AWS のサービス および AWS SDK との互換性
- S3 オペレーションとマルチリージョンアクセスポイントの互換性
- マルチリージョンアクセスポイントのルーティング設定を表示する
- 基になる Amazon S3 バケットポリシーを更新する
- マルチリージョンアクセスポイントのルート設定を更新する
- マルチリージョンアクセスポイントのバケットへのオブジェクトの追加
- マルチリージョンアクセスポイントからのオブジェクトの取得

- マルチリージョンアクセスポイントの基礎となるバケットに保存されているオブジェクトのリスト表示
- マルチリージョンアクセスポイントで署名付き URL を使用する
- マルチリージョンアクセスポイントでリクエスタ支払いが設定されたバケットを使用する

マルチリージョンアクセスポイントと AWS のサービス および AWS SDK との互換性

Amazon S3 バケット名を必要とするアプリケーションで、マルチリージョンアクセスポイントを使用するには、AWS SDK を使用してリクエストするときにマルチリージョンアクセスポイントの Amazon リソースネーム (ARN) を使用します。AWS SDK がマルチリージョンのアクセスポイントと互換性があるかどうかを確認するには、「AWS SDK との互換性」を参照してください。

S3 オペレーションとマルチリージョンアクセスポイントの互換性

次の Amazon S3 データプレーン API オペレーションを使用して、マルチリージョンアクセスポイントに関連付けられているバケット内のオブジェクトに対してアクションを実行できます。以下の S3 オペレーションでは、マルチリージョンアクセスポイント ARN を使用できます。

- AbortMultipartUpload
- CompleteMultipartUpload
- CreateMultipartUpload
- DeleteObject
- DeleteObjectTagging
- GetObject
- GetObjectAcl
- GetObjectLegalHold
- GetObjectRetention
- GetObjectTagging
- HeadObject
- ListMultipartUploads
- ListObjectsV2
- ListParts
- PutObject
- PutObjectAcl

- PutObjectLegalHold
- PutObjectRetention
- PutObjectTagging
- RestoreObject
- UploadPart

> **Note**
>
> マルチリージョンアクセスポイントは、マルチリージョンアクセスポイント ARN を使用する場合に限り、マルチリージョンアクセスポイントを宛先とするコピー操作をサポートします。

マルチリージョンアクセスポイントの作成と管理には、次の Amazon S3 コントロールプレーンオペレーションを使用できます。

- CreateMultiRegionAccessPoint
- DescribeMultiRegionAccessPointOperation
- GetMultiRegionAccessPoint
- GetMultiRegionAccessPointPolicy
- GetMultiRegionAccessPointPolicyStatus
- GetMultiRegionAccessPointRoutes
- ListMultiRegionAccessPoints
- PutMultiRegionAccessPointPolicy
- SubmitMultiRegionAccessPointRoutes

マルチリージョンアクセスポイントのルーティング設定を表示する

AWS CLI

次のコマンド例では、マルチリージョンアクセスポイントのルート設定を取得して、バケットの現在のルーティングステータスを確認できるようにします。このコマンドの例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3control get-multi-region-access-point-routes
```

```
--region eu-west-1
--account-id 111122223333
--mrap arn:aws:s3::111122223333:accesspoint/abcdef0123456.mrap
```

SDK for Java

次の SDK for Java コードは、マルチリージョンアクセスポイントのルート設定を取得して、バケットの現在のルーティングステータスを確認できるようにします。この構文例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
S3ControlClient s3ControlClient = S3ControlClient.builder()
    .region(Region.US_EAST_1)
    .credentialsProvider(credentialsProvider)
    .build();

GetMultiRegionAccessPointRoutesRequest request =
 GetMultiRegionAccessPointRoutesRequest.builder()
    .accountId("111122223333")
    .mrap("arn:aws:s3::111122223333:accesspoint/abcdef0123456.mrap")
    .build();

GetMultiRegionAccessPointRoutesResponse response =
 s3ControlClient.getMultiRegionAccessPointRoutes(request);
```

SDK for JavaScript

次の SDK for JavaScript コードは、マルチリージョンアクセスポイントのルート設定を取得して、バケットの現在のルーティングステータスを確認できるようにします。この構文例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
const REGION = 'us-east-1'

const s3ControlClient = new S3ControlClient({
  region: REGION
})

export const run = async () => {
  try {
    const data = await s3ControlClient.send(
      new GetMultiRegionAccessPointRoutesCommand({
        AccountId: '111122223333',
        Mrap: 'arn:aws:s3::111122223333:accesspoint/abcdef0123456.mrap',
      })
```

```
    )
    console.log('Success', data)
    return data
  } catch (err) {
    console.log('Error', err)
  }
}

run()
```

SDK for Python

次の SDK for Python コードは、マルチリージョンアクセスポイントのルート設定を取得して、バケットの現在のルーティングステータスを確認できるようにします。この構文例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
s3.get_multi_region_access_point_routes(
        AccountId=111122223333,
        Mrap=arn:aws:s3::111122223333:accesspoint/abcdef0123456.mrap)['Routes']
```

基になる Amazon S3 バケットポリシーを更新する

適切なアクセスを許可するには、基になる Amazon S3 バケットポリシーも更新する必要があります。以下の例では、アクセスコントロールをマルチリージョンアクセスポイントポリシーに委任します。マルチリージョンアクセスポイントポリシーにアクセスコントロールを委任すると、マルチリージョンアクセスポイントを介してリクエストを行うときバケットポリシーがアクセスコントロールに使用されなくなります。

マルチリージョンアクセスポイントポリシーにアクセスコントロールを委任するバケットポリシーの例を次に示します。このバケットポリシーの例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。このポリシーを AWS CLI `put-bucket-policy` コマンドを使用して適用するには、次の例に示すように、ポリシーをファイルに保存します (例：`policy.json`)。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Principal": { "AWS": "*" },
    "Effect": "Allow",
    "Action": ["s3:*"],
    "Resource": ["arn:aws:s3:::111122223333/*", "arn:aws:s3:::amzn-s3-demo-bucket"],
```

```
    "Condition": {
      "StringEquals": {
        "s3:DataAccessPointAccount": "444455556666"
      }
    }
  }
}
```

次の put-bucket-policy 例では、更新された S3 バケットポリシーを S3 バケットに関連付けます。

```
aws s3api put-bucket-policy
  --bucket amzn-s3-demo-bucket
  --policy file:///tmp/policy.json
```

マルチリージョンアクセスポイントのルート設定を更新する

以下のコマンド例では、マルチリージョンアクセスポイントのルート設定も更新します。マルチリージョンアクセスポイントのルートコマンドは、次の 5 つのリージョンに対して実行できます。

- ap-southeast-2
- ap-northeast-1
- us-east-1
- us-west-2
- eu-west-1

マルチリージョンアクセスポイントのルーティング設定では、バケットをアクティブまたはパッシブのルーティングステータスに設定できます。アクティブバケットはトラフィックを受信しますが、パッシブバケットは受信しません。バケットの TrafficDialPercentage 値を 100 に設定するとアクティブ、0 に設定するとパッシブになり、バケットのルーティングステータスを設定できます。

AWS CLI

以下のコマンド例では、マルチリージョンアクセスポイントのルーティング設定も更新します。この例では、*amzn-s3-demo-bucket1* がアクティブステータスに設定され、*amzn-s3-demo-bucket2* がパッシブに設定されています。このコマンドの例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3control submit-multi-region-access-point-routes
```

```
--region ap-southeast-2
--account-id 111122223333
--mrap arn:aws:s3::111122223333:accesspoint/abcdef0123456.mrap
--route-updates Bucket=amzn-s3-demo-bucket1,TrafficDialPercentage=100
                Bucket=amzn-s3-demo-bucket2,TrafficDialPercentage=0
```

SDK for Java

次の SDK for Java コードは、マルチリージョンアクセスポイントのルーティング設定も更新します。この構文例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
S3ControlClient s3ControlClient = S3ControlClient.builder()
    .region(Region.ap-southeast-2)
    .credentialsProvider(credentialsProvider)
    .build();

SubmitMultiRegionAccessPointRoutesRequest request =
 SubmitMultiRegionAccessPointRoutesRequest.builder()
    .accountId("111122223333")
    .mrap("arn:aws:s3::111122223333:accesspoint/abcdef0123456.mrap")
    .routeUpdates(
        MultiRegionAccessPointRoute.builder()
            .region("eu-west-1")
            .trafficDialPercentage(100)
            .build(),
        MultiRegionAccessPointRoute.builder()
            .region("ca-central-1")
            .bucket("111122223333")
            .trafficDialPercentage(0)
            .build()
    )
    .build();

SubmitMultiRegionAccessPointRoutesResponse response =
 s3ControlClient.submitMultiRegionAccessPointRoutes(request);
```

SDK for JavaScript

次の SDK for JavaScript コードは、マルチリージョンアクセスポイントのルート設定も更新します。この構文例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
const REGION = 'ap-southeast-2'

const s3ControlClient = new S3ControlClient({
  region: REGION
})

export const run = async () => {
  try {
    const data = await s3ControlClient.send(
      new SubmitMultiRegionAccessPointRoutesCommand({
        AccountId: '111122223333',
        Mrap: 'arn:aws:s3::111122223333:accesspoint/abcdef0123456.mrap',
        RouteUpdates: [
          {
            Region: 'eu-west-1',
            TrafficDialPercentage: 100,
          },
          {
            Region: 'ca-central-1',
            Bucket: 'amzn-s3-demo-bucket1',
            TrafficDialPercentage: 0,
          },
        ],
      })
    )
    console.log('Success', data)
    return data
  } catch (err) {
    console.log('Error', err)
  }
}

run()
```

SDK for Python

次の SDK for Python コードは、マルチリージョンアクセスポイントのルート設定も更新します。この構文例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
s3.submit_multi_region_access_point_routes(
        AccountId=111122223333,
        Mrap=arn:aws:s3::111122223333:accesspoint/abcdef0123456.mrap,
```

```
        RouteUpdates= [{
            'Bucket': amzn-s3-demo-bucket,
            'Region': ap-southeast-2,
            'TrafficDialPercentage': 10
        }])
```

マルチリージョンアクセスポイントのバケットへのオブジェクトの追加

マルチリージョンアクセスポイントに関連付けられているバケットにオブジェクトを追加するには、PutObject オペレーションを使用できます。マルチリージョンアクセスポイントのすべてのバケットを同期させるには、[クロスリージョンレプリケーション] を有効にします。

> **Note**
>
> このオペレーションを使用するには、マルチリージョンアクセスポイントの `s3:PutObject` アクセス許可が必要です。マルチリージョンアクセスポイントのアクセス許可の要件の詳細については、「アクセス許可」を参照してください。

AWS CLI

次の例のデータプレーンリクエストは、指定されたマルチリージョンアクセスポイントに *example.txt* をアップロードします。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3api put-object --bucket
 arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap --key example.txt --
body example.txt
```

SDK for Java

```
S3Client s3Client = S3Client.builder()
        .build();

PutObjectRequest objectRequest = PutObjectRequest.builder()
        .bucket("arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap")
        .key("example.txt")
        .build();

s3Client.putObject(objectRequest, RequestBody.fromString("Hello S3!"));
```

SDK for JavaScript

```
const client = new S3Client({});

async function putObjectExample() {
    const command = new PutObjectCommand({
        Bucket: "arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap",
        Key: "example.txt",
        Body: "Hello S3!",
    });

    try {
        const response = await client.send(command);
        console.log(response);
    } catch (err) {
        console.error(err);
    }
}
```

SDK for Python

```
import boto3

client = boto3.client('s3')
client.put_object(
    Bucket='arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap',
    Key='example.txt',
    Body='Hello S3!'
)
```

マルチリージョンアクセスポイントからのオブジェクトの取得

マルチリージョンアクセスポイントからオブジェクトを取得するには、GetObject オペレーションを使用できます。

> **Note**
>
> この API オペレーションを使用するには、マルチリージョンアクセスポイントの s3:GetObject アクセス許可が必要です。マルチリージョンアクセスポイントのアクセス許可の要件の詳細については、「アクセス許可」を参照してください。

AWS CLI

次のデータプレーンリクエストの例では、指定されたマルチリージョンアクセスポイントから *example.txt* を取得し、それを *downloaded_example.txt* としてダウンロードします。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3api get-object --bucket
 arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap --
key example.txt downloaded_example.txt
```

SDK for Java

```
S3Client s3 = S3Client
   .builder()
   .build();

GetObjectRequest getObjectRequest = GetObjectRequest.builder()
    .bucket("arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap")
    .key("example.txt")
    .build();

s3Client.getObject(getObjectRequest);
```

SDK for JavaScript

```
const client = new S3Client({})

async function getObjectExample() {
    const command = new GetObjectCommand({
        Bucket: "arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap",
        Key: "example.txt"
    });

    try {
        const response = await client.send(command);
        console.log(response);
    } catch (err) {
        console.error(err);
    }
}
```

SDK for Python

```
import boto3

client = boto3.client('s3')
client.get_object(
    Bucket='arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap',
    Key='example.txt'
)
```

マルチリージョンアクセスポイントの基礎となるバケットに保存されているオブジェクトのリスト表示

マルチリージョンアクセスポイントの基礎となるバケットに保存されたオブジェクトのリストを返すには、ListObjectsV2 オペレーションを使用します。次のコマンド例では、マルチリージョンアクセスポイントの ARN を使用して、マルチリージョンアクセスポイントのすべてのオブジェクトがリスト表示されます。この場合、マルチリージョンアクセスポイントの ARN は次のようになります。

`arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap`

> **Note**
>
> この API オペレーションを使用するには、マルチリージョンアクセスポイントと基礎となるバケットの `s3:ListBucket` アクセス許可が必要です。マルチリージョンアクセスポイントのアクセス許可の要件の詳細については、「アクセス許可」を参照してください。

AWS CLI

次のデータプレーンリクエストの例では、ARN で指定されたマルチリージョンアクセスポイントの基礎となるバケット内のオブジェクトをリスト表示します。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3api list-objects-v2 --bucket
 arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap
```

SDK for Java

```
S3Client s3Client = S3Client.builder()
```

```
        .build();

String bucketName = "arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap";

ListObjectsV2Request listObjectsRequest = ListObjectsV2Request
    .builder()
    .bucket(bucketName)
    .build();

 s3Client.listObjectsV2(listObjectsRequest);
```

SDK for JavaScript

```
const client = new S3Client({});

async function listObjectsExample() {
    const command = new ListObjectsV2Command({
        Bucket: "arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap",
    });

    try {
        const response = await client.send(command);
        console.log(response);
    } catch (err) {
        console.error(err);
    }
}
```

SDK for Python

```
import boto3

client = boto3.client('s3')
client.list_objects_v2(
    Bucket='arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap'
)
```

マルチリージョンアクセスポイントで署名付き URL を使用する

署名付き URL を使用すると、他のユーザーが Amazon S3 マルチリージョンアクセスポイントを介して Amazon S3 バケットにアクセスするための URL を生成することができます。署名付

き URL を作成したら、その署名付き URL を S3 アップロード (PutObject) や S3 ダウンロード (GetObject) などの特定のオブジェクトアクションに関連付けます。署名付き URL を共有すると、URL へのアクセス権を持つユーザーは、URL に埋め込まれたアクションを、元の署名ユーザーであるかのように実行できます。

署名付き URL には有効期限があります。有効期限に達すると、URL は機能しなくなります。

署名付き URL で S3 マルチリージョンアクセスポイントを使用する前に、Sigv4A アルゴリズムと AWS SDK との互換性を確認してください。ご使用の SDK バージョンが、グローバル AWS リージョン リクエストの署名に使用される署名実装として SigV4AA をサポートしていることを確認してください。Amazon S3 での署名付き URL の使用について詳しくは、「Sharing objects by using presigned URL」(署名付き URL を使用してオブジェクトを共有する) を参照してください。

以下の例は、署名付き URL と共にマルチリージョンアクセスポイントを使用する方法を示しています。これらの例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

AWS CLI

```
aws s3 presign
 arn:aws:s3::123456789012:accesspoint/MultiRegionAccessPoint_alias/example-file.txt
```

SDK for Python

```
import logging
import boto3
from botocore.exceptions import ClientError

s3_client = boto3.client('s3',aws_access_key_id='xxx',aws_secret_access_key='xxx')
s3_client.generate_presigned_url(HttpMethod='PUT',ClientMethod="put_object",
 Params={'Bucket':'arn:aws:s3::123456789012:accesspoint/
abcdef0123456.mrap','Key':'example-file'})
```

SDK for Java

```
S3Presigner s3Presigner = S3Presigner.builder()
    .credentialsProvider(StsAssumeRoleCredentialsProvider.builder()
        .refreshRequest(assumeRole)
        .stsClient(stsClient)
        .build())
```

```
    .build();

GetObjectRequest getObjectRequest = GetObjectRequest.builder()
    .bucket("arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap")
    .key("example-file")
    .build();

GetObjectPresignRequest preSignedReq = GetObjectPresignRequest.builder()
    .getObjectRequest(getObjectRequest)
    .signatureDuration(Duration.ofMinutes(10))
    .build();

PresignedGetObjectRequest presignedGetObjectRequest =
 s3Presigner.presignGetObject(preSignedReq);
```

> **Note**
>
> SigV4A を一時的なセキュリティ認証情報と共に使用する場合、例えば IAM ロールを使用する場合には、必ずグローバルエンドポイントではなく、AWS Security Token Service (AWS STS) 内のリージョンエンドポイントから一時的認証情報をリクエストしてください。AWS STS (sts.amazonaws.com) にグローバルエンドポイントを使用すると、AWS STS はグローバルエンドポイントから、Sig4A ではサポートされていない一時的な認証情報を生成します。その結果、エラーが発生します。この問題を解決するには、AWS STS 用のリージョンエンドポイントにリストされているいずれかのエンドポイントを使用してください。

マルチリージョンアクセスポイントでリクエスタ支払いが設定されたバケットを使用する

マルチリージョンアクセスポイントに関連付けられている S3 バケットがリクエスタ支払いを使用するように設定されている場合、リクエスタはバケットリクエスト、ダウンロードおよびマルチリージョンアクセスポイントに関連する費用を支払います。詳細については、「Amazon S3 の料金」を参照してください。

リクエスタ支払いバケットに接続されたマルチリージョンアクセスポイントへのデータプレーンリクエストの例を次に示します。

AWS CLI

リクエスタ支払いバケットに接続したマルチリージョンアクセスポイントからオブジェクトをダウンロードするには、get-object リクエストの一部として `--request-payer requester` を指

定する必要があります。また、バケット内のファイルの名前と、ダウンロードファイルを保存する場所を指定する必要があります。

```
aws s3api get-object --bucket MultiRegionAccessPoint_ARN --request-payer requester
 --key example-file-in-bucket.txt example-location-of-downloaded-file.txt
```

SDK for Java

リクエスタ支払いバケットに接続したマルチリージョンアクセスポイントからオブジェクトをダウンロードするには、GetObject リクエストの一部として RequestPayer.REQUESTER を指定する必要があります。また、バケット内のファイルの名前と、ファイルを保存する場所を指定する必要があります。

```
GetObjectResponse getObjectResponse = s3Client.getObject(GetObjectRequest.builder()
    .key("example-file.txt")
    .bucket("arn:aws:s3::
123456789012:accesspoint/abcdef0123456.mrap")
    .requestPayer(RequestPayer.REQUESTER)
    .build()
).response();
```

マルチリージョンアクセスポイントから基盤となるリソースへのリクエストのモニタリングとログ記録

Amazon S3 は、マルチリージョンアクセスポイントを介して行われたリクエストと、アクセスポイントを管理する API オペレーションに対するリクエスト (CreateMultiRegionAccessPoint や GetMultiRegionAccessPointPolicy など) をログに記録します。マルチリージョンアクセスポイントを介して Amazon S3 に行われたリクエストは、アクセスポイントのホスト名と共に、Amazon S3 サーバーのアクセスログと AWS CloudTrail のログに表示されます。アクセスポイントのホスト名は、*MRAP_alias*.accesspoint.s3-global.amazonaws.com という形式になります。例えば、次のバケットとマルチリージョンアクセスポイントの設定があるとします。

- オブジェクト my-image.jpg を含む、リージョン us-west-2 の my-bucket-usw2 という名前のバケット。
- オブジェクト my-image.jpg を含む、リージョン ap-south-1 の my-bucket-aps1 という名前のバケット。
- my-image.jpg という名前のオブジェクト を含まないリージョン eu-central-1 の my-bucket-euc1 という名前のバケット。

- 名前が my-mrap であり、エイリアスが mfzwi23gnjvgw.mrap であるマルチリージョンアクセスポイントは、3 つのバケットすべてからのリクエストを満たすように設定されています。
- お客様の AWS アカウント ID は 123456789012 です。

バケットから my-image.jpg を直接取得するリクエストは、ホスト名 *bucket_name*.s3.*Region*.amazonaws.com と共にログに表示されます。

代わりにマルチリージョンアクセスポイント経由でリクエストを行うと、Amazon S3 は最初に、異なるリージョン内のバケットのうち、どれが最も近いかを判断します。Amazon S3 は、リクエストを処理するために使用するバケットを決定した後、そのバケットにリクエストを送信し、マルチリージョンアクセスポイントのホスト名を使用してオペレーションを記録します。この例では、Amazon S3 がリクエストを my-bucket-aps1 にリレーした場合、ログはホスト名 mfzwi23gnjvgw.mrap.accesspoint.s3-global.amazonaws.com を使用して、my-bucket-aps1 から、my-image.jpg に対して成功した GET リクエストを反映します。

> **Important**
>
> マルチリージョンアクセスポイントは、基になるバケットのデータコンテンツを認識しません。そのため、リクエストを受け取ったバケットには、リクエストされたデータが含まれていない可能性があります。例えば、Amazon S3 が my-bucket-euc1 バケットが最も低いと判断した場合、ログはホスト名 mfzwi23gnjvgw.mrap.accesspoint.s3-global.amazonaws.com を使用して、my-bucket-euc1 から my-image.jpg に対して失敗した GET リクエストを反映します。リクエストが代わりに my-bucket-usw2 にルーティングされると、ログは成功した GET リクエストを表示します。

Amazon S3 サーバーのアクセスログの詳細については、「サーバーアクセスログによるリクエストのログ記録」を参照してください。AWS CloudTrail の詳細については、AWS CloudTrail ユーザーガイド の AWS CloudTrail とは を参照してください。

マルチリージョンアクセスポイント管理 API オペレーションに対するリクエストのモニタリングとログ記録

Amazon S3 は、CreateMultiRegionAccessPoint および GetMultiRegionAccessPointPolicy など、マルチリージョンアクセスポイントを管理するためのいくつかの API オペレーションを提供します。AWS Command Line Interface (AWS CLI)、AWS SDK、または Amazon S3 REST API を使用して、これらの API オペレーションにリクエストを実行すると、Amazon S3 はこれらのリクエストを非同期的に処理します。リクエストに対して適

切な許可がある場合、Amazon S3 は、リクエストに対してトークンを返します。このトークンは、`DescribeAsyncOperation` が実行中の非同期オペレーションのステータスを表示するのに役立ちます。Amazon S3 は、`DescribeAsyncOperation` リクエストを同期的に処理します。非同期リクエストのステータスを表示するには、Amazon S3 コンソール、AWS CLI、SDK、または REST API を使用できます。

> **Note**
>
> コンソールには、過去 14 日以内に行われた非同期リクエストのステータスのみが表示されます。古いリクエストのステータスを表示するには、AWS CLI、SDK、または REST API を使用します。

非同期管理オペレーションは、次の状態のいずれかになります。

NEW

Amazon S3 がリクエストを受け取り、オペレーションの実行準備を進めています。

IN_PROGRESS

Amazon S3 は現在、オペレーションを実行しています。

SUCCESS

オペレーションは成功しました。応答には、`CreateMultiRegionAccessPoint` リクエストのマルチリージョンアクセスポイントのエイリアスなど、関連情報が含まれます。

FAILED

このオペレーションは失敗しました。応答には、リクエストが失敗した理由を示すエラーメッセージが含まれます。

AWS CloudTrail とマルチリージョンアクセスポイントの使用

AWS CloudTrail を使用して、AWS インフラストラクチャ全体のアカウントアクティビティを表示、検索、ダウンロード、アーカイブ、分析、応答できます。マルチリージョンのアクセスポイントと CloudTrail のログ記録では、次のことを識別できます。

- 誰が、または何が、どのアクションを実行したか
- どのリソースに基づいて処理が行われたか

- イベントが発生した時刻
- イベントに関するその他の詳細

このログ記録情報は、マルチリージョンアクセスポイントを通じて発生したアクティビティの分析と対応に役立ちます。

マルチリージョンアクセスポイントの AWS CloudTrail のセットアップ方法

マルチリージョンアクセスポイントの作成または保守に関するオペレーションで CloudTrail ログを有効にするには、米国西部 (オレゴン) リージョン内のイベントを記録するように CloudTrail ログを設定する必要があります。リクエストの実行時にどのリージョンにいるか、またはマルチリージョンアクセスポイントがどのリージョンをサポートしているかに関係なく、この方法でログ記録設定をセットアップする必要があります。マルチリージョンアクセスポイントを作成または維持するためのすべてのリクエストは、米国西部 (オレゴン) リージョンを通じてルーティングされます。このリージョンを既存の追跡に追加するか、このリージョンとマルチリージョンアクセスポイントに関連付けられたすべてのリージョンを含む新しい追跡を作成することをお勧めします。

Amazon S3 は、マルチリージョンアクセスポイントを介して行われたすべてのリクエストと、アクセスポイントを管理する API に対するリクエスト (`CreateMultiRegionAccessPoint` や `GetMultiRegionAccessPointPolicy` など) をログに記録します。マルチリージョンアクセスポイントを介してこれらのリクエストを記録すると、マルチリージョンアクセスポイントのホスト名を使用して AWS CloudTrail ログに表示されます。例えば、マルチリージョンのアクセスポイントを介してバケットにエイリアス `mfzwi23gnjvgw.mrap` でリクエストを行った場合、CloudTrail ログのエントリのホスト名は `mfzwi23gnjvgw.mrap.accesspoint.s3-global.amazonaws.com` になります。

マルチリージョンアクセスポイントは、リクエストを最も近いバケットにルーティングします。この動作のため、マルチリージョンアクセスポイントの CloudTrail ログを見ると、基となるバケットに対してリクエストが行われていることがわかります。ここうしたリクエストの一部は、マルチリージョンアクセスポイントを経由しない、バケットへの直接リクエストである場合があります。トラフィックを確認するときは、この点に注意してください。バケットがマルチリージョンアクセスポイントにある場合でも、マルチリージョンアクセスポイントを経由しなくても、そのバケットに対してリクエストを直接行うことができます。

マルチリージョンアクセスポイントの作成と管理には、非同期イベントがあります。非同期リクエストでは、CloudTrail ログに完了イベントはありません。リクエストの再試行の詳細については、「マルチリージョンアクセスポイント管理 API オペレーションに対するリクエストのモニタリングとログ記録」を参照してください。

AWS CloudTrail の詳細については、AWS CloudTrail ユーザーガイド の AWS CloudTrail とは を参照してください。

S3 バージョニングによる複数のバージョンのオブジェクトの保持

Amazon S3 のバージョニングとは、同じバケット内でオブジェクトの複数のバリアントを保持する手段のことです。S3 のバージョニング機能を使用すると、バケットに保存されたすべてのオブジェクトのすべてのバージョンを、保存、取得、復元することができます。バージョニングを使用すれば、意図しないユーザーアクションからもアプリケーション障害からも、より簡単に復旧できます。バケットのバージョニングを有効にすると、Amazon S3 が同じオブジェクトに対する複数の書き込みリクエストを同時に受信した場合に、すべてのオブジェクトが保存されます。

バージョニングを有効にしたバケットは、オブジェクトを誤って削除したり上書きしたりしても、復元が簡単に行えます。例えば、オブジェクトを削除した場合、Amazon S3 は、オブジェクトを完全に削除する代わりに削除マーカーを挿入します。その削除マーカーが、最新のオブジェクトバージョンになります。オブジェクトを上書きすると、バケット内の新しいオブジェクトバージョンになります。いつでも以前のバージョンを復元できます。詳細については、「バージョニングが有効なバケットからのオブジェクトバージョンの削除」を参照してください。

デフォルトではバケットの S3 バージョニングは無効になっているので、明示的に有効にする必要があります。詳細については、「バケットでのバージョニングの有効化」を参照してください。

> **Note**
>
> - SOAP API は、S3 バージョニングをサポートしていません。SOAP のサポートは HTTP 経由では廃止されましたが、HTTPS 経由では引き続き利用可能です。Amazon S3 の新機能は SOAP でサポートされていません。
> - 通常の Amazon S3 料金は、保存または移行されるオブジェクトのバージョンごとに適用されます。オブジェクトの各バージョンはオブジェクト全体であり、以前のバージョンの単なる差分ではありません。したがって、オブジェクトの 3 つのバージョンを保存している場合、3 つのオブジェクトに対して課金されます。

バージョニングが無効なバケット、有効なバケット、停止されているバケット

バケットは、次の 3 つの状態のいずれかになります。

- Unversioned (バージョニングが無効) (デフォルト)
- Versioning-enabled (バージョニングが有効)
- Versioning-suspended (バージョニングが停止)

バージョニングは、バケットレベルで有効化および停止します。一度バケットのバージョニングを有効にすると、バージョニング無効の状態に戻すことはできません。ただし、そのバケットのバージョニングを一時停止することは可能です。

バージョニング状態は、バケット内の一部ではなくすべてのオブジェクトに適用されます。バケットでバージョニングを有効にすると、すべての新しいオブジェクトがバージョニングされ、一意のバージョン ID が割り当てられます。バージョニングが有効化された時点でバケット内に既に存在していたオブジェクトは、それ以降常にバージョニングされ、将来のリクエストによって変更されたときに一意のバージョン ID が割り当てられます。次の点に注意してください。

- バージョニング状態を設定する前にバケットに保存したオブジェクトのバージョン ID は `null` です。バージョニングを有効にした場合、バケットに含まれる既存のオブジェクトは変更されません。変更されるのは、Amazon S3 が今後のリクエストでオブジェクトを処理する方法です。詳細については、「バージョニングが有効なバケットでのオブジェクトの操作」を参照してください。
- バケット所有者 (または適切なアクセス許可を持つユーザー) は、バージョニングを停止してオブジェクトバージョンの生成を中断できます。バージョニングを停止しても、バケットに含まれる既存のオブジェクトは変更されません。変更されるのは、Amazon S3 が今後のリクエストでオブジェクトを処理する方法です。詳細については、「バージョニングが停止されたバケットのオブジェクトの操作」を参照してください。

S3 ライフサイクルでの S3 バージョニングの使用

データ保持のアプローチやストレージコストの管理をカスタマイズするには、S3 ライフサイクルでオブジェクトバージョニングを使用します。詳細については、「オブジェクトのライフサイクルの管理」を参照してください。AWS Management Console、AWS CLI、AWS SDK、または REST API を使って S3 ライフサイクル設定を作成する方法の詳細は、「バケットに S3 ライフサイクル設定を設定する」を参照してください。

> **Important**
>
> バージョニングが無効であるバケットに、オブジェクトの有効期限ライフサイクル設定があり、有効化したときに同一の完全な削除動作を維持させたいときは、以前の有効期限切れ

設定を追加する必要があります。以前の有効期限切れのライフサイクル設定は、バージョニングが有効なバケットで、以前のオブジェクトバージョンの削除を管理します (バージョニングが有効なバケットは、1 個の最新のオブジェクトバージョン と、0 個以上の以前のバージョンを維持します)。詳細については、「バケットに S3 ライフサイクル設定を設定する」を参照してください。

S3 バージョニングの操作に関する詳細は、以下のトピックを参照してください。

トピック

- S3 バージョニングの仕組み
- バケットでのバージョニングの有効化
- MFA 削除の設定
- バージョニングが有効なバケットでのオブジェクトの操作
- バージョニングが停止されたバケットのオブジェクトの操作
- バージョニングのトラブルシューティング

S3 バージョニングの仕組み

S3 バージョニングを使用すると、オブジェクトの複数のバージョンを 1 つのバケットに保持し、誤って削除または上書きされたオブジェクトを復元できます。例えば、S3 バージョニングをバケットに適用すると、次の変更が行われます。

- オブジェクトを削除した場合、Amazon S3 では、オブジェクトを完全に削除する代わりに削除マーカーを挿入し、それが最新のオブジェクトバージョンになります。これにより、以前のバージョンを復元できます。詳細については、「バージョニングが有効なバケットからのオブジェクトバージョンの削除」を参照してください。
- オブジェクトを上書きすると、Amazon S3 のバケットに新しいオブジェクトバージョンが追加されます。以前のバージョンはバケットに残りますが、最新のバージョンではなくなります。以前のバージョンは復元することができます。

> **Note**
>
> 通常の Amazon S3 料金は、保存または移行されるオブジェクトのバージョンごとに適用されます。オブジェクトの各バージョンはオブジェクト全体であり、以前のバージョンの差分

ではありません。したがって、オブジェクトの 3 つのバージョンを保存している場合、3 つのオブジェクトに対して課金されます。

作成する各 S3 バケットには、それに関連付けられたバージョニングのサブリソースがあります。(詳しくは、汎用バケットの設定オプション を参照してください)。デフォルトでは、バケットのバージョニングは無効で、バージョニングのサブリソースには、以下のとおり、空のバージョニング設定が保存されます。

```
<VersioningConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
</VersioningConfiguration>
```

バージョニングを有効にするには、Enabled ステータスを含むバージョニング設定を使用して、Amazon S3 にリクエストを送信します。

```
<VersioningConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Status>Enabled</Status>
</VersioningConfiguration>
```

バージョニングを停止するには、ステータス値を Suspended に設定します。

> **Note**
>
> バケットで初めてバージョニングを有効にした場合、変更が完全に反映されるまでに少し時間がかかることがあります。この変更が反映されるまでの間に、バージョニングを有効にして作成または更新したオブジェクトへのリクエストで断続的な HTTP 404 NoSuchKey エラーが発生する可能性があります。バケットのオブジェクトへの書き込みオペレーション (PUT または DELETE) は、バージョニングを有効にして 15 分待ってから発行することをお勧めします。

バケット所有者とすべての承認済み AWS Identity and Access Management (IAM) ユーザーは、バージョニングを有効にすることができます。バケット所有者はバケットを作成する AWS アカウントです。権限の詳細については、「Amazon S3 用 Identity and Access Management」を参照してください。

AWS Management Console、AWS Command Line Interface (AWS CLI)、または REST API を使用した S3 バージョニングの有効化と無効化の詳細については、「the section called “バケットでのバージョニングの有効化”」を参照してください。

トピック

- バージョン ID
- バージョニングのワークフロー

バージョン ID

バケットのバージョニングを有効にすると、Amazon S3 は、保存されるオブジェクトに対して一意のバージョン ID を自動的に生成します。例えば、1 つのバケット内に、photo.gif (バージョン 111111) と photo.gif (バージョン 121212) のように、同じキー (オブジェクト名) でもバージョン ID が異なる 2 つのオブジェクトを保持することができます。
キーは同じでもバージョン ID が異なる 2 つのオブジェクトがある、バージョニングが有効になっているバケットを示す図。

S3 バージョニングが有効になっているかどうかにかかわらず、各オブジェクトにはバージョン ID があります。S3 バージョニングが有効にされていない場合、Amazon S3 はバージョン ID の値を null に設定します。S3 バージョニングを有効にした場合、Amazon S3 がオブジェクトにバージョン ID 値を割り当てます。この値により、そのオブジェクトが同じキーの他のバージョンと区別されます。

既存のバケットで S3 バージョニングを有効にしても、バケットにすでに保存されているオブジェクトは変更されません。バージョン ID (null)、コンテンツ、アクセス権限が変更されることはありません。S3 バージョニングを有効にすると、バケットに追加された各オブジェクトにバージョン ID が与えられ、同じキーの他のバージョンと区別されます。

バージョン ID を生成できるのは Amazon S3 のみです。また、編集はできません。バージョン ID は、Unicode、UTF-8 エンコード、URL 対応の不透明な文字列で、長さは 1,024 バイト以下です。次に例を示します。

```
3sL4kqtJlcpXroDTDmJ+rmSpXd3dIbrHY+MTRCxf3vjVBH40Nr8X8gdRQBpUMLUo
```

> **Note**
>
> 簡素化のため、本トピックの他の例ではさらに短い ID を使用します。

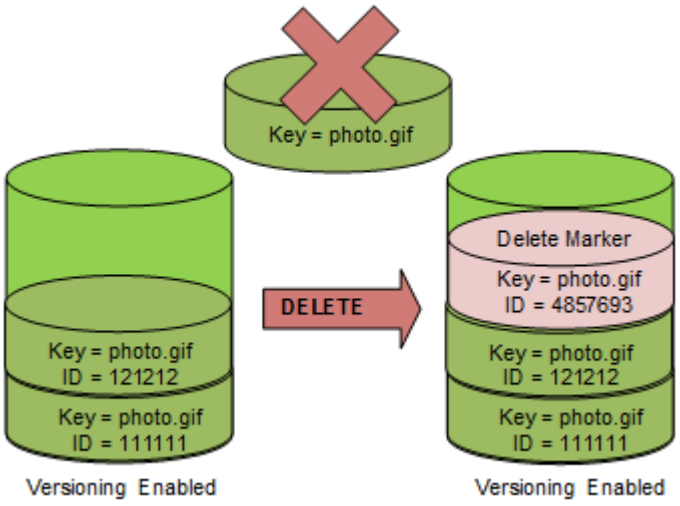
バージョニングのワークフロー

バージョニングが有効になっているバケットにオブジェクトを PUT しても、以前のバージョンは上書きされません。次の図に示すように、既に同じ名前のオブジェクトが入っているバケットに新しいバージョンの photo.gif が PUT された場合、以下の挙動が生じます。

- 元のオブジェクト (ID = 111111) はバケットに残ります。
- Amazon S3 は新しいバージョン ID (121212) を生成し、この新しいバージョンのオブジェクトをバケットに追加します。

この機能を使用すると、オブジェクトが誤って上書きまたは削除された場合に、オブジェクトの以前のバージョンを取得できます。

オブジェクトの DELETE を実行すると、次の図に示すように、バケット内のすべてのバージョンが残り、Amazon S3 によって削除マーカーが挿入されます。



削除マーカーはオブジェクトの最新バージョンになります。デフォルトで、GET リクエストは最後に保存されたバージョンを取得します。最新バージョンが削除マーカーである場合に GET Object リクエストを実行すると、次の図に示すように 404 Not Found エラーが返されます。

ただし、バージョン ID を指定すれば、オブジェクトの以前のバージョンを GET することができます。次の図では、特定のオブジェクトバージョン 111111 の GET を実行します。これはオブジェクトの最新バージョンではありませんが、Amazon S3 はこのバージョンを返します。

詳細については、「バージョニングが有効なバケットからのオブジェクトバージョンの取得」を参照してください。

オブジェクトを完全に削除するには、削除するバージョンを指定します。Amazon S3 バケット所有者または権限のある IAM ユーザーのみが、特定のバージョンを永久に削除することができます。DELETE オペレーションで versionId を指定すると、そのオブジェクトバージョンは完全に削除され、Amazon S3 による削除マーカーの挿入も行われません。

多要素認証 (MFA) Delete に対応するようにバケットを設定すると、セキュリティを強化できます。多要素認証 (MFA) Delete を有効にすると、バケット所有者は特定のバージョンを削除したりバケットのバージョニング状態を変更したりするために、すべてのリクエストに 2 つの認証形態を含める必要があります。詳細については、「MFA 削除の設定」を参照してください。

オブジェクトの新しいバージョンが作成されるのはどのような場合か

オブジェクトの新しいバージョンは、新しいオブジェクトを PUT した場合にのみ作成されます。CopyObject のような特定のアクションは、PUT オペレーションを実装することにより機能することに注意してください。

現在のオブジェクトを変更するアクションを実行しても、新しいオブジェクトを PUT しないため、新しいバージョンは作成されません。これには、オブジェクトのタグの変更などのアクションが含まれます。

> **Important**
>
> S3 バージョニングを有効にしたバケットへの Amazon S3 PUT または DELETE オブジェクトリクエストに対して受信される HTTP 503 (Service Unavailable) レスポンスの数が著しく増加した場合、バケットに数百万のバージョンが存在するオブジェクトがある可能性があります。詳細については、バージョニングのトラブルシューティングの「S3 バージョニングの使用」セクションを参照してください。

バケットでのバージョニングの有効化

S3 バージョニングを使用すると、1 つのバケットで複数バージョンのオブジェクトを維持できます。このセクションでは、コンソール、REST API、AWS SDK、AWS Command Line Interface (AWS CLI) を使って、バケットでバージョニングを有効にする方法の例を説明します。

> **Note**
>
> バケットで初めてバージョニングを有効にしたときは、変更が S3 システム全体に完全に反映されるまでに、最長で 15 分かかることがあります。この間、バージョニングを有効にし

た後で作成または更新したオブジェクトへの GET リクエストは、HTTP 404 NoSuchKey エラーになる可能性があります。バケット内のオブジェクトへの書き込みオペレーション (PUT または DELETE) は、バージョニングを有効にした後で 15 分待ってから実行することをお勧めします。この待機時間は、オブジェクトの可視性とバージョンの追跡に伴う潜在的な問題を回避するのに役立ちます。

S3 バージョニングの詳細については、「S3 バージョニングによる複数のバージョンのオブジェクトの保持」を参照してください。バージョニングが有効になっているバケットでの、オブジェクトの操作に関する詳細は、「バージョニングが有効なバケットでのオブジェクトの操作」を参照してください。

S3 バージョニングを使用してデータを保護する方法の詳細については、「Tutorial: Protecting data on Amazon S3 against accidental deletion or application bugs using S3 Versioning, S3 Object Lock, and S3 Replication」(チュートリアル: S3 バージョニング、S3 オブジェクトロック、S3 レプリケーションを使用して、Amazon S3 上のデータを予期しない削除やアプリケーションのバグから保護する) を参照してください。

作成する各 S3 バケットには、それに関連付けられたバージョニングのサブリソースがあります。(詳しくは、汎用バケットの設定オプション を参照してください)。デフォルトでは、バケットのバージョニングは無効で、バージョニングのサブリソースには、以下のとおり、空のバージョニング設定が保存されます。

```
<VersioningConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
</VersioningConfiguration>
```

バージョニングを有効にするには、状態を含むバージョニング設定を使用して、Amazon S3 にリクエストを送信します。

```
<VersioningConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Status>Enabled</Status>
</VersioningConfiguration>
```

バージョニングを停止するには、ステータス値を Suspended に設定します。

バケット所有者とすべての承認されたユーザーは、バージョニングを有効にすることができます。バケット所有者は、バケットを作成した AWS アカウント (ルートアカウント) です。 権限の詳細については、 を参照してくださいAmazon S3 用 Identity and Access Management

以下のセクションでは、コンソール、AWS CLI、AWS SDK を使って S3 バージョニングを有効にする方法の詳細を説明します。

S3 コンソールの使用

AWS Management Console を使用して、S3 バケットでバージョニングを有効にするには、次の手順に従います。

S3 汎用バケットのバージョニングを有効または無効にするには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[汎用バケット] を選択します。
3. バケットリストで、バージョニングを有効にするバケットの名前を選択します。
4. [プロパティ] を選択します。
5. [バケットのバージョニング] で [編集] を選択します。
6. [中断] または [有効化] を選択し、[変更を保存] を選択します。

> **Note**
>
> バージョニングで AWS 多要素認証 (MFA) を使用できます。バージョニングに MFA を使用しているときに、オブジェクトバージョンを完全に削除したり、バージョニングを停止または再有効化したりする場合は、AWS アカウント のアクセスキーと有効なコードを、アカウントの MFA デバイスから指定することが必要になります。
> バージョニングで MFA を使用するには、`MFA Delete` を有効にします。ただし、AWS Management Console を使用して `MFA Delete` を有効にすることはできません。AWS Command Line Interface (AWS CLI) または API を使用する必要があります。詳細については、「MFA 削除の設定」を参照してください。

AWS CLI の使用

次の例では、S3 汎用バケットでバージョニングを有効にします。

```
aws s3api put-bucket-versioning --bucket amzn-s3-demo-bucket1 --versioning-
configuration Status=Enabled
```

次の例では、バケットで S3 バージョニングと多要素認証 (MFA) 削除を有効にします。

```
aws s3api put-bucket-versioning --bucket amzn-s3-demo-bucket1 --versioning-
configuration Status=Enabled,MFADelete=Enabled --mfa "SERIAL 123456"
```

> **Note**
>
> MFA 削除を使用するときは、承認済みの物理または仮想の認証デバイスが必要です。Amazon S3 での MFA 削除の使用に関する詳細は、「MFA 削除の設定」を参照してください。

AWS CLI を使用したバージョニングの有効化に関する詳細は、AWS CLI CLI コマンドリファレンスの「put-bucket-versioning」を参照してください。

AWS SDK の使用

次の例では、バケットでバージョニングを有効にし、AWS SDK for Java と AWS SDK for .NET を使ってバージョニングの状態を復元します。他の AWS SDK の使用の詳細については、「AWS デベロッパーセンター」を参照してください。

.NET

コード例を設定および実行する方法の詳細については、「AWS SDK for .NET デベロッパーガイド」の「AWS SDK for .NET の開始方法」 を参照してください。

```
using System;
using Amazon.S3;
using Amazon.S3.Model;

namespace s3.amazon.com.docsamples
{
    class BucketVersioningConfiguration
    {
        static string bucketName = "*** bucket name ***";

        public static void Main(string[] args)
        {
            using (var client = new AmazonS3Client(Amazon.RegionEndpoint.USEast1))
            {
```

```
                try
                {
                    EnableVersioningOnBucket(client);
                    string bucketVersioningStatus =
RetrieveBucketVersioningConfiguration(client);
                }
                catch (AmazonS3Exception amazonS3Exception)
                {
                    if (amazonS3Exception.ErrorCode != null &&
                        (amazonS3Exception.ErrorCode.Equals("InvalidAccessKeyId")
                        ||
                        amazonS3Exception.ErrorCode.Equals("InvalidSecurity")))
                    {
                        Console.WriteLine("Check the provided AWS Credentials.");
                        Console.WriteLine(
                        "To sign up for service, go to http://aws.amazon.com/s3");
                    }
                    else
                    {
                        Console.WriteLine(
                         "Error occurred. Message:'{0}' when listing objects",
                         amazonS3Exception.Message);
                    }
                }
            }

            Console.WriteLine("Press any key to continue...");
            Console.ReadKey();
        }

        static void EnableVersioningOnBucket(IAmazonS3 client)
        {

                PutBucketVersioningRequest request = new PutBucketVersioningRequest
                {
                    BucketName = bucketName,
                    VersioningConfig = new S3BucketVersioningConfig
                    {
                        Status = VersionStatus.Enabled
                    }
                };

                PutBucketVersioningResponse response =
client.PutBucketVersioning(request);
```

```
        }


        static string RetrieveBucketVersioningConfiguration(IAmazonS3 client)
        {
                GetBucketVersioningRequest request = new GetBucketVersioningRequest
                {
                    BucketName = bucketName
                };

                GetBucketVersioningResponse response =
 client.GetBucketVersioning(request);
                return response.VersioningConfig.Status;
            }
    }
}
```

Java

作業サンプルの作成方法およびテスト方法については、「AWS SDK for Java のデベロッパーガイド」の「使用開始」を参照してください。

```
import java.io.IOException;

import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Region;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3Client;
import com.amazonaws.services.s3.model.AmazonS3Exception;
import com.amazonaws.services.s3.model.BucketVersioningConfiguration;
import com.amazonaws.services.s3.model.SetBucketVersioningConfigurationRequest;

public class BucketVersioningConfigurationExample {
    public static String bucketName = "*** bucket name ***";
    public static AmazonS3Client s3Client;

    public static void main(String[] args) throws IOException {
        s3Client = new AmazonS3Client(new ProfileCredentialsProvider());
        s3Client.setRegion(Region.getRegion(Regions.US_EAST_1));
        try {

            // 1. Enable versioning on the bucket.
         BucketVersioningConfiguration configuration =
```

```
            new BucketVersioningConfiguration().withStatus("Enabled");

    SetBucketVersioningConfigurationRequest setBucketVersioningConfigurationRequest
 =
        new SetBucketVersioningConfigurationRequest(bucketName,configuration);


 s3Client.setBucketVersioningConfiguration(setBucketVersioningConfigurationRequest);

    // 2. Get bucket versioning configuration information.
    BucketVersioningConfiguration conf =
 s3Client.getBucketVersioningConfiguration(bucketName);
      System.out.println("bucket versioning configuration status:    " +
 conf.getStatus());

          } catch (AmazonS3Exception amazonS3Exception) {
              System.out.format("An Amazon S3 error occurred. Exception: %s",
 amazonS3Exception.toString());
          } catch (Exception ex) {
              System.out.format("Exception: %s", ex.toString());
          }
      }
}
```

Python

次の Python コードの例では、Amazon S3 バケットを作成し、バージョニング用に有効にして、オブジェクトの最新ではないバージョンが 7 日後に失効するライフサイクルを設定しています。

```
def create_versioned_bucket(bucket_name, prefix):
    """
    Creates an Amazon S3 bucket, enables it for versioning, and configures a
 lifecycle
    that expires noncurrent object versions after 7 days.

    Adding a lifecycle configuration to a versioned bucket is a best practice.
    It helps prevent objects in the bucket from accumulating a large number of
    noncurrent versions, which can slow down request performance.

    Usage is shown in the usage_demo_single_object function at the end of this
 module.

    :param bucket_name: The name of the bucket to create.
```

```
    :param prefix: Identifies which objects are automatically expired under the
                   configured lifecycle rules.
    :return: The newly created bucket.
    """
    try:
        bucket = s3.create_bucket(
            Bucket=bucket_name,
            CreateBucketConfiguration={
                "LocationConstraint": s3.meta.client.meta.region_name
            },
        )
        logger.info("Created bucket %s.", bucket.name)
    except ClientError as error:
        if error.response["Error"]["Code"] == "BucketAlreadyOwnedByYou":
            logger.warning("Bucket %s already exists! Using it.", bucket_name)
            bucket = s3.Bucket(bucket_name)
        else:
            logger.exception("Couldn't create bucket %s.", bucket_name)
            raise

    try:
        bucket.Versioning().enable()
        logger.info("Enabled versioning on bucket %s.", bucket.name)
    except ClientError:
        logger.exception("Couldn't enable versioning on bucket %s.", bucket.name)
        raise

    try:
        expiration = 7
        bucket.LifecycleConfiguration().put(
            LifecycleConfiguration={
                "Rules": [
                    {
                        "Status": "Enabled",
                        "Prefix": prefix,
                        "NoncurrentVersionExpiration": {"NoncurrentDays":
expiration},
                    }
                ]
            }
        )
        logger.info(
            "Configured lifecycle to expire noncurrent versions after %s days "
            "on bucket %s.",
```

```
            expiration,
            bucket.name,
        )
    except ClientError as error:
        logger.warning(
            "Couldn't configure lifecycle on bucket %s because %s. "
            "Continuing anyway.",
            bucket.name,
            error,
        )

    return bucket
```

MFA 削除の設定

Amazon S3 バケットで S3 バージョニングを行うときに、MFA (多要素認証) Delete が有効になるようにバケットを設定すれば、セキュリティをさらに強化できます。この設定を行うと、バケット所有者は、特定のバージョンを削除したりバケットのバージョニング状態を変更したりするリクエストに、2 つの認証形式を含めることが必要になります。

MFA Delete では、以下のいずれかの操作で追加の認証が必要になります。

- バケットのバージョニング状態を変更する
- オブジェクトバージョンを完全に削除する

MFA Delete では、2 つの認証形式の組み合わせが必要になります。

- セキュリティ認証情報
- 有効なシリアル番号、スペース、および承認済みの認証デバイスに表示される 6 桁のコードを連結した文字

MFA Delete は、このようにして、認証情報に不正なアクセスがあった場合などにセキュリティを強化します。MFA 削除は、削除アクションを開始したユーザーに MFA コードを使って MFA デバイスの物理的所有を証明するように要求したり、削除アクションに摩擦とセキュリティのレイヤーをさらに追加したりすることで、バケットの偶発的な削除を防ぎます。

MFA 削除が有効になっているバケットを特定するには、Amazon S3 ストレージレンズメトリクスを使用できます。S3 ストレージレンズは、オブジェクトストレージの使用状況とアクティビティを組織全体で可視化するために使用できるクラウドストレージの分析機能です。詳細については、「S3 Storage Lens を使用したストレージのアクティビティと使用状況の評価」を参照してください。メトリクスの完全なリストについては、「S3 ストレージレンズメトリクスに関する用語集」を参照してください。

バケット所有者、バケットを作成した AWS アカウント (ルートアカウント)、およびすべての承認されたユーザーは、バージョニングを有効にすることができます。ただし、MFA Delete を有効化できるのは、バケット所有者 (ルートアカウント) のみです。詳細については、AWS セキュリティブログの「MFA を使用した AWS へのアクセスの保護」を参照してください。

> **Note**
>
> バージョニングで MFA Delete を使用するには、`MFA Delete` を有効にします。ただし、AWS Management Console を使用して `MFA Delete` を有効にすることはできません。AWS Command Line Interface (AWS CLI) または API を使用する必要があります。
> バージョニングで MFA Delete を使用する例については、トピック バケットでのバージョニングの有効化 の具体例のセクションを参照してください。
> ライフサイクル設定で MFA 削除を使用することはできません。ライフサイクル設定と、それらが他の設定とやり取りする方法の詳細については、「S3 ライフサイクルは他のバケット設定とどのように相互作用するか」を参照してください。

MFA 削除を有効または無効にするには、バケットのバージョニングの設定に使用するものと同じ API を使用します。Amazon S3 では、バケットのバージョニング状態を格納しているものを同じバージョニングサブリソースに、MFA Delete の設定が格納されます。

```
<VersioningConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Status>VersioningState</Status>
  <MfaDelete>MfaDeleteState</MfaDelete>
</VersioningConfiguration>
```

MFA Delete を使用するときは、ハードウェアデバイスまたは仮想 MFA デバイスを使用して認証コードを生成します。次の例は、生成された認証コードがハードウェアデバイスに表示されている様子を示しています。

MFA Delete と MFA で保護された API アクセスは、異なるシナリオで保護を行うことを目的とした機能です。バケットに MFA Delete を設定することで、バケット内のデータが誤って削除されることのないようにします。MFA で保護された API アクセスは、Amazon S3 の機密リソースにアクセスする場合に、別の認証要素 (MFA コード) を適用するために使用します。これらの Amazon S3 リソースに対するすべてのオペレーションが、MFA を使用した一時証明書によって実行されるように要求できます。例については、「MFA が必要」を参照してください。

認証デバイスの購入およびアクティベートの方法の詳細については、「多要素認証」を参照してください。

S3 バージョニングを有効にして MFA 削除を設定するには

AWS CLI を使用する場合

シリアル番号は、MFA デバイスを一意に識別する番号です。物理 MFA デバイスの場合、これはデバイスに提供される一意のシリアル番号です。仮想 MFA デバイスの場合、シリアル番号はデバイス ARN です。

次の例では、バケットで S3 バージョニングと多要素認証 (MFA) 削除を有効にします。

```
aws s3api put-bucket-versioning --bucket amzn-s3-demo-bucket1 --versioning-
configuration Status=Enabled,MFADelete=Enabled --mfa "SERIAL 123456"
```

REST API の使用

Amazon S3 REST API を使用したルーティングルールの設定の詳細については、Amazon Simple Storage Service API リファレンスの「PutBucketVersioning」を参照してください。

バージョニングが有効なバケットでのオブジェクトの操作

バージョニング状態を設定する前に Amazon S3 バケットに保存されたオブジェクトのバージョン ID は、null です。バージョニングを有効にした場合、バケットに含まれる既存のオブジェクトは変更されません。変更されるのは、Amazon S3 が今後のリクエストでオブジェクトを処理する方法です。

オブジェクトバージョンの移行

明確なライフサイクルが定義されているオブジェクトに対してライフサイクル設定ルールを定義することにより、オブジェクトの有効期間内の特定の時点でオブジェクトバージョンを S3 Glacier Flexible Retrieval ストレージクラスに移行できます。詳細については、「オブジェクトのライフサイクルの管理」を参照してください。

このセクションのトピックでは、バージョニングが有効なバケットでのさまざまなオブジェクトのオペレーションについて説明します。バージョニングの詳細については、「S3 バージョニングによる複数のバージョンのオブジェクトの保持」を参照してください。

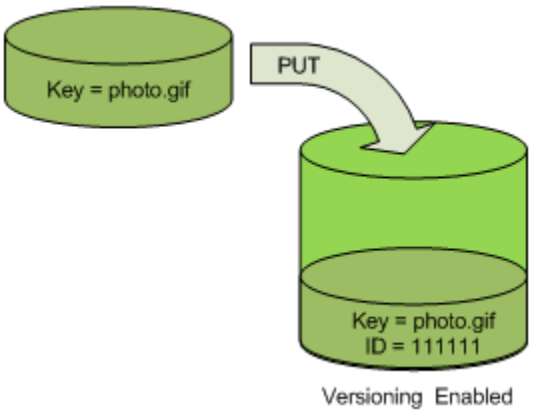
トピック

- バージョニングが有効なバケットへのオブジェクトの追加
- バージョニングが有効なバケットでのオブジェクトのリスト取得
- バージョニングが有効なバケットからのオブジェクトバージョンの取得
- バージョニングが有効なバケットからのオブジェクトバージョンの削除
- バージョン管理されたオブジェクトのアクセス許可の設定

バージョニングが有効なバケットへのオブジェクトの追加

バケットでバージョニングを有効にすると、Amazon S3 は (PUT、POST、または CopyObject を使用して) バケットに保存されたすべてのオブジェクトに、一意のバージョン ID を自動的に追加します。

次の図は、バージョニングが有効なバケットにオブジェクトが追加されたときに、Amazon S3 がそのオブジェクトに一意のバージョン ID を追加する方法を示しています。



> **Note**
>
> Amazon S3 が割り当てるバージョン ID の値は URL セーフです (URI の一部として含めることができます) 。

バージョニングの詳細については、「S3 バージョニングによる複数のバージョンのオブジェクトの保持」を参照してください。バージョニングが有効なバケットにオブジェクトバージョンを追加するときは、コンソール、AWS SDK、REST API を使用します。

コンソールを使用する

手順については、「オブジェクトのアップロード」を参照してください。

AWS SDK の使用

AWS SDK for Java、.NET、PHP を使用してオブジェクトをアップロードする例については、「オブジェクトのアップロード」を参照してください。バージョニングが設定されていないバケットでも、バージョニングが有効なバケットでもオブジェクトをアップロードする例は同じです。ただし、バージョニングが有効なバケットでは、Amazon S3 によってバージョン番号が割り当てられます。それ以外の場合、バージョン番号は null になります。

他の AWS SDK の使用の詳細については、「AWS デベロッパーセンター」を参照してください。

REST API の使用

バージョニングが有効なバケットにオブジェクトを追加するには

1. `PutBucketVersioning` リクエストを使用して、バケットでバージョニングを有効にします。

   詳細については、「Amazon Simple Storage Service API リファレンス」の「PutBucketVersioning」を参照してください。
2. PUT、POST、または `CopyObject` リクエストを送信して、バケットにオブジェクトを格納します。

バージョニングが有効なバケットにオブジェクトを追加すると、Amazon S3 は、次の例に示すとおり、`x-amz-version-id` レスポンスヘッダーでオブジェクトのバージョン ID を返します。

```
x-amz-version-id: 3/L4kqtJlcpXroDTDmJ+rmSpXd3dIbrHY
```

バージョニングが有効なバケットでのオブジェクトのリスト取得

このセクションでは、バージョニングが有効なバケットの、オブジェクトバージョンをリスト化する例を説明します。Amazon S3 では、オブジェクトのバージョン情報は、バケットに関連付けられているバージョンのサブリソースに格納されます。詳細については、「汎用バケットの設定オプション」を参照してください。バージョニングが有効なバケット内のオブジェクトを一覧表示するには、`ListBucketVersions` アクセス許可が必要です。

S3 コンソールの使用

以下の手順では、Amazon S3 コンソールを使用して、オブジェクトの異なるバージョンを表示する方法を説明します。

オブジェクトの複数のバージョンを表示する方法

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. [バケット] リストで、オブジェクトが含まれるバケットの名前を選択します。
3. バケット内のオブジェクトのバージョン一覧を表示するには、[Show versions] (バージョンのリスト) スイッチを選択します。

   各オブジェクトバージョンについて、一意のバージョン ID、そのバージョンが作成された日時、その他のプロパティがコンソールに表示されます。(バージョニング状態を設定する前にバケットに格納されているオブジェクトには、バージョン ID [null] が付けられています)。

   バージョンのないオブジェクトをリストするには、[バージョンのリスト] スイッチを選択します。

オブジェクトのバージョンは、コンソールの [オブジェクト概要] ペインでも、確認、ダウンロード、削除が行えます。詳細については、「Amazon S3 コンソールでのオブジェクトのプロパティの表示」を参照してください。

> **Note**
>
> 300 バージョンより前のオブジェクトバージョンにアクセスするには、AWS CLI またはオブジェクトの URL を使用する必要があります。

> **Important**
>
> 最新 (現在) のバージョンとして削除された場合のみ、オブジェクトを復元できます。削除されたオブジェクトの以前のバージョンを復元することはできません。詳細については、「S3 バージョニングによる複数のバージョンのオブジェクトの保持」を参照してください。

AWS SDK の使用

このセクションの例では、バージョニングが有効なバケットのオブジェクトを一覧表示する方法を示します。各リクエストは最大 1,000 個のバージョンを返します (これ未満の数を指定した場合を除きます)。バケット内のバージョン数が、この上限数を超えている場合は、複数のリクエストを送信してすべてのバージョンを一覧表示します。このように「ページ」に分けて結果を返すプロセスは、ページ分割と呼ばれます。

ページ分割の仕組みを示すために、例ではレスポンスごとのオブジェクトバージョン数を 2 個に制限しています。各例では、最初のページの結果を取得すると、バージョンリストが切り詰められているかどうかを確認します。切り詰められている場合は、引き続きページの取得を繰り返し、すべてのバージョンを取得します。

> **Note**
>
> 以下の例は、バージョニングが有効になっていないバケットや、個別のバージョンを持たないオブジェクトにも使用できます。これらの場合、Amazon S3 で返される各オブジェクトのバージョン ID は `null` になります。

他の AWS SDK の使用の詳細については、「AWS デベロッパーセンター」を参照してください。

Java

作業サンプルの作成およびテストの手順については、「AWS SDK for Java のデベロッパーガイド」の「使用開始」を参照してください。

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
```

```
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.ListVersionsRequest;
import com.amazonaws.services.s3.model.S3VersionSummary;
import com.amazonaws.services.s3.model.VersionListing;

public class ListKeysVersioningEnabledBucket {

    public static void main(String[] args) {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();

            // Retrieve the list of versions. If the bucket contains more versions
            // than the specified maximum number of results, Amazon S3 returns
            // one page of results per request.
            ListVersionsRequest request = new ListVersionsRequest()
                    .withBucketName(bucketName)
                    .withMaxResults(2);
            VersionListing versionListing = s3Client.listVersions(request);
            int numVersions = 0, numPages = 0;
            while (true) {
                numPages++;
                for (S3VersionSummary objectSummary :
 versionListing.getVersionSummaries()) {
                    System.out.printf("Retrieved object %s, version %s\n",
                            objectSummary.getKey(),
                            objectSummary.getVersionId());
                    numVersions++;
                }
                // Check whether there are more pages of versions to retrieve. If
                // there are, retrieve them. Otherwise, exit the loop.
                if (versionListing.isTruncated()) {
                    versionListing =
 s3Client.listNextBatchOfVersions(versionListing);
                } else {
                    break;
                }
            }
```

```
            System.out.println(numVersions + " object versions retrieved in " +
 numPages + " pages");
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

.NET

コード例を設定および実行する方法の詳細については、「AWS SDK for .NET デベロッパーガイド」の「AWS SDK for .NET の開始方法」を参照してください。

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class ListObjectsVersioningEnabledBucketTest
    {
        static string bucketName = "*** bucket name ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;

        public static void Main(string[] args)
        {
            s3Client = new AmazonS3Client(bucketRegion);
            GetObjectListWithAllVersionsAsync().Wait();
        }

        static async Task GetObjectListWithAllVersionsAsync()
```

```
        {
            try
            {
                ListVersionsRequest request = new ListVersionsRequest()
                {
                    BucketName = bucketName,
                    // You can optionally specify key name prefix in the request
                    // if you want list of object versions of a specific object.

                    // For this example we limit response to return list of 2
versions.
                    MaxKeys = 2
                };
                do
                {
                    ListVersionsResponse response = await
s3Client.ListVersionsAsync(request);
                    // Process response.
                    foreach (S3ObjectVersion entry in response.Versions)
                    {
                        Console.WriteLine("key = {0} size = {1}",
                            entry.Key, entry.Size);
                    }

                    // If response is truncated, set the marker to get the next
                    // set of keys.
                    if (response.IsTruncated)
                    {
                        request.KeyMarker = response.NextKeyMarker;
                        request.VersionIdMarker = response.NextVersionIdMarker;
                    }
                    else
                    {
                        request = null;
                    }
                } while (request != null);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
writing an object", e.Message);
            }
            catch (Exception e)
            {
```

```
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
        }
    }
}
```

REST API の使用

Example - バケット内のすべてのオブジェクトバージョンをリスト化

バケット内の各オブジェクトのすべてのバージョンを一覧表示するには、versions リクエストで GET Bucket サブリソースを使用します。Amazon S3 で取得できるオブジェクトは最大 1,000 個です。各オブジェクトバージョンが 1 個のオブジェクトとしてフルにカウントされます。したがって、バケット内に 2 つのキー (例: photo.gif と picture.jpg) があり、最初のキーに 990 個のバージョン、2 番目のキーに 400 個のバージョンがある場合、1 つのリクエストで取得されるバージョンは、photo.gif の 990 個と、picture.jpg のうち最新の 10 個のみです。

Amazon S3 は、最も新しく保存されたバージョンから開始して、保存された順序でオブジェクトバージョンを返します。

GET Bucket リクエストに、versions サブリソースを含めます。

```
GET /?versions HTTP/1.1
Host: bucketName.s3.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 +0000
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU=
```

Example - キーのすべてのバージョンの取得

オブジェクトバージョンのサブセットを取得するには、GET Bucket のリクエストパラメータを使用します。詳細については、「GET Bucket」を参照してください。

1. prefix パラメータを、取得したいオブジェクトのキーに設定します。
2. GET Bucket サブリソースおよび versions を使用して、prefix リクエストを送信します。

   ```
   GET /?versions&prefix=objectName HTTP/1.1
   ```

Example - プレフィックスを使用したオブジェクトの取得

次の例では、キーが myObject であるか、またはそれで始まるオブジェクトを取得します。

```
GET /?versions&prefix=myObject HTTP/1.1
Host: bucket.s3.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU=
```

オブジェクトのすべてのバージョンのサブセットを取得するには、他のリクエストパラメータを使用します。詳細については、「Amazon Simple Storage Service API リファレンス」の「GET Bucket」を参照してください。

Example - レスポンスが切り詰められた後の残ったオブジェクトのリスト取得

GET リクエストで返すことができるオブジェクトの数が max-keys の値を超えた場合、レスポンスには <isTruncated>true</isTruncated> と、リクエストを満たすが返されなかった最初のキー (NextKeyMarker 内) および最初のバージョン ID (NextVersionIdMarker 内) が含まれます。GET リクエストを満たす追加のオブジェクトを取得する後続のリクエストで、これらの戻り値を開始位置として使用します。

バケットの元の GET Bucket versions リクエストを満たす追加のオブジェクトを取得するには、以下の手順に従ってください。key-marker、version-id-marker、NextKeyMarker、および NextVersionIdMarker の詳細については、「Amazon Simple Storage Service API リファレンス」の「GET Bucket」を参照してください。

以下は、元の GET リクエストを満たす追加のレスポンスです。

- key-marker の値を、前のレスポンスの NextKeyMarker で返されたキーに設定します。
- version-id-marker の値を、前のレスポンスの NextVersionIdMarker で返されたバージョン ID に設定します。
- GET Bucket versions および key-marker を使用して version-id-marker リクエストを送信します。

Example - 指定したキーおよびバージョン ID を始点としたオブジェクトの取得

```
GET /?versions&key-marker=myObject&version-id-marker=298459348571 HTTP/1.1
Host: bucket.s3.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 GMT
```

```
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU=
```

AWS CLI を使用する場合

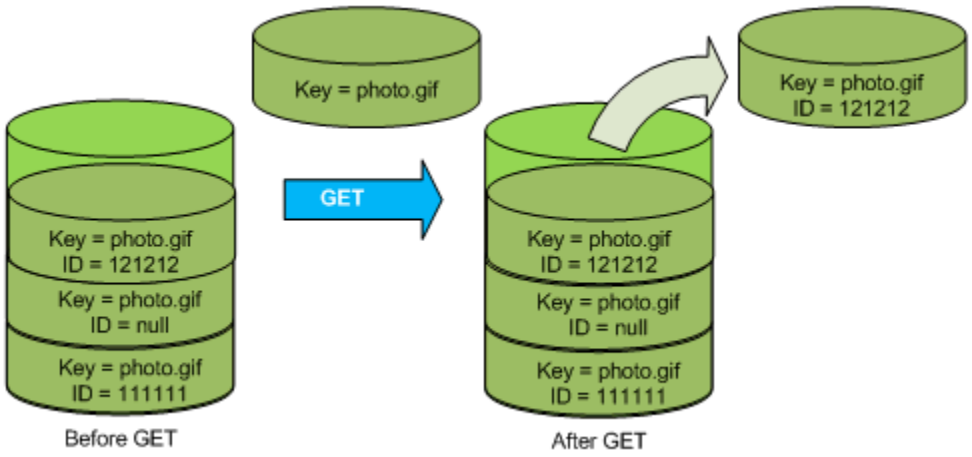
次のコマンドは、バケット内のオブジェクトのすべてのバージョンに関するメタデータを返します。

```
aws s3api list-object-versions --bucket amzn-s3-demo-bucket1
```

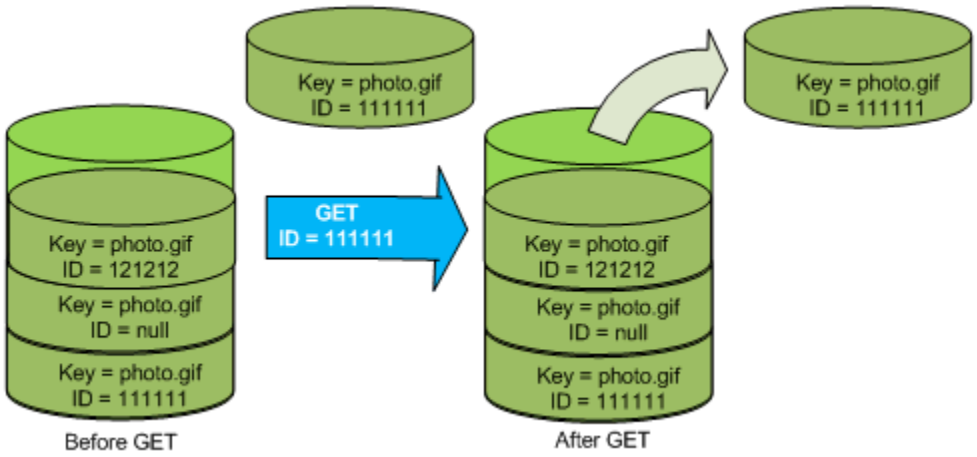
`list-object-versions` の使用に関する詳細は、「AWS CLI コマンドリファレンス」の「list-object-versions」を参照してください。

バージョニングが有効なバケットからのオブジェクトバージョンの取得

Amazon S3 のバージョニングとは、同じバケット内に、オブジェクトの複数のバリアントを保持する手段のことです。シンプルな GET リクエストは、オブジェクトの最新バージョンを取得します。次の図は、GET がオブジェクト (photo.gif) の最新バージョンを返す方法を示しています。



特定のバージョンを取得するには、そのバージョン ID を指定する必要があります。次の図は、GET versionId リクエストがオブジェクトの指定したバージョン (最新とは限らない) を取得する方法を示しています。



コンソール、AWS SDK、または REST API を使用して、Amazon S3 にオブジェクトバージョンを取得できます。

> **Note**
>
> 300 バージョンより前のオブジェクトバージョンにアクセスするには、AWS CLI またはオブジェクトの URL を使用する必要があります。

S3 コンソールの使用

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. [Buckets] (バケット) リストで、オブジェクトが含まれるバケットの名前を選択します。
3. オブジェクト一覧から、オブジェクトの名前を選択します。
4. [バージョン] を選択します。

   Amazon S3 にオブジェクトのバージョンがすべて表示されます。
5. 取得するバージョンのバージョン ID の、横のチェックボックスをオンにします。
6. [アクション] を選択し、[ダウンロード] を選択して、オブジェクトを保存します。

オブジェクトの概要パネルでも、オブジェクトのバージョンの確認、ダウンロード、および削除ができます。詳細については、「Amazon S3 コンソールでのオブジェクトのプロパティの表示」を参照してください。

> **Important**
>
> 最新 (現在) のバージョンとして削除された場合のみ、オブジェクトを復元できます。削除されたオブジェクトの以前のバージョンを復元することはできません。詳細については、「S3 バージョニングによる複数のバージョンのオブジェクトの保持」を参照してください。

AWS SDK の使用

バージョニングが無効なバケットと有効なバケットにオブジェクトをアップロードする場合の例は、同一です。ただし、バージョニングが有効なバケットには、Amazon S3 がバージョン番号を割り当てます。それ以外の場合、バージョン番号は null になります。

AWS SDKs for Java、.NET、および PHP を使用してオブジェクトをダウンロードする例については、オブジェクトのダウンロードを参照してください。

.NET と Rust のAWS SDK を使用してオブジェクトのバージョンを一覧表示する例については、「Amazon S3 バケット内のオブジェクトのバージョンを一覧表示する」を参照してください。

REST API の使用

特定のオブジェクトバージョンを取得するには

1. `versionId` を、取得するオブジェクトのバージョン ID に設定します。
2. `GET Object versionId` リクエストを送信します。

Example - バージョニングされたオブジェクトの取得

次のリクエストは、`L4kqtJlcpXroDTDmpUMLUo` のバージョン `my-image.jpg` を取得します。

```
GET /my-image.jpg?versionId=L4kqtJlcpXroDTDmpUMLUo HTTP/1.1
Host: bucket.s3.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU=
```

オブジェクトの (コンテンツではなく) メタデータのみを取得できます。詳細については、「the section called “バージョンメタデータの取得”」を参照してください。

以前のオブジェクトバージョンを復元する方法については、「the section called “以前のバージョンの復元”」を参照してください。

オブジェクトバージョンのメタデータの取得

オブジェクトのメタデータのみを取得するには (コンテンツを除く)、HEAD オペレーションを使用します。デフォルトでは、最新バージョンのメタデータが取得されます。特定のオブジェクトバージョンのメタデータを取得するには、そのバージョン ID を指定します。

オブジェクトバージョンのメタデータを取得するには

1. versionId を、メタデータを取得するオブジェクトのバージョン ID に設定します。
2. HEAD Object versionId リクエストを送信します。

Example - バージョニングされたオブジェクトのメタデータの取得

次のリクエストは、my-image.jpg のバージョン 3HL4kqCxf3vjVBH40Nrjfkd のメタデータを取得します。

```
HEAD /my-image.jpg?versionId=3HL4kqCxf3vjVBH40Nrjfkd HTTP/1.1
Host: bucket.s3.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU=
```

以下に、サンプルレスポンスを示します。

```
HTTP/1.1 200 OK
x-amz-id-2: ef8yU9AS1ed4OpIszj7UDNEHGran
x-amz-request-id: 318BC8BC143432E5
x-amz-version-id: 3HL4kqtJlcpXroDTDmjVBH40Nrjfkd
Date: Wed, 28 Oct 2009 22:32:00 GMT
Last-Modified: Sun, 1 Jan 2006 12:00:00 GMT
ETag: "fba9dede5f27731c9771645a39863328"
Content-Length: 434234
Content-Type: text/plain
Connection: close
Server: AmazonS3
```

以前のバージョンの復元

バージョニングを使用すると、オブジェクトの以前のバージョンを取得できます。この機能を実行するには 2 つの方法があります。

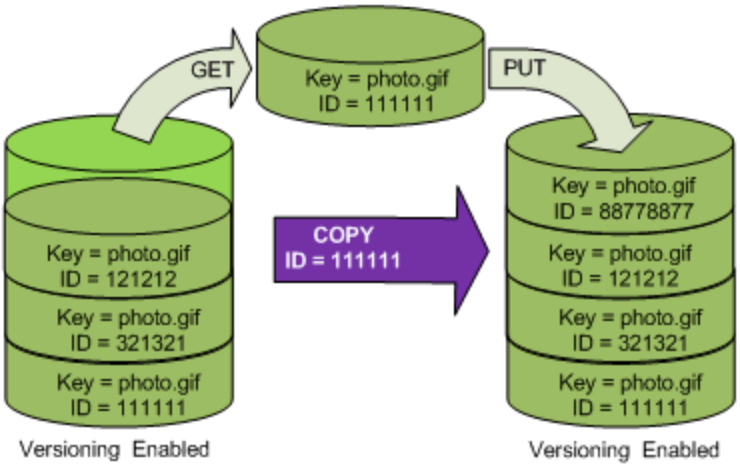
- オブジェクトの以前のバージョンを同じバケットにコピーします。

コピーされたオブジェクトはそのオブジェクトの最新バージョンになり、すべてのオブジェクトバージョンが維持されます。

- オブジェクトの最新バージョンを完全に削除します。

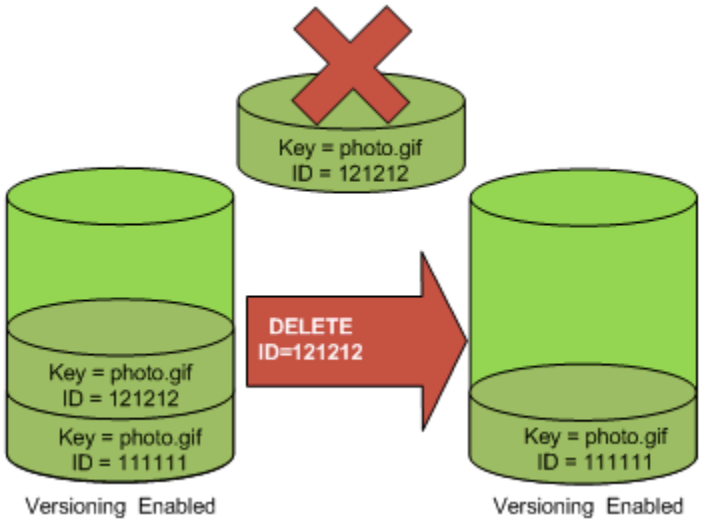
  最新のオブジェクトバージョンを削除すると、結果として、以前のバージョンがそのオブジェクトの最新バージョンになります。

すべてのオブジェクトバージョンが維持されるため、オブジェクトの特定のバージョンをバケットにコピーすることにより、以前の任意のバージョンを最新バージョンにすることができます。次の図では、ソースオブジェクト (ID = 111111) が同じバケットにコピーされます。Amazon S3 が新しい ID (88778877) を指定し、それがオブジェクトの最新バージョンになります。したがって、バケットには元のオブジェクトバージョン (111111) とそのコピー (88778877) の両方が存在します。以前のバージョンを取得してからアップロードして最新のバージョンにする方法の詳細については、バージョニングが有効なバケットからのオブジェクトバージョンの取得およびオブジェクトのアップロードを参照してください。



後続の GET が、バージョン 88778877 を取得します。

次の図では、オブジェクトの最新バージョン (121212) を削除して、以前のバージョン (111111) を最新のオブジェクトとして残す方法を示しています。オブジェクトの削除の詳細については、「1 つのオブジェクトの削除」を参照してください。



後続の GET が、バージョン 111111 を取得します。

> **Note**
>
> オブジェクトバージョンをバッチで復元する場合は、CopyObject オペレーションを使用できます。CopyObject オペレーションは、マニフェストで指定した各オブジェクトをコピーします。ただし、オブジェクトは、必ずしもマニフェストに表示されている順序と同じ順序でコピーされるとは限らないため、注意してください。バージョン管理されたバケットでは、現在のバージョンまたは以前のバージョンの順序を維持することが重要な場合は、最初に以前のバージョンをすべてコピーする必要があります。次に、最初のジョブが完了したら、後続のジョブで現在のバージョンをコピーします。

以前のオブジェクトバージョンを復元する

削除されたオブジェクトを復元する方法の詳細については、AWS re:Post ナレッジセンターで「バージョニングが有効になっているバケットで削除された Amazon S3 オブジェクトを取得するにはどうすればよいですか?」を参照してください。

S3 コンソールの使用

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. [Buckets] (バケット) リストで、オブジェクトが含まれるバケットの名前を選択します。
3. オブジェクト一覧から、オブジェクトの名前を選択します。

4. [バージョン] を選択します。

   Amazon S3 にオブジェクトのバージョンがすべて表示されます。
5. 取得するバージョンのバージョン ID の、横のチェックボックスをオンにします。
6. [アクション] を選択し、[ダウンロード] を選択して、オブジェクトを保存します。

オブジェクトの概要パネルでも、オブジェクトのバージョンの確認、ダウンロード、および削除ができます。詳細については、「Amazon S3 コンソールでのオブジェクトのプロパティの表示」を参照してください。

> **Important**
>
> 最新 (現在) のバージョンとして削除された場合のみ、オブジェクトを復元できます。削除されたオブジェクトの以前のバージョンを復元することはできません。詳細については、「S3 バージョニングによる複数のバージョンのオブジェクトの保持」を参照してください。

AWS SDK の使用

他の AWS SDK の使用の詳細については、「AWS デベロッパーセンター」を参照してください。

Python

以下の Python コード例は、指定されたロールバックバージョンの後で生成されたすべてのバージョンを削除することによって、バージョン管理されたオブジェクトの以前のバージョンを復元します。

```
def rollback_object(bucket, object_key, version_id):
    """
    Rolls back an object to an earlier version by deleting all versions that
    occurred after the specified rollback version.

    Usage is shown in the usage_demo_single_object function at the end of this
 module.

    :param bucket: The bucket that holds the object to roll back.
    :param object_key: The object to roll back.
    :param version_id: The version ID to roll back to.
    """
    # Versions must be sorted by last_modified date because delete markers are
```

```
    # at the end of the list even when they are interspersed in time.
    versions = sorted(
        bucket.object_versions.filter(Prefix=object_key),
        key=attrgetter("last_modified"),
        reverse=True,
    )

    logger.debug(
        "Got versions:\n%s",
        "\n".join(
            [
                f"\t{version.version_id}, last modified {version.last_modified}"
                for version in versions
            ]
        ),
    )

    if version_id in [ver.version_id for ver in versions]:
        print(f"Rolling back to version {version_id}")
        for version in versions:
            if version.version_id != version_id:
                version.delete()
                print(f"Deleted version {version.version_id}")
            else:
                break

        print(f"Active version is now {bucket.Object(object_key).version_id}")
    else:
        raise KeyError(
            f"{version_id} was not found in the list of versions for "
f"{object_key}."
        )
```

バージョニングが有効なバケットからのオブジェクトバージョンの削除

オブジェクトのバージョンは Amazon S3 バケットからいつでも削除できます。さらに、明確なライフサイクルが定義されているオブジェクトのライフサイクル設定ルールを定義することにより、最新のオブジェクトバージョンを有効期限切れにしたり、以前のオブジェクトバージョンを完全に削除したりするよう Amazon S3 にリクエストできます。バケットでバージョニングが有効であるか、バージョニングが停止されている場合、ライフサイクル設定アクションは次のように動作します。

- `Expiration` アクションは、最新のオブジェクトバージョンに適用されます。Amazon S3 は、最新のオブジェクトバージョンを削除するのではなく、削除マーカーを追加してそれを最新バージョンにします。これにより、最新バージョンは以前のバージョンとして保持されます。
- `NoncurrentVersionExpiration` アクションは、以前のオブジェクトバージョンに適用されます。Amazon S3 はこれらのオブジェクトバージョンを完全に削除します。完全に削除したオブジェクトは復元できません。

S3 ライフサイクルの詳細については、「オブジェクトのライフサイクルの管理」および「S3 ライフサイクル設定の例」を参照してください。

バケットにある現在のオブジェクトバージョンと最新でないオブジェクトバージョンの数を確認するには、Amazon S3 ストレージレンズメトリクスを使用できます。S3 ストレージレンズは、オブジェクトストレージの使用状況とアクティビティを組織全体で可視化するために使用できるクラウドストレージの分析機能です。詳細については、「S3 Storage Lens を使用したストレージコストの最適化」を参照してください。メトリクスの完全なリストについては、「S3 Storage Lens のメトリクスに関する用語集」を参照してください。

> **Note**
>
> 通常の Amazon S3 料金は、最新ではないオブジェクトのバージョンなど、保存または移行されるオブジェクトのバージョンごとに適用されます。詳細については、「Amazon S3 の料金」を参照してください。

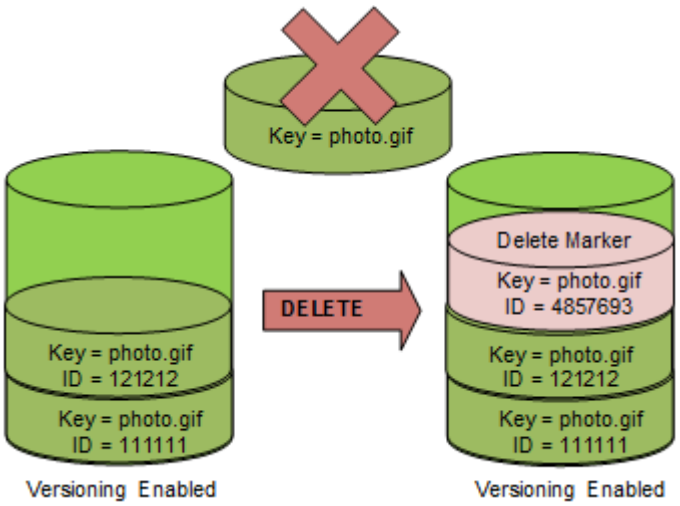
リクエストのユースケースを削除する

`DELETE` リクエストには次のユースケースがあります。

- バージョニングが有効になっている場合、単純な `DELETE` はオブジェクトを完全に削除することはできません (単純な `DELETE` リクエストとは、バージョン ID を指定しないリクエストです)。代わりに、Amazon S3 はバケットに削除マーカーを挿入します。このマーカーが新しい ID を持つオブジェクトの最新バージョンになります。

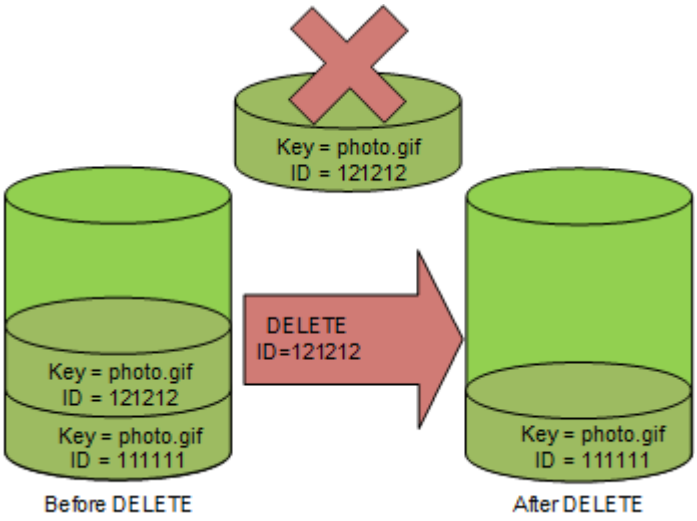
  最新バージョンが削除マーカーであるオブジェクトを `GET` しようとすると、Amazon S3 は、オブジェクトが (消去されていなくても) 削除されたものとして動作し、エラー 404 を返します。詳細については、「削除マーカーの使用」を参照してください。

次の図は、シンプルな DELETE が、指定したオブジェクトを実際には削除しないことを示しています。代わりに、Amazon S3 は削除マーカーを挿入します。



- バージョニングされたオブジェクトを完全に削除するときは、必ず DELETE Object versionId を使用します。

  次の図は、指定したオブジェクトバージョンを削除することによって、そのオブジェクトを完全に削除する方法を示しています。



オブジェクトバージョンを削除するには

Amazon S3 内のオブジェクトバージョンは、コンソール、AWS SDK、REST API、または AWS Command Line Interface を使用して削除できます。

S3 コンソールの使用

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. [Buckets] (バケット) リストで、オブジェクトが含まれるバケットの名前を選択します。
3. オブジェクト一覧から、オブジェクトの名前を選択します。
4. [バージョン] を選択します。

   Amazon S3 にオブジェクトのバージョンがすべて表示されます。
5. 完全に削除するバージョンのバージョン ID の横のチェックボックスをオンにします。
6. [削除] を選択します。
7. [オブジェクトを完全に削除しますか?] に、**`permanently delete`** と入力します。

   > ⚠ Warning
   >
   > オブジェクトバージョンを完全に削除すると、アクションを元に戻すことができません。
8. [オブジェクトの削除] を選択します。

   Amazon S3 がオブジェクトのバージョンを削除します。

AWS SDK の使用

AWS SDK for Java、.NET、PHP を使用してオブジェクトを削除する例については、Amazon S3 オブジェクトの削除 を参照してください。バージョニングが無効なバケットと有効なバケットでオブジェクトを削除する場合の例は、同一です。ただし、バージョニングが有効なバケットには、Amazon S3 がバージョン番号を割り当てます。それ以外の場合、バージョン番号は null になります。

他の AWS SDK の使用の詳細については、「AWS デベロッパーセンター」を参照してください。

Python

次の Python コード例は、すべてのバージョンを削除することによってバージョニングされたオブジェクトを完全に削除する方法を示しています。

```
def permanently_delete_object(bucket, object_key):
```

```
    """
    Permanently deletes a versioned object by deleting all of its versions.

    Usage is shown in the usage_demo_single_object function at the end of this
module.

    :param bucket: The bucket that contains the object.
    :param object_key: The object to delete.
    """
    try:
        bucket.object_versions.filter(Prefix=object_key).delete()
        logger.info("Permanently deleted all versions of object %s.", object_key)
    except ClientError:
        logger.exception("Couldn't delete all versions of %s.", object_key)
        raise
```

REST API の使用

オブジェクトの特定のバージョンを削除するには

- DELETE でバージョン ID を指定します。

Example - 特定のバージョンの削除

次の例では、photo.gif のバージョン UIORUnfnd89493jJFJ を削除します。

```
DELETE /photo.gif?versionId=UIORUnfnd89493jJFJ HTTP/1.1
Host: bucket.s3.amazonaws.com
Date: Wed, 12 Oct 2009 17:50:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:xQE0diMbLRepdf3YB+FIEXAMPLE=
Content-Type: text/plain
Content-Length: 0
```

AWS CLI を使用する場合

次のコマンドは、*amzn-s3-demo-bucket1* という名前のバケットから test.txt という名前のオブジェクトを削除します。特定のバージョンのオブジェクトを削除するには、バケット所有者として、バージョン ID サブリソースを使用する必要があります。

```
aws s3api delete-object --bucket amzn-s3-demo-bucket1 --key test.txt --version-
id versionID
```

delete-object に関する詳細については、「AWS CLI コマンドリファレンス」の「delete-object」を参照してください。

オブジェクトバージョンの削除の詳細については、以下のトピックを参照してください。

- 削除マーカーの使用
- 古いバージョンを現行バージョンにするための削除マーカーの削除
- MFA Delete が有効なバケットからのオブジェクトの削除

削除マーカーの使用

Amazon S3 の削除マーカーは、単純な DELETE リクエストで指定された、バージョニングされたオブジェクトのプレースホルダー (またはマーカー) です。単純な DELETE リクエストとは、バージョン ID を指定しないリクエストです。オブジェクトがバージョニングが有効なバケット内にあるため、そのオブジェクトは削除されません。ただし、削除マーカーにより、Amazon S3 はオブジェクトが削除されたかのように動作します。削除マーカーに対しては、Amazon S3 API DELETE コールを使用できます。これを行うには、適切なアクセス許可を持つ AWS Identity and Access Management (IAM) ユーザーまたはロールを使用して DELETE リクエストを行う必要があります。

削除マーカーには、他のすべてのオブジェクトと同様に、キー名 (またはキー) とバージョン ID があります。ただし、削除マーカーは次のような点で他のオブジェクトとは異なります。

- 削除マーカーには、データが関連付けられていません。
- 削除マーカーには、アクセスコントロールリスト (ACL) の値が関連付けられていません。
- 削除マーカーに対する GET リクエストを発行しても、削除マーカーにはデータがないため、GET リクエストでは何も取得されません。具体的には、GET リクエストで versionId を指定しない場合、404 (Not Found) エラーが表示されます。

削除マーカーにより、Amazon S3 内のストレージに対して最低料金が発生します。削除マーカーのストレージサイズは、その削除マーカーのキー名のサイズと同じです。キー名は一連の Unicode 文字です。キー名の UTF-8 エンコーディングでは、名前の文字ごとに 1～4 バイトのストレージがバケットに追加されます。削除マーカーは S3 Standard ストレージクラスに保存されます。

削除マーカーの保有数と、保存先のストレージクラスを確認する場合は、Amazon S3 ストレージレンズを使用できます。詳細については、「Amazon S3 ストレージレンズを使用してストレージのアクティビティと使用状況を評価する」および「Amazon S3 Storage Lens のメトリクスに関する用語集」を参照してください。

有効なキー名の詳細については、Amazon S3 オブジェクトに命名する を参照してください。削除マーカーの削除の詳細については、「削除マーカーの管理」を参照してください。

Amazon S3 のみが削除マーカーを作成することができ、バージョニングが有効なバケットまたは停止されたバケット内のオブジェクトに対して `DeleteObject` リクエストが送信されるたびにこの作成を行います。`DELETE` リクエストで指定したオブジェクトは実際には削除されず、代わりに削除マーカーがオブジェクトの最新バージョンになります。オブジェクトのキー名 (またはキー) が削除マーカーのキーになります。

リクエストで `versionId` を指定せずにオブジェクトを取得するときに、現在のバージョンが削除マーカーである場合、Amazon S3 は次のように応答します。

- 404 (Not Found) エラー
- レスポンスヘッダー、`x-amz-delete-marker: true`

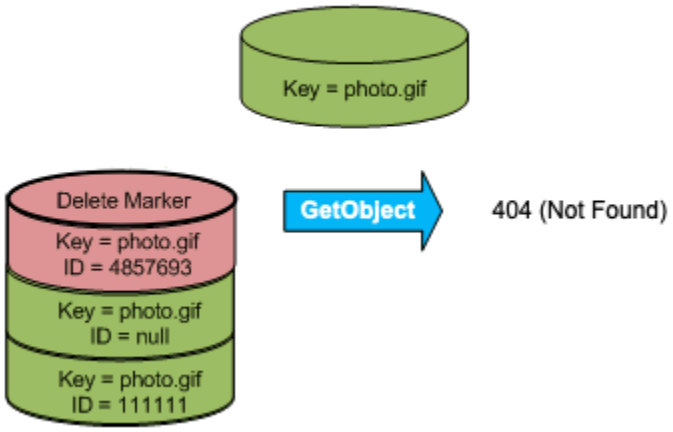
リクエストで `versionId` を指定してオブジェクトを取得するときに、指定したバージョンが削除マーカーである場合、Amazon S3 は次のように応答します。

- 405 (Method Not Allowed) エラー
- レスポンスヘッダー、`x-amz-delete-marker: true`
- レスポンスヘッダー、`Last-Modified: timestamp` (HeadObject または GetObject API オペレーションを使用する場合のみ)

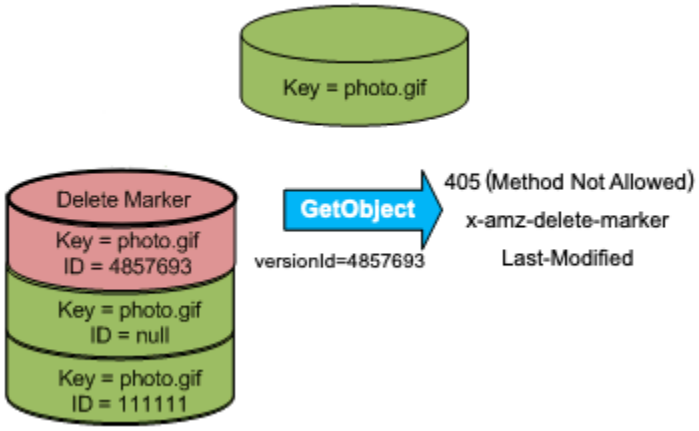
`x-amz-delete-marker: true` レスポンスヘッダーから、アクセスしたオブジェクトが削除マーカーであったことがわかります。値が `false` である場合、オブジェクトの現在のバージョンまたは指定したバージョンは削除マーカーではないため、このレスポンスヘッダーは `false` を返しません。

`Last-Modified` レスポンスヘッダーには削除マーカーの作成時間が表示されます。

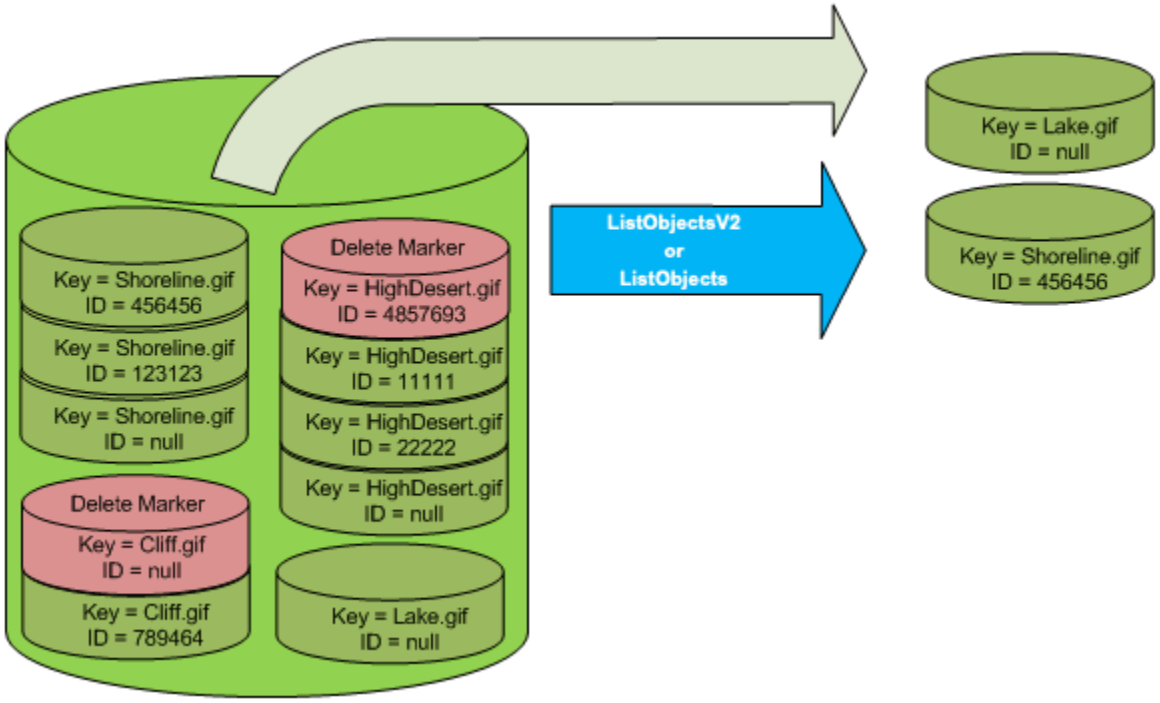
次の図は、現在のバージョンが削除マーカーであるオブジェクトに対する `GetObject` API コールから返される 404 (No Found) エラーと、レスポンスヘッダーに含まれる `x-amz-delete-marker: true` を示しています。



リクエストで `versionId` を指定してオブジェクトに対して `GetObject` コールを行った場合、指定したバージョンが削除マーカーであると、Amazon S3 は 405 (Method Not Allowed) エラーで応答し、レスポンスヘッダーには `x-amz-delete-marker: true` と `Last-Modified: timestamp` が含まれます。



削除マーカー (およびオブジェクトのその他のバージョン) をリストするには、ListObjectVersions リクエストで `versions` サブリソースを使用するしかありません。次の図で、ListObjectsV2 リクエストや ListObjects リクエストは、現在のバージョンが削除マーカーであるオブジェクトを返さないことを示しています。



削除マーカーの管理

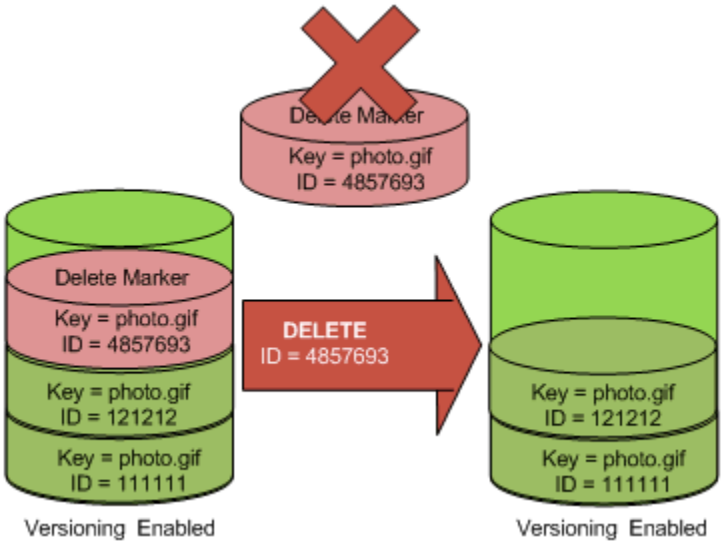
期限切れの削除マーカーを自動的にクリーンアップするライフサイクルの設定

期限切れのオブジェクト削除マーカーは、すべてのオブジェクトバージョンが削除され、単一の削除マーカーだけが残っている場合のマーカーです。ライフサイクル設定が現行バージョンを削除するように設定されている、または `ExpiredObjectDeleteMarker` アクションが明示的に設定されている場合、Amazon S3 は期限切れのオブジェクト削除マーカーを削除します。例については、「バージョニングが有効なバケットで期限切れのオブジェクト削除マーカーを削除する」を参照してください。

古いバージョンを現行バージョンにするための削除マーカーの削除

バージョニングが有効なバケット内のオブジェクトを削除すると、すべてのバージョンがバケット内に残り、Amazon S3 はオブジェクトの削除マーカーを作成します。削除したオブジェクトを復元するには、この削除マーカーを削除する必要があります。バージョニングと削除マーカーの詳細については、「S3 バージョニングによる複数のバージョンのオブジェクトの保持」を参照してください。

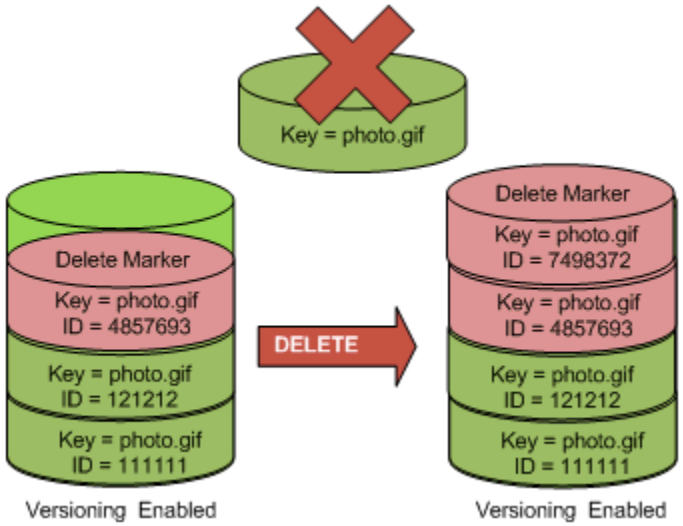
削除マーカーを完全に削除するには、`DeleteObject versionId` リクエストにそのバージョン ID を含める必要があります。次の図は、`DeleteObject versionId` リクエストが削除マーカーを完全に削除する方法を示しています。



削除マーカーを削除すると、シンプルな GET リクエストがオブジェクトの現行バージョン ID (121212) を取得するようになります。

> **Note**
>
> 現行バージョンが削除マーカーである場合に、削除マーカーのバージョン ID を指定せずに DeleteObject リクエストを使用すると、Amazon S3 は削除マーカーを削除せず、その代わりに別の削除マーカーを PUTs します。

NULL バージョン ID を持つ削除マーカーを削除するには、DeleteObject リクエストのバージョン ID として NULL を渡す必要があります。以下の図は、現行バージョンが削除マーカーになっているときに、バージョンID なしで実行されたシンプルな DeleteObject リクエストが何も削除せず、その代わりに一意のバージョン ID (7498372) を持つ削除マーカーをさらに追加する状況を示しています。



S3 コンソールの使用

S3 バケットから削除されたフォルダ以外のオブジェクト (フォルダ内のオブジェクトも含む) を復元するには、以下の手順を実行します。

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. [Buckets (バケット)] リストで、目的のバケットの名前を選択します。
3. バケット内のオブジェクトのバージョン一覧を表示するには、[バージョンのリスト] を選択します。削除されたオブジェクトの削除マーカーを表示できます。
4. 削除したオブジェクトを復元するには、削除マーカーを削除する必要があります。復元するオブジェクトの削除マーカーの横にあるチェックボックスを選択し、次に [削除] を選択します。
5. [オブジェクトの削除] ページで削除を確認します。
   a. [オブジェクトを完全に削除しますか?] に、**`permanently delete`** と入力します。
   b. [オブジェクトの削除] を選択します。

> **Note**
>
> Amazon S3 コンソールでは、削除されたフォルダを元に戻すことはできません。AWS CLI または SDK を使用する必要があります。例については、AWS ナレッジセンターのバージョニングが有効なバケットで削除された Amazon S3 オブジェクトを取得する方法を教えてくださいを参照してください。

REST API の使用

削除マーカーを完全に削除するには

1. `versionId` を、削除する削除マーカーのバージョン ID に設定します。
2. `DELETE Object versionId` リクエストを送信します。

Example - 削除マーカーの削除

次の例では、`photo.gif` のバージョン 4857693 の削除マーカーを削除します。

```
DELETE /photo.gif?versionId=4857693 HTTP/1.1
Host: bucket.s3.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU=
```

削除マーカーを削除すると、Amazon S3 はレスポンスに以下を含めます。

```
204 NoContent
x-amz-version-id: versionID
x-amz-delete-marker: true
```

AWS SDK の使用

他の AWS SDK の使用の詳細については、「AWS デベロッパーセンター」を参照してください。

Python

次の Python コード例は、オブジェクトから削除マーカーを削除し、最新でないバージョン (最新に最も近いもの) をオブジェクトの最新のバージョンにする方法を示しています。

```
def revive_object(bucket, object_key):
    """
    Revives a versioned object that was deleted by removing the object's active
    delete marker.
    A versioned object presents as deleted when its latest version is a delete
 marker.
    By removing the delete marker, we make the previous version the latest version
    and the object then presents as *not* deleted.

    Usage is shown in the usage_demo_single_object function at the end of this
 module.
```

```
    :param bucket: The bucket that contains the object.
    :param object_key: The object to revive.
    """
    # Get the latest version for the object.
    response = s3.meta.client.list_object_versions(
        Bucket=bucket.name, Prefix=object_key, MaxKeys=1
    )

    if "DeleteMarkers" in response:
        latest_version = response["DeleteMarkers"][0]
        if latest_version["IsLatest"]:
            logger.info(
                "Object %s was indeed deleted on %s. Let's revive it.",
                object_key,
                latest_version["LastModified"],
            )
            obj = bucket.Object(object_key)
            obj.Version(latest_version["VersionId"]).delete()
            logger.info(
                "Revived %s, active version is now %s  with body '%s'",
                object_key,
                obj.version_id,
                obj.get()["Body"].read(),
            )
        else:
            logger.warning(
                "Delete marker is not the latest version for %s!", object_key
            )
    elif "Versions" in response:
        logger.warning("Got an active version for %s, nothing to do.", object_key)
    else:
        logger.error("Couldn't get any version info for %s.", object_key)
```

MFA Delete が有効なバケットからのオブジェクトの削除

バケットのバージョニング設定で MFA Delete が有効になっている場合に、オブジェクトバージョンを完全に削除したり、バケットのバージョニング状態を変更したりするには、バケット所有者はリクエストに x-amz-mfa リクエストヘッダーを含める必要があります。x-amz-mfa を含むリクエストでは、HTTPS を使用する必要があります。

ヘッダーの値は、認証デバイスのシリアル番号、スペース、および認証デバイスに表示される認証コードの連結文字です。このリクエストヘッダーを含めないと、リクエストは失敗します。

認証デバイスの詳細については、「多要素認証」を参照してください。

Example - MFA Delete が有効なバケットからのオブジェクトの削除

次の例は、my-image.jpg を (バージョンを指定して) 削除しています。これは、MFA Delete が有効に設定されたバケットの中にあります。

[SerialNumber] と *[AuthenticationCode]* の間のスペースに注意してください。詳細については、「Amazon Simple Storage Service API リファレンス」の「DeleteObject」を参照してください。

```
DELETE /my-image.jpg?versionId=3HL4kqCxf3vjVBH40Nrjfkd HTTPS/1.1
Host: bucketName.s3.amazonaws.com
x-amz-mfa: 20899872 301749
Date: Wed, 28 Oct 2009 22:32:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU=
```

MFA Delete の有効化の詳細については、「MFA 削除の設定」を参照してください。

バージョン管理されたオブジェクトのアクセス許可の設定

Amazon S3 のオブジェクトのアクセス許可は、バージョンレベルで設定されています。各バージョンには個々のオブジェクト所有者がいます。この所有者は、オブジェクトバージョンを作成する AWS アカウントです。したがって、同じオブジェクトの異なるバージョンに対して、異なるアクセス許可を設定することができます。これを行うには、PUT Object versionId acl リクエストでアクセス権限を設定するオブジェクトのバージョン ID を指定する必要があります。ACL の使用の詳細と手順については、「Amazon S3 用 Identity and Access Management」を参照してください。

Example - オブジェクトバージョンに対するアクセス許可の設定

次のリクエストは、キー my-image.jpg、バージョンID 3HL4kqtJvjVBH40Nrjfkd に対して、被付与者 BucketOwner@amazon.com の許可を FULL_CONTROL に設定するものです。

```
PUT /my-image.jpg?acl&versionId=3HL4kqtJvjVBH40Nrjfkd HTTP/1.1
Host: bucket.s3.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU=
Content-Length: 124
```

```
<AccessControlPolicy>
  <Owner>
    <ID>75cc57f09aa0c8caeab4f8c24e99d10f8e7faeebf76c078efc7c6caea54ba06a</ID>
    <DisplayName>mtd@amazon.com</DisplayName>
  </Owner>
  <AccessControlList>
    <Grant>
      <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:type="CanonicalUser">
        <ID>a9a7b886d6fd24a52fe8ca5bef65f89a64e0193f23000e241bf9b1c61be666e9</ID>
        <DisplayName>BucketOwner@amazon.com</DisplayName>
      </Grantee>
      <Permission>FULL_CONTROL</Permission>
    </Grant>
  </AccessControlList>
  </AccessControlPolicy>
```

同様に、特定のオブジェクトバージョンに対するアクセス許可を取得するには、GET Object versionId acl リクエストでそのバージョン ID を指定する必要があります。デフォルトでは GET Object acl はオブジェクトの最新バージョンに対するアクセス許可を返すため、バージョン ID を含める必要があります。

Example - 指定したオブジェクトバージョンに対するアクセス許可の取得

次の例では、Amazon S3 はキー my-image.jpg、バージョン ID DVBH40Nr8X8gUMLUo に対するアクセス許可を返します。

```
GET /my-image.jpg?versionId=DVBH40Nr8X8gUMLUo&acl HTTP/1.1
Host: bucket.s3.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU
```

詳細については、「Amazon Simple Storage Service API リファレンス」の「GetObjectAcl」を参照してください。

バージョニングが停止されたバケットのオブジェクトの操作

Amazon S3 では、バケット内で同じオブジェクトの新しいバージョンが生成されないようにするには、バージョニングを停止します。この作業は、バケット内のオブジェクトのバージョンが 1 つだけ必要な場合に行います。あるいは、複数のバージョンで料金を発生させたくない場合などです。

バージョニングを停止しても、バケットに含まれる既存のオブジェクトは変更されません。変更されるのは、Amazon S3 が今後のリクエストでオブジェクトを処理する方法です。このセクションのトピックでは、バージョニングが停止されたバケットでの、オブジェクトの追加、取得、削除など、さまざまなオペレーションについて説明します。

S3 バージョニングの詳細については、S3 バージョニングによる複数のバージョンのオブジェクトの保持 を参照してください。オブジェクトバージョンの取得の詳細については、「バージョニングが有効なバケットからのオブジェクトバージョンの取得」を参照してください。

トピック

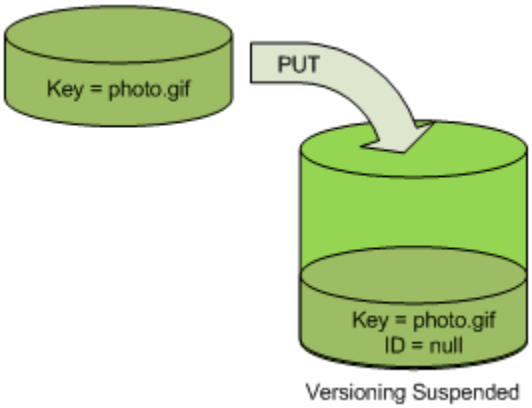
- バージョニングが停止されたバケットへのオブジェクトの追加
- バージョニングが停止されたバケットからのオブジェクトの取得
- バージョニングが停止されたバケットからのオブジェクトの削除

バージョニングが停止されたバケットへのオブジェクトの追加

Amazon S3 でバージョニングが停止されたバケットにオブジェクトを追加すると、null バージョン ID の付いたオブジェクトが作成されるか、または同じバージョン ID のオブジェクトバージョンが上書きされます。

バケットでバージョニングを停止すると、Amazon S3 は (PUT、POST、CopyObject を使用して) その後そのバケットに保存された後続のすべてのオブジェクトに、null バージョン ID を自動的に追加します。

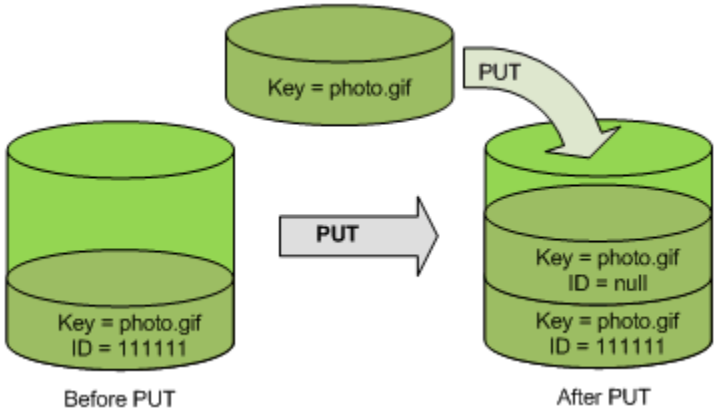
次の図は、バージョニングが停止されたバケットにオブジェクトが追加されたときに、Amazon S3 がそのオブジェクトにバージョン ID null を追加する方法を示しています。



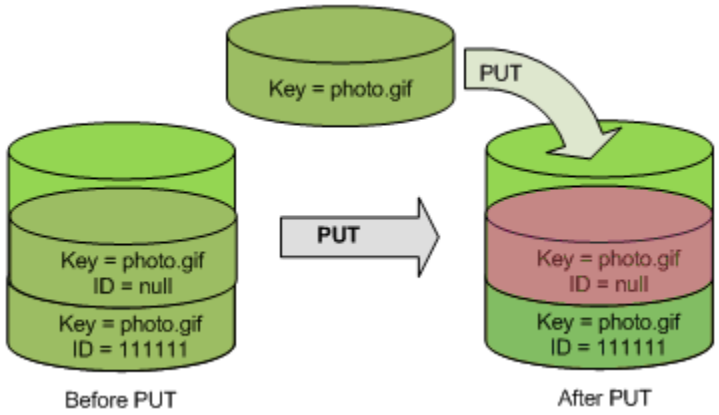
バケット内に null バージョンが既に存在しており、同じキーを持つ別のオブジェクトを追加した場合、元の null バージョンは、追加したオブジェクトによって上書きされます。

バケット内にバージョニングされたオブジェクトがある場合、PUT したバージョンはオブジェクトの最新バージョンになります。次の図は、バージョニングされたオブジェクトを含むバケットにオブジェクトを追加しても、バケット内に既に存在するオブジェクトを上書きしないことを示しています。

この場合、バケット内にバージョン 111111 がすでに存在しています。Amazon S3 は、追加されるオブジェクトに null のバージョン ID をアタッチし、バケット内に保存します。バージョン 111111 は上書きされません。



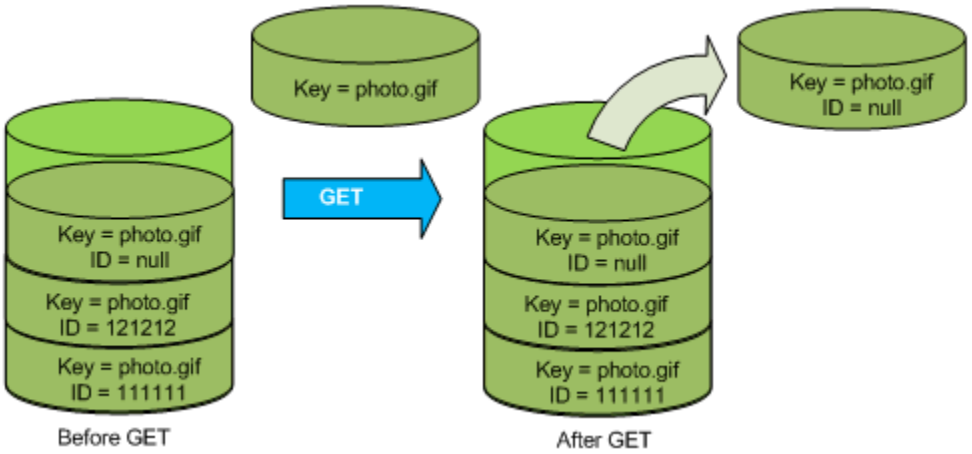
次の図に示すように、バケット内に null バージョンが既に存在する場合、null バージョンは上書きされます。



null バージョンのキーおよびバージョン ID (`null`) は PUT の前後で同じですが、バケット内に元々格納されていた null バージョンの内容は、バケット内のオブジェクト PUT の内容に置き換えられます。

バージョニングが停止されたバケットからのオブジェクトの取得

GET Object リクエストは、バケットでバージョニングを有効にしているかどうかにかかわらず、オブジェクトの最新バージョンを返します。次の図は、シンプルな GET がオブジェクトの最新バージョンを返す方法を示しています。



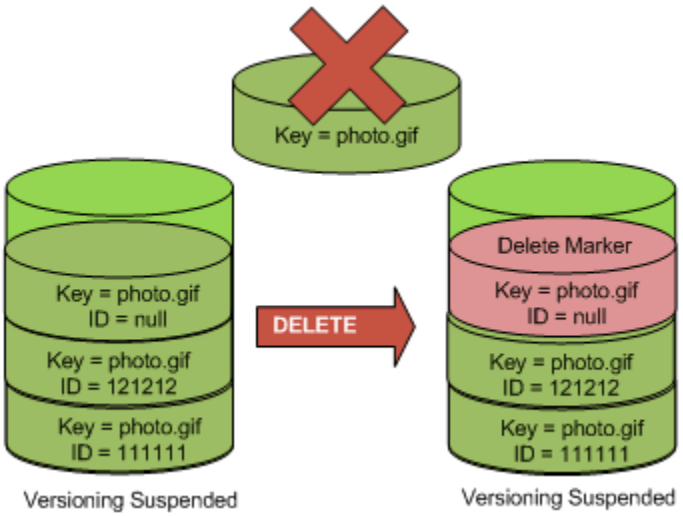
バージョニングが停止されたバケットからのオブジェクトの削除

バージョニングが停止されたバケットからオブジェクトを削除することで、null バージョン ID の付いたオブジェクトを削除します。

バケットのバージョニングが停止されている場合、DELETE リクエストは次のように動作します。

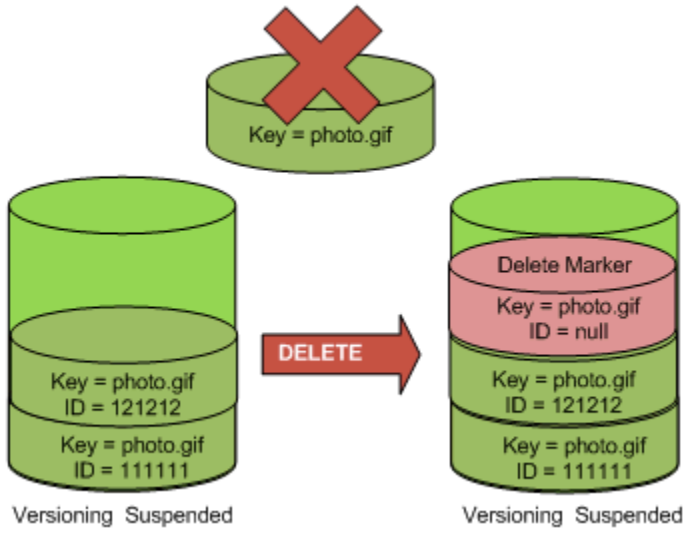
- バージョン ID が null であるオブジェクトのみを削除できる。
- バケット内にオブジェクトの null バージョンが存在しない場合は、何も削除しません。
- バケットに削除マーカーを挿入する。

バケットバージョニングが停止されている場合、オペレーションは null versionId を持つオブジェクトを削除します。バージョン ID が存在する場合、Amazon S3 はオブジェクトの最新バージョンとなる削除マーカーを挿入します。次の図は、単純な DELETE が null バージョンを削除し、代わりに Amazon S3 がその位置に null のバージョン ID を持つ削除マーカーを挿入する方法を示しています。

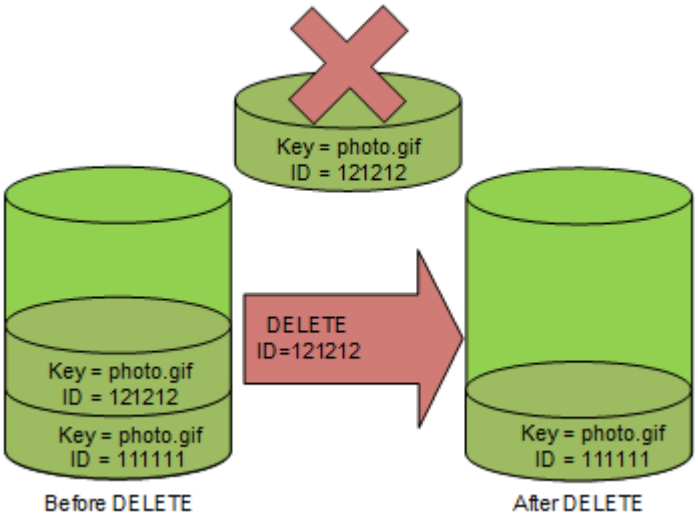


versionId を持つオブジェクトを完全に削除するには、オブジェクトの versionId をリクエストに含める必要があります。削除マーカーにはコンテンツが含まれていないため、削除マーカーが置き換えられると、null バージョンのコンテンツが失われます。

次の図は、null バージョンが存在しないバケットを示しています。この場合、DELETE は何も削除しません。代わりに、Amazon S3 は削除マーカーを挿入します。



バージョニングが停止されたバケットでも、バケット所有者は DELETE リクエスト内のバージョン IDを含む指定バージョンを完全に削除できます。次の図は、指定したオブジェクトバージョンを削除することによって、そのオブジェクトのバージョンを完全に削除する方法を示しています。バケット所有者のみが、指定したオブジェクトバージョンを削除することができます。



バージョニングのトラブルシューティング

次のトピックは Amazon S3 のバージョニングのよくある問題をトラブルシューティングするのに役立ちます。

トピック

- バージョニングが有効なバケットで、誤って削除されたオブジェクトを復元する
- バージョニングされたオブジェクトを完全に削除する
- バケットのバージョニングを有効にした後、パフォーマンスが低下している

バージョニングが有効なバケットで、誤って削除されたオブジェクトを復元する

一般に、S3 バケットからオブジェクトバージョンが削除された場合、それらを Amazon S3 で復元する方法はありません。ただし、S3 バケットで S3 バージョニングを有効にしている場合、バージョン ID を指定しない DELETE リクエストでは、オブジェクトを完全に削除できません。代わりに、削除マーカーがプレースホルダーとして追加されます。この削除マーカーはオブジェクトの最新バージョンになります。

削除したオブジェクトが完全に削除されているのか、一時的に削除されているのか (その場所に削除マーカーが表示されているか) を確認するには、次の手順に従います。

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。
3. [バケット] リストで、オブジェクトが含まれるバケットの名前を選択します。

4. [オブジェクト]リストで、検索バーの右側にある[バージョンの表示]トグルをオンにして、検索バーで削除されたオブジェクトを検索します。このトグルは、バケットで以前にバージョニングが有効だった場合に限り使用できます。

   S3 インベントリを使用して、削除されたオブジェクトを検索することもできます。

5. [バージョンの表示] の切り替えや、インベントリレポートの作成の後にオブジェクトが見つからず、オブジェクトの削除マーカーも見つからない場合、完全に削除され、オブジェクトを復元することはできません。

また、AWS Command Line Interface (AWS CLI) の HeadObject API オペレーションを使用して、削除されたオブジェクトの状態を確認できます。それには、次の head-object コマンドを使用して、*user input placeholders* を自分の情報に置き換えます。

```
aws s3api head-object --bucket amzn-s3-demo-bucket --key index.html
```

最新バージョンが削除マーカーであるバージョニングされたオブジェクトに対して head-object コマンドを実行すると、404 Not Foundエラーが表示されます。例:

HeadObject オペレーションの呼び出し時にエラーが発生しました (404): Not Found

バージョニングされたオブジェクトに対して head-object コマンドを実行し、オブジェクトのバージョン ID を指定すると、Amazon S3 はオブジェクトのメタデータを取得し、オブジェクトがまだ存在し、完全に削除されていないことを確認します。

```
aws s3api head-object --bucket amzn-s3-demo-bucket --key index.html --
version-id versionID
```

```
{
"AcceptRanges": "bytes",
"ContentType": "text/html",
"LastModified": "Thu, 16 Apr 2015 18:19:14 GMT",
"ContentLength": 77,
"VersionId": "Zg5HyL7m.eZU9iM7AVlJkrqAiE.0UG4q",
"ETag": "\"30a6ec7e1a9ad79c203d05a589c8b400\"",
"Metadata": {}
}
```

オブジェクトが見つかり、最新バージョンが削除マーカーの場合、オブジェクトの以前のバージョンがまだ存在します。削除マーカーはオブジェクトの最新バージョンであるため、削除マーカーを削除することでオブジェクトを復元できます。

削除マーカーを完全に削除すると、2 番目に新しいバージョンのオブジェクトが最新のバージョンのオブジェクトになり、オブジェクトを再び使用できるようになります。オブジェクトの復元方法を視覚的に説明するには、「削除マーカーの削除」を参照してください。

特定のバージョンのオブジェクトを削除するには、バケット所有者になる必要があります。削除マーカーを完全に削除するには、DeleteObject リクエストにそのバージョン ID を含める必要があります。それには、次のコマンドを使用して、*user input placeholders* を自分の情報に置き換えます。

```
aws s3api delete-object --bucket amzn-s3-demo-bucket --key index.html --
version-id versionID
```

delete-object コマンドの詳細については、AWS CLI コマンドリファレンスの「delete-object」を参照してください。削除マーカーの完全削除の詳細については、「削除マーカーの管理」を参照してください。

バージョニングされたオブジェクトを完全に削除する

バージョニングが有効なバケットでは、バージョン ID のない DELETE リクエストではオブジェクトを完全に削除することはできません。このようなリクエストでは、代わりに削除マーカーが挿入されます。

バージョニングされたオブジェクトを完全に削除するには、以下の方法から選択できます。

- S3 ライフサイクルルールを作成して、最新ではないバージョンを完全に削除します。最新ではないバージョンのオブジェクトを完全に削除するには、[現在のバージョンではないオブジェクトを完全に削除する]を選択し、[オブジェクトが最新バージョンでなくなってからの日数]に日数を入力します。オプションで、[Number of newer versions to retain] (保持する新しいバージョンの数) に値を入力して、保持する新しいバージョンの数を指定できます。このルールの作成については、「S3 ライフサイクル設定の指定」を参照してください。
- DELETE リクエストにバージョン ID を含め、指定されたバージョンを削除します。詳細については、「バージョニングされたオブジェクトの完全削除方法」を参照してください。
- 現在のバージョンを期限切れにするライフサイクルルールを作成します。オブジェクトの現在のバージョンを期限切れにするには、[オブジェクトの現行バージョンを期限切れにする]を選択し、[オブジェクトの作成後の日数]に日数を入力します。このライフサイクルルールの作成については、「S3 ライフサイクル設定の指定」を参照してください。
- バージョニングされたオブジェクトと削除マーカーをすべて完全に削除するには、2 つのライフサイクルルールを作成します。1 つは現在のバージョンを期限切れにして古いバージョンのオブ

ジェクトを完全に削除するルールで、もう 1 つは期限切れのオブジェクト削除マーカーを削除するルールです。

バージョニングが有効なバケットでは、バージョン ID を指定しない DELETE リクエストでは、NULL バージョン ID を持つオブジェクトのみを削除できます。バージョニングが有効の場合にオブジェクトがアップロードされた場合、バージョン ID を指定しない DELETE リクエストにより、そのオブジェクトの削除マーカーを作成します。

> **Note**
>
> S3 オブジェクトロックが有効なバケットでは、保護されたオブジェクトバージョン ID を含む DELETE オブジェクトリクエストにより、403 Access Denied エラーが発生します。バージョン ID のない DELETE オブジェクトリクエストでは、200 OK レスポンスでオブジェクトの最新バージョンとして削除マーカーが追加されます。オブジェクトロックで保護されているオブジェクトは、その保存期間とリーガルホールドが解除されるまで完全に削除できません。詳細については、「the section called “S3 オブジェクトロックの仕組み”」を参照してください。

バケットのバージョニングを有効にした後、パフォーマンスが低下している

削除マーカーやバージョニングされたオブジェクトが多すぎる場合や、ベストプラクティスに従わない場合、バージョニングが有効なバケットでパフォーマンスが低下する可能性があります。

削除マーカーが多すぎる

バケットでバージョニングを有効にすると、オブジェクトに対してバージョン ID を持たない DELETE リクエストを行うと、一意のバージョン ID の削除マーカーが作成されます。現在のバージョンのオブジェクトを期限切れにするルールを含むライフサイクル設定では、すべてのオブジェクトに一意のバージョン ID を持つ削除マーカーが追加されます。削除マーカーが多すぎると、バケットのパフォーマンスが低下する可能性があります。

バケットでバージョニングが停止すると、Amazon S3 では新しく作成されたオブジェクトに対するバージョン ID を NULL としてマークします。バージョニングが停止されたバケットで期限切れアクションを行うと、Amazon S3 がバージョン ID として NULL を使用する削除マーカーを作成します。バージョニングが停止されたバケットでは、すべての削除リクエストに対して NULL 削除マーカーが作成されます。これらの NULL 削除マーカーは、すべてのオブジェクトバージョンが削除され、単一

の削除マーカーだけが残っている場合、期限切れオブジェクト削除マーカーとも呼ばれます。NULL 削除マーカーが多すぎると、バケットのパフォーマンスが低下します。

バージョニングされたオブジェクトが多すぎる

バージョニングが有効なバケットに数百万のバージョンのオブジェクトが含まれている場合、503 Service Unavailable エラーが増える可能性があります。バージョニングを有効にしたバケットへの PUT または DELETE オブジェクトリクエストに対して受信される HTTP 503 Service Unavailable レスポンスの数が著しく増加した場合、バケットに数百万のバージョンが存在するオブジェクトがある可能性があります。何百万ものバージョンのオブジェクトがある場合、Amazon S3 はバケットへのリクエストを自動的に制限します。リクエストのスロットリングによって、過剰なリクエストトラフィックからバケットを保護しますが、同じバケットに対して行われた他のリクエストに支障がある可能性があります。

数百万のバージョンがあるオブジェクトを確認するには、S3 インベントリを使用します。S3 インベントリは、バケット内のオブジェクトのフラットファイルリストを提供するレポートを生成します。詳細については、「S3 インベントリを使用したデータのカタログ化と分析」を参照してください。

バケット内でバージョニングされたオブジェクト数が多いかどうかを確認するには、S3 Storage Lens メトリクスを使用して、現在のバージョンのオブジェクト数、最新ではないバージョンのオブジェクト数、削除マーカーのオブジェクト数を表示します。Storage Lens メトリクスの詳細については、「Amazon S3 Storage Lens のメトリクスに関する用語集」を参照してください。

Amazon S3 チームでは、同じオブジェクトを繰り返し上書きし、そのオブジェクトに対して数百万のバージョンを作成する可能性のあるアプリケーションを調査して、アプリケーションが意図どおり動作しているかどうか調査することをお客様にお勧めしています。例えば、アプリケーションが毎分同じオブジェクトを 1 週間上書きすると、1 万を超えるバージョンが作成されることになります。各オブジェクトに保存するバージョンは 10 万未満にすることをお勧めします。単一または複数の Amazon S3 オブジェクトに対して数百万のバージョンを必要とするユースケースがある場合の最適なソリューションを決定するには、AWS サポート チームにご相談ください。

ベストプラクティス

バージョニングに関連したパフォーマンス低下の問題を防ぐため、次のベストプラクティスを採用することをお勧めします。

- ライフサイクルルールを有効にして、以前のバージョンのオブジェクトを期限切れにする。例えば、オブジェクトが最新ではない状態になってから 30 日後に、最新ではないバージョンを期限切れにするライフサイクルルールを作成できます。すべてを削除する必要がない場合は、最新では

ないバージョンを複数保持することもできます。詳細については、「S3 ライフサイクル設定の指定」を参照してください。

- ライフサイクルルールを有効にして、バケットに関連するデータオブジェクトがない期限切れのオブジェクト削除マーカーを削除します。詳細については、「期限切れオブジェクト削除マーカーの削除」を参照してください。

Amazon S3 のパフォーマンス最適化に関するその他のベストプラクティスについては、「ベストプラクティスのデザインパターン」を参照してください。

S3 Object Lock を使用したオブジェクトのロック

S3 オブジェクトロックは、Amazon S3 オブジェクトが一定期間または無期限に削除または上書きされるのを防ぐのに役立ちます。オブジェクトロックは、write-once-read-many (WORM) モデルを使用してオブジェクトを保存します。Object Lock を使用して、WORM ストレージを必要とする規制要件を満たしたり、オブジェクトの変更や削除に対する保護レイヤーを追加したりできます。

> **Note**
>
> S3 オブジェクトロックは、SEC 17a-4、CFTC、および FINRA の各規制に従った環境での使用について、Cohasset Associates によって評価済みです。オブジェクトロックとこのような規制との関連性の詳細については、「Cohasset Associates Compliance Assessment」を参照してください。

オブジェクトロックは、オブジェクトリテンションの管理をするための 2 つの方法、保持期間およびリーガルホールドを提供します。オブジェクトバージョンには、保持期間とリーガルホールド、またはその両方を含めることができます。

- 保持期間 – オブジェクトバージョンがロックされたままである一定期間を指定します。個々のオブジェクトに固有の保持期間を設定できます。また、S3 バケットにデフォルトの保持期間を設定できます。バケットポリシーの `s3:object-lock-remaining-retention-days` 条件キーを使用して、許容される最小保持期間と最大保持期間を制限することもできます。これにより、保持期間の範囲を定めて、保持期間がこの範囲より短くなったり長くなったりするのを制限することができます。
- リーガルホールド – リーガルホールドは、保持期間と同じ保護を提供します。ただし、有効期限はありません。代わりに、明示的に削除するまで、リーガルホールドは維持されます。リーガルホールドは、保持期間から独立しており、個々のオブジェクトバージョンに付与されます。

オブジェクトロックは S3 バージョニングが有効になっているバケットでのみ機能します。オブジェクトバージョンをロックすると、Amazon S3 はそのオブジェクトバージョンのメタデータにロック情報を保存します。オブジェクトに保持期間またはリーガルホールドを設定すると、リクエストで指定されたバージョンのみが保護されます。保持期間とリーガルホールドを使用しても、オブジェクトの新しいバージョンの作成が阻止されたり、オブジェクトの上に追加されるマーカーが削除されたりすることはありません。S3 バージョニングの詳細については、「S3 バージョニングによる複数のバージョンのオブジェクトの保持」を参照してください。

同じオブジェクトキー名を持つ既存の保護対象オブジェクトが既に含まれているバケットにオブジェクトを配置すると、Amazon S3 はそのオブジェクトの新しいバージョンを作成します。オブジェクトの既存の保護バージョンは、その保持設定に従ってロックされたままになります。

S3 オブジェクトロックの仕組み

トピック

- 保持期間
- リテンションモード
- リーガルホールド
- S3 Object Lock を使用するためのベストプラクティス
- 必要なアクセス許可

保持期間

保持期間は、一定期間オブジェクトバージョンを保護します。オブジェクトバージョンに保持期間を設定すると、Amazon S3 はオブジェクトバージョンのメタデータにタイムスタンプを保存して、保持期間の有効期限を示します。保持期間が終了すると、オブジェクトバージョンを上書きまたは削除することができます。

個々のオブジェクトバージョンまたはバケットのプロパティに明示的に保存期間を設定して、バケット内のすべてのオブジェクトに自動的に適用されるようにすることができます。オブジェクトバージョンに保持期間を明示的に適用する場合は、オブジェクトバージョンに対して [リテンション期日] を指定します。Amazon S3 はこの日付をオブジェクトバージョンのメタデータにを保存します。

バケットのプロパティに保持期間を設定することもできます。バケットに保持期間を設定する場合、バケット内に配置されたすべてのオブジェクトバージョンを保護する期間を日数または年単位で指定します。バケットにオブジェクトを配置すると、Amazon S3 は、オブジェクトバージョンの作成タ

イムスタンプに指定された期間を追加してオブジェクトバージョンの保持期日を算出します。これにより、オブジェクトバージョンは、オブジェクトバージョンにその保持期間のロックを明示的に配置した場合と同様に保護されます。

> **Note**
>
> 個別の保存モードと期間が明示的に設定されているオブジェクトバージョンをバケット内に PUT すると、オブジェクトバージョンの個々のオブジェクトロック設定が、バケットプロパティの保存設定よりも優先されます。

他のすべての オブジェクトロック設定と同様に、保持期間は個々のオブジェクトバージョンに適用されます。単一のオブジェクトのバージョンが異なれば、リテンションモードや期間も異なる可能性があります。

たとえば、30 日間の保持期間に 15 日のオブジェクトがあり、同じ名前と 60 日間の保持期間を持つオブジェクトを Amazon S3 に PUT するとします。この場合、PUT は正常に実行され、Amazon S3 は保持期間が 60 日の新しいバージョンを作成します。古いバージョンは元の保持期間を維持し、15 日後に削除可能になります。

保持設定をオブジェクトバージョンに適用した後、保持期間を延長することができます。これを行うには、現在設定されているオブジェクトバージョンよりも後の保持期間を持つオブジェクトバージョンの新しいオブジェクトロックリクエストを送信します。Amazon S3 は、既存の保持期間を新しい、より長い期間に置き換えます。オブジェクトの保持期間を設定するアクセス許可を持つユーザーは、オブジェクトバージョンの保持期間を延長できます。保持期間を設定するには、`s3:PutObjectRetention` アクセス許可が必要です。

オブジェクトまたは S3 バケットに保持期間を設定する場合、コンプライアンスまたはガバナンスの 2 つの保持モードのいずれかを選択する必要があります。

リテンションモード

S3 オブジェクトロックでは、オブジェクトに異なるレベルの保護を適用する次の 2 つの保持モードが提供されています。

- コンプライアンスモード
- ガバナンスモード

コンプライアンスモードでは、AWS アカウント の root ユーザーを含め、ユーザーが、保護されたオブジェクトのバージョンを上書きまたは削除することはできません。コンプライアンスモードでオブジェクトをロックすると、そのリテンションモードを変更することはできず、保持期間を短縮することはできません。コンプライアンスモードでは、保持期間中にオブジェクトのバージョンを上書きまたは削除できないようにします。

> **Note**
>
> 保持期限が切れる前にコンプライアンスモードのオブジェクトを削除する唯一の方法は、関連する AWS アカウント を削除することです。

ガバナンスモードでは、特別なアクセス許可を持たない限り、ユーザーはオブジェクトのバージョンの上書きや削除、ロック設定を変更することはできません。ガバナンスモードでは、ほとんどのユーザーがオブジェクトを削除できないように保護できます。ただし必要に応じて、一部のユーザーに保持設定を変更したり、オブジェクトを削除したりするアクセス許可を付与することもできます。ガバナンスモードを使用して、コンプライアンスモードの保持期間を作成する前に、保持期間の設定をテストすることもできます。

ガバナンスモードのリテンション設定を上書きまたは削除するには、ユーザーは `s3:BypassGovernanceRetention` アクセス許可を持っている必要があり、また、ガバナンスモードの上書きを必要とするリクエストで、`x-amz-bypass-governance-retention:true` をリクエストヘッダーとして明示的に含める必要があります。

> **Note**
>
> Amazon S3 コンソールにはデフォルトで、`x-amz-bypass-governance-retention:true` ヘッダーが含まれています。ガバナンスモードで保護されているオブジェクトを削除する場合、`s3:BypassGovernanceRetention` アクセス許可があれば、そのオペレーションは正常に完了します。

リーガルホールド

オブジェクトロックを使用すると、オブジェクトバージョンにリーガルホールドを設定することもできます。保持期間と同様に、リーガルホールドは、オブジェクトバージョンが上書きまたは削除されるのを防ぎます。ただし、リーガルホールドには関連する保持期間はなく、削除するまで有効です。

リーガルホールドは、s3:PutObjectLegalHold アクセス許可を持つ任意のユーザーが自由に適用および解除できます。

リーガルホールドは、保持期間から独立しています。オブジェクトバージョンをリーガルホールドしても、そのオブジェクトバージョンのリテンションモードや保持期間には影響しません。

例えば、オブジェクトバージョンをリーガルホールドして、オブジェクトバージョンも保持期間で保護するとします。保持期間が終了すると、オブジェクトは WORM 保護を失いません。むしろ、リーガルホールドでは、許可されたユーザーが明示的に解除するまでオブジェクトの保護が継続されます。同様に、オブジェクトバージョンに有効な保持期間がある間にリーガルホールドを解除すると、保護期間が終了するまでオブジェクトバージョンは保護されたままになります。

S3 Object Lock を使用するためのベストプラクティス

事前定義された保持期間中にほとんどのユーザーがオブジェクトを削除しないようにするが、同時に特別なアクセス許可を持つ一部のユーザーに保持設定を変更したり、オブジェクトを削除したりできる柔軟性を持たせたい場合は、「ガバナンスモード」の使用を検討してください。

AWS アカウント のルートユーザーを含むユーザーが、事前定義された保持期間中にオブジェクトを削除できないようにしたい場合は、「コンプライアンスモード」の使用を検討してください。このモードは、準拠したデータを保存する必要がある場合に使用できます。

「リーガルホールド」は、オブジェクトを変更不可能な状態に保つ期間が不明な場合に使用できます。これを使用する理由として、データの外部監査が今後予定されていて監査が完了するまでオブジェクトを変更不可能な状態に保ちたい、といったことが考えられます。または、進行中のプロジェクトがあり、プロジェクトが完了するまで変更不可能な状態を保ちたいデータセットを使用している場合もあります。

必要なアクセス許可

オブジェクトロックオペレーションにはアクセス許可が必要です。実行しようとする個別のオペレーションによっては、次の許可のいずれかが必要になる場合があります。

- s3:BypassGovernanceRetention
- s3:GetBucketObjectLockConfiguration
- s3:GetObjectLegalHold
- s3:GetObjectRetention
- s3:PutBucketObjectLockConfiguration
- s3:PutObjectLegalHold

- `s3:PutObjectRetention`

Amazon S3 のアクセス許可の説明付きの完全なリストについては、「サービス認可リファレンス」の「Amazon S3 のアクション、リソース、および条件キー」を参照してください。

S3 リソースタイプ別の S3 API オペレーションへのアクセス許可の詳細については、「Amazon S3 API オペレーションに必要なアクセス許可」を参照してください。

アクセス許可で条件を使用する方法の詳細については、「条件キーを使用したバケットポリシーの例」を参照してください。

オブジェクトロックの考慮事項

Amazon S3 オブジェクトロックは、オブジェクトが一定期間または無期限に削除または上書きされるのを防ぐのに役立ちます。

Amazon S3 コンソール、AWS Command Line Interface (AWS CLI)、AWS SDK、または Amazon S3 REST API を使用して、オブジェクトロック情報を表示したり設定したりできます。S3オブジェクトロック機能全般については、「S3 Object Lock を使用したオブジェクトのロック」を参照してください。

> **Important**
>
> - オブジェクトロックを有効にしたバケットを作成した後、オブジェクトロックを無効にしたり、バケットのバージョニングを停止することはできません。
> - S3 オブジェクトロックが有効になっている S3 バケットは、サーバーアクセスログの送信先バケットとしては使用できません。詳細については、「the section called “サーバーアクセスのログ記録”」を参照してください。

トピック

- ロック情報を表示するためのアクセス許可
- ガバナンスモードのバイパス
- S3 レプリケーションでのオブジェクトロックの使用
- Object Lock で暗号化を使用する
- AmazonS3 インベントリでのオブジェクトロックの使用
- Object Lock による S3 ライフサイクルポリシーの管理

- Object Lock による削除マーカーの管理
- オブジェクトロックでの S3 Storage Lens の使用
- Object Lock が有効なバケットへのオブジェクトのアップロード
- イベントと通知の設定
- バケットポリシーを使用する保持期間の制限の設定

ロック情報を表示するためのアクセス許可

HeadObject オペレーションまたは GetObject オペレーションを使用して、Amazon S3 オブジェクトバージョンのオブジェクトロックステータスをプログラムで表示できます。いずれのオペレーションでも、指定されたオブジェクトバージョンの保持モード、保持期日、リーガルホールドステータスが返されます。また、S3 インベントリを使用して、S3 バケット内の複数のオブジェクトの Object Lock ステータスを表示できます。

オブジェクトバージョンのリテンションモードおよび保存期間を表示するには、`s3:GetObjectRetention` アクセス許可が必要です。オブジェクトバージョンのリーガルホールドステータスを表示するには、`s3:GetObjectLegalHold` アクセス許可が必要です。バケットのデフォルトの保持期間を表示するには、`s3:GetBucketObjectLockConfiguration` アクセス許可が必要です。S3 オブジェクトロックが有効になっていないバケットに対してオブジェクトロック設定をリクエストしりｔｐ、Amazon S3 はエラーを返します。

ガバナンスモードのバイパス

`s3:BypassGovernanceRetention` アクセス許可がある場合は、ガバナンスモードでロックされているオブジェクトバージョンに対して、保護されていない場合と同様にオペレーションを実行できます。このようなオペレーションには、オブジェクトバージョンの削除、保持期間の短縮以外にも、空のパラメータを指定した新しい `PutObjectRetention` リクエストの発行によるオブジェクトロック保持期間の解除があります。

ガバナンスモードをバイパスするには、このモードをバイパスするリクエストに明示的に示す必要があります。これを行うには、`PutObjectRetention` API オペレーションリクエストに `x-amz-bypass-governance-retention:true` ヘッダーを含めるか、AWS CLI または AWS SDK を介したリクエストで同等のパラメータを使用します。`s3:BypassGovernanceRetention` アクセス許可がある場合、S3 コンソールは、S3 コンソールを通じて行われたリクエストにこのヘッダーを自動的に適用します。

> **Note**
>
> ガバナンスモードをバイパスしても、オブジェクトバージョンのリーガルホールドステータスには影響しません。オブジェクトバージョンでリーガルホールドが有効になっている場合、リーガルホールドは有効のままで、オブジェクトバージョンの上書きまたは削除のリクエストが避けられます。

S3 レプリケーションでのオブジェクトロックの使用

S3 レプリケーションでオブジェクト ロックを使用すると、S3 バケット間でロックされたオブジェクトとその保持メタデータの自動非同期コピーを有効にすることができます。つまり、レプリケートされたオブジェクトの場合、Amazon S3 はレプリケート元バケットのオブジェクトロック設定を受け取ります。言い換えると、ソースバケットで Object Lock が有効になっている場合は、レプリケート先バケットでも Object Lock が有効になっている必要があります。オブジェクトが (S3 レプリケーションの外部で) レプリケート先バケットに直接アップロードされると、レプリケート先バケットに設定された Object Lock が取得されます。レプリケーションを使用すると、ソースバケット内のオブジェクトは、単一または複数の送信先バケットにレプリケートされます。

オブジェクトロックが有効になっているバケットにレプリケーションを設定するには、S3 コンソール、AWS CLI、Amazon S3 REST API 、または AWS SDK を使用できます。

> **Note**
>
> レプリケーションでオブジェクトロックを使用するには、レプリケーションの設定に使用する AWS Identity and Access Management (IAM) ロールで、ソース S3 バケットに対する 2 つの追加のアクセス許可を付与する必要があります。2 つの新しいアクセス許可とは `s3:GetObjectRetention` と `s3:GetObjectLegalHold` です。ロールに `s3:Get*` アクセス許可がある場合、そのステートメントは要件を満たしています。詳細については、「ライブレプリケーションのアクセス許可の設定」を参照してください。
> S3 レプリケーション全般については、「リージョン内およびリージョン間でのオブジェクトのレプリケート」を参照してください。
> S3 レプリケーションの設定の詳細については、「ライブレプリケーションの設定例」を参照してください。

Object Lock で暗号化を使用する

Amazon S3 は、デフォルトですべての新しいオブジェクトを暗号化します。暗号化されたオブジェクトで Object Lock を使用できます。詳細については、「暗号化によるデータの保護」を参照してください。

Object Lock は、Amazon S3 オブジェクトの削除や上書きを防ぐのに役立ちますが、暗号化キーへのアクセスが失われたり、暗号化キーが削除されたりするのを防ぐことはできません。例えば、AWS KMS サーバー側の暗号化でオブジェクトを暗号化し、AWS KMS キーが削除されると、オブジェクトが読み取り不可能になる可能性があります。

AmazonS3 インベントリでのオブジェクトロックの使用

定義されたスケジュールに従って S3 バケット内のオブジェクトのリストを作成するように Amazon S3 インベントリを設定できます。オブジェクトの次のオブジェクトロック メタデータを含めるように Amazon S3 インベントリを設定できます。

- 保持期日
- 保持モード
- リーガルホールドステータス

詳細については、「S3 インベントリを使用したデータのカタログ化と分析」を参照してください。

Object Lock による S3 ライフサイクルポリシーの管理

オブジェクトライフサイクルの管理設定は、削除マーカーの配置も含めて、保護されたオブジェクトで引き続き正常に機能します。ただし、S3 ライフサイクルの有効期限ポリシーでは、オブジェクトのロックされたバージョンを削除することはできません。Object Lock は、オブジェクトが保存されているストレージクラスに関係なく、またストレージクラス間での S3 ライフサイクル移行全体を通して維持されます。

オブジェクトのライフサイクルの管理の詳細については、「オブジェクトのライフサイクルの管理」を参照してください。

Object Lock による削除マーカーの管理

保護されたオブジェクトバージョンを削除することはできませんが、そのオブジェクトの削除マーカーを作成することはできます。オブジェクトに削除マーカーを配置しても、オブジェクトや、そのオブジェクトバージョンは削除されません。ただし、オブジェクトが削除されたかのように Amazon

S3 をほとんどの方法で動作させます。詳細については、「削除マーカーの使用」を参照してください。

> **Note**
>
> 削除マーカーは、基盤となるオブジェクトでの保持期間またはリーガルホールドに関係なく、WORM 保護されません。

オブジェクトロックでの S3 Storage Lens の使用

オブジェクトロックが有効なストレージバイト数とオブジェクト数のメトリクスを表示するには、Amazon S3 Storage Lens を使用できます。S3 Storage Lens は、オブジェクトストレージの使用状況とアクティビティを組織全体で可視化するために使用できるクラウドストレージ分析機能です。

詳細については、「S3 ストレージレンズによるデータ保護」を参照してください。

メトリクスの一覧については、「Amazon S3 Storage Lens のメトリクスに関する用語集」を参照してください。

Object Lock が有効なバケットへのオブジェクトのアップロード

`Content-MD5` または `x-amz-sdk-checksum-algorithm` ヘッダーは、Object Lock を使用して設定された保持期間のあるオブジェクトをアップロードするすべてのリクエストに必要です。これらのヘッダーは、アップロード中にオブジェクトの整合性を検証するための手段です。

Amazon S3 コンソールでオブジェクトをアップロードすると、S3 は自動的に `Content-MD5` ヘッダーを追加します。オプションで、追加のチェックサム関数とチェックサム値を `x-amz-sdk-checksum-algorithm` ヘッダーとしてコンソールから指定できます。PutObject API を使用する場合は、`Content-MD5` ヘッダー、`x-amz-sdk-checksum-algorithm` ヘッダー、またはその両方を指定して、Object Lock の保持期間を設定する必要があります。

詳細については、「Amazon S3 でのオブジェクトの整合性のチェック」を参照してください。

イベントと通知の設定

Amazon S3 イベント通知を使用して、AWS CloudTrail で、オブジェクトロック設定およびデータへのアクセスと変更を追跡できます。CloudTrail の詳細については、「AWS CloudTrail ユーザーガイド」の「AWS CloudTrail とは」を参照してください。

また、Amazon CloudWatch を使用してこのデータに基づいてアラートを生成することもできます。CloudWatch の詳細については、「Amazon CloudWatch ユーザーガイド」の「Amazon CloudWatch とは」を参照してください。

バケットポリシーを使用する保持期間の制限の設定

バケットポリシーを使用してバケットの最小と最大の許容保持期間を設定できます。最大保存期間は 100 年です。

以下の例は、s3:object-lock-remaining-retention-days 条件キーを使用して最大保持期間を 10 日間に設定するバケットポリシーを示しています。

```
{
    "Version": "2012-10-17",
    "Id": "SetRetentionLimits",
    "Statement": [
        {
            "Sid": "SetRetentionPeriod",
            "Effect": "Deny",
            "Principal": "*",
            "Action": [
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
            "Condition": {
                "NumericGreaterThan": {
                    "s3:object-lock-remaining-retention-days": "10"
                }
            }
        }
    ]
}
```

> **Note**
>
> バケットがレプリケーション設定の送信先バケットである場合は、レプリケーションを使用して作成されるオブジェクトレプリカの最小および最大許容保存期間を設定できます。これを実行するには、バケットポリシーで s3:ReplicateObject アクションを許可する必要があります。レプリケーションのアクセス許可の詳細については、「the section called “アクセス許可のセットアップ”」を参照してください。

バケットポリシーの詳細については、後続のトピックを参照してください。

- 「サービス認可リファレンス」の「Actions, resources, and condition keys for Amazon S3」

  S3 リソースタイプ別の S3 API オペレーションへのアクセス許可の詳細については、「Amazon S3 API オペレーションに必要なアクセス許可」を参照してください。
- オブジェクト操作
- 条件キーを使用したバケットポリシーの例

オブジェクトロックの設定

S3 Object Lockでは、Write-Once-Read-Many (WORM) モデルを使用して Amazon S3 汎用バケットにオブジェクトを保存できます。S3 Object オブジェクトロックを使用して、オブジェクトが固定期間または無期限に削除または上書きされることを防止できます。オブジェクトロック機能全般については、「S3 Object Lock を使用したオブジェクトのロック」を参照してください。

オブジェクトをロックする前に、汎用バケットで S3 バージョニングと Object Lock を有効にする必要があります。その後、保持期間とリーガルホールド、またはその両方を設定できます。

オブジェクトロックを使用するには、特定のアクセス許可が必要です。さまざまなオブジェクトロックオペレーションに関連するアクセス許可のリストについては、「the section called “必要なアクセス許可”」を参照してください。

> **Important**
>
> - オブジェクトロックを有効にしたバケットを作成した後、オブジェクトロックを無効にしたり、バケットのバージョニングを停止することはできません。
> - S3 オブジェクトロックが有効になっている S3 バケットは、サーバーアクセスログの送信先バケットとしては使用できません。詳細については、「the section called “サーバーアクセスのログ記録”」を参照してください。

トピック

- 新しい S3 汎用バケット作成時に Object Lock を有効にする
- 既存の S3 バケットでオブジェクトロックを有効にする
- S3 オブジェクトのリーガルホールドを設定または変更する

- S3 オブジェクトの保持期間を設定または変更する
- S3 バケットのデフォルト保持期間を設定または変更する

新しい S3 汎用バケット作成時に Object Lock を有効にする

Amazon S3 コンソール、AWS Command Line Interface (AWS CLI)、AWS SDK、または Amazon S3 REST API を使用して新しい S3 汎用バケットを作成する際に Object Lock を有効にできます。

S3 コンソールの使用

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 左のナビゲーションペインで、[汎用バケット] を選択します。
3. [Create bucket (バケットの作成)] を選択します。

   [バケットの作成] ページが開きます。
4. [バケット名] にバケットの名前を入力します。

   > **Note**
   >
   > バケット作成後に名前は変更できません。バケットの命名の詳細については、「汎用バケットの命名規則」を参照してください。

5. [リージョン] で、バケットを保存する AWS リージョンを選択します。
6. [オブジェクト所有者] で、アクセスコントロールリスト (ACL) を無効または有効にするかを選択して、バケットにアップロードされたオブジェクトの所有権を制御します。
7. [このバケットのパブリックアクセスブロック設定] で、バケットに適用するブロックパブリックアクセス設定を選択します。
8. [バケットのバージョニング] では、[有効にする] をオンにします。

   オブジェクトロックはバージョニング対応バケットでのみ機能します。
9. (オプション) [Tags] (タグ) では、バケットにタグを追加することを選択できます。タグは、ストレージの分類とコストの割り当てに使用されるキーバリューのペアです。
10. [詳細設定] の下で [オブジェクトロック] を探して、[有効にする] をオンにします。

    オブジェクトロックを有効にすると、このバケット内のオブジェクトは永久にロックされることを認識しておく必要があります。

11. [バケットを作成] を選択します。

AWS CLI の使用

次の `create-bucket` の例では、オブジェクトロックを有効にした *amzn-s3-demo-bucket1* という名前の新しい S3 バケットを作成します。

```
aws s3api create-bucket --bucket amzn-s3-demo-bucket1 --object-lock-enabled-for-bucket
```

詳細と例については、「AWS CLI コマンドリファレンス」の「create-bucket」を参照してください。

> **Note**
>
> AWS CloudShell を使用してコンソールから AWS CLI コマンドを実行できます。AWS CloudShell はブラウザベースの事前認証されたシェルであり、AWS Management Console から直接起動できます。詳細については、「AWS CloudShell User Guide」の「CloudShell とは」を参照してください。

REST API の使用

REST API を使用して、オブジェクトロックを有効にした新しい S3 バケットを作成できます。詳細については、「Amazon Simple Storage Service API リファレンス」の「CreateBucket」を参照してください。

AWS SDK の使用

AWS SDK を使用して新しい S3 バケットを作成するときに Object Lock を有効にする方法の例については、「Amazon S3 API リファレンス」の「コード例」を参照してください。

AWS SDK で現在の Object Lock 設定を取得する方法の例については、「Amazon S3 API リファレンス」の「コード例」を参照してください。

AWS SDK を使用して別の Object Lock 機能のデモンストレーションを行うインタラクティブシナリオについては、「Amazon S3 API リファレンス」の「コード例」を参照してください。

さまざまな AWS SDK の使用に関する一般的な情報については、「Amazon S3 API リファレンス」の「AWS SDK を使用した Amazon S3 での開発」を参照してください。

既存の S3 バケットでオブジェクトロックを有効にする

Amazon S3 コンソール、AWS CLI、AWS SDK、または Amazon S3 REST API を使用して、既存の S3 バケットのオブジェクトロックを有効にできます。

S3 コンソールの使用

> **Note**
>
> オブジェクトロックはバージョニング対応バケットでのみ機能します。

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。
3. [バケット] リストで、サーバーアクセスのログ記録を有効にするバケットの名前を選択します。
4. [プロパティ] タブを選択します。
5. [プロパティ] の下で、[オブジェクトロック] セクションまで下にスクロールして、[編集] をクリックします。
6. [オブジェクトロック] で [有効にする] をオンにします。

   オブジェクトロックを有効にすると、このバケット内のオブジェクトは永久にロックされることを認識しておく必要があります。
7. [Save changes] (変更の保存) をクリックします。

AWS CLI の使用

次の `put-object-lock-configuration` コマンド例は、*amzn-s3-demo-bucket1* という名前のバケットに 50 日間のオブジェクトロック保持期間を設定します。

```
aws s3api put-object-lock-configuration --bucket amzn-s3-demo-bucket1 --object-
lock-configuration='{ "ObjectLockEnabled": "Enabled", "Rule": { "DefaultRetention":
 { "Mode": "COMPLIANCE", "Days": 50 }}}'
```

詳細と例については、「AWS CLI コマンドリファレンス」の「put-object-lock-configuration」を参照してください。

> **Note**
>
> AWS CloudShell を使用してコンソールから AWS CLI コマンドを実行できます。AWS CloudShell はブラウザベースの事前認証されたシェルであり、AWS Management Console から直接起動できます。詳細については、「AWS CloudShell User Guide」の「CloudShell とは」を参照してください。

REST API の使用

Amazon S3 REST API を使用して、既存の S3 バケットのオブジェクトロックを有効にできます。詳細については、「Amazon Simple Storage Service API リファレンス」の「PutObjectLockConfiguration」を参照してください。

AWS SDK の使用

AWS SDK を使用して既存の S3 バケットで Object Lock を有効にする方法の例については、「Amazon S3 API リファレンス」の「コード例」を参照してください。

AWS SDK で現在の Object Lock 設定を取得する方法の例については、「Amazon S3 API リファレンス」の「コード例」を参照してください。

AWS SDK を使用して別の Object Lock 機能のデモンストレーションを行うインタラクティブシナリオについては、「Amazon S3 API リファレンス」の「コード例」を参照してください。

さまざまな AWS SDK の使用に関する一般的な情報については、「Amazon S3 API リファレンス」の「AWS SDK を使用した Amazon S3 での開発」を参照してください。

S3 オブジェクトのリーガルホールドを設定または変更する

Amazon S3 コンソール、AWS CLI、AWS SDK、または Amazon S3 REST API を使用して、S3 バケットのオブジェクトロックを設定したり、解除できます。

> **Important**
>
> - オブジェクトにリーガルホールドを設定する場合は、オブジェクトのバケットでオブジェクトロックがすでに有効になっている必要があります。

- 個別の保存モードと期間が明示的に設定されているオブジェクトバージョンをバケット内に PUT すると、オブジェクトバージョンの個々のオブジェクトロック設定が、バケットプロパティの保存設定よりも優先されます。

詳細については、「the section called “リーガルホールド”」を参照してください。

S3 コンソールの使用

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。
3. [バケット] リストで、リーガルホールドを設定したり変更したりするオブジェクトがあるバケットの名前を選択します。
4. [オブジェクト] リストで、リーガルホールドを設定したり変更したりするオブジェクトを選択します。
5. [オブジェクトプロパティ] ページで、[オブジェクトロックのリーガルホールド] セクションを探して、[編集] をクリックします。
6. [有効にする] をオンにしてリーガルホールドを設定するか、[無効にする] をオンにしてリーガルホールドを解除します。
7. [Save changes] (変更の保存) をクリックします。

AWS CLI の使用

次の put-object-legal-hold 例では、*amzn-s3-demo-bucket1* という名前のバケットのオブジェクト *my-image.fs* にリーガルホールドを設定します。

```
aws s3api put-object-legal-hold --bucket amzn-s3-demo-bucket1 --key my-image.fs --
legal-hold="Status=ON"
```

次の put-object-legal-hold 例では、*amzn-s3-demo-bucket1* という名前のバケットのオブジェクト *my-image.fs* のリーガルホールドを解除します。

```
aws s3api put-object-legal-hold --bucket amzn-s3-demo-bucket1 --key my-image.fs --
legal-hold="Status=OFF"
```

詳細と例については、「AWS CLI コマンドリファレンス」の「put-object-legal-hold」を参照してください。

> **Note**
>
> AWS CloudShell を使用してコンソールから AWS CLI コマンドを実行できます。AWS CloudShell はブラウザベースの事前認証されたシェルであり、AWS Management Console から直接起動できます。詳細については、「AWS CloudShell User Guide」の「CloudShell とは」を参照してください。

REST API の使用

REST API を使用して、オブジェクトのリーガルホールドを設定または変更できます。詳細については、「Amazon Simple Storage Service API リファレンス」の「PutObjectLegalHold」を参照してください。

AWS SDK の使用

AWS SDK を使用してオブジェクトにリーガルホールドを設定する方法の例については、「Amazon S3 API リファレンス」の「コードの例」を参照してください。

AWS SDK を使用して現在のリーガスホールドのステータスを取得する方法の例については、「Amazon S3 API リファレンス」の「コードの例」を参照してください。

AWS SDK を使用して別の Object Lock 機能のデモンストレーションを行うインタラクティブシナリオについては、「Amazon S3 API リファレンス」の「コード例」を参照してください。

さまざまな AWS SDK の使用に関する一般的な情報については、「Amazon S3 API リファレンス」の「AWS SDK を使用した Amazon S3 での開発」を参照してください。

S3 オブジェクトの保持期間を設定または変更する

Amazon S3 コンソール、AWS CLI、AWS SDK、または Amazon S3 REST API を使用して、S3 バケットの保持期間を設定したり変更したりできます。

> **Important**
>
> - オブジェクトに保持期間を設定する場合は、オブジェクトのバケットでオブジェクトロックがすでに有効になっている必要があります。

- 個別の保存モードと期間が明示的に設定されているオブジェクトバージョンをバケット内に PUT すると、オブジェクトバージョンの個々のオブジェクトロック設定が、バケットプロパティの保存設定よりも優先されます。
- 保持期限が切れる前にコンプライアンスモードのオブジェクトを削除する唯一の方法は、関連する AWS アカウント を削除することです。

詳細については、「保持期間」を参照してください。

S3 コンソールの使用

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。
3. [バケット] リストで、保持期間を設定したり変更したりするオブジェクトがあるバケットの名前を選択します。
4. [オブジェクト] リストで、保持期間を設定したり変更したりするオブジェクトを選択します。
5. [オブジェクトプロパティ] ページで、[オブジェクトロックの保持] セクションを探して、[編集] をクリックします。
6. [保持] の下で、[有効にする] をオンにして保持期間を設定したり、[無効にする] をオンにして保持期間を解除したりします。
7. [有効にする] をオンにする場合は、[保持モード] で [ガバナンスモード] または [コンプライアンスモード] のいずれかを選択します。詳細については、「リテンションモード」を参照してください。
8. [保持期間] の下で、保持期間を終了する日付を選択します。この間、オブジェクトは WORM で保護され、上書きまたは削除することはできません。詳細については、「保持期間」を参照してください。
9. [Save changes] (変更の保存) をクリックします。

AWS CLI の使用

次の `put-object-retention` 例では、*`amzn-s3-demo-bucket1`* という名前のバケットのオブジェクト *`my-image.fs`* に保持期間を設定します。

```
aws s3api put-object-retention --bucket amzn-s3-demo-bucket1 --key my-image.fs --
retention='{ "Mode": "GOVERNANCE", "RetainUntilDate": "2025-01-01T00:00:00" }'
```

詳細と例については、「AWS CLI コマンドリファレンス」の「put-object-retention」を参照してください。

> **Note**
>
> AWS CloudShell を使用してコンソールから AWS CLI コマンドを実行できます。AWS CloudShell はブラウザベースの事前認証されたシェルであり、AWS Management Console から直接起動できます。詳細については、「AWS CloudShell User Guide」の「CloudShell とは」を参照してください。

REST API の使用

REST API を使用して、オブジェクトの保持期間を設定または変更できます。詳細については、「Amazon Simple Storage Service API リファレンス」の「PutObjectRetention」を参照してください。

AWS SDK の使用

AWS SDK を使用してオブジェクトに保持期間を設定する方法の例については、「Amazon S3 API リファレンス」の「コードの例」を参照してください。

AWS SDK を使用してオブジェクトの保持期間を取得する方法の例については、「Amazon S3 API リファレンス」の「コードの例」を参照してください。

AWS SDK を使用して別の Object Lock 機能のデモンストレーションを行うインタラクティブシナリオについては、「Amazon S3 API リファレンス」の「コード例」を参照してください。

さまざまな AWS SDK の使用に関する一般的な情報については、「Amazon S3 API リファレンス」の「AWS SDK を使用した Amazon S3 での開発」を参照してください。

S3 バケットのデフォルト保持期間を設定または変更する

Amazon S3 コンソール、AWS CLI、AWS SDK、または Amazon S3 REST API を使用して、S3 バケットのデフォルトの保持期間を設定したり変更したりできます。バケットに配置されたすべてのオブジェクトのバージョンを保護する期間を日または年で指定します。

> **Important**
>
> - バケットのデフォルトの保持期間を設定する場合は、バケットでオブジェクトロックがすでに有効になっている必要があります。
> - 個別の保存モードと期間が明示的に設定されているオブジェクトバージョンをバケット内に PUT すると、オブジェクトバージョンの個々のオブジェクトロック設定が、バケットプロパティの保存設定よりも優先されます。
> - 保持期限が切れる前にコンプライアンスモードのオブジェクトを削除する唯一の方法は、関連する AWS アカウント を削除することです。

詳細については、「保持期間」を参照してください。

S3 コンソールの使用

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。
3. [バケット] リストで、デフォルトの保持期間を設定したり変更したりするバケットの名前を選択します。
4. [プロパティ] タブを選択します。
5. [プロパティ] の下で、[オブジェクトロック] セクションまで下にスクロールして、[編集] をクリックします。
6. [保持] の下で、[有効にする] をオンにしてデフォルトの保持期間を設定したり、[無効にする] をオンにしてデフォルトの保持期間を解除したりします。
7. [有効にする] をオンにする場合は、[保持モード] で [ガバナンスモード] または [コンプライアンスモード] のいずれかを選択します。詳細については、「リテンションモード」を参照してください。
8. [デフォルトの保存期間] で、保存期間を有効にする日数または年数を選択します。このバケットに保存されるオブジェクトは、指定した日数または年数の間ロックされます。詳細については、「保持期間」を参照してください。
9. [Save changes] (変更の保存) をクリックします。

AWS CLI の使用

次の put-object-lock-configuration コマンド例は、*amzn-s3-demo-bucket1* という名前のバケットにコンプライアンスモードを使用して 50 日間のオブジェクトロック保持期間を設定します。

```
aws s3api put-object-lock-configuration --bucket amzn-s3-demo-bucket1 --object-
lock-configuration='{ "ObjectLockEnabled": "Enabled", "Rule": { "DefaultRetention":
 { "Mode": "COMPLIANCE", "Days": 50 }}}'
```

次の put-object-lock-configuration 例では、バケットのデフォルトの保持設定を解除します。

```
aws s3api put-object-lock-configuration --bucket amzn-s3-demo-bucket1 --object-lock-
configuration='{ "ObjectLockEnabled": "Enabled"}'
```

詳細と例については、「AWS CLI コマンドリファレンス」の「put-object-lock-configuration」を参照してください。

> **Note**
>
> AWS CloudShell を使用してコンソールから AWS CLI コマンドを実行できます。AWS CloudShell はブラウザベースの事前認証されたシェルであり、AWS Management Console から直接起動できます。詳細については、「AWS CloudShell User Guide」の「CloudShell とは」を参照してください。

REST API の使用

REST API を使用して既存の S3 バケットにデフォルトの保持期間を設定できます。詳細については、「Amazon Simple Storage Service API リファレンス」の「PutObjectLockConfiguration」を参照してください。

AWS SDK の使用

AWS SDK を使用して既存の S3 バケットにデフォルトの保持期間を設定する方法の例については、「Amazon S3 API リファレンス」の「コードの例」を参照してください。

AWS SDK を使用して別の Object Lock 機能のデモンストレーションを行うインタラクティブシナリオについては、「Amazon S3 API リファレンス」の「コード例」を参照してください。

さまざまな AWS SDK の使用に関する一般的な情報については、「Amazon S3 API リファレンス」の「AWS SDK を使用した Amazon S3 での開発」を参照してください。

Amazon S3 データのバックアップ

Amazon S3 は、AWS Backup とネイティブに統合されたフルマネージド型のポリシーベースのサービスであるため、バックアップポリシーを一元的に定義して、Amazon S3 内のデータを保護できます。バックアップポリシーを定義し、Amazon S3 リソースをポリシーに割り当てると、AWS Backup は Amazon S3 バックアップの作成を自動化し、バックアッププランで指定した暗号化されたバックアップボールトにバックアップを安全に保存します。

AWS Backup を Amazon S3 に使用すると、以下のアクションを実行できます。

- 継続的なバックアップと定期的なバックアップを作成します。継続的なバックアップは、特定の時点への復元の場合に便利であり、 および定期的なバックアップは、長期的なデータ-保持のニーズを満たすのに便利です。
- バックアップポリシーを一元的に構成して、バックアップのスケジュールと保存を自動化します。
- Amazon S3 データのバックアップを、指定した特定の時点に復元します。

AWS Backup と同様に、S3 バージョニングと S3 レプリケーションを使用して、偶発的な削除から回復し、独自のセルフリカバリーオペレーションを実行できます。

前提条件

AWS Backup がバケットをバックアップするには、その前に、バケットの S3 バージョニングを有効にする必要があります。

> **Note**
>
> バックアップするバージョニングが有効なバケットのライフサイクルの有効期限ルールを設定することをお勧めします。ライフサイクルの有効期限を設定しなかった場合、AWS Backup は Amazon S3 データのすべてのバージョンを保持するため、Amazon S3 のストレージコストが増加する可能性があります。

使用開始

Amazon S3 で AWS Backup の使用を開始するには、「AWS Backup デベロッパーガイド」の「Amazon S3 バックアップの作成」を参照してください。

制約と制限

制限について学ぶには、「AWS Backup デベロッパーガイド」の「Amazon S3 バックアップの作成」を参照してください。

コスト最適化

Amazon S3 には、データライフサイクル全体でコストを最適化するのに役立つさまざまな機能とストレージクラスが用意されています。ストレージクラスは、前払い料金やコンテンツの保存量に対するコミットメントなしで、対応するコストで異なるデータアクセスレベルを提供し、コストを管理する柔軟性を提供します。他の AWS のサービスと同様、従量制料金でのお支払いとなります。

Amazon S3 ストレージクラスは、さまざまなアクセスパターンに対して最も低コストのストレージを提供するように特別に設計されています。具体的には次のとおりです。

- S3 Standard は頻繁にアクセスされるデータ用の汎用ストレージ。
- Amazon S3 Express One Zone は、単一のアベイラビリティーゾーンで頻繁にアクセスされる高性能データ用。
- S3 Intelligent-Tiering は、アクセスパターンが不明または変化するデータのストレージコストを自動的に最適化。
- S3 Standard-IA (S3 Standard-IA) と S3 One Zone-IA (S3 One Zone-IA) は、長期間保存されるがアクセス頻度の低いデータ用。
- S3 Glacier Instant Retrieval は、即時アクセスを必要とするアーカイブデータ用。
- S3 Glacier は、即時アクセスは必要ないが、大量のデータセットを無料で取得できる柔軟性が必要なアーカイブデータ用。
- S3 Glacier Deep Archive は、クラウドで最も低いストレージコストで長期アーカイブとデジタル保存を実現。

オブジェクトは、最もコスト効率の高いストレージクラスにいつでも移動できます。さらに、Amazon S3 にはデータライフサイクルを管理する機能が用意されています。例えば、S3 ライフサイクル設定を使用して、オブジェクトをより費用対効果の高いストレージクラスへの移行を自動化したり、定義したルールに基づいて期限切れのオブジェクトを自動的に削除したりできます。

S3 ストレージクラス分析、コスト配分タグ付け、請求と使用状況レポートなどの機能は、コストと使用状況パターンの分析に役立ちます。

トピック

- Amazon S3 の請求および使用状況レポート
- Amazon S3 ストレージクラスの理解と管理
- オブジェクトのライフサイクルの管理

Amazon S3 の請求および使用状況レポート

Amazon S3 を使用する場合、前払い金を支払ったり、コンテンツの保存量をコミットしたりする必要はありません。他の AWS のサービス と同様、使用したときに使用した分のみのお支払いとなります。

AWS では、Amazon S3 について次のレポートを提供します。

- 請求レポート – Amazon S3 を含む、使用している AWS のサービス のすべてのアクティビティの概要ビューを提供する複数のレポート。AWS は、バケットがリクエスタ支払いバケットとして作成された場合を除き、常に S3 バケットの所有者に Amazon S3 料金を請求します。リクエスタ支払いの詳細については、「ストレージの転送と使用にリクエスタ支払い汎用バケットを使用する」を参照してください。請求レポートの詳細については、「Amazon S3 の AWS Billing レポート」を参照してください。
- 使用状況レポート – 特定のサービスのアクティビティを時間、日、または月単位で集計した概要。含める使用タイプ、オペレーションを選択できます。また、データの収集方法も選択できます。詳細については、「Amazon S3 の AWS 使用状況レポート」を参照してください。

以下のトピックでは、Amazon S3 の請求と使用状況レポートについての情報を説明しています。

トピック

- S3 バケットタグでのコスト配分タグの使用
- Amazon S3 の AWS Billing レポート
- Amazon S3 の AWS 使用状況レポート
- Amazon S3 の AWS 請求および使用状況レポートを理解する
- Amazon S3 のエラーレスポンスに対する請求

S3 バケットタグでのコスト配分タグの使用

個々のプロジェクトまたはプロジェクトのグループのストレージコストや他の基準を追跡するには、コスト配分タグを使用して Amazon S3 バケットにラベルを付けます。コスト割り当てタグはキーと値のペアで、ユーザーが S3 バケットに関連付けます。コスト配分タグを有効にすると、AWS はコスト配分レポートでリソースのコストの整理にタグを使用します。コスト割り当てタグは、バケットにラベルを付けるためだけに使用できます。オブジェクトにラベルを付けるために使用されるタグについては、「タグを使用してストレージを分類する」を参照してください。

コスト配分レポートには、アカウントの AWS 使用状況が製品カテゴリ別およびリンクされたアカウントユーザー別に表示されます。レポートには、同じ明細項目が詳細な請求レポートとして含まれ(「Amazon S3 の AWS 請求および使用状況レポートを理解する」を参照)、タグキーは追加列に含まれます。

AWS には、AWS が生成するタグとユーザー定義タグの 2 種類のコスト配分タグが用意されています。AWS は、Amazon S3 の CreateBucket イベントの後に、AWS が生成する `createdBy` タグを定義、作成、適用します。ユーザーは S3 バケットのユーザー定義タグを、定義、作成、適用します。

請求レポートに表示するには、請求およびコスト管理コンソールで両方の種類のタグを個別に有効化する必要があります。AWS が生成するタグの詳細については、「AWS 生成コスト配分タグ」を参照してください。

- コンソールでタグを作成するときは、「S3 汎用バケットのプロパティの表示」を参照してください。
- Amazon S3 API を使用してタグを作成するには、Amazon Simple Storage Service API リファレンスの「PUT バケットタグ付け」を参照してください。
- AWS CLI を使用してタグを作成するには、AWS CLI コマンドリファレンスの「put-bucket-tagging」を参照してください。
- タグの有効化の詳細については、AWS Billing ユーザーガイドのコスト配分タグの使用を参照してください。

ユーザー定義のコスト配分タグ

ユーザー定義コスト配分タグには以下のコンポーネントがあります。

- タグキー。タグキーは、タグ名です。たとえば、project/Trinity タグでは project がキーです。タグキーは大文字小文字を区別する文字列で、1 ~ 128 個の Unicode 文字を含めることができます。

- タグ値。タグ値は必須文字列です。たとえば、project/Trinity タグでは Trinity が値です。タグ値は大文字小文字を区別する文字列で、0 ~ 256 個の Unicode 文字を含めることができます。

ユーザー定義タグで使用できる文字や他の制限の詳細については、AWS Billing ユーザーガイドのユーザー定義タグの制限を参照してください。ユーザー定義タグの詳細については、AWS Billing ユーザーガイドのユーザー定義のコスト配分タグを参照してください。

S3 バケットのタグ

各 S3 バケットはタグセットがあります。タグセットには、そのバケットに割り当てられているすべてのタグが含まれています。タグセットには最大 50 個のタグを含めることができ、空にすることもできます。キーはタグセット内で一意にする必要がありますが、タグセット内の値は一意である必要はありません。たとえば、同じ値を持つタグ project/Trinity と cost-center/Trinity を、同じタグセット内に持つことができます。

既存のタグと同じキーを持つタグをバケットに追加した場合、古い値は新しい値によって上書きされます。

AWS はタグに意味論的意味を適用しません。単なる文字列としてタグを解釈します。

タグを追加、一覧表示、編集、削除するには、Amazon S3 コンソール、AWS Command Line Interface (AWS CLI)、または Amazon S3 API を使用します。

詳細

- AWS Billing ユーザーガイドの「コスト配分タグの使用」
- Amazon S3 の AWS 請求および使用状況レポートを理解する
- Amazon S3 の AWS Billing レポート

Amazon S3 の AWS Billing レポート

AWS からの毎月の請求書では、使用状況の情報とコストが AWS のサービス と機能ごとに分けられています。月別レポート、コスト割り当てレポート、詳細な請求レポートなど、利用できる複数の AWS Billing レポートがあります。請求レポートを表示する方法については、AWS Billing ユーザーガイドの「請求の表示」を参照してください。

AWS の使用状況を追跡し、アカウントに関連する推定請求額を示すよう AWS Cost and Usage Reports をセットアップできます。詳細については、「AWS Data Exports ガイド」の「AWSCost and Usage Reports とは」を参照してください。

Amazon S3 ストレージ使用状況に関する、請求レポートよりもさらに詳細な使用状況レポートをダウンロードできます。詳細については、「Amazon S3 の AWS 使用状況レポート」を参照してください。

次の表は、Amazon S3 の使用に関連する料金をまとめたものです。

料金	コメント
ストレージ	S3 バケットにオブジェクトを保存すると料金が発生します。請求される料金は、オブジェクトのサイズ、その月の間のオブジェクトの保存期間、およびそれらのストレージクラスによって異なります。Amazon S3 には、S3 Standard、S3 Express One Zone、S3 Intelligent-Tiering、S3 Standard-IA (IA は少頻度アクセスを意味します)、S3 One Zone-IA、S3 Glacier Instant Retrieval、S3 Glacier Flexible Retrieval、S3 Glacier Deep Archive、または 低冗長化ストレージ (RRS) のストレージクラスが用意されています。ストレージクラスの詳細については、「Amazon S3 ストレージクラスの理解と管理」を参照してください。 S3 バージョニングが有効になっている場合、保持されているオブジェクトのバージョンごとに課金されることに注意してください。バージョニングの詳細については、「S3 バージョニングの仕組み」を参照してください。
汎用バケット	アカウントで作成した最初の 2,000 個の汎用バケットには請求が発生しません。ただし、最初の 2,000 個を超えて作成した各バケットにはバケット単位の料金がかかります。この料金はバケット/月ごとに請求されます。汎用バケットの料金については、「Amazon S3の料金」を参照してください。
モニタリングと自動化	アクセスパターンをモニタリングし、S3 Intelligent-Tiering のアクセス層間でオブジェクトを移動するには、S3 Intelligent-Tiering ストレージクラスに保管されているオブジェクトごとにモニタリングとオートメーションの月額料金をお支払いいただきます。

料金	コメント
リクエスト	また、S3 バケットやオブジェクトに対して行われた GET リクエストなど、リクエストに対しても料金が発生します。これには、ライフサイクル リクエストが含まれます。リクエストのレートは、リクエストの種類によって異なります。リクエストの料金の詳細については、「Amazon S3 の料金」を参照してください。
取得	S3 標準 – IA、S3 1 ゾーン – IA、S3 Glacier Instant Retrieval、S3 Glacier Flexible Retrieval、およびS3 Glacier Deep Archiveストレージに保存されているオブジェクトを取り出す時に料金が発生します。
早期削除	最小ストレージコミットメントを満たす前に S3 標準 – IA、S3 1 ゾーン – IA、S3 Glacier Flexible Retrieval、または S3 Glacier Deep Archive storage に保存されたオブジェクトを削除する場合、そのオブジェクトの早期削除料金が発生します。
ストレージ管理	アカウントのバケットで有効になっているストレージ管理機能 (Amazon S3 インベントリ、分析、オブジェクトのタグ付け) に対してお支払いいただきます。

料金	コメント
[帯域幅]	次の場合を除き、Amazon S3 に出入りするすべての帯域幅に対してお支払いいただきます。 • インターネットからのデータ転送 • インスタンスが S3 バケットと同じ AWS リージョン にある場合、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスに転送されたデータ。 • Amazon CloudFront (CloudFront) に転送されたデータ。 また、Amazon S3 Transfer Acceleration を使用して転送されたデータに対しても料金をお支払いいただきます。

Amazon S3 のストレージ、データ転送、サービスの利用料金の詳細は、「Amazon S3 の料金」および「Amazon S3 のよくある質問」を参照してください。

Amazon S3 の請求および使用状況レポートで使用されるコードと略語については、「Amazon S3 の AWS 請求および使用状況レポートを理解する」を参照してください。

詳細情報

- Amazon S3 の AWS 使用状況レポート
- S3 バケットタグでのコスト配分タグの使用
- AWS Billing とコスト管理
- Amazon S3 の料金

Amazon S3 の AWS 使用状況レポート

使用状況レポートをダウンロードする際、使用状況を時間、日、または月単位で集計できます。Amazon S3 使用状況レポートでは、使用タイプおよび AWS リージョン 別にオペレーションが

一覧表示されます。Amazon S3 ストレージの使用状況の詳細なレポートについては、動的に生成された AWS の使用状況レポートをダウンロードしてください。含める使用タイプ、オペレーション、期間を選択できます。また、データの収集方法も選択できます。使用状況レポートの詳細については、「AWS Data Exports ユーザーガイド」の「AWS 使用状況レポート」を参照してください。

Amazon S3 使用状況レポートには次の情報が含まれます。

- サービス – Amazon S3
- オペレーション – バケットまたはオブジェクトに対して実行されたオペレーション。Amazon S3 オペレーションの詳細な説明については、「使用状況レポートの追跡オペレーション」を参照してください。
- 使用状況 – 以下の値のいずれかです。
  - ストレージのタイプを識別するコード
  - リクエストのタイプを識別するコード
  - 取得のタイプを識別するコード
  - データ転送のタイプを識別するコード
  - S3 Intelligent-Tiering、S3 標準 – IA、S3 1 ゾーン低頻度アクセス (S3 1 ゾーン – IA)、S3 One Zone-Infrequent Access (S3 One Zone-IA)、S3 Glacier Flexible Retrieval、または S3 Glacier Deep Archive ストレージからの早期削除を識別するコード
  - `StorageObjectCount` – 特定のバケット内に保存されたオブジェクトの数

  Amazon S3 使用タイプの詳細な説明については、「Amazon S3 の AWS 請求および使用状況レポートを理解する」を参照してください。
- Resource – リストされた使用状況に関連付けられたバケットの名前。
- StartTime – 使用状況が適用される協定世界時 (UTC) による日付の開始時間。
- EndTime – 使用状況が適用がされる協定世界時 (UTC) による日付の終了時間。
- UsageValue – 以下のボリューム値のいずれかです。データの典型的な測定単位はギガバイト (GB) です。ただし、サービスとレポートによっては、テラバイト (TB) が代わりに表示されることがあります。
  - 指定した期間のリクエストの数
  - データ転送量
  - 指定された時間内に格納されたデータの量
  - S3 標準 – IA、または S3 1 ゾーン – IA、S3 Glacier Flexible Retrieval、または S3 Glacier Deep Archive ストレージからの復元に関連付けられたデータの量 (バイト単位)

> **Tip**
>
> オブジェクトに関して Amazon S3 が受信するすべてのリクエストに関する詳細な情報は、バケットのサーバーアクセスログ記録をオンにすると取得できます。詳細については、「サーバーアクセスログによるリクエストのログ記録」を参照してください。

使用状況レポートは、XML またはコンマ区切り値 (CSV) ファイルでダウンロードできます。スプレッドシートアプリケーションで開いた CSV 使用状況レポートの例を次に示します。

Service	Operation	UsageType	Resource	StartTime	EndTime	UsageValue
AmazonS3	HeadBucket	USW2-C3DataTransfer-Out-Bytes	admin-created3	6/1/2017 0:00	7/1/2017 0:00	15309
AmazonS3	PutObject	USW2-C3DataTransfer-In-Bytes	admin-created3	6/1/2017 0:00	7/1/2017 0:00	19062
AmazonS3	HeadBucket	USW2-Requests-Tier2	admin-created3	6/1/2017 0:00	7/1/2017 0:00	68
AmazonS3	PutObjectForRepl	USW1-Requests-SIA-Tier1	ca-example-bucket	6/1/2017 0:00	7/1/2017 0:00	178294
AmazonS3	PutObjectForRepl	USW1-USW2-AWS-In-Bytes	ca-example-bucket	6/1/2017 0:00	7/1/2017 0:00	387929083
AmazonS3	GetObjectForRepl	USW2-Requests-NoCharge	admin-created3	6/1/2017 0:00	7/1/2017 0:00	108
AmazonS3	GetObjectForRepl	USW2-USW1-AWS-Out-Bytes	my-test-bucket-bash	6/1/2017 0:00	7/1/2017 0:00	387910021

詳細については、「Amazon S3 の AWS 請求および使用状況レポートを理解する」を参照してください。

AWS 使用状況レポートのダウンロード

使用状況レポートは XML または CSV ファイルでダウンロードできます。

使用状況レポートのダウンロード

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. タイトルバーで、ユーザー名またはアカウント ID を選択し、[請求とコスト管理] を選択します。
3. ナビゲーションペインで、[レガシーページ] を選択し、[コストと使用状況レポート] を選択します。
4. [AWS 使用状況レポート] で、[使用状況レポートの作成] を選択します。
5. [使用状況レポートのダウンロード] ページで、次の設定を選択します。
   - [サービス] – [Amazon Simple Storage Service] を選択します。
   - [Usage Types] (使用タイプ) – Amazon S3 の使用タイプの詳細については、Amazon S3 の AWS 請求および使用状況レポートを理解する を参照してください。

- [Operation] (オペレーション) – Amazon S3 オペレーションの詳細については、使用状況レポートの追跡オペレーション を参照してください。
- [Time Period] (期間) – レポートの対象とする期間。
- [Report Granularity (レポートの詳細度)] – 時間、日、月単位の小計をレポートに含めるかどうか。

6. [ダウンロード] を選択し、ダウンロード形式 (XML レポートまたは CSV レポート) を選択し、プロンプトに従ってレポートを開くか保存します。

詳細情報

- Amazon S3 の AWS 請求および使用状況レポートを理解する
- Amazon S3 の AWS Billing レポート

Amazon S3 の AWS 請求および使用状況レポートを理解する

Amazon S3 請求および使用状況レポートではコードと略名を使用します。次に示す表の使用法タイプでは、*region*、*region1*、*region2* をこのリストの略語に置き換えます。

- APE1: アジアパシフィック (香港)
- APN1: アジアパシフィック (東京)
- APN2: アジアパシフィック (ソウル)
- APN3: アジアパシフィック (大阪)
- APS1: アジアパシフィック (シンガポール)
- APS2: アジアパシフィック (シドニー)
- APS3: アジアパシフィック (ムンバイ)
- APS4: アジアパシフィック (ジャカルタ)
- APS5: アジアパシフィック (ハイデラバード)
- APS6: アジアパシフィック (メルボルン)
- APS7: アジアパシフィック (マレーシア)
- APS9: アジアパシフィック (タイ)
- CAN1: カナダ (中部)
- CAN2: カナダ西部 (カルガリー)

- CNN1: 中国 (北京)
- CNW1: 中国 (寧夏)
- AFS1: アフリカ (ケープタウン)
- EUC2: 欧州 (チューリッヒ)
- EUN1: 欧州 (ストックホルム)
- EUS2: 欧州 (スペイン)
- EUC1: 欧州 (フランクフルト)
- EU: 欧州 (アイルランド)
- EUS1: 欧州 (ミラノ)
- EUW2: 欧州 (ロンドン)
- EUW3: 欧州 (パリ)
- ILC1: イスラエル (テルアビブ)
- MEC1: 中東 (アラブ首長国連邦)
- MES1: 中東 (バーレーン)
- MXC1: メキシコ (中部)
- SAE1: 南米 (サンパウロ)
- UGW1: AWS GovCloud (米国西部)
- UGE1: AWS GovCloud (米国東部)
- USE1 (またはプレフィックスなし): 米国東部 (バージニア北部)
- USE2: 米国東部 (オハイオ)
- USW1: 米国西部 (北カリフォルニア)
- USW2: 米国西部 (オレゴン)

次の表に示す S3 のマルチリージョンアクセスポイントの使用法タイプでは、*regiongroup1* と *regiongroup2* をこのリストの略語に置き換えます。

- AP: アジア太平洋
- AU: オーストラリア
- EU: ヨーロッパ
- IN: インド
- NA: 北米

- SA: 南米

リージョングループは、複数の AWS リージョン を地理的にグループ化したものです。詳細については、「リージョンとアベイラビリティーゾーン」を参照してください。AWS リージョン 別の料金については、「Amazon S3 の料金」を参照してください。

次の表の 1 列目は、請求および使用状況レポートに記載される使用タイプです。データの典型的な測定単位はギガバイト (GB) です。ただし、サービスとレポートによっては、テラバイト (TB) が代わりに表示されることがあります。

使用タイプ	単位	詳細度	説明
region1-*region2*-AWS-In-ABytes	GB	毎時	*region2* から *region1* に転送される高速データ量
region1-*region2*-AWS-In-ABytes-T1	GB	毎時	*region2* から *region1* に転送される T1 高速データの量。T1 は、米国、欧州、および日本の Point of Presence (POPs) への CloudFront リクエストを指します。
region1-*region2*-AWS-In-ABytes-T2	GB	毎時	*region2* から *region1* に転送される T2 高速データの量。T2 は、その他すべての AWS エッジロケーションにある POPs への CloudFront リクエストを指します。
region1-*region2*-AWS-In-Bytes	GB	毎時	*region2* から *region1* に転送されるデータ量
region1-*region2*-AWS-Out-ABytes	GB	毎時	*region1* から *region2* に転送される高速データ量

使用タイプ	単位	詳細度	説明
region1-*region2*-AWS-Out-ABytes-T1	GB	毎時	*region1* から *region2* に転送される T1 高速データの量。T1 は、米国、欧州、および日本の POP への CloudFront リクエストを指します。
region1-*region2*-AWS-Out-ABytes-T2	GB	毎時	*region1* から *region2* に転送される T2 高速データの量。T2 は、その他すべての AWS エッジロケーションにある POP への CloudFront リクエストを指します。
region1-*region2*-AWS-Out-Bytes	GB	毎時	*region1* から *region2* に転送されるデータ量
region-BatchOperations-Jobs	カウント	時間単価	実行された S3 バッチオペレーションジョブの数
region-BatchOperations-Objects	カウント	時間単価	S3 バッチオペレーションによって実行されたオブジェクトオペレーションの数
region-Bulk-Retrieval-Bytes	GB	毎時	Bulk S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive リクエストで取得したデータの量

使用タイプ	単位	詳細度	説明
region-BytesDeleted-GDA	GB	月別	DeleteObject オペレーションによって S3 Glacier Deep Archive ストレージから削除されたデータの量
region-BytesDeleted-GIR	GB	月別	DeleteObject オペレーションによって S3 Glacier Instant Retrieval ストレージから削除されたデータの量。
region-BytesDeleted-GLACIER	GB	月別	DeleteObject オペレーションによって S3 Glacier Flexible Retrieval ストレージから削除されたデータの量
region-BytesDeleted-INT	GB	月別	DeleteObject オペレーションによって S3 Intelligent-Tiering ストレージから削除されたデータの量
region-BytesDeleted-RRS	GB	月別	DeleteObject オペレーションによって低冗長化ストレージ (RRS) から削除されたデータの量
region-BytesDeleted-SIA	GB	月別	DeleteObject オペレーションによって S3 Standard-IA ストレージから削除されたデータの量

使用タイプ	単位	詳細度	説明
region-BytesDeleted-STANDARD	GB	月別	DeleteObject オペレーションによって S3 Standard ストレージから削除されたデータの量
region-BytesDeleted-ZIA	GB	月別	DeleteObject オペレーションによって S3 One Zone-IA ストレージから削除されたデータの量
region-C3DataTransfer-In-Bytes	GB	時間単価	同じ AWS リージョン内で Amazon EC2 から Amazon S3 に転送されたデータの量
region-C3DataTransfer-Out-Bytes	GB	時間単価	同じ AWS リージョン内の Amazon S3 から Amazon EC2 に転送されるデータの量
region-CloudFront-In-Bytes	GB	時間単価	CloudFront ディストリビューションから AWS リージョン に転送されたデータの量
region-CloudFront-Out-Bytes	GB	時間単価	AWS リージョン から CloudFront ディストリビューションに転送されたデータ量
region-DataTransfer-In-Bytes	GB	時間単価	インターネットから Amazon S3 に転送されたデータの量

使用タイプ	単位	詳細度	説明
region-DataTransfer-Out-Bytes	GB	時間単価	Amazon S3 からインターネット[1] に転送されたデータ量
region-DataTransfer-Regional-Bytes	GB	時間単価	同じ AWS リージョン 内で Amazon S3 から AWS リソースに転送されたデータの量
region-EarlyDelete-ByteHrs	GB-時間	毎時	90 日間の最低コミットメントが終了する前に、S3 Glacier Flexible Retrieval ストレージから削除されたオブジェクトの、比例配分されたストレージの使用量 [2]
region-EarlyDelete-GDA	GB-時間	時間単価	180 日間の最低コミットメントが終了する前に S3 Glacier Deep Archive ストレージから削除されたオブジェクトの、按分計算されたストレージの使用量2
region-EarlyDelete-GIR	GB-時間	毎時	90 日間の最低コミットメントが終了する前に、S3 Glacier Instant Retrieval から削除されたオブジェクトの比例配分されたストレージの使用量。

使用タイプ	単位	詳細度	説明
region-EarlyDelete-GIR-SmObjects	GB-時間	毎時	90 日間の最低コミットメントが終了する前に S3 Glacier Instant Retrieval から削除された小さなオブジェクト (128 KB未満) の比例配分されたストレージ使用量。
region-EarlyDelete-SIA	GB-時間	時間単価	30 日間の最低コミットメントが終了する前に S3 Standard – IA ストレージから削除されたオブジェクトの、按分計算されたストレージの使用状況[3]
region-EarlyDelete-SIA-SmObjects	GB-時間	時間単価	30 日間の最低コミットメントが終了する前に S3 Standard – IA ストレージから削除された小さなオブジェクト (128 KB 未満) の、按分計算されたストレージの使用状況[3]
region-EarlyDelete-ZIA	GB-時間	時間単価	30 日間の最低コミットメントが終了する前に S3 1 ゾーン – IA ストレージから削除されたオブジェクトの、按分計算されたストレージの使用状況[3]

使用タイプ	単位	詳細度	説明
region-EarlyDelete-ZIA-SmObjects	GB-時間	時間単価	30 日間の最低コミットメントが終了する前に S3 1 ゾーン – IA ストレージから削除された小さなオブジェクト (128 KB 未満) の、按分計算されたストレージの使用状況[3]
region-Expedited-Retrieval-Bytes	GB	毎時	Expedited S3 Glacier Flexible Retrieval リクエストを使用して取得されるデータの量
Global-Bucket-Hrs-FreeTier	バケット	月別	アカウントレベルの無料利用枠 (2,000 バケット) 内の、アカウントの汎用バケット数
Global-Bucket-Hrs	バケット	月別	アカウントレベルの無料利用枠 (2,000 バケット) を超える、アカウントの汎用バケット数
region-Inventory-Objects Listed	オブジェクト	時間単価	インベントリリストで、オブジェクトグループごとにリストされるオブジェクトの数 (オブジェクトはバケットまたはプレフィックスごとにグループ化される)
region-Metadata-Updates	更新	毎時	S3 メタデータによって処理される更新に対する更新あたりの料金

使用タイプ	単位	詳細度	説明
region-Monitoring-Automation-INT	オブジェクト	時間単価	S3 Intelligent-Tiering ストレージクラスの監視および自動階層化された一意のオブジェクトの数
region-MRAP-Out-Bytes	GB	毎時	S3 のマルチリージョンアクセスポイントエンドポイントを介してリージョン内のバケットから転送されるデータの量 (MRAP データルーティング料金)。
region-MRAP-In-Bytes	GB	毎時	S3 のマルチリージョンアクセスポイントエンドポイントを介してリージョン内のバケットから転送されるデータの量 (MRAP データルーティング料金)。
regiongroup1-regiongroup2--MRAP-Out-Bytes	GB	毎時	S3 のマルチリージョンアクセスポイントエンドポイントを介して、*regiongroup1* のバケットから AWS ネットワーク外にある *regiongroup2* のクライアントに転送されるデータの量。

使用タイプ	単位	詳細度	説明
regiongroup1-regiongroup2- -MRAP-In-Bytes	GB	毎時	S3 のマルチリージョンアクセスポイントエンドポイントを介して、*regiongroup1* のバケットに AWS ネットワーク外にある *regiongroup2* のクライアントから転送されるデータの量。
region-OverwriteBytes-Copy-GDA	GB	月別	CopyObject オペレーションによって S3 Glacier Deep Archive ストレージで上書きされたデータの量
region-OverwriteBytes-Copy-GIR	GB	月別	CopyObject オペレーションによって S3 Glacier Instant Retrieval ストレージで上書きされたデータの量。
region-OverwriteBytes-Copy-GLACIER	GB	月別	CopyObject オペレーションによって S3 Glacier Flexible Retrieval ストレージで上書きされたデータの量
region-OverwriteBytes-Copy-INT	GB	月別	CopyObject オペレーションによって S3 Intelligent-Tiering ストレージで上書きされたデータの量

使用タイプ	単位	詳細度	説明
region-OverwriteBytes-Copy-RRS	GB	月別	CopyObject オペレーションによって低冗長化ストレージ (RRS) で上書きされたデータの量
region-OverwriteBytes-Copy-SIA	GB	月別	CopyObject オペレーションによって S3 Standard-IA ストレージで上書きされたデータの量
region-OverwriteBytes-Copy-STANDARD	GB	月別	CopyObject オペレーションによって S3 Standard ストレージで上書きされたデータの量
region-OverwriteBytes-Copy-ZIA	GB	月別	CopyObject オペレーションによって S3 One Zone-IA ストレージで上書きされたデータの量
region-OverwriteBytes-Put-GDA	GB	月別	PutObject オペレーションによって S3 Glacier Deep Archive ストレージで上書きされたデータの量
region-OverwriteBytes-Put-GIR	GB	月別	PutObject オペレーションによって S3 Glacier Instant Retrieval ストレージで上書きされたデータの量。

使用タイプ	単位	詳細度	説明
region-OverwriteBytes-Put-GLACIER	GB	月別	PutObject オペレーションによって S3 Glacier Flexible Retrieval ストレージで上書きされたデータの量
region-OverwriteBytes-Put-INT	GB	月別	PutObject オペレーションによって S3 Intelligent-Tiering ストレージで上書きされたデータの量
region-OverwriteBytes-Put-RRS	GB	月別	PutObject オペレーションによって低冗長化ストレージ (RRS) で上書きされたデータの量
region-OverwriteBytes-Put-SIA	GB	月別	PutObject オペレーションによって S3 Standard-IA ストレージで上書きされたデータの量
region-OverwriteBytes-Put-STANDARD	GB	月別	PutObject オペレーションによって S3 Standard ストレージで上書きされたデータの量
region-OverwriteBytes-Put-ZIA	GB	月別	PutObject オペレーションによって S3 One Zone-IA ストレージで上書きされたデータの量

使用タイプ	単位	詳細度	説明
region1-*region2*-S3RTC-In-Bytes	GB	月別	PutObject ReplTime 、GetObject ReplTime 、InitiateMultipartUploadReplTime 、UploadPartReplTime 、CompleteMultipartUploadReplTime 、WriteACLReplTime オペレーションによって S3 Replication Time Control (S3 RTC) で *region2* から *region1* に転送されたデータ量

使用タイプ	単位	詳細度	説明
region1-*region2*-S3RTC-Out-Bytes	GB	月別	PutObjectReplTime 、GetObjectReplTime 、InitiateMultipartUploadReplTime 、UploadPartReplTime 、CompleteMultipartUploadReplTime 、WriteACLReplTime オペレーションによって S3 Replication Time Control (S3 RTC) で *region1* から *region2* に転送されたデータ量
region-Requests-GDA-Tier1	カウント	毎時	S3 Glacier Deep Archive オブジェクトの PUT、COPY、POST、CreateMultipartUpload 、UploadPart 、または CompleteMultipartUpload リクエストの数 [6]
region-Requests-GDA-Tier2	カウント	毎時	S3 Glacier Deep Archive オブジェクトの GET および HEAD リクエストの数
region-Requests-GDA-Tier3	カウント	時間単価	S3 Glacier Deep Archive 標準復元リクエストの数

使用タイプ	単位	詳細度	説明
region-Requests-GDA-Tier5	カウント	時間単価	Bulk S3 Glacier Deep Archive の復元リクエストの数
region-Requests-GIR-Tier1	カウント	毎時	S3 Glacier Instant Retrieval オブジェクトに対する PUT、COPY、または POST リクエストの数。
region-Requests-GIR-Tier2	カウント	毎時	S3 Glacier Instant Retrieval オブジェクトに対する GET および他のすべての S3 Glacier Instant Retrieval-Tier1 以外のリクエストの数。
region-Requests-GLACIER-Tier1	カウント	毎時	S3 Glacier Flexible Retrieval オブジェクトに対する PUT、COPY、POST、CreateMultipartUpload 、UploadPart 、またはCompleteMultipartUpload リクエストの数 [6]
region-Requests-GLACIER-Tier2	カウント	毎時	S3 Glacier Flexible Retrieval オブジェクトに表示されていない GET および他のすべてのリクエストの数

使用タイプ	単位	詳細度	説明
region-Requests-INT-Tier1	カウント	毎時	S3 Intelligent-Tiering オブジェクトに対する PUT、COPY、または POST リクエストの数
region-Requests-INT-Tier2	カウント	毎時	S3 Intelligent-Tiering オブジェクトに対する GET および他のすべての Tier1 以外のリクエストの数
region-Requests-SIA-Tier1	カウント	毎時	S3 Standard–IA オブジェクトに対する PUT、COPY、または POST リクエストの数
region-Requests-SIA-Tier2	カウント	毎時	S3 Standard-IA オブジェクトに対する GET および他のすべての S3 Glacier Instant Retrieval-Tier1 以外のリクエストの数。
region-Requests-Tier1	カウント	毎時	S3 Standard、RRS、タグに対する PUT、COPY、または POST リクエストに加え、すべてのバケットとオブジェクトに対する LIST リクエストの数
region-Requests-Tier2	カウント	毎時	GET および他のすべての Tier1 以外のリクエストの数

使用タイプ	単位	詳細度	説明
region-Requests-Tier3	カウント	毎時	S3 Glacier Flexible Retrieval または S3 Glacier Deep Archiveへのライフサイクルリクエスト、および標準 S3 Glacier Flexible Retrieval 復元リクエストの数。
region-Requests-Tier4	カウント	毎時	S3 Glacier Flexible Retrieval、S3 Intelligent-Tiering、S3 Standard-IA、または S3 One Zone-IA ストレージへのライフサイクル移行数
region-Requests-Tier5	カウント	毎時	Bulk S3 Glacier Flexible Retrieval 復元リクエストの数
region-Requests-Tier6	カウント	毎時	Expedited S3 Glacier Flexible Retrieval 復元リクエストの数
region-Requests-Tier8	カウント	毎時	S3 Access Grants リクエストの数
region-Requests-XZ-Tier1	カウント	毎時	S3 Express One Zone オブジェクトに対する PUT または COPY リクエストの数
region-Requests-XZ-Tier2	カウント	毎時	S3 Express One Zone オブジェクトに対する GET およびその他すべての S3 Express One Zone-Tier1 以外のリクエストの数

使用タイプ	単位	詳細度	説明
region-Requests-ZIA-Tier1	カウント	毎時	S3 One Zone-IA オブジェクトに対する PUT、COPY、または POST リクエストの数
region-Requests-ZIA-Tier2	カウント	毎時	S3 One Zone-IA オブジェクトに対する GET および他のすべての S3 One Zone-IA-Tier1 以外のリクエストの数
region-Retrieval-GIR	GB	毎時	S3 Glacier Instant Retrieval ストレージから取得したデータの量。
region-Retrieval-SIA	GB	時間単価	S3 Standard – IA ストレージから取得したデータの量
region-Retrieval-XZ	GB	毎時	S3 Express One Zone ストレージでの特定の取り出しリクエスト (PUT または COPY) で 512 KB を超えるデータの一部
region-Retrieval-ZIA	GB	時間単価	S3 1 ゾーン – IA ストレージから取得したデータの量
region-S3DSSE-In-Bytes	GB	月別	Amazon S3 によって二重暗号化されたデータの量
region-S3DSSE-Out-Bytes	GB	月別	Amazon S3 によって復号された二重暗号化されたデータの量

使用タイプ	単位	詳細度	説明
region-S3G-DataTransfer-In-Bytes	GB	毎時	S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive ストレージからオブジェクトを復元するために Amazon S3 に転送されるデータの量
region-S3G-DataTransfer-Out-Bytes	GB	毎時	オブジェクトを S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive ストレージに移行するために Amazon S3 から転送されたデータの量
region-Select-Returned-Bytes	GB	時間単価	S3 Standard ストレージから Select リクエストを使用して返されたデータの量
region-Select-Returned-GIR-Bytes	GB	毎時	S3 Glacier Instant Retrieval ストレージから選択リクエストを使用して返されたデータの量
region-Select-Returned-INT-Bytes	GB	時間単価	S3 Intelligent-Tiering ストレージから Select リクエストを使用して返されたデータの量
region-Select-Returned-SIA-Bytes	GB	時間単価	S3 Standard – IA ストレージから Select リクエストを使用して返されたデータの量

使用タイプ	単位	詳細度	説明
region-Select-Returned-ZIA-Bytes	GB	時間単価	S3 1 ゾーン – IA ストレージから Select リクエストを使用して返されたデータの量
region-Select-Scanned-Bytes	GB	時間単価	S3 Standard ストレージから Select リクエストを使用してスキャンされたデータの量
region-Select-Scanned-GIR-Bytes	GB	毎時	S3 Glacier Instant Retrieval ストレージから選択リクエストを使用してスキャンされたデータの量。
region-Select-Scanned-INT-Bytes	GB	時間単価	S3 Intelligent-Tiering ストレージから Select リクエストを使用してスキャンされたデータの量
region-Select-Scanned-SIA-Bytes	GB	時間単価	S3 Standard – IA ストレージから Select リクエストを使用してスキャンされたデータの量
region-Select-Scanned-ZIA-Bytes	GB	時間単価	S3 1 ゾーン – IA ストレージから Select リクエストを使用してスキャンされたデータの量
region-Standard-Retrieval-Bytes	GB	毎時	標準 S3 Glacier Instant Retrieval または S3 Glacier Deep Archive リクエストで取得したデータの量

使用タイプ	単位	詳細度	説明
region-StorageAnalytics-ObjCount	オブジェクト	毎時	各ストレージクラス分析設定でモニタリングされる一意のオブジェクトの数。
region-StorageLens-ObjCount	オブジェクト	1 日 1 回	S3 Storage Lens の高度なメトリクスとレコメンデーションによって追跡される、各 S3 Storage Lens ダッシュボードの一意のオブジェクトの数。
region-StorageLensFreeTier-ObjCount	オブジェクト	1 日 1 回	S3 Storage Lens の使用状況メトリクスによって追跡される、各 S3 Storage Lens ダッシュボードの一意のオブジェクトの数。
StorageObjectCount	カウント	1 日 1 回	特定のバケット内に保存されたオブジェクトの数
region-Tables-CompactedObjects	オブジェクト	毎時	Amazon S3 テーブルバケットに圧縮されたオブジェクトの数
region-Tables-MonitoredObjects	オブジェクト	毎時	Amazon S3 テーブルバケット内のオブジェクトの数
region-Tables-ProcessedBytes	GB	毎時	Amazon S3 テーブルバケットで圧縮のために処理されるデータの量

使用タイプ	単位	詳細度	説明
region-Tables-Requests-Tier1	カウント	毎時	Amazon S3 テーブルバケットの PUT リクエストの数
region-Tables-Requests-Tier2	カウント	毎時	Amazon S3 テーブルバケットに対する GET および他のすべての non-Tier1 リクエストの数
region-Tables-TimedStorage-ByteHrs	GB-月	1 日 1 回	Amazon S3 テーブルバケットにデータが保存された GB-月の数
region-TagStorage-TagHrs	タグ時間	1 日 1 回	時間毎にレポートされる、バケット内のすべてのオブジェクトのタグの合計
region-TimedStorage-ByteHrs	GB-月	1 日 1 回	S3 Standard ストレージに保存されたデータの GB-月の数
region-TimedStorage-GDA-ByteHrs	GB-月	1 日 1 回	S3 Glacier Deep Archive ストレージに保存されたデータの GB-月の数
region-TimedStorage-GDA-Staging	GB-月	1 日 1 回	S3 Glacier Deep Archive ステージングストレージに保存されたデータの GB-月の数
region-TimedStorage-GIR-ByteHrs	GB-月	1 日 1 回	S3 Glacier Instant Retrieval ストレージに保存されたデータの GB-月の数。

使用タイプ	単位	詳細度	説明
region-TimedStorage-GIR-SmObjects	GB-月	1 日 1 回	S3 Glacier Flexible Retrieval の IA ストレージに保存された小さなオブジェクト (128 KB 未満) の GB-月の数
region-TimedStorage-GlacierByteHrs	GB-月	1 日 1 回	S3 Glacier Flexible Retrieval ストレージに保存されたデータの GB-月の数
region-TimedStorage-GlacierStaging	GB-月	1 日 1 回	S3 Glacier Flexible Retrieval staging ストレージに保存されたデータの GB-月の数
region-TimedStorage-INT-FA-ByteHrs	GB-月	1 日 1 回	S3 Intelligent-Tiering ストレージの高頻度のアクセス階層に保存されたデータの GB-月の数[5]
region-TimedStorage-INT-IA-ByteHrs	GB-月	1 日 1 回	S3 Intelligent-Tiering ストレージの小頻度のアクセス階層に保存されたデータの GB-月の数
region-TimedStorage-INT-AA-ByteHrs	GB-月	1 日 1 回	S3 Intelligent-Tiering ストレージのアーカイブのアクセス階層に保存されたデータの GB-月の数
region-TimedStorage-INT-AIA-ByteHrs	GB-月	1 日 1 回	S3 Intelligent-Tiering ストレージのアーカイブのインスタントアクセス階層に保存されたデータの GB-月の数

使用タイプ	単位	詳細度	説明
region-TimedStorage-INT-DAA-ByteHrs	GB-月	1 日 1 回	S3 Intelligent-Tiering ストレージの Deep アーカイブのアクセス階層に保存されたデータの GB-月の数
region-TimedStorage-RRS-ByteHrs	GB-月	1 日 1 回	低冗長化ストレージ (RRS) に保存されたデータの GB-月の数
region-TimedStorage-SIA-ByteHrs	GB-月	1 日 1 回	S3 Standard-IA ストレージに保存されたデータの GB-月の数
region-TimedStorage-SIA-SmObjects	GB-月	1 日 1 回	S3 Standard – IA ストレージに保存された小さなオブジェクト (128 KB 未満) の GB-月の数[4]
region-TimedStorage-XZ-ByteHrs	GB-月	1 日 1 回	S3 Express One Zone ストレージに保存されたデータの GB-月の数
region-TimedStorage-ZIA-ByteHrs	GB-月	1 日 1 回	S3 1 ゾーン – IA ストレージに保存されたデータの GB-月の数
region-TimedStorage-ZIA-SmObjects	GB-月	1 日 1 回	S3 One Zone-IA ストレージに保存された小さなオブジェクト (128 KB 未満) の GB-月の数

使用タイプ	単位	詳細度	説明
region-Upload-XZ	GB	毎時	S3 Express One Zone での特定のアップロードリクエスト (PUT または COPY) で 512 KB を超えるデータの量

メモ

1. Global-Bucket-Hrs および Global-Bucket-Hrs-FreeTier の使用タイプは、商用の AWS リージョンおよび AWS GovCloud (US) の汎用バケットに適用されます。
2. 完了前に転送を終了すると、転送されるデータ量がアプリケーションが受け取るデータ量を超える可能性があります。この不一致は、転送終了リクエストを即時に実行することができず、終了リクエストの実行が保留されている間にある程度の量のデータが転送中である可能性があるために発生する可能性があります。この転送中のデータは、「アウト」された転送データとして請求されます。
3. S3 Glacier または S3 Glacier Deep Archive ストレージクラスにアーカイブされたオブジェクトは、最小ストレージコミットメントが経過する前に削除または上書きされるか、別のストレージクラスに移行されます (S3 Glacier Instant Retrieval および S3 Glacier Flexible Retrieval の場合は 90 日、S3 Glacier Deep Archive の場合は 180 日)。残りの日数に対しては、ギガバイト単位で比例配分された料金が適用されます。
4. S3 Standard-IA または S3 One Zone-IA ストレージのオブジェクトを 30 日より前に削除、上書き、または他のストレージクラスに移行すると、残りの日数に対してはギガバイト単位で比例配分された料金が適用されます。
5. S3 Standard-IA または S3 One Zone-IA ストレージの小さい (128 KB より小さい) オブジェクトを 30 日より前に削除、上書き、または他のストレージクラスに移行すると、残りの日数に対してはギガバイト単位で按分計算された料金が適用されます。
6. S3 Intelligent-Tiering ストレージクラスのオブジェクトには、請求可能な最小オブジェクトサイズはありません。128 KB 未満のオブジェクトは、モニタリングされないか、自動階層化の対象となります。小さいオブジェクトは必ず S3 Intelligent-Tiering 高頻度アクセス階層に保存されます。
7. S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive ストレージクラスのいずれかに対して「CreateMultipartUpload」、「UploadPart」、または「UploadPartCopy」リクエストを開始すると、マルチパートアップロードが完了するまで、リクエストは S3 Standard のリクエスト料金で請求されます。アップロードが完了すると、送信先の S3 Glacier ストレージの PUT

料金で 1 つの CompleteMultipartUpload リクエストが請求されます。S3 Glacier Flexible Retrieval ストレージクラスへの PUT の処理中のマルチパートアップロードパートは、アップロードが完了するまで S3 Glacier Flexible Retrieval ステージングストレージとして S3 Standard ストレージ料金で請求されます。同様に、S3 Glacier Deep Archive ストレージクラスへの PUT のための処理中のマルチパートアップロードパートは、アップロードが完了するまで S3 Glacier Deep Archive ステージングストレージとして S3 Standard ストレージ料金で請求されます。

8. S3 Express One Zone では、リクエストサイズが 512 KB 以下の場合、リクエストごとの定額料金が適用されます。リクエストの 512 KB を超える部分の PUT リクエストと GET リクエストには、GB あたりの追加料金が適用されます。
9. S3 Express One Zone ストレージクラスでサポートされている機能については、「ディレクトリバケットでサポートされていない Amazon S3 の機能」を参照してください。
10. GB 単位で請求される単位の使用タイプは、使用状況レポートでバイト単位で計算されます。
11. GB-月は、GB-時間の数を 1 か月で集計し、その月の時間数で割って算出されます。詳細については、「Amazon S3 のよくある質問: Amazon S3 の利用には、どのように課金され、請求されますか?」を参照してください。

> **Note**
>
> 一般に、S3 バケット所有者は、HTTP 200 OK 成功レスポンスと HTTP 4XX クライアントエラーレスポンスを含むリクエストに対して課金されます。バケット所有者は、HTTP 503 Slow Down エラーなどの HTTP 5XX サーバーエラーレスポンスに対しては課金されません。HTTP 3XX の S3 エラーコードと請求されない 4XX ステータスコードの詳細については、「Amazon S3 のエラーレスポンスに対する請求」を参照してください。バケットがリクエスタ支払いバケットとして設定されている場合の請求の詳細については、「リクエスタ支払いの課金の仕組み」を参照してください。

使用状況レポートの追跡オペレーション

オペレーションは、お役様の AWS オブジェクトまたはバケットで実行されるアクションを、特定の使用タイプによって記述します。オペレーションは、PutObject や ListBucket のような、見ればすぐわかるコードによって示されます。特定の使用タイプがバケットのどのアクションで発生しているかを確認するには、これらのコードを使用します。使用状況レポートを作成する場合、レポートに [All Operations] (すべてのオペレーション) を含めるか、GetObject など特定のオペレーションのみを含めるかを選択できます。

詳細情報

- Amazon S3 の AWS 使用状況レポート
- Amazon S3 の AWS Billing レポート
- Amazon S3 の料金
- Amazon S3 のよくある質問

Amazon S3 のエラーレスポンスに対する請求

一般に、S3 バケット所有者は、HTTP 200 OK 成功レスポンスと HTTP 4XX クライアントエラーレスポンスを含むリクエストに対して課金されます。バケット所有者は、HTTP 503 Slow Down エラーなどの HTTP 5XX サーバーエラーレスポンスに対しては課金されません。バケットがリクエスタ支払いバケットとして設定されている場合の請求の詳細については、「リクエスタ支払いの課金の仕組み」を参照してください。

次の表は、HTTP 3XX および 4XX ステータスコードで、請求されない特定のエラーコードの一覧です。ウェブサイトホスティングで設定されたバケットでは、S3 がカスタムエラードキュメントを返した場合、またはカスタムリダイレクトを行った場合は、該当するリクエストおよびその他の料金が適用されます。

> **Note**
>
> AccessDenied (HTTP 403 Forbidden) の場合、リクエストがバケット所有者の個々の AWS アカウントまたはバケット所有者の AWS 組織外で開始されても、S3 ではバケット所有者への請求を行いません。

HTTP ステータスコード	エラーコード	エラーコードの説明	
301 Moved Permanently	PermanentRedirect	アクセスしようとしているバケットは、指定されたエンドポイントを使用してアドレス指定する必要があります。今後のリ	

HTTP ステータスコード	エラーコード	エラーコードの説明
		クエストはこのエンドポイントに送信してください。
	PermanentRedirectControlError	アクセスしようとしている API 操作は、指定されたエンドポイントを使用してアドレス指定する必要があります。今後のリクエストはこのエンドポイントに送信してください。
一時的なダイレクト (302)	TemporaryRedirect	ドメインネームシステム (DNS) サーバーが更新されている間、このバケットにリダイレクトされています。
400 Bad Request	AuthorizationHeaderMalformed	指定した認可ヘッダーが無効です。
	AuthorizationQueryParametersError	指定した認可クエリパラメータが無効です。
	ConnectionClosedByRequester	WriteGetObjectResponse 本文の読み取り中にエラーが発生した場合に、呼び出し元に返されます。
	DeviceNotActiveError	デバイスは現在アクティブではありません。

HTTP ステータスコード	エラーコード	エラーコードの説明	
	EndpointNotFound	リクエストを正しいエンドポイントに直接送信してください。	
	ExpiredToken	提供されたトークンの有効期限が切れています。	
	IllegalLocationConstraintException	バケットが存在するリージョンとは異なるリージョンからバケットにアクセスしようとしています。このエラーを回避するには、`--region` オプションを使用します。例: `aws s3 cp awsexample.txt s3://amzn-s3-demo-bucket/ --region ap-east-1` 。	

HTTP ステータスコード	エラーコード	エラーコードの説明	
	InvalidArgument	このエラーは、次の原因によって発生する可能性があります。 • 指定された引数は有効ではありませんでした。 • リクエストに必要なヘッダーがありませんでした。 • 指定された引数が不完全であるか、形式が正しくありませんでした。 • 指定された引数は、3 以上の長さである必要があります。	
	InvalidBucketOwnerAWSAccountID	期待されるバケット所有者パラメータの値は AWS アカウント ID である必要があります。	
	InvalidDigest	指定した Content-MD5 またはチェックサム値が無効です。	
	InvalidEncryptionAlgorithmError	指定した暗号化リクエストが無効です。有効値は AES256 です。	

HTTP ステータスコード	エラーコード	エラーコードの説明	
	InvalidHostHeader	リクエストで指定されたホストヘッダーに適正でない形式のアドレス指定が使用されていました。	
	InvalidHttpMethod	リクエストが、予期しない HTTP メソッドを使用して実行されました。	

HTTP ステータスコード	エラーコード	エラーコードの説明	
	InvalidRequest	このエラーは、次の原因によって発生する可能性があります。 • リクエストで間違った署名バージョンを使用しています。AWS4-HMAC-SHA256 (署名バージョン 4) を使用してください。 • アクセスポイントは、既存のバケットに対してのみ作成できます。 • アクセスポイントが削除可能な状態ではありません。 • アクセスポイントは、既存のバケットに対してのみ作成できます。 • 次のトークンが無効です。 • ライフサイクルルールで少なくとも 1 つのアクションを指定する必要があります。 • 少なくとも 1 つのライフサイクルルールを	

HTTP ステータスコード	エラーコード	エラーコードの説明	
		指定する必要があります。 • ライフサイクルルールの数は、許可されている 1000 ルールの制限を超えてはなりません。 • `MaxResults` パラメータの範囲が無効です。 • SOAP リクエストは HTTPS 接続を介して行う必要があります。 • Amazon S3 Transfer Acceleration は、DNS に準拠していない名前のバケットではサポートされていません。 • Amazon S3 Transfer Acceleration は、ピリオド (.) が名前に含まれているバケットではサポートされていません。 • Amazon S3 Transfer Acceleration エンドポイントは、仮想スタイ	

HTTP ステータスコード	エラーコード	エラーコードの説明	
		ルのリクエストのみをサポートします。 • Amazon S3 Transfer Acceleration は、このバケットでは設定されていません。 • Amazon S3 Transfer Acceleration は、このバケットでは無効になっています。 • Amazon S3 Transfer Acceleration は、このバケットではサポートされていません。サポートが必要な場合は、サポート にお問い合わせください。 • Amazon S3 Transfer Acceleration はこのバケットでは有効にできません。サポートが必要な場合は、サポート にお問い合わせください。 • HTTP ヘッダーとクエリパラメータで指定された値が競合しています。	

HTTP ステータスコード	エラーコード	エラーコードの説明	
		• HTTP ヘッダーと POST フォームフィールドで指定された値が競合しています。 • サイズが 5GB を超えるオブジェクトに対して CopyObject 要求が行われました。	
	InvalidSessionException	タイムアウトしたか有効期限が切れたために、セッションがこれ以上存在しなくなった場合に返されます。	
	InvalidSignature	計算したリクエスト署名が、指定された署名と一致しません。AWS シークレットアクセスキーと署名方法を確認してください。詳細については、「REST リクエストの署名と認証」を参照してください。	
	InvalidSOAPRequest	SOAP リクエスト本文が無効です。	
	InvalidStorageClass	指定されたストレージクラスが無効です。	

HTTP ステータスコード	エラーコード	エラーコードの説明	
	InvalidTag	リクエストに無効なタグ入力が含まれています。例えば、リクエストに重複するキー、長すぎるキーまたは値、またはシステムタグが含まれている可能性があります。	
	InvalidToken	指定されたトークンは形式に誤りがあるか無効です。	
	InvalidURI	指定された URI を解析できませんでした。	
	KeyTooLongError	キーが長すぎます。	
	KMS.DisabledException	指定された KMS キーが有効になってないため、リクエストが拒否されました。	

HTTP ステータスコード	エラーコード	エラーコードの説明	
	KMS.InvalidKeyUsageException	次のいずれかの理由でリクエストが拒否されました。 • KMS キーの KeyUsage 値が API オペレーションと互換性がありません。 • オペレーションで指定された暗号化アルゴリズムまたは署名アルゴリズムが、KMS キーのキーマテリアルタイプ (KeySpec) と互換性がありません。 データキーの暗号化、復号、再暗号化、生成を行うには、KeyUsage が ENCRYPT_DECRYPT である必要があります。メッセージに署名して検証するには、KeyUsage が SIGN_VERIFY である必要があります。メッセージ認証コード (MAC) を生成して検証するには、KeyUsage が GENERATE_VERIFY_MAC である必要があります。キーアグリーメントシークレッ	

HTTP ステータスコード	エラーコード	エラーコードの説明	
		トを取得するには、KeyUsage が KEY_AGREEMENT である必要があります。KMS キーの KeyUsage を検索するには、DescribeKey オペレーションを使用します。 特定の KMS キーでサポートされている暗号化アルゴリズムまたは署名アルゴリズムを検索するには、DescribeKey オペレーションを使用します。	

HTTP ステータスコード	エラーコード	エラーコードの説明	
	KMS.KMSInvalidStateException	指定されたリソースの状態がこのリクエストに対して有効ではないため、リクエストが拒否されました。この例外は、次のいずれかを意味します。 • KMS キーのキーの状態は、このオペレーションと互換性がありません。 キーの状態を検索するには、DescribeKey オペレーションを使用します。各 KMS オペレーションと互換性があるキーの状態の詳細については、「AWS Key Management Service デベロッパーガイド」の「AWS KMS keys のキーの状態」を参照してください。 • カスタムキーストアの KMS キーへの暗号化オペレーションの場合、この例外は、多くの原因が想定できる、一般的な障害を意味します。原因を特定するには、例外に付随する工	

HTTP ステータスコード	エラーコード	エラーコードの説明	
		ラーメッセージを使用します。	
	KMS.NotFoundException	指定されたエンティティまたはリソースが見つからないため、リクエストが拒否されました。	
	LambdaInvalidResponse	WriteGetObjectResponse が AWS Lambda に ValidationError で応答すると、呼び出し元に返されます。詳細については、ValidationError メッセージを参照してください。ValidationError のすべてのケースで LambdaInvalidResponse エラーが発生するとは限りません。	

HTTP ステータスコード	エラーコード	エラーコードの説明	
	LambdaInvocationFailed	Lambda 関数の呼び出しに失敗しました。S3 Object Lambda が設定された Lambda 関数の呼び出しを正常に完了できない場合、呼び出し元は次のエラーを受け取る場合があります。このエラーメッセージには、関数を呼び出す際に AWS Lambda サービスが返す結果のエラーの詳細 (ステータスコード、エラーコード、エラーメッセージ、リクエスト ID など) が含まれている場合があります。	
	MalformedACLError	指定された ACL の書式に誤りがあるか、AWS の公開済みスキーマに一致しませんでした。	
	MalformedPOSTRequest	POST リクエストの本文が正しい形式の multipart/form-data ではありません。	
	MalformedXML	指定された XML の書式に誤りがあるか、Amazon の公開済みスキーマに一致しませんでした。	

HTTP ステータスコード	エラーコード	エラーコードの説明	
	MaxPostPreDataLengthExceededError	アップロードファイルの前の POST リクエストフィールドが大きすぎます。	
	MetadataTooLarge	メタデータヘッダーが許容されるメタデータの最大サイズを超えています。	
	MissingAttachment	SOAP アタッチメントが想定されていたにもかかわらず、見つかりませんでした。	
	MissingRequestBodyError	空の XML ドキュメントをリクエストとして送信しました。	
	MissingSecurityHeader	リクエストに必要なヘッダーがありません。	
	NoLoggingStatusForKey	キーのログ記録ステータスサブリソースのようなものはありません。	
	NotDeviceOwnerError	トークンを生成したデバイスを、認証済みのユーザーが所有していません。	

HTTP ステータスコード	エラーコード	エラーコードの説明	
	ResponseInterrupted	WriteGetObjectResponse 本文の読み取り中にエラーが発生した場合に、呼び出し元に返されます。	
	RequestHeaderSectionTooLarge	The request header and query parameters used to make the request exceed the maximum allowed sizes	
	TokenCodeInvalidError	指定したシリアル番号および/またはトークンコードが無効です。	
	UnexpectedContent	This request contains unsupported content.	
	UnsupportedArgument	リクエストにサポートされていない引数が含まれていました。	
	UnsupportedSignature	提供されたリクエストは、サポートされていない STS トークンのバージョンで署名されているか、署名のバージョンがサポートされていません。	

HTTP ステータスコード	エラーコード	エラーコードの説明	
	UserKeyMustBeSpecified	バケット POST リクエストは、指定されたフィールド名を含んでいなければなりません。指定されている場合は、フィールドの順序を確認してください。	
	IncorrectEndpoint	指定されたバケットが別のリージョンに存在します。リクエストを正しいエンドポイントに直接送信してください。	
	ValidationError	検証エラーは、WriteGetObjectResponse API オペレーションから返され、発生した理由はさまざまである可能性があります。詳細については、エラーメッセージを参照してください。	
403 Forbidden	RequestTimeTooSkewed	リクエスト時間とサーバー時間の差が大きすぎます。	

HTTP ステータスコード	エラーコード	エラーコードの説明
	SignatureDoesNotMatch	計算したリクエスト署名が、指定された署名と一致しません。AWS シークレットアクセスキーと署名方法を確認してください。詳細については、「REST リクエストの署名と認証」および「SOAP リクエストの認証方法」を参照してください。
	NotSignedUp	アカウントが Amazon S3 に対してサインアップされていません。Amazon S3 を使用する前に、サインアップする必要があります。サインアップは https://aws.amazon.com/s3 で行うことができます。
	InvalidSecurity	提供されたセキュリティ認証情報が無効です。
	InvalidPayer	このオブジェクトへのすべてのアクセスが無効になっています。詳細については、「AWS に問い合わせる」を参照してください。

HTTP ステータスコード	エラーコード	エラーコードの説明
	InvalidAccessKeyId	指定された AWS アクセスキー ID が見つかりません。
	AccountProblem	AWS アカウント アカウントに問題があり、それによりオペレーションを正常に完了することができません。詳細については、「AWS に問い合わせる」を参照してください。
	UnauthorizedAccessError	中国リージョンにのみ適用されます。ICP ライセンスを持たないバケットに対してリクエストが行われたときに返されます。詳細については、「ICP Recordal」を参照してください。
	UnexpectedIPError	中国リージョンにのみ適用されます。予期されない IP であったため、このリクエストは拒否されました。
	MissingAuthenticationToken	リクエストに署名がありませんでした。

HTTP ステータスコード	エラーコード	エラーコードの説明	
	LambdaPermissionError	呼び出し元は Lambda 関数を呼び出す権限がありません。呼び出し元には Lambda 関数を呼び出すアクセス許可が必要です。呼び出し元にアタッチされているポリシーを調べて、設定された関数に `lambda:Invoke` を使用することが許可されていることを確認します。このエラーメッセージには、関数を呼び出す際に Lambda サービスが返す結果のエラーの詳細 (ステータスコード、エラーコード、エラーメッセージ、リクエスト ID など) が含まれている場合があります。	

HTTP ステータスコード	エラーコード	エラーコードの説明	
404 Not Found	LambdaNotFound	AWS Lambda 関数が見つかりませんでした。設定済みの Lambda 関数、バージョン、またはエイリアスが、呼び出し試行時に見つかりませんでした。S3 Object Lambda アクセスポイントの設定が適切な Lambda 関数 ARN を指していることを確認します。このエラーメッセージには、関数を呼び出す際に AWS Lambda サービスが返す結果のエラーの詳細 (ステータスコード、エラーコード、エラーメッセージ、リクエスト ID など) が含まれている場合があります。	
	NoSuchAsyncRequest	指定されたリソースは見つかりませんでした。	
	NoSuchObjectLockConfiguration	指定されたオブジェクトには ObjectLock 設定がありません。	

HTTP ステータスコード	エラーコード	エラーコードの説明	
	NoSuchUpload	指定されたマルチパートアップロードは存在しません。アップロード ID が無効であるか、マルチパートアップロードが中止または完了した可能性があります。	
	NoSuchWebsiteConfiguration	指定されたバケットにはウェブサイト設定がありません。	
	NoTransformationDefined	この Object Lambda アクセスポイントの変換が見つかりませんでした。	
	ObjectLockConfigurationNotFoundError	このバケットにはオブジェクトロック設定が存在しません。	
405 Method Not Allowed	MethodNotAllowed	指定されたメソッドは、このリソースに対して許可されていません。	
409 Conflict	BucketAlreadyExists	リクエストされたバケット名は使用できません。バケット名前空間は、システムのすべてのユーザーによって共有されています。別の名前を使用してもう一度試してください。	

HTTP ステータスコード	エラーコード	エラーコードの説明
	InvalidBucketState	リクエストはバケットの現在の状態で有効ではありません。
	OperationAborted	競合する条件付きオペレーションが現在このリソースに対して進行中です。もう一度試してください。
411 Length Required	MissingContentLength	Content-Length HTTP ヘッダーを指定する必要があります。
412 Precondition Failed	RequestIsNotMultiPartContent	バケット POST リクエストは、enctype が multipart/form-data である必要があります。
416 Requested Range Not Satisfiable	InvalidRange	リクエストされた範囲はこのリクエストに対して有効ではありません。別の範囲を試してください。

Amazon S3 ストレージクラスの理解と管理

Amazon S3 内にある各オブジェクトには、ストレージクラスが関連付けられています。デフォルトでは、S3 のオブジェクトは S3 Standard ストレージクラスに保存されますが、Amazon S3 は、保存するオブジェクトに対して、広範なストレージクラスを提供します。ユースケースシナリオおよびパフォーマンスアクセス要件を考慮してクラスを選択します。ユースケースに合わせて設計されたストレージクラスを選択すると、オブジェクトのストレージコスト、パフォーマンス、可用性を最適化できます。このストレージクラスはすべて高度な耐久性を提供します。

以下のセクションでは、さまざまなストレージクラスの詳細と、オブジェクトにストレージクラスを設定する方法について説明します。

トピック

- アクセス頻度の高いオブジェクトのストレージクラス
- アクセスパターンが変化する、またはアクセスパターンが不明なデータを、自動的に最適化するためのストレージクラス
- アクセス頻度の低いオブジェクトのストレージクラス
- ほとんどアクセスすることのないオブジェクトのストレージクラス
- Amazon S3 on Outposts のストレージクラス
- Amazon S3 ストレージクラスの比較
- オブジェクトのストレージクラスを設定
- Amazon S3 分析 – ストレージクラス分析
- Amazon S3 Intelligent-Tiering によるストレージコストの管理
- 長期データストレージとしての S3 Glacier ストレージクラスを理解する
- アーカイブされたオブジェクトの操作

アクセス頻度の高いオブジェクトのストレージクラス

パフォーマンス重視のユースケース (ミリ秒単位のアクセス時間を要するユースケース) とアクセス頻度の高いデータには、Amazon S3 は次のストレージクラスを提供しています。

- S3 Standard (STANDARD) – デフォルトのストレージクラス。オブジェクトのアップロード時にストレージクラスを指定しない場合、Amazon S3 Standard ストレージクラスが割り当てられます。S3 Standard と S3 Standard-IA 間のコストを最適化するために、「Amazon S3 分析 – ストレージクラス分析」を使用できます。
- S3 Express One Zone (EXPRESS_ONEZONE) – Amazon S3 Express One Zone は、最もレイテンシーの影響を受けやすいアプリケーションに 1 桁のミリ秒単位で一貫したデータアクセスを提供することを目的として構築された、高パフォーマンスのシングルアベイラビリティーゾーンの Amazon S3 ストレージクラスです。S3 Express One Zone は、現在入手可能なレイテンシーが最も低いクラウドオブジェクトストレージクラスで、データアクセス速度は最大 10 倍速く、リクエストコストは S3 スタンダードよりも 50% 低減されます。S3 Express One Zone では、データは単一のアベイラビリティーゾーン内で冗長的に複数のデバイスに保存されます。詳細については、「S3 Express One Zone」を参照してください。

- 低冗長化ストレージ (REDUCED_REDUNDANCY) – 低冗長化ストレージ (RRS) のクラスは、それほど重要ではない再生可能なデータを、S3 Standard ストレージクラスより低いレベルの冗長性で保存することができます。

  > **Important**
  >
  > このストレージクラスの使用は推奨しません。S3 Standard ストレージクラスの方がコスト効果に優れています。

  耐久性について、RRS オブジェクトの平均年間予測喪失率は 0.01 パーセントです。RRS オブジェクトが紛失した場合、Amazon S3 はそのオブジェクトへのリクエストに 405 エラーを返します。

アクセスパターンが変化する、またはアクセスパターンが不明なデータを、自動的に最適化するためのストレージクラス

S3 Intelligent-Tiering (INTELLIGENT_TIERING) は、パフォーマンスへの影響やオペレーション上のオーバーヘッドを発生させることなく、データを最も費用効果の高いアクセス階層に自動的に移動することで、ストレージコストを最適化できるように設計された Amazon S3 ストレージクラスです。S3 Intelligent-Tiering は、アクセスパターンが変更されたときに、アクセス階層間で、細かなオブジェクトレベルでデータを移動することにより、自動的にコスト削減を実現する唯一のクラウドストレージクラスです。S3 Intelligent-Tiering は、アクセスパターンが不明または変化するデータのストレージコストを最小限に抑える場合に最適なストレージクラスです。S3 Intelligent-Tiering には取り出し料金は発生しません。

オブジェクトのモニタリングとオートメーションに対して発生する少額の月額料金で、S3 Intelligent-Tiering はアクセスパターンをモニタリングし、あまりアクセスされていないオブジェクトをより低コストのアクセス階層へ自動的に移動させることができます。S3 Intelligent-Tiering は、3 つの低レイテンシーかつ高スループットのアクセス階層で、自動的にストレージコストを削減できます。非同期でアクセスできるデータの場合は、S3 Intelligent-Tiering ストレージクラスで自動アーカイブ機能をアクティブ化することもできます。S3 Intelligent-Tiering は、99.9% の可用性と 99.999999999% の耐久性を実現するように設計されています。

S3 Intelligent-Tiering は、3 つのアクセス階層にオブジェクトを自動的に保存します。

- 高頻度アクセス – S3 Intelligent-Tiering にアップロードまたは転送されたオブジェクトは、高頻度アクセス階層に自動的に保存されます。

- 低頻度アクセス – S3 Intelligent-Tiering では、30 日間連続してアクセスされなかったオブジェクトは低頻度アクセス階層に移動されます。
- アーカイブインスタントアクセス – S3 Intelligent-Tiering では、90 日間連続してアクセスされていない既存のオブジェクトは、アーカイブインスタントアクセス階層に自動的に移動されます。

S3 Intelligent-Tiering では、これらの 3 つの階層に加えて、オプションとして次の 2 つのアーカイブアクセス階層が用意されています。

- アーカイブアクセス – S3 Intelligent-Tiering では、非同期的にアクセスできるデータ向けにアーカイブアクセス層をアクティブ化するオプションが提供されます。アクティブ化された後、アーカイブアクセス階層は 90 日間以上してアクセスされなかったオブジェクトを自動的にアーカイブします。
- ディープアーカイブアクセス – S3 Intelligent-Tiering では、非同期的にアクセスできるデータ向けにディープアーカイブアクセス階層をアクティブ化するオプションが提供されます。アクティブ化後、ディープアーカイブアクセス階層は 180 日間連続してアクセスされなかったオブジェクトを自動的にアーカイブします。

> **Note**
>
> - アーカイブインスタントアクセス階層をバイパスしたい場合は、アーカイブアクセス階層を 90 日間だけアクティブ化します。アーカイブアクセス階層は、分単位から時間単位の取得時間でストレージコストをわずかに削減します。アーカイブインスタントアクセス階層は、ミリ秒単位のアクセスと高いスループットパフォーマンスを実現します。
> - アプリケーションがオブジェクトに非同期でアクセスできる場合にのみ、アーカイブアクセス階層とディープアーカイブアクセス階層をアクティブにします。取得するオブジェクトがアーカイブアクセス階層またはディープアーカイブアクセス階層に保存されている場合は、まず `RestoreObject` を使用してオブジェクトを復元します。

新しく作成されたデータを S3 Intelligent-Tiering に移動して、デフォルトのストレージクラスとして設定することができます。また、`PutBucketIntelligentTieringConfiguration` API オペレーション、AWS CLI、または Amazon S3 コンソールを使用して、アーカイブアクセス階層の 1 つまたは両方をアクティブ化することもできます。S3 Intelligent-Tiering の使用方法およびアクティブアクセス階層のアクティブ化の詳細については、「S3 Intelligent-Tiering の使用」を参照してください。

Archive Access または Deep Archive Access 階層のオブジェクトにアクセスするには、まずそれらを復元する必要があります。詳細については、「S3 Intelligent-Tiering アーカイブアクセス階層からのオブジェクトの復元」を参照してください。

> **Note**
>
> オブジェクトのサイズが 128 KB 未満の場合は、モニタリングされず、自動階層化に適していません。小さいオブジェクトは必ず高頻度アクセス階層に保存されます。S3 Intelligent-Tiering の詳細については、「S3 Intelligent-Tiering アクセス階層」を参照してください。

アクセス頻度の低いオブジェクトのストレージクラス

S3 Standard – IA と S3 1 ゾーン – IA のストレージクラスは、存続期間が長く、アクセス頻度の低いデータ用に設計されています (IA は infrequent access (低頻度アクセス) の略です)。S3 Standard – IA オブジェクトおよび S3 1 ゾーン – IA オブジェクトは、ミリ秒のアクセスに使用できます (S3 Standard ストレージクラスに似ています)。Amazon S3 では、これらのオブジェクトに取り出し料金が発生するため、アクセスが頻繁ではないデータに最適です。料金については、「Amazon S3 の料金」を参照してください。

例えば、S3 Standard – IA と S3 1 ゾーン – IA のストレージクラスを選択し、次のことを行います。

- バックアップの保存
- アクセスが頻繁ではないが、ミリ秒単位のアクセスを必要とする旧いデータに適しています。例えば、データのアップロード時に S3 Standard ストレージクラスを選択し、Amazon S3 がオブジェクトを S3 Standard – IA または S3 1 ゾーン – IA クラスに移動するようにライフサイクル設定を使用することができます。

  ライフサイクル管理の詳細については、「オブジェクトのライフサイクルの管理」を参照してください。

> **Note**
>
> S3 Standard – IA と S3 1 ゾーン – IA ストレージクラスは、サイズが 128 KB 以上あり、少なくとも 30 日間保存する予定のオブジェクトに最適です。オブジェクトが 128 KB 以下の場合、Amazon S3 は 128 KB に相当する料金を請求します。最小ストレージ期間の 30 日が過ぎる前にオブジェクトを削除した場合は、30 日分の料金が発生します。30 日前に削除、上書き、または別のストレージクラスに移行されたオブジェクトは、通常のストレージ使

用料に加えて、最低 30 日間の残りの期間分の日割り料金が発生します。料金については、「Amazon S3 の料金」を参照してください。

ストレージクラスの違いについては下記をご覧ください。

- S3 Standard-IA (STANDARD_IA) – Amazon S3 は、地理的に分離された複数のアベイラビリティーゾーン間でオブジェクトデータを冗長的に保存します (S3 Standard ストレージクラスに似ています)。S3 Standard – IA オブジェクトはアベイラビリティーゾーンに障害が発生した場合の回復性に優れています。このストレージクラスは S3 1 ゾーン – IA クラスよりも優れた高可用性と回復性を提供します。S3 Standard と S3 Standard-IA 間のコストを最適化するために、「Amazon S3 分析 – ストレージクラス分析」を使用できます。
- S3 One Zone-IA (ONEZONE_IA) – Amazon S3 はオブジェクトデータを 1 つのアベイラビリティーゾーンでのみ保存するため、S3 Standard-IA よりも安価になります。ただし、地震や洪水といった災害によるアベイラビリティーゾーンの物理的な損失時においてデータの回復性はありません。S3 One Zone-IA ストレージクラスは S3 Standard-IA に並ぶ耐久性を備えていますが、可用性と回復性は劣ります。ストレージクラスの耐久性および可用性の比較情報については、このセクションの最後にある「Amazon S3 ストレージクラスの比較」を参照してください。料金については、「Amazon S3 の料金」を参照してください。データレジデンシーと分離のユースケースでは、AWS Local Zones にディレクトリバケットを作成し、S3 Express One Zone (EXPRESS_ONEZONE) および S3 One Zone-IA (ONEZONE_IA) ストレージクラスを使用できます。Local Zones のディレクトリバケットの詳細については、「データレジデンシーワークロード」を参照してください。

次の構成を推奨します。

- S3 Standard-IA (STANDARD_IA) – プライマリまたは再作成できないデータのコピーでのみ使用します。
- S3 One Zone-IA (ONEZONE_IA) – S3 クロスリージョンレプリケーション (CRR) を設定する際にアベイラビリティーゾーンで障害が発生した場合、オブジェクトレプリカ用にデータを再作成できるときに使用します。また、データレジデンシーと分離のために、AWS Local Zones にディレクトリバケットを作成し、S3 One Zone-IA ストレージクラスを使用できます。

ほとんどアクセスすることのないオブジェクトのストレージクラス

S3 Glacier Instant Retrieval (GLACIER_IR)、S3 Glacier Flexible Retrieval (GLACIER)、S3 Glacier Deep Archive (DEEP_ARCHIVE) ストレージクラスは、低コストで長期保存するために使用できるデータストレージおよびデータアーカイブ向けに設計されています。これらのストレージクラスでは、最小限のストレージ期間と取得料金になるため、ほとんどアクセスされないデータに対して最も効果的です。S3 Glacier ストレージクラスの詳細については、「長期データストレージとしての S3 Glacier ストレージクラスを理解する」を参照してください。

Amazon S3 は以下の S3 Glacier ストレージクラスを提供します:

- S3 Glacier Instant Retrieval (GLACIER_IR) – ほとんどアクセスされず、ミリ秒単位の取得が必要な長期データに使用します。このストレージクラスのデータにはリアルタイムアクセスできます。
- S3 Glacier Flexible Retrieval (GLACIER) – データの一部を数分で取得する必要があるアーカイブに使用します。このストレージクラスのデータはアーカイブされ、リアルタイムアクセスできなくなります。
- S3 Glacier Deep Archive (DEEP_ARCHIVE) – ほとんどアクセスする必要がないデータのアーカイブに使用します。このストレージクラスのデータはアーカイブされ、リアルタイムアクセスできなくなります。

アーカイブ済みオブジェクトの取得

オブジェクトのストレージクラスを S3 Glacier Flexible Retrieval (GLACIER) または S3 Glacier Deep Archive (DEEP_ARCHIVE) に設定するには、セクション オブジェクトのストレージクラスを設定 で説明しているように、他のストレージクラスに対して行う場合と同様の方法で行います。ただし、S3 Glacier Flexible Retrieval および S3 Glacier Deep Archive オブジェクトはアーカイブされ、リアルタイムでアクセスできなくなります。詳細については、「S3 Glacier Flexible Retrieval および S3 Glacier Deep Archive はアーカイブストレージクラスです。」を参照してください。

> **Note**
>
> S3 Glacier ストレージクラスを使用する場合、オブジェクトは Amazon S3 に残ります。Amazon S3 Glacier サービスを別途使用して直接アクセスすることはできません。Amazon S3 Glacier の詳細については、「Amazon S3 Glacier デベロッパーガイド」を参照してください。

Amazon S3 on Outposts のストレージクラス

Amazon S3 on Outposts を使用すると、AWS Outposts リソースで S3 バケットを作成し、ローカルデータアクセス、ローカルデータ処理、データレジデンシーを必要とするアプリケーション用に、オンプレミスのオブジェクトを保存および取得できます。AWS Outposts では、Amazon S3 と同じ API オペレーションと機能 (アクセスポリシー、暗号化、タグ付けを含む) を使用できます。AWS Management Console、AWS CLI、AWS SDK、または REST API を使用して S3 on Outposts を使用できます。

S3 on Outposts は、新しいストレージクラスである S3 Outposts (OUTPOSTS) を提供します。S3 Outposts のストレージクラスは、Outposts のバケットに格納されたオブジェクトに対してのみ使用できます。AWS リージョン の S3 バケットでこのストレージクラスを使用しようとすると、`InvalidStorageClass` エラーが発生します。さらに、S3 on Outposts に保存されているオブジェクトで他の S3 ストレージクラスを使用しようとすると、同じエラー応答が発生します。

S3 Outposts (OUTPOSTS) ストレージクラスに格納されているオブジェクトは、デフォルトでは Amazon S3 マネージド暗号化キー (SSE-S3) によるサーバー側の暗号化を使用して常に暗号化されます。詳細については、「Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3)」を参照してください。

お客様が用意した暗号化キー (SSE-C) を使用したサーバー側の暗号化を使用して、S3 Outposts ストレージクラスに格納されたオブジェクトを明示的に暗号化することもできます。詳細については、「お客様が指定したキーによるサーバー側の暗号化 (SSE-C) の使用」を参照してください。

> **Note**
>
> S3 on Outposts は、AWS Key Management Service (AWS KMS) キー (SSE-KMS) を使用したサーバー側暗号化をサポートしていません。

Outposts 上の S3 の詳細については、「Amazon S3 on Outposts ユーザーガイド」の「What is S3 on Outposts」を参照してください。

Amazon S3 ストレージクラスの比較

ストレージクラスの可用性、耐久性、最小ストレージ期間、その他の考慮すべき事項を含め、次の表で比較しています。

Storage Class	Designed for	Durability (designed for)	Availability (designed for)	Availability Zones	Min storage duration	Min billable object size	Other Considerations
STANDARD	Frequently accessed data	99.999999999%	99.99%	>= 3	None	None	None
STANDARD_IA	Long-lived, infrequently accessed data	99.999999999%	99.9%	>= 3	30 days	128 KB	Per GB retrieval fees apply.
INTELLIGENT_TIERING	Long-lived data with changing or unknown access patterns	99.999999999%	99.9%	>= 3	30 days	None	Monitoring and automation fees per object apply. No retrieval fees.
ONEZONE_IA	Long-lived, infrequently accessed, non-critical data	99.999999999%	99.5%	1	30 days	128 KB	Per GB retrieval fees apply. Not resilient to the loss of the Availability Zone.
GLACIER	Long-term data archiving with retrieval times ranging from minutes to hours	99.999999999%	99.99% (after you restore objects)	>= 3	90 days	None	Per GB retrieval fees apply. You must first restore archived objects before you can access them. For more information, see Restoring Archived Objects.
DEEP_ARCHIVE	Archiving rarely accessed data with a default retrieval time of 12 hours	99.999999999%	99.99% (after you restore objects)	>= 3	180 days	None	Per GB retrieval fees apply. You must first restore archived objects before you can access them. For more information, see Restoring Archived Objects.
RRS (Not recommended)	Frequently accessed, non-critical data	99.99%	99.99%	>= 3	None	None	None

* S3 Glacier Flexible Retrieval では、アーカイブされたオブジェクトごとに 40 KB の追加メタデータが必要です。これには、S3 Glacier Flexier Flexible Retrieval レート (データの識別と取得に必要) で請求される 32 KB のメタデータと、S3 スタンダートレートで請求される追加の 8 KB データが含まれます。S3 Glacier Flexible Retrieval にアーカイブされたオブジェクトのユーザー定義名とメタデータを維持するには、S3 スタンダートレートが必要です。ストレージクラスの詳細については、「Amazon S3 ストレージクラス」を参照してください。

** S3 Glacier Deep Archive には、アーカイブされたオブジェクトごとに 40 KB の追加メタデータが必要です。これには、S3 Glacier Deep Archive レート (データの識別と取得に必要) で請求される 32 KB のメタデータと、S3 スタンダートレートで請求される追加の 8 KB データが含まれます。Amazon S3 Glacier Deep Archive にアーカイブされたオブジェクトのユーザー定義の名前とメタデータを維持するには、S3 スタンダートレートが必要です。ストレージクラスの詳細については、「Amazon S3 ストレージクラス」を参照してください。

S3 One Zone-IA (ONEZONE_IA) と S3 Express One Zone (EXPRESS_ONEZONE) を除くすべてのストレージクラスは、災害によるアベイラビリティーゾーンの物理的な損失に対して回復力を持つように設計されていることに注意します。また、アプリケーションシナリオのパフォーマンス要件の他に、コストについても考慮してください。ストレージクラスの料金については「Amazon S3 の料金」をご覧ください。

オブジェクトのストレージクラスを設定

オブジェクトをアップロードするときに、そのオブジェクトのストレージクラスを指定できます。そうでない場合は、Amazon S3 は汎用バケットのオブジェクトにデフォルトの Amazon S3 Standard

ストレージクラスを使用します。Amazon S3 汎用バケットに既に保存されているオブジェクトのストレージクラスを、Amazon S3 コンソール、AWS SDK、AWS Command Line Interface (AWS CLI) を使用して他のストレージクラスに変更することもできます。これらのアプローチはすべて、Amazon S3 API オペレーションを使用して Amazon S3 にリクエストを送信します。

> **Note**
>
> ディレクトリバケットに保存されているオブジェクトのストレージクラスを変更することはできません。

バケットに S3 ライフサイクル設定を追加すると、Amazon S3 がオブジェクトのストレージクラスを自動的に変更します。詳細については、「オブジェクトのライフサイクルの管理」を参照してください。

S3 レプリケーションを設定する場合、レプリケートされたオブジェクトのストレージクラスを別のストレージクラスに設定できます。ただし、S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive ストレージクラスに保存されているオブジェクトをレプリケートすることはできません。詳細については、「レプリケーション設定ファイル要素」を参照してください。

ストレージクラスをプログラムで設定する場合、ストレージクラスの値を指定します。以下は、ストレージクラスのコンソール名と対応する API 値のリストです。

- 低冗長ストレージ – `REDUCED_REDUNDANCY`
- S3 Express One Zone – `EXPRESS_ONEZONE`
- S3 Glacier Deep Archive – `DEEP_ARCHIVE`
- S3 Glacier Flexible Retrieval – `GLACIER`
- S3 Glacier Instant Retrieval – `GLACIER_IR`
- S3 Intelligent-Tiering – `INTELLIGENT_TIERING`
- S3 One Zone-IA – `ONEZONE_IA`
- S3 Standard – `STANDARD`
- S3 Standard-IA – `STANDARD_IA`

新しいオブジェクトのストレージクラスを設定

オブジェクトをアップロードするときにストレージクラスを設定するには、次の方法を使用できます。

S3 コンソールの使用

コンソールで新しいオブジェクトをアップロードするときにストレージクラスを設定するには

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 左のナビゲーションペインで、[汎用バケット] を選択します。
3. バケットリストで、フォルダやファイルのアップロード先のバケットの名前を選択します。
4. [Upload (アップロード)] を選択します。
5. [アップロード] ウィンドウで、[プロパティ] を選択します。
6. [ストレージクラス] で、アップロードするファイルのストレージクラスを選択します。
7. (オプション) アップロードするファイルの追加のプロパティを設定します。詳細については、「オブジェクトのアップロード」を参照してください。
8. [Upload] (アップロード) ウィンドウで、次のいずれかの操作を行います。
   - ファイルとフォルダを [アップロード] ウィンドウにドラッグします。
   - [ファイルの追加] または [フォルダの追加] を選択し、アップロードするファイルまたはフォルダを選択して [開く] を選択します。
9. ページの最下部で [アップロード] をクリックします。

REST API の使用

PutObject、POST Object オブジェクト、および CreateMultipartUpload API オペレーションを使用してオブジェクトを作成するときに、オブジェクトのストレージクラスを指定し、x-amz-storage-class リクエストヘッダーを追加できます。このヘッダーを追加しない場合は、Amazon S3 では、デフォルトのストレージクラスである S3 Standard (STANDARD) を使用します。

このリクエスト例では、PutObject コマンドを使用して新しいオブジェクトのストレージクラスを S3 Intelligent-Tiering に設定します。

```
PUT /my-image.jpg HTTP/1.1
Host: amzn-s3-demo-bucket1.s3.Region.amazonaws.com
Date: Wed, 12 Oct 2009 17:50:00 GMT
Authorization: authorization string
Content-Type: image/jpeg
Content-Length: 11434
Expect: 100-continue
```

```
x-amz-storage-class: INTELLIGENT_TIERING
```

AWS CLI を使用する場合

この例では、put-object コマンドを使用して、*GLACIER* ストレージクラスの *my_images.tar.bz2* を *amzn-s3-demo-bucket1* にアップロードします。

```
aws s3api put-object --bucket amzn-s3-demo-bucket1 --key dir-1/my_images.tar.bz2 --
storage-class GLACIER --body my_images.tar.bz2
```

オブジェクトサイズが 5 GB を超える場合は、次のコマンドを使用してストレージクラスを設定します。

```
aws s3 cp large_test_file s3://amzn-s3-demo-bucket1 --storage-class GLACIER
```

既存のオブジェクトのストレージクラスの変更

オブジェクトをアップロードするときにストレージクラスを設定するには、次の方法を使用します。

S3 コンソールの使用

オブジェクトのサイズが 5 GB 未満の場合は、Amazon S3 コンソールを使用してオブジェクトのストレージクラスを変更できます。それ以上大きい場合は、S3 Lifecycle の設定を追加すると、オブジェクトのストレージクラスを変更できます。

コンソールでオブジェクトのストレージクラスを変更するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[汎用バケット] を選択します。
3. バケットリストで、変更するオブジェクトが含まれるバケットの名前を選択します。
4. 変更するオブジェクトの名前の左にあるチェックボックスをオンにします。
5. [アクション] メニューに表示されるオプションのリストから [ストレージクラスの編集] を選択します。

6. オブジェクトで使用できるストレージクラスから選択します。
7. [追加のコピー設定] で、[ソース設定をコピー] するか、[設定を指定しない] か、[設定を指定] するかを選択します。[ソース設定をコピー] がデフォルトのオプションです。ソース設定の属性なしでオブジェクトのみをコピーする場合は、[設定を指定しない] を選択します。ストレージクラス、ACL、オブジェクトタグ、メタデータ、サーバー側の暗号化、その他のチェックサムの設定を指定するには、[設定を指定] を選択します。
8. 右下の [変更の保存] を選択します。Amazon S3 は変更を保存します。

REST API の使用

既存のオブジェクトのストレージクラスを変更するには、次の方法を使用します。

このリクエスト例では、PutObject コマンドを使用して既存のオブジェクトのストレージクラスを S3 Intelligent-Tiering に設定します。

```
PUT /my-image.jpg HTTP/1.1
Host: amzn-s3-demo-bucket1.s3.Region.amazonaws.com
Date: Wed, 12 Oct 2009 17:50:00 GMT
Authorization: authorization string
Content-Type: image/jpeg
Content-Length: 11434
Expect: 100-continue
x-amz-storage-class: INTELLIGENT_TIERING
```

AWS CLI を使用する場合

この例では、cp コマンドを使用して、既存のオブジェクトのストレージクラスを現在のストレージクラスから *DEEP_ARCHIVE* ストレージクラスに変更します。

```
aws s3 cp object_S3_URI object_S3_URI --storage-class DEEP_ARCHIVE
```

アクセスポリシーのアクセス許可を特定のストレージクラスに制限する

Amazon S3 オペレーションのアクセスポリシーアクセス許可を付与する場合、s3:x-amz-storage-class 条件キーを使用して、アップロードされたオブジェクトを保存するときに使用す

るストレージクラスを制限できます。例えば、`s3:PutObject` アクセス許可を付与すると、オブジェクトのアップロードを特定のストレージクラスに制限できます。ポリシーの例については例: オブジェクトのアップロードを特定のストレージクラスのオブジェクトに制限するを参照してください。

ポリシーでの条件の使用方法および Amazon S3 条件キーの完全なリストについては、以下のトピックを参照してください。

- 「サービス認可リファレンス」の「Actions, resources, and condition keys for Amazon S3」を参照してください。

  S3 リソースタイプ別の S3 API オペレーションへのアクセス許可の詳細については、「Amazon S3 API オペレーションに必要なアクセス許可」を参照してください。
- 条件キーを使用したバケットポリシーの例

Amazon S3 分析 – ストレージクラス分析

Amazon S3 分析のストレージクラス分析を使用することにより、ストレージアクセスパターンを分析し、適切なデータをいつ適切なストレージクラスに移行すべきかを判断できます。この新しい Amazon S3 分析機能は、アクセス頻度の低い STANDARD ストレージをいつ STANDARD_IA (IA: 低頻度アクセス) ストレージクラスに移行すべきかを判断できるように、データアクセスパターンを確認します。ストレージクラスの詳細については、「Amazon S3 ストレージクラスの理解と管理」を参照してください。

ストレージクラス分析が、フィルタリングされたデータセットの低頻度アクセスパターンを一定期間監視すると、分析結果を使用してライフサイクル設定を改善できます。ストレージクラス分析を設定し、バケット内のすべてのオブジェクトを分析できます。または、共通のプレフィックス (つまり、共通の文字列で始まる名前を持つオブジェクト)、オブジェクトタグ、プレフィックスとタグの両方によってオブジェクトを分析のためにグループ化するフィルターを設定できます。多くの場合、ストレージクラス分析を有効活用するには、オブジェクトグループによるフィルタリングが最適な方法です。

> **Important**
>
> ストレージクラス分析では、標準 ~ 標準 IA クラスのレコメンデーションのみが提供されます。

バケットあたり複数のストレージクラス分析フィルター (最大 1,000 個) を設定でき、フィルターごとに別個の分析を受け取ります。複数のフィルター設定を使用すると、オブジェクトの特定のグループを分析し、オブジェクトを STANDARD_IA に移行するライフサイクル設定を改善できます。

ストレージクラス分析では、Amazon S3 コンソールにストレージの使用状況が可視化され、毎日更新されます。この毎日の使用状況データを S3 バケットにエクスポートし、スプレッドシートアプリケーションやビジネスインテリジェンスツール (QuickSight など) で表示することもできます。

ストレージクラスの分析に関連するコストがあります。料金については、「管理とインサイト」および「Amazon S3 の料金」を参照してください。

トピック

- ストレージクラス分析をセットアップする方法
- ストレージクラス分析を使用する方法
- ストレージクラス分析データをエクスポートする方法
- ストレージクラス分析の設定

ストレージクラス分析をセットアップする方法

ストレージクラス分析は、分析するオブジェクトを設定することによりセットアップできます。ストレージクラス分析で以下の処理が行われるように設定できます。

- バケットのコンテンツ全体を分析する。

  バケット内のすべてのオブジェクトの分析を受け取ります。
- プレフィックスとタグによってグループ化されたオブジェクトを分析する。

  プレフィックス、オブジェクトタグ、プレフィックスとタグの組み合わせによってオブジェクトを分析のためにグループ化するフィルターを設定できます。設定したフィルターごとに別個の分析を受け取ります。バケットあたり複数のフィルター (最大 1,000 個) を設定できます。
- 分析データをエクスポートする。

  バケットまたはフィルターのストレージクラス分析を設定するとき、分析データを毎日ファイルにエクスポートすることを選択できます。その日の分析がファイルに追加され、構成されたフィルターの履歴分析ログが形成されます。ファイルは、選択したエクスポート先で毎日更新されます。データのエクスポートを選択した場合、ファイルが書き込まれるエクスポート先バケットとオプションのエクスポート先プレフィックスを指定します。

Amazon S3 コンソール、REST API、AWS CLI、または AWS SDK を使用して、ストレージクラス分析を設定できます。

- Amazon S3 コンソールでストレージクラス分析を設定する方法については、「ストレージクラス分析の設定」を参照してください。
- Amazon S3 API を使用するには、AWS CLI または AWS SDK から PutBucketAnalyticsConfiguration REST API または同等の API を使用します。

ストレージクラス分析を使用する方法

データアクセスパターンを一定期間監視し、STANDARD_IA ストレージのライフサイクル管理の改善に役立つ情報を収集するには、ストレージクラス分析を使用します。フィルターを設定すると、フィルターに基づくデータ分析が 24 ~ 48 時間 Amazon S3 コンソールに表示され始め続けます。ただし、ストレージクラス分析はフィルタリングされたデータセットのアクセスパターンを 30 日以上監視し、分析のために情報を収集してから結果を生成します。最初の結果の後も分析は実行され続け、アクセスパターンが変わると結果が更新されます。

最初にフィルターを設定するとき、Simple Storage Service (Amazon S3) コンソールではデータの分析に時間がかかることがあります。

ストレージクラス分析は、フィルタリングされたオブジェクトデータセットのアクセスパターンを 30 日以上監視し、分析のために十分な情報を収集します。ストレージクラス分析が十分な情報を収集した後、Amazon S3 コンソールに分析の完了を示すメッセージが表示されます。

アクセス頻度の低いオブジェクトの分析を実行すると、ストレージクラス分析は、Amazon S3 にアップロードされてからの経過時間に基づいてグループ化された、フィルタリングされたオブジェクトセットを監視します。ストレージクラス分析は、フィルタリングされたデータセットの以下の要素を監視することで、経過時間グループのアクセス頻度が低いかどうかを判断します。

- STANDARD ストレージクラス内の 128 KB を超えるオブジェクト。
- 経過時間グループごとの合計ストレージ量の平均。
- 経過時間グループごとの平均転送 (アウト) バイト数 (頻度ではありません)。
- 分析のエクスポートデータには、ストレージクラスの分析に関連するデータのリクエストのみが含まれます。これにより、リクエストの数、および合計アップロードバイト数およびリクエストバイト数と、ストレージメトリクスで表示される数またはお客様独自の内部システムによって追跡される値との比較で違いが生じる可能性があります。
- 失敗した GET および PUT リクエストは分析でカウントされません。ただし、ストレージメトリクスには失敗したリクエストが含まれます。

取得したストレージの量。

Amazon S3 コンソールでは、フィルタリングされたデータセット内で観察期間内に取得されたストレージの量がグラフ化されます。

取得したストレージの割合。

Amazon S3 コンソールでは、フィルタリングされたデータセット内で観察期間内に取得されたストレージの割合もグラフ化されます。

このトピックですでに述べたように、アクセス頻度の低いオブジェクトの分析を実行すると、ストレージクラス分析は、Amazon S3 にアップロードされてからの経過時間に基づいてグループ化された、フィルタリングされたオブジェクトセットを監視します。ストレージクラス分析は、以下の定義済みオブジェクト経過時間グループを使用します。

- 15 日未満経過の Amazon S3 オブジェクト
- 15 ~ 29 日経過の Amazon S3 オブジェクト
- 30 ~ 44 日経過の Amazon S3 オブジェクト
- 45 ~ 59 日経過の Amazon S3 オブジェクト
- 60 ~ 74 日経過の Amazon S3 オブジェクト
- 75 ~ 89 日経過の Amazon S3 オブジェクト
- 90 ~ 119 日経過の Amazon S3 オブジェクト
- 120 ~ 149 日経過の Amazon S3 オブジェクト
- 150 ~ 179 日経過の Amazon S3 オブジェクト
- 180 ~ 364 日経過の Amazon S3 オブジェクト
- 365 ~ 729 日経過の Amazon S3 オブジェクト
- 730 日以上経過の Amazon S3 オブジェクト

通常は、分析結果の生成に十分な情報を収集するには、アクセスパターンの監視に約 30 日かかります。データ独自のアクセスパターンによっては、30 日より長くかかることもあります。ただし、フィルターを設定すると、フィルターに基づくデータ分析が 24 ~ 48 時間 Amazon S3 コンソールに表示され始め続けます。Amazon S3 コンソールでは、オブジェクト経過時間グループごとに分けられたオブジェクトアクセスの分析を毎日確認できます。

アクセス頻度の低いストレージの量。

Amazon S3 コンソールには、事前定義されたオブジェクトの経過時間グループごとにアクセスパターンがグループ分けされて表示されます。表示される [アクセスが頻繁] または [アクセスが頻繁ではない] というテキストは、ライフサイクルの作成プロセスに役立つ視覚補助として提供されています。

ストレージクラス分析データをエクスポートする方法

ストレージクラス分析が分析レポートをカンマ区切り値 (CSV) フラットファイルにエクスポートすることを選択できます。レポートは毎日更新され、設定したオブジェクト経過時間グループフィルターに基づいています。Amazon S3 コンソールを使用すると、フィルターの作成時にレポートのエクスポートオプションを選択できます。データのエクスポートを選択した場合、ファイルが書き込まれるエクスポート先バケットとオプションのエクスポート先プレフィックスを指定します。データは、別のアカウントのエクスポート先バケットにエクスポートできます。エクスポート先バケットは、分析対象として設定したバケットと同じリージョンにある必要があります。

AWS アカウント がバケットを所有していることを確認し、定義された場所にあるバケットにオブジェクトを書き込むには、Amazon S3 への許可を付与するバケットポリシーをエクスポート先バケットで作成する必要があります。ポリシーの例については、「S3 インベントリおよび S3 分析に対するアクセス許可の付与」を参照してください。

ストレージクラス分析レポートを設定すると、24 時間後からエクスポートされたレポートが毎日生成され始めます。その後、Amazon S3 はモニタリングを続けて、エクスポートを毎日行います。

CSV ファイルは、スプレッドシートアプリケーションで開くか、Amazon QuickSight など、他のアプリケーションにインポートできます。Amazon QuickSight での Amazon S3 ファイルの使用については、Amazon QuickSight ユーザーガイドの「Create a Data Set Using Amazon S3 Files」を参照してください。

エクスポートされたファイルのデータは、次の例に示すように、オブジェクトの経過時間グループ内の日付でソートされます。ストレージクラスが STANDARD の場合、行には `ObjectAgeForSIATransition` 列と `RecommendedObjectAgeForSIATransition` 列のデータも含まれます。

Date	ConfigId	Filter	StorageClass	ObjectAge	ObjectCount	DataUploaded_MB	Storage_MB	DataRetrieved_MB	GetRequestCount	CumulativeAccessRatio	ObjectAgeForSIATransition	RecommendedObjectAgeForSIATransition
8/17/2021	SalesMaterial	SalesMaterial	STANDARD	000-014			0.4313			0		
9/2/2021	SalesMaterial	SalesMaterial	STANDARD	000-014						0.04096734		
8/22/2021	SalesMaterial	SalesMaterial	STANDARD	000-014			0.4313			0		
8/25/2021	SalesMaterial	SalesMaterial	STANDARD	000-014			0.4313			0		
9/6/2021	SalesMaterial	SalesMaterial	STANDARD	000-014						0.04096734		
8/30/2021	SalesMaterial	SalesMaterial	STANDARD	000-014						0.04096734		
8/28/2021	SalesMaterial	SalesMaterial	STANDARD	000-014						0.04096734		
8/21/2021	SalesMaterial	SalesMaterial	STANDARD	000-014			0.4313			0		
9/5/2021	SalesMaterial	SalesMaterial	STANDARD	000-014						0.04096734		

レポートの最後に、オブジェクトの経過時間グループが ALL として示されます。ALL 行には、その日のすべての経過時間グループの累計 (128 KB 未満のオブジェクトを含む) が表示されます。

8/24/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3	0.4599		0	000-014
9/3/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3	0.4599		0.02426125	015-029
8/28/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3	0.4599		0.03545875	015-029
8/17/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3	0.4599		0	000-014
8/25/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3	0.4599		0	000-014
9/6/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3	0.4599		0.0209529	015-029
9/4/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3	0.4599		0.02304819	015-029
8/22/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3	0.4599		0	000-014
8/21/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3	0.4599		0	000-014
8/30/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3	0.4599		0.03073092	015-029
8/20/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3	0.4599		0	000-014

次のセクションでは、レポートで使用される列について説明します。

エクスポートされたファイルのレイアウト

次の表は、Amazon S3 ストレージクラス分析エクスポートファイルレイアウトを示しています。

ストレージクラス分析の設定

Amazon S3 分析のストレージクラス分析ツールを使用することにより、ストレージアクセスパターンを分析し、適したデータをいつ適切なストレージクラスに移行すべきかを判断できます。ストレージクラス分析では、アクセス頻度の低い STANDARD ストレージをいつ STANDARD_IA (IA: 低頻度アクセス) ストレージクラスに移行すべきかを判断できるように、データアクセスパターンを確認します。STANDARD_IA の詳細については、Amazon S3 のよくある質問と「Amazon S3 ストレージクラスの理解と管理」を参照してください。

ストレージクラス分析は、分析するオブジェクトを設定することによりセットアップできます。ストレージクラス分析で以下の処理が行われるように設定できます。

- バケットのコンテンツ全体を分析する。

  バケット内のすべてのオブジェクトの分析を受け取ります。

- プレフィックスとタグによってグループ化されたオブジェクトを分析する。

  プレフィックス、オブジェクトタグ、プレフィックスとタグの組み合わせによってオブジェクトを分析のためにグループ化するフィルターを設定できます。設定したフィルターごとに別個の分析を受け取ります。バケットあたり複数のフィルター (最大 1,000 個) を設定できます。

- 分析データをエクスポートする。

  バケットまたはフィルターのストレージクラス分析を設定するとき、分析データを毎日ファイルにエクスポートすることを選択できます。その日の分析がファイルに追加され、構成されたフィルターの履歴分析ログが形成されます。ファイルは、選択したエクスポート先で毎日更新されます。データのエクスポートを選択した場合、ファイルが書き込まれるエクスポート先バケットとオプションのエクスポート先プレフィックスを指定します。

Amazon S3 コンソール、REST API、AWS CLI、または AWS SDK を使用して、ストレージクラス分析を設定できます。

> **Important**
>
> ストレージクラス分析では、ONEZONE_IA または S3 Glacier Flexible Retrieval ストレージクラスへの移行に関するレコメンデーションを提供しません。
> 検出結果を .csv ファイルとしてエクスポートするようにストレージクラス分析を設定し、送信先バケットで AWS KMS key でデフォルトのバケット暗号化を使用する場合は、AWS KMS キーポリシーを更新して Amazon S3 に .csv ファイルを暗号化するための許可を付与する必要があります。手順については、「カスタマーマネージドキーを暗号化に使用するためのアクセス許可を Amazon S3 に付与する」を参照してください。

分析の詳細については、「Amazon S3 分析 – ストレージクラス分析」を参照してください。

S3 コンソールの使用

ストレージクラス分析を設定するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[汎用バケット] または [ディレクトリバケット] を選択します。
3. バケットリストで、ストレージクラス分析を設定するバケットの名前を選択します。
4. [Metrics] タブを選択します。
5. [Storage Class Analysis (ストレージクラス分析)] で、[Create analytics configuration (分析構成の作成)] を選択します。
6. フィルターの名前を入力します。バケット全体を分析する場合は、[Prefix (プレフィックス)] フィールドを空のままにします。
7. [Prefix (プレフィックス)] フィールドに、分析するオブジェクトの接頭辞のテキストを入力します。
8. タグを追加するには、[タグの追加] を選択します。タグのキーと値を入力します。1 つのプレフィックスと複数のタグを入力できます。
9. 必要に応じて、[CSV のエクスポート] で [有効化] を選択して、分析レポートをカンマ区切り値 (.csv) フラットファイルにエクスポートできます。ファイルを保存できる保存先のバケットを選択します。保存先バケットのプレフィックスを入力できます。ターゲットバケットは、分析を

セットアップするバケットと同じ AWS リージョン にある必要があります。ターゲットバケットは、別の AWS アカウント にある場合があります。

.csv ファイルの送信先バケットで KMS キーでデフォルトのバケット暗号化を使用する場合は、AWS KMS キーポリシーを更新して、Amazon S3 に .csv ファイルを暗号化するための許可を付与する必要があります。手順については、「カスタマーマネージドキーを暗号化に使用するためのアクセス許可を Amazon S3 に付与する」を参照してください。

10. [Create Configuration (設定の作成)] を選択します。

Amazon S3 は、Amazon S3 に書き込みアクセス許可を付与するバケットポリシーをターゲットバケットで作成します。これにより、バケットにエクスポート データを書き込むことができます。

バケットポリシーを作成しようとしたときにエラーが発生した場合、解決するための手順が表示されます。例えば、別の AWS アカウント 内のターゲットバケットを選択したが、バケットポリシーの読み書きを行う許可がない場合、次のメッセージが表示されます。ターゲットバケットの所有者に表示されたバケットポリシーをターゲットバケットに追加してもらう必要があります。ポリシーがターゲットバケットに追加されない場合、Amazon S3 にはターゲットバケットに書き込むアクセス許可がないため、エクスポートデータを取得できません。ソースバケットが現在のユーザー以外のアカウントによって所有されている場合、ポリシーでソースバケットの正しいアカウント ID に置き換える必要があります。

エクスポートされたデータとフィルターの動作の仕組みについては、「Amazon S3 分析 – ストレージクラス分析」を参照してください。

REST API の使用

REST API を使用してストレージクラス分析を設定するには、 PutBucketAnalyticsConfiguration を使用します。AWS CLI または AWS SDK で同等のオペレーションを使用することもできます。

次の REST API を使用してストレージクラス分析を操作できます。

- DELETE バケット分析設定
- GET バケット分析設定
- List バケット分析設定

Amazon S3 Intelligent-Tiering によるストレージコストの管理

S3 Intelligent-Tiering ストレージクラスは、アクセスパターンが変化した際に、オペレーション上のオーバーヘッドやパフォーマンスへの影響を排除し、データを最もコスト効率の高いアクセス層に自動的に移動させることで、ストレージコストを最適化するように設計されています。オブジェクトのモニタリングとオートメーションに対して発生する少額の月額料金で、S3 Intelligent-Tiering はアクセスパターンをモニタリングし、あまりアクセスされていないオブジェクトをより低コストのアクセス階層へ自動的に移動させることができます。

S3 Intelligent-Tiering は、3 つの低レイテンシーかつ高スループットのアクセス階層で、自動ストレージコスト削減を実現します。非同期でアクセスできるデータの場合は、S3 Intelligent-Tiering ストレージクラスで自動アーカイブ機能をアクティブ化することもできます。S3 Intelligent-Tiering には取り出し料金は発生しません。低頻度のアクセス階層または Archive Instant Access 階層にあるオブジェクトに後からアクセスすると、自動的に高頻度のアクセス階層に戻されます。S3 Intelligent-Tiering ストレージクラスのアクセス階層間でオブジェクトを移動させるときに追加の階層化料金は発生しません。

S3 Intelligent-Tiering は、データレイク、データ分析、新しいアプリケーションなど、オブジェクトのサイズや保持期間に関係なく、アクセスパターンが不明、変更される、または予測不可能なデータに対して推奨されるストレージクラスです。

S3 Intelligent-Tiering ストレージクラスは、以下を含む Amazon S3 のすべての機能をサポートします。

- オブジェクトのアクセス層を検証する S3 インベントリ
- データを任意の AWS リージョン にレプリケートする S3 レプリケーション
- S3 Storage Lens でのストレージの使用状況とアクティビティに関するメトリクスの表示
- オブジェクトデータ保護のためのサーバー側の暗号化
- データを誤って削除しないようにする S3 オブジェクトロック
- 仮想プライベートクラウド (VPC) のプライベートエンドポイントを介して Amazon S3 にアクセスするための AWS PrivateLink

S3 Intelligent-Tiering の使用方法については、以下のセクションを参照してください。

トピック

- S3 Intelligent-Tiering の仕組み

- S3 Intelligent-Tiering の使用
- S3 Intelligent-Tiering の管理

S3 Intelligent-Tiering の仕組み

Amazon S3 Intelligent-Tiering ストレージクラスは、3 つのアクセス階層に自動的にオブジェクトを保存します。1 つの階層は高頻度アクセス用に最適化され、1 つの低コスト階層は低頻度アクセス用に最適化されます。またもう 1 つの極めてコストの低い階層は、ほとんどアクセスされていないデータに最適化されます。オブジェクトのモニタリングおよびオートメーションにかかる月額料金を抑えるために、S3 Intelligent-Tiering はアクセスパターンをモニタリングし、30 日間連続してアクセスがなかったオブジェクトを、低頻度アクセス階層に自動的に移動します。90 日間アクセスされていない場合に、オブジェクトはパフォーマンスへの影響や運用上のオーバーヘッドなしで、アーカイブインスタントアクセス階層に移動されます。

数分から数時間でアクセスできるデータのストレージコストを最小限に抑えるには、アーカイブ機能を有効にして 2 つのアクセス階層を追加します。オブジェクトをアーカイブアクセス階層、ディープアーカイブアクセス階層、またはその両方に階層を下げることができます。アーカイブアクセスにより、S3 Intelligent-Tiering は 90 日間以上連続してアクセスされていないオブジェクトをアーカイブアクセス階層に移動します。ディープアーカイブアクセスにより、S3 Intelligent-Tiering は 180 日間以上連続してアクセスされていないオブジェクトをディープアーカイブアクセス階層に移動します。どちらの階層でも、必要に応じて非アクセス日数を設定できます。

以下のアクションによるアクセスでは、オブジェクトが下位のアーカイブアクセス階層やディープアーカイブアクセス階層に移動されません。

- Amazon S3 コンソールを通じてオブジェクトをダウンロードまたはコピーする。
- CopyObject または UploadPartCopy を呼び出すか、S3 バッチレプリケーションでオブジェクトをレプリケートする。これらの場合、コピーやレプリケーションオペレーションのソースオブジェクトは上位の階層に移動されます。
- GetObject、PutObject、RestoreObject、CompleteMultipartUpload、ListParts、または SelectObjectContent を呼び出す。

例えば、指定した非アクセス日数 (180 日など) より前に `SelectObjectContent` を通じてオブジェクトがアクセスされると、そのアクションによりタイマーがリセットされます。最後の `SelectObjectContent` リクエストが、指定した日数に達するまでは、オブジェクトはアーカイブアクセス階層またはディープアーカイブアクセス階層に移動しません。

低頻度アクセス階層またはアーカイブインスタントアクセス階層にあるオブジェクトに後からアクセスすると、自動的に高頻度アクセス階層に戻されます。

以下のアクションは、オブジェクトを低頻度アクセス階層やアーカイブインスタントアクセス階層から高頻度アクセス階層に自動的に戻すアクセスを構成します。

- Amazon S3 コンソールを通じてオブジェクトをダウンロードまたはコピーする。
- CopyObject または UploadPartCopy を呼び出すか、バッチレプリケーションでオブジェクトをレプリケートする。これらの場合、コピーやレプリケーションオペレーションのソースオブジェクトは上位の階層に移動されます。
- GetObject、PutObject、RestoreObject、CompleteMultipartUpload、または ListParts を呼び出す。

他のアクションは、オブジェクトを低頻度アクセス階層やアーカイブインスタントアクセス階層から高頻度アクセス階層に自動的に戻すアクセスを構成しません。次に示すのは、そのようなアクションのリストのサンプルであり、決定的なものではありません。

- HeadObject、GetObjectTagging、PutObjectTagging、ListObjects、ListObjectsV2、または ListObjectVersions を呼び出す。
- SelectObjectContent の呼び出しは、オブジェクトを上位の高頻度アクセス階層に移動するアクセスを構成しません。また、高頻度アクセス階層から低頻度アクセス階層へのオブジェクトの移動、さらにアーカイブインスタントアクセス階層への移動を妨げません。

S3 Intelligent-Tiering を新しく作成されたデータのデフォルトのストレージクラスとして使用するには、`PutObject`、`CopyObject`、または `CreateMultipartUpload` オペレーションを呼び出すときに `x-amz-storage-class` リクエストヘッダーで `INTELLIGENT-TIERING` を指定します。S3 Intelligent-Tiering は、99.9% の可用性と99.999999999% の耐久性を実現するように設計されています。

> **Note**
>
> オブジェクトのサイズが 128 KB 未満の場合は、モニタリングされず、自動階層化に適していません。小さいオブジェクトは必ず高頻度アクセス階層に保存されます。

S3 Intelligent-Tiering アクセス階層

次のセクションでは、さまざまな自動アクセス階層とオプションのアクセス階層について説明します。オブジェクトがアクセス階層間を移動しても、ストレージクラス (S3 Intelligent-Tiering) は変わりません。

高頻度アクセス階層 (自動)

これは、S3 Intelligent-Tiering で作成されたオブジェクトや S3 Intelligent-Tiering に移行したオブジェクトのライフサイクルを開始するデフォルトのアクセス階層です。オブジェクトは、アクセスされている限り、この階層に残ります。高頻度アクセス階層は、低レイテンシーと高スループットのパフォーマンスを提供します。

低頻度アクセス階層 (自動)

オブジェクトが 30 日間連続してアクセスされない場合、オブジェクトは低頻度アクセス階層に移行します。低頻度アクセス階層は、低レイテンシーと高スループットのパフォーマンスを提供します。

アーカイブインスタントアクセス階層 (自動)

オブジェクトが 90 日間連続してアクセスされない場合、オブジェクトはアーカイブインスタントアクセス階層に移行します。アーカイブインスタントアクセス階層は、低レイテンシーと高スループットのパフォーマンスを提供します。

アーカイブアクセス階層 (オプション)

S3 Intelligent-Tiering では、非同期的にアクセスできるデータのためにアーカイブアクセス層をアクティブ化するオプションが提供されます。アクティブ化された後、アーカイブアクセス階層は 90 日間以上してアクセスされなかったオブジェクトを自動的にアーカイブします。アーカイブの最終アクセス時間は、最大 730 日間まで延長できます。アーカイブアクセス階層は、S3 Glacier Flexible Retrieval ストレージクラスと同じパフォーマンスです。

このアクセス階層の標準取得時間は、3 ~ 5 時間の範囲です。S3 バッチオペレーションを使用して復元リクエストを開始した場合、復元は数分以内に開始されます。取り出しオプションの詳細については、「the section called “S3 Intelligent-Tiering アーカイブアクセス階層からのオブジェクトの復元”」を参照してください。

> **Note**
>
> アーカイブインスタントアクセス階層をバイパスしたい場合は、アーカイブアクセス階層を 90 日間だけアクティブ化します。アーカイブアクセス階層は、数分から数時間の取得

時間により、ストレージコストをわずかに削減します。アーカイブインスタントアクセス階層は、ミリ秒単位のアクセスと高いスループットパフォーマンスを実現します。

ディープアーカイブアクセス階層（オプション）

S3 Intelligent-Tiering では、非同期的にアクセスできるデータのために ディープアーカイブアクセス階層をアクティブ化するオプションが提供されます。アクティブ化後、ディープアーカイブアクセス階層は 180 日間連続してアクセスされなかったオブジェクトを自動的にアーカイブします。アーカイブの最終アクセス時間は、最大 730 日間まで延長できます。ディープアーカイブアクセス階層のパフォーマンスは、S3 Glacier Deep Archive ストレージクラスと同じです。

このアクセス層のオブジェクトの標準取得は、12 時間以内に行われます。S3 バッチオペレーションを使用して復元リクエストを開始した場合、復元は 9 時間以内に開始されます。取り出しオプションの詳細については、「the section called “S3 Intelligent-Tiering アーカイブアクセス階層からのオブジェクトの復元”」を参照してください。

> **Note**
>
> アプリケーションがオブジェクトに非同期でアクセスできる場合にのみ、アーカイブアクセス階層とディープアーカイブアクセス階層をアクティブにします。取得するオブジェクトがアーカイブアクセス階層またはディープアーカイブアクセス階層に保存されている場合は、まず `RestoreObject` オペレーションを使用してオブジェクトを復元する必要があります。

S3 Intelligent-Tiering の使用

S3 Intelligent-Tiering ストレージクラスを使用すると、ストレージコストを自動的に最適化できます。S3 Intelligent-Tiering は、アクセスパターンが変更されたときに、アクセス階層間で、細かなオブジェクトレベルでデータを移動することにより、自動的にコスト削減を実現します。非同期でアクセスできるデータの場合は、AWS Management Console、AWS CLI、または Amazon S3 API を使用して、S3 Intelligent-Tiering ストレージクラスで自動アーカイブ機能をアクティブ化することもできます。

S3 Intelligent-Tiering へのデータの移行

S3 Intelligent-Tiering にデータを移動するには、2つの方法があります。オブジェクトは、コンソールから S3 Intelligent-Tiering に直接アップロードすることも、PUT オペレーションを使用してプログラ

ムでアップロードすることもできます。詳細については、「オブジェクトのストレージクラスを設定」を参照してください。S3 Standard または S3 標準頻度から S3 Intelligent-Tiering にオブジェクトを移動させるように S3 ライフサイクル設定を設定することもできます。

Direct Put を使用した S3 Intelligent-Tiering へのデータのアップロード

PUT API オペレーションを使用して S3 Intelligent-Tiering ストレージクラスにオブジェクトをアップロードする場合、`x-amz-storage-class` リクエストヘッダーで S3 Intelligent-Tiering を指定します。

次のリクエストは、イメージ、`my-image.jpg` を `myBucket` バケットに保存します。このリクエストでは、`x-amz-storage-class` ヘッダーを使用して、オブジェクトが S3 Intelligent-Tiering ストレージクラスを使用して保存されるようにリクエストできます。

Example

```
PUT /my-image.jpg HTTP/1.1
Host: myBucket.s3.<Region>.amazonaws.com (http://amazonaws.com/)
Date: Wed, 1 Sep 2021 17:50:00 GMT
Authorization: authorization string
Content-Type: image/jpeg
Content-Length: 11434
Expect: 100-continue
x-amz-storage-class: INTELLIGENT_TIERING
```

S3 ライフサイクルを使用した S3 標準または S3 Standard-低頻度アクセスから S3 Intelligent-Tiering へのデータの移行

S3 ライフサイクルの設定にルールを追加して、オブジェクトをあるストレージクラスから別のストレージクラスに移行するように Amazon S3 に指示することができます。サポートされている移行および関連する制約の詳細については、「S3 ライフサイクルを使用したオブジェクトの移行」を参照してください。

S3 ライフサイクル設定は、バケットレベルまたはプレフィックスレベルで指定できます。この S3 ライフサイクル設定ルールでは、フィルターはキープレフィックス (`documents/`) を指定しています。したがって、ルールは、キー名プレフィックスが `documents/` のオブジェクト (`documents/doc1.txt`、`documents/doc2.txt` など) に適用されます。このルールは、作成から 0 日後にオブジェクトを S3 Intelligent-Tiering ストレージクラスに移行するように Amazon S3 に指示する `Transition` アクションを指定します。この場合、オブジェクトは、作成後の午前 0 時 (UTC) に S3 Intelligent-Tiering に移行できます。

Example

```
<LifecycleConfiguration>
  <Rule>
    <ID>ExampleRule</ID>
    <Filter>
       <Prefix>documents/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>INTELLIGENT_TIERING</StorageClass>
    </Transition>
 </Rule>
</LifecycleConfiguration>
```

バケットのバージョニングが有効になっている場合は、最新のオブジェクトバージョン 1 個と、0 個以上の以前のバージョンが維持されます。現在のオブジェクトバージョンと以前のオブジェクトバージョン用に異なるライフサイクルルールを定義できます。

詳細については、「ライフサイクル設定の要素」を参照してください。

S3 Intelligent-Tiering のアーカイブアクセスおよびディープアーカイブアクセスの有効化

数分から数時間でアクセス可能なデータのストレージコストを最低限に抑えるには、AWS Management Console、AWS CLI、または Amazon S3 API を使用してバケットレベル、プレフィックスレベル、またはオブジェクトタグレベルの設定を作成することで、アーカイブアクセス階層の 1 つまたは両方を有効にすることができます。

S3 コンソールの使用

S3 Intelligent-Tiering 自動アーカイブを有効にするには

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. [Buckets (バケット)] リストで、目的のバケットの名前を選択します。
3. [プロパティ] を選択します。
4. S3 Intelligent-Tiering アーカイブの設定セクションに移動し、[設定を作成] を選択します。
5. アーカイブ構成の設定セクションで、S3 Intelligent-Tiering アーカイブ設定に分かりやすい設定名を指定します。

6. [設定範囲の選択] で、使用する設定範囲を選択します。オプションとして、共有プレフィックス、オブジェクトタグ、またはその組み合わせを使用して、バケット内の指定されたオブジェクトの設定範囲を制限することもできます。

   a. 設定の範囲を制限するには、[1 つ以上のフィルターを使用して、この設定の範囲を制限] を選択します。

   b. 単一のプレフィックスを使用して設定の範囲を制限するには、[プレフィックス] の下にプレフィックスを入力します。

   c. オブジェクトタグを使用して設定の範囲を制限するには、[タグの追加] を選択し、キーの値を入力します。

7. [ステータス] で [有効] を選択します。

8. [アーカイブ設定] セクションで、有効にするアーカイブアクセス階層の 1 つまたは両方を選択します。

9. [Create] (作成) を選択します。

AWS CLI の使用

次の AWS CLI コマンドを使用して、S3 Intelligent-Tiering 設定を管理できます。

- `delete-bucket-intelligent-tiering-configuration`
- `get-bucket-intelligent-tiering-configuration`
- `list-bucket-intelligent-tiering-configurations`
- `put-bucket-intelligent-tiering-configuration`

AWS CLI の設定の手順については、「Amazon S3 API リファレンス」の「AWS CLI を使用した Amazon S3 での開発」を参照してください。

AWS CLI を使用する場合、設定を XML ファイルとして指定することはできません。代わりに JSON を指定する必要があります。サンプル XML S3 Intelligent-Tiering 設定と、AWS CLI コマンドで指定できる同等の JSON を以下に示します。

次の例では、指定したバケットに S3 Intelligent-Tiering 設定を配置します。

Example [put-bucket-intelligent-tiering-configuration]

JSON

```
{
  "Id": "string",
  "Filter": {
    "Prefix": "string",
    "Tag": {
      "Key": "string",
      "Value": "string"
    },
    "And": {
      "Prefix": "string",
      "Tags": [
        {
          "Key": "string",
          "Value": "string"
        }
        ...
      ]
    }
  },
  "Status": "Enabled"|"Disabled",
  "Tierings": [
    {
      "Days": integer,
      "AccessTier": "ARCHIVE_ACCESS"|"DEEP_ARCHIVE_ACCESS"
    }
    ...
  ]
}
```

XML

```
PUT /?intelligent-tiering&id=Id HTTP/1.1
Host: Bucket.s3.amazonaws.com
<?xml version="1.0" encoding="UTF-8"?>
<IntelligentTieringConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
   <Id>string</Id>
   <Filter>
      <And>
         <Prefix>string</Prefix>
```

```
            <Tag>
               <Key>string</Key>
               <Value>string</Value>
            </Tag>
            ...
         </And>
         <Prefix>string</Prefix>
         <Tag>
            <Key>string</Key>
            <Value>string</Value>
         </Tag>
      </Filter>
      <Status>string</Status>
      <Tiering>
         <AccessTier>string</AccessTier>
         <Days>integer</Days>
      </Tiering>
      ...
</IntelligentTieringConfiguration>
```

PUT API オペレーションの使用

指定したバケットとバケットごとに最大 1,000 の S3 Intelligent-Tiering 設定に対して[PutBucketIntelligentTieringConfiguration](#)オペレーションを使用できます。共有プレフィックスまたはオブジェクトタグを使用して、アーカイブアクセス階層の対象となるバケット内のオブジェクトを定義できます。共有プレフィックスまたはオブジェクトタグを使用して、特定のビジネスアプリケーション、ワークフロー、または内部組織に合わせることができます。また、アーカイブアクセス階層、ディープアーカイブアクセス階層、またはその両方を柔軟にアクティブにすることもできます。

S3 Intelligent-Tiering を使用した開始方法

S3 Intelligent-Tiering の使用方法の詳細については、「[チュートリアル: S3 Intelligent-Tiering の使用を開始する](#)」を参照してください。

S3 Intelligent-Tiering の管理

S3 Intelligent-Tiering ストレージクラスは、3 つの低レイテンシーかつ高スループットのアクセス階層で、ストレージコストの自動的な削減を実現します。また、数分から数時間でアクセス可能なデータに対して最小限のストレージコストを実現できるように、オプションのアーカイブ機能が提供されます。

どの S3 Intelligent-Tiering アクセス階層オブジェクトが保存されているかを特定する

オブジェクトとその対応するメタデータ (S3 Intelligent-Tiering アクセス階層を含む) のリストを取得するには、Amazon S3 インベントリ を使用します。S3 インベントリは、CSV、ORC、またはオブジェクトとそれに対応するメタデータを一覧表示する Parquet 出力ファイルを提供します。Amazon S3 バケットまたは共有プレフィックスについて、これらのインベントリレポートを日単位または週単位で受け取ることができます。(共有プレフィックスとは、共通の文字列で始まる名前を持つオブジェクトのことです。)

S3 Intelligent-Tiering のオブジェクトのアーカイブステータスを見る

S3 Intelligent-Tiering ストレージクラス内のオブジェクトが、Archive Access tier または Deep Archive Access 階層のいずれかに移動したときに通知を受け取るには、Amazon S3 イベント通知を設定できます。詳細については、イベント通知を有効にするを参照してください。

Amazon S3 は、Amazon Simple Notification Service (Amazon SNS) トピック、Amazon Simple Queue Service (Amazon SQS) キュー、または AWS Lambda 関数にイベント通知を発行できます。詳細については、「Amazon S3 イベント通知」を参照してください。

次は Amazon S3 が `s3:IntelligentTiering` イベントを発行するために送信するメッセージの例です。詳細については、「the section called “イベントメッセージの構造”」を参照してください。

```
{
   "Records":[
      {
         "eventVersion":"2.3",
         "eventSource":"aws:s3",
         "awsRegion":"us-west-2",
         "eventTime":"1970-01-01T00:00:00.000Z",
         "eventName":"IntelligentTiering",
         "userIdentity":{
            "principalId":"s3.amazonaws.com"
         },
         "requestParameters":{
            "sourceIPAddress":"s3.amazonaws.com"
         },
         "responseElements":{
            "x-amz-request-id":"C3D13FE58DE4C810",
            "x-amz-id-2":"FMyUVURIY8/IgAtTv8xRjskZQpcIZ9KG4V5Wp6S7S/
JRWeUWerMUE5JgHvANOjpD"
         },
         "s3":{
```

```
            "s3SchemaVersion":"1.0",
            "configurationId":"testConfigRule",
            "bucket":{
               "name":"amzn-s3-demo-bucket",
               "ownerIdentity":{
                  "principalId":"A3NL1KOZZKExample"
               },
               "arn":"arn:aws:s3:::amzn-s3-demo-bucket"
            },
            "object":{
               "key":"HappyFace.jpg",
               "size":1024,
               "eTag":"d41d8cd98f00b204e9800998ecf8427e",
            }
         },
         "intelligentTieringEventData":{
            "destinationAccessTier": "ARCHIVE_ACCESS"
            }
      }
   ]
}
```

また、HEAD オブジェクトリクエストを使用して、オブジェクトのアーカイブのステータスを表示することもできます。オブジェクトが S3 Intelligent-Tiering ストレージクラスを使用して保存され、現在アーカイブ層の 1 つにある場合、HEAD オブジェクト応答には現在のアーカイブ層が表示されます。アーカイブ階層を表示するために、リクエストでは x-amz-archive-statusヘッダーを使用します。

次の HEAD オブジェクトリクエストは、オブジェクトのメタデータ (この場合は *my-image.jpg*) を返します。

Example

```
HEAD /my-image.jpg HTTP/1.1
Host: bucket.s3.region.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:02236Q3V0RonhpaBX5sCYVf1bNRuU=
```

また、HEAD オブジェクトリクエストは、restore-object リクエストのステータスをモニタリングするためにも使用できます。アーカイブの復元が進行中の場合、HEAD オブジェクトの応答には x-amz-restore ヘッダーが含まれます。

以下は、復元リクエストの処理中に S3 Intelligent-Tiering を使用してアーカイブされたオブジェクトを示す HEAD オブジェクト応答のサンプルです。

Example

```
HTTP/1.1 200 OK
x-amz-id-2: FSVaTMjrmBp3Izs1NnwBZeu7M19iI8UbxMbi0A8AirHANJBo+hEftBuiESACOMJp
x-amz-request-id: E5CEFCB143EB505A
Date: Fri, 13 Nov 2020 00:28:38 GMT
Last-Modified: Mon, 15 Oct 2012 21:58:07 GMT
ETag: "1accb31fcf202eba0c0f41fa2f09b4d7"
x-amz-storage-class: 'INTELLIGENT_TIERING'
x-amz-archive-status: 'ARCHIVE_ACCESS'
x-amz-restore: 'ongoing-request="true"'
x-amz-restore-request-date: 'Fri, 13 Nov 2020 00:20:00 GMT'
Accept-Ranges: bytes
Content-Type: binary/octet-stream
Content-Length: 300
Server: AmazonS3
```

S3 Intelligent-Tiering アーカイブアクセス階層からのオブジェクトの復元

S3 Intelligent-Tiering Archive Access および Deep Archive のアクセス階層のオブジェクトにアクセスするには、復元リクエストを開始して、オブジェクトが高頻度アクセス階層に移動するまで待機する必要があります。アーカイブされたオブジェクトの詳細については、「the section called “アーカイブされたオブジェクトの操作”」を参照してください。

アーカイブアクセス階層または Deep Archive アクセス階層から復元すると、オブジェクトは高頻度アクセス階層に戻ります。その後、連続 30 日が経過した後もオブジェクトにアクセスがなければ、自動的に低頻度アクセス階層に移行します。次に、90 日以上連続でアクセスされないと、オブジェクトが Archive Access 階層に移行します。180 日以上連続でアクセスされないと、オブジェクトは Deep Archive Access 階層に自動的に移行します。詳細については、「the section called “S3 Intelligent-Tiering の仕組み”」を参照してください。

アーカイブされたオブジェクトは、Amazon S3 コンソール、S3 バッチオペレーション、Amazon S3 REST API、AWS SDK、または AWS Command Line Interface (AWS CLI) を使用して復元できます。詳細については、「the section called “アーカイブされたオブジェクトの操作”」を参照してください。

長期データストレージとしての S3 Glacier ストレージクラスを理解する

Amazon S3 S3 Glacier ストレージクラスを使用すると、頻繁にはアクセスされない長期データを保存するためのコスト効率の高いソリューションを提供できます。S3 Glacier ストレージクラスは、次の 3 種類のストレージクラスに分類されます。

- S3 Glacier Instant Retrieval
- S3 Glacier Flexible Retrieval
- S3 Glacier Deep Archive

データにアクセスする頻度とデータの取り出し速度に応じて、これらのストレージクラスのいずれかを選択します。各ストレージクラスは S3 Standard ストレージクラスと同様の耐久性と回復性を、より低いストレージコストで提供します。S3 Glacier ストレージクラスの詳細については、https://aws.amazon.com/s3/storage-classes/glacier/ を参照してください。

トピック

- S3 Glacier ストレージクラスの比較
- S3 Glacier Instant Retrieval
- S3 Glacier Flexible Retrieval
- S3 Glacier Deep Archive
- S3 Glacier Flexible Retrieval および S3 Glacier Deep Archive はアーカイブストレージクラスです。
- S3 標準ストレージクラスと S3 Glacier サービスの違い

S3 Glacier ストレージクラスの比較

各 S3 Glacier ストレージクラスには、すべてのオブジェクトについて、最小ストレージ期間があります。最小ストレージ期間より前にオブジェクトを削除、上書き、または別のストレージクラスに移行した場合、その期間の残りに対して料金が請求されます。

S3 Glacier ストレージクラスの一部はアーカイブ用で、これらのクラスに保存されているオブジェクトはアーカイブされ、リアルタイムアクセスには使用できません。詳細については、「S3 Glacier Flexible Retrieval および S3 Glacier Deep Archive はアーカイブストレージクラスです。」を参照してください。

取り出し時間が長い低頻度アクセスパターン用に設計されたストレージクラスでは、ストレージコストがより低くなります。料金情報については、https://aws.amazon.com/s3/pricing/ を参照してください。

次の表は、S3 Glacier ストレージクラスを選択する際に検討すべき重要ポイントをまとめたものです。

S3 Glacier Instant Retrieval

S3 Glacier Instant Retrieval は、四半期に一度のアクセス頻度で、ミリ秒単位での取り出しが要求される長期データに使用することをお勧めします。このストレージクラスは、画像ホスティング、ファイル共有アプリケーション、予約時にアクセスする医療記録の保存など、パフォーマンスが重視されるユースケースに最適です。

S3 Glacier Instant Retrieval ストレージクラスは、S3 Standard-IA ストレージクラスと同じレイテンシーとスループットパフォーマンスで、オブジェクトにリアルタイムでアクセスできます。S3 Glacier Instant Retrieval は、 S3 Standard-IA と比較して、ストレージコストは低くなりますが、データアクセスコストは高くなります。

S3 Glacier Instant Retrieval ストレージクラスに保存されるデータの最小オブジェクトサイズは 128 KB です。また、このストレージクラスの最小ストレージ期間は 90 日間です。

S3 Glacier Flexible Retrieval

S3 Glacier Flexible Retrieval は、1 年に 1～2 回のアクセス頻度で、即時アクセスを必要としないアーカイブデータに使用することをお勧めします。S3 Glacier Flexible Retrieval では柔軟な取り出し時間を選択でき、数分から数時間のアクセス時間と、無料の一括取り出しによるコストとのバランスをとるのに役立ちます。このストレージクラスは、バックアップとディザスタリカバリに最適です。

S3 Glacier Flexible Retrieval に保存されたオブジェクトは、アーカイブされ、リアルタイムでアクセスできなくなります。詳細については、「S3 Glacier Flexible Retrieval および S3 Glacier Deep Archive はアーカイブストレージクラスです。」を参照してください。これらのオブジェクトにアクセスするには、まず復元リクエストを開始し、リクエストの完了時にアクセスできるオブジェクトの一時コピーを作成します。詳細については、「アーカイブされたオブジェクトの操作」を参照してください。オブジェクトを復元するときは、ユースケースに合わせて取り出し階層を選択でき、復元時間が長くなるほど、コストは低くなります。

S3 Glacier Flexible Retrieval では、次の取り出し階層を使用できます。

- 迅速取り出し — 通常、1～5 分でオブジェクトを復元します。迅速取り出しは、需要に応じて使用します。信頼性が高く、予測可能な復元時間を確保するには、プロビジョンド取り出しキャパシ

ティを購入することをお勧めします。詳細については、「プロビジョンドキャパシティー」を参照してください。

- 標準取り出し — 通常、3～5 時間でオブジェクトを復元します。S3 バッチオペレーションを使用すると、1 分～5 時間以内にオブジェクトを復元します。詳細については、「バッチオペレーションを使ってオブジェクトを復元する」を参照してください。
- 一括取り出し — 通常、5～12 時間以内にオブジェクトを復元します。一括取り出しは無料です。

S3 Glacier Flexible Retrieval ストレージクラスのオブジェクトの最小ストレージ期間は 90 日間です。

S3 Glacier Flexible Retrieval では、オブジェクトごとに 40 KB の追加メタデータが必要です。これには、データの特定と取得に必要な 32 KB のメタデータが含まれ、S3 Glacier Flexible Retrieval のデフォルトレートで課金されます。アーカイブされたオブジェクトのユーザー定義の名前とメタデータを維持するには、追加の 8 KB データが必要で、S3 標準レートで課金されます。

S3 Glacier Deep Archive

アクセス頻度が 1 年に 1 回未満のアーカイブデータには、S3 Glacier Deep Archive を使用することをお勧めします。このストレージクラスは、コンプライアンス要件を満たすためにデータセットを複数年間保持するように設計されており、バックアップやディザスタリカバリ、または取り出しまで最大 72 時間待機できるアクセス頻度の低いデータにも使用できます。S3 Glacier Deep Archive は、AWS で最も低コストのストレージオプションです。

S3 Glacier Deep Archive に保存されたオブジェクトは、アーカイブされ、リアルタイムでアクセスできなくなります。詳細については、「S3 Glacier Flexible Retrieval および S3 Glacier Deep Archive はアーカイブストレージクラスです。」を参照してください。これらのオブジェクトにアクセスするには、まず復元リクエストを開始し、リクエストの完了時にアクセスできるオブジェクトの一時コピーを作成します。詳細については、「アーカイブされたオブジェクトの操作」を参照してください。オブジェクトを復元するときは、ユースケースに合わせて取り出し階層を選択でき、復元時間が長くなるほど、コストは低くなります。

S3 Glacier Deep Archive では、次の取り出し階層を使用できます。

- 標準取り出し — 通常、12 時間以内にオブジェクトを復元します。S3 バッチオペレーションを使用すると、9～12 時間以内にオブジェクトを復元します。詳細については、「バッチオペレーションを使ってオブジェクトを復元する」を参照してください。
- 一括取り出し — 通常、標準取り出し階層のコストのごく一部で、48 時間以内にオブジェクトを復元します。

S3 Glacier Deep Archive ストレージクラスのオブジェクトの最小ストレージ期間は 180 日間です。

S3 Glacier Deep Archive には、オブジェクトごとに 40 KB の追加メタデータが必要です。これには、データの特定と取得に必要な 32 KB のメタデータが含まれ、S3 Glacier Deep Archive のデフォルトレートで課金されます。アーカイブされたオブジェクトのユーザー定義の名前とメタデータを維持するには、追加の 8 KB データが必要で、S3 標準レートで課金されます。

S3 Glacier Flexible Retrieval および S3 Glacier Deep Archive はアーカイブストレージクラスです。

S3 Glacier Flexible Retrieval および S3 Glacier Deep Archive はアーカイブストレージクラスです。つまり、これらのストレージクラスにオブジェクトを保存すると、そのオブジェクトはアーカイブされ、直接アクセスできなくなります。アーカイブされたオブジェクトにアクセスするには、そのオブジェクトの復元リクエストを送信し、サービスによりオブジェクトが復元されるまで待ちます。復元リクエストによりオブジェクトの一時コピーが復元され、このリクエストで指定した期間が終了すると、そのコピーは削除されます。詳細については、「アーカイブされたオブジェクトの操作」を参照してください。

S3 Glacier Deep Archive ストレージクラスへのオブジェクトの移行は一方向のみです。

アーカイブされたオブジェクトのストレージクラスをその他のストレージクラスに変更する場合、まず復元オペレーションを使用してオブジェクトの一時コピーを作成する必要があります。その後、コピーオペレーションを使用して、ストレージクラスとして S3 Standard、S3 Intelligent-Tiering、S3 標準 – IA、S3 1 ゾーン – IA、 S3 Glacier Instant Retrieval、S3 Glacier Flexible Retrieval、または Reduced Redundancy Storage を指定しているオブジェクトを上書きします。

> **Note**
>
> Amazon S3 コンソールでは、S3 Glacier Flexible Retrieval ストレージクラスまたは S3 Glacier Deep Archive ストレージクラス内のオブジェクトに対する、復元したオブジェクトのコピー操作はサポートしていません。このタイプのコピー操作には、AWS Command Line Interface (AWS CLI)、AWS SDK、または REST API を使用します。

これらのストレージクラスのアーカイブされたオブジェクトは、AWS リージョンあたりアカウントごとに最大 1,000 トランザクション/秒 (TPS) のオブジェクト復元リクエストで復元できます。

コストに関する考慮事項

アクセス頻度の高いデータを数か月あるいは数年間アーカイブする場合、S3 Glacier および S3 Glacier Deep Archive ストレージクラスを使用する事でストレージコストを削減できます。ただし、S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive ストレージクラスが適切であることを確認するために、以下の点を考慮してください。

- ストレージオーバーヘッド料金 – アーカイブされた各オブジェクトには 40 KB の追加メタデータが必要です。これには、データの特定と取得に必要な 32 KB のメタデータが含まれ、そのストレージクラスのデフォルトレートで課金されます。アーカイブされたオブジェクトのユーザー定義の名前とメタデータを維持するには、追加の 8 KB データが必要で、S3 標準レートで課金されます。

  小さいオブジェクトをアーカイブする場合は、これらのストレージ料金を考慮する必要があります。オーバーヘッドコストを削減するには、多数の小さいオブジェクトを少数の大きいオブジェクトに集約する方法があります。

- マルチパートアップロード料金 – S3-storage-class-glacier のオブジェクト、および S3 Glacier Deep Archive のオブジェクトは、マルチパートアップロードを使用してアップロードすると S3 Standard ストレージクラス料金で請求されます。詳細については、「マルチパートアップロードと料金」を参照してください。

- 最低 30 日間のストレージ料 – S3 Glacier Flexible Retrieval および S3 Glacier Deep Archive は、長期アーカイブソリューションです。最小ストレージ期間は、S3 Glacier ストレージクラスの場合は 90 日、S3 Glacier Deep Archive の場合は 180 日です。これらのストレージクラスにアーカイブされたデータを削除しても、削除するオブジェクトが最小ストレージ期間より長い期間アーカイブされている場合は無料です。アーカイブされたオブジェクトを最小ストレージ期間以内に削除または上書きする場合は、Amazon S3 ではその期間の残りに対して料金が発生します。

- データ取得料金 – アーカイブされたオブジェクトを S3 Glacier Flexible Retrieval および S3 Glacier Deep Archive に復元する場合、リクエストごとのデータ取得料金が発生します。これらの料金は、復元を開始するときに選択した取り出し階層によって異なります。料金については、[Amazon S3 の料金] を参照してください。

- S3 ライフサイクル – アーカイブされたオブジェクトを S3 Glacier Flexible Retrieval および S3 Glacier Deep Archive に復元する場合、リクエストごとのデータ取得料金が発生します。これらの料金は、復元を開始するときに選択した取り出し階層によって異なります。料金については、[Amazon S3 の料金] を参照してください。

アーカイブされたオブジェクトの復元

アーカイブされたオブジェクトにはリアルタイムでアクセスできません。まず復元リクエストを開始してから、リクエストで指定した期間中にオブジェクトの一時コピーが利用できるようになるまで待ちます。復元されたオブジェクトの一時コピーの取得後も、オブジェクトのストレージクラスは S3 Glacier または S3 Glacier Deep Archive が保持されます。(HeadObject または GetObject API オペレーションリクエストは、S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive をストレージクラスとして返します)。

> **Note**
>
> アーカイブを復元する場合、アーカイブの費用 (S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive 料金) の他に、一時的に復元されたコピーの費用 (S3 標準ストレージ料金) も発生します。料金については、「Amazon S3 の料金」を参照してください。

オブジェクトのコピーは、プログラムによって、あるいは Amazon S3 コンソールを使用して復元できます。Amazon S3 は、各オブジェクトに対して一度に 1 つの復元リクエストのみを処理します。詳細については、「アーカイブされたオブジェクトの復元」を参照してください。

S3 標準ストレージクラスと S3 Glacier サービスの違い

S3 Glacier ストレージクラスは Amazon S3 サービスの一部であり、データをオブジェクトとして S3 バケットに保存します。これらのストレージクラスのオブジェクトは、S3 コンソールを使用するか、S3 API または SDK を使用して、プログラムによって管理できます。S3 Glacier ストレージクラスにオブジェクトを保存すると、高度な暗号化、オブジェクトのタグ付け、S3 ライフサイクル設定などの S3 機能を使用して、データのアクセシビリティとコストを管理できます。

> **Important**
>
> あらゆる長期データには、Amazon S3 サービス内の S3 Glacier ストレージクラスを使用することをお勧めします。

Amazon S3 Glacier (S3 Glacier) サービスは、データをボールト内のアーカイブとして保存する個別のサービスです。このサービスは Amazon S3 機能に対応しておらず、データのアップロードおよびダウンロード操作のコンソールのサポートも提供していません。長期データに S3 Glacier サービスを使用することはお勧めしません。このサービスに保存されたデータは、Amazon S3 サービス

からアクセスできません。S3 Glacier サービスの詳細については、「Amazon S3 Glacier デベロッパーガイド」を参照してください。Amazon S3 Glacier サービスから Amazon S3 のストレージクラスにデータを転送するには、AWS ソリューションライブラリの「Amazon S3 Glacier ボールトから Amazon S3 へのデータ転送」を参照してください。

アーカイブされたオブジェクトの操作

アクセス頻度の低いオブジェクトのストレージコストを削減するには、それらのオブジェクトをアーカイブできます。オブジェクトをアーカイブすると、そのオブジェクトは低コストのストレージに移動されるため、リアルタイムでアクセスすることはできません。

アーカイブされたオブジェクトにはリアルタイムではアクセスできませんが、ストレージクラスによっては数分または数時間で復元できます。アーカイブされたオブジェクトは、Amazon S3 コンソール、S3 バッチオペレーション、REST API、AWS SDK、および AWS Command Line Interface (AWS CLI) を使用して復元できます。手順については、アーカイブされたオブジェクトの復元 を参照してください。

次のストレージクラスまたは階層の Amazon S3 オブジェクトはアーカイブされ、リアルタイムでアクセスできなくなります。

- S3 Glacier Flexible Retrieval ストレージクラス
- S3 Glacier Deep Archive ストレージクラス
- S3 Intelligent-Tiering Archive アクセス階層
- S3 Intelligent-Tiering Deep Archive アクセス階層

アーカイブされたオブジェクトを復元するには、以下の手順を実行する必要があります。

- S3 Glacier Flexible Retrieval ストレージクラスと S3 Glacier Deep Archive ストレージクラスのオブジェクトの場合は、復元リクエストを行い、オブジェクトの一時コピーが使用可能になるまで待機する必要があります。復元されたオブジェクトの一時コピーが作成されると、オブジェクトのストレージクラスは引き続き同じです。(HeadObject または GetObject API オペレーションリクエストは、S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive をストレージクラスとして返します)。
- S3 Intelligent-Tiering アーカイブアクセス階層および Deep Archive アクセス階層にあるオブジェクトの場合、復元リクエストを開始し、オブジェクトが高頻度アクセス階層に移動されるまで待機する必要があります。

Amazon S3 のすべてのストレージクラスの比較の詳細については、[Amazon S3 ストレージクラスの理解と管理] を参照してください。S3 Intelligent-Tiering の詳細については、「the section called "S3 Intelligent-Tiering の仕組み"」を参照してください。

復元ジョブが完了するのにかかる時間は、使用するアーカイブストレージクラスまたはストレージ階層、および、迅速 (S3 Glacier Flexible Retrieval と S3 Intelligent-Tiering Archive Access のみで使用可能)、標準、大容量のどの取り出しオプションを指定するかによって変わってきます。詳細については、「アーカイブ取得オプションを理解する」を参照してください。

Amazon S3 イベント通知を使用して、復元が完了したときに通知を受けることができます。詳細については、「Amazon S3 イベント通知」を参照してください。

S3 Glacier からのオブジェクトの復元

S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive を使用した場合、Amazon S3 は指定された期間のみ、オブジェクトの一時コピーを復元します。その期間が終了すると、復元されたオブジェクトのコピーは削除されます。復元されたコピーの有効期限を変更するには、復元リクエストを再発行します。この場合、Amazon S3 は、現在の時刻を基準にして有効期限を更新します。

> **Note**
>
> S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive からアーカイブされたオブジェクトを復元する場合、アーカイブしたオブジェクトと一時的に復元したコピーの両方の費用が発生します。料金については、「Amazon S3 の料金」を参照してください。

Amazon S3 は、復元リクエストで指定された日数をリクエストされた復元が完了した時刻に加算することで、復元されたオブジェクトの有効期限を計算します。結果として得られた時刻は、Amazon S3 によって、深夜の協定世界時 (UTC) の翌日に丸められます。例えば、復元されたオブジェクトのコピーが 2012 年 10 月 15 日午前 10 時 30 分 (UTC) に作成され、復元期間が 3 日間として指定されたとします。この場合、復元されたコピーの有効期限は 2012 年 10 月 19 日 00:00 (UTC) に切れ、その時点で Amazon S3 はオブジェクトコピーを削除します。

S3 Intelligent-Tiering からのオブジェクトの復元

S3 Intelligent-Tiering Archive アクセス階層、または S3 Intelligent-Tiering Deep Archive アクセス階層からオブジェクトの復元を行うと、オブジェクトは S3 Intelligent-Tiering 高頻度アクセス階層に戻ります。連続 30 日が経過した後もオブジェクトにアクセスがなければ、自動的に低頻度アクセス階層に移行します。90 日以上連続でアクセスがない場合、オブジェクトは S3 Intelligent-Tiering

Archive アクセス階層に移行します。オブジェクトが 180 日間連続してアクセスされない場合、オブジェクトは Deep Archive アクセス階層に移行します。

> **Note**
>
> S3 Glacier Flexible Retrieval や S3 Glacier Deep Archive のストレージクラスとは異なり、S3 Intelligent-Tiering オブジェクトの復元リクエストは、`Days` 値を受け付けません。

復元リクエストでの S3 バッチ操作の使用

1 つのリクエストで複数の Amazon S3 オブジェクトを復元するには、S3 バッチオペレーションを使用できます。S3 バッチ操作には、オペレーション対象のオブジェクトのリストを指定します。S3 バッチオペレーションは、各 API オペレーションを呼び出して、指定されたオペレーションを実行します。1 つのバッチオペレーションジョブで、エクサバイトのデータを含む数十億ものオブジェクトに対して、指定されたオペレーションを実行できます。

トピック

- アーカイブ取得オプションを理解する
- アーカイブされたオブジェクトの復元

アーカイブ取得オプションを理解する

以下は、Amazon S3 にアーカイブされたオブジェクトを復元する際に使用できる取り出しオプションです。

- 迅速 – S3 Glacier Flexible Retrieval ストレージクラスまたは S3 Intelligent-Tiering Archive アクセス階層に保存されているデータにすばやくアクセスします。このオプションは、アーカイブのサブセットに対する不定期の緊急リクエストが必要になった場合に利用できます。最大規模のアーカイブオブジェクト (250 MB 以上) を除くすべてのアーカイブオブジェクトについては、迅速取り出しでアクセスしたデータは通常 1〜5 分以内で使用可能になります。

  > **Note**
  >
  > 緊急取得はプレミアム機能であり、緊急リクエストと取得の料金が発生します。Amazon S3 の料金に関する詳細については、「Amazon S3 の料金」を参照してください。

プロビジョンドキャパシティーを使用すると、S3 Glacier Flexible Retrieval の迅速な取り出しの取得容量を、必要なときに確実に利用できます。詳細については、「プロビジョンドキャパシティー」を参照してください。

- 標準 – 数時間以内に、アーカイブされたどのオブジェクトにもアクセスできます。標準は、取り出しオプションを指定しないで取り出しリクエストを行った場合にデフォルトで適用されます。標準取り出しは、S3 Glacier Flexible Retrieval ストレージクラスまたは S3 Intelligent-Tiering Archive アクセス階層に保存されているオブジェクトで、通常 3〜5 時間以内に終了します。S3 Glacier Deep Archive ストレージクラスまたは S3 Intelligent-Tiering Deep Archive アクセス階層に保存されているオブジェクトの場合、これらの取り出しは通常 12 時間以内に終了します。標準取り出しは、S3 Intelligent-Tiering に保存されたオブジェクトについては無料です。

  > **Note**
  >
  > - S3 Glacier Flexible Retrieval ストレージクラスまたは S3 Intelligent-Tiering Archive アクセス階層に保存されているオブジェクトの場合、S3 バッチオペレーションの復元オペレーションを使用して開始される標準取得は、通常、数分以内に開始され、3 ~ 5 時間以内に終了します。
  > - S3 Glacier Deep Archive ストレージクラスまたは S3 Intelligent-Tiering Deep Archive アクセス階層に保存されているオブジェクトの場合、S3 バッチオペレーションの復元オペレーションを使用して開始される標準取得は、通常 9 時間以内に開始され、12 時間以内に終了します。

- 大容量 – Amazon S3 Glacier の最も安価な取り出しオプションを使用してデータにアクセスします。大容量取り出しでは、大量のデータ (ペタバイト規模を含む) を安価に取得できます。

  S3 Glacier Flexible Retrieval ストレージクラスまたは S3 Intelligent-Tiering Archive アクセス階層に保存されているオブジェクトの場合、一括取得は、通常 5 ~ 12 時間以内に終了します。S3 Glacier Deep Archive ストレージクラスまたは S3 Intelligent-Tiering Deep Archive アクセス階層に保存されているオブジェクトの場合、一括取得は、通常 48 時間以内に終了します。

  一括取得は、S3 Glacier Flexible Retrieval または S3 Intelligent-Tiering に保存されたオブジェクトについては無料です。

次の表は、アーカイブの取り出しオプションをまとめたものです。料金については、「Amazon S3 の料金」を参照してください。

`Expedited`、`Standard`、または `Bulk` の取り出しを行うには、RestoreObject REST API リクエストの `Tier` リクエスト要素を、必要なオプションに設定するか、AWS Command Line Interface (AWS CLI) または AWS SDK の同等な値に設定します。プロビジョンドキャパシティーを購入すると、すべての Expedited 取り出しはプロビジョンドキャパシティーを通じて自動的に提供されます。

プロビジョンドキャパシティー

プロビジョンドキャパシティーを使用すると、S3 Glacier Flexible Retrieval の迅速な取り出しの取得容量を、必要なときに確実に利用できます。容量の各単位について 5 分ごとに 3 回以上の迅速取り出しを提供し、1 秒あたり最大 150 メガバイト (MBps) の取り出しスループットを提供します。

ワークロードからデータのサブセットにアクセスする際に非常に高い信頼性と予測可能性が求められる場合は、プロビジョニングされた取り出し容量の購入を検討してください。プロビジョンドキャパシティーがなくても、需要が異常に高い期間は、迅速取り出しを使用できない可能性があります。環境を問わず、どのような場合でも迅速取り出しにアクセスするには、プロビジョンドキャパシティーを購入することをお勧めします。

プロビジョンドキャパシティーユニットは、ユーザーの AWS アカウントに割り当てられます。そのため、バケット所有者ではなく、データの迅速取り出しのリクエスタが、プロビジョンドキャパシティーユニットを購入する必要があります。

プロビジョンドキャパシティーは、Amazon S3 コンソール、Amazon S3 Glacier コンソール、プロビジョンドキャパシティーの購入 REST API オペレーション、AWS SDK、AWS CLI のいずれかを使用して購入できます。プロビジョンドキャパシティーの料金情報については、[Amazon S3 の料金]を参照してください。

S3 Glacier 復元開始リクエストのレート

S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive ストレージクラスに保存されているオブジェクトに復元リクエストを開始すると、復元リクエストのクォータが AWS アカウント に適用されます。S3 Glacier は、1 秒あたり最大 1,000 トランザクションのレートで復元リクエストをサポートします。このレートを超えると、有効なリクエストが制限または拒否され、Amazon S3 が `ThrottlingException` エラーを返します。

必要に応じて、S3 バッチオペレーションを使用して、S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive ストレージクラスに保存されている多数のオブジェクトを 1 回のリクエストで取得することもできます。詳細については、「バッチオペレーションでオブジェクトオペレーションを一括で実行する」を参照してください。

アーカイブされたオブジェクトの復元

次のストレージクラスまたは階層の Amazon S3 オブジェクトはアーカイブされ、リアルタイムでアクセスできなくなります。

- S3 Glacier Flexible Retrieval ストレージクラス
- S3 Glacier Deep Archive ストレージクラス
- S3 Intelligent-Tiering Archive アクセス階層
- S3 Intelligent-Tiering Deep Archive アクセス階層

S3 Glacier Flexible Retrieval ストレージクラスまたは S3 Glacier Deep Archive ストレージクラスに保存されている Amazon S3 オブジェクトは、すぐにはアクセスできません。これらのストレージクラスのオブジェクトにアクセスするには、指定された期間 (日数) の間、オブジェクトの一時コピーを S3 バケットに復元する必要があります。オブジェクトの永続的なコピーが必要な場合は、オブジェクトを復元して、Amazon S3 バケット内にそのオブジェクトのコピーを作成します。復元したオブジェクトのコピーは Amazon S3 コンソールではサポートされていません。このタイプのコピー操作には、AWS Command Line Interface (AWS CLI)、AWS SDK、または REST API を使用します。コピーを作成してストレージクラスを変更しない限り、オブジェクトは S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive ストレージクラスに保存されます。これらのストレージクラスの使用方法については、「ほとんどアクセスすることのないオブジェクトのストレージクラス」を参照してください。

S3 Intelligent-Tiering アーカイブアクセスおよび ディープアーカイブアクセス階層のオブジェクトにアクセスするには、復元リクエストを開始しオブジェクトが高頻度アクセス階層に移動するまで待機する必要があります。アーカイブアクセス階層または Deep Archive アクセス階層から復元すると、オブジェクトは高頻度アクセス階層に戻ります。これらのストレージクラスの使用方法については、「アクセスパターンが変化する、またはアクセスパターンが不明なデータを、自動的に最適化するためのストレージクラス」を参照してください。

オブジェクトのアーカイブについては、「アーカイブされたオブジェクトの操作」を参照してください。

> **Note**
>
> - S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive からアーカイブしたオブジェクトを復元する場合、アーカイブしたオブジェクトと一時的に復元したコピーの両方について料金が発生します。

- S3 Intelligent-Tiering からオブジェクトを復元する場合、標準取得または一括取得での取得料金は発生しません。
- 既に復元したアーカイブ済みのオブジェクトに対して呼び出されたその後の復元リクエストは、GET リクエストの料金が発生します。料金については、「Amazon S3 の料金」を参照してください。

アーカイブされたオブジェクトの復元

アーカイブされたオブジェクトは、Amazon S3 コンソール、S3 REST API、AWS SDK、AWS Command Line Interface (AWS CLI)、または S3 バッチオペレーションを使用して復元できます。

S3 コンソールの使用

Amazon S3 コンソールを使用してオブジェクトを復元する

次の手順を使用して、S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive ストレージクラス、または S3 Intelligent-Tiering Archive Access または Deep Archive Access ストレージ層にアーカイブされたオブジェクトを復元します。

アーカイブされたオブジェクトを復元するには

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 左のナビゲーションペインで、[汎用バケット] を選択します。
3. バケットのリストで、復元するオブジェクトが含まれるバケットの名前を選択します。
4. [オブジェクト] リストで復元するオブジェクトを選択し、[アクション] を選択して、[復元の開始] を選択します。
5. S3 Glacier または S3 Glacier Deep Archive から復元する場合は、[復元されたコピーを使用できる日数] ボックスに、アーカイブデータをアクセス可能にする日数を入力します。
6. [保持期間] で次のいずれかの操作を行います。

   - [大容量取り出し] または [標準取り出し] を選択し、[復元の開始] を選択します。
   - [迅速な取り出し] (S3 Glacier Flexible Retrieval または S3 Intelligent-Tiering Archive アクセスのみに使用可能) を選択します。S3 Glacier Flexible Retrieval でオブジェクトを復元する場合、迅速取り出し用にプロビジョンドキャパシティーを購入するかどうかを選択できます。プロビジョンドキャパシティーを購入する場合は、次のステップに進んでください。購入しない場合は、[復元の開始] を選択してください。

> **Note**
>
> S3 Intelligent-Tiering Archive Access と Deep Archive Access 階層からのオブジェクトは、自動的に高頻度アクセス階層に復元されます。

7. (オプション) S3 Glacier Flexible Retrieval でオブジェクトを復元し、迅速取り出しを選択した場合、プロビジョンドキャパシティーを購入するかどうかを選択できます。プロビジョンドキャパシティーは、S3 Glacier Flexible Retrieval のオブジェクトにのみ使用できます。プロビジョンドキャパシティーを持っている場合、[復元の開始] を選択してプロビジョニングされた取り出しを開始します。

   プロビジョンドキャパシティーを持っている場合、すべての迅速取り出しはプロビジョンドキャパシティーにより処理されます。詳細については、「プロビジョンドキャパシティー」を参照してください。

   - プロビジョンドキャパシティーを持っておらず、購入する予定もない場合、[復元の開始] を選択します。
   - プロビジョンドキャパシティーはないが、プロビジョンドキャパシティーユニット (PCU) を購入したい場合は、[PCU を購入] を選択してください。[PCU を購入] ダイアログボックスで、購入する PCU の数を選択し、購入を確認して、[PCU を購入] を選択します。[購入完了] メッセージが表示されたら、[復元の開始] を選択してプロビジョニングされた取り出しを開始します。

AWS CLI の使用

S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive からオブジェクトを復元する

次の例では `restore-object` コマンドを使用して、25 日間でバケット *amzn-s3-demo-bucket* にオブジェクト *dir1/example.obj* を復元します。

```
aws s3api restore-object --bucket amzn-s3-demo-bucket --key dir1/example.obj --restore-request '{"Days":25,"GlacierJobParameters":{"Tier":"Standard"}}'
```

この例で使用されている JSON 構文が原因で Windows クライアントにエラーが生じる場合は、復元リクエストを以下の構文に置き換えてください。

```
--restore-request Days=25,GlacierJobParameters={"Tier"="Standard"}
```

S3 Intelligent-Tiering Archive Access と Deep Archive Access からオブジェクトを復元する

次の例では `restore-object` コマンドを使用して、バケット *amzn-s3-demo-bucket* のオブジェクト *dir1/example.obj* を高頻度アクセス階層に復元します。

```
aws s3api restore-object --bucket amzn-s3-demo-bucket --key dir1/example.obj --restore-request '{}'
```

> **Note**
>
> S3 Glacier Flexible Retrieval や S3 Glacier Deep Archive のストレージクラスとは異なり、S3 Intelligent-Tiering オブジェクトの復元リクエストは、`Days` 値を受け付けません。

復元ステータスを監視する

`restore-object` リクエストのステータスをモニタリングするには、次の `head-object` コマンドを使用します。

```
aws s3api head-object --bucket amzn-s3-demo-bucket --key dir1/example.obj
```

詳細については、AWS CLI コマンドリファレンスの「restore-object」を参照してください。

REST API の使用

Amazon S3 には、アーカイブされたオブジェクトの復元を開始するための API オペレーションが用意されています。詳細については、「Amazon Simple Storage Service API リファレンス」の「RestoreObject」を参照してください。

AWS SDK の使用

AWS SDK を使って S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive 内にアーカイブされたオブジェクトを復元する方法の例については、「Amazon S3 API リファレンス」の「Code examples」を参照してください。

S3 バッチオペレーションの使用

1 つのリクエストで複数のアーカイブされたオブジェクトを復元するには、S3 バッチオペレーションを使用できます。S3 バッチオペレーションには、オペレーションターゲットのオブジェクトのリストを指定します。S3 バッチオペレーションは、各 API オペレーションを呼び出して、指定された

オペレーションを実行します。1 つのバッチオペレーションジョブで、エクサバイトのデータを含む数十億ものオブジェクトに対して、指定されたオペレーションを実行できます。

バッチオペレーションジョブを作成するには、復元するオブジェクトのみを含むマニフェストが必要です。S3 Inventory を使用してマニフェストを作成することも、必要な情報を含む CSV ファイルを提供することもできます。詳細については、「the section called “マニフェストの指定”」を参照してください。

S3 バッチオペレーションジョブを作成して実行する前に、お客様に代わって S3 バッチオペレーションを実行するためのアクセス権限を Amazon S3 に付与する必要があります。必要なアクセス許可については、「the section called “アクセス許可の付与”」を参照してください。

> **Note**
>
> バッチ操作ジョブは、S3 Glacier Flexible Retrieval および S3 Glacier Deep Archive ストレージクラスオブジェクト、または S3 Intelligent-Tiering Archive Access および Deep Archive Access ストレージ階層オブジェクトのいずれかで操作できます。バッチオペレーションは、同じジョブ内の両方のタイプのアーカイブオブジェクトに対して操作できません。両方のタイプのオブジェクトを復元するには、別個のバッチ操作ジョブを作成する必要があります。バッチオペレーションを使用してアーカイブオブジェクトを復元する方法の詳細については、「the section called “オブジェクトの復元”」を参照してください。

S3 Initiate Restore Object Batch Operations ジョブを作成するには

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 左のナビゲーションペインで、[バッチ操作] を選択します。
3. [ジョブの作成]を選択します。
4. AWS リージョン については、ジョブを作成する [Region (リージョン)] を選択します。
5. [マニフェストの形式] で、使用するマニフェストのタイプを選択します。

   - [S3 インベントリレポート] を選択した場合Amazon S3 が CSV 形式のインベントリレポートの一部として生成した `manifest.json` オブジェクトへのパスを入力します。最新のバージョンではなく特定のマニフェストバージョンを使用する場合には、オプションでマニフェストオブジェクトのバージョン ID を含めることもできます。
   - [CSV] を選択する場合は、CSV 形式のマニフェストオブジェクトへのパスを入力します。マニフェストオブジェクトは、コンソールで説明される形式に従う必要があります。最新のバー

ジョンではなく特定のバージョンを使用する場合には、オプションでマニフェストオブジェクトのバージョン ID を含めることもできます。

6. [Next] を選択します。
7. [オペレーション] セクションで、[復元] を選択します。
8. [復元] セクションの [ソースを復元] で、[Glacier Flexible Retrieval または Glacier Deep Archive] か [Intelligent-Tiering Archive Access 階層または Deep Archive Access 階層] のいずれかを選択します。

   [Glacier Flexible Retrieval または Glacier Deep Archive] を選択した場合、[復元したコピーが使用できる日数] に数字を入力します。

   [取得階層] の場合、使用する階層を選択します。
9. [Next] を選択します。
10. [追加オプションを設定する] ページで、以下のセクションに情報を入力します。

    - [その他のオプション] セクションに、ジョブの説明を入力し、ジョブの優先度番号を指定します。番号が大きいほど、優先度が高いことを表します。詳細については、「the section called “ジョブの優先度の割り当て”」を参照してください。
    - [完了レポート] セクションで、バッチオペレーションで完了レポートを作成するかどうかを選択します。完了レポートに関する詳細については、「the section called “完了レポート”」を参照してください。
    - [許可] セクションでは、ユーザーに代わってバッチオペレーションを実行するためのアクセス権限を Amazon S3 に付与する必要があります。必要なアクセス許可については、「the section called “アクセス許可の付与”」を参照してください。
    - (オプション) [ジョブタグ] セクションで、キーと値のペアにタグを追加します。詳細については、「the section called “タグの使用”」を参照してください。

    完了したら、[Next (次へ)] を選択します。
11. [確認] ページで、設定を確認します。変更が必要な場合は、[戻る] を選択します。それ以外の場合は、[ジョブの作成] を選択します。

バッチオペレーションの詳細については、「バッチオペレーションを使ってオブジェクトを復元する」と「S3 バッチオペレーションジョブの作成」を参照してください。

復元ステータスおよび有効期限日の確認

復元リクエストのステータスや有効期限は、Amazon S3 コンソール、Amazon S3 イベント通知、AWS CLI、または Amazon S3 REST API を使用して確認できます。

> **Note**
>
> S3 Glacier Flexible Retrieval および S3 Glacier Deep Archive のストレージクラスから復元されたオブジェクトが保存されるのは、指定した期間のみです。次のプロシージャは、このようなコピーの有効期限を返します。
> S3 Intelligent-Tiering Archive および Deep Archive のアクセス階層から復元されたオブジェクトには有効期限がない代わりに高頻度アクセス階層に戻されます。

S3 コンソールの使用

Amazon S3 コンソールでオブジェクトの復元ステータスと有効期限を確認するには

1. https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開きます。
2. 左のナビゲーションペインで、[汎用バケット] を選択します。
3. バケットリストで、復元しているオブジェクトが含まれるバケットの名前を選択します。
4. [オブジェクト]リストで、復元するオブジェクトを選択します。オブジェクトの詳細ページが表示されます。

   - 復元が完了していない場合は、ページの上部に [復元中] セクションが表示されます。
   - 復元が完了した場合は、ページの上部に [復元中] と書かれたセクションが表示されます。S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive から復元する場合、このセクションには [復元の有効期限] も表示されます。Amazon S3 は、この日にアーカイブされたオブジェクトの復元済みコピーを削除します。

Amazon S3 イベント通知の使用

Amazon S3 イベント通知機能を使って、`s3:ObjectRestore:Completed` アクションを使用すると、オブジェクトの復元完了の通知を受け取ることができます。イベント通知を有効にする方法の詳細については、「Amazon SQS、Amazon SNS、および AWS Lambda を使用した通知の有効化」を参照してください。さまざまな `ObjectRestore` イベントタイプの詳細については、「the section called “SQS、SNS、および Lambda でサポートされているイベントタイプ”」を参照してください。

AWS CLI の使用

オブジェクトのリストアステータスと有効期限を AWS CLI コマンドで確認します。

次の例では head-object コマンドを使用して、バケット *amzn-s3-demo-bucket* のオブジェクト *dir1/example.obj* のメタデータを表示します。復元中のオブジェクトに対してこのコマンドを実行すると、Amazon S3 は復元が進行中であるかどうか、さらには有効期限を返します (該当する場合)。

```
aws s3api head-object --bucket amzn-s3-demo-bucket --key dir1/example.obj
```

期待される出力 (復元中):

```
{
    "Restore": "ongoing-request=\"true\"",
    "LastModified": "2020-06-16T21:55:22+00:00",
    "ContentLength": 405,
    "ETag": "\"b662d79adeb7c8d787ea7eafb9ef6207\"",
    "VersionId": "wbYaE2vtOV0iIBXrOqGAJt3fP1cHB8Wi",
    "ContentType": "binary/octet-stream",
    "ServerSideEncryption": "AES256",
    "Metadata": {},
    "StorageClass": "GLACIER"
}
```

期待される出力 (復元完了):

```
{
    "Restore": "ongoing-request=\"false\", expiry-date=\"Wed, 12 Aug 2020 00:00:00 GMT
\"",
    "LastModified": "2020-06-16T21:55:22+00:00",
    "ContentLength": 405,
    "ETag": "\"b662d79adeb7c8d787ea7eafb9ef6207\"",
    "VersionId": "wbYaE2vtOV0iIBXrOqGAJt3fP1cHB8Wi",
    "ContentType": "binary/octet-stream",
    "ServerSideEncryption": "AES256",
    "Metadata": {},
    "StorageClass": "GLACIER"
}
```

head-object の詳細については、「AWS CLI コマンドリファレンス」の「head-object」を参照してください。

REST API の使用

Amazon S3 には、オブジェクトメタデータを取得するための API オペレーションが用意されています。REST API を使用してアーカイブされたオブジェクトの復元ステータスと有効期限を確認するには、「Amazon Simple Storage Service API リファレンス」の「HeadObject」を参照してください。

進行中の復元速度のアップグレード

復元が進行中でも、復元速度をアップグレードできます。

進行中の復元をより高速の階層にアップグレードするには

1. https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。
3. [バケット] リストで、復元するオブジェクトが含まれるバケットの名前を選択します。
4. [オブジェクト]リストで、復元するオブジェクトを選択します。オブジェクトの詳細ページが表示されます。オブジェクトの詳細ページで、[取得階層をアップグレード] を選択します。オブジェクトの復元状況の確認については、[復元ステータスおよび有効期限日の確認] を参照してください。
5. アップグレードする階層を選択し、[復元] を選択します。

オブジェクトのライフサイクルの管理

S3 ライフサイクルは、オブジェクトを低コストのストレージクラスに移行するか、ユーザーに代わって期限切れのオブジェクトを削除することで、ライフサイクル全体でコスト効率の高い方法でオブジェクトを保存するのに役立ちます。オブジェクトのライフサイクルを管理するには、バケットの S3 ライフサイクル設定を作成します。S3 ライフサイクル設定は、Amazon S3 がオブジェクトのグループに適用するアクションを定義するルールのセットです。次の 2 種類のアクションがあります。

- Transition actions — 別のストレージクラスにオブジェクトを移行するタイミングを定義します。例えば、作成から 30 日後に S3 標準 – IA ストレージクラスにオブジェクトを移行するか、作成から 1 年後に S3 Glacier Flexible Retrieval ストレージクラスにオブジェクトをアーカイブするよう選択することができます。詳細については、[Amazon S3 ストレージクラスの理解と管理] を参照してください。

  ライフサイクル移行リクエストにはコストが発生します。料金については、[Amazon S3 の料金] を参照してください。

- [有効期限切れアクション] — このアクションではオブジェクトの有効期限を定義します。Amazon S3 はユーザーに代わって有効期限切れのオブジェクトを削除します。例えば、オブジェクトが規制コンプライアンス期間にわたって保存された後に、オブジェクトの有効期限が切れるように選択できます。詳細については、「オブジェクトの有効期限」を参照してください。

  最小ストレージ期間でストレージクラスのオブジェクトを期限切れにする場合にのみ、ライフサイクルの有効期限切れに関連する潜在的なコストが発生します。詳細については、「最小ストレージ期間料金」を参照してください。

> **Important**
>
> 汎用バケット – バケットポリシーを使用して、S3 ライフサイクルルールによる削除や移行を防ぐことはできません。例えば、バケットポリシーがすべてのプリンシパルのすべてのアクションを拒否する場合でも、S3 ライフサイクル設定は通常どおり機能します。

既存のオブジェクトと新しいオブジェクト

ライフサイクル設定をバケットに追加すると、設定ルールは既存のオブジェクトとそれ以降に追加されるオブジェクトの両方に適用されます。例えば、オブジェクトが作成から 30 日後に有効期限を迎えるようにする失効アクションを備えたライフサイクル設定ルールを本日追加すると、Amazon S3 により作成から 30 日以上が経過している既存のオブジェクトがすべて削除キューに追加されます。

請求の変更

オブジェクトがライフサイクルアクションの対象になるときと、Amazon S3 がオブジェクトを転送または期限切れにするまでの間に遅延がある場合は、オブジェクトがライフサイクルアクションの対象となり次第すぐに請求の変更が適用されます。例えば、オブジェクトの有効期限がスケジュール済みであり、Amazon S3 がそのオブジェクトを直ちに有効期限切れにしない場合、有効期限が過ぎてもストレージに対する料金は発生しません。

この動作の例外として、S3 Intelligent-Tiering ストレージクラスに移行するライフサイクルルールがある場合があります。オブジェクトが S3 Intelligent-Tiering に移行するまで、請求の変更は行われません。S3 ライフサイクルルールの詳細については、[ライフサイクル設定の要素] を参照してください。

> **Note**
>
> ライフサイクル移行にはデータ取り出し料金はかかりません。ただし、PUT、COPY、またはライフサイクルルールを使用してデータを任意の S3 ストレージクラスに移動する場合、リクエストごとに取り込み料金が発生します。オブジェクトをいずれかのストレージクラスに移動する前に、取り込みコストや移行コストについて検討してください。コストに関する考慮事項の詳細については、「Amazon S3 の料金」を参照してください。

ライフサイクルルールの影響のモニタリング

アクティブなライフサイクルルールによって行われた更新の影響をモニタリングするには、「the section called “ライフサイクルルールによって実行されたアクションをモニタリングするにはどうすればよいですか？”」を参照してください。

オブジェクトの完全なライフサイクルの管理

S3 ライフサイクル設定ルールを使用すると、より安価なストレージクラスへのオブジェクトの移行、またはアーカイブや削除を Amazon S3 に指定できます。例:

- 定期的なログをバケットにアップロードする場合、アプリケーションは 1 週間または 1 か月間、それを必要とする可能性があります。その後は、削除することができます。
- ドキュメントには、一定の期間中に頻繁にアクセスされるものがあります。その後は、頻繁にアクセスされません。ある時点で、リアルタイムでアクセスする必要はないものの、所属している組織や規則によって、特定の期間アーカイブしておくよう要求される場合があります。その期間が過ぎれば、削除してかまいません。
- 主にアーカイブ目的のため、ある種類のデータを Amazon S3 にアップロードする場合があります。例えば、デジタルメディア、財務や医療の記録、生のゲノムシーケンスデータ、データベースの長期バックアップ、法規制準拠のために保管が必要なデータをアーカイブできます。

これらの S3 ライフサイクルアクションを組み合わせることにより、オブジェクトの完全なライフサイクルを管理できます。たとえば、作成するオブジェクトに、よく定義されたライフサイクルがあるとします。最初に、オブジェクトは 30 日の期間にわたり頻繁にアクセスされます。次に、オブジェクトは最大 90 日間まで、頻繁にアクセスされません。その後は、オブジェクトは不要になるため、アーカイブまたは削除することができます。

このシナリオでは、S3 Intelligent-Tiering、S3 Standard – IA、または S3 1 ゾーン – IA のストレージへの最初の移行アクション、アーカイブのための S3 Glacier ストレージへの別の移行アクション、

および失効アクションを指定する S3 ライフサイクルのルールを作成できます。あるストレージクラスから別のストレージクラスにオブジェクトを移動すると、ストレージコストを節約できます。コストに関する考慮事項の詳細については、「Amazon S3 の料金」を参照してください。

トピック

- Amazon S3 ライフサイクルを使用したオブジェクトの移行
- オブジェクトの有効期限
- バケットに S3 ライフサイクル設定を設定する
- S3 ライフサイクルは他のバケット設定とどのように相互作用するか
- S3 ライフサイクルイベント通知の設定
- ライフサイクル設定の要素
- Amazon S3 がライフサイクル設定の競合を処理する方法
- S3 ライフサイクル設定の例
- Amazon S3 ライフサイクル問題のトラブルシューティング

Amazon S3 ライフサイクルを使用したオブジェクトの移行

S3 ライフサイクルの設定に移行アクションを追加して、別の Amazon S3 ストレージクラスにオブジェクトを移行するように Amazon S3 に指定できます。ストレージクラスの詳細については、「Amazon S3 ストレージクラスの理解と管理」を参照してください。この方法で S3 ライフサイクル設定を使用する場合の例を次に示します。

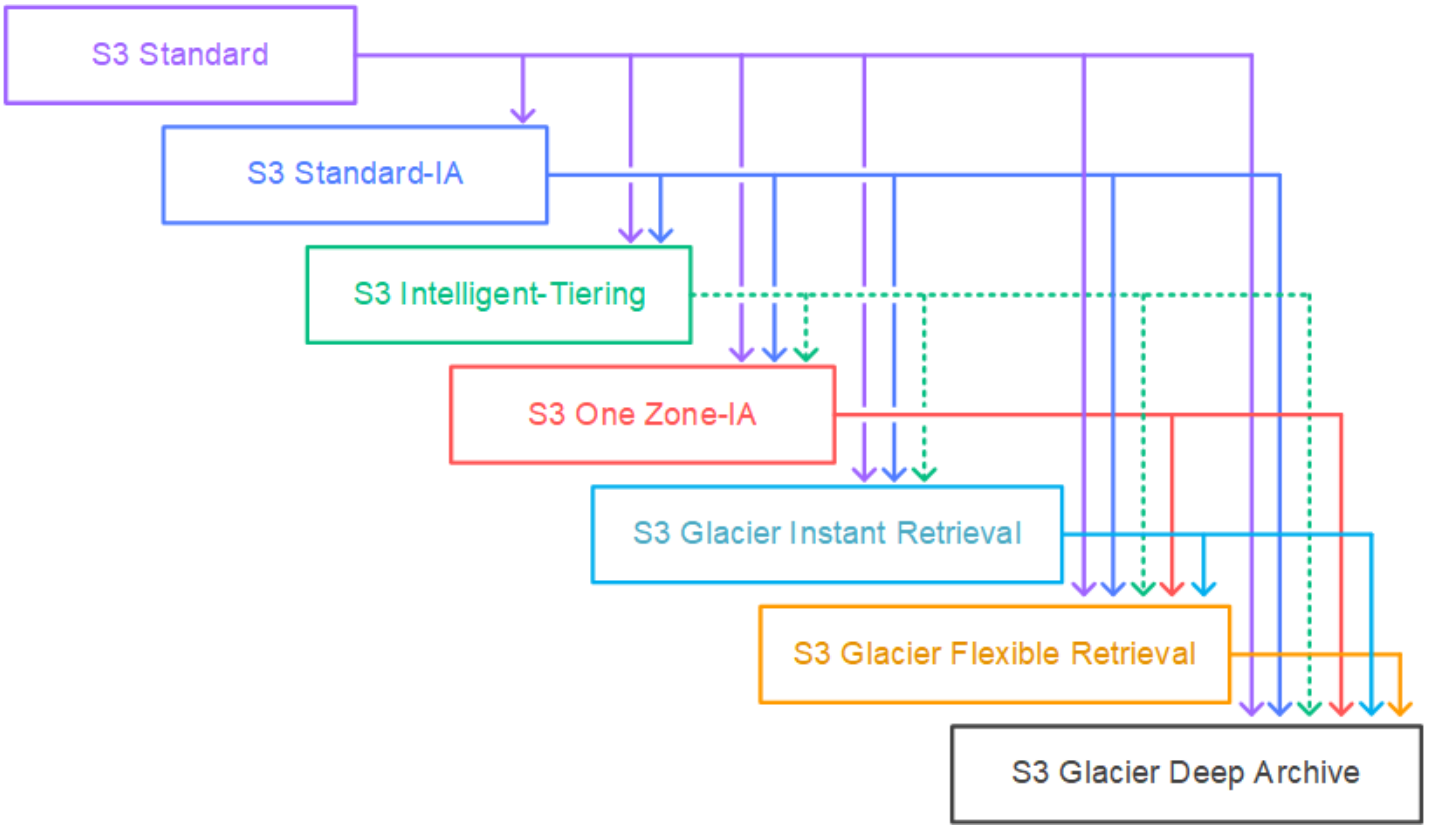
- これらのオブジェクトのアクセス頻度が低いことがわかった場合は、オブジェクトを S3 Standard – IA ストレージクラスに移行できます。
- リアルタイムでアクセスする必要のないオブジェクトは、S3 Glacier Flexible Retrieval ストレージクラスまたは S3 Glacier Deep Archive ストレージクラスへのアーカイブを推奨します。

> **Note**
>
> 暗号化済みオブジェクトは、ストレージクラスの移行プロセス全体を通して暗号化されたままになります。

サポートされている移行

S3 ライフサイクル設定では、1 つのストレージクラスから別のストレージクラスにオブジェクトを移行し、ストレージのコストを節約できるルールを定義できます。オブジェクトのアクセスパターンが不明、またはアクセスパターンが時間の経過とともに変化している場合、コストを自動的に削減するためにオブジェクトを S3 Intelligent-Tiering ストレージクラスに移行できます。ストレージクラスについては、[Amazon S3 ストレージクラスの理解と管理] を参照してください。

Amazon S3 は、以下の図のようにストレージクラス間の移行のためのウォーターフォールモデルをサポートします。



サポートされているライフサイクル移行

Amazon S3 では、S3 ライフサイクル設定を使用したストレージクラス間の以下のライフサイクル移行をサポートします。

- S3 標準ストレージクラスを S3 Standard–IA、S3 Intelligent-Tiering、S3 One Zone-IA、S3 Glacier Instant Retrieval、S3 Glacier Flexible Retrieval、または S3 Glacier Deep Archive ストレージクラスに移行する。

- S3 標準 – IA ストレージクラスを S3 Intelligent-Tiering、S3 1 ゾーン – IA、S3 Glacier Instant Retrieval、S3 Glacier Flexible Retrieval、または S3 Glacier Deep Archive ストレージクラスに移行する。
- S3 Intelligent-Tiering ストレージクラスは、S3 Intelligent-Tiering アクセス層に応じて異なるストレージクラスに移行できます。アクセス層ごとに次の移行が可能です。
  - 高頻度アクセス層または低頻度アクセス層から S3 One Zone-IA、S3 Glacier Instant Retrieval、S3 Glacier Flexible Retrieval、または S3 Glacier Deep Archive ストレージクラスへ。
  - アーカイブインスタントアクセス層から、S3 Glacier Instant Retrieval、S3 Glacier Flexible Retrieval、または S3 Glacier Deep Archive ストレージクラスへ。
  - アーカイブアクセス層から S3 Glacier Flexible Retrieval、または S3 Glacier Deep Archive ストレージクラスへ。
  - Deep Archive アクセス層から S3 Glacier Deep Archive ストレージクラスへ。
- S3 One Zone-IA ストレージクラスを S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive ストレージクラスに移行する。
- S3 Glacier Instant Retrieval ストレージクラスを S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive ストレージクラスに移行する。
- S3 Glacier Flexible Retrieval から S3 Glacier Deep Archive ストレージクラスに移行する。

> **Note**
>
> バージョニングが有効なバケットまたはバージョニングが停止されたバケットの場合、レプリケーションステータスが `Pending` のオブジェクトを移行することはできません。

移行に関する制約と考慮事項

ライフサイクルストレージクラス移行には、次の制約があります。

128 KB 未満のオブジェクトは、デフォルトではどのストレージクラスにも移行されません。

Amazon S3 は S3 ライフサイクル設定にデフォルトの動作を適用し、128 KB 未満のオブジェクトが任意のストレージクラスに移行されないようにします。128 KB 未満のオブジェクトの移行はお勧めしません。オブジェクトごとに移行リクエストが課金されるためです。つまり、オブジェクトが小さいほど、移行コストがストレージの節約額を上回る可能性があります。移行リクエストのコストの詳

細については、Amazon S3 料金ページのストレージとリクエストタブの「リクエストとデータの取得」を参照してください。

小さいオブジェクトを移行できるようにするには、カスタム最小サイズ (ObjectSizeGreaterThan) または最大サイズ (ObjectSizeLessThan) を指定するオブジェクトサイズフィルターをライフサイクル移行ルールに追加できます。詳細については、「例: 128 KB 未満のオブジェクトの移行を許可する」を参照してください。

> **Note**
>
> 2024 年 9 月、Amazon S3 は小さなオブジェクトのデフォルトの移行動作を次のように更新しました。
>
> - デフォルトの移行動作の更新 — 2024 年 9 月以降、デフォルトの動作により、128 KB 未満のオブジェクトが任意のストレージクラスに移行されることを回避します。
> - 以前のデフォルトの移行動作 — 2024 年 9 月以前は、デフォルトの動作により、128 KB 未満のオブジェクトは S3 Glacier および S3 Glacier Deep Archive ストレージクラスにのみ移行できました。
>
> 2024 年 9 月より前に作成された設定は、変更しない限り、以前の移行動作を保持します。つまり、ルールを作成、編集、または削除すると、設定のデフォルトの移行動作が更新された動作に変わります。ユースケースで必要な場合は、128KB 未満のオブジェクトが S3 Glacier および S3 Glacier Deep Archive に移行するように、デフォルトの移行動作を変更できます。これを行うには、PutBucketLifecycleConfiguration リクエストでオプションの `x-amz-transition-default-minimum-object-size` ヘッダーを使用します。

オブジェクトは、S3 Standard–IA または S3 One Zone-IA に移行する前に、30 日間保存する必要があります。

S3 標準 - IA または S3 1 ゾーン - IA にオブジェクトを移行する前に、これらのオブジェクトを少なくとも 30 日間 Amazon S3 に保存する必要があります。例えば、作成から 1 日後にオブジェクトを S3 標準 – IA ストレージクラスに移行するライフサイクルルールを作成することはできません。Amazon S3 は最初の 30 日間はこの移行をサポートしません。新しいオブジェクトはアクセス頻度が高く、S3 標準 – IA または S3 1 ゾーン – IA ストレージに適した期間よりも早く削除されることが多いためです。

同様に、(バージョニング対応のバケットで) 以前のオブジェクトを移行する場合、少なくとも 30 日は最新でないオブジェクトのみを S3 Standard – IA または S3 1 ゾーン – IA ストレージに移行できます。すべてのストレージクラスの最小ストレージ期間のリストについては、「Amazon S3 ストレージクラスの比較」を参照してください。

最小ストレージ期間より前にオブジェクトを移行すると料金が発生します。

特定のストレージクラスには、オブジェクトストレージの最小期間があります。最小期間より前にこれらのストレージクラスからオブジェクトを移行すると、その期間の残りの期間に対して課金されます。どのストレージクラスに最小ストレージ期間があるかの詳細については、「Amazon S3 ストレージクラスの比較」を参照してください。

最小ストレージ期間が経過する前に、オブジェクトをあるストレージクラスから別のストレージクラスに移行する単一のライフサイクルルールを作成することはできません。

例えば、S3 Glacier Instant Retrieval の最小ストレージ期間は 90 日間です。4 日後にオブジェクトを S3 Glacier Instant Retrieval に移行し、20 日後にオブジェクトを S3 Glacier Deep Archive に移行するライフサイクルルールを指定することはできません。この場合、S3 Glacier Deep Archive の移行は、少なくとも 94 日後に行う必要があります。

2 つのルールを指定してこれを達成できますが、最小ストレージ期間の料金が発生します。コストに関する考慮事項の詳細については、「Amazon S3 の料金」を参照してください。

S3 ライフサイクルの作成に関する詳細については、「バケットに S3 ライフサイクル設定を設定する」を参照してください。

S3 Glacier Flexible Retrieval と S3 Glacier Deep Archive ストレージクラスへの移行 (オブジェクトのアーカイブ)

S3 ライフサイクル設定を使用すると、オブジェクトをアーカイブ用に S3 Glacier または S3 Glacier Deep Archive のストレージクラスに移行できます。

オブジェクトをアーカイブする前に、以下の関連する考慮事項のセクションを確認してください。

一般的な考慮事項

オブジェクトをアーカイブする前に検討する必要のある一般的な考慮事項を以下に示します。

- 暗号化済みオブジェクトは、ストレージクラスの移行プロセス全体を通して暗号化されたままになります。

- S3 Glacier または S3 Glacier Deep Archive ストレージクラスに保存されているオブジェクトはリアルタイムでは利用できません。

  アーカイブされたオブジェクトは Amazon S3 オブジェクトですが、アーカイブされたオブジェクトにアクセスする前に、まずその一時コピーを復元する必要があります。復元されたオブジェクトのコピーは、復元リクエストで指定した期間内のみ利用できます。その後、Amazon S3 によって一時コピーが削除され、オブジェクトは Amazon S3 Glacier Flexible Retrieval にアーカイブされたまま残ります。

  Amazon S3 コンソールを使用して、またはプログラムのコード内で AWS SDK ラッパーライブラリや Amazon S3 REST API を使用して、オブジェクトを復元することができます。詳細については、「アーカイブされたオブジェクトの復元」を参照してください。

- S3 Glacier Flexible Retrieval ストレージクラスに格納されているオブジェクトは、S3 Glacier Deep Archive ストレージクラスにのみ移行できます。

  S3 ライフサイクル設定ルールを使用した場合、S3 Glacier から S3 Glacier Deep Archive ストレージクラスにのみオブジェクトのストレージクラスを変換できます。S3 Glacier に格納されているオブジェクトのストレージクラスを S3 Glacier Deep Archive 以外のストレージクラスに変更する場合は、まず復元オペレーションを使用してオブジェクトの一時的なコピーを作成する必要があります。その後、コピーオペレーションを使用して、ストレージクラスとして S3 Standard、S3 Intelligent-Tiering、S3 Standard – IA、S3 1 ゾーン – IA、または低冗長化を指定しているオブジェクトを上書きします。

- S3 Glacier Deep Archive ストレージクラスへのオブジェクトの移行は一方向のみです。

  S3 ライフサイクル設定ルールを使用して、オブジェクトのストレージクラスを S3 Glacier Deep Archive からその他のストレージクラスに変換することはできません。アーカイブされたオブジェクトのストレージクラスをその他のストレージクラスに変更する場合、まず復元オペレーションを使用してオブジェクトの一時コピーを作成する必要があります。その後、コピーオペレーションを使用して、ストレージクラスとして S3 Standard、S3 Intelligent-Tiering、S3 標準 – IA、S3 1 ゾーン – IA、 S3 Glacier Instant Retrieval、S3 Glacier Flexible Retrieval、または Reduced Redundancy Storage を指定しているオブジェクトを上書きします。

  > **Note**
  >
  > Amazon S3 コンソールでは、S3 Glacier Flexible Retrieval ストレージクラスまたは S3 Glacier Deep Archive ストレージクラス内のオブジェクトに対する、復元したオブジェク

トのコピー操作はサポートしていません。このタイプのコピー操作には、AWS Command Line Interface (AWS CLI)、AWS SDK、または REST API を使用します。

S3 Glacier および S3 Glacier Deep Archive ストレージクラスに保存されているオブジェクトは、Amazon S3 でのみ表示され、使用できます。個々の Amazon S3 Glacier サービスから使用することはできません。

これらは Amazon S3 オブジェクトであるため、Amazon S3 コンソールまたは Amazon S3 API を使用することによってのみアクセスできます。アーカイブされたオブジェクトに、個々の Amazon S3 Glacier コンソールまたは Amazon S3 Glacier API 経由でアクセスすることはできません。

コストに関する考慮事項

アクセス頻度の高いデータを数か月あるいは数年間アーカイブする場合、S3 Glacier および S3 Glacier Deep Archive ストレージクラスを使用する事でストレージコストを削減できます。ただし、S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive ストレージクラスが適切であることを確認するために、以下の点を考慮してください。

- [ストレージオーバーヘッド料金] - オブジェクトを S3 Glacier または S3 Glacier Deep Archive ストレージクラスに移行すると、そのオブジェクトを管理するメタデータを収容するために、各オブジェクトに対して一定量のストレージが追加されます。
  - S3 Glacier または S3 Glacier Deep Archive にアーカイブされたオブジェクトごとに、Amazon S3 ではオブジェクトの名前とその他のメタデータに 8 KB のストレージを使用します。Amazon S3 でこのメタデータを保存する目的は、ユーザーが Amazon S3 API を使用して、アーカイブされたオブジェクトのリアルタイムのリストを取得できるようにすることです。詳細については、[GET Bucket (List Objects)] を参照してください。この追加のストレージに対しては、S3 Standard 料金が発生します。
  - S3 Glacier または S3 Glacier Deep Archive にアーカイブされるオブジェクトごとに、Amazon S3 はインデックスおよび関連するメタデータ用に 32 KB のストレージを追加します。この追加データは、オブジェクトを特定して復元するのに必要です。この追加ストレージに対しては、S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive のレートが課金されます。

  小さいオブジェクトをアーカイブする場合は、これらのストレージ料金を考慮する必要があります。オーバーヘッドコストを削減するには、多数の小さいオブジェクトを少数の大きいオブジェクトに集約する方法があります。

- [オブジェクトをアーカイブしておく日数] — S3 Glacier Flexible Retrieval および S3 Glacier Deep Archive は長期間のアーカイブを行うソリューションです。最小ストレージ期間は、S3 Glacier ストレージクラスの場合は 90 日、S3 Glacier Deep Archive の場合は 180 日です。Amazon S3 Glacier にアーカイブされているデータの削除は、削除するオブジェクトが最小ストレージ期間より長い期間アーカイブされている場合は無料です。アーカイブされたオブジェクトを最小ストレージ期間以内に削除または上書きする場合は、Amazon S3 によって比例配分された早期削除料金が課金されます。早期削除料金の詳細については、「Amazon S3 Glacier から格納後 90 日未満のオブジェクトを削除するにはいくらかかりますか?」を参照してください。質問については、[Amazon S3 のよくある質問] を参照してください。
- [S3 Glacier Flexible Retrieval および S3 Glacier Deep Archive 移行リクエスト料金] — S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive ストレージクラスに移行するオブジェクトごとに 1 つの移行リクエストが作成されます。アーカイブリクエストごとにコストが発生します。多数のオブジェクトを移行する場合は、リクエストのコストを考慮する必要があります。小さなオブジェクト、特に 128KB 未満のオブジェクトを含むオブジェクトを混在させてアーカイブする場合は、ライフサイクルオブジェクトサイズフィルタを使用して移行から小さなオブジェクトを除外し、リクエストコストを削減することをお勧めします。
- [S3 Glacier Flexible Retrieval および S3 Glacier Deep Archive データ復元料金] — S3 Glacier Flexible Retrieval および S3 Glacier Deep Archive は、頻繁にアクセスしないデータの長期アーカイブ用に設計されています。データ復元料金の詳細については、「Amazon S3 Glacier からのデータの復元には、どれだけコストがかかりますか?」を参照してください。質問については、[Amazon S3 のよくある質問] を参照してください。Amazon S3 Glacier からデータを復元する方法については、[アーカイブされたオブジェクトの復元] を参照してください。

> **Note**
>
> S3 ライフサイクルは、オブジェクトを S3 Glacier Flexible Retrieval および S3 Glacier Deep Archive に非同期的に移行します。S3 ライフサイクル設定ルールによる移行の日付と、物理的な移行の日付の間には、遅延が発生する場合があります。この場合、ルールで指定された移行日に基づいて、移行元のストレージクラスのデフォルトレートが課金されます。

Amazon S3 製品詳細ページに、Amazon S3 オブジェクトをアーカイブする場合の料金表情報と計算例が掲載されています。詳細については、次のトピックを参照してください。

- Amazon S3 Glacier にアーカイブされた Amazon S3 オブジェクトのストレージ料金はどのように計算されますか? 質問については、[Amazon S3 のよくある質問] を参照してください。

- Amazon S3 Glacier から格納後 90 日未満のオブジェクトを削除するにはいくらかかりますか? 質問については、[Amazon S3 のよくある質問] を参照してください。
- Amazon S3 Glacier からデータを取り出すのにどれだけのコストがかかりますか? 質問については、[Amazon S3 のよくある質問] を参照してください。
- 標準ストレージクラスと別のストレージクラスのストレージコストを示す Amazon S3 の料金

アーカイブされたオブジェクトの復元

アーカイブされたオブジェクトにはリアルタイムでアクセスできません。まず復元リクエストを開始してから、リクエストで指定した期間中にオブジェクトの一時コピーが利用できるようになるまで待ちます。復元されたオブジェクトの一時コピーの取得後も、オブジェクトのストレージクラスは S3 Glacier または S3 Glacier Deep Archive が保持されます。(HeadObject または GetObject API オペレーションリクエストは、S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive をストレージクラスとして返します)。

> **Note**
>
> アーカイブを復元する場合、アーカイブの費用 (S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive 料金) の他に、一時的に復元されたコピーの費用 (S3 標準ストレージ料金) も発生します。料金については、「Amazon S3 の料金」を参照してください。

オブジェクトのコピーは、プログラムによって、あるいは Amazon S3 コンソールを使用して復元できます。Amazon S3 は、各オブジェクトに対して一度に 1 つの復元リクエストのみを処理します。詳細については、[アーカイブされたオブジェクトの復元] を参照してください。

オブジェクトの有効期限

移行アクションを S3 ライフサイクル設定に追加して、有効期間終了時にオブジェクトを削除するように Amazon S3 に指示できます。ライフサイクル設定に基づいて、オブジェクトの存続期間が終了すると、Amazon S3 はバケットの S3 バージョニング状態に応じて `Expiration` アクションを実行します。

- バージョニングされていないバケット – Amazon S3 はオブジェクトを削除キューに追加して非同期的に削除し、オブジェクトを完全に削除します。
- バージョニングが有効なバケット – 現在のオブジェクトバージョンが削除マーカーではない場合、Amazon S3 は固有のバージョン ID を持つ削除マーカーを追加します。これにより、最新のバージョンが最新以外のバージョンとなり、削除マーカーが最新バージョンになります。

- バージョニングが停止されたバケット — Amazon S3 はバージョン ID として null を使用する削除マーカーを作成します。この削除マーカーは、バージョン階層においてあらゆるオブジェクトバージョンをバージョン ID null に置き換えるため、オブジェクトが効率的に削除されます。

バージョニング対応のバケット (つまり、バージョニングが有効であるかバージョニングが停止されている) の場合、Amazon S3 による `Expiration` アクションの処理方法を決める考慮事項がいくつかあります。バージョニングが有効なバケットまたはバージョニングが停止されたバケットには、以下が適用されます。

- オブジェクトの有効期限は、オブジェクトの最新のバージョンにのみ適用されます(最新以外のバージョンには影響しません)。
- 1 つ以上のオブジェクトバージョンがあり、削除マーカーが最新バージョンである場合、Amazon S3 はアクションを実行しません。
- 現在のオブジェクトバージョンが唯一のオブジェクトバージョンであり、削除マーカーでもある場合 (「期限切れオブジェクト削除マーカー」とも呼ばれます。すべてのオブジェクトバージョンが削除され、削除マーカーのみ残ります)、Amazon S3 は期限切れのオブジェクト削除マーカーを削除します。また、`Expiration` アクションを使用して、期限切れオブジェクト削除マーカーをすべて削除するよう Amazon S3 に指示することもできます。例については、「バージョニングが有効なバケットで期限切れのオブジェクト削除マーカーを削除する」を参照してください。
- アクション要素 `NoncurrentVersionExpiration` を使用すると、Amazon S3 が最新以外のオブジェクトのバージョンを永続的に削除するように指示できます。このように削除されたオブジェクトは復元することはできません。この有効期限切れは、オブジェクトが最新でなくなった以降の特定の日数に基づいて設定できます。日数以外にも、保持する最新以外のバージョンの最大数 (1 ~ 100 の間) を指定することもできます。この値は、Amazon S3 で関連付けられたアクションが実行できるまでに、最新でないバージョンがいくつ必要かを指定します。最新以外のバージョンの最大数を指定するには、`Filter` 要素も指定する必要があります。`Filter` 要素を指定しないで最新以外のバージョンの最大数を指定すると、Amazon S3 で `InvalidRequest` エラーが発生します。アクション要素 `NoncurrentVersionExpiration` の使用方法の詳細については、「the section called “ライフサイクルアクションを記述する要素”」を参照してください。
- Amazon S3 は、S3 オブジェクトロック設定が適用されており、最新でないバージョンのオブジェクトに対しては、アクションを実行しません。
- `Pending` レプリケーションステータスのオブジェクトの場合、オブジェクトの現在のバージョンまたは以前のバージョンに対して Amazon S3 はアクションを実行しません。

詳細については、「S3 バージョニングによる複数のバージョンのオブジェクトの保持」を参照してください。

> **Important**
>
> S3 ライフサイクル設定に複数のルールがある場合、1 つのオブジェクトが同じ日に複数の S3 ライフサイクルアクションの対象になることがあります。このような場合、Amazon S3 は以下の一般的なルールに従います。
>
> - 完全な削除は、移行より優先されます。
> - 移行は、削除マーカーの作成より優先されます。
> - オブジェクトが S3 Glacier Flexible Retrieval と S3 Standard-IA (または S3 One Zone-IA) 移行の両方の対象になる場合、Amazon S3 は S3 Glacier Flexible Retrieval 移行を選択します。
>
> 例については「重複するフィルタ、競合するライフサイクルアクションの例」を参照してください。

既存のオブジェクトと新しいオブジェクト

ライフサイクル設定をバケットに追加すると、設定ルールは既存のオブジェクトとそれ以降に追加されるオブジェクトの両方に適用されます。例えば、特定のプレフィックスが付いたオブジェクトが作成から 30 日後に有効期限を迎えるようにする失効アクションを備えたライフサイクル設定ルールを本日追加すると、Amazon S3 により作成から 30 日以上が経過し、指定されたプレフィックスを持つ既存のオブジェクトがすべて削除キューに追加されます。

> **Important**
>
> バケットポリシーを使用して、S3 ライフサイクルルールによる削除や移行を防ぐことはできません。例えば、バケットポリシーがすべてのプリンシパルのすべてのアクションを拒否する場合でも、S3 ライフサイクル設定は通常どおり機能します。

オブジェクトの有効期限を確認する方法

オブジェクトの現在のバージョンに設定されている有効期限を確認するには、HeadObject または GetObject の API オペレーションを使用します。これらの API オペレーションでは、オブジェクト

の現在のバージョンがキャッシュ可能でなくなる日時が指定されたレスポンスヘッダーが返されます。

> **Note**
>
> - 有効期限が切れる日と Amazon S3 がオブジェクトを削除する日との間に遅延が生じることがあります。期限切れのオブジェクトに関連付けられている有効期限切れ、またはストレージ期間に対する料金は請求されません。
> - ライフサイクルルールを更新、無効化、または削除する前に、LIST API オペレーション (ListObjectsV2、ListObjectVersions、ListMultipartUploads など) または S3 インベントリを使用したデータのカタログ化と分析 を使用して、ユースケースに基づき、Amazon S3 が移行済みで対象となるオブジェクトの有効期限が切れていることを確認します。

最小ストレージ期間料金

S3 Standard – IA、または S3 1 ゾーン – IA のストレージにあった期間が 30 日未満のオブジェクトを失効させる S3 ライフサイクル失効ルールを作成すると、30 日間の料金が発生します。S3 Glacier ストレージにあった期間が 90 日未満のオブジェクトを失効させるライフサイクル有効期限ルールを作成すると、90 日間の料金が発生します。S3 Glacier Deep Archive ストレージにあった期間が 180 日未満のオブジェクトを失効させるライフサイクル失効ルールを作成すると、180 日間の料金が発生します。

詳細については、「Amazon S3 の料金」を参照してください。

バケットに S3 ライフサイクル設定を設定する

Amazon S3 コンソール、AWS Command Line Interface (AWS CLI)、AWS SDK、または Amazon S3 REST API を使用して、バケットに Amazon S3 ライフサイクル設定を指定できます。S3 ライフサイクル設定については、「オブジェクトのライフサイクルの管理」を参照してください。

> **Note**
>
> ディレクトリバケットのライフサイクル設定を表示または編集するには、AWS CLI、AWS SDK、または Amazon S3 REST API を使用します。詳細については、「ディレクトリバケットの S3 ライフサイクルの使用」を参照してください。

S3 ライフサイクル設定では、ライフサイクルルールを使用して、オブジェクトの存続期間中に Amazon S3 が実行するアクションを定義します。例えば、オブジェクトを別のストレージクラスに移行したり、オブジェクトをアーカイブしたり、指定した期間後にオブジェクトを期限切れ (削除) したりするルールを定義できます。

S3 ライフサイクルに関する考慮事項

ライフサイクル設定を設定する前に、次の点に注意してください。

ライフサイクル設定の伝播の遅延

バケットに対してライフサイクル設定を追加する場合、新しい、あるいは更新された S3 ライフサイクル設定がすべての Amazon S3 システムに完全に伝達されるまでには、通常、多少のタイムラグがあります。ライフサイクル設定が完全に有効になるまで、数分間程度の遅延を想定してください。この遅延は、S3 ライフサイクル設定を削除するときにも発生することがあります。

移行または有効期限の遅延

ライフサイクルルールが満たされてから、ルールのアクションが完了するまでに遅延が生じる場合があります。例えば、ライフサイクルルールによって一連のオブジェクトの有効期限が 1 月 1 日に切れるとします。有効期限ルールは 1 月 1 日に満たされますが、Amazon S3 は数日後または数週間後までこれらのオブジェクトを実際に削除しない場合があります。この遅延は、S3 ライフサイクルがオブジェクトを移行または有効期限のためのキューに非同期的に入れるために発生します。請求の変更は、通常、アクションが完了していなくても、ライフサイクルルールが満たされた際に適用されます。詳細については、「請求の変更」を参照してください。アクティブなライフサイクルルールによって行われた更新の影響をモニタリングするには、「the section called “ライフサイクルルールによって実行されたアクションをモニタリングするにはどうすればよいですか？”」を参照してください。

ライフサイクルルールの更新、無効化、または削除

ライフサイクルルールを無効にする、あるいは削除すると、わずかなタイムラグの後に、Amazon S3 は新しいオブジェクトの削除や移行のスケジューリングを停止します。スケジュール済みのオブジェクトはスケジュール解除され、削除または移行されません。

> **Note**
>
> ライフサイクルルールを更新、無効化、または削除する前に、LIST API オペレーション (ListObjectsV2、ListObjectVersions、ListMultipartUploads など) または S3 インベントリを使用したデータのカタログ化と分析 を使用して、ユースケースに基づき、Amazon S3 が移

行済みで対象となるオブジェクトの有効期限が切れていることを確認します。ライフサイクルルールの更新、無効化、削除に問題がある場合は、「Amazon S3 ライフサイクル問題のトラブルシューティング」を参照してください。

既存のオブジェクトと新しいオブジェクト

ライフサイクル設定をバケットに追加すると、設定ルールは既存のオブジェクトとそれ以降に追加されるオブジェクトの両方に適用されます。例えば、特定のプレフィックスが付いたオブジェクトが作成から 30 日後に有効期限を迎えるようにする失効アクションを備えたライフサイクル設定ルールを本日追加すると、Amazon S3 により作成から 30 日以上が経過し、指定されたプレフィックスを持つ既存のオブジェクトがすべて削除キューに追加されます。

ライフサイクルルールの影響のモニタリング

アクティブなライフサイクルルールによって行われた更新の影響をモニタリングするには、「the section called “ライフサイクルルールによって実行されたアクションをモニタリングするにはどうすればよいですか？”」を参照してください。

請求の変更

ライフサイクル設定のルールが満たされてから、実際にアクションが実行されるまでの間には、遅延が発生する場合があります。ただし、アクションが実行されていなくても、ライフサイクル設定のルールが満たされた段階で、請求にはすぐに変更が反映されます。

たとえば、オブジェクトの有効期限が切れると、オブジェクトがすぐに削除されなくても、そのストレージは課金対象から外されます。同様に、オブジェクトの移行期間を過ぎると、オブジェクトがすぐに S3 Glacier Flexible Retrieval ストレージクラスに移行されていなくても、S3 Glacier Flexible Retrieval ストレージ料金が請求されます。

ただし、S3 Intelligent-Tiering ストレージクラスへのライフサイクルの移行については例外です。オブジェクトが S3 Intelligent-Tiering ストレージクラスに移行するまで、請求の変更は行われません。

複数のルールまたは競合するルール

S3 ライフサイクル設定に複数のルールがある場合、1 つのオブジェクトが同じ日に複数の S3 ライフサイクルアクションの対象になることがあります。このような場合、Amazon S3 は以下の一般的なルールに従います。

- 完全な削除は、移行より優先されます。

- 移行は、削除マーカーの作成より優先されます。
- オブジェクトが S3 Glacier Flexible Retrieval と S3 Standard-IA (または S3 One Zone-IA) 移行の両方の対象になる場合、Amazon S3 は S3 Glacier Flexible Retrieval 移行を選択します。

例については「重複するフィルタ、競合するライフサイクルアクションの例」を参照してください。

S3 ライフサイクル設定を設定する方法

Amazon S3 コンソール、AWS Command Line Interface (AWS CLI)、AWS SDK、または Amazon S3 REST API を使用して、汎用バケットに Amazon S3 ライフサイクル設定を指定できます。

AWS CloudFormation テンプレートと例の詳細については、「AWS CloudFormation ユーザーガイド」の「AWS CloudFormation テンプレートの使用」および「AWS::S3::Bucket」を参照してください。

S3 コンソールの使用

共有プレフィックス (共通の文字列から始まるオブジェクト名) またはタグを使用して、バケット内のすべてのオブジェクトまたはオブジェクトのサブセットに対してライフサイクルルールを定義できます。ライフサイクルルールでは、現在のバージョンまたは以前のバージョンのオブジェクトに対して独自のアクションを定義できます。詳細については次を参照してください:

- オブジェクトのライフサイクルの管理
- S3 バージョニングによる複数のバージョンのオブジェクトの保持

ライフサイクルルールを作成するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[汎用バケット] を選択します。
3. バケットリストで、ライフサイクルルールを作成するバケットの名前を選択します。
4. [Management (管理)] タブを選択して、[Create lifecycle rule (ライフサイクルルールを作成する)] を選択します。
5. [Lifecycle rule name (ライフサイクルルール名)] に、ルールの名前を入力します。

   その名前はバケット内で一意である必要があります。
6. ライフサイクルルールのスコープを選択します。

- 特定のプレフィックスまたはタグを持つすべてのオブジェクトにこのライフサイクルルールを適用するには、[スコープを特定のプレフィックスまたはタグに制限] を選択します。
  - スコープをプレフィックスで制限するには、[Prefix (プレフィックス)] にプレフィックスを入力します。
  - スコープをタグで制限するには、[Add tag (タグの追加)] を選択してタグのキーと値を入力します。

  オブジェクト名のプレフィックスの詳細については、「Amazon S3 オブジェクトに命名する」を参照してください。オブジェクトロックの詳細については、タグを使用してストレージを分類するをご参照ください。
- このライフサイクルルールをバケット内のすべてのオブジェクトに適用するには、[このルールは、バケット内のすべてのオブジェクトに適用されます] を選択して、[このライフサイクルルールがバケット内のすべてのオブジェクトに適用されることを了承します] を選択します。

7. オブジェクトサイズでルールをフィルタリングするには、[最小オブジェクトサイズを指定]、[最大オブジェクトサイズを指定]、または両方のオプションを選択します。

   - [最小オブジェクトサイズ] または [最大オブジェクトサイズ] の値を指定する際は、0 バイトより大きく、5 TB 未満の範囲の値を指定する必要があります。この値はバイト、KB、MB、または GB で指定できます。
   - 両方の値を指定する際は、最大オブジェクトサイズを最小オブジェクトサイズよりも大きい値に設定する必要があります。

   > **Note**
   >
   > [最小オブジェクトサイズ] フィルターおよび [最大オブジェクトサイズ] フィルターは、指定された値を除外します。例えば、[最小オブジェクトサイズ] で 128 KB のオブジェクトを期限切れにするようにフィルターを設定した場合、128 KB ちょうどのオブジェクトは期限切れになりません。代わりに、このルールは 128 KB より大きいサイズのオブジェクトにのみ適用されます。

8. [Lifecycle rule actions (ライフサイクルルールのアクション)] で、ライフサイクルルールで実行するアクションを以下から選択します。

   - オブジェクトの現在のバージョンをストレージクラス間で移行する
   - オブジェクトの以前のバージョンをストレージクラス間で移動する
   - オブジェクトの現在のバージョンを期限切れにする

> **Note**
>
> S3 バージョニングが有効化されていないバケットの場合、現在のバージョンの有効期限が切れると、Amazon S3 はオブジェクトを完全に削除します。詳細については、「the section called “ライフサイクルのアクションとバケットのバージョニング状態”」を参照してください。

- オブジェクトの以前のバージョンを完全に削除する
- 期限切れの削除マーカーまたは未完了のマルチパートアップロードを削除する

選択したアクションに応じて、異なるオプションが表示されます。

9. オブジェクトの現在のバージョンをストレージクラス間で移行するには、[オブジェクトの現在のバージョンをストレージクラス間で移行する] で以下を行います。

   a. [ストレージクラスへの移行] で、移行するストレージクラスを選択します。利用できる移行のリストについては、「the section called “サポートされているライフサイクル移行”」を参照してください。以下のストレージクラスから選択できます。

      - S3 Standard – IA
      - S3 Intelligent-Tiering
      - S3 1 ゾーン - IA
      - S3 Glacier インスタント取得
      - S3 Glacier Flexible Retrieval
      - S3 Glacier Deep Archive

   b. [Days after object creation (オブジェクトが作成されてからの日数)] に、オブジェクトの作成から移行までの日数を入力します。

   ストレージクラスの詳細については、「Amazon S3 ストレージクラスの理解と管理」を参照してください。オブジェクトの現在のバージョンだけ、以前のバージョンだけ、または現在と以前の両方のバージョンについて、移行を定義できます。バージョニングを使用すると、1 つのバケットで複数バージョンのオブジェクトを維持できます。バージョニングの詳細については、「S3 コンソールの使用」を参照してください。

> **Important**
>
> S3 Glacier Instant Retrieval、S3 Glacier Flexible Retrieval あるいは Glacier Deep Archive ストレージクラスを選択した場合は、オブジェクトは Amazon S3 に保持されます。Amazon S3 Glacier サービスを別途使用して直接アクセスすることはできません。詳細については、「Amazon S3 ライフサイクルを使用したオブジェクトの移行」を参照してください。

10. ストレージクラス間で最新以外のオブジェクトを移行するには、[オブジェクトの非現行バージョンをストレージクラス間で移行する] で以下を行います。

    a. [ストレージクラスへの移行] で、移行するストレージクラスを選択します。利用できる移行のリストについては、「the section called “サポートされているライフサイクル移行”」を参照してください。以下のストレージクラスから選択できます。

       - S3 Standard – IA
       - S3 Intelligent-Tiering
       - S3 1 ゾーン - IA
       - S3 Glacier インスタント取得
       - S3 Glacier Flexible Retrieval
       - S3 Glacier Deep Archive

    b. [Days after object becomes noncurrent] に、オブジェクトの作成日から移行日までの日数を入力します。

11. オブジェクトの現行バージョンを期限切れにするには、[Expire current versions of objects] (オブジェクトの現行バージョンを期限切れにする) で、[Number of days after object creation] (オブジェクトの作成後の日数) に日数を入力します。

> **Important**
>
> バージョニング非対応のバケットの場合、アクションを実行すると、Amazon S3 はオブジェクトを完全に削除します。ライフサイクルアクションの詳細については、「ライフサイクルアクションを記述する要素」を参照してください。

12. オブジェクトの以前のバージョンを完全に削除するには、[Permanently delete noncurrent versions of objects] (現在のバージョンではないオブジェクトを完全に削除する) で、[Days after objects become noncurrent] (オブジェクトが最新バージョンでなくなってからの日数) に日数を

入力します。オプションで、[Number of newer versions to retain] (保持する新しいバージョンの数) に値を入力して、保持する新しいバージョンの数を指定できます。

13. [Delete expired delete markers or incomplete multipart uploads (期限切れの削除マーカーまたは未完了のマルチパートアップロードを削除する)] で、[Delete expired object delete markers (期限切れのオブジェクト削除マーカーを削除する)] と [Delete incomplete multipart uploads (不完全なマルチパートアップロードを削除)] を選択します。次に、マルチパートアップロードの開始から未完了のマルチパートアップロードを終了してクリーンアップするまでの日数を入力します。

    マルチパートアップロードの詳細については、「Amazon S3 でのマルチパートアップロードを使用したオブジェクトのアップロードとコピー」を参照してください。

14. [Create rule] を選択します。

    ルールにエラーがない場合は、Amazon S3 によって有効にされ、[Management (管理)] タブの [Lifecycle rules (ライフサイクルルール)] に表示されます。

AWS CLI の使用

次の AWS CLI コマンドを使用して、S3 ライフサイクル設定を管理できます。

- `put-bucket-lifecycle-configuration`
- `get-bucket-lifecycle-configuration`
- `delete-bucket-lifecycle`

AWS CLI の設定の手順については、「Amazon S3 API リファレンス」の「AWS CLI を使用した Amazon S3 での開発」を参照してください。

Amazon S3 ライフサイクル設定は XML ファイルである点に注意してください。ただし、AWS CLI を使用する場合、XML 形式を指定することはできません。代わりに JSON 形式を指定する必要があります。XML ライフサイクル設定の例と、AWS CLI コマンドで指定できる同等の JSON の設定は、次のとおりです。

次のサンプル S3 ライフサイクル設定を検討してください。

Example 例 1

Example

XML

```
<LifecycleConfiguration>
    <Rule>
        <ID>ExampleRule</ID>
        <Filter>
           <Prefix>documents/</Prefix>
        </Filter>
        <Status>Enabled</Status>
        <Transition>
           <Days>365</Days>
           <StorageClass>GLACIER</StorageClass>
        </Transition>
        <Expiration>
             <Days>3650</Days>
        </Expiration>
    </Rule>
</LifecycleConfiguration>
```

JSON

```
{
    "Rules": [
        {
            "Filter": {
                "Prefix": "documents/"
            },
            "Status": "Enabled",
            "Transitions": [
                {
                    "Days": 365,
                    "StorageClass": "GLACIER"
                }
            ],
            "Expiration": {
                "Days": 3650
            },
            "ID": "ExampleRule"
```

```
        }
    ]
}
```

Example 例 2

Example

XML

```
<LifecycleConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
    <Rule>
        <ID>id-1</ID>
        <Expiration>
            <Days>1</Days>
        </Expiration>
        <Filter>
            <And>
                <Prefix>myprefix</Prefix>
                <Tag>
                    <Key>mytagkey1</Key>
                    <Value>mytagvalue1</Value>
                </Tag>
                <Tag>
                    <Key>mytagkey2</Key>
                    <Value>mytagvalue2</Value>
                </Tag>
            </And>
        </Filter>
        <Status>Enabled</Status>
    </Rule>
</LifecycleConfiguration>
```

JSON

```
{
    "Rules": [
        {
            "ID": "id-1",
            "Filter": {
                "And": {
```

```
                    "Prefix": "myprefix",
                    "Tags": [
                        {
                            "Value": "mytagvalue1",
                            "Key": "mytagkey1"
                        },
                        {
                            "Value": "mytagvalue2",
                            "Key": "mytagkey2"
                        }
                    ]
                }
            },
            "Status": "Enabled",
            "Expiration": {
                "Days": 1
            }
        }
    ]
}
```

以下のように put-bucket-lifecycle-configuration をテストできます。

設定をテストする

1. JSON のライフサイクル設定をファイル (*lifecycle.json* など) に保存します。
2. 以下の AWS CLI コマンドを実行して、バケットにライフサイクル設定を指定します。*user input placeholders* を、ユーザー自身の情報に置き換えます。

```
$ aws s3api put-bucket-lifecycle-configuration  \
--bucket amzn-s3-demo-bucket  \
--lifecycle-configuration file://lifecycle.json
```

3. 検証するには、次のとおり get-bucket-lifecycle-configuration AWS CLI コマンドを使用して S3 ライフサイクル設定を取得します。

```
$ aws s3api get-bucket-lifecycle-configuration  \
--bucket amzn-s3-demo-bucket
```

4. S3 ライフサイクル設定を削除するには、次のとおり delete-bucket-lifecycle AWS CLI コマンドを使用します。

```
aws s3api delete-bucket-lifecycle \
--bucket amzn-s3-demo-bucket
```

AWS SDK の使用

Java

AWS SDK for Java を使用して、バケットの S3 ライフサイクル設定を管理できます。S3 ライフサイクル設定の管理の詳細については、「オブジェクトのライフサイクルの管理」を参照してください。

> **Note**
>
> バケットに S3 ライフサイクル設定を追加すると、Amazon S3 でバケットの現在のライフサイクル設定 (ある場合) が置き換えられます。設定を更新するには、設定を取得して必要な変更を加え、変更済みの設定をバケットに追加します。

以下の例では、AWS SDK for Java を使用してバケットのライフサイクル設定を追加、更新、削除する方法を示します。この例では、次のような処理を実行します。

- ライフサイクル設定をバケットに追加します。
- ライフサイクル設定を取得し、別のルールを追加して設定を更新します。
- バケットに変更済みのライフサイクル設定を追加します。Amazon S3 によって既存の設定が置き換えられます。
- 設定をもう一度取得し、ルールの数を出力して、適切な数のルールがあることを確認します。
- ライフサイクル設定を削除し、削除済みであることを確認するために、設定の取得を再度試行します。

作業サンプルの作成およびテストの手順については、「AWS SDK for Java デベロッパーガイド」の「使用開始」を参照してください。

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
```

```
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.BucketLifecycleConfiguration;
import com.amazonaws.services.s3.model.BucketLifecycleConfiguration.Transition;
import com.amazonaws.services.s3.model.StorageClass;
import com.amazonaws.services.s3.model.Tag;
import com.amazonaws.services.s3.model.lifecycle.LifecycleAndOperator;
import com.amazonaws.services.s3.model.lifecycle.LifecycleFilter;
import com.amazonaws.services.s3.model.lifecycle.LifecyclePrefixPredicate;
import com.amazonaws.services.s3.model.lifecycle.LifecycleTagPredicate;

import java.io.IOException;
import java.util.Arrays;

public class LifecycleConfiguration {

        public static void main(String[] args) throws IOException {
                Regions clientRegion = Regions.DEFAULT_REGION;
                String bucketName = "*** Bucket name ***";

                // Create a rule to archive objects with the "glacierobjects/"
 prefix to Glacier
                // immediately.
                BucketLifecycleConfiguration.Rule rule1 = new
 BucketLifecycleConfiguration.Rule()
                                .withId("Archive immediately rule")
                                .withFilter(new LifecycleFilter(new
 LifecyclePrefixPredicate("glacierobjects/")))
                                .addTransition(new
 Transition().withDays(0).withStorageClass(StorageClass.Glacier))
                                .withStatus(BucketLifecycleConfiguration.ENABLED);

                // Create a rule to transition objects to the Standard-Infrequent
 Access storage
                // class
                // after 30 days, then to Glacier after 365 days. Amazon S3 will
 delete the
                // objects after 3650 days.
                // The rule applies to all objects with the tag "archive" set to
 "true".
                BucketLifecycleConfiguration.Rule rule2 = new
 BucketLifecycleConfiguration.Rule()
                                .withId("Archive and then delete rule")
```

```
                                .withFilter(new LifecycleFilter(new
LifecycleTagPredicate(new Tag("archive", "true"))))
                                .addTransition(new Transition().withDays(30)

.withStorageClass(StorageClass.StandardInfrequentAccess))
                                .addTransition(new
Transition().withDays(365).withStorageClass(StorageClass.Glacier))
                                .withExpirationInDays(3650)
                                .withStatus(BucketLifecycleConfiguration.ENABLED);

                // Add the rules to a new BucketLifecycleConfiguration.
                BucketLifecycleConfiguration configuration = new
BucketLifecycleConfiguration()
                                .withRules(Arrays.asList(rule1, rule2));

                try {
                        AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                                        .withCredentials(new
ProfileCredentialsProvider())
                                        .withRegion(clientRegion)
                                        .build();

                        // Save the configuration.
                        s3Client.setBucketLifecycleConfiguration(bucketName,
configuration);

                        // Retrieve the configuration.
                        configuration =
s3Client.getBucketLifecycleConfiguration(bucketName);

                        // Add a new rule with both a prefix predicate and a tag
predicate.
                        configuration.getRules().add(new
BucketLifecycleConfiguration.Rule().withId("NewRule")
                                        .withFilter(new LifecycleFilter(new
LifecycleAndOperator(
                                                        Arrays.asList(new
LifecyclePrefixPredicate("YearlyDocuments/"),
                                                                        new
LifecycleTagPredicate(new Tag(

   "expire_after",

   "ten_years"))))))
```

```
                                        .withExpirationInDays(3650)

 .withStatus(BucketLifecycleConfiguration.ENABLED));

                        // Save the configuration.
                        s3Client.setBucketLifecycleConfiguration(bucketName,
 configuration);

                        // Retrieve the configuration.
                        configuration =
 s3Client.getBucketLifecycleConfiguration(bucketName);

                        // Verify that the configuration now has three rules.
                        configuration =
 s3Client.getBucketLifecycleConfiguration(bucketName);
                        System.out.println("Expected # of rules = 3; found: " +
 configuration.getRules().size());

                        // Delete the configuration.
                        s3Client.deleteBucketLifecycleConfiguration(bucketName);

                        // Verify that the configuration has been deleted by
 attempting to retrieve it.
                        configuration =
 s3Client.getBucketLifecycleConfiguration(bucketName);
                        String s = (configuration == null) ? "No configuration
 found." : "Configuration found.";
                        System.out.println(s);
                } catch (AmazonServiceException e) {
                        // The call was transmitted successfully, but Amazon S3
 couldn't process
                        // it, so it returned an error response.
                        e.printStackTrace();
                } catch (SdkClientException e) {
                        // Amazon S3 couldn't be contacted for a response, or the
 client
                        // couldn't parse the response from Amazon S3.
                        e.printStackTrace();
                }
        }
}
```

.NET

AWS SDK for .NET を使用して、バケットの S3 ライフサイクル設定を管理できます。ライフサイクル設定の管理の詳細については、「オブジェクトのライフサイクルの管理」を参照してください。

> **Note**
>
> ライフサイクル設定を追加すると、Amazon S3 で、指定したバケットの既存のライフサイクル設定が置き換えられます。設定を更新するには、まずライフサイクル設定を取得して変更を加え、次に変更済みのライフサイクル設定をバケットに追加する必要があります。

以下の例では、AWS SDK for .NET を使用してバケットのライフサイクル設定を追加、更新、削除する方法を示します。このコード例では、以下を行います。

- ライフサイクル設定をバケットに追加します。
- ライフサイクル設定を取得し、別のルールを追加して設定を更新します。
- バケットに変更済みのライフサイクル設定を追加します。Amazon S3 によって既存のライフサイクル設定が置き換えられます。
- 再び設定を取得し、設定のルール数を出力して適切な数であることを確認します。
- ライフサイクル設定を削除し、削除を確認します。

コード例を設定および実行する方法の詳細については、「AWS SDK for .NET デベロッパーガイド」の「AWS SDK for .NET の開始方法」を参照してください。

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Collections.Generic;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class LifecycleTest
    {
        private const string bucketName = "*** bucket name ***";
```

```
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
RegionEndpoint.USWest2;
        private static IAmazonS3 client;
        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            AddUpdateDeleteLifecycleConfigAsync().Wait();
        }

        private static async Task AddUpdateDeleteLifecycleConfigAsync()
        {
            try
            {
                var lifeCycleConfiguration = new LifecycleConfiguration()
                {
                    Rules = new List<LifecycleRule>
                        {
                            new LifecycleRule
                            {
                                 Id = "Archive immediately rule",
                                 Filter = new LifecycleFilter()
                                 {
                                     LifecycleFilterPredicate = new
LifecyclePrefixPredicate()
                                     {
                                         Prefix = "glacierobjects/"
                                     }
                                 },
                                 Status = LifecycleRuleStatus.Enabled,
                                 Transitions = new List<LifecycleTransition>
                                 {
                                      new LifecycleTransition
                                      {
                                           Days = 0,
                                           StorageClass = S3StorageClass.Glacier
                                      }
                                  },
                            },
                            new LifecycleRule
                            {
                                 Id = "Archive and then delete rule",
                                  Filter = new LifecycleFilter()
                                 {
```

```
                                    LifecycleFilterPredicate = new
LifecyclePrefixPredicate()
                                    {
                                        Prefix = "projectdocs/"
                                    }
                                },
                                Status = LifecycleRuleStatus.Enabled,
                                Transitions = new List<LifecycleTransition>
                                {
                                     new LifecycleTransition
                                     {
                                          Days = 30,
                                          StorageClass =
S3StorageClass.StandardInfrequentAccess
                                     },
                                     new LifecycleTransition
                                     {
                                       Days = 365,
                                       StorageClass = S3StorageClass.Glacier
                                     }
                                },
                                Expiration = new LifecycleRuleExpiration()
                                {
                                      Days = 3650
                                }
                            }
                        }
                };

                // Add the configuration to the bucket.
                await AddExampleLifecycleConfigAsync(client,
lifeCycleConfiguration);

                // Retrieve an existing configuration.
                lifeCycleConfiguration = await RetrieveLifecycleConfigAsync(client);

                // Add a new rule.
                lifeCycleConfiguration.Rules.Add(new LifecycleRule
                {
                    Id = "NewRule",
                    Filter = new LifecycleFilter()
                    {
                        LifecycleFilterPredicate = new LifecyclePrefixPredicate()
                        {
```

```
                            Prefix = "YearlyDocuments/"
                        }
                    },
                    Expiration = new LifecycleRuleExpiration()
                    {
                        Days = 3650
                    }
                });

                // Add the configuration to the bucket.
                await AddExampleLifecycleConfigAsync(client,
lifeCycleConfiguration);

                // Verify that there are now three rules.
                lifeCycleConfiguration = await RetrieveLifecycleConfigAsync(client);
                Console.WriteLine("Expected # of rulest=3; found:{0}",
lifeCycleConfiguration.Rules.Count);

                // Delete the configuration.
                await RemoveLifecycleConfigAsync(client);

                // Retrieve a nonexistent configuration.
                lifeCycleConfiguration = await RetrieveLifecycleConfigAsync(client);

            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered ***. Message:'{0}' when writing
an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
writing an object", e.Message);
            }
        }

        static async Task AddExampleLifecycleConfigAsync(IAmazonS3 client,
LifecycleConfiguration configuration)
        {

            PutLifecycleConfigurationRequest request = new
PutLifecycleConfigurationRequest
            {
```

```
                BucketName = bucketName,
                Configuration = configuration
            };
            var response = await client.PutLifecycleConfigurationAsync(request);
        }

        static async Task<LifecycleConfiguration>
 RetrieveLifecycleConfigAsync(IAmazonS3 client)
        {
            GetLifecycleConfigurationRequest request = new
 GetLifecycleConfigurationRequest
            {
                BucketName = bucketName
            };
            var response = await client.GetLifecycleConfigurationAsync(request);
            var configuration = response.Configuration;
            return configuration;
        }

        static async Task RemoveLifecycleConfigAsync(IAmazonS3 client)
        {
            DeleteLifecycleConfigurationRequest request = new
 DeleteLifecycleConfigurationRequest
            {
                BucketName = bucketName
            };
            await client.DeleteLifecycleConfigurationAsync(request);
        }
    }
}
```

Ruby

AWS SDK for Ruby を使用すると、AWS::S3::BucketLifecycleConfiguration クラスを使用してバケットの S3 ライフサイクル設定を管理できます。S3 ライフサイクル設定の管理の詳細については、「オブジェクトのライフサイクルの管理」を参照してください。

REST API の使用

「Amazon Simple Storage Service API リファレンス」の以下のトピックでは、S3 ライフサイクル設定に関連する REST API オペレーションについて説明しています。

- PutBucketLifecycleConfiguration
- GetBucketLifecycleConfiguration
- DeleteBucketLifecycle

S3 ライフサイクルのトラブルシューティング

S3 ライフサイクルの使用時に発生する可能性がある一般的な問題については、「the section called "ライフサイクル問題のトラブルシューティング"」を参照してください。

S3 ライフサイクルは他のバケット設定とどのように相互作用するか

S3 ライフサイクル設定に加えて、バケットに他の設定を関連付けることができます。このセクションでは、S3 ライフサイクル設定と他のバケット設定の関連について説明します。

S3 ライフサイクルと S3 バージョニング

S3 ライフサイクル設定は、バージョニング対応および非対応のどちらのバケットにも追加できます。詳細については、[S3 バージョニングによる複数のバージョンのオブジェクトの保持] を参照してください。

バケットのバージョニングが有効になっている場合は、最新のオブジェクトバージョン 1 個と、0 個以上の以前のバージョンが維持されます。現在のオブジェクトバージョンと以前のオブジェクトバージョン用に異なるライフサイクルルールを定義できます。

詳細については、「ライフサイクル設定の要素」を参照してください。

> **Important**
>
> S3 ライフサイクル設定に複数のルールがある場合、1 つのオブジェクトが同じ日に複数の S3 ライフサイクルアクションの対象になることがあります。このような場合、Amazon S3 は以下の一般的なルールに従います。
>
> - 完全な削除は、移行より優先されます。
> - 移行は、削除マーカーの作成より優先されます。
> - オブジェクトが S3 Glacier Flexible Retrieval 移行と S3 標準 – IA 移行 (または S3 1 ゾーン – IA 移行) の両方の対象になる場合、Amazon S3 は S3 Glacier Flexible Retrieval の移行を選択します。

例については「重複するフィルタ、競合するライフサイクルアクションの例」を参照してください。

MFA が有効なバケットでの S3 ライフサイクル設定

多要素認証のバケットで S3 ライフサイクル設定を MFA 削除に設定することはサポートされていません。詳細については、「MFA 削除の設定」を参照してください。

S3 ライフサイクルとログ記録

Amazon S3 ライフサイクルアクションは、AWS CloudTrail オブジェクトレベルのログ記録ではキャプチャされません。CloudTrail は外部の Amazon S3 エンドポイントに対して行われた API リクエストをキャプチャしますが、S3 ライフサイクルアクションは内部の Amazon S3 エンドポイントを使用して実行されます。

S3 バケットで Amazon S3 サーバーアクセスログを有効にして、別のストレージクラスへのオブジェクトの移行やオブジェクトの失効など、S3 ライフサイクル関連のアクションをキャプチャして、完全な削除または論理的な削除を行うことができます。詳細については、「the section called "サーバーアクセスのログ記録"」を参照してください。

バケットでログ記録を有効にしている場合、Amazon S3 サーバーアクセスログで以下のオペレーションの結果がレポートされます。

オペレーションログ	説明
`S3.EXPIRE.OBJECT`	Amazon S3 は、ライフサイクルの `Expiration` アクションに沿って、オブジェクトを完全に削除します。
`S3.CREATE.DELETEMARKER`	Amazon S3 はバージョニングが有効なバケットに削除マーカーを追加することにより、現在のバージョンを論理的に削除します。
`S3.TRANSITION_SIA.OBJECT`	Amazon S3 はオブジェクトを S3 Standard – IA ストレージクラスに移行しました。

オペレーションログ	説明
S3.TRANSITION_ZIA.OBJECT	Amazon S3 はオブジェクトを S3 1 ゾーン – IA ストレージクラスに移行しました。
S3.TRANSITION_INT.OBJECT	Amazon S3 はオブジェクトを S3 Intelligent-Tiering ストレージクラスに移行します。
S3.TRANSITION_GIR.OBJECT	Amazon S3 は、オブジェクトの S3 Glacier Instant Retrieval ストレージクラスへの移行を開始します。
S3.TRANSITION.OBJECT	Amazon S3 は、オブジェクトの S3 Glacier Flexible Retrieval ストレージクラスへの移行を開始します。
S3.TRANSITION_GDA.OBJECT	Amazon S3 は、オブジェクトの S3 Glacier Deep Archive ストレージクラスへの移行を開始します。
S3.DELETE.UPLOAD	Amazon S3 は不完全なマルチパートアップロードを中止します。

> **Note**
>
> Amazon S3 サーバーアクセスログレコードは、ベストエフォートベースで配信され、すべての Amazon S3 リクエストの完全なアカウンティングには使用できません。

S3 ライフサイクルイベント通知の設定

S3 ライフサイクルルールに従った結果、Amazon S3 がオブジェクトを削除したり、別の Amazon S3 ストレージクラスに移行したりした場合に通知を受け取るには、Amazon S3 イベント通知を設定することができます。

次の S3 ライフサイクルイベントの通知を受信できます。

- 移行イベント – s3:LifecycleTransition イベントタイプを使用すると、S3 ライフサイクル設定により、ある Amazon S3 ストレージクラスから別のストレージクラスにオブジェクトが移行された場合に通知を受け取ることができます。
- 有効期限切れ (削除) イベント – LifecycleExpiration イベントタイプを使用すると、Amazon S3 が S3 ライフサイクル設定に基づいてオブジェクトを削除する都度、通知を受け取ることができます。

  有効期限切れイベントには 2 つのタイプがあります。

  - s3:LifecycleExpiration:Delete イベントタイプは、バージョン設定されていないバケット内のオブジェクトが削除されたときに通知します。s3:LifecycleExpiration:Delete は、S3 ライフサイクル設定によってオブジェクトバージョンが完全に削除されたときにも通知します。
  - この s3:LifecycleExpiration:DeleteMarkerCreated は、バージョニングされているバケット内のオブジェクトの最新バージョンが削除され、S3 ライフサイクルが削除マーカーを作成した場合に通知します。S3 ライフサイクルは、削除マーカーの作成時間を現在の日の 00:00 UTC (午前 0 時) に設定します。この作成時間は、S3 が送信する s3:LifecycleExpiration:DeleteMarkerCreated 通知のイベント時間とは異なる場合があります。詳細については、「the section called “オブジェクトバージョンの削除”」を参照してください。

Amazon S3 は、Amazon Simple Notification Service (Amazon SNS) トピック、Amazon Simple Queue Service (Amazon SQS) キュー、または AWS Lambda 関数にイベント通知を発行できます。詳細については、「Amazon S3 イベント通知」を参照してください。

Amazon S3 イベント通知を設定する手順については、「Amazon SQS、Amazon SNS、および AWS Lambda を使用した通知の有効化」を参照してください。

次は Amazon S3 が s3:LifecycleExpiration:Delete イベントを発行するために送信するメッセージの例です。詳細については、「the section called “イベントメッセージの構造”」を参照してください。

```
{
   "Records":[
      {
         "eventVersion":"2.3",
         "eventSource":"aws:s3",
         "awsRegion":"us-west-2",
         "eventTime":"1970-01-01T00:00:00.000Z",
```

```
         "eventName":"LifecycleExpiration:Delete",
         "userIdentity":{
            "principalId":"s3.amazonaws.com"
         },
         "requestParameters":{
            "sourceIPAddress":"s3.amazonaws.com"
         },
         "responseElements":{
            "x-amz-request-id":"C3D13FE58DE4C810",
            "x-amz-id-2":"FMyUVURIY8/IgAtTv8xRjskZQpcIZ9KG4V5Wp6S7S/
JRWeUWerMUE5JgHvANOjpD"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"testConfigRule",
            "bucket":{
               "name":"amzn-s3-demo-bucket",
               "ownerIdentity":{
                  "principalId":"A3NL1KOZZKExample"
               },
               "arn":"arn:aws:s3:::amzn-s3-demo-bucket"
            },
            "object":{
               "key":"expiration/delete",
               "sequencer":"0055AED6DCD90281E5",
            }
         }
      }
   ]
}
```

s3:LifecycleTransition イベントを公開するために Amazon S3 が送信するメッセージには、次の情報も含まれます。

```
"lifecycleEventData":{
    "transitionEventData": {
        "destinationStorageClass": the destination storage class for the object
    }
}
```

ライフサイクル設定の要素

S3 ライフサイクル設定は、Amazon S3 がオブジェクトの有効期間中に実行するアクションを記述するさまざまな要素を含むライフサイクルルールで構成されます。Amazon S3 ライフサイクル設定を XML として指定します。これは 1 つ以上のライフサイクルルールで構成され、各ルールは 1 つ以上の要素で構成されます。

```
<LifecycleConfiguration>
    <Rule>
         <Element>
    </Rule>
    <Rule>
         <Element>
         <Element>
    </Rule>
</LifecycleConfiguration>
```

各ルールには次が含まれます。

- ルール ID とルールが有効か無効かを示すステータスを含むルールメタデータ。ルールが無効な場合、Amazon S3 はルールで指定されているアクションを実行しません。
- ルールが適用されるオブジェクトを特定するフィルター。フィルターを指定するには、オブジェクトサイズ、オブジェクトキープレフィックス、単一または複数のオブジェクトタグ、またはフィルターの組み合わせを使用できます。
- 指定されたアクションを Amazon S3 に実行させる場合、オブジェクトの有効期間内の日付または期間が指定された 1 つ以上の移行または失効アクション。

トピック

- ID 要素
- Status 要素
- Filter 要素
- ライフサイクルアクションを記述する要素
- ライフサイクルルールへのフィルタの追加

以下のセクションでは、S3 ライフサイクル設定における XML 要素について説明します。設定例については、「S3 ライフサイクル設定の例」を参照してください。

ID 要素

S3 ライフサイクル設定には最大 1,000 個のルールを記述できます。この制限は調整できません。<ID> 要素は、ルールを一意に識別します。ID の長さは、255 文字に制限されています。

Status 要素

<Status> 要素の値は、Enabled または Disabled のいずれかです。ルールが無効な場合、Amazon S3 はルールで定義されたアクションを実行しません。

Filter 要素

S3 ライフサイクルルールは、ルールで指定した <Filter> 要素に基づいて、バケット内のすべてのオブジェクトまたはオブジェクトのサブセットに適用できます。

オブジェクトは、キープレフィックス、オブジェクトタグ、またはそれらの組み合わせ (この場合、Amazon S3 は論理 AND を使用してフィルタを組み合わせます) により、オブジェクトをフィルタできます。フィルターの例と詳細については、「ライフサイクルルールへのフィルタの追加」を参照してください。

- キープレフィックスを使用したフィルターの指定 – この例は、キー名のプレフィックス (logs/) に基づいてオブジェクトのサブセットに適用される S3 ライフサイクルルールを示しています。例えば、ライフサイクルルールはオブジェクト logs/mylog.txt、logs/temp1.txt、logs/test.txt に適用されます。このルールは、オブジェクト example.jpg には適用されません。

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
           <Prefix>logs/</Prefix>
        </Filter>
        transition/expiration actions
         ...
    </Rule>
    ...
</LifecycleConfiguration>
```

異なるキー名のプレフィックスに基づいてオブジェクトのサブセットにライフサイクルアクションを適用する場合は、別のルールを指定します。各ルールでは、プレフィックスベースのフィルタを指定します。例えば、キープレフィックスが projectA/ と projectB/ のオブジェクトのライフサイクルアクションを作成するには、次のとおり 2 つのルールを指定します。

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
           <Prefix>projectA/</Prefix>
        </Filter>
        transition/expiration actions
         ...
    </Rule>

    <Rule>
        <Filter>
           <Prefix>projectB/</Prefix>
        </Filter>
        transition/expiration actions
         ...
    </Rule>
</LifecycleConfiguration>
```

オブジェクトキーの詳細については、「Amazon S3 オブジェクトに命名する」を参照してください。

- オブジェクトタグに基づくフィルターの指定 – 次の例では、ライフサイクルルールはタグ (*key*) と値 (*value*) に基づいてフィルターを指定します。この場合、ルールは特定のタグを持つオブジェクトのサブセットにのみ適用されます。

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
           <Tag>
              <Key>key</Key>
              <Value>value</Value>
           </Tag>
        </Filter>
        transition/expiration actions
        ...
    </Rule>
</LifecycleConfiguration>
```

複数のタグに基づいてフィルタを指定できます。次の例で示されるとおり、<And> 要素でタグを囲む必要があります。ルールは、2 つのタグ (特定のタグキーと値を持つ) が付与されたオブジェクトでライフサイクルアクションを実行するように Amazon S3 に指示します。

```
<LifecycleConfiguration>
    <Rule>
      <Filter>
         <And>
            <Tag>
               <Key>key1</Key>
               <Value>value1</Value>
            </Tag>
            <Tag>
               <Key>key2</Key>
               <Value>value2</Value>
            </Tag>
             ...
         </And>
      </Filter>
      transition/expiration actions
    </Rule>
</Lifecycle>
```

ライフサイクルルールは、指定された両方のタグが付与されたオブジェクトに適用されます。Amazon S3 は論理 AND を実行します。次の点に注意してください:

- 各タグは、キーと値の両方で正確に一致する必要があります。<Key> 要素のみを指定し、<Value> 要素を指定しない場合、ルールはタグキーと一致し、値が指定されていないオブジェクトにのみ適用されます。
- ルールは、ルールで指定されたすべてのタグが付与されたオブジェクトのサブセットに適用されます。オブジェクトに追加のタグが指定されていても、ルールは引き続き適用されます。

> **Note**
>
> フィルタで複数のタグを指定する場合、各タグキーは一意である必要があります。

- プレフィックスと単一または複数のタグの両方に基づくフィルターの指定 – ライフサイクルルールでは、キープレフィックスと単一または複数のタグの両方に基づいてフィルターを指定できます。繰り返しになりますが、次に示すとおり、これらすべてを <And> 要素で囲む必要があります。

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
```

```
            <And>
               <Prefix>key-prefix</Prefix>
               <Tag>
                  <Key>key1</Key>
                  <Value>value1</Value>
               </Tag>
               <Tag>
                  <Key>key2</Key>
                  <Value>value2</Value>
               </Tag>
                ...
            </And>
         </Filter>
         <Status>Enabled</Status>
         transition/expiration actions
    </Rule>
</LifecycleConfiguration>
```

Amazon S3 は、論理 AND を使用してこのようなフィルターを組み合わせます。つまり、ルールは指定したキープレフィックスと特定のタグを持つオブジェクトのサブセットに適用されます。フィルタのプレフィックスは最大 1 個、タグは 0 個以上にします。

- 空のフィルタ を指定できます。その場合、ルールはオブジェクト内のすべてのバケットに適用されます。

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
        </Filter>
        <Status>Enabled</Status>
        transition/expiration actions
    </Rule>
</LifecycleConfiguration>
```

- [object size] によりルールをフィルタリングするには、最小サイズ、(ObjectSizeGreaterThan) または最大サイズ (ObjectSizeLessThan) を指定するか、またはオブジェクトのサイズの範囲を指定できます。

  オブジェクトサイズの値はバイト単位です。デフォルトでは、128 KB 未満のオブジェクトは、最小サイズ (ObjectSizeGreaterThan) または最大サイズ (ObjectSizeLessThan) を指定しない限り、どのストレージクラスにも移行されません。詳細については、「例: 128 KB 未満のオブジェクトの移行を許可する」を参照してください。

```
                    <LifecycleConfiguration>
    <Rule>
        <Filter>
            <ObjectSizeGreaterThan>500</ObjectSizeGreaterThan>
        </Filter>
        <Status>Enabled</Status>
        transition/expiration actions
    </Rule>
</LifecycleConfiguration>
```

> **Note**
>
> ObjectSizeGreaterThan フィルターおよび ObjectSizeLessThan フィルターは、指定された値を除外します。例えば、S3 Standard ストレージクラスから S3 Standard-IA ストレージクラスに移動するためにオブジェクトのサイズを 128 KB から 1024 KB に設定した場合、1024 KB ちょうどのオブジェクトと 128 KB ちょうどのオブジェクトは S3 Standard-IA に移動されません。代わりに、このルールは 128 KB より大きく 1024 KB よりも小さいサイズのオブジェクトにのみ適用されます。

オブジェクトサイズの範囲を指定する場合は、ObjectSizeGreaterThan 整数は ObjectSizeLessThan 値未満にする必要があります。複数のフィルタを使用する場合は、<And> エレメントのフィルタを包む必要があります。次の例は、500 バイトから 64,000 バイトの範囲でオブジェクトを指定する方法を示しています。

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
            <And>
                <Prefix>key-prefix</Prefix>
                <ObjectSizeGreaterThan>500</ObjectSizeGreaterThan>
                <ObjectSizeLessThan>64000</ObjectSizeLessThan>
            </And>
        </Filter>
        <Status>Enabled</Status>
        transition/expiration actions
    </Rule>
```

```
</LifecycleConfiguration>
```

ライフサイクルアクションを記述する要素

次の定義済みのアクションのうち 1 つ以上を S3 ライフサイクルルールに指定することで、オブジェクトの有効期間中に特定のアクションを実行するように Amazon S3 に指示することができます。これらのアクションの効果は、バケットのバージョニング状態によって異なります。

- **Transition** アクション要素 – オブジェクトを別のストレージクラスに移行するには、Transition アクションを指定します。オブジェクトの移行の詳細については、「サポートされている移行」を参照してください。オブジェクトの有効期間内の指定の日付または期間に到達すると、Amazon S3 は移行を実行します。

  バージョニング対応のバケット (バージョニングが有効なバゲットまたはバージョニングが停止されたバケット) の場合、Transition アクションは最新のオブジェクトバージョンに適用されます。以前のバージョンを管理する場合、Amazon S3 は NoncurrentVersionTransition アクション (以下で説明されます) を定義します。

- **Expiration** アクション要素 – Expiration アクションは、ルールで特定されたオブジェクトを期限切れにします。これは、Amazon S3 のいずれかのストレージクラスの該当するオブジェクトに適用されます。ストレージクラスの詳細については、「Amazon S3 ストレージクラスの理解と管理」を参照してください。Amazon S3 により有効期限切れになったオブジェクトはいずれも使用できなくなります。オブジェクトが完全に削除されるかどうかは、バケットのバージョニング状態によって異なります。

  - バージョニング非対応のバケット – Expiration アクションを実行すると、Amazon S3 はオブジェクトを完全に削除します。
  - バージョニング対応バケット – バージョニング対応バケット (つまり、バージョニングが有効であるかバージョニングが停止されている) の場合、Amazon S3 による Expiration アクションの処理方法を決める考慮事項がいくつかあります。バージョニングが有効なバケットまたはバージョニングが停止されたバケットには、以下が適用されます。

    - Expiration アクションは、最新のバージョンにのみ適用されます (最新以外のバージョンには影響しません)。
    - 1 つ以上のオブジェクトバージョンがあり、削除マーカーが最新バージョンである場合、Amazon S3 はアクションを実行しません。

- 現在のオブジェクトバージョンが唯一のオブジェクトバージョンであり、削除マーカーでもある場合 (「期限切れオブジェクト削除マーカー」とも呼ばれます。すべてのオブジェクトバージョンが削除され、削除マーカーのみ残ります)、Amazon S3 は期限切れのオブジェクト削除マーカーを削除します。また、expiration アクションを使用して、期限切れオブジェクト削除マーカーをすべて削除するよう Amazon S3 に指示することもできます。例については、「バージョニングが有効なバケットで期限切れのオブジェクト削除マーカーを削除する」を参照してください。

詳細については、「S3 バージョニングによる複数のバージョンのオブジェクトの保持」を参照してください。

有効期限を管理するために Amazon S3 をセットアップする場合は、次の点も考慮します。

- バージョニングが有効なバケット

  現在のオブジェクトバージョンが削除マーカーではない場合、Amazon S3 は固有のバージョン ID を持つ削除マーカーを追加します。これにより、最新のバージョンが最新以外のバージョンとなり、削除マーカーが最新バージョンになります。

- バージョニングが停止されたバケット

  バージョニングを停止したバケットでは、有効期限切れアクションにより Amazon S3 がバージョン ID として `null` を使用する削除マーカーを作成します。この削除マーカーは、バージョン階層においてあらゆるオブジェクトバージョンをバージョン ID null に置き換えるため、オブジェクトが効率的に削除されます。

さらに、Amazon S3 はバージョン対応のバケット (つまり、バージョニングが有効なバケットとバージョニングが停止されているバケット) で以前のオブジェクトバージョンを管理するために使用できる次のアクションを提供します。

- **`NoncurrentVersionTransition`** アクション要素 – このアクションを使用して、Amazon S3 がオブジェクトを指定したストレージクラスに移行するタイミングを指定します。この有効期限切れは、オブジェクトが最新でなくなった以降の特定の日数 (`<NoncurrentDays>`) に基づいて設定できます。日数以外にも、保持する最新以外のバージョンの最大数 (`<NewerNoncurrentVersions>`) (1 ~ 100 の間) を指定することもできます。この値は、Amazon S3 が特定のバージョンに移行する前に、最新でないバージョンがいくつ必要かを決定します。Amazon S3 は、保持すると指定された数を超える最新でないバージョンをすべて移行します。移行を実行するには、`<NoncurrentDays>` および `<NewerNoncurrentVersions>` の両方の値を超える必要があります。

保持する最新以外のバージョンの数を指定するには、<Filter> 要素も指定する必要があります。<Filter> 要素を指定しないで保持する最新以外のバージョンの数を指定すると、Amazon S3 で InvalidRequest エラーが発生します。

オブジェクトの移行の詳細については、「サポートされている移行」を参照してください。NoncurrentVersionTransition アクション中の日数を指定した日付を Amazon S3 が計算する方法の詳細については、ライフサイクルルール: オブジェクトの存在時間に基づく を参照してください。

- **NoncurrentVersionExpiration** アクション要素 – Amazon S3 に最新以外のオブジェクトのバージョンを完全に削除することを指示するには、このアクションを使用します。このように削除されたオブジェクトは復元することはできません。この有効期限切れは、オブジェクトが最新でなくなった以降の特定の日数 (<NoncurrentDays>) に基づいて設定できます。日数以外にも、保持する最新以外のバージョンの最大数 (<NewerNoncurrentVersions>) (1 ~ 100 の間) を指定することもできます。この値は、Amazon S3 が特定のバージョンを期限切れにする前に、最新でないバージョンがいくつ必要かを指定します。Amazon S3 は、保存すると指定された数を超える最新でないバージョンをすべて完全に削除します。削除が行われるには、<NoncurrentDays> および <NewerNoncurrentVersions> の両方の値を超える必要があります。

  保持する最新以外のバージョンの数を指定するには、<Filter> 要素も指定する必要があります。<Filter> 要素を指定しないで保持する最新以外のバージョンの数を指定すると、Amazon S3 で InvalidRequest エラーが発生します。

  以前のオブジェクトをこのように遅れて削除すると、誤って削除または上書きを修正する必要がある場合に役立ちます。たとえば、最新以外のバージョンになってから 5 日後に削除する有効期間ルールを設定できます。例えば、2014 年 1 月 1 日 10:30 AM (UTC) に、photo.gif (バージョン ID 111111) というオブジェクトを作成したとします。2014 年 1 月 2 日 11:30 AM (UTC) に、photo.gif (バージョン ID 111111) を誤って削除したとします。これにより、新しいバージョン ID (バージョン ID 4857693 など) の削除マーカーが作成されます。この場合、完全な削除が行われるまでの 5 日間は、元のバージョンの photo.gif (バージョン ID 111111) を復元することができます。2014 年 1 月 8 日 00:00 (UTC) に、有効期限切れのライフサイクルルールが実行され、photo.gif (バージョン ID 111111) は完全に削除されます。これは、このバージョンが最新バージョンでなくなってから 5 日後です。

  NoncurrentVersionExpiration アクションの日数を指定した日付を Amazon S3 が計算する方法の詳細については、ライフサイクルルール: オブジェクトの存在時間に基づく を参照してください。

> **Note**
>
> オブジェクトの有効期限切れを決定するライフサイクル設定では、不完全なマルチパートアップロードは削除されません。不完全なマルチパートアップロードを削除するには、`AbortIncompleteMultipartUpload` というライフサイクル設定アクションを使用する必要があります。このアクションについては、このセクションの後半で説明します。

この移行アクションと有効期限切れアクション以外にも、次のライフサイクル設定アクションを使用して、不完全なマルチパートアップロードを停止するか、有効期限切れのオブジェクト削除マーカーを削除するように Amazon S3 に指示できます。

- **`AbortIncompleteMultipartUpload`** アクション要素 – この要素を使用すると、マルチパートアップロードの進行を許可する最大時間 (日数) を指定できます。対象となるマルチパートアップロード (ライフサイクルルールで指定されているキー名の `prefix` で特定) が所定の期間内に正常に完了していない場合、Amazon S3 は不完全なマルチパートアップロードを中止します。詳細については、「マルチパートアップロードの中止」を参照してください。

  > **Note**
  >
  > このライフサイクルアクションは、オブジェクトタグを使用するフィルターが含まれるルールでは指定できません。

- **`ExpiredObjectDeleteMarker`** アクション要素 – バージョニングが有効になっているバケットでは、最新以外のバージョンが 0 の削除マーカーは、期限切れオブジェクト削除マーカーと呼ばれます。このライフサイクルアクションを使用して、期限切れオブジェクト削除マーカーを削除するように S3 に指示できます。例については、「バージョニングが有効なバケットで期限切れのオブジェクト削除マーカーを削除する」を参照してください。

  > **Note**
  >
  > このライフサイクルアクションは、オブジェクトタグを使用するフィルターが含まれるルールでは指定できません。

オブジェクトが最新でなくなってからの期間を Amazon S3 が計算する方法

バージョニングが有効なバケットで、オブジェクトの複数のバージョンを所持することができます。最新バージョンが常に 1 個、最新以外のバージョンが 0 個以上存在します。オブジェクトをアップロードするたびに、最新バージョンは以前のバージョンとして保持され、新しく追加されたバージョンがその代わりに最新バージョンになります。オブジェクトが最新でなくなってからの日数を知るために、Amazon S3 はその次の最新バージョンがいつ作成されたかを調べます。Amazon S3 は、オブジェクトの次の最新バージョンが作成されてからの日数を、オブジェクトが最新でなくなってからの日数として使用します。

S3 ライフサイクル設定を使用する場合のオブジェクトの以前のバージョンの復元

「以前のバージョンの復元」で説明したとおり、次の 3 つの方法のいずれかを使用して、オブジェクトの以前のバージョンを取得できます。

- 方法 1 – オブジェクトの最新以外のバージョンを同じバケットにコピーします。コピーされたオブジェクトはそのオブジェクトの最新バージョンになり、すべてのオブジェクトバージョンが維持されます。
- 方法 2 – オブジェクトの現在のバージョンを完全に削除します。最新のオブジェクトバージョンを削除すると、結果として、以前のバージョンがそのオブジェクトの最新バージョンになります。

バージョニングが有効になっているバケットで S3 ライフサイクル設定ルールを使用している場合は、ベストプラクティスとして、方法 1 を使用することをお勧めします。
S3 ライフサイクルは、結果整合性モデル下で動作します。最新バージョンが完全に削除されても、変更がすべての Amazon S3 システムに反映されるまで消えない場合があります。(このため、Amazon S3 はこのような削除を一時的に認識しない場合があります)。一方で、以前のオブジェクトを有効期限切れにするように設定したライフサイクルルールは、復元したいオブジェクトを含む以前のオブジェクトを完全に削除する可能性があります。つまり、方法 1 でお勧めしたとおり、代替方法として古いバージョンをコピーする方が安全です。

ライフサイクルのアクションとバケットのバージョニング状態

ライフサイクルルール: オブジェクトの存在時間に基づく

Amazon S3 が指定したアクションを実行できる期間は、オブジェクトの作成 (または変更) からの日数で指定できます。

日数を S3 ライフサイクル設定の `Transition` アクションおよび `Expiration` アクションで指定する場合は、以下の点に注意してください。

- 指定する値は、オブジェクトの作成からアクションが発生するまでの日数です。
- Amazon S3 は、ルールで指定された日数をオブジェクト作成時刻に加え、その結果の時刻を翌日の UTC 午前 0 時に切り上げて時刻を算出します。例えば、あるオブジェクトが 2014 年 1 月 15 日 10:30 AM (UTC) に作成され、移行ルールで 3 日と指定した場合、オブジェクトの移行日は 2014 年 1 月 19 日 00:00 (UTC) となります。

> **Note**
>
> Amazon S3 は、各オブジェクトの最終更新日のみを維持します。例えば、Amazon S3 コンソールでは、オブジェクトの [プロパティ] ペインに [最終更新日時] が表示されています。新しいオブジェクトを最初に作成する際は、この日付はオブジェクトの作成日を表示します。オブジェクトを置き換えた場合、日付はそれに応じて変わります。つまり、オブジェクトの作成日と [最終更新日時] は同期しています。

日数をライフサイクル設定の `NoncurrentVersionTransition` アクションおよび `NoncurrentVersionExpiration` アクションで指定する場合は、以下の点に注意してください。

- 指定する値は、オブジェクトのバージョンが最新ではなくなった日時 (つまり、オブジェクトが上書きまたは削除された日時) から、Amazon S3 が指定したオブジェクトに対してアクションを実行するまでの日数です。
- Amazon S3 は、オブジェクトの次の最新バージョンが作成された時刻にルールで指定された日数を加算して、その結果の時刻を翌日の UTC 午前 0 時に切り上げて時刻を算出します。例えば、バケット内に 2014 年 1 月 1 日の 10:30 AM (UTC) に作成されたオブジェクトの最新バージョンがあるとします。この最新バージョンを置き換えるオブジェクトの新しいバージョンが 2014 年 1 月 15 日の 10:30 AM (UTC) に作成され、移行ルールで 3 日を指定した場合、オブジェクトの移行日は 2014 年 1 月 19 日 00:00 (UTC) と算出されます。

ライフサイクルルール: 特定の日付に基づく

S3 ライフサイクルルールでアクションを指定する際に、Amazon S3 がアクションを実行する日付を指定できます。特定の日付になると、Amazon S3 は (フィルタ条件に基づいて) すべての対象オブジェクトにアクションに適用します。

過去の日付を使用して S3 ライフサイクルアクションを指定すると、すべての対象オブジェクトは、直ちにそのライフサイクルアクションの対象となります。

> **Important**
>
> 日付ベースのアクションは、1 回限りのアクションではありません。Amazon S3 は、日付が過ぎた後も、ルールのステータスが `Enabled` である限り、継続して日付ベースのアクションを適用します。
> 例えば、すべてのオブジェクトを削除する日付ベースの `Expiration` アクションを指定するとします (このルールにはフィルターが指定されていないと仮定します)。Amazon S3 は特定の日付に、バケットのすべてのオブジェクトを期限切れにします。Amazon S3 は、バケット内に作成した新しいオブジェクトも続けて有効期限切れにします。ライフサイクルアクションを停止するには、ライフサイクルルールからアクションを削除するか、ルールを無効にするか、ライフサイクル設定からルールを削除する必要があります。

日付の値は、ISO 8601 形式に従う必要があります。この時刻は常に午前 0 時 (UTC) となります。

> **Note**
>
> Amazon S3 コンソールを使用して日付ベースのライフサイクルルールを作成することはできません。ただし、このようなルールを表示、無効化、または削除することはできます。

ライフサイクルルールへのフィルタの追加

フィルタはオプションのライフサイクルルール要素であり、ルールが適用されるオブジェクトを指定するために使用できます。

オブジェクトをフィルタリングするには、次の要素を使用できます。

キープレフィックス

プレフィックスに基づいてオブジェクトをフィルタリングできます。異なるプレフィックスを持つオブジェクトのサブセットにライフサイクルアクションを適用する場合は、アクションごとに個別のルールを作成します。

オブジェクトタグ

1 つ以上のタグに基づいてオブジェクトをフィルタリングできます。各タグはキーと値の両方に正確に一致する必要があります。複数のタグを指定する場合、各タグキーは一意である必要があります。複数のオブジェクトタグを持つフィルタは、すべてのタグが指定されているオブジェクトのサブセットに適用されます。オブジェクトに追加のタグが指定されていても、フィルタは引き続き適用されます。

> **Note**
>
> Key 要素のみを指定し、Value 要素を指定しない場合、ルールはタグキーと一致し、値が指定されていないオブジェクトにのみ適用されます。

最小または最大オブジェクトサイズ

サイズに基づいてオブジェクトをフィルタリングできます。最小サイズ (ObjectSizeGreaterThan)、または最大サイズ (ObjectSizeLessThan) を指定するか、同じでフィルタでオブジェクトサイズの範囲を指定することができます。オブジェクトサイズの値はバイト単位です。フィルターの最大サイズは 5 TB です。Amazon S3 は、ライフサイクル設定にデフォルトの最小オブジェクトサイズを適用します。詳細については、「例: 128 KB 未満のオブジェクトの移行を許可する」を参照してください。

さまざまなフィルタ要素を組み合わせることができます。その場合、Amazon S3 は論理 AND を使用します。

フィルタ例

次の例は、さまざまなフィルタ要素を使用する方法を示しています。

- キープレフィックスを使用したフィルターの指定 – この例は、キー名のプレフィックス (logs/) に基づいてオブジェクトのサブセットに適用される S3 ライフサイクルルールを示しています。例えば、ライフサイクルルールはオブジェクト logs/mylog.txt、logs/temp1.txt、logs/test.txt に適用されます。このルールは、オブジェクト example.jpg には適用されません。

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
           <Prefix>logs/</Prefix>
        </Filter>
```

```
        transition/expiration actions
         ...
    </Rule>
    ...
</LifecycleConfiguration>
```

> **Note**
>
> 同じ文字で始まるプレフィックスが 1 つ以上ある場合は、末尾のスラッシュ (/) を除外した部分的なプレフィックスをフィルターで指定することで、これらのプレフィックスをすべてルールに含めることができます。例えば、次のようなプレフィックスがあるとします。
>
> ```
> sales1999/
>                sales2000/
>                sales2001/
> ```
>
> ルールに 3 つのプレフィックスをすべて含めるには、ライフサイクルルールで sales をプレフィックスとして指定します。

異なるキー名のプレフィックスに基づいてオブジェクトのサブセットにライフサイクルアクションを適用する場合は、別のルールを指定します。各ルールでは、プレフィックスベースのフィルタを指定します。例えば、キープレフィックスが projectA/ と projectB/ のオブジェクトのライフサイクルアクションを作成するには、次のとおり 2 つのルールを指定します。

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
           <Prefix>projectA/</Prefix>
        </Filter>
        transition/expiration actions
         ...
    </Rule>

    <Rule>
        <Filter>
           <Prefix>projectB/</Prefix>
        </Filter>
        transition/expiration actions
```

```
        ...
    </Rule>
</LifecycleConfiguration>
```

オブジェクトキーの詳細については、「Amazon S3 オブジェクトに命名する」を参照してください。

- オブジェクトタグに基づくフィルターの指定 – 次の例では、ライフサイクルルールはタグ (*key*) と値 (*value*) に基づいてフィルターを指定します。この場合、ルールは特定のタグを持つオブジェクトのサブセットにのみ適用されます。

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
           <Tag>
              <Key>key</Key>
              <Value>value</Value>
           </Tag>
        </Filter>
        transition/expiration actions
        ...
    </Rule>
</LifecycleConfiguration>
```

複数のタグに基づいてフィルタを指定できます。次の例で示されるとおり、<And> 要素でタグを囲む必要があります。ルールは、2 つのタグ (特定のタグキーと値を持つ) が付与されたオブジェクトでライフサイクルアクションを実行するように Amazon S3 に指示します。

```
<LifecycleConfiguration>
    <Rule>
      <Filter>
         <And>
            <Tag>
               <Key>key1</Key>
               <Value>value1</Value>
            </Tag>
            <Tag>
               <Key>key2</Key>
               <Value>value2</Value>
            </Tag>
             ...
          </And>
```

```
      </Filter>
      transition/expiration actions
    </Rule>
</Lifecycle>
```

ライフサイクルルールは、指定された両方のタグが付与されたオブジェクトに適用されます。Amazon S3 は論理 AND を実行します。次の点に注意してください:

- 各タグは、キーと値の両方で正確に一致する必要があります。<Key> 要素のみを指定し、<Value> 要素を指定しない場合、ルールはタグキーと一致し、値が指定されていないオブジェクトにのみ適用されます。
- ルールは、ルールで指定されたすべてのタグが付与されたオブジェクトのサブセットに適用されます。オブジェクトに追加のタグが指定されていても、ルールは引き続き適用されます。

> **Note**
>
> フィルタで複数のタグを指定する場合、各タグキーは一意である必要があります。

- プレフィックスと単一または複数のタグの両方に基づくフィルターの指定 – ライフサイクルルールでは、キープレフィックスと単一または複数のタグの両方に基づいてフィルターを指定できます。繰り返しになりますが、次に示すとおり、これらすべてを <And> 要素で囲む必要があります。

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
          <And>
             <Prefix>key-prefix</Prefix>
             <Tag>
                <Key>key1</Key>
                <Value>value1</Value>
             </Tag>
             <Tag>
                <Key>key2</Key>
                <Value>value2</Value>
             </Tag>
              ...
          </And>
        </Filter>
        <Status>Enabled</Status>
        transition/expiration actions
```

```
    </Rule>
</LifecycleConfiguration>
```

Amazon S3 は、論理 AND を使用してこのようなフィルターを組み合わせます。つまり、ルールは指定したキープレフィックスと特定のタグを持つオブジェクトのサブセットに適用されます。フィルタのプレフィックスは最大 1 個、タグは 0 個以上にします。

- 空のフィルタを指定 – 空のフィルタを指定できます。その場合、ルールはオブジェクト内のすべてのバケットに適用されます。

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
        </Filter>
        <Status>Enabled</Status>
        transition/expiration actions
    </Rule>
</LifecycleConfiguration>
```

- オブジェクトサイズフィルタを指定 – オブジェクトサイズでルールをフィルタリングするには、最小サイズ (ObjectSizeGreaterThan) または最大サイズ (ObjectSizeLessThan) を指定するか、またはオブジェクトのサイズの範囲を指定できます。

  オブジェクトサイズの値はバイト単位です。フィルターの最大サイズは 5 TB です。ストレージクラスによっては、オブジェクトサイズに最小制限があります。詳細については、「Amazon S3 ストレージクラスの比較」を参照してください。

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
            <ObjectSizeGreaterThan>500</ObjectSizeGreaterThan>
        </Filter>
        <Status>Enabled</Status>
        transition/expiration actions
    </Rule>
</LifecycleConfiguration>
```

> **Note**
>
> ObjectSizeGreaterThan フィルターおよび ObjectSizeLessThan フィルターは、指定された値を除外します。例えば、S3 Standard ストレージクラスから S3 Standard-IA

ストレージクラスに移動するためにオブジェクトのサイズを 128 KB から 1024 KB に設定した場合、1024 KB ちょうどのオブジェクトと 128 KB ちょうどのオブジェクトは S3 Standard-IA に移動されません。代わりに、このルールは 128 KB より大きく 1024 KB よりも小さいサイズのオブジェクトにのみ適用されます。

オブジェクトサイズの範囲を指定する場合は、ObjectSizeGreaterThan 整数は ObjectSizeLessThan 値未満にする必要があります。複数のフィルタを使用する場合は、<And> エレメントのフィルタを包む必要があります。次の例は、500 バイトから 64,000 バイトの範囲でオブジェクトを指定する方法を示しています。

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
            <And>
                <Prefix>key-prefix</Prefix>
                <ObjectSizeGreaterThan>500</ObjectSizeGreaterThan>
                <ObjectSizeLessThan>64000</ObjectSizeLessThan>
            </And>
        </Filter>
        <Status>Enabled</Status>
        transition/expiration actions
    </Rule>
</LifecycleConfiguration>
```

Amazon S3 がライフサイクル設定の競合を処理する方法

一般的に、Amazon S3 ライフサイクルはコストに合わせて最適化されます。たとえば、2 つの有効期限ポリシーが重複している場合は、短い有効期限ポリシーが適用されるため、データが予想よりも長く保存されることはありません。同様に、2 つの移行ポリシーが重複している場合は、S3 ライフサイクルによってオブジェクトが低コストのストレージクラスに移行されます。

いずれの場合でも、S3 ライフサイクルによって、最も安価なパスが選択されます。この一般的なルールの例外として、S3 Intelligent-Tiering ストレージクラスの場合があります。S3 Intelligent-Tiering は、S3 Glacier および S3 Glacier Deep Archive ストレージクラスを除くどのストレージクラスよりも S3 ライフサイクルで優先されます。

S3 ライフサイクル設定に複数のルールがある場合、1 つのオブジェクトが同じ日に複数の S3 ライフサイクルアクションの対象になることがあります。このような場合、Amazon S3 は以下の一般的なルールに従います。

- 完全な削除は、移行より優先されます。
- 移行は、削除マーカーの作成より優先されます。
- オブジェクトが S3 Glacier Flexible Retrieval と S3 Standard-IA (または S3 One Zone-IA) 移行の両方の対象になる場合、Amazon S3 は S3 Glacier Flexible Retrieval 移行を選択します。

重複するフィルタ、競合するライフサイクルアクションの例

重複するプレフィックスまたはアクションを指定する S3 ライフサイクル設定を指定する場合があります。次の例では、競合の可能性を Amazon S3 でどのように解決するかを示します。

Example 1: 重複したプレフィックス (競合なし)

以下の設定例には、次のように重複するプレフィックスを指定する 2 つのルールがあります。

- 1 番目のルールは、空のフィルターを指定することで、バケット内のすべてのオブジェクトを示しています。
- 2 番目のルールは、キー名プレフィックス (logs/) を指定することで、オブジェクトのサブセットのみを示しています。

ルール 1 では、すべてのオブジェクトを作成後 1 年で削除するように Amazon S3 にリクエストします。ルール 2 では、オブジェクトのサブセットを作成後 30 日で S3 Standard – IA ストレージクラスに移行するように Amazon S3 にリクエストします。

```
<LifecycleConfiguration>
  <Rule>
    <ID>Rule 1</ID>
    <Filter>
    </Filter>
    <Status>Enabled</Status>
    <Expiration>
      <Days>365</Days>
    </Expiration>
  </Rule>
  <Rule>
    <ID>Rule 2</ID>
```

```
    <Filter>
      <Prefix>logs/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <StorageClass>STANDARD_IA</StorageClass>
      <Days>30</Days>
    </Transition>
   </Rule>
</LifecycleConfiguration>
```

この場合、競合は発生しないため、Amazon S3 は作成から 30 日後に logs/ プレフィックスを持つオブジェクトを S3 標準 – IA ストレージクラスへ移行させます。オブジェクトの作成後 1 年に達すると、そのオブジェクトは削除されます。

Example 2: 競合するライフサイクルアクション

この設定例には、オブジェクトの有効期間内の同じ時点で同じオブジェクトセットに対して 2 つの異なるアクションを実行するよう Amazon S3 に指示する 2 つのルールがあります。

- 両方のルールで同じキー名プレフィックスが指定されているので、どちらのルールも同じオブジェクトのセットに適用されます。
- どちらのルールでも、オブジェクトが作成されてから同じ 365 日後にルールを適用するように指定されています。
- 1 つのルールは、オブジェクトを S3 Standard – IA ストレージクラスに移行するように Amazon S3 に指示しています。もう 1 つのルールは、同じタイミングでオブジェクトを有効期限切れにするよう Amazon S3 に指示しています。

```
<LifecycleConfiguration>
  <Rule>
    <ID>Rule 1</ID>
    <Filter>
      <Prefix>logs/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Expiration>
      <Days>365</Days>
    </Expiration>
  </Rule>
  <Rule>
```

```
    <ID>Rule 2</ID>
    <Filter>
      <Prefix>logs/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <StorageClass>STANDARD_IA</StorageClass>
      <Days>365</Days>
    </Transition>
   </Rule>
</LifecycleConfiguration>
```

この場合、ユーザーはオブジェクトを有効期限切れに (削除予定) するよう望んでおり、ストレージクラスを変更しても意味がないため、Amazon S3 はこれらのオブジェクトに対して失効アクションを選択します。

Example 3: ライフサイクルアクションが競合する重複したプレフィックス

この例の設定には、次のように重複するプレフィックスを指定する 2 つのルールがあります。

- ルール 1 では、空のプレフィックス (すべてのオブジェクトを示します) が指定されています。
- ルール 2 では、すべてのオブジェクトのサブセットを識別するキー名プレフィックス (logs/) が指定されています。

キー名プレフィックスが logs/ のオブジェクトのサブセットには、両方のルールの S3 ライフサイクルアクションが適用されます。片方のルールは作成されてから 10 日後にオブジェクトを移行するよう Amazon S3 に指示しており、もう一方のルールは作成されてから 365 日後にオブジェクトを移行するよう Amazon S3 に指示しています。

```
<LifecycleConfiguration>
  <Rule>
    <ID>Rule 1</ID>
    <Filter>
      <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <StorageClass>STANDARD_IA</StorageClass>
      <Days>10</Days>
    </Transition>
  </Rule>
```

```
  <Rule>
    <ID>Rule 2</ID>
    <Filter>
      <Prefix>logs/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <StorageClass>STANDARD_IA</StorageClass>
      <Days>365</Days>
    </Transition>
   </Rule>
</LifecycleConfiguration>
```

この場合、Amazon S3 は作成後 10 日での移行を選択します。

Example 4: タグベースのフィルタ処理の結果によるライフサイクルアクションの競合

それぞれがタグフィルターを指定する 2 つのルールを含む次のような S3 ライフサイクル設定があるものとします。

- ルール 1 では、タグベースのフィルタ (tag1/value1) が指定されています。このルールは、作成されてから 365 日後にオブジェクトを S3 Glacier Flexible Retrieval ストレージクラスに移行するよう Amazon S3 に指示します。
- ルール 2 では、タグベースのフィルタ (tag2/value2) が指定されています。このルールは、作成されてから 14 日後にオブジェクトを期限切れにするよう Amazon S3 に指示します。

S3 ライフサイクル設定は以下のようになります。

```
<LifecycleConfiguration>
  <Rule>
    <ID>Rule 1</ID>
    <Filter>
      <Tag>
         <Key>tag1</Key>
         <Value>value1</Value>
      </Tag>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <StorageClass>GLACIER</StorageClass>
      <Days>365</Days>
```

```
    </Transition>
  </Rule>
  <Rule>
    <ID>Rule 2</ID>
    <Filter>
      <Tag>
         <Key>tag2</Key>
         <Value>value2</Value>
      </Tag>
    </Filter>
    <Status>Enabled</Status>
    <Expiration>
      <Days>14</Days>
    </Expiration>
   </Rule>
</LifecycleConfiguration>
```

オブジェクトに両方のタグがある場合、Amazon S3 はどのルールに従うかを決定する必要があります。この場合、Amazon S3 は作成されてから 14 日後にオブジェクトを期限切れにします。オブジェクトは削除されるため、移行アクションは行われません。

S3 ライフサイクル設定の例

このセクションでは、S3 ライフサイクル設定の例を示します。それぞれの例では、各サンプルシナリオで XML をどのように指定するかを示します。

トピック

- 作成後 1 日以内にすべてのオブジェクトをアーカイブする
- ライフサイクルルールの一時的な無効化
- オブジェクトの有効期間全体にわたってストレージクラスの層を下げる
- 複数のリソースの指定
- バージョニングが有効なバケットへのライフサイクルルールを指定する
- バージョニングが有効なバケットで期限切れのオブジェクト削除マーカーを削除する
- マルチパートアップロードを中止するライフサイクル設定
- データがない旧オブジェクトの有効期限
- 例: 128 KB 未満のオブジェクトの移行を許可する

作成後 1 日以内にすべてのオブジェクトをアーカイブする

各 S3 ライフサイクルルールには、S3 ライフサイクルルール適用先バケット内のオブジェクトのサブセットを識別するのに使用できるフィルターが含まれます。以下の S3 ライフサイクル設定は、フィルタを指定する方法の例です。

- この S3 ライフサイクル設定ルールでは、フィルターはキープレフィックス (tax/) を指定しています。したがって、ルールは、キー名プレフィックスが tax/ のオブジェクト (tax/doc1.txt、tax/doc2.txt など) に適用されます。

  このルールは、Amazon S3 に以下のことを命じる 2 つのアクションを指定します。

  - 作成されてから 365 日後にオブジェクトを S3 Glacier Flexible Retrieval ストレージクラスに移行します。
  - 作成から 3,650 日 (10 年) 後にオブジェクトを削除する (Expiration アクション)。

```
<LifecycleConfiguration>
  <Rule>
    <ID>Transition and Expiration Rule</ID>
    <Filter>
       <Prefix>tax/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>365</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
    <Expiration>
      <Days>3650</Days>
    </Expiration>
  </Rule>
</LifecycleConfiguration>
```

  オブジェクトの経過日数を作成後の日数で指定する代わりに、各アクションの日付を指定できます。ただし、Date と Days の両方を同じルールで使用することはできません。

- バケット内のすべてのオブジェクトに S3 ライフサイクルルールを適用する場合は、空のプレフィックスを指定します。以下の設定では、作成から 0 日後にオブジェクトを S3 Glacier Flexible Retrieval ストレージクラスに移行するよう Amazon S3 に指示する Transition アクションをルールとして指定しています。このルールは、オブジェクトが作成後の 午前 0 時 (UTC) に S3

Glacier Flexible Retrieval へのアーカイブ対象となることを意味します。ライフサイクルの制約の詳細については、「移行に関する制約と考慮事項」を参照してください。

```
<LifecycleConfiguration>
  <Rule>
    <ID>Archive all object same-day upon creation</ID>
    <Filter>
      <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

- フィルタ内にゼロまたは 1 個のキー名のプレフィックスと 0 個以上のオブジェクトタグを指定できます。以下のコード例では、キープレフィックスが tax/ のオブジェクトのサブセットと、指定したキーと値の 2 つのタグを含むオブジェクトに、S3 ライフサイクルルールを適用しています。複数のフィルターを指定するときは、次に示すように <And> 要素を含める必要があることに注意してください (Amazon S3 では論理 AND を適用して、指定されたフィルター条件を結合します)。

```
...
<Filter>
   <And>
      <Prefix>tax/</Prefix>
      <Tag>
         <Key>key1</Key>
         <Value>value1</Value>
      </Tag>
      <Tag>
         <Key>key2</Key>
         <Value>value2</Value>
      </Tag>
    </And>
</Filter>
...
```

- オブジェクトのフィルタはタグに基づいてのみ行うことができます。たとえば、以下の S3 ライフサイクルルールは、2 つのタグが指定されている (プレフィックスは指定されていない) オブジェクトに適用されます。

```
...
<Filter>
   <And>
      <Tag>
         <Key>key1</Key>
         <Value>value1</Value>
      </Tag>
      <Tag>
         <Key>key2</Key>
         <Value>value2</Value>
      </Tag>
    </And>
</Filter>
...
```

Important

S3 ライフサイクル設定に複数のルールがある場合、1 つのオブジェクトが同じ日に複数の S3 ライフサイクルアクションの対象になることがあります。このような場合、Amazon S3 は以下の一般的なルールに従います。

- 完全な削除は、移行より優先されます。
- 移行は、削除マーカーの作成より優先されます。
- オブジェクトが S3 Glacier Flexible Retrieval と S3 Standard-IA (または S3 One Zone-IA) 移行の両方の対象になる場合、Amazon S3 は S3 Glacier Flexible Retrieval 移行を選択します。

例については「重複するフィルタ、競合するライフサイクルアクションの例」を参照してください。

ライフサイクルルールの一時的な無効化

status 要素を使用して、S3 ライフサイクルルールを一時的に無効にできます。これは、既存のルールを上書きすることなく、新しいルールをテストしたり、設定に関する問題をトラブルシューティングしたりする場合に役立ちます。以下の S3 ライフサイクル設定では、2 つのルールを指定しています。

- ルール 1 は、logs/ プレフィックスを持つオブジェクトを作成直後に S3 Glacier Flexible Retrieval ストレージクラスに移行するよう、Amazon S3 に指示します。
- ルール 2 は、documents/ プレフィックスを持つオブジェクトを作成直後に S3 Glacier Flexible Retrieval ストレージクラスに移行するよう、Amazon S3 に指示します。

設定では、ルール 1 は有効で、ルール 2 は無効です。Amazon S3 は無効なルールを無視します。

```
<LifecycleConfiguration>
  <Rule>
    <ID>Rule1</ID>
    <Filter>
      <Prefix>logs/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
  <Rule>
    <ID>Rule2</ID>
    <Filter>
      <Prefix>documents/</Prefix>
    </Filter>
    <Status>Disabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

オブジェクトの有効期間全体にわたってストレージクラスの層を下げる

この例では、S3 ライフサイクル設定を使用して、有効期間全体にわたってオブジェクトのストレージクラスの階層を下げます。層を下げると、ストレージコストを削減できます。料金に関する詳細については、「Amazon S3 の料金」を参照してください。

次の S3 ライフサイクル設定では、キー名プレフィックス `logs/` が付いたオブジェクトに適用されるルールを指定します。このルールは、次のアクションを指定します。

- 2 つの移行アクション:
  - 作成されてから 30 日後にオブジェクトを S3 Standard – IA ストレージクラスに移行します。
  - 作成されてから 90 日後にオブジェクトを S3 Glacier Flexible Retrieval ストレージクラスに移行します。
- 作成されてから 1 年後にオブジェクトを削除するよう Amazon S3 に指示する 1 つの失効アクション。

```
<LifecycleConfiguration>
  <Rule>
    <ID>example-id</ID>
    <Filter>
       <Prefix>logs/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>30</Days>
      <StorageClass>STANDARD_IA</StorageClass>
    </Transition>
    <Transition>
      <Days>90</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
    <Expiration>
      <Days>365</Days>
    </Expiration>
  </Rule>
</LifecycleConfiguration>
```

> **Note**
>
> すべてのアクションがオブジェクトの同じセットに適用される場合 (フィルターによって識別)、すべての S3 ライフサイクルアクションを記述する 1 つのルールを使用できます。それ以外の場合、それぞれが異なるフィルタを指定する複数のルールを追加できます。

> **Important**
>
> S3 ライフサイクル設定に複数のルールがある場合、1 つのオブジェクトが同じ日に複数の S3 ライフサイクルアクションの対象になることがあります。このような場合、Amazon S3 は以下の一般的なルールに従います。
>
> - 完全な削除は、移行より優先されます。
> - 移行は、削除マーカーの作成より優先されます。
> - オブジェクトが S3 Glacier Flexible Retrieval と S3 Standard-IA (または S3 One Zone-IA) 移行の両方の対象になる場合、Amazon S3 は S3 Glacier Flexible Retrieval 移行を選択します。
>
> 例については「重複するフィルタ、競合するライフサイクルアクションの例」を参照してください。

複数のリソースの指定

オブジェクトごとに異なる S3 ライフサイクルアクションが必要な場合、複数のルールを指定できます。以下の S3 ライフサイクル設定には 2 つのルールがあります。

- ルール 1 は、キー名プレフィックス `classA/` が付いたオブジェクトに適用されます。作成されてから 1 年後にオブジェクトを S3 Glacier Flexible Retrieval ストレージクラスに移行し、作成されてから 10 年後にそれらのオブジェクトを期限切れにするよう、Amazon S3 に指示します。
- ルール 2 は、キー名プレフィックス `classB/` が付いたオブジェクトに適用されます。作成されてから 90 日後にオブジェクトを S3 Standard – IA ストレージクラスに移行し、作成されてから 1 年後に削除するよう Amazon S3 に指示します。

```
<LifecycleConfiguration>
```

```
    <Rule>
        <ID>ClassADocRule</ID>
        <Filter>
           <Prefix>classA/</Prefix>
        </Filter>
        <Status>Enabled</Status>
        <Transition>
           <Days>365</Days>
           <StorageClass>GLACIER</StorageClass>
        </Transition>
        <Expiration>
             <Days>3650</Days>
        </Expiration>
    </Rule>
    <Rule>
        <ID>ClassBDocRule</ID>
        <Filter>
            <Prefix>classB/</Prefix>
        </Filter>
        <Status>Enabled</Status>
        <Transition>
           <Days>90</Days>
           <StorageClass>STANDARD_IA</StorageClass>
        </Transition>
        <Expiration>
             <Days>365</Days>
        </Expiration>
    </Rule>
</LifecycleConfiguration>
```

Important

S3 ライフサイクル設定に複数のルールがある場合、1 つのオブジェクトが同じ日に複数の S3 ライフサイクルアクションの対象になることがあります。このような場合、Amazon S3 は以下の一般的なルールに従います。

- 完全な削除は、移行より優先されます。
- 移行は、削除マーカーの作成より優先されます。
- オブジェクトが S3 Glacier Flexible Retrieval と S3 Standard-IA (または S3 One Zone-IA) 移行の両方の対象になる場合、Amazon S3 は S3 Glacier Flexible Retrieval 移行を選択します。

例については「重複するフィルタ、競合するライフサイクルアクションの例」を参照してください。

バージョニングが有効なバケットへのライフサイクルルールを指定する

バージョニングが有効なバケットがあるとします。つまり、各オブジェクトに、最新のバージョンと以前のバージョンが 0 個以上あります。(S3 バージョニングの詳細については、S3 バージョニングによる複数のバージョンのオブジェクトの保持 を参照してください。)

次の例では、1 年間分の履歴を維持し、5 つの旧バージョンを保持します。S3 ライフサイクル設定では、任意のオブジェクトを 1 ~ 100 バージョンまで保持できます。Amazon S3 が特定のバージョンを期限切れにするには、5 以上の旧バージョンが存在する必要があることに注意してください。Amazon S3 は、保存すると指定された数を超える最新でないバージョンをすべて完全に削除します。削除が行われるには、NoncurrentDays と NewerNoncurrentVersions の両方の値を超える必要があります。

ストレージコストを節約するために、最新でないバージョンが最新でなくなってから 30 日後に、S3 Glacier Flexible Retrieval に移動する方法 (これらの最新でないオブジェクトは、リアルタイムアクセスが必要ないコールドデータを想定しています) 。また、最新のバージョンへのアクセス頻度は作成されてから 90 日後に低下すると予想されるため、これらのオブジェクトを S3 Standard-IA ストレージクラスに移動することもできます。

```
<LifecycleConfiguration>
    <Rule>
        <ID>sample-rule</ID>
        <Filter>
           <Prefix></Prefix>
        </Filter>
        <Status>Enabled</Status>
        <Transition>
           <Days>90</Days>
           <StorageClass>STANDARD_IA</StorageClass>
        </Transition>
        <NoncurrentVersionTransition>
            <NoncurrentDays>30</NoncurrentDays>
            <StorageClass>GLACIER</StorageClass>
        </NoncurrentVersionTransition>
       <NoncurrentVersionExpiration>
```

```
            <NewerNoncurrentVersions>5</NewerNoncurrentVersions>
            <NoncurrentDays>365</NoncurrentDays>
        </NoncurrentVersionExpiration>
    </Rule>
</LifecycleConfiguration>
```

バージョニングが有効なバケットで期限切れのオブジェクト削除マーカーを削除する

バージョニングが有効なバケットで、各オブジェクトに最新のバージョン 1 個と、最新でないバージョンが 0 個以上存在します。オブジェクトを削除するときは、次のことに注意してください。

- 削除リクエストでバージョン ID を指定しない場合、Amazon S3 はオブジェクトを削除する代わりに削除マーカーを追加します。現在のオブジェクトバージョンが最新でなくなり、削除マーカーが現在のバージョンになります。
- 削除リクエストでバージョン ID を指定した場合、Amazon S3 はそのオブジェクトバージョンを完全に削除します (削除マーカーは作成されません)。
- 最新でないバージョンが 0 の削除マーカーは、有効期限切れオブジェクト削除マーカー と呼ばれます。

この例では、バケットに期限切れオブジェクト削除マーカーを作成できるシナリオと、S3 ライフサイクル設定を使用して期限切れオブジェクト削除マーカーを削除するよう Amazon S3 に指示する方法を示します。

以下に示すように、NoncurrentVersionExpiration アクションを使用して、最新でないバージョンがそのようになってから 30 日後に削除し、10 個の旧バージョンを保持する S3 ライフサイクル設定を記述するとします。Amazon S3 が特定のバージョンを期限切れにするには、10 以上の旧バージョンが存在する必要があることに注意してください。Amazon S3 は、保存すると指定された数を超える最新でないバージョンをすべて完全に削除します。削除が行われるには、NoncurrentDays と NewerNoncurrentVersions の両方の値を超える必要があります。

```
<LifecycleConfiguration>
    <Rule>
        ...
        <NoncurrentVersionExpiration>
            <NewerNoncurrentVersions>10</NewerNoncurrentVersions>
            <NoncurrentDays>30</NoncurrentDays>
        </NoncurrentVersionExpiration>
    </Rule>
```

```
</LifecycleConfiguration>
```

NoncurrentVersionExpiration アクションは、現在のオブジェクトバージョンには適用されません。最新以外のバージョンのみ削除されます。

現在のオブジェクトバージョンの場合、現在のオブジェクトバージョンが明確に定義されたライフサイクルに従うかどうかに応じて存続期間を管理する以下のオプションがあります。

- 現在のオブジェクトバージョンが明確に定義されたライフサイクルに従う。

  この場合、次の例に示すように、現在のバージョンを削除するよう Amazon S3 に指示する Expiration アクションを含む S3 ライフサイクル設定を使用できます。

```
<LifecycleConfiguration>
    <Rule>
        ...
        <Expiration>
           <Days>60</Days>
        </Expiration>
        <NoncurrentVersionExpiration>
            <NewerNoncurrentVersions>10</NewerNoncurrentVersions>
            <NoncurrentDays>30</NoncurrentDays>
        </NoncurrentVersionExpiration>
    </Rule>
</LifecycleConfiguration>
```

  この例では、Amazon S3 は、現在の各オブジェクトバージョンに削除マーカーを追加することで、作成から 60 日後に現在のバージョンを削除します。このプロセスにより、現在のバージョンが最新でなくなり、削除マーカーが現在のバージョンになります。詳細については、「S3 バージョニングによる複数のバージョンのオブジェクトの保持」を参照してください。

  > **Note**
  >
  > 同じルールに Days と ExpiredObjectDeleteMarker のタグの両方を指定することはできません。Amazon S3は削除マーカーが経過機関の基準を満たすと、Days タグを指定することで、自動的に ExpiredObjectDeleteMarker クリーンアップを実行します。削除マーカーが唯一のバージョンになったらすぐにクリーンアップできるよう、ExpiredObjectDeleteMarker タグだけを含む別のルールを作成します。

同じ S3 ライフサイクル設定の NoncurrentVersionExpiration アクションは、最新でないオブジェクトが最新でなくなってから 30 日後に削除します。したがって、この例では、すべてのオブジェクトバージョンがオブジェクトの作成から 90 日後に完全に削除されます。この例では、Amazon S3 が特定のバージョンを期限切れにするには、10 以上の旧バージョンが存在する必要があることに注意してください。Amazon S3 は、保存すると指定された数を超える最新でないバージョンをすべて完全に削除します。削除が行われるには、NoncurrentDays と NewerNoncurrentVersions の両方の値を超える必要があります。

この過程で期限切れのオブジェクト削除マーカーが作成されますが、Amazon S3 が検知して削除します。

- 現在のオブジェクトバージョンに明確に定義されたライフサイクルがない。

  この場合、必要でない場合はオブジェクトを削除できます。このとき、1 つ以上の最新でないバージョンとともに削除マーカーが作成されます。NoncurrentVersionExpiration アクションを含む S3 ライフサイクル設定が最新でないすべてのバージョンを削除した場合、期限切れオブジェクト削除マーカーが生成されます。

  特にこのシナリオのために、S3 ライフサイクル設定には、期限切れオブジェクト削除マーカーを削除するために使用できる Expiration アクションを提供します。

```
<LifecycleConfiguration>
    <Rule>
       <ID>Rule 1</ID>
        <Filter>
          <Prefix>logs/</Prefix>
        </Filter>
        <Status>Enabled</Status>
        <Expiration>
           <ExpiredObjectDeleteMarker>true</ExpiredObjectDeleteMarker>
        </Expiration>
        <NoncurrentVersionExpiration>
            <NewerNoncurrentVersions>10</NewerNoncurrentVersions>
            <NoncurrentDays>30</NoncurrentDays>
        </NoncurrentVersionExpiration>
    </Rule>
</LifecycleConfiguration>
```

`ExpiredObjectDeleteMarker` アクションで `true` 要素を `Expiration` に設定することで、期限切れオブジェクト削除マーカーを削除するよう Amazon S3 に指示できます。

> **Note**
>
> `ExpiredObjectDeleteMarker` S3 ライフサイクルアクションを指定するときは、ルールではタグベースのフィルターを指定できません。

マルチパートアップロードを中止するライフサイクル設定

Amazon S3 マルチパートアップロード REST API オペレーションを使用すると、大容量オブジェクトをいくつかに分けてアップロードできます。マルチパートアップロードの詳細については、「Amazon S3 でのマルチパートアップロードを使用したオブジェクトのアップロードとコピー」を参照してください。

S3 ライフサイクル設定を使用すると、不完全なマルチパートアップロード (ルールで指定したキー名プレフィックスで特定) が開始後指定した日数以内に完了しない場合、アップロードを停止するように Amazon S3 に指示できます。Amazon S3 は、マルチパートアップロードを中止するとき、マルチパートアップロードに関連付けられているすべてのパートを削除します。このプロセスでは、Amazon S3 に保存されているパートを含む不完全なマルチパートアップロードがないことが保証されるので、ストレージコストを制御するのに役立ちます。

> **Note**
>
> `AbortIncompleteMultipartUpload` S3 ライフサイクルアクションを指定するときは、ルールではタグベースのフィルターを指定できません。

`AbortIncompleteMultipartUpload` アクションにルールを指定する S3 ライフサイクル設定の例を次に示します。このアクションは、開始されたから 7 日後に不完全なマルチパートアップロードを停止するように Amazon S3 に指示します。

```
<LifecycleConfiguration>
    <Rule>
        <ID>sample-rule</ID>
        <Filter>
           <Prefix>SomeKeyPrefix/</Prefix>
        </Filter>
```

```
        <Status>rule-status</Status>
        <AbortIncompleteMultipartUpload>
          <DaysAfterInitiation>7</DaysAfterInitiation>
        </AbortIncompleteMultipartUpload>
    </Rule>
</LifecycleConfiguration>
```

データがない旧オブジェクトの有効期限

オブジェクトのサイズのみに基づいてオブジェクトを移行するルールを作成できます。オブジェクトのサイズは、最小 (ObjectSizeGreaterThan) または最大 (ObjectSizeLessThan) を指定することも、バイト数で範囲を指定することもできます。プレフィックスとサイズの規則のように、複数のフィルターを使用する場合は、フィルターを <And> 要素で囲む必要があります。

```
<LifecycleConfiguration>
  <Rule>
    <ID>Transition with a prefix and based on size</ID>
    <Filter>
       <And>
          <Prefix>tax/</Prefix>
          <ObjectSizeGreaterThan>500</ObjectSizeGreaterThan>
       </And>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>365</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

ObjectSizeGreaterThan と ObjectSizeLessThan の両方の要素を使用して範囲を指定する場合、最大オブジェクトサイズは最小オブジェクトサイズより大きくなければなりません。複数のフィルターを使用する場合は、フィルターを <And> 要素で囲む必要があります。次の例は、500 バイトから 64,000 バイトの範囲でオブジェクトを指定する方法を示しています。範囲を指定する場合、ObjectSizeGreaterThan フィルターと ObjectSizeLessThan フィルターは指定された値を除外します。詳細については、「the section called “Filter 要素”」を参照してください。

```
<LifecycleConfiguration>
    <Rule>
        ...
```

```
            <And>
               <ObjectSizeGreaterThan>500</ObjectSizeGreaterThan>
               <ObjectSizeLessThan>64000</ObjectSizeLessThan>
            </And>
      </Rule>
</LifecycleConfiguration>
```

バージョニングが有効になっているバケットで作成された最新でない削除マーカーオブジェクトなど、データがなく、最新でないオブジェクトに限り期限切れにするルールを作成することもできます。次の例では、NoncurrentVersionExpiration アクションを使用して、あるバージョンが最新のバージョンでなくなってから 30 日後に削除し、10 の旧バージョンを保持します。またこの例では、ObjectSizeLessThan エレメントを使用してデータのないオブジェクトのみをフィルタリングします。

Amazon S3 が特定のバージョンを期限切れにするには、10 以上の旧バージョンが存在する必要があることに注意してください。Amazon S3 は、保存すると指定された数を超える最新でないバージョンをすべて完全に削除します。削除が行われるには、NoncurrentDays と NewerNoncurrentVersions の両方の値を超える必要があります。

```
<LifecycleConfiguration>
  <Rule>
    <ID>Expire noncurrent with size less than 1 byte</ID>
    <Filter>
       <ObjectSizeLessThan>1</ObjectSizeLessThan>
    </Filter>
    <Status>Enabled</Status>
    <NoncurrentVersionExpiration>
       <NewerNoncurrentVersions>10</NewerNoncurrentVersions>
       <NoncurrentDays>30</NoncurrentDays>
    </NoncurrentVersionExpiration>
  </Rule>
</LifecycleConfiguration>
```

例: 128 KB 未満のオブジェクトの移行を許可する

Amazon S3 はライフサイクル設定にデフォルトの動作を適用し、128 KB 未満のオブジェクトが任意のストレージクラスに移行されないようにします。最小サイズ (ObjectSizeGreaterThan) または最大サイズ (ObjectSizeLessThan) フィルターを追加して、小さいオブジェクトを移行することを許可できます。このフィルターでは、設定に小さいサイズを指定します。次の例では、128 KB 未満のオブジェクトを S3 Glacier Instant Retrieval ストレージクラスに移行します。

```
<LifecycleConfiguration>
  <Rule>
    <ID>Allow small object transitions</ID>
    <Filter>
          <ObjectSizeGreaterThan>1</ObjectSizeGreaterThan>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>365</Days>
      <StorageClass>GLACIER_IR</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

Note

2024 年 9 月、Amazon S3 は小さなオブジェクトのデフォルトの移行動作を次のように更新しました。

- デフォルトの移行動作の更新 — 2024 年 9 月以降、デフォルトの動作により、128 KB 未満のオブジェクトが任意のストレージクラスに移行されることを回避します。
- 以前のデフォルトの移行動作 — 2024 年 9 月以前は、デフォルトの動作により、128 KB 未満のオブジェクトは S3 Glacier および S3 Glacier Deep Archive ストレージクラスにのみ移行できました。

2024 年 9 月より前に作成された設定は、変更しない限り、以前の移行動作を保持します。つまり、ルールを作成、編集、または削除すると、設定のデフォルトの移行動作が更新された動作に変わります。ユースケースで必要な場合は、128KB 未満のオブジェクトが S3 Glacier および S3 Glacier Deep Archive に移行するように、デフォルトの移行動作を変更できます。これを行うには、PutBucketLifecycleConfiguration リクエストでオプションの `x-amz-transition-object-size-minimum-default` ヘッダーを使用します。

次の例は、PutBucketLifecycleConfiguration リクエストで `x-amz-transition-object-size-minimum-default` ヘッダーを使用して、S3 ライフサイクル設定に `varies_by_storage_class` のデフォルトの移行動作を適用する方法を示しています。この動作により、128 KB 未満のオブジェクトを S3 Glacier または S3 Glacier Deep Archive ストレージクラスに移行できます。デフォルトでは、他のすべてのストレージクラスは 128 KB 未満の移行を回避します。カスタムフィルターを使用

して、任意のストレージクラスの最小移行サイズを変更できます。カスタムフィルターは常にデフォルトの移行動作よりも優先されます。

```
HTTP/1.1 200
x-amz-transition-object-size-minimum-default: varies_by_storage_class
<?xml version="1.0" encoding="UTF-8"?>
...
```

Amazon S3 ライフサイクル問題のトラブルシューティング

以下の情報は、Amazon S3 ライフサイクル問題のトラブルシューティングに役立ちます。

トピック

- バケットでリストオペレーションを実行したところ、有効期限が切れているか、ライフサイクルルールによって移行されたと思われるオブジェクトが表示されました。
- ライフサイクルルールによって実行されたアクションをモニタリングするにはどうすればよいですか？
- バージョニング対応のバケットにライフサイクルルールを設定したにもかかわらず、S3 オブジェクトの数が増え続けています。
- ライフサイクルルールを使用して S3 バケットを空にするにはどうすればよいですか?
- オブジェクトを低コストのストレージクラスに移行した後、Amazon S3 の請求額が増加しました。
- バケットポリシーを更新しましたが、S3 オブジェクトが期限切れのライフサイクルルールによってまだ削除されたままです。
- S3 ライフサイクルルールによって期限切れになった S3 オブジェクトを回復できますか?
- 有効期限切れと移行のライフサイクルアクションが実行されないのはなぜでしょうか。
- ライフサイクルルールからプレフィックスを除外するにはどうすればよいですか?
- ライフサイクルルールに複数のプレフィックスを含めるにはどうすればよいですか?

バケットでリストオペレーションを実行したところ、有効期限が切れているか、ライフサイクルルールによって移行されたと思われるオブジェクトが表示されました。

S3 ライフサイクルオブジェクトの移行とオブジェクトの有効期限は非同期リストオペレーションです。そのため、オブジェクトが期限切れまたは移行の対象となる時点と、実際に移行または期限切れになるまでに遅延が生じる可能性があります。請求の変更は、アクションが完了していなくても、ライフサイクル ルールが満たされるとすぐに適用されます。この動作の例外は、ライフサイクルルー

ルが S3 Intelligent-Tiering ストレージクラスに移行するように設定されている場合です。オブジェクトが S3 Intelligent-Tiering に移行するまで、請求の変更は行われません。請求の変更の詳細については、「バケットのライフサイクル設定を設定する」を参照してください。

> **Note**
>
> Amazon S3 は、128 KB 未満のオブジェクトを S3 標準または S3 標準 - IA ストレージクラスから S3 Intelligent-Tiering、S3 標準 - IA、または S3 1 ゾーン - IA ストレージクラスに移行しません。

ライフサイクルルールによって実行されたアクションをモニタリングするにはどうすればよいですか？

ライフサイクルルールによって実行されたアクションをモニタリングするには、以下の機能を使用します。

- S3 イベント通知 - S3 ライフサイクルの有効期限や移行イベントが通知されるように S3 イベント通知を設定できます。
- S3 サーバーアクセスログ - S3 バケットのサーバーアクセスログを有効にして、別のストレージクラスへのオブジェクトの移行やオブジェクトの失効など、S3 ライフサイクル関連のアクションをキャプチャできます。詳細については、「ライフサイクルおよびログ記録」を参照してください。

ライフサイクルアクションによるストレージの変更を毎日確認するには、Amazon CloudWatch メトリクスを使用する代わりに S3 Storage Lens ダッシュボードを使用することをお勧めします。Storage Lens ダッシュボードでは、オブジェクト数またはサイズをモニタリングする以下のメトリクスを表示できます。

- 現行バージョンのバイト数
- 現行バージョンのオブジェクト数
- 旧バージョンのバイト数
- 旧バージョンのオブジェクト数
- 削除マーカーのオブジェクト数
- 削除マーカーのストレージバイト数
- 不完全なマルチパートアップロードのバイト数
- 不完全なマルチパートアップロードのオブジェクト数

バージョニング対応のバケットにライフサイクルルールを設定したにもかかわらず、S3 オブジェクトの数が増え続けています。

バージョニングが有効なバケットでは、オブジェクトの有効期限が切れた場合でも、オブジェクトはバケットから完全には削除されません。代わりに、オブジェクトの最新バージョンとして削除マーカーが作成されます。削除マーカーは引き続きオブジェクトとしてカウントされます。したがって、現在のバージョンのみを期限切れにするライフサイクルルールを作成した場合、S3 バケット内のオブジェクト数は減少するのではなく実際に増加します。

例えば、S3 バケットで 100 個のオブジェクトでバージョニングが有効になっていて、そのオブジェクトの現在のバージョンが 7 日後に期限切れになるようにライフサイクルルールが設定されているとします。7 日目以降は、元のオブジェクト 100 個 に加え、非現行バージョンとなる削除マーカーが 100 個作成されるため、オブジェクト数は 200 個に増加します。バージョニングが有効なバケットの S3 ライフサイクル設定ルールアクションの詳細については、「バケットのライフサイクル設定を設定する」を参照してください。

オブジェクトを完全に削除するには、ライフサイクル設定を追加して、以前のバージョンのオブジェクト、期限切れの削除マーカー、および不完全なマルチパートアップロードを削除します。新しいライフサイクルルールを作成する方法については、「バケットにライフサイクル設定を設定する」を参照してください。

> **Note**
>
> - Amazon S3 は、オブジェクトの移行日または有効期限を翌日の午前 0 時 (UTC) に丸めます。
>
> ライフサイクルアクションのオブジェクトを評価する場合、Amazon S3 は UTC でのオブジェクトの作成時間を使用します。例えば、バージョン管理されていないバケットで、1 日後にオブジェクトを期限切れにするように設定されたライフサイクルルールがあるとします。オブジェクトが 1 月 1 日 17:05 太平洋夏時間 (PDT) に作成されたとします。これは UTC では 1 月 2 日 00:05 になります。オブジェクトは 1 月 3 日の 00:05 UTC に 1 日経過し、S3 ライフサイクルが 1 月 4 日の 00:00 UTC にオブジェクトを評価すると、オブジェクトは有効期限の対象となります。
>
> Amazon S3 ライフサイクルアクションは非同期で実行されるため、ライフサイクルルールで指定された日付とオブジェクトの実際の物理的な移行の間に多少の遅延が生じる場合があります。詳細については、「移行または有効期限の遅延」を参照してください。

詳細については、「ライフサイクルルール: オブジェクトの存在時間に基づく」を参照してください。

- オブジェクトロックで保護されている S3 オブジェクトの場合、現在のバージョンは完全には削除されません。代わりに、削除マーカーがオブジェクトに追加され、オブジェクトは最新ではなくなります。その後、最新でないバージョンは保存され、永久に期限切れになることはありません。

ライフサイクルルールを使用して S3 バケットを空にするにはどうすればよいですか?

S3 ライフサイクルルールは、何百万ものオブジェクトがある S3 バケットを空にする効果的なツールです。S3 バケットから多数のオブジェクトを削除するには、必ず次の 2 組のライフサイクルルールを使用してください。

- 現在のバージョンのオブジェクトを期限切れにし、以前のバージョンのオブジェクトを完全に削除する
- 期限切れの削除マーカーを削除し、未完了のマルチパートアップロードを削除する

ライフサイクル設定ルールを作成する手順については、「バケットにライフサイクル設定を設定する」を参照してください。

> **Note**
>
> オブジェクトロックで保護されている S3 オブジェクトの場合、現在のバージョンは完全には削除されません。代わりに、削除マーカーがオブジェクトに追加され、オブジェクトは最新ではなくなります。その後、最新でないバージョンは保存され、永久に期限切れになることはありません。

オブジェクトを低コストのストレージクラスに移行した後、Amazon S3 の請求額が増加しました。

オブジェクトを低コストのストレージクラスに移行した後に請求額が増加する理由はいくつかあります。

- 小さなオブジェクトの S3 Glacier オーバーヘッド料金

S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive に移行した各オブジェクトについて、このストレージ更新に関連する合計 40 KB のオーバーヘッドが発生します。40 KB のオーバーヘッドの一部として、8 KB がメタデータとオブジェクト名の保存に使用されます。この 8 KB は S3 標準料金に従って請求されます。残りの 32 KB はインデックス作成と関連メタデータに使用されます。この 32 KB は、Glacier Flexible Retrieval または S3 Glacier Deep Archive の料金に従って請求されます。

そのため、小さいサイズのオブジェクトを多数保存する場合は、ライフサイクル移行の使用はお勧めしません。オーバーヘッド料金を削減するには、Amazon S3 に保存する前に、多数の小さなオブジェクトを少数の大きなオブジェクトに集約することを検討してください。コストに関する考慮事項の詳細については、「S3 Glacier Flexible Retrieval と S3 Glacier Deep Archive ストレージクラスへの移行 (オブジェクトのアーカイブ)」を参照してください。

- 最小ストレージ料金

  一部の S3 ストレージクラスには、最小ストレージ期間要件があります。最小期間が満たされる前にそれらのクラスから削除、上書き、または移行されたオブジェクトには、日割り計算による早期移行料金または削除料金が請求されます。これらの最小ストレージ期間要件は次のとおりです。

  - S3 標準 - IA および S3 1 ゾーン - IA - IA - 30 日
  - S3 Glacier Flexible Retrieval および S3 Glacier Instant Retrieval – 90 日
  - S3 Glacier Deep Archive – 180 日

  これらの要件の詳細については、S3 ライフサイクルを使用したオブジェクトの移行の「制約」セクションを参照してください。一般的な S3 料金情報については、「Amazon S3 の料金表」と「AWS料金計算ツール」を参照してください。

- ライフサイクル移行料金

  オブジェクトがライフサイクルルールによって別のストレージクラスに移行されるたびに、Amazon S3 はその移行を 1 つの移行リクエストとしてカウントします。これらの移行リクエストの料金は、これらのストレージクラスの料金に追加されます。多数のオブジェクトを移行する場合は、下位の階層に移行するときに、リクエストの料金を考慮してください。詳細については、「Amazon S3 の料金」を参照してください。

バケットポリシーを更新しましたが、S3 オブジェクトが期限切れのライフサイクルルールによってまだ削除されたままです。

バケットポリシーの Deny ステートメントは、ライフサイクルルールで定義されているオブジェクトの有効期限を妨げません。ライフサイクルアクション (移行や有効期限など) は S3 DeleteObject オペレーションを使用しません。代わりに、S3 ライフサイクルアクションは内部の S3 エンドポイントを使用して実行されます。(詳細については、「ライフサイクルおよびログ記録」を参照してください)

ライフサイクルルールでアクションが実行されないようにするには、ルールを編集、削除、または無効にする必要があります。

S3 ライフサイクルルールによって期限切れになった S3 オブジェクトを回復できますか?

S3 ライフサイクルによって期限切れになったオブジェクトを回復する唯一の方法は、バージョニングを使用することです。バージョニングは、オブジェクトが期限切れの対象となる前に実施する必要があります。ライフサイクルルールによって実行された有効期限オペレーションは元に戻せません。適用されている S3 ライフサイクルルールによってオブジェクトが完全に削除された場合、それらのオブジェクトを復元することはできません。バケットのバージョニングを有効にするには、「the section called “オブジェクトの複数のバージョンを保持する”」を参照してください。

バケットにバージョニングを適用しても、オブジェクトの最新バージョンがそのまま残っている場合は、期限切れのオブジェクトの以前のバージョンを復元できます。S3 ライフサイクルルールアクションの動作とバージョニングステータスの詳細については、「ライフサイクルアクションを記述する要素」の「ライフサイクルのアクションとバケットのバージョニング状態」テーブルを参照してください。

> **Note**
>
> S3 バケットが AWS バックアップ または S3 レプリケーションによって保護されている場合、これらの機能を使用して期限切れのオブジェクトを回復できる場合もあります。

有効期限切れと移行のライフサイクルアクションが実行されないのはなぜでしょうか。

バージョニングが有効であるか一時停止されているバケットの場合、Amazon S3 が Expiration アクションをどのように処理するかは、次の点を考慮すると理解しやすくなります。

- オブジェクトの有効期限は、オブジェクトの最新のバージョンにのみ適用されます(最新以外のバージョンには影響しません)。
- 1 つ以上のオブジェクトバージョンがあり、削除マーカーが最新バージョンである場合、Amazon S3 はアクションを実行しません。
- Amazon S3 は、S3 Object Lock が適用されているオブジェクトの非現行バージョンに対して、何もアクションを実行しません。
- PENDING レプリケーションステータスのオブジェクトの場合、Amazon S3 はオブジェクトの現行バージョンまたは非現行バージョンに対して、何もアクションを実行しません。

ライフサイクルストレージクラス移行には、次の制約があります。

- デフォルトでは、128 KB 未満のオブジェクトはどのストレージクラスにも移行されません。
- オブジェクトは S3 Standard-IA または S3 One Zone-IA に移行される前に、30 日間以上保存されている必要があります。
- バージョニングが有効であるか一時停止されているバケットの場合、PENDING レプリケーションステータスのオブジェクトは移行できません。

ライフサイクルルールからプレフィックスを除外するにはどうすればよいですか?

S3 ライフサイクルでは、ルール内のプレフィックスを除外することはサポートされていません。代わりに、タグを使用して、ルールに含めるすべてのオブジェクトにタグ付けします。ライフサイクルルールでのタグの使用については、「the section called “作成後 1 日以内にすべてのオブジェクトをアーカイブする”」を参照してください。

ライフサイクルルールに複数のプレフィックスを含めるにはどうすればよいですか?

S3 ライフサイクルでは、ルールに複数のプレフィックスを含めることはサポートされていません。代わりに、タグを使用して、ルールに含めるすべてのオブジェクトにタグ付けします。ライフサイクルルールでのタグの使用については、「the section called “作成後 1 日以内にすべてのオブジェクトをアーカイブする”」を参照してください。

ただし、同じ文字で始まるプレフィックスが 1 つ以上ある場合は、末尾のスラッシュ (/) を除外した部分的なプレフィックスをフィルターで指定することで、これらのプレフィックスをすべてルールに含めることができます。例えば、次のようなプレフィックスがあるとします。

```
sales1999/
sales2000/
```

```
sales2001/
```

ルールに 3 つのプレフィックスをすべて含めるには、ライフサイクルルールで <Prefix>sales</Prefix> を指定します。

Amazon S3 での口グ記録とモニタリング

モニタリングは、Amazon S3 および AWS ソリューションの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。マルチポイント障害が発生した場合は、その障害をより簡単にデバッグできるように、AWS ソリューションのすべての部分からモニタリングデータを収集することをお勧めします。Simple Storage Service (Amazon S3) のモニタリングを開始する前に、以下の質問に対する回答を反映したモニタリング計画を作成する必要があります。

- どのような目的でモニタリングしますか?
- どのリソースをモニタリングしますか?
- どのくらいの頻度でこれらのリソースをモニタリングしますか?
- どのモニタリングツールを利用しますか?
- 誰がモニタリングタスクを実行しますか?
- 問題が発生したときに誰が通知を受け取りますか?

Amazon S3 での口グ記録とモニタリングの詳細については、以下のトピックを参照してください。

> **Note**
>
> Amazon S3 Express One Zone ストレージクラスをディレクトリバケットで使用する方法の詳細については、「S3 Express One Zone」と「ディレクトリバケットの使用」を参照してください。

モニタリングは、Amazon S3 および AWS ソリューションの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。マルチポイント障害が発生した場合は、その障害をより簡単にデバッグできるように、AWS ソリューションのすべての部分からモニタリングデータを収集する必要があります。AWS には、Amazon S3 リソースをモニタリングし、潜在的なインシデントに対応するための複数のツールが用意されています。

Amazon CloudWatch アラーム

Amazon CloudWatch アラームを使用して、指定した期間中、1 つのメトリクスをモニタリングします。メトリクスが特定の閾値を超えると、Amazon SNS トピックまたは AWS Auto Scaling ポリシーに通知が送信されます。CloudWatch アラームは、特定の状態にあるという理由ではアク

ションを呼び出しません。状態が変わり、それが指定した期間だけ維持される必要があります。詳細については、Amazon CloudWatch によるメトリクスのモニタリング を参照してください。

AWS CloudTrail ログ

CloudTrail は、Amazon S3 のユーザー、ロール、または AWS のサービスによって実行されたアクションの記録を提供します。CloudTrail で収集された情報を使用して、Amazon S3 に対するリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。詳細については、「AWS CloudTrail を使用した Amazon S3 API コールのログ記録」を参照してください。

Amazon GuardDuty

Amazon GuardDuty は、アカウント、コンテナ、ワークロード、および AWS 環境内のデータを継続的にモニタリングし、S3 バケットに対する潜在的な脅威やセキュリティリスクを特定する脅威検出サービスです。また、GuardDuty は、検出した脅威に関する詳細なコンテキストも提供します。GuardDuty は、脅威の AWS CloudTrail 管理ログを監視し、セキュリティ関連情報を表示します。例えば、GuardDuty には、リクエストを行ったユーザー、リクエストが行われた場所、リクエストされた具体的な API など、環境で異常である可能性がある API リクエストの要素が含まれます。GuardDuty S3 Protection は、CloudTrail によって収集された S3 データイベントを監視し、環境内のすべての S3 バケットで異常および悪意のある可能性のある動作を特定します。

Amazon S3 アクセスログ

サーバーアクセスログでは、バケットに対して行われたリクエストの詳細なレコードが提供されます。サーバーアクセスのログは、多くのアプリケーションに役立ちます。例えば、アクセスのログ情報は、セキュリティやアクセスの監査に役立ちます。詳細については、サーバーアクセスログによるリクエストのログ記録 を参照してください。

AWS Trusted Advisor

Trusted Advisor は、AWS の数十万のお客様にサービスを提供することにより得られた、運用実績から学んだベストプラクティスを活用しています。Trusted Advisor はお客様の AWS 環境を検査し、システムの可用性とパフォーマンスを向上させたりセキュリティギャップを埋めたりする機会がある場合には、推奨事項を作成します。すべての AWS のお客様は、Trusted Advisor の 5 つのチェックにアクセスできます。ビジネスまたはエンタープライズサポートプランをご利用のお客様は、すべての Trusted Advisor チェックを表示できます。

Trusted Advisor には、以下の Amazon S3 関連のチェックがあります。

- Amazon S3 バケットのログ記録設定のチェック。
- オープンなアクセス許可がある Amazon S3 バケットのセキュリティチェック。

- バージョニングが有効になっていない、またはバージョニングが停止されている Amazon S3 バケットの耐障害性チェック。

詳細については、サポート ユーザーガイドの AWS Trusted Advisor を参照してください。

Amazon S3 Storage Lens

Amazon S3 ストレージレンズは、オブジェクトストレージの使用状況とアクティビティを組織全体で可視化するために使用できるクラウドストレージの分析機能です。S3 ストレージレンズメトリクスを使用することで、組織全体でどれだけのストレージがあるか、または最も急速に成長しているバケットとプレフィックスは何かなどの、要約されたインサイトを生成できます。S3 ストレージレンズメトリクスを使用して、コスト最適化の機会を特定し、データ保護とセキュリティのベストプラクティスを実装し、アプリケーションワークロードのパフォーマンスを向上させることもできます。

S3 ストレージレンズはメトリクスを集約し、Amazon S3 コンソールの [バケット] ページの [アカウントのスナップショット] セクションにこの情報を表示します。S3 Storage Lens は、インサイトと傾向を可視化したり、外れ値にフラグ付けしたり、ストレージコストの最適化やデータ保護のベストプラクティスの適用に関するレコメンデーション事項を受け取ったりするために使用できるインタラクティブダッシュボードも提供します。ダッシュボードには、組織、アカウント、AWS リージョン、ストレージクラス、バケット、プレフィックス、またはストレージレンズのグループレベルでインサイトを生成して可視化できる、ドリルダウンオプションが用意されています。詳細については、「Amazon S3 ストレージレンズを理解する」を参照してください。

Amazon S3 インベントリ

Amazon S3 インベントリは、オブジェクトのクエリと管理に使用できるオブジェクトとメタデータのリストを生成します。このインベントリレポートを使用して、オブジェクトサイズ、最終更新日、暗号化ステータス、その他のフィールドなどの詳細なデータを生成できます。これらのレポートは日次または週次で利用でき、最新のリストを自動的に提供します。

例えば、Amazon S3 インベントリを使用して、ビジネス、コンプライアンス、および規制上のニーズに合わせてオブジェクトのレプリケーションと暗号化のステータスを監査し、レポートを作成できます。また、Amazon S3 インベントリを使用してビジネスワークフローやビッグデータジョブを簡素化、高速化することもできます。これは、Amazon S3 同期 `List` API オペレーションのスケジュールされた代替手段を提供します。Amazon S3 インベントリは、`List` API オペレーションを使用してオブジェクトを監査しないため、バケットのリクエストレートには影響しません。詳細については、「S3 インベントリを使用したデータのカタログ化と分析」を参照してください。

Amazon S3イベント通知

Amazon S3 イベント通知機能で、S3 バケット内で特定のイベントが発生したときに、通知を受けることができます。通知を有効にするには、Amazon S3 から発行するイベントを識別する通知設定を追加します。詳細については、「Amazon S3 イベント通知」を参照してください。

Amazon S3 および AWS X-Ray

は、Amazon S3 と統合して、アプリケーションの S3 バケットを更新するアップストリームリクエストをトレースします。サービスが X-Ray SDK を使用してリクエストをトレースする場合、Amazon S3 は、Λ、Amazon SQS、Amazon SNS などのダウンストリームイベントサブスクライバーにトレースヘッダーを送信できます。X-Ray は Amazon S3 イベント通知のトレースメッセージを有効にします。X-Ray トレースマップを使用して、Amazon S3 およびアプリケーションが使用する他のサービス間の接続を表示できます。詳細については、「Amazon S3 and X-Ray」を参照してください。

以下のセキュリティのベストプラクティスも口グ記録とモニタリングに対処します。

- Identify and audit all your Amazon S3 buckets
- Implement monitoring using Amazon Web Services monitoring tools
- AWS Config の有効化
- Enable Amazon S3 server access logging
- Use CloudTrail
- Monitor Amazon Web Services security advisories

トピック

- モニタリングツール
- Amazon S3 の口グ記録オプション
- AWS CloudTrail を使用した Amazon S3 API コールの口グ記録
- サーバーアクセスログによるリクエストの口グ記録
- Amazon CloudWatch によるメトリクスのモニタリング
- Amazon S3 イベント通知
- Amazon S3 ストレージレンズを使用してストレージのアクティビティと使用状況を評価する
- S3 インベントリを使用したデータのカタログ化と分析

モニタリングツール

AWS では、Amazon S3 のモニタリングに使用できるさまざまなツールを提供しています。これらのツールの中には、自動モニタリングを設定できるものもあれば、手操作を必要とするものもあります。モニタリングタスクをできるだけ自動化することをお勧めします。

自動モニタリングツール

以下の自動化されたモニタリングツールを使用して、Amazon S3 をモニタリングし、問題が発生したときにレポートできます。

- Amazon CloudWatch のアラーム – 単一のメトリクスを指定した期間モニタリングし、特定の閾値に対する複数の期間にわたるメトリクスの値に基づいて、1 つ以上のアクションを実行します。アクションは、Amazon Simple Notification Service (Amazon SNS) のトピックまたは Amazon EC2 Auto Scaling のポリシーに送信される通知です。CloudWatch アラームは、特定の状態にあるという理由だけではアクションを呼び出しません。状態が変わって、変わった状態が指定期間にわたって維持される必要があります。詳細については、Amazon CloudWatch によるメトリクスのモニタリング を参照してください。
- AWS CloudTrail のログのモニタリング – アカウント間でログファイルを共有し、CloudTrail のログファイルを CloudWatch Logs に送信してリアルタイムでモニタリングします。また、ログを処理するアプリケーションを Java で作成し、CloudTrail からの提供後にログファイルが変更されていないことを確認します。詳細については、AWS CloudTrail を使用した Amazon S3 API コールのログ記録 を参照してください。

手動モニタリングツール

Amazon S3 のモニタリングでもう 1 つ重要な点は、CloudWatch のアラームのターゲット外の項目を手動でモニタリングすることです。Amazon S3、CloudWatch、Trusted Advisor、その他の AWS Management Consoleのダッシュボードには、AWS 環境の状態が一目でわかるビューが表示されます。サーバーアクセスのログ記録を有効にして、バケットへのアクセスを求めるリクエストを追跡できます。各アクセスログレコードには、1 つのアクセスリクエストに関する詳細が含まれます。内容は、リクエスタ、バケット名、リクエスト時刻、リクエストアクション、応答ステータス、およびエラーコード (存在する場合) です。詳細については、サーバーアクセスログによるリクエストのログ記録 を参照してください。

- Amazon S3 ダッシュボードには、次の情報が表示されます。
  - 含まれるバケット、オブジェクト、およびプロパティ。

- CloudWatch のホームページでは以下について確認できます。
  - 現在のアラームとステータス
  - アラームとリソースのグラフ
  - サービスのヘルスステータス

  また、CloudWatch を使用して以下のことを行えます。
  - 重要なサービスをモニタリングするためにカスタマイズされたダッシュボードを作成する。
  - メトリクスデータをグラフ化して、問題のトラブルシューティングを行い、傾向を確認する。
  - AWS リソースのすべてのメトリクスを検索およびブラウズする。
  - 問題があることを通知するアラームを作成/編集する。
- AWS Trusted Advisor は、AWS リソースのパフォーマンス、信頼性、セキュリティ、費用効率を向上するためのモニタリングに役立ちます。すべてのユーザーは、4 つの Trusted Advisor; チェックを利用できます。ビジネスまたはエンタープライズサポートプランのユーザーは、50 以上のチェックを利用できます。詳細については、「AWS Trusted Advisor」を参照してください。

  Trusted Advisor には Amazon S3 に関連する以下のチェックがあります。
  - Amazon S3 バケットのログ記録設定をチェックします。
  - オープンなアクセス許可がある Amazon S3 バケットのセキュリティチェック。
  - バージョニングが有効になっていない、またはバージョニングが停止されている Amazon S3 バケットの耐障害性チェック。

Amazon S3 のログ記録オプション

ユーザー、ロール、または AWS のサービス よって実行されたアクションを Amazon S3 リソースに記録し、監査およびコンプライアンス目的でログレコードを管理することができます。これを行うには、サーバーアクセスのログ記録、AWS CloudTrail ログ記録、またはその両方を組み合わせて使用します。Amazon S3 リソースのバケットレベルおよびオブジェクトレベルのアクションをログ記録するには、CloudTrail を使用することをお勧めします。以下のセクションに各オプションの詳細を示します。

- サーバーアクセスログによるリクエストのログ記録
- AWS CloudTrail を使用した Amazon S3 API コールのログ記録

CloudTrail ログおよび Amazon S3 サーバーアクセスログの主なプロパティを次の表に示します。テーブルとメモを確認し、CloudTrail がセキュリティ要件を満たしていることを確認してください。

ログのプロパティ	AWS CloudTrail	Amazon S3 サーバーログ
他のシステム (Amazon CloudWatch Logs、Amazon CloudWatch Events) に転送可能	はい	No
ログを複数の宛先に配信する (例えば、同じログを 2 つの異なるバケットに送信する)	はい	No
オブジェクトのサブセット (プレフィックス) のログを有効にする	はい	No
クロスアカウントログ配信 (異なるアカウントが所有するターゲットバケットとソースバケット)	はい	No
デジタル署名またはハッシュを使用したログファイルの整合性の検証	はい	No
ログファイルの暗号化 (デフォルトまたはカスタム)	はい	No
オブジェクトオペレーション (Amazon S3 API を使用)	はい	はい
バケットオペレーション (Amazon S3 API を使用)	はい	はい
ログの検索可能な UI	はい	No
オブジェクトロックパラメータのフィールド。ログ記録用	はい	No

ログのプロパティ	AWS CloudTrail	Amazon S3 サーバーログ
の Amazon S3 Select プロパティ		
ログレコードの `Object Size`、`Total Time`、`Turn-Around Time` 、`HTTP Referer` の各フィールド	いいえ	はい
ライフサイクルの移行、失効、復元	いいえ	はい
バッチ削除オペレーションでのキーのログ記録	いいえ	はい
認証の失敗 1	いいえ	はい
ログが配信されるアカウント	バケット所有者 [2]、リクエスタ	バケット所有者名のみ
Performance and Cost	AWS CloudTrail	Amazon S3 Server Logs
価格	管理イベント (初回配信) は無料です。データイベントには料金がかかります (ログの保存は別料金)。	ログの保存にかかる料金以外の追加コストなし
ログ配信の速度	データイベント (5 分ごと)、管理イベント (15 分ごと)	数時間以内
ログの形式	JSON	スペース区切りの改行区切りレコードを含むログファイル

メモ

1. CloudTrail では、認証に失敗したリクエスト (提供された認証情報が有効でない場合) またはリダイレクトが原因で失敗したリクエスト (エラーコード `301 Moved Permanently`) のログは配信されません。ただし、承認に失敗したリクエスト (`AccessDenied`) および匿名ユーザーによるリクエストのログは含まれます。

2. リクエスト内のオブジェクトへのフルアクセス権がそのアカウントに付与されていない場合、S3 バケット所有者に CloudTrail ログが送信されます。詳細については、「クロスアカウントのシナリオでの Amazon S3 オブジェクトレベルのアクション」を参照してください。
3. S3 は、VPC エンドポイントポリシーで拒否されている場合、または VPC ポリシーが評価される前にリクエストが失敗した場合、VPC エンドポイントリクエストの CloudTrail ログまたはサーバーアクセスログのリクエスタまたはバケット所有者への配信をサポートしません。

AWS CloudTrail を使用した Amazon S3 API コールのログ記録

Amazon S3 は、ユーザー、ロール、または AWS のサービス が実行したアクションの記録を提供するサービスである AWS CloudTrail と統合されています。CloudTrail は、Amazon S3 へのすべての API コールをイベントとしてキャプチャします。キャプチャされた呼び出しには、Amazon S3 コンソールからの呼び出しと、Amazon S3 API オペレーションへのコード呼び出しが含まれます。CloudTrail で収集された情報を使用して、Amazon S3 に対するリクエスト、リクエスト元の IP アドレス、リクエストの作成日時、その他の詳細を確認できます。

各イベントまたはログエントリには、リクエストの生成者に関する情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます。

- ルートユーザーまたはユーザー認証情報のどちらを使用してリクエストが送信されたか。
- リクエストが IAM Identity Center ユーザーに代わって行われたかどうか。
- リクエストがロールまたはフェデレーションユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- リクエストが、別の AWS のサービス によって送信されたかどうか。

アカウントを作成すると、AWS アカウント で CloudTrail がアクティブになり、自動的に CloudTrail の[イベント履歴] にアクセスできるようになります。CloudTrail の [イベント履歴] では、AWS リージョン で過去 90 日間に記録された 管理イベントの表示、検索、およびダウンロードが可能で、変更不可能な記録を確認できます。詳細については、「AWS CloudTrail ユーザーガイド」の「CloudTrail イベント履歴の使用」を参照してください。[イベント履歴] の閲覧には CloudTrail の料金はかかりません。

AWS アカウント で過去 90 日間のイベントを継続的に記録するには、証跡または CloudTrail Lake イベントデータストアを作成します。

CloudTrail 証跡

証跡により、CloudTrail はログファイルを Amazon S3 バケットに配信できます。AWS Management Console を使用して作成した証跡はマルチリージョンです。AWS CLI を使用する際は、単一リージョンまたは複数リージョンの証跡を作成できます。アカウント内のすべて AWS リージョン でアクティビティを把握するため、マルチリージョン証跡を作成することをお勧めします。単一リージョンの証跡を作成する場合、証跡の AWS リージョン に記録されたイベントのみを表示できます。証跡の詳細については、「AWS CloudTrail ユーザーガイド」の「AWS アカウント の証跡の作成」および「組織の証跡の作成」を参照してください。

証跡を作成すると、進行中の管理イベントのコピーを 1 つ無料で CloudTrail から Amazon S3 バケットに配信できますが、Amazon S3 ストレージには料金がかかります。CloudTrail の料金の詳細については、「AWS CloudTrail の料金」を参照してください。Amazon S3 の料金に関する詳細については、「Amazon S3 の料金」を参照してください。

CloudTrail Lake イベントデータストア

[CloudTrail Lake] を使用すると、イベントに対して SQL ベースのクエリを実行できます。CloudTrail Lake は、行ベースの JSON 形式の既存のイベントを Apache ORC 形式に変換します。ORC は、データを高速に取得するために最適化された単票ストレージ形式です。イベントは、イベントデータストアに集約されます。イベントデータストアは、高度なイベントセレクタを適用することによって選択する条件に基づいた、イベントのイミュータブルなコレクションです。どのイベントが存続し、クエリに使用できるかは、イベントデータストアに適用するセレクタが制御します。CloudTrail Lake の詳細については、「AWS CloudTrail ユーザーガイド」の「AWS CloudTrail Lake の使用」を参照してください。

CloudTrail Lake のイベントデータストアとクエリにはコストがかかります。イベントデータストアを作成する際に、イベントデータストアに使用する料金オプションを選択します。料金オプションによって、イベントの取り込みと保存にかかる料金、および、そのイベントデータストアのデフォルトと最長の保持期間が決まります。CloudTrail の料金の詳細については、「AWS CloudTrail の料金」を参照してください。

必要な場合はログファイルを自身のバケットに保管できますが、ログファイルを自動的にアーカイブまたは削除するように Amazon S3 ライフサイクルルールを定義することもできます。デフォルトでは Amazon S3 のサーバー側の暗号化 (SSE) を使用して、ログファイルが暗号化されます。

CloudTrail ログを Amazon S3 サーバーアクセスログと CloudWatch Logs と併用する

AWS CloudTrail ログは、Amazon S3 のユーザー、ロール、または AWS のサービスによって実行されたアクションの記録を提供するのに対し、Amazon S3 サーバーアクセスログは、S3 バケットに対して行われたリクエストの詳細な記録を提供します。ログ別の機能とプロパティ、パフォーマンス、コストの詳細については、the section called “ログ記録オプション” を参照してください。

AWS CloudTrail ログは、Amazon S3 のサーバーアクセスログと一緒に使用できます。CloudTrail ログを使用すると、Amazon S3 バケットレベルおよびオブジェクトレベルのオペレーションの詳細な API トラッキングが提供されます。Amazon S3 のサーバーアクセスログでは、Amazon S3 内のオブジェクトレベルのデータオペレーションが可視化されます。サーバーアクセスログの詳細については、サーバーアクセスログによるリクエストのログ記録 を参照してください。

CloudTrail ログは、Amazon S3 の Amazon CloudWatch と一緒に使用することもできます。CloudTrail を CloudWatch Logs と統合すると、CloudTrail が取得した S3 バケットレベル API アクティビティが、指定した CloudWatch ロググループの CloudWatch ログストリームに送られます。特定の API アクティビティをモニタリングする CloudWatch アラームを作成し、その API アクティビティが発生した時に電子メールの通知を受け取ることができます。特定の API アクティビティをモニタリングするための CloudWatch アラームの詳細については、AWS CloudTrail ユーザーガイドを参照してください。Amazon S3 と CloudWatch の併用の詳細については、Amazon CloudWatch によるメトリクスのモニタリング を参照してください。

> **Note**
>
> S3 は、VPC エンドポイントポリシーで拒否されている場合、VPC エンドポイントリクエストのリクエスタまたはバケット所有者への CloudTrail ログの配信をサポートしません。

Amazon S3 SOAP API コールを使用した CloudTrail トラッキング

CloudTrail は、Amazon S3 SOAP API コールを追跡します。Amazon S3 SOAP のサポートは HTTP 経由で非推奨ですが、HTTPS 経由では引き続き利用可能です。Amazon S3 SOAP サポートの詳細については、「Amazon S3 API リファレンス」の「Appendix: SOAP API」を参照してください。

> **Important**
>
> 新しい Amazon S3 機能は、SOAP ではサポートされません。REST API か AWS SDK を使用することをお勧めします。

次の表は、CloudTrail の口グ記録によって追跡される Amazon S3 SOAP アクションを示しています。

SOAP API 名	CloudTrail ログで使用される API イベント名
ListAllMyBuckets	`ListBuckets`
CreateBucket	`CreateBucket`
DeleteBucket	`DeleteBucket`
GetBucketAccessControlPolicy	`GetBucketAcl`
SetBucketAccessControlPolicy	`PutBucketAcl`
GetBucketLoggingStatus	`GetBucketLogging`
SetBucketLoggingStatus	`PutBucketLogging`

CloudTrail と Amazon S3 の詳細については、以下のトピックを参照してください。

トピック

- Amazon S3 CloudTrail イベント
- Simple Storage Service (Amazon S3) と S3 on Outposts の CloudTrail ログファイルエントリ
- S3 バケットとオブジェクトの CloudTrail イベントログ記録の有効化
- CloudTrail を使用した Amazon S3 リクエストの識別

Amazon S3 CloudTrail イベント

> **Important**
>
> Amazon S3 では、Amazon S3 内のすべてのバケットの基本レベルの暗号化として、Amazon S3 が管理するキー (SSE-S3) によるサーバー側の暗号化が適用されるようになりました。2023 年 1 月 5 日以降、Amazon S3 にアップロードされるすべての新しいオブジェクトは、追加費用なしで、パフォーマンスに影響を与えずに自動的に暗号化されます。S3 バケットのデフォルト暗号化設定と新しいオブジェクトのアップロードのための自動暗号化ステータスは、AWS CloudTrail ログ、S3 インベントリ、S3 ストレージレンズ、Amazon S3 コンソール、および AWS Command Line Interface と AWS SDK の追加の Amazon S3 API レスポンスヘッダーとして利用できるようになりました。詳細については、「デフォルト暗号化に関するよくある質問」を参照してください。

このセクションでは、S3 が CloudTrail に記録するイベントについて説明します。

CloudTrail の Amazon S3 データイベント

データイベントでは、リソース上またはリソース内で実行されるリソースオペレーション (Amazon S3 オブジェクトの読み取りまたは書き込みなど) についての情報が得られます。これらのイベントは、データプレーンオペレーションとも呼ばれます。データイベントは、多くの場合、高ボリュームのアクティビティです。デフォルトでは、CloudTrail はデータイベントをログ記録しません。CloudTrail [イベント履歴] にはデータイベントは記録されません。

追加の変更がイベントデータに適用されます。CloudTrail の料金の詳細については、「AWS CloudTrail の料金」を参照してください。

CloudTrail コンソール、AWS CLI、または CloudTrail API オペレーションを使用して、Amazon S3 リソースタイプのデータイベントをログ記録できます。データイベントをログに記録する方法の詳細については、「AWS CloudTrail ユーザーガイド」の「AWS Management Console を使用したデータイベントのログ記録」および「AWS Command Line Interface を使用したデータイベントのログ記録」を参照してください。

次の表に、データイベントをログに記録できる Amazon S3 リソースタイプを示します。データイベントタイプ (コンソール) 列には、CloudTrail コンソールの[データイベントタイプ]リストから選択する値が表示されます。resources.type 値列には、AWS CLI または CloudTrail API を使用して高度なイベントセレクタを設定するときに指定する `resources.type` 値が表示されます。CloudTrail に

記録されたデータ API 列には、リソース タイプの CloudTrail に口グ記録された API コールが表示されます。

データイベントタイプ (コンソール)	resources.type 値	CloudTrail に口グ記録されたデータ API
S3	`AWS::S3::Object`	• AbortMultipartUpload • CompleteMultipartUpload • CopyObject • CreateMultipartUpload • DeleteObject • DeleteObjectTagging • DeleteObjects • GetObject • GetObjectAcl • GetObjectAttributes • GetObjectLegalHold • GetObjectRetention • GetObjectTagging • GetObjectTorrent • HeadObject • HeadBucket • ListMultipartUploads • ListObjectVersions • ListObjects • ListParts • PutObject • PutObjectAcl • PutObjectLegalHold • PutObjectRetention • PutObjectTagging

データイベントタイプ (コンソール)	resources.type 値	CloudTrail にログ記録されたデータ API
		• RestoreObject • SelectObjectContent • UploadPart • UploadPartCopy
S3 Express One Zone	`AWS::S3Express::Object`	• AbortMultipartUpload • CompleteMultipartUpload • CreateSession • CopyObject • CreateMultipartUpload • DeleteObject • DeleteObjects • GetObject • GetObjectAttributes • HeadBucket • HeadObject • ListObjectsV2 • ListParts • PutObject • UploadPart • UploadPartCopy

データイベントタイプ (コンソール)	resources.type 値	CloudTrail にログ記録されたデータ API
S3 アクセスポイント	`AWS::S3::Access Point`	• AbortMultipartUpload • CompleteMultipartUpload • CopyObject (同じリージョンへのコピーのみ) • CreateMultipartUpload • DeleteObject • DeleteObjectTagging • GetBucketAcl • GetBucketCors • GetBucketLocation • GetBucketNotificationConfiguration • GetBucketPolicy • GetObject • GetObjectAcl • GetObjectAttributes • GetObjectLegalHold • GetObjectRetention • GetObjectTagging • HeadBucket • HeadObject • ListMultipartUploads • ListObjects • ListObjectsV2 • ListObjectVersions • ListParts • Presign • PutObject

データイベントタイプ (コンソール)	resources.type 値	CloudTrail にログ記録されたデータ API
		• PutObjectLegalHold • PutObjectRetention • PutObjectAcl • PutObjectTagging • RestoreObject • UploadPart • UploadPartCopy (同じリージョンへのコピーのみ)

データイベントタイプ (コンソール)	resources.type 値	CloudTrail にログ記録されたデータ API
S3 Object Lambda	`AWS::S3ObjectLambda::AccessPoint`	• AbortMultipartUpload • CompleteMultipartUpload • CopyObject (同じリージョンへのコピーのみ) • CreateMultipartUpload • DeleteObject • DeleteObjectTagging • GetObject • GetObjectAcl • GetObjectLegalHold • GetObjectRetention • GetObjectTagging • HeadObject • ListMultipartUploads • ListObjects • ListObjectVersions • ListParts • PutObject • PutObjectLegalHold • PutObjectRetention • PutObjectAcl • PutObjectTagging • RestoreObject • UploadPart • WriteGetObjectResponse

データイベントタイプ (コンソール)	resources.type 値	CloudTrail にログ記録されたデータ API
S3 Outposts	`AWS::S3Outposts::Object`	• AbortMultipartUpload • CompleteMultipartUpload • CopyObject (同じリージョンへのコピーのみ) • CreateMultipartUpload • DeleteObject • DeleteObjectTagging • GetObject • GetObjectTagging • HeadObject • ListMultipartUploads • ListObjects • ListObjectsV2 • ListParts • PutObject • PutObjectTagging • UploadPart • UploadPartCopy

`eventName`、`readOnly`、および `resources.ARN` フィールドでフィルタリングして、自分にとって重要なイベントのみをログに記録するように高度なイベントセレクタを設定できます。オブジェクトの詳細については、「AWS CloudTrail API リファレンス」の「AdvancedFieldSelector」を参照してください。

CloudTrail の Amazon S3 管理イベント

Amazon S3 は、すべてのコントロールプレーンオペレーションを管理イベントとして記録します。S3 API オペレーションの詳細については、「Amazon S3 API Reference」を参照してください。

CloudTrail が Amazon S3 に対して行われたリクエストをキャプチャする方法

デフォルトでは、CloudTrail は過去 90 日間の S3 バケットレベルの API コールをログに記録しますが、オブジェクトに対して行われたログリクエストは記録しません。バケットレベルの呼び出しには `CreateBucket`、`DeleteBucket`、`PutBucketLifecycle`、`PutBucketPolicy` などのイベントが含まれます。バケットレベルのイベントは CloudTrail コンソールで確認できますが、そこでデータイベント (Amazon S3 オブジェクトレベルのコール) を確認することはできません。それらについて CloudTrail ログを解析またはクエリする必要があります。

CloudTrail ロギングによって追跡される Amazon S3 アカウントレベルのアクション

CloudTrail はアカウントレベルのアクションを記録します。Amazon S3 レコードは、他の AWS のサービス のレコードと一緒にログファイルに記録されます。CloudTrail は、期間とファイルサイズに基づいて、新しいファイルをいつ作成して書き込むかを決定します。

このセクションでは、CloudTrail によるログ記録でサポートされている Amazon S3 アカウントレベルのアクションの一覧を示します。

CloudTrail のログ記録によって追跡される Amazon S3 アカウントレベルの API アクションは、以下のイベント名で表示されます。CloudTrail イベント名は API アクション名とは異なります。例えば、DeletePublicAccessBlock は DeleteAccountPublicAccessBlock です。

- DeleteAccountPublicAccessBlock
- GetAccountPublicAccessBlock
- PutAccountPublicAccessBlock

CloudTrail ログ記録によって追跡される Amazon S3 バケットレベルのアクション

デフォルトでは、CloudTrail はバケットレベルのアクションをログに記録します。Amazon S3 レコードは、他の AWS のサービスレコードと一緒にログファイルに記録されます。CloudTrail は、期間とファイルサイズに基づいて、新しいファイルをいつ作成して書き込むかを決定します。

このセクションには、CloudTrail によるログ記録でサポートされている Amazon S3 バケットレベルのアクションの一覧が記載されています。

CloudTrail のログ記録によって追跡される Amazon S3 バケットレベルの API アクションは、以下のイベント名で表示されます。CloudTrail イベント名が API アクション名と異なる場合があります。たとえば、`PutBucketLifecycleConfiguration` は `PutBucketLifecycle` です。

- CreateBucket
- CreateBucketMetadataTableConfiguration
- DeleteBucket
- DeleteBucketAnalyticsConfiguration
- DeleteBucketCors
- DeleteBucketEncryption
- DeleteBucketIntelligentTieringConfiguration
- DeleteBucketInventoryConfiguration
- DeleteBucketLifecycle
- DeleteBucketMetadataTableConfiguration
- DeleteBucketMetricsConfiguration
- DeleteBucketOwnershipControls
- DeleteBucketPolicy
- DeleteBucketPublicAccessBlock
- DeleteBucketReplication
- DeleteBucketTagging
- GetAccelerateConfiguration
- GetBucketAcl
- GetBucketAnalyticsConfiguration
- GetBucketCors
- GetBucketEncryption
- GetBucketIntelligentTieringConfiguration
- GetBucketInventoryConfiguration
- GetBucketLifecycle
- GetBucketLocation
- GetBucketLogging
- GetBucketMetadataTableConfiguration
- GetBucketMetricsConfiguration
- GetBucketNotification

- GetBucketObjectLockConfiguration
- GetBucketOwnershipControls
- GetBucketPolicy
- GetBucketPolicyStatus
- GetBucketPublicAccessBlock
- GetBucketReplication
- GetBucketRequestPayment
- GetBucketTagging
- GetBucketVersioning
- GetBucketWebsite
- HeadBucket
- ListBuckets
- PutAccelerateConfiguration
- PutBucketAcl
- PutBucketAnalyticsConfiguration
- PutBucketCors
- PutBucketEncryption
- PutBucketIntelligentTieringConfiguration
- PutBucketInventoryConfiguration
- PutBucketLifecycle
- PutBucketLogging
- PutBucketMetricsConfiguration
- PutBucketNotification
- PutBucketObjectLockConfiguration
- PutBucketOwnershipControls
- PutBucketPolicy
- PutBucketPublicAccessBlock
- PutBucketReplication
- PutBucketRequestPayment
- PutBucketTagging

- PutBucketVersioning
- PutBucketWebsite

これらの API オペレーションに加えて、OPTIONS オブジェクトのオブジェクトレベルのアクションを使用することもできます。このアクションは、バケットの CORS 設定を確認するため、CloudTrail ログ記録のバケットレベルアクションと同様に扱われます。

CloudTrail ログ記録が追跡する Amazon S3 Express One Zone バケットレベル (リージョン API エンドポイント) アクション

デフォルトでは、CloudTrail はディレクトリバケットのバケットレベルのアクションを管理イベントとして記録します。S3 Express One Zone の CloudTrail 管理イベントの `eventsource` は、`s3express.amazonaws.com` です。

次のリージョンエンドポイント API オペレーションが CloudTrail に記録されます。

- CreateBucket
- DeleteBucket
- DeleteBucketPolicy
- GetBucketPolicy
- PutBucketPolicy
- ListDirectoryBuckets
- PutBucketEncryption
- GetBucketEncryption
- DeleteBucketEncryption

詳細については、「S3 Express One Zone の AWS CloudTrail による ログ記録」を参照してください。

クロスアカウントのシナリオでの Amazon S3 オブジェクトレベルのアクション

クロスアカウントのシナリオでオブジェクトレベルの API コールに関連する特殊なユースケースと CloudTrail ログが報告される方法を次に示します。CloudTrail は、ログエントリが編集または省略される一部のアクセス拒否ケースを除き、リクエスタ (API コールを行ったアカウント) にログを配信します。クロスアカウントアクセスを設定する際には、このセクションの例を検討します。

> **Note**
>
> 例では、CloudTrail ログが適切に設定されていることを前提とします。

例 1: CloudTrail がバケット所有者にログを配信する

CloudTrail は、バケット所有者が同じオブジェクト API オペレーションに対するアクセス許可を持たない場合でも、バケット所有者にログを配信します。次のクロスアカウントのシナリオを検討してください。

- アカウント A がバケットを所有しています。
- アカウント B (リクエスタ) が、そのバケット内のオブジェクトへのアクセスを試みます。
- アカウント C がオブジェクトを所有しています。アカウント C はアカウント A と同じアカウントである場合とそうでない場合があります。

> **Note**
>
> CloudTrail は、常にオブジェクトレベルの API ログをリクエスタ (アカウント B) に配信します。さらに、CloudTrail は、バケット所有者 (アカウント A) がそのオブジェクト (アカウント C) を所有していないか、そのオブジェクトに対する同じ API オペレーションへのアクセス許可がない場合でも、バケット所有者に同じログを配信します。

例 2: CloudTrail は設定オブジェクト ACL で使用されている E メールアドレスを拡散しない

次のクロスアカウントのシナリオを検討してください。

- アカウント A がバケットを所有しています。
- アカウント B (リクエスタ) は、E メールアドレスを使用してオブジェクト ACL の付与を設定するためのリクエストを送信します。ACL の詳細については、「アクセスコントロールリスト (ACL) の概要」を参照してください。

リクエスタは E メール情報と共にログを取得します。ただし、例 1 のようにバケット所有者がログの受信資格を持つ場合、バケット所有者はイベントを報告する CloudTrail ログを取得します。一方、バケット所有者は ACL 設定情報 (具体的には被付与者の E メールと権限) を取得しません。ログ

がバケット所有者に通知する情報は、アカウント B によって ACL API コールが行われたということだけです。

Simple Storage Service (Amazon S3) と S3 on Outposts の CloudTrail ログファイルエントリ

> **Important**
>
> Amazon S3 では、Amazon S3 内のすべてのバケットの基本レベルの暗号化として、Amazon S3 が管理するキー (SSE-S3) によるサーバー側の暗号化が適用されるようになりました。2023 年 1 月 5 日以降、Amazon S3 にアップロードされるすべての新しいオブジェクトは、追加費用なしで、パフォーマンスに影響を与えずに自動的に暗号化されます。S3 バケットのデフォルト暗号化設定と新しいオブジェクトのアップロードのための自動暗号化ステータスは、AWS CloudTrail ログ、S3 インベントリ、S3 ストレージレンズ、Amazon S3 コンソール、および AWS Command Line Interface と AWS SDK の追加の Amazon S3 API レスポンスヘッダーとして利用できるようになりました。詳細については、「デフォルト暗号化に関するよくある質問」を参照してください。

各イベントは任意の送信元からの単一のリクエストを表し、リクエストされた API オペレーション、オペレーションの日時、リクエストパラメータなどに関する情報を含みます。CloudTrail ログファイルは、パブリック API コールの順序付けられたスタックトレースではないため、イベントは特定の順序で表示されません。

> **Note**
>
> Amazon S3 Express One Zone の CloudTrail ログファイルの例を表示するには、「S3 Express One Zone の CloudTrail ログファイルの例」を参照してください。

詳細については、以下の例を参照してください。

トピック

- 例: Amazon S3 の CloudTrail ログファイルのエントリ

例: Amazon S3 の CloudTrail ログファイルのエントリ

次は、GET サービス、PutBucketAcl および GetBucketVersioning のアクションを示す CloudTrail ログエントリの例です。


```
{
    "Records": [
    {
        "eventVersion": "1.03",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "111122223333",
            "arn": "arn:aws:iam::111122223333:user/myUserName",
            "accountId": "111122223333",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "userName": "myUserName"
        },
        "eventTime": "2019-02-01T03:18:19Z",
        "eventSource": "s3.amazonaws.com",
        "eventName": "ListBuckets",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "[]",
        "requestParameters": {
            "host": [
                "s3.us-west-2.amazonaws.com"
            ]
        },
        "responseElements": null,
        "additionalEventData": {
            "SignatureVersion": "SigV2",
            "AuthenticationMethod": "QueryString",
            "aclRequired": "Yes"
    },
        "requestID": "47B8E8D397DCE7A6",
        "eventID": "cdc4b7ed-e171-4cef-975a-ad829d4123e8",
        "eventType": "AwsApiCall",
        "recipientAccountId": "444455556666",
        "tlsDetails": {
            "tlsVersion": "TLSv1.2",
            "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
            "clientProvidedHostHeader": "s3.amazonaws.com"
    }
```

```
    },
    {
       "eventVersion": "1.03",
       "userIdentity": {
            "type": "IAMUser",
            "principalId": "111122223333",
            "arn": "arn:aws:iam::111122223333:user/myUserName",
            "accountId": "111122223333",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "userName": "myUserName"
        },
      "eventTime": "2019-02-01T03:22:33Z",
      "eventSource": "s3.amazonaws.com",
      "eventName": "PutBucketAcl",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "",
      "userAgent": "[]",
      "requestParameters": {
          "bucketName": "",
          "AccessControlPolicy": {
              "AccessControlList": {
                  "Grant": {
                      "Grantee": {
                          "xsi:type": "CanonicalUser",
                          "xmlns:xsi": "http://www.w3.org/2001/XMLSchema-instance",
                          "ID":
"d25639fbe9c19cd30a4c0f43fbf00e2d3f96400a9aa8dabfbbebe1906Example"
                       },
                      "Permission": "FULL_CONTROL"
                   }
              },
              "xmlns": "http://s3.amazonaws.com/doc/2006-03-01/",
              "Owner": {
                  "ID":
"d25639fbe9c19cd30a4c0f43fbf00e2d3f96400a9aa8dabfbbebe1906Example"
              }
          },
          "host": [
              "s3.us-west-2.amazonaws.com"
          ],
          "acl": [
              ""
          ]
      },
```

```
      "responseElements": null,
      "additionalEventData": {
          "SignatureVersion": "SigV4",
          "CipherSuite": "ECDHE-RSA-AES128-SHA",
          "AuthenticationMethod": "AuthHeader"
      },
      "requestID": "BD8798EACDD16751",
      "eventID": "607b9532-1423-41c7-b048-ec2641693c47",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333",
      "tlsDetails": {
            "tlsVersion": "TLSv1.2",
            "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
            "clientProvidedHostHeader": "s3.amazonaws.com"
    }
    },
    {
      "eventVersion": "1.03",
      "userIdentity": {
          "type": "IAMUser",
          "principalId": "111122223333",
          "arn": "arn:aws:iam::111122223333:user/myUserName",
          "accountId": "111122223333",
          "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
          "userName": "myUserName"
        },
      "eventTime": "2019-02-01T03:26:37Z",
      "eventSource": "s3.amazonaws.com",
      "eventName": "GetBucketVersioning",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "",
      "userAgent": "[]",
      "requestParameters": {
          "host": [
              "s3.us-west-2.amazonaws.com"
          ],
          "bucketName": "amzn-s3-demo-bucket1",
          "versioning": [
              ""
          ]
      },
      "responseElements": null,
      "additionalEventData": {
          "SignatureVersion": "SigV4",
```

```
            "CipherSuite": "ECDHE-RSA-AES128-SHA",
            "AuthenticationMethod": "AuthHeader"
        },
          "requestID": "07D681279BD94AED",
          "eventID": "f2b287f3-0df1-4961-a2f4-c4bdfed47657",
          "eventType": "AwsApiCall",
          "recipientAccountId": "111122223333",
          "tlsDetails": {
                "tlsVersion": "TLSv1.2",
                "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
                "clientProvidedHostHeader": "s3.amazonaws.com"
        }
        }
      ]
}
```

S3 バケットとオブジェクトの CloudTrail イベントログ記録の有効化

CloudTrail データイベントを使用して、Amazon S3 のバケットおよびオブジェクトレベルのリクエストに関する情報を取得できます。すべてのバケットまたは特定のバケットのリストの CloudTrail データイベントを有効にするには、CloudTrail で手動で証跡を作成する必要があります。

> **Note**
>
> - CloudTrail のデフォルト設定では、管理イベントのみが検出されます。アカウントに対してデータイベントを有効にしていることをチェックして確認します。
> - 高いワークロードを生成している S3 バケットがある場合、短期間で数千のログを生成する可能性があります。ビジーなバケットでは、CloudTrail データイベントを有効にする期間にご注意ください。

CloudTrail は、選択した S3 バケットに Amazon S3 データイベントを保存します。クエリと分析を簡素化するには、所有する複数のバケットのイベントを適切にまとめられるように別の AWS アカウント のバケットの使用を検討することをお勧めします。AWS Organizations では、モニタリングしているバケットを所有しているアカウントにリンクされた AWS アカウント を簡単に作成することができます。詳細については、『AWS Organizations ユーザーガイド』の「What is AWS Organizations? (とは ?)」 を参照してください。

CloudTrail で証跡のデータイベントをログに記録する場合、汎用バケットに保存されたオブジェクトのデータイベントを記録するために、高度なイベントセレクタとベーシックイベントセレクタのどち

らを使用するかを選択できます。ディレクトリバケットに保存されているオブジェクトのデータイベントをログに記録するには、高度なイベントセレクタを使用する必要があります。詳細については、「S3 Express One Zone の AWS CloudTrail による口グ記録」を参照してください。

アドバンストイベントセレクタを使用して CloudTrail コンソールで証跡を作成する場合、データイベントセクションで、[ログセレクタテンプレート] の [すべてのイベントをログに記録する] を選択して、すべてのオブジェクトレベルのイベントをログ記録できます。ベーシックイベントセレクタを使用して CloudTrail コンソールで証跡を作成する場合、データイベントセクションで、[アカウントのすべての S3 バケットを選択する] チェックボックスを選択して、すべてのオブジェクトレベルイベントをログ記録できます。

> **Note**
>
> - ベストプラクティスとして、AWS CloudTrail データイベントバケットに対してライフサイクル設定を作成することをお勧めします。ログファイルを監査する必要があると考える期間が経過したらログファイルを定期的に削除するように、ライフサイクル設定を設定します。これにより、各クエリで Athena が分析するデータの量が減ります。詳細については、バケットに S3 ライフサイクル設定を設定する を参照してください。
> - ロギング形式の詳細については、AWS CloudTrail を使用した Amazon S3 API コールの口グ記録 を参照してください。
> - CloudTrail ログをクエリする方法の例については、AWS ビッグデータブログの記事 Analyze Security, Compliance, and Operational Activity Using AWS CloudTrail and Amazon Athena を参照してください。

コンソールを使用してバケット内のオブジェクトの口グ記録を有効にする

Amazon S3 コンソールを使用し、AWS CloudTrail 証跡を設定して、S3 バケット内のオブジェクトのデータイベントをログに記録できます。CloudTrail では、`GetObject`、`DeleteObject`、`PutObject` など、Amazon S3 オブジェクトレベルの API オペレーションの口グ記録がサポートされます。これらのイベントは、データイベントと呼ばれます。

デフォルトでは CloudTrail 証跡はデータイベントを記録しませんが、証跡を設定して、指定した S3 バケットのデータイベントを記録するか、AWS アカウントですべての Amazon S3 バケットのデータイベントを記録するようにできます。詳細については、AWS CloudTrail を使用した Amazon S3 API コールの口グ記録 を参照してください。

CloudTrail では、CloudTrail イベント履歴にデータイベントが設定されません。さらに、すべてのバケットレベルのアクションが CloudTrail イベント履歴に入力されるわけではありません。CloudTrail のログ記録によって追跡される Amazon S3 バケットレベルの API アクションの詳細については、「CloudTrail ログ記録によって追跡される Amazon S3 バケットレベルのアクション」を参照してください。CloudTrail ログのクエリ方法の詳細については、Amazon CloudWatch Logs のフィルタパターンと Amazon Athena を使用した CloudTrail ログのクエリに関する AWS ナレッジセンターの記事を参照してください。

S3 バケットのデータイベントをログに記録するように証跡を設定する場合、AWS CloudTrail コンソールまたは Amazon S3 コンソールのいずれかを使用できます。AWS アカウント内のすべての Amazon S3 バケットのデータイベントを記録するように証跡を設定する場合は、CloudTrail コンソールを使用する方が簡単です。CloudTrail コンソールを使用して S3 データイベントを記録するように証跡を設定する方法については、AWS CloudTrail ユーザーガイドのデータイベントを参照してください。

> **Important**
>
> 追加の変更がイベントデータに適用されます。詳細については、AWS CloudTrail 料金表を参照してください。

以下の手順では、Amazon S3 コンソールを使用して、CloudTrail の証跡で S3 バケットのデータイベントの記録を設定する方法を示します。

S3 汎用バケットまたは S3 ディレクトリバケットでオブジェクトの CloudTrail データイベントの記録を有効にするには

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. [バケット名] リストで、バケットの名前を選択します。
3. [プロパティ] を選択します。
4. AWS CloudTrailデータイベントで、CloudTrail の設定を選択します。

   新しい CloudTrail の証跡を作成するか、既存の証跡を再利用して、証跡に記録するように Amazon S3 データイベントを設定できます。CloudTrail コンソールで証跡を作成する方法については、AWS CloudTrail ユーザーガイドのコンソールで証跡を作成および更新するを参照してください。CloudTrail コンソールで Amazon S3 データイベントロギングを設定する方法につい

ては、AWS CloudTrail ユーザーガイドの Amazon S3 オブジェクトのデータイベントをログに記録するを参照してください。

> **Note**
>
> S3 バケットのデータイベントをログに記録するための証跡の設定に CloudTrail コンソールまたは Amazon S3 コンソールを使用する場合、そのバケットに対してオブジェクトレベルのロギングが有効化されていることが Amazon S3 コンソールに表示されます。

S3 バケットでオブジェクトの CloudTrail データイベントの記録を無効にするには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/cloudtrail/で CloudTrail コンソールを開きます。
2. 左のナビゲーションペインで、[証跡] を選択します。
3. バケットのイベントを記録するために作成した証跡の名前を選択します。
4. 証跡の詳細ページで、右上隅にある [ロギングを停止] を選択します。
5. 表示されたダイアログボックスで [ロギングを停止] を選択します。

S3 バケットを作成するときにオブジェクトレベルのログ記録を有効にする方法の詳細については、汎用バケットの作成 を参照してください。

S3 バケットを使用した CloudTrail ログ記録の詳細については、以下のトピックを参照してください。

- S3 汎用バケットのプロパティの表示
- AWS CloudTrail を使用した Amazon S3 API コールのログ記録
- AWS CloudTrail ユーザーガイドの CloudTrail ログファイルの操作

CloudTrail を使用した Amazon S3 リクエストの識別

Amazon S3 では、AWS CloudTrail イベントログを使用してリクエストを識別することができます。AWS CloudTrail は、Amazon S3 リクエストを識別する上で推奨される方法ですが、Amazon S3 サーバーアクセスログを使用している場合は、the section called “S3 リクエストの識別” を参照してください。

トピック

- CloudTrail ログで Amazon S3 に対して行われたリクエストを特定する
- CloudTrail を使用した Amazon S3 Signature Version 2 リクエストの識別
- CloudTrail を使用した S3 オブジェクトへのアクセスの識別

CloudTrail ログで Amazon S3 に対して行われたリクエストを特定する

バケットにイベントを送信するために CloudTrail をセットアップした後、Amazon S3 コンソールで送信先のバケットにオブジェクトが送信されるのを確認できるようになります。これらは次の形式になっています。

`s3://amzn-s3-demo-bucket1/AWSLogs/111122223333/CloudTrail/Region/yyyy/mm/dd`

CloudTrail により口グ記録されたイベントは、S3 バケットにある圧縮された gzipped JSON オブジェクトに保存されます。リクエストを効率的に見つけるには、Amazon Athena などのサービスを利用して CloudTrail ログにインデックスを作成し、クエリします。

CloudTrail と Athena の詳細については、「Amazon Athena ユーザーガイド」の「パーティション射影を使用した Athena での AWS CloudTrail ログ用のテーブルの作成」を参照してください。

CloudTrail を使用した Amazon S3 Signature Version 2 リクエストの識別

CloudTrail イベントログを使用して、Amazon S3 でリクエストに署名するために使用された API 署名バージョンを特定できます。署名バージョン 2 のサポートがオフになる (廃止される) ため、この機能は重要です。その後、Amazon S3 は署名バージョン 2 を使用するリクエストを受け入れず、すべてのリクエストに Signature Version 4 署名を使用する必要があります。

CloudTrail を使用して、署名バージョン 2 の署名を使用しているワークフローがあるかどうかを確認することを強くお勧めします。業務に影響が出ないように、Signature Version 4 を使用してライブラリとコードをアップグレードし、修正します。

詳細については、AWS re:Post の「お知らせ: Amazon S3 用の AWS CloudTrail は、セキュリティ監査を強化するための新しいフィールドを追加します」を参照してください。

> **Note**
>
> Amazon S3 の CloudTrail イベントには、キー名である「`additionalEventData`」のリクエスト詳細に署名バージョンが含まれます。Amazon S3 にあるオブジェクトに対する `GET`、`PUT`、`DELETE` などのリクエストで Signature Version を見つけるには、CloudTrail

データイベントを有効にする必要があります。(デフォルトでは、この機能はオフになっています。)

Signature Version 2 リクエストを識別する方法として、AWS CloudTrail が推奨されます。Amazon S3 のサーバーアクセスログを使用している場合は、「Amazon S3 アクセスログを使用した Signature Version 2 リクエストの識別」を参照してください。

トピック

- Amazon S3 署名バージョン 2 リクエストを識別する Athena クエリの例
- 署名バージョン 2 データのパーティション化

Amazon S3 署名バージョン 2 リクエストを識別する Athena クエリの例

Example — Signature Version 2 のイベントをすべて選択し、**EventTime**、**S3_Action**、**Request_Parameters**、**Region**、**SourceIP**、**UserAgent** のみを印刷する

以下の Athena クエリで、*s3_cloudtrail_events_db.cloudtrail_table* を Athena の詳細と置き換え、必要に応じて上限を引き上げるか削除します。

```
SELECT EventTime, EventName as S3_Action, requestParameters as Request_Parameters,
 awsregion as AWS_Region, sourceipaddress as Source_IP, useragent as User_Agent
FROM s3_cloudtrail_events_db.cloudtrail_table
WHERE eventsource='s3.amazonaws.com'
AND json_extract_scalar(additionalEventData, '$.SignatureVersion')='SigV2'
LIMIT 10;
```

Example – 署名バージョン 2 トラフィックを送信しているすべてのリクエスタを選択します。

```
SELECT useridentity.arn, Count(requestid) as RequestCount
FROM s3_cloudtrail_events_db.cloudtrail_table
WHERE eventsource='s3.amazonaws.com'
    and json_extract_scalar(additionalEventData, '$.SignatureVersion')='SigV2'
Group by useridentity.arn
```

署名バージョン 2 データのパーティション化

クエリするデータが大量にある場合、パーティション化されたテーブルを作成することにより Athena のコストを削減しランタイムを短縮できます。

それには、次のようなパーティションがある新しいテーブルを作成します。

```
CREATE EXTERNAL TABLE s3_cloudtrail_events_db.cloudtrail_table_partitioned(
     eventversion STRING,
     userIdentity STRUCT<
         type:STRING,
         principalid:STRING,
         arn:STRING,
         accountid:STRING,
         invokedby:STRING,
         accesskeyid:STRING,
         userName:STRING,
      sessioncontext:STRUCT<
                 attributes:STRUCT<
                 mfaauthenticated:STRING,
                 creationdate:STRING>,
                 sessionIssuer:STRUCT<
                 type:STRING,
                 principalId:STRING,
                 arn:STRING,
                 accountId:STRING,
                 userName:STRING>
             >
          >,
     eventTime STRING,
     eventSource STRING,
     eventName STRING,
     awsRegion STRING,
     sourceIpAddress STRING,
     userAgent STRING,
     errorCode STRING,
     errorMessage STRING,
     requestParameters STRING,
     responseElements STRING,
     additionalEventData STRING,
     requestId STRING,
     eventId STRING,
     resources ARRAY<STRUCT<ARN:STRING,accountId: STRING,type:STRING>>,
```

```
        eventType STRING,
        apiVersion STRING,
        readOnly STRING,
        recipientAccountId STRING,
        serviceEventDetails STRING,
        sharedEventID STRING,
        vpcEndpointId STRING
    )
    PARTITIONED BY (region string, year string, month string, day string)
    ROW FORMAT SERDE 'org.apache.hadoop.hive.ql.io.orc.OrcSerde'
    STORED AS INPUTFORMAT 'org.apache.hadoop.hive.ql.io.SymlinkTextInputFormat'
    OUTPUTFORMAT 'org.apache.hadoop.hive.ql.io.HiveIgnoreKeyTextOutputFormat'
    LOCATION 's3://amzn-s3-demo-bucket1/AWSLogs/111122223333/';
```

その後で個々にパーティションを作成します。作成していない日付から結果を取得することはできません。

```
ALTER TABLE s3_cloudtrail_events_db.cloudtrail_table_partitioned ADD
    PARTITION (region= 'us-east-1', year= '2019', month= '02', day= '19') LOCATION
 's3://amzn-s3-demo-bucket1/AWSLogs/111122223333/CloudTrail/us-east-1/2019/02/19/'
    PARTITION (region= 'us-west-1', year= '2019', month= '02', day= '19') LOCATION
 's3://amzn-s3-demo-bucket1/AWSLogs/111122223333/CloudTrail/us-west-1/2019/02/19/'
    PARTITION (region= 'us-west-2', year= '2019', month= '02', day= '19') LOCATION
 's3://amzn-s3-demo-bucket1/AWSLogs/111122223333/CloudTrail/us-west-2/2019/02/19/'
    PARTITION (region= 'ap-southeast-1', year= '2019', month= '02', day= '19') LOCATION
 's3://amzn-s3-demo-bucket1/AWSLogs/111122223333/CloudTrail/ap-southeast-1/2019/02/19/'
    PARTITION (region= 'ap-southeast-2', year= '2019', month= '02', day= '19') LOCATION
 's3://amzn-s3-demo-bucket1/AWSLogs/111122223333/CloudTrail/ap-southeast-2/2019/02/19/'
    PARTITION (region= 'ap-northeast-1', year= '2019', month= '02', day= '19') LOCATION
 's3://amzn-s3-demo-bucket1/AWSLogs/111122223333/CloudTrail/ap-northeast-1/2019/02/19/'
    PARTITION (region= 'eu-west-1', year= '2019', month= '02', day= '19') LOCATION
 's3://amzn-s3-demo-bucket1/AWSLogs/111122223333/CloudTrail/eu-west-1/2019/02/19/'
    PARTITION (region= 'sa-east-1', year= '2019', month= '02', day= '19') LOCATION
 's3://amzn-s3-demo-bucket1/AWSLogs/111122223333/CloudTrail/sa-east-1/2019/02/19/';
```

これらのパーティションに基づいてリクエストを実行でき、バケット全体を読み込む必要はありません。

```
SELECT useridentity.arn,
```

```
Count(requestid) AS RequestCount
FROM s3_cloudtrail_events_db.cloudtrail_table_partitioned
WHERE eventsource='s3.amazonaws.com'
AND json_extract_scalar(additionalEventData, '$.SignatureVersion')='SigV2'
AND region='us-east-1'
AND year='2019'
AND month='02'
AND day='19'
Group by useridentity.arn
```

CloudTrail を使用した S3 オブジェクトへのアクセスの識別

AWS CloudTrail イベントログを使用して、GetObject、DeleteObject、PutObject などのデータイベントに対する Amazon S3 オブジェクトアクセスリクエストを識別し、それらのリクエストに関する追加情報を確認できます。

以下の例は、AWS CloudTrail イベントログから Amazon S3 のすべての PUT オブジェクトリクエストを取得する方法を示しています。

トピック

- Amazon S3 オブジェクトアクセスリクエストを識別する Athena クエリの例

Amazon S3 オブジェクトアクセスリクエストを識別する Athena クエリの例

以下の Athena クエリの例で、*s3_cloudtrail_events_db.cloudtrail_table* を Athena の詳細と置き換え、必要に応じてデータ範囲を変更します。

Example — **PUT** オブジェクトアクセス要求のあるイベントをすべて選択し、**EventTime**、**EventSource**、**SourceIP**、**UserAgent**、**BucketName**、**object**、**UserARN** のみ印刷する

```
SELECT
  eventTime,
  eventName,
  eventSource,
  sourceIpAddress,
  userAgent,
  json_extract_scalar(requestParameters, '$.bucketName') as bucketName,
  json_extract_scalar(requestParameters, '$.key') as object,
  userIdentity.arn as userArn
```

```
FROM
  s3_cloudtrail_events_db.cloudtrail_table
WHERE
  eventName = 'PutObject'
  AND eventTime BETWEEN '2019-07-05T00:00:00Z' and '2019-07-06T00:00:00Z'
```

Example — **GET** オブジェクトアクセス要求のあるイベントをすべて選択し、**EventTime**、**EventSource**、**SourceIP**、**UserAgent**、**BucketName**、**object**、**UserARN** のみ印刷する

```
SELECT
  eventTime,
  eventName,
  eventSource,
  sourceIpAddress,
  userAgent,
  json_extract_scalar(requestParameters, '$.bucketName') as bucketName,
  json_extract_scalar(requestParameters, '$.key') as object,
  userIdentity.arn as userArn
FROM
  s3_cloudtrail_events_db.cloudtrail_table
WHERE
  eventName = 'GetObject'
  AND eventTime BETWEEN '2019-07-05T00:00:00Z' and '2019-07-06T00:00:00Z'
```

Example — 特定の期間にバケットに対して行われた匿名のリクエストイベントをすべて選択し、**EventTime**、**EventName**、**EventSource**、**SourceIP**、**UserAgent**、**BucketName**、**UserARN**、**Ac** のみ印刷する

```
SELECT
  eventTime,
  eventName,
  eventSource,
  sourceIpAddress,
  userAgent,
  json_extract_scalar(requestParameters, '$.bucketName') as bucketName,
  userIdentity.arn as userArn,
  userIdentity.accountId
FROM
  s3_cloudtrail_events_db.cloudtrail_table
WHERE
```

```
  userIdentity.accountId = 'anonymous'
  AND eventTime BETWEEN '2019-07-05T00:00:00Z' and '2019-07-06T00:00:00Z'
```

Example — 承認に ACL が必要なリクエストをすべて特定する

次の Amazon Athena のクエリの例は、承認のためにアクセスコントロールリスト (ACL) が必要な S3 バケットへのすべてのリクエストを特定する方法を示しています。リクエストに承認用の ACL が必要な場合、additionalEventData の aclRequired の値は Yes です。ACL が不要な場合は、aclRequired は存在しません。この情報を使用して、これらの ACL 権限を適切なバケットポリシーに移行できます。これらのバケットポリシーを作成したら、これらのバケットの ACL を無効にできます。ACL の無効化の詳細については、「ACL を無効にする前提条件。」を参照してください。

```
SELECT
  eventTime,
  eventName,
  eventSource,
  sourceIpAddress,
  userAgent,
  userIdentity.arn as userArn,
  json_extract_scalar(requestParameters, '$.bucketName') as bucketName,
  json_extract_scalar(requestParameters, '$.key') as object,
  json_extract_scalar(additionalEventData, '$.aclRequired') as aclRequired
FROM
  s3_cloudtrail_events_db.cloudtrail_table
WHERE
  json_extract_scalar(additionalEventData, '$.aclRequired') = 'Yes'
  AND eventTime BETWEEN '2022-05-10T00:00:00Z' and '2022-08-10T00:00:00Z'
```

Note

- このクエリの例は、セキュリティのモニタリングにも役立つ場合があります。予期しないまたは不正な IP アドレスやリクエスタからの PutObject または GetObject コールの結果を確認し、バケットへの匿名リクエストを特定できます。
- このクエリでは、ログ記録が有効になった時間以降の情報のみ取得されます。

Amazon S3 のサーバーアクセスログを使用している場合は、Amazon S3 アクセスログを使用したオブジェクトアクセスリクエストの識別 を参照してください。

サーバーアクセスログによるリクエストのログ記録

サーバーアクセスのログには、バケットに対するリクエストの詳細が記録されます。サーバーアクセスのログは、多くのアプリケーションに役立ちます。例えば、アクセスのログ情報は、セキュリティやアクセスの監査に役立ちます。この情報は、顧客基盤の把握や Amazon S3 の請求の理解にもつながります。

> **Note**
>
> サーバーアクセスログには、2019 年 3 月 20 日以降に開設されたリージョンで発生するリージョン違いによるリダイレクトエラーに関する情報は記録されません。リージョン違いによるリダイレクトエラーは、オブジェクトまたはバケットに対するリクエストがそのバケットがあるリージョン以外で行われた場合に発生します。

ログ配信を有効にするにはどうすればよいですか?

ログ配信を有効にするには、次の基本的な手順を実行します。詳細については、「Amazon S3 サーバーアクセスログを有効にします。」を参照してください。

1. 送信先バケット (別名ターゲットバケット) の名前を指定します。このバケットは、Amazon S3 がアクセスログをオブジェクトとして保存する場所です。ソースと送信先バケットの両方が同じ AWS リージョン にあり、同じアカウントが所有している必要があります。送信先バケットには S3 オブジェクトロックのデフォルト保持期間設定を指定できません。また、送信先バケットでは [リクエスタ支払い] を有効にできません。

   ログの保存先のバケットとして、ソースバケットと同じリージョンにあるユーザー所有のバケットを指定できます。これにはソースバケット自体も含まれます。ただし、ログを管理しやすくするため、アクセスログは別のバケットに保存することをお勧めします。

   ソースバケットと送信先バケットが同じである場合、バケットに書き込まれるログに関する追加のログが作成されます。ストレージの請求額がいくらか増える可能性があるため、この方法はお勧めしていません。また、ログに関する追加のログのために、必要なログを見つけにくくなります。

   アクセス ログをソースバケットに保存する場合は、すべてのログオブジェクトキーに対して送信先プレフィックス (別名ターゲットプレフィックス) を指定することをお勧めします。プレフィックスを指定すると、すべてのログオブジェクト名が共通の文字列で始まるため、ログオブジェクトを識別しやすくなります。

2. (オプション) Amazon S3 のすべてのログオブジェクトのキーにプレフィックスを割り当てます。送信先プレフィクス (別名ターゲットプレフィックス) を使用すると、ログオブジェクトを識別しやすくなります。例えば、プレフィックスの値として `logs/` を指定すると、Amazon S3 で作成する各ログオブジェクトのキーの先頭に `logs/` というプレフィックスが付けられます。

```
logs/2013-11-01-21-32-16-E568B2907131C0C0
```

プレフィックス値 `logs` を指定すると、ログオブジェクトは次のように表示されます。

```
logs2013-11-01-21-32-16-E568B2907131C0C0
```

プレフィックス は、複数のバケットログが同じ送信先バケットにログを記録する場合にもソースバケットの識別に役立ちます。

キープレフィックスは、ログを削除する際にも役に立ちます。例えば、特定のキープレフィックスを使用して、Amazon S3 のライフサイクル設定ルールを指定することができます。詳細については、「Amazon S3 ログファイルの削除」を参照してください。

3. (オプション) 生成されたログをその他のユーザーが利用するために、アクセス許可を設定します。デフォルトでは、バケット所有者のみにログオブジェクトへのフルアクセスが許可されます。(サーバーアクセスログが保存されている) 送信先バケットが S3 オブジェクト所有権のバケット所有者強制設定を使用してアクセスコントロールリスト (ACL) を無効化する場合、ACL を使用する送信先権限のアクセス許可を付与することはできません。ただし、送信先バケットのバケットポリシーを更新して、その他のユーザーにアクセスを付与することはできます。詳細については、「Amazon S3 用 Identity and Access Management」および「ログ配信許可」を参照してください。

4. (オプション) ログファイルのログオブジェクトキー形式を設定します。ログオブジェクトキーの形式 (別名ターゲットオブジェクトキー形式) には 2 つのオプションがあります。

   - 日付ベース以外のパーティション分割 – これはオリジナルのログオブジェクトキーの形式です。この形式を選択すると、ログファイルのキー形式は次のとおりになります。

     ```
     [DestinationPrefix][YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]
     ```

     例えば、`logs/` をプレフィックスとして指定すると、ログオブジェクトには次のような名前が付けられます。

     ```
     logs/2013-11-01-21-32-16-E568B2907131C0C0
     ```

- 日付ベースのパーティション分割 – 日付ベースのパーティショニングを選択した場合、ログ形式で使用される日付ソースとして、ログファイルのイベント時間または配信時間を選択できます。この形式を使用すると、ログのクエリが簡単になります。

  日付ベースのパーティション分割を選択すると、ログファイルのキー形式は次のとおりになります。

  ```
  [DestinationPrefix][SourceAccountId]/[SourceRegion]/[SourceBucket]/[YYYY]/[MM]/
  [DD]/[YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]
  ```

  例えば、logs/ をターゲットプレフィックスとして指定すると、ログオブジェクトには次のような名前が付けられます。

  ```
  logs/123456789012/us-west-2/amzn-s3-demo-source-
  bucket/2023/03/01/2023-03-01-21-32-16-E568B2907131C0C0
  ```

  配信時間配信の場合、ログファイル名の時刻はログファイルの配信時間に対応します。

  イベント時間配信の場合、年、月、日はイベントが発生した日に対応し、時、分、秒はキーで 00 に設定されます。このようなログファイルに配信されるログは、特定の日のみを対象とします。

AWS Command Line Interface (AWS CLI)、AWS SDK、または Amazon S3 REST API を使用してログを設定する場合は、TargetObjectKeyFormat を使用してログオブジェクトのキー形式を指定します。日付ベース以外のパーティション分割を指定するには、SimplePrefix を使用します。日付ベースのパーティション分割を指定するには、PartitionedPrefix を使用します。PartitionedPrefix を使用する場合は、PartitionDateSource で EventTime または DeliveryTime を指定します。

SimplePrefix の場合、ログファイルキー形式は、次のとおりです。

```
[TargetPrefix][YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]
```

イベント時刻または配信時刻の PartitionedPrefix の場合、ログファイルのキー形式は次のとおりになります。

```
[TargetPrefix][SourceAccountId]/[SourceRegion]/[SourceBucket]/[YYYY]/[MM]/[DD]/
[YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]
```

ログオブジェクトのキーフォーマット

Amazon S3 では、送信先バケットにログオブジェクトをアップロードする際に、次のオブジェクトキー形式を使用します。

- 日付ベース以外のパーティション分割 – これはオリジナルのログオブジェクトキーの形式です。この形式を選択すると、ログファイルのキー形式は次のとおりになります。

  ```
  [DestinationPrefix][YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]
  ```

- 日付ベースのパーティション分割 – 日付ベースのパーティショニングを選択した場合、ログ形式で使用される日付ソースとして、ログファイルのイベント時間または配信時間を選択できます。この形式を使用すると、ログのクエリが簡単になります。

  日付ベースのパーティション分割を選択すると、ログファイルのキー形式は次のとおりになります。

  ```
  [DestinationPrefix][SourceAccountId]/[SourceRegion]/[SourceBucket]/[YYYY]/[MM]/[DD]/
  [YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]
  ```

ログオブジェクトキーでは、YYYY、MM、DD、hh、mm、ss は、ログファイルを配信した年、月、日、時、分、秒をそれぞれ表す数字になります。これらの日付と時刻は協定世界時 (UTC) です。

ある時点で配信されたログファイルには、その時点より前に書き込まれたレコードが含まれます。特定の期間のすべてのログレコードが配信されたかどうかを知る方法はありません。

キーの UniqueString コンポーネントは、ファイルの上書きを防止するためのものです。意味はないため、ログ処理ソフトウェアでは無視されます。

ログを配信する方法

Amazon S3 は定期的にアクセスログレコードを収集し、レコードをまとめてログファイルを作成し、そのログファイルを、ログオブジェクトとして送信先バケットにアップロードします。複数のソースバケットでログ記録の配信先が同じ送信先バケットである場合、これらのすべてのソースバ

ケットのアクセスログが送信先バケットに配信されます。ただし、各ログオブジェクトは、ソースバケット別にアクセスログレコードをレポートします。

Amazon S3 は特別なログ配信アカウントを使用してサーバーアクセスログを書き込みます。このような書き込みは、通常のアクセスコントロールの制約に従います。送信先バケットのバケットポリシーを更新して、アクセスログ配信用のログ記録サービスプリンシパル (`logging.s3.amazonaws.com`) へのアクセス権を付与することをお勧めします。バケットのアクセスコントロールリスト (ACL) を介して S3 ログ配信グループにアクセスログ配信のためのアクセスを付与することもできます。ただし、バケット ACL を使用して S3 ログ配信グループへのアクセスを許可することはお勧めしません。

サーバーアクセスのログ記録を有効にして、バケットポリシーを通じてアクセスログ配信のアクセスを許可する場合は、送信先バケットのバケットポリシーを更新して、`s3:PutObject` にログ記録サービスプリンシパルのアクセスを許可します。Amazon S3 コンソールを使用してサーバーアクセスのログ記録を有効にすると、コンソールは、送信先バケットのバケットポリシーを自動的に更新して、ログ記録サービスのプリンシパルにこれらの許可を付与します。サーバーアクセスのログ配信許可の付与の詳細については、ログ配信許可 を参照してください。

> **Note**
>
> S3 は、VPC エンドポイントポリシーで拒否されている場合、または VPC ポリシーが評価される前にリクエストが失敗した場合、VPC エンドポイントリクエストの CloudTrail ログまたはサーバーアクセスログのリクエスタまたはバケット所有者への配信をサポートしません。

S3 オブジェクト所有権のバケット所有者強制設定

送信先バケットが、オブジェクト所有権のバケット所有者強制設定を使用している場合、ACL は無効になり、アクセス許可への影響はなくなります。送信先バケットのバケットポリシーを更新して、アクセスログ配信用のログ記録サービスプリンシパルへのアクセス権を付与する必要があります。オブジェクトの所有権の詳細については、「サーバーアクセスのログ記録用の S3 ログ配信グループへのアクセスを付与する」を参照してください。

ベストエフォート型のサーバーログ配信

サーバーアクセスログレコードの配信は、ベストエフォートベースで行われます。ログ記録用に適切にバケットを設定した場合、そのバケットへのほとんどのリクエストについてログレコードが配信されます。ほとんどのログレコードは、記録された時間から数時間以内に配信されますが、配信間隔は短くなる場合もあります。

サーバーログの完全性や適時性は保証されません。リクエストのログレコードが、リクエストが実際に処理されてからかなり後に配信されたり、配信すらされないこともあり得ます。ログレコードが重複している場合さえあります。サーバーログの目的は、バケットに対するトラフィックの特性を理解することです。ログレコードが損失したり、ログレコードが重複したりすることはまれであるとはいえ、すべてのリクエストが完全に報告されるとは限りません。

サーバーログ作成機能はベストエフォート型であるため、使用状況レポートには、サーバーログに記録されていないアクセスリクエストが含まれる場合があります。このような使用状況レポートは、AWS Billing and Cost Management コンソールの [Cost & usage reports] で確認できます。

バケットのログ記録ステータスの変更が有効になるまでには時間がかかる

バケットのログ記録ステータスの変更がログファイルの配信に反映されるまでには時間がかかります。例えば、バケットのログを有効にする場合、その後数時間に行われるリクエストは記録される場合もあれば、されない場合もあります。ログ記録の送信先バケットをバケット A からバケット B に変更すると、その後 1 時間は一部のログがバケット A に引き続き配信されたり、新しいターゲットバケット B に配信されたりします。いずれにしても、最終的に新しい設定が有効になるため、ユーザー側の操作は一切必要ありません。

ログ記録とログファイルの詳細については、次のセクションを参照してください。

トピック

- Amazon S3 サーバーアクセスログを有効にします。
- Amazon S3 サーバーアクセスログの形式
- Amazon S3 ログファイルの削除
- Amazon S3 アクセスログを使用したリクエストの識別
- サーバーのアクセスログ記録のトラブルシューティング

Amazon S3 サーバーアクセスログを有効にします。

サーバーアクセスのログには、Amazon S3 バケットに対するリクエストの詳細が記録されます。サーバーアクセスのログは、多くのアプリケーションに役立ちます。例えば、アクセスのログ情報は、セキュリティやアクセスの監査に役立ちます。この情報は、顧客基盤の把握や Amazon S3 の請求の理解にもつながります。

デフォルトでは、Amazon S3 によってサーバーアクセスログは収集されません。ログ記録を有効にすると、Amazon S3 は、ソースバケットのアクセスログを選択された送信先バケット(ターゲットバ

ケット) に配信します。ソースと送信先バケットの両方が同じ AWS リージョン にあり、同じ AWS アカウント が所有している必要があります。

アクセスログのレコードには、バケットに対するリクエストの詳細が取り込まれます。この情報には、リクエストタイプ、リクエストで指定したリソース、リクエストを処理した日時などが含まれます。ログ記録の基本の詳細については、サーバーアクセスログによるリクエストのログ記録 を参照してください。

Important

- Amazon S3 バケットに対してサーバーアクセスログ記録を有効にしても追加料金はかかりません。ただし、システムが配信するいずれのログファイルの格納に対しても通常の料金がかかります (ログはいつでも削除できます)。ログファイルの配信にデータ転送料金はかかりません。ただし、ログファイルへのアクセスには通常のデータ転送料金がかかります。
- 送信先バケットでサーバーアクセスのログ記録が有効になっているべきではありません。ログの保存先のバケットとして、ソースバケットと同じリージョンにあるユーザー所有のバケットを指定できます。これにはソースバケット自体も含まれます。ただし、ソースバケットにログを配信すると、ログの無限ループが発生するため、お勧めしません。ログを管理しやすくするため、アクセスログは別のバケットに保存することをお勧めします。詳細については、ログ配信を有効にするにはどうすればよいですか?を参照してください。
- S3 オブジェクトロックが有効になっている S3 バケットは、サーバーアクセスログの送信先バケットとして使用できません。送信先バケットにはデフォルト保持期間設定を指定できません。
- 送信先バケットでは [リクエスタ支払い] を有効にすることはできません。
- 送信先バケットでデフォルトのバケット暗号化を使用できるのは、256 ビットの高度暗号化標準 (AES-256) を使用する Amazon S3 マネージドキー S3 によるサーバー側の暗号化を使用する場合のみです。AWS Key Management Service (AWS KMS) キーを使用したデフォルトのサーバー側の暗号化 (SSE-KMS) はサポートされていません。

Amazon S3 コンソール、Amazon S3 API、AWS Command Line Interface (AWS CLI)、AWS SDK を使用して、サーバーアクセスのログ記録を有効または無効にできます。

ログ配信許可

Amazon S3 は特別なログ配信アカウントを使用してサーバーアクセスログを書き込みます。このような書き込みは、通常のアクセスコントロールの制約に従います。アクセスログを配信するには、ロギングサービスプリンシパル (logging.s3.amazonaws.com) に送信先バケットへのアクセス権を付与する必要があります。

Amazon S3 にログ配信アクセス許可を付与するには、送信先バケットの S3 オブジェクト所有権の設定に応じて、バケットポリシーまたはバケットアクセスコントロールリスト (ACL) を使用できます。ただし、ACL の代わりにバケットポリシーを使用することをお勧めします。

S3 オブジェクト所有権のバケット所有者強制設定

送信先バケットが、オブジェクト所有権のバケット所有者強制設定を使用している場合、ACL は無効になり、アクセス許可への影響はなくなります。この場合は、送信先バケットのバケットポリシーを更新して、アクセスログ配信用のログ記録サービスプリンシパルへのアクセス権を付与する必要があります。S3 ログ配信グループへのアクセスを許可すると、バケット ACL を更新できません。また、送信先権限 (別名ターゲット権限) PutBucketLogging を設定に含めることもできません。

アクセスログ配信用の既存のバケット ACL をバケットポリシーに移行する方法については、「サーバーアクセスのログ記録用の S3 ログ配信グループへのアクセスを付与する」を参照してください。オブジェクトの所有権の詳細については、「オブジェクトの所有権の制御とバケットの ACL の無効化。」を参照してください。新しいバケットを作成するとき、ACL はデフォルトでは無効になっています。

バケットポリシーを使用したアクセスの付与

送信先バケットでバケットポリシーを使用してアクセスを許可するには、バケットポリシーを更新して、ログ記録サービスプリンシパルに s3:PutObject アクセス許可を付与します。Amazon S3 コンソールを使用してサーバーアクセスのログ記録を有効にすると、コンソールは、送信先バケットのバケットポリシーを自動的に更新して、ログ記録サービスプリンシパルにこのようなアクセス許可を付与します。プログラムでサーバーアクセスのログ記録を有効にする場合、送信先バケットのバケットポリシーを手動で更新して、アクセスログ配信用のログ記録サービスプリンシパルへのアクセス権を付与する必要があります。

ログ記録サービスプリンシパルのリソースへのアクセスを制限するバケットポリシーの例については、「the section called “バケットポリシーを使用して、ロギングサービスプリンシパルに許可を付与”」を参照してください。

バケット ACL を使用したアクセスの付与

代わりに、バケット ACL を使用して、アクセスログ配信のアクセスを許可できます。S3 ログ配信グループに WRITE と READ_ACP の許可を付与する許可エントリーをバケット ACL に追加します。ただし、バケット ACL を使用して S3 ログ配信グループへのアクセスを許可することはお勧めしません。詳細については、「オブジェクトの所有権の制御とバケットの ACL の無効化。」を参照してください。アクセスログ配信用の既存のバケット ACL をバケットポリシーに移行する方法については、「サーバーアクセスのログ記録用の S3 ログ配信グループへのアクセスを付与する」を参照してください。ログ記録サービスプリンシパルのリソースへのアクセスを制限する ACL の例については、「the section called “バケット ACL を使用して、ログ配信グループにアクセス許可を付与します。”」を参照してください。

バケットポリシーを使用して、ロギングサービスプリンシパルに許可を付与

このバケットポリシーの例は、s3:PutObject アクセス許可を口グ記録サービスプリンシパル (logging.s3.amazonaws.com) に付与します。このバケットポリシーを実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。次のポリシーでは、*amzn-s3-demo-destination-bucket* はサーバーアクセスログが配信される送信先バケットで、*amzn-s3-demo-source-bucket* は送信元バケットです。*EXAMPLE-LOGGING-PREFIX* は、ログオブジェクトに使用するオプションの送信先のプレフィックス (別称 ターゲットプレフィックス) です。*SOURCE-ACCOUNT-ID* は、AWS アカウント ソースバケットを所有するグループです。

> **Note**
>
> バケットポリシーに Deny ステートメントがある場合は、それらが Amazon S3 からのアクセスログの配信を防止していないことを確認します。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3ServerAccessLogsPolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "logging.s3.amazonaws.com"
            },
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/EXAMPLE-LOGGING-PREFIX*",
```

```
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:s3:::amzn-s3-demo-source-bucket"
                },
                "StringEquals": {
                    "aws:SourceAccount": "SOURCE-ACCOUNT-ID"
                }
            }
        }
    ]
}
```

バケット ACL を使用して、ログ配信グループにアクセス許可を付与します。

> **Note**
>
> セキュリティ上のベストプラクティスとして、Amazon S3 はすべての新しいバケットのアクセスコントロールリスト (ACL) をデフォルトで無効にします。Amazon S3 コンソールでの ACL アクセス権限の詳細については、「ACL の設定」を参照してください。

バケット ACL を使用してログ配信グループに許可を付与することはできますが、この方法はお勧めしません。ただし、送信先バケットが、オブジェクト所有権のバケット所有者強制設定を使用している場合、バケット ACL や オブジェクト ACL を設定することはできません。また、送信先権限 (別名ターゲット権限) PutBucketLogging を設定に含めることもできません。代わりに、ロギングサービスプリンシパル (logging.s3.amazonaws.com) にアクセス許可を付与するために、バケットポリシーを使用する必要があります。詳細については、「ログ配信許可」を参照してください。

バケット ACL では、ログ配信グループは次の URL で示されます。

```
http://acs.amazonaws.com/groups/s3/LogDelivery
```

WRITE と READ_ACP (ACL 読み取り) アクセス許可を付与するには、送信先バケット ACL に次の権限を追加します。

```
<Grant>
    <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  xsi:type="Group">
        <URI>http://acs.amazonaws.com/groups/s3/LogDelivery</URI>
    </Grantee>
    <Permission>WRITE</Permission>
```

```
</Grant>
<Grant>
    <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  xsi:type="Group">
        <URI>http://acs.amazonaws.com/groups/s3/LogDelivery</URI>
    </Grantee>
    <Permission>READ_ACP</Permission>
</Grant>
```

プログラムを使用して ACL アクセス権限を追加する例については、ACL の設定 を参照してください。

> **Important**
>
> バケットで AWS CloudFormation 使用して Amazon S3 サーバーアクセスロギングを有効にし、ACL を使用して S3 ログ配信グループへのアクセスを許可する場合は、CloudFormation テンプレートにも「`AccessControl": "LogDeliveryWrite"`」を追加する必要があります。このようなアクセス許可はバケット ACL を作成することによってのみ付与できます。CloudFormation ではバケットのカスタム ACL を作成できないため、これを実行することは重要です。CloudFormation で使用できるのは既定 ACL のみです。

サーバーアクセスのログ記録を有効にします

Amazon S3 コンソール、Amazon S3 REST API、AWS SDK、AWS CLI を使用してサーバーアクセスのログ記録を有効にするには、次の手順を実行します。

S3 コンソールの使用

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 左のナビゲーションペインで、[汎用バケット] を選択します。
3. バケットリストで、サーバーアクセスログを有効にするバケットの名前を選択します。
4. [プロパティ] を選択します。
5. [サーバーアクセスのログ記録] で、[編集] を選択します。
6. [Server access logging] (サーバーアクセスのログ記録) で[Enable] (有効) を選択します。
7. [送信先バケット] の下で、バケットとオプションのプレフィックスを指定します。プレフィックスを指定する場合は、ログを検出しやすくするために、プレフィックスの後にスラッシュ (/) を付けることをお勧めします。

> **Note**
>
> スラッシュ (/) を使用したプレフィックスを指定すると、ログオブジェクトが見つけやすくなります。例えば、プレフィックスの値として `logs/` を指定すると、次のとおり Amazon S3 で作成する各ログオブジェクトのキーの先頭に `logs/` というプレフィックスが付けられます。
>
> ```
> logs/2013-11-01-21-32-16-E568B2907131C0C0
> ```
>
> プレフィックス値 `logs` を指定すると、ログオブジェクトは次のように表示されます。
>
> ```
> logs2013-11-01-21-32-16-E568B2907131C0C0
> ```

8. [ログオブジェクトキーの形式] の下で、次を設定します。

   - 日付ベース以外のパーティション分割を選択するには、[DestinationPrefix][YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString] を選択します。
   - 日付ベースでパーティション分割するには、[DestinationPrefix][SourceAccountId]/[SourceRegion]/[SourceBucket]/[YYYY]/[MM]/[DD]/[YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString] を選択してから、[S3 イベント時刻] または [ログファイルの配信時刻] を選択します。

9. [Save changes] (変更の保存) をクリックします。

   バケットでサーバーアクセスのログ記録を有効にすると、コンソールはソースバケットでのログ記録を有効にして、送信先バケットのバケットポリシーを更新し、ログ記録サービスプリンシパル (`logging.s3.amazonaws.com`) に `s3:PutObject` アクセス許可を付与します。バケットポリシーの詳細については、バケットポリシーを使用して、ロギングサービスプリンシパルに許可を付与 を参照してください。

   ログは 送信先バケットで確認できます。サーバーアクセスのログ記録を有効にすると、ログがターゲットバケットに配信されるまでに数時間かかることがあります。ログ配信の方法と間隔の詳細については、ログを配信する方法 を参照してください。

詳細については、「S3 汎用バケットのプロパティの表示」を参照してください。

REST API の使用

ログ記録を有効にするには、PutBucketLogging リクエストを送信してソースバケットにログ記録の設定を追加します。リクエストでは、送信先バケット (別名 ターゲットバケット) を指定し、必要に応じて、すべてのログオブジェクトキーに使用するプレフィックスを指定します。

送信先バケットとして *amzn-s3-demo-destination-bucket* を、プレフィックスとして *logs/* を指定する例は次のとおりです。

```
<BucketLoggingStatus xmlns="http://doc.s3.amazonaws.com/2006-03-01">
  <LoggingEnabled>
    <TargetBucket>amzn-s3-demo-destination-bucket</TargetBucket>
    <TargetPrefix>logs/</TargetPrefix>
  </LoggingEnabled>
</BucketLoggingStatus>
```

送信先バケットとして *amzn-s3-demo-destination-bucket* を、プレフィックスとして *logs/* を、ログオブジェクトキーの形式として EventTime を指定する例は次のとおりです。

```
<BucketLoggingStatus xmlns="http://doc.s3.amazonaws.com/2006-03-01">
  <LoggingEnabled>
    <TargetBucket>amzn-s3-demo-destination-bucket</TargetBucket>
    <TargetPrefix>logs/</TargetPrefix>
    <TargetObjectKeyFormat>
      <PartitionedPrefix>
         <PartitionDateSource>EventTime</PartitionDateSource>
      </PartitionedPrefix>
  </TargetObjectKeyFormat>
  </LoggingEnabled>
</BucketLoggingStatus>
```

ログオブジェクトはログ配信アカウントが作成および所有し、バケット所有者はログオブジェクトへの完全な許可を付与されます。必要に応じて、送信先権限 (別名ターゲット権限) をして、他のユーザーがログにアクセスできるようにアクセス許可を付与できます。詳細については、「PutBucketLogging」を参照してください。

> **Note**
>
> 送信先バケットが、オブジェクト所有権のバケット所有者強制設定を使用している場合、送信先権限を使用してその他のユーザーにアクセス許可を付与することはできません。その他

のユーザーにアクセス許可を付与するには、送信先バケットのバケットポリシーを更新します。詳細については、「ログ配信許可」を参照してください。

バケットのログ記録設定を取得するには、GetBucketLogging API オペレーションを使用します。

ログ記録設定を削除するには、PutBucketLogging リクエストで空の BucketLoggingStatus を指定して送信します。

```
<BucketLoggingStatus xmlns="http://doc.s3.amazonaws.com/2006-03-01">
</BucketLoggingStatus>
```

バケットでログ記録を有効にするには、Amazon S3 API または AWS SDK ラッパーライブラリを使用できます。

AWS SDK の使用

バケットでログ記録を有効化する例は次のとおりです。ソースバケットと送信先 (ターゲット) バケットの 2 つのバケットを作成する必要があります。 この例ではまず、送信先バケットのバケット ACL を更新します。この例では、まず送信先バケットにログを書き込むために必要なアクセス許可をログ配信グループに付与して、次にソースバケットでのログ記録を有効にしています。

このような例では、オブジェクト所有権のバケット所有者の強制設定を使用する送信先バケットでは機能しません。

送信先 (ターゲット) バケットが、オブジェクト所有権にバケット所有者の強制設定を使用している場合、バケット ACL や オブジェクト ACL を設定することはできません。PutBucketLogging 設定には、送信先 (ターゲット) 権限を含めることもできません。ロギングサービスプリンシパル (logging.s3.amazonaws.com) に許可を付与するために、バケットポリシーを使用する必要があります。詳細については、「ログ配信許可」を参照してください。

.NET

SDK for .NET

> **Note**
>
> GitHub には、その他のリソースもあります。AWS コード例リポジトリ で全く同じ例を見つけて、設定と実行の方法を確認してください。

```
    using System;
    using System.IO;
    using System.Threading.Tasks;
    using Amazon.S3;
    using Amazon.S3.Model;
    using Microsoft.Extensions.Configuration;

    /// <summary>
    /// This example shows how to enable logging on an Amazon Simple Storage
    /// Service (Amazon S3) bucket. You need to have two Amazon S3 buckets for
    /// this example. The first is the bucket for which you wish to enable
    /// logging, and the second is the location where you want to store the
    /// logs.
    /// </summary>
    public class ServerAccessLogging
    {
        private static IConfiguration _configuration = null!;

        public static async Task Main()
        {
            LoadConfig();

            string bucketName = _configuration["BucketName"];
            string logBucketName = _configuration["LogBucketName"];
            string logObjectKeyPrefix = _configuration["LogObjectKeyPrefix"];
            string accountId = _configuration["AccountId"];

            // If the AWS Region defined for your default user is different
            // from the Region where your Amazon S3 bucket is located,
            // pass the Region name to the Amazon S3 client object's constructor.
            // For example: RegionEndpoint.USWest2 or RegionEndpoint.USEast2.
            IAmazonS3 client = new AmazonS3Client();

            try
            {
                // Update bucket policy for target bucket to allow delivery of
logs to it.
                await SetBucketPolicyToAllowLogDelivery(
                    client,
                    bucketName,
                    logBucketName,
                    logObjectKeyPrefix,
                    accountId);
```

```
                // Enable logging on the source bucket.
                await EnableLoggingAsync(
                    client,
                    bucketName,
                    logBucketName,
                    logObjectKeyPrefix);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine($"Error: {e.Message}");
            }
        }

        /// <summary>
        /// This method grants appropriate permissions for logging to the
        /// Amazon S3 bucket where the logs will be stored.
        /// </summary>
        /// <param name="client">The initialized Amazon S3 client which will be
used
        /// to apply the bucket policy.</param>
        /// <param name="sourceBucketName">The name of the source bucket.</param>
        /// <param name="logBucketName">The name of the bucket where logging
        /// information will be stored.</param>
        /// <param name="logPrefix">The logging prefix where the logs should be
delivered.</param>
        /// <param name="accountId">The account id of the account where the
source bucket exists.</param>
        /// <returns>Async task.</returns>
        public static async Task SetBucketPolicyToAllowLogDelivery(
            IAmazonS3 client,
            string sourceBucketName,
            string logBucketName,
            string logPrefix,
            string accountId)
        {
            var resourceArn = @"""arn:aws:s3:::" + logBucketName + "/" +
logPrefix + @"*""";

            var newPolicy = @"{
                                ""Statement"":[{
                                ""Sid"": ""S3ServerAccessLogsPolicy"",
                                ""Effect"": ""Allow"",
```

```
                                ""Principal"": { ""Service"":
 ""logging.s3.amazonaws.com"" },
                                ""Action"": [""s3:PutObject""],
                                ""Resource"": [" + resourceArn + @"],
                                ""Condition"": {
                                ""ArnLike"": { ""aws:SourceArn"":
 ""arn:aws:s3:::" + sourceBucketName + @""" },
                                ""StringEquals"": { ""aws:SourceAccount"": """ +
 accountId + @""" }
                                        }
                                    }]
                                }";
            Console.WriteLine($"The policy to apply to bucket {logBucketName} to
 enable logging:");
            Console.WriteLine(newPolicy);

            PutBucketPolicyRequest putRequest = new PutBucketPolicyRequest
            {
                BucketName = logBucketName,
                Policy = newPolicy,
            };
            await client.PutBucketPolicyAsync(putRequest);
            Console.WriteLine("Policy applied.");
        }

        /// <summary>
        /// This method enables logging for an Amazon S3 bucket. Logs will be
 stored
        /// in the bucket you selected for logging. Selected prefix
        /// will be prepended to each log object.
        /// </summary>
        /// <param name="client">The initialized Amazon S3 client which will be
 used
        /// to configure and apply logging to the selected Amazon S3 bucket.</
param>
        /// <param name="bucketName">The name of the Amazon S3 bucket for which
 you
        /// wish to enable logging.</param>
        /// <param name="logBucketName">The name of the Amazon S3 bucket where
 logging
        /// information will be stored.</param>
        /// <param name="logObjectKeyPrefix">The prefix to prepend to each
        /// object key.</param>
        /// <returns>Async task.</returns>
```

```
        public static async Task EnableLoggingAsync(
            IAmazonS3 client,
            string bucketName,
            string logBucketName,
            string logObjectKeyPrefix)
        {
            Console.WriteLine($"Enabling logging for bucket {bucketName}.");
            var loggingConfig = new S3BucketLoggingConfig
            {
                TargetBucketName = logBucketName,
                TargetPrefix = logObjectKeyPrefix,
            };

            var putBucketLoggingRequest = new PutBucketLoggingRequest
            {
                BucketName = bucketName,
                LoggingConfig = loggingConfig,
            };
            await client.PutBucketLoggingAsync(putBucketLoggingRequest);
            Console.WriteLine($"Logging enabled.");
        }

        /// <summary>
        /// Loads configuration from settings files.
        /// </summary>
        public static void LoadConfig()
        {
            _configuration = new ConfigurationBuilder()
                .SetBasePath(Directory.GetCurrentDirectory())
                .AddJsonFile("settings.json") // Load settings from .json file.
                .AddJsonFile("settings.local.json", true) // Optionally, load
local settings.
                .Build();
        }
    }
```

- API の詳細については、「AWS SDK for .NET API リファレンス」の「PutBucketLogging」を参照してください。

Java

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.services.s3.model.BucketLoggingStatus;
import software.amazon.awssdk.services.s3.model.LoggingEnabled;
import software.amazon.awssdk.services.s3.model.PartitionedPrefix;
import software.amazon.awssdk.services.s3.model.PutBucketLoggingRequest;
import software.amazon.awssdk.services.s3.model.TargetObjectKeyFormat;

// Class to set a bucket policy on a target S3 bucket and enable server access
 logging on a source S3 bucket.
public class ServerAccessLogging {
    private static S3Client s3Client;

    public static void main(String[] args) {
        String sourceBucketName = "SOURCE-BUCKET";
        String targetBucketName = "TARGET-BUCKET";
        String sourceAccountId = "123456789012";
        String targetPrefix = "logs/";

        // Create S3 Client.
        s3Client = S3Client.builder().
                region(Region.US_EAST_2)
                .build();

        // Set a bucket policy on the target S3 bucket to enable server access
 logging by granting the
        // logging.s3.amazonaws.com principal permission to use the PutObject
 operation.
        ServerAccessLogging serverAccessLogging = new ServerAccessLogging();
        serverAccessLogging.setTargetBucketPolicy(sourceAccountId, sourceBucketName,
 targetBucketName);

        // Enable server access logging on the source S3 bucket.
        serverAccessLogging.enableServerAccessLogging(sourceBucketName,
 targetBucketName,
                targetPrefix);

    }

    // Function to set a bucket policy on the target S3 bucket to enable server
 access logging by granting the
    // logging.s3.amazonaws.com principal permission to use the PutObject operation.
```

```
    public void setTargetBucketPolicy(String sourceAccountId, String
 sourceBucketName, String targetBucketName) {
        String policy = "{\n" +
                "    \"Version\": \"2012-10-17\",\n" +
                "    \"Statement\": [\n" +
                "        {\n" +
                "            \"Sid\": \"S3ServerAccessLogsPolicy\",\n" +
                "            \"Effect\": \"Allow\",\n" +
                "            \"Principal\": {\"Service\": \"logging.s3.amazonaws.com
\"},\n" +
                "            \"Action\": [\n" +
                "                \"s3:PutObject\"\n" +
                "            ],\n" +
                "            \"Resource\": \"arn:aws:s3:::" + targetBucketName + "/*
\",\n" +
                "            \"Condition\": {\n" +
                "                \"ArnLike\": {\n" +
                "                    \"aws:SourceArn\": \"arn:aws:s3:::" +
 sourceBucketName + "\"\n" +
                "                },\n" +
                "                \"StringEquals\": {\n" +
                "                    \"aws:SourceAccount\": \"" + sourceAccountId +
 "\"\n" +
                "                }\n" +
                "            }\n" +
                "        }\n" +
                "    ]\n" +
                "}";
        s3Client.putBucketPolicy(b -> b.bucket(targetBucketName).policy(policy));
    }

    // Function to enable server access logging on the source S3 bucket.
    public void enableServerAccessLogging(String sourceBucketName, String
 targetBucketName,
            String targetPrefix) {
        TargetObjectKeyFormat targetObjectKeyFormat =
 TargetObjectKeyFormat.builder()

 .partitionedPrefix(PartitionedPrefix.builder().partitionDateSource("EventTime").build())
                .build();
        LoggingEnabled loggingEnabled = LoggingEnabled.builder()
                .targetBucket(targetBucketName)
                .targetPrefix(targetPrefix)
                .targetObjectKeyFormat(targetObjectKeyFormat)
```

```
                .build();
        BucketLoggingStatus bucketLoggingStatus = BucketLoggingStatus.builder()
                .loggingEnabled(loggingEnabled)
                .build();
        s3Client.putBucketLogging(PutBucketLoggingRequest.builder()
                .bucket(sourceBucketName)
                .bucketLoggingStatus(bucketLoggingStatus)
                .build());
    }

}
```

AWS CLI を使用する場合

S3 バケットがある各 AWS リージョンに専用のログ記録バケットを作成することをお勧めします。その後、Amazon S3 アクセスログをその S3 バケットに配信します。詳細と例については、「AWS CLI リファレンス」の「put-bucket-logging」を参照してください。

送信先 (ターゲット) バケットが、オブジェクト所有権にバケット所有者の強制設定を使用している場合、バケット ACL や オブジェクト ACL を設定することはできません。PutBucketLogging 設定には、送信先 (ターゲット) 権限を含めることもできません。ロギングサービスプリンシパル (logging.s3.amazonaws.com) に許可を付与するために、バケットポリシーを使用する必要があります。詳細については、ログ配信許可 を参照してください。

Example – 2 つのリージョンの 5 つのバケットでアクセスログを有効にする

この例では、次の 5 つのバケットがあります。

- *amzn-s3-demo-source-bucket*-us-east-1
- *amzn-s3-demo-source-bucket1*-us-east-1
- *amzn-s3-demo-source-bucket2*-us-east-1
- *amzn-s3-demo-bucket1*-us-west-2
- *amzn-s3-demo-bucket2*-us-west-2

> **Note**
>
> 次の手順の最後のステップでは、ログ記録バケットを作成して、そのバケットでサーバーアクセスのログ記録を有効にするために使用できる bash スクリプトの例が示されています。

このようなスクリプトを使用するには、次の手順で説明されるとおり、policy.json と logging.json ファイルを作成する必要があります。

1. 米国西部 (オレゴン) リージョンと米国東部 (バージニア北部) リージョンに 2 つのログ記録先バケットを作成して、次の名前を付けます。
   - *amzn-s3-demo-destination-bucket*-logs-us-east-1
   - *amzn-s3-demo-destination-bucket1*-logs-us-west-2
2. このステップの後半では、次のとおりサーバーアクセスのログ記録を有効にします。
   - *amzn-s3-demo-source-bucket*-us-east-1 は、プレフィックス *amzn-s3-demo-destination-bucket*-logs-us-east-1 を使用して S3 バケット *amzn-s3-demo-source-bucket*-us-east-1 にログを記録します。
   - *amzn-s3-demo-source-bucket1*-us-east-1 は、プレフィックス *amzn-s3-demo-destination-bucket*-logs-us-east-1 を使用して S3 バケット *amzn-s3-demo-source-bucket1*-us-east-1 にログを記録します。
   - *amzn-s3-demo-source-bucket2*-us-east-1 は、プレフィックス *amzn-s3-demo-destination-bucket*-logs-us-east-1 を使用して S3 バケット *amzn-s3-demo-source-bucket2*-us-east-1 にログを記録します。
   - *amzn-s3-demo-bucket1*-us-west-2 は、プレフィックス *amzn-s3-demo-destination-bucket1*-logs-us-west-2 を使用して S3 バケット *amzn-s3-demo-bucket1*-us-west-2 にログを記録します。
   - *amzn-s3-demo-bucket2*-us-west-2 は、プレフィックス *amzn-s3-demo-destination-bucket1*-logs-us-west-2 を使用して S3 バケット *amzn-s3-demo-bucket2*-us-west-2 にログを記録します。
3. バケット ACL またはバケットポリシーを使用して、サーバーアクセスのログ記録の配信の許可を付与します。
   - バケットポリシーの更新 (推奨) – ロギングサービスプリンシパルにアクセス許可を付与するには、次の put-bucket-policy コマンドを使用します。*amzn-s3-demo-destination-bucket*-logs を、宛先のバケットの名前に置き換えます。

```
aws s3api put-bucket-policy --bucket amzn-s3-demo-destination-bucket-logs --
policy file://policy.json
```

Policy.json は、次のバケットポリシーを含む現在のフォルダ内の JSON ドキュメントです。このバケットポリシーを実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。次のポリシーでは、*amzn-s3-demo-destination-bucket-logs* はサーバーアクセスログが配信される送信先バケットであり、*amzn-s3-demo-source-bucket* はソースバケットです。*SOURCE-ACCOUNT-ID* は、ソースバケットを所有する AWS アカウント です。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3ServerAccessLogsPolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "logging.s3.amazonaws.com"
            },
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket-logs/*",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:s3:::amzn-s3-demo-source-bucket"
                },
                "StringEquals": {
                    "aws:SourceAccount": "SOURCE-ACCOUNT-ID"
                }
            }
        }
    ]
}
```

- バケット ACL の更新 – S3 ログ配信グループに許可を付与するには、次の put-bucket-acl コマンドを使用します。*amzn-s3-demo-destination-bucket-logs* は、送信先 (ターゲット) バケット名前に置き換えます。

```
aws s3api put-bucket-acl --bucket amzn-s3-demo-destination-bucket-logs  --
grant-write URI=http://acs.amazonaws.com/groups/s3/LogDelivery --grant-read-acp
 URI=http://acs.amazonaws.com/groups/s3/LogDelivery
```

4. 次に、(次の 3 つの例のうちのいずれかに基づいた) ログ記録設定を含む logging.json ファイルを作成します。logging.json ファイルを作成したら、次の put-bucket-logging コマンドを使用してログ記録設定を適用できます。*amzn-s3-demo-destination-bucket-logs* は、送信先 (ターゲット) バケット名前に置き換えます。

```
aws s3api put-bucket-logging --bucket amzn-s3-demo-destination-bucket-logs --
bucket-logging-status file://logging.json
```

> **Note**
>
> この put-bucket-logging コマンドを使用して各送信先バケットにログ記録設定を適用する代わりに、次のステップで提供される bash スクリプトのいずれかを使用できます。このようなスクリプトを使用するには、次の手順のとおり、policy.json と logging.json ファイルを作成する必要があります。

logging.json ファイルは、ログ記録設定を含む現在のフォルダ内の JSON ドキュメントです。送信先バケットがオブジェクト所有権に対してバケット所有者の強制設定を使用している場合、ログ記録設定に送信先 (ターゲット) の権限を含めることはできません。詳細については、「ログ配信許可」を参照してください。

Example — 送信先 (ターゲット) 権限なしの **logging.json**

次の例の logging.json ファイルには、送信先 (ターゲット) 権限が含まれていません。そのため、オブジェクト所有権のバケット所有者の強制設定を使用する送信先 (ターゲット) バケットにこの設定を適用できます。

```
{
    "LoggingEnabled": {
        "TargetBucket": "amzn-s3-demo-destination-bucket-logs",
        "TargetPrefix": "amzn-s3-demo-destination-bucket/"
     }
```

```
  }
```

Example — 送信先 (ターゲット) 権限のある **logging.json**

次の例の logging.json ファイルには、送信先 (ターゲット) 権限が含まれています。

送信先バケットが、オブジェクト所有権のバケット所有者の強制設定を使用している場合、PutBucketLogging 設定に送信先 (ターゲット) 権限を含めることはできません。詳細については、「ログ配信許可」を参照してください。

```
{
    "LoggingEnabled": {
        "TargetBucket": "amzn-s3-demo-destination-bucket-logs",
        "TargetPrefix": "amzn-s3-demo-destination-bucket/",
        "TargetGrants": [
             {
                "Grantee": {
                    "Type": "AmazonCustomerByEmail",
                    "EmailAddress": "user@example.com"
                 },
                "Permission": "FULL_CONTROL"
             }
         ]
     }
 }
```

被付与者の値

アクセス権を割り当てる先のユーザー (被付与者) は、以下の方法で (リクエスト要素を使用して) 指定できます。

- ユーザーの ID の場合:

```
{
  "Grantee": {
    "Type": "CanonicalUser",
    "ID": "ID",
    "DisplayName": "GranteesEmail"
  }
```

```
}
```

DisplayName はオプションであり、リクエストでは無視されます。

- E メールアドレスの場合:

```
{
  "Grantee": {
    "Type": "AmazonCustomerByEmail",
    "EmailAddress": "username@example.com"
  }
}
```

被付与者は CanonicalUser に解決され、GetObjectAcl リクエストへの応答で、CanonicalUser として表示されます。

> **Note**
>
> E メールアドレスを使用した被付与者の指定は、一部の AWS リージョンでのみサポートされています。詳細については、「Amazon S3 API リファレンス」の「Grantee」を参照してください。

- URI の場合:

```
{
  "Grantee": {
    "Type": "Group",
    "URI": "http://acs.amazonaws.com/groups/global/AuthenticatedUsers"
  }
}
```

Example – ログオブジェクトキーを S3 イベント時刻に設定した **logging.json**

次の logging.json ファイルは、ログオブジェクトキーの形式を S3 イベント時刻に変更します。暗号化キーの使用の詳細については、「the section called “ログ配信を有効にするにはどうすればよいですか?”」を参照してください。

```
{
  "LoggingEnabled": {
```

```
        "TargetBucket": "amzn-s3-demo-destination-bucket-logs",
        "TargetPrefix": "amzn-s3-demo-destination-bucket/",
        "TargetObjectKeyFormat": {
            "PartitionedPrefix": {
                "PartitionDateSource": "EventTime"
            }
         }
    }
}
```

5. アカウントのすべてのバケットに対するアクセスログを追加するには、次の bash スクリプトのいずれかを使用します。*amzn-s3-demo-destination-bucket-logs* は、送信先 (ターゲット) バケットの名前に置き換え、*us-west-2* はバケットが配置されているリージョンの名前に置き換えます。

> **Note**
>
> これはすべてのバケットが同じリージョンにある場合にのみ機能します。複数のリージョンにバケットがある場合は、スクリプトを調整する必要があります。

Example — バケットポリシーによるアクセスを許可し、アカウントのバケットのロギングを追加します

```
loggingBucket='amzn-s3-demo-destination-bucket-logs'
region='us-west-2'


# Create the logging bucket.
aws s3 mb s3://$loggingBucket --region $region

aws s3api put-bucket-policy --bucket $loggingBucket --policy file://policy.json

# List the buckets in this account.
buckets="$(aws s3 ls | awk '{print $3}')"

# Put a bucket logging configuration on each bucket.
for bucket in $buckets
    do
      # This if statement excludes the logging bucket.
```

```
        if [ "$bucket" == "$loggingBucket" ] ; then
            continue;
        fi
        printf '{
          "LoggingEnabled": {
            "TargetBucket": "%s",
            "TargetPrefix": "%s/"
        }
      }' "$loggingBucket" "$bucket"  > logging.json
      aws s3api put-bucket-logging --bucket $bucket --bucket-logging-status file://
logging.json
      echo "$bucket done"
  done

  rm logging.json

  echo "Complete"
```

Example — バケット ACL でアクセス権を付与し、アカウントのバケットのロギングを追加します

```
  loggingBucket='amzn-s3-demo-destination-bucket-logs'
  region='us-west-2'


  # Create the logging bucket.
  aws s3 mb s3://$loggingBucket --region $region

  aws s3api put-bucket-acl --bucket $loggingBucket --grant-write URI=http://
acs.amazonaws.com/groups/s3/LogDelivery --grant-read-acp URI=http://
acs.amazonaws.com/groups/s3/LogDelivery

  # List the buckets in this account.
  buckets="$(aws s3 ls | awk '{print $3}')"

  # Put a bucket logging configuration on each bucket.
  for bucket in $buckets
      do
        # This if statement excludes the logging bucket.
        if [ "$bucket" == "$loggingBucket" ] ; then
            continue;
        fi
```

```
        printf '{
          "LoggingEnabled": {
            "TargetBucket": "%s",
            "TargetPrefix": "%s/"
          }
        }' "$loggingBucket" "$bucket"  > logging.json
        aws s3api put-bucket-logging --bucket $bucket --bucket-logging-status file://
logging.json
        echo "$bucket done"
  done

  rm logging.json

  echo "Complete"
```

サーバーアクセスログ設定の検証

サーバーアクセスロギングを有効にしたら、以下の手順を実行します。

- 送信先バケットにアクセスして、ログファイルが配信されていることを確認します。アクセスログが設定されると、Amazon S3 はすぐにリクエストのキャプチャと口グ記録を開始します。ただし、ログが送信先バケットに送られるまでに数時間かかる場合があります。詳細については、「the section called “バケットの口グ記録ステータスの変更が有効になるまでには時間がかかる”」および「the section called “ベストエフォート型のサーバーログ配信”」を参照してください。

  Amazon S3 リクエストメトリクスを使用し、これらのメトリックスに Amazon CloudWatch アラームを設定することで、口グ配信を自動的に検証することもできます。詳細については、「Amazon CloudWatch によるメトリクスのモニタリング」を参照してください。
- ログファイルのコンテンツを開いて読み取ることができることを確認します。

サーバアクセスロギングのトラブルシューティング情報については、サーバーのアクセスログ記録のトラブルシューティング を参照してください。

Amazon S3 サーバーアクセスログの形式

サーバーアクセスのログには、Amazon S3 バケットに対するリクエストの詳細が記録されます。サーバーアクセスログは次の目的で使用できます。

- セキュリティ監査とアクセス監査の実施

- 顧客ベースについて学ぶ
- Amazon S3 の請求書を理解する

このセクションでは、Amazon S3 サーバーアクセスログファイルの形式およびその他の詳細について説明します。

サーバーアクセスのログファイルは、一連のログレコードを改行で区切って構成します。各ログレコードは 1 個のリクエストを表し、各フィールドをスペースで区切って構成します。

次に示すのは、5 個のログレコードで構成されるログの例です。

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 amzn-s3-demo-bucket1 [06/Feb/2019:00:00:38 +0000] 192.0.2.3
 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be 3E57427F3EXAMPLE
 REST.GET.VERSIONING - "GET /amzn-s3-demo-bucket1?versioning HTTP/1.1" 200 - 113 - 7 -
 "-" "S3Console/0.4" - s9lzHYrFp76ZVxRcpX9+5cjAnEH2ROuNkd2BHfIa6UkFVdtjf5mKR3/eTPFvsiP/
XV/VLi31234= SigV4 ECDHE-RSA-AES128-GCM-SHA256 AuthHeader amzn-s3-demo-bucket1.s3.us-
west-1.amazonaws.com TLSV1.2 arn:aws:s3:us-west-1:123456789012:accesspoint/example-AP
 Yes
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 amzn-s3-demo-bucket1 [06/Feb/2019:00:00:38 +0000] 192.0.2.3
 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be 891CE47D2EXAMPLE
 REST.GET.LOGGING_STATUS - "GET /amzn-s3-demo-bucket1?logging HTTP/1.1" 200 -
 242 - 11 - "-" "S3Console/0.4" - 9vKBE6vMhrNiWHZmb2L0mXOcqPGzQOI5XLnCtZNPxev+Hf
+7tpT6sxDwDty4LHBUOZJG96N1234= SigV4 ECDHE-RSA-AES128-GCM-SHA256 AuthHeader amzn-s3-
demo-bucket1.s3.us-west-1.amazonaws.com TLSV1.2 - -
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 amzn-s3-demo-bucket1 [06/Feb/2019:00:00:38 +0000] 192.0.2.3
 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be A1206F460EXAMPLE
 REST.GET.BUCKETPOLICY - "GET /amzn-s3-demo-bucket1?policy HTTP/1.1" 404
 NoSuchBucketPolicy 297 - 38 - "-" "S3Console/0.4" - BNaBsXZQQDbssi6xMBdBU2sLt
+Yf5kZDmeBUP35sFoKa3sLLeMC78iwEIWxs99CRUrbS4n11234= SigV4 ECDHE-RSA-AES128-GCM-SHA256
 AuthHeader amzn-s3-demo-bucket1.s3.us-west-1.amazonaws.com TLSV1.2 - Yes
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 amzn-s3-demo-bucket1 [06/Feb/2019:00:01:00 +0000] 192.0.2.3
 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be 7B4A0FABBEXAMPLE
 REST.GET.VERSIONING - "GET /amzn-s3-demo-bucket1?versioning HTTP/1.1" 200 -
 113 - 33 - "-" "S3Console/0.4" - Ke1bUcazaN1jWuUlPJaxF64cQVpUEhoZKEG/hmy/gijN/
I1DeWqDfFvnpybfEseEME/u7ME1234= SigV4 ECDHE-RSA-AES128-GCM-SHA256 AuthHeader amzn-s3-
demo-bucket1.s3.us-west-1.amazonaws.com TLSV1.2 - -
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 amzn-s3-demo-bucket1 [06/Feb/2019:00:01:57 +0000] 192.0.2.3
```

```
 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 DD6CC733AEXAMPLE REST.PUT.OBJECT s3-dg.pdf "PUT /amzn-s3-demo-bucket1/
s3-dg.pdf HTTP/1.1" 200 - - 4406583 41754 28 "-" "S3Console/0.4" -
 10S62Zv81kBW7BB6SX4XJ48o6kpcl6LPwEoizZQQxJd5qDSCTLX0TgS37kYUBKQW3+bPdrg1234= SigV4
 ECDHE-RSA-AES128-SHA AuthHeader amzn-s3-demo-bucket1.s3.us-west-1.amazonaws.com
 TLSV1.2 - Yes
```

> **Note**
>
> 任意のフィールドを - に設定して、データが不明または使用不可であること、またはフィールドがこのリクエストに適用されなかったことを示すことができます。

トピック

- ログレコードフィールド
- コピーオペレーションの追加ログ記録
- カスタムアクセスログ情報
- 拡張可能なサーバーアクセスログの形式のプログラミングに関する考慮事項

ログレコードフィールド

次のリストは、ログレコードのフィールドについて説明しています。

Bucket Owner

ソースバケット所有者の正規ユーザー ID。正規ユーザー ID は、別の形式の AWS アカウント ID です。正規ユーザー ID の詳細については、AWS 全般のリファレンス の「AWS アカウント IDID」を参照してください。アカウントの正規ユーザー ID を検索する方法については、「AWS アカウントの正規ユーザー ID を検索する」を参照してください。

エントリ例

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

バケット

リクエストの処理ターゲットのバケットの名前。システムで受け取ったリクエストの形式に誤りがあり、バケットを特定できない場合、そのリクエストはサーバーアクセスログに表示されません。

エントリ例

```
amzn-s3-demo-bucket1
```

時間

リクエストが受信された時間。これらの日付と時刻は協定世界時 (UTC) です。strftime() terminology を使用した形式は次のようになります: [%d/%b/%Y:%H:%M:%S %z]

エントリ例

```
[06/Feb/2019:00:00:38 +0000]
```

リモート IP

リクエスタの表面上の IP アドレス。中間プロキシやファイアウォールにより、リクエストを作成したマシンの実際の IP アドレスが不明確になる場合があります。

エントリ例

```
192.0.2.3
```

リクエスタ

リクエスタの正規ユーザー ID。認証されていないリクエストの場合は - です。リクエスタが IAM ユーザーであった場合、このフィールドは、リクエスタの IAM ユーザー名と IAM ユーザーが属する AWS アカウントを返します。この識別子は、アクセスコントロールに使用されるものと同じです。

エントリ例

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

リクエスタが引き受けたロールを使用している場合、このフィールドは、引き受けた IAM ロールを返します。

エントリ例

```
arn:aws:sts::123456789012:assumed-role/roleName/test-role
```

リクエスト ID

各リクエストを一意に識別するために Amazon S3 で生成される文字列。

エントリ例

```
3E57427F33A59F07
```

オペレーション

ここに表示されているオペレーション
は、SOAP.*operation*、REST.*HTTP_method*.*resource_type*、WEBSITE.*HTTP_method*.*resourc*
または BATCH.DELETE.OBJECT、または S3 ライフサイクルとログ記録 の
S3.action.resource_type として宣言されます。

エントリ例

```
REST.PUT.OBJECT
```

キー

リクエストのキー (オブジェクト名) 部分。

エントリ例

```
/photos/2019/08/puppy.jpg
```

Request-URI

HTTP リクエストメッセージの Request-URI の部分。

エントリ例

```
"GET /amzn-s3-demo-bucket1/photos/2019/08/puppy.jpg?x-foo=bar HTTP/1.1"
```

HTTP ステータス

レスポンスの HTTP ステータスの数値。

エントリ例

```
200
```

エラーコード

Amazon S3 エラーレスポンス、またはエラーが発生しなかった場合は「-」。

エントリ例

```
NoSuchBucket
```

送信バイト数

送信されたレスポンスのバイト数 (HTTP プロトコルオーバーヘッドを除きます)。ゼロの場合は「-」。

エントリ例

```
2662992
```

オブジェクトのサイズ

該当するオブジェクトの合計サイズ。

エントリ例

```
3462992
```

合計時間

サーバーから見た、リクエストの転送中の時間数 (ミリ秒単位)。これは、リクエストが受信されてから、レスポンスの最終バイトが送信されるまでの時間を計測した値です。クライアント側での計測値は、ネットワーク遅延により長くなる場合があります。

エントリ例

```
70
```

Turn-Around Time

Amazon S3 でリクエストの処理に要した時間数 (ミリ秒単位)。これは、リクエストの最終バイトが受信されてから、レスポンスの先頭バイトが送信されるまでの時間を計測した値です。

エントリ例

```
10
```

Referer

HTTP Referer ヘッダーの値 (存在する場合)。一般に、HTTP ユーザーエージェント (ブラウザなど) は、このヘッダーをリクエスト作成時のリンクページや埋め込みページの URL に設定します。

エントリ例

```
"http://www.example.com/webservices"
```

User-Agent

HTTP User-Agent ヘッダーの値

エントリ例

```
"curl/7.15.1"
```

バージョン ID

リクエストのバージョン ID、または オペレーションが versionId パラメータを取らない場合は「-」。

エントリ例

```
3HL4kqtJvjVBH40Nrjfkd
```

ホスト ID

x-amz-id-2 または Amazon S3 拡張リクエスト ID。

エントリ例

```
s9lzHYrFp76ZVxRcpX9+5cjAnEH2ROuNkd2BHfIa6UkFVdtjf5mKR3/eTPFvsiP/XV/VLi31234=
```

署名バージョン

署名バージョン SigV2 か SigV4 (リクエストの認証に使用)、または - (認証されていないリクエストの場合)。

エントリ例

```
SigV2
```

暗号スイート

HTTPS リクエストまたは HTTP の - に対してネゴシエートされた Transport Layer Security (TLS) 暗号。

エントリ例

```
ECDHE-RSA-AES128-GCM-SHA256
```

認証タイプ

使用されるリクエスト認証のタイプ。認証ヘッダーは AuthHeader、クエリ文字列 (署名付き URL) は QueryString、認証されていないリクエストには「-」。

エントリ例

```
AuthHeader
```

ホストヘッダー

Amazon S3 への接続に使用するエンドポイント。

エントリ例

```
s3.us-west-2.amazonaws.com
```

一部の古いリージョンでは、レガシーエンドポイントがサポートされています。これらのエンドポイントは、サーバーアクセスログまたは AWS CloudTrail ログに表示される場合があります。詳細については、「レガシーエンドポイント」を参照してください。Amazon S3 リージョンとエンドポイントの完全なリストについては、Amazon Web Services 全般のリファレンス の「Amazon S3 エンドポイントとクォータ」を参照してください。

TLS のバージョン

クライアントによってネゴシエートされた Transport Layer Security (TLS) バージョン。値は TLSv1.1、TLSv1.2、TLSv1.3、- のいずれかです (TLS を使用しなかった場合)。

エントリ例

```
TLSv1.2
```

アクセスポイント ARN

リクエストのアクセスポイントの Amazon リソースネーム (ARN) です。アクセスポイントの ARN の形式が不正、または使用されていない場合、このフィールドには「-」が含まれます。アクセスポイントの詳細については、「汎用バケットでの Amazon S3 アクセスポイントの使用」を参照してください。ARN の詳細については、「AWS リファレンスガイド」の「Amazon リソースネーム (ARN)」を参照してください。

エントリ例

```
arn:aws:s3:us-east-1:123456789012:accesspoint/example-AP
```

aclRequired

リクエストの承認のためにアクセスコントロールリスト (ACL) が必要かどうかを示す文字列。リクエストに承認用の ACL が必要な場合、文字列は「Yes」です。ACL が必要なかった場合、文字列は「-」です。ACL の詳細については、「アクセスコントロールリスト (ACL) の概要」を参照してください。aclRequired フィールドを使用して ACL を無効にする方法の詳細については、オブジェクトの所有権の制御とバケットの ACL の無効化。 を参照してください。

エントリ例

```
Yes
```

コピーオペレーションの追加ログ記録

コピーオペレーションには GET と PUT が含まれます。このため、コピーオペレーションの実行時には 2 つのログレコードが記録されます。前述のセクションでは、コピーオペレーションの PUT 部分に関連するフィールドを説明しています。次のリストでは、コピーオペレーションの GET 部分に関連するフィールドを説明します。

バケット所有者

コピーされたオブジェクトを格納するバケットの正規ユーザー ID。正規ユーザー ID は、別の形式の AWS アカウント ID です。正規ユーザー ID の詳細については、AWS 全般のリファレンスの「AWS アカウント IDID」を参照してください。アカウントの正規ユーザー ID を検索する方法については、「AWS アカウントの正規ユーザー ID を検索する」を参照してください。

エントリ例

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

バケット

コピー対象オブジェクトのオブジェクトを格納するバケットの名前。

エントリ例

```
amzn-s3-demo-bucket1
```

時間

リクエストが受信された時間。これらの日付と時刻は協定世界時 (UTC) です。strftime() terminology を使用した形式は次のようになります: [%d/%B/%Y:%H:%M:%S %z]

エントリ例

```
[06/Feb/2019:00:00:38 +0000]
```

リモート IP

リクエスタの表面上の IP アドレス。中間プロキシやファイアウォールにより、リクエストを作成したマシンの実際の IP アドレスが不明確になる場合があります。

エントリ例

```
192.0.2.3
```

リクエスタ

リクエスタの正規ユーザー ID。認証されていないリクエストの場合は - です。リクエスタが IAM ユーザーであった場合、このフィールドは、リクエスタの IAM ユーザー名と IAM ユーザーが属

する AWS アカウントのルートユーザーを返します。この識別子は、アクセスコントロールに使用されるものと同じです。

エントリ例

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

リクエスタが引き受けたロールを使用している場合、このフィールドは、引き受けた IAM ロールを返します。

エントリ例

```
arn:aws:sts::123456789012:assumed-role/roleName/test-role
```

リクエスト ID

各リクエストを一意に識別するために Amazon S3 で生成される文字列。

エントリ例

```
3E57427F33A59F07
```

操作

ここに表示されているオペレーション
は、SOAP.*operation*、REST.*HTTP_method*.*resource_type*、WEBSITE.*HTTP_method*.*resourc*
または BATCH.DELETE.OBJECT と表示されます。

エントリ例

```
REST.COPY.OBJECT_GET
```

キー

コピー対象オブジェクトのキー (オブジェクト名) 部分。オペレーションがキーパラメータを取らない場合は「-」。

エントリ例

```
/photos/2019/08/puppy.jpg
```

Request-URI

HTTP リクエストメッセージの Request-URI の部分。

エントリ例

```
"GET /amzn-s3-demo-bucket1/photos/2019/08/puppy.jpg?x-foo=bar"
```

HTTP ステータス

コピーオペレーションの GET 部分の HTTP ステータスの数値。

エントリ例

```
200
```

エラーコード

コピーオペレーションの GET 部分の Amazon S3 エラーレスポンス、またはエラーがない場合は「-」。

エントリ例

```
NoSuchBucket
```

送信バイト数

送信されたレスポンスのバイト数 (HTTP プロトコルオーバーヘッドを除く)。ゼロの場合は「-」。

エントリ例

```
2662992
```

オブジェクトのサイズ

該当するオブジェクトの合計サイズ。

エントリ例

```
3462992
```

合計時間

サーバーから見た、リクエストの転送中の時間数 (ミリ秒単位)。これは、リクエストが受信されてから、レスポンスの最終バイトが送信されるまでの時間を計測した値です。クライアント側での計測値は、ネットワーク遅延により長くなる場合があります。

エントリ例

```
70
```

Turn-Around Time

Amazon S3 でリクエストの処理に要した時間数 (ミリ秒単位)。これは、リクエストの最終バイトが受信されてから、レスポンスの先頭バイトが送信されるまでの時間を計測した値です。

エントリ例

```
10
```

Referer

HTTP `Referer` ヘッダーの値 (存在する場合)。一般に、HTTP ユーザーエージェント (ブラウザなど) は、このヘッダーをリクエスト作成時のリンクページや埋め込みページの URL に設定します。

エントリ例

```
"http://www.example.com/webservices"
```

User-Agent

HTTP `User-Agent` ヘッダーの値

エントリ例

```
"curl/7.15.1"
```

バージョン ID

コピー対象オブジェクトのバージョン ID、または `x-amz-copy-source` ヘッダーでコピー元の一部として `versionId` パラメータを指定しなかった場合は「-」。

エントリ例

```
3HL4kqtJvjVBH40Nrjfkd
```

ホスト ID

x-amz-id-2 または Amazon S3 拡張リクエスト ID。

エントリ例

```
s9lzHYrFp76ZVxRcpX9+5cjAnEH2ROuNkd2BHfIa6UkFVdtjf5mKR3/eTPFvsiP/XV/VLi31234=
```

署名バージョン

Signature Version、SigV2 か SigV4 (リクエストの認証に使用)、または - (認証されていないリクエストの場合)。

エントリ例

```
SigV4
```

暗号スイート

HTTPS リクエストまたは HTTP の - に対してネゴシエートされた Transport Layer Security (TLS) 暗号。

エントリ例

```
ECDHE-RSA-AES128-GCM-SHA256
```

認証タイプ

使用されるリクエスト認証のタイプ。認証ヘッダーは AuthHeader、クエリ文字列 (署名付き URL) は QueryString、認証されていないリクエストには「-」。

エントリ例

```
AuthHeader
```

ホストヘッダー

Amazon S3 への接続に使用するエンドポイント。

エントリ例

```
s3.us-west-2.amazonaws.com
```

一部の古いリージョンでは、レガシーエンドポイントがサポートされています。これらのエンドポイントは、サーバーアクセスログまたは AWS CloudTrail ログに表示される場合があります。詳細については、「レガシーエンドポイント」を参照してください。Amazon S3 リージョンとエンドポイントの完全なリストについては、Amazon Web Services 全般のリファレンス の「Amazon S3 エンドポイントとクォータ」を参照してください。

TLS のバージョン

クライアントによってネゴシエートされた Transport Layer Security (TLS) バージョン。値は TLSv1.1、TLSv1.2、TLSv1.3、- のいずれかです (TLS を使用しなかった場合)。

エントリ例

```
TLSv1.2
```

アクセスポイント ARN

リクエストのアクセスポイントの Amazon リソースネーム (ARN) です。アクセスポイントの ARN の形式が不正、または使用されていない場合、このフィールドには「-」が含まれます。アクセスポイントの詳細については、「汎用バケットでの Amazon S3 アクセスポイントの使用」を参照してください。ARN の詳細については、「AWS リファレンスガイド」の「Amazon リソースネーム (ARN)」を参照してください。

エントリ例

```
arn:aws:s3:us-east-1:123456789012:accesspoint/example-AP
```

aclRequired

リクエストの承認のためにアクセスコントロールリスト (ACL) が必要かどうかを示す文字列。リクエストに承認用の ACL が必要な場合、文字列は「Yes」です。ACL が必要なかった場合、文字列は「-」です。ACL の詳細については、「アクセスコントロールリスト (ACL) の概要」を参照してください。aclRequired フィールドを使用して ACL を無効にする方法の詳細については、オブジェクトの所有権の制御とバケットの ACL の無効化。 を参照してください。

エントリ例

```
Yes
```

カスタムアクセスログ情報

リクエストのアクセスログレコードに保存するカスタム情報を含めることができます。これを行うには、リクエストの URL にカスタムクエリ文字列パラメータを追加します。Amazon S3 では、「x-」で始まるクエリ文字列パラメータは無視されますが、これらのパラメータはログレコードの Request-URI フィールドの一部として、リクエストのアクセスログレコードに追加されます。

例えば、GET の "s3.amazonaws.com/amzn-s3-demo-bucket1/photos/2019/08/puppy.jpg?x-user=johndoe" リクエストは、"s3.amazonaws.com/amzn-s3-demo-bucket1/photos/2019/08/puppy.jpg" のリクエストと同じように動作します。ただし 、"x-user=johndoe" 文字列は関連付けられたログレコードの Request-URI フィールドに含まれている点が異なります。この機能は REST インターフェイスでのみ利用できます。

拡張可能なサーバーアクセスログの形式のプログラミングに関する考慮事項

場合によっては、新しいフィールドを各行末に追加することで、アクセスログレコードの形式を拡張することがあります。したがって、サーバーアクセスログを解析するコードは、理解できない可能性のある後続フィールドを処理するよう作成する必要があります。

Amazon S3 ログファイルの削除

Amazon S3 バケットでサーバーアクセスのログ記録が有効になっていると、時間の経過とともに多数のサーバーログオブジェクトが蓄積される場合があります。アクセスログは、作成後アプリケーションで必要な期間が過ぎたら、削除できます。Amazon S3 のライフサイクル設定でルールを指定しておくことで、このようなオブジェクトのライフサイクルが終了すると、自動的にオブジェクトを削除キューに入れることができます。

共有プレフィックスを使用して、S3 バケット内のオブジェクトのサブセットのライフサイクル設定を定義できます。サーバーアクセスのログ記録設定でプレフィックスを指定した場合は、そのプレフィックスが付いたログオブジェクトを削除するライフサイクル設定ルールを指定できます。

例えば、ログオブジェクトに logs/ というプレフィックスがあるとします。ライフサイクル設定ルールを指定して、指定した期間後に logs/ プレフィックスを持つバケット内のすべてのオブジェクトを削除できます。

ライフサイクル設定についての詳細は、オブジェクトのライフサイクルの管理 を参照してください。

サーバーアクセスログ記録の一般情報については、サーバーアクセスログによるリクエストのログ記録 を参照してください。

Amazon S3 アクセスログを使用したリクエストの識別

Amazon S3 アクセスログを使用して、Amazon S3 リクエストを識別できます。

> **Note**
>
> - Amazon S3 リクエストを識別するには、Amazon S3 アクセスログの代わりに AWS CloudTrail データイベントを使用することをお勧めします。CloudTrail データイベントは、設定が容易で、より多くの情報が含まれています。詳細については、「CloudTrail を使用した Amazon S3 リクエストの識別」を参照してください。
> - 取得したアクセスリクエスト数に応じて、ログの分析にリソースや時間がさらに必要になる場合があります。

トピック

- Amazon Athena を使用したリクエストのアクセスログのクエリ
- Amazon S3 アクセスログを使用した Signature Version 2 リクエストの識別
- Amazon S3 アクセスログを使用したオブジェクトアクセスリクエストの識別

Amazon Athena を使用したリクエストのアクセスログのクエリ

Amazon Athena を使って、Amazon S3 のアクセスログで、Amazon S3 リクエストを識別できます。

Amazon S3 は、サーバーのアクセスログを S3 バケット内のオブジェクトとして保存します。多くの場合、Amazon S3 のログを分析できるツールを使用する方が簡単です。Athena は S3 オブジェクトの分析をサポートしてしるため、Amazon S3 アクセスログに対してクエリを実行するのに使用できます。

Example

次の例は、Amazon Athena で Amazon S3 サーバーアクセスログをクエリする方法を示しています。次の例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

> **Note**
>
> Athena クエリで Amazon S3 のロケーションを指定するには、ログの送信先となるバケットの S3 URI を指定する必要があります。この URI には、次の形式でバケット名とプレフィックスを含める必要があります。s3://*amzn-s3-demo-bucket1-logs/prefix/*

1. https://console.aws.amazon.com/athena/ で Athena コンソールを開きます。
2. クエリエディタで、次のようなコマンドを実行します。*s3_access_logs_db* は、データベースにつける名前に置き換えます。

```
CREATE DATABASE s3_access_logs_db
```

> **Note**
>
> ベストプラクティスとして、データベースは、S3 バケットと同じ AWS リージョンで作成することをお勧めします。

3. クエリエディタで次のようなコマンドを実行して、ステップ 2 で作成したデータベースでテーブルスキーマを作成します。*s3_access_logs_db.mybucket_logs* は、テーブルにつける名前に置き換えます。STRING および BIGINT データ型の値はアクセスログのプロパティです。これらのプロパティは Athena でクエリできます。LOCATION の場合は、前述のように S3 バケットとプレフィックスパスを入力します。

   Date-based paritioning

```
CREATE EXTERNAL TABLE s3_access_logs_db.mybucket_logs(
 `bucketowner` STRING,
 `bucket_name` STRING,
 `requestdatetime` STRING,
 `remoteip` STRING,
 `requester` STRING,
 `requestid` STRING,
 `operation` STRING,
 `key` STRING,
 `request_uri` STRING,
 `httpstatus` STRING,
 `errorcode` STRING,
 `bytessent` BIGINT,
```

```
 `objectsize` BIGINT,
 `totaltime` STRING,
 `turnaroundtime` STRING,
 `referrer` STRING,
 `useragent` STRING,
 `versionid` STRING,
 `hostid` STRING,
 `sigv` STRING,
 `ciphersuite` STRING,
 `authtype` STRING,
 `endpoint` STRING,
 `tlsversion` STRING,
 `accesspointarn` STRING,
 `aclrequired` STRING)
 PARTITIONED BY (
   `timestamp` string)
ROW FORMAT SERDE
 'org.apache.hadoop.hive.serde2.RegexSerDe'
WITH SERDEPROPERTIES (
 'input.regex'='([^ ]*) ([^ ]*) \\[(.*?)\\] ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*)
 ([^ ]*) (\"[^\"]*\"|-) (-|[0-9]*) ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*)
 ([^ ]*) (\"[^\"]*\"|-) ([^ ]*)(?: ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*)
 ([^ ]*) ([^ ]*) ([^ ]*))?.*$')
STORED AS INPUTFORMAT
 'org.apache.hadoop.mapred.TextInputFormat'
OUTPUTFORMAT
 'org.apache.hadoop.hive.ql.io.HiveIgnoreKeyTextOutputFormat'
LOCATION
 's3://bucket-name/prefix-name/account-id/region/source-bucket-name/'
 TBLPROPERTIES (
  'projection.enabled'='true',
  'projection.timestamp.format'='yyyy/MM/dd',
  'projection.timestamp.interval'='1',
  'projection.timestamp.interval.unit'='DAYS',
  'projection.timestamp.range'='2024/01/01,NOW',
  'projection.timestamp.type'='date',
  'storage.location.template'='s3://bucket-name/prefix-name/account-id/region/
source-bucket-name/${timestamp}')
```

Non-date-based partitioning

```
CREATE EXTERNAL TABLE `s3_access_logs_db.mybucket_logs`(
```

```
  `bucketowner` STRING,
  `bucket_name` STRING,
  `requestdatetime` STRING,
  `remoteip` STRING,
  `requester` STRING,
  `requestid` STRING,
  `operation` STRING,
  `key` STRING,
  `request_uri` STRING,
  `httpstatus` STRING,
  `errorcode` STRING,
  `bytessent` BIGINT,
  `objectsize` BIGINT,
  `totaltime` STRING,
  `turnaroundtime` STRING,
  `referrer` STRING,
  `useragent` STRING,
  `versionid` STRING,
  `hostid` STRING,
  `sigv` STRING,
  `ciphersuite` STRING,
  `authtype` STRING,
  `endpoint` STRING,
  `tlsversion` STRING,
  `accesspointarn` STRING,
  `aclrequired` STRING)
ROW FORMAT SERDE
  'org.apache.hadoop.hive.serde2.RegexSerDe'
WITH SERDEPROPERTIES (
  'input.regex'='([^ ]*) ([^ ]*) \\[(.*?)\\] ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*)
 ([^ ]*) (\"[^\"]*\"|-) (-|[0-9]*) ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*)
 ([^ ]*) (\"[^\"]*\"|-) ([^ ]*)(?: ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*)
 ([^ ]*) ([^ ]*) ([^ ]*))?.*$')
STORED AS INPUTFORMAT
  'org.apache.hadoop.mapred.TextInputFormat'
OUTPUTFORMAT
  'org.apache.hadoop.hive.ql.io.HiveIgnoreKeyTextOutputFormat'
LOCATION
  's3://amzn-s3-demo-bucket1-logs/prefix/'
```

4. ナビゲーションペインにある、[データベース] で、データベースを選択します。
5. [テーブル] で、テーブル名の横にある、[Preview table (テーブルのプレビュー)] を選択します。

[結果] ペインに、サーバーアクセスログのデータ (bucketowner、bucket、requestdatetime など) が表示されます。これは、Athena テーブルが正常に作成されたことを意味します。これで Amazon S3 サーバーアクセスログのクエリを実行できるようになりました。

Example – 誰がいつオブジェクトを削除したか (タイムスタンプ、IP アドレス、および IAM ユーザー) を表示する

```
SELECT requestdatetime, remoteip, requester, key
FROM s3_access_logs_db.mybucket_logs
WHERE key = 'images/picture.jpg' AND operation like '%DELETE%';
```

Example – IAM ユーザーによって実行されたすべてのオペレーションを表示する

```
SELECT *
FROM s3_access_logs_db.mybucket_logs
WHERE requester='arn:aws:iam::123456789123:user/user_name';
```

Example – 特定の期間にオブジェクトに対して実行されたすべてのオペレーションを表示する

```
SELECT *
FROM s3_access_logs_db.mybucket_logs
WHERE Key='prefix/images/picture.jpg'
    AND parse_datetime(requestdatetime,'dd/MMM/yyyy:HH:mm:ss Z')
    BETWEEN parse_datetime('2017-02-18:07:00:00','yyyy-MM-dd:HH:mm:ss')
    AND parse_datetime('2017-02-18:08:00:00','yyyy-MM-dd:HH:mm:ss');
```

Example – 特定の期間、特定の IP アドレスに送信されたデータの量を表示する

```
SELECT coalesce(SUM(bytessent), 0) AS bytessenttotal
FROM s3_access_logs_db.mybucket_logs
WHERE remoteip='192.0.2.1'
```

```
AND parse_datetime(requestdatetime,'dd/MMM/yyyy:HH:mm:ss Z')
BETWEEN parse_datetime('2022-06-01','yyyy-MM-dd')
AND parse_datetime('2022-07-01','yyyy-MM-dd');
```

Example — 特定の期間内の HTTP 5xx エラーに対応するリクエスト ID を検索する

```
SELECT requestdatetime, key, httpstatus, errorcode, requestid, hostid
FROM s3_access_logs_db.mybucket_logs
WHERE httpstatus like '5%' AND timestamp
BETWEEN '2024/01/29'
AND '2024/01/30'
```

> **Note**
>
> ログを保持する時間を短縮するために、サーバーアクセスログバケットの Amazon S3 ライフサイクル設定を作成できます。ライフサイクル設定ルールを作成して、定期的にログファイルを削除します。これにより、各クエリで Athena が分析するデータの量が減ります。詳細については、「バケットに S3 ライフサイクル設定を設定する」を参照してください。

Amazon S3 アクセスログを使用した Signature Version 2 リクエストの識別

Signature Version 2 の Amazon S3 サポートがオフになります (非推奨)。その後、Amazon S3 は署名バージョン 2 を使用するリクエストを受け入れず、すべてのリクエストに Signature Version 4 署名を使用する必要があります。Amazon S3 アクセスログを使用して、Signature Version 2 アクセスリクエストを識別できます。

> **Note**
>
> Signature Version 2 リクエストを識別するには、Amazon S3 アクセスログの代わりに AWS CloudTrail データイベントを使用することをお勧めします。CloudTrail データイベントは、サーバーアクセスログと比べ、設定が容易で、より多くの情報が含まれています。詳細については、「CloudTrail を使用した Amazon S3 Signature Version 2 リクエストの識別」を参照してください。

Example – 署名バージョン 2 トラフィックを送信しているすべてのリクエスタを表示する

```
SELECT requester, sigv, Count(sigv) as sigcount
FROM s3_access_logs_db.mybucket_logs
GROUP BY requester, sigv;
```

Amazon S3 アクセスログを使用したオブジェクトアクセスリクエストの識別

Amazon S3 サーバーアクセスログに対するクエリを使用して、GET、PUT、DELETE などのオペレーションに対する Amazon S3 オブジェクトアクセスリクエストを識別し、それらのリクエストに関する詳細情報を確認することができます。

次の Amazon Athena クエリの例は、サーバーアクセスログから Amazon S3 に対するすべての PUT オブジェクトリクエストを取得する方法を示しています。

Example – 一定期間内に **PUT** オブジェクトリクエストを送信しているすべてのリクエスタを表示する

```
SELECT bucket_name, requester, remoteip, key, httpstatus, errorcode, requestdatetime
FROM s3_access_logs_db
WHERE operation='REST.PUT.OBJECT' AND
parse_datetime(requestdatetime,'dd/MMM/yyyy:HH:mm:ss Z')
BETWEEN parse_datetime('2019-07-01:00:42:42','yyyy-MM-dd:HH:mm:ss')
AND
parse_datetime('2019-07-02:00:42:42','yyyy-MM-dd:HH:mm:ss')
```

次の Amazon Athena クエリの例は、サーバーアクセスログから Amazon S3 に対するすべての GET オブジェクトリクエストを取得する方法を示しています。

Example – 一定期間内に **GET** オブジェクトリクエストを送信しているすべてのリクエスタを表示する

```
SELECT bucket_name, requester, remoteip, key, httpstatus, errorcode, requestdatetime
FROM s3_access_logs_db
WHERE operation='REST.GET.OBJECT' AND
parse_datetime(requestdatetime,'dd/MMM/yyyy:HH:mm:ss Z')
BETWEEN parse_datetime('2019-07-01:00:42:42','yyyy-MM-dd:HH:mm:ss')
AND
```

```
parse_datetime('2019-07-02:00:42:42','yyyy-MM-dd:HH:mm:ss')
```

次の Amazon Athena のクエリの例は、S3 バケットへのすべての匿名リクエストをサーバーアクセスログから取得する方法を示しています。

Example – 特定の期間にバケットにリクエストを行っているすべての匿名リクエスタを表示する

```
SELECT bucket_name, requester, remoteip, key, httpstatus, errorcode, requestdatetime
FROM s3_access_logs_db.mybucket_logs
WHERE requester IS NULL AND
parse_datetime(requestdatetime,'dd/MMM/yyyy:HH:mm:ss Z')
BETWEEN parse_datetime('2019-07-01:00:42:42','yyyy-MM-dd:HH:mm:ss')
AND
parse_datetime('2019-07-02:00:42:42','yyyy-MM-dd:HH:mm:ss')
```

次の Amazon Athena のクエリは、承認のためにアクセスコントロールリスト (ACL) が必要な S3 バケットへのすべてのリクエストを特定する方法を示しています。この情報を使用して、これらの ACL 権限を適切なバケットポリシーに移行し、ACL を無効にすることができます。これらのバケットポリシーを作成したら、これらのバケットの ACL を無効にできます。ACL の無効化の詳細については、「ACL を無効にする前提条件。」を参照してください。

Example — 承認に ACL が必要なリクエストをすべて特定する

```
SELECT bucket_name, requester, key, operation, aclrequired, requestdatetime
FROM s3_access_logs_db
WHERE aclrequired = 'Yes' AND
parse_datetime(requestdatetime,'dd/MMM/yyyy:HH:mm:ss Z')
BETWEEN parse_datetime('2022-05-10:00:00:00','yyyy-MM-dd:HH:mm:ss')
AND parse_datetime('2022-08-10:00:00:00','yyyy-MM-dd:HH:mm:ss')
```

> **Note**
>
> - ニーズに合わせられるように、必要に応じてデータ範囲を変更することができます。
> - このクエリの例は、セキュリティのモニタリングにも役立つ場合があります。予期しないまたは不正な IP アドレスやリクエスタからの `PutObject` または `GetObject` コールの結果を確認し、バケットへの匿名リクエストを特定できます。

- このクエリでは、ログ記録が有効になった時間以降の情報のみ取得されます。
- AWS CloudTrail ログを使用している場合は、「CloudTrail を使用した S3 オブジェクトへのアクセスの識別」を参照してください。

サーバーのアクセスログ記録のトラブルシューティング

次のトピックは、Amazon S3 でログ記録された問題をトラブルシューティングするのに役立ちます。

トピック

- ログ記録設定時のよくあるエラーメッセージ
- 配信失敗のトラブルシューティング

ログ記録設定時のよくあるエラーメッセージ

AWS Command Line Interface (AWS CLI) と AWS SDK を使用してログ記録を有効にすると、次のようなエラーメッセージが表示されることがよくあります。

エラー: S3 ロケーションをまたがるロギングは許可されていません

送信先バケット (別名ターゲットバケット) がソースバケットとは別のリージョンに配置されている場合、Cross S3 location logging not allowed エラーが発生します。このエラーを解決するには、アクセスログを受信するように設定された送信先バケットがソースバケットと同じ AWS リージョン の AWS アカウント にあることを確認します。

エラー: ログを記録するバケットの所有者とターゲットバケットの所有者は同じである必要があります

サーバーアクセスのログ記録を有効にしている場合、指定された送信先バケットが別のアカウントに属している場合にこのエラーが発生します。このエラーを解決するには、送信先バケットがソースバケットと同じ AWS アカウント にあることを確認します。

> **Note**
>
> ソースバケットとは別のターゲットバケットを選択することをお勧めします。ソースバケットと送信先バケットが同じ場合、バケットに書き込まれるログに関する追加のログが作成され、ストレージ料金が増大する可能性があります。また、追加のログがあると、探してい

る特定のログを見つけるのが難しくなることがあります。ログを管理しやすくするため、アクセスログは別のバケットに保存することをお勧めします。詳細については、「the section called “ログ配信を有効にするにはどうすればよいですか?”」を参照してください。

エラー: ログ記録のターゲットバケットが存在しません。

送信先バケットは、設定する前に存在している必要があります。このエラーは、送信先バケットが存在しないか、見つからないことを示しています。バケット名のスペルが正しいことを確認してから、もう一度試してください。

エラー: バケット所有者が強制するバケットにターゲット許可が付与されていません

このエラーは、送信先バケットが S3 オブジェクト所有権のバケット所有者の強制設定を使用していることを示しています。バケット所有者の強制設定は、送信先 (ターゲット) 権限をサポートしていません。詳細については、「ログ配信許可」を参照してください。

配信失敗のトラブルシューティング

サーバーアクセスの log 記録の問題を回避するには、次のベストプラクティスに従っていることを確認してください。

- S3 ログ配信グループに送信先バケットへの書き込みアクセス許可があること - S3 ログ配信グループは、送信先バケットにサーバーアクセスログを配信します。バケットポリシーまたはバケットアクセスコントロールリスト (ACL) を使用して、送信先バケットへの書き込みアクセスを付与できます。ただし、ACL の代わりにバケットポリシーを使用することをお勧めします。送信先バケットへの書き込みアクセスを許可する方法の詳細については、「ログ配信許可」を参照してください。

  > **Note**
  >
  > 送信先バケットが、オブジェクト所有権にバケット所有者の強制設定を使用している場合は、次の点に注意します。
  >
  > - ACL は無効になり、アクセス権限には影響しません。つまり、S3 ログ配信グループへのアクセスを許可すると、バケット ACL を更新できません。代わりに、ログサービスプリンシパルへのアクセスを許可するために、送信先バケットのバケットポリシーを更新する必要があります。
  > - `PutBucketLogging` 設定には、送信先権限を含めることできません。

- 送信先バケットのバケットポリシーがログへのアクセスを許可していること – ターゲットバケットのバケットポリシーを確認します。`"Effect": "Deny"` を含むステートメントをバケットポリシーで検索します。次に、Deny ステートメントがアクセスログのバケットへの書き込みを妨げていないことを確認します。
- S3 オブジェクトロックがターゲットバケットで有効になっていないこと – ターゲットバケットでオブジェクトロックが有効になっているかを確認します。オブジェクトロックにより、サーバーアクセスログの配信をブロックします。オブジェクトロックが有効になっていない送信先バケットを選択する必要があります。
- 送信先バケットでデフォルトの暗号化が有効になっている場合、Amazon S3 マネージドキー (SSE-S3) が選択されていること – Amazon S3 マネージドキー (SSE-S3) でサーバー側の暗号化を使用する場合に限り、送信先バケットでデフォルトのバケット暗号化を使用できます。サーバーアクセスのログ記録の送信先バケットでは、AWS Key Management Service (AWS KMS) キー (SSE-KMS) によるデフォルトのサーバー側の暗号化はサポートされていません。デフォルトの暗号化の有効にする方法の詳細については、「デフォルトの暗号化の設定」を参照してください。
- ターゲットバケットでリクエスタ支払いが有効になっていないこと – サーバーアクセスのログ記録でのリクエスタ支払いバケットの使用はサポートされていません。サーバーアクセスログの配信を許可するには、ターゲットバケットのリクエスタ支払いオプションを無効にします。
- AWS Organizations のサービスコントロールポリシー (SCP) とリソースコントロールポリシー (RCP) を確認する - AWS Organizations を使用している場合は、サービスコントロールポリシーとリソースコントロールポリシーをチェックして、Amazon S3 へのアクセスが許可されていることを確認します。これらのポリシーは、影響を受けるアカウントのプリンシパルとリソースに対する最大数のアクセス許可を指定します。`"Effect": "Deny"` を含むステートメントをポリシーで検索し、バケットへのアクセスログの書き込みを Deny ステートメントが妨げていないことを確認します。詳細については、「AWS Organizations IAM ユーザーガイド」の「Authorization policies in AWS Organizations」を参照してください。
- 最新のロギング設定の変更が有効になるまで時間がかかること - サーバーアクセスのログ記録を最初に有効にした場合や、ログの送信先バケットを変更した場合は、すべてが有効になるまでに時間がかかります。すべてのリクエストが正しく記録され、配信されるまでに 1 時間以上かかる場合があります。

  ログ配信の失敗を確認するには、Amazon CloudWatch でリクエストメトリクスを有効にします。ログが数時間以内に配信されない場合は、ログ配信の失敗を示す `4xxErrors` メトリクスを探してください。リクエストメトリクスの有効化の詳細については、「the section called “すべてのオブジェクトに対するメトリクス設定の作成”」を参照してください。

Amazon CloudWatch によるメトリクスのモニタリング

Amazon S3 の Amazon CloudWatch メトリクスは、Amazon S3 を使用するアプリケーションのパフォーマンスを理解して向上させるのに役立つことがあります。Amazon S3 で CloudWatch を使用する方法は複数あります。

バケットの日次ストレージメトリクス

バケットストレージは、CloudWatch を使用してモニタリングできます。これは、Amazon S3 からのストレージデータを収集し、読み取り可能な日次のメトリクスに加工します。これらの Amazon S3 のストレージメトリクスは 1 日に 1 回報告され、すべてのお客様に追加料金なしで提供されます。

リクエストメトリクス

Amazon S3 リクエストをモニタリングし、オペレーションの問題をすばやく特定して対応します。メトリクスは、処理のレイテンシーの後に 1 分間隔で使用できます。これらの CloudWatch メトリクスは、Amazon CloudWatch カスタムメトリクスと同じレートで請求されます。CloudWatch の料金の詳細については、Amazon CloudWatch の料金をご覧ください。これらのメトリクスの取得をオプトインする方法の詳細については、CloudWatch メトリクスの設定 を参照してください。

有効にすると、すべてのオブジェクトオペレーションのリクエストメトリクスが報告されます。デフォルトでは、Amazon S3 バケットレベルでこれらの 1 分のメトリクスが利用可能です。共有プレフィックス、オブジェクトタグ、またはアクセスポイントを使用してメトリクスにフィルタを定義することもできます。

- アクセスポイント – アクセスポイントは、バケットに接続され、S3 の共有データセットの大規模なデータアクセスの管理を簡素化する名前付きネットワークエンドポイントです。アクセスポイントフィルタを使用すると、アクセスポイントの使用状況に関するインサイトを得ることができます。アクセスポイントの詳細については、汎用バケットのアクセスポイントのモニタリングと口グ記録 を参照してください。
- プレフィックス – Amazon S3 データモデルはフラット構造ですが、プレフィックスを使用して階層を推測できます。プレフィックスは、バケット内の類似オブジェクトをグループ化できるディレクトリ名に似ています。S3 コンソールはフォルダの概念でこれらのプレフィックスをサポートします。プレフィックスでフィルタリングした場合、同じプレフィックスを持つオブジェクトがメトリクス設定に含まれます。 プレフィックスの詳細については、プレフィックスを使用してオブジェクトを整理する を参照してください。

- タグ – タグは、オブジェクトに追加できるキーと値の名前のペアです。タグを使用すると、オブジェクトを簡単に検索および整理できます。メトリクス設定のフィルタとしてタグを使用して、それらのタグを持つオブジェクトのみがメトリクス設定に含められるようにすることもできます。オブジェクトタグの詳細については、タグを使用してストレージを分類するを参照してください。

共有プレフィックス、オブジェクトタグ、またはアクセスポイントでフィルタリングすると、こうしたメトリクスを特定のビジネスアプリケーション、ワークフロー、または内部組織に合わせることができます。

レプリケーションメトリクス

レプリケーションを保留している S3 API オペレーションの合計数、レプリケーションを保留しているオブジェクトの合計サイズ、およびレプリケート先 AWS リージョンへの最大レプリケーション時間、およびレプリケーションに失敗したオペレーションの合計数をモニタリングします。S3 Replication Time Control (S3 RTC) または S3 レプリケーションメトリクスが有効になっているレプリケーションルールがレプリケーションメトリクスを発行します。

詳細については、メトリクス、イベント通知、ステータスによるレプリケーションのモニタリング または S3 Replication Time Control (S3 RTC)を使用してコンプライアンス要件を満たす を参照してください。

Amazon S3 ストレージレンズメトリクス

S3 StorageLens の使用状況とアクティビティのメトリクスを Amazon CloudWatch に公開して、CloudWatch ダッシュボード で運用状態の統一されたビューを作成できます。`AWS/S3/Storage-Lens` 名前空間で S3 Storage Lens のメトリクスは可能です。CloudWatch 公開オプションは、アドバンストメトリクスとレコメンデーションにアップグレードされた S3 StorageLens ダッシュボードで利用できます。S3 Storage Lens の新規または既存のダッシュボード設定に対して CloudWatch 公開オプションを有効にできます。

詳細については、CloudWatch で S3 Storage Lens のメトリクスをモニタリング を参照してください。

すべての CloudWatch 統計は 15 か月間保持されるため、履歴情報にアクセスしてウェブアプリケーションまたはサービスの動作をより的確に把握することができます。CloudWatch の詳細については、「Amazon CloudWatch ユーザーガイド」の「Amazon CloudWatch とは」を参照してください。ユースケースによっては、CloudWatch アラームに追加の設定が必要になる場合があります。例えば、メトリクスの数式を使用してアラームを作成できます。詳細については、「Amazon CloudWatch ユーザーガイド」の「CloudWatch メトリクスを使用する」、「Metric Math を使用す

る」、「Amazon CloudWatch アラームの使用」、および「メトリクス数式に基づく CloudWatch アラームの作成」を参照してください。

ベストエフォート型の CloudWatch メトリクス配信

CloudWatch メトリクスは、ベストエフォートで配信されます。リクエストメトリクスを持つ Amazon S3 オブジェクトのほとんどのリクエストにより、データポイントが CloudWatch に送信されます。

メトリクスの完全性や適時性は保証されません。特定のリクエストのデータポイントが、リクエストが実際に処理されたよりも後のタイムスタンプで返される場合があります。1 分のデータポイントは CloudWatch を通じて利用可能になるまで遅延する場合や、まったく提供されない場合があります。CloudWatch リクエストメトリクスは、バケットに対するトラフィックの特性をほぼリアルタイムで示します。すべてのリクエストを完全に報告するためのものではありません。

この機能はベストエフォート型であるため、請求情報とコスト管理ダッシュボードで利用できるレポートには、バケットメトリクスに表示されない 1 つ以上のアクセスリクエストが含まれることがあります。

詳細については、以下のトピックを参照してください。

トピック

- メトリクスとディメンション
- CloudWatch メトリクスへのアクセス
- CloudWatch メトリクスの設定

メトリクスとディメンション

Amazon S3 が Amazon CloudWatch に送信するストレージメトリクスとディメンションを次の表に一覧表示します。

ベストエフォート型の CloudWatch メトリクス配信

CloudWatch メトリクスは、ベストエフォートで配信されます。リクエストメトリクスを持つ Amazon S3 オブジェクトのほとんどのリクエストにより、データポイントが CloudWatch に送信されます。

メトリクスの完全性や適時性は保証されません。特定のリクエストのデータポイントが、リクエストが実際に処理されたよりも後のタイムスタンプで返される場合があります。1 分のデータポイントは CloudWatch を通じて利用可能になるまで遅延する場合や、まったく提供されない場合がありま

す。CloudWatch リクエストメトリクスは、バケットに対するトラフィックの特性をほぼリアルタイムで示します。すべてのリクエストを完全に報告するためのものではありません。

この機能はベストエフォート型であるため、請求情報とコスト管理ダッシュボードで利用できるレポートには、バケットメトリクスに表示されない 1 つ以上のアクセスリクエストが含まれることがあります。

トピック

- CloudWatch のバケットの Amazon S3 デイリーストレージメトリクス。
- CloudWatch の Amazon S3 リクエストメトリクス
- CloudWatch の S3 レプリケーションメトリクス
- CloudWatch での S3 Storage Lens のメトリクス
- CloudWatch の S3 Object Lambda リクエスト
- CloudWatch の Amazon S3 ディメンション
- CloudWatch の S3 レプリケーションディメンション
- CloudWatch の S3 Storage Lens のディメンション。
- CloudWatch の S3 Object Lambda リクエストのディメンション
- Amazon S3 使用状況メトリクス

CloudWatch のバケットの Amazon S3 デイリーストレージメトリクス。

AWS/S3 名前空間には、バケットの以下の日次ストレージメトリクスが含まれます。

メトリクス	説明
BucketSizeBytes	次のストレージクラスのバケットに保存されているデータ量 (バイト単位): • S3 低冗長ストレージ (RRS) (REDUCED_REDUNDANCY) • S3 Express One Zone (EXPRESS_ONEZONE) • S3 Glacier Deep Archive (DEEP_ARCHIVE) • S3 Glacier Flexible Retrieval (GLACIER) • S3 Glacier Instant Retrieval (GLACIER_IR) • S3 Intelligent-Tiering (INTELLIGENT_TIERING)

メトリクス	説明
	• S3 One Zone-Infrequent Access (ONEZONE_IA) • S3 Standard (STANDARD) • S3 Standard-Infrequent Access (STANDARD_IA) この値は、バケット内のすべてのオブジェクト (現行オブジェクトと旧オブジェクトの両方) とメタデータ (バケット名など) のサイズを合計することによって計算され、これにはバケットに対する未完了のすべてのマルチパートアップロードのすべてのパートのサイズも含まれます。 Note S3 Express One Zone ストレージクラスは、ディレクトリバケットでのみ使用できます。 有効なストレージタイプのフィルタ (StorageType ディメンションを参照) • 低冗長ストレージ (RRS): ReducedRedundancyStorage • S3 Express One Zone: ExpressOneZoneStorage • S3 Glacier Deep Archive: DeepArchiveObjectOverhead 、DeepArchiveS3ObjectOverhead 、DeepArchiveStagingStorage 、DeepArchiveStorage • S3 Glacier Flexible Retrieval: GlacierObjectOverhead 、GlacierS3ObjectOverhead 、GlacierStagingStorage 、GlacierStorage • S3 Glacier Instant Retrieval: GlacierInstantRetrievalStorage 、GlacierIRSizeOverhead • S3 Intelligent-Tiering: IntelligentTieringAAStorage 、IntelligentTieringAIAStorage 、IntelligentTieringDAAStorage 、IntelligentTieringFAStorage 、IntelligentTieringIAStorage

メトリクス	説明
	• S3 One Zone-Infrequent Access: `OneZoneIASizeOverhead` 、`OneZoneIAStorage` • S3 Standard: `StandardStorage` • S3 Standard-Infrequent Access: `StandardIAObjectOverhead` 、`StandardIASizeOverhead` 、`StandardIAStorage` 単位: バイト 有効な統計: Average `StorageType` ディメンションの詳細については、the section called “CloudWatch の Amazon S3 ディメンション”を参照してください。
`NumberOfObjects`	すべてのストレージクラスのバケットに保存されたオブジェクトの合計数。この値を計算するには、バケット内のすべてのオブジェクト (最新のオブジェクトと最新でないオブジェクトの両方)、削除マーカー、およびバケットに対するすべての不完全なマルチパートアップロードの合計パート数をカウントします。S3 Express One Zone ストレージ クラスのオブジェクトがあるディレクトリバケットの場合、この値はバケット内のすべてのオブジェクトをカウントすることによって算出されます。ただし、バケットへの完了しなかった複数のアップロードは含まれません。 有効なストレージタイプのフィルタ: `AllStorageTypes` (`StorageType` ディメンションを参照) 単位: 個 有効な統計: 平均

CloudWatch の Amazon S3 リクエストメトリクス

`AWS/S3` 名前空間には、次のリクエストメトリクスが含まれます。これらのメトリクスには、請求対象外のリクエスト (`CopyObject` および Replication からの `GET` リクエストの場合) が含まれます。

> **Note**
>
> CloudWatch の Amazon S3 リクエストメトリクスは、ディレクトリバケットではサポートされません。

メトリクス	説明
`AllRequests`	タイプに関係なく、Amazon S3 バケットに対して行われた HTTP リクエストの総数。フィルターでメトリクス設定を使用している場合、このメトリクスはフィルターの要件を満たす HTTP リクエストのみを返します。 単位: カウント 有効な統計: Sum
`GetRequests`	Amazon S3 バケット内のオブジェクトに対して行われた HTTP `GET` リクエストの数。これには、リストオペレーションは含まれません。このメトリクスは、`CopyObject` リクエストのリクエスト元ごとに増加します。 単位: カウント 有効な統計: Sum **Note** ListMultipartUploads、ListParts、ListObjectVersions など、ページ分割されたリスト指向のリクエストは、このメトリクスに含まれません。
`PutRequests`	Amazon S3 バケット内のオブジェクトに対して行われた HTTP PUT リクエストの数。このメトリクスは、`CopyObject` リクエストのリクエスト先ごとに増加します。 単位: カウント

メトリクス	説明
	有効な統計: Sum
DeleteRequests	Amazon S3 バケット内のオブジェクトに対して行われた HTTP DELETE リクエストの数。このメトリクスには DeleteObjects リクエストも含まれます。このメトリクスは、削除されるオブジェクトの数ではなく作成されたリクエストの数を示します。 単位: カウント 有効な統計: Sum
HeadRequests	Amazon S3 バケットに対して行われた HTTP HEAD リクエストの数。 単位: カウント 有効な統計: Sum
PostRequests	Amazon S3 バケットに対して行われた HTTP POST リクエストの数。 単位: カウント 有効な統計: Sum **Note** DeleteObjects および SelectObjectContent リクエストはこのメトリクスに含まれません。
SelectRequests	Amazon S3 バケット内のオブジェクトに対して行われた Amazon S3 の SelectObjectContent リクエストの数。 単位: カウント 有効な統計: Sum

メトリクス	説明
SelectBytesScanned	Amazon S3 バケットの Amazon S3 の SelectObjectContent リクエストでスキャンされたデータのバイト数。 単位: バイト 有効な統計: Average (リクエストあたりのバイト数)、Sum (期間あたりのバイト数)、Sample Count、Min、Max (p100 と同じ)、p0.0 ~ p99.9 のパーセンタイル
SelectBytesReturned	Amazon S3 バケットの Amazon S3 の SelectObjectContent リクエストで返されたデータのバイト数。 単位: バイト 有効な統計: Average (リクエストあたりのバイト数)、Sum (期間あたりのバイト数)、Sample Count、Min、Max (p100 と同じ)、p0.0 ~ p99.9 のパーセンタイル
ListRequests	バケットの内容をリストする HTTP リクエストの数。 単位: 個 有効な統計: Sum
BytesDownloaded	Amazon S3 バケットに対する、レスポンスに本文が含まれるリクエストに対してダウンロードしたバイト数。 単位: バイト 有効な統計: Average (リクエストあたりのバイト数)、Sum (期間あたりのバイト数)、Sample Count、Min、Max (p100 と同じ)、p0.0 ~ p99.9 のパーセンタイル

メトリクス	説明
BytesUploaded	Amazon S3 バケットに対する、リクエストに本文が含まれるリクエストに対してアップロードしたバイト数。 単位: バイト 有効な統計: Average (リクエストあたりのバイト数)、Sum (期間あたりのバイト数)、Sample Count、Min、Max (p100 と同じ)、p0.0 ~ p99.9 のパーセンタイル
4xxErrors	Amazon S3 バケットに対して行われた、値が 0 または 1 の HTTP 4xx クライアントエラーステータスコードリクエストの数。Average 統計はエラーレートを示し、Sum 統計は各期間中のそのタイプのエラー数を示します。 単位: カウント 有効な統計: Average (リクエストあたりの報告数)、Sum (期間あたりの報告数)、Min、Max、Sample Count
5xxErrors	Amazon S3 バケットに対して行われた、値が 0 または 1 の HTTP 5xx サーバーエラーステータスコードリクエストの数。Average 統計はエラーレートを示し、Sum 統計は各期間中のそのタイプのエラー数を示します。 単位: カウント 有効な統計: Average (リクエストあたりの報告数)、Sum (期間あたりの報告数)、Min、Max、Sample Count
FirstByte Latency	Amazon S3 バケットがリクエスト全体を受信してからレスポンスの返信が開始するまでのリクエストあたりの時間。 単位: ミリ秒 有効な統計: Average、Sum、Min、Max (p100 と同じ)、Sample Count、p0.0 ~ p100 のパーセンタイル

メトリクス	説明
TotalRequestLatency	最初のバイトが受信されてから Amazon S3 バケットに最後のバイトが送信されるまでのリクエストあたりの経過時間。このメトリクスには、FirstByteLatency には含まれない、リクエストボディの受信とレスポンス本文の送信にかかった時間が含まれます。 単位: ミリ秒 有効な統計: Average、Sum、Min、Max (p100 と同じ)、Sample Count、p0.0 ~ p100 のパーセンタイル

CloudWatch の S3 レプリケーションメトリクス

保留中のバイト数、保留中のオペレーション、およびレプリケーションのレイテンシーを追跡することにより、S3 レプリケーションメトリクスを使用してレプリケーションの進行状況をモニタリングできます。詳細については、「レプリケーションメトリクスによる進捗状況のモニタリング」をご参照ください。

> **Note**
>
> Amazon CloudWatch でレプリケーションメトリクスのアラームを有効にできます。レプリケーションメトリクスのアラームを設定する場合は、[Missing data treatment (欠落データの処理)] フィールドを [Treat missing data as ignore (maintain the alarm state) (欠落データの処理方法: 無視 (アラームの状態を維持)] に設定します。

メトリクス	説明
ReplicationLatency	特定のレプリケーションルールについて、レプリケート先 AWS リージョン がレプリケート元 AWS リージョン より遅れる最大秒数。 単位: 秒 有効な統計: Max
BytesPendingReplication	特定のレプリケーションルールについて、レプリケーションが保留中のオブジェクトの合計バイト数。

メトリクス	説明
	単位: バイト 有効な統計: Max
`OperationsPendingReplication`	特定のレプリケーションルールについて、レプリケーションが保留中のオペレーションの数。 単位: カウント 有効な統計: Max
`OperationsFailedReplication`	特定のレプリケーションルールについて、レプリケートに失敗したオペレーションの数。 単位: カウント 有効な統計: 合計 (失敗した操作の総数)、平均 (失敗率)、サンプル数 (レプリケーションオペレーションの総数)

CloudWatch での S3 Storage Lens のメトリクス

S3 StorageLens の使用状況とアクティビティのメトリクスを Amazon CloudWatch に公開して、CloudWatch ダッシュボードで運用状態の統一されたビューを作成できます。CloudWatch 内の `AWS/S3/Storage-Lens` 名前空間 S3 Storage Lens メトリクスを公開します。CloudWatch 公開オプションは、アドバンストメトリクスとレコメンデーションにアップグレードされている S3 StorageLens ダッシュボードで利用できます。

CloudWatch に公開された S3 Storage Lens メトリクスの一覧については、「Amazon S3 Storage Lens のメトリクスに関する用語集」を参照してください。ディメンションの詳細なリストについては、ディメンション を参照してください。

CloudWatch の S3 Object Lambda リクエスト

S3 Object Lambda には、次のリクエストメトリクスが含まれます。

メトリクス	説明
AllRequests	Object Lambda アクセスポイントを使用して Amazon S3 バケットに対して行われた HTTP リクエストの総数。 単位: カウント 有効な統計: Sum
GetRequests	Object Lambda アクセスポイントを使用してオブジェクトに対して行われた HTTP GET リクエストの数。このメトリクスにはリストオペレーションは含まれません。 単位: カウント 有効な統計: Sum
BytesUploaded	Object Lambda アクセスポイントを使用して Amazon S3 バケットにアップロードされたバイト数。リクエストには本文が含まれます。 単位: バイト 有効な統計: Average (リクエストあたりのバイト数)、Sum (期間あたりのバイト数)、Sample Count、Min、Max (p100 と同じ)、p0.0 ~ p99.9 のパーセンタイル
PostRequests	Object Lambda アクセスポイントを使用して Amazon S3 バケットに対して行われた HTTP POST リクエストの数。 単位: カウント 有効な統計: Sum
PutRequests	Object Lambda アクセスポイントを使用して Amazon S3 バケット内のオブジェクトに対して行われた HTTP PUT リクエストの数。 単位: カウント 有効な統計: Sum

メトリクス	説明
DeleteRequests	Object Lambda アクセスポイントを使用して Amazon S3 バケット内のオブジェクトに対して行われた HTTP DELETE リクエストの数。このメトリクスには DeleteObjects リクエストが含まれます。このメトリクスは、削除されるオブジェクトの数ではなく作成されたリクエストの数を示します。 単位: カウント 有効な統計: Sum
BytesDownloaded	Amazon S3 バケットに対する、レスポンスに本文が含まれる Object Lambda のアクセスポイントを使用したリクエストに対してダウンロードしたバイト数。 単位: バイト 有効な統計: Average (リクエストあたりのバイト数)、Sum (期間あたりのバイト数)、Sample Count、Min、Max (p100 と同じ)、p0.0 ~ p99.9 のパーセンタイル
FirstByteLatency	Amazon S3 バケットが Object Lambda を経由してリクエスト全体を受信してからレスポンスの返信が開始するまでのリクエストあたりの時間。このメトリクスは、AWS Lambda 関数が Object Lambda アクセスポイントにバイトを返すまでにオブジェクトを変換する関数の実行時間によって異なります。 単位: ミリ秒 有効な統計: Average、Sum、Min、Max (p100 と同じ)、Sample Count、p0.0 ~ p100 のパーセンタイル

メトリクス	説明
TotalRequestLatency	最初のバイトが受信されてから Object Lambda アクセスポイントに最後のバイトが送信されるまでのリクエストあたりの経過時間。このメトリクスには、FirstByteLatency には含まれない、リクエストボディの受信とレスポンス本文の送信にかかった時間が含まれます。 単位: ミリ秒 有効な統計: Average、Sum、Min、Max (p100 と同じ)、Sample Count、p0.0 ~ p100 のパーセンタイル
HeadRequests	Object Lambda アクセスポイントを使用して Amazon S3 バケットに対して行われた HTTP HEAD リクエストの数。 単位: カウント 有効な統計: Sum
ListRequests	Amazon S3 バケットの内容をリストする HTTP GET リクエストの数。このメトリクスには、ListObjects および ListObjectsV2 オペレーションの両方が含まれます。 単位: カウント 有効な統計: Sum
4xxErrors	Object Lambda アクセスポイントを使用して Amazon S3 バケットに対して行われた、値が 0 または 1 の HTTP 4xx クライアントエラーステータスコードリクエストの数。AAverage 統計はエラーレートを示し、Sum 統計は各期間中のそのタイプのエラー数を示します。 単位: カウント 有効な統計: Average (リクエストあたりの報告数)、Sum (期間あたりの報告数)、Min、Max、Sample Count

メトリクス	説明
5xxErrors	Object Lambda アクセスポイントを使用して Amazon S3 バケットに対して行われた、値が 0 または 1 の HTTP 5xx サーバーエラーステータスコードリクエストの数。AAverage 統計はエラーレートを示し、Sum 統計は各期間中のそのタイプのエラー数を示します。 単位: カウント 有効な統計: Average (リクエストあたりの報告数)、Sum (期間あたりの報告数)、Min、Max、Sample Count
ProxiedRequests	標準の Amazon S3 API レスポンスを返す Object Lambda アクセスポイントへの HTTP リクエストの数。(このようなリクエストには Lambda 関数は設定されていません。) 単位: カウント 有効な統計: Sum
InvokedLambda	Lambda 関数が呼び出された S3 オブジェクトへの HTTP リクエストの数。 単位: カウント 有効な統計: Sum
LambdaResponseRequests	Lambda 関数によって行われた WriteGetObjectResponse リクエストの数。このメトリクスは、GetObject リクエストにのみ適用されます。
LambdaResponse4xx	Lambda 関数から WriteGetObjectResponse を呼び出すときに発生する HTTP 4xx クライアントエラーの数。このメトリクスは 4xxErrors 呼び出しと同じ情報を提供しますが、対象は WriteGetObjectResponse 呼び出しのみです。
LambdaResponse5xx	Lambda 関数から WriteGetObjectResponse を呼び出すときに発生する HTTP 5xx サーバーエラーの数。このメトリクスは 5xxErrors 呼び出しと同じ情報を提供しますが、対象は WriteGetObjectResponse 呼び出しのみです。

CloudWatch の Amazon S3 ディメンション

以下のディメンションは、Amazon S3 メトリクスをフィルタリングするために使用されます。

ディメンション	説明
`BucketName`	このディメンションを指定すると、リクエストしたデータがフィルタリングされて、指定のバケットのものだけになります。
`StorageType`	このディメンションは、バケットに保存されたデータを、以下のストレージタイプでフィルタリングします。 • `DeepArchiveObjectOverhead` - アーカイブされたオブジェクトごとに、S3 Glacier は、インデックスおよび関連するメタデータ用に 32 KB のストレージを追加します。この追加データは、オブジェクトを特定して復元するのに必要です。この追加ストレージに対しては、S3 Glacier または S3 Glacier Deep Archive の料金が課金されます。 • `DeepArchiveS3ObjectOverhead` – S3 Glacier ディープアーカイブにアーカイブされたオブジェクトごとに、Simple Storage Service (Amazon S3) はオブジェクトの名前とその他のメタデータに 8 KB のストレージを使用します。この追加のストレージに対しては、S3 Standard 料金が発生します。 • `DeepArchiveStagingStorage` – S3 Glacier Deep Archive ストレージクラスのオブジェクトの `CompleteMultipartUpload` (複数アップロード完了) リクエストが完了する前に、マルチパートアップロードオブジェクトに使用されているバイト数。 • `DeepArchiveStorage` – S3 Glacier ディープアーカイブストレージクラスのオブジェクトに使用されているバイト数。 • `ExpressOneZoneStorage` – S3 Express One Zone ストレージクラスのオブジェクトに使用されているバイト数。

ディメンション	説明
	• `GlacierInstantRetrievalStorage` – S3 Glacier Instant Retrieval ストレージクラスのオブジェクトに使用されているバイト数。 • `GlacierIRSizeOverhead` – S3 Glacier Instant Retrieval ストレージクラスの 128 KB より小さなオブジェクトに使用されているバイト数。 • `GlacierObjectOverhead` - アーカイブされたオブジェクトごとに、S3 Glacier は、インデックスおよび関連するメタデータ用に 32 KB のストレージを追加します。この追加データは、オブジェクトを特定して復元するのに必要です。この追加ストレージに対しては、S3 Glacier Flexible Retrieval のレートが課金されます。 • `GlacierS3ObjectOverhead` - S3 Glacier Flexible Retrieval にアーカイブされたオブジェクトごとに、Simple Storage Service (Amazon S3) はオブジェクトの名前とその他のメタデータに 8 KB のストレージを使用します。この追加のストレージに対しては、S3 Standard 料金が発生します。 • `GlacierStagingStorage` - S3 Glacier Flexible Retrieval ストレージクラスのオブジェクトの `CompleteMultipartUpload` リクエストが完了する前に、マルチパートアップロードオブジェクトのパートに使用されていたバイト数。 • `GlacierStorage` – S3 Glacier Flexible Retrieval ストレージクラスのオブジェクトに使用されているバイト数。 • `IntAAObjectOverhead` - アーカイブアクセス層の `INTELLIGENT_TIERING` ストレージクラスの各オブジェクトについて、S3 Glacier はインデックスと関連メタデータ用に 32 KB のストレージを追加します。この追加データは、オブジェクトを特定して復元するのに必要です。この追加ストレージに対しては、S3 Glacier Flexible Retrieval のレートが課金されます。 • `IntAAS3ObjectOverhead` - アーカイブアクセス層の `INTELLIGENT_TIERING` ストレージクラスの各オブジェクトについて、Simple Storage Service (Amazon S3) はオ

ディメンション	説明
	ブジェクトの名前とその他のメタデータに 8 KB のストレージを使用します。この追加のストレージに対しては、S3 Standard 料金が発生します。 • IntDAAObjectOverhead - ディープアーカイブアクセス階層の INTELLIGENT_TIERING ストレージクラスの各オブジェクトについて、S3 Glacier はインデックスと関連メタデータ用に 32 KB のストレージを追加します。この追加データは、オブジェクトを特定して復元するのに必要です。この追加ストレージに対しては、S3 Glacier Deep Archive のストレージ料金が課金されます。 • IntDAAS3ObjectOverhead - ディープアーカイブアクセス階層の INTELLIGENT_TIERING ストレージクラスの各オブジェクトについて、Amazon S3 はインデックスと関連メタデータ用に 8 KB のストレージを追加します。この追加データは、オブジェクトを特定して復元するのに必要です。この追加のストレージに対しては、S3 Standard 料金が発生します。 • IntelligentTieringAAStorage - INTELLIGENT_TIERING ストレージクラスのアーカイブアクセス層にあるオブジェクトに使用されているバイト数。 • IntelligentTieringAIAStorage - INTELLIGENT_TIERING ストレージクラスの アーカイブインスタントアクセス層のオブジェクトに使用されているバイト数。 • IntelligentTieringDAAStorage - INTELLIGENT_TIERING ストレージクラスのアーカイブアクセス層にあるオブジェクトに使用されているバイト数。 • IntelligentTieringFAStorage - INTELLIGENT_TIERING ストレージクラスの高頻度アクセス層のオブジェクトに使用されているバイト数。 • IntelligentTieringIAStorage - INTELLIGENT_TIERING ストレージクラスの低頻度アクセス層のオブジェクトに使用されているバイト数。

ディメンション	説明
	• OneZoneIASizeOverhead – ONEZONE_IA ストレージクラスの 128 KB 未満のオブジェクトに使用されているバイト数。 • OneZoneIAStorage - S3 One Zone 低頻度アクセス (ONEZONE_IA) ストレージクラスのオブジェクトに使用されているバイト数。 • ReducedRedundancyStorage – 低冗長化ストレージ (RRS) クラスのオブジェクトに使用されているバイト数。 • StandardIASizeOverhead – STANDARD_IA ストレージクラスの 128 KB 未満のオブジェクトに使用されているバイト数。 • StandardIAStorage – S3 標準低頻度アクセス (STANDARD_IA) ストレージクラスのオブジェクトに使用されているバイト数。 • StandardStorage - STANDARD ストレージクラスのオブジェクトに使用されているバイト数。
FilterId	このディメンションは、バケットに対するリクエストメトリクスに対して指定するメトリクス設定をフィルタリングします。メトリクス設定を作成するときは、フィルター ID (プレフィックス、タグ、アクセスポイントなど) を指定します。詳細については、メトリクス設定の作成を参照してください。

CloudWatch の S3 レプリケーションディメンション

以下のディメンションは、S3 レプリケーションメトリクスをフィルタリングするために使用されます。

ディメンション	説明
SourceBucket	オブジェクトのレプリケート元となるバケットの名前。
DestinationBucket	オブジェクトのレプリケート先となるバケットの名前。

ディメンション	説明
RuleId	このレプリケーションメトリクスの更新をトリガーしたルールの一意の識別子。

CloudWatch の S3 Storage Lens のディメンション。

CloudWatch で S3 Storage Lens メトリクスのフィルタリングに使用されるディメンションのリストについては、「ディメンション」を参照してください。

CloudWatch の S3 Object Lambda リクエストのディメンション

次のディメンションを使用して、Object Lambda アクセスポイントからのデータをフィルタリングします。

ディメンション	説明
AccessPointName	リクエストが行われているアクセスポイントの名前。
DataSourceARN	Object Lambda アクセスポイントがデータを取得しているソース。リクエストが Lambda 関数を呼び出す場合、これは Lambda Amazon リソースネーム (ARN) を指します。それ以外の場合は、アクセスポイント ARN を指します。

Amazon S3 使用状況メトリクス

CloudWatch 使用状況メトリクスを使用して、アカウントのリソースの使用状況を把握できます。これらのメトリクスを使用して、CloudWatch グラフやダッシュボードで現在のサービスの使用状況を可視化できます。

Amazon S3 使用状況メトリクスは、AWS の Service Quotas に対応しています。使用量がサービスクォータに近づいたときに警告するアラームを設定することもできます。CloudWatch とサービスクオータの統合については「Amazon CloudWatch ユーザーガイド」の「AWS 使用状況メトリクス」を参照してください。

Amazon S3 は、AWS/Usage 名前空間に以下のメトリクスを公開します。

メトリクス	説明
ResourceCount	アカウントで実行されている指定されたリソースの数。リソースはメトリクスに関連付けられたディメンションによって定義されます。

次のディメンションは、Amazon S3 によって発行される使用状況メトリクスを絞り込むために使用されます。

ディメンション	説明
Service	リソースを含む AWS のサービスの名前。Amazon S3 使用状況メトリクスの場合、このディメンションの値は S3 です。
Type	報告されるエンティティタイプ。現在、Amazon S3 使用状況メトリクスの有効な値は Resource のみです。
Resource	実行中のリソースタイプ。現在、Amazon S3 使用状況メトリクスの有効な値は GeneralPurposeBuckets のみです。これは、AWS アカウント内の汎用バケットの数を返します。汎用バケットでは、S3 Express One Zone 以外のすべてのストレージクラスにオブジェクトを保存できます。

CloudWatch メトリクスへのアクセス

以下の手順を使用して、Amazon S3 のストレージメトリクスを表示できます。Amazon S3 メトリクスを含めるには、開始と終了のタイムスタンプを設定する必要があります。特定の 24 時間あたりのメトリクスの場合は、期間を 1 日の秒数である 86400 秒に設定します。また、BucketName および StorageType ディメンションを忘れずに設定してください。

AWS CLI を使用する場合

例えば、AWS CLI を使用して特定のバケットの平均サイズ (バイト単位) を取得する場合、次のコマンドを使用できます。

```
aws cloudwatch get-metric-statistics --metric-name BucketSizeBytes --namespace AWS/S3
 --start-time 2016-10-19T00:00:00Z --end-time 2016-10-20T00:00:00Z --statistics Average
```

```
 --unit Bytes --region us-west-2 --dimensions Name=BucketName,Value=amzn-s3-demo-bucket
 Name=StorageType,Value=StandardStorage --period 86400 --output json
```

この例では、次の出力が生成されます。

```
{
    "Datapoints": [
        {
            "Timestamp": "2016-10-19T00:00:00Z",
            "Average": 1025328.0,
            "Unit": "Bytes"
        }
    ],
    "Label": "BucketSizeBytes"
}
```

S3 コンソールの使用

Amazon CloudWatch コンソールを使用してメトリクスを表示するには

1. CloudWatch コンソールの https://console.aws.amazon.com/cloudwatch/ を開いてください。
2. 左のナビゲーションペインで [Metrics] (メトリクス) を選択します。
3. [S3] 名前空間を選択します。
4. (オプション) メトリクスを表示するには、検索ボックスにメトリクス名を入力します。
5. (オプション) [StorageType] ディメンションでフィルタする場合は、検索ボックスにストレージクラスの名前を入力します。

AWS CLI を使用して AWS アカウント に保存された有効なメトリクスのリストを表示するには

- コマンドプロンプトで、以下のコマンドを使用します。

  ```
  aws cloudwatch list-metrics --namespace "AWS/S3"
  ```

CloudWatch のアクセス許可の詳細については「Amazon CloudWatch ユーザーガイド」の「CloudWatch ダッシュボード許可の更新」を参照してください。

CloudWatch メトリクスの設定

Amazon S3 の Amazon CloudWatch リクエストメトリクスを使うと、1 分の CloudWatch メトリクスの受信、CloudWatch アラームの設定、および CloudWatch ダッシュボードへのアクセスによって、Amazon S3 ストレージの運用とパフォーマンスをほぼリアルタイムで確認できます。クラウドストレージに依存するアプリケーションの場合、これらのメトリクスを使用すると、オペレーションの問題を迅速に特定して対応できます。有効になっている場合、デフォルトでは、Amazon S3 バケットレベルでこれらの 1 分のメトリクスが利用可能です。

バケット内のオブジェクトに対する CloudWatch リクエストメトリクスを取得するには、そのバケットのメトリクス設定を作成する必要があります。詳細については、バケット内のすべてのオブジェクトに対する CloudWatch メトリクス設定を作成する を参照してください。

共有プレフィックス、オブジェクトタグ、またはアクセスポイントを使用して、収集したメトリクスのフィルタを定義することもできます。フィルタを定義するこの方法を使用すると、メトリクスフィルタを特定のビジネスアプリケーション、ワークフロー、または内部組織に合わせることができます。詳細については、プレフィックス、オブジェクトタグ、またはアクセスポイントでのメトリクス設定の作成 を参照してください。使用可能な CloudWatch メトリクスとストレージおよびリクエストメトリクスの違いの詳細については、Amazon CloudWatch によるメトリクスのモニタリング を参照してください。

メトリクス設定を使用するときは、以下に注意してください。

- バケットあたりの最大メトリクス設定数は 1000 です。
- フィルタを使用して、メトリクス設定に含めるバケット内のオブジェクトを選択できます。共有プレフィックス、オブジェクトタグ、またはアクセスポイントでフィルタリングすると、メトリクスを特定のビジネスアプリケーション、ワークフロー、または内部組織に合わせることができます。バケット全体のメトリクスをリクエストするには、フィルタのないメトリクス設定を作成します。
- メトリクス設定は、リクエストメトリクスを有効にするためにのみ必要です。バケットレベルでの日次ストレージメトリクスは常にオンになり、追加料金なしで提供されます。現在、フィルタリングされたオブジェクトサブセットの日次ストレージメトリクスを取得することはできません。
- 各メトリクス設定では、使用可能なリクエストメトリクスのフルセットが有効になります。オペレーション固有のメトリクス (`PostRequests` など) は、バケットまたはフィルタにそのタイプのリクエストがある場合にのみ報告されます。
- リクエストメトリクスは、オブジェクトレベルのオペレーションに対して報告されます。それらは、GET Bucket (List Objects)、GET Bucket Object Versions、および マルチパートアップロードのリスト など、バケット内容を一覧表示するオペレーションについても報告されますが、その他のバケットオペレーションでは報告されません。

- リクエストメトリクスでは、プレフィックス、オブジェクトタグ、またはアクセスポイントによるフィルタリングがサポートされますが、ストレージメトリクスではサポートされません。

ベストエフォート型の CloudWatch メトリクス配信

CloudWatch メトリクスは、ベストエフォートで配信されます。リクエストメトリクスを持つ Amazon S3 オブジェクトのほとんどのリクエストにより、データポイントが CloudWatch に送信されます。

メトリクスの完全性や適時性は保証されません。特定のリクエストのデータポイントが、リクエストが実際に処理されたよりも後のタイムスタンプで返される場合があります。1 分のデータポイントは CloudWatch を通じて利用可能になるまで遅延する場合や、まったく提供されない場合があります。CloudWatch リクエストメトリクスは、バケットに対するトラフィックの特性をほぼリアルタイムで示します。すべてのリクエストを完全に報告するためのものではありません。

この機能はベストエフォート型であるため、請求情報とコスト管理ダッシュボードで利用できるレポートには、バケットメトリクスに表示されない 1 つ以上のアクセスリクエストが含まれることがあります。

Amazon S3 での CloudWatch メトリクスの操作方法の詳細については、以下のトピックを参照してください。

トピック

- バケット内のすべてのオブジェクトに対する CloudWatch メトリクス設定を作成する
- プレフィックス、オブジェクトタグ、またはアクセスポイントでのメトリクス設定の作成
- メトリクスフィルタの削除

バケット内のすべてのオブジェクトに対する CloudWatch メトリクス設定を作成する

リクエストメトリクスを設定するときは、バケット内のすべてのオブジェクトに対して CloudWatch メトリクス設定を作成するか、プレフィックス、オブジェクトタグ、またはアクセスポイントでフィルタリングすることができます。このトピックの手順は、バケット内のすべてのオブジェクトに対して設定を作成する方法を説明します。オブジェクトタグ、プレフィックス、またはアクセスポイントでフィルタリングする設定を作成するには、プレフィックス、オブジェクトタグ、またはアクセスポイントでのメトリクス設定の作成 を参照してください。

Amazon S3 の Amazon CloudWatch メトリクスには、ストレージメトリクス、リクエストメトリクス、レプリケーションメトリクスの 3 種類があります。ストレージメトリクスは、1 日に 1 回レ

ポートされ、すべてのお客様に追加料金なしで提供されます。リクエストメトリクスは、処理のレイテンシーの後に 1 分間隔で使用できます。リクエストメトリクスには、CloudWatch の標準料金が課金されます。コンソールで設定するか、Amazon S3 API を使用して、リクエストメトリクスを取得する必要があります。S3 レプリケーションメトリクス は、レプリケーション設定のレプリケーションルールの詳細なメトリクスを提供します。レプリケーションメトリクスを使って、保留中のバイト数、保留中のオペレーション、レプリケーションに失敗したオペレーション、レプリケーションのレイテンシーを追跡すると、レプリケーションの進行状況を 1 分単位でモニタリングできます。

Amazon S3 の CloudWatch メトリクスの詳細については、「Amazon CloudWatch によるメトリクスのモニタリング」を参照してください。

Amazon S3 コンソール、AWS Command Line Interface (AWS CLI)、または Amazon S3 REST API を使用して、バケットにメトリクス設定を追加できます。

S3 コンソールの使用

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 左のナビゲーションペインで、[汎用バケット] を選択します。
3. バケットリストで、メトリクスをリクエストするオブジェクトが含まれるバケットの名前を選択します。
4. [Metrics] (メトリクス) タブをクリックします。
5. [バケットメトリクス] で、[その他のグラフを表示] をクリックします。
6. [リクエストメトリクス] タブをクリックします。
7. [フィルターの作成] をクリックします。
8. [フィルタ名] ボックスに、フィルタ名を入力します。

   名前には、文字、数字、ピリオド、ダッシュ、アンダースコアのみを使用できます。すべてのオブジェクトに適用されるフィルタには、名前 `EntireBucket` を使用することをお勧めします。
9. [フィルタ範囲] で、[このフィルタはバケット内のすべてのオブジェクトに適用されます] を選択します。

   フィルタを定義することで、バケット内のオブジェクトのサブセットに関するメトリクスのみを収集してレポートすることもできます。詳細については、プレフィックス、オブジェクトタグ、またはアクセスポイントでのメトリクス設定の作成 を参照してください。
10. [Save changes] (変更の保存) をクリックします。
11. [リクエストメトリクス] タブの [フィルタ] で、作成したフィルタを選択します。

約 15 分後、CloudWatch はこれらのリクエストメトリクスの追跡を開始します。これらは、[リクエストメトリクス] タブで確認できます。メトリクスのグラフは、Amazon S3 または CloudWatch コンソールでレプリケーションメトリクスで表示できます。リクエストメトリクスには、CloudWatch の標準料金が課金されます。詳細については、Amazon CloudWatch の料金を参照してください。

REST API の使用

Amazon S3 REST API でメトリクス設定をプログラムで追加することもできます。メトリクス設定の追加と使用の詳細については、「Amazon Simple Storage Service API リファレンス」で以下のトピックを参照してください。

- PUT Bucket Metric Configuration
- GET Bucket Metric Configuration
- List Bucket Metric Configuration
- DELETE Bucket Metric Configuration

AWS CLI の使用

1. AWS CLI をインストールしてセットアップします。手順については、「AWS Command Line Interface ユーザーガイド」の「AWS CLI のインストール、更新、およびアンインストール」を参照してください。
2. ターミナルを開きます。
3. 以下のコマンドを実行してメトリクス設定を追加します。

```
aws s3api put-bucket-metrics-configuration --endpoint https://s3.us-
west-2.amazonaws.com --bucket bucket-name --id metrics-config-id --metrics-
configuration '{"Id":"metrics-config-id"}'
```

プレフィックス、オブジェクトタグ、またはアクセスポイントでのメトリクス設定の作成

Amazon S3 の Amazon CloudWatch メトリクスには、ストレージメトリクス、リクエストメトリクス、レプリケーションメトリクスの 3 種類があります。ストレージメトリクスは、1 日に 1 回レポートされ、すべてのお客様に追加料金なしで提供されます。リクエストメトリクスは、処理のレイ

テンシーの後に 1 分間隔で使用できます。リクエストメトリクスには、CloudWatch の標準料金が課金されます。コンソールで設定するか、Amazon S3 API を使用して、リクエストメトリクスを取得する必要があります。S3 レプリケーションメトリクス は、レプリケーション設定のレプリケーションルールの詳細なメトリクスを提供します。レプリケーションメトリクスを使って、保留中のバイト数、保留中のオペレーション、レプリケーションに失敗したオペレーション、レプリケーションのレイテンシーを追跡すると、レプリケーションの進行状況を 1 分単位でモニタリングできます。

Amazon S3 の CloudWatch メトリクスの詳細については、「Amazon CloudWatch によるメトリクスのモニタリング」を参照してください。

CloudWatch メトリクスを設定する場合、バケット内のすべてのオブジェクトに対してフィルタを作成することも、1 つのバケット内の関連オブジェクトのグループに設定をフィルタリングすることもできます。以下のフィルタタイプの 1 つ以上に基づいて、メトリクス設定に含めるバケット内のオブジェクトをフィルタリングできます。

- オブジェクトキー名のプレフィックス – Amazon S3 データモデルはフラット構造ですが、プレフィックスを使用して階層を推測できます。Amazon S3 コンソールはフォルダの概念でこれらのプレフィックスをサポートします。プレフィックスでフィルタリングした場合、同じプレフィックスを持つオブジェクトがメトリクス設定に含まれます。 プレフィックスの詳細については、プレフィックスを使用してオブジェクトを整理する を参照してください。
- タグ – オブジェクトにタグ (キー値と名前のペア) を追加できます。タグを使用すると、オブジェクトを簡単に検索および整理できます。メトリクス設定のフィルタとしてタグを使用することもできます。オブジェクトタグの詳細については、タグを使用してストレージを分類するを参照してください。
- アクセスポイント – S3 アクセスポイントは、バケットに接続され、S3 の共有データセットの大規模なデータアクセスの管理を簡素化する名前付きネットワークエンドポイントです。アクセスポイントフィルタを作成すると、Amazon S3 には、メトリクス設定で指定したアクセスポイントへのリクエストが含まれます。詳細については、汎用バケットのアクセスポイントのモニタリングとログ記録 を参照してください。

> **Note**
>
> アクセスポイントでフィルタリングするメトリクス設定を作成する場合は、アクセスポイントのエイリアスではなく、アクセスポイントの Amazon リソースネーム (ARN) を使用する必要があります。ARN は、特定のオブジェクトの ARN ではなく、アクセスポイント自体に使用してください。アクセスポイントの ARN の詳細については、「汎用バケットでの Amazon S3 アクセスポイントの使用」を参照してください。

フィルタを指定した場合、単一のオブジェクトで機能するリクエストのみがフィルタと一致し、報告されたメトリクスに含められます。DeleteObjects や ListObjects のリクエストは、フィルターによる設定のメトリクスを一切返しません。

より複雑なフィルタリングをリクエストするには、複数の工レメントを選択します。これらのすべての工レメントを持つオブジェクトのみがメトリクス設定に含められます。フィルタを設定しない場合、バケット内のすべてのオブジェクトがメトリクス設定に含められます。

S3 コンソールの使用

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 左のナビゲーションペインで、[汎用バケット] を選択します。
3. バケットリストで、メトリクスをリクエストするオブジェクトが含まれるバケットの名前を選択します。
4. [Metrics] (メトリクス) タブをクリックします。
5. [バケットメトリクス] で、[その他のグラフを表示] をクリックします。
6. [リクエストメトリクス] タブをクリックします。
7. [フィルターの作成] をクリックします。
8. [フィルタ名] ボックスに、フィルタ名を入力します。

   名前には、文字、数字、ピリオド、ダッシュ、アンダースコアのみを使用できます。
9. [フィルタの範囲] で、プレフィックス、オブジェクトタグ、S3 アクセスポイント、または 3 つすべての組み合わせを使用して、このフィルタの範囲を制限します。。
10. [フィルタのタイプで、フィルタタイプをプレフィックス、オブジェクトタグ、またはアクセスポイントから少なくとも 1 つ選択します。
11. [プレフィックス] ボックスにプレフィックスを入力して、プレフィックスフィルタを定義し、フィルタの範囲を単一のパスに制限します。
12. オブジェクトタグフィルタを定義するには、[オブジェクトタグ] で、[タグの追加] を選択し、タグのキーおよび値を入力します。
13. アクセスポイントフィルタを定義するには、[S3 アクセスポイント] フィールドに、アクセスポイント ARN を入力するか、[S3 を参照] を選択して、アクセスポイントに移動します。

> **Important**
>
> アクセスポイントのエイリアスは入力できません。特定のオブジェクトの ARN ではなく、アクセスポイント自体の ARN を入力する必要があります。

14. [Save changes] (変更の保存) をクリックします。

    Amazon S3 は、指定したプレフィックス、タグ、またはアクセスポイントを使用するフィルタを作成します。

15. [リクエストメトリクス] タブの [フィルタ] で、作成したフィルタを選択します。

    これで、リクエストメトリクスの範囲をプレフィックス、タグ、またはアクセスポイントで制限するフィルタが作成されました。CloudWatch がこれらのリクエストメトリクスの追跡を開始してから約 15 分後に、Amazon S3 コンソールと CloudWatch コンソールの両方でメトリクスのグラフを表示できるようになります。リクエストメトリクスには、CloudWatch の標準料金が課金されます。詳細については、Amazon CloudWatch の料金を参照してください。

    バケットレベルでリクエストメトリクスを設定することもできます。詳細については、「バケット内のすべてのオブジェクトに対する CloudWatch メトリクス設定を作成する」を参照してください。

AWS CLI の使用

1. AWS CLI をインストールしてセットアップします。手順については、「AWS Command Line Interface ユーザーガイド」の「AWS CLI のインストール、更新、およびアンインストール」を参照してください。
2. ターミナルを開きます。
3. 以下のコマンドを実行してメトリクス設定を追加します。

   Example : プレフィックスでフィルタリングするには

```
aws s3api put-bucket-metrics-configuration --bucket amzn-s3-demo-bucket --
id metrics-config-id --metrics-configuration '{"Id":"metrics-config-id", "Filter":
{"Prefix":"prefix1"}} '
```

Example : タグでフィルタリングするには

```
aws s3api put-bucket-metrics-configuration --bucket amzn-s3-demo-bucket --
id metrics-config-id --metrics-configuration '{"Id":"metrics-config-id", "Filter":
{"Tag": {"Key": "string", "Value": "string"}} '
```

Example : アクセスポイントでフィルタリングするには

```
aws s3api put-bucket-metrics-configuration --bucket amzn-s3-demo-bucket --
id metrics-config-id --metrics-configuration '{"Id":"metrics-config-id", "Filter":
{"AccessPointArn":"arn:aws:s3:Region:account-id:accesspoint/access-point-name"}} '
```

Example : プレフィックス、タグ、アクセスポイントでフィルタリングするには

```
aws s3api put-bucket-metrics-configuration --endpoint https://
s3.Region.amazonaws.com --bucket amzn-s3-demo-bucket --id metrics-config-id --
metrics-configuration '
{
    "Id": "metrics-config-id",
    "Filter": {
        "And": {
            "Prefix": "string",
            "Tags": [
                {
                    "Key": "string",
                    "Value": "string"
                }
            ],
            "AccessPointArn": "arn:aws:s3:Region:account-id:accesspoint/access-
point-name"
        }
    }
}'
```

REST API の使用

Amazon S3 REST API でメトリクス設定をプログラムで追加することもできます。メトリクス設定の追加と使用の詳細については、「Amazon Simple Storage Service API リファレンス」で以下のトピックを参照してください。

- PUT Bucket Metric Configuration
- GET Bucket Metric Configuration
- List Bucket Metric Configuration
- DELETE Bucket Metric Configuration

メトリクスフィルタの削除

Amazon CloudWatch リクエストメトリクスフィルタが不要になった場合は、削除できます。フィルタを削除すると、その特定のフィルタを使用するリクエストメトリクスに対して課金されなくなります。ただし、存在する他のフィルタ設定については、引き続き課金されます。

フィルタを削除すると、リクエストメトリクスにフィルタを使用できなくなります。フィルタを削除すると、元に戻すことはできません。

リクエストメトリクスフィルタの作成については、次のトピックを参照してください。

- バケット内のすべてのオブジェクトに対する CloudWatch メトリクス設定を作成する
- プレフィックス、オブジェクトタグ、またはアクセスポイントでのメトリクス設定の作成

S3 コンソールの使用

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 左のナビゲーションペインで、[汎用バケット] を選択します。
3. バケットリストで、リクエストメトリクスフィルタを削除するバケットの名前を選択します。
4. [Metrics] (メトリクス) タブをクリックします。
5. [バケットメトリクス] で、[その他のグラフを表示] をクリックします。
6. [Request metrics] (リクエストメトリクス) タブをクリックします。
7. [フィルタの管理] を選択します。
8. フィルタを選択します。

> **Important**
>
> フィルタを削除すると、元に戻すことはできません。

9. [削除] を選択します。

Amazon S3 によってフィルタが削除されます。

REST API の使用

Amazon S3 REST API でメトリクス設定をプログラムで追加することもできます。メトリクス設定の追加と使用の詳細については、「Amazon Simple Storage Service API リファレンス」で以下のトピックを参照してください。

- PUT Bucket Metric Configuration
- GET Bucket Metric Configuration
- List Bucket Metric Configuration
- DELETE Bucket Metric Configuration

Amazon S3 イベント通知

Amazon S3 イベント通知機能を使用して、S3 バケットで特定のイベントが発生したときに通知を受け取ることができます。通知を有効にするには、Amazon S3 から発行するイベントを識別する通知設定を追加します。Amazon S3 から通知を送信する宛先も指定されていることを確認してください。この設定は、バケットに関連付けられた通知サブリソースに保存します 詳細については、汎用バケットの設定オプション を参照してください。Amazon S3 では、このサブリソースを管理するための API も利用できます。

> **Important**
>
> Amazon S3 イベント通知は、少なくとも 1 回配信されるように設計されています。通常、イベント通知は数秒で配信されますが、1 分以上かかる場合もあります。

Amazon S3 イベント通知の概要。

現在、Amazon S3 は次のイベントの通知を発行できます。

- 新しいオブジェクトの作成イベント
- オブジェクトの削除イベント
- オブジェクトイベントの復元

- 低冗長化ストレージ (RRS) オブジェクトの紛失イベント
- レプリケーションイベント
- S3 ライフサイクルの有効期限イベント
- S3 ライフサイクルの移行イベント
- S3 Intelligent-Tiering 自動アーカイブイベント
- オブジェクトのタグ付けイベント
- オブジェクト ACL PUT イベント

サポートしたすべてのイベントタイプの詳細は、SQS、SNS、および Lambda でサポートされているイベントタイプ を参照してください。

Amazon S3 は、次の宛先にイベントの通知メッセージを送信できます。通知設定でこれらの送信先の Amazon リソースネーム (ARN) 値を指定します。

- Amazon Simple Notification Service (Amazon SNS) のトピック
- Amazon Simple Queue Service Amazon SQS キュー
- AWS Lambda 関数
- Amazon EventBridge

詳細については、「サポートされているイベントの送信先」を参照してください。

> **Note**
>
> Amazon Simple キューサービス FIFO (先入れ先出し) キューは、Amazon S3 イベント通知の送信先としてサポートされていません。Amazon S3 イベントの通知を Amazon SQS FIFO キューに送信するには、Amazon EventBridge を使用できます。詳細については、「Amazon EventBridge を有効にします」を参照してください。

> **Warning**
>
> 通知が通知をトリガーするのと同じバケットに書き込むと、実行ループが発生する可能性があります。例えば、オブジェクトがアップロードされるたびにバケットで Lambda 関数をトリガーし、その関数によってオブジェクトがバケットにアップロードされると、その関数によって間接的にその関数自体がトリガーされます。これを回避するには、2 つのバケット

を使用するか、受信オブジェクトで使用されるプレフィックスにのみ適用されるようにトリガーを設定します。
AWS Lambda で Amazon S3 通知を使用する方法の詳細と例については、「AWS Lambda デベロッパーガイド」の「AWS Lambda を Amazon S3 に使用する」を参照してください。

バケットごとに作成できるイベント通知設定数の詳細については、AWS 全般のリファレンスの「Amazon S3 サービスクォータ」を参照してください。

イベント通知の詳細については、以下のセクションを参照してください。

トピック

- イベント通知のタイプおよび送信先
- Amazon SQS、Amazon SNS、Lambda を使用します
- EventBridge の使用

イベント通知のタイプおよび送信先

Amazon S3 では、通知を発行できるいくつかのイベント通知のタイプと送信先がサポートされています。イベント通知を設定するときに、イベントタイプと送信先を指定できます。各イベント通知に指定できる送信先は 1 つだけです。Amazon S3 イベント通知は、通知メッセージごとに 1 つのイベントエントリを送信します。

トピック

- サポートされているイベントの送信先
- SQS、SNS、および Lambda でサポートされているイベントタイプ
- Amazon EventBridge でサポートされているイベントタイプ。
- イベントの順序付けと重複イベント

サポートされているイベントの送信先

Amazon S3 は、次の宛先にイベントの通知メッセージを送信できます。

- Amazon Simple Notification Service (Amazon SNS)のトピック
- Amazon Simple Queue Service Amazon SQS キュー
- AWS Lambda

- Amazon EventBridge

ただし、各イベント通知に指定できる送信先タイプは 1 つだけです。

> **Note**
>
> Amazon SNS トピックまたは Amazon SQS キューにメッセージを投稿するには、Amazon S3 のアクセス許可を付与する必要があります。また、ユーザーに代わって AWS Lambda 関数を呼び出すためにも Amazon S3 の許可を付与する必要があります。これらの許可を付与する方法については、宛先にイベント通知メッセージを発行するアクセス許可の付与 を参照してください。

Amazon SNS トピック

Amazon SNS は、柔軟性に優れたフルマネージド型のプッシュメッセージングサービスです。このサービスを使用すると、モバイルデバイスまたは配信サービスにメッセージを配信できます。SNS で 一度メッセージを送信すると、1 回または複数回配信できます。現在 、 標準 SNS は S3 イベント通知の宛先としてのみ許可されていますが、SNS FIFO は許可されていません。

Amazon SNS は承認エンドポイントやクライアントへのメッセージの配信または送信の調整と管理を行います。Amazon SNS コンソールを使用して、通知の送信先にする Amazon SNS トピックを作成できます。

トピックは、Amazon S3 バケットと同じ AWS リージョンにある必要があります。Amazon SNS トピックの作成方法の詳細については、Amazon Simple Notification Service デベロッパーガイドの Amazon SNS の開始方法および Amazon SNS のよくある質問 を参照してください。

イベント通知宛先として作成した Amazon SNS トピックを使用するには、以下のものが必要です。

- Amazon SNS トピックの Amazon リソースネーム (ARN)
- 有効な Amazon SNS トピックサブスクリプション。これにより、Amazon SNS トピックにメッセージが公開されると、トピックのサブスクライバーに通知されます。

Amazon SQS キュー

Amazon SQS には、コンピュータ間で送受信されるメッセージを格納するための、信頼性の高いスケーラブルなホストされたキューが用意されています。Amazon SQS を使用すると、どのような量

のデータでも転送することができ、他のサービスが常に利用可能である必要もありません。Amazon SQS コンソールを使用すると、通知の送信先にする Amazon SQS キューを作成できます。

Amazon SQS キューは、Amazon S3 バケットと同じ AWS リージョン に存在する必要があります。Amazon SQS キューの作成方法の説明は、「Amazon Simple Queue Service デベロッパーガイド」の「Amazon Simple Queue Service とは」および「Amazon SQS の開始方法」を参照してください。

イベント通知の送信先として Amazon SQS キューを使用するには、以下が必要です。

- Amazon SQS キューの Amazon リソースネーム (ARN)

> **Note**
>
> Amazon Simple キューサービス FIFO (先入れ先出し) キューは、Amazon S3 イベント通知の送信先としてサポートされていません。Amazon S3 イベントの通知を Amazon SQS FIFO キューに送信するには、Amazon EventBridge を使用できます。詳細については、「Amazon EventBridge を有効にします」を参照してください。

Lambda 関数

AWS Lambda を使用して、AWS の他のサービスをカスタムロジックで拡張したり、AWS のスケール、パフォーマンス、セキュリティで動作する独自のバックエンドを作成したりすることができます。Lambda を使用すると、必要な場合にのみ実行される離散イベント駆動型アプリケーションを作成できます。また、これを使用して、これらのアプリケーションを 1 日数回のリクエストから 1 秒あたり数千回のリクエストに自動的にスケーリングすることもできます。

Lambda は、Amazon S3 バケットイベントに応答してカスタムコードを実行できます。カスタムコードを Lambda にアップロードし、Lambda 関数と呼ばれるものを作成します。Amazon S3 は特定のタイプのイベントを検出すると、そのイベントを AWS Lambda に公開し、Lambda で関数を呼び出すことができます。それに応じて、Lambda が関数を実行します。例えば、検出される可能性のあるイベントタイプの 1 つは、オブジェクトで作成されたイベントです。

AWS Lambda コンソールを使用すると、AWS インフラストラクチャを使用してユーザーに代わってコードを実行する Lambda 関数を作成できます。Lambda 関数は S3 バケットと同じリージョンに存在する必要があります。Lambda 関数をイベント通知の送信先として設定するには、Lambda 関数の名前または ARN も必要になります。

> **Warning**
>
> 通知が通知をトリガーするのと同じバケットに書き込むと、実行ループが発生する可能性があります。例えば、オブジェクトがアップロードされるたびにバケットで Lambda 関数をトリガーし、その関数によってオブジェクトがバケットにアップロードされると、その関数によって間接的にその関数自体がトリガーされます。これを回避するには、2 つのバケットを使用するか、受信オブジェクトで使用されるプレフィックスにのみ適用されるようにトリガーを設定します。
>
> AWS Lambda で Amazon S3 通知を使用する方法の詳細と例については、「AWS Lambda デベロッパーガイド」の「AWS Lambda を Amazon S3 に使用する」を参照してください。

Amazon EventBridge

Amazon EventBridge はサーバーレスのイベントバスで、AWS サービスからのイベントを受信します。イベントに一致するルールを設定し、それらを AWS サービスや HTTP エンドポイントなどのターゲットに配信できます。詳細については、「Amazon EventBridge ユーザーガイド」の「Amazon EventBridge とは」を参照してください。

他の宛先とは異なり、バケットの EventBridge へのイベントの配信を有効または無効にすることができます。配信を有効にすると、すべてのイベントが EventBridge に送信されます。さらに、EventBridge ルールを使用して、イベントを追加のターゲットに送信することもできます。

SQS、SNS、および Lambda でサポートされているイベントタイプ

Amazon S3 は、次のタイプのイベントを発行できます。通知設定で、これらのイベントタイプを指定します。

イベントタイプ	説明
`s3:TestEvent`	通知が有効な場合、Amazon S3 はテスト通知を公開します これは、トピックが存在し、バケット所有者が指定されたトピックを公開する許可があることを保証するためです。 通知の有効化に失敗した場合、テスト通知を受信しません。
`s3:ObjectCreated:*`	PUT、POST、COPY などの Amazon S3 API オペレーションはオブジェクトを作成できます。これらのイベントタイプ

イベントタイプ	説明
s3:ObjectCreated:Put s3:ObjectCreated:Post s3:ObjectCreated:Copy s3:ObjectCreated:CompleteMultipartUpload	で、特定の API を使用してオブジェクトが作成されたときに通知を有効にできます。または、オブジェクトの作成に使用された API に関係なく、s3:ObjectCreated:* イベントタイプを使用して通知を要求できます。 s3:ObjectCreated:CompleteMultipartUpload には、コピーオペレーションの UploadPartCopy を使用して作成されたオブジェクトが含まれます。
s3:ObjectRemoved:* s3:ObjectRemoved:Delete s3:ObjectRemoved:DeleteMarkerCreated	ObjectRemoved イベントタイプを使用することで、オブジェクトまたはオブジェクトのバッチがバケットから削除されたときに通知を有効にできます。 s3:ObjectRemoved:Delete イベントタイプを使用することで、オブジェクトが削除されたとき、またはバージョニングが有効なオブジェクトが完全に削除されたときに通知が送信されるようにリクエストできます。その代わりに、s3:ObjectRemoved:DeleteMarkerCreated を使用することで、削除マーカーがバージョニング・オブジェクトを作成すると、通知が送信されるようにリクエストできます。バージョン管理されたオブジェクトを削除する方法については、バージョニングが有効なバケットからのオブジェクトバージョンの削除 を参照してください。ワイルドカードとして s3:ObjectRemoved:* を使用することで、オブジェクトが削除されるたびに通知が送信されるようにリクエストできます。 これらのイベント通知では、ライフサイクル設定や失敗したオペレーションから自動削除のアラートはありません。

イベントタイプ	説明
s3:ObjectRestore:* s3:ObjectRestore:Post s3:ObjectRestore:Completed s3:ObjectRestore:Delete	ObjectRestore イベントタイプを使用することで、S3 Glacier Flexible Retrieval ストレージクラス、S3 Glacier Deep Archive ストレージクラス、S3 Intelligent-Tiering アーカイブアクセス階層、および S3 Intelligent-Tiering Deep アーカイブアクセス階層からオブジェクトを復元するときに、開始および完了の通知を受け取ることができます。オブジェクトの復元されたコピーの有効期限が切れたときの通知を受け取ることもできます。 s3:ObjectRestore:Post イベントタイプは、オブジェクトの復元開始を通知します。s3:ObjectRestore:Completed イベントタイプは、復元完了を通知します。s3:ObjectRestore:Delete イベントタイプは、復元されたオブジェクトの一時コピーの有効期限が切れると通知します。
s3:ReducedRedundancyLostObject	この通知イベントは、Amazon S3 が RRS ストレージクラスのオブジェクトが失われたことを検出したときに受け取ります。

イベントタイプ	説明

`s3:Replication:*`
 	
`s3:Replication:OperationFailedReplication`
 	
`s3:Replication:OperationMissedThreshold`
 	
`s3:Replication:OperationReplicatedAfterThreshold`
 	
`s3:Replication:OperationNotTracked`
	`Replication` イベントタイプを使用すると、S3 レプリケーションメトリクスまたは S3 Replication Time Control (S3 RTC) が有効になっているレプリケーション構成の通知を受信できます。保留中のバイト数、保留中のオペレーション、およびレプリケーションのレイテンシーを追跡すると、レプリケーションイベントの進行状況を 1 分単位でモニタリングできます。レプリケーションメトリクスについては、「メトリクス、イベント通知、ステータスによるレプリケーションのモニタリング」をご参照ください。
	
	• `-s3:Replication:OperationFailedReplication` イベントタイプは、レプリケーションのターゲットであったオブジェクトがレプリケートに失敗したときに通知を受け取ります。
	• `s3:Replication:OperationMissedThreshold` イベントタイプは、S3 RTC を使用するレプリケーションの対象であったオブジェクトがレプリケーションの 15 分の閾値を超えたときに通知します。
	• `s3:Replication:OperationReplicatedAfterThreshold` イベントタイプは、S3 RTC を使用するレプリケーションの対象であったオブジェクトが 15 分の閾値を超えてレプリケートされたときに通知します。
	• `s3:Replication:OperationNotTracked` イベントタイプは、ライブレプリケーションの対象であったオブジェクト (同一リージョンレプリケーション [SRR] またはクロスリージョンレプリケーション [CRR]) がレプリケーションメトリクスによって追跡されなくなったときに通知します。

イベントタイプ	説明
s3:LifecycleExpiration:* s3:LifecycleExpiration:Delete s3:LifecycleExpiration:DeleteMarkerCreated	LifecycleExpiration イベントタイプを使用すると、Amazon S3 が S3 ライフサイクル設定に基づいてオブジェクトを削除したときに通知を受け取ることができます。 s3:LifecycleExpiration:Delete イベントタイプは、バージョン管理されていないバケット内のオブジェクトが削除されたときに通知します。また、S3 ライフサイクル設定によってオブジェクトバージョンが完全に削除された場合にも通知されます。s3:LifecycleExpiration:DeleteMarkerCreated イベントタイプは、バージョン対応バケット内のオブジェクトの現在のバージョンが削除されたときに S3 ライフサイクル が削除マーカーを作成したときに通知します。
s3:LifecycleTransition	この通知イベントは、S3 ライフサイクル設定によってオブジェクトが別の Amazon S3 ストレージクラスに移行されたときに受信されます。
s3:IntelligentTiering	この通知イベントは、S3 Intelligent-Tiering ストレージクラス内のオブジェクトがアーカイブアクセス層またはディープアーカイブアクセス層に移動したときに受信されます。
s3:ObjectTagging:* s3:ObjectTagging:Put s3:ObjectTagging:Delete	ObjectTagging イベントタイプを使用すると、オブジェクトタグがオブジェクトに追加またはオブジェクトから削除されたときに通知を有効にできます。 s3:ObjectTagging:Put イベントタイプは、タグがオブジェクトの PUT であるか、既存のタグが更新されたときに通知します。s3:ObjectTagging:Delete イベントタイプは、タグがオブジェクトから削除されたときに通知します。

イベントタイプ	説明
s3:ObjectAcl:Put	この通知イベントは、ACL がオブジェクトに PUT されたとき、または既存の ACL が変更されたときに受け取ります。リクエストによってオブジェクトの ACL が変更されない場合、イベントは生成されません。

Amazon EventBridge でサポートされているイベントタイプ。

Amazon S3 から Amazon EventBridge に送信するイベントタイプのリストについては、「EventBridge の使用」を参照してください。

イベントの順序付けと重複イベント

Amazon S3 イベント通知は、通知を少なくとも 1 回配信するように設計されていますが、イベントが発生したのと同じ順序で通知が受信されるとは限りません。まれに、Amazon S3 の再試行メカニズムによって、同じオブジェクトイベントに対して重複する S3 イベント通知が発生することがあります。重複イベントまたは順序が異なるイベント処理の詳細については、「AWS Storage Blog」の「Manage event ordering and duplicate events with Amazon S3 Event Notifications」を参照してください。

Amazon SQS、Amazon SNS、Lambda を使用します

通知の有効化は、バケットレベルのオペレーションです。バケットに関連付けられた 通知 サブリソースに通知設定情報が格納されます。通常、バケット通知設定を作成または変更してから、変更が有効になるまで通常 5 分かかります。通知が最初に有効になったとき、s3:TestEvent が発生します。次のいずれかの方法を使用して通知設定の管理を行います。

- Amazon S3 コンソールの使用 – コンソール UI では、コードを記述しなくても、バケットの通知設定を指定できます。詳細については、Amazon S3 コンソールを使用したイベント通知の有効化と設定 を参照してください。
- AWS SDK をプログラムで使用する – 内部的には、コンソールも SDK も Amazon S3 REST API を呼び出して、バケットに関連付けられた通知サブリソースを管理します。AWS SDK を使用した通知設定の例については、チュートリアル: 通知 (SNS トピックまたは SQS キュー) のバケットを設定する を参照してください。

> **Note**
>
> コードから直接 Amazon S3 REST API を呼び出すこともできます。しかし、そうするのはリクエストを認証するためのコードを作成する必要があるため面倒な場合もあります。

使用する方法を問わず、Amazon S3 は通知設定を XML として、バケットに関連付けられた 通知 サブリソースに保存します。バケットのサブリソースの詳細については、汎用バケットの設定オプション を参照してください。

> **Note**
>
> 削除された送信先が原因で複数の失敗したイベント通知を受け取った場合、削除しようとすると [以下の送信先設定を検証できません] と表示される場合があります。これは、S3 コンソールで失敗した通知をすべて同時に削除することで解決できます。

トピック

- 宛先にイベント通知メッセージを発行するアクセス許可の付与
- Amazon S3 コンソールを使用したイベント通知の有効化と設定
- プログラムによるイベント通知の設定
- チュートリアル: 通知 (SNS トピックまたは SQS キュー) のバケットを設定する
- オブジェクトキー名のフィルタリングを使用したイベント通知の設定
- イベントメッセージの構造

宛先にイベント通知メッセージを発行するアクセス許可の付与

Amazon S3 プリンシパルに、SNS トピック、SQS キュー、Lambda 関数へメッセージを公開する関連する API を呼び出すため必要なアクセス許可を付与する必要があります。これは、Amazon S3 がイベント通知メッセージを宛先に公開できるようにするためです。

イベント通知メッセージを送信先に公開する場合のトラブルシューティングについては、「Amazon S3 イベント通知を Amazon Simple Notification Service に公開するためのトラブルシューティング」トピックを参照してください。

トピック

- AWS Lambda 関数を呼び出すアクセス許可の付与
- SNS トピックまたは SQS キューにメッセージを発行するアクセス許可の付与

AWS Lambda 関数を呼び出すアクセス許可の付与

Amazon S3 は Lambda 関数を呼び出してイベントメッセージを AWS Lambda に発行し、イベントメッセージを引数として指定します。

Amazon S3 コンソールを使用して Lambda 関数の AmazonS3 バケットにイベント通知を設定すると、コンソールは Lambda 関数に必要なアクセス許可を設定します。これは、Amazon S3 がバケットから関数を呼び出す許可があるからです。詳細については、Amazon S3 コンソールを使用したイベント通知の有効化と設定 を参照してください。

AWS Lambda から Amazon S3 の許可を付与して、Lambda 関数を呼び出すこともできます。詳細については、AWS Lambda デベロッパーガイドのチュートリアル: Amazon S3 で AWS Lambda を使用するを参照してください。

SNS トピックまたは SQS キューにメッセージを発行するアクセス許可の付与

SNS トピックや SQS キューにメッセージを発行する許可を Amazon S3 に付与するには、AWS Identity and Access Management (IAM) ポリシーを宛先 SNS トピックや SQS キューにアタッチします。

SNS トピックや SQS キューにポリシーをアタッチする方法の例については、チュートリアル: 通知 (SNS トピックまたは SQS キュー) のバケットを設定する を参照してください。アクセス許可の詳細については、次のトピックを参照してください。

- 「Amazon Simple Notification Service デベロッパーガイド」の「Amazon SNS アクセスコントロールのケース例」
- 「Amazon Simple Queue サービスデベロッパーガイド」の「Amazon SQS での Identity and Access Management」

発行先 SNS トピックの IAM ポリシー

発行先の SNS トピックにアタッチする AWS Identity and Access Management (IAM) ポリシーの例を次に示します。このポリシーを使用してイベント通知の宛先 Amazon SNS トピックを設定する方法については、チュートリアル: 通知 (SNS トピックまたは SQS キュー) のバケットを設定する を参照してください。

```
{
    "Version": "2012-10-17",
    "Id": "example-ID",
    "Statement": [
        {
            "Sid": "Example SNS topic policy",
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": [
                "SNS:Publish"
            ],
            "Resource": "SNS-topic-ARN",
            "Condition": {
                "ArnEquals": {
                    "aws:SourceArn": "arn:aws:s3:::amzn-s3-demo-bucket"
                },
                "StringEquals": {
                    "aws:SourceAccount": "bucket-owner-account-id"
                }
            }
        }
    ]
}
```

発行先 SQS キューの IAM ポリシー

以下は、発行先 SQS キューにアタッチする IAM ポリシーの例です。このポリシーを使用してイベント通知の宛先 Amazon SQS キューを設定する方法については、チュートリアル: 通知 (SNS トピックまたは SQS キュー) のバケットを設定する を参照してください。

このポリシーを使用するには、Amazon SQS キューの ARN、バケット名、およびバケット所有者の AWS アカウント ID を更新する必要があります。

```
{
    "Version": "2012-10-17",
    "Id": "example-ID",
    "Statement": [
        {
            "Sid": "example-statement-ID",
            "Effect": "Allow",
```

```
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": [
                "SQS:SendMessage"
            ],
            "Resource": "arn:aws:sqs:Region:account-id:queue-name",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:s3:*:*:awsexamplebucket1"
                },
                "StringEquals": {
                    "aws:SourceAccount": "bucket-owner-account-id"
                }
            }
        }
    ]
}
```

Amazon SNS および Amazon SQS IAM ポリシーの両方について、StringLike 条件の代わりにポリシーで ArnLike 条件を指定できます。

ArnLike を使用する場合、ARN のパーティション、サービス、アカウント ID、リソースタイプ、および部分的なリソース ID 部分が、リクエストコンテキストの ARN と完全に一致する必要があります。部分一致が許可されるのは、リージョンとリソースパスのみです。

ArnLike の代わりに StringLike を使用すると、マッチングでは ARN 構造が無視され、ワイルドカードで指定された部分に関係なく部分一致が可能になります。詳細については、「IAM ユーザーガイド」の「IAM JSON のポリシー要素」を参照してください。

```
"Condition": {
  "StringLike": { "aws:SourceArn": "arn:aws:s3:*:*:amzn-s3-demo-bucket" }
  }
```

AWS KMS キーポリシー

SQS キューまたは SNS トピックが AWS Key Management Service (AWS KMS) カスタマーマネージドキーで暗号化されている場合は、暗号化されたトピックまたはキューを操作するための許可を Amazon S3 サービスプリンシパルに付与する必要があります。Amazon S3 サービスプリンシパルに許可を付与するには、カスタマーマネージドキーのキーポリシーに次のステートメントを追加します。

```
{
    "Version": "2012-10-17",
    "Id": "example-ID",
    "Statement": [
        {
            "Sid": "example-statement-ID",
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS KMS キーポリシーの詳細については、AWS Key Management Service デベロッパーガイドの AWS KMS でキーポリシーを使用する を参照してください。

Amazon SQS および Amazon SNS 用の AWS KMS でのサーバー側の暗号化の使用の詳細については、以下を参照してください。

- 「Amazon Simple Notification Service デベロッパーガイド」の「キー管理」。
- 「Amazon Simple Queue Service デベロッパーガイド」の「キー管理」。
- AWS KMS コンピューティングブログ の Encrypting messages published to Amazon SNS with AWS。

Amazon S3 コンソールを使用したイベント通知の有効化と設定

イベントが発生するたびに送信先へ通知メッセージを送信する特定の Amazon S3 汎用バケットイベントを有効にできます。このセクションでは、Amazon S3 コンソールを使用してイベント通知を有効にする方法について説明します。AWS SDK および Amazon S3 REST API でイベント通知を使用する方法については、プログラムによるイベント通知の設定 を参照してください。

前提条件: バケットのイベント通知を有効にするには、送信先タイプのいずれか 1 つを設定し、アクセス許可を設定する必要があります。詳細については、サポートされているイベントの送信先 および 宛先にイベント通知メッセージを発行するアクセス許可の付与 を参照してください。

> **Note**
>
> Amazon Simple キューサービス FIFO (先入れ先出し) キューは、Amazon S3 イベント通知の送信先としてサポートされていません。Amazon S3 イベントの通知を Amazon SQS FIFO キューに送信するには、Amazon EventBridge を使用できます。詳細については、「Amazon EventBridge を有効にします」を参照してください。

トピック

- Amazon S3 コンソールを使用して Amazon SNS、Amazon SQS、または Lambda 通知を有効にします。

Amazon S3 コンソールを使用して Amazon SNS、Amazon SQS、または Lambda 通知を有効にします。

S3 バケットのイベント通知を有効化および設定するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[汎用バケット] を選択します。
3. バケットリストで、イベントを有効にするバケットの名前を選択します。
4. [プロパティ] を選択します。
5. [Event Notifications (イベント通知)] セクションに移動し、[Create event notification (イベント通知の作成)] を選択します。
6. [General configuration (全般設定)] セクションで、イベント通知にわかりやすいイベント名を指定します。オプションで、プレフィックスとサフィックスを指定して、指定した文字で終わるキーを持つオブジェクトのみに通知を制限することもできます。

   a. [Event name (イベント名)] の説明を入力します。

      名前を入力しない場合は、グローバル一意識別子 (GUID) が生成され、名前に使用されます。

   b. (オプション) プレフィックスでイベント通知をフィルタリングするには、プレフィックスを入力します。

      例えば、特定のフォルダ (`images/` など) にファイルが追加されたときにのみ通知を受信するようにプレフィックスフィルタを設定できます。

c. (オプション) サフィックスでイベント通知をフィルタリングするには、サフィックスを入力します。

詳細については、オブジェクトキー名のフィルタリングを使用したイベント通知の設定 を参照してください。

7. イベントタイプセクションで、通知を受信する 1 つ以上のイベントタイプを選択します。

異なるイベントタイプのリスト化については、SQS、SNS、および Lambda でサポートされているイベントタイプ を参照してください。

8. [Destination (ターゲット)] セクションで、イベント通知の送信先を選択します。

> **Note**
>
> イベント通知を公開する前に、Amazon S3 プリンシパルが関連 API を呼び出すために必要なアクセス許可を付与する必要があります。これは、Lambda 関数、SNS トピック、または SQS キューに通知を発行できるようにするためです。

a. ターゲットタイプ ([Lambda Function (Lambda 関数)]、[SNS Topic (SNS トピック)]、または [SQS Queue (SQS キュー)]) を選択します。

b. ターゲットタイプを選択したら、リストから関数、トピック、またはキューを選択します。

c. または、Amazon リソースネーム (ARN) を指定する場合は、[Enter ARN (ARN を入力)] を選択して ARN を入力します。

詳細については、サポートされているイベントの送信先 を参照してください。

9. [Save Changes (変更の保存)] を選択すると、Amazon S3 がテストメッセージをイベント通知の送信先に送信します。

プログラムによるイベント通知の設定

デフォルトで、通知はどのタイプのイベントにも有効ではありません。したがって、通知サブリソースに最初は空の設定で格納されています。

```
<NotificationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
</NotificationConfiguration>
```

特定のタイプのイベントに対して通知を有効にするには、XML を、Amazon S3 がパブリッシュするイベントのタイプとパブリッシュ先を識別する適切な設定に置き換えます。各宛先には、対応する XML 設定を追加します。

イベントメッセージを SQS キューに発行するには

1 つ以上のイベントタイプの通知の送信先として SQS キューを設定するには、QueueConfiguration を追加します。

```
<NotificationConfiguration>
  <QueueConfiguration>
    <Id>optional-id-string</Id>
    <Queue>sqs-queue-arn</Queue>
    <Event>event-type</Event>
    <Event>event-type</Event>
     ...
  </QueueConfiguration>
   ...
</NotificationConfiguration>
```

イベントメッセージを SNS トピックに発行するには

特定のイベントタイプの通知の送信先として SNS トピックを設定するには、TopicConfiguration を追加します。

```
<NotificationConfiguration>
  <TopicConfiguration>
     <Id>optional-id-string</Id>
     <Topic>sns-topic-arn</Topic>
     <Event>event-type</Event>
     <Event>event-type</Event>
      ...
  </TopicConfiguration>
   ...
</NotificationConfiguration>
```

AWS Lambda 関数を呼び出し、イベントメッセージを引数として指定するには

特定のイベントタイプの通知の送信先として Lambda 関数を設定するには、CloudFunctionConfiguration を追加します。

```
<NotificationConfiguration>
```

```
   <CloudFunctionConfiguration>
      <Id>optional-id-string</Id>
      <CloudFunction>cloud-function-arn</CloudFunction>
      <Event>event-type</Event>
      <Event>event-type</Event>
       ...
   </CloudFunctionConfiguration>
    ...
</NotificationConfiguration>
```

バケットで設定されているすべての通知を削除するには

バケットに設定されたすべての通知を削除するには、notification サブリソースに空の <NotificationConfiguration/> エレメントを保存します。

Amazon S3 は、特定のタイプのイベントを検出すると、そのイベント情報を含むメッセージを発行します。詳細については、イベントメッセージの構造 を参照してください。

イベント通知の設定の詳細については、次のトピックを参照してください。

- チュートリアル: 通知 (SNS トピックまたは SQS キュー) のバケットを設定する.
- オブジェクトキー名のフィルタリングを使用したイベント通知の設定

チュートリアル: 通知 (SNS トピックまたは SQS キュー) のバケットを設定する

Amazon S3 通知は、Amazon Simple Notification Service (Amazon SNS) または Amazon Simple Queue Service (Amazon SQS) を使用して受信できます。このチュートリアルでは、Amazon SNS トピックと Amazon SQS キューを使用して、バケットに通知設定を追加します。

> **Note**
>
> Amazon Simple キューサービス FIFO (先入れ先出し) キューは、Amazon S3 イベント通知の送信先としてサポートされていません。Amazon S3 イベントの通知を Amazon SQS FIFO キューに送信するには、Amazon EventBridge を使用できます。詳細については、「Amazon EventBridge を有効にします」を参照してください。

トピック

- チュートリアルの概要

- ステップ 1: Amazon SQS キューを作成する
- ステップ 2: Amazon SNS トピックを作成する
- ステップ 3: 通知設定をバケットに追加する
- ステップ 4: セットアップをテストする

チュートリアルの概要

このチュートリアルは、以下を行う際に役立ちます。

- `s3:ObjectCreated:*` タイプのイベントを Amazon SQS キューに発行する。
- `s3:ReducedRedundancyLostObject` タイプのイベントを Amazon SNS トピックに発行する。

通知設定の情報については、Amazon SQS、Amazon SNS、Lambda を使用します を参照してください。

コンソールを使用して、コードを記述することなく、これらの手順をすべて実行できます。また、通知設定をプログラムで追加できるように、AWS SDK for Java および .NET を使用したコード例も用意されています。

この手順には、以下のステップが含まれます。

1. Amazon SQS キュー を作成する。

   Amazon SQS コンソールを使用して、SQS キューを作成します。Amazon S3 がそのキューにプログラムで送信するどのメッセージにもアクセスできます。ただし、このチュートリアルでは、コンソールで通知メッセージを確認します。

   キューにアクセスポリシーをアタッチして、メッセージを発行するための Amazon S3 アクセス許可を付与します。
2. Amazon SNS トピックを作成する。

   Amazon SNS コンソールを使用して、SNS トピックを作成し、トピックにサブスクライブします。これにより、そこに投稿されたすべてのイベントが配信されます。通信プロトコルとして E メールを指定します。トピックを作成すると、Amazon SNS から E メールが送信されます。E メール内のリンクを使用して、トピックのサブスクリプションを確認します。

   トピックにアクセスポリシーをアタッチして、メッセージを発行するための Amazon S3 アクセス許可を付与します。

3. 通知設定をバケットに追加します。

ステップ 1: Amazon SQS キューを作成する

次の手順に従い、Amazon Simple Queue Service (Amazon SQS) キューを作成し、このキューにサブスクライブします。

1. Amazon SQS コンソールを使用して、キューを作成します。手順については、「Amazon Simple Queue Service デベロッパーガイド」の「Getting Started with Amazon SQS」を参照してください。
2. キューに添付したアクセスポリシーを次のポリシーに置き換えます。

   a. Amazon SQS コンソールの [Queues] (キュー) リストで、キューの名前を選択します。

   b. [Access policy] (アクセスポリシー) タブで [Edit] (編集) をクリックします。

   c. キューに添付されているアクセスポリシーを置き換えます。その中で、Amazon SQS ARN、ソースバケット名、バケット所有者アカウント ID を提供します。

```
{
    "Version": "2012-10-17",
    "Id": "example-ID",
    "Statement": [
        {
            "Sid": "example-statement-ID",
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": [
                "SQS:SendMessage"
            ],
            "Resource": "SQS-queue-ARN",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:s3:*:*:awsexamplebucket1"
                },
                "StringEquals": {
                    "aws:SourceAccount": "bucket-owner-account-id"
                }
            }
        }
    ]
```

```
}
```

d. [保存] を選択します。

3. (オプション) Amazon SQS キューまたは Amazon SNS トピックで、AWS Key Management Service (AWS KMS) によるサーバー側の暗号化が有効になっている場合は、次のポリシーを関連する対称暗号化カスタマーマネージドキーに追加します。

   Amazon SQS または Amazon SNS 用の AWS マネージドキーは変更できないため、カスタマーマネージドキーにポリシーを追加する必要があります。

```
{
    "Version": "2012-10-17",
    "Id": "example-ID",
    "Statement": [
        {
            "Sid": "example-statement-ID",
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "*"
        }
    ]
}
```

   AWS KMS で Amazon SQS および Amazon SNS で SSE を使用する方法の詳細については、以下を参照してください。

   - 「Amazon Simple Notification Service デベロッパーガイド」の「Key management」。
   - 「Amazon Simple Queue Service デベロッパーガイド」の「Key management」。

4. キューの ARN を書き留めます。

   作成した SQS キューは、AWS アカウント 内の別のリソースです。固有の Amazon リソースネーム (ARN) があります。この ARN は次のステップで必要になります。ARN の形式は次のとおりです。

```
arn:aws:sqs:aws-region:account-id:queue-name
```

ステップ 2: Amazon SNS トピックを作成する

手順に従って、Amazon SNS トピックを作成してサブスクライブします。

1. Amazon SNS コンソールを使用してトピックを作成します。詳細については、「Amazon Simple Notification Service デベロッパーガイド」の「Creating an Amazon SNS topic」を参照してください。
2. トピックを受信します。この演習では、通信プロトコルとしてメールを使用します。手順については、Amazon Simple Notification Service デベロッパーガイドの Amazon SNS トピックへのサブスクライブを参照してください。

   トピックのサブスクリプションの確認を求めるメールがお客様宛てに送信されます。サブスクリプションを確認します。
3. トピックにアタッチされたアクセスポリシーを次のポリシーに置き換えます。その中で、SNS トピックの ARN、バケット名、バケット所有者のアカウント ID を提供します。

```
{
    "Version": "2012-10-17",
    "Id": "example-ID",
    "Statement": [
        {
            "Sid": "Example SNS topic policy",
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": [
                "SNS:Publish"
            ],
            "Resource": "SNS-topic-ARN",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:s3:*:*:amzn-s3-demo-bucket"
                },
                "StringEquals": {
                    "aws:SourceAccount": "bucket-owner-account-id"
                }
```

```
            }
        }
    ]
}
```

4. トピックの ARN を書き留めておきます。

   作成した SNS トピックは、AWS アカウント内の別のリソースであり、一意の ARN があります。この ARN は次のステップで必要になります。ARN は次のような形式になります。

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

ステップ 3: 通知設定をバケットに追加する

Amazon S3 コンソールを使用するか、プログラムで AWS SDK を使用して、バケットの通知を有効にすることができます。バケットでの通知を設定するオプションのいずれかを選択します。このセクションでは、AWS SDK for Java および .NET を使用するコード例を示します。

オプション A: コンソールを使用してバケットの通知を有効にする

Amazon S3 コンソールを使用して、Amazon S3 に次のアクションをリクエストする通知設定を追加します。

- [All object create events (すべてのオブジェクト作成イベント)] タイプのイベントを Amazon SQS キューに発行する。
- [Object in RRS lost (RRS オブジェクトの紛失)] タイプのイベントを Amazon SNS トピックに発行する。

通知設定を保存すると、Amazon S3 からテストメッセージが発行され、このメッセージが E メールで送信されます。

手順については、Amazon S3 コンソールを使用したイベント通知の有効化と設定 を参照してください。

オプション B: AWS SDK を使用してバケットの通知を有効にする

.NET

次の C# のコード例では、バケットに通知設定を追加する完全なコードのリストを示します。コードを更新して、バケット名と SNS トピックの ARN を提供する必要があります。コード例

を設定および実行する方法の詳細については、「AWS SDK for .NET デベロッパーガイド」の「AWS SDK for .NET の開始方法」を参照してください。

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Collections.Generic;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class EnableNotificationsTest
    {
        private const string bucketName = "*** bucket name ***";
        private const string snsTopic = "*** SNS topic ARN ***";
        private const string sqsQueue = "*** SQS topic ARN ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 client;

        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            EnableNotificationAsync().Wait();
        }

        static async Task EnableNotificationAsync()
        {
            try
            {
               PutBucketNotificationRequest request = new
 PutBucketNotificationRequest
                {
                    BucketName = bucketName
                };

                TopicConfiguration c = new TopicConfiguration
                {
                    Events = new List<EventType> { EventType.ObjectCreatedCopy },
                    Topic = snsTopic
                };
```

```
                request.TopicConfigurations = new List<TopicConfiguration>();
                request.TopicConfigurations.Add(c);
                request.QueueConfigurations = new List<QueueConfiguration>();
                request.QueueConfigurations.Add(new QueueConfiguration()
                {
                    Events = new List<EventType> { EventType.ObjectCreatedPut },
                    Queue = sqsQueue
                });

                PutBucketNotificationResponse response = await
 client.PutBucketNotificationAsync(request);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' ",
 e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown error encountered on server.
 Message:'{0}' ", e.Message);
            }
        }
    }
}
```

Java

次の例では、バケットに通知設定を追加する方法を示します。作業サンプルの作成方法およびテスト方法については、「AWS SDK for Java のデベロッパーガイド」の「使用開始」を参照してください。

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.*;

import java.io.IOException;
import java.util.EnumSet;
```

```
public class EnableNotificationOnABucket {

    public static void main(String[] args) throws IOException {
        String bucketName = "*** Bucket name ***";
        Regions clientRegion = Regions.DEFAULT_REGION;
        String snsTopicARN = "*** SNS Topic ARN ***";
        String sqsQueueARN = "*** SQS Queue ARN ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();
            BucketNotificationConfiguration notificationConfiguration = new
 BucketNotificationConfiguration();

            // Add an SNS topic notification.
            notificationConfiguration.addConfiguration("snsTopicConfig",
                    new TopicConfiguration(snsTopicARN,
 EnumSet.of(S3Event.ObjectCreated)));

            // Add an SQS queue notification.
            notificationConfiguration.addConfiguration("sqsQueueConfig",
                    new QueueConfiguration(sqsQueueARN,
 EnumSet.of(S3Event.ObjectCreated)));

            // Create the notification configuration request and set the bucket
 notification
            // configuration.
            SetBucketNotificationConfigurationRequest request = new
 SetBucketNotificationConfigurationRequest(
                    bucketName, notificationConfiguration);
            s3Client.setBucketNotificationConfiguration(request);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
```

```
}
```

ステップ 4: セットアップをテストする

さて、バケットにオブジェクトをアップロードしたり、Amazon SQS コンソールのイベント通知を検証することでセットアップをテストできます。手順については、Amazon Simple Queue Service デベロッパーガイドの開始方法」セクションのメッセージの受信を参照してください。

オブジェクトキー名のフィルタリングを使用したイベント通知の設定

Amazon S3 イベント通知を設定する場合、Amazon S3 による通知の送信をトリガーするサポートターゲットの Amazon S3 イベントタイプを指定する必要があります。指定しなかったイベントタイプが S3 バケットで発生しても、Amazon S3 は通知を送信しません。

通知がオブジェクトのキー名のプレフィックスまたはサフィックスでフィルタリングされるように設定できます。例えば、ファイル名の拡張子が `.jpg` であるイメージファイルがバケットに追加されたときにのみ、通知が送信されるように設定できます。または、「`images/`」というプレフィックスの付いたオブジェクトがバケットに追加されたときに Amazon SNS トピックに通知が送信されるように設定し、同じバケット内にある「`logs/`」というプレフィックスの付いたオブジェクトの通知が AWS Lambda 関数に渡されるようにすることができます。

> **Note**
>
> ワイルドカード文字 (「*」) は、フィルタでプレフィックスまたはサフィックスとして使用することはできません。プレフィックスまたはサフィックスにスペースが含まれている場合は、それを「+」文字に置き換える必要があります。プレフィックスまたはサフィックスの値に他の特殊文字を使用する場合は、URL エンコード (パーセントエンコード) 形式で入力する必要があります。イベント通知のプレフィックスまたはサフィックスに使用する場合で、URL エンコード形式に変換する必要がある特殊文字の一覧については、「セーフ文字」を参照してください。

Amazon S3 コンソールでオブジェクトキー名フィルタリングを使用する通知設定を設定できます。これを行うには、AWS SDK または REST API を介して、Amazon S3 API を直接使用します。コンソール UI を使用してバケットの通知設定をセットアップする方法については、Amazon S3 コンソールを使用したイベント通知の有効化と設定 を参照してください。

Amazon S3 は、「Amazon SQS、Amazon SNS、Lambda を使用します」で説明されているように、バケットに関連付けられている notification サブリソースに通知設定を XML 形式で保存します。`Filter` XML 構造を使用して、オブジェクトキー名のプレフィックスまたはサフィックスでフィルタして通知のルールを定義します。`Filter` XML 構造の詳細については、Amazon Simple Storage Service API リファレンスの PUT Bucket 通知 を参照してください。

`Filter` を使用する通知設定では、プレフィックスの重複、サフィックスの重複、またはプレフィックスとサフィックスの重複があるフィルタリングルールを定義できません。以下のセクションでは、オブジェクトキー名フィルタリングを使用した有効な通知設定の例を示します。プレフィックス/サフィックスが重複しているために無効である通知設定の例も示します。

トピック

- オブジェクトキー名によるフィルタ処理を使用した有効な通知設定の例
- 無効なプレフィックスやサフィックスの重複がある通知設定の例。

オブジェクトキー名によるフィルタ処理を使用した有効な通知設定の例

次の通知設定には、Amazon SQS キューを識別するキュー設定が含まれており、これにより Amazon S3 は `s3:ObjectCreated:Put` タイプのイベントを発行できます。イベントは、`images/` のプレフィックスと `jpg` サフィックスの付いたオブジェクトがバケットに PUT されるたびに発行されます。

```
<NotificationConfiguration>
  <QueueConfiguration>
      <Id>1</Id>
      <Filter>
          <S3Key>
              <FilterRule>
                  <Name>prefix</Name>
                  <Value>images/</Value>
              </FilterRule>
              <FilterRule>
                  <Name>suffix</Name>
                  <Value>jpg</Value>
              </FilterRule>
          </S3Key>
      </Filter>
      <Queue>arn:aws:sqs:us-west-2:444455556666:s3notificationqueue</Queue>
      <Event>s3:ObjectCreated:Put</Event>
  </QueueConfiguration>
```

```
</NotificationConfiguration>
```

次の通知設定には、複数の重複していないプレフィックスがあります。この設定では、images/ フォルダ内の PUT リクエストの通知を queue-A に送信し、logs/ フォルダ内の PUT リクエストの通知を queue-B に送信するように定義しています。

```
<NotificationConfiguration>
  <QueueConfiguration>
     <Id>1</Id>
     <Filter>
            <S3Key>
                <FilterRule>
                    <Name>prefix</Name>
                    <Value>images/</Value>
                </FilterRule>
            </S3Key>
     </Filter>
     <Queue>arn:aws:sqs:us-west-2:444455556666:sqs-queue-A</Queue>
     <Event>s3:ObjectCreated:Put</Event>
  </QueueConfiguration>
  <QueueConfiguration>
     <Id>2</Id>
     <Filter>
            <S3Key>
                <FilterRule>
                    <Name>prefix</Name>
                    <Value>logs/</Value>
                </FilterRule>
            </S3Key>
     </Filter>
     <Queue>arn:aws:sqs:us-west-2:444455556666:sqs-queue-B</Queue>
     <Event>s3:ObjectCreated:Put</Event>
  </QueueConfiguration>
</NotificationConfiguration>
```

次の通知設定には、複数の重複していないサフィックスがあります。この設定では、バケットに新しく追加される .jpg イメージは Lambda の cloud-function-A によって処理され、新しく追加される .png イメージは cloud-function-B によって処理されるように定義されています。.png と .jpg は、末尾の 1 文字が同じであっても、重複していると見なされません。文字列が両方のサフィックスで終わる可能性がある場合には、2 つのサフィックスは、重複していると見なされます。文字列が

.png と .jpg の両方で終わることはないので、この設定例の 2 つのサフィックスは重複していません。

```
<NotificationConfiguration>
  <CloudFunctionConfiguration>
     <Id>1</Id>
     <Filter>
            <S3Key>
                <FilterRule>
                    <Name>suffix</Name>
                    <Value>.jpg</Value>
                </FilterRule>
            </S3Key>
     </Filter>
     <CloudFunction>arn:aws:lambda:us-west-2:444455556666:cloud-function-A</
CloudFunction>
     <Event>s3:ObjectCreated:Put</Event>
  </CloudFunctionConfiguration>
  <CloudFunctionConfiguration>
     <Id>2</Id>
     <Filter>
            <S3Key>
                <FilterRule>
                    <Name>suffix</Name>
                    <Value>.png</Value>
                </FilterRule>
            </S3Key>
     </Filter>
     <CloudFunction>arn:aws:lambda:us-west-2:444455556666:cloud-function-B</
CloudFunction>
     <Event>s3:ObjectCreated:Put</Event>
  </CloudFunctionConfiguration>
</NotificationConfiguration>
```

Filter を使用する通知設定では、同じイベントタイプのプレフィックスが重複するフィルタリングルールを定義できません。重複しないサフィックスと一緒に使用される重複するプレフィックスがある場合にのみ、そうすることができます。次の設定例は、プレフィックスは重複しており、サフィックスは重複していないオブジェクトがどのように別々の場所に送られるかを示しています。

```
<NotificationConfiguration>
  <CloudFunctionConfiguration>
     <Id>1</Id>
```

```
     <Filter>
            <S3Key>
                <FilterRule>
                    <Name>prefix</Name>
                    <Value>images</Value>
                </FilterRule>
                <FilterRule>
                    <Name>suffix</Name>
                    <Value>.jpg</Value>
                </FilterRule>
            </S3Key>
     </Filter>
     <CloudFunction>arn:aws:lambda:us-west-2:444455556666:cloud-function-A</
CloudFunction>
     <Event>s3:ObjectCreated:Put</Event>
  </CloudFunctionConfiguration>
  <CloudFunctionConfiguration>
     <Id>2</Id>
     <Filter>
            <S3Key>
                <FilterRule>
                    <Name>prefix</Name>
                    <Value>images</Value>
                </FilterRule>
                <FilterRule>
                    <Name>suffix</Name>
                    <Value>.png</Value>
                </FilterRule>
            </S3Key>
     </Filter>
     <CloudFunction>arn:aws:lambda:us-west-2:444455556666:cloud-function-B</
CloudFunction>
     <Event>s3:ObjectCreated:Put</Event>
  </CloudFunctionConfiguration>
</NotificationConfiguration>
```

無効なプレフィックスやサフィックスの重複がある通知設定の例。

ほとんどの場合、Filter を使用する通知構成では、同じイベントタイプのプレフィックス、サフィックス、またはプレフィックスとサフィックスの組み合わせが重複するフィルタのルールを定義できません。サフィックスが重複していなければ、プレフィックスが重複していても問題ありません。例については、オブジェクトキー名のフィルタリングを使用したイベント通知の設定 を参照してください。

イベントタイプが異なれば、重複しているオブジェクトキー名フィルタを使用できます。例えば、image/ イベントタイプにプレフィックス ObjectCreated:Put と image/ イベントタイプにプレフィックス ObjectRemoved:* を使用する通知設定を作成できます。

Amazon S3 コンソールまたは API の使用時に、同じイベントタイプに対して名前が重複する無効なフィルタを使用する通知設定を保存しようとすると、エラーが発生します。このセクションでは、重複する名前のフィルタにより、無効である通知設定の例を示します。

既存の通知構成ルールには、他のプレフィックスとサフィックスとそれぞれ一致するデフォルトのプレフィックスとサフィックスがあると想定されます。次の通知設定は、重複するプレフィックスがあるために無効です。具体的には、ルートプレフィックスが他のプレフィックスと重複します。この例のように、プレフィックスではなくサフィックスを使用するのも true です。ルートサフィックスが他のサフィックスと重複します。

```
<NotificationConfiguration>
     <TopicConfiguration>
         <Topic>arn:aws:sns:us-west-2:444455556666:sns-notification-one</Topic>
         <Event>s3:ObjectCreated:*</Event>
    </TopicConfiguration>
    <TopicConfiguration>
         <Topic>arn:aws:sns:us-west-2:444455556666:sns-notification-two</Topic>
         <Event>s3:ObjectCreated:*</Event>
         <Filter>
             <S3Key>
                 <FilterRule>
                     <Name>prefix</Name>
                     <Value>images</Value>
                 </FilterRule>
            </S3Key>
        </Filter>
    </TopicConfiguration>
</NotificationConfiguration>
```

次の通知設定は、重複するサフィックスがあるために無効です。文字列が両方のサフィックスで終わる可能性がある場合には、2 つのサフィックスは、重複していると見なされます。文字列は jpg とpg で終わることができます。したがって、サフィックスは重なり合います。プレフィックスについても同様です。文字列が両方のプレフィックスで始まる可能性があれば、2 つのプレフィックスは重複していると見なされます。

```
 <NotificationConfiguration>
     <TopicConfiguration>
```

```
        <Topic>arn:aws:sns:us-west-2:444455556666:sns-topic-one</Topic>
        <Event>s3:ObjectCreated:*</Event>
        <Filter>
            <S3Key>
                <FilterRule>
                    <Name>suffix</Name>
                    <Value>jpg</Value>
                </FilterRule>
           </S3Key>
        </Filter>
    </TopicConfiguration>
    <TopicConfiguration>
        <Topic>arn:aws:sns:us-west-2:444455556666:sns-topic-two</Topic>
        <Event>s3:ObjectCreated:Put</Event>
        <Filter>
            <S3Key>
                <FilterRule>
                    <Name>suffix</Name>
                    <Value>pg</Value>
                </FilterRule>
           </S3Key>
        </Filter>
    </TopicConfiguration>
</NotificationConfiguration
```

次の通知設定は、重複するプレフィックスとサフィックスがあるために無効です。

```
<NotificationConfiguration>
     <TopicConfiguration>
        <Topic>arn:aws:sns:us-west-2:444455556666:sns-topic-one</Topic>
        <Event>s3:ObjectCreated:*</Event>
        <Filter>
            <S3Key>
                <FilterRule>
                    <Name>prefix</Name>
                    <Value>images</Value>
                </FilterRule>
                <FilterRule>
                    <Name>suffix</Name>
                    <Value>jpg</Value>
                </FilterRule>
           </S3Key>
        </Filter>
```

```
    </TopicConfiguration>
    <TopicConfiguration>
         <Topic>arn:aws:sns:us-west-2:444455556666:sns-topic-two</Topic>
         <Event>s3:ObjectCreated:Put</Event>
         <Filter>
             <S3Key>
                 <FilterRule>
                     <Name>suffix</Name>
                     <Value>jpg</Value>
                 </FilterRule>
            </S3Key>
        </Filter>
    </TopicConfiguration>
</NotificationConfiguration>
```

イベントメッセージの構造

Amazon S3 がイベントを発行するために送信する通知メッセージは JSON 形式です。

イベント通知の設定に関する一般的な概要と手順については、Amazon S3 イベント通知 を参照してください。

次の例は、イベント通知 JSON 構造体のバージョン 2.2 を示します。Amazon S3 は、このイベント構造体のバージョン 2.1 、 2.2 、 2.3 を使用します。Amazon S3 は、クロスリージョンレプリケーションイベント通知にバージョン 2.2 を使用します。S3 ライフサイクル、S3 Intelligent-Tiering、オブジェクト ACL、オブジェクトのタグ付け、オブジェクトの復元削除イベントにバージョン 2.3 を使用します。これらのバージョンには、これらのオペレーションに固有の追加情報が含まれています。バージョン 2.2 および 2.3 は、バージョン 2.1 と互換性があり、Amazon S3 が現在すべてのイベント通知タイプで使用されています。

```
{
   "Records":[
      {
         "eventVersion":"2.2",
         "eventSource":"aws:s3",
         "awsRegion":"us-west-2",
         "eventTime":"The time, in ISO-8601 format, for example,
 1970-01-01T00:00:00.000Z, when Amazon S3 finished processing the request",
         "eventName":"event-type",
         "userIdentity":{
            "principalId":"Amazon-customer-ID-of-the-user-who-caused-the-event"
         },
```

```
        "requestParameters":{
           "sourceIPAddress":"ip-address-where-request-came-from"
        },
        "responseElements":{
           "x-amz-request-id":"Amazon S3 generated request ID",
           "x-amz-id-2":"Amazon S3 host that processed the request"
        },
        "s3":{
           "s3SchemaVersion":"1.0",
           "configurationId":"ID found in the bucket notification configuration",
           "bucket":{
              "name":"amzn-s3-demo-bucket",
              "ownerIdentity":{
                 "principalId":"Amazon-customer-ID-of-the-bucket-owner"
              },
              "arn":"bucket-ARN"
           },
           "object":{
              "key":"object-key",
              "size":"object-size in bytes",
              "eTag":"object eTag",
              "versionId":"object version if bucket is versioning-enabled, otherwise
 null",
              "sequencer": "a string representation of a hexadecimal value used to
 determine event sequence, only used with PUTs and DELETEs"
           }
        },
        "glacierEventData": {
           "restoreEventData": {
              "lifecycleRestorationExpiryTime": "The time, in ISO-8601 format, for
 example, 1970-01-01T00:00:00.000Z, of Restore Expiry",
              "lifecycleRestoreStorageClass": "Source storage class for restore"
           }
        }
     }
  ]
}
```

イベントメッセージ構造について、以下の点に注意してください。

- <major> 形式でメジャーおよびマイナーバージョンを含む eventVersion キーの値。<minor>

Amazon S3 が、後方互換性のないイベント構造に変更を加えた場合、メジャーバージョンは増分されます。これには、すでに存在する JSON フィールドの削除や、フィールドのコンテンツの表現方法 (日付形式など) の変更が含まれます。

Amazon S3 が、イベント構造に新しいフィールドを追加した場合、マイナーバージョンは増分されます。これは、既存のイベントの一部またはすべてに対して新しい情報が提供された場合に発生します。これは、新しく導入されたイベントタイプでのみ新しい情報が提供されている場合にも発生します。イベント構造の新しいマイナーバージョンとの将来の互換性を保つには、アプリケーションは新しいフィールドを無視する必要があります。

新しいイベントタイプが導入したが、イベントの構造が変更されていない場合、イベントのバージョンは変更されません。

アプリケーションがイベント構造を正しく解析できるようにするため、メジャーバージョン番号が同等かどうかの比較を行うことをお勧めします。アプリケーションで想定されるフィールドが存在することを確認するため、マイナーバージョンが同等以上かを比較することをお勧めします。

- `eventName` はイベント通知タイプのリストを参照しますが、`s3:` プレフィックスが含まれていません。
- `responseElements` キー値は、AWS サポート のサポートによってリクエストを追跡する場合に役立ちます。`x-amz-request-id` と `x-amz-id-2` のどちらも、Amazon S3 が個々のリクエストを追跡するのに役立ちます。これらの値は、イベントを開始するリクエストへの応答として Amazon S3 が返す値と同じです。これは、イベントをリクエストに一致させるために使用できます。
- `s3` キーは、イベントに関与したバケットとオブジェクトに関する情報を提供します。オブジェクトのキー名の値は URL エンコードされます。例えば、「red flower.jpg」は「red+flower.jpg」となります (Amazon S3 はコンテンツタイプとして「`application/x-www-form-urlencoded`」をレスポンスで返します)。
- イベントのシーケンスを決定する方法の 1 つとして、`sequencer` キーがあります。イベントが発生した順序でイベント通知が届く保証はありません。ただし、オブジェクト (PUT) を作成するイベントからの通知 と削除オブジェクトは `sequencer` を含みます。これは、特定のオブジェクトキーのイベントの順序を決定するために使用できます。

  同じオブジェクトキーに対する 2 つのイベント通知の `sequencer` の文字列を比較すると、`sequencer` の 16 進値が大きいほうのイベント通知が後に発生したイベントであることがわかります。イベント通知を使用して Amazon S3 オブジェクトの別のデータベースまたはインデッ

クスを維持している場合は、イベント通知を処理するたびに sequencer の値を比較し、保存することを推奨します。

次の点に注意してください:

- 複数のオブジェクトキーのイベントの順序を決定するために sequencer を使用することはできません。
- sequencer の長さが異なる場合があります。これらの値を比較するには、最初に短い方の値を右に 0 と挿入してから、辞書式比較を実行します。

- glacierEventData キーは s3:ObjectRestore:Completed イベントに対してのみ表示されます。
- restoreEventData キーは、復元リクエストに関連する属性が含まれます。
- replicationEventData キーは、レプリケーションイベントに対してのみ表示されます。
- intelligentTieringEventData キーは S3 Intelligent-Tiering イベントのみ表示されます。
- lifecycleEventData キーは S3 ライフサイクルの移行イベントのみ表示されます。

メッセージの例

Amazon S3 イベント通知メッセージの例を次に示します。

Amazon S3 テストメッセージ

バケットにイベント通知を設定すると、Amazon S3 は次のようなテストメッセージを送信します。

```
{
   "Service":"Amazon S3",
   "Event":"s3:TestEvent",
   "Time":"2014-10-13T15:57:02.089Z",
   "Bucket":"amzn-s3-demo-bucket",
   "RequestId":"5582815E1AEA5ADF",
   "HostId":"8cLeGAmw098X5cv4Zkwcmo8vvZa3eH3eKxsPzbB9wrR+YstdA6Knx4Ip8EXAMPLE"
}
```

PUT リクエストを使用してオブジェクトが作成された場合のメッセージの例

次のメッセージは、Amazon S3 が s3:ObjectCreated:Put イベントを発行するために送信するメッセージの例です。

```
{
```

```
   "Records":[
      {
         "eventVersion":"2.1",
         "eventSource":"aws:s3",
         "awsRegion":"us-west-2",
         "eventTime":"1970-01-01T00:00:00.000Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"AIDAJDPLRKLG7UEXAMPLE"
         },
         "requestParameters":{
            "sourceIPAddress":"127.0.0.1"
         },
         "responseElements":{
            "x-amz-request-id":"C3D13FE58DE4C810",
            "x-amz-id-2":"FMyUVURIY8/IgAtTv8xRjskZQpcIZ9KG4V5Wp6S7S/
JRWeUWerMUE5JgHvANOjpD"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"testConfigRule",
            "bucket":{
               "name":"amzn-s3-demo-bucket",
               "ownerIdentity":{
                  "principalId":"A3NL1KOZZKExample"
               },
               "arn":"arn:aws:s3:::amzn-s3-demo-bucket"
            },
            "object":{
               "key":"HappyFace.jpg",
               "size":1024,
               "eTag":"d41d8cd98f00b204e9800998ecf8427e",
               "versionId":"096fKKXTRTtl3on89fVO.nfljtsv6qko",
               "sequencer":"0055AED6DCD90281E5"
            }
         }
      }
   ]
}
```

各 IAM 識別プレフィクス (AIDA、AROA、AGPA など) の定義については、IAM ユーザーガイドの IAM 識別子を参照してください。

EventBridge の使用

Amazon S3 は、バケット内で特定のイベントが発生するたびに Amazon EventBridge にイベントを送信できます。他の宛先とは異なり、配信するイベントタイプを選択する必要はありません。EventBridge を有効にすると、以下のすべてのイベントが EventBridge に送信されます。EventBridge ルールを使用すると、イベントを追加のターゲットにルートできます。Amazon S3 が EventBridge に送信するイベントを以下に示します。

イベントタイプ	説明
オブジェクトの作成	オブジェクトが作成されました。 イベントメッセージ構造の理由フィールドは、PutObject、POST Object、CopyObject、CompleteMultipartUpload などのオブジェクトの作成に使用された S3 API を示します。
オブジェクトが削除されました (DeleteObject) オブジェクトが削除されました (ライフサイクルの有効期限切れ)	オブジェクトが削除されました。 S3 API コールを使用してオブジェクトを削除すると、理由フィールドが deleteObject に設定されます。S3 ライフサイクルの有効期限切れルールによってオブジェクトを削除すると、理由フィールドがライフサイクルの有効期限切れに設定されます。詳細については、オブジェクトの有効期限 を参照してください。 バージョン管理されていないオブジェクトが削除されるか、バージョン管理されたオブジェクトが完全に削除されると、削除タイプフィールドは PermanentlyDeleted に設定されます。バージョン管理されたオブジェクトに対して削除マーカーが作成されると、削除タイプフィールドは作成したマーカーの削除に設定されます。詳細については、バージョニングが有効なバケットからのオブジェクトバージョンの削除 を参照してください。
オブジェクトの復元の開始	オブジェクトの復元は、S3 Glacier、S3 Glacier Deep Archive ストレージクラス、S3 Intelligent-Tiering アーカイブアクセス、Deep Archive アクセス階層から開始されまし

イベントタイプ	説明
	た。詳細については、アーカイブされたオブジェクトの操作 を参照してください。
オブジェクトの復元の完了	オブジェクトの復元が完了しました。
オブジェクトの復元の期限切れ	S3 Glacier または S3 Glacier Deep Archive から復元されたオブジェクトの一時コピーの有効期限切れのため削除されました。
オブジェクトストレージクラスの変更	オブジェクトが別のストレージクラスに移行されました。詳細については、Amazon S3 ライフサイクルを使用したオブジェクトの移行 を参照してください。
オブジェクトアクセス階層が変更されました	オブジェクトが S3 Intelligent-Tiering アーカイブアクセス階層または Deep Archive アクセス階層に移行されました。詳細については、Amazon S3 Intelligent-Tiering によるストレージコストの管理 を参照してください。
オブジェクト ACL が更新されました	オブジェクトのアクセスコントロールリスト (ACL) が PutObjectACL を使用して設定されました。リクエストによってオブジェクトの ACL が変更されない場合、イベントは生成されません。詳細については、アクセスコントロールリスト (ACL) の概要 を参照してください。
追加されたオブジェクトタグ	PutObjectTagging を使用して、一連のタグがオブジェクトに追加されました。詳細については、タグを使用してストレージを分類する を参照してください。
削除済みのオブジェクトタグ	DeleteObjectTagging を使用して、すべてのタグがオブジェクトから削除されました。詳細については、タグを使用してストレージを分類する を参照してください。

> **Note**
>
> Amazon S3 イベントタイプを EventBridge イベントタイプにマッピングする方法の詳細については、Amazon EventBridge のマッピングとトラブルシューティング を参照してください。

EventBridge で Amazon S3 イベント通知を使用して、バケットでイベントが発生したときにアクションを実行するルールを記述できます。例えば、通知を送信するように設定できます。詳細については、Amazon EventBridge ユーザーガイドの Amazon EventBridge とは を参照してください。

EventBridge API を使用して利用できるアクションとデータ型の詳細については、「Amazon EventBridge API リファレンス」の「Amazon EventBridge API Reference」を参照してください。

料金の詳細については、Amazon EventBridge の料金を参照してください。

トピック

- Amazon EventBridge アクセス許可
- Amazon EventBridge を有効にします
- EventBridge イベントメッセージの構造
- Amazon EventBridge のマッピングとトラブルシューティング

Amazon EventBridge アクセス許可

Amazon S3 では、Amazon EventBridge にイベントを配信するための追加のアクセス権限は必要ありません。

Amazon EventBridge を有効にします

S3 コンソール AWS Command Line Interface (AWS CLI)、または Amazon S3 REST API を使用して Amazon EventBridge を有効にできます。

> **Note**
>
> EventBridge を有効にすると、変更が適用されるまで約 5 分かかります。

S3 コンソールの使用

S3 コンソールで EventBridge イベント配信を有効にします。

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[汎用バケット] を選択します。
3. バケットリストで、イベントを有効にするバケットの名前を選択します。
4. [プロパティ] を選択します。
5. イベント通知セクションに移動し、Amazon EventBridge サブセクションを見つけます。[編集] を選択します。
6. このバケット内のすべてのイベント用の Amazon EventBridge に通知を送信するの下にある On を選択します。

AWS CLI を使用する場合

次の例では、amzn-s3-demo-bucket1 Amazon EventBridge が有効であるバケットのバケット通知設定を作成します。

```
aws s3api put-bucket-notification-configuration --bucket amzn-s3-demo-bucket1 --
notification-configuration='{ "EventBridgeConfiguration": {} }'
```

REST API の使用

Amazon S3 REST API を呼び出して、バケット上で Amazon EventBridge をプログラムで有効にできます。詳細については、「Amazon S3 API リファレンス」の「PutBucketNotificationConfiguration」を参照してください。

次の例は、Amazon EventBridge を有効にしたバケット通知設定を作成するために使用される XML を示しています。

```
<NotificationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <EventBridgeConfiguration>
  </EventBridgeConfiguration>
</NotificationConfiguration>
```

EventBridge ルールの作成

有効にすると、特定のタスクに対して Amazon EventBridge ルールを作成できます。例えば、オブジェクトが作成されたときに電子メール通知を送信できます。完全なチュートリアルについては、Amazon EventBridge ユーザーガイドのチュートリアル: Amazon S3 オブジェクトが作成されたとき通知を送信するを参照してください。

EventBridge イベントメッセージの構造

Amazon S3 がイベントを発行するために送信する通知メッセージは JSON 形式です。Amazon S3 が Amazon EventBridge にイベントを送信すると、次のフィールドが表示されます。

- バージョン — 現在、すべてのイベントで 0 (ゼロ)。
- id – イベントごとに生成される UUID。
- 詳細タイプ — 送信されるイベントのタイプ。イベントタイプのリスト化については、EventBridge の使用 を参照してください。
- source – イベントを生成したサービスを識別します。
- アカウント — バケット所有者の 12 桁の AWS アカウント ID。
- 時間 — イベントが発生した時刻。
- リージョン — バケットの AWS リージョン を識別します。
- リソース — バケットの Amazon リソースネーム (ARN) を含む JSON 配列。
- 詳細 – イベントに関する情報を含む JSON オブジェクト。このフィールドに含めることができる内容の詳細については、「イベントメッセージ詳細フィールド」を参照してください。

イベントメッセージの構造の例

Amazon EventBridge に送信できる Amazon S3 イベント通知メッセージの例を次に示します。

オブジェクトの作成

```
{
  "version": "0",
  "id": "17793124-05d4-b198-2fde-7ededc63b103",
  "detail-type": "Object Created",
  "source": "aws.s3",
  "account": "111122223333",
  "time": "2021-11-12T00:00:00Z",
  "region": "ca-central-1",
```

```
  "resources": [
    "arn:aws:s3:::amzn-s3-demo-bucket1"
  ],
  "detail": {
    "version": "0",
    "bucket": {
      "name": "amzn-s3-demo-bucket1"
    },
    "object": {
      "key": "example-key",
      "size": 5,
      "etag": "b1946ac92492d2347c6235b4d2611184",
      "version-id": "IYV3p45BT0ac8hjHg1houSdS1a.Mro8e",
      "sequencer": "617f08299329d189"
    },
    "request-id": "N4N7GDK58NMKJ12R",
    "requester": "123456789012",
    "source-ip-address": "1.2.3.4",
    "reason": "PutObject"
  }
}
```

(DeleteObject を使用して) オブジェクトが削除されました

```
{
  "version": "0",
  "id": "2ee9cc15-d022-99ea-1fb8-1b1bac4850f9",
  "detail-type": "Object Deleted",
  "source": "aws.s3",
  "account": "111122223333",
  "time": "2021-11-12T00:00:00Z",
  "region": "ca-central-1",
  "resources": [
    "arn:aws:s3:::amzn-s3-demo-bucket1"
  ],
  "detail": {
    "version": "0",
    "bucket": {
      "name": "amzn-s3-demo-bucket1"
    },
    "object": {
      "key": "example-key",
```

```
      "etag": "d41d8cd98f00b204e9800998ecf8427e",
      "version-id": "1QW9g1Z99LUNbvaaYVpW9xDlOLU.qxgF",
      "sequencer": "617f0837b476e463"
    },
    "request-id": "0BH729840619AG5K",
    "requester": "123456789012",
    "source-ip-address": "1.2.3.4",
    "reason": "DeleteObject",
    "deletion-type": "Delete Marker Created"
  }
}
```

(ライフサイクルの有効期限切れのため) オブジェクトが削除されました

```
{
  "version": "0",
  "id": "ad1de317-e409-eba2-9552-30113f8d88e3",
  "detail-type": "Object Deleted",
  "source": "aws.s3",
  "account": "111122223333",
  "time": "2021-11-12T00:00:00Z",
  "region": "ca-central-1",
  "resources": [
    "arn:aws:s3:::amzn-s3-demo-bucket1"
  ],
  "detail": {
    "version": "0",
    "bucket": {
      "name": "amzn-s3-demo-bucket1"
    },
    "object": {
      "key": "example-key",
      "etag": "d41d8cd98f00b204e9800998ecf8427e",
      "version-id": "mtB0cV.jejK63XkRNceanNMC.qXPWLeK",
      "sequencer": "617b398000000000"
    },
    "request-id": "20EB74C14654DC47",
    "requester": "s3.amazonaws.com",
    "reason": "Lifecycle Expiration",
    "deletion-type": "Delete Marker Created"
  }
}
```

オブジェクトの復元の完了

```
{
  "version": "0",
  "id": "6924de0d-13e2-6bbf-c0c1-b903b753565e",
  "detail-type": "Object Restore Completed",
  "source": "aws.s3",
  "account": "111122223333",
  "time": "2021-11-12T00:00:00Z",
  "region": "ca-central-1",
  "resources": [
    "arn:aws:s3:::amzn-s3-demo-bucket1"
  ],
  "detail": {
    "version": "0",
    "bucket": {
      "name": "amzn-s3-demo-bucket1"
    },
    "object": {
      "key": "example-key",
      "size": 5,
      "etag": "b1946ac92492d2347c6235b4d2611184",
      "version-id": "KKsjUC1.6gIjqtvhfg5AdMI0eCePIiT3"
    },
    "request-id": "189F19CB7FB1B6A4",
    "requester": "s3.amazonaws.com",
    "restore-expiry-time": "2021-11-13T00:00:00Z",
    "source-storage-class": "GLACIER"
  }
}
```

イベントメッセージ詳細フィールド

詳細フィールドは、イベントに関する情報のある JSON オブジェクトを含みます。詳細フィールドには、次のフィールドが存在する可能性があります。

- バージョン — 現在、すべてのイベントで 0 (ゼロ)。
- バケット — イベントに関与した Amazon S3 バケットに関する情報。
- オブジェクト — イベントに関与した Amazon S3 オブジェクトに関する情報。

- リクエスト ID — S3 レスポンスのリクエスト ID。
- リクエスタ — AWS アカウント ID または AWS リクエスタのサービスプリンシパル。
- 送信元 IP アドレス — S3 リクエストの出典 IP アドレス。S3 リクエストによってトリガーされたイベントにのみ存在します。
- 理由 — オブジェクトの作成イベントの場合、オブジェクトの作成に使用される S3 API: PutObject、POST Object、CopyObject、CompleteMultipartUpload。オブジェクトの作成イベントの場合、これは、オブジェクトが S3 API コールによって削除された場合は DeleteObject に設定され、オブジェクトが S3 ライフサイクル有効期限切れルールによって削除された場合は LifecycleExpiration に設定されます。詳細については、オブジェクトの有効期限 を参照してください。
- deletion-type (削除タイプ) — オブジェクトの削除イベントの場合、バージョン管理されていないオブジェクトが削除されるか、バージョン管理されたオブジェクトが完全に削除されると、これは完全に削除されます。バージョン化したオブジェクトに削除マーカーが作成されると、これは削除マーカーの作成に設定されます。詳細については、「バージョニングが有効なバケットからのオブジェクトバージョンの削除」を参照してください。

  > **Note**
  >
  > 一部のオブジェクト属性 (`etag` や `size` など) は、削除マーカーが作成された場合にのみ示されます。

- restore-expiry-time (保存有効期限) — オブジェクト保存完了 イベントの場合、オブジェクトの一時コピーが S3 から削除される時刻。詳細については、アーカイブされたオブジェクトの操作 を参照してください。
- source-storage-class (ソースストレージクラス) — オブジェクト復元開始およびオブジェクト復元完了イベントの場合の、復元されるオブジェクトのストレージクラス。詳細については、アーカイブされたオブジェクトの操作 を参照してください。
- destination-storage-class (デスティネーション・ストレージ・クラス) — オブジェクトストレージクラスの変更イベントの場合の、オブジェクトの新しいストレージクラス。詳細については、Amazon S3 ライフサイクルを使用したオブジェクトの移行 を参照してください。
- destination-access-tier (宛先アクセス階層) — オブジェクトアクセス階層の変更イベントの場合、オブジェクトの新しいアクセス階層。詳細については、Amazon S3 Intelligent-Tiering によるストレージコストの管理 を参照してください。

Amazon EventBridge のマッピングとトラブルシューティング

次の表では、Amazon S3 イベントタイプが Amazon EventBridge イベントタイプにどのようにマッピングされるかを説明します。

S3 イベントタイプ	Amazon EventBridge の詳細タイプ
ObjectCreated:Put ObjectCreated:Post ObjectCreated:Copy ObjectCreated:CompleteMultipartUpload	オブジェクトの作成
ObjectRemoved:Delete ObjectRemoved:DeleteMarkerCreated LifecycleExpiration:Delete LifecycleExpiration:DeleteMarkerCreated	削除したオブジェクト
ObjectRestore:Post	オブジェクトの復元の開始
ObjectRestore:Completed	オブジェクト復元の完了
ObjectRestore:Delete	オブジェクト復元の有効期限切れ
LifecycleTransition	オブジェクトストレージクラスの変更
IntelligentTiering	オブジェクトアクセス階層が変更されました
ObjectTagging:Put	追加されたオブジェクトタグ
ObjectTagging:Delete	削除済みのオブジェクトタグ
ObjectACL:Put	オブジェクト ACL が更新されました

Amazon EventBridge のトラブルシューティング

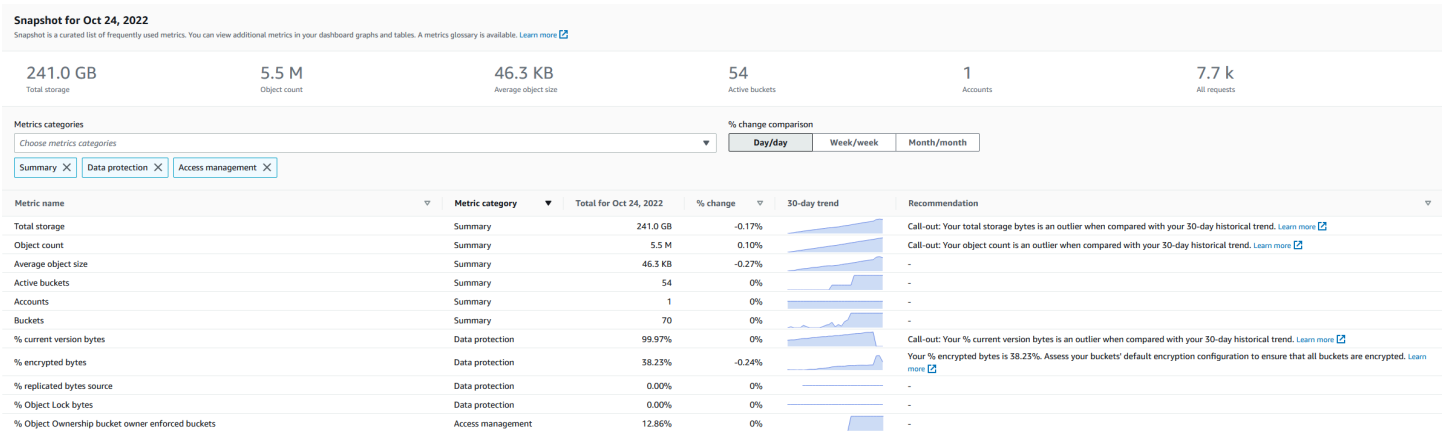
EventBridge のトラブルシューティング方法の詳細については、「Amazon EventBridge ユーザーガイド」の「Troubleshooting Amazon EventBridgeを参照してください 。

Amazon S3 ストレージレンズを使用してストレージのアクティビティと使用状況を評価する

Amazon S3 ストレージレンズは、オブジェクトストレージおよびアクティビティを組織全体で可視化するために使用できるクラウドストレージ分析機能です。また、S3 Storage Lens は、メトリクスを分析して、ストレージコストを最適化し、データ保護に関するベストプラクティスを適用するために使用できるコンテキストに応じた推奨事項を提供します。

S3 Storage Lens メトリクスを使用して、概要の分析情報を生成できます。例えば、組織全体でどれだけのストレージがあるか、または最も急速に成長しているバケットとプレフィックスは何かなどを把握することができます。S3 Storage Lens メトリクスを使用して、コスト最適化の機会を特定し、データ保護とアクセス管理のベストプラクティスを実装し、アプリケーションワークロードのパフォーマンスを向上させることができます。例えば、S3 ライフサイクルルールが設定されていないバケットを特定して、7 日を超えた未完了のマルチパートアップロードを有効期限切れにすることができます。また、S3 レプリケーションや S3 バージョニングの使用など、データ保護のベストプラクティスに従っていないバケットを特定することもできます。

S3 ストレージレンズはメトリクスを集約し、Amazon S3 コンソールの [Buckets] (バケット) ページの [Account snapshot] (アカウントスナップショット) セクションにこの情報を表示します。S3 Storage Lens は、インサイトと傾向を可視化したり、外れ値にフラグ付けしたり、ストレージコストの最適化やデータ保護のベストプラクティスの適用に関するレコメンデーション事項を受け取ったりするために使用できるインタラクティブダッシュボードも提供します。ダッシュボードには、組織、アカウント、AWS リージョン、ストレージクラス、バケット、プレフィックス、またはストレージレンズのグループレベルでインサイトを生成して可視化できる、ドリルダウンオプションが用意されています。1 日 1 回のメトリクスのエクスポートを CSV 形式または Parquet 形式で S3 バケットに送信することもできます。



S3 ストレージレンズのメトリクスと機能

S3 ストレージレンズでは、毎日更新されるインタラクティブなデフォルトダッシュボードが利用できます。S3 ストレージレンズではこのダッシュボードが事前定義されており、アカウント全体の要約されたインサイトとトレンドを視覚化し、S3 コンソールで毎日更新します。このダッシュボードのメトリクスは、[Buckets] (バケット) ページのアカウントスナップショットにも要約されます。詳細については、「デフォルトのダッシュボード」を参照してください。

他のダッシュボードを作成し、AWS リージョン、S3 バケットまたはアカウント (AWS Organizations 用) でスコープを設定するには、S3 ストレージレンズダッシュボード設定を作成します。AmazonS3 コンソール、AWS Command Line Interface、(AWS CLI)、AWS SDK、または Amazon S3 REST API を使用して S3 Storage Lens ダッシュボード設定を作成および管理できます。S3 Storage Lens ダッシュボードを作成または編集するとき、ダッシュボードのスコープとメトリクスの選択を定義します。

S3 ストレージレンズでは、無料のメトリクスと、追加料金でアップグレードできるアドバンストメトリクスとレコメンデーションをご利用になれます。アドバンストメトリクスとレコメンデーションをご利用になれば、ストレージに関するインサイトが得られる追加のメトリクスや機能にアクセスできます。これらの機能には、高度なメトリクスカテゴリ、プレフィックス集約、コンテキストに応じた推奨事項、Amazon CloudWatch パブリッシングなどがあります。プレフィックス集約とコンテキストに応じた推奨事項は、Amazon S3 コンソールでのみ使用できます。S3 Storage Lens の料金の詳細については、Amazon S3 の料金を参照してください。

メトリクスのカテゴリ

無料層とアドバンスト層で、メトリクスはコストの最適化やデータ保護などの主要なユースケースに合わせてカテゴリに分類されます。無料のメトリクスには、概要、コスト最適化、データ保護、アクセス管理、パフォーマンス、イベントメトリクスが含まれます。アドバンストメトリクスとレコメ

ンデーションにアップグレードすると、高度なコスト最適化とデータ保護メトリクスを有効にできます。これらの高度なメトリクスを使用すると、S3 ストレージのコストをさらに削減し、データ保護スタンスを向上させることができます。アクティビティメトリクスと詳細なステータスコードメトリクスを有効にして、S3 バケットにアクセスしているアプリケーションワークロードのパフォーマンスを向上させることもできます。無料のメトリクスと高度なメトリクスのカテゴリの詳細については、「メトリクスの選択」を参照してください。

暗号化、S3 オブジェクトロック、または S3 バージョニングが有効になっているバケットの割合を分析するなど、S3 のベストプラクティスに基づいてストレージを評価できます。また、潜在的なコスト削減の機会を特定することもできます。例えば、S3 ライフサイクルルール数メトリクスを使用して、ライフサイクルの有効期限または移行ルールがないバケットを特定できます。また、バケットごとのリクエストアクティビティを分析して、コストのより低いストレージクラスにオブジェクトの移行が可能なバケットを見つけることもできます。詳細については、「Amazon S3 ストレージレンズメトリクスのユースケース」を参照してください。

メトリクスのエクスポート

S3 コンソールのダッシュボードで表示するだけでなく、メトリクスを CSV または Parquet 形式で S3 バケットにエクスポートして、選択した分析ツールでさらに分析することができます。詳細については、「データエクスポートで Amazon S3 Storage Lens のメトリクスを確認する」を参照してください。

Amazon CloudWatch パブリッシング

S3 ストレージレンズの使用状況とアクティビティメトリクスを Amazon CloudWatch に公開し、CloudWatch ダッシュボードで運用状況を一元的に表示することができます。また、アラームやトリガーアクション、メトリクス計算、異常検出などの CloudWatch 機能を使用して、S3 ストレージレンズメトリクスをモニタリングして対処することができます。さらに CloudWatch API オペレーションにより、サードパーティープロバイダーを含むアプリケーションが S3 ストレージレンズメトリクスにアクセスできるようになります。CloudWatch の公開オプションは、S3 ストレージレンズのアドバンストメトリクスとレコメンデーションにアップグレードされたダッシュボードで利用可能です。CloudWatch での S3 ストレージレンズメトリクスの詳細については、「CloudWatch で S3 Storage Lens のメトリクスをモニタリング」を参照してください。

S3 ストレージレンズの使用の詳細については、次のトピックを参照してください。

トピック

- Amazon S3 ストレージレンズを理解する
- Amazon S3 Storage Lens のメトリクスに関する用語集

- Amazon S3 ストレージレンズアクセス許可の設定
- コンソールと API を使用した Amazon S3 ストレージレンズの使用
- Amazon S3 ストレージレンズでのメトリクスの表示
- AWS Organizations での Amazon S3 ストレージレンズの使用
- S3 ストレージレンズグループを使用したメトリクスのフィルタリングと集計

Amazon S3 ストレージレンズを理解する

> **Important**
>
> Amazon S3 では、Amazon S3 内のすべてのバケットの基本レベルの暗号化として、Amazon S3 が管理するキー (SSE-S3) によるサーバー側の暗号化が適用されるようになりました。2023 年 1 月 5 日以降、Amazon S3 にアップロードされるすべての新しいオブジェクトは、追加費用なしで、パフォーマンスに影響を与えずに自動的に暗号化されます。S3 バケットのデフォルト暗号化設定と新しいオブジェクトのアップロードのための自動暗号化ステータスは、AWS CloudTrail ログ、S3 インベントリ、S3 ストレージレンズ、Amazon S3 コンソール、および AWS Command Line Interface と AWS SDK の追加の Amazon S3 API レスポンスヘッダーとして利用できるようになりました。詳細については、「デフォルト暗号化に関するよくある質問」を参照してください。

Amazon S3 ストレージレンズは、オブジェクトストレージの使用状況とアクティビティを組織全体で可視化するために使用できるクラウドストレージの分析機能です。S3 ストレージレンズメトリクスを使用することで、組織全体でどれだけのストレージがあるか、または最も急速に成長しているバケットとプレフィックスは何かなどの、要約されたインサイトを生成できます。S3 ストレージレンズメトリクスを使用して、コスト最適化の機会を特定し、データ保護とセキュリティのベストプラクティスを実装し、アプリケーションワークロードのパフォーマンスを向上させることもできます。例えば、S3 ライフサイクルルールがないバケットを特定して、7 日以上経過した未完了のマルチパートアップロードを有効期限切れにできます。また、S3 レプリケーションや S3 バージョニング使用など、データ保護のベストプラクティスに従っていないバケットを特定することもできます。また、S3 ストレージレンズは、メトリクスを分析して、ストレージコストを最適化し、データ保護に関するベストプラクティスを適用するために使用できるコンテキストに応じた推奨事項を提供します。

S3 ストレージレンズはメトリクスを集約し、Amazon S3 コンソールの [Buckets] (バケット) ページの [Account snapshot] (アカウントスナップショット) セクションにこの情報を表示します。S3

Storage Lens は、インサイトと傾向を可視化したり、外れ値にフラグ付けしたり、ストレージコストの最適化やデータ保護のベストプラクティスの適用に関するレコメンデーション事項を受け取ったりするために使用できるインタラクティブダッシュボードも提供します。ダッシュボードには、組織、アカウント、AWS リージョン、ストレージクラス、バケット、プレフィックス、またはストレージレンズのグループレベルでインサイトを生成して可視化できる、ドリルダウンオプションが用意されています。1 日 1 回のメトリクスのエクスポートを CSV 形式または Parquet 形式で S3 バケットに送信することもできます。AmazonS3 コンソール、AWS Command Line Interface、(AWS CLI)、AWS SDK、または Amazon S3 REST API を使用して S3 Storage Lens ダッシュボードを作成および管理できます。

S3 ストレージレンズの概念と用語

このセクションは、Amazon S3 ストレージレンズを適切に理解し使用するために不可欠な、用語と概念に関する解説で構成されています。

トピック

- ダッシュボード設定
- デフォルトのダッシュボード
- ダッシュボード
- アカウントスナップショット
- メトリクスのエクスポート
- ホームリージョン
- 保持期間
- メトリクスのカテゴリ
- レコメンデーション
- メトリクスの選択
- S3 ストレージレンズと AWS Organizations

ダッシュボード設定

S3 ストレージレンズでは、ユーザーに代わってメトリクスを集計するのに必要なプロパティを含むダッシュボード設定が必要となります。これらは、単一のダッシュボード、もしくはエクスポートのために使用されます。設定を作成するときは、ダッシュボード名とホームリージョンを選択します。これらはダッシュボードの作成後に変更できません。オプションでタグを追加し、CSV または Parquet 形式でメトリクスをエクスポートするように設定できます。

ダッシュボード設定では、ダッシュボードのスコープとメトリクスの選択も定義します。スコープには、組織アカウントのすべてのストレージ、またはリージョン、バケット、アカウントでフィルタリングされたセクションのストレージを含めることができます。メトリクスの選択を設定する際、無料のメトリクスまたは追加料金でアップグレードできるアドバンストメトリクスとレコメンデーションのいずれかを選択します。アドバンストメトリクスとレコメンデーションにより、その他のメトリクスや機能にアクセスできます。これらの機能には、高度なメトリクスカテゴリ、プレフィックスレベルでの集約、コンテキストに応じた推奨事項、Amazon CloudWatch パブリッシングなどがあります。S3 ストレージレンズの料金の詳細については、Amazon S3 の料金を参照してください。

デフォルトのダッシュボード

コンソールの S3 ストレージレンズのデフォルトダッシュボードの名前は、default-account-dashboard です。S3 ではこのダッシュボードが事前定義されており、アカウント全体の要約されたインサイトとトレンドを視覚化し、S3 コンソールで毎日更新します。デフォルトのダッシュボードのスコープ設定を変更することはできませんが、選択するメトリクスを、無料メトリクスからアドバンストメトリクスとレコメンデーションにアップグレードすることはできます。オプションで、メトリクスのエクスポートを設定したり、ダッシュボードを無効にしたりもできます。ただし、デフォルトのダッシュボードを削除することはできません。

> **Note**
>
> デフォルトのダッシュボードを無効にすると、更新されなくなります。S3 ストレージレンズダッシュボード、メトリクスエクスポート、または S3 [バケット] ページのアカウントスナップショットで、新しい日次メトリクスを受け取ることはなくなります。ダッシュボードで高度なメトリクスや推奨事項を使用していても、請求は発生しなくなります。データクエリの 14 日の有効期限が切れるまでは、ダッシュボードで履歴データを引き続き表示できます。アドバンストメトリクスとレコメンデーションを有効にしている場合、この期間は 15 か月です。有効期限内にダッシュボードを再度有効にすれば、履歴データにアクセスできます。

ダッシュボード

追加の S3 ストレージレンズダッシュボードを作成し、AWS リージョン、S3 バケット、またはアカウント (AWS Organizations の場合) によってスコープを設定できます。S3 ストレージレンズダッシュボードを作成または編集するとき、ダッシュボードのスコープとメトリクスの選択を定義します。S3 ストレージレンズでは、無料のメトリクスと、追加料金でアップグレードできるアドバンストメトリクスとレコメンデーションをご利用になれます。アドバンストメトリクスとレコメンデー

ションをご利用になれば、ストレージに関するインサイトが得られる追加のメトリクスや機能にアクセスできます。これらには、高度なメトリクスカテゴリ、プレフィックスレベルでの集約、コンテキストに応じた推奨事項、Amazon CloudWatch パブリッシングなどがあります。S3 Storage Lens の料金の詳細については、「Amazon S3 の料金」を参照してください。

また、ダッシュボードを無効化または削除することも可能です。ダッシュボードを無効にすると、そのダッシュボードは更新されなくなるので、日次で新しいメトリクスが生成されることもなくなります。14 日の有効期限の間は、履歴データを表示できます。そのダッシュボードでアドバンストメトリクスとレコメンデーションを有効にした場合、この期間は 15 か月です。有効期限内にダッシュボードを再度有効にすれば、履歴データにアクセスできます。

ダッシュボードを削除すると、それまでの設定内容はすべて失われます。削除されたダッシュボードからは、それ以後の新しい日次のメトリクスは受信できなくなり、そのダッシュボードに関連付けられた履歴データにもアクセスできなくなります。削除したダッシュボードの履歴データにアクセスする場合は、同じホームリージョンで同じ名前を使用しながら、新たなダッシュボードを作成する必要があります。

> **Note**
>
> - S3 ストレージレンズをご使用のお客様は、ホームリージョンごとに最大 50 個のダッシュボードを作成いただけます。
> - 組織レベルのダッシュボードは、リージョンのスコープにのみ制限できます。

アカウントスナップショット

S3 ストレージレンズの [Account snapshot] (アカウントスナップショット) は、デフォルトのダッシュボードからメトリクスを要約し、S3 コンソールの ([Buckets] (バケット) ページに、ストレージ合計、オブジェクト数、および平均オブジェクトサイズを表示します。このアカウントスナップショットでは、[Buckets] (バケット) ページから移動することなく、ストレージに関するインサイトにすばやくアクセスできます。アカウントスナップショットから、インタラクティブな S3 ストレージレンズダッシュボードにワンクリックでアクセスすることもできます。

ダッシュボードでは、インサイトと傾向を可視化したり、外れ値にフラグ付けしたりできます。また、ストレージコストの最適化や、データ保護のベストプラクティスの適用に関するレコメンデーション事項を受け取ることもできます。ダッシュボードには、組織、アカウント、バケット、オブジェクト、またはプレフィックスレベルでインサイトを生成できる、ドリルダウンオプションが用意

されています。1 日 1 回のメトリクスのエクスポートを CSV 形式または Parquet 形式で S3 バケットに送信することもできます。

default-account-dashboard のスコープは、アカウントスナップショットにリンクされているため、変更できません。ただし、default-account-dashboard のメトリクス選択を、無料のメトリクスから有料のアドバンストメトリクスとレコメンデーションにアップグレードできます。アップグレード後、すべてのリクエスト、アップロードされたバイト数、およびダウンロードされたバイト数を S3 ストレージレンズのアカウントスナップショットで表示できます。

> **Note**
>
> デフォルトのダッシュボードを無効にすると、アカウントスナップショットは更新されなくなります。アカウントスナップショットでのメトリクスの表示を再開するには、default-account-dashboard を再度有効にします。

メトリクスのエクスポート

S3 ストレージレンズでは、1 つのファイルとしてメトリクスのエクスポートを作成します。このファイルには、S3 ストレージレンズの設定で指定された、すべてのメトリクスが含まれています。この情報は、CSV または Parquet 形式で毎日生成され、S3 バケットに送信されます。メトリクスをエクスポートすれば、お好みのメトリクスツールでさらに分析することができます。メトリクスのエクスポート用の S3 バケットは、S3 ストレージレンズ設定と同じリージョンに存在する必要があります。ダッシュボードの設定を編集することで、S3 コンソールから S3 ストレージレンズメトリクスのエクスポートを生成できます。AWS CLI および AWS SDK を使用してメトリクスのエクスポートを設定することもできます。

ホームリージョン

ホームリージョンとは、特定のダッシュボード設定のすべての S3 ストレージレンズメトリクスが保存される AWS リージョン です。S3 ストレージレンズのダッシュボード設定を作成する際には、ホームリージョンを選択する必要があります。いったん選択したホームリージョンは変更できません。また、Storage Lens グループを作成する場合は、Storage Lens ダッシュボードと同じホームリージョンを選択することをお勧めします。

> **Note**
>
> 次のいずれかの地域をホームリージョンとして選択できます。
>
> - 米国東部 (バージニア北部) – `us-east-1`

- 米国東部 (オハイオ) – us-east-2
- 米国西部 (北カリフォルニア) – us-west-1
- 米国西部 (オレゴン) – us-west-2
- アジアパシフィック (ムンバイ) – ap-south-1
- アジアパシフィック (ソウル) – ap-northeast-2
- アジアパシフィック (シンガポール) – ap-southeast-1
- アジアパシフィック (シドニー) – ap-southeast-2
- アジアパシフィック (東京) – ap-northeast-1
- カナダ (中部) – ca-central-1
- 中国 (北京) – cn-north-1
- 中国 (寧夏) – cn-northwest-1
- 欧州 (フランクフルト) – eu-central-1
- 欧州 (アイルランド) – eu-west-1
- 欧州 (ロンドン) – eu-west-2
- 欧州 (パリ) – eu-west-3
- 欧州 (ストックホルム) – eu-north-1
- 南米 (サンパウロ) – sa-east-1

保持期間

S3 Storage Lens のメトリクスは保持されるため、過去の傾向を確認したり、ストレージの使用状況やアクティビティの変動を時間の経過を追って比較したりするために使用できます。Amazon S3 ストレージレンズのメトリクスをクエリに使用することで、過去の傾向を確認し、ストレージの使用量とアクティビティの違いを時系列で比較することができます。

すべての S3 ストレージレンズメトリクスは 15 か月間保持されます。ただし、メトリクスは特定の期間のクエリでのみ使用できます。これは、選択したメトリクスの種類によって異なります。この期間は変更できません。無料のメトリクスは 14 日間、アドバンストメトリクスは 15 か月間のクエリで利用可能です。

メトリクスのカテゴリ

無料層とアドバンスト層で、S3 ストレージレンズメトリクスはコストの最適化やデータ保護などの主要なユースケースに合わせてカテゴリに分類されます。無料のメトリクスには、概要、コスト最

適化、データ保護、アクセス管理、パフォーマンス、イベントメトリクスが含まれます。高度なメトリクスとレコメンデーションにアップグレードすると、追加のコスト最適化とデータ保護メトリクスを有効にして、S3 ストレージのコストをさらに削減し、データ保護を確実にできます。また、アクティビティメトリクスと詳細なステータスコードメトリクスを有効にして、アプリケーションワークロードのパフォーマンスを向上させために使用することもできます。

次のリストは、すべての無料および高度なメトリクスのカテゴリを示しています。各カテゴリに含まれる個々のメトリクスの完全なリストについては、「メトリクスの用語集」を参照してください。

サマリーメトリクス

サマリーメトリクスは、ストレージの合計バイト数やオブジェクト数など、S3 ストレージに関する一般的な情報を提供します。

コスト最適化メトリクス

コスト最適化メトリクスは、ストレージコストの管理と最適化に役立つインサイトを提供します。例えば、7 日以上経過した不完全なマルチパートアップロードを特定できます。

アドバンストメトリクスとレコメンデーションにより、高度なコスト最適化メトリクスを有効にできます。これらのメトリクスには、バケットごとの有効期限と移行 S3 ライフサイクルルール数を取得するために使用できる S3 ライフサイクルルールカウントメトリクスが含まれています。

データ保護メトリクス

データ保護メトリクスは、暗号化や S3 バージョニングなどのデータ保護機能に関するインサイトを提供します。これらのメトリクスを使用して、データ保護のベストプラクティスに従っていないバケットを特定できます。例えば、デフォルトの暗号化に AWS Key Management Service キー (SSE-KMS) を使用していないバケットや、S3 バージョニングを使用していないバケットを特定できます。

アドバンストメトリクスとレコメンデーションにより、高度なデータ保護メトリクスを有効にできます。これらのメトリクスには、バケットごとのレプリケーションルール数メトリクスが含まれます。

アクセス管理メトリクス

アクセス管理メトリクスは、S3 オブジェクト所有権に関するインサイトを提供します。これらのメトリクスを使用して、バケットが使用しているオブジェクト所有権設定を確認できます。

イベントメトリクス

イベントメトリクスは、S3 イベント通知に関するインサイトを提供します。イベントメトリクスでは、どのバケットに S3 イベント通知が設定されているかを確認できます。

パフォーマンスメトリクス

パフォーマンスメトリクスは、S3 Transfer Acceleration のインサイトを提供します。パフォーマンスメトリクスでは、どのバケットで Transfer Acceleration が有効になっているかを確認できます。

アクティビティメトリクス (アドバイスト)

ダッシュボードを高度なメトリクスとレコメンデーションにアップグレードすると、アクティビティメトリクスを有効にできます。アクティビティメトリクスは、ストレージがどのようにリクエストされたか (例えば、ALL リクエスト、GET リクエスト、PUT リクエストなど)、アップロードまたはダウンロードされたバイト数、エラーなどに関する詳細を提供します。

プレフィックスレベルのアクティビティメトリクスを使用すると、使用頻度の低いプレフィックスを特定できるため、S3 ライフサイクルを使用してより最適なストレージクラスに移行できます。

詳細なステータスコードメトリクス (アドバンスト)

ダッシュボードを高度なメトリクスとレコメンデーションにアップグレードすると、詳細なステータスコードメトリクスを有効にできます。詳細なステータスコードメトリクスにより、403 Forbidden や 503 Service Unavailable などの HTTP ステータスコードに関するインサイトが得られ、アクセスやパフォーマンスの問題のトラブルシューティングに使用できます。例えば、403 Forbidden エラー数メトリクスを見ると、適切なアクセス権限が適用されていない状態でバケットにアクセスしているワークロードを特定できます。

プレフィックスレベルの詳細なステータスコードメトリクスを使用すると、プレフィックスごとの HTTP ステータスコードの発生に関する理解を深めることができます。例えば、503 エラーカウントメトリクスを使用すると、データインジェスト中にスロットリングリクエストを受信したプレフィックスを特定できます。

レコメンデーション

S3 ストレージレンズでは、ストレージの最適化に役立つ自動化された推奨事項が提供されます。それぞれの推奨事項は、関連のあるメトリクスとともに、文脈に応じた形で S3 ストレージレンズダッシュボード上に表示されます。履歴データは、推奨事項の対象になりません。推奨事項は、最近に発生した事象に関連しています。推奨事項は、関連性が存在する場合にのみ表示されます。

S3 ストレージレンズの推奨事項は、次のような形式で構成されます。

- 提案

  提案は、ストレージとアクティビティでのトレンドに関する注意を促します。この場合、ストレージコストの最適化や、データ保護のベストプラクティスを実施できる可能性があります。Amazon

S3 ユーザーガイドで、この提案に関するトピックを参照できます。同時に、S3 Storage Lens ダッシュボードから特定のリージョン、バケット、またはプレフィックスにドリルダウンすることができます。

- コールアウト

  コールアウトは、ストレージおよびアクティビティに関し、一定期間に発生して関心を向けるべき異常を通知するための推奨事項です。これらの結果には、さらなる注意や監視が必要となる場合があります。

  - 外れ値のコールアウト

    S3 ストレージレンズでは、最近の 30 日間の傾向に基づいて判断した、外れ値のメトリクスに関するコールアウトが利用できます。外れ値は、Z-score とも呼ばれる標準スコアを使用して算出されています。このスコアでは、当日のメトリクスが、同じメトリクスの直近 30 日間の平均から減算されます。次に、当日のメトリクスが、同じメトリクスの直近 30 日間の標準偏差により除算されます。結果として得られるスコアは、通常 -3 ~ +3 の間の値となります。この数値は、当該日のメトリクスの、平均値からの標準偏差を表しています。

    S3 ストレージレンズでは、スコアが 2 から -2 の範囲を上下に超えるメトリクスは外れ値と見なされます。理由は、この値が正規分布データの 95% よりも高い、あるいは低くなるためです。

  - 顕著な変化についてのコールアウト

    顕著な変化についてのコールアウトは、変化する頻度が低いことが想定されているメトリクスに対し適用されます。このため、この値の計算では、外れ値の計算よりも高い感度が設定されます。この感度には通常、前日、前週、または前月に比べて +/-20% の範囲が指定されます。

    ストレージの使用状況とアクティビティに関するコールアウトへの対応 – 顕著な変化についてのコールアウトを受け取った場合でも、必ずしも問題が存在することにはなりません。コールアウトは、ストレージで予定された変更の結果である可能性もあります。たとえば、多数の新しいオブジェクトの追加や多数のオブジェクトの削除を最近行っていたり、それと同様の計画的な変更を行ったりした場合など、このコールアウトの原因となり得ます。

    ダッシュボード上に、顕著な変化についてのコールアウトが表示される場合は、それを記録した上で、その原因が、最近の状況によって説明できるかどうかを確認します。原因が見つからない場合は、S3 ストレージレンズダッシュボードを使用して詳細をドリルダウンしながら、変動要因となっている特定のリージョン、バケット、またはプレフィックスを調査します。

- リマインダー

リマインダーにより、Amazon S3 の動作についてのインサイトが提供されます。リマインダーは、ストレージコストの削減や、データ保護のベストプラクティスの適用のための S3 の機能の使用方法について、詳しく知るために利用できます。

メトリクスの選択

S3 ストレージレンズのダッシュボードとエクスポートでは、メトリクスを、無料のメトリクスとアドバンストメトリクスとレコメンデーションという 2 種類から選択できます。

- 無料のメトリクス

  S3 ストレージレンズの無料のメトリクスは、すべてのダッシュボードと設定で使用できます。無料のメトリクスには、アカウント内のバケットやオブジェクトの数など、ストレージに関連するメトリクスが含まれています。無料のメトリクスには、ストレージが S3 のベストプラクティスに従って設定されているかどうかを調べるために使用できるユースケースベースのメトリクス (コスト最適化やデータ保護メトリクスなど) も含まれています。すべての無料メトリクスは毎日収集されます。データは、14 日間クエリで利用可能です。無料のメトリクスについては、「Amazon S3 Storage Lens のメトリクスに関する用語集」を参照してください。

- アドバンストメトリクスとレコメンデーション

  S3 ストレージレンズでは、すべてのダッシュボードと構成に対して無料のメトリクスを提供していますが、さらに、アドバンストメトリクスとレコメンデーションにアップグレードできるオプションも用意されています。追加の変更が適用されます。詳細については、「Amazon S3 の料金」を参照してください。

  アドバンストメトリクスとレコメンデーションには、無料のメトリクスに含まれるすべてのメトリクスに加えて、高度なデータ保護やコスト最適化のメトリクス、アクティビティメトリクス、詳細なステータスコードメトリクスなどの追加のメトリクスが含まれます。また、アドバンストメトリクスとレコメンデーションは、ストレージの最適化に役立つ推奨事項も提供します。それぞれの推奨事項は、関連するメトリクスとともに、文脈に応じた形でダッシュボード上に表示されます。

  また、高度なメトリクスとレコメンデーションには以下の機能も含まれています。

  - アドバンストメトリクス — 追加のメトリクスを生成します。アドバンストメトリクスカテゴリの完全なリストについては、「メトリクスのカテゴリ」を参照してください。メトリクスの一覧については、「Amazon S3 Storage Lens のメトリクスに関する用語集」を参照してください。
  - Amazon CloudWatch パブリッシング – S3 Storage Lens メトリクスを CloudWatch に公開して、CloudWatch ダッシュボードで運用の健全性を一元的に把握できます。また、アラームやト

リガーアクション、メトリクス計算、異常検出などの CloudWatch API オペレーションと機能を使用して、S3 ストレージレンズメトリクスをモニタリングして対処することができます。詳細については、「CloudWatch で S3 Storage Lens のメトリクスをモニタリング」を参照してください。

- プレフィックス集約 – プレフィックスレベルでメトリクスを集約します。[プレフィックス集約] を有効にすると、ダッシュボード設定に含まれるすべてのメトリクスがプレフィックスレベルで拡張されます。メトリクスは、設定したしきい値を満たすプレフィックスに対してのみ生成されます。プレフィックスレベルで適用できるメトリクスは、バケットレベルの設定とルールカウントメトリクスを除き、[プレフィックス集約]で利用できることに注意してください。プレフィックスレベルのメトリクスは CloudWatch に公開されません。
- Storage Lens グループ集約 — Storage Lens グループレベルでメトリクスを収集します。[高度なメトリクスとレコメンデーション] と [Storage Lens グループ集約] を有効にすると、どの Storage Lens グループを Storage Lens ダッシュボードに含めたり除外したりするかを指定できます (少なくとも 1 つの Storage Lens グループを指定する必要があります)。指定する Storage Lens グループは、ダッシュボードアカウントの指定されたホームリージョン内にも存在している必要があります。Storage Lens グループレベルのメトリクスは CloudWatch に公開されません。

すべてのアドバンストメトリクスは毎日収集されます。データは最長 15 か月間クエリで使用できます。S3 ストレージレンズによって集計されるストレージメトリクスの詳細については、「Amazon S3 Storage Lens のメトリクスに関する用語集」を参照してください。

> **Note**
>
> 推奨事項が利用できるのは、Amazon S3 コンソールで S3 Storage Lens ダッシュボードを使用している場合だけです。

S3 ストレージレンズと AWS Organizations

AWS Organizations は、1 つの組織階層に属する、すべての AWS アカウント を集約するための AWS のサービス です。Amazon S3 ストレージレンズを AWS Organizations と連携させることで、Amazon S3 ストレージ全体でのオブジェクトによるストレージとそのアクティビティを、単一的なビューで表示することができます。

詳細については、「AWS Organizations での Amazon S3 ストレージレンズの使用」を参照してください。

- 信頼されたアクセス

  組織内のすべてのメンバーアカウントから、ストレージのメトリクスと使用状況に関するデータを集約するためには、組織の管理アカウントを使用して、S3 ストレージレンズの信頼されたアクセスを有効にする必要があります。その後、管理アカウントを直接使用するか、組織内の他のアカウントに管理者アクセス権限を委任すること (委任管理者) により、組織で使用するダッシュボードまたはエクスポートを作成できるようになります。

  S3 ストレージレンズの信頼できるアクセスはいつでも無効にできます。これにより S3 ストレージレンズは、組織に関するメトリクスの集約を停止します。

- 委任管理者

  組織の S3 ストレージレンズのダッシュボードとメトリクスの作成は、AWS Organizations の管理アカウントを使用するか、組織内の他のアカウントに委任管理者権限を付与することで実行できます。委任管理者の登録はいつでも解除できます。また、委任管理者の登録を解除すると、委任管理者によって作成されたすべての組織レベルのダッシュボードで、ストレージのメトリクスの新たな集計が自動的に停止されます。

詳細については、AWS Organizations ユーザーガイドの 「Amazon S3 ストレージレンズと AWS Organizations」 を参照してください。

Amazon S3 ストレージレンズでのサービスにリンクされたロール

AWS Organizations での信頼されたアクセスに加えて、Amazon S3 ストレージレンズでは、AWS Identity and Access Management (IAM) の、サービスにリンクされたロールも使用できます。サービスにリンクされたロールは S3 ストレージレンズに直接リンクされた一意のタイプの IAM ロールです。サービスにリンクされたロールは、S3 Storage Lens によって事前定義されています。このロールには、組織内のメンバーアカウントからストレージとアクティビティに関する日次のメトリクスを収集するために必要な、すべてのアクセス権限が含まれています。

詳細については、「Amazon S3 ストレージレンズでのサービスにリンクされたロールの使用」を参照してください。

Amazon S3 Storage Lens のメトリクスに関する用語集

Amazon S3 ストレージレンズメトリクスの用語集には、S3 Storage Lensの無料および高度なメトリクスの完全なリストが提供されています。

S3 ストレージレンズでは、すべてのダッシュボードと構成に対して無料のメトリクスを提供していますが、さらに、高度なメトリクスにアップグレードできるオプションも用意されています。

- 無料のメトリクスには、アカウント内のバケットやオブジェクトの数など、ストレージ使用状況に関連するメトリクスが含まれています。無料のメトリクスには、コスト最適化メトリクスやデータ保護メトリクスなどのユースケースに基づくメトリクスも含まれています。すべての無料メトリクスは毎日収集され、データは最長 14 日間のクエリに使用できます。
- 高度なメトリクスとレコメンデーションには、無料のメトリクスに含まれるすべてのメトリクスに加えて、高度なデータ保護やコスト最適化メトリクスなどの追加のメトリクスが含まれます。高度なメトリクスには、アクティビティメトリクスや詳細なステータスコードメトリクスなど、その他のメトリクスカテゴリも含まれます。高度なメトリクスのデータは 15 か月間クエリで使用できます。

  S3 Storage Lens で高度な推奨のメトリクスを使用すると、追加料金が発生します。詳細については、「Amazon S3 の料金」を参照してください。高度なメトリクスとレコメンデーションの詳細については、「メトリクスの選択」を参照してください。

> **Note**
>
> Storage Lens グループでは、無料利用枠のストレージメトリクスしか使用できません。高度なメトリクスは、Storage Lens グループレベルで利用できません。

メトリクス名

次の表のメトリクス名列には、S3 コンソールの各 S3 ストレージレンズの名前が表示されます。CloudWatch とエクスポート列には、Amazon CloudWatch の各メトリクスの名前と、S3 ストレージレンズダッシュボードで設定できるメトリクスエクスポートファイルが表示されます。

派生メトリクスの式

派生メトリクスは、メトリクスのエクスポートおよび CloudWatch 公開オプションでは使用できません。ただし、派生メトリクスの式列に表示されているメトリクス式を使用してコンピューティングすることは可能です。

Amazon S3 ストレージレンズメトリクスの単位倍数プレフィックス記号 (K、M、G など) の解釈

Amazon S3 ストレージレンズメトリクスの単位倍数はプレフィックス記号で書き込まれます。これらのプレフィックス記号は、国際度量衡局 (BIPM) によって標準化されている国際単位系 (SI) 記号と

一致しています。また、これらの記号は、測定単位の統一コード (UCUM) でも使用されています。詳細については、「SI プレフィックス記号の一覧」を参照してください。

> **Note**
>
> - S3 ストレージバイトの測定単位はバイナリギガバイト (GB) で、1 GB は 2^{30} バイト、1 TB は 2^{40} バイト、1 PB は 2^{50} バイトです。この測定単位は、国際電気標準会 (IEC) で定義されているように、ギビバイト (GiB) とも呼ばれます。
> - ライフサイクル設定に基づいて、オブジェクトが有効期限に達すると、存続期間が終了したオブジェクトは自動的に Amazon S3 削除キューに追加され、非同期的に削除されます。そのため、有効期限が切れる日と Amazon S3 がオブジェクトを削除する日との間に遅延が生じることがあります。S3 Storage Lens には、有効期限が切れても削除されていないオブジェクトのメトリクススは含まれません。S3 ライフサイクルの有効期限アクションの詳細については、「オブジェクトの有効期限」を参照してください。

次の表は、S3 ストレージレンズメトリクスの用語集を示しています。

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
合計ストレージ	StorageBytes	不完全なマルチパートアップロード、オブジェクトメタデータ、削除マーカーを含む、合計ストレージ	空き	概要	N	-

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
Object count (オブジェクト数)	ObjectCount	オブジェクトの総数	空き	概要	N	-
平均のオブジェクトサイズ	-	平均のオブジェクトサイズ	空き	概要	Y	sum(StorageBytes)/sum(ObjectCount)
Active buckets (アクティブなバケット)	-	ストレージが 0 バイトを超えるバケットの合計数	空き	概要	Y	-
バケット	-	バケットの合計数	空き	概要	Y	-
アカウント	-	ストレージがスコープ内にあるアカウントの数	空き	概要	Y	-
Current version bytes (現在のバージョンのバイト数)	CurrentVersionStorageBytes	オブジェクトの現在のバージョンのバイト数	空き	コスト最適化	N	-

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
% Current Version Bytes (現在のバージョンのバイト数)	-	オブジェクトの現在のバージョンであるスコープ内のバイトの割合	空き	コスト最適化	Y	sum(CurrentVersionStorageBytes)/sum(StorageBytes)
Current version object count (現在のバージョンのオブジェクト数)	現在のバージョンのオブジェクト数	現在のバージョンのオブジェクトの数	空き	データ保護	N	-
% current version objects (現在のバージョンのオブジェクト)	-	スコープ内のオブジェクトのうち、現在のバージョンであるオブジェクトの割合	空き	コスト最適化	Y	sum(CurrentVersionObjectCount)/sum(ObjectCount)

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
Noncurrent version bytes (現在のバージョンではないバイト数)	現在のバージョンではないストレージバイト数	現在のバージョンではないバイト数	空き	コスト最適化	N	-
% noncurrent version bytes (現在のバージョンではないバイト数)	-	スコープ内で、現在のバージョンではないバイトの割合	空き	コスト最適化	Y	sum(NonCurrentVersionStorageBytes)/ sum(StorageBytes)
Noncurrent version object count (現在のバージョンではないオブジェクト数)	現在のバージョンではないオブジェクト数	現在のバージョンではないオブジェクトの数	空き	コスト最適化	N	-

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
% noncurrent version objects (現在のバージョンではないオブジェクト数)	-	スコープ内のオブジェクトのうち、現在のバージョンではないオブジェクトの割合	空き	コスト最適化	Y	sum(NonCurrentVersionObjectCount)/ sum(ObjectCount)
Delete marker bytes (削除マーカーのバイト数)	DeleteMarkerStorageBytes	削除マーカーとなるスコープ内のバイト数	空き	コスト最適化	N	-
% delete marker bytes (削除マーカーバイト数)	-	削除マーカーであるバイト数の、スコープ内での割合	空き	コスト最適化	Y	sum(DeleteMarkerStorageBytes)/ sum(StorageBytes)

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
Delete marker object count (削除マーカーオブジェクト数)	DeleteMarkerObjectCount 削除マーカーオブジェクト数	削除マーカーがあるオブジェクトの総数	空き	コスト最適化	N	-
% delete marker objects (削除マーカーオブジェクト)	-	削除マーカーのあるオブジェクトの、スコープ内での割合	空き	コスト最適化	Y	sum(DeleteMarkerObjectCount)/sum(ObjectCount)
Incomplete multipart upload bytes (未完了のマルチパートアップロードのバイト数)	不完全なマルチパートアップロードストレージバイト数	スコープ内で未完了のマルチパートアップロードの合計バイト数	空き	コスト最適化	N	-

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
% incomplete multipart upload bytes (未完了のマルチパートアップロードのバイト数)	-	未完了のマルチパートアップロードの結果であるバイト数の、スコープ内での割合	空き	コスト最適化	Y	sum(IncompleteMultipartUploadStorageBytes)/ sum(StorageBytes)
Incomplete multipart upload object count (未完了のマルチパートアップロードのオブジェクト数)	MultipartUploadObjectCount 不完全なマルチパートアップロードストレージオブジェクト数	スコープ内でマルチパートアップロードが不完全であるオブジェクトの数	空き	コスト最適化	N	-
% incomplete multipart upload objects (未完了のマルチパートアップロードオブジェクト)	-	マルチパートアップロードが不完全であるオブジェクト数の、スコープ内での割合	空き	コスト最適化	Y	sum(IncompleteMultipartUploadObjectCount)/ sum(ObjectCount)

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
Incomplete multipart upload storage bytes greater than 7 days old (7 日以上経過した未完了のマルチパートアップロードストレージバイト数)	IncompleteMPUStorageBytesOlderThan7Days	7 日以上経過した未完了のマルチパートアップロードのスコープ内の合計バイト数	空き	コスト最適化	N	-
% incomplete multipart upload storage bytes greater than 7 days old (7 日以上経過した未完了のマルチパートアップロードストレージバイト)	-	7 日以上経過した未完了のマルチパートアップロードのバイトの割合	空き	コスト最適化	Y	sum(IncompleteMPUStorageBytesOlderThan7Days)/sum(StorageBytes)

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
Incomplete multipart upload object count greater than 7 days old (7 日以上経過した未完了のマルチパートアップロードオブジェクト数の割合)	IncompleteMPUObjectCountOlderThan7Days	7 日以上経過した未完了のマルチパートアップロードであるオブジェクトの数	空き	コスト最適化	N	-
% incomplete multipart upload object count greater than 7 days old (7 日以上経過した未完了のマルチパートアップロードオブジェクト数)	-	7 日以上経過した未完了のマルチパートアップロードであるオブジェクトの割合	空き	コスト最適化	Y	sum(IncompleteMPUObjectCountOlderThan7Days)/sum(ObjectCount)

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
Transition lifecycle rule count (移行ライフサイクルルールの数)	TransitionLifecycleRuleCount	オブジェクトを別のストレージクラスに移行するためのライフサイクルルールの数	アドバンスト	コスト最適化	N	-
Average transition lifecycle rules per bucket (バケットあたりの平均移行ライフサイクルルール)	-	オブジェクトを別のストレージクラスに移行するライフサイクルルールの平均数	アドバンスト	コスト最適化	Y	sum(TransitionLifecycleRuleCount)/sum(DistinctNumberOfBuckets)
Expiration lifecycle rule count (有効期限切れのライフサイクルルールの数)	ExpirationLifecycleRuleCount	オブジェクトを期限切れにするライフサイクルルールの数	アドバンスト	コスト最適化	N	-

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
Average expiration lifecycle rules per bucket (バケットあたりの平均有効期限ライフサイクルルール)	-	オブジェクトを期限切れにするライフサイクルルールの平均数	アドバンスト	コスト最適化	Y	sum(ExpirationLifecycleRuleCount)/sum(DistinctNumberOfBuckets)
Noncurrent version transition lifecycle rule count (最新バージョン移行ライフサイクルルール数)	NoncurrentVersionTransitionLifecycleRuleCount	最新でないオブジェクトバージョンを別のストレージクラスに移行するためのライフサイクルルールの数	アドバンスト	コスト最適化	N	
Average noncurrent version transition lifecycle rules per bucket (バケットごとの非最新バージョン移行ライフサイクルルールの平均数)	-	最新でないオブジェクトバージョンを別のストレージクラスに移行するためのライフサイクルルールの平均数	アドバンスト	コスト最適化	Y	sum(NoncurrentVersionTransitionLifecycleRuleCount)/sum(DistinctNumberOfBuckets)

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
Noncurrent version expiration lifecycle rule count (最新バージョンの有効期限切れライフサイクルルール数)	NoncurrentVersionExpirationLifecycleRuleCount	最新でないオブジェクトバージョンを期限切れにするライフサイクルルールの数	アドバンスト	コスト最適化	N	-
Average noncurrent version expiration lifecycle rules per bucket (バケットごとの最新でないバージョンの有効期限ライフサイクルルールの平均数)	-	最新でないオブジェクトバージョンを期限切れにするライフサイクルルールの平均数	アドバンスト	コスト最適化	Y	sum(NoncurrentVersionExpirationLifecycleRuleCount)/sum(DistinctNumberOfBuckets)

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
Abort incomplete multipart upload lifecycle rule count (未完了のマルチパートアップロードのライフサイクルルール数の中止	AbortIncompleteMPULifecycleRuleCount	未完了のマルチパートアップロードを削除するライフサイクルルールの数	アドバンスト	コスト最適化	N	-
Average abort incomplete multipart upload lifecycle rules per bucket (バケットあたりの未完了のマルチパートアップロードライフサイクルルールの平均中止数)	-	未完了のマルチパートアップロードを削除するライフサイクルルールの平均数	アドバンスト	コスト最適化	Y	sum(AbortIncompleteMPULifecycleRuleCount)/sum(DistinctNumberOfBuckets)

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
Expired object delete marker lifecycle rule count (期限切れオブジェクト削除マーカーのライフサイクルルール数)	ExpiredObjectDeleteMarkerLifecycleRuleCount	期限切れオブジェクト削除マーカーを削除するライフサイクルルールの数	アドバンスト	コスト最適化	N	-
Average expired object delete marker lifecycle rules per bucket (バケットあたりの期限切れオブジェクト削除マーカーのライフサイクルルールの平均値)	-	期限切れオブジェクト削除マーカーを削除するライフサイクルルールの平均数	アドバンスト	コスト最適化	Y	sum(ExpiredObjectDeleteMarkerLifecycleRuleCount)/sum(DistinctNumberOfBuckets)
Total lifecycle rule count (ライフサイクルルールの総数)	TotalLifecycleRuleCount	ライフサイクルルールの総数	アドバンスト	コスト最適化	N	-

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
Average lifecycle rule count per bucket (バケットあたりの平均ライフサイクルルール数)	-	ライフサイクルルールの平均数	アドバンスト	コスト最適化	Y	sum(TotalLifecycleRuleCount)/sum(DistinctNumberOfBuckets)
Encrypted bytes (暗号化されたバイト数)	暗号化ストレージバイト数	暗号化されたバイトの合計数	空き	データ保護	N	-
% encrypted bytes (暗号化されたバイト数)	-	暗号化された合計バイト数の割合	空き	データ保護	Y	sum(EncryptedObjectCount)/sum(StorageBytes)
Encrypted object count (暗号化されたオブジェクトの数)	EncryptedObjectCount	暗号化されたオブジェクトの合計数	空き	データ保護	N	-

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
% encrypted objects (暗号化されたオブジェクト数)	-	暗号化されたオブジェクトの割合	空き	データ保護	Y	sum(EncryptedStorageBytes)/sum(ObjectCount)
Unencrypted bytes (暗号化されていないバイト数)	UnencryptedStorageBytes	暗号化されていないバイト数	空き	データ保護	Y	sum(StorageBytes) - sum(EncryptedStorageBytes)
% unencrypted bytes (暗号化されていないバイト数)	-	暗号化されていないバイト数の割合	空き	データ保護	Y	sum(UnencryptedStorageBytes)/sum(StorageBytes)
Unencrypted object count (暗号化されていないオブジェクト数)	UnencryptedObjectCount	暗号化されていないオブジェクトの総数	空き	データ保護	Y	sum(ObjectCount) - sum(EncryptedObjectCount)

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
% unencrypted objects (暗号化されていないオブジェクト数)	-	暗号化されていないオブジェクトの割合	空き	データ保護	Y	sum(UnencryptedStorageBytes)/ sum(ObjectCount)
Replicated storage bytes source (レプリケートされたストレージバイト数ソース)	ReplicatedStorageBytesSource	ソースバケットからレプリケートされた合計バイト数	空き	データ保護	N	-
% replicated bytes source (レプリケートされたバイトソース)	-	ソースバケットからレプリケートされた合計バイト数の割合	空き	データ保護	Y	sum(ReplicatedStorageBytesSource)/ sum(StorageBytes)

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
Replicated object count source (レプリケートされたオブジェクト数のソース)	ReplicatedObjectCountSource	ソースバケットからレプリケートされたオブジェクトの数	空き	データ保護	N	-
% replicated objects source (レプリケートされたオブジェクトソース)	-	ソースバケットからレプリケートされた全オブジェクト数の割合	空き	データ保護	Y	sum(ReplicatedStorageObjectCount)/sum(ObjectCount)
レプリケートされたストレージバイトの送信先	レプリケートされたストレージバイト数	送信先バケットにレプリケートされた合計バイト数	空き	データ保護	N	-
% replicated bytes destination (レプリケートされるバイト数送信先)	-	送信先バケットにレプリケートされた合計バイト数の割合	空き	データ保護	Y	sum(ReplicatedStorageBytesSource)/sum(StorageBytes)

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
Replicated object count destination (レプリケートされたオブジェクト数の送信先)	レプリケートされたオブジェクト数	送信先バケットにレプリケートされたオブジェクトの数	空き	データ保護	N	-
% replicated objects destination (レプリケートされたオブジェクトの送信先)	-	送信先バケットにレプリケートされた全オブジェクト数の割合	空き	データ保護	Y	sum(ReplicatedObjectCount)/sum(ObjectCount)
Object Lock bytes (オブジェクトロックバイト数)	オブジェクトロックが有効なストレージバイト数	オブジェクトロックが有効なストレージバイトの総数	空き	データ保護	N	sum(UnencryptedStorageBytes)/sum(ObjectLockEnabledStorageCount) - sum(ObjectLockEnabledStorageBytes)

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
% Object Lock bytes (オブジェクトロックバイト数)	-	オブジェクトロックが有効なストレージバイトの割合	空き	データ保護	Y	sum(ObjectLockEnabledStorageBytes)/sum(StorageBytes)
Object Lock object count (オブジェクトロックオブジェクト数)	不完全なマルチパートアップロードストレージオブジェクト数	オブジェクトロックオブジェクトの総数	空き	データ保護	N	-
% Object Lock objects (オブジェクトロックオブジェクト数)	-	オブジェクトロックが有効になっている全オブジェクト数の割合	空き	データ保護	Y	sum(ObjectLockEnabledObjectCount)/sum(ObjectCount)
Versioning-enabled bucket count (バージョニングが有効なバケット数)	VersioningEnabledBucketCount	S3 バージョニングが有効になっているバケットの数	空き	データ保護	N	-

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
% versioning-enabled buckets (バージョニングが有効なバケット)	-	S3 バージョニングが有効になっているバケットの割合	空き	データ保護	Y	sum(VersioningEnabledBucketCount)/ sum(DistinctNumberOfBuckets)
MFA delete-enabled bucket count (MFA Delete が有効なバケット数)	MFADeleteEnabledBucketCount	MFA (多要素認証) Delete が有効になっているバケット数	空き	データ保護	N	-
% MFA delete-enabled buckets (MFA Delete が有効化されたバケット)	-	MFA (多要素認証) Delete が有効化されたバケットの割合	空き	データ保護	Y	sum(MFADeleteEnabledBucketCount)/ sum(DistinctNumberOfBuckets)

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
SSE-KMS enabled bucket count (SSE-KMS が有効化されたバケット数)	SSEKMSEnabledBucketCount	デフォルトのバケット暗号化に AWS Key Management Service キーのサーバー側暗号化 (SSE-KMS) を使用しているバケット数	空き	データ保護	N	-
% SSE-KMS enabled buckets (SSE-KMS が有効化されたバケット)	-	デフォルトのバケット暗号化に SSE-KMS を使用しているバケットの割合	空き	データ保護	Y	sum(SSEKMSEnabledBucketCount)/sum(DistinctNumberOfBuckets)
All unsupported signature requests (サポートされていないすべての署名リクエスト)	AllUnsupportedSignatureRequests	サポートされていない AWS 署名バージョンを使用したリクエストの総数	アドバンスト	データ保護	N	-

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
% all unsupported signature requests (サポートされていないすべての署名リクエスト)	-	サポートされていない AWS 署名バージョンを使用するリクエストの割合	アドバンスト	データ保護	Y	sum(AllUnsupportedSignatureRequests) / sum(AllRequests)
All unsupported TLS requests (サポートされていないすべての TLS リクエスト)	AllUnsupportedTLSRequests	サポートされていない Transport Layer Security (TLS) を使用するリクエストの数	アドバンスト	データ保護	N	-
% all unsupported TLS requests (サポートされていないすべての TLS リクエスト)	-	サポートされていない TLS バージョンを使用するリクエストの割合	アドバンスト	データ保護	Y	sum(AllUnsupportedTLSRequests)/ sum(AllRequests)

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
All SSE-KMS requests (すべての SSE-KMS リクエスト)	AllSSEKMSRequests	SSE-KMS を指定したリクエストの総数	アドバンスト	データ保護	N	-
% all SSE-KMS requests (すべての SSE-KMS リクエスト)	-	SSE-KMS を指定したリクエストの割合	アドバンスト	データ保護	Y	sum(AllSSEKMSRequests)/sum(AllRequests)
Same-Region Replication rule count (同一リージョンレプリケーションルールの数)	SameRegionReplicationRuleCount	同一リージョンレプリケーション (SRR) のレプリケーションルールの数	アドバンスト	データ保護	N	-

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
Average Same-Region Replication rules per bucket (バケットあたりの同一リージョンレプリケーションルールの平均数)	-	SRR の平均レプリケーションルールの数	アドバンスト	データ保護	Y	sum(SameRegionReplicationRuleCount)/sum(DistinctNumberOfBuckets)
Cross-Region Replication rule count (クロスリージョンレプリケーションルールの数)	CrossRegionReplicationRuleCount	クロスリージョンレプリケーション (CRR) のレプリケーションルールの数	アドバンスト	データ保護	N	-
Average Cross-Region Replication rules per bucket (バケットあたりのクロスリージョンレプリケーションの平均数)	-	CRR のレプリケーションルールの平均数	アドバンスト	データ保護	Y	sum(CrossRegionReplicationRuleCount) / sum(DistinctNumberOfBuckets)

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
Same-account replication rule count (同一アカウントレプリケーションルールの数)	SameAccountReplicationRuleCount	同じアカウント内のレプリケーション用のレプリケーションルールの数	アドバンスト	データ保護	N	-
Average same-account replication rules per bucket (バケットあたりの同一アカウントレプリケーションルール平均数)	-	同じアカウント内のレプリケーション用のレプリケーションルールの平均数	アドバンスト	データ保護	Y	sum(SameAccountReplicationRuleCount) / sum(DistinctNumberOfBuckets)
Cross-account replication rule count (クロスアカウントレプリケーションルールの数)	CrossAccountReplicationRuleCount	クロスアカウントレプリケーションのレプリケーションルールの数	アドバンスト	データ保護	N	-

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
Average cross-account replication rules per bucket (バケットあたりのクロスアカウントレプリケーションルールの平均数)	-	クロスアカウントレプリケーションのレプリケーションルールの平均数	アドバンスト	データ保護	Y	sum(CrossAccountReplicationRuleCount)/sum(DistinctNumberOfBuckets)
Invalid destination replication rule count (無効な送信先レプリケーションルールの数)	InvalidDestinationReplicationRuleCount	レプリケーション先が有効でないレプリケーションルールの数	アドバンスト	データ保護	N	-
Average invalid destination replication rules per bucket (バケットあたりの無効な送信先レプリケーションルールの平均数)	-	レプリケーション先が有効でないレプリケーションルールの平均数	アドバンスト	データ保護	Y	sum(InvalidReplicationRuleCount)/sum(DistinctNumberOfBuckets)

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
Total replication rule count (レプリケーションルールの総数)	-	レプリケーションルールの総数	アドバンスト	データ保護	Y	-
Average replication rule count per bucket (バケットあたりの平均レプリケーションルール数)	-	レプリケーションルールの合計数の平均	アドバンスト	データ保護	Y	sum(all replication rule count metrics)/ sum(DistinctNumberOfBuckets)
Object Ownership bucket owner enforced bucket count (オブジェクトの所有権のバケット所有者強制バケット数)	ObjectOwnershipBucketOwnerEnforcedBucketCount	オブジェクトの所有権のバケット所有者強制設定を使用して、アクセスコントロールリスト (ACL) を無効にしたバケットの総数	空き	アクセス管理	N	-

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
% Object Ownership bucket owner enforced buckets (オブジェクトの所有権のバケット所有者強制バケット)	-	オブジェクトの所有権のバケット所有者強制設定を使用して ACL を無効にしたバケットの割合	空き	アクセス管理	Y	sum(ObjectOwnershipBucketOwnerEnforcedBucketCount)/ sum (DistinctNumberOfBuckets)
Object Ownership bucket owner preferred bucket count (オブジェクトの所有権のバケット所有者の優先バケット数)	ObjectOwnershipBucketOwnerPreferredBucketCount	オブジェクト所有権のバケット所有者優先設定を使用するバケットの総数	空き	アクセス管理	N	-

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
% Object Ownership bucket owner preferred buckets (オブジェクトの所有権のバケット所有者優先バケット)	-	オブジェクトの所有権のバケット所有者優先設定を使用するバケットの割合	空き	アクセス管理	Y	sum(ObjectOwnershipBucketOwnerPreferredBucketCount)/ sum(DistinctNumberOfBuckets)
Object Ownership object writer bucket count (オブジェクトの所有権オブジェクトライターバケット数)	ObjectOwnershipObjectWriterBucketCount	オブジェクトの所有権のオブジェクトライター設定を使用するバケットの総数	空き	アクセス管理	N	-

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
% Object Ownership object writer buckets (オブジェクトの所有権のオブジェクトライターバケット)	-	オブジェクト所有権のオブジェクトライター設定を使用するバケットの割合	空き	アクセス管理	Y	sum(ObjectOwnershipObjectWriterBucketCount)/sum(DistinctNumberOfBuckets)
Transfer Acceleration enabled bucket count (Transfer Acceleration が有効化されたバケット数)	TransferAccelerationEnabledBucketCount	Transfer Acceleration が有効化されたバケットの総数	空き	パフォーマンス	N	-
% Transfer Acceleration enabled buckets (Transfer Acceleration が有効化されたバケット)	-	Transfer Acceleration が有効化されたバケットの割合	空き	パフォーマンス	Y	sum(TransferAccelerationEnabledBucketCount)/sum(DistinctNumberOfBuckets)

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
Event Notification enabled bucket count (イベント通知が有効化されたバケット数)	EventNotificationEnabledBucketCount	イベント通知が有効化されたバケットの総数	空き	イベント	N	
% Event Notification enabled buckets (イベント通知が有効化されたバケット)	-	イベント通知が有効化されたバケットの割合	空き	イベント	Y	sum(EventNotificationEnabledBucketCount)/sum(DistinctNumberOfBuckets)
すべてのリクエスト	AllRequests	作成されたリクエストの総数	アドバンスト	アクティビティ	N	-

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
リクエストの取得	GetRequests	作成された GET リクエストの総数	アドバンスト	アクティビティ	N	-
Put requests (Put リクエスト)	PutRequests	作成された PUT リクエストの総数	アドバンスト	アクティビティ	N	-
Head requests (Head リクエスト)	HeadRequests	作成された HEAD リクエストの総数	アドバンスト	アクティビティ	N	-
Delete requests (Delete リクエスト)	DeleteRequests	作成された DELETE リクエストの総数	アドバンスト	アクティビティ	N	-

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
リクエストを一覧表示	ListRequests	作成された LIST リクエストの総数	アドバンスト	アクティビティ	N	-
Post requests (Post リクエスト)	PostRequests	作成された POST リクエストの総数。	アドバンスト	アクティビティ	N	-
Select requests (Select リクエスト)	SelectRequests	S3 Select リクエストの総数	アドバンスト	アクティビティ	N	-
Select scanned bytes (スキャンされた Select バイト)	SelectScannedBytes	スキャンされた S3 Select バイトの数	アドバンスト	アクティビティ	N	-

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
Select returned bytes (返された Select バイト)	SelectReturnedBytes	返された S3 Select バイトの数	アドバンスト	アクティビティ	N	-
ダウンロードされたバイト数	BytesDownloaded	ダウンロードされたバイトの数	アドバンスト	アクティビティ	N	-
% retrieval rate (取得率)	-	ダウンロードされたバイト数の割合	アドバンスト	アクティビティ	Y	sum(BytesDownloaded)/sum(StorageBytes)
アップロードされたバイト数	BytesUploaded	アップロード済みとなっているバイト数。	アドバンスト	アクティビティ	N	-

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
% ingest ratio (取り込み率)	-	アップロード済みとなっているバイト数の割合	アドバンスト	アクティビティ	Y	sum(BytesUploaded) / sum(StorageBytes)
4xx errors (4xx エラー)	4xxErrors	HTTP 4xx ステータスコードの総数	アドバンスト	アクティビティ	N	-
5xx errors (5xx エラー)	5xxErrors	HTTP 5xx ステータスコードの総数	アドバンスト	アクティビティ	N	-
Total errors (エラー総数)	-	4xx と 5xx のすべてのエラーを合計した数	アドバンスト	アクティビティ	Y	sum(4xxErrors) + sum(5xxErrors)

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
% error rate (エラー率)	-	4xx と 5xx のエラーの総数がリクエストの総数に占める割合	アドバンスト	アクティビティ	Y	sum(TotalErrors)/sum(TotalRequests)
200 OK status count (200 OK ステータスの数)	200OKStatusCount	200 OK ステータスコードの総数	アドバンスト	詳細なステータスコード	N	-

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
% 200 OK status (200 OK ステータス)	-	200 OK ステータスコードの総数がリクエストの総数に占める割合	アドバンスト	詳細なステータスコード	Y	sum(200OKStatusCount)/sum(AllRequests)
206 Partial Content status count (206 部分コンテンツステータスの数)	206PartialContentStatusCount	206 部分コンテンツステータスコードの総数	アドバンスト	詳細なステータスコード	N	-

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
% 206 Partial Content status (206 部分コンテンツステータス)	-	206 部分コンテンツステータスコードの合計数がリクエストの総数に占める割合	アドバンスト	詳細なステータスコード	Y	sum(206PartialContentStatusCount)/sum(AllRequests)
400 Bad Request error count (400 Bad Request エラー数)	400BadRequestErrorCount	400 Bad Request ステータスコードの総数	アドバンスト	詳細なステータスコード	N	-

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
% 400 Bad Request errors (400 Bad Request エラー)	-	400 Bad Request ステータスコードの合計数がリクエストの総数に占める割合	アドバンスト	詳細なステータスコード	Y	sum(400BadRequestErrorCount)/sum(All Requests)
403 Forbidden error count (403 Forbidden エラー数)	403ForbiddenErrorCount	403 Forbidden ステータスコードの総数	アドバンスト	詳細なステータスコード	N	-

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
% 403 Forbidden errors (403 Forbidden エラー)	-	403 Forbidden ステータスコードの総数がリクエストの総数に占める割合	アドバンスト	詳細なステータスコード	Y	sum(403ForbiddenErrorCount) / sum(AllRequests)
404 Not Found error count (404 Not Found エラー数)	404NotFoundErrorCount	404 Not Found ステータスコードの総数	アドバンスト	詳細なステータスコード	N	-

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
% 404 Not Found errors (404 Not Found エラー)	-	404 Not Found ステータスコードの合計数がリクエストの総数に占める割合	アドバンスト	詳細なステータスコード	Y	sum(404NotFoundErrorCount)/sum(AllRequests)
500 Internal Server Error count (500 Internal Server Error の数)	500InternalServerErrorCount	500 Internal Server Error ステータスコードの総数	アドバンスト	詳細なステータスコード	N	-

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
% 500 Internal Server Errors	-	500 Internal Server Errors の合計数がリクエストの総数に占める割合	アドバンスト	詳細なステータスコード	Y	sum(500InternalServerErrorCount)/sum(AllRequests)
503 Service Unavailable error count (503 Service Unavailable エラー数)	503ServiceUnavailableErrorCount	503 Service Unavailableステータスコードの総数	アドバンスト	詳細なステータスコード	N	-

メトリクス名	CloudWatch とエクスポート	説明	ティア[1]	カテゴリ[2]	派生	派生メトリクスの式
% 503 Service Unavailable errors (503 Service Unavailable エラー)	-	503 Service Unavailable ステータスコードの合計数がリクエスト総数に占める割合	アドバンスト	詳細なステータスコード	Y	sum(503ServiceUnavailableErrorCount) / sum(AllRequests)

[1] すべての無料ティアストレージメトリクスは、Storage Lens グループレベルで利用できます。高度なメトリクスは、Storage Lens グループレベルで利用できません。

[2] ルール数メトリクスとバケット設定メトリクスは、プレフィックスレベルで使用できません。

Amazon S3 ストレージレンズアクセス許可の設定

Amazon S3 ストレージレンズでは、S3 ストレージレンズの各アクションへのアクセスを許可するために、AWS Identity and Access Management (IAM) の新しいアクセス許可が必要となります。これらのアクセス許可を付与するには、アイデンティティベースの IAM ポリシーを使用できます。このポリシーを、IAM ユーザー、グループ、またはロールにアタッチして、アクセス許可を付与することができます。このようなアクセス許可には、S3 Storage Lens の有効化または無効化や、S3 Storage Lens ダッシュボードや設定へのアクセスなどが含まれます。

これらの IAM ユーザーまたはロールは、以下の条件の両方に当てはまる場合を除き、ダッシュボードまたはその設定を作成または所有しているアカウントに属している必要があります。

- アカウントが AWS Organizations のメンバーです。
- 委任管理者として管理アカウントによって、組織レベルのダッシュボードを作成するアクセスを付与されています。

> **Note**
>
> - Amazon S3 ストレージレンズダッシュボードを表示するために、アカウントのルートユーザーの認証情報を使用することはできません。S3 ストレージレンズダッシュボードにアクセスするには、新規または既存の IAM ユーザーに対し、必要な IAM アクセス許可を付与する必要があります。その後、それらのユーザーの認証情報によりサインインを行い、S3 Storage Lens ダッシュボードにアクセスします。詳細については、「IAM ユーザーガイド」の「IAM でのセキュリティベストプラクティス」を参照してください。
> - Amazon S3 コンソールで S3 ストレージレンズを使用するには、複数のアクセス許可が必要になることがあります。例えば、コンソールでダッシュボードを編集するには、次の許可が必要です。
>   - `s3:ListStorageLensConfigurations`
>   - `s3:GetStorageLensConfiguration`
>   - `s3:PutStorageLensConfiguration`

トピック

- アカウントで S3 ストレージレンズを使用するためのアクセス許可の設定
- アカウントで S3 Storage Lens グループを使用するためのアクセス許可の設定
- AWS Organizations を使用した S3 ストレージレンズを使用するための許可の設定

アカウントで S3 ストレージレンズを使用するためのアクセス許可の設定

S3 Storage Lens ダッシュボードと Storage Lens ダッシュボード設定を作成して管理するには、実行するアクションに応じて次の権限が必要です。

次の表は、Amazon S3 ストレージレンズに関連する IAM アクセス許可を示しています。

アクション	IAM アクセス許可
Amazon S3 コンソールで S3 ストレージレンズダッシュボードを作成または更新します。	s3:ListStorageLensConfigurations s3:GetStorageLensConfiguration s3:GetStorageLensConfigurationTagging s3:PutStorageLensConfiguration s3:PutStorageLensConfigurationTagging
Amazon S3 コンソールで S3 ストレージレンズダッシュボードのタグを取得します。	s3:ListStorageLensConfigurations s3:GetStorageLensConfigurationTagging
Amazon S3 コンソールに S3 ストレージレンズダッシュボードを表示します。	s3:ListStorageLensConfigurations s3:GetStorageLensConfiguration s3:GetStorageLensDashboard
Amazon S3 コンソールで S3 ストレージレンズダッシュボードを削除します。	s3:ListStorageLensConfigurations s3:GetStorageLensConfiguration s3:DeleteStorageLensConfiguration
AWS CLI または AWS SDK により S3 ストレージレンズの設定を作成または更新します。	s3:PutStorageLensConfiguration s3:PutStorageLensConfigurationTagging
AWS CLI または AWS SDK により S3 ストレージレンズの設定のタグを取得します。	s3:GetStorageLensConfigurationTagging

アクション	IAM アクセス許可
AWS CLI または AWS SDK により S3 ストレージレンズの設定を表示します。	`s3:GetStorageLensConfiguration`
AWS CLI または AWS SDK により S3 ストレージレンズの設定を削除します。	`s3:DeleteStorageLensConfiguration`

Note

- IAM ポリシーでリソースタグを使用すると、アクセス許可を管理できます。
- これらのアクセス許可を持つ IAM ユーザーまたはロールは、バケットおよびプレフィックスからのメトリクスを参照できます。ただし、オブジェクトの読み出しまたは一覧表示のための、直接的なアクセス許可がない場合があります。
- プレフィックスレベルのメトリクスが有効になっている S3 Storage Lens ダッシュボードでは、選択したプレフィックスパスがオブジェクトキーと一致すると、ダッシュボードにそのオブジェクトキーが別のプレフィックスとして表示されることがあります。
- ご自身のアカウントのバケットに保存されているメトリクスをエクスポートする場合は、IAM ポリシー内の既存の `s3:GetObject` アクセス許可により権限が付与されます。これと同様に、AWS Organizations エンティティであれば、組織の管理アカウントまたは委任管理者アカウントとして IAM ポリシーを使用することで、組織レベルのダッシュボードと設定への許可を管理できます。

アカウントで S3 Storage Lens グループを使用するためのアクセス許可の設定

S3 Storage Lens グループを使用すると、プレフィックス、サフィックス、オブジェクトタグ、オブジェクトサイズ、またはオブジェクト経過時間に基づいてバケット内のストレージの分布を把握できます。Storage Lens グループをダッシュボードにアタッチすると、集約されたメトリクスを表示できます。

Storage Lens グループを操作するには、特定の権限が必要です。詳細については、「the section called “Storage Lens グループのアクセス許可。”」を参照してください。

AWS Organizations を使用した S3 ストレージレンズを使用するための許可の設定

Amazon S3 ストレージレンズを使用することで、AWS Organizations の階層に属しているすべてのアカウントから、ストレージのメトリクスと使用状況に関するデータを収集できます。次の表は、Organizations での S3 ストレージレンズの使用に関連する、アクションとアクセス許可を示しています。

アクション	IAM アクセス許可
S3ストレージレンズのために、信頼されたアクセスを組織内で有効にします。	`organizations:EnableAWSServiceAccess`
組織内で、S3 ストレージレンズのために信頼されたアクセスを無効にします。	`organizations:DisableAWSServiceAccess`
組織内で、S3 ストレージレンズダッシュボードまたはその設定を作成するために、委任管理者を登録します。	`organizations:RegisterDelegatedAdministrator`
委任管理者の登録を解除して、組織の S3 ストレージレンズダッシュボードまたは設定を作成できないようにします。	`organizations:DeregisterDelegatedAdministrator`

組織全体のために S3 ストレージレンズの設定を作成するための追加のアクセス許可	`organizations:DescribeOrganization`
	`organizations:ListAccounts`
	`organizations:ListAWSServiceAccessForOrganization`
	`organizations:ListDelegatedAdministrators`
	`iam:CreateServiceLinkedRole`

コンソールと API を使用した Amazon S3 ストレージレンズの使用

Amazon S3 ストレージレンズは、オブジェクトストレージの使用状況とアクティビティを組織全体で可視化するために使用できるクラウドストレージの分析機能です。S3 ストレージレンズメトリクスを使用することで、組織全体でどれだけのストレージがあるか、または最も急速に成長しているバケットとプレフィックスは何かなどの、要約されたインサイトを生成できます。S3 ストレージレンズメトリクスを使用して、コスト最適化の機会を特定し、データ保護とセキュリティのベストプラクティスを実装し、アプリケーションワークロードのパフォーマンスを向上させることもできます。例えば、S3 ライフサイクルルールがないバケットを特定して、7 日以上経過した未完了のマルチパートアップロードを有効期限切れにできます。また、S3 レプリケーションや S3 バージョニング使用など、データ保護のベストプラクティスに従っていないバケットを特定することもできます。また、S3 ストレージレンズは、メトリクスを分析して、ストレージコストを最適化し、データ保護に関するベストプラクティスを適用するために使用できるコンテキストに応じた推奨事項を提供します。

S3 ストレージレンズはメトリクスを集約し、Amazon S3 コンソールの [Buckets] (バケット) ページの [Account snapshot] (アカウントスナップショット) セクションにこの情報を表示します。S3 Storage Lens は、インサイトと傾向を可視化したり、外れ値にフラグ付けしたり、ストレージコストの最適化やデータ保護のベストプラクティスの適用に関するレコメンデーション事項を受け取ったりするために使用できるインタラクティブダッシュボードも提供します。ダッシュボードには、組織、アカウント、AWS リージョン、ストレージクラス、バケット、プレフィックス、またはストレージレンズのグループレベルでインサイトを生成して可視化できる、ドリルダウンオプションが用意されています。1 日 1 回のメトリクスのエクスポートを CSV 形式または Parquet 形式で S3 バケットに送信することもできます。

以下のセクションでは、S3 Storage Lens の設定の作成、更新、表示例を示します。また、機能に関連した操作例もご覧いただけます。ここでの例には、AWS Organizations で S3 Storage Lens を使用している場合のユースケースも含まれます。この例の中の変数の値は、ご自身の用途に合った値に置き換えてご使用になれます。

トピック

- Amazon S3 ストレージレンズダッシュボードを作成する
- Amazon S3 ストレージレンズダッシュボードの更新
- Amazon S3 ストレージレンズダッシュボードの無効化
- Amazon S3 ストレージレンズダッシュボードの削除
- Amazon S3 ストレージレンズダッシュボードを一覧表示する

- Amazon S3 ストレージレンズダッシュボード設定の詳細を表示する
- S3 ストレージレンズによる AWS リソースタグの管理
- Amazon S3 ストレージレンズを使用するためのヘルパーファイル

Amazon S3 ストレージレンズダッシュボードを作成する

AWS Organizations の組織、またはアカウント内の特定の AWS リージョンやバケットにスコープを設定できる、追加の S3 ストレージレンズカスタムダッシュボードを作成できます。

> **Note**
>
> ダッシュボード構成への更新が正確に表示または視覚化されるまでに最大 48 時間かかる場合があります。

S3 コンソールの使用

Amazon S3 コンソールで Amazon S3 Storage Lens ダッシュボードを作成するには、次の手順に従います。

ステップ 1: ダッシュボードのスコープを定義する

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ページ上部にあるナビゲーションバーで、現在表示されている AWS リージョンの名前をクリックします。次に、切り替え先のリージョンを選択します。
3. ナビゲーションペインの、[S3 ストレージレンズ] で、[ダッシュボード] を選択します。
4. [ダッシュボードの作成] を選択します。
5. ダッシュボードページの [全般] セクションで、次の操作を行います。
   a. ダッシュボードの [ホームリージョン] を表示します。ホームリージョンとは、この Storage Lens ダッシュボード設定とメトリクスが保存される AWS リージョン です。
   b. ダッシュボード名を入力します。

      ダッシュボード名は 65 文字未満で記述する必要があり、特殊文字またはスペースを含めることはできません。

> **Note**
>
> ダッシュボードが作成された後は、このダッシュボード名を変更することはできません。

c. 必要に応じて、ダッシュボードにタグを追加することもできます。タグは、ダッシュボードのアクセス許可を管理し、S3 Storage Lens のコストを追跡するために使用できます。

詳細については、IAM ユーザーガイドのリソースタグを使用したアクセスの制御、および AWS Billing ユーザーガイドの AWS 生成コスト配分タグを参照してください。

> **Note**
>
> ダッシュボードの設定には、最大 50 個のタグを追加できます。

6. [ダッシュボードスコープ] セクションで、次の操作を行います。

a. S3 Storage Lens でダッシュボードに含める、または除外するリージョンとバケットを選択します。

b. S3 Storage Lens で含める、または除外するバケットを、選択したリージョンの中で選択します。バケットを含めるか除外するかの設定は可能ですが、両方を同時に設定することはできません。このオプションは、組織レベルのダッシュボードを作成するときには使用できません。

> **Note**
>
> - リージョンとバケットを、含めるか除外するかの選択が可能です。組織内のメンバーアカウント間で組織レベルのダッシュボードを作成する場合には、このオプションはリージョンのみに対し使用できます。
> - 含めるか除外するバケットは最大 50 個まで選択できます。

ステップ 2: メトリクスの選択を設定する

1. [メトリクスの選択] セクションで、このダッシュボードで集約するメトリクスのタイプを選択します。

- バケットレベルで集計され、14 日間のクエリに使用できる無料のメトリクスを含めるには、[Free metrics] (無料のメトリクス) を選択します。
- 高度なメトリクスやその他の詳細オプションを有効にするには、[Advanced metrics and recommendations] (高度なメトリクスとレコメンデーション) を選択します。これらのオプションには、高度なプレフィックス集約、Amazon CloudWatch パブリッシング、コンテキストに応じた推奨事項が含まれます。データは 15 か月間クエリで使用できます。高度な高度なメトリクスとレコメンデーションには追加料金がかかります。詳細については、「Amazon S3 の料金」を参照してください。

  無料のメトリクスと高度なメトリクスの詳細については、「メトリクスの選択」を参照してください。

2. [Advanced metrics and recommendations features] (高度なメトリクスとレコメンデーション機能) で、有効にするオプションを選択します。

   - Advanced metrics (高度なメトリクス)
   - [CloudWatch publishing] (CloudWatch パブリッシング)
   - プレフィックス集約

   > **Important**
   >
   > S3 Storage Lens 設定で [プレフィックス集約] を有効にすると、プレフィックスレベルのメトリクスは CloudWatch に公開されません。バケット、アカウント、組織レベルの S3 Storage Lens メトリクスのみが CloudWatch に公開されます。

3. [Advanced metrics] (高度なメトリクス) を有効にした場合は、S3 ストレージレンズダッシュボードに表示する [Advanced metrics categories] (高度なメトリクスのカテゴリ) を選択します。

   - アクティビティのメトリクス
   - [Detailed status code metrics] (詳細なステータスコードメトリクス)
   - [Advanced cost optimization metrics] (高度なコスト最適化メトリクス)
   - [Advanced data protection metrics] (高度なデータ保護メトリクス)

   メトリクスのカテゴリの詳細については、「メトリクスのカテゴリ」を参照してください。メトリクスの一覧については、「Amazon S3 Storage Lens のメトリクスに関する用語集」を参照してください。

4. [プレフィックス集約] を有効にする場合は、次の設定を行います。

   a. このダッシュボードのプレフィックスしきい値の最小サイズを選択します。

      例えば、プレフィックスのしきい値を 5% とした場合は、バケットの合計ストレージサイズが 5% 以上を占めるプレフィックスが集約されることを示します。

   b. プレフィックスの深度を選択します。

      この設定は、プレフィックスが評価される階層レベルの最大数を示します。プレフィックスの深度は、10 未満で指定する必要があります。

   c. プレフィックスの区切り文字を入力します。

      この値は、各プレフィックスのレベルを識別するために使用されます。Amazon S3 でのデフォルト値は、/ 文字ですが、実際のストレージ構造では他の区切り文字を使用することも可能です。

(オプション) ステップ 3: ダッシュボードでメトリクスをエクスポートする

1. [Metrics export] (メトリクスのエクスポート) セクションで、選択した保存先バケットに毎日出力されるメトリクスのエクスポートを作成するには、[Enable] (有効化) をクリックします。

   メトリクスのエクスポートは、CSV または Apache Parquet 形式で作成されます。メトリクスのエクスポートには、S3 Storage Lens ダッシュボードのデータと同じスコープが適用され、レコメンデーション事項は付加されません。

2. メトリクスのエクスポートを有効にした場合は、日次メトリクスのエクスポートの出力形式として、[CSV] または [Apache Parquet] を選択します。

   Parquet は、Hadoop 用のオープンソースなファイル形式で、ネストされたデータを平坦な列指向形式で格納します。

3. メトリクスのエクスポート先の S3 バケットを選択します。

   バケットは、S3 Storage Lens ダッシュボードを使用している現在のアカウント内で選択できます。また、エクスポート先バケットへの許可と、そのバケットの所有者アカウント ID がある場合は、別の AWS アカウント を選択することも可能です。

4. 送信先 S3 バケット (形式: `s3://`*`bucket-name`*`/`*`prefix`*) を選択します。

   バケットのアドレスは、S3 ストレージレンズダッシュボードのホームリージョンにある必要があります。S3 コンソールには、Amazon S3 によって保存先バケットのポリシーに追加さ

れる [Destination bucket permission] (エクスポート先バケットのアクセス許可) が表示されます。Amazon S3 は、エクスポート先バケットのバケットポリシーを更新し、S3 がそのバケットにデータを配置できるようにします。

5. (オプション) メトリクスのエクスポートでサーバー側の暗号化を有効にするには、[Specify an encryption key] (暗号化キーの指定) を選択します。その後、[暗号化タイプ] として [Amazon S3 マネージドキー (SSE-S3)] または [AWS Key Management Service キー (SSE-KMS)] を選択します。

   キーのタイプは、Amazon S3 が管理するキー (SSE-S3) と AWS Key Management Service (AWS KMS) キー (SSE-KMS) のいずれかから選択できます。

6. (オプション) AWS KMS キーを指定するには、KMS マスターキーを選択するか、キーとなる Amazon リソースネーム (ARN) を入力する必要があります。

   カスタマーマネージドキーを選択した場合、Amazon S3 ストレージレンズに暗号化する許可を AWS KMS キーポリシーで付与する必要があります。詳細については、「AWS KMS key を使用してメトリクスのエクスポートを暗号化する」を参照してください。

7. [ダッシュボードの作成] を選択します。

AWS CLI を使用する場合

Example

次のコマンド例では、タグを使用して Amazon S3 ストレージレンズ設定を作成します。これらの例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3control put-storage-lens-configuration --account-id=111122223333 --
config-id=example-dashboard-configuration-id --region=us-east-1 --storage-lens-
configuration=file://./config.json --tags=file://./tags.json
```

Example

次のコマンド例では、タグなしで Amazon S3 ストレージレンズ設定を作成します。これらの例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3control put-storage-lens-configuration --account-id=222222222222 --config-
id=your-configuration-id --region=us-east-1 --storage-lens-configuration=file://./
config.json
```

AWS SDK for Java の使用

Example – Amazon S3 ストレージレンズ 設定を作成および更新する

以下の例では、SDK for Java により、Amazon S3 ストレージレンズ設定を作成して更新します。

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.AccountLevel;
import com.amazonaws.services.s3control.model.ActivityMetrics;
import com.amazonaws.services.s3control.model.BucketLevel;
import com.amazonaws.services.s3control.model.CloudWatchMetrics;
import com.amazonaws.services.s3control.model.Format;
import com.amazonaws.services.s3control.model.Include;
import com.amazonaws.services.s3control.model.OutputSchemaVersion;
import com.amazonaws.services.s3control.model.PrefixLevel;
import com.amazonaws.services.s3control.model.PrefixLevelStorageMetrics;
import com.amazonaws.services.s3control.model.PutStorageLensConfigurationRequest;
import com.amazonaws.services.s3control.model.S3BucketDestination;
import com.amazonaws.services.s3control.model.SSES3;
import com.amazonaws.services.s3control.model.SelectionCriteria;
import com.amazonaws.services.s3control.model.StorageLensAwsOrg;
import com.amazonaws.services.s3control.model.StorageLensConfiguration;
import com.amazonaws.services.s3control.model.StorageLensDataExport;
import com.amazonaws.services.s3control.model.StorageLensDataExportEncryption;
import com.amazonaws.services.s3control.model.StorageLensTag;

import java.util.Arrays;
import java.util.List;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class CreateAndUpdateDashboard {

    public static void main(String[] args) {
        String configurationId = "ConfigurationId";
        String sourceAccountId = "111122223333";
        String exportAccountId = "Destination Account ID";
```

```
        String exportBucketArn = "arn:aws:s3:::destBucketName"; // The destination
 bucket for your metrics export must be in the same Region as your S3 Storage Lens
 configuration.
        String awsOrgARN = "arn:aws:organizations::123456789012:organization/o-
abcdefgh";
        Format exportFormat = Format.CSV;

        try {
            SelectionCriteria selectionCriteria = new SelectionCriteria()
                    .withDelimiter("/")
                    .withMaxDepth(5)
                    .withMinStorageBytesPercentage(10.0);
            PrefixLevelStorageMetrics prefixStorageMetrics = new
 PrefixLevelStorageMetrics()
                    .withIsEnabled(true)
                    .withSelectionCriteria(selectionCriteria);
            BucketLevel bucketLevel = new BucketLevel()
                    .withActivityMetrics(new ActivityMetrics().withIsEnabled(true))
                    .withAdvancedCostOptimizationMetrics(new
 AdvancedCostOptimizationMetrics().withIsEnabled(true))
                    .withAdvancedDataProtectionMetrics(new
 AdvancedDataProtectionMetrics().withIsEnabled(true))
                    .withDetailedStatusCodesMetrics(new
 DetailedStatusCodesMetrics().withIsEnabled(true))
                    .withPrefixLevel(new
 PrefixLevel().withStorageMetrics(prefixStorageMetrics));
            AccountLevel accountLevel = new AccountLevel()
                    .withActivityMetrics(new ActivityMetrics().withIsEnabled(true))
                    .withAdvancedCostOptimizationMetrics(new
 AdvancedCostOptimizationMetrics().withIsEnabled(true))
                    .withAdvancedDataProtectionMetrics(new
 AdvancedDataProtectionMetrics().withIsEnabled(true))
                    .withDetailedStatusCodesMetrics(new
 DetailedStatusCodesMetrics().withIsEnabled(true))
                    .withBucketLevel(bucketLevel);

            Include include = new Include()
                    .withBuckets(Arrays.asList("arn:aws:s3:::bucketName"))
                    .withRegions(Arrays.asList("us-west-2"));

            StorageLensDataExportEncryption exportEncryption = new
 StorageLensDataExportEncryption()
                    .withSSES3(new SSES3());
            S3BucketDestination s3BucketDestination = new S3BucketDestination()
```

```
                .withAccountId(exportAccountId)
                .withArn(exportBucketArn)
                .withEncryption(exportEncryption)
                .withFormat(exportFormat)
                .withOutputSchemaVersion(OutputSchemaVersion.V_1)
                .withPrefix("Prefix");
        CloudWatchMetrics cloudWatchMetrics = new CloudWatchMetrics()
                .withIsEnabled(true);
        StorageLensDataExport dataExport = new StorageLensDataExport()
                .withCloudWatchMetrics(cloudWatchMetrics)
                .withS3BucketDestination(s3BucketDestination);

        StorageLensAwsOrg awsOrg = new StorageLensAwsOrg()
                .withArn(awsOrgARN);

        StorageLensConfiguration configuration = new StorageLensConfiguration()
                .withId(configurationId)
                .withAccountLevel(accountLevel)
                .withInclude(include)
                .withDataExport(dataExport)
                .withAwsOrg(awsOrg)
                .withIsEnabled(true);

        List<StorageLensTag> tags = Arrays.asList(
                new StorageLensTag().withKey("key-1").withValue("value-1"),
                new StorageLensTag().withKey("key-2").withValue("value-2")
        );

        AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                .withCredentials(new ProfileCredentialsProvider())
                .withRegion(US_WEST_2)
                .build();

        s3ControlClient.putStorageLensConfiguration(new
PutStorageLensConfigurationRequest()
                .withAccountId(sourceAccountId)
                .withConfigId(configurationId)
                .withStorageLensConfiguration(configuration)
                .withTags(tags)
        );
    } catch (AmazonServiceException e) {
        // The call was transmitted successfully, but Amazon S3 couldn't process
        // it and returned an error response.
        e.printStackTrace();
```

```
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

ストレージをさらに可視化するには、1 つ以上の S3 Storage Lens グループを作成してダッシュボードに関連付けることができます。S3 Storage Lens グループは、プレフィックス、サフィックス、オブジェクトタグ、オブジェクトサイズ、オブジェクト経過時間、またはこれらのフィルターの組み合わせに基づいて、オブジェクト用にカスタム定義されたフィルターです。

S3 Storage Lens グループを使用すると、データレイクなどの大規模な共有バケットをきめ細かく可視化し、情報に基づいたビジネス上の意思決定を行うことができます。例えば、1 つのバケット内または複数のバケットにまたがる個々のプロジェクトやコストセンターの特定のオブジェクトグループにストレージ使用量を分類することで、ストレージ割り当てを効率化し、コストレポートを最適化できます。

S3 Storage Lens グループを使用するには、高度なメトリクスとレコメンデーションを使用するようにダッシュボードをアップグレードする必要があります。S3 Storage Lens グループの詳細については、「the section called “S3 ストレージレンズグループの使用”」を参照してください。

Amazon S3 ストレージレンズダッシュボードの更新

Amazon S3 ストレージレンズのデフォルトダッシュボードは `default-account-dashboard` です。このダッシュボードは Amazon S3 によって事前定義されており、無料のメトリクスおよび高度なメトリクスをアカウント全体で集計し、その概要と傾向をコンソール上で可視化するのに役立ちます。デフォルトダッシュボードのスコープ設定を変更することはできませんが、メトリクスの選択を無料メトリクスから有料の高度なメトリクスとレコメンデーションにアップグレードしたり、オプションのメトリクスエクスポートを構成したり、デフォルトダッシュボードを無効にすることは可能です。デフォルトのダッシュボードは削除できません。また、無効にすることのみが可能です。詳細については、「S3 コンソールの使用」を参照してください。

S3 コンソールの使用

Amazon S3 コンソールで Amazon S3 Storage Lens ダッシュボードを更新するには、次の手順に従います。

ステップ 1: ダッシュボードのスコープを更新する

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ナビゲーションペインで、[Storage Lens] (ストレージレンズ)、[Dashboards] (ダッシュボード) の順にクリックします。
3. 編集するダッシュボードを選択し、 [編集] をクリックします。

   Edit dashboard (ダッシュボードの編集) ページが開きます。

   > **Note**
   >
   > 次の項目は変更できません。
   >
   > - ダッシュボード名
   > - ホームリージョン
   > - デフォルトのダッシュボードの (アカウントのストレージ全体を対象としている) ダッシュボードスコープ

4. ダッシュボード設定ページの [General] (全般) セクションで、更新およびダッシュボードにタグを追加します。

   タグを使用して、ダッシュボードへのアクセス許可を管理し、また S3 Storage Lens のコストを追跡できます。詳細については、IAM ユーザーガイドのリソースタグを使用したアクセスの制御、および AWS Billing ユーザーガイドの AWS 生成コスト配分タグを参照してください。

   > **Note**
   >
   > ダッシュボードの設定には、最大 50 個のタグを追加できます。

5. [ダッシュボードスコープ] セクションで、次の操作を行います。

   a. S3 Storage Lens がダッシュボードに含める、または除外するリージョンとバケットを更新します。

> **Note**
>
> - リージョンとバケットを、含めるか除外するかの選択が可能です。組織内のメンバーアカウント間で組織レベルのダッシュボードを作成する場合には、このオプションはリージョンのみに対し使用できます。
> - 含めるか除外するバケットは最大 50 個まで選択できます。

b. 選択したリージョンにあるバケットを更新し、S3 Storage Lens に含めるか、除外するかを指定します。バケットを含めるか除外するかの設定は可能ですが、両方を同時に設定することはできません。このオプションは、組織レベルのダッシュボードを作成している場合には表示されません。

ステップ 2: メトリクスの選択を更新する

1. [メトリクスの選択] セクションで、このダッシュボードで集約するメトリクスのタイプを選択します。

   - バケットレベルで集計され、14 日間のクエリに使用できる無料のメトリクスを含めるには、[Free metrics] (無料のメトリクス) を選択します。
   - 高度なメトリクスやその他の詳細オプションを有効にするには、[Advanced metrics and recommendations] (高度なメトリクスとレコメンデーション) を選択します。これらのオプションには、高度なプレフィックス集約、Amazon CloudWatch パブリッシング、コンテキストに応じた推奨事項が含まれます。データは 15 か月間クエリで使用できます。高度な高度なメトリクスとレコメンデーションには追加料金がかかります。詳細については、「Amazon S3 の料金」を参照してください。

     無料のメトリクスと高度なメトリクスの詳細については、「メトリクスの選択」を参照してください。

2. [Advanced metrics and recommendations features] (高度なメトリクスとレコメンデーション機能) で、有効にするオプションを選択します。

   - Advanced metrics (高度なメトリクス)
   - [CloudWatch publishing] (CloudWatch パブリッシング)
   - プレフィックス集約

> **Important**
>
> S3 Storage Lens 設定で [プレフィックス集約] を有効にすると、プレフィックスレベルのメトリクスは CloudWatch に公開されません。バケット、アカウント、組織レベルの S3 Storage Lens メトリクスのみが CloudWatch に公開されます。

3. [Advanced metrics] (高度なメトリクス) を有効にした場合は、S3 ストレージレンズダッシュボードに表示する [Advanced metrics categories] (高度なメトリクスのカテゴリ) を選択します。

   - アクティビティのメトリクス
   - [Detailed status code metrics] (詳細なステータスコードメトリクス)
   - [Advanced cost optimization metrics] (高度なコスト最適化メトリクス)
   - [Advanced data protection metrics] (高度なデータ保護メトリクス)

   メトリクスカテゴリの詳細については、「メトリクスのカテゴリ」を参照してください。メトリクスの一覧については、「Amazon S3 Storage Lens のメトリクスに関する用語集」を参照してください。

4. [プレフィックス集約] を有効にする場合は、次の設定を行います。

   a. このダッシュボードのプレフィックスしきい値の最小サイズを選択します。

      例えば、プレフィックスのしきい値を 5% とした場合は、バケットの合計ストレージサイズが 5% 以上を占めるプレフィックスが集約されることを示します。

   b. プレフィックスの深度を選択します。

      この設定は、プレフィックスが評価される階層レベルの最大数を示します。プレフィックスの深度は、10 未満で指定する必要があります。

   c. プレフィックスの区切り文字を入力します。

      これは、各プレフィックスのレベルを識別するために使用される値です。Amazon S3 でのデフォルト値は、/ 文字ですが、実際のストレージ構造では他の区切り文字を使用することも可能です。

(オプション) ステップ 3: ダッシュボードでメトリクスをエクスポートする

1. [Metrics export] (メトリクスのエクスポート) セクションで、選択した保存先バケットに毎日出力されるメトリクスのエクスポートを作成するには、[Enable] (有効化) をクリックします。メトリクスのエクスポートを無効にするには、[Disable] (無効化) を選択します。

   メトリクスのエクスポートは、CSV または Apache Parquet 形式で作成されます。メトリクスのエクスポートには、S3 Storage Lens ダッシュボードのデータと同じスコープが適用され、レコメンデーション事項は付加されません。

2. この機能を有効にした場合は、日次メトリクスのエクスポートの出力形式として、[CSV] または [Apache Parquet] を選択します。

   Parquet は、Hadoop 用のオープンソースなファイル形式で、ネストされたデータを平坦な列指向形式で格納します。

3. メトリクスのエクスポート先の S3 バケットを選択します。

   バケットは、S3 Storage Lens ダッシュボードを使用している現在のアカウント内で選択できます。また、エクスポート先バケットへの許可と、そのバケットの所有者アカウント ID がある場合は、別の AWS アカウント を選択することも可能です。

4. 送信先 S3 バケット (形式: `s3://`*`bucket-name`*`/`*`prefix`*) を選択します。

   バケットのアドレスは、S3 ストレージレンズダッシュボードのホームリージョンにある必要があります。S3 コンソールには、Amazon S3 によって保存先バケットのポリシーに追加される [Destination bucket permission] (エクスポート先バケットのアクセス許可) が表示されます。Amazon S3 は、エクスポート先バケットのバケットポリシーを更新し、S3 がそのバケットにデータを配置できるようにします。

5. (オプション) メトリクスのエクスポートでサーバー側の暗号化を有効にするには、[Specify an encryption key] (暗号化キーの指定) を選択します。その後、[暗号化タイプ] として [Amazon S3 マネージドキー (SSE-S3)] または [AWS Key Management Service キー (SSE-KMS)] を選択します。

   キーのタイプは、Amazon S3 が管理するキー (SSE-S3) と AWS Key Management Service (AWS KMS) キー (SSE-KMS) のいずれかから選択できます。

6. (オプション) AWS KMS キーを指定するには、KMS マスターキーを選択するか、キーとなる Amazon リソースネーム (ARN) を入力する必要があります。[AWS KMS キー] で、次のいずれかの方法で KMS キーを指定します。

- 使用可能な KMS キーのリストから選択するには、[AWS KMS keys から選択する] を選択し、使用可能なキーのリストから自分の KMS キーを選択します。

  AWS マネージドキー (aws/s3) とカスタマーマネージドキーの両方がこのリストに表示されます。カスタマーマネージドキーの詳細については、AWS Key Management Serviceデベロッパーガイドの「カスタマーキーと AWS キー」を参照してください。

  > **Note**
  >
  > AWS マネージドキー (aws/S3) は S3 ストレージレンズでの SSE-KMS 暗号化ではサポートされていません。

- KMS キー ARN を入力するには、[AWS KMS key ARN を入力] を選択し、表示されるフィールドに KMS キー ARN を入力します。
- AWS KMS コンソールで新しいカスタマーマネージドキーを作成するには、[KMS キーを作成] を選択します。

  カスタマーマネージドキーを選択した場合、Amazon S3 ストレージレンズに暗号化する許可を AWS KMS キーポリシーで付与する必要があります。詳細については、「AWS KMS key を使用してメトリクスのエクスポートを暗号化する」を参照してください。

  AWS KMS key の作成の詳細については、「AWS Key Management Service デベロッパーガイド」の「キーの作成」を参照してください。

7. [Save changes] (変更の保存) をクリックします。

ストレージをさらに可視化するには、1 つ以上の S3 Storage Lens グループを作成してダッシュボードに関連付けることができます。S3 Storage Lens グループは、プレフィックス、サフィックス、オブジェクトタグ、オブジェクトサイズ、オブジェクト経過時間、またはこれらのフィルターの組み合わせに基づいて、オブジェクト用にカスタム定義されたフィルターです。

S3 Storage Lens グループを使用すると、データレイクなどの大規模な共有バケットをきめ細かく可視化し、情報に基づいたビジネス上の意思決定を行うことができます。例えば、1 つのバケット内または複数のバケットにまたがる個々のプロジェクトやコストセンターの特定のオブジェクトグループにストレージ使用量を分類することで、ストレージ割り当てを効率化し、コストレポートを最適化できます。

S3 Storage Lens グループを使用するには、高度なメトリクスとレコメンデーションを使用するようにダッシュボードをアップグレードする必要があります。S3 Storage Lens グループの詳細については、「the section called “S3 ストレージレンズグループの使用”」を参照してください。

AWS CLI を使用する場合

Example

次のコマンド例では、Amazon S3 ストレージレンズダッシュボード設定を更新します。これらの例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3control put-storage-lens-configuration --account-id=111122223333 --
config-id=example-dashboard-configuration-id --region=us-east-1 --storage-lens-
configuration=file://./config.json --tags=file://./tags.json
```

AWS SDK for Java の使用

Example – 高度なメトリクスと推奨を使用して Amazon S3 ストレージレンズ設定を更新する

次の例は、SDK for Java の高度なメトリクスと推奨を使用してデフォルトの S3 ストレージレンズ設定を更新する方法を示しています。

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.AccountLevel;
import com.amazonaws.services.s3control.model.ActivityMetrics;
import com.amazonaws.services.s3control.model.BucketLevel;
import com.amazonaws.services.s3control.model.Format;
import com.amazonaws.services.s3control.model.Include;
import com.amazonaws.services.s3control.model.OutputSchemaVersion;
import com.amazonaws.services.s3control.model.PrefixLevel;
import com.amazonaws.services.s3control.model.PrefixLevelStorageMetrics;
import com.amazonaws.services.s3control.model.PutStorageLensConfigurationRequest;
import com.amazonaws.services.s3control.model.S3BucketDestination;
import com.amazonaws.services.s3control.model.SSES3;
import com.amazonaws.services.s3control.model.SelectionCriteria;
import com.amazonaws.services.s3control.model.StorageLensAwsOrg;
import com.amazonaws.services.s3control.model.StorageLensConfiguration;
```

```
import com.amazonaws.services.s3control.model.StorageLensDataExport;
import com.amazonaws.services.s3control.model.StorageLensDataExportEncryption;
import com.amazonaws.services.s3control.model.StorageLensTag;

import java.util.Arrays;
import java.util.List;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class UpdateDefaultConfigWithPaidFeatures {

    public static void main(String[] args) {
        String configurationId = "default-account-dashboard"; // This configuration ID
 cannot be modified.
        String sourceAccountId = "111122223333";

        try {
            SelectionCriteria selectionCriteria = new SelectionCriteria()
                    .withDelimiter("/")
                    .withMaxDepth(5)
                    .withMinStorageBytesPercentage(10.0);
            PrefixLevelStorageMetrics prefixStorageMetrics = new
 PrefixLevelStorageMetrics()
                    .withIsEnabled(true)
                    .withSelectionCriteria(selectionCriteria);
            BucketLevel bucketLevel = new BucketLevel()
                    .withActivityMetrics(new ActivityMetrics().withIsEnabled(true))
                    .withPrefixLevel(new
 PrefixLevel().withStorageMetrics(prefixStorageMetrics));
            AccountLevel accountLevel = new AccountLevel()
                    .withActivityMetrics(new ActivityMetrics().withIsEnabled(true))
                    .withBucketLevel(bucketLevel);

            StorageLensConfiguration configuration = new StorageLensConfiguration()
                    .withId(configurationId)
                    .withAccountLevel(accountLevel)
                    .withIsEnabled(true);

            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();
```

```
            s3ControlClient.putStorageLensConfiguration(new
 PutStorageLensConfigurationRequest()
                    .withAccountId(sourceAccountId)
                    .withConfigId(configurationId)
                    .withStorageLensConfiguration(configuration)
            );

        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

> **Note**
>
> 高度なメトリクスとレコメンデーション事項には追加料金が適用されます。詳細については、「高度なメトリクスとレコメンデーション事項」を参照してください。

Amazon S3 ストレージレンズダッシュボードの無効化

Amazon S3 ストレージレンズダッシュボードは、Amazon S3 コンソールから無効にすることができます。ダッシュボードを無効化すると、その後メトリクスは生成されなくなります。無効化されたダッシュボードは引き続き設定情報を保持するため、簡単に再有効化して復帰させることができます。無効化されたダッシュボードは、クエリに使用できなくなるまで、履歴データを保持します。

S3 コンソールの使用

Amazon S3 コンソールで Amazon S3 ストレージレンズダッシュボードを無効するには、次の手順に従います。

Amazon S3 ストレージレンズダッシュボードを無効にするには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。

2. ナビゲーションペインで、[Storage Lens] (ストレージレンズ)、[Dashboards] (ダッシュボード) の順にクリックします。
3. [ダッシュボード] の一覧から、無効にするダッシュボードを選択し、その一覧の上部にある [無効化] をクリックします。
4. 確認ページで、ダッシュボードの無効化を確認するために、テキストフィールドに対象のダッシュボードの名前を入力した上で、[確認] をクリックします。

Amazon S3 ストレージレンズダッシュボードの削除

デフォルトのダッシュボードを削除することはできません。ただし、無効にすることは可能です。作成したダッシュボードを削除する前に、次の点を考慮してください。

- ダッシュボードを削除する代わりに、無効化することもできます。この場合、将来的に同じダッシュボードを再度有効化できます。詳細については、「S3 コンソールの使用」を参照してください。
- ダッシュボードを削除すると、そのダッシュボードに関連付けられているすべての構成設定が削除されます。
- また、ダッシュボードを削除すると、すべての履歴メトリクスデータも利用できなくなります。この履歴データは 15 か月間保持されます。このデータに再度アクセスする場合は、削除されたものと同じホームリージョンで、同じ名前のダッシュボードを再度作成します。

S3 コンソールの使用

Amazon S3 ストレージレンズダッシュボードは、Amazon S3 コンソールから削除できます。ただし、削除されたダッシュボードからは、その後メトリクスは生成されなくなります。

Amazon S3 Storage Lens ダッシュボードの削除

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ナビゲーションペインで、[Storage Lens] (ストレージレンズ)、[Dashboards] (ダッシュボード) の順にクリックします。
3. [ダッシュボード] の一覧から、削除するダッシュボードを選択した上で、その一覧の上部にある [削除] をクリックします。
4. ダッシュボードの削除を確認するために、ダッシュボードの削除ページのテキストフィールドに、対象のダッシュボードの名前を入力します。[Confirm] (確認) を選択します。

AWS CLI を使用する場合

Example

次の例では、S3 ストレージレンズ設定を削除します。これらの例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3control delete-storage-lens-configuration --account-id=222222222222 --region=us-east-1 --config-id=your-configuration-id
```

AWS SDK for Java の使用

Example – Amazon S3 ストレージレンズダッシュボードの設定を削除する

次の例は、SDK for Java を使用して S3 ストレージレンズ設定を削除する方法を示しています。

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.DeleteStorageLensConfigurationRequest;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class DeleteDashboard {

    public static void main(String[] args) {
        String configurationId = "ConfigurationId";
        String sourceAccountId = "111122223333";
        try {
            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            s3ControlClient.deleteStorageLensConfiguration(new
 DeleteStorageLensConfigurationRequest()
                    .withAccountId(sourceAccountId)
                    .withConfigId(configurationId)
            );
```

```
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Amazon S3 ストレージレンズダッシュボードを一覧表示する

S3 コンソールの使用

S3 ストレージレンズダッシュボードを一覧表示するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[ストレージレンズ] に移動します。
3. [ダッシュボード] を選択します。これで AWS アカウントにダッシュボードを表示できるようになりました。

AWS CLI を使用する場合

Example

次のコマンド例では、AWS アカウントの S3 ストレージレンズダッシュボードを一覧表示します。これらの例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3control list-storage-lens-configurations --account-id=222222222222 --region=us-east-1 --next-token=abcdefghij1234
```

Example

次の例では、次のトークンを含まずに、S3 ストレージレンズ設定を一覧表示します。これらの例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3control list-storage-lens-configurations --account-id=222222222222 --region=us-
east-1
```

AWS SDK for Java の使用

Example – S3 ストレージレンズダッシュボード設定を一覧表示する

次の例は、SDK for Java で S3 ストレージレンズ設定を一覧表示する方法を示しています。この例を使用するには、*user input placeholders* を実際の情報に置き換えます。各例の説明を参照してください。

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.ListStorageLensConfigurationEntry;
import com.amazonaws.services.s3control.model.ListStorageLensConfigurationsRequest;

import java.util.List;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class ListDashboard {

    public static void main(String[] args) {
        String sourceAccountId = "111122223333";
        String nextToken = "nextToken";

        try {
            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            final List<ListStorageLensConfigurationEntry> configurations =
                    s3ControlClient.listStorageLensConfigurations(new
 ListStorageLensConfigurationsRequest()
                            .withAccountId(sourceAccountId)
                            .withNextToken(nextToken)
                    ).getStorageLensConfigurationList();
```

```
            System.out.println(configurations.toString());
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Amazon S3 ストレージレンズダッシュボード設定の詳細を表示する

Amazon S3 ストレージレンズダッシュボードは、Amazon S3 コンソール、AWS CLI、および SDK for Java で表示できます。

S3 コンソールの使用

S3 ストレージレンズダッシュボード設定の詳細を表示するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[ストレージレンズ] に移動します。
3. [ダッシュボード] を選択します。
4. [ダッシュボード] リストで、表示するダッシュボードをクリックします。これで、ストレージレンズダッシュボードの詳細を確認できます。

AWS CLI を使用する場合

Example

次の例では、設定の詳細を表示できるように S3 ストレージレンズ設定を取得します。これらの例を実行するには、*`user input placeholders`* をユーザー自身の情報に置き換えます。

```
aws s3control get-storage-lens-configuration --account-id=222222222222 --config-
id=your-configuration-id --region=us-east-1
```

AWS SDK for Java の使用

Example – S3 ストレージレンズ設定を取得して表示する

次の例は、SDK for Java で S3 ストレージレンズ設定を取得して、設定の詳細を表示できるようにする方法を示しています。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.GetStorageLensConfigurationRequest;
import com.amazonaws.services.s3control.model.GetStorageLensConfigurationResult;
import com.amazonaws.services.s3control.model.StorageLensConfiguration;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class GetDashboard {

    public static void main(String[] args) {
        String configurationId = "ConfigurationId";
        String sourceAccountId = "111122223333";

        try {
            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            final StorageLensConfiguration configuration =
                    s3ControlClient.getStorageLensConfiguration(new
 GetStorageLensConfigurationRequest()
                            .withAccountId(sourceAccountId)
                            .withConfigId(configurationId)
                    ).getStorageLensConfiguration();

            System.out.println(configuration.toString());
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
```

```
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

S3 ストレージレンズによる AWS リソースタグの管理

Amazon S3 ストレージレンズダッシュボードはそれぞれ独自の Amazon リソースネーム (ARN) を持つ AWS リソースとみなされます。そのため、ストレージレンズダッシュボードを設定するときに、オプションでダッシュボードに AWS リソースタグを追加できます。ストレージレンズダッシュボードごとに最大 50 個のタグを追加できます。タグを使用して ストレージレンズダッシュボードを作成するには、次の S3 ストレージレンズアクセス許可が必要です。

- `s3:ListStorageLensConfigurations`
- `s3:GetStorageLensConfiguration`
- `s3:GetStorageLensConfigurationTagging`
- `s3:PutStorageLensConfiguration`
- `s3:PutStorageLensConfigurationTagging`

AWS リソースタグを使用して、部門、事業内容、またはプロジェクトごとにリソースを分類できます。これは、同じ種類のリソースが多い場合に役立ちます。タグを適用すると、割り当てたタグに基づいて特定の S3 ストレージレンズダッシュボードをすばやく識別できます。また、コストの追跡と割り当てにもタグを使用できます。

さらに、ストレージレンズダッシュボードに AWS リソースタグを追加すると、属性ベースのアクセス制御 (ABAC) が有効になります。ABAC は、タグなどの属性に基づいて権限を定義する認可戦略です。IAM ポリシーでリソースタグを指定する条件を使用して、AWS リソースへのアクセスを制御できます。

タグのキーと値は編集でき、タグはリソースからいつでも削除できます。また、次の点について注意してください:

- キーとタグの値は大文字と小文字が区別されます。

- 特定のリソースについて既存のタグと同じキーを持つタグを追加した場合、以前の値は新しい値によって上書きされます。
- リソースを削除すると、リソースのタグも削除されます。
- AWS リソースタグにはプライベートデータや機密データを含めないでください。
- システムタグ (aws: で始まるタグキーの場合) はサポートされていません。
- 各タグキーの長さは 128 文字以下にする必要があります。各タグ値の長さは 256 文字以下にする必要があります。

次の例は、ストレージレンズダッシュボードで AWS リソースタグを使用する方法を示しています。

トピック

- ストレージレンズダッシュボードに AWS リソースタグを追加する
- ストレージレンズダッシュボードの AWS リソースタグを取得する
- ストレージレンズダッシュボードタグの更新
- S3 ストレージレンズダッシュボードから AWS リソースタグを削除する

ストレージレンズダッシュボードに AWS リソースタグを追加する

次の例は、S3 ストレージレンズダッシュボードに AWS リソースタグを使用する方法を示しています。Amazon S3 コンソール AWS Command Line Interface (AWS CLI)、および AWS SDK for Java を使用してリソースタグを追加できます。

S3 コンソールの使用

ストレージレンズダッシュボードに AWS リソースタグを追加するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、左側のナビゲーションパネルにある [ストレージレンズ] に移動します。
3. [ダッシュボード] を選択します。
4. 更新するストレージレンズダッシュボードのラジオボタンを選択します。続いて、[Edit] (編集) をクリックします。
5. [全般] で、[編集] を選択します。
6. [タグの追加] ページで、新しいキーと値のペアを追加します。

> **Note**
>
> 既存のタグと同じ新しいタグを追加すると、以前のタグ値は上書きされます。

7. (オプション) 複数の新しいタグを追加するには、[タグを追加] を再度選択して新しいエントリを追加し続けます。ストレージレンズダッシュボードには、最大 50 個の AWS リソースタグを追加できます。
8. (オプション) 新規追加されたエントリを削除する場合は、削除するタグの横にある[削除] を選びます。
9. [Save changes] (変更の保存) をクリックします。

AWS CLI を使用する場合

Example

次のコマンド例では、S3 ストレージレンズダッシュボード設定にタグを追加します。これらの例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3control put-storage-lens-configuration-tagging --account-id=222222222222 --
region=us-east-1 --config-id=your-configuration-id --tags=file://./tags.json
```

AWS SDK for Java の使用

次の例では、SDK for Java により、Amazon S3 ストレージレンズ設定にタグを追加します。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

Example – S3 ストレージレンズ設定にタグを追加する

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import
 com.amazonaws.services.s3control.model.PutStorageLensConfigurationTaggingRequest;
import com.amazonaws.services.s3control.model.StorageLensTag;

import java.util.Arrays;
```

```
import java.util.List;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class PutDashboardTagging {

    public static void main(String[] args) {
        String configurationId = "ConfigurationId";
        String sourceAccountId = "111122223333";

        try {
            List<StorageLensTag> tags = Arrays.asList(
                    new StorageLensTag().withKey("key-1").withValue("value-1"),
                    new StorageLensTag().withKey("key-2").withValue("value-2")
            );

            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            s3ControlClient.putStorageLensConfigurationTagging(new
 PutStorageLensConfigurationTaggingRequest()
                    .withAccountId(sourceAccountId)
                    .withConfigId(configurationId)
                    .withTags(tags)
            );
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

ストレージレンズダッシュボードの AWS リソースタグを取得する

次の例は、S3 ストレージレンズダッシュボードの AWS リソースタグを取得する方法を示しています。Amazon S3 コンソール、AWS Command Line Interface (AWS CLI)、および AWS SDK for Java を使用してリソースタグを取得できます。

S3 コンソールの使用

ストレージレンズダッシュボードの AWS リソースタグを取得するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[ストレージレンズ] に移動します。
3. [ダッシュボード] を選択します。
4. 表示するストレージレンズダッシュボード設定のラジオボタンを選択します。次に、[ダッシュボード設定を表示] を選択します。
5. [タグ] で、ダッシュボードに関連付けられているタグを確認します。
6. (オプション) 新しいタグを追加する場合は、[編集] を選択します。次に、[タグの追加] を選択します。[タグの追加] ページで、新しいキーと値のペアを追加します。

   > **Note**
   >
   > 既存のタグと同じ新しいタグを追加すると、以前のタグ値は上書きされます。

7. (オプション) 新規追加されたエントリを削除する場合は、削除するタグの横にある[削除] を選びます。
8. [Save changes] (変更の保存) をクリックします。

AWS CLI を使用する場合

Example

次のコマンド例では、S3 ストレージレンズダッシュボード設定のタグを取得します。これらの例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3control get-storage-lens-configuration-tagging --account-id=222222222222 --
region=us-east-1 --config-id=your-configuration-id --tags=file://./tags.json
```

AWS SDK for Java の使用

Example – S3 ストレージレンズダッシュボード設定のタグを取得する

次の例は、SDK for Java で S3 ストレージレンズダッシュボード設定のタグを取得する方法を示しています。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.DeleteStorageLensConfigurationRequest;
import
 com.amazonaws.services.s3control.model.GetStorageLensConfigurationTaggingRequest;
import com.amazonaws.services.s3control.model.StorageLensTag;

import java.util.List;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class GetDashboardTagging {

    public static void main(String[] args) {
        String configurationId = "ConfigurationId";
        String sourceAccountId = "111122223333";
        try {
            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            final List<StorageLensTag> s3Tags = s3ControlClient
                    .getStorageLensConfigurationTagging(new
 GetStorageLensConfigurationTaggingRequest()
                            .withAccountId(sourceAccountId)
                            .withConfigId(configurationId)
                    ).getTags();

            System.out.println(s3Tags.toString());
```

```
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

ストレージレンズダッシュボードタグの更新

以下の例は、Amazon S3 コンソール、AWS Command Line Interface (AWS CLI)、および AWS SDK for Java を使用してストレージレンズダッシュボードを更新する方法を示しています。

S3 コンソールの使用

ストレージレンズダッシュボードの AWS リソースタグを更新するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[ストレージレンズ] に移動します。
3. [ダッシュボード] を選択します。
4. 表示するストレージレンズダッシュボード設定のラジオボタンを選択します。次に、[ダッシュボード設定を表示] を選択します。
5. [タグ] で、ダッシュボードに関連付けられているタグを確認します。
6. (オプション) 新しいタグを追加する場合は、[編集] を選択します。次に、[タグの追加] を選択します。[タグの追加] ページで、新しいキーと値のペアを追加します。

   > **Note**
   >
   > 既存のタグと同じ新しいタグを追加すると、以前のタグ値は上書きされます。

7. (オプション) 新規追加されたエントリを削除する場合は、削除するタグの横にある[削除] を選びます。
8. [Save changes] (変更の保存) をクリックします。

AWS CLI を使用する場合

Example

次のコマンド例では、既存の Amazon S3 ストレージレンズダッシュボード設定にタグを追加または置き換えます。これらの例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3control put-storage-lens-configuration-tagging --account-id=111122223333 --
config-id=example-dashboard-configuration-id --region=us-east-1 --config-id=your-
configuration-id
```

AWS SDK for Java の使用

次の AWS SDK for Java 例では、既存の ストレージレンズダッシュボードの AWS リソースタグを更新します。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

Example – 既存のストレージレンズダッシュボード設定のタグを更新する

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import
 com.amazonaws.services.s3control.model.PutStorageLensConfigurationTaggingRequest;
import com.amazonaws.services.s3control.model.StorageLensTag;

import java.util.Arrays;
import java.util.List;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class PutDashboardTagging {

    public static void main(String[] args) {
        String configurationId = "ConfigurationId";
        String sourceAccountId = "111122223333";

        try {
```

```
            List<StorageLensTag> tags = Arrays.asList(
                    new StorageLensTag().withKey("key-1").withValue("value-1"),
                    new StorageLensTag().withKey("key-2").withValue("value-2")
            );

            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            s3ControlClient.putStorageLensConfigurationTagging(new
 PutStorageLensConfigurationTaggingRequest()
                    .withAccountId(sourceAccountId)
                    .withConfigId(configurationId)
                    .withTags(tags)
            );
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

S3 ストレージレンズダッシュボードから AWS リソースタグを削除する

次の例は、既存のストレージレンズダッシュボードから AWS リソースタグを削除する方法を示しています。Amazon S3 コンソール AWS Command Line Interface (AWS CLI)、および AWS SDK for Java を使用してタグを削除できます。

S3 コンソールの使用

既存のストレージレンズダッシュボードから AWS リソースタグを削除するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[ストレージレンズ] に移動します。
3. [ダッシュボード] を選択します。

4. 表示するストレージレンズダッシュボード設定のラジオボタンを選択します。次に、[ダッシュボード設定を表示] を選択します。
5. [タグ] で、ダッシュボードに関連付けられているタグを確認します。
6. 削除するタグの横にある [削除] を選択します。
7. [Save changes] (変更の保存) をクリックします。

AWS CLI を使用する場合

次の AWS CLI コマンドは、既存の ストレージレンズダッシュボードから AWS リソースタグを削除します。このコマンド例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

Example

```
aws s3control delete-storage-lens-configuration-tagging --account-id=222222222222 --
config-id=your-configuration-id --region=us-east-1
```

AWS SDK for Java の使用

次の AWS SDK for Java 例では、アカウント *111122223333* で指定した Amazon リソースネーム (ARN) を使用して、ストレージレンズダッシュボードから 2 つの AWS リソースタグを削除します。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

Example – S3 ストレージレンズダッシュボード設定のタグを削除する

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import
 com.amazonaws.services.s3control.model.DeleteStorageLensConfigurationTaggingRequest;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class DeleteDashboardTagging {

    public static void main(String[] args) {
        String configurationId = "ConfigurationId";
```

```
        String sourceAccountId = "111122223333";
        try {
            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            s3ControlClient.deleteStorageLensConfigurationTagging(new
 DeleteStorageLensConfigurationTaggingRequest()
                    .withAccountId(sourceAccountId)
                    .withConfigId(configurationId)
            );
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Amazon S3 ストレージレンズを使用するためのヘルパーファイル

次の JSON ファイルとキー入力を例として使用します。

JSON の S3 Storage Lens 例の設定

Example **config.json**

config.json ファイルには、S3 ストレージレンズの組織レベルの高度なメトリクスとレコメンデーションに関する設定の詳細が含まれています。次の例を使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

> **Note**
>
> 高度なメトリクスとレコメンデーションには追加料金が適用されます。詳細については、「高度なメトリクスとレコメンデーション事項」を参照してください。

```
{
  "Id": "SampleS3StorageLensConfiguration", //Use this property to identify your S3
 Storage Lens configuration.
  "AwsOrg": { //Use this property when enabling S3 Storage Lens for AWS Organizations.
    "Arn": "arn:aws:organizations::123456789012:organization/o-abcdefgh"
  },
  "AccountLevel": {
    "ActivityMetrics": {
      "IsEnabled":true
    },
    "AdvancedCostOptimizationMetrics": {
      "IsEnabled":true
    },
    "AdvancedDataProtectionMetrics": {
      "IsEnabled":true
    },
    "DetailedStatusCodesMetrics": {
      "IsEnabled":true
    },
    "BucketLevel": {
      "ActivityMetrics": {
        "IsEnabled":true
      },
      "AdvancedDataProtectionMetrics": {
      "IsEnabled":true
      },
      "AdvancedCostOptimizationMetrics": {
        "IsEnabled":true
      },
      "DetailedStatusCodesMetrics": {
        "IsEnabled":true
      },
      "PrefixLevel":{
        "StorageMetrics":{
          "IsEnabled":true,
          "SelectionCriteria":{
            "MaxDepth":5,
            "MinStorageBytesPercentage":1.25,
            "Delimiter":"/"
          }
        }
      }
    }
```

```
  },
  "Exclude": { //Replace with "Include" if you prefer to include Regions.
    "Regions": [
      "eu-west-1"
    ],
    "Buckets": [ //This attribute is not supported for AWS Organizations-level
 configurations.
      "arn:aws:s3:::amzn-s3-demo-source-bucket"
    ]
  },
  "IsEnabled": true, //Whether the configuration is enabled
  "DataExport": { //Details about the metrics export
    "S3BucketDestination": {
      "OutputSchemaVersion": "V_1",
      "Format": "CSV", //You can add "Parquet" if you prefer.
      "AccountId": "111122223333",
      "Arn": "arn:aws:s3:::
amzn-s3-demo-destination-bucket", // The destination bucket for your metrics export
 must be in the same Region as your S3 Storage Lens configuration.
      "Prefix": "prefix-for-your-export-destination",
      "Encryption": {
        "SSES3": {}
      }
    },
    "CloudWatchMetrics": {
      "IsEnabled": true
    }
  }
}
```

JSON の Storage Lens グループを使用した S3 Storage Lens の設定例

Example **config.json**

config.json ファイルには、Storage Lens グループを使用する際に Storage Lens 設定に適用する詳細が含まれています。例を使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

すべての Storage Lens グループをダッシュボードにアタッチするには、Storage Lens 設定を以下の構文で更新します。

```
{
  "Id": "ExampleS3StorageLensConfiguration",
```

```
  "AccountLevel": {
    "ActivityMetrics": {
      "IsEnabled":true
    },
    "AdvancedCostOptimizationMetrics": {
      "IsEnabled":true
    },
    "AdvancedDataProtectionMetrics": {
      "IsEnabled":true
    },
    "BucketLevel": {
      "ActivityMetrics": {
      "IsEnabled":true
      },
    "StorageLensGroupLevel": {},
  "IsEnabled": true
}
```

Storage Lens ダッシュボード設定に 2 つの Storage Lens グループ (*slg-1* と *slg-2*) のみを含めるには、次の構文を使用します。

```
{
  "Id": "ExampleS3StorageLensConfiguration",
  "AccountLevel": {
    "ActivityMetrics": {
      "IsEnabled":true
    },
    "AdvancedCostOptimizationMetrics": {
      "IsEnabled":true
    },
    "AdvancedDataProtectionMetrics": {
      "IsEnabled":true
    },
    "BucketLevel": {
      "ActivityMetrics": {
      "IsEnabled":true
      },
   "StorageLensGroupLevel": {
        "SelectionCriteria": {
            "Include": [
                "arn:aws:s3:us-east-1:111122223333:storage-lens-group/slg-1",
                "arn:aws:s3:us-east-1:444455556666:storage-lens-group/slg-2"
            ]
```

```
    },
  "IsEnabled": true
}
```

特定の Storage Lens グループのみがダッシュボード設定にアタッチされないようにするには、次の構文を使用します。

```
{
  "Id": "ExampleS3StorageLensConfiguration",
  "AccountLevel": {
    "ActivityMetrics": {
      "IsEnabled":true
    },
    "AdvancedCostOptimizationMetrics": {
      "IsEnabled":true
    },
    "AdvancedDataProtectionMetrics": {
      "IsEnabled":true
    },
    "BucketLevel": {
      "ActivityMetrics": {
      "IsEnabled":true
      },
   "StorageLensGroupLevel": {
        "SelectionCriteria": {
            "Exclude": [
                "arn:aws:s3:us-east-1:111122223333:storage-lens-group/slg-1",
                "arn:aws:s3:us-east-1:444455556666:storage-lens-group/slg-2"
            ]
    },
  "IsEnabled": true
}
```

JSON の S3 Storage Lens タグ例の設定

Example **tags.json**

tags.json ファイルには、S3 ストレージレンズ設定に適用するためのタグが含まれています。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
[
    {
        "Key": "key1",
```

```
        "Value": "value1"
    },
    {
        "Key": "key2",
        "Value": "value2"
    }
]
```

S3 Storage Lens での IAM アクセス許可の設定例

Example **permissions.json** — 特定のダッシュボード名

このポリシー例は、特定のダッシュボード名が指定されている S3 ストレージレンズ IAM アクセス許可を示しています。*value1*、*us-east-1*、*your-dashboard-name*、*example-account-id* を独自の値に置き換えます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetStorageLensConfiguration",
                "s3:DeleteStorageLensConfiguration",
                "s3:PutStorageLensConfiguration"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/key1": "value1"
                }
            },
            "Resource": "arn:aws:s3:us-east-1:example-account-id:storage-lens/your-
dashboard-name"
        }
    ]
}
```

Example **permissions.json** — 特定のダッシュボード名がない場合

このポリシー例は、特定のダッシュボード名が指定されていない S3 ストレージレンズ IAM アクセス許可を示しています。*value1*、*us-east-1*、*example-account-id* を独自の値に置き換えます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetStorageLensConfiguration",
                "s3:DeleteStorageLensConfiguration",
                "s3:PutStorageLensConfiguration"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/key1": "value1"
                }
            },
            "Resource": "arn:aws:s3:us-east-1:example-account-id:storage-lens/*"
        }
    ]
}
```

Amazon S3 ストレージレンズでのメトリクスの表示

S3 ストレージレンズはメトリクスを集約し、Amazon S3 コンソールの [Buckets] (バケット) ページの [Account snapshot] (アカウントのスナップショット) セクションにこの情報を表示します。S3 Storage Lens は、インサイトと傾向を可視化したり、外れ値にフラグ付けしたり、ストレージコストの最適化やデータ保護のベストプラクティスの適用に関するレコメンデーション事項を受け取ったりするために使用できるインタラクティブダッシュボードも提供します。ダッシュボードには、組織、アカウント、AWS リージョン、ストレージクラス、バケット、プレフィックス、またはストレージレンズのグループレベルでインサイトを生成して可視化できる、ドリルダウンオプションが用意されています。1 日 1 回のメトリクスのエクスポートを CSV 形式または Parquet 形式で S3 バケットに送信することもできます。

デフォルトで、すべてのダッシュボードには無料のメトリクスが設定されています。メトリクスには、S3 ストレージ全体の使用状況とアクティビティを把握し、ストレージコストを最適化し、データ保護とアクセス管理のベストプラクティスを実装するために使用できるメトリクスが含まれています。無料のメトリクスはバケットレベルまで下って集計されます。データは、最長 14 日間のクエリで利用可能です。

高度なメトリクスとレコメンデーションには、ストレージ全体の使用状況やアクティビティを詳細に把握するために使用できる以下の追加機能や、ストレージを最適化するためのベストプラクティスが含まれています。

- コンテキストレコメンデーション (ダッシュボードでのみ使用可能)
- 高度なメトリクス (バケットごとに集計されたアクティビティメトリクスを含む)
- プレフィックス集約
- Storage Lens グループ集約
- Storage Lens グループ集約
- Amazon CloudWatch パブリッシング

高度なメトリクスデータは 15 か月間クエリで使用できます。S3 ストレージレンズで高度なメトリクスを使用するには、追加料金がかかります。詳細については、「Amazon S3 の料金」を参照してください。無料のメトリクスと高度なメトリクスの詳細については、「メトリクスの選択」を参照してください。

トピック

- ダッシュボードで S3 Storage Lens のメトリクスを表示する
- データエクスポートで Amazon S3 Storage Lens のメトリクスを確認する
- CloudWatch で S3 Storage Lens のメトリクスをモニタリング
- Amazon S3 ストレージレンズメトリクスのユースケース

ダッシュボードで S3 Storage Lens のメトリクスを表示する

Amazon S3 コンソールでは、S3 Storage Lens により提供されるインタラクティブなデフォルトダッシュボードを使用して、データのインサイトと傾向を可視化できます。このダッシュボードでは、外れ値にフラグ付けして、ストレージコストの最適化や、データ保護のベストプラクティスの適用に関するレコメンデーション事項を受け取ることもできます。ダッシュボードには、アカウント、バケット、AWS リージョン、またはプレフィックス、または Storage Lens グループレベルでインサイトを生成できる、ドリルダウンオプションが用意されています。S3 Storage Lens と AWS Organizations が連携できるようにした場合は、組織レベルでインサイトを生成することもできます (AWS Organizations ヒエラルキーに属するすべてのアカウントのデータなど)。ダッシュボードでは常に、メトリクスの集計が可能な、最新の日付で読み込みが行われます。

コンソールの S3 ストレージレンズのデフォルトダッシュボードの名前は、default-account-dashboard です。Amazon S3 ではこのダッシュボードが事前定義されており、アカウント全体の要約されたインサイトとトレンドを視覚化し、S3 コンソールで毎日更新します。デフォルトのダッシュボードのスコープ設定を変更することはできませんが、選択するメトリクスを、無料メトリクスから有料の高度な推奨のメトリクスに、アップグレードすることはできます。高度なメトリクスとレコメンデーションにより、その他のメトリクスや機能にアクセスできます。これらの機能には、高度なメトリクスカテゴリ、プレフィックスレベルでの集約、コンテキストに応じたレコメンデーション、Amazon CloudWatch パブリッシングなどがあります。

デフォルトのダッシュボードは無効にできますが、削除はできません。デフォルトのダッシュボードを無効にすると、更新されなくなります。S3 Storage Lens または S3 [Buckets] (バケット) ページのアカウントスナップショットで、新しい毎日のメトリクスを受け取ることはなくなります。データクエリの 14 日の有効期限が切れるまでは、デフォルトダッシュボードで履歴データを引き続き表示できます。高度なメトリクスとレコメンデーションを有効にしている場合、この期間は 15 か月です。このデータにアクセスするには、有効期限内にダッシュボードを再度有効化します。

追加の S3 Storage Lens ダッシュボードを作成し、、S3 バケット、またはアカウント (の場合) によってスコープを設定できます。Storage Lens が AWS Organizations と連携できるようにしている場合は、組織別にダッシュボードの範囲を設定することもできます。S3 Storage Lens ダッシュボードを作成または編集するとき、ダッシュボードのスコープとメトリクスの選択を定義します。

作成したその他のダッシュボードは無効化または削除できます。

- ダッシュボードを無効にすると、そのダッシュボードは更新されなくなるので、日次で新しいメトリクスが生成されることもなくなります。無料メトリクスの履歴データについては、14 日間の有効期限まで参照することが可能です。そのダッシュボードで高度なメトリクスとレコメンデーションを有効にした場合、この期間は 15 か月です。有効期限内であれば、ダッシュボードを再度有効化することで、このデータにアクセスできるようになります。
- ダッシュボードを削除すると、それまでの設定内容はすべて失われます。削除されたダッシュボードからは、それ以後の新しい日次のメトリクスは受信できなくなり、そのダッシュボードに関連付けられた履歴データにもアクセスできなくなります。削除したダッシュボードの履歴データにアクセスする場合は、同じホームリージョンで同じ名前を使用しながら、新たなダッシュボードを作成する必要があります。

トピック

- Amazon S3 Storage Lens ダッシュボードの表示
- S3 Storage Lens ダッシュボードを理解する

Amazon S3 Storage Lens ダッシュボードの表示

以下の手順は、S3 コンソールで S3 ストレージレンズダッシュボードを表示する方法です。ダッシュボードを使用してコストを最適化する方法、ベストプラクティスを実装する方法、S3 バケットにアクセスするアプリケーションのパフォーマンスを向上させる方法を示すユースケースベースのチュートリアルについては、「Amazon S3 ストレージレンズメトリクスのユースケース」を参照してください。

> **Note**
>
> Amazon S3 ストレージレンズダッシュボードを表示するために、アカウントのルートユーザーの認証情報を使用することはできません。S3 ストレージレンズダッシュボードにアクセスするには、新規または既存の IAM ユーザーに対し、必要な AWS Identity and Access Management (IAM) アクセス許可を付与する必要があります。その後、それらのユーザーの認証情報によりサインインを行い、S3 Storage Lens ダッシュボードにアクセスします。詳細については、IAM ユーザーガイドの「Amazon S3 ストレージレンズアクセス許可の設定」と「IAM でのセキュリティベストプラクティス」を参照してください。

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ナビゲーションペインで、[Storage Lens] (ストレージレンズ)、[Dashboards] (ダッシュボード) の順にクリックします。
3. [Dashboards] (ダッシュボード) リストで、表示するダッシュボードを選択します。

   ダッシュボードは S3 ストレージレンズで開きます。[Snapshot for date] (日付のスナップショット) セクションには、S3 ストレージレンズがメトリクスを収集した最新の日付が表示されます。ダッシュボードでは常に、メトリクスの集計が可能な、最新の日付で読み込みが行われます。
4. (オプション) S3 ストレージレンズダッシュボードの日付を変更するには、右上の日付セレクターで新しい日付を選択します。
5. (オプション) ダッシュボードのデータの範囲をさらに限定するために一時的なフィルターを適用するには、次の操作を行います。

   a. [フィルター] セクションを展開します。

b. 特定のアカウント、AWS リージョン、ストレージクラス、またはバケット、プレフィックス、または Strage Lens グループでフィルタリングするには、フィルタリングするオプションを選択します。

> **Note**
>
> プレフィックスフィルターと Storage Lens グループフィルターは同時に適用できません。

c. フィルターを更新するには、[Apply] (適用) を選択します。

d. フィルターを削除するには、フィルターの横にある [X] をクリックします。

6. S3 ストレージレンズダッシュボードのどのセクションでも、特定のメトリクスのデータを表示するには、[Metric] (メトリクス) でメトリクス名を選択します。

7. S3 Storage Lens ダッシュボードのどのグラフや可視化でも、[アカウント]、AWS リージョン、[ストレージクラス]、[バケット]、[プレフィックス]、または [Storage Lens グループ] タブを使用して、より深いレベルの集約にドリルダウンできます。例については、コールド Amazon S3 バケットを検出するを参照してください。

S3 Storage Lens ダッシュボードを理解する

S3 ストレージレンズダッシュボードには、基本の [Overview] (概要) タブと、個別の集計レベルを表示するための最大 5 つの追加タブがあります。

- アカウント
- AWS リージョン
- ストレージクラス
- バケット
- プレフィックス
- Storage Lens グループ

[Overview] (概要) タブでは、ダッシュボードのデータが [Snapshot for date] (日付のスナップショット)、[Trends and distributions] (傾向とディストリビューション)、[Top N overview] (トップ N の概要) の 3 つのセクションに集約されます。

S3 ストレージレンズの詳細については、次のセクションを参照してください。

Snapshot

[Snapshot for date] (日付のスナップショット) セクションには、選択した日付で S3 ストレージレンズにより集計されたメトリクスの概要が表示されます。これらの要約メトリクスには、以下の指標が含まれます。

- 合計ストレージ — 使用されているストレージの合計容量 (バイト単位)。
- オブジェクト数 — AWS アカウント 内のオブジェクトの総数。
- 平均オブジェクトサイズ – オブジェクトの平均サイズ。
- アクティブなバケット – アカウントでストレージが 0 バイトを超える、アクティブに使用されているアクティブなバケットの総数。
- アカウント – ストレージがスコープ内にあるアカウントの数。AWS Organizations を使用している場合を除き、この値は 1 です。この場合、S3 ストレージレンズには、有効なサービスにリンクされたロールを持つ、信頼されたアクセス権があります。詳細については、「Amazon S3 ストレージレンズでのサービスにリンクされたロールの使用」を参照してください。
- バケット — アカウント内のバケットの総数。

メトリクスデータ

スナップショットに表示される各メトリクスについて、次のデータが表示されます。

- メトリクス名 – メトリクスの名前。
- メトリクスカテゴリ – メトリクスが分類されるカテゴリ。
- 日付の合計 – 選択した日付の合計数。
- % change – 最後のスナップショット日からの変化率。
- 30 日間のトレンド – 30 日間のメトリクスの変化を示すトレンドライン。
- レコメンデーション – スナップショットで提供されたデータに基づく状況に応じたレコメンデーション。レコメンデーションには、高度なメトリクスとレコメンデーションが用意されています。詳細については、「レコメンデーション」を参照してください。

メトリクスカテゴリ

必要に応じて、ダッシュボードの [Snapshot for date] (日付のスナップショット) セクションを更新して、他のカテゴリのメトリクスを表示できます。その他のメトリクスのスナップショットデータを表示したい場合は、以下の [Metrics categories] (メトリクスカテゴリ) から選択できます。

- コスト最適化
- データ保護
- アクティビティ (高度なメトリクスで利用可能)
- アクセス管理
- パフォーマンス
- イベント

[Snapshot for date] (日付のスナップショット) セクションには、各カテゴリの選択したメトリクスのみが表示されます。特定のカテゴリのすべての指標を確認するには、[Trends and distributions] (傾向とディストリビューション)、[Top N overview] (トップ N の概要) セクションで指標を選択します。Storage Lens グループに メトリクスのカテゴリ リソースタグを追加する S3 ストレージレンズメトリクスの完全なリストについては、「Amazon S3 Storage Lens のメトリクスに関する用語集」を参照してください。

傾向と分布

[Overview] (概要) タブの 2 番目のセクションは、[Trends and distributions] (傾向とディストリビューション) です。[Trends and distributions] (傾向とディストリビューション) セクションでは、定義した日付範囲で比較するメトリクスを 2 つ選択できます。[Trends and distributions] (傾向とディストリビューション) セクションには、2 つのメトリクスの経時的な関係が表示されます。追跡している 2 つの傾向の間で、[Storage class] (ストレージクラス) と [Region] (リージョン) での分布を確認できます。オプションで、いずれかのチャートのデータポイントにドリルダウンして、より詳細な分析を行うことができます。

[Trends and distributions] (傾向とディストリビューション) セクションを使ったチュートリアルについては、「AWS KMS によるデフォルトの暗号化 (SSE-KMS) でサーバー側暗号化を使用しないバケットを識別する」を参照してください。

トップ N の概要

S3 Storage Lens ダッシュボードの 3 番目のセクションは、(昇順または降順でソートされた) トップ N の概要です。このセクションでは、AWS リージョン、バケット、プレフィックス、または Storage Lens グループの上位の数から選択したメトリクスが表示されます。S3 Storage Lens と AWS Organizations が連携できるようにした場合は、選択したメトリクスを組織全体で表示することもできます。

[Top N overview] (トップ N の概要) セクションを使用するチュートリアルについては、「最大の S3 バケットを特定する」を参照してください。

オプションによるドリルダウンと次により分析

S3 Storage Lens ダッシュボードには、グラフ上の値を選択したときに表示される、アクションメニューが用意されており、これにより分析のための円滑な操作を実現しています。このメニューを使用するには、関連するメトリクス値を表示するには、グラフから任意の値を選択してから、表示されるボックスで次の 2 つのオプションから選択します。

- [Drill down] (ドリルダウン) アクションでは、選択した値が、ダッシュボードのすべてのタブでフィルターとして適用されます。その値にドリルダウンして、より深い分析を行うことができます。
- [次により分析:] アクションを実行すると、選択する [ディメンション] タブに移動し、そのタブ値をフィルターとして適用します。これらのタブには、[アカウント]、AWS リージョン、[ストレージクラス]、[バケット]、[プレフィックス] ([高度なメトリクス] と [プレフィックス集約] が有効になっているダッシュボード用)、および [Storage Lens グループ] ([高度なメトリクス] と [Storage Lens グループ集約] が有効になっているダッシュボード用) が含まれます。[次により分析:] を使うと、データを新しいディメンションのコンテキストで表示しながら、より深い分析を行うことができます。

非論理的な結果が出力された場合、あるいは値が存在しない場合には、[ドリルダウン] と [次により分析:] アクションが無効化されることがあります。[ドリルダウン] と [次により分析:] アクションでは、ダッシュボードのすべてのタブにわたって、既存のフィルターの上に新たなフィルタが適用されます。必要に応じて、フィルタを削除することも可能です。

タブ

ディメンションレベルタブには、特定のディメンション内のすべての値に関する詳細が表示されます。例えば、[AWS リージョン] タブにはすべての AWS リージョン のメトリクスが表示され、[バケット] タブにはすべてのバケットのメトリクスが表示されます。各ディメンションタブは、次の 4 つのセクションからなる共通のレイアウトで構成されています。

- 選択したメトリクスのディメンション内で、直近 30 日間の上位 N 個の項目を表示する傾向グラフ。このグラフが表示する項目数は、デフォルトで上位 10 個に設定されていますが、上位 3 個に減らしたり、50 個まで増やしたりすることができます。
- 選択した日付とメトリクスについての縦棒グラフを表示する ヒストグラムグラフ。このグラフに表示されるアイテムの数が非常に多い場合は、水平方向にスクロールする必要がある場合があります。

- ディメンション内のすべての項目をプロットするバブル分析チャート。このチャートは X 軸に 1 番目のメトリクスを、Y 軸に 2 番目のメトリクスを表します。3 番目のメトリクスはバブルのサイズで表されます。
- 行内でリストされた、ディメンション内の各アイテムを表示する、メトリクスグリッドビュー。列には、利用可能なメトリクスがメトリクスカテゴリのタブで整理されて表示されるので、ナビゲーションが容易に行えます。

データエクスポートで Amazon S3 Storage Lens のメトリクスを確認する

Amazon S3 ストレージレンズのメトリクスは、CSV または Apache Parquet 形式を使用した、メトリクスのエクスポートファイルとして毎日生成され、アカウントの S3 バケットに保存されます。バケットにエクスポートされたメトリクスは、Amazon QuickSight や Amazon Athena などの任意の分析ツールに取り込むことで、ストレージの使用状況とアクティビティの傾向を分析できるようになります。

トピック

- AWS KMS key を使用してメトリクスのエクスポートを暗号化する
- S3 Storage Lens のエクスポートマニフェストとは?
- Amazon S3 Storage Lens のエクスポートスキーマを理解する

AWS KMS key を使用してメトリクスのエクスポートを暗号化する

カスタマーマネージドキーを使用してメトリクスのエクスポートを暗号化するアクセス許可を Amazon S3 ストレージレンズに付与するには、キーポリシーを使用する必要があります。S3 ストレージレンズのメトリクスのエクスポートの暗号化に KMS を使用できるようにキーポリシーを変更するには、次の手順に従います。

S3 ストレージレンズに KMS キーを使用したデータの暗号化のアクセス許可を付与するには

1. カスタマーマネージドキーを所有する AWS アカウント を使用して、AWS Management Console にサインインします。
2. AWS KMS コンソール (https://console.aws.amazon.com/kms) を開きます。
3. AWS リージョン を変更するには、ページの右上隅にあるリージョンセレクターを使用します。
4. 左のナビゲーションペインで、[Customer managed keys] を選択します。

5. [カスタマーマネージドキー] で、メトリクスのエクスポートを暗号化するために使用するキーを選択します。AWS KMS keys はリージョン固有で、メトリクスのエクスポート先である S3 バケットと同じリージョンにある必要があります。
6. [Key policy] 行で、[Switch to policy view] を選択します。
7. [編集] をクリックし、キーポリシーを更新します。
8. [キーポリシーの編集] で、既存のキーポリシーに次のキーポリシーを追加します。このポリシーを使用するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
{
    "Sid": "Allow Amazon S3 Storage Lens use of the KMS key",
     "Effect": "Allow",
    "Principal": {
        "Service": "storage-lens.s3.amazonaws.com"
    },
    "Action": [
        "kms:GenerateDataKey"
    ],
    "Resource": "*",
    "Condition": {
       "StringEquals": {
           "aws:SourceArn": "arn:aws:s3:us-east-1:source-account-id:storage-
lens/your-dashboard-name",
           "aws:SourceAccount": "source-account-id"
        }
     }
}
```

9. [Save changes] (変更の保存) をクリックします。

カスタマーマネージドキーの作成とキーポリシーの使用の詳細については、AWS Key Management Service デベロッパーガイドの以下のトピックを参照してください。

- 入門
- AWS KMS でのキーポリシーの使用

また、AWS KMS PUT キーポリシー API オペレーション (PutKeyPolicy) を使用して、カスタマーマネージドキーにキーポリシーをコピーすることもできます。このポリシーは、REST API、AWS CLI、および SDK を使用してメトリクスのエクスポートを暗号化する際に使用します。

S3 Storage Lens のエクスポートマニフェストとは?

集計されるデータが大量の場合、S3 Storage Lens の日次メトリクスのエクスポートは、複数のファイルに分割されます。マニフェストファイル manifest.json には、その日のメトリクスのエクスポートファイルが保存された場所が記述されています。新しいエクスポートが配信されるたびに、マニフェストも新たに添付されます。manifest.json ファイルに含まれる各マニフェストには、対象のエクスポートに関するメタデータおよびその他の基本的な情報が記載されています。

マニフェストの情報には、次のプロパティが含まれています。

- sourceAccountId – その設定の所有者であるアカウント ID。
- configId – ダッシュボードの一意の識別子。
- destinationBucket – メトリクスのエクスポートが保存されるバケットの、Amazon リソースネーム (ARN)。
- reportVersion – エクスポートのバージョン。
- reportDate – レポートの日付。
- reportFormat – レポートの形式。
- reportSchema – レポートのスキーマ。
- reportFiles – 保存先のバケットにある、実際のエクスポートレポートファイルのリスト。

CSV 形式で作成されたエクスポートの、manifest.json ファイルに記述されたマニフェストの例を次に示します。

```
{
   "sourceAccountId":"123456789012",
   "configId":"my-dashboard-configuration-id",
   "destinationBucket":"arn:aws:s3:::amzn-s3-demo-destination-bucket",
   "reportVersion":"V_1",
   "reportDate":"2020-11-03",
   "reportFormat":"CSV",

 "reportSchema":"version_number,configuration_id,report_date,aws_account_number,aws_region,stor
   "reportFiles":[
        {
            "key":"DestinationPrefix/StorageLens/123456789012/my-dashboard-
configuration-id/V_1/reports/dt=2020-11-03/a38f6bc4-2e3d-4355-ac8a-e2fdcf3de158.csv",
            "size":1603959,
```

```
            "md5Checksum":"2177e775870def72b8d84febe1ad3574"
        }
      ]
}
```

Parquet 形式のエクスポート用の manifest.json ファイルに含まれるマニフェストの例を次に示します。

```
{
   "sourceAccountId":"123456789012",
   "configId":"my-dashboard-configuration-id",
   "destinationBucket":"arn:aws:s3:::amzn-s3-demo-destination-bucket",
   "reportVersion":"V_1",
   "reportDate":"2020-11-03",
   "reportFormat":"Parquet",
   "reportSchema":"message s3.storage.lens { required string version_number;
 required string configuration_id; required string report_date; required string
 aws_account_number; required string aws_region; required string storage_class;
 required string record_type; required string record_value; required string
 bucket_name; required string metric_name; required long metric_value; }",
   "reportFiles":[
      {
         "key":"DestinationPrefix/StorageLens/123456789012/my-dashboard-configuration-
id/V_1/reports/dt=2020-11-03/bd23de7c-b46a-4cf4-bcc5-b21aac5be0f5.par",
         "size":14714,
         "md5Checksum":"b5c741ee0251cd99b90b3e8eff50b944"
      }
}
```

メトリクスのエクスポートの生成は、Amazon S3 コンソールでダッシュボード設定の一部とするか、Amazon S3 REST API、AWS CLI、および SDK を使用するかの、どちらかで実行できます。

Amazon S3 Storage Lens のエクスポートスキーマを理解する

次の表に、S3 Storage Lens でのメトリクスのエクスポートスキーマを示します。

Attribute Nameは	データ型	列名	説明
VersionNumber	文字列	version_number	使用中の S3 Storage Lens メトリクスのバージョン。

Attribute Nameは	データ型	列名	説明
ConfigurationId	String	configuration_id	S3 ストレージレンズ設定の configuration_id 。
ReportDate	String	report_date	メトリクスが追跡された日付。
AwsAccountNumber	String	aws_account_number	お客様の AWS アカウント 番号。
AwsRegion	文字列	aws_region	メトリクスが追跡されている AWS リージョン。
StorageClass	文字列	storage_class	調査対象のバケットのストレージクラス。
RecordType	ENUM	record_type	レポートされているアーティファクトのタイプ (ACCOUNT、BUCKET、もしくは PREFIX)。
RecordValue	String	record_value	RecordType アーティファクトの値。 **Note** record_value は、URL エンコードされています。
BucketName	String	bucket_name	レポートされているバケットの名前。

Attribute Nameは	データ型	列名	説明
`MetricName`	文字列	`metric_name`	レポートされているメトリクスの名前。
`MetricValue`	Long	`metric_value`	レポートされているメトリクスの値。

S3 Storage Lens でのメトリクスのエクスポート例

次に示すのは、前出のスキーマに基づく S3 Storage Lens でのメトリクスのエクスポートの例です。

> **Note**
>
> Storage Lens グループのメトリクスは、`record_type` 列内の `STORAGE_LENS_GROUP_BUCKET` または `STORAGE_LENS_GROUP_ACCOUNT` 値を探すことで識別できます。`record_value` 列には、Storage Lens グループの Amazon リソースネーム (ARN) が表示されます (例: `arn:aws:s3:us-east-1:123456789012:storage-lens-group/slg-1`)。

version_r	configuration_id	report_date	aws_account_number	aws_region	storage_class	record_type	record_value	bucket_name	metric_name	metric_value
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			StorageBytes	2478830621
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			ObjectCount	1598962
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			ReplicatedStorageBytes	20000
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			ReplicatedObjectCount	20
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			EncryptedStorageBytes	2478828742
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			EncryptedObjectCount	1598961
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			DeleteMarkerObjectCount	1500
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			ObjectLockEnabledStorageBytes	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			ObjectLockEnabledObjectCount	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			CurrentVersionStorageBytes	2478830621
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			CurrentVersionObjectCount	1598962
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			NonCurrentVersionStorageBytes	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			NonCurrentVersionObjectCount	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			IncompleteMultipartUploadStorageBytes	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			IncompleteMultipartUploadObjectCount	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sf	StorageBytes	29996800
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sf	ObjectCount	12264
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sf	ReplicatedStorageBytes	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sf	ReplicatedObjectCount	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sf	EncryptedStorageBytes	29996800
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sf	EncryptedObjectCount	12264
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sf	DeleteMarkerObjectCount	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sf	ObjectLockEnabledStorageBytes	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sf	ObjectLockEnabledObjectCount	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sf	CurrentVersionStorageBytes	29996800
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sf	CurrentVersionObjectCount	12264
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sf	NonCurrentVersionStorageBytes	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sf	NonCurrentVersionObjectCount	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sf	IncompleteMultipartUploadStorageBytes	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sf	IncompleteMultipartUploadObjectCount	0

以下は、Storage Lens グループのデータを使った Storage Lens メトリクスのエクスポートの例です。

version_numbe	configuration_id	report_date	aws_account_num	aws_region	storage_class	record_type	record_value	bucket_name	metric_name	metric_value
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		StorageBytes	3128548856
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		ObjectCount	4440
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		ReplicatedStorageBytes	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		ReplicatedObjectCount	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		EncryptedStorageBytes	3128548856
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		EncryptedObjectCount	4440
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		DeleteMarkerObjectCount	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		ObjectLockEnabledStorageBytes	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		ObjectLockEnabledObjectCount	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		CurrentVersionStorageBytes	3128548856
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		CurrentVersionObjectCount	4440
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		NonCurrentVersionStorageBytes	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		NonCurrentVersionObjectCount	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		IncompleteMultipartUploadStorageBytes	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		IncompleteMultipartUploadObjectCount	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		DeleteMarkerStorageBytes	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		ReplicatedStorageBytesSource	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		ReplicatedObjectCountSource	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		IncompleteMPUStorageBytesOlderThan7Days	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		IncompleteMPUObjectCountOlderThan7Days	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	StorageBytes	676863200
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	ObjectCount	3000
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	ReplicatedStorageBytes	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	ReplicatedObjectCount	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	EncryptedStorageBytes	676863200
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	EncryptedObjectCount	3000
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	DeleteMarkerObjectCount	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	ObjectLockEnabledStorageBytes	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	ObjectLockEnabledObjectCount	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	CurrentVersionStorageBytes	676863200
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	CurrentVersionObjectCount	3000
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	NonCurrentVersionStorageBytes	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	NonCurrentVersionObjectCount	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	IncompleteMultipartUploadStorageBytes	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	IncompleteMultipartUploadObjectCount	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	DeleteMarkerStorageBytes	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	ReplicatedStorageBytesSource	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	ReplicatedObjectCountSource	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	IncompleteMPUStorageBytesOlderThan7Days	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	IncompleteMPUObjectCountOlderThan7Days	0

CloudWatch で S3 Storage Lens のメトリクスをモニタリング

S3 ストレージレンズのメトリクスを Amazon CloudWatch に公開すると、CloudWatch ダッシュボードで運用状況を一元的に表示できます。また、アラームやトリガーアクション、メトリクス計算、異常検出などの CloudWatch 機能を使用して、S3 ストレージレンズのメトリクスをモニタリングしてアクションを実行できます。さらに CloudWatch API オペレーションにより、サードパーティープロバイダーを含むアプリケーションが S3 ストレージレンズのメトリクスにアクセスできるようになります。CloudWatch Events の詳細については、「Amazon CloudWatch ユーザーガイド」を参照してください。

Amazon S3 コンソール、Amazon S3 REST API、AWS CLI および AWS SDK を使用して、新規または既存のダッシュボードの設定で CloudWatch 公開オプションを有効にできます。S3 Storage Lens のアドバンストメトリクスとレコメンデーションにアップグレードされたダッシュボードは、CloudWatch の公開オプションを使用できます。S3 ストレージレンズの高度なメトリクスとレコメンデーションの料金については、「Amazon S3 料金表」を参照してください。追加の CloudWatch メトリクスの公開料金は適用されません。ただし、ダッシュボード、アラーム、API コールなどのその他の CloudWatch 料金が適用されます。詳細については、「Amazon CloudWatch の料金」を参照してください。

S3 Storage Lens のメトリクスは、S3 Storage Lens の設定を所有するアカウント内の CloudWatch に公開されます。高度なメトリクスとレコメンデーションで CloudWatch 公開オプションを有効にすると、CloudWatch の組織、アカウント、バケットレベルのメトリクスにアクセスできます。プレフィックスレベルのメトリクスは CloudWatch では使用できません。

> **Note**
>
> S3 Storage Lens メトリクスは毎日のメトリクスであり、CloudWatch に 1 日 1 回公開されます。CloudWatch で S3 Storage Lens メトリクスをクエリする場合、クエリの期間は 1 日 (86400 秒) にする必要があります。毎日の S3 Storage Lens メトリクスが Amazon S3 コンソールの S3 Storage Lens ダッシュボードに表示された後、これらの同じメトリクスが CloudWatch に表示されるには数時間かかることがあります。初めて S3 Storage Lens メトリクスの CloudWatch 公開オプションを有効にすると、メトリクスが CloudWatch に公開されるまで最大で 24 時間かかることがあります。

CloudWatch 公開オプションを有効にすると、次の CloudWatch 機能を使用して S3 ストレージ lensStorage レンズデータをモニタリングおよび分析できます。

- ダッシュボード - CloudWatch ダッシュボードを使用して、カスタマイズされた S3 Storage Lens ダッシュボードを作成します。CloudWatch ダッシュボードを AWS アカウント に直接アクセスできないユーザー (チーム間、ステークホルダー、組織外の人) と共有します。
- アラームとトリガーされたアクション - メトリクスを監視し、閾値に違反したときにアクションを起こすアラームを構成することができます。例えば、未完了のマルチパートアップロードバイトメトリクスが 3 日間連続で 1 GB を超えた場合に Amazon SNS 通知を送信するアラームを設定できます。
- 異常検出 - 異常検出を有効にして、メトリクスを継続的に分析し、正常なベースラインを決定後、異常を表面化させます。メトリクスの想定値に基づいて異常検出アラームを作成できます。例えば、オブジェクトロックが有効になっているバイト数メトリクスに異常がないかをモニタリングすると、オブジェクトロック設定の不正な削除を検出できます。
- Metric Math - これにより複数の S3 Storage Lens メトリクスをクエリし、数式を使用して、これらのメトリクスに基づく新しい時系列を作成できます。例えば、`StorageBytes` を `ObjectCount` で割って、平均オブジェクトサイズを取得するための新しいメトリクスを作成できます。

S3 Storage Lens メトリクスの CloudWatch 公開オプションの詳細については、以下のトピックを参照してください。

トピック

- S3 Storage Lens のメトリクスとディメンション
- S3 Storage Lens 用の CloudWatch パブリッシングの有効化

- CloudWatch で S3 Storage Lens のメトリクスを表示します。

S3 Storage Lens のメトリクスとディメンション

S3 Storage Lens メトリクスを CloudWatch に送信するには、S3 Storage Lens のアドバンストメトリクスとレコメンデーションにある CloudWatch 公開オプションを有効にする必要があります。高度なメトリクスを有効にすると、CloudWatch ダッシュボードを使用して、S3 ストレージレンズのメトリクスを他のアプリケーションメトリクスとともにモニタリングし、運用状態の統一ビューを作成できます。ディメンションを使用して CloudWatch の S3 Storage Lens メトリクスを組織、アカウント、バケット、ストレージクラス、リージョン、メトリクスの設定 ID でフィルタリングできます。

S3 Storage Lens のメトリクスは、S3 Storage Lens の設定を所有するアカウント内の CloudWatch に公開されます。高度なメトリクスとレコメンデーションで CloudWatch 公開オプションを有効にすると、CloudWatch の組織、アカウント、バケットレベルのメトリクスにアクセスできます。プレフィックスレベルのメトリクスは CloudWatch では使用できません。

> **Note**
>
> S3 Storage Lens メトリクスは毎日のメトリクスであり、CloudWatch に 1 日 1 回公開されます。CloudWatch で S3 Storage Lens メトリクスをクエリする場合、クエリの期間は 1 日 (86400 秒) にする必要があります。毎日の S3 Storage Lens メトリクスが Amazon S3 コンソールの S3 Storage Lens ダッシュボードに表示された後、これらの同じメトリクスが CloudWatch に表示されるには数時間かかることがあります。初めて S3 Storage Lens メトリクスの CloudWatch 公開オプションを有効にすると、メトリクスが CloudWatch に公開されるまで最大で 24 時間かかることがあります。

CloudWatch での S3 Storage Lens のメトリクスとディメンションの詳細については、以下のトピックを参照してください。

トピック

- メトリクス
- ディメンション

メトリクス

S3 ストレージレンズのメトリクスは、CloudWatch 内でメトリクスとして使用できます。S3 Storage Lens のメトリクスは、`AWS/S3/Storage-Lens` 名前空間に公開されます。この名前空間は

S3 Storage Lens のメトリクス専用です。Amazon S3 バケット、リクエスト、レプリケーションのメトリックスは、AWS/S3 名前空間に公開されます。

S3 Storage Lens のメトリクスは、S3 Storage Lens の設定を所有するアカウント内の CloudWatch に公開されます。高度なメトリクスとレコメンデーションで CloudWatch 公開オプションを有効にすると、CloudWatch の組織、アカウント、バケットレベルのメトリクスにアクセスできます。プレフィックスレベルのメトリクスは CloudWatch では使用できません。

S3 Storage Lens では、メトリクスが集計され、指定されたホームリージョンにのみ保存されます。S3 Storage Lens の設定で指定した、ホームリージョン内の CloudWatch にも S3 Storage Lens メトリクスが公開されます。

CloudWatch で使用可能なメトリックスのリストを含む S3 Storage Lens メトリクスの完全なリストについては、Amazon S3 Storage Lens のメトリクスに関する用語集 を参照してください。

> **Note**
>
> CloudWatch での S3 Storage Lens メトリクスの有効な統計情報は、Average です。CloudWatch での統計の詳細については、Amazon CloudWatch ユーザーガイドの CloudWatch 統計定義を参照してください。

CloudWatch での S3 Storage Lens のメトリクスの粒度について

S3 Storage Lens は、組織、アカウント、バケット、プレフィックスの粒度のメトリクスを提供します。S3 Storage Lens は、組織、アカウント、バケットレベルの S3 Storage Lens メトリクスを CloudWatch に公開します。プレフィクスレベルの S3 Storage Lens メトリクスは CloudWatch では使用できません。

CloudWatch で使用できる S3 Storage Lens メトリクスの粒度の詳細については、以下のリストを参照してください。

- 組織 - 組織内のメンバーアカウント全体で集計されたメトリクス。S3 Storage Lens は、メンバーアカウントのメトリクスを管理アカウントの CloudWatch に公開します。
  - 組織とアカウント - 組織のメンバーアカウントのメトリクス。
  - 組織とバケット - 組織のメンバーアカウントの Amazon S3 バケットのメトリクス。
- アカウント (組織レベル以外) - アカウントのバケット全体で集計されたメトリクス。

- バケット (組織レベル以外) - 特定のバケットのメトリクス。CloudWatch では、 S3 Storage Lens はこれらのメトリクスを、 S3 Storage Lens の設定を作成した AWS アカウント に公開します。S3 Storage Lens は、組織外の構成に対してのみ、これらのメトリクスを公開します。

ディメンション

S3 ストレージレンズで CloudWatch にデータが送信される際、ディメンションが各メトリクスにアタッチされます。ディメンションは、メトリクスの特性を記述するカテゴリです。CloudWatch が返す結果にフィルタを掛ける際にディメンションを使用できます。

例えば、 CloudWatch のすべての S3 Storage Lens のメトリクスは `configuration_id` ディメンションを持っています。このディメンションを使用して、特定の S3 Storage Lens 設定に関連付けられているメトリクスを区別できます。`organization_id` は、組織レベルのメトリクスを示します。CloudWatch のディメンションの詳細については、「CloudWatch ユーザーガイド 」の「ディメンション」を参照してください。

S3 ストレージレンズのメトリクスでは、メトリクスの粒度に応じて異なるディメンションを使用できます。例えば、`organization_id` ディメンションを使用して、組織レベルのメトリクスを AWS Organizations ID でフィルタリングすることができます。ただし、このディメンションをバケットおよびアカウントレベルのメトリクスに使用することはできません。詳細については、「ディメンションを使用した指標のフィルタリング」を参照してください。

S3 Storage Lens 構成で使用できるディメンションを確認するには、次の表を参照してください。

ディメンション	説明	バケット	アカウント	組織	組織とバケット	組織とアカウント
`configuration_id`	メトリクスでレポートされた S3 ストレージレンズ設定のダッシュボード名	.	.	.	.	.
`metrics_version`	S3 ストレージレンズのメトリクスのバージョン このメトリクスのバージョンには固定値 `1.0` が含まれます。	.	.	.	.	.

ディメンション	説明	バケット	アカウント	組織	組織とバケット	組織とアカウント
organization_id	メトリクスの AWS Organizations ID					
aws_account_number	メトリクスに関連付けられた AWS アカウント。					
aws_region	メトリクスの AWS リージョン					
bucket_name	メトリクスでレポートされた S3 バケットの名前					
storage_class	メトリクスでレポートされたバケットのストレージクラス					
record_type	メトリクスの粒度: 組織、アカウント、バケット	バケット	アカウント	バケット	アカウント	組織

S3 Storage Lens 用の CloudWatch パブリッシングの有効化

S3 ストレージレンズのメトリクスを Amazon CloudWatch に公開すると、CloudWatch ダッシュボードで運用状況を一元的に表示できます。また、アラームやトリガーアクション、メトリクス計算、異常検出などの CloudWatch 機能を使用して、S3 ストレージレンズのメトリクスをモニタリングしてアクションを実行できます。さらに CloudWatch API オペレーションにより、サードパー

ティープロバイダーを含むアプリケーションが S3 ストレージレンズのメトリクスにアクセスできるようになります。CloudWatch Events の詳細については、「Amazon CloudWatch ユーザーガイド」を参照してください。

S3 Storage Lens のメトリクスは、S3 Storage Lens の設定を所有するアカウント内の CloudWatch に公開されます。高度なメトリクスとレコメンデーションで CloudWatch 公開オプションを有効にすると、CloudWatch の組織、アカウント、バケットレベルのメトリクスにアクセスできます。プレフィックスレベルのメトリクスは CloudWatch では使用できません。

S3 コンソール、Amazon S3 REST API、AWS CLI および AWS SDK を使用して、新規または既存のダッシュボード構成で CloudWatch サポートを有効にすることができます。CloudWatch の公開オプションは、S3 ストレージレンズの高度なメトリクスとレコメンデーションにアップグレードされたダッシュボードで利用可能です。S3 ストレージレンズの高度なメトリクスとレコメンデーションの料金については、「Amazon S3 料金表」を参照してください。追加の CloudWatch メトリクスの公開料金は適用されません。ただし、ダッシュボード、アラーム、API コールなどのその他の CloudWatch 料金が適用されます。

S3 Storage Lens メトリクスの CloudWatch パブリッシングオプションを有効にするには、以下のトピックを参照してください。

> **Note**
>
> S3 Storage Lens メトリクスは毎日のメトリクスであり、CloudWatch に 1 日 1 回公開されます。CloudWatch で S3 Storage Lens メトリクスをクエリする場合、クエリの期間は 1 日 (86400 秒) にする必要があります。毎日の S3 Storage Lens メトリクスが Amazon S3 コンソールの S3 Storage Lens ダッシュボードに表示された後、これらの同じメトリクスが CloudWatch に表示されるには数時間かかることがあります。初めて S3 Storage Lens メトリクスの CloudWatch 公開オプションを有効にすると、メトリクスが CloudWatch に公開されるまで最大で 24 時間かかることがあります。
> 現在、S3 ストレージレンズのメトリクスは CloudWatch ストリームを介して使用することはできません。

S3 コンソールの使用

S3 ストレージレンズのダッシュボードを更新するとき、ダッシュボード名、またはホームリージョンを変更することはできません。また、デフォルトダッシュボードのスコープを変更することもできません。これは、アカウント全体のストレージにスコープされています。

S3 ストレージレンズのダッシュボードを更新して CloudWatch パブリッシングを有効にするには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ナビゲーションペインで、[S3 Storage Lens] (S3 ストレージレンズ)、[Dashboards] (ダッシュボード) の順にクリックします。
3. 編集するダッシュボードを選択し、 [編集] をクリックします。
4. メトリクスの選択で [Advanced metrics and recommendations] (アドバンストメトリクスとレコメンデーション) を選択します。

   アドバンストメトリクスとレコメンデーションには追加料金が適用されます。高度なメトリクスとレコメンデーションには、データクエリの 15 か月間、プレフィックスレベルで集計された使用状況メトリクス、バケットごとに集計されたアクティビティメトリクス、CloudWatch 公開オプション、ストレージコストの最適化とデータ保護のベストプラクティスの適用に役立つコンテキストに基づいた推奨事項が含まれています。詳細については、「Amazon S3 の料金」を参照してください。
5. [Select Advanced metrics and recommendations features] (高度なメトリクスとレコメンデーションを選択) から [CloudWatch publishing] (CloudWatch パブリッシング) を選択します。

   > **Important**
   >
   > 設定で使用状況メトリクスのプレフィクス集約を有効にすると、プレフィックスレベルのメトリックスは CloudWatch に公開されません。バケット、アカウント、組織レベルの S3 Storage Lens メトリクスのみが CloudWatch に公開されます。
6. [Save changes] (変更の保存) をクリックします。

CloudWatch サポートを有効にする新しい S3 Storage Lens ダッシュボードを作成するには、次のようにします。

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ナビゲーションペインで、[Storage Lens] (ストレージレンズ)、[Dashboards] (ダッシュボード) の順にクリックします。
3. [ダッシュボードの作成] を選択します。
4. [General] (全般) で、次の設定オプションを定義します。

a. [Dashboard name] (ダッシュボード名) に、ダッシュボード名を入力します。

ダッシュボード名は 65 文字未満で記述する必要があり、特殊文字またはスペースを含めることはできません。ダッシュボードの作成後にダッシュボード名を変更することはできません。

b. [ホームリージョン] から、ダッシュボードに対応するものを選択します。

このダッシュボードスコープに含まれるすべてのリージョンのメトリクスは、指定されたホームリージョンに集約され保存されます。CloudWatch を使用した S3 Storage Lens メトリクスはホームリージョンでも利用できます。ダッシュボードの作成後にホームリージョンを変更することはできません。

5. (オプション) タグを追加するには、[タグを追加] を選択し、そのタグの キー と 値 を入力します。

> **Note**
>
> ダッシュボードの設定には、最大 50 個のタグを追加できます。

6. 設定のスコープを定義します。

a. 組織レベルの設定を作成する場合は、[Include all accounts in your configuration] (設定にすべてのアカウントを含める) または [Limit the scope to your signed-in account] (サインインしたアカウントに範囲を制限する) のいずれかの設定に含めるアカウントを選択します。

> **Note**
>
> すべてのアカウントを含める組織レベルの設定を作成する場合、含めたり、除外したりできるのはリージョンのみで、バケットはできません。

b. S3 ストレージレンズをダッシュボード構成に含めるリージョンとバケットを選択するには、以下の手順を実行します。

- すべてのリージョンを含めるには、[Include Regions and buckets] (リージョンとバケットを含める) を選択します。
- 特定のリージョンを含めるには、[Include all Regions] (すべてのリージョンを含める) をクリアにします。[Choose Regions to include] (含めるリージョンを選択) で、S3 Storage Lens がダッシュボードに含めるリージョンを選択します。

- 特定のバケットを含めるには、[Include all buckets] (すべてのバケットを含める) をクリアにします。[Choose buckets to include] (含めるバケットを選択) で、 S3 Storage Lens がダッシュボードに含めるバケットを選択します。

> **Note**
>
> バケットは最大 50 個まで選択できます。

7. [Metrics selection] (メトリクスの選択) で [Advanced metrics and recommendations] (高度なメトリクスとレコメンデーション) を選択します。

   高度なメトリクスとレコメンデーションの料金設定の詳細については、[Amazon S3 pricing] (Amazon S3 の料金) を参照してください。。

8. [Advanced metrics and recommendations features] (高度なメトリクスとレコメンデーションの機能) で、有効にするオプションを選択します。

   - Advanced metrics (高度なメトリクス)
   - [CloudWatch publishing] (CloudWatch パブリッシング)

   > **Important**
   >
   > S3 Storage Lens 設定で [プレフィックス集約] を有効にすると、プレフィックスレベルのメトリクスは CloudWatch に公開されません。バケット、アカウント、組織レベルの S3 Storage Lens メトリクスのみが CloudWatch に公開されます。

   - プレフィックス集約

   > **Note**
   >
   > 高度なメトリクスとレコメンデーションの機能の詳細については、「メトリクスの選択」を参照してください。

9. [Advanced metrics] (高度なメトリクス) を有効にした場合は、S3 ストレージレンズのダッシュボードに表示する [Advanced metrics categories] (高度なメトリクスのカテゴリ) を選択します。

   - アクティビティのメトリクス
   - [Detailed status code metrics] (詳細なステータスコードメトリクス)

- [Advanced cost optimization metrics] (高度なコスト最適化メトリクス)
- [Advanced data protection metrics] (高度なデータ保護メトリクス)

メトリクスのカテゴリの詳細については、「メトリクスのカテゴリ」を参照してください。メトリクスの一覧については、「Amazon S3 Storage Lens のメトリクスに関する用語集」を参照してください。

10. (オプション) メトリクスのエクスポートを設定します。

    ウィザードの各ステップの設定方法については、「S3 コンソールの使用」を参照してください。

11. [ダッシュボードの作成] を選択します。

AWS CLI を使用する場合

次の AWS CLI の例では、S3 ストレージレンズの組織レベルの高度なメトリクスとレコメンデーションの構成を使用して、CloudWatch の公開オプションを有効にします。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3control put-storage-lens-configuration --account-id=555555555555 --config-
id=your-configuration-id --region=us-east-1 --storage-lens-configuration=file://./
config.json

config.json
{
  "Id": "SampleS3StorageLensConfiguration", //Use this property to identify your S3
 Storage Lens configuration.
  "AwsOrg": { //Use this property when enabling S3 Storage Lens for AWS Organizations.
    "Arn": "arn:aws:organizations::123456789012:organization/o-abcdefgh"
  },
  "AccountLevel": {
    "ActivityMetrics": {
      "IsEnabled":true
    },
    "AdvancedCostOptimizationMetrics": {
      "IsEnabled":true
    },
    "AdvancedDataProtectionMetrics": {
      "IsEnabled":true
    },
    "DetailedStatusCodesMetrics": {
```

```
      "IsEnabled":true
    },
    "BucketLevel": {
      "ActivityMetrics": {
        "IsEnabled":true //Mark this as false if you want only free metrics.
      },
      "ActivityMetrics": {
        "IsEnabled":true //Mark this as false if you want only free metrics.
      },
      "AdvancedCostOptimizationMetrics": {
        "IsEnabled":true //Mark this as false if you want only free metrics.
      },
      "DetailedStatusCodesMetrics": {
        "IsEnabled":true //Mark this as false if you want only free metrics.
      },
      "PrefixLevel":{
        "StorageMetrics":{
          "IsEnabled":true, //Mark this as false if you want only free metrics.
          "SelectionCriteria":{
            "MaxDepth":5,
            "MinStorageBytesPercentage":1.25,
            "Delimiter":"/"
          }
        }
      }
    }
  },
  "Exclude": { //Replace with "Include" if you prefer to include Regions.
    "Regions": [
      "eu-west-1"
    ],
    "Buckets": [ //This attribute is not supported for AWS Organizations-level
configurations.
      "arn:aws:s3:::amzn-s3-demo-source-bucket "
    ]
  },
  "IsEnabled": true, //Whether the configuration is enabled
  "DataExport": { //Details about the metrics export
    "S3BucketDestination": {
      "OutputSchemaVersion": "V_1",
      "Format": "CSV", //You can add "Parquet" if you prefer.
      "AccountId": "111122223333",
```

```
      "Arn": "arn:aws:s3:::amzn-s3-demo-destination-bucket", // The destination
 bucket for your metrics export must be in the same Region as your S3 Storage Lens
 configuration.
      "Prefix": "prefix-for-your-export-destination",
      "Encryption": {
        "SSES3": {}
      }
    },
    "CloudWatchMetrics": {
      "IsEnabled": true //Mark this as false if you want to export only free metrics.
    }
  }
}
```

AWS SDK for Java の使用

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.AccountLevel;
import com.amazonaws.services.s3control.model.ActivityMetrics;
import com.amazonaws.services.s3control.model.BucketLevel;
import com.amazonaws.services.s3control.model.CloudWatchMetrics;
import com.amazonaws.services.s3control.model.Format;
import com.amazonaws.services.s3control.model.Include;
import com.amazonaws.services.s3control.model.OutputSchemaVersion;
import com.amazonaws.services.s3control.model.PrefixLevel;
import com.amazonaws.services.s3control.model.PrefixLevelStorageMetrics;
import com.amazonaws.services.s3control.model.PutStorageLensConfigurationRequest;
import com.amazonaws.services.s3control.model.S3BucketDestination;
import com.amazonaws.services.s3control.model.SSES3;
import com.amazonaws.services.s3control.model.SelectionCriteria;
import com.amazonaws.services.s3control.model.StorageLensAwsOrg;
import com.amazonaws.services.s3control.model.StorageLensConfiguration;
import com.amazonaws.services.s3control.model.StorageLensDataExport;
import com.amazonaws.services.s3control.model.StorageLensDataExportEncryption;
import com.amazonaws.services.s3control.model.StorageLensTag;

import java.util.Arrays;
```

```
import java.util.List;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class CreateAndUpdateDashboard {

    public static void main(String[] args) {
        String configurationId = "ConfigurationId";
        String sourceAccountId = "Source Account ID";
        String exportAccountId = "Destination Account ID";
        String exportBucketArn = "arn:aws:s3:::amzn-s3-demo-destination-bucket"; //
 The destination bucket for your metrics export must be in the same Region as your S3
 Storage Lens configuration.
        String awsOrgARN = "arn:aws:organizations::123456789012:organization/o-
abcdefgh";
        Format exportFormat = Format.CSV;

        try {
            SelectionCriteria selectionCriteria = new SelectionCriteria()
                    .withDelimiter("/")
                    .withMaxDepth(5)
                    .withMinStorageBytesPercentage(10.0);
            PrefixLevelStorageMetrics prefixStorageMetrics = new
 PrefixLevelStorageMetrics()
                    .withIsEnabled(true)
                    .withSelectionCriteria(selectionCriteria);
            BucketLevel bucketLevel = new BucketLevel()
                    .withActivityMetrics(new ActivityMetrics().withIsEnabled(true))
                    .withAdvancedCostOptimizationMetrics(new
 AdvancedCostOptimizationMetrics().withIsEnabled(true))
                    .withAdvancedDataProtectionMetrics(new
 AdvancedDataProtectionMetrics().withIsEnabled(true))
                    .withDetailedStatusCodesMetrics(new
 DetailedStatusCodesMetrics().withIsEnabled(true))
                    .withPrefixLevel(new
 PrefixLevel().withStorageMetrics(prefixStorageMetrics));
            AccountLevel accountLevel = new AccountLevel()
                    .withActivityMetrics(new ActivityMetrics().withIsEnabled(true))
                    .withAdvancedCostOptimizationMetrics(new
 AdvancedCostOptimizationMetrics().withIsEnabled(true))
                    .withAdvancedDataProtectionMetrics(new
 AdvancedDataProtectionMetrics().withIsEnabled(true))
                    .withDetailedStatusCodesMetrics(new
 DetailedStatusCodesMetrics().withIsEnabled(true))
```

```
                .withBucketLevel(bucketLevel);

        Include include = new Include()
                .withBuckets(Arrays.asList("arn:aws:s3:::amzn-s3-demo-bucket"))
                .withRegions(Arrays.asList("us-west-2"));

        StorageLensDataExportEncryption exportEncryption = new
StorageLensDataExportEncryption()
                .withSSES3(new SSES3());
        S3BucketDestination s3BucketDestination = new S3BucketDestination()
                .withAccountId(exportAccountId)
                .withArn(exportBucketArn)
                .withEncryption(exportEncryption)
                .withFormat(exportFormat)
                .withOutputSchemaVersion(OutputSchemaVersion.V_1)
                .withPrefix("Prefix");
        CloudWatchMetrics cloudWatchMetrics = new CloudWatchMetrics()
                .withIsEnabled(true);
        StorageLensDataExport dataExport = new StorageLensDataExport()
                .withCloudWatchMetrics(cloudWatchMetrics)
                .withS3BucketDestination(s3BucketDestination);

        StorageLensAwsOrg awsOrg = new StorageLensAwsOrg()
                .withArn(awsOrgARN);

        StorageLensConfiguration configuration = new StorageLensConfiguration()
                .withId(configurationId)
                .withAccountLevel(accountLevel)
                .withInclude(include)
                .withDataExport(dataExport)
                .withAwsOrg(awsOrg)
                .withIsEnabled(true);

        List<StorageLensTag> tags = Arrays.asList(
                new StorageLensTag().withKey("key-1").withValue("value-1"),
                new StorageLensTag().withKey("key-2").withValue("value-2")
        );

        AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                .withCredentials(new ProfileCredentialsProvider())
                .withRegion(US_WEST_2)
                .build();
```

```
            s3ControlClient.putStorageLensConfiguration(new
 PutStorageLensConfigurationRequest()
                    .withAccountId(sourceAccountId)
                    .withConfigId(configurationId)
                    .withStorageLensConfiguration(configuration)
                    .withTags(tags)
            );
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

REST API の使用

Amazon S3 REST API を使用して CloudWatch 公開オプションを有効にするには、PutStorageLensConfiguration を使用します。

次のステップ

CloudWatch 公開オプションを有効にすると、 CloudWatch の S3 Storage Lens メトリクスにアクセスできます。CloudWatch 機能を活用して、CloudWatch で S3 Storage Lens データをモニタリングおよび分析することもできます。詳細については、以下の各トピックを参照してください。

- S3 Storage Lens のメトリクスとディメンション
- CloudWatch で S3 Storage Lens のメトリクスを表示します。

CloudWatch で S3 Storage Lens のメトリクスを表示します。

S3 ストレージレンズのメトリクスを Amazon CloudWatch に公開すると、CloudWatch ダッシュボードで運用状況を一元的に表示できます。また、アラームやトリガーアクション、メトリクス計算、異常検出などの CloudWatch 機能を使用して、S3 ストレージレンズのメトリクスをモニタリングしてアクションを実行できます。さらに CloudWatch API オペレーションにより、サードパーティープロバイダーを含むアプリケーションが S3 ストレージレンズのメトリクスにアクセスできる

ようになります。CloudWatch Events の詳細については、「Amazon CloudWatch ユーザーガイド」を参照してください。

Amazon S3 コンソール、Amazon S3 REST API、AWS CLI および AWS SDK を使用して、新規または既存のダッシュボード構成で CloudWatch 公開オプションを有効にすることができます。CloudWatch の公開オプションは、S3 ストレージレンズの高度なメトリクスとレコメンデーションにアップグレードされたダッシュボードで利用可能です。S3 ストレージレンズの高度なメトリクスとレコメンデーションの料金については、「Amazon S3 料金表」を参照してください。追加の CloudWatch メトリクスの公開料金は適用されません。ただし、ダッシュボード、アラーム、API コールなどのその他の CloudWatch 料金が適用されます。詳細については、「Amazon CloudWatch の料金」を参照してください。

S3 Storage Lens のメトリクスは、S3 Storage Lens の設定を所有するアカウント内の CloudWatch に公開されます。高度なメトリクスとレコメンデーションで CloudWatch 公開オプションを有効にすると、CloudWatch の組織、アカウント、バケットレベルのメトリクスにアクセスできます。プレフィックスレベルのメトリクスは CloudWatch では使用できません。

> **Note**
>
> S3 Storage Lens メトリクスは毎日のメトリクスであり、CloudWatch に 1 日 1 回公開されます。CloudWatch で S3 Storage Lens メトリクスをクエリする場合、クエリの期間は 1 日 (86400 秒) にする必要があります。毎日の S3 Storage Lens メトリクスが Amazon S3 コンソールの S3 Storage Lens ダッシュボードに表示された後、これらの同じメトリクスが CloudWatch に表示されるには数時間かかることがあります。初めて S3 Storage Lens メトリクスの CloudWatch 公開オプションを有効にすると、メトリクスが CloudWatch に公開されるまで最大で 24 時間かかることがあります。
>
> 現在、S3 ストレージレンズのメトリクスは CloudWatch ストリームを介して使用することはできません。

CloudWatch での S3 Storage Lens メトリクスの操作方法の詳細については、以下のトピックを参照してください。

トピック

- CloudWatch ダッシュボードの使用
- アラームの設定、アクションのトリガー、異常検出の使用
- ディメンションを使用した指標のフィルタリング
- メトリクス数学による新しいメトリクスの計算

- グラフでの検索式の使用

CloudWatch ダッシュボードの使用

CloudWatch ダッシュボードを使用して、S3 Storage Lens メトリクスを他のアプリケーションメトリクスとともにモニタリングし、運用状態の統一ビューを作成できます。ダッシュボードは、CloudWatch コンソールのカスタマイズ可能なホームページで、 リソースを単一のビューでリソースをモニタリングするために使用できます。

CloudWatch には、特定のメトリクスまたはディメンションへのアクセスの制限をサポートしない幅広い権限コントロールがあります。CloudWatch へのアクセス権を持つアカウントまたは組織のユーザーは、CloudWatch サポートオプションが有効になっているすべての S3 Storage Lens 設定のメトリクスにアクセスできます。S3 Storage Lens では、特定のダッシュボードのアクセス許可を管理することはできません。CloudWatch のアクセス許可の詳細については Amazon CloudWatch ユーザーガイドの CloudWatch リソースに対するアクセス許可の管理を参照してください。

CloudWatch ダッシュボードの使用とアクセス許可の設定の詳細については、 Amazon CloudWatch ユーザーガイドの Amazon CloudWatch ダッシュボードの使用および CloudWatch ダッシュボードの共有を参照してください。

アラームの設定、アクションのトリガー、異常検出の使用

CloudWatch で S3 Storage Lens メトリクスを監視し、しきい値を超えたときにアクションを実行する CloudWatch アラームを設定できます。例えば、未完了のマルチパートアップロードバイトメトリクスが 3 日間連続で 1 GB を超えた場合に Amazon SNS 通知を送信するアラームを設定できます。

また、異常検出を有効にして S3 Storage Lens のメトリクスを継続的に分析し、通常のベースラインを決定後、異常を検出できます。メトリクスの想定値に基づいて異常検出アラームを作成できます。例えば、オブジェクトロックが有効になっているバイト数メトリクスに異常がないかをモニタリングすると、オブジェクトロック設定の不正な削除を検出できます。

詳細な説明と例については、「Amazon CloudWatch アラームを使用する」そして 「Amazon CloudWatch ユーザーガイド」の「グラフのメトリクスからアラームを作成する」を参照してください。

ディメンションを使用した指標のフィルタリング

ディメンションを使用して、CloudWatch コンソールで S3 Storage Lens メトリクスをフィルタリングできます。例えば、次のようにフィルタリングできます。`configuration_id`、`aws_account_number`、`aws_region`、`bucket_name`、など。

S3 Storage Lens は、アカウントごとに複数のダッシュボード構成をサポートします。つまり、異なる構成に同じバケットを含めることができます。これらのメトリクスが CloudWatch に公開されると、バケットは CloudWatch 内に重複するメトリクスを持つことになります。CloudWatch の特定の S3 Storage Lens 設定のメトリクスだけを表示するには、configuration_id ディメンションを使用できます。configuration_id でフィルタリングすると、特定した構成に関連付けられたメトリクスのみが表示されます。

設定 ID によるフィルタリングの詳細については、「Amazon CloudWatch ユーザーガイド」の「利用可能なメトリクスの検索」を参照してください。

メトリクス数学による新しいメトリクスの計算

メトリクス数学により複数の S3 Storage Lens メトリクスをクエリし、数式を使用して、これらのメトリクスに基づく新しい時系列を作成できます。例えば、オブジェクト数から暗号化されたオブジェクト数を引いて、暗号化されていないオブジェクトの新しいメトリクスを作成できます。また、StorageBytes を ObjectCount で割って平均オブジェクトサイズを、BytesDownloaded を StorageBytes で割って 1 日にアクセスしたバイト数を取得するためのメトリクスを作成することもできます。

詳細については、「Amazon CloudWatch ユーザーガイド」の「Amazon CloudWatch メトリクス数学の使用」を参照してください。

グラフでの検索式の使用

S3 ストレージレンズのメトリクスを使用すると、検索式を作成することができます。例えば、IncompleteMultipartUploadStorageBytes と呼ばれるすべてのメトリクスの検索式を作成して、SUM を式に追加することができます。この検索式を使用すると、ストレージのすべてのディメンションで未完了のマルチパートアップロードバイトの合計を 1 つのメトリクスで確認できます。

この例では、IncompleteMultipartUploadStorageBytes と呼ばれるすべてのメトリクスの検索式を作成するために使用する構文を示します。

```
SUM(SEARCH('{AWS/S3/Storage-
Lens,aws_account_number,aws_region,configuration_id,metrics_version,record_type,storage_class}
 MetricName="IncompleteMultipartUploadStorageBytes"', 'Average',86400))
```

この構文の詳細については、「Amazon CloudWatch ユーザーガイド」の「CloudWatch 検索式の構文」を参照してください。検索式を使用した CloudWatch グラフを作成するには、「Amazon CloudWatch ユーザーガイド」の「検索式を使用した CloudWatch グラフの作成」を参照してください。

Amazon S3 ストレージレンズメトリクスのユースケース

Amazon S3 ストレージレンズのダッシュボードを使用して、インサイトと傾向を可視化し、外れ値にフラグを付け、レコメンデーションを受け取ることができます。S3 ストレージレンズメトリクスは、主要なユースケースに合致するカテゴリに整理されます。これらのメトリクスを使用して、次のことができます。

- コスト最適化の機会の特定
- データ保護のベストプラクティスの適用
- アクセス管理のベストプラクティスの適用
- アプリケーションワークロードのパフォーマンスの向上

例えば、コスト最適化メトリクスを使用して、Amazon S3 のストレージコストを削減する機会を特定することができます。7 日以上経過したマルチパートアップロードのあるバケットや、最新ではないバージョンが蓄積されているバケットを特定できます。

同様に、データ保護メトリクスを使用することで、組織内のデータ保護のベストプラクティスに従っていないバケットを特定できます。例えば、デフォルトの暗号化に AWS Key Management Service キー (SSE-KMS) を使用しないバケットや、S3 バージョニングが有効になっていないバケットを特定できます。

S3 ストレージレンズのアクセス管理メトリクスでは、S3 オブジェクト所有権のバケット設定を特定でき、アクセスコントロールリスト (ACL) アクセス許可をバケットポリシーに移行して ACL を無効にできます。

S3 ストレージレンズの高度なメトリクスを有効にしている場合は、詳細なステータスコードメトリクスを使用してリクエストの成功または失敗の数を取得し、アクセスやパフォーマンスの問題のトラブルシューティングに使用できます。

高度なメトリクスを使用すると、追加のコスト最適化メトリクスやデータ保護メトリクスにアクセスして、S3 ストレージ全体のコストをさらに削減し、データ保護のベストプラクティスとの整合性を高める機会を特定することもできます。例えば、高度なコスト最適化メトリクスにはライフサイクルルール数が含まれます。このメトリクスを使用して、7 日以上経過した未完了のマルチパートアップロードを失効させるライフサイクルルールがないバケットを特定できます。高度なデータ保護メトリクスには、レプリケーションルール数が含まれます。

メトリクスのカテゴリの詳細については、「メトリクスのカテゴリ」を参照してください。S3 ストレージレンズメトリクスの完全なリストについては、「Amazon S3 Storage Lens のメトリクスに関する用語集」を参照してください。

トピック

- Amazon S3 ストレージレンズを使用したストレージコストの最適化
- S3 ストレージレンズによるデータ保護
- オブジェクト所有権設定を監査するための S3 の使用
- S3 ストレージレンズのメトリクスを使用してパフォーマンスを改善する

Amazon S3 ストレージレンズを使用したストレージコストの最適化

S3 ストレージレンズのコスト最適化メトリクスを使用すると、S3 ストレージの全体的なコストを削減できます。コスト最適化メトリクスは、Amazon S3 をコスト効率よく、ベストプラクティスに従って設定したことを確認するのに役立ちます。例えば、次のようなコスト最適化の機会を特定できます。

- 7 日以上経過した未完了のマルチパートアップロードを含むバケット
- 多数の旧バージョンが蓄積されているバケット
- 未完了のマルチパートアップロードを中止するためのライフサイクルルールが設定されていないバケット
- 旧バージョンのオブジェクトを期限切れにするライフサイクルルールがないバケット
- オブジェクトを別のストレージクラスに移行するためのライフサイクルルールがないバケット

その後、このデータを使用して、バケットにライフサイクルルールを追加できます。

次の例は、S3 ストレージレンズダッシュボードでコスト最適化メトリクスを使用してストレージコストを最適化する方法を示しています。

トピック

- 最大の S3 バケットを特定する
- コールド Amazon S3 バケットを検出する
- 未完了のマルチパートアップロードを特定する
- 保持する旧バージョンの数を減らす
- ライフサイクルルールがないバケットを特定し、ライフサイクルルール数を確認する

最大の S3 バケットを特定する

料金は S3 バケットでのオブジェクトの保存に対して発生します。請求される料金は、オブジェクトのサイズ、オブジェクトの保存期間、およびそれらのストレージクラスに応じて異なります。S3 ストレージレンズで、アカウント内のすべてのバケットを一元的に表示できます。組織が持つすべてのアカウントのバケットをすべて表示するには、AWS Organizations レベルの S3 ストレージレンズダッシュボードを設定できます。最大のバケットは、このダッシュボードのビューから特定できます。

ステップ 1: 最大のバケットを特定する

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ナビゲーションペインで、[Storage Lens] (ストレージレンズ)、[Dashboards] (ダッシュボード) の順にクリックします。
3. [Dashboards] (ダッシュボード) リストで、表示するダッシュボードを選択します。

   ダッシュボードが開くと、S3 ストレージレンズがメトリクスを収集した最新の日付を確認できます。ダッシュボードでは常に、メトリクスの集計が可能な、最新の日付で読み込が行われます。
4. 選択した日付範囲の [Total storage] (ストレージの合計) メトリクスで最大バケットのランキングを表示するには、[Top N overview for date] (日付の上位 N の概要) セクションまでスクロールダウンします。

   ソート順序を切り替えて、最も小さいバケットを表示できます。また、[Metric] (メトリクス) の選択を調整して、使用可能なメトリクスのいずれかでバケットをランク付けすることもできます。[Top N overview for date] (日付の上位 N の概要) セクションには、前日または前週からの変化率と、トレンドを視覚化するスパークラインも表示されます。この傾向は、無料メトリクスの場合は 14 日間、高度なメトリクスとレコメンデーションの場合は 30 日間の傾向です。

   > **Note**
   >
   > S3 ストレージレンズの高度なメトリクスとレコメンデーションの場合、メトリクスは 15 か月間クエリで利用できます。詳細については、「メトリクスの選択」を参照してください。
5. バケットに関するより詳細な情報については、ページの上部までスクロールし、[Bucket] (バケット) タブを選択します。

[Buckets] (バケット) タブでは、最近の増加率、平均的なオブジェクトサイズ、最大のプレフィックス、およびオブジェクトの数などの詳細を確認できます。

ステップ 2: バケットに移動して調査する

最大の S3 バケットを特定したら、S3 コンソール内の各バケットに移動してバケット内のオブジェクトを表示し、関連するワークロードを理解し、内部所有者を特定できます。バケットの所有者に連絡すれば、この増加が見込まれていたものかどうか、またはこの増加をさらにモニタリングして制御する必要があるかどうかを確認できます。

コールド Amazon S3 バケットを検出する

S3 ストレージレンズの高度なメトリクス を有効にしている場合は、アクティビティメトリクスを使用して、S3 バケットがどの程度「コールド」かを理解できます。「コールド」なバケットとは、そのストレージがアクセスされなくなった (またはほとんどアクセスされない) バケットです。通常、このアクティビティの欠如はバケットのオブジェクトが頻繁にアクセスされていないことを示します。

[GET Requests] (GET リクエスト) および [Download Bytes] (ダウンロード済みバイト数) などのアクティビティメトリクスは、バケットが毎日どのくらいの頻度でアクセスされるかを示します。アクセスパターンの一貫性を理解し、まったくアクセスされなくなったバケットを特定するために、このデータの数か月間にわたる傾向を得ることができます。[Download bytes / Total storage] (ダウンロード済みバイト数÷ストレージの合計) として計算される [Retrieval rate] (取得率) メトリクスは、毎日アクセスされるバケット内のストレージの比率を示します。

> **Note**
>
> 1 日に同じオブジェクトが複数回ダウンロードされる場合は、ダウンロードのバイト数が重複します。

前提条件

S3 ストレージレンズダッシュボードでアクティビティメトリクスを表示するには、S3 ストレージレンズ [Advanced metrics and recommendations] (高度なメトリクスとレコメンデーション) を有効にしてから、[Activity metrics] (アクティビティメトリクス) を選択する必要があります。詳細については、「S3 コンソールの使用」を参照してください。

ステップ 1: アクティブなバケットを特定する

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ナビゲーションペインで、[Storage Lens] (ストレージレンズ)、[Dashboards] (ダッシュボード) の順にクリックします。
3. [Dashboards] (ダッシュボード) リストで、表示するダッシュボードを選択します。
4. [Bucket] (バケット) タブを選択してから、[Bubble analysis by buckets for date] (日付別のバケット別によるバブル分析) セクションまでスクロールダウンします。

   [Bubble analysis by buckets for date] (日付別のバケット別によるバブル分析) セクションでは、バブルの [X-axis] (X 軸)、[Y-axis] (Y 軸)、および [Size] (サイズ) を表す 3 つのメトリクスを使用して、バケットを複数のディメンションにプロットできます。
5. コールドになったバケットを見つけるには、[X-axis] (X 軸)、[Y-axis] (Y 軸)、および [Size] (サイズ) で、[Total storage] (合計ストレージ)、[% retrieval rate] (% 取り出し率)、および [Average object size] (平均オブジェクトサイズ) のメトリクスを選択します。
6. [Bubble analysis by buckets for date] (日付別のバケットごとのバブル分析) セクションで、取得率がゼロ (またはゼロに近い) で、かつ相対的なストレージサイズが大きいバケットを探し、そのバケットを表すバブルを選択します。

   より詳細なインサイトの選択肢が記載されたボックスが表示されます。次のいずれかを行います：

   a. [Bucket] (バケット) タブを更新して、選択したバケットのメトリクスのみを表示するには、[Drill down] (ドリルダウン)、[Apply] (適用) を順に選択します。
   b. バケットレベルのデータをアカウント、AWS リージョン、ストレージクラス、またはバケットごとに集約するには、[Analyze by] (分析基準)、[Dimension] (ディメンション) の順に選択します。例えば、ストレージクラス別に集計するには、[Dimension] (ディメンション) に [Storage class] (ストレージクラス) を選択します。

   コールドになったバケットを見つけるには、[Total storage] (ストレージの合計)、[% retrieval rate] (% 取得率)、および [Average object size] (平均オブジェクトサイズ) メトリクスを使用してバブル分析を実行します。取得率がゼロ (またはゼロに近い) で、かつ相対的なストレージサイズが大きいバケットを探します。

ダッシュボードの [Bucket] (バケット) タブが更新され、選択した集計またはフィルターのデータが表示されます。ストレージクラスまたは別のディメンション別に集計した場合、その新しいタブがダッシュボードに表示されます (例えば、[Storage class] (ストレージクラス) タブ)。

ステップ 2: コールドバケットを調査する

そこからアカウントまたは組織内のコールドバケットの所有者を特定し、そのストレージが引き続き必要かどうかを確認できます。その後、バケットにライフサイクル有効期限設定を設定する、またはデータを Amazon S3 Glacier ストレージクラスにアーカイブすることによって、コストを最適化できます。

将来のコールドバケット問題を回避するには、S3 ライフサイクル設定を使用してデータを自動的に移行させる、または S3 Intelligent-Tiering による自動アーカイブを有効にすることができます。

ステップ 1 を実施してホットバケットを識別することもできます。次に、これらのバケットが正しい S3 ストレージクラスを使用するようにして、パフォーマンスとコストの面で最も効果的にリクエストに応えられるようにします。

未完了のマルチパートアップロードを特定する

スループットを向上させ、ネットワーク問題からより迅速に復旧するため、マルチパートアップロードを使用して超大型のオブジェクト (最大 5 TB) を複数のパートから成るセットとしてアップロードすることができます。マルチパートアップロードのプロセスが完了しなかった場合、未完了のなパートが使用不可能な状態でバケットに残ります。これらの未完了のパートには、アップロードプロセスが完了するか、未完了の部分が削除されるまで、ストレージコストが発生します。詳細については、「Amazon S3 でのマルチパートアップロードを使用したオブジェクトのアップロードとコピー」を参照してください。

S3 ストレージレンズを使用すると、7 日以上経過した未完了のマルチパートアップロードを含め、アカウント内、または組織全体にある未完了のマルチパートアップロードのバイト数を特定できます。未完了のマルチパートアップロードメトリクスの完全なリストについては、「Amazon S3 Storage Lens のメトリクスに関する用語集」を参照してください。

ベストプラクティスとして、特定の日数を過ぎた未完了のマルチパートアップロードを期限切れにするように、ライフサイクルルールを設定することをおすすめします。未完了のマルチパートアップロードを期限切れにするライフサイクルルールを作成する場合は、7 日間から始めることをお勧めします。

ステップ 1: 未完了のマルチパートアップロードの全体的なトレンドを確認する

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ナビゲーションペインで、[Storage Lens] (ストレージレンズ)、[Dashboards] (ダッシュボード) の順にクリックします。
3. [Dashboards] (ダッシュボード) リストで、表示するダッシュボードを選択します。
4. [Snapshot for date] (日付のスナップショット) セクションの [Metrics categories] (メトリクスのカテゴリ) で、[Cost optimization] (コスト最適化) を選択します。

   [Snapshot for date] (日付のスナップショット) セクションが更新され、[Incomplete multipart upload bytes greater than 7 days old] (7 日以上経過した未完了のマルチパートアップロードバイト数) を含む [Cost optimization] (コスト最適化) メトリクスが表示されます。

   S3 ストレージレンズダッシュボードのどのグラフでも、未完了のマルチパートアップロードのメトリクスを確認できます。これらのメトリクスを使用して、全体的な増加傾向に対するそれらの寄与度などを含め、ストレージに対する未完了のマルチパートアップロードのバイト数の影響をさらに評価することができます。また、[Account] (アカウント)、[AWS リージョン]、[Bucket] (バケット)、[Storage class] (ストレージクラス) の各タブを使用して、より詳細な集計レベルまで掘り下げてデータを分析することもできます。例については、コールド Amazon S3 バケットを検出するを参照してください。

ステップ 2: マルチパートアップロードバイト数が最も多く、未完了のマルチパートアップロードを中止するライフサイクルルールがないバケットを特定する

前提条件

S3 ストレージレンズダッシュボードに [Abort incomplete multipart upload lifecycle rule count] (未完了のマルチパートアップロードの中止ライフサイクルルール数) メトリクスを表示するには、S3 ストレージレンズの [Advanced metrics and recommendations] (高度なメトリクスとレコメンデーション) を有効にしてから [Advanced cost optimization metrics] (高度なコスト最適化メトリクス) を選択する必要があります。詳細については、「S3 コンソールの使用」を参照してください。

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ナビゲーションペインで、[Storage Lens] (ストレージレンズ)、[Dashboards] (ダッシュボード) の順にクリックします。

3. [Dashboards] (ダッシュボード) リストで、表示するダッシュボードを選択します。
4. 7 日以上経過した未完了のマルチパートアップロードが蓄積されているバケットを特定するには、[Top N overview for date] (日付の上位 N の概要) セクションに移動します。

   デフォルトでは、[Top N overview for date] (日付の上位 N の概要) セクションには、上位 3 つのバケットのメトリクスが表示されます。[Top N] (トップ N) のフィールドでバケット数を増減できます。[Top N overview for date] (日付の上位 N の概要) セクションには、前日または前週からの変化率と、トレンドを視覚化するスパークラインも表示されます。(このトレンドは、無料メトリクスの場合は 14 日間、高度なメトリクスとレコメンデーションの場合は 30 日間のトレンドです。)

   > **Note**
   >
   > S3 ストレージレンズの高度なメトリクスとレコメンデーションの場合、メトリクスは 15 か月間クエリで利用できます。詳細については、「メトリクスの選択」を参照してください。

5. [Metric] (メトリクス) で、[Cost optimization] (コスト最適化) カテゴリの [Incomplete multipart upload bytes greater than 7 days old] (7 日以上経過した未完了のマルチパートアップロードバイト数) を選択します。

   [Top number buckets] (上位バケット) には、7 日以上経過している未完了のマルチパートアップロードのストレージバイト数が最も多いバケットが表示されます。
6. 未完了のマルチパートアップロードに関する詳細なバケットレベルのメトリクスを表示するには、ページの一番上までスクロールして、[Bucket] (バケット) タブを選択します。
7. [Buckets] (バケット) セクションまで下にスクロールします。[Metrics categories] (メトリクスのカテゴリ) で、[Cost optimization] (コスト最適化) を選択します。次に，[Summary] (概要) を選択解除します。

   [Buckets] (バケット) リストが更新され、表示されているバケットで利用可能なすべての [Cost optimization] (コスト最適化) メトリクスが表示されます。
8. [Buckets] (バケット) リストをフィルタリングして特定のコスト最適化メトリクスのみを表示するには、設定アイコン
   ( )
   を選択します。
9. [Incomplete multipart upload bytes greater than 7 days old] (7 日以上経過した未完了のマルチパートアップロードバイト数) および [Abort incomplete multipart upload lifecycle rule count] (未

完了のマルチパートアップロードの中止ライフサイクルルール数) 以外のすべてのコスト最適化メトリクスのトグルを選択解除します。

10. (オプション) [Page size] (ページサイズ) で、リストに表示するバケットの数を選択します。
11. [確認] を選択してください。

    [Buckets] (バケット) リストが更新され、未完了のマルチパートアップロードのバケットレベルのメトリクスとライフサイクルルール数が表示されます。このデータを使用して、7 日以上経過した未完了のマルチパートアップロードバイト数が最も多く、未完了のマルチパートアップロードを中止するライフサイクルルールが欠落しているバケットを特定できます。次に、S3 コンソールでこれらのバケットに移動し、ライフサイクルルールを追加して、放棄された未完了のマルチパートアップロードを削除できます。

ステップ 3: 未完了のマルチパートアップロードを 7 日後に削除するライフサイクルルールを追加する

未完了のマルチパートアップロードを自動的に管理するには、S3 コンソールを使用して、指定された日数後にバケットから未完了のマルチパートアップロードのバイトを失効させるライフサイクル設定を作成できます。詳細については、「不完全なマルチパートアップロードを削除するためのバケットライフサイクル設定の設定」を参照してください。

保持する旧バージョンの数を減らす

S3 バージョニング機能を有効にすると、同じオブジェクトの複数の異なるバージョンが保持されます。これらは、オブジェクトが誤って削除または上書きされた場合にデータをすばやく回復させるために使用できます。旧バージョンを移行または期限切れにするライフサイクルルールを設定せずに S3 バージョニングを有効にした場合、旧バージョンが大量に蓄積され、ストレージコストに影響する可能性があります。詳細については、「S3 バージョニングによる複数のバージョンのオブジェクトの保持」を参照してください。

ステップ 1: 最新でないオブジェクトバージョンが最も多いバケットを特定する

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ナビゲーションペインで、[Storage Lens] (ストレージレンズ)、[Dashboards] (ダッシュボード) の順にクリックします。
3. [Dashboards] (ダッシュボード) リストで、表示するダッシュボードを選択します。
4. [Snapshot for date] (日付のスナップショット) セクションの [Metrics categories] (メトリクスのカテゴリ) で、[Cost optimization] (コスト最適化) を選択します。

[Snapshot for date] (日付のスナップショット) セクションが更新され、[Cost optimization] (コスト最適化) メトリクスが表示されます。これには、[% noncurrent version bytes] (旧バージョンのバイト数 %) メトリクスが含まれます。[% noncurrent version bytes] (旧バージョンのバイト数 %) のメトリクスは、ダッシュボードの範囲内かつ選択された日付に関して、ストレージの合計バイト数のうち、旧バージョンに起因するバイト数の割合を表します。

> **Note**
>
> [% noncurrent version bytes] (旧バージョンのバイト数 %) がアカウントレベルでストレージの 10 パーセントを超過する場合、保存しているオブジェクトバージョンの数が多すぎる可能性があります。

5. 旧バージョンが大量に蓄積されているバケットを特定するには:

   a. [Top N overview for date] (日付の上位 N の概要) セクションまで下にスクロールします。[Top N] (上位 N) には、データを表示したいバケットの数を入力します。

   b. [Metric] (メトリクス) で、[% noncurrent version bytes] (旧バージョンのバイト数 %) を選択します。

      [Top number buckets] (バケットの上位) の下に、[% noncurrent version bytes] (旧バージョンのバイト数 %) が最も高い (指定した数の) バケットが表示されます。[Top N overview for date] (日付の上位 N の概要) セクションには、前日または前週からの変化率と、トレンドを視覚化するスパークラインも表示されます。この傾向は、無料メトリクスの場合は 14 日間、高度なメトリクスとレコメンデーションの場合は 30 日間の傾向です。

      > **Note**
      >
      > S3 ストレージレンズの高度なメトリクスとレコメンデーションの場合、メトリクスは 15 か月間クエリで利用できます。詳細については、「メトリクスの選択」を参照してください。

   c. 最新でないオブジェクトバージョンに関する詳細なバケットレベルのメトリクスを表示するには、ページの一番上までスクロールして、[Bucket] (バケット) タブを選択します。

      S3 ストレージレンズダッシュボードのどのグラフや可視化でも、[Account] (アカウント)、[AWS リージョン]、[Storage class] (ストレージクラス)、または [Bucket] (バケット) タブを使用して、より深いレベルの集計にドリルダウンできます。例については、コールド Amazon S3 バケットを検出するを参照してください。

d. [Buckets] (バケット) セクションの [Metric categories] (メトリクスカテゴリ) で、[Cost optimization] (コスト最適化) を選択します。次に。[Summary] (概要) を選択解除します。

   旧バージョンに関連する他のメトリクスと共に、[% noncurrent version bytes] (旧バージョンのバイト数 %) メトリクスを確認できるようになりました。

ステップ 2: 旧バージョンを管理するための移行および有効期限のライフサイクルルールがないバケットを特定する

前提条件

S3 ストレージレンズダッシュボードで [Noncurrent version transition lifecycle rule count] (旧バージョン移行ライフサイクルルール数) および [Noncurrent version expiration lifecycle rule count] (旧バージョン有効期限ライフサイクルルール数) メトリクスを確認するには、S3 ストレージレンズの [Advanced metrics and recommendations] (高度なメトリクスとレコメンデーション)を有効にしてから、[Advanced cost optimization metrics] (高度なコスト最適化メトリクス) を選択する必要があります。詳細については、「S3 コンソールの使用」を参照してください。

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ナビゲーションペインで、[Storage Lens] (ストレージレンズ)、[Dashboards] (ダッシュボード) の順にクリックします。
3. [Dashboards] (ダッシュボード) リストで、表示するダッシュボードを選択します。
4. ストレージレンズダッシュボードで、[Bucket] (バケット) タブを選択します。
5. [Buckets] (バケット) セクションまで下にスクロールします。[Metrics categories] (メトリクスのカテゴリ) で、[Cost optimization] (コスト最適化) を選択します。次に，[Summary] (概要) を選択解除します。

   [Buckets] (バケット) リストが更新され、表示されているバケットで利用可能なすべての [Cost optimization] (コスト最適化) メトリクスが表示されます。
6. [Buckets] (バケット) リストをフィルタリングして特定のコスト最適化メトリクスのみを表示するには、設定アイコン
   ( )
   を選択します。
7. 次の項目だけが選択された状態になるまで、他のすべてのコスト最適化メトリクスを選択解除します。

- % noncurrent version bytes (旧バージョンのバイト数 %)
- Noncurrent version transition lifecycle rule count (旧バージョン移行ライフサイクルルール数)
- Noncurrent version expiration lifecycle rule count (旧バージョン有効期限ライフサイクルルール数)

8. (オプション) [Page size] (ページサイズ) で、リストに表示するバケットの数を選択します。
9. [確認] を選択してください。

   [Buckets] (バケット)リストが更新され、旧バージョンのバイト数と旧バージョンのライフサイクルルール数のメトリクスが表示されます。このデータを使用して、旧バージョンのバイト数の割合が高いが、移行および有効期限のライフサイクルルールが欠落しているバケットを特定できます。次に、S3 コンソールでこれらのバケットに移動し、これらのバケットにライフサイクルルールを追加できます。

ステップ 3: ライフサイクルルールを追加して最新でないオブジェクトバージョンを移行または期限切れにする

追加の調査が必要なバケットを判断したら、S3 コンソールでそのバケットに移動し、指定した日数後に旧バージョンを失効させるライフサイクルルールを追加できます。あるいは、旧バージョンを保持したままコストを削減するために、旧バージョンを Amazon S3 Glacier ストレージクラスのいずれかに移行するライフサイクルルールを設定することもできます。詳細については、「バージョニングが有効なバケットへのライフサイクルルールを指定する」を参照してください。

ライフサイクルルールがないバケットを特定し、ライフサイクルルール数を確認する

S3 ストレージレンズには、ライフサイクルルールがないバケットを特定するために使用できる S3 ライフサイクルルール数メトリクスが用意されています。ライフサイクルルールがないバケットを見つけるには、[Total buckets without lifecycle rules] (ライフサイクルルールがないバケットの合計数) メトリクスを使用できます。S3 ライフサイクル設定のないバケットには、不要になったストレージや、低コストのストレージクラスに移行できるストレージがある可能性があります。ライフサイクルルール数メトリクスを使用して、有効期限ルールや移行ルールなど、特定の種類のライフサイクルルールが欠落しているバケットを特定することもできます。

前提条件

S3 ライフサイクルダッシュボードでライフサイクルルール数のメトリクスと [Total buckets without lifecycle rules] (ライフサイクルルールがないバケットの合計数) メトリクスを表示するには、S3 ストレージレンズの [Advanced metrics and recommendations] (高度なメトリクスとレコメンデーション)

を有効にしてから [Advanced cost optimization metrics] (高度なコスト最適化メトリクス) を選択する必要があります。詳細については、「S3 コンソールの使用」を参照してください。

ステップ 1: ライフサイクルルールが設定されていないバケットを特定する

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ナビゲーションペインで、[Storage Lens] (ストレージレンズ)、[Dashboards] (ダッシュボード) の順にクリックします。
3. [Dashboards] (ダッシュボード) リストで、表示するダッシュボードを選択します。
4. ライフサイクルルールのない特定のバケットを確認するには、[Top N overview for date] (日付の上位 N の概要) セクションまで下にスクロールします。

   デフォルトでは、[Top N overview for date] (日付の上位 N の概要) セクションには、上位 3 つのバケットのメトリクスが表示されます。[Top N] (トップ N) のフィールドでバケット数を増やすことができます。[Top N overview for date] (日付のトップ N の概要) セクションには、前日または前週からの変化率と、傾向を視覚化するスパークラインも表示されます。この傾向は、無料メトリクスの場合は 14 日間、高度なメトリクスとレコメンデーションの場合は 30 日間の傾向です。

   > **Note**
   >
   > S3 ストレージレンズの高度なメトリクスとレコメンデーションの場合、メトリクスは 15 か月間クエリで利用できます。詳細については、「メトリクスの選択」を参照してください。

5. [Metric] (メトリクス) で、[Total buckets without lifecycle rules] (ライフサイクルルールがないバケットの合計数) を [Cost optimization] (コスト最適化) カテゴリから選択します。
6. [Total buckets without lifecycle rules] (ライフサイクルルールがないバケットの合計数) については、次のデータを確認してください:

   - Top number accounts (アカウント上位) – ライフサイクルルールのないバケット数が最も多いアカウントを確認できます。
   - Top number Regions (地域の上位) – ライフサイクルルールのないバケットの内訳を地域別に表示します。
   - Top number buckets (バケットの上位) – どのバケットにライフサイクルルールがないかを確認できます。

S3 ストレージレンズダッシュボードのどのグラフや可視化でも、[Account] (アカウント)、[AWS リージョン]、[Storage class] (ストレージクラス)、または [Bucket] (バケット) タブを使用して、より深いレベルの集計にドリルダウンできます。例については、コールド Amazon S3 バケットを検出するを参照してください。

ライフサイクルルールがないバケットを特定したら、バケットの特定のライフサイクルルール数を確認することもできます。

ステップ 2: バケットのライフサイクルルール数を確認する

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ナビゲーションペインで、[Storage Lens] (ストレージレンズ)、[Dashboards] (ダッシュボード) の順にクリックします。
3. [Dashboards] (ダッシュボード) リストで、表示するダッシュボードを選択します。
4. S3 ストレージレンズダッシュボードで、[Bucket] (バケット) タブを選択します。
5. [Buckets] (バケット) セクションまで下にスクロールします。[Metrics categories] (メトリクスのカテゴリ) で、[Cost optimization] (コスト最適化) を選択します。次に , [Summary] (概要) を選択解除します。

   [Buckets] (バケット) リストが更新され、表示されているバケットで利用可能なすべての [Cost optimization] (コスト最適化) メトリクスが表示されます。
6. [Buckets] (バケット) リストをフィルタリングして特定のコスト最適化メトリクスのみを表示するには、設定アイコン
   ( )
   を選択します。
7. 次の項目だけが選択された状態になるまで、他のすべてのコスト最適化メトリクスを選択解除します。

   - Transition lifecycle rule count (移行ライフサイクルルール数)
   - Expiration lifecycle rule count (有効期限ライフサイクルルール数)
   - Noncurrent version transition lifecycle rule count (旧バージョン移行ライフサイクルルール数)
   - Noncurrent version expiration lifecycle rule count (旧バージョン有効期限ライフサイクルルール数)

- Abort incomplete multipart upload lifecycle rule count (未完了のマルチパートアップロードの中止ライフサイクルルール数)
- Total lifecycle rule count (ライフサイクルルールの合計数)

8. (オプション) [Page size] (ページサイズ) で、リストに表示するバケットの数を選択します。
9. [確認] を選択してください。

   [Buckets] (バケット) リストが更新され、バケットのライフサイクルルール数メトリクスが表示されます。このデータを使用して、ライフサイクルルールがないバケットや、有効期限や移行ルールなどの特定の種類のライフサイクルルールがないバケットを特定できます。次に、S3 コンソールでこれらのバケットに移動し、これらのバケットにライフサイクルルールを追加できます。

ステップ 3: ライフサイクルルールを追加する

ライフサイクルルールのないバケットを特定したら、ライフサイクルルールを追加できます。詳細については、「バケットに S3 ライフサイクル設定を設定する」および「S3 ライフサイクル設定の例」を参照してください。

S3 ストレージレンズによるデータ保護

Amazon S3 ストレージレンズのデータ保護メトリクスを使用して、データ保護のベストプラクティスが適用されていないバケットを特定できます。これらのメトリクスを使用して対策を講じ、ベストプラクティスに沿った標準設定を適用して、アカウントや組織内のさまざまなバケットにわたってデータを保護できます。例えば、データ保護メトリクスを使用して、デフォルトの暗号化に AWS Key Management Service (AWS KMS) キー (SSE-KMS) を使用しないバケットや、AWS Signature Version 2 (SigV2) を使用するリクエストを特定できます。

以下のユースケースでは、S3 ストレージレンズダッシュボードを使用して外れ値を特定し、S3 バケット全体にデータ保護のベストプラクティスを適用する戦略を提供します。

トピック

- AWS KMS によるデフォルトの暗号化 (SSE-KMS) でサーバー側暗号化を使用しないバケットを識別する
- S3 バージョニングが有効なバケットを識別する
- AWS Signature Version 2 (SigV2) を使用したリクエストを識別する
- 各バケットのレプリケーションルールの総数を数える
- オブジェクトロックバイトのパーセンテージを識別する

AWS KMS によるデフォルトの暗号化 (SSE-KMS) でサーバー側暗号化を使用しないバケットを識別する

Amazon S3 のデフォルトの暗号化を使用して、S3 バケットのデフォルト暗号化の動作を設定できます。詳細については、「the section called “デフォルトのバケット暗号化の設定”」を参照してください。

[SSE-KMS enabled bucket count] (SSE-KMS 対応バケット数) と[% SSE-KMS enabled buckets] (% SSE-KMS 対応バケット) メトリクスを使用して、デフォルトの暗号化に AWS KMS キー (SSE-KMS) によるサーバー側暗号化を使用しているバケットを特定できます。S3 ストレージレンズは、暗号化されていないバイト、暗号化されていないオブジェクト、暗号化されたバイト、および暗号化されたオブジェクトのメトリクスも提供します。メトリクスの一覧については、「Amazon S3 Storage Lens のメトリクスに関する用語集」を参照してください。

SSE-KMS 暗号化メトリクスを一般的な暗号化メトリクスのコンテキストで分析すると、SSE-KMS を使用していないバケットを特定できます。アカウントまたは組織のすべてのバケットに SSE-KMS を使用する場合は、これらのバケットのデフォルトの暗号化設定を SSE-KMS を使用するように更新できます。SSE-KMS に加え、Amazon S3 で管理されたキー (SSE-S3) またはお客様から提供されたキー (SSE-C) によりサーバー側の暗号化を使用できます。詳細については、「暗号化によるデータの保護」を参照してください。

ステップ 1: どのバケットがデフォルトの暗号化に SSE-KMS を使用しているかを特定する

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ナビゲーションペインで、[Storage Lens] (ストレージレンズ)、[Dashboards] (ダッシュボード) の順にクリックします。
3. [Dashboards] (ダッシュボード) リストで、表示するダッシュボードを選択します。
4. [Trends and distributions] (傾向とディストリビューション) セクションで、プライマリメトリクスには [% SSE-KMS enabled bucket count] (% SSE-KMS 対応バケット数) を選択し、セカンダリメトリクスには [% encrypted bytes] (% 暗号化バイト数) を選択します。

   [Trend for date] (日付の傾向) グラフが更新され、SSE-KMS と暗号化されたバイトの傾向が表示されます。
5. SSE-KMS の詳細なバケットレベルのインサイトを表示するには:

   a. グラフ上のポイントを選択します。より詳細なインサイトの選択肢が記載されたボックスが表示されます。

b. [Buckets] (バケット) ディメンションを選択します。次に、適用を選択します。

6. [Distribution by buckets for date] (日付のバケット別分布) グラフで、[SSE-KMS enabled bucket count] (SSE-KMS 対応のバケット数) メトリクスを選択します。
7. これで、SSE-KMS が有効になっているバケットと有効になっていないバケットを確認できます。

ステップ 2: バケットのデフォルトの暗号化設定を更新する

どのバケットが [% encrypted bytes] (% 暗号化バイト) のコンテキストで SSE-KMS を使用するかを確認できたので、SSE-KMS を使用しないバケットを特定できます。その後、オプションで S3 コンソール内のこれらのバケットに移動し、デフォルトの暗号化設定を SSE-KMS または SSE-S3 を使用するように更新できます。詳細については、「デフォルトの暗号化の設定」を参照してください。

S3 バージョニングが有効なバケットを識別する

S3 バージョニング機能を有効にすると、同じオブジェクトの複数のバージョンが保持されます。これらは、オブジェクトが誤って削除された、または上書きされた場合にデータをすばやく回復させるために使用できます。[Versioning-enabled bucket count] (バージョニングが有効なバケット数) メトリクスを使用して、どのバケットが S3 バージョニングを使用しているかを確認できます。次に、S3 コンソールでアクションを実行して、他のバケットの S3 バージョニングを有効にできます。

ステップ 1: S3 バージョニングが有効なバケットを識別する

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. ナビゲーションペインで、[Storage Lens]、[ダッシュボード] の順にクリックします。
3. [Dashboards] (ダッシュボード) リストで、表示するダッシュボードを選択します。
4. [Trends and distributions] (傾向とディストリビューション) セクションで、プライマリメトリクスには [Versioning-enabled bucket count] (バージョニングが有効なバケット数) を選択し、セカンダリメトリクスには [Buckets] (バケット) を選択します。

   [Trend for date] (日付の傾向) グラフが更新され、S3 バージョニングが有効なバケットの傾向が表示されます。トレンドラインのすぐ下に、[Storage class distribution] (ストレージクラスディストリビューション) と[Region distribution] (リージョンディストリビューション) サブセクションが表示されます。
5. [Trend for date] (日付の傾向) グラフに表示されているバケットについてより詳細なインサイトを表示して、より詳細な分析を実行できるようにするには、次の操作を行います。

a. グラフ上のポイントを選択します。より詳細なインサイトの選択肢が記載されたボックスが表示されます。

b. データに適用するディメンションを [Account] (アカウント)、[AWS リージョン]、[Storage class] (ストレージクラス)、[Bucket] (バケット) から選択して、より詳細な分析を行います。次に、適用を選択します。

6. [Bubble analysis by buckets for date] (日付別のバケットによるバブル分析) セクションで、[Versioning-enabled bucket count] (バージョニングが有効なバケット数)、[Buckets] (バケット)、[Active buckets] (アクティブバケット) のメトリクスを選択します。

   [Bubble analysis by buckets for date] (日付別のバケットごとのバブル分析) セクションが更新され、選択したメトリクスのデータが表示されます。このデータを使用して、合計バケット数に関連して、どのバケットで S3 バージョニングが有効になっているかを確認できます。[Bubble analysis by buckets for date] (日付のバケットによるバブル分析) セクションでは、バブルの [X-axis](X 軸)、[Y-axis] (Y 軸)、および [Size] (サイズ) を表す 3 つのメトリクスを使用して、バケットを複数のディメンションにプロットできます。

ステップ 2: S3 バージョニングを有効にする

S3 バージョニングが有効になっているバケットを特定したら、S3 バージョニングが有効になっていないバケット、またはバージョニングが停止されているバケットを特定できます。次に、オプションで S3 コンソールでこれらのバケットのバージョニングを有効にできます。詳細については、「バケットでのバージョニングの有効化」を参照してください。

AWS Signature Version 2 (SigV2) を使用したリクエストを識別する

[All unsupported signature requests] (すべてのサポートされていない署名リクエスト) メトリクスを使用して、AWS Signature Version 2 (SigV2) を使用するリクエストを特定できます。このデータは、SigV2 を使用している特定のアプリケーションを特定するのに役立ちます。その後、これらのアプリケーションを AWS Signature Version 4 (SigV4) に移行できます。

SigV4 はすべての新しい S3 アプリケーションに推奨される署名方法です。SigV4 はセキュリティが向上し、すべての AWS リージョン でサポートされています。詳細については、「Amazon S3 更新 - SigV2 の非推奨期間の延長および変更」を参照してください。

前提条件

[All unsupported signature requests] (すべてのサポートされていない署名リクエスト) を S3 ストレージレンズダッシュボードに表示するには、S3 ストレージレンズの [Advanced metrics and

recommendations] (高度なメトリクスとレコメンデーション) を有効にしてから、[Advanced data protection metrics] (高度なデータ保護メトリクス) を選択します。詳細については、「S3 コンソールの使用」を参照してください。

ステップ 1: SigV2 署名の傾向を AWS アカウント、リージョン、バケット別に調べる

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ナビゲーションペインで、[Storage Lens] (ストレージレンズ)、[Dashboards] (ダッシュボード) の順にクリックします。
3. [Dashboards] (ダッシュボード) リストで、表示するダッシュボードを選択します。
4. SigV2 を使用するリクエストがある特定のバケット、アカウント、リージョンを特定するには:

   a. [Top N] (トップ N) の [Top N overview for date] (日付のトップ N 概要) に、データを表示したいバケットの数を入力します。

   b. [Metric] (メトリクス) では、[Data protection] (データ保護) カテゴリから [All unsupported signature requests] (すべてのサポートされていない署名リクエスト) を選択します。

      [Top N overview for date] (日付のトップ N 概要) が更新され、アカウント、AWS リージョン、バケット別に SigV2 リクエストのデータが表示されます。[Top N overview for date] (日付のトップ N の概要) セクションには、前日または前週からの変化率と、傾向を視覚化するスパークラインも表示されます。この傾向は、無料メトリクスの場合は 14 日間、高度なメトリクスとレコメンデーションの場合は 30 日間の傾向です。

      > **Note**
      >
      > S3 ストレージレンズの高度なメトリクスとレコメンデーションの場合、メトリクスは 15 か月間クエリで利用できます。詳細については、「メトリクスの選択」を参照してください。

ステップ 2: SigV2 リクエストを通じてアプリケーションからアクセスされるバケットを特定する

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ナビゲーションペインで、[Storage Lens] (ストレージレンズ)、[Dashboards] (ダッシュボード) の順にクリックします。

3. [Dashboards] (ダッシュボード) リストで、表示するダッシュボードを選択します。
4. ストレージレンズダッシュボードで、[Bucket] (バケット) タブを選択します。
5. [Buckets] (バケット) セクションまで下にスクロールします。[Metrics categories] (メトリクスのカテゴリ) で、[Data protection] (データ保護) を選択します。次に、[Summary] (概要) を選択解除します。

   [Buckets] (バケット) リストが更新され、表示されているバケットで利用可能なすべての [Data protection] (データ保護) メトリクスが表示されます。
6. [Buckets] (バケット) リストをフィルタリングして特定のデータ保護メトリクスのみを表示するには、設定アイコン
   ( )
   を選択します。
7. 次の項目だけが選択された状態になるまで、他のすべてのデータ保護メトリクスを選択解除します。

   - [All unsupported signature requests] (すべてのサポートされていない署名リクエスト)
   - [% all unsupported signature requests] (% すべてのサポートされていない署名リクエスト)
8. (オプション) [Page size] (ページサイズ) で、リストに表示するバケットの数を選択します。
9. [確認] を選択してください。

   [Buckets] (バケット) リストが更新され、SigV2 リクエストのバケットレベルのメトリクスが表示されます。このデータを使用して、SigV2 リクエストがある特定のバケットを特定できます。次に、この情報を使用してアプリケーションを SigV4 に移行できます。詳細については、Amazon Simple Storage Service API リファレンスの「リクエストの認証 (AWS 署名バージョン 4)」を参照してください。

各バケットのレプリケーションルールの総数を数える

S3 レプリケーションを使用すると、Amazon S3 バケット間でオブジェクトを自動で非同期的にコピーできます。オブジェクトのレプリケーション用に設定されたバケットは、同じ AWS アカウントが所有することも、異なるアカウントが所有することもできます。詳細については、「リージョン内およびリージョン間でのオブジェクトのレプリケート」を参照してください。

S3 ストレージレンズのレプリケーションルール数メトリクスを使用して、レプリケーション用に設定されているバケットに関する詳細なバケットごとの情報を取得できます。この情報には、バケット内とリージョン内およびバケット間とリージョン間のレプリケーションルールが含まれます。

前提条件

レプリケーションルール数メトリクスを S3 ストレージレンズダッシュボードに表示するには、S3 ストレージレンズ [Advanced metrics and recommendations] (高度なメトリクスとレコメンデーション) を有効にしてから、[Advanced data protection metrics] (高度なデータ保護メトリクス) を選択します。詳細については、「S3 コンソールの使用」を参照してください。

ステップ 1: 各バケットのレプリケーションルールの総数を数える

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ナビゲーションペインで、[Storage Lens] (ストレージレンズ)、[Dashboards] (ダッシュボード) の順にクリックします。
3. [Dashboards] (ダッシュボード) リストで、表示するダッシュボードを選択します。
4. ストレージレンズダッシュボードで、[Bucket] (バケット) タブを選択します。
5. [Buckets] (バケット) セクションまで下にスクロールします。[Metrics categories] (メトリクスのカテゴリ) で、[Data protection] (データ保護) を選択します。次に、[Summary] (概要) を選択解除します。
6. [Buckets] (バケット) リストをフィルタリングしてレプリケーションルール数メトリクスのみを表示するには、設定アイコン ( ) を選択します。
7. レプリケーションルール数メトリクスだけが選択された状態になるまで、他のすべてのデータ保護メトリクスを選択解除します。
   - [Same-Region Replication rule count] (同一リージョンレプリケーションのルール数)
   - [Cross-Region Replication rule count] (クロスリージョンレプリケーションルール数)
   - [Same-account replication rule count] (同一アカウントレプリケーションのルール数)
   - [Cross-account replication rule count] (クロスリージョンレプリケーションルール数)
   - [Total replication rule count] (レプリケーションルールの合計数)
8. (オプション) [Page size] (ページサイズ) で、リストに表示するバケットの数を選択します。
9. [確認] を選択してください。

ステップ 2: レプリケーションルールを追加する

バケットごとのレプリケーションルール数が決まったら、オプションで追加のレプリケーションルールを作成できます。詳細については、「ライブレプリケーションの設定例」を参照してください。

オブジェクトロックバイトのパーセンテージを識別する

S3 オブジェクトロックでは、write-once-read-many (WORM) モデルを使用してオブジェクトを保存できます。オブジェクトロックを使用して、オブジェクトが削除または上書きされることを、一定期間または無期限に防止できます。オブジェクトロックは、バケットを作成する場合にのみ有効にでき、S3 バージョニングも有効化できます。ただし、個々のオブジェクトバージョンの保存期間を編集したり、オブジェクトロックが有効になっているバケットにリーガルホールドを適用したりできます。詳細については、「S3 Object Lock を使用したオブジェクトのロック」を参照してください。

S3 ストレージレンズのオブジェクトロックメトリクスを使用して、アカウントまたは組織の [% Object Lock bytes] (% オブジェクトロックバイト) メトリクスを確認できます。この情報を使用して、アカウントまたは組織内のどのバケットがデータ保護のベストプラクティスに従っていないかを特定できます。

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ナビゲーションペインで、[Storage Lens] (ストレージレンズ)、[Dashboards] (ダッシュボード) の順にクリックします。
3. [Dashboards] (ダッシュボード) リストで、表示するダッシュボードを選択します。
4. [Snapshot] (スナップショット) セクションの [Metrics categories] (メトリクスのカテゴリ) で、[Data protection] (データ保護) を選択します。

   [Snapshot] (スナップショット) セクションが更新され、[% Object Lock bytes] (% オブジェクトロックバイト) メトリクスを含むデータ保護メトリクスが表示されます。アカウントまたは組織のオブジェクトロックバイトの全体のパーセンテージを確認できます。
5. バケットあたりの [% Object Lock bytes] (% オブジェクトロックバイト) を確認するには、[Top N overview] (トップ N の概要) セクションまでスクロールしてください。

   オブジェクトロックのオブジェクトレベルのデータを取得するには、[Object Lock object count] (オブジェクトロックオブジェクト数) と[% Object Lock objects] (% オブジェクトロックオブジェクト) メトリクスを使用することもできます。
6. [Metric] (メトリクス) には、[Data protection] (データ保護) カテゴリから [% Object Lock bytes] (% オブジェクトロックバイト) を選択します。

デフォルトでは、[Top N overview for date] (日付のトップ N の概要) セクションには、上位 3 つのバケットのメトリクスが表示されます。[Top N] (トップ N) のフィールドでバケット数を増やすことができます。[Top N overview for date] (日付のトップ N の概要) セクションには、前日または前週からの変化率と、傾向を視覚化するスパークラインも表示されます。この傾向は、無料メトリクスの場合は 14 日間、高度なメトリクスとレコメンデーションの場合は 30 日間の傾向です。

> **Note**
>
> S3 ストレージレンズの高度なメトリクスとレコメンデーションの場合、メトリクスは 15 か月間クエリで利用できます。詳細については、「メトリクスの選択」を参照してください。

7. [% Object Lock bytes] (% オブジェクトロックバイト) については、次のデータを確認してください。

   - [Top number accounts] (上位アカウント数) – [% Object Lock bytes] (% オブジェクトロックバイト) が最も高いアカウントと最も低いアカウントを確認できます。
   - [Top number Regions] (上位リージョン数) – リージョン別の [% Object Lock bytes] (% オブジェクトロックバイト) の内訳を表示します。
   - [Top number buckets] (上位バケット数) – [% Object Lock bytes] (% オブジェクトロックバイト) が最も高いバケットと最も低いバケットを確認できます。

オブジェクト所有権設定を監査するための S3 の使用

Amazon S3 オブジェクト所有権は、S3 バケットレベルの設定で、アクセスコントロールリスト (ACL) を無効にし、バケット内のオブジェクトの所有権を制御するために使用できます。オブジェクト所有権をバケット所有者強制に設定する場合、アクセスコントロールリスト (ACL) を無効にして、バケット内のすべてのオブジェクトの所有権を取得できます。この方法により、Amazon S3 に保存されているデータのアクセス管理を簡素化できます。

デフォルトでは、別の AWS アカウント がオブジェクトを S3 バケットにアップロードすると、そのアカウント (オブジェクトライター) がオブジェクトを所有し、そのオブジェクトにアクセスでき、ACL を介して他のユーザーにそのオブジェクトへのアクセスを許可できます。オブジェクトの所有権を使用して、このデフォルトの動作を変更できます。

Amazon S3 の最新のユースケースの大部分では ACL を使用する必要がなくなっています。そのため、オブジェクトごとに個別に制御する必要がある異常な状況を除き、ACL を無効にすることをお勧めします。オブジェクトの所有権をバケット所有者に強制設定することで、ACL を無効にして、アクセスコントロールに関するポリシーに依存できます。詳細については、「オブジェクトの所有権の制御とバケットの ACL の無効化。」を参照してください。

S3 ストレージレンズのアクセス管理メトリクスを使用すると、ACL が無効になっていないバケットを特定できます。これらのバケットを特定したら、ACL のアクセス許可をポリシーに移行し、これらのバケットの ACL を無効にできます。

トピック

- ステップ 1: オブジェクト所有権設定の一般的な傾向を特定する
- ステップ 2: オブジェクト所有権設定のバケットレベルの傾向を把握する
- ステップ 3: オブジェクト所有権の設定をバケット所有者強制に更新し、ACL を無効にする

ステップ 1: オブジェクト所有権設定の一般的な傾向を特定する

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ナビゲーションペインで、[Storage Lens] (ストレージレンズ)、[Dashboards] (ダッシュボード) の順にクリックします。
3. [Dashboards] (ダッシュボード) リストで、表示するダッシュボードを選択します。
4. [Snapshot for date] (日付のスナップショット) セクションの [Metrics categories] (メトリクスのカテゴリ) で、[Access management] (アクセス管理) を選択します。

   [Snapshot for date] (日付のスナップショット) セクションが更新され、[% Object Ownership bucket owner enforced] (% オブジェクト所有権のバケット所有者強制) メトリクスが表示されます。アカウントまたは組織内のバケットで、オブジェクト所有権のバケット所有者強制設定を使用して ACL を無効にしているバケット全体の割合を確認することができます。

ステップ 2: オブジェクト所有権設定のバケットレベルの傾向を把握する

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ナビゲーションペインで、[Storage Lens] (ストレージレンズ)、[Dashboards] (ダッシュボード) の順にクリックします。

3. [Dashboards] (ダッシュボード) リストで、表示するダッシュボードを選択します。
4. バケットレベルの詳細なメトリクスを表示するには、[Bucket] (バケット) タブを選択します。
5. [Distribution by buckets for date] (日付のバケットによる配分) セクションで、[% Object Ownership bucket owner enforced] (% オブジェクト所有権のバケット所有者強制) メトリクスを選択します。

   グラフが更新され、[% Object Ownership bucket owner enforced].(% オブジェクト所有権のバケット所有者強制) のバケットごとの内訳が表示されます。どのバケットがオブジェクト所有権のバケット所有者強制設定を使用して ACL を無効にしているかを確認できます。
6. バケット所有者強制設定をコンテキストで確認するには、[Buckets] (バケット) セクションまでスクロールします。[Metrics categories] (メトリクスのカテゴリ) で、[Access management] (アクセス管理) を選択します。次に、[Summary] (概要) を選択解除します。

   [Buckets] (バケット) リストには、バケット所有者強制、バケット所有者優先、オブジェクト作成者の 3 つのオブジェクト所有権設定すべてのデータが表示されます。
7. [Buckets] (バケット) リストをフィルタリングして特定のオブジェクト所有権設定のみのメトリクスを表示するには、設定アイコン ( ) を選択します。
8. 表示しないメトリクスを選択解除します。
9. (オプション) [Page size] (ページサイズ) で、リストに表示するバケットの数を選択します。
10. [確認] を選択してください。

ステップ 3: オブジェクト所有権の設定をバケット所有者強制に更新し、ACL を無効にする

オブジェクト所有権にオブジェクト作成者およびバケット所有者優先設定を使用しているバケットを特定したら、ACL アクセス許可をバケットポリシーに移行できます。ACL アクセス許可の移行が完了したら、オブジェクト所有権の設定をバケット所有者強制に更新して ACL を無効にできます。詳細については、「ACL を無効にする前提条件。」を参照してください。

S3 ストレージレンズのメトリクスを使用してパフォーマンスを改善する

S3 ストレージレンズの高度なメトリクスを有効にしている場合は、詳細なステータスコードのメトリクスを使用して、リクエストの成功または失敗の数を取得できます。この情報は、アクセスまたはパフォーマンス問題のトラブルシューティングに役立てることができます。詳細なステータスコードのメトリクスには、「403 Forbidden」や「503 Service Unavailable」などの HTTP ステータスコー

ドの数が表示されます。S3 バケット、アカウント、組織にわたる詳細なステータスコードのメトリクスの全体的な傾向を調べることができます。次に、バケットレベルのメトリクスを詳しく調べて、そのバケットに現在アクセスしていてエラーの原因となっているワークロードを特定できます。

例えば、403 Forbidden エラー数メトリクスを見ると、適切なアクセス権限が適用されていない状態でバケットにアクセスしているワークロードを特定できます。これらのワークロードを特定したら、S3 ストレージレンズ以外で詳しく調べて 403 Forbidden エラーのトラブルシューティングを行うことができます。

この例では、403 Forbidden エラー数と % 403 Forbidden エラーのメトリクスを使用して、403 Forbidden エラーの傾向分析を行う方法を示しています。これらのメトリクスを使用すると、適切なアクセス権限が適用されていないバケットにアクセスしているワークロードを特定できます。他の[Detailed status code metrics] (詳細なステータスコードのメトリクス) についても同様の傾向分析を行うことができます。詳細については、「Amazon S3 Storage Lens のメトリクスに関する用語集」を参照してください。

前提条件

S3 ストレージレンズのダッシュボードに[Detailed status code metrics] (詳細なステータスコードのメトリクス) を表示するには、S3 ストレージレンズの [Advanced metrics and recommendations] (高度なメトリクスとレコメンデーション) を有効にしてから、[Detailed status code metrics] (詳細なステータスコードのメトリクス) を選択する必要があります。詳細については、「S3 コンソールの使用」を参照してください。

トピック

- ステップ 1: 個々の HTTP ステータスコードの傾向分析を行う
- ステップ 2: バケットごとのエラー数を分析する
- ステップ 3: エラーをトラブルシューティングする

ステップ 1: 個々の HTTP ステータスコードの傾向分析を行う

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ナビゲーションペインで、[Storage Lens] (ストレージレンズ)、[Dashboards] (ダッシュボード) の順にクリックします。
3. [Dashboards] (ダッシュボード) リストで、表示するダッシュボードの名前を選択します。

4. [Trends and distributions] (傾向とディストリビューション) セクションの [Primary metric] (プライマリメトリクス) で、[Detailed status codes] (詳細なステータスコード) カテゴリから [403 Forbidden error count] (403 Forbidden エラー数) を選択します。[Secondary metric] (セカンダリメトリクス) で、[% 403 Forbidden errors] (% 403 Forbidden エラー) を選択します。
5. [Top N overview for date] (日付の上位 N の概要) セクションまで下にスクロールします。[Metrics] (メトリクス) では、[Detailed status codes] (詳細なステータスコード) カテゴリから [403 Forbidden error count] (403 Forbidden エラー数) または [% 403 Forbidden errors] (% 403 Forbidden エラー)を選択します。

   [Top N overview for date] (日付の上位 N の概要) セクションが更新され、アカウント、AWS リージョン、バケット別の上位の 403 Forbidden エラー数が表示されます。

ステップ 2: バケットごとのエラー数を分析する

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ナビゲーションペインで、[Storage Lens] (ストレージレンズ)、[Dashboards] (ダッシュボード) の順にクリックします。
3. [Dashboards] (ダッシュボード) リストで、表示するダッシュボードを選択します。
4. ストレージレンズダッシュボードで、[Bucket] (バケット) タブを選択します。
5. [Buckets] (バケット) セクションまで下にスクロールします。[Metrics categories] (メトリクスのカテゴリ) で、[Detailed status codes] (詳細なステータスコード) のメトリクスを選択します。次に、[Summary] (概要) を選択解除します。

   [Bucket] (バケット) リストが更新され、詳細なステータスコードの利用可能なメトリクスがすべて表示されます。この情報を使用して、特定の HTTP ステータスコードの割合が高いバケットと、バケット間で共通するステータスコードを確認できます。
6. [Bucket] (バケット) リストをフィルタリングして特定の詳細なステータスコードのメトリクスのみを表示するには、設定アイコン ( ) を選択します。
7. [Bucket] (バケット) リストに表示したくない詳細なステータスコードのメトリクスがある場合は、トグルをオフにします。
8. (オプション) [Page size] (ページサイズ) で、リストに表示するバケットの数を選択します。
9. [確認] を選択してください。

[Bucket] (バケット) リストには、指定したバケットの数のエラー数メトリクスが表示されます。この情報を使用して、多くのエラーが発生している特定のバケットを特定し、バケットごとにエラーをトラブルシューティングできます。

ステップ 3: エラーをトラブルシューティングする

特定の HTTP ステータスコードの割合が高いバケットを特定したら、これらのエラーをトラブルシューティングできます。詳細については次を参照してください:

- Amazon S3 でファイルをアップロードしようとすると、「403 Forbidden」(403 禁止) エラーが表示されるのはなぜですか?
- Amazon S3 のバケットポリシーを変更しようとすると、「403 Forbidden」(403 禁止) エラーが表示されるのはなぜですか?
- すべてのリソースが同じ AWS アカウント に属している Amazon S3 バケットの「403 Forbidden」(403 禁止) エラーをトラブルシューティングするにはどうすればよいですか?
- Amazon S3 からの HTTP 500 または 503 エラーをトラブルシューティングするにはどうすればよいですか?

AWS Organizations での Amazon S3 ストレージレンズの使用

Amazon S3 ストレージレンズは、オブジェクトストレージの使用状況とアクティビティを組織全体で可視化するために使用できるクラウドストレージの分析機能です。S3 ストレージレンズメトリクスを使用することで、組織全体でどれだけのストレージがあるか、または最も急速に成長しているバケットとプレフィックスは何かなどの、要約されたインサイトを生成できます。また、Amazon S3 ストレージレンズを使用することで、AWS Organizations の階層に属しているすべての AWS アカウントから、ストレージのメトリクスと使用状況に関するデータを収集できます。これを行うには、AWS Organizations を使用している必要があります。また、AWS Organizations 管理アカウントを使用して、S3 ストレージレンズに対し、信頼されたアクセスを有効にする必要があります。

信頼されたアクセスを有効にしてから、組織内のアカウントに対し、委任管理者の権限を追加します。委任管理者アカウントは、組織全体のストレージメトリクスとユーザーデータを収集する S3 ストレージレンズの設定とダッシュボードを作成するために使用されます。信頼されたアクセスの有効化の詳細については、AWS Organizations ユーザーガイドの「Amazon S3 ストレージレンズと AWS Organizations」を参照してください。

トピック

- S3 ストレージレンズのための信頼されたアクセスを有効にする
- S3 ストレージレンズのための信頼されたアクセスを無効にする
- S3 ストレージレンズでの委任管理者の登録
- S3ストレージレンズでの委任管理者の登録を解除する

S3 ストレージレンズのための信頼されたアクセスを有効にする

信頼されたアクセスが有効化された Amazon S3 ストレージレンズでは、AWS Organizations API オペレーションを通じて、AWS Organizations の階層、メンバーシップ、および構造にアクセスできるようになります。S3 ストレージレンズは、組織全体の構造で信頼されたサービスとして認識されます。

ダッシュボードの設定が作成されるたびに、組織の管理アカウントまたは委任管理者アカウントのために、サービスにリンクされたロールが S3 ストレージレンズにより作成されます。サービスにリンクされたロールにより、S3 ストレージレンズは次の操作を実行できます。

- 組織を説明する
- アカウントを一覧表示する
- 組織の AWS のサービスアクセスリストを検証する
- 組織の委任管理者を取得する

S3 ストレージレンズは、組織のアカウントのクロスアカウントメトリクスを収集するためのアクセスを確実に有しているようにできます。詳細については、「Amazon S3 ストレージレンズでのサービスにリンクされたロールの使用」を参照してください。

信頼されたアクセスを有効にしておくと、組織内のアカウントに対し、委任管理者権限を割り当てることができます。サービスに対する委任管理者としてマークされたアカウントには、組織内で、すべての読み取り専用 API オペレーションにアクセスするための承認が与えられます。このアクセス権により、委任管理者には組織のメンバーと構造に対する可視性が提供され、彼らも S3 ストレージレンズダッシュボードを作成できるようになります。

> **Note**
>
> - 信頼されたアクセスは、管理アカウントからのみ有効化できます。

- 組織に対し、S3 Storage Lens ダッシュボードまたは、その設定を作成できるのは、管理アカウントと委任された管理者のみです。

S3 コンソールの使用

S3 ストレージレンズに AWS Organizations での信頼されたアクセスが付与されるには

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 左側のナビゲーションペインで、[ストレージレンズ] に移動します。
3. [AWS Organizations 設定] を選択します。[ストレージレンズへの AWS Organizations アクセス] ページが表示されます。
4. [AWS Organizations 信頼されたアクセス] で、[編集] を選択します。

   [AWS Organizations アクセス] ページが表示されます。
5. [有効化] を選択して、S3 ストレージレンズダッシュボードの信頼されたアクセスを有効にします。
6. [Save changes] (変更の保存) をクリックします。

AWS CLI を使用する場合

Example

次の例は、AWS CLI で S3 ストレージレンズの AWS Organizations での信頼されたアクセスを有効にする方法を示しています。

```
aws organizations enable-aws-service-access --service-principal storage-
lens.s3.amazonaws.com
```

AWS SDK for Java の使用

Example – SDK for Java を使用して S3 ストレージレンズで AWS Organizations での信頼されたアクセスを有効にする

次の例は、SDK for Java で S3 ストレージレンズの信頼されたアクセスを有効にする方法を示しています。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.organizations.AWSOrganizations;
import com.amazonaws.services.organizations.AWSOrganizationsClient;
import com.amazonaws.services.organizations.model.EnableAWSServiceAccessRequest;

public class EnableOrganizationsTrustedAccess {
 private static final String S3_STORAGE_LENS_SERVICE_PRINCIPAL = "storage-
lens.s3.amazonaws.com";

 public static void main(String[] args) {
  try {
            AWSOrganizations organizationsClient = AWSOrganizationsClient.builder()
                .withCredentials(new ProfileCredentialsProvider())
                .withRegion(Regions.US_EAST_1)
                .build();

            organizationsClient.enableAWSServiceAccess(new
 EnableAWSServiceAccessRequest()
                .withServicePrincipal(S3_STORAGE_LENS_SERVICE_PRINCIPAL));
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but AWS Organizations couldn't
 process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // AWS Organizations couldn't be contacted for a response, or the client
            // couldn't parse the response from AWS Organizations.
            e.printStackTrace();
        }
 }
}
```

S3 ストレージレンズのための信頼されたアクセスを無効にする

委任された管理者としてのアカウントを削除するか、信頼されたアクセスを無効化すると、アカウント所有者の S3 ストレージレンズダッシュボードのメトリクスは、アカウントレベルでのみ機能するように制限されます。そのため、各アカウント保有者は、自身のアカウントの範囲に限定して S3 ストレージレンズが提供する機能にアクセスでき、組織全体へのアクセスはできなくなります。

S3 ストレージレンズで信頼されたアクセスを無効にすると、信頼されたアクセスを必要とするダッシュボードは更新されなくなります。作成された組織ダッシュボードも更新されなくなります。代わりに、S3 ストレージレンズダッシュボードの履歴データをクエリできるのは、データが引き続き利用可能である間のみです。

> **Note**
>
> - また、S3 ストレージレンズの信頼されたアクセスを無効にすると、すべての組織レベルのダッシュボードで、ストレージのメトリクスの収集と集計が自動的に停止されます。これは、S3 ストレージレンズが組織アカウントへの信頼されたアクセスを失ったためです。
> - 管理アカウントと委任管理者アカウントは、無効化されたダッシュボードの履歴データを引き続き表示することができます。また、この履歴データは、利用可能である間は引き続きクエリできます。

S3 コンソールの使用

S3 Storage Lens の信頼されたアクセスを無効にするには、

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 左側のナビゲーションペインで、[ストレージレンズ] に移動します。
3. [AWS Organizations 設定] を選択します。[ストレージレンズへの AWS Organizations アクセス] ページが表示されます。
4. [AWS Organizations 信頼されたアクセス] で、[編集] を選択します。

   [AWS Organizations アクセス] ページが表示されます。
5. [無効化] を選択して、S3 ストレージレンズダッシュボードの信頼されたアクセスを無効にします。
6. [Save changes] (変更の保存) をクリックします。

AWS CLI を使用する場合

Example

次の例では、AWS CLI を使用して S3 ストレージレンズの信頼されたアクセスを無効にします。

```
aws organizations disable-aws-service-access --service-principal storage-
lens.s3.amazonaws.com
```

AWS SDK for Java の使用

Example – S3 ストレージレンズの AWS Organizations での信頼されたアクセスを無効にします。

次の例は、SDK for Java で S3 ストレージレンズの AWS Organizations での信頼されたアクセスを無効にする方法を示しています。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.organizations.AWSOrganizations;
import com.amazonaws.services.organizations.AWSOrganizationsClient;
import com.amazonaws.services.organizations.model.DisableAWSServiceAccessRequest;

public class DisableOrganizationsTrustedAccess {
 private static final String S3_STORAGE_LENS_SERVICE_PRINCIPAL = "storage-
lens.s3.amazonaws.com";

 public static void main(String[] args) {
  try {
            AWSOrganizations organizationsClient = AWSOrganizationsClient.builder()
                .withCredentials(new ProfileCredentialsProvider())
                .withRegion(Regions.US_EAST_1)
                .build();

            // Make sure to remove any existing delegated administrator for S3 Storage
 Lens
            // before disabling access; otherwise, the request will fail.
            organizationsClient.disableAWSServiceAccess(new
 DisableAWSServiceAccessRequest()
                .withServicePrincipal(S3_STORAGE_LENS_SERVICE_PRINCIPAL));
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but AWS Organizations couldn't
 process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // AWS Organizations couldn't be contacted for a response, or the client
```

```
            // couldn't parse the response from AWS Organizations.
            e.printStackTrace();
        }
    }
}
```

S3 ストレージレンズでの委任管理者の登録

組織の管理アカウントまたは委任管理者アカウントからは、組織レベルのダッシュボードを作成できます。委任管理者アカウントでは、管理アカウントを除く他のアカウントに対し、組織レベルのダッシュボードの作成を許可できます。他のアカウントを組織の委任管理者として登録および登録解除できるのは、その組織の管理者アカウントのみです。

信頼されたアクセスを有効にすると、管理アカウントの AWS Organizations REST API、AWS CLI、または SDK を使用して、組織内のアカウントへの委任管理者アクセスを登録できます。(詳細については、AWS Organizations API リファレンスの「RegisterDelegatedAdministrator」を参照してください。) アカウントが委任された管理者として登録されると、そのアカウントがら AWS Organizations のすべての読み取り専用 API オペレーションにアクセスすることが承認されます。これにより、ユーザーに代わって S3 Storage Lens ダッシュボードを作成するための可視性が、組織のメンバーと構造に対し提供されます。

> **Note**
>
> AWS Organizations の REST API、AWS CLI、または SDK を使用して委任管理者を指定するには、その前に、EnableAWSOrganizationsAccess オペレーションを呼び出す必要があります。

S3 コンソールの使用

S3 Storage Lens のための委任された管理者を登録するには、

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 左側のナビゲーションペインで、[ストレージレンズ] に移動します。
3. [AWS Organizations 設定] を選択します。
4. [委任管理者] で、[アカウントを登録] を選択します。

5. アカウントを委任管理者として登録するための AWS アカウント ID を追加します。委任管理者は、組織内のすべてのアカウントとストレージのために組織レベルのダッシュボードを作成できます。
6. [アカウントを登録] を選択します。

AWS CLI を使用する場合

Example

次の例は、AWS CLI を使用して、S3 ストレージレンズで Organizations の委任管理者を登録する方法を示しています。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws organizations register-delegated-administrator --service-principal storage-
lens.s3.amazonaws.com --account-id 111122223333
```

AWS SDK for Java の使用

Example – S3 ストレージレンズで Organizations の委任された管理者を登録する

次の例は、SDK for Java で S3 ストレージレンズの AWS Organizations 委任管理者を登録する方法を示しています。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.organizations.AWSOrganizations;
import com.amazonaws.services.organizations.AWSOrganizationsClient;
import
 com.amazonaws.services.organizations.model.RegisterDelegatedAdministratorRequest;

public class RegisterOrganizationsDelegatedAdministrator {
 private static final String S3_STORAGE_LENS_SERVICE_PRINCIPAL = "storage-
lens.s3.amazonaws.com";

 public static void main(String[] args) {
  try {
            String delegatedAdminAccountId = "111122223333"; // Account Id for the
 delegated administrator.
```

```
            AWSOrganizations organizationsClient = AWSOrganizationsClient.builder()
                .withCredentials(new ProfileCredentialsProvider())
                .withRegion(Regions.US_EAST_1)
                .build();

            organizationsClient.registerDelegatedAdministrator(new
 RegisterDelegatedAdministratorRequest()
                .withAccountId(delegatedAdminAccountId)
                .withServicePrincipal(S3_STORAGE_LENS_SERVICE_PRINCIPAL));
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but AWS Organizations couldn't
 process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // AWS Organizations couldn't be contacted for a response, or the client
            // couldn't parse the response from AWS Organizations.
            e.printStackTrace();
        }
 }
}
```

S3ストレージレンズでの委任管理者の登録を解除する

信頼されたアクセスを有効にした後で、組織内のアカウントに対する委任管理者のアクセス権限を登録解除できます。委任管理者アカウントでは、管理アカウントを除く他のアカウントに対し、組織レベルのダッシュボードの作成を許可できます。組織の管理アカウントのみが、その組織内の委任管理者のアカウントの登録を解除できます。

また、管理アカウントから AWS Organizations AWS Management Console、REST API、AWS CLI、または AWS SDK を使用することで、委任管理者の登録を解除できます。詳細については、AWS Organizations API リファレンスの「DeregisterDelegatedAdministrator」を参照してください。

アカウントが委任管理者として登録解除されると、アカウントは次のものにアクセスできなくなります。

- 組織のメンバーと構造を可視化するすべての読み取り専用 AWS Organizations API オペレーション。

- 委任管理者が作成したすべての組織レベルのダッシュボード。また、委任管理者の登録を解除すると、委任管理者によって作成されたすべての組織レベルのダッシュボードで、ストレージのメトリクスの新たな集計が自動的に停止されます。

> **Note**
>
> 登録解除された委任管理者は、データがクエリに利用できる間は、作成したものの無効化されたダッシュボードの履歴データを引き続き見ることができます。

S3 コンソールの使用

S3 ストレージレンズの委任管理者を登録解除するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左側のナビゲーションペインで、[ストレージレンズ] に移動します。
3. [AWS Organizations 設定] を選択します。
4. [委任管理者] で、登録解除するアカウントを選択します。
5. [アカウントの登録解除] を選択します。登録解除されたアカウントは委任管理者ではなくなり、組織内のすべてのアカウントとストレージに対して組織レベルのダッシュボードを作成できなくなります。
6. [アカウントを登録] を選択します。

AWS CLI を使用する場合

Example

次の例は、AWS CLI を使用して S3 ストレージレンズで Organizations の委任管理者を登録解除する方法を示しています。この例を実行するには、*111122223333* をユーザー自身の AWS アカウント ID に置き換えます。

```
aws organizations deregister-delegated-administrator --service-principal storage-lens.s3.amazonaws.com --account-id 111122223333
```

AWS SDK for Java の使用

Example – S3 ストレージレンズで Organizations の委任管理者の登録を解除する

次の例は、SDK for Java を使用して S3 ストレージレンズで Organizations 委任管理者を登録解除する方法を示しています。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.organizations.AWSOrganizations;
import com.amazonaws.services.organizations.AWSOrganizationsClient;
import
 com.amazonaws.services.organizations.model.DeregisterDelegatedAdministratorRequest;

public class DeregisterOrganizationsDelegatedAdministrator {
 private static final String S3_STORAGE_LENS_SERVICE_PRINCIPAL = "storage-
lens.s3.amazonaws.com";

 public static void main(String[] args) {
  try {
            String delegatedAdminAccountId = "111122223333"; // Account Id for the
 delegated administrator.
            AWSOrganizations organizationsClient = AWSOrganizationsClient.builder()
                .withCredentials(new ProfileCredentialsProvider())
                .withRegion(Regions.US_EAST_1)
                .build();

            organizationsClient.deregisterDelegatedAdministrator(new
 DeregisterDelegatedAdministratorRequest()
                .withAccountId(delegatedAdminAccountId)
                .withServicePrincipal(S3_STORAGE_LENS_SERVICE_PRINCIPAL));
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but AWS Organizations couldn't
 process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // AWS Organizations couldn't be contacted for a response, or the client
            // couldn't parse the response from AWS Organizations.
            e.printStackTrace();
```

```
        }
  }
}
```

S3 ストレージレンズグループを使用したメトリクスのフィルタリングと集計

Amazon S3 ストレージレンズグループは、オブジェクトメタデータに基づくカスタムフィルタを使用してメトリクスを集約します。Storage Lens グループを使用すると、経過時間別のオブジェクトの分布や最も一般的なファイルタイプなど、データの特性を掘り下げて調べることができます。例えば、メトリクスをオブジェクトタグでフィルタリングして急速に増加しているデータセットを特定したり、オブジェクトのサイズと経過時間に基づいてストレージを視覚化してストレージアーカイブ戦略に役立てたりすることができます。結果として、Amazon S3 ストレージレンズグループは、S3 ストレージの理解と最適化に役立ちます。

Storage Lens グループを使用すると、プレフィックス、サフィックス、オブジェクトタグ、オブジェクトサイズ、オブジェクト経過時間などのオブジェクトメタデータを使用して S3 Storage Lens メトリクスを分析およびフィルタリングできます。また、これらのフィルタを組み合わせて適用できます。Storage Lens グループを S3 Storage Lens ダッシュボードにアタッチすると、Amazon S3 ストレージレンズグループによって集約された S3 Storage Lens メトリクスをダッシュボードで直接表示できます。

例えば、オブジェクトサイズや経過時間層でメトリクスをフィルタリングして、ストレージのどの部分が小さなオブジェクトで構成されているかを判断することもできます。その後、この情報を S3 Intelligent-Tiering や S3 Lifecycle で使用して、小さなオブジェクトをさまざまなストレージクラスに移行することで、コストとストレージの最適化を図ることができます。

トピック

- S3 Storage Lens グループの仕組み
- Storage Lens グループの使用

S3 Storage Lens グループの仕組み

Storage Lens グループを使用すると、オブジェクトメタデータに基づくカスタムフィルタを使用してメトリクスを集約できます。カスタムフィルタを定義する場合、プレフィックス、サフィックス、オブジェクトタグ、オブジェクトサイズ、オブジェクト経過時間、またはこれらのカスタムフィルタの組み合わせを使用できます。Storage Lens グループの作成時には、1 つのフィルタまたは複数の

フィルタ条件を含めることもできます。複数のフィルタ条件を指定するには、And または Or 論理演算子を使用します。

Storage Lens グループを作成して設定すると、Storage Lens グループ自体が、グループを関連付けるダッシュボードのカスタムフィルタとして機能します。その後、ダッシュボードで Storage Lens グループフィルタを使用して、グループで定義したカスタムフィルタに基づくストレージメトリクスを取得できます。

S3 Storage Lens ダッシュボードで Storage Lens グループのデータを表示するには、グループを作成した後でグループをダッシュボードにアタッチする必要があります。Storage Lens グループを Storage Lens ダッシュボードにアタッチすると、ダッシュボードは 48 時間以内にストレージ使用状況のメトリクスを収集します。その後、このデータを Storage Lens ダッシュボードで視覚化するか、メトリクスのエクスポートを使用して エクスポートできます。Storage Lens グループをダッシュボードにアタッチし忘れると、Storage Lens グループのデータがキャプチャされず、どこにも表示されなくなります。

> **Note**
>
> - S3 Storage Lens グループを作成すると、AWS リソースが作成されます。したがって、各 Storage Lens グループには独自の Amazon リソースネーム (ARN) があり、S3 Storage Lens ダッシュボードにアタッチしたり、S3 Storage Lens ダッシュボードから除外したりするときに指定できます。
> - Storage Lens グループがダッシュボードに関連付けられていない場合、Storage Lens グループの作成に追加料金は発生しません。
> - S3 Storage Lens は、一致するすべての Storage Lens グループのオブジェクトの使用状況メトリクスを集約します。そのため、オブジェクトが 2 つ以上の Storage Lens グループのフィルタ条件に一致すると、ストレージ使用状況全体で同じオブジェクトの数が繰り返し表示されます。

指定したホームリージョン (サポート対象 AWS リージョン のリストから) のアカウントレベルで Storage Lens グループを作成できます。これで、ダッシュボードが同じ AWS アカウント とホームリージョンにある限り、Storage Lens グループを複数の Storage Lens ダッシュボードに接続できます。それぞれの AWS アカウント でホームリージョンごとに最大 50 の Storage Lens グループを作成できます。

AmazonS3 コンソール、AWS Command Line Interface、(AWS CLI)、AWS SDK、または Amazon S3 REST API を使用して S3 Storage Lens グループを作成および管理できます。

トピック

- Storage Lens グループ集約メトリクスの表示
- Storage Lens グループのアクセス許可。
- Storage Lens グループの設定
- AWS リソースタグ
- Storage Lens グループメトリクスのエクスポート

Storage Lens グループ集約メトリクスの表示

グループをダッシュボードにアタッチすることにより、Storage Lens グループの集約されたメトリクスを表示できます。アタッチする Storage Lens グループは、ダッシュボードアカウントの指定されたホームリージョン内に存在している必要があります。

Storage Lens グループをダッシュボードにアタッチするには、ダッシュボード設定の Storage Lens グループ集約セクションでグループを指定する必要があります。複数の Storage Lens グループがある場合、Storage Lens グループ集約結果をフィルタして、目的のグループを含めたり除外したりできます。グループをダッシュボードに関連付ける方法の詳細については、「the section called “Storage Lens グループをアタッチまたは削除する。”」を参照してください。

グループをアタッチした後、48 時間以内にダッシュボードに追加の Storage Lens グループ集約データが表示されます。

> **Note**
>
> Storage Lens グループ集約メトリクスを表示するには、そのグループを S3 Storage Lens ダッシュボードにアタッチする必要があります。

Storage Lens グループのアクセス許可。

Storage Lens グループでは、S3 Storage Lens のアクションへのアクセスを許可するために、AWS Identity and Access Management (IAM) で特定のアクセス許可が必要となります。これらのアクセス許可を付与するには、アイデンティティベースの IAM ポリシーを使用できます。このポリシーを、IAM ユーザー、グループ、またはロールにアタッチして、アクセス許可を付与することができます。このようなアクセス許可には、Storage Lens グループの作成や削除、設定の表示、タグの管理などが含まれます。

アクセス許可を付与する IAM ユーザーまたはロールは、Storage Lens グループを作成または所有するアカウントに属している必要があります。

Storage Lens グループを使用し、Storage Lens グループのメトリクスを表示するには、まず S3 Storage Lens を使用するための適切なアクセス許可が必要です。詳細については、「the section called “ 許可の設定”」を参照してください。

S3 Storage Lens グループを作成して管理するには、実行するアクションに応じて次の IAM アクセス許可が必要です。

アクション	IAM 許可
新しい Storage Lens グループを作成する	`s3:CreateStorageLensGroup`
タグ付きの新しい Storage Lens グループを作成する	`s3:CreateStorageLensGroup` , `s3:TagResource`
既存の Storage Lens グループを更新する	`s3:UpdateStorageLensGroup`
Storage Lens グループ設定の詳細を返す	`s3:GetStorageLensGroup`
ホームリージョンのすべての Storage Lens グループを一覧表示する	`s3:ListStorageLensGroups`
Storage Lens グループを削除する。	`s3:DeleteStorageLensGroup`
Storage Lens グループに追加されたタグを一覧表示する	`s3:ListTagsForResource`
既存の Storage Lens グループの Storage Lens グループタグを追加または更新する	`s3:TagResource`
Storage Lens グループからタグを削除する	`s3:UntagResource`

Storage Lens グループを作成するアカウントで IAM ポリシーを設定する方法の例を次に示します。このポリシーを使用するには、*`us-east-1`* を Storage Lens グループがあるホームリージョンに置き換えてください。*`111122223333`* を自分の ID と置き換え、AWS アカウント を Storage Lens グループの名前と置き換えます。これらのアクセス許可をすべての Storage Lens グループに適用するには、*`example-storage-lens-group`* を *`*`* と置き換えてください。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EXAMPLE-Statement-ID",
            "Effect": "Allow",
            "Action": [
                "s3:CreateStorageLensGroup",
                "s3:UpdateStorageLensGroup",
                "s3:GetStorageLensGroup",
                "s3:ListStorageLensGroups",
                "s3:DeleteStorageLensGroup,
                "s3:TagResource",
                "s3:UntagResource",
                "s3:ListTagsForResource"
                ],
            "Resource": "arn:aws:s3:us-east-1:111122223333:storage-lens-group/example-storage-lens-group"
        }
    ]
}
```

S3 Storage Lens アクセス許可の詳細については、「Amazon S3 ストレージレンズアクセス許可の設定」を参照してください。IAM ポリシー言語については、「Amazon S3 のポリシーとアクセス許可」を参照してください。

Storage Lens グループの設定

S3 Storage Lens グループ名

ダッシュボードにアタッチするグループを簡単に判断できるように、Storage Lens グループには用途を示す名前を付けることをお勧めします。Storage Lens グループをダッシュボードにアタッチするには、ダッシュボード設定の [Storage Lens グループ集約] セクションでグループを指定する必要があります。

Storage Lens グループ名はアカウント内で一意である必要があります。名前は、64 文字以下にし、使用できるのは、文字 (a ~ z、A ~ Z)、数字 (0-9)、ハイフン (-)、およびアンダースコア (_) のみです。

ホームリージョン

ホームリージョンは、Storage Lens グループを作成および管理する AWS リージョン です。Storage Lens グループは、Amazon S3 ストレージレンズダッシュボードと同じホームリージョンに作成されます。Storage Lens グループの設定とメトリクスもこのリージョンに保存されます。ホームリージョンごとに最大 50 の Storage Lens グループを作成できます。

Storage Lens グループを作成した後は、ホームリージョンを編集できません。

スコープ

Storage Lens グループにオブジェクトを含めるには、そのオブジェクトが Amazon S3 ストレージレンズダッシュボードの範囲内にある必要があります。Storage Lens ダッシュボードの範囲は、S3 Storage Lens ダッシュボード設定のダッシュボードスコープに含めたバケットによって決まります。

オブジェクトにさまざまなフィルタを使用して Storage Lens グループの範囲を定義できます。S3 Storage Lens ダッシュボードでこれらの Storage Lens グループのメトリクスを表示するには、オブジェクトが Storage Lens グループに追加したフィルタと一致している必要があります。例えば、Storage Lens グループにプレフィックス `marketing` とサフィックス `.png` が付いたオブジェクトが含まれているが、それらの条件に一致するオブジェクトがないとします。この場合、この Storage Lens グループのメトリクスは毎日のメトリクスのエクスポートでは生成されず、このグループのメトリクスはダッシュボードに表示されません。

フィルタ

S3 Storage Lens グループでは以下のフィルタを使用できます。

- プレフィックス — 含まれるオブジェクトのプレフィックスを指定します。これはオブジェクトキー名の先頭にある文字列です。例えば、[プレフィックス] フィルタの値 `images` には、`images/`、`images-marketing`、`images/production` のいずれかのプレフィックスを持つオブジェクトが含まれます。プレフィックスの最大長は、1,024 バイトです。
- サフィックス — 含まれるオブジェクトのサフィックスを指定します (`.png`、`.jpeg`、`.csv` など)。プレフィックスの最大長は、1,024 バイトです。
- オブジェクトタグ — フィルタの対象となるオブジェクトタグのリストを指定します。タグキーは 128 Unicode 文字、タグ値は 256 Unicode 文字を超過してはいけません。オブジェクトタグ値フィールドを空のままにした場合、S3 Storage Lens グループは、空のタグ値も持つ他のオブジェクトとオブジェクトのみを一致させることに注意してください。

- 経過時間 — 含まれるオブジェクトのオブジェクト経過時間範囲を日数で指定します。整数のみがサポートされます。
- サイズ — 含まれるオブジェクトのオブジェクトサイズをバイト単位で指定します。整数のみがサポートされます。許容される最大値は 5 TB です。

Storage Lens グループのオブジェクトタグ

最大 10 個のオブジェクトタグフィルタを含む Storage Lens グループを作成できます。次の例には、*Marketing-Department* という名前の Storage Lens グループのフィルタとして 2 つのオブジェクトタグのキーと値のペアが含まれています。この例を使用するには、*Marketing-Department* をグループの名前に置き換え、*object-tag-key-1*、*object-tag-value-1* をフィルタリングするオブジェクトタグのキーと値のペアに置き換えます。

```
{
    "Name": "Marketing-Department",
    "Filter": {
     "MatchAnyTag":[
                {
                    "Key": "object-tag-key-1",
                    "Value": "object-tag-value-1"
                },
                {
                    "Key": "object-tag-key-2",
                    "Value": "object-tag-value-2"
                }
            ]
    }
}
```

論理演算子 (**Or** または **And**)

Storage Lens グループに複数のフィルタ条件を含めるには、論理演算子 (And または Or) を使用できます。次の例では、*Marketing-Department* という名前の Storage Lens グループに Prefix、ObjectAge、ObjectSize フィルタを含む And 演算子があります。And 演算子が使用されるため、これらのフィルタ条件をすべて満たすオブジェクトのみが Storage Lens グループのスコープに含まれます。

この例を使用するには、*user input placeholders* をフィルタする値に置き換えます。

```
{
```

```
    "Name": "Marketing-Department",
    "Filter": {
        "And": {
            "MatchAnyPrefix": [
                "prefix-1",
                "prefix-2",
                "prefix-3/sub-prefix-1"
            ],
             "MatchObjectAge": {
                "DaysGreaterThan": 10,
                "DaysLessThan": 60
            },
            "MatchObjectSize": {
                "BytesGreaterThan": 10,
                "BytesLessThan": 60
            }
        }
    }
}
```

> **Note**
>
> フィルタの条件のいずれかに一致するオブジェクトを含める場合は、この例では And 論理演算子を Or 論理演算子に置き換えてください。

AWS リソースタグ

S3 ストレージレンズグループはそれぞれ独自の Amazon AWS リソースネーム (ARN) を持つリソースとみなされます。そのため、Storage Lens グループを設定するときに、AWS オプションでグループにリソースタグを追加できます。Storage Lens グループごとに最大 50 個のタグを追加できます。タグ付きの Storage Lens グループを作成するには、`s3:CreateStorageLensGroup` と `s3:TagResource` の権限が必要です。

AWS リソースタグを使用して、部門、事業内容、またはプロジェクトごとにリソースを分類できます。そうすることで、同じ種類のリソースが多い場合に役立ちます。タグを適用すると、割り当てたタグに基づいて特定の Storage Lens グループをすばやく識別できます。また、コストの追跡と割り当てにもタグを使用できます。

さらに、Storage Lens グループに AWS リソースタグを追加すると、属性ベースのアクセス制御 (ABAC) が有効になります。ABAC は、このケースタグの属性に基づいて権限を定義する認可戦略で

す。IAM ポリシーでリソースタグを指定する条件を使用して、AWS リソースへのアクセスを制御できます。

タグのキーと値は編集でき、タグはリソースからいつでも削除できます。また、次の点について注意してください:

- キーとタグの値は大文字と小文字が区別されます。
- 特定のリソースについて既存のタグと同じキーを持つタグを追加した場合、以前の値は新しい値によって上書きされます。
- リソースを削除すると、リソースのタグも削除されます。
- AWS リソースタグにはプライベートデータや機密データを含めないでください。
- システムタグ (または `aws:` で始まるタグキーを持つタグ) はサポートされていません。
- 各タグキーの長さは 128 文字以下にする必要があります。各タグ値の長さは 256 文字以下にする必要があります。

Storage Lens グループメトリクスのエクスポート

S3 Storage Lens グループメトリクスは、Storage Lens グループがアタッチされているダッシュボードの Amazon S3 ストレージレンズメトリクスエクスポートに含まれています。Storage Lens メトリクスのエクスポート機能に関する一般的な情報については、「データエクスポートで Amazon S3 Storage Lens のメトリクスを確認する」を参照してください。

Storage Lens グループのメトリクスエクスポートには、Storage Lens グループをアタッチしたダッシュボードの範囲内にあるすべての S3 Storage Lens メトリクスが含まれます。エクスポートには、Storage Lens グループの追加メトリクスデータも含まれます。

Storage Lens グループを作成すると、そのグループの所属するダッシュボードのメトリクスエクスポートを設定したときに選択したバケットに、メトリクスのエクスポートが毎日送信されます。最初のエクスポートを受信するに最大 48 時間かかることがあります。

日次エクスポートでメトリクスを生成するには、オブジェクトが Storage Lens グループに含めたフィルタと一致する必要があります。Storage Lens グループに含められたフィルタに一致するオブジェクトがない場合、メトリクスは生成されません。ただし、オブジェクトが 2 つ以上の Storage Lens グループと一致する場合、そのオブジェクトはメトリクスのエクスポートに表示される際、グループごとに別々に表示されます。

Storage Lens グループのメトリクスは、ダッシュボードのメトリクスエクスポートの `record_type` 列で以下のいずれかの値を探すことにより特定できます。

- STORAGE_LENS_GROUP_BUCKET
- STORAGE_LENS_GROUP_ACCOUNT

record_value 列には、Storage Lens グループのリソース ARN が表示されます (例: arn:aws:s3:*us-east-1*:*111122223333*:storage-lens-group/*Marketing-Department*)。

Storage Lens グループの使用

Amazon S3 ストレージレンズグループは、オブジェクトメタデータに基づくカスタムフィルタを使用してメトリクスを集約します。プレフィックス、サフィックス、オブジェクトタグ、オブジェクトサイズ、オブジェクト経過時間使用して S3 Storage Lens メトリクスを分析およびフィルタリングできます。Amazon S3 ストレージレンズのグループを使用して、Amazon S3 バケット間での使用状況を分類することもできます。その結果、S3 ストレージの理解を深め最適化できるようになります。

Storage Lens グループのデータの視覚化を開始するには、まず Storage Lens グループを S3 Storage Lens ダッシュボードにアタッチする必要があります。Storage Lens グループをダッシュボードで管理する必要がある場合は、ダッシュボードの設定を編集できます。アカウントにどの Storage Lens グループがあるかを確認するには、それらのグループを一覧表示できます。どの Storage Lens グループがダッシュボードにアタッチされているかを確認するには、ダッシュボードの [Storage Lens グループ] タブを随時確認できます。既存の Storage Lens グループのスコープを確認または更新するには、その詳細を表示できます。Storage Lens グループを完全に削除することもできます。

権限を管理するために、ユーザー定義の AWS リソースタグを作成して Storage Lens グループに追加できます。AWS リソースタグを使用して、部門、事業内容、またはプロジェクトごとにリソースを分類できます。そうすることで、同じ種類のリソースが多い場合に役立ちます。タグを適用すると、割り当てたタグに基づいて特定の Storage Lens グループをすばやく識別できます。

さらに、Storage Lens グループに AWS リソースタグを追加すると、属性ベースのアクセス制御 (ABAC) が有効になります。ABAC は、このケースタグの属性に基づいて権限を定義する認可戦略です。IAM ポリシーでリソースタグを指定する条件を使用して、AWS リソースへのアクセスを制御できます。

トピック

- Storage Lens グループの作成
- S3 Storage Lens グループをダッシュボードにアタッチまたは削除する、またはダッシュボードから S3 Storage Lens グループを削除する

- Storage Lens グループのデータの視覚化
- Storage Lens グループの更新
- Storage Lens グループによる AWS リソースタグの管理
- すべての Storage Lens グループの一覧表示
- Storage Lens グループ詳細の表示
- Storage Lens グループの削除

Storage Lens グループの作成

以下の例は、Amazon S3 コンソール AWS Command Line Interface (AWS CLI)、および AWS SDK for Java を使用して Amazon S3 ストレージレンズグループを作成する方法を示しています。

S3 コンソールの使用

Storage Lens グループを作成するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ページ上部にあるナビゲーションバーで、現在表示されている AWS リージョンの名前をクリックします。次に、切り替え先のリージョンを選択します。
3. ナビゲーションペインで、[Storage Lens グループ]を選択します。
4. [Storage Lens グループの作成] を選択します。
5. [全般] で、現在の [ホームリージョン] を表示して、[ストレージレンズグループ名] を入力します。
6. [スコープ] で、Storage Lens グループに適用するためのフィルタを選択します。複数のフィルタを適用するには、フィルタを選択し、AND または OR 論理演算子を選択します。

   - [プレフィックス] フィルタでは、[プレフィックス] を選択し、プレフィックス文字列を入力します。複数のプレフィックスを追加するには、[プレフィックスを追加] を選択します。プレフィックスを削除するには、削除するボリュームの横にある [削除] を選択します。
   - [オブジェクトタグ] フィルタでは、[オブジェクトタグ] を選択し、オブジェクトのキーと値のペアを入力します。次に、[タグを追加] を選択します。タグを削除するには、削除したいタグの横にある[削除] を選択します。
   - [サフィックス] フィルタでは、[サフィックス] を選択し、サフィックス文字列を入力します。複数のサフィックスを追加するには、[サフィックスを追加] を選択します。サフィックスを削除するには、削除したいサフィックスの横にある[削除] を選択します。

- [経過時間] フィルタでは、オブジェクトの有効期間を日単位で指定します。[オブジェクトの最短経過時間を指定] を選択し、オブジェクトの最低経過時間を入力します。次に、[オブジェクトの最長経過時間を指定] を選択し、オブジェクトの最長経過時間を入力します。
- [サイズ] フィルタで、オブジェクトサイズの範囲と測定単位を指定します。[最小オブジェクトサイズを指定] を選択し、オブジェクトの最小オブジェクトサイズを入力します。[最大オブジェクトサイズを指定] を選択し、オブジェクトの最大オブジェクトサイズを入力します。

7. (オプション) AWS リソースタグには、キーと値のペアを追加し、[タグを追加] を選択します。
8. [Storage Lens グループの作成] を選択します。

AWS CLI を使用する場合

次の AWS CLI コマンド例は、Storage Lens グループを作成します。このコマンド例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3control create-storage-lens-group --account-id 111122223333 \
--region us-east-1 --storage-lens-group=file://./marketing-department.json
```

次の AWS CLI コマンド例は、2 つの AWS リソースタグを持つ Storage Lens グループを作成します。このコマンド例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3control create-storage-lens-group --account-id 111122223333 \
--region us-east-1 --storage-lens-group=file://./marketing-department.json \
--tags Key=k1,Value=v1 Key=k2,Value=v2
```

JSON 設定例については、「Storage Lens グループの設定」を参照してください。

AWS SDK for Java の使用

次の AWS SDK for Java 例は、Storage Lens グループを作成します。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

Example — 1 つのフィルタで Storage Lens グループを作成します。

次の例は、*Marketing-Department* という Storage Lens グループを作成します。このグループには、経過時間範囲を *30* ~ *90* 日で指定するオブジェクト経過時間フィルタがあります。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
package aws.example.s3control;
```

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.CreateStorageLensGroupRequest;
import software.amazon.awssdk.services.s3control.model.MatchObjectAge;
import software.amazon.awssdk.services.s3control.model.StorageLensGroup;
import software.amazon.awssdk.services.s3control.model.StorageLensGroupFilter;

public class CreateStorageLensGroupWithObjectAge {
    public static void main(String[] args) {
        String storageLensGroupName = "Marketing-Department";
        String accountId = "111122223333";

        try {
            StorageLensGroupFilter objectAgeFilter = StorageLensGroupFilter.builder()
                    .matchObjectAge(MatchObjectAge.builder()
                            .daysGreaterThan(30)
                            .daysLessThan(90)
                            .build())
                    .build();

            StorageLensGroup storageLensGroup = StorageLensGroup.builder()
                    .name(storageLensGroupName)
                    .filter(objectAgeFilter)
                    .build();

            CreateStorageLensGroupRequest createStorageLensGroupRequest =
 CreateStorageLensGroupRequest.builder()
                    .storageLensGroup(storageLensGroup)
                    .accountId(accountId).build();

            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            s3ControlClient.createStorageLensGroup(createStorageLensGroupRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
```

```
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Example — 複数のフィルタを含む **AND** 演算子を使用して Storage Lens グループを作成します。

次の例は、*Marketing-Department* という Storage Lens グループを作成します。このグループ AND は演算子を使用して、オブジェクトがすべてのフィルタ条件に一致する必要があることを示します。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.CreateStorageLensGroupRequest;
import software.amazon.awssdk.services.s3control.model.MatchObjectAge;
import software.amazon.awssdk.services.s3control.model.MatchObjectSize;
import software.amazon.awssdk.services.s3control.model.S3Tag;
import software.amazon.awssdk.services.s3control.model.StorageLensGroup;
import software.amazon.awssdk.services.s3control.model.StorageLensGroupAndOperator;
import software.amazon.awssdk.services.s3control.model.StorageLensGroupFilter;


public class CreateStorageLensGroupWithAndFilter {
    public static void main(String[] args) {
        String storageLensGroupName = "Marketing-Department";
        String accountId = "111122223333";

        try {
            // Create object tags.
            S3Tag tag1 = S3Tag.builder()
                    .key("object-tag-key-1")
                    .value("object-tag-value-1")
                    .build();
            S3Tag tag2 = S3Tag.builder()
                    .key("object-tag-key-2")
```

```
                    .value("object-tag-value-2")
                    .build();

            StorageLensGroupAndOperator andOperator =
StorageLensGroupAndOperator.builder()
                    .matchAnyPrefix("prefix-1", "prefix-2", "prefix-3/sub-prefix-1")
                    .matchAnySuffix(".png", ".gif", ".jpg")
                    .matchAnyTag(tag1, tag2)
                    .matchObjectAge(MatchObjectAge.builder()
                            .daysGreaterThan(30)
                            .daysLessThan(90).build())
                    .matchObjectSize(MatchObjectSize.builder()
                            .bytesGreaterThan(1000L)
                            .bytesLessThan(6000L).build())
                    .build();

            StorageLensGroupFilter andFilter = StorageLensGroupFilter.builder()
                    .and(andOperator)
                    .build();

            StorageLensGroup storageLensGroup = StorageLensGroup.builder()
                    .name(storageLensGroupName)
                    .filter(andFilter)
                    .build();

            CreateStorageLensGroupRequest createStorageLensGroupRequest =
CreateStorageLensGroupRequest.builder()
                    .storageLensGroup(storageLensGroup)
                    .accountId(accountId).build();

            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            s3ControlClient.createStorageLensGroup(createStorageLensGroupRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
```

```
    }
}
```

Example — 複数のフィルタを含む **OR** 演算子を使用して Storage Lens グループを作成します。

次の例は、*Marketing-Department* という Storage Lens グループを作成します。このグループは、OR 演算子を使用してプレフィックスフィルタ (*prefix-1*、*prefix-2*、*prefix3/sub-prefix-1*) または *1000* ~ *6000* バイトまでのサイズ範囲を持つオブジェクトサイズフィルタを適用します。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.CreateStorageLensGroupRequest;
import software.amazon.awssdk.services.s3control.model.MatchObjectSize;
import software.amazon.awssdk.services.s3control.model.StorageLensGroup;
import software.amazon.awssdk.services.s3control.model.StorageLensGroupFilter;
import software.amazon.awssdk.services.s3control.model.StorageLensGroupOrOperator;

public class CreateStorageLensGroupWithOrFilter {
    public static void main(String[] args) {
        String storageLensGroupName = "Marketing-Department";
        String accountId = "111122223333";

        try {
            StorageLensGroupOrOperator orOperator =
 StorageLensGroupOrOperator.builder()
                    .matchAnyPrefix("prefix-1", "prefix-2", "prefix-3/sub-prefix-1")
                    .matchObjectSize(MatchObjectSize.builder()
                            .bytesGreaterThan(1000L)
                            .bytesLessThan(6000L)
                            .build())
                    .build();

            StorageLensGroupFilter orFilter = StorageLensGroupFilter.builder()
                    .or(orOperator)
                    .build();
```

```
            StorageLensGroup storageLensGroup = StorageLensGroup.builder()
                    .name(storageLensGroupName)
                    .filter(orFilter)
                    .build();

            CreateStorageLensGroupRequest createStorageLensGroupRequest =
 CreateStorageLensGroupRequest.builder()
                    .storageLensGroup(storageLensGroup)
                    .accountId(accountId).build();

            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            s3ControlClient.createStorageLensGroup(createStorageLensGroupRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Example — 1 つのフィルタと 2 つの AWS リソースタグを持つ Storage Lens グループを作成します。

次の例は、サフィックスフィルタを持つ *Marketing-Department* という Storage Lens グループを作成します。この例では、Storage Lens グループに 2 AWS つのリソースタグも追加しています。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.CreateStorageLensGroupRequest;
import software.amazon.awssdk.services.s3control.model.StorageLensGroup;
```

```
import software.amazon.awssdk.services.s3control.model.StorageLensGroupFilter;
import software.amazon.awssdk.services.s3control.model.Tag;

public class CreateStorageLensGroupWithResourceTags {
    public static void main(String[] args) {
        String storageLensGroupName = "Marketing-Department";
        String accountId = "111122223333";

        try {
            // Create AWS resource tags.
            Tag resourceTag1 = Tag.builder()
                    .key("resource-tag-key-1")
                    .value("resource-tag-value-1")
                    .build();
            Tag resourceTag2 = Tag.builder()
                    .key("resource-tag-key-2")
                    .value("resource-tag-value-2")
                    .build();

            StorageLensGroupFilter suffixFilter = StorageLensGroupFilter.builder()
                    .matchAnySuffix(".png", ".gif", ".jpg")
                    .build();

            StorageLensGroup storageLensGroup = StorageLensGroup.builder()
                    .name(storageLensGroupName)
                    .filter(suffixFilter)
                    .build();

            CreateStorageLensGroupRequest createStorageLensGroupRequest =
 CreateStorageLensGroupRequest.builder()
                    .storageLensGroup(storageLensGroup)
                    .tags(resourceTag1, resourceTag2)
                    .accountId(accountId).build();

            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            s3ControlClient.createStorageLensGroup(createStorageLensGroupRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
```

```
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

JSON 設定例については、「Storage Lens グループの設定」を参照してください。

S3 Storage Lens グループをダッシュボードにアタッチまたは削除する、またはダッシュボードから S3 Storage Lens グループを削除する

Amazon S3 ストレージレンズの高度なティアにアップグレードしたら、Storage Lens グループをダッシュボードにアタッチできます。複数の Storage Lens グループがある場合、目的のグループを含めたり除外したりできます。

Storage Lens グループは、ダッシュボードアカウントの指定されたホームリージョン内に存在している必要があります。Storage Lens グループをダッシュボードに接続すると、48 時間以内にメトリクスのエクスポートで追加の Storage Lens グループの集約データを受け取ります。

> **Note**
>
> Storage Lens グループの集約メトリクスを表示するには、そのデータを Storage Lens ダッシュボードにアタッチする必要があります。Storage Lens グループの JSON 設定ファイルの例については、「JSON の Storage Lens グループを使用した S3 Storage Lens の設定例」を参照してください。

S3 コンソールの使用

Storage Lens グループを Storage Lens ダッシュボードにアタッチするには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左ナビゲーションペインの、[S3 Storage Lens] で、[ダッシュボード] を選択します。
3. Storage Lens グループをアタッチする Storage Lens ダッシュボードのオプションボタンを選択します。
4. [編集] を選択します。

5. メトリクスの選択で [Advanced metrics and recommendations] (アドバンストメトリクスとレコメンデーション) を選択します。
6. [Storage Lens グループ集約] を選択します。

> **Note**
>
> デフォルトでは、[高度なメトリクス] も選択されています。ただし、Storage Lens グループのデータを集約する必要がないため、この設定の選択を解除することもできます。

7. [Storage Lens グループ集約] までスクロールし、データ集約に含める、または除外する 1 つまたは複数の Storage Lens グループを指定します。次のフィルタリングオプションを設定できます。
   - 特定の Storage Lens グループを含める場合は、[Storage Lens グループを含める] を選択します。[含めるStorage Lens グループ] で、Storage Lens グループを選択します。
   - すべての Storage Lens グループを含める場合は、[ホームリージョンのすべてのStorage Lens グループをこのアカウントに含める] を選択します。
   - 特定の Storage Lens グループを除外する場合は、[Storage Lens グループを除外する] を選択します。[除外する Storage Lens グループ] で、除外する Storage Lens グループを選択します。
8. [Save changes] (変更の保存) をクリックします。Storage Lens グループを正しく設定していれば、48 時間以内にダッシュボードに追加の Storage Lens グループ集約データが表示されます。

S3 Storage Lens ダッシュボードから Storage Lens グループを削除するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ナビゲーションペインの、[S3 Storage Lens] で、[ダッシュボード] を選択します。
3. Storage Lens グループを削除する Storage Lens ダッシュボードのオプションボタンを選択します。
4. [ダッシュボード設定を表示] を選択します。
5. [編集] を選択します。
6. [メトリクスの選択] セクションまで下にスクロールします。

7. [Storage Lens グループ集約] で、削除する Storage Lens グループの横にある [X] を選択します。これにより、Storage Lens グループが削除されます。

   すべての Storage Lens グループをダッシュボードに含めた場合は、[このアカウントにホームリージョンのすべての Storage Lens グループを含める] の横にあるチェックボックスをオフにします。

8. [Save changes] (変更の保存) をクリックします。

> **Note**
>
> ダッシュボードに設定の更新が反映されるまでに最大 48 時間かかることがあります。

AWS SDK for Java の使用

Example – すべての ストレージレンズグループをダッシュボードにアタッチする

次の SDK for Java の例では、アカウント *111122223333* のすべての Storage Lens グループを *DashboardConfigurationId* ダッシュボードにアタッチします。

```
package aws.example.s3control;


import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.BucketLevel;
import com.amazonaws.services.s3control.model.PutStorageLensConfigurationRequest;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.model.AccountLevel;
import com.amazonaws.services.s3control.model.StorageLensConfiguration;
import com.amazonaws.services.s3control.model.StorageLensGroupLevel;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class CreateDashboardWithStorageLensGroups {
    public static void main(String[] args) {
        String configurationId = "ExampleDashboardConfigurationId";
        String sourceAccountId = "111122223333";

        try {
```

```
            StorageLensGroupLevel storageLensGroupLevel = new StorageLensGroupLevel();

            AccountLevel accountLevel = new AccountLevel()
                    .withBucketLevel(new BucketLevel())
                    .withStorageLensGroupLevel(storageLensGroupLevel);

            StorageLensConfiguration configuration = new StorageLensConfiguration()
                    .withId(configurationId)
                    .withAccountLevel(accountLevel)
                    .withIsEnabled(true);

            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            s3ControlClient.putStorageLensConfiguration(new
 PutStorageLensConfigurationRequest()
                    .withAccountId(sourceAccountId)
                    .withConfigId(configurationId)
                    .withStorageLensConfiguration(configuration)
            );
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Example – 2 つの ストレージレンズグループをダッシュボードにアタッチする

次の AWS SDK for Java 例では、2 つの Storage Lens グループ (*StorageLensGroupName1* と *StorageLensGroupName2*) を *ExampleDashboardConfigurationId* ダッシュボードにアタッチします。

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
```

```
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.AccountLevel;
import com.amazonaws.services.s3control.model.BucketLevel;
import com.amazonaws.services.s3control.model.PutStorageLensConfigurationRequest;
import com.amazonaws.services.s3control.model.StorageLensConfiguration;
import com.amazonaws.services.s3control.model.StorageLensGroupLevel;
import com.amazonaws.services.s3control.model.StorageLensGroupLevelSelectionCriteria;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class CreateDashboardWith2StorageLensGroups {
    public static void main(String[] args) {
        String configurationId = "ExampleDashboardConfigurationId";
        String storageLensGroupName1 = "StorageLensGroupName1";
        String storageLensGroupName2 = "StorageLensGroupName2";
        String sourceAccountId = "111122223333";

        try {
            StorageLensGroupLevelSelectionCriteria selectionCriteria = new
 StorageLensGroupLevelSelectionCriteria()
                    .withInclude(
                            "arn:aws:s3:" + US_WEST_2.getName() + ":" + sourceAccountId
 + ":storage-lens-group/" + storageLensGroupName1,
                            "arn:aws:s3:" + US_WEST_2.getName() + ":" + sourceAccountId
 + ":storage-lens-group/" + storageLensGroupName2);

            System.out.println(selectionCriteria);
            StorageLensGroupLevel storageLensGroupLevel = new StorageLensGroupLevel()
                    .withSelectionCriteria(selectionCriteria);

            AccountLevel accountLevel = new AccountLevel()
                    .withBucketLevel(new BucketLevel())
                    .withStorageLensGroupLevel(storageLensGroupLevel);

            StorageLensConfiguration configuration = new StorageLensConfiguration()
                    .withId(configurationId)
                    .withAccountLevel(accountLevel)
                    .withIsEnabled(true);

            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
```

```
                    .withRegion(US_WEST_2)
                    .build();

            s3ControlClient.putStorageLensConfiguration(new
 PutStorageLensConfigurationRequest()
                    .withAccountId(sourceAccountId)
                    .withConfigId(configurationId)
                    .withStorageLensConfiguration(configuration)
            );
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Example – 除外項目を含むすべてのストレージレンズグループをアタッチする

次の SDK for Java 例では、2 つの Storage Lens グループを *ExampleDashboardConfigurationId* ダッシュボードにアタッチします (指定した *StorageLensGroupName1* と *StorageLensGroupName2* を除く):

```
package aws.example.s3control;


import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.AccountLevel;
import com.amazonaws.services.s3control.model.BucketLevel;
import com.amazonaws.services.s3control.model.PutStorageLensConfigurationRequest;
import com.amazonaws.services.s3control.model.StorageLensConfiguration;
import com.amazonaws.services.s3control.model.StorageLensGroupLevel;
import com.amazonaws.services.s3control.model.StorageLensGroupLevelSelectionCriteria;

import static com.amazonaws.regions.Regions.US_WEST_2;
```

```
public class CreateDashboardWith2StorageLensGroupsExcluded {
    public static void main(String[] args) {
        String configurationId = "ExampleDashboardConfigurationId";
        String storageLensGroupName1 = "StorageLensGroupName1";
        String storageLensGroupName2 = "StorageLensGroupName2";
        String sourceAccountId = "111122223333";

        try {
            StorageLensGroupLevelSelectionCriteria selectionCriteria = new
 StorageLensGroupLevelSelectionCriteria()
                    .withInclude(
                            "arn:aws:s3:" + US_WEST_2.getName() + ":" + sourceAccountId
 + ":storage-lens-group/" + storageLensGroupName1,
                            "arn:aws:s3:" + US_WEST_2.getName() + ":" + sourceAccountId
 + ":storage-lens-group/" + storageLensGroupName2);

            System.out.println(selectionCriteria);
            StorageLensGroupLevel storageLensGroupLevel = new StorageLensGroupLevel()
                    .withSelectionCriteria(selectionCriteria);

            AccountLevel accountLevel = new AccountLevel()
                    .withBucketLevel(new BucketLevel())
                    .withStorageLensGroupLevel(storageLensGroupLevel);

            StorageLensConfiguration configuration = new StorageLensConfiguration()
                    .withId(configurationId)
                    .withAccountLevel(accountLevel)
                    .withIsEnabled(true);

            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            s3ControlClient.putStorageLensConfiguration(new
 PutStorageLensConfigurationRequest()
                    .withAccountId(sourceAccountId)
                    .withConfigId(configurationId)
                    .withStorageLensConfiguration(configuration)
            );
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
```

```
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Storage Lens グループのデータの視覚化

Storage Lens グループのデータは、Amazon S3 ストレージレンズダッシュボードにグループをアタッチすることで視覚化できます。ダッシュボード設定の Storage Lens グループ集約に Storage Lens グループを含めてから、Storage Lens グループのデータがダッシュボードに表示されるまでに最大 48 時間かかることがあります。

ダッシュボードの設定が更新されると、新しくアタッチされた Storage Lens グループが [Storage Lens グループ] タブの使用可能なリソースのリストに表示されます。データを別の次元でスライスすることで、[概要] タブでストレージ使用状況をさらに分析することもできます。例えば、上位 3 つのカテゴリにリストされている項目の 1 つを選択し、[分析基準] を選択すると、データを別のディメンションで分割できます。フィルタ自体と同じディメンションを適用することはできません。

> **Note**
>
> Storage Lens グループフィルタとプレフィックスフィルタ、またはその逆は適用できません。また、プレフィックスフィルタを使用して Storage Lens グループをさらに分析することもできません。

Amazon S3 ストレージレンズダッシュボードの [Storage Lens グループ] タブを使用して、ダッシュボードにアタッチされている Storage Lens グループのデータ視覚化をカスタマイズできます。ダッシュボードに添付されている一部の Storage Lens グループ、またはすべてのデータを視覚化できます。

S3 Storage Lens のデータを視覚化するときは、次の点に注意してください。

- S3 Storage Lens は、一致するすべての Storage Lens グループのオブジェクトの使用状況メトリクスを集約します。そのため、オブジェクトが 2 つ以上の Storage Lens グループのフィルタ条件に一致すると、ストレージ使用状況全体で同じオブジェクトの数が繰り返し表示されます。

- オブジェクトは、Storage Lens グループに含めるフィルタと一致する必要があります。Storage Lens グループに含めるフィルタに一致するオブジェクトがない場合、メトリクスは生成されません。未割り当てのオブジェクトがないかどうかを確認するには、ダッシュボードでアカウントレベルとバケットレベルの合計オブジェクト数を確認します。

Storage Lens グループの更新

以下の例は、Amazon S3 ストレージレンズグループを更新する方法を示しています。Amazon S3 コンソール AWS Command Line Interface (AWS CLI)、および AWS SDK for Java を使用して Storage Lens グループを更新できます。

S3 コンソールの使用

Storage Lens グループを更新するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ナビゲーションペインで、[Storage Lens グループ]を選択します。
3. [Storage Lens グループ] で、更新する Storage Lens グループを選択します。
4. [スコープ] で、[編集] を選択します。
5. [スコープ] ページで、Storage Lens グループに適用するためのフィルタを選択します。複数のフィルタを適用するには、フィルタを選択し、AND または OR の論理演算子を選択します。

   - [プレフィックス] フィルタでは、[プレフィックス] を選択し、プレフィックス文字列を入力します。複数のプレフィックスを追加するには、[プレフィックスを追加] を選択します。プレフィックスを削除するには、削除するボリュームの横にある [削除] を選択します。
   - [オブジェクトタグ] フィルタでは、オブジェクトのキーと値のペアを入力します。次に、[タグの追加] を選択します。タグを削除するには、削除したいタグの横にある[削除] を選択します。
   - [サフィックス] フィルタでは、[サフィックス] を選択し、サフィックス文字列を入力します。複数のサフィックスを追加するには、[サフィックスを追加] を選択します。サフィックスを削除するには、削除したいサフィックスの横にある[削除] を選択します。
   - [経過時間] フィルタでは、オブジェクトの有効期間を日単位で指定します。[オブジェクトの最短経過時間を指定] を選択し、オブジェクトの最低経過時間を入力します。[オブジェクトの最長経過時間を指定] を選択し、オブジェクトの最長経過時間を入力します。

- [サイズ] フィルタで、オブジェクトサイズの範囲と測定単位を指定します。[最小オブジェクトサイズを指定] を選択し、オブジェクトの最小オブジェクトサイズを入力します。[最大オブジェクトサイズを指定] に、オブジェクトの最大オブジェクトサイズを入力します。

6. [Save changes] (変更の保存) をクリックします。Storage Lens グループの詳細ページが表示されます。
7. (オプション) 新しい AWS リソースタグを追加する場合は、[AWS リソースタグ] セクションまでスクロールし、[タグを追加] を選択します。タグの追加 ページが表示されます。

   新しいキーと値のペアを追加し、[変更の保存] を選択します。Storage Lens グループの詳細ページが表示されます。
8. (オプション) 既存の AWS リソースタグを削除する場合は、[AWS リソースタグ] セクションまでスクロールし、リソースタグを選択します。その後、[削除] をクリックします。[AWS タグの削除] ダイアログボックスが表示されます。

   AWS リソースタグを完全に削除するには、もう一度 [削除] を選択します。

> **Note**
>
> AWS リソースタグを完全に削除すると、元に戻すことはできません。

AWS CLI を使用する場合

以下の AWS CLI 例コマンドでは、*marketing-department* という名前の Storage Lens グループの設定の詳細を返します。このコマンド例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3control get-storage-lens-group --account-id 111122223333 \
--region us-east-1 --name marketing-department
```

次の AWS CLI 例は、Storage Lens グループを更新します。このコマンド例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3control update-storage-lens-group --account-id 111122223333 \
--region us-east-1 --storage-lens-group=file://./marketing-department.json
```

JSON 設定例については、「Storage Lens グループの設定」を参照してください。

AWS SDK for Java の使用

以下の AWS SDK for Java 例では、アカウント *111122223333* の *Marketing-Department* Storage Lens グループの設定の詳細を返します。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.GetStorageLensGroupRequest;
import software.amazon.awssdk.services.s3control.model.GetStorageLensGroupResponse;

public class GetStorageLensGroup {
    public static void main(String[] args) {
        String storageLensGroupName = "Marketing-Department";
        String accountId = "111122223333";

        try {
            GetStorageLensGroupRequest getRequest =
 GetStorageLensGroupRequest.builder()
                    .name(storageLensGroupName)
                    .accountId(accountId).build();
            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            GetStorageLensGroupResponse response =
 s3ControlClient.getStorageLensGroup(getRequest);
            System.out.println(response);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
```

```
}
```

以下の例では、アカウント *111122223333* で *Marketing-Department* という名前の Storage Lens グループを更新します。この例では、*.png*、*.gif*、*.jpg*、または *.jpeg* のいずれかのサフィックスに一致するオブジェクトを含むようにダッシュボードスコープを更新します。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.StorageLensGroup;
import software.amazon.awssdk.services.s3control.model.StorageLensGroupFilter;
import software.amazon.awssdk.services.s3control.model.UpdateStorageLensGroupRequest;

public class UpdateStorageLensGroup {
    public static void main(String[] args) {
        String storageLensGroupName = "Marketing-Department";
        String accountId = "111122223333";

        try {
            // Create updated filter.
            StorageLensGroupFilter suffixFilter = StorageLensGroupFilter.builder()
                    .matchAnySuffix(".png", ".gif", ".jpg", ".jpeg")
                    .build();

            StorageLensGroup storageLensGroup = StorageLensGroup.builder()
                    .name(storageLensGroupName)
                    .filter(suffixFilter)
                    .build();

            UpdateStorageLensGroupRequest updateStorageLensGroupRequest =
 UpdateStorageLensGroupRequest.builder()
                    .name(storageLensGroupName)
                    .storageLensGroup(storageLensGroup)
                    .accountId(accountId)
                    .build();

            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
```

```
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            s3ControlClient.updateStorageLensGroup(updateStorageLensGroupRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

JSON 設定例については、「Storage Lens グループの設定」を参照してください。

Storage Lens グループによる AWS リソースタグの管理

Amazon S3 ストレージレンズグループはそれぞれ独自の Amazon AWS リソースネーム (ARN) を持つリソースとみなされます。そのため、Storage Lens グループを設定するときに、AWS オプションでグループにリソースタグを追加できます。Storage Lens グループごとに最大 50 個のタグを追加できます。タグ付きの Storage Lens グループを作成するには、`s3:CreateStorageLensGroup` と `s3:TagResource` の権限が必要です。

AWS リソースタグを使用して、部門、事業内容、またはプロジェクトごとにリソースを分類できます。そうすることで、同じ種類のリソースが多い場合に役立ちます。タグを適用すると、割り当てたタグに基づいて特定の Storage Lens グループをすばやく識別できます。また、コストの追跡と割り当てにもタグを使用できます。

さらに、Storage Lens グループに AWS リソースタグを追加すると、属性ベースのアクセス制御 (ABAC) が有効になります。ABAC は、このケースタグの属性に基づいて権限を定義する認可戦略です。IAM ポリシーでリソースタグを指定する条件を使用して、AWS リソースへのアクセスを制御できます。

タグのキーと値は編集でき、タグはリソースからいつでも削除できます。また、次の点について注意してください:

- キーとタグの値は大文字と小文字が区別されます。
- 特定のリソースについて既存のタグと同じキーを持つタグを追加した場合、以前の値は新しい値によって上書きされます。

- リソースを削除すると、リソースのタグも削除されます。
- AWS リソースタグにはプライベートデータや機密データを含めないでください。
- システムタグ (aws: で始まるタグキーの場合) はサポートされていません。
- 各タグキーの長さは 128 文字以下にする必要があります。各タグ値の長さは 256 文字以下にする必要があります。

次の例は、Storage Lens グループで AWS リソースタグを使用する方法を示しています。

トピック

- Storage Lens グループに AWS リソースタグを追加する
- Storage Lens グループのタグ値の更新
- Storage Lens グループから AWS リソースタグを削除する
- Storage Lens グループのタグの一覧表示

Storage Lens グループに AWS リソースタグを追加する

次の例は、Amazon S3 ストレージレンズグループに AWS リソースタグを使用する方法を示しています。Amazon S3 コンソール AWS Command Line Interface (AWS CLI)、および AWS SDK for Java を使用してリソースタグを追加できます。

S3 コンソールの使用

Storage Lens グループに AWS リソースタグを追加するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ナビゲーションペインで、[Storage Lens グループ]を選択します。
3. [Storage Lens グループ] で、更新する Storage Lens グループを選択します。
4. [AWS リソースタグ] で [タグを追加] を選択します。
5. [タグの追加] ページで、新しいキーと値のペアを追加します。

> **Note**
>
> 既存のタグと同じ新しいタグを追加すると、以前のタグ値は上書きされます。

6. (オプション) 複数の新しいタグを追加するには、[タグを追加] を再度選択して新しいエントリを追加し続けます。Storage Lens グループには、最大 50 個の AWS リソースタグを追加できます。
7. (オプション) 新規追加されたエントリを削除する場合は、削除するタグの横にある[削除] を選びます。
8. [Save changes] (変更の保存) をクリックします。

AWS CLI を使用する場合

以下の AWS CLI コマンド例では、*marketing-department* という名前の既存の Storage Lens グループに 2 つのリソースタグを追加しています。このコマンド例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3control tag-resource --account-id 111122223333 \
--resource-arn arn:aws:s3:us-east-1:111122223333:storage-lens-group/marketing-
department \
--region us-east-1 --tags Key=k1,Value=v1 Key=k2,Value=v2
```

AWS SDK for Java の使用

以下の AWS SDK for Java 例では、既存の Storage Lens グループに 2 つの AWS リソースタグを追加しています。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.Tag;
import software.amazon.awssdk.services.s3control.model.TagResourceRequest;

public class TagResource {
    public static void main(String[] args) {
        String resourceARN = "Resource_ARN";
        String accountId = "111122223333";

        try {
```

```
            Tag resourceTag1 = Tag.builder()
                .key("resource-tag-key-1")
                .value("resource-tag-value-1")
                .build();
            Tag resourceTag2 = Tag.builder()
                    .key("resource-tag-key-2")
                    .value("resource-tag-value-2")
                    .build();
            TagResourceRequest tagResourceRequest = TagResourceRequest.builder()
                    .resourceArn(resourceARN)
                    .tags(resourceTag1, resourceTag2)
                    .accountId(accountId)
                    .build();
            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            s3ControlClient.tagResource(tagResourceRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Storage Lens グループのタグ値の更新

以下の例は、Amazon S3 コンソール、AWS Command Line Interface (AWS CLI)、および AWS SDK for Java を使用して Storage Lens グループを更新する方法を示しています。

S3 コンソールの使用

Storage Lens グループの AWS リソースタグを更新するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ナビゲーションペインで、[Storage Lens グループ]を選択します。
3. [Storage Lens グループ] で、更新する Storage Lens グループを選択します。

4. [AWSリソースタグ] で、更新するタグを選択します。
5. 更新するキーと値のペアの同じキーを使用して、新しいタグ値を追加します。チェックマークアイコンを選択してタグの値を更新します。

> **Note**
>
> 既存のタグと同じ新しいタグを追加すると、以前のタグ値は上書きされます。

6. (オプション) 新しいタグを追加する場合は、[タグの追加] を選択して新しいエントリを追加します。タグの追加 ページが表示されます。

   Storage Lens グループには、最大 50 個の AWS リソースタグを追加できます。新しいタグの追加を完了したら、[変更の保存] を選択します。
7. (オプション) 新規追加されたエントリを削除する場合は、削除するタグの横にある[削除] を選びます。タグの削除を完了したら、[タグの保存] を選択します。

AWS CLI を使用する場合

次の AWS CLI コマンド例は、*marketing-department* という名前の Storage Lens グループの 2 つのタグ値を更新します。このコマンド例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3control tag-resource --account-id 111122223333 \
--resource-arn arn:aws:s3:us-east-1:111122223333:storage-lens-group/marketing-
department \
--region us-east-1 --tags Key=k1,Value=v3 Key=k2,Value=v4
```

AWS SDK for Java の使用

次の AWS SDK for Java 例では、2 つの Storage Lens グループのタグ値を更新します。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.Tag;
```

```
import software.amazon.awssdk.services.s3control.model.TagResourceRequest;

public class UpdateTagsForResource {
    public static void main(String[] args) {
        String resourceARN = "Resource_ARN";
        String accountId = "111122223333";

        try {
            Tag updatedResourceTag1 = Tag.builder()
                .key("resource-tag-key-1")
                .value("resource-tag-updated-value-1")
                .build();
            Tag updatedResourceTag2 = Tag.builder()
                    .key("resource-tag-key-2")
                    .value("resource-tag-updated-value-2")
                    .build();
            TagResourceRequest tagResourceRequest = TagResourceRequest.builder()
                    .resourceArn(resourceARN)
                    .tags(updatedResourceTag1, updatedResourceTag2)
                    .accountId(accountId)
                    .build();
            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            s3ControlClient.tagResource(tagResourceRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Storage Lens グループから AWS リソースタグを削除する

次の例は、Storage Lens グループから AWS リソースタグを削除する方法を示しています。Amazon S3 コンソール AWS Command Line Interface (AWS CLI)、および AWS SDK for Java を使用してタグを削除できます。

S3 コンソールの使用

Storage Lens グループから AWS リソースタグを削除するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ナビゲーションペインで、[Storage Lens グループ]を選択します。
3. [Storage Lens グループ] で、更新する Storage Lens グループを選択します。
4. [AWSリソースタグ] で、削除するキーと値のペアを選択します。
5. [削除] を選択します。[AWSリソースタグの削除] ダイアログボックスが表示されます。

> **Note**
>
> タグを使用してアクセスを制御すると、関連するリソースに影響を与える可能性があります。タグを完全に削除すると、元に戻すことはできません。

6. [削除] を選択してキー値のペアを完全に削除します。

AWS CLI を使用する場合

次の AWS CLI コマンドは、既存の Storage Lens グループから 2 つの AWS リソースタグを削除します。このコマンド例を使用するには、*user input placeholders* を独自の情報に置き換えてください。

```
aws s3control untag-resource --account-id 111122223333 \
--resource-arn arn:aws:s3:us-east-1:111122223333:storage-lens-group/Marketing-Department \
--region us-east-1 --tag-keys k1 k2
```

AWS SDK for Java の使用

次の AWS SDK for Java 例では、アカウント *111122223333* で指定した Storage Lens グループの Amazon リソースネーム (ARN) から 2 つの AWS リソースタグを削除します。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
```

```
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.UntagResourceRequest;

public class UntagResource {
    public static void main(String[] args) {
        String resourceARN = "Resource_ARN";
        String accountId = "111122223333";

        try {
            String tagKey1 = "resource-tag-key-1";
            String tagKey2 = "resource-tag-key-2";
            UntagResourceRequest untagResourceRequest = UntagResourceRequest.builder()
                    .resourceArn(resourceARN)
                    .tagKeys(tagKey1, tagKey2)
                    .accountId(accountId)
                    .build();
            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            s3ControlClient.untagResource(untagResourceRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Storage Lens グループのタグの一覧表示

以下の例は、Storage Lens グループに関連付けられている AWS リソースタグを一覧表示する方法を示しています。Amazon S3 コンソール AWS Command Line Interface (AWS CLI)、および AWS SDK for Java を使用してタグを一覧表示できます。

S3 コンソールの使用

Storage Lens グループのタグとタグ値のリストを確認するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ナビゲーションペインで、[Storage Lens グループ]を選択します。
3. [Storage Lens グループ] で、対象となる Storage Lens グループを選択します。
4. [AWS リソースタグ] セクションまでスクロールダウンします。Storage Lens グループに追加されたすべてのユーザー定義 AWS リソースタグが、そのタグ値とともに一覧表示されます。

AWS CLI を使用する場合

次の AWS CLI コマンド例では、*marketing-department* という名前の Storage Lens グループの Storage Lens グループタグすべてを一覧表示しています。このコマンド例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3control list-tags-for-resource --account-id 111122223333 \
--resource-arn arn:aws:s3:us-east-1:111122223333:storage-lens-group/marketing-
department \
--region us-east-1
```

AWS SDK for Java の使用

次の AWS SDK for Java 例では、指定した Storage Lens グループ Amazon リソースネーム (ARN) のStorage Lens グループタグ値を一覧表示しています。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.ListTagsForResourceRequest;
import software.amazon.awssdk.services.s3control.model.ListTagsForResourceResponse;

public class ListTagsForResource {
```

```
    public static void main(String[] args) {
        String resourceARN = "Resource_ARN";
        String accountId = "111122223333";

        try {
            ListTagsForResourceRequest listTagsForResourceRequest =
 ListTagsForResourceRequest.builder()
                    .resourceArn(resourceARN)
                    .accountId(accountId)
                    .build();
            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            ListTagsForResourceResponse response =
 s3ControlClient.listTagsForResource(listTagsForResourceRequest);
            System.out.println(response);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

すべての Storage Lens グループの一覧表示

以下の例は、AWS アカウント およびホームリージョン内のすべての Amazon S3 ストレージレンズグループを一覧表示する方法を示しています。これらの例は、Amazon S3 コンソール AWS Command Line Interface (AWS CLI)、および AWS SDK for Java を使用してすべての Storage Lens グループを一覧表示する方法を示しています。

S3 コンソールの使用

アカウントとホームリージョンのすべての Amazon S3 ストレージレンズグループを一覧表示するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。

2. ナビゲーションペインで、[Storage Lens グループ] を選択します。
3. Storage Lens グループには、アカウント内の Storage Lens グループのリストが表示されます。

AWS CLI を使用する場合

次の AWS CLI 例では、アカウントのすべての Storage Lens グループを一覧表示しています。このコマンド例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3control list-storage-lens-groups --account-id 111122223333 \
--region us-east-1
```

AWS SDK for Java の使用

次の AWS SDK for Java 例では、アカウント *111122223333* の Storage Lens グループを一覧表示しています。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.ListStorageLensGroupsRequest;
import software.amazon.awssdk.services.s3control.model.ListStorageLensGroupsResponse;

public class ListStorageLensGroups {
    public static void main(String[] args) {
        String accountId = "111122223333";

        try {
            ListStorageLensGroupsRequest listStorageLensGroupsRequest =
 ListStorageLensGroupsRequest.builder()
                    .accountId(accountId)
                    .build();
            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
```

```
            ListStorageLensGroupsResponse response =
 s3ControlClient.listStorageLensGroups(listStorageLensGroupsRequest);
            System.out.println(response);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Storage Lens グループ詳細の表示

以下の例は、Amazon S3 ストレージレンズグループ設定の詳細を表示する方法を示しています。Amazon S3 コンソール、AWS Command Line Interface (AWS CLI)、および AWS SDK for Java を使用してこれらの詳細を表示できます。

S3 コンソールの使用

Storage Lens グループ設定の詳細を表示するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ナビゲーションペインで、[Storage Lens グループ]を選択します。
3. [Storage Lens グループ] で、対象となる Storage Lens グループの横にあるオプションボタンを選択します。
4. [詳細を表示] を選択します。これで、Storage Lens グループの詳細を確認できます。

AWS CLI を使用する場合

次の AWS CLI 例では、Storage Lens グループの設定の詳細を返します。このコマンド例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3control get-storage-lens-group --account-id 111122223333 \
--region us-east-1 --name marketing-department
```

AWS SDK for Java の使用

以下の AWS SDK for Java 例では、アカウント *111122223333* の *Marketing-Department* という Storage Lens グループの設定の詳細を返します。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.GetStorageLensGroupRequest;
import software.amazon.awssdk.services.s3control.model.GetStorageLensGroupResponse;

public class GetStorageLensGroup {
    public static void main(String[] args) {
        String storageLensGroupName = "Marketing-Department";
        String accountId = "111122223333";

        try {
            GetStorageLensGroupRequest getRequest =
 GetStorageLensGroupRequest.builder()
                    .name(storageLensGroupName)
                    .accountId(accountId).build();
            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            GetStorageLensGroupResponse response =
 s3ControlClient.getStorageLensGroup(getRequest);
            System.out.println(response);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
```

```
}
```

Storage Lens グループの削除

以下の例は、Amazon S3 コンソール AWS Command Line Interface (AWS CLI)、および AWS SDK for Java を使用して Amazon S3 ストレージレンズグループを削除する方法を示しています。

S3 コンソールの使用

Storage Lens グループを削除するには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. ナビゲーションペインで、[Storage Lens グループ] を選択します。
3. [Storage Lens グループ] で、削除する Storage Lens グループの横にあるオプションボタンを選択します。
4. [削除] を選択します。[Storage Lens グループの削除] ダイアログボックスが表示されます。
5. もう一度 [削除] を選択すると、Storage Lens グループが完全に削除されます。

> **Note**
>
> Storage Lens グループを削除すると、復元することはできません。

AWS CLI を使用する場合

以下の AWS CLI 例は、*marketing-department* という名前の Storage Lens グループを削除します。このコマンド例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
aws s3control delete-storage-lens-group --account-id 111122223333 \
--region us-east-1 --name marketing-department
```

AWS SDK for Java の使用

以下の AWS SDK for Java 例は、アカウント *111122223333* で *Marketing-Department* という名前の Storage Lens グループを削除します。この例を実行するには、*user input placeholders* をユーザー自身の情報に置き換えます。

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.DeleteStorageLensGroupRequest;

public class DeleteStorageLensGroup {
    public static void main(String[] args) {
        String storageLensGroupName = "Marketing-Department";
        String accountId = "111122223333";

        try {
            DeleteStorageLensGroupRequest deleteStorageLensGroupRequest =
 DeleteStorageLensGroupRequest.builder()
                    .name(storageLensGroupName)
                    .accountId(accountId).build();
            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            s3ControlClient.deleteStorageLensGroup(deleteStorageLensGroupRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

S3 インベントリを使用したデータのカタログ化と分析

Amazon S3 インベントリを使用してストレージを管理できます。例えば、ビジネス、コンプライアンス、および規制上のニーズに対応して、オブジェクトのレプリケーションや暗号化のステータスを監査およびレポートするために使用できます。また、Amazon S3 同期 `List` API オペレーションのスケジュールされた代替手段として Amazon S3 インベントリを使用し、ビジネスワークフローや

ビッグデータジョブを簡素化、高速化できます。Amazon S3 インベントリは、List API オペレーションを使用してオブジェクトを監査しないため、バケットのリクエストレートには影響しません。

Amazon S3 インベントリは、カンマ区切り値 (CSV)、Apache Optimized Row Columnar (ORC)、または Apache Parquet 出力ファイルを通じて、S3 バケットや共有プレフィックス (オブジェクト名の先頭が共通文字列) を持つオブジェクトについて、オブジェクトおよび対応するメタデータを毎日または毎週一覧表示します。毎週のインベントリを設定すると、最初のレポートの後は毎週日曜日 (UTC タイムゾーン) にレポートが生成されます。Amazon S3 インベントリの料金に関する詳細については、Amazon S3 の料金 を参照してください。

1 つのバケットに対して複数のインベントリリストを設定できます。インベントリリストを設定する場合、以下を指定できます。

- インベントリに含めるオブジェクトメタデータ
- すべてのオブジェクトバージョンを一覧表示するか、現在のバージョンのみを一覧表示するか
- インベントリリストファイル出力を保存する場所
- インベントリを毎日生成するか、毎週生成するか
- インベントリリストファイルを暗号化するかどうか

Amazon S3 インベントリを標準 SQL クエリを使用してクエリするには、Amazon Athena、Amazon Redshift Spectrum、その他のツール (Presto、Apache Hive、Apache Spark など) を使用できます。Athena を使用してインベントリファイルをクエリする方法の詳細については、「the section called “Athena でインベントリをクエリする”」を参照してください。

> **Note**
>
> Amazon S3 が最初のインベントリレポートを配信するまでに最大 48 時間かかることがあります。

ソースバケットと保存先バケット

インベントリでオブジェクトをリストする対象のバケットは、ソースバケットと呼ばれます。インベントリリストファイルを保存する先のバケットは、保存先バケットと呼ばれます。

ソースバケット

インベントリは、ソースバケットに格納されているオブジェクトをリストします。バケット全体のインベントリリストを取得することも、オブジェクトキー名のプレフィックスでリストをフィルタリングすることもできます。

ソースバケット:

- インベントリにリストされているオブジェクトが含まれます。
- インベントリの設定が含まれます。

保存先バケット

Amazon S3 インベントリリストのファイルは、保存先バケットに書き込まれます。すべてのインベントリリストファイルを保存先バケットの共通の場所にグループ化するには、インベントリ設定で保存先のプレフィックスを指定できます。

保存先バケット:

- インベントリのファイルリストが含まれます。
- 保存先バケットに保存されているすべてのインベントリリストファイルを一覧表示するマニフェストファイルが含まれます。詳細については、「インベントリマニフェスト」を参照してください。
- バケットの所有権を検証するためのアクセス許可と、バケットにファイルを書き込むためのアクセス許可を Amazon S3 に付与する、バケットポリシーが必要です。
- ソースバケットと同じ AWS リージョン に存在する必要があります。
- ソースバケットと同じでもかまいません。
- ソースバケットを所有するアカウントとは別の AWS アカウント によって所有されていてもかまいません。

Amazon S3 インベントリのリスト

インベントリリストファイルには、ソースバケット内のオブジェクトのリストと、各オブジェクトのメタデータが含まれます。インベントリリストファイルは、次のいずれかの形式で保存先バケットに保存されます。

- GZIP で圧縮された CSV ファイル
- ZLIB で圧縮された Apache Optimized Row Columnar (ORC)
- Snappy で圧縮された Apache Parquet ファイル

> **Note**
>
> Amazon S3 インベントリレポートのオブジェクトのソート結果は一切保証されません。

インベントリリストファイルには、ソースバケット内のオブジェクトのリストと、リストされた各オブジェクトのメタデータが含まれます。

- バケット名 – インベントリ対象のバケットの名前。
- キー名 – バケット内のオブジェクトを一意に識別するオブジェクトのキー名 (またはキー)。CSV ファイル形式を使用すると、キー名は URL エンコードされるため、これをデコードしてから使用する必要があります。
- バージョン ID – オブジェクトのバージョン ID。バケットのバージョニングを有効にすると、Amazon S3 はバケットに追加されたオブジェクトにバージョン番号を割り当てます。詳細については、「S3 バージョニングによる複数のバージョンのオブジェクトの保持」を参照してください。リストを現在のバージョンのオブジェクトのみに設定した場合、このフィールドは含まれません。
- IsLatest – オブジェクトが現在のバージョンのオブジェクトである場合は、`True` に設定されます リストを現在のバージョンのオブジェクトのみに設定した場合、このフィールドは含まれません。
- 削除マーカー – オブジェクトが削除マーカーである場合は、`True` に設定されます。詳細については、「S3 バージョニングによる複数のバージョンのオブジェクトの保持」を参照してください。(オブジェクトのすべてのバージョンを含めるようにレポートを設定している場合、このフィールドはレポートに自動的に追加されます)。
- サイズ - バイト単位のオブジェクトサイズ。不完全なマルチパートアップロード、オブジェクトメタデータ、削除マーカーのサイズは含まれません。
- 最終更新日 – オブジェクトの作成日または最終更新日のどちらか新しい方。
- ETag – エンティティタグ (ETag) は、オブジェクトのハッシュです。ETag は、変更をオブジェクトのコンテンツにのみ反映し、メタデータには反映しません。ETag は、オブジェクトデータの MD5 ダイジェストである場合があります。どちらであるかは、オブジェクトの作成方法と暗号化方法によって決まります。詳細については、「Amazon Simple Storage Service API リファレンス」の「Object」を参照してください。
- ストレージクラス – オブジェクトの保存に使用するストレージクラス。`STANDARD`、`REDUCED_REDUNDANCY`、`STANDARD_IA`、`ONEZONE_IA`、`INTELLIGENT_TIERING`、`G` または `SNOW` に設定します。詳細については、「Amazon S3 ストレージクラスの理解と管理」を参照してください。

> **Note**
>
> S3 インベントリは S3 Express One Zone をサポートしていません。

- マルチパートアップロードフラグ – オブジェクトがマルチパートアップロードとしてアップロードされた場合は、True に設定されます。詳細については、「Amazon S3 でのマルチパートアップロードを使用したオブジェクトのアップロードとコピー」を参照してください。
- レプリケーションステータス — PENDING、COMPLETED、FAILED または REPLICA に設定します。詳細については、「レプリケーションステータス情報の取得」を参照してください。
- 暗号化ステータス – 使用される暗号化キーの種類に応じた、サーバー側の暗号化ステータス。Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3)、AWS Key Management Service (AWS KMS) キーによるサーバー側の暗号化 (SSE-KMS)、AWS KMS キーによる二層式サーバー側の暗号化 (DSSE-KMS)、またはお客様が指定したキーによるサーバー側の暗号化 (SSE-C) のいずれかとなります。SSE-S3、SSE-KMS、DSSE-KMS、SSE-C、または NOT-SSE に設定します。ステータスが NOT-SSE の場合、オブジェクトはサーバー側の暗号化を使用して暗号化されません。詳細については、「暗号化によるデータの保護」を参照してください。
- S3 オブジェクトロック: 日付までの保持期限 – ロックされたオブジェクトを削除できなくなる日付。詳細については、「S3 Object Lock を使用したオブジェクトのロック」を参照してください。
- S3 オブジェクトロック: 保持モード – ロックされたオブジェクトの Governance または Compliance に設定します。詳細については、「S3 Object Lock を使用したオブジェクトのロック」を参照してください。
- S3 オブジェクトロック: リーガルホールドステータス – リーガルホールドがオブジェクトに適用されている場合は On に設定します。それ以外の場合は、Off に設定されます。詳細については、「S3 Object Lock を使用したオブジェクトのロック」を参照してください。
- S3 Intelligent-Tiering: アクセス階層 – S3 Intelligent-Tiering ストレージクラスがオブジェクトの保存先である場合、オブジェクトのアクセス階層 (高頻度または低頻度)。FREQUENT、INFREQUENT、ARCHIVE_INSTANT_ACCESS、ARCHIVE、または DEEP_ARCHIVE に設定します。詳細については、「アクセスパターンが変化する、またはアクセスパターンが不明なデータを、自動的に最適化するためのストレージクラス」を参照してください。
- S3 バケットキーステータス — ENABLED または DISABLED に設定します。オブジェクトが SSE-KMS に S3 バケットキーを使用するかどうかを示します。詳細については、「Amazon S3 バケットキーの使用」を参照してください。

- チェックサムアルゴリズム - オブジェクトのチェックサムを作成するために使用されるアルゴリズムを示します。詳細については、「サポートされているチェックサムアルゴリズムの使用」を参照してください。
- オブジェクトアクセスコントロールリスト — このオブジェクトへのアクセスを許可する AWS アカウントまたはグループと、許可するアクセスの種類を定義するアクセスコントロールリスト (ACL)。オブジェクト ACL フィールドは JSON 形式で定義します。S3 インベントリレポートには、ACL がバケットで無効になっている場合でも、ソースバケット内のオブジェクトに関連付けられた ACL が含まれます。詳細については、「オブジェクト ACL フィールドの使用」および「アクセスコントロールリスト (ACL) の概要」を参照してください。

> **Note**
>
> オブジェクト ACL フィールドは JSON 形式で定義します。インベントリレポートには、オブジェクト ACL フィールドの値が base64 エンコードされた文字列として表示されます。
> 例えば、次のオブジェクト ACL フィールドが JSON 形式で存在するとします。
>
> ```
> {
>         "version": "2022-11-10",
>         "status": "AVAILABLE",
>         "grants": [{
>             "canonicalId": "example-canonical-user-ID",
>             "type": "CanonicalUser",
>             "permission": "READ"
>         }]
> }
> ```
>
> オブジェクト ACL フィールドはエンコードされ、次の base64 エンコードされた文字列として表示されます。
>
> ```
> eyJ2ZXJzaW9uIjoiMjAyMi0xMS0xMCIsInN0YXR1cyI6IkFWQUlMQUJMRSIsImdyYW50cyI6W3siY2Fub25pY2Fs
> ```
>
> オブジェクト ACL フィールドのデコードされた値を JSON で取得するには、Amazon Athena でこのフィールドをクエリできます。クエリの例については、「Amazon Athena で Amazon S3 インベントリをクエリする」を参照してください。

- オブジェクト所有者 – オブジェクトの所有者の正規ユーザー ID。詳細については、「AWS Account Management リファレンスガイド」の「AWS の正規ユーザー ID を検索する」を参照してください。

> **Note**
>
> ライフサイクル設定に基づいて、オブジェクトの存続期間が終了すると、Amazon S3 が削除キューに追加し、非同期的に削除します。そのため、有効期限が切れる日と Amazon S3 がオブジェクトを削除する日との間に遅延が生じることがあります。インベントリレポートには、有効期限が切れていてもまだ削除されていないオブジェクトが含まれます。S3 ライフサイクルの有効期限アクションの詳細については、「オブジェクトの有効期限」を参照してください。

以下は、4 つのレコードで構成される追加のメタデータフィールドを含むインベントリレポートの例です。

```
amzn-s3-demo-bucket1    example-object-1    EXAMPLEDC8l.XJCENlF7LePaNIIvs001    TRUE
     1500    2024-08-15T15:28:26.0004    EXAMPLE21e1518b92f3d92773570f600    STANDARD
  FALSE    COMPLETED    SSE-KMS    2025-01-25T15:28:26.000Z    COMPLIANCE    Off
 ENABLED
 eyJ2ZXJzaW9uIjoiMjAyMi0xMS0xMCIsInN0YXR1cyI6IkFWQUlMQUJMRSIsImdyYW50cyI6W3sicGVybWlzc2lvbiI6Ik
    EXAMPLE766e8f6b115d93d41df2eac420aa4a465d177c1398bc6a088c76b7000
amzn-s3-demo-bucket1    example-object-2    EXAMPLEDC8l.XJCENlF7LePaNIIvs002
 TRUE        200    2024-08-21T15:28:26.000Z    EXAMPLE21e1518b92f3d92773570f601
  INTELLIGENT_TIERING    FALSE    COMPLETED    SSE-KMS    2025-01-25T15:28:26.000Z
    COMPLIANCE    Off    INFREQUENT    ENABLED    SHA-256
 eyJ2ZXJzaW9uIjoiMjAyMi0xMS0xMCIsInN0YXR1cyI6IkFWQUlMQUJMRSIsImdyYW50cyI6W3sicGVybWlzc2lvbiI6Ik
    EXAMPLE766e8f6b115d93d41df2eac420aa4a465d177c1398bc6a088c76b7001
amzn-s3-demo-bucket1    example-object-3    EXAMPLEDC8l.XJCENlF7LePaNIIvs003    TRUE
      12500    2023-01-15T15:28:30.000Z    EXAMPLE21e1518b92f3d92773570f602    STANDARD
    FALSE    REPLICA    SSE-KMS    2025-01-25T15:28:26.000Z    GOVERNANCE    On
 ENABLED
 eyJ2ZXJzaW9uIjoiMjAyMi0xMS0xMCIsInN0YXR1cyI6IkFWQUlMQUJMRSIsImdyYW50cyI6W3sicGVybWlzc2lvbiI6Ik
    EXAMPLE766e8f6b115d93d41df2eac420aa4a465d177c1398bc6a088c76b7002
amzn-s3-demo-bucket1    example-object-4    EXAMPLEDC8l.XJCENlF7LePaNIIvs004    TRUE
      100    2021-02-15T15:28:27.000Z    EXAMPLE21e1518b92f3d92773570f603    STANDARD
  FALSE    COMPLETED    SSE-KMS    2025-01-25T15:28:26.000Z    COMPLIANCE    Off
 ENABLED
```

```
eyJ2ZXJzaW9uIjoiMjAyMi0xMS0xMCIsInN0YXR1cyI6IkFWQUlMQUJMRSIsImdyYW50cyI6W3sicGVybWlzc2lvbiI6Ik
   EXAMPLE766e8f6b115d93d41df2eac420aa4a465d177c1398bc6a088c76b7003
```

古いインベントリリストを削除するライフサイクルポリシーを作成することをお勧めします。詳細については、「オブジェクトのライフサイクルの管理」を参照してください。

s3:PutInventoryConfiguration アクセス許可により、ユーザーは、インベントリリストを設定するとき、各オブジェクトについて以前にリストされたすべてのメタデータフィールドを選択することと、インベントリを保存する保存先バケットを指定することの両方ができるようになります。保存先バケット内のオブジェクトへの読み取りアクセス権を持つユーザーは、インベントリリストで利用可能なすべてのオブジェクトメタデータフィールドにアクセスできます。インベントリレポートへのアクセスを制限するには、「S3 インベントリおよび S3 分析に対するアクセス許可の付与」を参照してください。

インベントリ整合性

すべてのオブジェクトが各インベントリリストに表示されない場合があります。インベントリリストは、PUT リクエスト (新しいオブジェクトと上書きの両方) および DELETE リクエストの結果整合性を提供します。バケットの各インベントリリストは、バケット項目のスナップショットです。これらのリストは結果的に整合します (つまり、リストには最近追加または削除されたオブジェクトが含まれない場合があります)。

オブジェクトに対してアクションを実行する前に、オブジェクトの状態を検証するには、HeadObject REST API リクエストを実行してオブジェクトのメタデータを取得するか、Amazon S3 コンソールでオブジェクトのプロパティを確認することをお勧めします。AWS CLI または AWS SDK でオブジェクトのメタデータを確認することもできます。詳細については、「Amazon Simple Storage Service API リファレンス」の「HeadObject」を参照してください。

Amazon S3インベントリの使用のさらなる詳細については、以下のトピックを参照してください。

トピック

- Amazon S3 インベントリの設定
- インベントリリストの検索
- インベントリ完了に関する Amazon S3 イベント通知の設定
- Amazon Athena で Amazon S3 インベントリをクエリする
- Amazon S3 インベントリレポートの空のバージョン ID 文字列を NULL 文字列に変換します。
- オブジェクト ACL フィールドの使用

Amazon S3 インベントリの設定

Amazon S3 インベントリには、定義したスケジュールに従ってオブジェクトとメタデータのフラットファイルリストが用意されています。Amazon S3 同期 `List` API オペレーションの代わりにスケジュールされた S3 インベントリを使用できます。S3 インベントリは、カンマ区切り値 (CSV)、Apache Optimized Row Columnar (ORC)、または Apache Parquet (Parquet) 出力ファイルを使用して、オブジェクトおよび対応するメタデータを一覧表示します。

S3 インベントリは、S3 バケットまたはプレフィックスを共有するオブジェクト (つまり、名前の先頭が同じ文字列のオブジェクト) に関して、インベントリリストが用意されています。詳細については、「S3 インベントリを使用したデータのカタログ化と分析」を参照してください。

このセクションでは、インベントリのソースバケットと保存先バケットに関する詳細を含め、インベントリを設定する方法について説明します。

トピック

- 概要
- ターゲットバケットポリシーの作成
- カスタマーマネージドキーを暗号化に使用するためのアクセス許可を Amazon S3 に付与する
- S3 コンソールを使用したインベントリの設定
- REST API を使用して S3 インベントリを操作する

概要

Amazon S3 インベントリは、定義したスケジュールで S3 バケット内のオブジェクトのリストを作成し、ストレージの管理に役立ちます。1 つのバケットに対して複数のインベントリリストを設定できます。インベントリリストは、保存先バケットの CSV、ORC、または Parquet ファイルに発行されます。

インベントリを設定する最も簡単な方法は、Amazon S3 を使用することですが、REST API、AWS Command Line Interface (AWS CLI)、または AWS SDK を使用することもできます。コンソールは、次の手順の最初のステップを実行します。保存先バケットへのバケットポリシーの追加。

S3 バケットの Amazon S3 インベントリをセットアップする方法

1. 保存先バケットのバケットポリシーを追加します。

定義された場所のバケットにオブジェクトを書き込むアクセス許可を Amazon S3 に付与するバケットポリシーを保存先バケットに作成する必要があります。ポリシーの例については、「S3 インベントリおよび S3 分析に対するアクセス許可の付与」を参照してください。

2. ソースバケットのオブジェクトをリストして保存先バケットにリストを発行するようにインベントリを設定します。

   ソースバケットのインベントリリストを設定するときは、リストを保存する保存先バケットと、リストを毎日または毎週のどちらで生成したいかを、指定します。また、すべてのオブジェクトバージョンまたは現在のバージョンだけのどちらをリストするか、どのオブジェクトメタデータを含めるかも設定できます。

   S3 インベントリレポート設定の一部のオブジェクトメタデータフィールドはオプションです。つまり、デフォルトで使用できますが、ユーザーに `s3:PutInventoryConfiguration` アクセス許可を付与すると制限できます。`s3:InventoryAccessibleOptionalFields` 条件キーを使用して、ユーザーがこれらのオプションのメタデータフィールドをレポートに含めることができるかどうかを制御できます。

   S3 インベントリで使用できるオプションのメタデータフィールドの詳細については、「Amazon Simple Storage Service API リファレンス」の「OptionalFields」を参照してください。インベントリ設定の特定のオプションのメタデータフィールドへのアクセスを制限する方法についての詳細は、「S3 インベントリレポート設定の作成を制御する」を参照してください。

   Amazon S3 マネージド キー (SSE-S3) または AWS Key Management Service (AWS KMS) カスタマーマネージドキー (SSE-KMS) を使用したサーバー側の暗号化により、インベントリリストファイルを暗号化するように指定できます。

   > **Note**
   >
   > AWS マネージドキー(`aws/s3`) は S3 インベントリでの SSE-KMS 暗号化ではサポートされていません。

   SSE-S3 および SSE-KMS に関する詳細は、「サーバー側の暗号化によるデータの保護」を参照してください。SSE-KMS 暗号化を使用する場合は、ステップ 3 を参照してください。

   - コンソールを使用してインベントリリストを設定する方法については、「S3 コンソールを使用したインベントリの設定」を参照してください。

- Amazon S3 API を使用してインベントリリストを設定するには、PutBucketInventoryConfiguration REST API オペレーションを使用するか、AWS CLI または AWS SDK の同等のオペレーションを使用します。

3. SSE-KMS を使用してインベントリリストファイルを暗号化するには、AWS KMS key を使用するための許可を Amazon S3 に付与します。

   Amazon S3 REST API、AWS CLI、または AWS SDK を使用してインベントリリストファイルの暗号化を設定することができます。どちらの方法を選択しても、 カスタマーマネージドキーを使用してインベントリファイルを暗号化する許可を Amazon S3 に付与する必要があります。Amazon S3 に許可を付与するには、インベントリファイルの暗号化に使用するカスタマーマネージドキーのキーポリシーを変更します。詳細については、「カスタマーマネージドキーを暗号化に使用するためのアクセス許可を Amazon S3 に付与する」を参照してください。

   インベントリリストファイルを保存する先のバケットは、ソースバケットを所有するアカウントとは異なる AWS アカウントが所有している場合があります。Amazon S3 インベントリのクロスアカウントオペレーションで SSE-KMS 暗号化を使用する場合は、S3 インベントリの設定時に、完全修飾された KMS キー ARN を使用することをお勧めします。詳細については、「Amazon Simple Storage Service API リファレンス」の「クロスアカウント操作での SSE-KMS 暗号化の使用」と「ServerSideEncryptionByDefault」を参照してください。

ターゲットバケットポリシーの作成

Amazon S3 コンソールを使用してインベントリ設定を作成する場合、Amazon S3 は、バケットへの書き込みアクセス許可を Amazon S3 に付与するバケットポリシーを、保存先バケットに自動的に作成します。ただし、AWS CLI、AWS SDK、または Amazon S3 REST API を使用してインベントリ設定を作成する場合は、バケットポリシーを保存先バケットに手動で追加する必要があります。S3 インベントリの送信先バケットポリシーにより、Amazon S3 がインベントリレポートのデータをバケットに書き込むことができるようになります。

以下は、バケットポリシーの例です。

```
{
      "Version": "2012-10-17",
      "Statement": [
        {
            "Sid": "InventoryExamplePolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
```

```
            },
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET/*"
            ],
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:s3:::DOC-EXAMPLE-SOURCE-BUCKET"
                },
                "StringEquals": {
                    "aws:SourceAccount": "source-account-id",
                    "s3:x-amz-acl": "bucket-owner-full-control"
                }
            }
        }
    ]
}
```

詳細については、「S3 インベントリおよび S3 分析に対するアクセス許可の付与」を参照してください。

バケットポリシーを作成しようとしたときにエラーが発生した場合、解決するための手順が表示されます。例えば、別の AWS アカウント 内のターゲットバケットを選択したが、バケットポリシーの読み書きを行う許可がない場合、次のエラーメッセージが表示されます。

この場合、ターゲットバケットの所有者は、バケットポリシーをターゲットバケットに追加する必要があります。ポリシーがターゲットバケットに追加されない場合、Amazon S3 にはターゲットバケットに書き込むアクセス許可がないため、インベントリレポートを取得できません。ソースバケットが現在のユーザー以外のアカウントによって所有されている場合、ポリシーでソースバケット所有者の正しいアカウント ID に置き換える必要があります。

> **Note**
>
> このバケットへのインベントリレポートの配信を妨げる Deny ステートメントが送信先バケットポリシーに追加されていないことを確認します。詳細については、「Amazon S3 インベントリレポートを生成できないのはなぜですか?」を参照してください。

カスタマーマネージドキーを暗号化に使用するためのアクセス許可を Amazon S3 に付与する

AWS Key Management Service (AWS KMS) カスタマーマネージドキーを使用して暗号化する許可を Amazon S3 に付与するには、キーポリシーを使用する必要があります。カスタマーマネージドキーを使用できるようにキーポリシーを更新するには、次の手順に従います。

カスタマーマネージドキーを使用して暗号化するアクセス許可を Amazon S3 に付与するには

1. カスタマーマネージドキーを所有する AWS アカウント を使用して、AWS Management Console にサインインします。
2. AWS KMS コンソール (https://console.aws.amazon.com/kms) を開きます。
3. AWS リージョン を変更するには、ページの右上隅にあるリージョンセレクターを使用します。
4. 左のナビゲーションペインで、[Customer managed keys] を選択します。
5. [カスタマーマネージドキー] で、インベントリファイルの暗号化に使用するカスタマーマネージドキーを選択します。
6. [Key Policy] (キーポリシー) セクションで、[Switch to policy view] (ポリシービューへの切り替え) を選択します。
7. [編集] をクリックし、キーポリシーを更新します。
8. [キーポリシーの編集] ページで、既存のキーポリシーに以下の行を追加します。*source-account-id* および *amzn-s3-demo-source-bucket* として、ユースケースに応じた値を入力します。

```
{
    "Sid": "Allow Amazon S3 use of the customer managed key",
    "Effect": "Allow",
    "Principal": {
        "Service": "s3.amazonaws.com"
    },
    "Action": [
        "kms:GenerateDataKey"
    ],
    "Resource": "*",
    "Condition":{
      "StringEquals":{
        "aws:SourceAccount":"source-account-id"
     },
      "ArnLike":{
```

```
            "aws:SourceARN": "arn:aws:s3:::amzn-s3-demo-source-bucket"
        }
    }
}
```

9. [Save changes] (変更の保存) をクリックします。

カスタマーマネージドキーの作成とキーポリシーの使用の詳細については、AWS Key Management Service デベロッパーガイドの次のリンクを参照してください。

- キーの管理
- AWS KMS のキーポリシー

> **Note**
>
> このバケットへのインベントリレポートの配信を妨げる Deny ステートメントが送信先バケットポリシーに追加されていないことを確認します。詳細については、「Amazon S3 インベントリレポートを生成できないのはなぜですか?」を参照してください。

S3 コンソールを使用したインベントリの設定

S3 コンソールを使用してインベントリを設定するには、次の手順を使用します。

> **Note**
>
> Amazon S3 が最初のインベントリレポートを配信するまでに最大 48 時間かかることがあります。

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[汎用バケット] を選択します。
3. バケットリストで、Amazon S3 インベントリを設定する対象のバケットの名前を選択します。
4. [管理] タブを選択します。
5. [インベントリ設定] で、[インベントリ設定の作成] を選択します。
6. [インベントリ設定名] に、名前を入力します。

7. [インベントリスコープ] で、次の操作を行います。

   - オプションのプレフィックスを入力します。
   - 含めるオブジェクトバージョンとして、[現在のバージョンのみ] または [すべてのバージョンを含める] のどちらかを選択します。

8. [Report details] (レポートの詳細) で、[This account] (このアカウント) または [A different account] (別のアカウント) のいずれかを、レポートを保存する AWS アカウント の場所として選択します。

9. [保存先] で、インベントリレポートを保存する先のバケットを選択します。

   ターゲットバケットは、インベントリをセットアップするバケットと同じ AWS リージョン にある必要があります。ターゲットバケットは、別の AWS アカウント にある場合があります。保存先バケットを指定するときに、インベントリレポートをグループ化するためのオプションのプレフィックスを含めることもできます。

   [送信先] バケットフィールドの下に、[送信先バケットのアクセス許可] と表示されます。このアクセス許可を送信先バケットポリシーに追加し、Amazon S3 がバケットにデータを配置できるようにします。詳細については、「ターゲットバケットポリシーの作成」を参照してください。

10. [頻度] の下で、レポートを生成する頻度として、[毎日] または [毎週] を選択します。

11. [出力形式] で、レポートの形式を以下から 1 つ選択します。

    - CSV — このインベントリレポートを S3 バッチオペレーションで使用するか、このレポートを Microsoft Excel などの別のツールで分析する場合は、[CSV] を選択します。
    - Apache ORC
    - Apache Parquet

12. [ステータス] の下で、[有効化] または [無効化] を選択します。

13. サーバー側の暗号化を設定するには、[インベントリ レポートの暗号化] で次の手順に従います。

    a. [サーバー側の暗号化] で、[暗号化キーを指定しない] または [暗号化キーを指定する] を選択してデータを暗号化します。

       - Amazon S3 にオブジェクトを格納するときに、バケット設定をデフォルトのサーバー側暗号化のままにするには、[暗号化キーを指定しない] を選択します。送信先バケットで S3 バケットキーが有効になっている限り、コピーオペレーションは送信先バケットに S3 バケットキーを適用します。

> **Note**
>
> 指定された宛先のバケットポリシーで、Amazon S3 に保存する前にオブジェクトを暗号化する必要がある場合は、[暗号化キーを指定する] を選択する必要があります。そうしないと、宛先へのオブジェクトのコピーが失敗します。

- オブジェクトを Amazon S3 に保存する前に暗号化するには、[暗号化キーを指定する] を選択します。

b. [暗号化キーを指定する] を選択した場合は、[暗号化タイプ] で [Amazon S3 マネージドキー (SSE-S3)] または [AWS Key Management Service キー (SSE-KMS)] を選択する必要があります。

SSE-S3 は、最強のブロック暗号の 1 つである 256 ビットの 高度暗号化規格 (AES-256) を使用して、各オブジェクトを暗号化します。SSE-KMS を使用すると、キーをより細かく制御できます。SSE-KMS に関する詳細は、「Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3)」を参照してください。SSE-KMS に関する詳細は、「AWS KMS キーによるサーバー側の暗号化 (SSE-KMS) の使用」を参照してください。

> **Note**
>
> SSE-KMS を使用してインベントリリストファイルを暗号化するには、カスタマーマネージドキーを使用するためのアクセス許可を Amazon S3 に付与する必要があります。手順については、「KMS キーを使用した暗号化のための Amazon S3 への許可の付与」を参照してください。

c. [AWS Key Management Service キー (SSE-KMS)] を選択した場合は、AWS KMS key で、以下のオプションのいずれかを使用して AWS KMS キーを指定できます。

> **Note**
>
> インベントリリストファイルを保存する送信先バケットが別の AWS アカウント によって所有されている場合は、完全修飾 KMS キー ARN を使用して KMS キーを指定するようにしてください。

- 使用可能な KMS キーのリストから選択するには、[AWS KMS キーから選択する] を選択し、使用可能なキーのリストから対称暗号化 KMS キーを選択します。KMS キーがバケットと同じリージョンにあることを確認します。

> **Note**
>
> AWS マネージドキー (aws/s3) とカスタマーマネージドキーの両方がリストに表示されます。ただし、AWS マネージドキー (aws/s3) は S3 インベントリでの SSE-KMS 暗号化には対応していません。

- KMS キー ARN を入力するには、[AWS KMS キー ARN を入力] を選択し、表示されるフィールドに KMS キー ARN を入力します。
- AWS KMS コンソールで新しいカスタマーマネージドキーを作成するには、[KMS キーを作成] を選択します。

14. [追加のメタデータフィールド] で、インベントリレポートに追加するフィールドを以下から 1 つ以上選択します。

- サイズ - バイト単位のオブジェクトサイズ。不完全なマルチパートアップロード、オブジェクトメタデータ、削除マーカーのサイズは含まれません。
- 最終更新日 – オブジェクトの作成日または最終更新日のどちらか新しい方。
- [マルチパートアップロード] – オブジェクトがマルチパートアップロードとしてアップロードされたことを指定します。詳細については、「Amazon S3 でのマルチパートアップロードを使用したオブジェクトのアップロードとコピー」を参照してください。
- [レプリケーションステータス] – オブジェクトのレプリケーションステータス。詳細については、「レプリケーションステータス情報の取得」を参照してください。
- 暗号化ステータス – オブジェクトの暗号化に使用するサーバー側の暗号化タイプ。詳細については、「サーバー側の暗号化によるデータの保護」を参照してください。
- バケットキーのステータス — AWS KMS で生成したバケットレベルのキーをオブジェクトに適用するかどうかを示します。詳細については、「Amazon S3 バケットキーを使用した SSE-KMS のコストの削減」を参照してください。
- オブジェクトアクセスコントロールリスト — このオブジェクトへのアクセスを許可する AWS アカウントまたはグループと、許可するアクセスのタイプを定義するオブジェクトごとのアクセスコントロールリスト (ACL)。このフィールドの詳細については、「オブジェク

ト ACL フィールドの使用」を参照してください。ACL の詳細については、「アクセスコントロールリスト (ACL) の概要」を参照してください。

- オブジェクト所有者 — オブジェクトの所有者。
- ストレージクラス – オブジェクトの保存に使用するストレージクラス。
- インテリジェントな階層化: アクセス階層 – S3 Intelligent-Tiering ストレージクラスがオブジェクトの保存先である場合、オブジェクトのアクセス階層 (高頻度または低頻度) を示します。詳細については、「アクセスパターンが変化する、またはアクセスパターンが不明なデータを、自動的に最適化するためのストレージクラス」を参照してください。
- ETag – エンティティタグ (ETag) は、オブジェクトのハッシュです。ETag は、変更をオブジェクトのコンテンツにのみ反映し、そのメタデータには反映しません。ETag は、オブジェクトデータの MD5 ダイジェストである場合と、そうでない場合があります。どちらであるかは、オブジェクトの作成方法と暗号化方法によって決まります。詳細については、「Amazon Simple Storage Service API リファレンス」の「Object」を参照してください。
- チェックサムアルゴリズム — オブジェクトのチェックサムを作成するために使用されるアルゴリズムを示します。詳細については、「サポートされているチェックサムアルゴリズムの使用」を参照してください。
- [すべてのオブジェクトロック設定] – オブジェクトのオブジェクトロックステータス (以下の設定が含まれます)。
  - オブジェクトロック: 保持モード – オブジェクトに適用される保護のレベル ([ガバナンス] または [コンプライアンス])。
  - オブジェクトロック: 日付までの保持期限 – ロックされたオブジェクトを削除できなくなる日付。
  - [オブジェクトロック: リーガルホールドステータス] – ロックされたオブジェクトのリーガルホールドステータス。

  S3 オブジェクトロックの詳細については、「S3 オブジェクトロックの仕組み」を参照してください。

インベントリレポートの内容の詳細については、「Amazon S3 インベントリのリスト」を参照してください。

インベントリ設定の特定のオプションのメタデータフィールドへのアクセスを制限する方法についての詳細は、「S3 インベントリレポート設定の作成を制御する」を参照してください。

15. [作成] を選択します。

REST API を使用して S3 インベントリを操作する

次に示すのは、Amazon S3 インベントリの操作に使用できる REST オペレーションです。

- DeleteBucketInventoryConfiguration
- GetBucketInventoryConfiguration
- ListBucketInventoryConfigurations
- PutBucketInventoryConfiguration

インベントリリストの検索

インベントリリストが発行されると、マニフェストファイルは保存先バケットの次の場所に発行されます。

```
destination-prefix/amzn-s3-demo-source-bucket/config-ID/YYYY-MM-DDTHH-MMZ/manifest.json
 destination-prefix/amzn-s3-demo-source-bucket/config-ID/YYYY-MM-DDTHH-MMZ/
manifest.checksum
 destination-prefix/amzn-s3-demo-source-bucket/config-ID/hive/dt=YYYY-MM-DD-HH-MM/
symlink.txt
```

- *destination-prefix* は、インベントリ設定でオプションで指定するオブジェクトキー名プレフィックスです。このプレフィックスを使用して、保存先バケット内の共通の場所に、すべてのインベントリリストファイルをグループ化できます。
- *amzn-s3-demo-source-bucket* は、インベントリリストの対象であるソースバケットです。複数の異なるソースバケットから複数のインベントリレポートが同じ保存先バケットに送信されたときの競合を避けるには、ソースバケット名を追加します。
- 同じソースバケットから同じ保存先バケットに複数のインベントリレポートが送信されたときの競合を避けるには、*config-ID* を追加します。*config-ID* は、インベントリレポートの設定から取得されるため、設定時に定義したレポートの名前になります。
- *YYYY-MM-DDTHH-MMZ* は、インベントリのレポート生成プロセスでバケットのスキャンを開始した日時を示すタイムスタンプです (例: 2016-11-06T21-32Z)。
- `manifest.json` はマニフェストファイルです。
- `manifest.checksum` は、`manifest.json` ファイルのコンテンツの MD5 ハッシュです。
- `symlink.txt` は Apache Hive 互換のマニフェストファイルです。

インベントリリストは、保存先バケットの次の場所に、毎日または毎週発行されます。

```
destination-prefix/amzn-s3-demo-source-bucket/config-ID/data/example-file-name.csv.gz
...
destination-prefix/amzn-s3-demo-source-bucket/config-ID/data/example-file-name-1.csv.gz
```

- *destination-prefix* は、インベントリ設定でオプションで指定するオブジェクトキー名プレフィックスです。このプレフィックスを使用して、保存先バケットの共通の場所にすべてのインベントリリストファイルをグループ化できます。
- *amzn-s3-demo-source-bucket* は、インベントリリストの対象であるソースバケットです。複数の異なるソースバケットから複数のインベントリレポートが同じ保存先バケットに送信されたときの競合を避けるには、ソースバケット名を追加します。
- *example-file-name*.csv.gz は、CSV インベントリファイルの 1 つです。ORC インベントリ名はファイル名拡張子 .orc で終わり、Parquet インベントリ名はファイル名拡張子 .parquet で終わります。

インベントリマニフェスト

マニフェストファイルの manifest.json と symlink.txt は、インベントリファイルの場所を記述します。新しいインベントリリストが配信されるたびに、新しいセットのマニフェストファイルが作成されます。これらのファイルは互いに上書きされる可能性があります。バージョニングが有効なバケットには、Amazon S3 はマニフェストファイルの新しいバージョンを作成します。

manifest.json ファイルに含まれる各マニフェストには、メタデータおよびその他のインベントリに関する基本的な情報が記載されています。この情報には以下が含まれます。

- ソースバケット名
- 保存先バケット名
- インベントリのバージョン
- インベントリのレポート生成プロセスでバケットのスキャンを開始した日時をエポック日付形式で示す、作成タイムスタンプ
- インベントリファイルの形式とスキーマ
- 保存先バケット内に存在するインベントリファイルのリスト

manifest.json ファイルを書き込むたびに、manifest.checksum ファイルのコンテンツの MD5 ハッシュとして manifest.json ファイルが添付されます。

Example **manifest.json** ファイル内のインベントリマニフェスト

manifest.json ファイルに含まれる、CSV、ORC、Parquet 形式インベントリ用のインベントリマニフェストの例を以下に示します。

CSV

CSV 形式のインベントリの manifest.json ファイルに含まれるマニフェストの例を次に示します。

```
{
    "sourceBucket": "amzn-s3-demo-source-bucket",
    "destinationBucket": "arn:aws:s3:::example-inventory-destination-bucket",
    "version": "2016-11-30",
    "creationTimestamp" : "1514944800000",
    "fileFormat": "CSV",
    "fileSchema": "Bucket, Key, VersionId, IsLatest, IsDeleteMarker,
 Size, LastModifiedDate, ETag, StorageClass, IsMultipartUploaded,
 ReplicationStatus, EncryptionStatus, ObjectLockRetainUntilDate, ObjectLockMode,
 ObjectLockLegalHoldStatus, IntelligentTieringAccessTier, BucketKeyStatus,
 ChecksumAlgorithm, ObjectAccessControlList, ObjectOwner",
    "files": [
        {
            "key": "Inventory/amzn-s3-demo-source-bucket/2016-11-06T21-32Z/
files/939c6d46-85a9-4ba8-87bd-9db705a579ce.csv.gz",
            "size": 2147483647,
            "MD5checksum": "f11166069f1990abeb9c97ace9cdfabc"
        }
    ]
}
```

ORC

ORC 形式のインベントリの manifest.json ファイルに含まれるマニフェストの例を次に示します。

```
{
    "sourceBucket": "amzn-s3-demo-source-bucket",
    "destinationBucket": "arn:aws:s3:::example-destination-bucket",
    "version": "2016-11-30",
    "creationTimestamp" : "1514944800000",
    "fileFormat": "ORC",
```

```
    "fileSchema":
 "struct<bucket:string,key:string,version_id:string,is_latest:boolean,is_delete_marker:boole
    "files": [
        {
            "key": "inventory/amzn-s3-demo-source-bucket/data/
d794c570-95bb-4271-9128-26023c8b4900.orc",
            "size": 56291,
            "MD5checksum": "5925f4e78e1695c2d020b9f6eexample"
        }
    ]
}
```

Parquet

manifest.json ファイルに含まれる Parquet 形式のインベントリ用のマニフェストの例を次に示します。

```
{
    "sourceBucket": "amzn-s3-demo-source-bucket",
    "destinationBucket": "arn:aws:s3:::example-destination-bucket",
    "version": "2016-11-30",
    "creationTimestamp" : "1514944800000",
    "fileFormat": "Parquet",
    "fileSchema": "message s3.inventory { required binary bucket (UTF8);
 required binary key (UTF8); optional binary version_id (UTF8); optional boolean
 is_latest; optional boolean is_delete_marker; optional int64 size; optional
 int64 last_modified_date (TIMESTAMP_MILLIS); optional binary e_tag (UTF8);
 optional binary storage_class (UTF8); optional boolean is_multipart_uploaded;
 optional binary replication_status (UTF8); optional binary encryption_status
 (UTF8); optional int64 object_lock_retain_until_date (TIMESTAMP_MILLIS); optional
 binary object_lock_mode (UTF8); optional binary object_lock_legal_hold_status
 (UTF8); optional binary intelligent_tiering_access_tier (UTF8); optional binary
 bucket_key_status (UTF8); optional binary checksum_algorithm (UTF8); optional
 binary object_access_control_list (UTF8); optional binary object_owner (UTF8);}",
    "files": [
        {
           "key": "inventory/amzn-s3-demo-source-bucket/data/
d754c470-85bb-4255-9218-47023c8b4910.parquet",
            "size": 56291,
            "MD5checksum": "5825f2e18e1695c2d030b9f6eexample"
        }
    ]
}
```

symlink.txt ファイルは、Hive がインベントリファイルおよび関連データファイルを自動的に検出できるようにする Apache Hive 互換のマニフェストファイルです。Hive 互換のマニフェストは、Athena や Amazon Redshift Spectrum など、Hive 互換のサービスで動作します。また、Presto、Apache Hive、Apache Spark など、多くの Hive 互換のアプリケーションでも動作します。

> **Important**
>
> symlink.txt Apache Hive 互換のマニフェストファイルは現在、AWS Glue では動作しません。
> Apache Hive および Apache Spark による symlink.txt ファイルの読み取りは、ORC 形式および Parquet 形式のインベントリファイルではサポートされていません。

インベントリ完了に関する Amazon S3 イベント通知の設定

マニフェストチェックサムファイルが作成されたら通知を受け取るように、Amazon S3 イベント通知をセットアップできます。これは、インベントリリストが保存先バケットに追加されたことを示します。マニフェストは、保存先の場所にあるすべてのインベントリリストの最新のリストです。

Amazon S3 は、Amazon Simple Notification Service (Amazon SNS) トピック、Amazon Simple Queue Service (Amazon SQS) キュー、または AWS Lambda 関数にイベントを発行できます。詳細については、「Amazon S3 イベント通知」を参照してください。

次の通知設定は、保存先バケットに新しく追加されるすべての manifest.checksum ファイルが AWS Lambda cloud-function-list-write によって処理されることを定義します。

```
<NotificationConfiguration>
  <QueueConfiguration>
      <Id>1</Id>
      <Filter>
          <S3Key>
              <FilterRule>
                  <Name>prefix</Name>
                  <Value>destination-prefix/source-bucket</Value>
              </FilterRule>
              <FilterRule>
                  <Name>suffix</Name>
                  <Value>checksum</Value>
              </FilterRule>
          </S3Key>
```

```
      </Filter>
      <CloudFunction>arn:aws:lambda:us-west-2:222233334444:cloud-function-list-write</
CloudFunction>
      <Event>s3:ObjectCreated:*</Event>
    </QueueConfiguration>
    </NotificationConfiguration>
```

詳細については、AWS Lambda デベロッパーガイドの Amazon S3 で AWS Lambda を使用するを参照してください。

Amazon Athena で Amazon S3 インベントリをクエリする

Athena を使用できるすべてのリージョンで、Amazon Athena で標準 SQL クエリを実行し、Amazon S3 インベントリのファイルをクエリできます。使用可能な AWS リージョン を確認するには、AWS リージョン 表を参照してください。

Athena は、Apache Optimized Row Columnar (ORC)、Apache Parquet、またはカンマ区切りの値 (CSV) 形式で Amazon S3 インベントリファイルをクエリできます。Athena を使用してインベントリファイルをクエリする場合は、ORC 形式または Parquet 形式のインベントリファイルを使用することをお勧めします。ORC 形式および Parquet 形式は、より高速なクエリパフォーマンスとより低いクエリコストを提供します。ORC および Parquet は、Apache Hadoop 向けに設計された自己記述型、型認識型の列指向ファイル形式です。列形式の場合、リーダーは現在のクエリに必要な列だけを読み取り、圧縮解除し、処理することができます。Amazon S3 インベントリの ORC 形式および Parquet 形式は、すべての AWS リージョンで使用できます。

Athena を使用して Amazon S3 インベントリファイルをクエリするには

1. Athena テーブルを作成します。テーブルの作成の詳細については、Amazon Athena ユーザーガイドの「 Amazon Athena でのテーブルの作成 」を参照してください。
2. クエリ対象のインベントリレポートが ORC 形式、Parquet 形式、CSV 形式のいずれであるかによって、以下のサンプルクエリテンプレートのいずれかを使用してクエリを作成します。

   - Athena を使用して ORC 形式のインベントリレポートをクエリするときは、次のサンプルクエリをテンプレートとして使用します。

     次のサンプルクエリには、ORC 形式のインベントリレポートのすべてのオプションフィールドが含まれています。

     このサンプルクエリを使用するには、以下を実行します。

     - *your_table_name* を、作成した Athena テーブルの名前に置き換えます。

- インベントリ用に選択しなかったすべてのオプションフィールドを削除し、クエリとインベントリ用に選択したフィールドを対応させます。
- 設定に応じて、次のバケット名とインベントリの場所 (設定 ID) を置き換えます。

  s3://*amzn-s3-demo-bucket*/*config-ID*/hive/

- projection.dt.range の *2022-01-01-00-00* 日付を、Athena でデータをパーティション化する時間範囲の最初の日に置き換えます。詳細については、「Athena でのデータのパーティション化」を参照してください。

```
CREATE EXTERNAL TABLE your_table_name(
         bucket string,
         key string,
         version_id string,
         is_latest boolean,
         is_delete_marker boolean,
         size bigint,
         last_modified_date timestamp,
         e_tag string,
         storage_class string,
         is_multipart_uploaded boolean,
         replication_status string,
         encryption_status string,
         object_lock_retain_until_date bigint,
         object_lock_mode string,
         object_lock_legal_hold_status string,
         intelligent_tiering_access_tier string,
         bucket_key_status string,
         checksum_algorithm string,
         object_access_control_list string,
         object_owner string
) PARTITIONED BY (
        dt string
)
ROW FORMAT SERDE 'org.apache.hadoop.hive.ql.io.orc.OrcSerde'
  STORED AS INPUTFORMAT 'org.apache.hadoop.hive.ql.io.SymlinkTextInputFormat'
  OUTPUTFORMAT 'org.apache.hadoop.hive.ql.io.IgnoreKeyTextOutputFormat'
  LOCATION 's3://source-bucket/config-ID/hive/'
  TBLPROPERTIES (
    "projection.enabled" = "true",
    "projection.dt.type" = "date",
    "projection.dt.format" = "yyyy-MM-dd-HH-mm",
    "projection.dt.range" = "2022-01-01-00-00,NOW",
```

```
    "projection.dt.interval" = "1",
    "projection.dt.interval.unit" = "HOURS"
  );
```

- Athena を使用して Parquet 形式のインベントリレポートをクエリする場合は、ORC 形式のレポートでサンプルクエリを使用します。ただし、`ROW FORMAT SERDE` ステートメントで ORC SerDe の代わりに次の Parquet SerDe を使用します。

```
ROW FORMAT SERDE 'org.apache.hadoop.hive.ql.io.parquet.serde.ParquetHiveSerDe'
```

- Athena を使用して CSV 形式のインベントリレポートをクエリするときは、次のサンプルクエリをテンプレートとして使用します。

  次のサンプルクエリには、CSV 形式のインベントリレポートのすべてのオプションフィールドが含まれています。

  このサンプルクエリを使用するには、以下を実行します。

  - *your_table_name* を、作成した Athena テーブルの名前に置き換えます。
  - インベントリ用に選択しなかったすべてのオプションフィールドを削除し、クエリとインベントリ用に選択したフィールドを対応させます。
  - 設定に応じて、次のバケット名とインベントリの場所 (設定 ID) を置き換えます。

    s3://*amzn-s3-demo-bucket*/*config-ID*/hive/

  - `projection.dt.range` の *2022-01-01-00-00* 日付を、Athena でデータをパーティション化する時間範囲の最初の日に置き換えます。詳細については、「Athena でのデータのパーティション化」を参照してください。

```
CREATE EXTERNAL TABLE your_table_name(
         bucket string,
         key string,
         version_id string,
         is_latest boolean,
         is_delete_marker boolean,
         size string,
         last_modified_date string,
         e_tag string,
         storage_class string,
         is_multipart_uploaded boolean,
         replication_status string,
         encryption_status string,
```

```
         object_lock_retain_until_date string,
         object_lock_mode string,
         object_lock_legal_hold_status string,
         intelligent_tiering_access_tier string,
         bucket_key_status string,
         checksum_algorithm string,
         object_access_control_list string,
         object_owner string
) PARTITIONED BY (
        dt string
)
ROW FORMAT SERDE 'org.apache.hadoop.hive.serde2.OpenCSVSerde'
  STORED AS INPUTFORMAT 'org.apache.hadoop.hive.ql.io.SymlinkTextInputFormat'
  OUTPUTFORMAT 'org.apache.hadoop.hive.ql.io.IgnoreKeyTextOutputFormat'
  LOCATION 's3://source-bucket/config-ID/hive/'
  TBLPROPERTIES (
    "projection.enabled" = "true",
    "projection.dt.type" = "date",
    "projection.dt.format" = "yyyy-MM-dd-HH-mm",
    "projection.dt.range" = "2022-01-01-00-00,NOW",
    "projection.dt.interval" = "1",
    "projection.dt.interval.unit" = "HOURS"
  );
```

3. 以下の例に示すように、インベントリに対してさまざまなクエリを実行できるようになりました。*user input placeholder* を、ユーザー自身の情報に置き換えます。

```
# Get a list of the latest inventory report dates available.
SELECT DISTINCT dt FROM your_table_name ORDER BY 1 DESC limit 10;

# Get the encryption status for a provided report date.
SELECT encryption_status, count(*) FROM your_table_name WHERE dt = 'YYYY-MM-DD-HH-
MM' GROUP BY encryption_status;

# Get the encryption status for inventory report dates in the provided range.
SELECT dt, encryption_status, count(*) FROM your_table_name
WHERE dt > 'YYYY-MM-DD-HH-MM' AND dt < 'YYYY-MM-DD-HH-MM' GROUP BY dt,
 encryption_status;
```

オブジェクトアクセスコントロールリスト (オブジェクト ACL) フィールドをインベントリレポートに追加するように S3 インベントリを設定すると、レポートにはオブジェクト ACL フィールドの値が base64 エンコードされた文字列として表示されます。オブジェクト ACL

フィールドのデコードされた値を JSON で取得するには、Athena を使用してこのフィールドをクエリできます。以下のクエリの例を参照してください。オブジェクト ACL フィールドの詳細については、「オブジェクト ACL フィールドの使用」を参照してください。

```
# Get the S3 keys that have Object ACL grants with public access.
WITH grants AS (
    SELECT key,
        CAST(
            json_extract(from_utf8(from_base64(object_access_control_list)),
 '$.grants') AS ARRAY(MAP(VARCHAR, VARCHAR))
        ) AS grants_array
    FROM your_table_name
)
SELECT key,
       grants_array,
       grant
FROM grants, UNNEST(grants_array) AS t(grant)
WHERE element_at(grant, 'uri') = 'http://acs.amazonaws.com/groups/global/AllUsers'
```

```
# Get the S3 keys that have Object ACL grantees in addition to the object owner.
WITH grants AS
    (SELECT key,
    from_utf8(from_base64(object_access_control_list)) AS
 object_access_control_list,
         object_owner,
         CAST(json_extract(from_utf8(from_base64(object_access_control_list)),
         '$.grants') AS ARRAY(MAP(VARCHAR, VARCHAR))) AS grants_array
    FROM your_table_name)
SELECT key,
       grant,
       objectowner
FROM grants, UNNEST(grants_array) AS t(grant)
WHERE cardinality(grants_array) > 1 AND element_at(grant, 'canonicalId') !=
 object_owner;
```

```
# Get the S3 keys with READ permission that is granted in the Object ACL.
WITH grants AS (
    SELECT key,
        CAST(
```

```
            json_extract(from_utf8(from_base64(object_access_control_list)),
 '$.grants') AS ARRAY(MAP(VARCHAR, VARCHAR))
        ) AS grants_array
    FROM your_table_name
)
SELECT key,
       grants_array,
       grant
FROM grants, UNNEST(grants_array) AS t(grant)
WHERE element_at(grant, 'permission') = 'READ';
```

```
# Get the S3 keys that have Object ACL grants to a specific canonical user ID.
WITH grants AS (
    SELECT key,
        CAST(
            json_extract(from_utf8(from_base64(object_access_control_list)),
 '$.grants') AS ARRAY(MAP(VARCHAR, VARCHAR))
        ) AS grants_array
    FROM your_table_name
)
SELECT key,
       grants_array,
       grant
FROM grants, UNNEST(grants_array) AS t(grant)
WHERE element_at(grant, 'canonicalId') = 'user-canonical-id';
```

```
# Get the number of grantees on the Object ACL.
SELECT key,
       object_access_control_list,
       json_array_length(json_extract(object_access_control_list,'$.grants')) AS
 grants_count
FROM your_table_name;
```

Athena の詳しい使用方法については、「Amazon Athena ユーザーガイド」を参照してください。

Amazon S3 インベントリレポートの空のバージョン ID 文字列を NULL 文字列に変換します。

> **Note**
>
> 以下の手順は、すべてのバージョンを含む Amazon S3 インベントリレポートにのみ適用されます。また、「すべてのバージョン」レポートが S3 バージョニングが有効になっているバケットの S3 バッチオペレーションのマニフェストとして使用される場合に限ります。現在のバージョンのみを指定する S3 インベントリレポートの文字列を変換する必要もありません。

S3 インベントリレポートは、S3 バッチ操作のマニフェストとして使用できます。ただし、バケットで S3 バージョニングが有効になっている場合、すべてのバージョンを含む S3 インベントリレポートはバージョン ID フィールドに空の文字列で NULL バージョン対応オブジェクトをマークします。インベントリレポートにすべてのオブジェクトバージョン ID が含まれる場合、バッチ操作は `null` 文字列をバージョン ID として使用しますが、空の文字列ではありません。

S3 バッチ操作ジョブが「すべてのバージョン」S3 インベントリレポートをマニフェストとして使用すると、バージョン ID フィールドに空の文字列を含むオブジェクトのすべてのタスクが失敗します。S3 インベントリレポートのバージョン ID フィールドの空文字列をバッチ操作用の `null` 文字列に変換するには、次の手順を使用します。

バッチ操作で使用するために Amazon S3 インベントリレポートを更新します。

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. S3 インベントリレポートに移動します。インベントリレポートの構成中に指定した宛先バケットにインベントリレポートを配置します。インベントリレポートの場所の詳細については、インベントリリストの検索 を参照してください。
   a. 宛先バケットを選択します。
   b. フォルダを選択します。フォルダの名前は、元のソースバケットにちなんで付けられます。
   c. インベントリ設定の名前が付いたフォルダを選択します。
   d. hive という名前のフォルダの横にあるチェックボックスを選択します。ページの上部で、[S3 URI をコピーする] を選択し、フォルダの S3 URI をコピーします。
3. https://console.aws.amazon.com/athena/ で Amazon Athena コンソールを開きます。

4. クエリエディタで、[設定] を選択し、[管理] を選択します。リポジトリの [設定の管理] ページのクエリ結果の場所 で、クエリ結果を保存する S3 バケットを選択します。
5. クエリエディタで、次のコマンドを使用して、インベントリレポートのデータを保持する Athena テーブルを作成します。任意の名前 *table_name* に置き換え、LOCATION 節に、以前にコピーした S3 URI を挿入します。その後、[Run] を選択してクエリを実行します。

```
CREATE EXTERNAL TABLE table_name(bucket string, key string,
 version_id string) PARTITIONED BY (dt string)ROW FORMAT SERDE
 'org.apache.hadoop.hive.serde2.OpenCSVSerde'STORED AS INPUTFORMAT
 'org.apache.hadoop.hive.ql.io.SymlinkTextInputFormat' OUTPUTFORMAT
 'org.apache.hadoop.hive.ql.io.IgnoreKeyTextOutputFormat' LOCATION 'Copied S3 URI';
```

6. クエリエディタをクリアするには、[Clear] を選択します。次のコマンドを使用して、インベントリレポートをテーブルにロードします。前のステップで選択したもの *table_name* に置き換えてください。その後、[Run] を選択してクエリを実行します。

```
MSCK REPAIR TABLE table_name;
```

7. クエリエディタをクリアするには、[Clear] を選択します。以下の SELECT クエリを実行して、元のインベントリレポートのすべてのエントリを取得し、空のバージョン ID を null 文字列に置き換えます。先に選択したもの *table_name* に置き換え、節内 *YYYY-MM-DD-HH-MM* をこのツールを実行させたいインベントリー・レポートの日付 WHERE に置き換えます。次に [Run] を選択して、クエリを実行します。

```
SELECT bucket as Bucket, key as Key, CASE WHEN version_id = '' THEN 'null' ELSE
 version_id END as VersionId FROM table_name WHERE dt = 'YYYY-MM-DD-HH-MM';
```

8. Amazon S3コンソール (https://console.aws.amazon.com/s3/) に戻り、先ほど クエリ結果の場所 として選択した S3 バケットに移動します。内部には、日付で終わる一連のフォルダがあるはずです。

   例えば、s3://***amzn-s3-demo-bucket***/***query-result-location***/Unsaved/2021/10/07/ のようなものがあるはずです。実行した .csv クエリの結果を含む SELECT ファイルが表示されるはずです。

   最新の更新日の CSV ファイルを選択してください。次のステップのために、このファイルをローカル・マシンにダウンロードします。

9. 生成された CSV ファイルには、ヘッダー行が含まれています。この CSV ファイルを S3 バッチ操作ジョブの入力として使用するには、ヘッダー行を削除する必要があります。これは、バッチ操作では CSV マニフェストのヘッダー行をサポートしないためです。

   ヘッダー行を削除するには、ファイルで次のいずれかのコマンドを実行します。*file.csv* を CSV ファイルの名前に置き換えてください。

   macOS および Linux マシンの場合、ターミナル ウィンドウで `tail` コマンドを実行します。

   ```
   tail -n +2 file.csv > tmp.csv && mv tmp.csv file.csv
   ```

   Windows マシンの場合、Windows PowerShell ウィンドウで次のスクリプトを実行します。*File-location* をファイルへのパスに置き換え、*file.csv* をファイルに置き換えます。

   ```
   $ins = New-Object System.IO.StreamReader File-location\file.csv
   $outs = New-Object System.IO.StreamWriter File-location\temp.csv
   try {
       $skip = 0
       while ( !$ins.EndOfStream ) {
           $line = $ins.ReadLine();
           if ( $skip -ne 0 ) {
               $outs.WriteLine($line);
           } else {
               $skip = 1
           }
       }
   } finally {
       $outs.Close();
       $ins.Close();
   }
   Move-Item File-location\temp.csv File-location\file.csv -Force
   ```

10. CSV ファイルからヘッダー行を削除したら、S3 バッチ操作ジョブのマニフェストとして使用する準備が整いました。CSV ファイルを S3 バケットまたは任意の場所にアップロードし、CSV ファイルをマニフェストとして使用して バッチ操作ジョブを作成します。

    バッチ操作のジョブの作成の詳細については、S3 バッチオペレーションジョブの作成 を参照してください。

オブジェクト ACL フィールドの使用

Amazon S3 インベントリレポートは、S3 ソースバケット内のオブジェクトのリストと、各オブジェクトのメタデータを表示します。オブジェクトアクセスコントロールリスト (ACL) フィールドは、Amazon S3 インベントリで使用できるメタデータフィールドです。オブジェクト ACL フィールドは、特に各オブジェクトのアクセスコントロールリスト (ACL) を示します。オブジェクトの ACL は、このオブジェクトへのアクセスを許可する AWS アカウントまたはグループと、付与するアクセスの種類を定義します。詳細については、「アクセスコントロールリスト (ACL) の概要」および「Amazon S3 インベントリのリスト」を参照してください。

Amazon S3 インベントリレポートのオブジェクト ACL フィールドは、JSON 形式で定義します。JSON データには、以下のデータが含まれます。

- `version` — インベントリレポートのオブジェクト ACL フィールド形式のバージョン。バージョンは日付形式 `yyyy-mm-dd` となります。
- `status` — 指定できる値は `AVAILABLE` または `UNAVAILABLE` です。オブジェクトでオブジェクト ACL が使用できるかどうかを示します。オブジェクト ACL のステータスが `UNAVAILABLE` である場合、インベントリレポートのオブジェクト所有者フィールドの値も `UNAVAILABLE` になります。
- `grants` — 被付与者とアクセス許可のペア。オブジェクト ACL から付与された被付与者ごとのアクセス許可のステータスを示します。被付与者に設定できる値は `CanonicalUser` および `Group` です。被付与者の詳細については、「アクセスコントロールリストの被付与者」を参照してください。

  `Group` タイプの被付与者の場合、付与者とアクセス許可のペアには以下の属性が含まれます。

  - `uri` — 事前定義された Amazon S3 グループ。
  - `permission` — オブジェクトに付与される ACL アクセス許可。詳細については、「オブジェクトに対する ACL アクセス許可」を参照してください。
  - `type` — タイプ `Group`。これは被付与者がグループであることを示します。

  `CanonicalUser` タイプの被付与者の場合、付与者とアクセス許可のペアには以下の属性が含まれます。

  - `canonicalId` — 難読化された形式の AWS アカウント ID。AWS アカウント の正規ユーザー ID は、そのアカウントに固有です。正規ユーザー ID を取得できます。詳細については、「AWS Account Management リファレンスガイド」の「AWS アカウント の正規ユーザー ID を検索する」を参照してください。

> **Note**
>
> ACL の被付与者が AWS アカウントの E メールアドレスである場合、S3 インベントリは、その AWS アカウントの canonicalId と CanonicalUser タイプを使用してこの被付与者を指定します。詳細については、「アクセスコントロールリストの被付与者」を参照してください。

- permission — オブジェクトに付与される ACL アクセス許可。詳細については、「オブジェクト対する ACL アクセス許可」を参照してください。
- type — タイプ CanonicalUser。これは、被付与者が AWS アカウントであることを示します。

次の例は、JSON 形式のオブジェクト ACL フィールドに指定できる値を示しています。

```
{
    "version": "2022-11-10",
    "status": "AVAILABLE",
    "grants": [{
        "uri": "http://acs.amazonaws.com/groups/global/AllUsers",
        "permission": "READ",
        "type": "Group"
    }, {
        "canonicalId": "example-canonical-id",
        "permission": "FULL_CONTROL",
        "type": "CanonicalUser"
    }]
}
```

> **Note**
>
> オブジェクト ACL フィールドは JSON 形式で定義されます。インベントリレポートには、オブジェクト ACL フィールドの値が base64 エンコードされた文字列として表示されます。例えば、次のオブジェクト ACL フィールドが JSON 形式で存在するとします。
>
> ```
> {
>         "version": "2022-11-10",
>         "status": "AVAILABLE",
>         "grants": [{
>             "canonicalId": "example-canonical-user-ID",
> ```

```
            "type": "CanonicalUser",
            "permission": "READ"
        }]
}
```

オブジェクト ACL フィールドはエンコードされ、次の base64 エンコードされた文字列として表示されます。

```
eyJ2ZXJzaW9uIjoiMjAyMi0xMS0xMCIsInN0YXR1cyI6IkFWQUlMQUJMRSIsImdyYW50cyI6W3siY2Fub25pY2FsSW
```

オブジェクト ACL フィールドのデコードされた値を JSON で取得するには、Amazon Athena でこのフィールドをクエリできます。クエリの例については、「Amazon Athena で Amazon S3 インベントリをクエリする」を参照してください。

設計パターンのベストプラクティス: Amazon S3 のパフォーマンスの最適化

Amazon S3 のストレージに対してアップロードおよび取得を行う際に、アプリケーションはリクエストのパフォーマンスとして 1 秒あたり数千のトランザクションを容易に達成できます。Amazon S3 は、高いリクエストレートに自動的にスケールされます。例えば、アプリケーションは、パーティショニングされた Amazon S3 プレフィックスごとに毎秒 3,500 回以上の PUT/COPY/POST/DELETE リクエストまたは 5,500 回以上の GET/HEAD リクエストを達成できます。バケット内のプレフィックスの数に制限はありません。並列化を使用することによって、読み取りまたは書き込みのパフォーマンスを向上させることができます。例えば、Amazon S3 バケットに 10 個のプレフィックスを作成して読み取りを並列化すると、読み取りパフォーマンスを 1 秒あたり 55,000 回の読み取りリクエストにスケールできます。同様に、複数のプレフィックスに書き込むことで、書き込みオペレーションをスケールできます。読み取りオペレーションと書き込みオペレーションの両方の場合、スケーリングは徐々に行われ、瞬時には行われません。実際のパフォーマンスは、特定のワークロードの特性、使用パターン、システム設定によって異なります。Amazon S3 が新たに高くなったリクエストレートに合わせてスケーリングしている間に、503 (Slow Down) エラーが表示される場合があります。これらのエラーは、スケーリングが完了すると解消されます。プレフィックスの作成と使用の詳細については、「プレフィックスを使用してオブジェクトを整理する」を参照してください。

Amazon S3 上のデータレイクアプリケーションによっては、ペタバイトを超えるデータに対して実行されるクエリで数百万から数十億のオブジェクトをスキャンします。これらのデータレイクアプリケーションは、Amazon EC2 インスタンスのネットワークインターフェイスの使用を最大限に高めて、単一のインスタンスで最大 100 Gb/s の転送レートを実現しています。その後、これらのアプリケーションは、複数のインスタンスにわたってスループットを集約して 1 秒あたり複数テラバイトを確保します。

ソーシャルメディアメッセージングアプリケーションなどの他のアプリケーションは、レイテンシーの影響を受けやすいアプリケーションです。このようなアプリケーションでは、小さなオブジェクト (大きなオブジェクトの場合は最初のバイトを受け取るまで) のレイテンシーで約 100～200 ミリ秒の一定のレイテンシーを実現できます。

他の AWS のサービスもさまざまなアプリケーションアーキテクチャのパフォーマンスの高速化に役立ちます。例えば、HTTP 接続ごとの転送レートを高めたい場合やレイテンシーをミリ秒単位に抑えたい場合は、Amazon CloudFront または Amazon ElastiCache を Amazon S3 のキャッシュとして使用します。

また、長距離間のクライアントと S3 バケットのデータ転送を高速化する場合は、Amazon S3 Transfer Acceleration を使用した高速かつ安全なファイル転送の設定 を使用します。Transfer Acceleration は、CloudFront の世界中に点在するエッジロケーションを使用して、長距離間のデータ転送を高速化します。Amazon S3 ワークロードが AWS KMS によるサーバー側の暗号化を使用している場合、ユースケースでサポートされるリクエスト率については、『AWS Key Management Service デベロッパーガイド』の「AWS KMS 制限」を参照してください。

以下のトピックでは、Amazon S3 を使用するアプリケーションのパフォーマンスを最適化するためのベストプラクティスガイドラインと設計パターンについて説明します。Amazon S3 のパフォーマンスの最適化に関する最新情報については、「Amazon S3 のパフォーマンスのガイドライン」および「Amazon S3 のパフォーマンスの設計パターン」を参照してください。

> **Note**
>
> Amazon S3 Express One Zone ストレージクラスをディレクトリバケットで使用する方法の詳細については、「S3 Express One Zone」と「ディレクトリバケットの使用」を参照してください。

トピック

- Amazon S3 のパフォーマンスのガイドライン
- Amazon S3 のパフォーマンスの設計パターン

Amazon S3 のパフォーマンスのガイドライン

Amazon S3 に対してオブジェクトのアップロードや取得を行うアプリケーションを作成する場合は、ベストプラクティスガイドラインに従ってパフォーマンスを最適化してください。また、より詳細な「Amazon S3 のパフォーマンスの設計パターン 」も提供しています。

アプリケーションで Amazon S3 の最適なパフォーマンスを得るために、以下のガイドラインを推奨しています。

トピック

- パフォーマンスを測定する
- ストレージ接続を水平にスケールする

- バイト範囲のフェッチを使用する
- レイテンシーの影響を受けやすいアプリケーションのリクエストを再試行する
- 同じ AWS リージョンで Amazon S3 (ストレージ) と Amazon EC2 (コンピューティング) を組み合わせる
- Amazon S3 Transfer Acceleration を使用して距離によるレイテンシーを最小限に抑える
- 最新バージョンの AWS SDK を使用する

パフォーマンスを測定する

パフォーマンスを測定する際、ネットワークスループット、CPU、および DRAM の要件を確認してください。これらのさまざまなリソースの要件の組み合わせに応じて、さまざまな Amazon EC2 インスタンスタイプを評価することをお勧めします。インスタンスタイプの詳細については、「Amazon EC2 ユーザーガイド」の「インスタンスタイプ」を参照してください。

これは、パフォーマンスの測定時に HTTP 分析ツールを使用して DNS ルックアップ時間、レイテンシー、およびデータ転送速度を確認する際にも役立ちます。

パフォーマンス要件を理解し、アプリケーションのパフォーマンスを最適化するために、受け取った 503 エラーレスポンスをモニタリングすることもできます。特定のパフォーマンスメトリクスのモニタリングには、追加費用が発生する場合があります。詳細については、「Amazon S3 の料金」を参照してください。

503 (Slow Down) ステータスエラーレスポンスの数のモニタリング

503 のステータスエラーレスポンス数をモニタリングするには、次のいずれかのオプションを使用できます。

- Amazon S3 に対する Amazon CloudWatch リクエストメトリクスの使用 CloudWatch リクエストメトリクスには、5xx ステータスレスポンスのメトリクスが含まれています。CloudWatch リクエストメトリクスの詳細については、「Amazon CloudWatch によるメトリクスのモニタリング」を参照してください。
- Amazon S3 ストレージレンズの [高度なメトリクス] セクションにある 503 (Service Unavailable) エラー数を使用してください。詳細については、「S3 ストレージレンズのメトリクスを使用してパフォーマンスを改善する」を参照してください。
- Amazon S3 サーバーアクセスロギングの使用 サーバーアクセスログを使用すると、503 (Internal Error) レスポンスを受け取ったすべてのリクエストをフィルタリングして確認できます。Amazon

Athena を使用して、ログを解析することもできます。サーバーアクセスログ記録の詳細については、「サーバーアクセスログによるリクエストのログ記録」を参照してください。

HTTP 503 ステータスエラーコードの数をモニタリングすることで、どのプレフィックス、キー、またはバケットが最もスロットリングリクエストを受け取っているかについて、貴重な分析情報を得られることがよくあります。

ストレージ接続を水平にスケールする

多くの接続間にリクエストを分散することが、パフォーマンスを水平にスケールする一般的な設計パターンです。パフォーマンスの高いアプリケーションを作成するには、Amazon S3 を従来のストレージサーバーのような 1 つのネットワークエンドポイントではなく、非常に大きな分散システムと考えます。最適なパフォーマンスは、複数の同時リクエストを Amazon S3 に発行することで実現できます。これらのリクエストを別々の接続に分散して、Amazon S3 の利用可能な帯域幅を最大化します。Amazon S3 には、バケットへの接続数に制限はありません。

バイト範囲のフェッチを使用する

GetObject リクエストで HTTP ヘッダーの `Range` を使用すると、オブジェクトのバイト範囲をフェッチして指定した部分のみを転送できます。Amazon S3 への同時接続を使用して、同じオブジェクトのさまざまなバイト範囲をフェッチできます。これにより、単一のオブジェクト全体のリクエストに対して高い集約スループットを実現できます。大きなオブジェクトの小さい範囲をフェッチすると、リクエストの中断時にアプリケーションで再試行回数の向上が可能になります。詳細については、「オブジェクトのダウンロード」を参照してください。

バイト範囲リクエストの標準的なサイズは 8 MB または 16 MB です。マルチパートアップロードを使用してオブジェクトを PUT する場合、最適なパフォーマンスのために同じパートサイズで (少なくともパート境界に沿って整列されている) それらのオブジェクトを GET することをお勧めします。GET リクエストは、個々のパートを直接アドレス指定できます (例えば、`GET ? partNumber=N.`)。

レイテンシーの影響を受けやすいアプリケーションのリクエストを再試行する

積極的なタイムアウトと再試行は、一定のレイテンシーの促進に役立ちます。Amazon S3 を大規模に利用している場合、最初のリクエストが遅くても、再試行のリクエストでは別のパスを選択してすぐに成功することがあります。AWS SDK には、特定のアプリケーションの許容値に調整できる設定可能なタイムアウト値と再試行値があります。

同じ AWS リージョンで Amazon S3 (ストレージ) と Amazon EC2 (コンピューティング) を組み合わせる

S3 のバケット名はグローバルに一意ですが、各バケットはバケットの作成時に選択したリージョンに保存されます。バケットの命名ガイドラインの詳細については、「バケットの概要」および「バケットの命名規則」を参照してください。パフォーマンスを最適化するには、可能であれば、同じ AWS リージョン の Amazon EC2 インスタンスからバケットにアクセスすることをお勧めします。これにより、ネットワークレイテンシーとデータ転送費用を低減できます。

データ転送費用の詳細については、「Amazon S3 の料金」を参照してください。

Amazon S3 Transfer Acceleration を使用して距離によるレイテンシーを最小限に抑える

Amazon S3 Transfer Acceleration を使用した高速かつ安全なファイル転送の設定 は、クライアントと S3 のバケットの長距離間の高速、簡単、安全なファイル転送を管理します。Transfer Acceleration は、Amazon CloudFront の世界中に点在するエッジロケーションを利用します。エッジロケーションに到着したデータは、最適化されたネットワークパスで Amazon S3 にルーティングされます。Transfer Acceleration は、大陸間で定期的にギガバイトからテラバイト単位のデータを転送するのに最適です。また、中央のバケットに対して世界中のお客様からアップロードが行われるクライアントにも役立ちます。

Amazon S3 Transfer Acceleration の速度比較ツールを使用すると、高速化した場合と高速化していない場合の Amazon S3 リージョン間でのアップロード速度を比較できます。速度比較ツールでは、マルチパートアップロードを使用して、ブラウザからさまざまな Amazon S3 のリージョンへのファイル転送を行い、Amazon S3 Transfer Acceleration を使用した場合と使用していない場合の比較が行われます。

最新バージョンの AWS SDK を使用する

AWS SDK では、Amazon S3 のパフォーマンスの最適化のために推奨されている多くのガイドラインが組み込みでサポートされています。SDK では、アプリケーションから Amazon S3 を利用するためのシンプルな API が提供されており、最新のベストプラクティスに従うように定期的に更新されます。例えば、SDK には、HTTP 503 エラーでリクエストを自動的に再試行するロジックが含まれており、遅い接続に応答して適用するためにコードに投資しています。

また、SDK では Transfer Manager も提供されています。これは、接続の水平スケーリングを自動化し、必要に応じてバイト範囲のリクエストを使用して 1 秒あたりに数千ものリクエストを実現しま

す。最新バージョンの AWS SDK を使用して最新のパフォーマンス最適化機能を取得することが重要です。

また、HTTP REST API リクエストを使用している場合は、パフォーマンスを最適化することもできます。REST API を使用する際、SDK の一部である同じベストプラクティスに従う必要があります。オブジェクトデータを同時フェッチできるように、リクエストが遅い場合のタイムアウトと再試行、および複数の接続を可能にしてください。REST API の使用については、Amazon Simple Storage Service API Reference を参照してください。

Amazon S3 のパフォーマンスの設計パターン

Amazon S3 に対してオブジェクトのアップロードや取得を行うアプリケーションを設計する場合は、アプリケーションの最適なパフォーマンスを実現するためにベストプラクティスの設計パターンを使用してください。また、アプリケーションのアーキテクチャの計画時に考慮すべきAmazon S3 のパフォーマンスのガイドライン も提供しています。

パフォーマンスを最適化するには、以下の設計パターンを使用します。

トピック

- 頻繁にアクセスされるコンテンツにキャッシュを使用する
- レイテンシーの影響を受けやすいアプリケーションのタイムアウトと再試行
- 高スループットのための水平スケーリングとリクエスト並列化
- Amazon S3 Transfer Acceleration を使用して長距離間のデータ転送を高速化する

頻繁にアクセスされるコンテンツにキャッシュを使用する

Amazon S3 にデータを保存するアプリケーションの多くは、ユーザーから繰り返しリクエストされる「作業セット」のデータを提供します。ワークロードで一連のよく使用されるオブジェクトに対して繰り返し GET リクエストを送信する場合は、Amazon CloudFront、Amazon ElastiCache、AWS Elemental MediaStore などのキャッシュを使用してパフォーマンスを最適化することができます。キャッシュ導入が成功すると、レイテンシーが低くなり、データ転送速度が速くなります。また、アプリケーションでキャッシュを使用すると Amazon S3 にリクエストを直接送信する回数も減るため、リクエストにかかる費用を削減できます。

Amazon CloudFront は、各地に点在する一連の大規模な POP (Point Of Presence) で Amazon S3 のデータを透過的にキャッシュする高速なコンテンツ配信ネットワーク (CDN) です。複数のリージョ

ンまたはインターネットからオブジェクトにアクセスする場合に CloudFront を使用すると、オブジェクトにアクセスするユーザーの近くにデータをキャッシュできます。これにより、Amazon S3 のアクセス数の多いコンテンツの配信パフォーマンスを高めることができます。CloudFront の詳細については、Amazon CloudFront 開発者ガイドを参照してください。

Amazon ElastiCache は、マネージド型のインメモリキャッシュです。ElastiCache を使用すると、オブジェクトをメモリにキャッシュする Amazon EC2 インスタンスをプロビジョニングできます。このキャッシュにより、GET レイテンシーが数桁減少し、ダウンロードスループットが大幅に向上します。ElastiCache を使用するには、アプリケーションのロジックを変更して、アクセス数の多いオブジェクトをキャッシュに保存し、Amazon S3 にそのオブジェクトをリクエストする前にキャッシュを確認するようにします。ElastiCache を使用して Amazon S3 の GET のパフォーマンスを向上させる例については、ブログ記事の「Turbocharge Amazon S3 with Amazon ElastiCache for Redis」を参照してください。

AWS Elemental MediaStore は、Amazon S3 の動画ワークフローとメディア配信のために特別に作成されたキャッシュおよびコンテンツ配信システムです。MediaStore には、動画専用のエンドツーエンドのストレージ API が用意されており、パフォーマンスが重視される動画ワークロードに最適です。MediaStore の詳細については、「AWS Elemental MediaStore ユーザーガイド」を参照してください。

レイテンシーの影響を受けやすいアプリケーションのタイムアウトと再試行

アプリケーションが Amazon S3 から再試行が必要なことを示すレスポンスを受け取る場合があります。Amazon S3 は、バケット名とオブジェクト名を関連するオブジェクトデータにマッピングします。アプリケーションで発生するリクエスト率が高い場合 (通常、少数のオブジェクトに対して 1 秒あたり 5,000 リクエストを超える率が持続される)、アプリケーションは HTTP 503 slowdown レスポンスを受信することがあります。これらのエラーが発生した場合、各 AWS SDK はエクスポネンシャルバックオフを使用して自動再試行ロジックを実装します。AWS SDK を使用していない場合は、HTTP 503 エラーの受信時に再試行ロジックを実装する必要があります。バックオフテクニックの詳細については、「AWS SDK とツールのリファレンスガイド」の「Retry behavior」を参照してください。

Amazon S3 は、処理を継続するための新しいリクエストレートに応じて自動的にスケールし、パフォーマンスを動的に最適化します。Amazon S3 が新しいリクエスト率のために内部的に最適化している間、最適化が完了するまで一時的に HTTP 503 リクエストレスポンスが送信されます。Amazon S3 が新しいリクエストレートに応じてパフォーマンスを内部的に最適化すると、リクエストはすべて再試行なしで通常どおり処理されます。

レイテンシーが重要なアプリケーションの場合、Amazon S3 では遅いオペレーションを追跡して積極的に再試行することをお勧めします。リクエストを再試行する際は、Amazon S3 に新しく接続して改めて DNS ルックアップを実行することをお勧めします。

可変サイズの大きいリクエスト (例えば、128 MB 超) を実行する際、達成されるスループットを追跡し、リクエストのうち、遅い方から 5 パーセントを再試行することをお勧めします。小さいリクエスト (例えば、512 KB 未満) を実行する際、レイテンシーの中央値が数十ミリ秒の範囲内であることが多い場合、2 秒後に GET または PUT オペレーションを再試行することをお勧めします。追加の再試行が必要な場合のベストプラクティスはバックオフすることです。例えば、2 秒後に 1 回目の再試行を発行し、さらに 4 秒後に 2 回目の再試行を発行することをお勧めします。

アプリケーションが Amazon S3 に固定サイズのリクエストを実行する場合は、それぞれのリクエストの応答時間はより一定になると考えられます。この場合、シンプルな戦略はリクエストのうち、遅い方から 1 パーセントを特定してそれらを再試行することです。1 回の再試行でもレイテンシーの低減において効果的でありことが多いです。

サーバー側の暗号化で AWS Key Management Service (AWS KMS) を使用している場合、ユースケースでサポートされるリクエスト率については、「AWS Key Management Service デベロッパーガイド」の「Quotas」を参照してください。

高スループットのための水平スケーリングとリクエスト並列化

Amazon S3 は大規模な分散システムです。その規模を活用できるように、並列リクエストを Amazon S3 のサービスエンドポイントに水平にスケールすることをお勧めします。このようなスケーリングのアプローチは、Amazon S3 でのリクエストの分散だけでなく、ネットワークで複数のパスに負荷を分散するためにも役立ちます。

転送のスループットを高めるために、Amazon S3 では複数の接続によってデータの GET や PUT を並列で行うアプリケーションを使用することをお勧めします。このような並列化は、AWS Java SDK の Amazon S3 Transfer Manager でサポートされています。また、その他のほとんどの AWS SDK でも同様の機能が提供されています。一部のアプリケーションでは、さまざまなアプリケーションスレッドで、またはさまざまなアプリケーションインスタンスで複数のリクエストを同時に起動することで、並列接続を実現できます。採用する最良のアプローチは、アプリケーション、およびアクセスするオブジェクトの構造によって異なります。

AWS SDK を使用して、AWS SDK で転送の管理を使用するのではなく GET リクエストまたは PUT リクエストを直接発行できます。このアプローチにより、ワークロードをより直接的に調整できると同時に、発生する可能性がある HTTP 503 レスポンスの再試行とその処理に引き続き SDK のサポートを活用できます。一般的なルールとして、リージョン内の大きなオブジェクトを Amazon S3 から

Amazon EC2 にダウンロードする場合は、8 ~ 16 MB の粒度でオブジェクトのバイト範囲の同時リクエストを実行することをお勧めします。同時リクエストは、必要なネットワークスループットの 85 ~ 90 MB/秒ごとに 1 つ実行します。10 Gb/s のネットワークインターフェイスカード (NIC) を使用するには、個別の接続で約 15 の同時リクエストを使用します。より多くの接続で同時リクエストをスケールアップして、25 Gb/s や 100 Gb/s の NIC などのより高速な NIC を使用できます。

パフォーマンスの測定は、同時に発行するリクエスト数を調整する場合に重要です。一度に 1 つのリクエストから始めることをお勧めします。達成されるネットワーク帯域幅とデータの処理でアプリケーションで使用されるその他のリソースの使用を測定します。その後、ボトルネックとなっているリソース (つまり、使用量が最も高いリソース) と有用である可能性が高いリクエスト数を特定できます。例えば、一度に 1 つのリクエストの処理で CPU 使用率が 25 パーセントの場合、これは最大 4 つの同時リクエストに対応できることを示しています。測定は不可欠であり、リクエスト率としてのリソース利用が向上していることを確認する価値があります。

アプリケーションで REST API を使用して Amazon S3 にリクエストを直接発行する場合は、HTTP 接続のプールを使用して、一連のリクエストで各接続を再利用することをお勧めします。リクエストごとの接続セットアップを回避すると、各リクエストで TCP スロースタートと Secure Sockets Layer (SSL) ハンドシェイクを実行する必要がなくなります。REST API の使用については、Amazon Simple Storage Service API Reference を参照してください。

最後に、DNS に注意するとともに、リクエストが Amazon S3 の広範な IP アドレスのプールに分散されていることを確認することもお勧めします。Amazon S3 の DNS の問い合わせは、多数の IP エンドポイントのリストを確認します。ただし、キャッシュリゾルバ、または 1 つの IP アドレスを再利用するアプリケーションコードでは、アドレス多様性とそれによる負荷分散のメリットが得られません。コマンドラインツールの `netstat` などのネットワークユーティリティツールを使用すると、Amazon S3 との通信に使用されている IP アドレスを確認できます。また、使用する DNS 設定のガイドラインも提供しています。これらのガイドラインの詳細については、「Amazon S3 API リファレンス」の「Making requests」を参照してください。

Amazon S3 Transfer Acceleration を使用して長距離間のデータ転送を高速化する

Amazon S3 Transfer Acceleration を使用した高速かつ安全なファイル転送の設定 は、世界中のクライアントと Amazon S3 を使用する特定のリージョンのアプリケーションの距離によるレイテンシーを最小限に抑える、またはなくすために有効です。Transfer Acceleration は、データの転送に CloudFront の世界中に点在するエッジロケーションを利用します。AWS エッジネットワークでは、50 を超えるロケーションに接続ポイントがあります。現在、このネットワークは、CloudFront

でのコンテンツの配信や Amazon Route 53 に対する DNS の問い合わせへの迅速な応答のために使用されています。

このエッジネットワークは、Amazon S3 との間のデータ転送の高速化にも役立ちます。これは、大陸全域または大陸間でデータを転送する、高速なインターネット接続がある、大きなオブジェクトを使用する、またはアップロードするコンテンツが多数あるアプリケーションに最適です。エッジロケーションに到着したデータは、最適化されたネットワークパスで Amazon S3 にルーティングされます。一般的に、Amazon S3 のリージョンから遠いほど、Transfer Acceleration による速度の向上が期待できます。

新しいバケットまたは既存のバケットで Transfer Acceleration をセットアップできます。離れた Amazon S3 Transfer Acceleration エンドポイントを使用して、AWS のエッジロケーションを使用することができます。Transfer Acceleration がクライアントのリクエストのパフォーマンスに役立つかどうかをテストする最も良い方法は、Amazon S3 Transfer Acceleration の速度比較ツールを使用することです。ネットワークの設定および条件は、随時、場所によって異なります。そのため、Amazon S3 Transfer Acceleration がアップロードのパフォーマンスを向上させることができると考えられる転送に対してのみ料金が発生します。さまざまな AWS SDK での Transfer Acceleration の使用については、「S3 Transfer Acceleration の有効化と使用」を参照してください。

Amazon S3 を使用して静的ウェブサイトをホスティングする

Amazon S3 を使用して、静的ウェブサイトをホストできます。静的ウェブサイトでは、個々のウェブページの内容は静的コンテンツです。ほかに、クライアント側スクリプトが含まれていることもあります。

> **Note**
>
> AWS Amplify ホスティングを使用して、S3 に保存されている静的ウェブサイトのコンテンツをホストすることをお勧めします Amplify ホスティングは、Amazon CloudFront を利用したグローバルに利用可能なコンテンツ配信ネットワーク (CDN) にウェブサイトを簡単にデプロイできるフルマネージドサービスです。これにより、安全な静的ウェブサイトホスティングが可能になります。
> AWS Amplify ホスティングを使用すると、汎用バケット内のオブジェクトの場所を選択して、コンテンツをマネージド CDN にデプロイし、ウェブサイトのパブリック HTTPS URL を生成してどこからでもアクセス可能にすることができます。Amplify ホスティングの詳細については、「AWS Amplify コンソールユーザーガイド」の「S3 汎用バケットから AWS Amplify Hosting への静的ウェブサイトのデプロイ」および「Amplify コンソールを使用した S3 からの静的ウェブサイトのデプロイ」を参照してください。

Amazon S3 での静的ウェブサイトのホストに関する詳細 (手順やステップバイステップのチュートリアルなど) については、以下のトピックを参照してください。

トピック

- ウェブサイトエンドポイント
- ウェブサイトのホスティングの有効化
- インデックスドキュメントの設定
- カスタムエラードキュメントの設定
- ウェブサイトアクセスのアクセス許可の設定
- (オプション) ウェブトラフィックのログ記録
- (オプション) ウェブページリダイレクトの設定
- Cross-Origin Resource Sharing (CORS) の使用

- 静的ウェブサイトのチュートリアル

ウェブサイトエンドポイント

バケットを静的ウェブサイトとして設定すると、そのウェブサイトは、バケットの AWS リージョン固有のウェブサイトエンドポイントで利用できます。ウェブサイトエンドポイントは、REST API リクエストを送信するエンドポイントとは別のものです。エンドポイントの違いの詳細については、「ウェブサイトエンドポイントと REST API エンドポイントの主な違い」を参照してください。

使用しているリージョンに応じて、Amazon S3 ウェブサイトエンドポイントは以下の 2 つの形式のいずれかになります。

- s3-website ダッシュ (-) リージョン - `http://bucket-name.s3-website-Region.amazonaws.com`
- s3-website ドット (.) リージョン -`http://bucket-name.s3-website.Region.amazonaws.com`

これらの URL にアクセスすると、ウェブサイト用に設定したデフォルトのインデックスドキュメントが返されます。Amazon S3 ウェブサイトエンドポイントの完全なリストについては、「Amazon S3 ウェブサイトエンドポイント」を参照してください。

> **Note**
>
> Amazon S3 の静的ウェブサイトのセキュリティを強化するために、Amazon S3 ウェブサイトのエンドポイントドメイン (s3-website-us-east-1.amazonaws.com や s3-website.ap-south-1.amazonaws.com など) はパブリックサフィックスリスト (PSL) に登録されています。セキュリティ強化のため、Amazon S3 統計 ウェブサイトのドメイン名に機密な Cookie を設定する必要が生じた場合は、__Host- プレフィックスの付いた Cookie の使用をお勧めします。このプラクティスは、クロスサイトリクエストフォージェリ (CSRF) 攻撃からドメインを防ぐ際に役立ちます。詳細については、Mozilla 開発者ネットワークの「Set-Cookie」ページを参照してください。

ウェブサイトを公開したい場合、顧客がウェブサイトエンドポイントにあるコンテンツにアクセスできるようにするには、すべてのコンテンツがパブリックに読み取り可能になっている必要があります。詳細については、「ウェブサイトアクセスのアクセス許可の設定」を参照してください。

Important

- Amazon S3 ウェブサイトエンドポイントは HTTPS またはアクセスポイントをサポートしていません。HTTPS を使用する場合は、次のいずれかを実行できます。
  - (推奨) S3 に保存された静的ウェブサイトコンテンツをホストするには、AWS Amplify ホスティング を使用します。Amplify ホスティングは、Amazon CloudFront を利用したグローバルに利用可能なコンテンツ配信ネットワーク (CDN) にウェブサイトを簡単にデプロイできるフルマネージドサービスです。これにより、安全な静的ウェブサイトホスティングが可能になります。

    AWS Amplify ホスティングを使用すると、汎用バケット内のオブジェクトの場所を選択して、コンテンツをマネージド CDN にデプロイし、ウェブサイトのパブリック HTTPS URL を生成してどこからでもアクセス可能にすることができます。Amplify ホスティングの詳細については、「AWS Amplify コンソールユーザーガイド」の「S3 汎用バケットから AWS Amplify Hosting への静的ウェブサイトのデプロイ」および「Amplify コンソールを使用した S3 からの静的ウェブサイトのデプロイ」を参照してください。
  - Amazon CloudFront を使用して、Amazon S3 でホストされる静的ウェブサイトを提供します。詳細については、CloudFront を使用して Amazon S3 バケットに対する HTTPS リクエストを処理するにはどうすればよいですか? を参照してください。カスタムドメインで HTTPS を使用するには、Route 53 に登録されたカスタムドメインを使用した静的ウェブサイトの設定を参照してください。
- 「リクエスタ支払い」バケットに、ウェブサイトエンドポイントを介してアクセスすることはできません。このようなバケットへのリクエストに対しては 403 Access Denied レスポンスを受け取ります。詳細については、「ストレージの転送と使用にリクエスタ支払い汎用バケットを使用する」を参照してください。

トピック

- ウェブサイトエンドポイントの例
- DNS CNAME の追加
- Route 53 でのカスタムドメインの使用
- ウェブサイトエンドポイントと REST API エンドポイントの主な違い

ウェブサイトエンドポイントの例

以下の例では、静的ウェブサイトとして設定されている Amazon S3 バケットにアクセスする方法を示しています。

Example — ルートレベルでのオブジェクトのリクエスト

バケットのルートレベルに保存されている特定のオブジェクトをリクエストするには、以下の URL 構造を使用します。

```
http://bucket-name.s3-website.Region.amazonaws.com/object-name
```

たとえば、以下の URL は、バケットのルートレベルに保存されている photo.jpg オブジェクトをリクエストするものです。

```
http://example-bucket.s3-website.us-west-2.amazonaws.com/photo.jpg
```

Example — プレフィックスでのオブジェクトのリクエスト

バケット内のフォルダに保存されているオブジェクトをリクエストするには、以下の URL 構造を使用します。

```
http://bucket-name.s3-website.Region.amazonaws.com/folder-name/object-name
```

以下の URL は、バケット内の docs/doc1.html オブジェクトをリクエストするものです。

```
http://example-bucket.s3-website.us-west-2.amazonaws.com/docs/doc1.html
```

DNS CNAME の追加

登録済みのドメインをお持ちの場合、Amazon S3 ウェブサイトエンドポイントを指し示す DNS CNAME エントリを追加することができます。たとえば、ドメイン www.example-bucket.com を登録した場合は、バケット www.example-bucket.com を作成し、www.example-bucket.com.s3-website.*Region*.amazonaws.com を参照する DNS CNAME エントリを追加できます。http://www.example-bucket.com へのリクエストはすべて、www.example-bucket.com.s3-website.*Region*.amazonaws.com にルーティングされます。

詳細については、「CNAME レコードを使用した Amazon S3 URL のカスタマイズ」を参照してください。

Route 53 でのカスタムドメインの使用

Amazon S3 ウェブサイトエンドポイントを使用してウェブサイトにアクセスする代わりに、Amazon Route 53 に登録された独自のドメイン (example.com など) を使用して、コンテンツを提供できます。ルートドメインでウェブサイトをホストするために、Amazon S3 を Route 53 とともに使用することができます。例えば、ルートドメインが example.com で、ウェブサイトを Amazon S3 でホスティングする場合に、そのウェブサイトにブラウザからアクセスするには「http://www.example.com」または「http://example.com」を入力します。

チュートリアル例については、「チュートリアル: Route 53 に登録されたカスタムドメインを使用した静的ウェブサイトの設定」を参照してください。

ウェブサイトエンドポイントと REST API エンドポイントの主な違い

Amazon S3 ウェブサイトエンドポイントは、ウェブブラウザを介してアクセスするように最適化されています。以下の表は、REST API エンドポイントとウェブサイトエンドポイントの主な違いをまとめたものです。

主な違い	REST API エンドポイント	ウェブサイトエンドポイント
アクセスコントロール	パブリックコンテンツとプライベートコンテンツの両方をサポートします。	公開で読み取り可能なコンテンツのみをサポートします。
エラーメッセージの処理	XML 形式のエラーレスポンスを返します。	HTML ドキュメントを返します。
リダイレクトのサポート	該当しません	オブジェクトレベルとバケットレベルの両方のリダイレクトをサポートします。
サポートされるリクエスト	バケットおよびオブジェクトのすべてのオペレーションをサポートします。	オブジェクトに対する GET および HEAD リクエストのみをサポートします。

主な違い	REST API エンドポイント	ウェブサイトエンドポイント
バケットのルートでの GET および HEAD リクエストに応答します。	バケット内のオブジェクトキーのリストを返します。	ウェブサイト設定で指定されているインデックスドキュメントを返します。
Secure Sockets Layer (SSL) のサポート	SSL 接続をサポートします。	SSL 接続をサポートしません。

Amazon S3 エンドポイントの完全なリストについては、AWS 全般のリファレンス の「Amazon S3 エンドポイントとクォータ」を参照してください。

ウェブサイトのホスティングの有効化

バケットを静的ウェブサイトとして設定する場合は、静的ウェブサイトホスティングの有効化、インデックスドキュメントの設定、およびアクセス許可の設定を行う必要があります。

Amazon S3 コンソール、REST API、AWS SDK、AWS CLI、または AWS CloudFormation を使用して、静的ウェブサイトホスティングを有効にすることができます。

カスタムドメインを使用してウェブサイトを設定するには、「チュートリアル: Route 53 に登録されたカスタムドメインを使用した静的ウェブサイトの設定」を参照してください。

S3 コンソールの使用

静的ウェブサイトホスティングを有効にするには

1. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
2. 左のナビゲーションペインで、[汎用バケット] を選択します。
3. バケットリストで、静的ウェブサイトホスティングを有効にするバケットの名前を選択します。
4. [プロパティ] を選択します。
5. [静的ウェブサイトホスティング] で [編集] を選択します。

6. [このバケットを使用してウェブサイトをホストする] を選択します。
7. [静的ウェブサイトホスティング] で [有効化] を選択します。
8. [インデックスドキュメント] に、インデックスドキュメントのファイル名 (通常は `index.html`) を入力します。

   インデックスドキュメント名の大文字と小文字は区別されます。この名前は、S3 バケットにアップロードする HTML インデックスドキュメントのファイル名と正確に一致する必要があります。バケットをウェブサイトホスティング用に設定するときは、インデックスドキュメントを指定する必要があります。Amazon S3 からこのインデックスドキュメントが返されるのは、ルートドメインまたはサブフォルダに対するリクエストが行われたときです。詳細については、「インデックスドキュメントの設定」を参照してください。
9. 4XX クラスエラーに関する独自のカスタムエラードキュメントを指定する場合は、[エラードキュメント] にカスタムエラードキュメントのファイル名を入力します。

   エラードキュメント名の大文字と小文字は区別されます。この名前は、S3 バケットにアップロードする HTML エラードキュメントのファイル名と正確に一致する必要があります。カスタムエラードキュメントを指定しない場合、エラーが発生すると、Amazon S3 からデフォルトの HTML エラードキュメントが返されます。詳細については、「カスタムエラードキュメントの設定」を参照してください。
10. (オプション) 高度なリダイレクトツールを指定する場合は、[Rredirection rules] (リダイレクトルール) に、JSON を入力してルールを記述します。

    例えば、条件に応じてリクエストのルーティング先を変えることができます。この条件として使用できるのは、リクエストの中の特定のオブジェクトキー名またはプレフィックスです。詳細については、「高度な条件付きリダイレクトを使用するようにリダイレクトルールを設定する」を参照してください。
11. [Save changes] (変更の保存) をクリックします。

    Amazon S3 では、バケットの静的ウェブサイトホスティングを有効にします。ページの下部の [静的ウェブサイトホスティング] の下に、バケットのウェブサイトエンドポイントが表示されます。
12. [静的 ウェブサイトホスティング] の下のエンドポイントを書き留めます。

    [Endpoint (エンドポイント)] は、バケットの Amazon S3 ウェブサイトエンドポイントです。バケットを静的ウェブサイトとして設定すると、このエンドポイントを使用してウェブサイトをテストできます。

REST API の使用

REST リクエストを直接送信して静的ウェブサイトホスティングを有効にする方法の詳細については、Amazon Simple Storage Service API リファレンスの以下のセクションを参照してください。

- PUT Bucket website
- GET Bucket website
- DELETE Bucket website

AWS SDK の使用

Amazon S3 で静的ウェブサイトをホスティングするには、Amazon S3 バケットをウェブサイトホスティング用に設定してから、ウェブサイトのコンテンツをそのバケットにアップロードします。AWS SDK を使用して、プログラムでウェブサイト設定を作成、更新、削除することもできます。SDK は、Amazon S3 REST API のラッパークラスを提供します。アプリケーションの必要性に応じて、アプリケーションから直接 REST API リクエストを送信することができます。

.NET

次の例では、AWS SDK for .NET を使用してバケットのウェブサイト設定を管理する方法を示します。バケットにウェブサイト設定を追加するには、バケット名とウェブサイト設定を指定します。ウェブサイト設定にはインデックスドキュメントを含める必要があります。また、オプションとしてエラードキュメントを含めることができます。これらのドキュメントは、バケット内に保存済みであることが必要です。詳細については、「PUT Bucket ウェブサイト」を参照してください。Amazon S3 ウェブサイト機能の詳細については、Amazon S3 を使用して静的ウェブサイトをホスティングする を参照してください。

次の C# コード例は、指定したバケットにウェブサイト設定を追加しています。この設定で、インデックスドキュメント名とエラードキュメント名の両方を指定します。コード例を設定および実行する方法の詳細については、「AWS SDK for .NET デベロッパーガイド」の「AWS SDK for .NET の開始方法」 を参照してください。

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
```

```
{
    class WebsiteConfigTest
    {
        private const string bucketName = "*** bucket name ***";
        private const string indexDocumentSuffix = "*** index object key ***"; //
 For example, index.html.
        private const string errorDocument = "*** error object key ***"; // For
 example, error.html.
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 client;
        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            AddWebsiteConfigurationAsync(bucketName, indexDocumentSuffix,
 errorDocument).Wait();
        }

        static async Task AddWebsiteConfigurationAsync(string bucketName,
                                            string indexDocumentSuffix,
                                            string errorDocument)
        {
            try
            {
                // 1. Put the website configuration.
                PutBucketWebsiteRequest putRequest = new PutBucketWebsiteRequest()
                {
                    BucketName = bucketName,
                    WebsiteConfiguration = new WebsiteConfiguration()
                    {
                        IndexDocumentSuffix = indexDocumentSuffix,
                        ErrorDocument = errorDocument
                    }
                };
                PutBucketWebsiteResponse response = await
 client.PutBucketWebsiteAsync(putRequest);

                // 2. Get the website configuration.
                GetBucketWebsiteRequest getRequest = new GetBucketWebsiteRequest()
                {
                    BucketName = bucketName
                };
```

```
                GetBucketWebsiteResponse getResponse = await
 client.GetBucketWebsiteAsync(getRequest);
                Console.WriteLine("Index document: {0}",
 getResponse.WebsiteConfiguration.IndexDocumentSuffix);
                Console.WriteLine("Error document: {0}",
 getResponse.WebsiteConfiguration.ErrorDocument);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
        }
    }
}
```

PHP

次の PHP の例では、指定したバケットにウェブサイト設定を追加します。`create_website_config` メソッドで、インデックスドキュメント名とエラードキュメント名を明示的に指定します。さらに、ウェブサイト設定を取得し、レスポンスを出力します。Amazon S3 ウェブサイト機能の詳細については、Amazon S3 を使用して静的ウェブサイトをホスティングする を参照してください。

AWS SDK for Ruby API の詳細については、AWS SDK for Ruby - バージョン 2 を参照してください。

```
 require 'vendor/autoload.php';

use Aws\S3\S3Client;

$bucket = '*** Your Bucket Name ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);
```

```
// Add the website configuration.
$s3->putBucketWebsite([
    'Bucket'                => $bucket,
    'WebsiteConfiguration'  => [
        'IndexDocument' => ['Suffix' => 'index.html'],
        'ErrorDocument' => ['Key' => 'error.html']
    ]
]);

// Retrieve the website configuration.
$result = $s3->getBucketWebsite([
    'Bucket' => $bucket
]);
echo $result->getPath('IndexDocument/Suffix');

// Delete the website configuration.
$s3->deleteBucketWebsite([
    'Bucket' => $bucket
]);
```

AWS CLI を使用する場合

AWS CLI を使用して S3 バケットを静的ウェブサイトとして設定する方法の詳細については、AWS CLI コマンドリファレンスのウェブサイトを参照してください。

次に、インデックスドキュメントの設定とアクセス許可の設定を行う必要があります。詳細については、「インデックスドキュメントの設定」および「ウェブサイトアクセスのアクセス許可の設定」を参照してください。

オプションとして、エラードキュメント、ウェブトラフィックのログ記録、またはリダイレクトを設定することもできます。

インデックスドキュメントの設定

ウェブサイトホスティングを有効にする場合は、インデックスドキュメントの設定とアップロードも必要です。インデックスドキュメントは、リクエストがウェブサイトのルートまたはサブフォルダに対して行われた場合に Amazon S3 によって返されるウェブページです。たとえば、ユーザーがブラウザに `http://www.example.com` と入力した場合は、このユーザーは特定のページをリクエスト

してはいません。この場合、Amazon S3 は、インデックスドキュメントを提供し、これがデフォルトページと見なされることがあります。

バケットに対して静的ウェブサイトホスティングを有効にする場合は、インデックスドキュメントの名前 (index.html など) を入力します。バケットに対して静的ウェブサイトホスティングを有効にした後、インデックスドキュメント名を含む HTML ファイルをバケットにアップロードします。

ルートレベル URL の末尾のスラッシュは省略可能です。たとえば、index.html をウェブサイトのインデックスドキュメントとして設定した場合は、以下の URL のどちらからも index.html が返されます。

```
http://example-bucket.s3-website.Region.amazonaws.com/
http://example-bucket.s3-website.Region.amazonaws.com
```

Amazon S3 ウェブサイトのエンドポイントの詳細については、「ウェブサイトエンドポイント」を参照してください。

インデックスドキュメントとフォルダ

Amazon S3 では、バケットはオブジェクトのフラットコンテナです。つまり、コンピュータのファイルシステムとは異なり、階層構造ではありません。ただし、論理的な階層を作成するには、フォルダ構造を暗示させる名前をオブジェクトキーに付けます。

たとえば、以下のキー名を持つ 3 つのオブジェクトを含むバケットがあるとします。これらは、物理的な階層構造で格納されているわけではありませんが、キー名から次のような論理フォルダ構造を推測できます。

- sample1.jpg — オブジェクトはバケットのルートにあります。
- photos/2006/Jan/sample2.jpg — オブジェクトは photos/2006/Jan サブフォルダにあります。
- photos/2006/Feb/sample3.jpg — オブジェクトは photos/2006/Feb サブフォルダにあります。

Amazon S3 コンソールでは、バケットにフォルダを作成することもできます。たとえば、photos という名前のフォルダを作成できます。バケットまたはバケット内の photos フォルダにオブジェクトをアップロードできます。オブジェクト sample.jpg をバケットに追加する場合、キー名は sample.jpg です。オブジェクトを photos フォルダにアップロードする場合、オブジェクトキー名は photos/sample.jpg です。

フォルダ構造をバケット内に作成する場合は、各レベルにインデックスドキュメントが存在している必要があります。各フォルダでは、インデックスドキュメントは同じ名前 (index.html など) であることが必要です。ユーザーが指定した URL がフォルダルックアップに似ている場合は、末尾のスラッシュの有無によって、ウェブサイトエンドポイントの動作が決まります。たとえば、末尾にスラッシュのある次の URL はphotos/index.html インデックスドキュメントを返します。

```
http://bucket-name.s3-website.Region.amazonaws.com/photos/
```

ただし、前の URL から末尾のスラッシュを除外した場合、Amazon S3 はまずバケット内のオブジェクト photos を検索します。photos オブジェクトが見つからない場合、インデックスドキュメント photos/index.html が検索されます。見つかった場合、Amazon S3 は 302 Found メッセージを返し、photos/ キーを指し示します。それ以降の photos/ に対するリクエストについて、Amazon S3 は photos/index.html を返します。インデックスドキュメントも見つからない場合、Amazon S3 はエラーを返します。

インデックスドキュメントを設定する

S3 コンソールを使用してインデックスドキュメントを設定するには、次の手順に従います。REST API、AWS SDK、AWS CLI、または AWS CloudFormation を使用してインデックスドキュメントを設定することもできます。

> **Note**
>
> バージョニングが有効なバケットでは、index.html のコピーを複数アップロードできますが、解決されるのは最新バージョンのみです。S3 バージョニングの詳細については、「S3 バージョニングによる複数のバージョンのオブジェクトの保持」を参照してください。

バケットに対して静的ウェブサイトホスティングを有効にする場合は、インデックスドキュメントの名前 (**index.html** など) を入力します。バケットに対して静的ウェブサイトホスティングを有効にした後、インデックスドキュメント名を含む HTML ファイルをバケットにアップロードします。

インデックスドキュメントを設定するには

1. index.html ファイルを作成します。

   index.html ファイルがない場合は、以下の HTML を使用して作成できます。

   ```
   <html xmlns="http://www.w3.org/1999/xhtml" >
   ```

```
<head>
    <title>My Website Home Page</title>
</head>
<body>
  <h1>Welcome to my website</h1>
  <p>Now hosted on Amazon S3!</p>
</body>
</html>
```

2. インデックスファイルをローカルに保存します。

   インデックスドキュメントファイル名は、[静的ウェブサイトホスティング] ダイアログボックスで入力したインデックスドキュメント名と正確に一致する必要があります。インデックスドキュメント名では、大文字と小文字が区別されます。例えば、[静的ウェブサイトホスティング] ダイアログボックスの [インデックスドキュメント] 名に「index.html」と入力する場合、インデックスドキュメントファイル名も Index.html ではなく index.html である必要があります。

3. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
4. 左のナビゲーションペインで、[汎用バケット] を選択します。
5. バケットリストで、静的ウェブサイトホスティングに使用するバケットの名前を選択します。
6. バケットに対して静的ウェブサイトホスティングを有効にし、インデックスドキュメントの正確な名前 (index.html など) を入力します。詳細については、「ウェブサイトのホスティングの有効化」を参照してください。

   静的ウェブサイトホスティングを有効にしたら、ステップ 6 に進みます。

7. インデックスドキュメントをバケットにアップロードするには、以下のいずれかを実行します。

   - インデックスファイルをコンソールバケットのリストにドラッグアンドドロップします。
   - [Upload] を選択し、プロンプトに従ってインデックスファイルを選択してアップロードします。

   手順については、「オブジェクトのアップロード」を参照してください。

8. (オプション) 他のウェブサイトコンテンツをバケットにアップロードします。

次に、ウェブサイトへのアクセス許可を設定する必要があります。詳細については、「ウェブサイトアクセスのアクセス許可の設定」を参照してください。

オプションとして、エラードキュメント、ウェブトラフィックのログ記録、またはリダイレクトを設定することもできます。

カスタムエラードキュメントの設定

バケットを静的ウェブサイトとして設定した後、エラーが発生すると、Amazon S3 から HTML エラードキュメントが返されます。オプションで、エラーが発生したときに Amazon S3 からそのドキュメントが返されるように、カスタムエラードキュメントを含むバケットを設定できます。

> **Note**
>
> ただし、エラーが発生した場合、一部のブラウザは独自のエラーメッセージを表示し、Amazon S3 が返すエラードキュメントを無視することがあります。たとえば、HTTP 404 Not Found エラーが発生した場合、Google Chrome は Amazon S3 が返すエラードキュメントを無視し、独自のエラーを表示することがあります。

トピック

- Amazon S3 HTTP レスポンスコード
- カスタムエラードキュメントの設定

Amazon S3 HTTP レスポンスコード

次の表は、エラーの発生時に Amazon S3 が返す HTTP レスポンスコードのサブセットをまとめたものです。

HTTP エラーコード	説明
301 Moved Permanently	ユーザーが Amazon S3 ウェブサイトエンドポイント (`http://s3-website.` *`Region`*`.amazonaws.com/`) に直接リクエストを送信した場合、Amazon S3 は 301 Moved Permanently レスポンスを返し、それらのリクエストを `https://aws.amazon.com/s3/` にリダイレクトします。
[302 Found]	Amazon S3 が末尾にスラッシュのないキー `x`、`http://`*`bucket-name`*`.s3-website.`*`Region`*`.amazonaws.com/x` に対するリクエストを

HTTP エラーコード	説明
	受け取った場合、まずキー名 x のオブジェクトを検索します。オブジェクトが見つからない場合、Amazon S3 はリクエストがサブフォルダ x に対するものであると判断し、末尾にスラッシュを追加して、リクエストをリダイレクトし、302 Found を返します。
[304 Not Modified]	Amazon S3 は、リクエストヘッダー `If-Modified-Since` 、`If-Unmodified-Since` 、`If-Match`、および/または `If-None-Match` を使用して、リクエストされたオブジェクトがクライアントで保持されているキャッシュされたコピーと同じであるかどうかを判断します。オブジェクトが同じである場合、ウェブサイトエンドポイントは [304 Not Modified] レスポンスを返します。
[400 Malformed Request]	ユーザーが誤ったリージョンエンドポイント経由でバケットにアクセスを試みると、ウェブサイトエンドポイントは [400 Malformed Request] で応答します。
403 Forbidden	ユーザーのリクエストが公開で読み取ることのできないオブジェクトに変換する場合、ウェブサイトエンドポイントは [403 Forbidden] で応答します。オブジェクト所有者は、バケットポリシーまたは ACL を使用して、オブジェクトを公開する必要があります。

HTTP エラーコード	説明
404 Not Found	ウェブサイトエンドポイントは、以下の理由により [404 Not Found] で応答します。 • ウェブサイトの URL が存在しないオブジェクトキーを参照しているものと、Amazon S3 が判断した。 • リクエストが存在しないインデックスドキュメントに対するものであると、Amazon S3 が推論した。 • URL に指定されたバケットが存在しない。 • URL に指定されたバケットは存在するが、ウェブサイトとして設定されていない。 [404 Not Found] で返すドキュメントをカスタマイズすることができます。必ず、このドキュメントをウェブサイトとして設定されたバケットにアップロードすると共に、このドキュメントを使用するようにウェブサイトホスティング設定を行ってください。 Amazon S3 がオブジェクトまたはインデックスドキュメントのリクエストとして URL をどのように解釈するかについては、「インデックスドキュメントの設定」を参照してください。
[500 Service Error]	内部サーバーエラーが発生した場合、ウェブサイトエンドポイントは [500 Service Error] で応答します。
503 Service Unavailable	Amazon S3 がユーザーのリクエスト頻度を減らす必要があると判断した場合に、ウェブサイトエンドポイントは 503 Service Unavailable で応答します。

これらの各エラーに対して、Amazon S3 は定義済みの HTML メッセージを返します。[403 Forbidden] レスポンスで返される HTML メッセージの例を次に示します。

カスタムエラードキュメントの設定

バケットを静的ウェブサイトとして設定する場合、ユーザーフレンドリーなエラーメッセージと追加のヘルプを含むカスタムエラードキュメントを提供できます。Amazon S3 は HTTP 4XX クラスのエラーコードに対してのみ、カスタムエラードキュメントを返します。

S3 コンソールを使用してカスタムエラードキュメントを設定するには、次の手順に従います。REST API、AWS SDK、AWS CLI、または AWS CloudFormation を使用してエラードキュメントを設定することもできます。詳細については、以下を参照してください。

- Amazon Simple Storage Service API リファレンスの「PutBucketWebsite」
- AWS CloudFormation ユーザーガイドの AWS::S3::Bucket WebsiteConfiguration
- AWS CLI コマンドリファレンスの put-bucket-website

バケットに対して静的ウェブサイトホスティングを有効にするときは、エラードキュメントの名前 (例: **`404.html`**) を入力します。バケットに対して静的ウェブサイトホスティングを有効にしたら、エラードキュメント名を含む HTML ファイルをバケットにアップロードします。

エラードキュメントを設定するには

1. エラードキュメント (例: `404.html`) を作成します。
2. エラードキュメントのファイルをローカルに保存します。

エラードキュメントの名前は、大文字と小文字を区別し、静的ウェブサイトホスティングを有効にする際に入力した名前と厳密に一致している必要があります。たとえば、[Static website hosting] (静的ウェブサイトホスティング) ダイアログボックスの [Error document] (エラードキュメント) 名に `404.html` と入力する場合、エラードキュメントのファイル名も `404.html` である必要があります。

3. AWS Management Console にサインインし、Amazon S3 コンソール https://console.aws.amazon.com/s3/ を開きます。
4. 左のナビゲーションペインで、[汎用バケット] を選択します。
5. バケットリストで、静的ウェブサイトホスティングに使用するバケットの名前を選択します。
6. バケットに対して静的ウェブサイトホスティングを有効にし、エラードキュメントの正確な名前 (例: `404.html`) を入力します。詳細については、「ウェブサイトのホスティングの有効化」および「カスタムエラードキュメントの設定」を参照してください。

   静的ウェブサイトホスティングを有効にしたら、ステップ 6 に進みます。
7. エラードキュメントをバケットにアップロードするには、以下のいずれかを実行します。

   - エラードキュメントファイルをコンソールバケットのリストにドラッグアンドドロップします。
   - [Upload] を選択し、プロンプトに従ってインデックスファイルを選択してアップロードします。

   手順については、「オブジェクトのアップロード」を参照してください。

ウェブサイトアクセスのアクセス許可の設定

バケットを静的ウェブサイトとして設定する場合、このウェブサイトを公開するときは、パブリック読み取りアクセスを許可できます。バケットをパブリックに読み取り可能にするには、バケットのパブリックアクセスブロック設定を無効にし、パブリック読み取りアクセスを許可するバケットポリシーを記述する必要があります。バケットにバケット所有者が所有していないオブジェクトが含まれている場合は、すべてのユーザーに読み取りアクセスを許可するオブジェクトアクセスコントロールリスト (ACL) の追加が必要になる場合があります。

バケットのパブリックアクセスのブロック設定を無効にするのではなく、ウェブサイトを公開したい場合は、Amazon CloudFront ディストリビューションを作成して、静的ウェブサイトを提供できます。詳細については、Amazon CloudFront によるウェブサイトの高速化 および「Amazon Route 53

デベロッパーガイド」の「Amazon CloudFront ディストリビューションを使用して静的ウェブサイトを提供する」を参照してください。

> **Note**
>
> ウェブサイトエンドポイント上に、ユーザーがリクエストしたオブジェクトが存在しない場合は、Amazon S3 から HTTP レスポンスコード 404 (Not Found) が返されます。オブジェクトが存在するが、そのオブジェクトの読み取りアクセス許可が付与されていない場合は、ウェブサイトエンドポイントから HTTP レスポンスコード 403 (Access Denied) が返されます。ユーザーはこのレスポンスコードを見て、特定のオブジェクトが存在するかどうかを推測できます。この動作を希望しない場合は、バケットのウェブサイトのサポートを有効にしないでください。

トピック

- ステップ 1: S3 のパブリックアクセスのブロック設定を編集する
- ステップ 2: バケットポリシーを追加する
- オブジェクトアクセスコントロールリスト

ステップ 1: S3 のパブリックアクセスのブロック設定を編集する

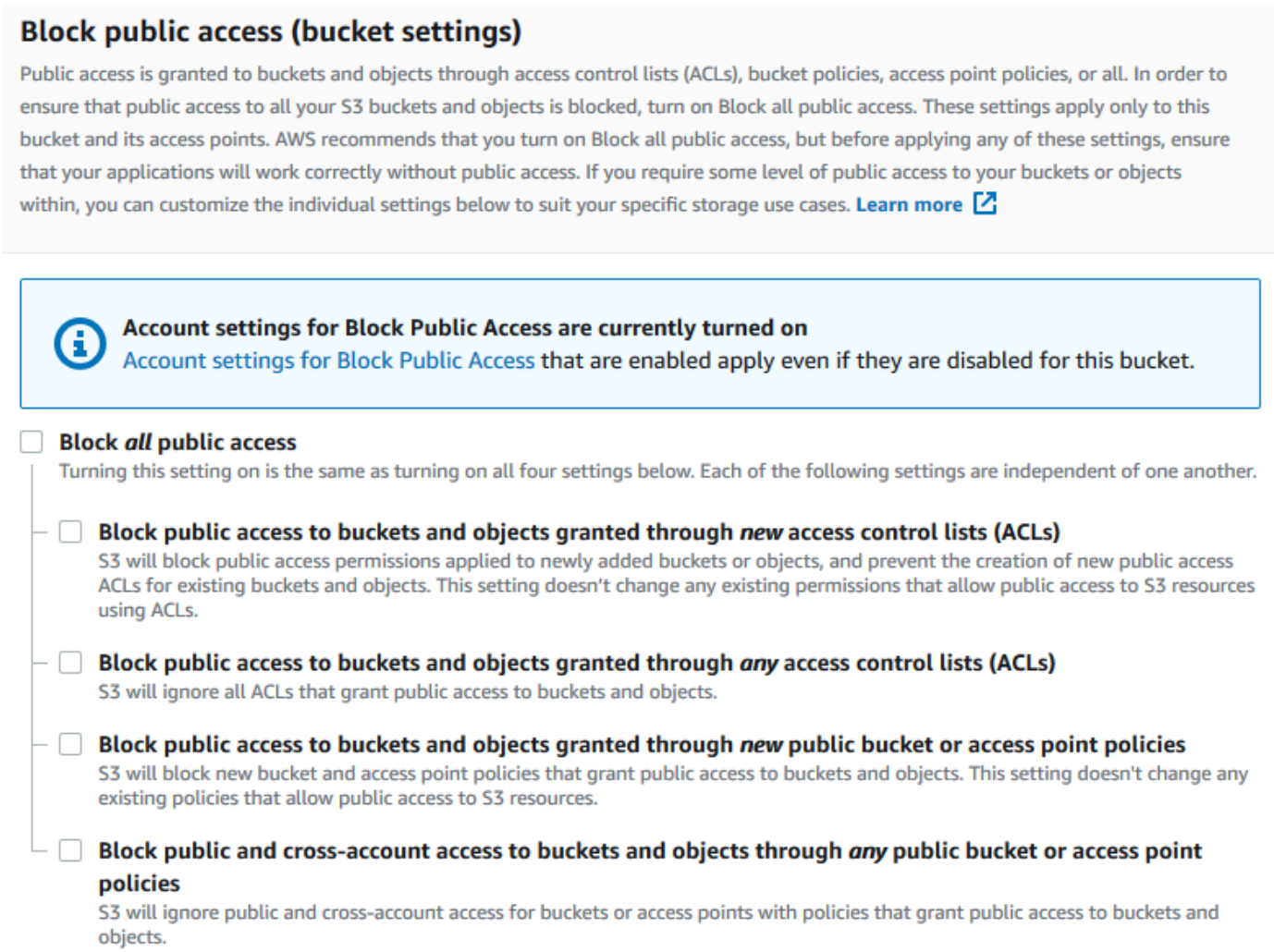
既存のバケットをパブリックアクセスを持つ静的ウェブサイトとして設定する場合は、そのバケットのパブリックアクセスのブロック設定を編集する必要があります。また、アカウントレベルでパブリックアクセスのブロック設定を編集する必要がある場合もあります。Amazon S3 は、アクセスポイントレベル、バケットレベル、アカウントレベルのパブリックアクセスのブロック設定で最も制限の厳しい組み合わせを適用します。

例えば、バケットのパブリックアクセスを許可し、アカウントレベルですべてのパブリックアクセスをブロックした場合、Amazon S3 はバケットへのパブリックアクセスを引き続きブロックします。このシナリオでは、バケットレベルとアカウントレベルのパブリックアクセスのブロック設定を編集する必要があります。詳細については、「Amazon S3 ストレージへのパブリックアクセスのブロック」を参照してください。

デフォルトでは、Amazon S3 はアカウントとバケットへのパブリックアクセスをブロックします。バケットを使用して静的ウェブサイトをホストする場合は、以下のステップを使用して、パブリックアクセスブロック設定を編集できます。

> **Warning**
>
> このステップを完了する前に「Amazon S3 ストレージへのパブリックアクセスのブロック」を読んで、パブリックアクセスを許可することに伴うリスクを理解し、了承してください。パブリックアクセスブロック設定をオフにしてバケットをパブリックにすると、インターネット上のだれでもバケットにアクセスできるようになります。バケットへのすべてのパブリックアクセスをブロックすることをお勧めします。

1. https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開きます。
2. 静的ウェブサイトとして設定されたバケットの名前を選択します。
3. [Permissions (アクセス許可)] を選択します。
4. [ブロックパブリックアクセス (バケット設定)] で [編集] を選択します。
5. [Block all public access (すべてのパブリックアクセスをブロックする)] をクリアし、[Save changes (変更の保存)] を選択します。



Amazon S3 で、バケットのブロックパブリックアクセス設定がオフになります。パブリックな静的ウェブサイトを作成するには、バケットポリシーを追加する前に、アカウントのブロックパブリックアクセス設定を編集する必要があります。アカウントのブロックパブリックアクセス設定が現在有効になっている場合は、[ブロックパブリックアクセス (バケット設定)] の下にメモが表示されます。

ステップ 2: バケットポリシーを追加する

バケット内のオブジェクトをパブリックに読み取り可能にするには、すべてのユーザーに `s3:GetObject` アクセス許可を付与するバケットポリシーを作成する必要があります。

S3 のパブリックアクセスブロック設定を編集した後で、バケットへのパブリック読み取りアクセスを許可するバケットポリシーを追加できます。パブリック読み取りアクセスを許可すると、インターネット上のだれでもバケットにアクセスできるようになります。

> **Important**
>
> 次のポリシーは、単なる例として、バケットのコンテンツへのフルアクセスを許可します。このステップに進む前に、「Amazon S3 バケット内のファイルを保護するにはどうすればよいですか?」を確認して、S3 バケット内のファイルを保護するためのベストプラクティスと、パブリックアクセスの許可に伴うリスクを理解してください。

1. [バケット] で、バケットの名前を選択します。
2. [Permissions (アクセス許可)] を選択します。
3. [Bucket Policy (バケットポリシー)] で [編集] を選択します。
4. ウェブサイトのパブリック読み取りアクセスを許可するには、次のバケットポリシーをコピーし、[Bucket policy editor (バケットポリシーエディター)] に貼り付けます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PublicReadGetObject",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::Bucket-Name/*"
            ]
        }
    ]
}
```

5. `Resource` をバケット名に更新します。

   前述のバケットポリシーの例では、*`Bucket-Name`* はバケット名のプレースホルダーです。このバケットポリシーを独自のバケットで使用するには、バケット名に合わせてこの名前を更新する必要があります。

6. [Save changes] (変更の保存) をクリックします。

   バケットポリシーが正常に追加されたことを示すメッセージが表示されます。

`Policy has invalid resource` というエラーが表示された場合は、バケットポリシー内のバケット名がバケット名と一致していることを確認します。バケットポリシーの追加については、「S3 バケットポリシーを追加する方法」を参照してください。

エラーメッセージが表示され、バケットポリシーを保存できない場合は、アカウントとバケットの [パブリックアクセスをブロックする] 設定をチェックして、バケットへのパブリックアクセスを許可していることを確認します。

オブジェクトアクセスコントロールリスト

バケットポリシーを使用して、オブジェクトに対するアクセス許可を付与できます。ただし、バケットポリシーは、バケット所有者が所有するオブジェクトにのみ適用されます。バケットに、バケット所有者として所有していないオブジェクトが含まれる場合は、バケット所有者は、オブジェクトのアクセスコントロールリスト (ACL) を使用して、それらのオブジェクトへのパブリック読み取りアクセス許可を付与する必要があります。

S3 オブジェクト所有権は、Amazon S3 バケットレベルの設定で、バケットにアップロードされる新しいオブジェクト所有権を制御し、ACL を無効にするのに使用できます。デフォルトでは、オブジェクト所有権はバケット所有者の強制設定に設定され、すべての ACL は無効になります。ACL を無効にすると、バケット所有者はバケット内のすべてのオブジェクトを所有し、アクセス管理ポリシーのみを使用してデータへのアクセスを管理します。

Amazon S3 の最新のユースケースの大部分では ACL を使用する必要がなくなっています。オブジェクトごとに個別に制御する必要がある通常ではない状況を除き、ACL は無効にしておくことをお勧めします。ACL を無効にすると、誰がオブジェクトをバケットにアップロードしたかに関係なく、ポリシーを使用してバケット内のすべてのオブジェクトへのアクセスを制御できます。詳細については、「オブジェクトの所有権の制御とバケットの ACL の無効化。」を参照してください。

> **Important**
>
> 汎用バケットで S3 のオブジェクト所有者に [バケット所有者の強制] 設定を使用する場合は、ポリシーを使用して汎用バケットとその中のオブジェクトへのアクセスを許可する必要があります。バケット所有者強制設定が有効になっている場合、アクセスコントロールリスト (ACL) の設定または ACL の更新は失敗し、`AccessControlListNotSupported` エラーコードが返されます。ACL の読み取りリクエストは引き続きサポートされています。

ACL を使用してオブジェクトを公開で読み取り可能にするには、次の許可要素に示すように、AllUsers グループに READ アクセス許可を付与します。この許可要素をオブジェクト ACL に追加します。ACL の管理の詳細については、「アクセスコントロールリスト (ACL) の概要」を参照してください。

```
<Grant>
  <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
           xsi:type="Group">
    <URI>http://acs.amazonaws.com/groups/global/AllUsers</URI>
  </Grantee>
  <Permission>READ</Permission>
</Grant>
```

(オプション) ウェブトラフィックのログ記録

オプションで、静的ウェブサイトとして設定されているバケットで Amazon S3 サーバーアクセスログを有効にできます。サーバーアクセスのログ記録では、バケットに対するリクエストの詳細が記録されます。詳細については、「サーバーアクセスログによるリクエストのログ記録」を参照してください。Amazon CloudFront を使用してウェブサイトを高速化する場合は、CloudFront のログ記録を使用することもできます。詳細については、Amazon CloudFront デベロッパーガイドの「アクセスログの設定および使用」を参照してください。

静的ウェブサイトバケット用のサーバーアクセスのログ記録を有効にするには

1. Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 静的ウェブサイトとして設定しているバケットを作成したのと同じリージョンで、ログ記録用の汎用バケットを作成します (例: logs.example.com)。
3. サーバアクセスのログを記録するログファイル用のフォルダを作成します (例: logs)。
4. (オプション) CloudFront を使用してウェブサイトのパフォーマンスを向上させる場合は、CloudFront ログファイル用のフォルダを作成します (例: cdn)。

   詳細については、「Amazon CloudFront によるウェブサイトの高速化」を参照してください。
5. [Buckets (バケット)] リストで、バケット名を選択します。
6. [プロパティ] を選択します。
7. [Server access logging (サーバーアクセスのログ記録)] で、[Edit (編集)] を選択します。
8. [Enable] を選択します。

9. [Target bucket (ターゲットバケット)] で、サーバーアクセスログのバケットとフォルダの宛先を選択します。

   - フォルダとバケットの場所を参照します。
     1. [Browse S3(S3 の参照)] を選択します。
     2. バケット名を選択し、ログフォルダを選択します。
     3. [Choose path (パスの選択)] を選択します。
   - S3 バケットパスを入力します (例: **`s3://logs.example.com/logs/`**)。
10. [Save changes] (変更の保存) をクリックします。

    ログバケットで、ログにアクセスできるようになりました。Amazon S3 は 2 時間おきにログバケットにウェブサイトアクセスログを書き込みます。

(オプション) ウェブページリダイレクトの設定

Amazon S3 バケットに対して静的ウェブサイトホスティングが設定されている場合は、バケットまたはそのバケット内のオブジェクトに対してリダイレクトを設定できます。リダイレクトを設定するには、次のオプションがあります。

トピック

- バケットのウェブサイトエンドポイントに対するリクエストを別のバケットまたはドメインにリダイレクトする
- 高度な条件付きリダイレクトを使用するようにリダイレクトルールを設定する
- オブジェクトのリクエストをリダイレクトする

バケットのウェブサイトエンドポイントに対するリクエストを別のバケットまたはドメインにリダイレクトする

バケットのウェブサイトエンドポイントに対するすべてのリクエストを、別のバケットまたはドメインにリダイレクトできます。すべてのリクエストをリダイレクトする場合、ウェブサイトエンドポイントに対して行われたすべてのリクエストが指定されたバケットまたはドメインにリダイレクトされます。

例えば、ルートドメインが `example.com` であり、`http://example.com` および `http://www.example.com` の両方のためのリクエストに対応する場合は、`example.com` および

www.example.com という 2 つのバケットを作成する必要があります。次に、example.com バケット内のコンテンツを保持し、他の www.example.com バケットからすべてのリクエストを example.com バケットにリダイレクトするように設定します。詳細については、「カスタムドメイン名を使用して静的ウェブサイトを設定する」を参照してください。

バケットウェブサイトエンドポイントにリクエストをリダイレクトするには

1. https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開きます。
2. [Buckets (バケット)] で、リクエストをリダイレクトするバケットの名前 (www.example.com など)を選択します。
3. [プロパティ] を選択します。
4. [静的ウェブサイトホスティング] で [編集] を選択します。
5. [Redirect requests for an object (オブジェクトのリクエストをリダイレクト)] を選択します。
6. [Host name (ホスト名)] ボックスに、バケットまたはカスタムドメインのウェブサイトエンドポイントを入力します。

   たとえば、ルートドメインアドレスにリダイレクトする場合は、「**example.com**」と入力します。
7. [Protocol (プロトコル)] で、リダイレクトされた要求のプロトコル ([none]、[http]、または [https]) を選択します。

   プロトコルを指定しない場合、デフォルトのオプションは [none] です。
8. [Save changes] (変更の保存) をクリックします。

高度な条件付きリダイレクトを使用するようにリダイレクトルールを設定する

高度な条件付きリダイレクトルールを使用すると、条件に応じてリクエストのルーティング先を変えることができます。この条件として使用できるのは、特定のオブジェクトキー名、リクエストの中のプレフィックス、またはレスポンスコードです。たとえば、バケット内のあるオブジェクトを削除する、または名前を変更する場合は、リクエストを別のオブジェクトにリダイレクトするルーティングルールを追加します。フォルダを使用できなくする場合は、ルーティングルールを追加して別のウェブページにリクエストをリダイレクトできます。ルーティングルールは、エラー状態を処理するために追加することもできます。その場合は、エラーの処理時に、エラーを発生させたリクエストを別のドメインにリダイレクトします。

バケットに対して静的ウェブサイトホスティングを有効にすると、オプションで高度なリダイレクトルールを指定できます。Amazon S3 では、ウェブサイト設定ごとのルーティングルールの数が 50 に制限されています。50 を超えるルーティングルールが必要な場合は、オブジェクトリダイレクトを使用できます。詳細については、「S3 コンソールの使用」を参照してください。

REST API を使用したルーティングルールの設定の詳細については、Amazon Simple Storage Service API リファレンスの「PutBucketWebsite」を参照してください。

> **Important**
>
> 新しい Amazon S3 コンソールでリダイレクトルールを作成するには、JSON を使用する必要があります。JSON の例については、「リダイレクトルールの例」を参照してください。

静的ウェブサイトのリダイレクトルールを設定するには

静的ウェブサイトホスティングがすでに有効になっているバケットのリダイレクトルールを追加するには、次の手順に従います。

1. Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 左のナビゲーションペインで、[汎用バケット] を選択します。
3. バケットリストで、静的ウェブサイトとして設定したバケットの名前を選択します。
4. [プロパティ] を選択します。
5. [静的ウェブサイトホスティング] で [編集] を選択します。
6. [Redirection rules (リダイレクトルール)] ボックスに、JSON にリダイレクトルールを入力します。

   S3 コンソールでは、JSON を使用してルールを記述します。JSON の例については、「リダイレクトルールの例」を参照してください。Amazon S3 では、ウェブサイト設定ごとのルーティングルールの数が 50 に制限されています。
7. [Save changes] (変更の保存) をクリックします。

ルーティングルール要素

JSON および XML でウェブサイト設定のルーティングルールを定義するための一般的な構文を次に示します。新しい S3 コンソールでリダイレクトルールを設定するには、JSON を使用する必要があります。JSON の例については、「リダイレクトルールの例」を参照してください。

JSON

```
[
    {
      "Condition": {
        "HttpErrorCodeReturnedEquals": "string",
        "KeyPrefixEquals": "string"
      },
      "Redirect": {
        "HostName": "string",
        "HttpRedirectCode": "string",
        "Protocol": "http"|"https",
        "ReplaceKeyPrefixWith": "string",
        "ReplaceKeyWith": "string"
      }
    }
  ]

Note: Redirect must each have at least one child element. You can have either
 ReplaceKeyPrefix with or ReplaceKeyWith but not both.
```

XML

```
<RoutingRules> =
    <RoutingRules>
         <RoutingRule>...</RoutingRule>
         [<RoutingRule>...</RoutingRule>
         ...]
    </RoutingRules>

<RoutingRule> =
   <RoutingRule>
      [ <Condition>...</Condition> ]
      <Redirect>...</Redirect>
   </RoutingRule>

<Condition> =
   <Condition>
      [ <KeyPrefixEquals>...</KeyPrefixEquals> ]
      [ <HttpErrorCodeReturnedEquals>...</HttpErrorCodeReturnedEquals> ]
   </Condition>
    Note: <Condition> must have at least one child element.
```

```
<Redirect> =
   <Redirect>
      [ <HostName>...</HostName> ]
      [ <Protocol>...</Protocol> ]
      [ <ReplaceKeyPrefixWith>...</ReplaceKeyPrefixWith>  ]
      [ <ReplaceKeyWith>...</ReplaceKeyWith> ]
      [ <HttpRedirectCode>...</HttpRedirectCode> ]
   </Redirect>

Note: <Redirect> must have at least one child element. You can have either
 ReplaceKeyPrefix with or ReplaceKeyWith but not both.
```

次の表は、ルーティングルールの要素をまとめたものです。

名前	説明
RoutingRules	RoutingRule 要素のコレクションを入れるコンテナ。
RoutingRule	条件とリダイレクトを明示したルール。この条件が満たされたときにこのリダイレクトが適用されます。 条件: • RoutingRules コンテナには、少なくとも 1 つのルーティングルールを含める必要があります。
Condition	条件を記述するためのコンテナ。この条件が満たされているときに、指定されたリダイレクトが適用されます。ルーティングルールの中に条件がない場合は、そのルールはすべてのリクエストに適用されます。
KeyPrefixEquals	リクエストをリダイレクトするオブジェクトキー名のプレフィックス。 KeyPrefixEquals HttpErrorCodeReturnedEquals が指定されていない場合は、 は必須です。KeyPrefixEquals と

名前	説明
	HttpErrorCodeReturnedEquals の両方が指定されている場合は、両方が真である場合に、条件が満たされていると見なされます。
HttpErrorCodeReturnedEquals	この HTTP エラーコードに一致している場合にのみ、リダイレクトが適用されます。エラーが発生した場合、エラーコードがこの値に等しい場合は、指定されたリダイレクトが適用されます。 HttpErrorCodeReturnedEquals KeyPrefixEquals が指定されていない場合は、 は必須です。KeyPrefixEquals と HttpErrorCodeReturnedEquals の両方が指定されている場合は、両方が真である場合に、条件が満たされていると見なされます。
Redirect	コンテナ要素。リクエストのリダイレクトに関する指示を表すのに使用されます。リクエストを別のホストや別のページにリダイレクトすることも、別のプロトコルの使用を指定することもできます。RoutingRule には Redirect 要素が必要です。1 つの Redirect 要素の中に、Protocol、HostName、ReplaceKeyPrefixWith 、ReplaceKeyWith 、HttpRedirectCode の兄弟要素のうち 1 つ以上が存在する必要があります。
Protocol	レスポンスとして返される http ヘッダーで使用されるプロトコル (https または Location) 。 同レベルの要素の 1 つが指定されている場合、Protocol は省略可能です。
HostName	レスポンスとして返される Location ヘッダーで使用されるホスト名。 同レベルの要素の 1 つが指定されている場合、HostName は省略可能です。

名前	説明
ReplaceKeyPrefixWith	リダイレクトリクエストの中の KeyPrefixEquals の値を置き換えるオブジェクトキー名のプレフィックス。 同レベルの要素の 1 つが指定されている場合、ReplaceKeyPrefixWith は省略可能です。これを指定できるのは、ReplaceKeyWith が指定されていない場合のみです。
ReplaceKeyWith	レスポンスとして返される Location ヘッダーで使用されるオブジェクトキー。 同レベルの要素の 1 つが指定されている場合、ReplaceKeyWith は省略可能です。これを指定できるのは、ReplaceKeyPrefixWith が指定されていない場合のみです。
HttpRedirectCode	レスポンスとして返される Location ヘッダーで使用される HTTP リダイレクトコード。 同レベルの要素の 1 つが指定されている場合、HttpRedirectCode は省略可能です。

リダイレクトルールの例

次の例では、一般的なリダイレクトタスクについて説明します。

> **Important**
> 新しい Amazon S3 コンソールでリダイレクトルールを作成するには、JSON を使用する必要があります。

Example 1: キープレフィックスの名前を変更した後にリダイレクトする

バケットに次のオブジェクトが含まれているとします。

- index.html

- docs/article1.html
- docs/article2.html

フォルダ名を docs/ から documents/ に変更することにしました。この変更を行った後は、プレフィックス docs/ に対するリクエストを documents/ にリダイレクトする必要があります。たとえば、docs/article1.html に対するリクエストを documents/article1.html にリダイレクトします。

この場合、次のルーティングルールをウェブサイト設定に追加します。

JSON

```
[
    {
        "Condition": {
            "KeyPrefixEquals": "docs/"
        },
        "Redirect": {
            "ReplaceKeyPrefixWith": "documents/"
        }
    }
]
```

XML

```
  <RoutingRules>
    <RoutingRule>
    <Condition>
      <KeyPrefixEquals>docs/</KeyPrefixEquals>
    </Condition>
    <Redirect>
      <ReplaceKeyPrefixWith>documents/</ReplaceKeyPrefixWith>
    </Redirect>
    </RoutingRule>
  </RoutingRules>
```

Example 2: 削除されたフォルダに対するリクエストをページにリダイレクトする

images/フォルダ (つまり、キープレフィックスが images/ のすべてのオブジェクト) を削除するとします。ルーティングルールを追加し、その中で、キープレフィックス images/ を持つオブジェ

クトに対するリクエストをすべて folderdeleted.html というページにリダイレクトするように設定します。

JSON

```
[
    {
        "Condition": {
            "KeyPrefixEquals": "images/"
        },
        "Redirect": {
            "ReplaceKeyWith": "folderdeleted.html"
        }
    }
]
```

XML

```
  <RoutingRules>
    <RoutingRule>
    <Condition>
       <KeyPrefixEquals>images/</KeyPrefixEquals>
    </Condition>
    <Redirect>
      <ReplaceKeyWith>folderdeleted.html</ReplaceKeyWith>
    </Redirect>
    </RoutingRule>
  </RoutingRules>
```

Example 3: HTTP エラーの場合にリダイレクトする

リクエストされたオブジェクトが見つからないときに、リクエストを Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにリダイレクトするとします。リダイレクトルールを追加し、その中で、HTTP ステータスコード 404 (Not Found) が返されたときに、リクエストを処理する Amazon EC2 インスタンスにリダイレクトするように設定します。

次に示す例では、オブジェクトキープレフィックス report-404/ もリダイレクトに挿入しています。たとえば、ExamplePage.html というページをリクエストした結果が HTTP 404 エラーとなったときは、指定の Amazon EC2 インスタンスにある report-404/ExamplePage.html というページにリクエストをリダイレクトします。ルーティングルールが何も設定されていない場合に HTTP エラー 404 が発生したときは、設定内で指定されているエラードキュメントが返されます。

JSON

```
[
    {
        "Condition": {
            "HttpErrorCodeReturnedEquals": "404"
        },
        "Redirect": {
            "HostName": "ec2-11-22-333-44.compute-1.amazonaws.com",
            "ReplaceKeyPrefixWith": "report-404/"
        }
    }
]
```

XML

```
  <RoutingRules>
    <RoutingRule>
    <Condition>
      <HttpErrorCodeReturnedEquals>404</HttpErrorCodeReturnedEquals >
    </Condition>
    <Redirect>
      <HostName>ec2-11-22-333-44.compute-1.amazonaws.com</HostName>
      <ReplaceKeyPrefixWith>report-404/</ReplaceKeyPrefixWith>
    </Redirect>
    </RoutingRule>
  </RoutingRules>
```

オブジェクトのリクエストをリダイレクトする

オブジェクトのメタデータでウェブサイトのリダイレクト場所を設定することで、オブジェクトのリクエストを別のオブジェクトまたは URL にリダイレクトできます。リダイレクトを設定するには、オブジェクトメタデータに `x-amz-website-redirect-location` プロパティを追加します。Amazon S3 コンソールで、オブジェクトのメタデータ内の [Website Redirect Location (ウェブサイトのリダイレクト場所)] を設定できます。Amazon S3 API を使用する場合は、`x-amz-website-redirect-location` を設定します。ウェブサイトは 301 リダイレクトとしてオブジェクトを解釈します。

リクエストを別のオブジェクトにリダイレクトするには、リダイレクト場所をターゲットオブジェクトのキーに設定します。リクエストを外部 URL にリダイレクトするには、リダイレクト場所を目的

の URL に設定します。オブジェクトメタデータの詳細については、システムで定義されたオブジェクトメタデータ を参照してください。

ページリダイレクトを設定するときに、ソースオブジェクトコンテンツを維持することも、削除することもできます。たとえば、バケットに page1.html オブジェクトがある場合、このページのリクエストを別のオブジェクト page2.html にリダイレクトできます。これには2つのオプションがあります。

- page1.html オブジェクトのコンテンツを維持して、ページリクエストをリダイレクトします。
- page1.html のコンテンツを削除し、page1.html という名前の 0 バイトのオブジェクトをアップロードして、既存のオブジェクトを置き換え、ページリクエストをリダイレクトします。

S3 コンソールの使用

1. https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開きます。
2. [Buckets (バケット)] リストで、静的ウェブサイトとして設定したバケットの名前を選択します (例: example.com)。
3. [Objects (オブジェクト)] でオブジェクトを選択します。
4. [Actions (アクション)] を選択し、[Edit metadata (メタデータの編集)] を選択します。
5. [メタデータ] を選択します。
6. [Add Metadata (メタデータの追加)] を選択します。
7. [Type (タイプ)] で、[System Defined (システム定義)] を選択します。
8. [Key (キー)]で、[x-amz-website-redirect-location] を選択します。
9. [値] に、リダイレクト先のオブジェクトのキー名を入力します (例: /page2.html)。

   同じバケット内の別のオブジェクトでは、値の / プレフィックスが必要です。値を外部 URL に設定することもできます (例: http://www.example.com)。
10. [Edit metadata (メタデータの編集)] を選択します。

REST API の使用

次の Amazon S3 API アクションは、リクエストの x-amz-website-redirect-location ヘッダーをサポートしています。Amazon S3 はオブジェクトメタデータのヘッダー値を x-amz-website-redirect-location として保存します。

- PUT Object

- Initiate Multipart Upload
- POST Object
- PUT Object − Copy

ウェブサイトホスティング用に設定されたバケットには、ウェブサイトエンドポイントと REST エンドポイントの両方があります。リクエストされたページが 301 リダイレクトとして設定されている場合の結果は、リクエストのエンドポイントに応じて、次のようになると考えられます。

- リージョン固有のウェブサイトエンドポイント – Amazon S3 は、`x-amz-website-redirect-location` プロパティの値に従ってページリクエストをリダイレクトします。
- REST エンドポイント – Amazon S3 はページリクエストをリダイレクトしません。リクエストされたオブジェクトを返します。

エンドポイントの詳細については、「ウェブサイトエンドポイントと REST API エンドポイントの主な違い」を参照してください。

ページリダイレクトを設定する場合、オブジェクトのコンテンツを維持するか、削除できます。たとえば、バケットに `page1.html` というオブジェクトがあるとします。

- `page1.html` のコンテンツを維持し、ページリクエストのリダイレクトのみを行う場合は、PUT Object - Copy リクエストを送信して新しい `page1.html` オブジェクトを作成し、送信元として既存の `page1.html` オブジェクトを使用するように設定します。リクエストに、`x-amz-website-redirect-location` ヘッダーを設定します。リクエストが完了すると、元のページのコンテンツは変更されないままですが、Amazon S3 によりページへのすべてのリクエストは指定されたリダイレクト場所にリダイレクトされます。
- `page1.html` オブジェクトのコンテンツを削除してこのページに対するリクエストをリダイレクトするには、PUT Object リクエストを送信して 0 バイトのオブジェクトをアップロードします。このオブジェクトには、同じオブジェクトキー `page1.html` を付けます。この PUT リクエストの中で、`x-amz-website-redirect-location` の `page1.html` を新しいオブジェクトに設定します。このリクエストが完了すると、`page1.html` にはコンテンツがない状態になり、リクエストは `x-amz-website-redirect-location` で指定された場所にリダイレクトされます。

GET Object アクションを使用して、他のオブジェクトメタデータと一緒にオブジェクトを取得すると、Amazon S3 はレスポンスで `x-amz-website-redirect-location` ヘッダーを返します。

Cross-Origin Resource Sharing (CORS) の使用

Cross-Origin Resource Sharing (CORS) は、特定のドメインにロードされたクライアントウェブアプリケーションが異なるドメイン内のリソースと通信する方法を定義します。Amazon S3 の CORS のサポートによって、Amazon S3 でリッチなクライアント側ウェブアプリケーションを構築し、Amazon S3 リソースへのクロスオリジンアクセスを選択的に許可できます。

このセクションでは、CORS の概要を示します。サブトピックでは、Amazon S3 コンソールを使用するか、Amazon S3 REST API や AWS SDK を使用して、プログラムによって CORS を有効にする方法について説明します。

Cross-Origin Resource Sharing: ユースケースのシナリオ

CORS のユースケースの例を以下に示します。

シナリオ 1

「Amazon S3 を使用して静的ウェブサイトをホスティングする」で説明されているように、`website` という名前の Amazon S3 バケットでウェブサイトをホストしているとします。ユーザーは、次のウェブサイトエンドポイントをロードします。

```
http://website.s3-website.us-east-1.amazonaws.com
```

このバケットに保存されているウェブページで JavaScript を使用し、バケットの Amazon S3 の API エンドポイント `website.s3.us-east-1.amazonaws.com` を使用して、同じバケットに対して認証済みの GET および PUT リクエストを行います。ブラウザは通常、それらのリクエストを許可しないように、JavaScript をブロックしますが、CORS を使用することにより、`website.s3-website.us-east-1.amazonaws.com` からのクロスオリジンリクエストを明示的に有効にするようにバケットを設定できます。

シナリオ 2

S3 バケットからウェブフォントをホストする必要があるとします。ここでも、ブラウザでウェブフォントを読み込むために CORS チェック (プリフライトチェックと呼ばれます) が必要です。ウェブフォントをホストしているバケットを、いずれのオリジンもこれらのリクエストを実行できるように設定します。

Amazon S3 でのバケットの CORS 設定の評価方法

Amazon S3 がブラウザからプリフライトリクエストを受け取ると、バケットの CORS 設定を評価し、受信ブラウザリクエストに一致する最初の `CORSRule` ルールを使用して、クロスオリジンリクエストを有効にします。ルールが一致するには、次の条件を満たしている必要があります。

- バケットへの CORS リクエストの `Origin` ヘッダーは、CORS 設定の `AllowedOrigins` エレメントのオリジンと一致している必要があります。
- バケットへの CORS リクエストの `Access-Control-Request-Method` で指定されている HTTP メソッドは、CORS 設定の `AllowedMethods` エレメントに含まれているメソッドと一致している必要があります。
- プリフライトリクエストの `Access-Control-Request-Headers` ヘッダーに含まれているヘッダーは、CORS 設定の `AllowedHeaders` エレメントのヘッダーと一致している必要があります。

> **Note**
>
> バケットの CORS 設定を有効にすると、ACL とポリシーが引き続き適用されます。

Object Lambda アクセスポイントで CORS をサポートする方法

S3 Object Lambda がブラウザからリクエストを受信するか、リクエストに `Origin` ヘッダーが含まれている場合、S3 Object Lambda は常に `"AllowedOrigins":"*"` ヘッダーフィールドを追加します。

CORS の使用の詳細については、次のトピックを参照してください。

トピック

- CORS 設定のエレメント
- Cross-Origin Resource Sharing (CORS) の設定
- CORS のテスト
- CORS のトラブルシューティング

CORS 設定のエレメント

クロスオリジンリクエストを許可するようバケットを設定するには、CORS 設定を作成します。CORS 設定は、バケットへのアクセスを許可するオリジン、各オリジンでサポートされるオペレーション (HTTP メソッド)、その他のオペレーション固有情報を識別するエレメントを持つ XML ドキュメントです。設定には、最大 100 のルールを追加できます。CORS 設定を `cors` サブリソースとしてバケットに追加できます。

S3 コンソールで CORS を設定する場合は、JSON を使用して CORS 設定を作成する必要があります。新しい S3 コンソールでは、JSON CORS 設定のみがサポートされます。

CORS 設定とそのエレメントの詳細については、以下のトピックを参照してください。CORS 設定を追加する方法については、Cross-Origin Resource Sharing (CORS) の設定 を参照してください。

> **Important**
>
> S3 コンソールでは、CORS 設定は JSON である必要があります。

トピック

- AllowedMethods 要素
- AllowedOrigins 要素
- AllowedHeaders 要素
- ExposeHeaders 要素
- MaxAgeSeconds 要素
- CORS 設定の例

`AllowedMethods` 要素

CORS 設定では、`AllowedMethods` エレメントに次の値を指定できます。

- GET
- PUT
- POST
- DELETE
- HEAD

AllowedOrigins 要素

AllowedOrigins エレメントに、クロスドメインリクエストを許可するオリジンを指定します (http://www.example.com など)。オリジン文字列には、1 つのワイルドカード文字 (*) のみを含めることができます。例えば、http://*.example.com などです。オプションで、オリジンに * を指定して、すべてのオリジンでクロスオリジンリクエストを送信できるようにすることができます。さらに、https を指定して、セキュリティで保護されたオリジンのみを有効にすることもできます。

AllowedHeaders 要素

AllowedHeaders エレメントは、Access-Control-Request-Headers ヘッダーによって、プリフライトリクエストで許可されるヘッダーを指定します。Access-Control-Request-Headers ヘッダー内の各ヘッダー名は、エレメントの対応するエントリと一致している必要があります。Amazon S3 は、レスポンスで、リクエストされたヘッダーのうち許可されたヘッダーのみを送信します。Amazon S3 へのリクエストで使用できるヘッダーのサンプルリストについては、Amazon Simple Storage Service API リファレンスの一般的なリクエストヘッダー を参照してください。

設定内の各 AllowedHeaders 文字列には、最大 1 つのワイルドカード文字 (*) を含めることができます。例えば、<AllowedHeader>x-amz-*</AllowedHeader> は Amazon 固有のすべてのヘッダーを有効にします。

ExposeHeaders 要素

各 ExposeHeader エレメントは、顧客がアプリケーションから (例えば、JavaScript XMLHttpRequest オブジェクトから) アクセスできるようにするレスポンス内のヘッダーを識別します。一般的な Amazon S3 レスポンスヘッダーのリストについては、Amazon Simple Storage Service API リファレンスの一般的なリクエストヘッダー を参照してください。

MaxAgeSeconds 要素

MaxAgeSeconds エレメントは、リソース、HTTP メソッド、およびオリジンによって識別されたプリフライトリクエストのレスポンスをブラウザでキャッシュできる時間を秒単位で指定します。

CORS 設定の例

ウェブサイトへのアクセスに Amazon S3 ウェブサイトエンドポイントを使用する代わりに、所有するドメイン、例えば example1.com を使用してコンテンツを配信できます。独自のドメインの使用

については、チュートリアル: Route 53 に登録されたカスタムドメインを使用した静的ウェブサイトの設定 を参照してください。

次の CORS 設定の例には 3 つのルールがあり、CORSRule エレメントとして指定されています。

- 最初のルールは、http://www.example1.com オリジンからのクロスオリジン PUT、POST、および DELETE リクエストを許可します。このルールは、Access-Control-Request-Headers ヘッダーによって、プリフライト OPTIONS リクエスト内のすべてのヘッダーも許可します。プリフライト OPTIONS リクエストへのレスポンスとして、Amazon S3 はリクエストされたヘッダーを返します。
- 2 つ目のルールは最初のルールと同じクロスオリジンリクエストを許可しますが、このルールは別のオリジン http://www.example2.com に適用されます。
- 3 つ目のルールは、すべてのオリジンからのクロスオリジン GET リクエストを許可します。ワイルドカード文字 * は、すべてのオリジンを表します。

JSON

```
[
    {
        "AllowedHeaders": [
            "*"
        ],
        "AllowedMethods": [
            "PUT",
            "POST",
            "DELETE"
        ],
        "AllowedOrigins": [
            "http://www.example1.com"
        ],
        "ExposeHeaders": []
    },
    {
        "AllowedHeaders": [
            "*"
        ],
        "AllowedMethods": [
            "PUT",
            "POST",
            "DELETE"
        ],
```

```
        "AllowedOrigins": [
            "http://www.example2.com"
        ],
        "ExposeHeaders": []
    },
    {
        "AllowedHeaders": [],
        "AllowedMethods": [
            "GET"
        ],
        "AllowedOrigins": [
            "*"
        ],
        "ExposeHeaders": []
    }
]
```

XML

```
<CORSConfiguration>
 <CORSRule>
   <AllowedOrigin>http://www.example1.com</AllowedOrigin>

   <AllowedMethod>PUT</AllowedMethod>
   <AllowedMethod>POST</AllowedMethod>
   <AllowedMethod>DELETE</AllowedMethod>

   <AllowedHeader>*</AllowedHeader>
 </CORSRule>
 <CORSRule>
   <AllowedOrigin>http://www.example2.com</AllowedOrigin>

   <AllowedMethod>PUT</AllowedMethod>
   <AllowedMethod>POST</AllowedMethod>
   <AllowedMethod>DELETE</AllowedMethod>

   <AllowedHeader>*</AllowedHeader>
 </CORSRule>
 <CORSRule>
   <AllowedOrigin>*</AllowedOrigin>
   <AllowedMethod>GET</AllowedMethod>
 </CORSRule>
</CORSConfiguration>
```

次の CORS 設定に示すように、CORS 設定ではオプションの設定パラメータも使用できます。この例で、CORS 設定は http://www.example.com オリジンからのクロスオリジン PUT、POST、および DELETE の各リクエストを許可します。

JSON

```
[
    {
        "AllowedHeaders": [
            "*"
        ],
        "AllowedMethods": [
            "PUT",
            "POST",
            "DELETE"
        ],
        "AllowedOrigins": [
            "http://www.example.com"
        ],
        "ExposeHeaders": [
            "x-amz-server-side-encryption",
            "x-amz-request-id",
            "x-amz-id-2"
        ],
        "MaxAgeSeconds": 3000
    }
]
```

XML

```
<CORSConfiguration>
 <CORSRule>
   <AllowedOrigin>http://www.example.com</AllowedOrigin>
   <AllowedMethod>PUT</AllowedMethod>
   <AllowedMethod>POST</AllowedMethod>
   <AllowedMethod>DELETE</AllowedMethod>
   <AllowedHeader>*</AllowedHeader>
  <MaxAgeSeconds>3000</MaxAgeSeconds>
  <ExposeHeader>x-amz-server-side-encryption</
ExposeHeader>
  <ExposeHeader>x-amz-request-id</
ExposeHeader>
  <ExposeHeader>x-amz-id-2</ExposeHeader>
```

```
 </CORSRule>
</CORSConfiguration>
```

前述の設定の CORSRule エレメントには、次のオプションのエレメントが含まれます。

- MaxAgeSeconds— 指定したリソースのプリフライト OPTIONS リクエストへの Amazon S3 レスポンスをブラウザでキャッシュする時間を秒単位で指定します (この例では 3,000)。レスポンスのキャッシュにより、元のリクエストが繰り返された場合に、ブラウザは Amazon S3 にプリフライトリクエストを送信する必要がありません。
- ExposeHeaders – 顧客がアプリケーションから (例えば JavaScript x-amz-server-side-encryption オブジェクトから) アクセスできるレスポンスヘッダー (この例では x-amz-request-id、x-amz-id-2、および XMLHttpRequest) を識別します。

Cross-Origin Resource Sharing (CORS) の設定

Cross-Origin Resource Sharing (CORS) は、特定のドメインにロードされたクライアントウェブアプリケーションが異なるドメイン内のリソースと通信する方法を定義します。Amazon S3 の CORS のサポートによって、Amazon S3 でリッチなクライアント側ウェブアプリケーションを構築し、Amazon S3 リソースへのクロスオリジンアクセスを選択的に許可できます。

このセクションでは、Amazon S3 コンソール、Amazon S3 REST API、および AWS SDK を使用して CORS を有効にする方法について説明します。クロスオリジンリクエストを許可するようバケットを設定するには、CORS 設定をバケットに追加します。CORS 設定は、バケットへのアクセスを許可するオリジン、各オリジンでサポートされるオペレーション (HTTP メソッド)、およびその他のオペレーション固有情報を識別するルールを定義するドキュメントです。S3 コンソールでは、CORS 設定は JSON ドキュメントである必要があります。

JSON および XML での CORS 設定の例については、CORS 設定のエレメント を参照してください。

S3 コンソールの使用

このセクションでは、Amazon S3 コンソールを使用して Cross-Origin Resource Sharing (CORS) 設定を S3 バケットに追加する方法について説明します。

バケットで CORS を有効にすると、アクセスコントロールリスト (ACL) およびその他のアクセス許可ポリシーが引き続き適用されます。

> **Important**
>
> S3 コンソールでは、CORS 設定は JSON である必要があります。JSON および XML での CORS 設定の例については、CORS 設定のエレメント を参照してください。

CORS 設定を S3 バケットに追加するには

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 左のナビゲーションペインで、[汎用バケット] を選択します。
3. バケットリストで、バケットポリシーを作成するバケットの名前を選択します。
4. [Permissions] を選択します。
5. [CORS (クロスオリジンリソース共有)] セクションで、[編集] を選択します。
6. [CORS configuration editor (CORS 構成エディタ)] テキストボックスに、新しい CORS 設定を入力またはコピーして貼り付けるか、既存の設定を編集します。

   CORS 設定は JSON ファイルです。エディタに入力するテキストは有効な JSON である必要があります。詳細については、CORS 設定のエレメント を参照してください。
7. [Save changes] (変更の保存) をクリックします。

> **Note**
>
> Amazon S3 では、[CORS configuration editor (CORS 構成エディタ)] のタイトルの横に、バケットの Amazon リソースネーム (ARN) が表示されます。ARN の詳細については、Amazon Web Services 全般のリファレンス の「Amazon リソースネーム (ARN) および AWS サービスの名前空間」を参照してください。

AWS SDK の使用

AWS SDK を使用して、バケットの Cross-Origin Resource Sharing (CORS) を管理できます。CORS の詳細については、Cross-Origin Resource Sharing (CORS) の使用 を参照してください。

以下の例を参照してください。

- CORS 設定を作成し、バケット上で設定を指定する

- 設定を取得し、ルールを追加してその設定を変更する
- 変更された設定をバケットに追加する
- 設定を削除する

Java

Example

Example

作業サンプルの作成方法およびテスト方法については、「AWS SDK for Java のデベロッパーガイド」の「使用開始」を参照してください。

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.BucketCrossOriginConfiguration;
import com.amazonaws.services.s3.model.CORSRule;

import java.io.IOException;
import java.util.ArrayList;
import java.util.Arrays;
import java.util.List;

public class CORS {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";

        // Create two CORS rules.
        List<CORSRule.AllowedMethods> rule1AM = new
 ArrayList<CORSRule.AllowedMethods>();
        rule1AM.add(CORSRule.AllowedMethods.PUT);
        rule1AM.add(CORSRule.AllowedMethods.POST);
        rule1AM.add(CORSRule.AllowedMethods.DELETE);
        CORSRule rule1 = new
 CORSRule().withId("CORSRule1").withAllowedMethods(rule1AM)
```

```
                .withAllowedOrigins(Arrays.asList("http://*.example.com"));

        List<CORSRule.AllowedMethods> rule2AM = new
ArrayList<CORSRule.AllowedMethods>();
        rule2AM.add(CORSRule.AllowedMethods.GET);
        CORSRule rule2 = new
CORSRule().withId("CORSRule2").withAllowedMethods(rule2AM)
                .withAllowedOrigins(Arrays.asList("*")).withMaxAgeSeconds(3000)
                .withExposedHeaders(Arrays.asList("x-amz-server-side-encryption"));

        List<CORSRule> rules = new ArrayList<CORSRule>();
        rules.add(rule1);
        rules.add(rule2);

        // Add the rules to a new CORS configuration.
        BucketCrossOriginConfiguration configuration = new
BucketCrossOriginConfiguration();
        configuration.setRules(rules);

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();

            // Add the configuration to the bucket.
            s3Client.setBucketCrossOriginConfiguration(bucketName, configuration);

            // Retrieve and display the configuration.
            configuration = s3Client.getBucketCrossOriginConfiguration(bucketName);
            printCORSConfiguration(configuration);

            // Add another new rule.
            List<CORSRule.AllowedMethods> rule3AM = new
ArrayList<CORSRule.AllowedMethods>();
            rule3AM.add(CORSRule.AllowedMethods.HEAD);
            CORSRule rule3 = new
CORSRule().withId("CORSRule3").withAllowedMethods(rule3AM)
                    .withAllowedOrigins(Arrays.asList("http://www.example.com"));

            rules = configuration.getRules();
            rules.add(rule3);
            configuration.setRules(rules);
            s3Client.setBucketCrossOriginConfiguration(bucketName, configuration);
```

```
            // Verify that the new rule was added by checking the number of rules in
the
            // configuration.
            configuration = s3Client.getBucketCrossOriginConfiguration(bucketName);
            System.out.println("Expected # of rules = 3, found " +
configuration.getRules().size());

            // Delete the configuration.
            s3Client.deleteBucketCrossOriginConfiguration(bucketName);
            System.out.println("Removed CORS configuration.");

            // Retrieve and display the configuration to verify that it was
            // successfully deleted.
            configuration = s3Client.getBucketCrossOriginConfiguration(bucketName);
            printCORSConfiguration(configuration);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }

    private static void printCORSConfiguration(BucketCrossOriginConfiguration
configuration) {
        if (configuration == null) {
            System.out.println("Configuration is null.");
        } else {
            System.out.println("Configuration has " +
configuration.getRules().size() + " rules\n");

            for (CORSRule rule : configuration.getRules()) {
                System.out.println("Rule ID: " + rule.getId());
                System.out.println("MaxAgeSeconds: " + rule.getMaxAgeSeconds());
                System.out.println("AllowedMethod: " + rule.getAllowedMethods());
                System.out.println("AllowedOrigins: " + rule.getAllowedOrigins());
                System.out.println("AllowedHeaders: " + rule.getAllowedHeaders());
                System.out.println("ExposeHeader: " + rule.getExposedHeaders());
                System.out.println();
            }
```

```
        }
    }
}
```

.NET

Example

コード例を設定および実行する方法の詳細については、「AWS SDK for .NET デベロッパーガイド」の「AWS SDK for .NET の開始方法」 を参照してください。

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Collections.Generic;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class CORSTest
    {
        private const string bucketName = "*** bucket name ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;

        public static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            CORSConfigTestAsync().Wait();
        }
        private static async Task CORSConfigTestAsync()
        {
            try
            {
                // Create a new configuration request and add two rules
                CORSConfiguration configuration = new CORSConfiguration
                {
                    Rules = new System.Collections.Generic.List<CORSRule>
                        {
                          new CORSRule
```

```
                            {
                              Id = "CORSRule1",
                              AllowedMethods = new List<string> {"PUT", "POST",
 "DELETE"},
                              AllowedOrigins = new List<string> {"http://
*.example.com"}
                            },
                            new CORSRule
                            {
                              Id = "CORSRule2",
                              AllowedMethods = new List<string> {"GET"},
                              AllowedOrigins = new List<string> {"*"},
                              MaxAgeSeconds = 3000,
                              ExposeHeaders = new List<string> {"x-amz-server-side-
encryption"}
                            }
                          }
                };

                // Add the configuration to the bucket.
                await PutCORSConfigurationAsync(configuration);

                // Retrieve an existing configuration.
                configuration = await RetrieveCORSConfigurationAsync();

                // Add a new rule.
                configuration.Rules.Add(new CORSRule
                {
                    Id = "CORSRule3",
                    AllowedMethods = new List<string> { "HEAD" },
                    AllowedOrigins = new List<string> { "http://www.example.com" }
                });

                // Add the configuration to the bucket.
                await PutCORSConfigurationAsync(configuration);

                // Verify that there are now three rules.
                configuration = await RetrieveCORSConfigurationAsync();
                Console.WriteLine();
                Console.WriteLine("Expected # of rulest=3; found:{0}",
 configuration.Rules.Count);
                Console.WriteLine();
                Console.WriteLine("Pause before configuration delete. To continue,
 click Enter...");
```

```
                Console.ReadKey();

                // Delete the configuration.
                await DeleteCORSConfigurationAsync();

                // Retrieve a nonexistent configuration.
                configuration = await RetrieveCORSConfigurationAsync();
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
writing an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
writing an object", e.Message);
            }
        }

        static async Task PutCORSConfigurationAsync(CORSConfiguration configuration)
        {

            PutCORSConfigurationRequest request = new PutCORSConfigurationRequest
            {
                BucketName = bucketName,
                Configuration = configuration
            };

            var response = await s3Client.PutCORSConfigurationAsync(request);
        }

        static async Task<CORSConfiguration> RetrieveCORSConfigurationAsync()
        {
            GetCORSConfigurationRequest request = new GetCORSConfigurationRequest
            {
                BucketName = bucketName

            };
            var response = await s3Client.GetCORSConfigurationAsync(request);
            var configuration = response.Configuration;
            PrintCORSRules(configuration);
            return configuration;
        }
```

```
        static async Task DeleteCORSConfigurationAsync()
        {
            DeleteCORSConfigurationRequest request = new
 DeleteCORSConfigurationRequest
            {
                BucketName = bucketName
            };
            await s3Client.DeleteCORSConfigurationAsync(request);
        }

        static void PrintCORSRules(CORSConfiguration configuration)
        {
            Console.WriteLine();

            if (configuration == null)
            {
                Console.WriteLine("\nConfiguration is null");
                return;
            }

            Console.WriteLine("Configuration has {0} rules:",
 configuration.Rules.Count);
            foreach (CORSRule rule in configuration.Rules)
            {
                Console.WriteLine("Rule ID: {0}", rule.Id);
                Console.WriteLine("MaxAgeSeconds: {0}", rule.MaxAgeSeconds);
                Console.WriteLine("AllowedMethod: {0}", string.Join(", ",
 rule.AllowedMethods.ToArray()));
                Console.WriteLine("AllowedOrigins: {0}", string.Join(", ",
 rule.AllowedOrigins.ToArray()));
                Console.WriteLine("AllowedHeaders: {0}", string.Join(", ",
 rule.AllowedHeaders.ToArray()));
                Console.WriteLine("ExposeHeader: {0}", string.Join(", ",
 rule.ExposeHeaders.ToArray()));
            }
        }
    }
}
```

REST API の使用

バケットで CORS 設定を指定するには、AWS Management Consoleを使用できます。必要に応じて、REST リクエストを直接送信することもできます。Amazon Simple Storage Service API リファレンスの以下のセクションでは、CORS 設定に関連する REST API アクションについて説明しています。

- PutBucketCors
- GetBucketCors
- DeleteBucketCors
- OPTIONS オブジェクト

CORS のテスト

CORS 設定をテストするために、CORS プリフライトリクエストを OPTIONS メソッドで送信して、リクエストの送信が許容できる場合にサーバーが応答できるようにします。Amazon S3 がブラウザからプリフライトリクエストを受け取ると、S3 はバケットの CORS 設定を評価し、受信ブラウザリクエストに一致する最初の CORSRule ルールを使用して、クロスオリジンリクエストを有効にします。ルールが一致するには、次の条件を満たしている必要があります。

- バケットへの CORS リクエストの Origin ヘッダーは、CORS 設定の AllowedOrigins エレメントのオリジンと一致している必要があります。
- バケットへの CORS リクエストの Access-Control-Request-Method で指定されている HTTP メソッドは、CORS 設定の AllowedMethods エレメントに含まれているメソッドと一致している必要があります。
- プリフライトリクエストの Access-Control-Request-Headers ヘッダーに含まれているヘッダーは、CORS 設定の AllowedHeaders エレメントのヘッダーと一致している必要があります。

CORS 設定の例を次に示します。CORS 設定を作成するには、「CORS の設定」を参照してください。CORS 設定の例については、「CORS 設定のエレメント」を参照してください。

CORS ルールの設定とトラブルシューティングのガイダンスについては、AWS re:Post ナレッジセンターの「Amazon S3 で CORS を設定し、cURL を使用して CORS ルールを確認する方法」を参照してください。

JSON

```
[
    {
        "AllowedHeaders": [
            "Authorization"
        ],
        "AllowedMethods": [
            "GET",
            "PUT",
            "POST",
            "DELETE"
        ],
        "AllowedOrigins": [
            "http://www.example1.com"
        ],
        "ExposeHeaders":  [
             "x-amz-meta-custom-header"
        ]

    }
]
```

CORS 設定をテストするには、次の CURL コマンドを使用してプリフライト OPTIONS チェックを送信できます。CURL は、S3 とのやり取りに使用できるコマンドラインツールです。詳細については、「CURL」を参照してください。

```
curl -v -X OPTIONS \
 -H "Origin: http://www.example1.com" \
 -H "Access-Control-Request-Method: PUT" \
 -H "Access-Control-Request-Headers: Authorization" \
 -H "Access-Control-Expose-Headers: x-amz-meta-custom-header"\
    "http://bucket_name.s3.amazonaws.com/object_prefix_name"
```

上記の例では、curl -v -x OPTIONS コマンドを使用してプリフライトリクエストを S3 に送信し、S3 がクロスオリジン http://www.example1.com からオブジェクトに PUT リクエストを送信することを許可しているかどうかを問い合わせます。ヘッダー Access-Control-Request-Headers と Access-Control-Expose-Headers はオプションです。

- プリフライト OPTIONS リクエストの Access-Control-Request-Method ヘッダーに応答して、Amazon S3 は、リクエストされたメソッドが一致する場合に、許可されたメソッドのリストを返します。
- プリフライト OPTIONS リクエストの Access-Control-Request-Headers ヘッダーに応答して、Amazon S3 は、リクエストされたヘッダーが一致する場合に、許可されたヘッダーのリストを返します。
- プリフライト OPTIONS リクエストの Access-Control-Expose-Headers ヘッダーに応答して、Amazon S3 は、リクエストされたヘッダーがブラウザで実行されているスクリプトによってアクセスできるヘッダーと一致する場合に、許可されたヘッダーのリストを返します。

> **Note**
>
> プリフライトリクエストを送信するときに、いずれかの CORS リクエストヘッダーが許可されていない場合、レスポンス CORS ヘッダーは返されません。

このプリフライト OPTIONS リクエストに応答して、200 OK レスポンスを受け取ります。CORS のテスト時に受信される一般的なエラーコードと、CORS 関連の問題を解決するための詳細については、「CORS のトラブルシューティング」を参照してください。

```
< HTTP/1.1 200 OK
< Date: Fri, 12 Jul 2024 00:23:51 GMT
< Access-Control-Allow-Origin: http://www.example1.com
< Access-Control-Allow-Methods: GET, PUT, POST, DELETE
< Access-Control-Allow-Headers: Authorization
< Access-Control-Expose-Headers: x-amz-meta-custom-header
< Access-Control-Allow-Credentials: true
< Vary: Origin, Access-Control-Request-Headers, Access-Control-Request-Method
< Server: AmazonS3
< Content-Length: 0
```

CORS のトラブルシューティング

次のトピックは S3 に関連する CORS の一般的な問題をトラブルシューティングするのに役立ちます。

トピック

- 403 Forbidden エラー: このバケットでは CORS が有効になっていません

- 403 Forbidden エラー: この CORS リクエストは許可されていません
- CORS レスポンスにヘッダーが見つからない
- S3 プロキシ統合での CORS に関する考慮事項

403 Forbidden エラー: このバケットでは CORS が有効になっていません

次の `403 Forbidden` エラーは、クロスオリジンリクエストが Amazon S3 に送信されたものの、CORS が S3 バケットに設定されていない場合に発生します。

エラー: HTTP/1.1 403 Forbidden CORS レスポンス: このバケットでは CORS が有効になっていません。

CORS 設定は、バケットへのアクセスを許可するオリジン、各オリジンでサポートされるオペレーション (HTTP メソッド)、その他のオペレーション固有情報を識別するルールを持つ XML ドキュメント、つまりポリシーです。Amazon S3 コンソール、AWS SDK、および REST API を使用して S3 で CORS を設定する方法を参照してください。CORS の詳細と CORS 設定の例については、「CORS 設定のエレメント」を参照してください。

403 Forbidden エラー: この CORS リクエストは許可されていません

次の `403 Forbidden` エラーは、CORS 設定の CORS ルールがリクエスト内のデータと一致しない場合に発生します。

エラー: HTTP/1.1 403 Forbidden CORS レスポンス: この CORS リクエストは許可されていません。

この `403 Forbidden` エラーは、さまざまな理由で発生する可能性があります。

- オリジンが許可されない。
- メソッドが許可されない。
- リクエストされたヘッダーが許可されない。

Amazon S3 が受信するリクエストごとに、リクエスト内のデータと一致する CORS ルールが CORS 設定に含まれている必要があります。

オリジンが許可されない

バケットへの CORS リクエストの `Origin` ヘッダーは、CORS 設定の `AllowedOrigins` エレメントのオリジンと一致している必要があります。`AllowedOrigins` エレメントで使用されるワイルド

カード文字 ("*") は、すべての HTTP メソッドと一致することになります。AllowedOrigins エレメントを更新する方法の詳細については、「Cross-Origin Resource Sharing (CORS) の設定」を参照してください。

例えば、AllowedOrigins エレメントに http://www.example1.com ドメインのみが含まれている場合、http://www.example2.com ドメインから送信された CORS リクエストには 403 Forbidden エラーが返されます。

次の例は、AllowedOrigins エレメントに http://www.example1.com ドメインが含まれる CORS 設定の一部を示しています。

```
"AllowedOrigins":[
   "http://www.example1.com"
]
```

http://www.example2.com ドメインから送信された CORS リクエストを成功させるには、CORS 設定の AllowedOrigins エレメントに http://www.example2.com ドメインを含める必要があります。

```
"AllowedOrigins":[
   "http://www.example1.com"
   "http://www.example2.com"
]
```

メソッドが許可されない

バケットへの CORS リクエストの Access-Control-Request-Method で指定されている HTTP メソッドは、CORS 設定の AllowedMethods エレメントに含まれているメソッドと一致している必要があります。AllowedMethods で使用されるワイルドカード文字 ("*") は、すべての HTTP メソッドと一致することになります。AllowedOrigins エレメントを更新する方法の詳細については、「Cross-Origin Resource Sharing (CORS) の設定」を参照してください。

CORS 設定では、AllowedMethods エレメントに次のメソッドを指定できます。

- GET
- PUT
- POST
- DELETE
- HEAD

次の例は、AllowedMethods エレメントに GET メソッドが含まれる CORS 設定の一部を示しています。GET メソッドが含まれるリクエストのみが成功します。

```
"AllowedMethods":[
   "GET"
]
```

HTTP メソッド (例: PUT) が CORS リクエストで使用されているか、バケットへのプリフライト CORS リクエストに含まれているものの、そのメソッドが CORS 設定に存在しない場合、リクエストは 403 Forbidden エラーとなります。この CORS リクエストまたは CORS プリフライトリクエストを許可するには、CORS 設定に PUT メソッドを追加する必要があります。

```
"AllowedMethods":[
   "GET"
   "PUT"
]
```

リクエストされたヘッダーが許可されない

プリフライトリクエストの Access-Control-Request-Headers ヘッダーに含まれているヘッダーは、CORS 設定の AllowedHeaders エレメントのヘッダーと一致している必要があります。Amazon S3 へのリクエストで使用できる一般的なヘッダーのリストについては、一般的なリクエストヘッダーを参照してください。AllowedHeaders エレメントを更新する方法の詳細については、「Cross-Origin Resource Sharing (CORS) の設定」を参照してください。

次の例は、AllowedHeaders エレメントに Authorization ヘッダーが含まれる CORS 設定の一部を示しています。Authorization ヘッダーのリクエストのみが成功します。

```
"AllowedHeaders":  [
    "Authorization"
]
```

ヘッダー (例: Content-MD5) が CORS リクエストに含まれているものの、そのヘッダーが CORS 設定に存在しない場合、リクエストは 403 Forbidden エラーとなります。この CORS リクエストを許可するには、CORS 設定に Content-MD5 ヘッダーを追加する必要があります。CORS リクエストで Authorization と Content-MD5 の両方のヘッダーをバケットに渡す場合は、両方のヘッダーが CORS 設定の AllowedHeadersエレメントに含まれていることを確認します。

```
"AllowedHeaders":  [
```

```
    "Authorization"
    "Content-MD5"
]
```

CORS レスポンスにヘッダーが見つからない

CORS 設定の ExposeHeaders エレメントは、CORS リクエストに応答して、ブラウザで実行されているスクリプトやアプリケーションからのアクセスを可能にするレスポンスヘッダーを特定します。

S3 バケットに保存されているオブジェクトに、レスポンスデータとともにユーザー定義のメタデータ (x-amz-meta-custom-header など) がある場合、このカスタムヘッダーには、クライアント側の JavaScript コードからのアクセスする追加のメタデータや情報が含まれる可能性があります。ただし、デフォルトでは、セキュリティ上の理由からカスタムヘッダーへのアクセスはブラウザによってブロックされます。クライアント側の JavaScript がカスタムヘッダーにアクセスできるようにするには、CORS 設定にヘッダーを含める必要があります。

以下の例では、ExposeHeaders エレメントに x-amz-meta-custom-header1 ヘッダーが含まれています。x-amz-meta-custom-header2 は ExposeHeaders エレメントに含まれておらず、CORS 設定にありません。レスポンスでは、ExposeHeaders エレメントに含まれる値のみが返されます。リクエストの Access-Control-Expose-Headers ヘッダーに x-amz-meta-custom-header2 ヘッダーが含まれていても、レスポンスは 200 OK を返します。ただし、許可されたヘッダー (例: x-amz-meta-custom-header) のみが返されてレスポンスに表示されます。

```
"ExposeHeaders":  [
    "x-amz-meta-custom-header1"
]
```

すべてのヘッダーがレスポンスに表示されるようにするには、以下のように、許可するすべてのヘッダーを CORS 設定の ExposeHeaders エレメントに追加します。

```
"ExposeHeaders":  [
    "x-amz-meta-custom-header1",
    "x-amz-meta-custom-header2"
]
```

S3 プロキシ統合での CORS に関する考慮事項

エラーの発生時に、S3 バケットの CORS 設定を既にチェックしていて、クロスオリジンリクエストが AWS CloudFront などのプロキシに送信されている場合は、以下を試してください。

- HTTP リクエストの OPTIONS メソッドを許可するように設定を行います。
- Origin、Access-Control-Request-Headers、Access-Control-Request-Method の各ヘッダーを転送するようにプロキシを設定します。
- オリジンヘッダーをキャッシュキーに含めるようにプロキシ設定を構成します。

一部のプロキシでは、CORS リクエスト用の事前定義済みの機能が提供されています。例えば、CloudFront では、ヘッダーを含むポリシーを設定できます。

このポリシーには、オリジンが Amazon S3 バケットである場合に、Cross-Origin Resource Sharing (CORS) リクエストを有効にするヘッダーが含まれます。

このポリシーの設定は以下のとおりです。

- オリジンリクエストに含まれるヘッダー:

  `Origin`

  `Access-Control-Request-Headers`

  `Access-Control-Request-Method`
- オリジンリクエストに含まれる Cookie: なし
- オリジンリクエストに含まれるクエリ文字列: なし

詳細については、「Amazon CloudFront デベロッパーガイド」の「ポリシーを使用してオリジンリクエストを制御する」または「マネージドオリジンリクエストポリシーを使用する」を参照してください。

静的ウェブサイトのチュートリアル

以下のチュートリアルまたはウォークスルーでは、静的ウェブサイトホスティングおよびオンデマンド動画ストリーミングのホスティング用に Amazon S3 汎用バケットを作成および設定する詳細な手順を示します。これらのチュートリアルの目的は、一般的なガイダンスを提供することです。これらのチュートリアルはラボ型環境向けであり、バケット名やユーザー名などの例を使用しています。お客様の組織環境に固有のニーズを満たすかどうかの十分な確認や調整をすることなく、本番環境で直接使用するためのものではありません。

- Amazon S3、Amazon CloudFront、Amazon Route 53 を使用したオンデマンドストリーミング動画のホスティング – Amazon S3 を Amazon CloudFront と共に使用すると、安全でスケーラブルな

方法でオンデマンド視聴用に動画をホストできます。ビデオを適切な形式に変換した後、サーバーまたは S3 汎用バケットに保存したら、ビューワーのリクエストに応じて CloudFront で配信できます。このチュートリアルでは、配信に CloudFront を使用し、ドメインネームシステム (DNS) およびカスタムドメイン管理に Amazon Route 53 を使用して、オンデマンド動画ストリーミングをホストするように汎用バケットを設定する方法について説明します。CloudFront はキャッシュから動画を提供し、まだキャッシュされていない場合にのみ、汎用バケットから動画を取得します。管理機能のキャッシュにより、低レイテンシー、高スループット、高速転送速度で、世界中のビューワーに動画を配信できます。CloudFront キャッシュ管理の詳細については、Amazon CloudFront デベロッパーガイドのキャッシュの最適化と可用性を参照してください。

- 静的ウェブサイトの設定 – ウェブサイトのように機能するように汎用バケットを設定できます。このチュートリアルでは、バケットの作成、S3 コンソールでの静的ウェブサイトホスティングの有効化、インデックスドキュメントの作成、エラードキュメントの作成など、Amazon S3 でウェブサイトをホストする手順について説明します。詳細については、「Amazon S3 を使用して静的ウェブサイトをホスティングする」を参照してください。
- Route 53 に登録されたカスタムドメインを使用した静的ウェブサイトの設定 – 静的ウェブサイトをホストする汎用バケットを作成および設定し、Amazon Route 53 に登録されたカスタムドメイン名を持つウェブサイトの S3 へのリダイレクトを作成できます。Route 53 を使用してドメインを登録し、ドメインのインターネットトラフィックをルーティングする先を定義します。このチュートリアルでは、ドメインおよびサブドメインのトラフィックを、HTML ファイルが含まれている汎用バケットにルーティングする Route 53 のエイリアスレコードを作成する方法を説明します。詳細については、「Amazon Route 53 デベロッパーガイド」の「Use your domain for a static website in an Amazon S3 bucket」を参照してください。このチュートリアルが完了したら、CloudFront を使ってウェブサイトのパフォーマンスを向上させることも可能です。詳細については、「Amazon CloudFront によるウェブサイトの高速化」を参照してください。
- S3 汎用バケットから AWS Amplify ホスティングへの静的ウェブサイトのデプロイ – S3 に保存されている静的ウェブサイトのコンテンツをホストするには、AWS Amplify ホスティングを使用することをお勧めします。Amplify ホスティングは、Amazon CloudFront を利用したグローバルに利用可能なコンテンツ配信ネットワーク (CDN) にウェブサイトを簡単にデプロイできるフルマネージドサービスです。これにより、大規模なセットアップなしで安全な静的ウェブサイトホスティングが可能になります。AWS Amplify ホスティングを使用すると、汎用バケット内のオブジェクトの場所を選択して、コンテンツをマネージド CDN にデプロイし、ウェブサイトのパブリック HTTPS URL を生成してどこからでもアクセス可能にすることができます。詳細については、「AWS Amplify ホスティングユーザーガイド」の「Amplify コンソールを使用して S3 から静的ウェブサイトをデプロイする」を参照してください。

チュートリアル: Amazon S3、Amazon CloudFront、Amazon Route 53 を使用したオンデマンドストリーミング動画のホスティング。

Amazon S3 を Amazon CloudFront とともに使用すると、セキュリティとスケーラビリティを備えたオンデマンド視聴用に動画をホストできます。オンデマンド動画 (VOD) ストリーミングの場合、動画コンテンツはサーバーに保存され、ビューワーはいつでも視聴できます。

CloudFront は、高速で安全性が高く、プログラム可能なコンテンツ配信ネットワーク (CDN) サービスです。CloudFront は、CloudFront のすべてのエッジロケーションから HTTPS 経由でコンテンツを安全に配信できます。CloudFront の詳細については、「Amazon CloudFront デベロッパーガイド」の「Amazon CloudFront とは」を参照してください。

CloudFront のキャッシングは、オリジンサーバーが直接応答するリクエストの数を減らします。ビューワー (エンドユーザー) が CloudFront で配信する動画をリクエストすると、リクエストはビューワーの場所により近いエッジロケーションにルーティングされます。CloudFront はキャッシュから動画を提供し、まだキャッシュされていない場合にのみ、S3 バケットから動画を取得します。管理機能のキャッシュにより、低レイテンシー、高スループット、高速転送速度で、世界中のビューワーに動画を配信できます。CloudFront キャッシュ管理の詳細については、Amazon CloudFront デベロッパーガイドのキャッシュの最適化と可用性を参照してください。

目的

このチュートリアルでは、配信に CloudFront を使用し、ドメインネームシステム (DNS) およびカスタムドメイン管理に Amazon Route 53 を使用して、オンデマンド動画ストリーミングをホストするように S3 バケットを設定します。

トピック

- 前提条件: カスタムドメインを Route 53 に登録し、設定する。
- ステップ 1: S3 バケットを作成する。
- ステップ 2: S3 バケットに動画をアップロードする。
- ステップ 3: CloudFront オリジンアクセスアイデンティティを作成する。
- ステップ 4: CloudFront ディストリビューションを作成する。
- ステップ 5: CloudFront ディストリビューション経由で動画にアクセスする。
- ステップ 6: カスタムドメイン名を使用するように CloudFront ディストリビューションを設定する。
- ステップ 7: カスタムドメイン名を使用して CloudFront ディストリビューションを介して S3 動画にアクセスする。
- (オプション)ステップ 8: CloudFront ディストリビューションが受信したリクエストに関するデータを表示する
- ステップ 9: クリーンアップする。
- 次のステップ

前提条件: カスタムドメインを Route 53 に登録し、設定する。

このチュートリアルを開始する前に、Route 53 により、後でカスタムドメイン名を使用するように CloudFront ディストリビューションを設定するために、カスタムドメイン (例、**example.com**) を登録し、設定する必要があります 。

カスタムドメイン名がなければ、S3 動画はパブリックにアクセスでき、CloudFront 経由でホストされる URL は、次のようになります。

```
https://CloudFront distribution domain name/Path to an S3 video
```

例えば、**https://d111111abcdef8.cloudfront.net/sample.mp4** と指定します。

Route 53 で設定されたカスタムドメイン名を使用するように CloudFront ディストリビューションを設定すると、S3 ビデオはパブリックにアクセス可能になり、CloudFront を介して次のような URL でホストされます。

```
https://CloudFront distribution alternate domain name/Path to an S3 video
```

例えば、**https://www.example.com/sample.mp4** と指定します。カスタムドメイン名は、ビューワーが使用するのに簡単で直感的です。

カスタムドメインの登録については、Amazon Route 53 デベロッパーガイド の「Route 53 を使用して新しいドメインを登録する」を参照してください。

Route 53 にドメイン名を登録すると、Route 53 によってホストゾーンが作成されます。このホストゾーンは、このチュートリアルの後半で使用します。このホストゾーンは、ドメインのトラフィックを、例えば Amazon EC2 インスタンスや CloudFront ディストリビューションにルーティングする方法についての情報を保存する場所です。

ドメイン登録、ホストゾーン、ドメインが受信した DNS クエリに関連する料金が発生します。詳細については、「Amazon Route 53 料金表」を参照してください。

> **Note**
>
> ドメインを登録すると、すぐに費用がかかり、元に戻せません。ドメインを自動更新しないことは選択できますが、前払いしてその年の所有権を取得することになります。詳細については、「Amazon Route 53 デベロッパーガイド」の「新しいドメインの登録」を参照してください。

ステップ 1: S3 バケットを作成する。

ストリーミングする元の動画を保存するには、バケットを作成します。

バケットを作成するには

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. ページ上部にあるナビゲーションバーで、現在表示されている AWS リージョン の名前をクリックします。次に、バケットを作成するリージョンを選択します。

> **Note**
>
> レイテンシーとコストを最小化するため、さらに規制条件に対応するために、最寄りのリージョンを選択します。明示的に別のリージョンに移動する場合を除き、特定のリージョンに保管されたオブジェクトは、そのリージョンから移動されることはありません。Amazon S3 AWS リージョン のリストについては、「Amazon Web Services 全般のリファレンス」の「AWS のサービス エンドポイント」を参照してください。

3. 左のナビゲーションペインで、[汎用バケット] を選択します。
4. [Create bucket (バケットの作成)] を選択します。[バケットの作成] ページが開きます。
5. [バケット名] に、バケットの名前 (例: **`tutorial-bucket`**) を入力します。

   Amazon S3 のバケット命名規則の詳細については、「汎用バケットの命名規則」を参照してください。
6. [リージョン] で、バケットを保存する AWS リージョンを選択します。

   可能であれば、ほとんどのビューワーに最も近いリージョンを選択します。バケットのリージョンの詳細については、「汎用バケットの概要」を参照してください。
7. [このバケットのブロックパブリックアクセス設定] が、デフォルト設定 (すべてのパブリックアクセスをブロックが有効) のままであることを確認します。

   すべてのパブリックアクセスをブロック を有効にしても、ビューワーは CloudFront 経由でアップロードされた動画にアクセスできます。この機能は、CloudFront を使用して S3 に保存された動画をホストすることの大きな利点です。

   ユースケースでオフにする必要のある設定が 1 つ以上あることがわかっている場合を除き、すべての設定を有効にしておくことをお勧めします。パブリックアクセスのブロックの詳細については、Amazon S3 ストレージへのパブリックアクセスのブロック を参照してください。
8. 残りの設定はデフォルトのままにしておきます。

   (オプション) 特定のユースケースに追加のバケット設定を設定する場合は、「汎用バケットの作成」を参照してください。
9. [バケットの作成] を選択します。

ステップ 2: S3 バケットに動画をアップロードする。

次の手順では、コンソールを使用して S3 バケットに動画ファイルをアップロードする方法を示します。S3 に動画ファイルをアップロードするときは、Amazon S3 Transfer Acceleration を使用して、高速かつ安全なファイル転送を設定します。転送アクセラレーションを使用すると、S3 バケットへの動画のアップロードを高速化して、大きな動画の長距離転送を行うことができます。詳細については、「Amazon S3 Transfer Acceleration を使用した高速かつ安全なファイル転送の設定」を参照してください。

バケットにファイルをアップロードするには

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 左のナビゲーションペインで、[汎用バケット] を選択します。
3. [汎用バケット] リストで、ステップ 1 で作成したバケットの名前を選択し (**`tutorial-bucket`** など)、ファイルをアップロードします。
4. バケットの [オブジェクト] タブで、[アップロード] を選択します。
5. [アップロード] ページの [ファイルとフォルダ] の下で、[ファイルを追加] を選択します。
6. アップロードするファイルを選択し、続いて [オープン] を選択します。

   例えば、`sample.mp4` という名前の動画ファイルをアップロードできます。
7. [アップロード] を選択します。

ステップ 3: CloudFront オリジンアクセスアイデンティティを作成する。

S3 バケットからの動画への直接アクセスを制限するには、オリジンアクセスアイデンティティ (OAI) という特別な CloudFront ユーザーを作成します。このチュートリアルの後半で OAI をディストリビューションに関連付けます。OAI を使用すると、ビューワーは CloudFront をバイパスして、S3 バケットから直接ビデオを取得できません。CloudFront OAI だけが S3 バケット内のファイルにアクセスできます。詳細については、Amazon CloudFront デベロッパーガイド の「オリジンアクセスアイデンティティを使用して Amazon S3 コンテンツへのアクセスを制限する 」を参照してください。

CloudFront OAI を作成するには

1. AWS Management Consoleにサインインし、https://console.aws.amazon.com/cloudfront/v4/home で CloudFront コンソールを開きます。

2. 左のナビゲーションペインで、[セキュリティ] セクションの [オリジンアクセス] を選択します。
3. [アイデンティティ] タブで、[オリジンアクセスアイデンティティを作成] を選択します。
4. 新しいオリジンアクセスアイデンティティとして、名前 (例えば、**S3-OAI**) を入力します。
5. [作成] を選択します。

ステップ 4: CloudFront ディストリビューションを作成する。

CloudFront を使用して S3 バケットで動画を提供および配信するには、CloudFront ディストリビューションを作成する必要があります。

サブステップ

- CloudFront ディストリビューションを作成する
- バケットポリシーの確認

CloudFront ディストリビューションを作成する

1. AWS Management Consoleにサインインし、https://console.aws.amazon.com/cloudfront/v4/home で CloudFront コンソールを開きます。
2. 左のナビゲーションペインで、ディストリビューション を選択します。
3. [ディストリビューションの作成] を選択します。
4. [オリジン] の [オリジンドメイン] で、ステップ 1 で作成した S3 バケットの名前から始まる、S3 オリジンのドメイン名 (例えば、**tutorial-bucket**) を選択します。
5. [オリジンアクセス]では、[レガシーアクセスアイデンティティ] を選択します。
6. [オリジンアクセスアイデンティティ] で、ステップ 3 で作成したオリジンアクセスアイデンティティを選択します (例えば、**S3-OAI**)。
7. [バケットポリシー] で、[はい、バケットポリシーを更新します] を選択します。
8. [ビューワープロトコルポリシー] の [デフォルトのキャッシュ動作] セクションで、[HTTP から HTTPS へリダイレクト] を選択します。

   この機能を選択する際は、HTTP リクエストは HTTPS に自動的にリダイレクトされ、ウェブサイトを保護し、ビューワーのデータを保護します。
9. [Default Cache Behavior(キャッシュ動作のデフォルト)] セクションの他の設定については、デフォルト値を使用します。

(オプション) CloudFront が別のリクエストをオリジンに転送するまでにファイルを CloudFront キャッシュに保持する期間をコントロールできます。この期間を短くすると、動的なコンテンツを供給できます。この期間を長くすると、ユーザー側のパフォーマンスは向上します。ファイルがエッジキャッシュから直接返される可能性が高くなるためです。期間を長くすると、オリジンの負荷も軽減されます。詳細については、Amazon CloudFront デベロッパーガイドの「コンテンツがエッジキャッシュに保持される期間の管理 (有効期限)」を参照してください。

10. その他のセクションでは、残りの設定はデフォルトのままにしておきます。

    異なる設定オプションの詳細については、Amazon CloudFront デベロッパーガイドの「ディストリビューションを作成または更新する場合に指定する値」を参照してください。

11. ページの最下部で、[ディストリビューションの作成] を選択します。

12. CloudFront ディストリビューションの [全般] タブの [詳細] で、ディストリビューションの [最終変更] 列の値が、[デプロイ] からディストリビューションが最後に変更されたタイムスタンプに変更されます。これには通常数分かかります。

バケットポリシーの確認

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。
3. [バケット] リストで、CloudFront ディストリビューションのオリジンとして上記で使用したバケットの名前を選択します (例えば、**tutorial-bucket**)。
4. [アクセス許可] タブを選択します。
5. [バケットポリシー] セクションのバケットポリシーテキストで、次のようなステートメントが表示されることを確認します。

```
{
    "Version": "2008-10-17",
    "Id": "PolicyForCloudFrontPrivateContent",
    "Statement": [
        {
            "Sid": "1",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access
 Identity EH1HDMB1FH2TC"
```

```
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::tutorial-bucket/*"
        }
    ]
}
```

これは、上記の [はい、バケットポリシーを更新します] を選択した際に、CloudFront ディストリビューションがバケットポリシーに追加したステートメントです。

このバケットポリシーの更新は、S3 バケットへのアクセスを制限するように CloudFront ディストリビューションを正常に構成したことを示します。この制限のため、バケット内のオブジェクトには CloudFront ディストリビューションからのみアクセスできます。

ステップ 5: CloudFront ディストリビューション経由で動画にアクセスする。

これで、CloudFront は S3 バケットに保存された動画を提供できます。CloudFront 経由で動画にアクセスするには、CloudFront ディストリビューションのドメイン名を S3 バケット内の動画へのパスの中に含めます。

CloudFront ディストリビューションドメイン名を使用して S3 動画の URL を作成するには

1. AWS Management Consoleにサインインし、https://console.aws.amazon.com/cloudfront/v4/home で CloudFront コンソールを開きます。
2. 左のナビゲーションペインで、[ディストリビューション] を選択します。
3. ディストリビューションのドメイン名を取得するには、次の手順を実行します。
   a. [オリジン] 列で、ステップ 1 で作成した S3 バケットで始まるオリジン名を見つけて、CloudFront ディストリビューションを識別します (例えば、**tutorial-bucket**)。
   b. リストからディストリビューションを見つけたら、[ドメイン名] 列を広げて、CloudFront ディストリビューションのドメイン名の値をコピーします。
4. 新しいブラウザタブで、上記でコピーしたディストリビューションドメイン名を貼り付けます。
5. 前のブラウザタブに戻り、https://console.aws.amazon.com/s3/ にある S3 コンソールを開きます。
6. 左側のナビゲーションペインで、[バケット] を選択します。
7. [バケット] リストで、ステップ 1 で作成したバケットの名前を選択します (例えば、**tutorial-bucket**)。

8. [オブジェクト] リストで、ステップ 2 でアップロードした動画の名前を選択します (例えば、`sample.mp4`)。
9. オブジェクト詳細ページで、オブジェクトの概要 セクションで、[キー] の値をコピーします。この値は、S3 バケット内でアップロードされたビデオオブジェクトへのパスです。
10. 以前にディストリビューションのドメイン名を貼り付けたブラウザタブに戻り、スラッシュ (**/**) を配信ドメイン名の後に入力し、前にコピーした動画へのパスを貼り付けます (例: `sample.mp4`)。

    これで、S3 動画はパブリックにアクセスでき、CloudFront 経由でホストされた URL は、次のようになります。

    ```
    https://CloudFront distribution domain name/Path to the S3 video
    ```

    `CloudFront ################` および *`S3 ######`* を適切な値で置き換えます。URL の例は **`https://d111111abcdef8.cloudfront.net/sample.mp4`** です。

ステップ 6: カスタムドメイン名を使用するように CloudFront ディストリビューションを設定する。

URL で CloudFront ドメイン名の代わりに独自のドメイン名を使用して S3 動画にアクセスするには、代替ドメイン名を CloudFront ディストリビューションに追加する必要があります。

サブステップ

- SSL 証明書をリクエストする。
- CloudFront ディストリビューションに代替ドメイン名を追加します。
- 代替ドメイン名のトラフィックを CloudFront ディストリビューションのドメイン名にルーティングする DNS レコードを作成する。
- ディストリビューションに対して IPv6 が有効になっているかどうかを確認し、必要に応じて別の DNS レコードを作成します。

SSL 証明書をリクエストする。

ビューワーが動画ストリーミングの URL で HTTPS とカスタムドメイン名を使用できるようにするには、AWS Certificate Manager (ACM) を使用して、Secure Sockets Layer (SSL) 証明書を要求します。SSL 証明書は、ウェブサイトへの暗号化されたネットワーク接続を確立します。

1. AWS Management Console にサインインして、ACM コンソール (https://console.aws.amazon.com/acm/home) を開きます。
2. 入門者向けページが表示されたら、[証明書のプロビジョニング] で [開始] を選択します。
3. [証明書のリクエスト] ページで、[パブリック証明書のリクエスト] を選択し、[証明書のリクエスト] を選択して続行します。
4. [ドメイン名の追加] ページで、SSL/TLS 証明書を使用して保護するサイトの完全修飾ドメイン名を入力します。アスタリスク (*) を使用して、同じドメイン内の複数のサイトを保護するワイルドカード証明書をリクエストします。このチュートリアルでは、[前提条件] で設定したカスタムドメイン名を入力します。例えば、**`*.example.com`** を使用し、[Next (次へ)] を選択します。

   詳細については、AWS Certificate Managerユーザーガイドの「ACM パブリック証明書をリクエストする (コンソール)」を参照してください。
5. [検証方法の選択] ページで、[DNS での検証] を選択します。[次へ] を選択します。

   DNS 設定を編集できる場合は、E メール検証ではなく DNS ドメイン検証を使用することをお勧めします。DNS 検証には E メール検証と比べていくつかの利点があります。詳細については、AWS Certificate Managerユーザーガイドのオプション 1: DNS 検証を参照してください。
6. (オプション) [タグの追加] ページで、メタデータを用いて証明書にタグを付けることができます。
7. [Review] (レビュー) を選択します。
8. [確認] ページで、ドメイン名および検証方法にある情報が正しいことを確認します。次に、[確認してリクエストする] を選択します。

   [検証] ページには、リクエストが処理中で、証明書ドメインが検証中であることが示されます。検証を待機している証明書は、検証保留中状態にあります。
9. [検証] ページで、カスタムドメイン名の左側にある下向き矢印を選択し、[Route 53 でレコードを作成する] を選択して、DNS によるドメインの所有権を検証します。

   これは、AWS Certificate Manager によって DNS 設定に提供される CNAME レコードを追加します。
10. [Route 53 でレコードを作成する] ダイアログボックスで、[作成] を選択します。

    これで、[検証] ページの一番下に、[成功] のステータス通知が表示されるようになりました。
11. [続行] を選択して、[証明書] リストページを表示します。

    新しい証明書のステータスは、30 分以内に [検証保留中] から [発行済み] に変わります。

CloudFront ディストリビューションに代替ドメイン名を追加します。

1. AWS Management Consoleにサインインし、https://console.aws.amazon.com/cloudfront/v4/home で CloudFront コンソールを開きます。
2. 左のナビゲーションペインで、[ディストリビューション] を選択します。
3. ステップ 4 で作成したディストリビューションの ID を選択します。
4. [全般] タブで、設定セクションに移動し、編集を選択します。
5. 編集設定ページの [代替ドメイン名 (CNAME) - オプション] で、[項目を追加] を選択して、この CloudFront ディストリビューションによって提供される S3 動画の URL で使用するカスタムドメイン名を追加します。

   このチュートリアルでは、例えば、`www.example.com` などのサブドメインのトラフィックをルーティングする場合、サブドメイン名 (`www`) とドメイン名 (`example.com`) を入力します。具体的には、**`www.example.com`** を入力します。

   > **Note**
   >
   > 追加する代替ドメイン名 (CNAME) は、CloudFront ディストリビューションに以前アタッチした SSL 証明書の対象である必要があります。

6. カスタム SSL 証明書 - オプション で、上記でリクエストした SSL 証明書を選択します (例えば、**`*.example.com`**)。

   > **Note**
   >
   > SSL 証明書をリクエストした直後に SSL 証明書が表示されない場合は、SSL 証明書を選択できるようになるまで 30 分間待機してから一覧を更新できます。

7. 残りの設定はデフォルト値のままにしておきます。[Save changes (変更を保存)] を選択します。
8. ディストリビューションの [全般] タブで、ディストリビューションの [最終変更] の値が [デプロイ] からディストリビューションが最後に変更されたタイムスタンプに変更されるまで待機します。

代替ドメイン名のトラフィックを CloudFront ディストリビューションのドメイン名にルーティングする DNS レコードを作成する。

1. AWS Management Console にサインインし、Route 53 コンソール (https://console.aws.amazon.com/route53/) を開きます。
2. 左のナビゲーションペインで [ホストゾーン] を選択します。
3. ホストゾーン ページの 前提条件 で Route 53 が作成したホストゾーンの名前を選択します (例えば、**example.com**)。
4. レコードを作成するを選択し、レコードのクイック作成方法を使用します。
5. [レコード名] で、レコード名の値を、上記で追加した CloudFront ディストリビューションの代替ドメイン名と同じにします。

   このチュートリアルでは、www.example.com などのサブドメインにトラフィックをルーティングするには、ドメイン名なしでサブドメイン名を入力します。例えば、カスタムドメイン名の前にあるテキストフィールドに「**www**」を入力します。
6. [レコードタイプ] で、[A - IPv4 アドレスと一部の AWS リソースにトラフィックをルーティング] を選択します。
7. [値] で、エイリアスリソースを有効にするには、エイリアス切り替えを選択します。
8. [トラフィックのルーティング先] で、[CloudFront ディストリビューションへのエイリアス] を選択します。
9. [ディストリビューションの選択] という検索ボックスで、ステップ 4 で作成した CloudFront ディストリビューションのドメイン名を選択します。

   CloudFront ディストリビューションのドメイン名を検索するには、以下の手順を実行します。

   a. 新しいブラウザタブで、AWS Management Console にサインインし、https://console.aws.amazon.com/cloudfront/v3/home で CloudFront コンソールを開きます。
   b. 左のナビゲーションペインで、[ディストリビューション] を選択します。
   c. [オリジン] 列で、ステップ 1 で作成した S3 バケットで始まるオリジン名を見つけて、CloudFront ディストリビューションを識別します (例えば、**tutorial-bucket**)。
   d. リストからディストリビューションを見つけたら、ドメイン名 列を広げて、CloudFront ディストリビューションのドメイン名の値を確認します。
10. Route 53 コンソールの [レコードを作成する] ページで、残りの設定はデフォルトのままにしておきます。
11. [レコードを作成] を選択します。

ディストリビューションに対して IPv6 が有効になっているかどうかを確認し、必要に応じて別の DNS レコードを作成します。

ディストリビューションに対して IPv6 が有効になっている場合は、別の DNS レコードを作成する必要があります。

1. ディストリビューションに対して IPv6 が有効になっているかどうかを確認するには、次の手順を実行します。

   a. AWS Management Consoleにサインインし、https://console.aws.amazon.com/cloudfront/v4/home で CloudFront コンソールを開きます。

   b. 左のナビゲーションペインで、[ディストリビューション] を選択します。

   c. ステップ 4 で作成した CloudFront ディストリビューションの ID を選択します。

   d. [全般] タブの [設定] で、IPv6 が有効になっているか確認します。

      ディストリビューションに対して IPv6 が有効になっている場合は、別の DNS レコードを作成する必要があります。

2. ディストリビューションに対して IPv6 が有効になっている場合は、以下を実行して DNS レコードを作成する必要があります。

   a. AWS Management Console にサインインし、Route 53 コンソール (https://console.aws.amazon.com/route53/) を開きます。

   b. 左のナビゲーションペインで [ホストゾーン] を選択します。

   c. ホストゾーン ページの 前提条件 で Route 53 が作成したホストゾーンの名前を選択します (例えば、**example.com**)。

   d. レコードを作成するを選択し、レコードのクイック作成方法を使用します。

   e. [レコード名] で、カスタムドメイン名の前のテキストフィールドに、上記の IPv4 DNS レコードを作成したときに入力したのと同じ値を入力します。例えば、このチュートリアルでは、サブドメイン `www.example.com` のトラフィックをルーティングするには、**www** のみを入力します。

   f. [レコードタイプ] で、[AAAA - IPv6 アドレスと一部の AWS リソースにトラフィックをルーティング] を選択します。

   g. [値] で、エイリアスリソースを有効にするには、エイリアス切り替えを選択します。

   h. [トラフィックのルーティング先] で、[CloudFront ディストリビューションへのエイリアス] を選択します。

i. [ディストリビューションの選択] という検索ボックスで、ステップ 4 で作成した CloudFront ディストリビューションのドメイン名を選択します。

j. 残りの設定はデフォルトのままにしておきます。

k. [レコードを作成] を選択します。

ステップ 7: カスタムドメイン名を使用して CloudFront ディストリビューションを介して S3 動画にアクセスする。

カスタム URL を使用して S3 動画にアクセスするには、代替ドメイン名と S3 バケット内の動画へのパスを組み合わせる必要があります。

CloudFront ディストリビューションを介して S3 動画にアクセスするためのカスタム URL を作成するには

1. AWS Management Consoleにサインインし、https://console.aws.amazon.com/cloudfront/v4/home で CloudFront コンソールを開きます。
2. 左のナビゲーションペインで、[ディストリビューション] を選択します。
3. CloudFront ディストリビューションの代替ドメイン名を取得するには、以下を実行します。

   a. [オリジン] 列で、ステップ 1 で作成した S3 バケットのバケット名で始まるオリジン名を見つけて、CloudFront ディストリビューションを識別します (例えば、**`tutorial-bucket`**)。

   b. リストからディストリビューションを見つけたら、代替ドメイン名 列を広げて、CloudFront ディストリビューションの代替ドメイン名の値をコピーします。
4. 新しいブラウザタブに、CloudFront ディストリビューションの代替ドメイン名を貼り付けます。
5. 前のブラウザタブに戻り、https://console.aws.amazon.com/s3/ にある Amazon S3 コンソールを開きます。
6. ステップ 5 で説明した S3 動画へのパスを見つけます。
7. 以前に代替ドメイン名を貼り付けたブラウザタブに戻り、スラッシュ (**/**) を入力し、S3 動画へのパスを貼り付けます (例えば、`sample.mp4`)。

   これで、S3 動画はパブリックにアクセス可能になり、CloudFront を介して次のようなカスタム URL でホストされます。

```
https://CloudFront distribution alternate domain name/Path to the S3 video
```

*CloudFront ##################*および *S3 #######*適切な値で置き換えます。URL の例は **https://www.example.com/sample.mp4** です。

(オプション)ステップ 8: CloudFront ディストリビューションが受信したリクエストに関するデータを表示する

CloudFront ディストリビューションが受信したリクエストに関するデータを表示するには

1. AWS Management Consoleにサインインし、https://console.aws.amazon.com/cloudfront/v4/home で CloudFront コンソールを開きます。
2. CloudFront コンソールの左側のナビゲーションペインで、[レポートと分析] で、コンソールから、キャッシュ統計、人気のあるオブジェクト、上位リファラー、使用状況、ビューワーなどのレポートを選択します。

   各レポートダッシュボードをフィルタリングできます。詳細については、Amazon CloudFront デベロッパーガイドの「コンソール内の CloudFront レポート」セクションを参照してください。
3. データをフィルタリングするには、ステップ 4 で作成した CloudFront ディストリビューションの ID を選択します。

ステップ 9: クリーンアップする。

学習演習としてのみ、CloudFront と Route 53 を使用して S3 ストリーミング動画をホストした場合は、割り当てた AWS リソースを削除して、料金が発生しないようにします。

> **Note**
>
> ドメインを登録すると、すぐに費用がかかり、元に戻せません。ドメインを自動更新しないことは選択できますが、前払いしてその年の所有権を取得することになります。詳細については、「Amazon Route 53 デベロッパーガイド」の「新しいドメインの登録」を参照してください。

サブステップ

- CloudFront ディストリビューションの削除
- DNS レコードの削除
- カスタムドメインのパブリックホストゾーンの削除
- Route 53 からカスタムドメイン名を削除します。
- S3 ソースバケットの元の動画を削除する。
- S3 ソースバケットを削除する

CloudFront ディストリビューションの削除

1. AWS Management Consoleにサインインし、https://console.aws.amazon.com/cloudfront/v4/home で CloudFront コンソールを開きます。
2. 左のナビゲーションペインで、[ディストリビューション] を選択します。
3. [オリジン] 列で、ステップ 1 で作成した S3 バケットのバケット名で始まるオリジン名を見つけて、CloudFront ディストリビューションを識別します (例えば、**`tutorial-bucket`**)。
4. CloudFront ディストリビューションを削除するには、まずディストリビューションを無効にする必要があります。

   - [ステータス] 列の値が [有効] で、[最終変更] の値がディストリビューションが最後に変更されたときのタイムスタンプである場合は、ディストリビューションを無効にしてから削除してください。
   - [ステータス] の値が [有効] で、[最終変更] の値がデプロイの場合、[ステータス] がディストリビューションが最後に変更されたタイムスタンプに変わるまで待ちます。次に、ディストリビューションを無効にしてから、ディストリビューションを削除します。
5. CloudFront ディストリビューションを無効にするには、次の手順を実行します。

   a. ディストリビューションリストで、削除するディストリビューションの ID の横にあるチェックボックスをオンにします。

   b. ディストリビューションを無効にするには、[無効] を選択し、[無効] を選択して確定します。

      代替ドメイン名が関連付けられているディストリビューションを無効にすると、CloudFront は、別のディストリビューションに同じドメイン (`*.example.com` など) と一致するワイルドカード(*) 付きの代替ドメイン名がある場合でも、このドメイン名 (`www.example.com` など) へのトラフィックの受信を停止します。

c. [状態] 列の値が直ちに [無効] に変わります。[最終変更] の値が [デプロイ] からディストリビューションが最後に変更されたタイムスタンプに変更されるまで待機します。

   CloudFront はこの変更をすべてのエッジロケーションに伝達する必要があるため、この更新が完了してディストリビューションを削除できるようになるまでに数分かかることがあります。

6. 無効になっているディストリビューションを削除するには、次の手順を実行します。

   a. 削除するディストリビューションの ID の横にあるチェックボックスをオンにします。

   b. 削除 を選択し、削除 を選択して確認します。

DNS レコードの削除

ドメインのパブリックホストゾーン (DNS レコードを含む) を削除する場合は、Amazon Route 53 デベロッパーガイドの カスタムドメインのパブリックホストゾーンの削除 を参照してください。 ステップ 6 で作成された DNS レコードを削除するだけの場合は、次の操作を行います。

1. AWS Management Console にサインインし、Route 53 コンソール (https://console.aws.amazon.com/route53/) を開きます。
2. 左のナビゲーションペインで [ホストゾーン] を選択します。
3. ホストゾーン ページの 前提条件 で Route 53 が作成したホストゾーンの名前を 選択します (例えば、**example.com**)。
4. レコードのリストで、削除するレコード (ステップ 6 で作成したレコード) の横にあるチェックボックスをオンにします。

   > **Note**
   >
   > [タイプ] の値が [NS] または [SOA] のレコードを削除することはできません。

5. [レコードセットの削除] を選択します。
6. 削除を確認するには、[削除] を選択します。

   レコードの変更が Route 53 DNS サーバーに伝達されるまでにしばらく時間がかかります。現在、変更が反映されたことを確認するには、GetChange API アクションを使用する方法しかありません。通常、変更は 60 秒以内にすべての Route 53 ネームサーバーに伝播されます。

カスタムドメインのパブリックホストゾーンの削除

Warning

ドメイン登録は維持するものの、ウェブサイトやウェブアプリケーションへのインターネットトラフィックのルーティングを停止する場合、ホストゾーンを削除する代わりに、ホストゾーン (上記) 内のレコードを削除することをお勧めします。
さらに、ホストゾーンを削除すると、他のユーザーがお客様のドメイン名を使用してドメインを使って自分のリソースにトラフィックをルーティングする可能性があります。
さらに、ホストゾーンを削除した場合、復元することはできません。新しいホストゾーンを作成して、ドメイン登録のネームサーバーを更新する必要があります。更新が有効になるには、最大 48 時間かかることがあります。
ドメインをインターネット上で利用できなくするには、DNS サービスを無料の DNS サービスに移行し、Route 53 のホストゾーンを削除することをお勧めします。これにより、今後 DNS クエリが誤ってルーティングされることを防ぐことができます。

1. ドメインが Route 53 に登録されている場合に、Route 53 ネームサーバーを新しい DNS サービスのネームサーバーで置き換える情報については、Amazon Route 53 デベロッパーガイドで、ドメインのネームサーバーとグルーレコードの追加または変更を参照してください。
2. ドメインが他のレジストラに登録されている場合、レジストラが提供する方法を使用してドメインのネームサーバーを変更します。

Note

サブドメイン (`www.example.com`) のホストゾーンを削除する場合は、ドメイン (`example.com`) のネームサーバーを変更する必要はありません。

1. AWS Management Console にサインインし、Route 53 コンソール (https://console.aws.amazon.com/route53/) を開きます。
2. 左のナビゲーションペインで [ホストゾーン] を選択します。
3. [ホストゾーン] ページで、削除するホストゾーンの名前を選択します。
4. ホストゾーンの [レコード] タブで、削除するホストゾーンに NS レコードと SOA レコードのみが含まれていることを確認します。

他のレコードが含まれている場合は、それらを削除します。

ホストゾーンでサブドメインの NS レコードを作成した場合は、それらのレコードも削除します。

5. ホストゾーンの DNSSEC 署名 タブで、DNSSEC 署名が有効になっている場合は無効にします。詳細については、「 Amazon Route 53 デベロッパーガイド」の「DNSSEC 署名の無効」を参照してください。
6. ホストゾーンの詳細ページの上部で、[ゾーンを削除] を選択します。
7. **delete** と入力して削除を確認し、[Delete (削除)] を選択します。

Route 53 からカスタムドメイン名を削除します。

最上位ドメイン (TLD) では、必要がなくなった登録を削除できます。登録が期限切れになる前に Route 53 からドメイン名登録を削除した場合でも、登録料は AWS から払い戻しされません。詳細については、Amazon Route 53 デベロッパーガイドの「ドメイン名の登録を削除する」を参照してください。

> **Important**
>
> AWS アカウント 間でドメインを移管する場合や、他のレジストラにドメインを移管する場合は、ドメインを削除せずにすぐに登録が予測されます。代わりに、「Amazon Route 53 デベロッパーガイド」で該当するドキュメントを参照してください。
>
> - 異なる AWS アカウント へのドメインの移管
> - Amazon Route 53 から別のレジストラへのドメインの移行

S3 ソースバケットの元の動画を削除する。

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。
3. [バケット名] リストで、ステップ 2 で動画をアップロードしたバケットの名前を選択します (例えば、**tutorial-bucket**)。
4. オブジェクト タブで、削除するオブジェクトの名前の左にあるチェックボックスをオンにします (例えば、`sample.mp4`)。

5. [削除] を選択します。
6. [オブジェクトを完全に削除しますか?] で、**permanently delete** と入力し、このオブジェクトを削除することを確定します。
7. [オブジェクトの削除] を選択します。

S3 ソースバケットを削除する

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。
3. [バケット] リストで、ステップ 1 で作成したバケットの名前の横にあるオプションボタンを選択します (例えば、**tutorial-bucket**)。
4. [削除] を選択します。
5. [バケットの削除] ページで、テキストフィールドにバケット名を入力することでバケットを削除することを確認し、[バケットを削除] を選択します。

次のステップ

このチュートリアルを完了すると、次の関連するユースケースをさらに調べることができます。

- CloudFront ディストリビューションでこれらの動画をホストする前に、特定のテレビや接続されたデバイスで必要なストリーミング形式に S3 動画をトランスコードします。

  Amazon S3 バッチオペレーション、AWS Lambda、および AWS Elemental MediaConvert を使用して、動画のコレクションをさまざまな出力メディア形式にバッチトランスコードする方法の詳細については、「チュートリアル: S3 バッチオペレーションを使用した動画のバッチトランスコーディング」を参照してください。
- CloudFront と Route 53 を使用して、画像、オーディオ、モーショングラフィックス、スタイルシート、HTML、JavaScript、React アプリなど、S3 に保存されている他のオブジェクトをホストします。

  例については、「チュートリアル: Route 53 に登録されたカスタムドメインを使用した静的ウェブサイトの設定」および「Amazon CloudFront によるウェブサイトの高速化」を参照してください。
- Amazon S3 Transfer Acceleration を使用して、高速かつ安全なファイル転送を設定します。転送アクセラレーションを使用すると、S3 バケットへの動画のアップロードを高速化して、大きな動

画の長距離転送を行うことができます。Transfer Acceleration は、CloudFront のグローバルに分散したエッジロケーションや AWS バックボーンネットワークを経由してトラフィックをルーティングすることで、転送パフォーマンスを向上させます。また、ネットワークプロトコルの最適化も利用します。詳細については、「Amazon S3 Transfer Acceleration を使用した高速かつ安全なファイル転送の設定」を参照してください。

チュートリアル: Amazon S3 での静的ウェブサイトの設定

> **Important**
>
> Amazon S3 では、Amazon S3 内のすべてのバケットの基本レベルの暗号化として、Amazon S3 が管理するキー (SSE-S3) によるサーバー側の暗号化が適用されるようになりました。2023 年 1 月 5 日以降、Amazon S3 にアップロードされるすべての新しいオブジェクトは、追加費用なしで、パフォーマンスに影響を与えずに自動的に暗号化されます。S3 バケットのデフォルト暗号化設定と新しいオブジェクトのアップロードのための自動暗号化ステータスは、AWS CloudTrail ログ、S3 インベントリ、S3 ストレージレンズ、Amazon S3 コンソール、および AWS Command Line Interface と AWS SDK の追加の Amazon S3 API レスポンスヘッダーとして利用できるようになりました。詳細については、「デフォルト暗号化に関するよくある質問」を参照してください。

Amazon S3 バケットは、ウェブサイトと同じように機能するように設定できます。この例では、Amazon S3 上でウェブサイトをホスティングするステップを説明します。

> **Important**
>
> 次のチュートリアルでは、[パブリックアクセスをブロック] を無効にする必要があります。[パブリックアクセスをブロック] 設定は、有効にしておくことをお勧めします。4 つすべての [パブリックアクセスをブロック] 設定を有効にしたまま、静的ウェブサイトをホストする場合は、Amazon CloudFront のオリジンアクセスコントロール (OAC) を使用できます。Amazon CloudFront は、セキュアな静的ウェブサイトをセットアップするために必要な機能を提供します。Amazon S3 静的ウェブサイトは、HTTP エンドポイントのみをサポートしています。Amazon CloudFront は、耐久性に優れた Amazon S3 のあるストレージを使用し、HTTPS などの、追加のセキュリティヘッダーを提供します。HTTPS では、通常の HTTP リクエストを暗号化し、一般的なサイバー攻撃から保護することで、セキュリティが

強化されます。詳細については、「Amazon CloudFront デベロッパーガイド」の「安全な静的ウェブサイトの使用開始」を参照してください。

トピック

- ステップ 1: バケットを作成する
- ステップ 2: 静的ウェブサイトホスティングを有効にする
- ステップ 3: パブリックアクセスブロック設定を編集する
- ステップ 4: バケットの内容の公開を許可するバケットポリシーを追加する
- ステップ 5: インデックスドキュメントを設定する
- ステップ 6: エラードキュメントの設定
- ステップ 7: ウェブサイトエンドポイントをテストする
- ステップ 8: クリーンアップする

ステップ 1: バケットを作成する

以下の手順では、ウェブサイトホスティングにバケットを作成する方法の概要を説明します。バケットの作成に関するステップバイステップの方法は、「汎用バケットの作成」を参照してください。

バケットを作成するには

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. [Create bucket] (バケットの作成) をクリックします。
3. [バケット名] (**example.com** など) を入力します。
4. バケットを作成するリージョンを選択します。

   レイテンシーとコストを最小限に抑えるため、または規制要件に対処するために、最寄りのリージョンを選択します。選択したリージョンによって、Amazon S3 ウェブサイトエンドポイントが決まります。詳細については、「ウェブサイトエンドポイント」を参照してください。
5. デフォルト設定をそのまま使用してバケットを作成するには、[作成] を選択します。

ステップ 2: 静的ウェブサイトホスティングを有効にする

バケットを作成したら、バケットの静的ウェブサイトホスティングを有効にできます。新しいバケットを作成することも、既存のバケットを使用することもできます。

静的ウェブサイトホスティングを有効にするには

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 左のナビゲーションペインで、[汎用バケット] を選択します。
3. バケットリストで、静的ウェブサイトホスティングを有効にするバケットの名前を選択します。
4. [プロパティ] を選択します。
5. [静的ウェブサイトホスティング] で [編集] を選択します。
6. [このバケットを使用してウェブサイトをホストする] を選択します。
7. [静的ウェブサイトホスティング] で [有効化] を選択します。
8. [インデックスドキュメント] に、インデックスドキュメントのファイル名 (通常は `index.html`) を入力します。

   インデックスドキュメント名の大文字と小文字は区別されます。この名前は、S3 バケットにアップロードする HTML インデックスドキュメントのファイル名と正確に一致する必要があります。バケットをウェブサイトホスティング用に設定するときは、インデックスドキュメントを指定する必要があります。Amazon S3 からこのインデックスドキュメントが返されるのは、ルートドメインまたはサブフォルダに対するリクエストが行われたときです。詳細については、「インデックスドキュメントの設定」を参照してください。
9. 4XX クラスエラーに関する独自のカスタムエラードキュメントを指定する場合は、[エラードキュメント] にカスタムエラードキュメントのファイル名を入力します。

   エラードキュメント名の大文字と小文字は区別されます。この名前は、S3 バケットにアップロードする HTML エラードキュメントのファイル名と正確に一致する必要があります。カスタムエラードキュメントを指定しない場合、エラーが発生すると、Amazon S3 からデフォルトの HTML エラードキュメントが返されます。詳細については、「カスタムエラードキュメントの設定」を参照してください。
10. (オプション) 高度なリダイレクトツールを指定する場合は、[Rredirection rules] (リダイレクトルール) に、JSON を入力してルールを記述します。

    例えば、条件に応じてリクエストのルーティング先を変えることができます。この条件として使用できるのは、リクエストの中の特定のオブジェクトキー名またはプレフィックスです。詳細に

ついては、「高度な条件付きリダイレクトを使用するようにリダイレクトルールを設定する」を参照してください。

11. [Save changes] (変更の保存) をクリックします。

    Amazon S3 では、バケットの静的ウェブサイトホスティングを有効にします。ページの下部の [静的ウェブサイトホスティング] の下に、バケットのウェブサイトエンドポイントが表示されます。

12. [静的 ウェブサイトホスティング] の下のエンドポイントを書き留めます。

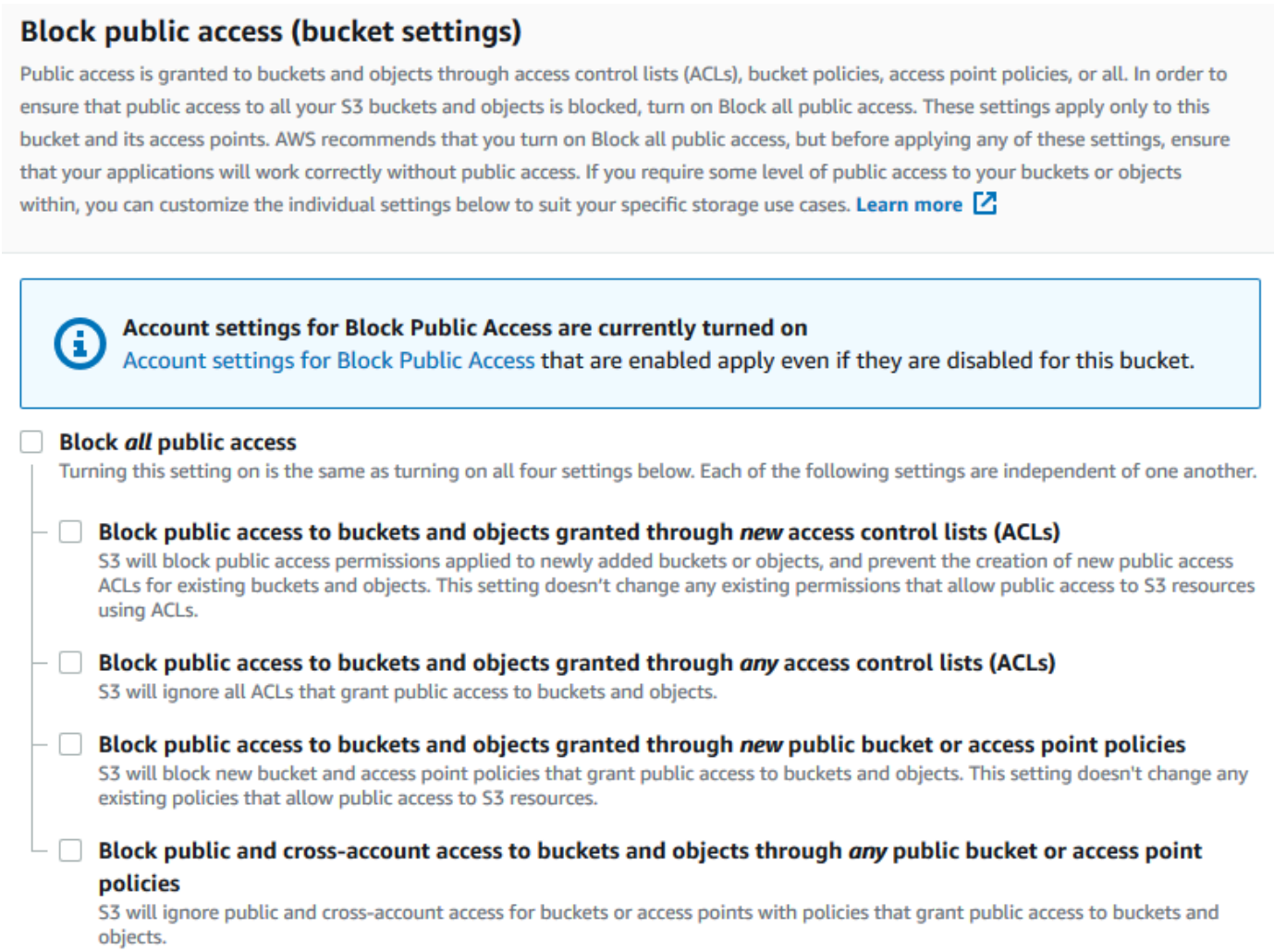
    [Endpoint (エンドポイント)] は、バケットの Amazon S3 ウェブサイトエンドポイントです。バケットを静的ウェブサイトとして設定すると、このエンドポイントを使用してウェブサイトをテストできます。

ステップ 3: パブリックアクセスブロック設定を編集する

デフォルトでは、Amazon S3 はアカウントとバケットへのパブリックアクセスをブロックします。バケットを使用して静的ウェブサイトをホストする場合は、以下のステップを使用して、パブリックアクセスブロック設定を編集できます。

> **Warning**
>
> このステップを完了する前に「Amazon S3 ストレージへのパブリックアクセスのブロック」を読んで、パブリックアクセスを許可することに伴うリスクを理解し、了承してください。パブリックアクセスブロック設定をオフにしてバケットをパブリックにすると、インターネット上のだれでもバケットにアクセスできるようになります。バケットへのすべてのパブリックアクセスをブロックすることをお勧めします。

1. https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開きます。
2. 静的ウェブサイトとして設定されたバケットの名前を選択します。
3. [Permissions (アクセス許可)] を選択します。
4. [ブロックパブリックアクセス (バケット設定)] で [編集] を選択します。
5. [Block all public access (すべてのパブリックアクセスをブロックする)] をクリアし、[Save changes (変更の保存)] を選択します。



Amazon S3 で、バケットのブロックパブリックアクセス設定がオフになります。パブリックな静的ウェブサイトを作成するには、バケットポリシーを追加する前に、アカウントのブロックパブリックアクセス設定を編集する必要があります。アカウントのブロックパブリックアクセス設定が現在有効になっている場合は、[ブロックパブリックアクセス (バケット設定)] の下にメモが表示されます。

ステップ 4: バケットの内容の公開を許可するバケットポリシーを追加する

S3 のパブリックアクセスブロック設定を編集した後で、バケットへのパブリック読み取りアクセスを許可するバケットポリシーを追加できます。パブリック読み取りアクセスを許可すると、インターネット上のだれでもバケットにアクセスできるようになります。

> **Important**
>
> 次のポリシーは、単なる例として、バケットのコンテンツへのフルアクセスを許可します。このステップに進む前に、「Amazon S3 バケット内のファイルを保護するにはどうすればよいですか?」を確認して、S3 バケット内のファイルを保護するためのベストプラクティスと、パブリックアクセスの許可に伴うリスクを理解してください。

1. [バケット] で、バケットの名前を選択します。
2. [Permissions (アクセス許可)] を選択します。
3. [Bucket Policy (バケットポリシー)] で [編集] を選択します。
4. ウェブサイトのパブリック読み取りアクセスを許可するには、次のバケットポリシーをコピーし、[Bucket policy editor (バケットポリシーエディター)] に貼り付けます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PublicReadGetObject",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::Bucket-Name/*"
            ]
        }
    ]
}
```

5. `Resource` をバケット名に更新します。

   前述のバケットポリシーの例では、*`Bucket-Name`* はバケット名のプレースホルダーです。このバケットポリシーを独自のバケットで使用するには、バケット名に合わせてこの名前を更新する必要があります。

6. [Save changes] (変更の保存) をクリックします。

   バケットポリシーが正常に追加されたことを示すメッセージが表示されます。

Policy has invalid resource というエラーが表示された場合は、バケットポリシー内のバケット名がバケット名と一致していることを確認します。バケットポリシーの追加については、「S3 バケットポリシーを追加する方法」を参照してください。

エラーメッセージが表示され、バケットポリシーを保存できない場合は、アカウントとバケットの [パブリックアクセスをブロックする] 設定をチェックして、バケットへのパブリックアクセスを許可していることを確認します。

ステップ 5: インデックスドキュメントを設定する

バケットに対して静的ウェブサイトホスティングを有効にする場合は、インデックスドキュメントの名前 (**index.html** など) を入力します。バケットに対して静的ウェブサイトホスティングを有効にした後、インデックスドキュメント名を含む HTML ファイルをバケットにアップロードします。

インデックスドキュメントを設定するには

1. index.html ファイルを作成します。

   index.html ファイルがない場合は、以下の HTML を使用して作成できます。

```
<html xmlns="http://www.w3.org/1999/xhtml" >
<head>
    <title>My Website Home Page</title>
</head>
<body>
  <h1>Welcome to my website</h1>
  <p>Now hosted on Amazon S3!</p>
</body>
</html>
```

2. インデックスファイルをローカルに保存します。

   インデックスドキュメントファイル名は、[静的ウェブサイトホスティング] ダイアログボックスで入力したインデックスドキュメント名と正確に一致する必要があります。インデックスドキュメント名では、大文字と小文字が区別されます。例えば、[静的ウェブサイトホスティング] ダイアログボックスの [インデックスドキュメント] 名に「index.html」と入力する場合、インデックスドキュメントファイル名も Index.html ではなく index.html である必要があります。

3. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
4. 左のナビゲーションペインで、[汎用バケット] を選択します。
5. バケットリストで、静的ウェブサイトホスティングに使用するバケットの名前を選択します。
6. バケットに対して静的ウェブサイトホスティングを有効にし、インデックスドキュメントの正確な名前 (`index.html` など) を入力します。詳細については、「ウェブサイトのホスティングの有効化」を参照してください。

   静的ウェブサイトホスティングを有効にしたら、ステップ 6 に進みます。
7. インデックスドキュメントをバケットにアップロードするには、以下のいずれかを実行します。

   - インデックスファイルをコンソールバケットのリストにドラッグアンドドロップします。
   - [Upload] を選択し、プロンプトに従ってインデックスファイルを選択してアップロードします。

   手順については、「オブジェクトのアップロード」を参照してください。
8. (オプション) 他のウェブサイトコンテンツをバケットにアップロードします。

ステップ 6: エラードキュメントの設定

バケットに対して静的ウェブサイトホスティングを有効にするときは、エラードキュメントの名前 (例: **`404.html`**) を入力します。バケットに対して静的ウェブサイトホスティングを有効にしたら、エラードキュメント名を含む HTML ファイルをバケットにアップロードします。

エラードキュメントを設定するには

1. エラードキュメント (例: `404.html`) を作成します。
2. エラードキュメントのファイルをローカルに保存します。

   エラードキュメントの名前は、大文字と小文字を区別し、静的ウェブサイトホスティングを有効にする際に入力した名前と厳密に一致している必要があります。たとえば、[Static website hosting] (静的ウェブサイトホスティング) ダイアログボックスの [Error document] (エラードキュメント) 名に `404.html` と入力する場合、エラードキュメントのファイル名も `404.html` である必要があります。
3. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。

4. 左のナビゲーションペインで、[汎用バケット] を選択します。
5. バケットリストで、静的ウェブサイトホスティングに使用するバケットの名前を選択します。
6. バケットに対して静的ウェブサイトホスティングを有効にし、エラードキュメントの正確な名前 (例: `404.html`) を入力します。詳細については、ウェブサイトのホスティングの有効化およびカスタムエラードキュメントの設定を参照してください。

   静的ウェブサイトホスティングを有効にしたら、ステップ 6 に進みます。
7. エラードキュメントをバケットにアップロードするには、以下のいずれかを実行します。

   - エラードキュメントファイルをコンソールバケットのリストにドラッグアンドドロップします。
   - [Upload] を選択し、プロンプトに従ってインデックスファイルを選択してアップロードします。

   手順については、「オブジェクトのアップロード」を参照してください。

ステップ 7: ウェブサイトエンドポイントをテストする

バケットに静的ウェブサイトホスティングを設定したら、ウェブサイトエンドポイントをテストできます。

> **Note**
>
> Amazon S3 は、ウェブサイトへの HTTPS アクセスをサポートしていません。HTTPS を使用する場合は、Amazon CloudFront を使用して Amazon S3 でホストされている静的ウェブサイトを提供できます。
> 詳細については、「CloudFront を使用して、Amazon S3 でホストされた静的ウェブサイトを公開するにはどうすればよいですか?」と「ビューワーと CloudFront との通信で HTTPS を必須にする」を参照してください。

1. [バケット] で、バケットの名前を選択します。
2. [プロパティ] を選択します。
3. ページの下部の [静的ウェブサイトホスティング] で、[Bucket website endpoint (バケットウェブサイトエンドポイント)] を選択します。

インデックスドキュメントが別のブラウザウィンドウで開きます。

これで、Amazon S3 でウェブサイトがホスティングされるようになりました。このウェブサイトには、Amazon S3 ウェブサイトエンドポイントの URL を指定してアクセスできます。ただし、作成したウェブサイトのコンテンツを配信するのに、`example.com` などのドメインを使用することもできます。また、Amazon S3 のルートドメインサポートを利用すると、`http://www.example.com` と `http://example.com` のどちらのリクエストでも処理できるようになります。このようにするには、追加のステップが必要です。例については、「チュートリアル: Route 53 に登録されたカスタムドメインを使用した静的ウェブサイトの設定」を参照してください。

ステップ 8: クリーンアップする

学習のためだけに静的ウェブサイトを作成した場合は、割り当てた AWS リソースを削除して、料金が発生しないようにします。AWS リソースを削除すると、ウェブサイトは使用できなくなります。詳細については、「汎用バケットの削除」を参照してください。

チュートリアル: Route 53 に登録されたカスタムドメインを使用した静的ウェブサイトの設定

Amazon S3 で静的ウェブサイトをホスティングするとします。ドメインは Amazon Route 53 で登録済みであり (例: `example.com`)、`http://www.example.com` と `http://example.com` へのリクエストに対しては Amazon S3 からコンテンツを配信するようにします。このチュートリアルでは、静的ウェブサイトをホスティングし、Route 53 に登録されているカスタムドメイン名を持つウェブサイトのリダイレクトを Amazon S3 で作成する方法について説明します。Amazon S3 でホストしようとしている既存のウェブサイトを使ってもよいですし、このチュートリアルで一から始めることもできます。

チュートリアルが完了したら、Amazon CloudFront を使ってウェブサイトのパフォーマンスを向上させることも可能です。詳細については、「Amazon CloudFront によるウェブサイトの高速化」を参照してください。

> **Note**
>
> Amazon S3 ウェブサイトエンドポイントは HTTPS またはアクセスポイントをサポートしていません。HTTPS を使用する場合は、Amazon CloudFront を使用して Amazon S3 でホストされている静的ウェブサイトを提供できます。

CloudFront と Amazon S3 でコンテンツを安全にホストする方法のチュートリアルについては、「チュートリアル: Amazon S3、Amazon CloudFront、Amazon Route 53 を使用したオンデマンドストリーミング動画のホスティング。」を参照してください。詳細については、「CloudFront を使用して、Amazon S3 でホストされた静的ウェブサイトを公開するにはどうすればよいですか?」と「ビューワーと CloudFrontとの通信で HTTPS を必須にする」を参照してください。

AWS CloudFormation テンプレートを使用した静的ウェブサイトの設定の自動化

AWS CloudFormation テンプレートを使用すると、静的ウェブサイトの設定を自動化することができます。AWS CloudFormation テンプレートによって安全な静的ウェブサイトをホストするために必要なコンポーネントが設定されるため、コンポーネントの設定よりもウェブサイトのコンテンツに注力できるようになります。

AWS CloudFormation テンプレートには、以下のコンポーネントが含まれています。

- Amazon S3 - 静的ウェブサイトをホストする Amazon S3 バケットを作成します。
- CloudFront - 静的ウェブサイトを高速化するために、CloudFront ディストリビューションを作成します。
- Lambda@Edge - Lambda@Edge を使用して、サーバーのすべてのレスポンスにセキュリティヘッダーを追加します。セキュリティヘッダーは、ウェブサーバーレスポンス内のヘッダーのグループであり、追加のセキュリティ対策を講じるようにウェブブラウザに指示します。詳細については、ブログ記事「Adding HTTP security headers using Lambda@Edge and Amazon CloudFront」を参照してください。

この AWS CloudFormation テンプレートは、ダウンロードして使用することができます。詳細および手順については、Amazon CloudFront デベロッパーガイドの「安全な静的ウェブサイトの使用開始」を参照してください。

トピック

- 開始する前に
- ステップ 1: カスタムドメインを Route 53 に登録する
- ステップ 2: バケットを 2 つ作成する
- ステップ 3: ウェブサイトホスティング用にルートドメインのバケットを設定する
- ステップ 4: ウェブサイトのリダイレクト用にサブドメインのバケットを設定する

- ステップ 5: ウェブサイトトラフィックのログ記録を設定する
- ステップ 6: インデックスとウェブサイトのコンテンツをアップロードする
- ステップ 7: エラードキュメントのアップロード
- ステップ 8: S3 のパブリックアクセスのブロック設定を編集する
- ステップ 9: バケットポリシーをアタッチする
- ステップ 10: ドメインエンドポイントをテストする
- ステップ 11: ドメインとサブドメインのエイリアスレコードを追加する
- ステップ 12: ウェブサイトをテストする
- Amazon CloudFront によるウェブサイトの高速化
- サンプルリソースのクリーンアップ

開始する前に

この例で実行するステップでは、以下のサービスを使用します。

Amazon Route 53 - Route 53 では、ドメインを登録し、ドメインのインターネットトラフィックをルーティングする先を定義します。以下の例では、Route 53 エイリアスレコードを作成して、ドメイン (`example.com`) とサブドメイン (`www.example.com`) のトラフィックを HTML ファイルが含まれている Amazon S3 バケットにルーティングする方法を示します。

Amazon S3 - Amazon S3 を使用して、バケットを作成したり、サンプルウェブサイトページをアップロードしたり、全員がコンテンツを表示できるようアクセス許可を設定したりします。また、ウェブサイトホスティング用にバケットを設定することもできます。

ステップ 1: カスタムドメインを Route 53 に登録する

登録済みドメイン名 (`example.com` など) がない場合は、Route 53 でドメイン名を登録します。詳細については、Amazon Route 53 デベロッパーガイドの「新しいドメインの登録」を参照してください。ドメイン名を登録したら、Amazon S3 バケットを作成してウェブサイトのホスティング用に設定できます。

ステップ 2: バケットを 2 つ作成する

ルートドメインとサブドメインからの両方のリクエストをサポートするには、2 つのバケットを作成します。

- ドメインバケット - `example.com`

- サブドメインバケット - www.example.com

これらのバケット名はドメイン名と厳密に一致している必要があります。この例では、ドメイン名は example.com です。コンテンツをルートドメインバケット (example.com) からホストします。サブドメインバケットのリダイレクトリクエストを作成します (www.example.com)。他のユーザーがブラウザに www.example.com を入力すると、example.com にリダイレクトされ、その名前で Amazon S3 バケットにホストされているコンテンツが表示されます。

バケットをウェブサイトホスティング用に作成するには

以下の手順では、ウェブサイトホスティングにバケットを作成する方法の概要を説明します。バケットの作成に関するステップバイステップの方法は、「汎用バケットの作成」を参照してください。

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. ルートドメインのバケットを作成します。

   a. ページ上部にあるナビゲーションバーで、現在表示されている AWS リージョン の名前をクリックします。次に、バケットを作成するリージョンを選択します。

   > **Note**
   >
   > レイテンシーとコストを最小化するため、さらに規制条件に対応するために、最寄りのリージョンを選択します。明示的に別のリージョンに移動する場合を除き、特定のリージョンに保管されたオブジェクトは、そのリージョンから移動されることはありません。Amazon S3 AWS リージョン のリストについては、「Amazon Web Services 全般のリファレンス」の「AWS のサービス エンドポイント」を参照してください。

   b. 左のナビゲーションペインで、[汎用バケット] を選択します。
   c. [Create bucket (バケットの作成)] を選択します。[バケットの作成] ページが開きます。
   d. [バケット名] (**example.com** など) を入力します。
   e. バケットを作成するリージョンを選択します。

      レイテンシーとコストを最小限に抑えるため、または規制要件に対処するために、最寄りのリージョンを選択します。選択したリージョンによって、Amazon S3 ウェブサイトエンドポイントが決まります。詳細については、「ウェブサイトエンドポイント」を参照してください。

f. デフォルト設定をそのまま使用してバケットを作成するには、[作成] を選択します。

3. サブドメインのバケットを作成します。

a. [Create bucket] (バケットの作成) をクリックします。

b. [バケット名] (**www.example.com** など) を入力します。

c. バケットを作成するリージョンを選択します。

レイテンシーとコストを最小限に抑えるため、または規制要件に対処するために、最寄りのリージョンを選択します。選択したリージョンによって、Amazon S3 ウェブサイトエンドポイントが決まります。詳細については、「ウェブサイトエンドポイント」を参照してください。

d. デフォルト設定をそのまま使用してバケットを作成するには、[作成] を選択します。

次のステップでは、ウェブサイトホスティング用に example.com を設定します。

ステップ 3: ウェブサイトホスティング用にルートドメインのバケットを設定する

このステップでは、ルートドメインのバケット (example.com) をウェブサイトとして設定します。このバケットには、ウェブサイトのコンテンツが含まれます。バケットをウェブサイトホスティング用に設定すると、そのウェブサイトには ウェブサイトエンドポイント を使用してアクセスできるようになります。

静的ウェブサイトホスティングを有効にするには

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 左のナビゲーションペインで、[汎用バケット] を選択します。
3. バケットリストで、静的ウェブサイトホスティングを有効にするバケットの名前を選択します。
4. [プロパティ] を選択します。
5. [静的ウェブサイトホスティング] で [編集] を選択します。
6. [このバケットを使用してウェブサイトをホストする] を選択します。
7. [静的ウェブサイトホスティング] で [有効化] を選択します。
8. [インデックスドキュメント] に、インデックスドキュメントのファイル名 (通常は index.html) を入力します。

インデックスドキュメント名の大文字と小文字は区別されます。この名前は、S3 バケットにアップロードする HTML インデックスドキュメントのファイル名と正確に一致する必要があります。バケットをウェブサイトホスティング用に設定するときは、インデックスドキュメントを指定する必要があります。Amazon S3 からこのインデックスドキュメントが返されるのは、ルートドメインまたはサブフォルダに対するリクエストが行われたときです。詳細については、「インデックスドキュメントの設定」を参照してください。

9. 4XX クラスエラーに関する独自のカスタムエラードキュメントを指定する場合は、[エラードキュメント] にカスタムエラードキュメントのファイル名を入力します。

   エラードキュメント名の大文字と小文字は区別されます。この名前は、S3 バケットにアップロードする HTML エラードキュメントのファイル名と正確に一致する必要があります。カスタムエラードキュメントを指定しない場合、エラーが発生すると、Amazon S3 からデフォルトの HTML エラードキュメントが返されます。詳細については、「カスタムエラードキュメントの設定」を参照してください。

10. (オプション) 高度なリダイレクトツールを指定する場合は、[Rredirection rules] (リダイレクトルール) に、JSON を入力してルールを記述します。

    例えば、条件に応じてリクエストのルーティング先を変えることができます。この条件として使用できるのは、リクエストの中の特定のオブジェクトキー名またはプレフィックスです。詳細については、「高度な条件付きリダイレクトを使用するようにリダイレクトルールを設定する」を参照してください。

11. [Save changes] (変更の保存) をクリックします。

    Amazon S3 では、バケットの静的ウェブサイトホスティングを有効にします。ページの下部の [静的ウェブサイトホスティング] の下に、バケットのウェブサイトエンドポイントが表示されます。

12. [静的 ウェブサイトホスティング] の下のエンドポイントを書き留めます。

    [Endpoint (エンドポイント)] は、バケットの Amazon S3 ウェブサイトエンドポイントです。バケットを静的ウェブサイトとして設定すると、このエンドポイントを使用してウェブサイトをテストできます。

パブリックアクセスのブロック設定を編集し、パブリック読み取りアクセスを許可するバケットポリシーを追加したら、ウェブサイトエンドポイントを使用してウェブサイトにアクセスできます。

次のステップで、リクエストをドメイン (www.example.com) にリダイレクトするように、サブドメイン (example.com) を設定します。

ステップ 4: ウェブサイトのリダイレクト用にサブドメインのバケットを設定する

ウェブサイトホスティング用にルートドメインのバケットを設定したら、このドメインにすべてのリクエストをリダイレクトするように、サブドメインのバケットを設定できます。この例では www.example.com のすべてのリクエストが example.com にリダイレクトされます。

リダイレクトリクエストを設定するには

1. Amazon S3 コンソールの [汎用バケット] リストで、サブドメインのバケット名 (この例では www.example.com) を選択します。
2. [プロパティ] を選択します。
3. [静的ウェブサイトホスティング] で [編集] を選択します。
4. [Redirect requests for an object (オブジェクトのリクエストをリダイレクト)] を選択します。
5. [Target bucket (ターゲットバケット)] ボックスに、ルートドメイン (**example.com** など) を入力します。
6. [Protocol (プロトコル)] で、[http] を選択します。
7. [Save changes] (変更の保存) をクリックします。

ステップ 5: ウェブサイトトラフィックのログ記録を設定する

ウェブサイトにアクセスする閲覧者の数を追跡するには、オプションでルートドメインのバケットのログ記録を有効にできます。詳細については、「サーバーアクセスログによるリクエストのログ記録」を参照してください。Amazon CloudFront を使用してウェブサイトを高速化する場合は、CloudFront のログ記録を使用することもできます。

ルートドメインバケット用のサーバーアクセスのログ記録を有効にするには

1. https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開きます。
2. 静的ウェブサイトとして設定しているバケットを作成したのと同じリージョンで、ログ記録用のバケットを作成します (例: logs.example.com)。
3. サーバアクセスのログを記録するログファイル用のフォルダを作成します (例: logs)。
4. (オプション) CloudFront を使用してウェブサイトのパフォーマンスを向上させる場合は、CloudFront ログファイル用のフォルダを作成します (例: cdn)。

> **Important**
>
> ディストリビューションを作成または更新して CloudFront のログを有効にすると、CloudFront はバケットのアクセスコントロールリスト (ACL) を更新して、バケットにログを書き込む `awslogsdelivery` アクセス許可を `FULL_CONTROL` アカウントに付与します。詳細については、「Amazon CloudFront デベロッパーガイド」の「標準ログ記録の設定とログファイルへのアクセスに必要なアクセス許可」を参照してください。ログを保存するバケットが S3 オブジェクト所有権のバケット所有者の強制設定を使用して ACL を無効にすると、CloudFront はバケットにログを書き込むことができません。詳細については、「オブジェクトの所有権の制御とバケットの ACL の無効化。」を参照してください。

5. [Bucket (バケット)] リストで、ルートドメインのバケットを選択します。
6. [プロパティ] を選択します。
7. [Server access logging (サーバーアクセスのログ記録)] で、[Edit (編集)] を選択します。
8. [Enable] を選択します。
9. [Target bucket (ターゲットバケット)] で、サーバーアクセスログのバケットとフォルダの宛先を選択します。

   - フォルダとバケットの場所を参照します。
     1. [Browse S3(S3 の参照)] を選択します。
     2. バケット名を選択し、ログフォルダを選択します。
     3. [Choose path (パスの選択)] を選択します。
   - S3 バケットパスを入力します (例: `s3://logs.example.com/logs/`)。
10. [Save changes] (変更の保存) をクリックします。

    ログバケットで、ログにアクセスできるようになりました。Amazon S3 は 2 時間おきにログバケットにウェブサイトアクセスログを書き込みます。

ステップ 6: インデックスとウェブサイトのコンテンツをアップロードする

このステップでは、インデックスドキュメントとオプションのウェブサイトコンテンツをルートドメインのバケットにアップロードします。

バケットに対して静的ウェブサイトホスティングを有効にする場合は、インデックスドキュメントの名前 (**index.html** など) を入力します。バケットに対して静的ウェブサイトホスティングを有効にした後、インデックスドキュメント名を含む HTML ファイルをバケットにアップロードします。

インデックスドキュメントを設定するには

1. index.html ファイルを作成します。

   index.html ファイルがない場合は、以下の HTML を使用して作成できます。

   ```
   <html xmlns="http://www.w3.org/1999/xhtml" >
   <head>
       <title>My Website Home Page</title>
   </head>
   <body>
     <h1>Welcome to my website</h1>
     <p>Now hosted on Amazon S3!</p>
   </body>
   </html>
   ```

2. インデックスファイルをローカルに保存します。

   インデックスドキュメントファイル名は、[静的ウェブサイトホスティング] ダイアログボックスで入力したインデックスドキュメント名と正確に一致する必要があります。インデックスドキュメント名では、大文字と小文字が区別されます。例えば、[静的ウェブサイトホスティング] ダイアログボックスの [インデックスドキュメント] 名に「index.html」と入力する場合、インデックスドキュメントファイル名も Index.html ではなく index.html である必要があります。

3. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
4. 左のナビゲーションペインで、[汎用バケット] を選択します。
5. バケットリストで、静的ウェブサイトホスティングに使用するバケットの名前を選択します。
6. バケットに対して静的ウェブサイトホスティングを有効にし、インデックスドキュメントの正確な名前 (index.html など) を入力します。詳細については、「ウェブサイトのホスティングの有効化」を参照してください。

   静的ウェブサイトホスティングを有効にしたら、ステップ 6 に進みます。
7. インデックスドキュメントをバケットにアップロードするには、以下のいずれかを実行します。

- インデックスファイルをコンソールバケットのリストにドラッグアンドドロップします。
- [Upload] を選択し、プロンプトに従ってインデックスファイルを選択してアップロードします。

手順については、「オブジェクトのアップロード」を参照してください。

8. (オプション) 他のウェブサイトコンテンツをバケットにアップロードします。

ステップ 7: エラードキュメントのアップロード

バケットに対して静的ウェブサイトホスティングを有効にするときは、エラードキュメントの名前 (例: **`404.html`**) を入力します。バケットに対して静的ウェブサイトホスティングを有効にしたら、エラードキュメント名を含む HTML ファイルをバケットにアップロードします。

エラードキュメントを設定するには

1. エラードキュメント (例: `404.html`) を作成します。
2. エラードキュメントのファイルをローカルに保存します。

   エラードキュメントの名前は、大文字と小文字を区別し、静的ウェブサイトホスティングを有効にする際に入力した名前と厳密に一致している必要があります。たとえば、[Static website hosting] (静的ウェブサイトホスティング) ダイアログボックスの [Error document] (エラードキュメント) 名に `404.html` と入力する場合、エラードキュメントのファイル名も `404.html` である必要があります。
3. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
4. 左のナビゲーションペインで、[汎用バケット] を選択します。
5. バケットリストで、静的ウェブサイトホスティングに使用するバケットの名前を選択します。
6. バケットに対して静的ウェブサイトホスティングを有効にし、エラードキュメントの正確な名前 (例: `404.html`) を入力します。詳細については、ウェブサイトのホスティングの有効化およびカスタムエラードキュメントの設定を参照してください。

   静的ウェブサイトホスティングを有効にしたら、ステップ 6 に進みます。
7. エラードキュメントをバケットにアップロードするには、以下のいずれかを実行します。

- エラードキュメントファイルをコンソールバケットのリストにドラッグアンドドロップします。
- [Upload] を選択し、プロンプトに従ってインデックスファイルを選択してアップロードします。

手順については、「オブジェクトのアップロード」を参照してください。

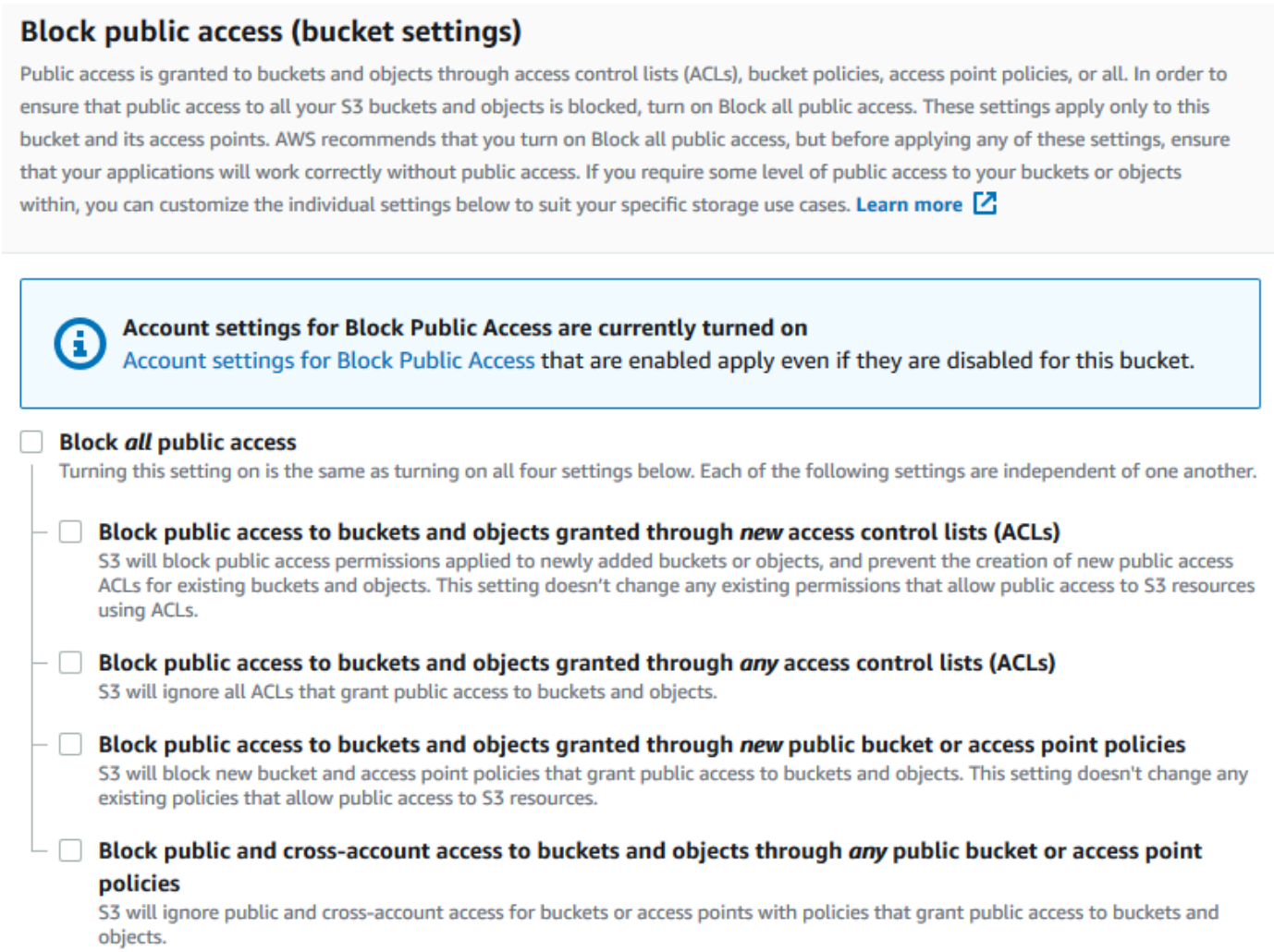
ステップ 8: S3 のパブリックアクセスのブロック設定を編集する

この例では、ドメインバケット (example.com) のパブリックアクセスブロック設定を編集して、パブリックアクセスを許可します。

デフォルトでは、Amazon S3 はアカウントとバケットへのパブリックアクセスをブロックします。バケットを使用して静的ウェブサイトをホストする場合は、以下のステップを使用して、パブリックアクセスブロック設定を編集できます。

> **Warning**
>
> このステップを完了する前に「Amazon S3 ストレージへのパブリックアクセスのブロック」を読んで、パブリックアクセスを許可することに伴うリスクを理解し、了承してください。パブリックアクセスブロック設定をオフにしてバケットをパブリックにすると、インターネット上のだれでもバケットにアクセスできるようになります。バケットへのすべてのパブリックアクセスをブロックすることをお勧めします。

1. https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開きます。
2. 静的ウェブサイトとして設定されたバケットの名前を選択します。
3. [Permissions (アクセス許可)] を選択します。
4. [ブロックパブリックアクセス (バケット設定)] で [編集] を選択します。
5. [Block all public access (すべてのパブリックアクセスをブロックする)] をクリアし、[Save changes (変更の保存)] を選択します。



Amazon S3 で、バケットのブロックパブリックアクセス設定がオフになります。パブリックな静的ウェブサイトを作成するには、バケットポリシーを追加する前に、アカウントのブロックパブリックアクセス設定を編集する必要があります。アカウントのブロックパブリックアクセス設定が現在有効になっている場合は、[ブロックパブリックアクセス (バケット設定)] の下にメモが表示されます。

ステップ 9: バケットポリシーをアタッチする

この例では、バケットポリシーをドメインバケット (`example.com`) にアタッチして、パブリック読み取りアクセスを許可します。例えば、バケットポリシーの例の *`Bucket-Name`* は、ドメインバケットの名前 (例: `example.com`) に置き換えます。

S3 のパブリックアクセスブロック設定を編集した後で、バケットへのパブリック読み取りアクセスを許可するバケットポリシーを追加できます。パブリック読み取りアクセスを許可すると、インターネット上のだれでもバケットにアクセスできるようになります。

> **Important**
>
> 次のポリシーは、単なる例として、バケットのコンテンツへのフルアクセスを許可します。このステップに進む前に、「Amazon S3 バケット内のファイルを保護するにはどうすればよいですか?」を確認して、S3 バケット内のファイルを保護するためのベストプラクティスと、パブリックアクセスの許可に伴うリスクを理解してください。

1. [バケット] で、バケットの名前を選択します。
2. [Permissions (アクセス許可)] を選択します。
3. [Bucket Policy (バケットポリシー)] で [編集] を選択します。
4. ウェブサイトのパブリック読み取りアクセスを許可するには、次のバケットポリシーをコピーし、[Bucket policy editor (バケットポリシーエディター)] に貼り付けます。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PublicReadGetObject",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::Bucket-Name/*"
            ]
        }
    ]
}
```

5. `Resource` をバケット名に更新します。

   前述のバケットポリシーの例では、*`Bucket-Name`* はバケット名のプレースホルダーです。このバケットポリシーを独自のバケットで使用するには、バケット名に合わせてこの名前を更新する必要があります。

6. [Save changes] (変更の保存) をクリックします。

   バケットポリシーが正常に追加されたことを示すメッセージが表示されます。

   `Policy has invalid resource` というエラーが表示された場合は、バケットポリシー内のバケット名がバケット名と一致していることを確認します。バケットポリシーの追加については、「S3 バケットポリシーを追加する方法」を参照してください。

   エラーメッセージが表示され、バケットポリシーを保存できない場合は、アカウントとバケットの [パブリックアクセスをブロックする] 設定をチェックして、バケットへのパブリックアクセスを許可していることを確認します。

次のステップでは、ウェブサイトのエンドポイントを判別し、ドメインエンドポイントをテストできます。

ステップ 10: ドメインエンドポイントをテストする

パブリックウェブサイトをホストするようにドメインバケットを設定したら、エンドポイントをテストできます。詳細については、「ウェブサイトエンドポイント」を参照してください。サブドメインバケットは、静的ウェブサイトホスティングではなくウェブサイトリダイレクト用に設定されているため、テストできるのはドメインバケットのエンドポイントのみです。

> **Note**
>
> Amazon S3 は、ウェブサイトへの HTTPS アクセスをサポートしていません。HTTPS を使用する場合は、Amazon CloudFront を使用して Amazon S3 でホストされている静的ウェブサイトを提供できます。
> 詳細については、「CloudFront を使用して、Amazon S3 でホストされた静的ウェブサイトを公開するにはどうすればよいですか?」と「ビューワーと CloudFront との通信で HTTPS を必須にする」を参照してください。

1. [バケット] で、バケットの名前を選択します。
2. [プロパティ] を選択します。
3. ページの下部の [静的ウェブサイトホスティング] で、[Bucket website endpoint (バケットウェブサイトエンドポイント)] を選択します。

   インデックスドキュメントが別のブラウザウィンドウで開きます。

次のステップでは、顧客が両方のカスタム URL を使用してサイトにアクセスできるように、Amazon Route 53 を使用します。

ステップ 11: ドメインとサブドメインのエイリアスレコードを追加する

このステップでは、ドメインマップ `example.com` と `www.example.com` のホストゾーンに追加するエイリアスレコードを作成します。IP アドレスを使用する代わりに、このエイリアスレコードでは Amazon S3 ウェブサイトエンドポイントが使用されます。Amazon Route 53 によって、エイリアスレコードと、Amazon S3 バケットが存在する IP アドレスとのマッピングが維持されます。ルートドメイン用とサブドメイン用の 2 つのエイリアスレコードを作成します。

ルートドメインとサブドメインのエイリアスレコードの追加

ルートドメインのエイリアスレコードを追加するには (**`example.com`**)

1. Route 53 コンソール (https://console.aws.amazon.com/route53/) を開きます。

   > **Note**
   >
   > Route 53 をまだ使用していない場合は、Amazon Route 53 デベロッパーガイドの「ステップ 1: ドメインの登録」を参照してください。セットアップが完了したら、指示を再開できます。

2. [Hosted zones (ホストゾーン)] を選択します。
3. ホストゾーンのリストで、ドメイン名に一致するホストゾーンの名前を選択します。
4. [Create record (レコードを作成)] を選択します。
5. [Switch to wizard] (ウィザードに切り替える) を選択します。

   > **Note**
   >
   > クイック作成を使用してエイリアスレコードを作成する場合は、「Route 53 を設定して S3 バケットにトラフィックをルーティングする」を参照してください。

6. [Simple routing (シンプルルーティング)] を選択して、[Next (次へ)] を選択します。
7. [Define simple record (シンプルなレコードを定義)] を選択します。
8. [レコード名] では、デフォルト値をそのまま使用します。これが、ホストゾーンとドメインの名前です。

9. [Value/Route traffic to (値/トラフィックのルーティング先)] で、[Alias to S3 website endpoint (S3 ウェブサイトエンドポイントへのエイリアス)] を選択します。
10. リージョンを選択します。
11. S3 バケットを選択します。

    バケット名は、[Name (名前)] ボックスに表示されている名前と一致する必要があります。[Choose S3 bucket] (S3 バケットを選択) リストに、バケットが作成されたリージョンの Amazon S3 ウェブサイトエンドポイントとともにバケット名が表示されます (例: `s3-website-us-west-1.amazonaws.com (example.com)`)。

    次の場合は、バケットをリストする S3 バケットを選択します。

    - バケットを静的ウェブサイトとして設定した場合。
    - バケットの名前が、作成するレコードの名前と同じである場合。
    - 現在の AWS アカウント でバケットを作成した場合。

    バケットが [Choose S3 bucket] (S3 バケットの選択) リストに表示されない場合は、バケットが作成されたリージョンの Amazon S3 ウェブサイトエンドポイント (例: **`s3-website-us-west-2.amazonaws.com`**) を入力します。Amazon S3 ウェブサイトエンドポイントの完全なリストについては、「Amazon S3 ウェブサイトエンドポイント」を参照してください。エイリアス先の詳細については、Amazon Route 53 デベロッパーガイドの「値/トラフィックのルーティング先」を参照してください。
12. [レコードタイプ] で、[A - IPv4 アドレスと一部の AWS リソースにトラフィックをルーティングします] を選択します。
13. [Evaluate target health (ターゲットの正常性の評価)] で [No (いいえ)] を選択します。
14. [Define simple record (シンプルなレコードを定義)] を選択します。

サブドメインのエイリアスレコードを追加するには (**`www.example.com`**)

1. [Configure records] (レコードを設定) で、[Define simple record] (シンプルなレコードを定義) を選択します。
2. サブドメインの [Record name (レコード名)] に「`www`」と入力します。
3. [Value/Route traffic to (値/トラフィックのルーティング先)] で、[Alias to S3 website endpoint (S3 ウェブサイトエンドポイントへのエイリアス)] を選択します。
4. リージョンを選択します。

5. S3 バケットを選択します (例: `s3-website-us-west-2.amazonaws.com (www.example.com)`)。

   バケットが [Choose S3 bucket] (S3 バケットの選択) リストに表示されない場合は、バケットが作成されたリージョンの Amazon S3 ウェブサイトエンドポイント (例: **`s3-website-us-west-2.amazonaws.com`**) を入力します。Amazon S3 ウェブサイトエンドポイントの完全なリストについては、「Amazon S3 ウェブサイトエンドポイント」を参照してください。エイリアス先の詳細については、Amazon Route 53 デベロッパーガイドの「値/トラフィックのルーティング先」を参照してください。
6. [レコードタイプ] で、[A - IPv4 アドレスと一部の AWS リソースにトラフィックをルーティングします] を選択します。
7. [Evaluate target health (ターゲットの正常性の評価)] で [No (いいえ)] を選択します。
8. [Define simple record (シンプルなレコードを定義)] を選択します。
9. [Configure records] (レコードを設定) ページで、[Create records] (レコードを作成) を選択します。

> **Note**
>
> 通常、変更は 60 秒以内にすべての Route 53 サーバーに伝播されます。伝播が完了すると、この手順で作成したエイリアスレコードの名前を使用して、トラフィックを Amazon S3 バケットにルーティングできます。

ルートドメインとサブドメインのエイリアスレコードの追加 (以前の Route 53 コンソール)

ルートドメインのエイリアスレコードを追加するには (**`example.com`**)

Route 53 コンソールは再設計されました。Route 53 コンソールでは、暫定的に以前のコンソールを使用することもできます。以前の Route 53 コンソールを使用する場合は、以下の手順に従ってください。

1. Route 53 コンソール (https://console.aws.amazon.com/route53/) を開きます。

> **Note**
>
> Route 53 をまだ使用していない場合は、Amazon Route 53 デベロッパーガイドの「ステップ 1: ドメインの登録」を参照してください。セットアップが完了したら、指示を再開できます。

2. [ホストゾーン] を選択します。
3. ホストゾーンのリストで、ドメイン名に一致するホストゾーンの名前を選択します。
4. [Create Record Set (レコードセットの作成)] を選択します。
5. 次の値を指定します。

   名前

   ホストゾーンとドメインの名前であるデフォルト値を受け入れます。

   ルートドメインの場合、[Name (名前)] フィールドに追加情報を入力する必要はありません。

   タイプ

   [A – IPv4 address (A – IPv4 address)] を選択します。

   エイリアス

   [Yes] を選択します。

   エイリアス先

   リストの [S3 website endpoints (S3 ウェブサイトエンドポイント)] セクションで、バケット名を選択します。

   バケット名は、[Name (名前)] ボックスに表示されている名前と一致する必要があります。[Alias Target (エイリアス先)] リストでは、バケット名の後にはバケットが作成されたリージョンの Amazon S3 ウェブサイトエンドポイントが続きます (例: `example.com (s3-website-us-west-2.amazonaws.com)`)。以下の場合は、[Alias Target] にバケットが表示されます。

   - バケットを静的ウェブサイトとして設定した場合。
   - バケットの名前が、作成するレコードの名前と同じである場合。
   - 現在の AWS アカウント でバケットを作成した場合。

バケットが [エイリアス先] リストに表示されない場合は、バケットが作成されたリージョンの Amazon S3 ウェブサイトエンドポイント (s3-website-us-west-2 など) を入力します。Amazon S3 ウェブサイトエンドポイントの完全なリストについては、「Amazon S3 ウェブサイトエンドポイント」を参照してください。エイリアス先の詳細については、Amazon Route 53 デベロッパーガイドの「値/トラフィックのルーティング先」を参照してください。

ルーティングポリシー

デフォルト値の [Simple] をそのまま使用します。

ターゲットの正常性の評価

デフォルト値の [No] をそのまま使用します。

6. [Create] を選択します。

サブドメインのエイリアスレコードを追加するには (**www.example.com**)

1. ルートドメイン (example.com) のホストゾーンで、[Create Record Set (レコードセットの作成)] を選択します。
2. 次の値を指定します。

名前

サブドメインの場合、ボックスに www と入力します。

タイプ

[A – IPv4 address (A – IPv4 address)] を選択します。

エイリアス

[Yes] を選択します。

エイリアス先

リストの [S3 website endpoints (S3 ウェブサイトエンドポイント)] セクションで、[Name (名前)] フィールドに表示される名前と同じバケット名を選択します (例: www.example.com (s3-website-us-west-2.amazonaws.com))。

ルーティングポリシー

デフォルト値の [Simple] をそのまま使用します。

ターゲットの正常性の評価

デフォルト値の [No] をそのまま使用します。

3. [Create] を選択します。

> **Note**
>
> 通常、変更は 60 秒以内にすべての Route 53 サーバーに伝播されます。伝播が完了すると、この手順で作成したエイリアスレコードの名前を使用して、トラフィックを Amazon S3 バケットにルーティングできます。

ステップ 12: ウェブサイトをテストする

ウェブサイトとリダイレクトが正しく機能することを確認します。ブラウザで、URL を入力します。この例では、次の URL を試すことができます。

- ドメイン (`http://example.com`) – `example.com` バケット内のインデックスドキュメントを表示します。
- サブドメイン (`http://www.example.com`) – リクエストを `http://example.com` にリダイレクトします。`example.com` バケット内のインデックスドキュメントが表示されます。

ウェブサイトやリダイレクトのリンクが機能しない場合は、以下のことを試してください。

- キャッシュのクリア– ウェブブラウザのキャッシュをクリアします。
- ネームサーバーの確認– キャッシュをクリアしてもウェブページやリダイレクトのリンクが機能しない場合は、ドメインのネームサーバーとホストゾーンのネームサーバーを比較します。ネームサーバーが一致しない場合は、ドメインのネームサーバーを更新してホストゾーンのネームサーバーと一致させる必要があります。詳細については、「ドメインのネームサーバーおよびグルーレコードの追加あるいは変更」を参照してください。

ルートドメインとサブドメインのテストが完了したら、Amazon CloudFront ディストリビューションを設定できます。これにより、ウェブサイトのパフォーマンスを向上させ、ウェブサイトのトラフィックの確認に使用できるログを指定できます。詳細については、「Amazon CloudFront によるウェブサイトの高速化」を参照してください。

Amazon CloudFront によるウェブサイトの高速化

Amazon CloudFront を使用すると、Amazon S3 ウェブサイトのパフォーマンスを高めることができます。CloudFront を使用すると、世界中のデータセンター (エッジロケーション と呼ばれる) からお客様のウェブサイトのファイル (HTML、画像、動画など) を使用できるようになります。閲覧者がウェブサイトからファイルをリクエストすると、CloudFront は自動的に最も近いエッジロケーションのファイルのコピーにリクエストをリダイレクトします。これにより、遠い場所にあるデータセンターからコンテンツをリクエストした場合よりもダウンロード時間が高速になります。

CloudFront は、指定した期間にわたってコンテンツをエッジロケーションにキャッシュします。閲覧者が有効期限より長くキャッシュされていたコンテンツをリクエストすると、CloudFront はオリジンサーバーをチェックしてより新しいバージョンのコンテンツがあるかどうかを確認します。新しいバージョンが利用可能である場合、CloudFront は新しいバージョンをエッジロケーションにコピーします。元のコンテンツへの変更は、閲覧者がコンテンツをリクエストすると、エッジロケーションにレプリケートされます。

Route 53 なしで CloudFront を使用する

このページのチュートリアルでは Route 53 を使用して CloudFront 配信をポイントしています。ただし、Route 53 を使用せずに CloudFront を使用して Amazon S3 バケットでホストされているコンテンツを配信する場合は、「Amazon CloudFront チュートリアル: Amazon S3 用の動的コンテンツ配信のセットアップ」を参照してください。CloudFront を使用して Amazon S3 バケットでホストされているコンテンツを配信する場合は、任意のバケット名を使用できます。また、HTTP と HTTPS の両方がサポートされます。

AWS CloudFormation テンプレートを使用した設定の自動化

ウェブサイトへの配信を行う CloudFront ディストリビューションを作成する安全な静的ウェブサイトを、AWS CloudFormation テンプレートを使用して設定する方法の詳細については、Amazon CloudFront デベロッパーガイドの「安全な静的ウェブサイトの開始方法」を参照してください。

トピック

- ステップ 1: CloudFront ディストリビューションを作成する
- ステップ 2: ドメインとサブドメインのレコードセットを更新する
- (オプション) ステップ 3: ログファイルを確認する

ステップ 1: CloudFront ディストリビューションを作成する

まず、CloudFront ディストリビューションを作成します。これにより、ウェブサイトは世界中のデータセンターから利用できるようになります。

Amazon S3 オリジンを使用してディストリビューションを作成するには

1. で CloudFront コンソールを開きますhttps://console.aws.amazon.com/cloudfront/v4/home
2. [Create Distribution] を選択します。
3. [ディストリビューションの作成] ページで、[オリジンの設定] セクションの [オリジンドメイン名] に、バケットの Amazon S3 ウェブサイトエンドポイントを入力します (例: **`example.com.s3-website.us-west-1.amazonaws.com`**)。

   CloudFront により自動的に [Origin ID (オリジン ID)] が入力されます。
4. [Default Cache Behavior Settings (キャッシュ動作のデフォルト設定)] の値はデフォルトのままにしておきます。

   [ビューワープロトコルポリシー] のデフォルト設定では、静的ウェブサイトに HTTPS を使用できます。これらの設定オプションの詳細については、Amazon CloudFront 開発者ガイドの「ウェブディストリビューションを作成または更新する場合に指定する値」を参照してください。
5. [Distribution Settings (ディストリビューションの設定)] で、以下の作業を行います。

   a. [Price Class (価格クラス)] は [Use All Edge Locations (Best Performance) (すべてのエッジロケーションを使用する (最適なパフォーマンス))] に設定されたままにしておきます。

   b. [代替ドメイン名 (CNAME)] をルートドメインと `www` サブドメインに設定します。このチュートリアルでは、`example.com` と `www.example.com` です。

   > **Important**
   >
   > このステップを実行する前に、代替ドメイン名を使用するための要件、特に有効な SSL/TLS 証明書の必要性について確認します。

   c. [SSL 証明書] で、[Custom SSL Certificate (example.com) (独自 SSL 証明書 (example.com))] を選択し、ドメイン名とサブドメイン名を対象とするカスタム証明書を選択します。

詳細については、Amazon CloudFront 開発者ガイドの「SSL 証明書」を参照してください。

d. [Default Root Object (デフォルトのルートオブジェクト)] に、インデックスドキュメントの名前を入力します (例: `index.html`)。

ディストリビューションにアクセスするために使用される URL にファイル名が含まれていない場合、CloudFront ディストリビューションはインデックスドキュメントを返します。[Default Root Object (デフォルトのルートオブジェクト)] は、静的ウェブサイトのインデックスドキュメントの名前と正確に一致する必要があります。詳細については、「インデックスドキュメントの設定」を参照してください。

e. [ログ記録] を [On (オン)] に設定します。

> **Important**
>
> ディストリビューションを作成または更新して CloudFront のログを有効にすると、CloudFront はバケットのアクセスコントロールリスト (ACL) を更新して、バケットにログを書き込む `awslogsdelivery` アクセス許可を `FULL_CONTROL` アカウントに付与します。詳細については、「Amazon CloudFront デベロッパーガイド」の「標準ログ記録の設定とログファイルへのアクセスに必要なアクセス許可」を参照してください。ログを保存するバケットが S3 オブジェクト所有権のバケット所有者の強制設定を使用して ACL を無効にすると、CloudFront はバケットにログを書き込むことができません。詳細については、「オブジェクトの所有権の制御とバケットの ACL の無効化。」を参照してください。

f. [Bucket for Logs (ログ用のバケット)] で、作成したログ記録バケットを選択します。

ログ記録バケットの設定の詳細については、「(オプション) ウェブトラフィックのログ記録」を参照してください。

g. CloudFront ディストリビューションへのトラフィックによって生成されたログをフォルダに保存する場合は、[Log Prefix (ログのプレフィックス)] にフォルダ名を入力します。

h. 他の設定はすべてデフォルト値のままにしておきます。

6. [Create Distribution] を選択します。

7. ディストリビューションのステータスを表示するには、コンソールでディストリビューションを見つけて、[ステータス] 列を確認します。

[InProgress] のステータスは、ディストリビューションがまだ完全にデプロイされていないことを示します。

ディストリビューションがデプロイされたら、新しい CloudFront ドメイン名でコンテンツを参照できます。

8. CloudFront コンソールに表示される [Domain Name (ドメイン名)] の値を書き留めます (例: `dj4p1rv6mvubz.cloudfront.net`)。
9. CloudFront ディストリビューションが正常に動作していることを確認するには、ウェブブラウザでディストリビューションのドメイン名を入力します。

   ウェブサイトが表示されている場合、CloudFront ディストリビューションは機能します。ウェブサイトに Amazon Route 53 で登録されたカスタムドメインがある場合は、次のステップでレコードセットを更新するために CloudFront ドメイン名が必要になります。

ステップ 2: ドメインとサブドメインのレコードセットを更新する

CloudFront ディストリビューションが正常に作成されたので、Route 53 でエイリアスレコードを更新して、新しい CloudFront ディストリビューションを指すようにします。

CloudFront ディストリビューションを指すようにエイリアスレコードを更新するには

1. Route 53 コンソール (https://console.aws.amazon.com/route53/) を開きます。
2. 左のナビゲーションで、[Hosted zones] (ホストゾーン) を選択します。
3. [Hosted Zones] (ホストゾーン) ページで、サブドメイン用に作成したホストゾーンを選択します (例: `www.example.com`)。
4. [Records] (レコード) で、サブドメイン用に作成した A レコードを選択します。
5. [Record details] (レコードの詳細) で、[Edit record] (レコードを編集) を選択します。
6. [Route traffic to] (トラフィックのルーティング先) で、[Alias to CloudFront distribution] (CloudFront ディストリビューションへのエイリアス) を選択します。
7. [Choose distribution] (ディストリビューションを選択) で、CloudFront ディストリビューションを選択します。
8. [Save] を選択します。
9. ルートドメインの A レコードを CloudFront ディストリビューションにリダイレクトするには、ルートドメイン用のこの手順を繰り返します (例: `example.com`)。

   レコードセットの更新は、2 ~ 48 時間以内に有効になります。

10. 新しい A レコードが有効かどうかを確認するには、ウェブブラウザで、サブドメイン URL を入力します (例: `http://www.example.com`)。

    ブラウザがルートドメイン (例: `http://example.com`) にリダイレクトしなくなった場合、新しい A レコードが有効になっています。新しい A レコードが有効になると、新しい A レコードによって CloudFront ディストリビューションにルーティングされるトラフィックが、ルートドメインにリダイレクトされなくなります。`http://example.com` または`http://www.example.com` を使用してサイトを参照する閲覧者は、最も近い CloudFront エッジロケーションにリダイレクトされるため、ダウンロード時間が短縮されます。

    > **Tip**
    >
    > ブラウザはリダイレクト設定をキャッシュできます。新しい A レコードの設定が有効になったと考えられるにもかかわらず、ブラウザによって`http://www.example.com` がまだ `http://example.com` にリダイレクトされる場合は、ブラウザアプリケーションを閉じてから再び開いてブラウザの履歴とキャッシュをクリアするか、異なるウェブブラウザを使用してみてください。

(オプション) ステップ 3: ログファイルを確認する

アクセスログにより、ウェブサイトを訪れたユーザーの数がわかります。また、Amazon EMR など他のサービスで分析できる貴重なビジネスデータも含まれています。

CloudFront ログは、CloudFront ディストリビューションを作成してログを有効にするときに選択したバケットとフォルダに保存されます。CloudFront は、対応するリクエストが行われると、24 時間以内にログバケットにログを書き込みます。

ウェブサイトのログファイルを表示するには

1. https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開きます。
2. ウェブサイトのログ記録バケットを選択します。
3. CloudFront ログフォルダを選択します。
4. CloudFront によって書き込まれた `.gzip` ファイルを開く前に、まずファイルをダウンロードします。

学習のためだけにウェブサイトを作成した場合は、割り当てたリソースを削除して、課金を停止できます。これを行うには、「サンプルリソースのクリーンアップ」を参照してください。AWS リソースを削除すると、ウェブサイトは使用できなくなります。

サンプルリソースのクリーンアップ

学習のために静的ウェブサイトを作成した場合は、割り当てた AWS リソースをここで削除して、課金を停止します。AWS リソースを削除すると、ウェブサイトは使用できなくなります。

タスク

- ステップ 1: Amazon CloudFront ディストリビューションを削除する
- ステップ 2: Route 53 ホストゾーンを削除する
- ステップ 3: ログ記録を無効にし、S3 バケットを削除する

ステップ 1: Amazon CloudFront ディストリビューションを削除する

Amazon CloudFront ディストリビューションを削除する前に、そのディストリビューションを無効にする必要があります。無効になったディストリビューションは機能しなくなり、料金も発生しません。無効にしたディストリビューションはいつでも有効にすることができます。無効にしたディストリビューションを削除すると、使用できなくなります。

CloudFront ディストリビューションを無効にして削除するには

1. で CloudFront コンソールを開きますhttps://console.aws.amazon.com/cloudfront/v4/home
2. 無効にするディストリビューションを選択してから [Disable (無効化)] を選択します。
3. 確認を求められたら、[Yes, Disable (はい、無効化する)] を選択します。
4. 無効にしたディストリビューションを選択してから [削除] を選択します。
5. 確認を求めるメッセージが表示されたら、[Yes, Delete (はい、削除します)] を選択します。

ステップ 2: Route 53 ホストゾーンを削除する

ホストゾーンを削除する前に、作成したレコードセットを削除する必要があります。NS レコードと SOA レコードを削除する必要はありません。これらはホストゾーンが削除されるときに自動的に削除されます。

レコードセットを削除するには

1. Route 53 コンソール (https://console.aws.amazon.com/route53/) を開きます。
2. ドメイン名のリストでドメイン名を選択し、[Go to Record Sets (レコードセットに移動)] を選択します。
3. レコードセットのリストで、作成した A レコードを選択します。

   各レコードセットのタイプは [タイプ] 列に表示されます。
4. [Delete Record Set (レコードセットの削除)] を選択します。
5. 確認を求められたら、[確認] を選択します。

Route 53 ホストゾーンを削除するには

1. 前のステップを終了した画面で [Back to Hosted Zones (ホストゾーンに戻る)] を選択します。
2. ドメイン名を選択してから [Delete Hosted Zone (ホストゾーンの削除)] を選択します。
3. 確認を求められたら、[確認] を選択します。

ステップ 3: ログ記録を無効にし、S3 バケットを削除する

S3 バケットを削除する前に、バケットのログ記録が無効であることを確認します。それ以外の場合、削除するバケットへのログの書き込みが AWS によって継続されます。

バケットのログ記録を無効にするには

1. https://console.aws.amazon.com/s3/ で Amazon S3 コンソールを開きます。
2. [バケット] でバケット名を選択し、[プロパティ] を選択します。
3. [プロパティ] から [ログ記録] を選択します。
4. [有効] チェックボックスをオフにします。
5. [Save] を選択します。

これで、バケットを削除できます。詳細については、「汎用バケットの削除」を参照してください。

S3 汎用バケットから AWS Amplify ホスティングへの静的ウェブサイトのデプロイ

AWS Amplify ホスティングを使用して、S3 に保存されている静的ウェブサイトのコンテンツをホストすることをお勧めします。Amplify ホスティングは、Amazon CloudFront を利用したグローバルに利用可能なコンテンツ配信ネットワーク (CDN) にウェブサイトを簡単にデプロイできるフルマネージドサービスです。これにより、大規模なセットアップなしで安全な静的ウェブサイトホスティングが可能になります。AWS Amplify ホスティングを使用すると、汎用バケット内のオブジェクトの場所を選択して、コンテンツをマネージド CDN にデプロイし、ウェブサイトのパブリック HTTPS URL を生成してどこからでもアクセス可能にすることができます。Amplify ホスティングを使用して静的ウェブサイトをデプロイすると、以下の利点と機能が得られます。

- Amazon CloudFront を利用した AWS コンテンツ配信ネットワーク (CDN) へのデプロイ - CloudFront は、ユーザーへの静的および動的ウェブコンテンツの配信を高速化するウェブサービスです。CloudFront では、エッジロケーションというデータセンターの世界的ネットワークを経由してコンテンツを配信します。CloudFront で提供しているコンテンツをユーザーがリクエストすると、リクエストはレイテンシー (遅延時間) が最小のエッジロケーションにルーティングされるため、コンテンツの配信が可能な限り最高のパフォーマンスとなり、信頼性と可用性が高まります。詳細については、「Amazon CloudFront デベロッパーガイド」の「CloudFront がコンテンツを配信する方法」を参照してください。
- HTTPS サポート - ウェブサイトとユーザーのウェブブラウザとの間で安全な通信とデータ転送を提供します。
- カスタムドメイン - Amazon Route 53 などのドメインレジストラから購入したカスタム URL にウェブサイトを簡単に接続します。
- カスタム SSL 証明書 - カスタムドメインを設定するときに、Amplify が自動でプロビジョニングするデフォルトのマネージド証明書を使用することも、選択したサードパーティの認証機関から購入した独自のカスタム証明書を使用することもできます。
- 組み込みメトリクスと CloudWatch モニタリング - ウェブサイトのトラフィック、エラー、データ転送、レイテンシーをモニタリングします。
- パスワード保護 - Amplify コンソールでユーザー名とパスワードの要件を設定することで、ウェブサイトへのアクセスを制限します。
- リダイレクトと書き換え - Amplify コンソールでリダイレクトと書き換えのルールを作成し、特定の URL から別の URL へのナビゲーションをウェブサーバーで再ルーティングできるようにします。

Amazon S3 汎用バケットから Amplify ホスティングにアプリケーションをデプロイする場合、AWS 料金は Amplify の料金モデルが基準となります。詳細については、AWS Amplify 料金を参照してください。

> **Important**
>
> Amplify ホスティングは、Amazon S3 が利用可能なすべての AWS リージョンで利用できるわけではありません。静的ウェブサイトを Amplify ホスティングにデプロイするには、ユーザーのウェブサイトを有する Amazon S3 汎用バケットが Amplify が利用可能なリージョンにある必要があります。Amplify が利用可能なリージョンのリストについては、「Amazon Web Services 全般のリファレンス」の「Amplify endpoints」を参照してください。

デプロイプロセスは、Amazon S3 コンソール、Amplify コンソール、AWS CLI、または AWS SDK から開始できます。独自のアカウントにある汎用バケットからのみ Amplify にデプロイできます。Amplify はクロスアカウントバケットアクセスをサポートしていません。

次の手順に従って Amazon S3 コンソールから開始し、Amazon S3 汎用バケットから Amplify ホスティングに静的ウェブサイトをデプロイします。

S3 コンソールから Amplify への静的ウェブサイトのデプロイ

Amazon S3 コンソールから静的ウェブサイトをデプロイするには

1. AWS Management Console にサインインし、Amazon S3 コンソール (https://console.aws.amazon.com/s3/) を開きます。
2. 左側のナビゲーションペインで、[バケット] を選択します。
3. [バケット] リストで、Amplify ホスティングにデプロイするウェブサイトが含まれている汎用バケットを選択します。
4. [プロパティ] タブを選択します。
5. [静的ウェブサイトホスティング] で、[Amplify アプリを作成] を選択します。このステップで、デプロイプロセスは Amplify コンソールに移動します。
6. [S3 によるデプロイ] ページで、次のいずれかのステップを実行します。
   a. [アプリ名] に、アプリまたはウェブサイトの名前を入力します。
   b. [ブランチ名] に、アプリのバックエンドの名前を入力します。

c. [ホストするオブジェクトの S3 の場所] で、汎用バケットへのディレクトリパスを入力するか、[S3 を参照] を選択して検索および選択します。

7. [保存してデプロイ] を選択します。

> **Note**
>
> Amplify でホストされている汎用バケットで静的ウェブサイトのいずれかのオブジェクトを更新した場合は、変更を有効にするためにアプリケーションを Amplify ホスティングに再デプロイする必要があります。Amplify ホスティングは、バケットへの変更を自動的には検出しません。詳細については、「AWS Amplify Hosting User Guide」の「Updating a static website deployed to Amplify from an S3 bucket」を参照してください。

Amplify コンソールから直接開始するには、「AWS Amplify ホスティングユーザーガイド」の「Amplify コンソールを使用して S3 から静的ウェブサイトをデプロイする」を参照してください。

AWS SDK を使用して開始するには、「AWS Amplify ホスティングユーザーガイド」の「AWS SDK を使用して S3 から静的ウェブサイトをデプロイするためのバケットポリシーの作成」を参照してください。

クォータ

AWS アカウント には、AWS のサービスごとにデフォルトのクォータ (以前は制限と呼ばれていました) があります。Amazon S3 クォータには、汎用バケット、ディレクトリバケット、アクセスポイントの数などが含まれます。一部のクォータについては引き上げをリクエストできますが、すべてのクォータについて引き上げ可能ではありません。引き上げはすぐには許可されないので、引き上げが有効になるまでに 2 ~ 3 日かかる場合があります。

Amazon S3 クォータとそのデフォルト値のリストについては、「AWS 全般のリファレンス」の「Amazon S3 quotas」を参照してください。

クォータの引き上げ

クォータの引き上げをリクエストするには

クォータの引き上げは、次のいずれかのオプションを使用してリクエストできます。

- AWS Management Console で、Service Quotas コンソールを開きます。ナビゲーションペインで、[AWS のサービス] を選択します。[Amazon S3] を選択し、クォータを選択してから、指示に従ってクォータの引き上げをリクエストします。詳細については、Service Quotas ユーザーガイドのクォータの引き上げのリクエストを参照してください。
- AWS CLI の場合: request-service-quota-increase AWS CLI コマンドを使用します。詳細については、Service Quotas ユーザーガイドのクォータの引き上げのリクエストを参照してください。

リファレンス

Amazon S3 コンソールに加えて、Amazon S3 REST API、AWS SDK、または AWS Command Line Interface (AWS CLI) を使用してプログラムで Amazon S3 を操作することができます。

- Amazon Simple Storage Service API リファレンス
- 「Amazon Simple Storage Service API リファレンス」の「Code examples」
- 「AWS Command Line Interface ユーザーガイド」の「AWS Command Line Interface」
- AWS SDK

SDK ドキュメント	コードの例
AWS SDK for C++	AWS SDK for C++ コードの例
AWS CLI	AWS CLI のコード例
AWS SDK for Go	AWS SDK for Go コードの例
AWS SDK for Java	AWS SDK for Java コードの例
AWS SDK for JavaScript	AWS SDK for JavaScript コードの例
AWS SDK for Kotlin	AWS SDK for Kotlin コードの例
AWS SDK for .NET	AWS SDK for .NET コードの例
AWS SDK for PHP	AWS SDK for PHP コードの例
AWS Tools for PowerShell	Tools for PowerShell のコード例
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) コードの例
AWS SDK for Ruby	AWS SDK for Ruby コードの例
AWS SDK for Rust	AWS SDK for Rust コードの例
AWS SDK for SAP ABAP	AWS SDK for SAP ABAP コードの例
AWS SDK for Swift	AWS SDK for Swift コードの例

ドキュメント履歴

- 現行 API バージョン: 2006-03-01

次の表に、Amazon Simple Storage Service API リファレンスおよび Amazon S3 ユーザーガイドの各リリースにおける重要な変更点が記されています。このドキュメントの更新に関する通知については、RSS フィードにサブスクライブできます。

変更	説明	日付
S3 Tables は、カスタマーマネージドキーを使用した SSE-KMS をサポートするようになりました。	S3 Tables は、カスタマーマネージドキーを使用した AWS Key Management Service (AWS KMS) キーによるサーバー側の暗号化 (SSE-KMS) をサポートするようになりました。SSE-KMS 暗号化は、テーブルバケットおよびテーブルレベルで適用できます。詳細については、「Using server-side encryption with AWS KMS keys (SSE-KMS) in table buckets」を参照してください。	2025 年 4 月 16 日
ディレクトリバケットのアクセスポイントが AWS ローカルゾーンで利用可能	ディレクトリバケットは、Amazon S3 の共有データセットにおける大規模なデータアクセス管理を簡素化するため、アクセスポイントのサポートするようになりました。この新しい機能により、バケットごとに数百のアクセスポイントを作成できます。各アクセスポイントには、アプリケーションごとにカスタ	2025 年 3 月 31 日

マイズされた個別の名前とアクセス許可があります。詳細については、「アクセスポイントを使用したディレクトリバケットの共有データセットへのアクセスの管理」を参照してください。

Amazon SageMaker Lakehouse との S3 テーブルバケット統合の一般提供を開始	S3 テーブルバケットを Amazon SageMaker Lakehouse と統合して、Amazon Athena、Amazon Redshift、QuickSight などの AWS 分析サービスからテーブルにアクセスできます。Amazon SageMaker Lakehouse は、Amazon S3 データレイクと Amazon Redshift データウェアハウス全体のデータを統合するため、データの 1 つのコピーに対して分析、機械学習 (ML)、生成 AI アプリケーションを構築できます。この統合により、AWS Glue Data Catalog にテーブルリソースが入力され、AWS Lake Formation でこれらのリソースへのアクセスがフェデレーションされます。この統合により、Lake Formation を通じたきめ細かなアクセスコントロールが可能になり、セキュリティが向上します。統合に関する詳細については、「AWS 分析サービスで Amazon S3 Tables を使用する」を参照してください。プレビューリリースで統合を設定した場合は、現在の統合を引き続き使用できます。ただし、更新された統合プロセスではパフォーマンスが向上しているため、移行することをお勧めします。更新	2025 年 3 月 13 日

	された統合に移行するには、「更新された統合プロセスへの移行」を参照してください。	
S3 Tables テーブルの作成とクエリテーブルのサポートが Amazon S3 コンソールに追加	S3 Tables は、Amazon Athena を使用して Amazon S3 コンソールから直接テーブルの作成とテーブルオペレーションのクエリをサポートするようになりました。この新しい機能を使用すると、Amazon S3 コンソールで、わずか数ステップでテーブルを作成し、データを入力して、クエリを実行できるようになりました。詳細については、「Amazon S3 テーブルの作成」および「Athena を使用した Amazon S3 テーブルのクエリ」を参照してください。	2025 年 3 月 13 日
S3 Tables に、テーブルの作成時にスキーマを追加するためのサポートを追加	オプションのメタデータフラグを追加することで、S3 Tables `CreateTable` API オペレーションを使用してスキーマを含むテーブルを作成できるようになりました。詳細については、「テーブルの作成」を参照してください。	2025 年 1 月 30 日

S3 Tables に、テーブルの作成時にスキーマを追加するためのサポートを追加	オプションのメタデータフラグを追加することで、S3 Tables `CreateTable` API オペレーションを使用してスキーマを含むテーブルを作成できるようになりました。詳細については、「テーブルの作成」を参照してください。	2025 年 1 月 30 日
Amazon S3 メタデータの一般提供を開始	Amazon S3 メタデータが一般提供されました。S3 メタデータは、ほぼリアルタイムで更新される自動クエリ可能なメタデータを使用して、S3 データを簡単に検出して理解するのに役立ちます。S3 メタデータを使用すると、ビジネス分析、人工知能と機械学習 (AI/ML) モデルトレーニングなどに S3 データをキュレート、識別、使用できます。S3 メタデータは、オブジェクトのサイズやソースなどのシステム定義の情報を含むオブジェクトメタデータと、製品 SKU、トランザクション ID、コンテンツ評価などの情報を含むタグなどのカスタムメタデータをサポートします。詳細については、「Accelerating data discovery with S3 Metadata」を参照してください。	2025 年 1 月 27 日
AWS マネージドポリシー – 新しいポリシー	S3 Tables に 2 つの新しい AWS マネージドポリシーが追加されました。	2024 年 12 月 6 日

S3 Tables	Amazon S3 Tables は、分析ワークロード用に最適化された S3 ストレージを提供します。また、クエリのパフォーマンスを向上させ、テーブルのストレージコストを削減し、大規模なデータレイクの運用を簡素化する機能を備えています。S3 Tables では、Apache Iceberg テーブルをサブリソースとして保存するために特別に設計されたテーブルバケットという新しいバケットタイプが導入されています。テーブルバケットは、S3 汎用バケットのセルフマネージドテーブルと比較して、1 秒あたりのトランザクション (TPS) が高く、クエリスループットが向上します。テーブルバケットは、Athena、Amazon Redshift、QuickSight などの AWS 分析サービスと自動的に統合できます。詳細については、「Working with Amazon S3 Tables and table buckets」を参照してください。	2024 年 12 月 3 日

S3 メタデータプレビュー	Amazon S3 メタデータは、ほぼリアルタイムで更新される自動クエリ可能なメタデータを使用して、S3 データを簡単に検出して理解するのに役立ちます。S3 メタデータを使用すると、ビジネス分析、人工知能と機械学習 (AI/ML) モデルトレーニングなどに S3 データをキュレート、識別、使用できます。S3 メタデータは、オブジェクトのサイズやソースなどのシステム定義の情報を含むオブジェクトメタデータと、製品 SKU、トランザクション ID、コンテンツ評価などの情報を含むタグなどのカスタムメタデータをサポートします。詳細については、「Accelerating data discovery with S3 Metadata」を参照してください。	2024 年 12 月 3 日
Storage Browser for S3	Storage Browser for S3 は、ウェブアプリケーションに追加して、S3 に保存されているデータのシンプルなインターフェイスをエンドユーザーに提供できるオープンソースコンポーネントです。詳細については、「Storage Browser for S3」を参照してください。	2024 年 12 月 1 日

新しい Amazon S3 チェックサムアルゴリズムと改善されたチェックサムの整合性機能	Amazon S3 では、CRC-64NVME チェックサムアルゴリズムと改善されたチェックサム整合性機能が追加されました。詳細については、「オブジェクトの整合性をチェックする」を参照してください。	2024 年 12 月 1 日
データレジデンシーワークロード	Dedicated Local Zones では、データレジデンシーと分離のユースケースのデータを保存するための S3 ディレクトリバケットを作成できます。詳細については、「Data residency workloads」を参照してください。	2024 年 12 月 1 日
条件付き書き込みを強制する新しい条件キー	Amazon S3 は、バケットポリシーで使用する新しい条件キー s3:if-match と s3:if-none-match を追加して、クライアントに If-None-Match または If-Match HTTP ヘッダーの使用を強制します。詳細については、「Enforce conditional writes on Amazon S3 buckets」を参照してください。	2024 年 11 月 25 日

オブジェクトが変更されたかどうかを確認するための条件付き書き込み用の新しい HTTP ヘッダー	Amazon S3 は、一部の API オペレーションでオブジェクトを書き込む前に、オブジェクトのエンティティタグ (ETag) をチェックする HTTP `If-Match` ヘッダーを追加します。このヘッダーを使用すると、Amazon S3 は指定された ETag 値と S3 内のオブジェクトの ETag 値を比較します。ETag 値が一致しない場合、オペレーションは失敗となります。詳細については、「条件付き書き込みによるオブジェクトの上書きを防ぐ方法」を参照してください。	2024 年 11 月 25 日
Amazon Redshift が S3 Access Grants と統合	Amazon Redshift のお客様は、S3 Access Grants を使用して S3 データのアクセス許可をスケールおよび管理できるようになりました。これにより、Amazon Redshift のお客様は、IAM ユーザーやグループの S3 アクセス許可をスケールするとともに、AWS IAM Identity Center を使用して企業 ID の S3 アクセス許可をスケールできます。詳細については、「Amazon Redshift と Amazon S3 Access Grants の統合」を参照してください。	2024 年 11 月 15 日

AWS Organizations メンバーアカウントで、誤ってロックされた Amazon S3 バケットへのアクセスが回復可能に	AWS Organizations メンバーアカウントは、AWS Identity and Access Management (IAM) を介した簡単なプロセスを使用して、誤ってロックされた Amazon S3 バケットへのアクセスを回復できるようになりました。詳細については、「AWS Identity and Access Management ユーザーガイド」の「AWS Organizations メンバーアカウントで特権タスクを実行する」を参照してください	2024 年 11 月 14 日
AWS Organizations の新しいタイプの認可ポリシーであるリソースコントロールポリシー (RCP) が Amazon S3 バケットでも利用可能に	AWS Organizations で管理する新しい認可ポリシーであるリソースコントロールポリシー (RCP) を使用して、組織全体の Amazon S3 バケットで利用可能な最大数のアクセス許可を設定できます。詳細については、「AWS Organizations ユーザーガイド」の「リソースコントロールポリシー (RCP)」を参照してください。	2024 年 11 月 13 日
Amazon S3 は、バケットクォータの増加を最大 1,000 バケットまで自動的に承認	Amazon S3 は、バケットクォータの増加を最大 1,000 バケットまで自動的に承認するようになりました。バケットの使用率を確認したり、増加をリクエストしたりするには、Service Quotas コンソールにアクセスしてください。	2024 年 9 月 30 日

Amazon S3 ライフサイクル設定の新しいデフォルトの最小オブジェクトサイズ移行動作	Amazon S3 は、128 KB 未満のオブジェクトが任意のストレージクラスに移行されないように、S3 ライフサイクル設定にデフォルトの動作を適用するようになりました。この動作を上書きする方法については、「128 KB 未満のオブジェクトの移行を許可する」を参照してください。	2024 年 9 月 24 日
ディレクトリバケットは、カスタマーマネージドキーを使用した SSE-KMS をサポートするようになりました。	ディレクトリバケットは、カスタマーマネージドキーを使用した AWS Key Management Service (AWS KMS) キーによるサーバー側の暗号化 (SSE-KMS) をサポートするようになりました。ディレクトリバケット内でデータを暗号化し、セキュリティを管理するためのオプションが増えました。詳細については、「Data protection and encryption in directory buckets」を参照してください。	2024 年 9 月 17 日

S3 Access Grants は、呼び出し元のアクセス許可を一覧表示する API アクションをサポート	IAM ID と IAM アイデンティティセンターの社内ディレクトリ ID は、`ListCallerAccessGrants` API を使用して、Amazon S3 S3 バケット、プレフィックス、およびオブジェクトを一覧表示できるようになりました。この API を使用して、IAM または企業ディレクトリ ID が S3 Access Grants を介してアクセスできるすべての S3 データを、特定の AWS アカウント内で検出します。詳細については、「呼び出し元のアクセス許可を一覧表示する」を参照してください。	2024 年 9 月 5 日

同じアカウントリクエストに対する拡張アクセス拒否メッセージ	Amazon S3 は、同じ AWS アカウント 内のリソースに対して行われたリクエストのアクセス拒否 (HTTP 403 Forbidden) エラーに追加コンテキストを含めるようになりました。この新しいコンテキストには、アクセスを拒否したポリシーのタイプ、拒否の理由、リソースへのアクセスをリクエストした AWS Identity and Access Management (IAM) ユーザーまたはロールに関する情報が含まれます。このコンテキストは、アクセス問題のトラブルシューティング、アクセス拒否エラーの根本原因の特定、関連するポリシーの更新による誤ったアクセスコントロールの修正に役立ちます。この追加のコンテキストは、AWS CloudTrail ログでも使用できます。AWS GovCloud (US) Regions および中国リージョンを含むすべての AWS リージョン で、同じアカウントリクエストに対する拡張アクセス拒否エラーメッセージが利用可能になりました。詳細については、「Amazon S3 でのアクセス拒否 (403 Forbidden) エラーのトラブルシューティング」を参照してください。	2024 年 8 月 21 日

Amazon S3 が PutObject および CompleteMultipartUpload の条件付き書き込みの使用をサポート	アップロード時の条件付き書き込みオペレーションを使用して、バケット内にオブジェクトが存在するかどうかを確認してからオブジェクトを作成できるようになりました。これにより、既存のデータの上書きを阻止できます。条件付き書き込みでは、バケット内に同じキー名を持つ既存のオブジェクトが存在しないことを検証します。詳細については、「条件付きリクエスト」を参照してください。	2024 年 8 月 20 日
Amazon S3 は、いくつかの HTTP エラーコードを課金対象から除外	Amazon S3 は、お客様が開始していない不正なリクエストに課金しないための変更を完了しました。詳細については、「Amazon S3 のエラーレスポンスに対する請求」を参照してください。	2024 年 8 月 19 日
新規のお客様への Amazon S3 Select の提供が終了	新規のお客様への Amazon S3 Select の提供は終了しました。Amazon S3 Select をご利用の既存のお客様は、今後も通常どおり使用できます。詳細はこちら。	2024 年 7 月 25 日

Amazon S3 インベントリが s3:InventoryAccessibleOptionalFields 条件キーをサポート	Amazon S3 インベントリは s3:InventoryAccessibleOptionalFields 条件キーをサポートしており、ユーザーがレポートにオプションのメタデータフィールドを含めることができるかどうかを制御します。詳細については、「S3 インベントリレポート設定の作成を制御する」を参照してください。	2024 年 2 月 20 日
S3 on Outposts の IPv6 サポート	S3 on Outposts デュアルスタックエンドポイント経由で IPv6 を使用して、S3 on Outposts バケットにアクセスできるようになりました。S3 on Outposts での IPv6 サポートにより、S3 on Outposts バケットとコントロールプレーンリソースを IPv6 ネットワーク経由で管理できます。	2024 年 1 月 16 日
新しい高パフォーマンスのシングルゾーン Amazon S3 ストレージクラス – S3 Express One Zone	Amazon S3 Express One Zone は、最もレイテンシーの影響を受けやすいアプリケーションに 1 桁のミリ秒単位で一貫したデータアクセスを提供することを目的として構築された、高パフォーマンスのシングルアベイラビリティーゾーンの Amazon S3 ストレージ クラスです。詳細については、「S3 Express One Zone」を参照してください。	2023 年 11 月 28 日

Mountpoint for Amazon S3 での S3 Express One Zone のサポートの追加	S3 Express One Zone のディレクトリバケットを Mountpoint を使用してマウントできるようになりました。	2023年11月28日
Lambda 呼び出しスキーマのバージョン	Amazon S3 バッチオペレーションでは、ディレクトリバケットで動作するバッチオペレーションジョブで使用するための新しい Lambda 呼び出しスキーマバージョンが導入されました。詳細については、「ディレクトリバケットでの Lambda と Amazon S3 のバッチオペレーションの使用」を参照してください。	2023年11月28日
ディレクトリバケットのインポートアクション	Amazon S3 でインポートアクションが提供されるようになりました。インポートは、オブジェクトを汎用バケットからディレクトリバケットにコピーする Amazon S3 バッチオペレーションジョブを作成するための効率的な方法です。詳細については、「ディレクトリバケットへのオブジェクトのインポート」を参照してください。	2023年11月28日

S3 Access Grants で S3 アクセスを管理する	Amazon S3 Access Grants を使用すると、AWS Identity and Access Management (IAM) プリンシパルのデータアクセス許可を大規模に管理できます。また、Azure AD などの企業ディレクトリからのディレクトリアイデンティティも管理できます。最小権限の S3 アクセス権限を強制し、ビジネスニーズに基づいてそれらのアクセス権限を簡単にスケーリングできるようになりました。詳細については、「S3 Access Grants でのアクセス管理」を参照してください。	2023 年 11 月 26 日
Mountpoint for Amazon S3 バッチオペレーション	Mountpoint で、繰り返しアクセスするデータのキャッシュを設定できるようになりました。	2023年11月22日

Amazon S3 バッチオペレーションのマニフェスト生成の拡張	ジョブを作成する際に指定するオブジェクトフィルタ条件に基づいたマニフェストの自動生成を Amazon S3 Batch オペレーションに指示できるようになりました。このオプションは、Amazon S3 コンソールで作成したバッチレプリケーションジョブ、または AWS CLI、AWS、Amazon S3 REST API を使用して作成した任意のジョブタイプで使用できます。詳細については、「Amazon S3 バッチオペレーションジョブの作成」を参照してください。	2023年11月22日
既存の Amazon S3 バケットでの Object Lock 設定の追加	既存の Amazon S3 バケットで Object Lock を有効にできるようになりました。新規または既存のバケットにリーガルホールドと保持期間を設定できます。詳細については、「オブジェクトロックの使用」を参照してください。	2023年11月20日
プレフィックスの S3 Storage Lens リクエストメトリクス	S3 Storage Lens は、Amazon S3 バケット内のプレフィックスに対してリクエストメトリクスを導入しています。詳細については、「メトリクスカテゴリ」を参照してください。	2023 年 11 月 17 日

Amazon S3 ストレージレンズグループ	S3 Storage Lens には、オブジェクトメタデータに基づいてオブジェクト用のカスタム定義フィルタである Storage Lens グループが導入されています。詳細については、「Amazon S3 ストレージレンズグループの使用」を参照してください。	2023 年 11 月 15 日
新しい IAM ポリシー	S3 on Outposts では、ネットワークリソースの管理に役立つ、サービスにリンクされたロール `AWSServiceRoleForS3OnOutposts` が導入されました。詳細については、「S3 on Outposts でのサービスにリンクされたロールの使用」を参照してください。	2023 年 10 月 3 日
Amazon S3 は、削除マーカーの `Last-Modified` 時間を提供します。	Amazon S3 は、S3 `Head` オペレーションと `Get` API オペレーションのレスポンスヘッダーに、削除マーカーの `Last-Modified` 時間を提供します。詳細については、「削除マーカーの使用」を参照してください。	2023 年 9 月 27 日
AWS マネージドポリシーに対する Amazon S3 の最新情報	Amazon S3 が `s3:Describe*` 許可を `AmazonS3ReadOnlyAccess` に追加しました。詳細については、「Amazon S3 の AWS マネージドポリシー」を参照してください。	2023 年 8 月 11 日

S3 バッチオペレーションによる標準復元リクエストの開始時間が短縮されました	S3 バッチオペレーションによる復元リクエストの標準取得を数分で開始できるようになりました。詳細については、「アーカイブの取り出しオプション」を参照してください。	2023 年 8 月 9 日
Amazon S3 バケットをローカルファイルシステムとしてマウントするための、高スループットのオープンソースファイルクライアントである、Mountpoint を追加しました。	Mountpoint を使うと、アプリケーションはファイルオペレーションを通じて Amazon S3 に保存されているオブジェクトにアクセスできるため、アプリケーションはファイルインターフェイスを通じて Amazon S3 の伸縮自在なストレージとスループットにアクセスできます。	2023 年 8 月 9 日
AWS Key Management Service キーによる二層式サーバー側の暗号化 (DSSE-KMS)	AWS Key Management Service (AWS KMS) キーによる二層式サーバー側の暗号化 (DSSE-KMS) を使用すると、オブジェクトが Amazon S3 にアップロードされるときに 2 つの暗号化レイヤーが適用されます。詳細については、「AWS KMS キーによる二層式サーバー側の暗号化の使用」を参照してください。	2023 年 6 月 13 日

Amazon S3 は、すべての新しいバケットについて、S3 ブロックパブリックアクセスを有効にし、S3 アクセスコントロールリスト (ACL) を無効にします。	Amazon S3 は、すべての AWS リージョンのすべての新しい S3 バケットについて、S3 ブロックパブリックアクセスを自動的に有効にし、S3 アクセスコントロールリスト (ACL) を無効にするようになりました。詳細については、「Amazon S3 ストレージへのパブリックアクセスをブロックする」と「オブジェクトの所有権の制御とバケットの ACL の無効化」を参照してください。	2023 年 4 月 27 日
S3 レプリケーションオペレーション失敗メトリクス	Amazon S3 には、S3 レプリケーションの失敗をモニタリングするための新しい Amazon CloudWatch メトリクスが追加されています。詳細については、「レプリケーションメトリクスによる進捗状況のモニタリング」を参照してください。	2023 年 4 月 5 日
プライベート DNS	Amazon S3 の AWS PrivateLink がプライベート DNS をサポートするようになりました。詳細については、「プライベート DNS」を参照してください。	2023 年 3 月 14 日

Amazon S3 コンソールでのクロスアカウントアクセスポイントのサポート	Amazon S3 では、Amazon S3 コンソールによるクロスアカウントのアクセスポイントの作成がサポートされるようになりました。詳細については、「アクセスポイントの作成」を参照してください。	2023 年 3 月 14 日
Amazon S3 on Outposts は S3 Replication on Outposts をサポートします	ローカル S3 レプリケーションを使用すると、オブジェクトを単一の Outposts レプリケート先バケットまたは複数のレプリケート先バケットに自動的に複製できます。レプリケート先バケットは、異なる AWS Outposts でも、レプリケート元バケットと同じ Outposts 内でも配置することができます。詳細については、「S3 on Outposts のオブジェクトのレプリケート」を参照してください。	2023 年 3 月 14 日

Amazon S3 Object Lambda アクセスポイントのエイリアス	Object Lambda アクセスポイントを作成すると、Amazon S3 は Object Lambda アクセスポイントの固有のエイリアスを自動的に生成します。アクセスポイントのデータプレーンオペレーションのリクエストで、Amazon S3 バケット名や Object Lambda アクセスポイント Amazon Resource Name (ARN) の代わりに、このエイリアスを使用することができます。詳細については、「Amazon S3 Object Lambda アクセスポイントの使用」を参照してください。	2023 年 3 月 14 日
Amazon S3 マルチリージョンアクセスポイントのクロスアカウントサポート	Amazon S3 では、Amazon S3 コンソールによるクロスアカウントのマルチリージョンアクセスポイントの作成がサポートされるようになりました。詳細については、「マルチリージョンアクセスポイントの作成」を参照してください。	2023 年 3 月 14 日

クロスアカウントアクセスポイント	Amazon S3 は、クロスアカウントアクセスポイントの作成をサポートしています。AWS Command Line Interface (AWS CLI) または REST API `CreateAccessPoint` オペレーションを使用してクロスアカウントアクセスポイントを作成できます。詳細については、「アクセスポイントの作成」を参照してください。	2022 年 11 月 30 日
Amazon S3 で Amazon S3 マルチリージョンアクセスポイントのフェイルオーバーコントロールをサポート	Amazon S3 で、Amazon S3 マルチリージョンアクセスポイントのフェイルオーバーコントロールが導入されました。これらのコントロールにより、Amazon S3 マルチリージョンアクセスポイントを経由する S3 データアクセスリクエストトラフィックを数分以内に別の AWS リージョン に移行し、可用性の高いアプリケーションをテストおよび構築することができます。詳細については、「Amazon S3 Multi-Region Access Point failover controls」(Amazon S3 マルチリージョンアクセスポイントのフェイルオーバーコントロール) を参照してください。	2022 年 11 月 28 日

Amazon S3 ストレージレンズの 34 の新しいメトリクスで組織全体の可視性を向上	S3 ストレージレンズは、より深いコスト最適化の機会を発見し、データ保護のベストプラクティスを特定し、アプリケーションワークフローのパフォーマンスを向上させるための 34 の追加メトリクスを導入しました。詳細については、「S3 Storage Lens metrics」(S3 ストレージレンズメトリクス) を参照してください。	2022 年 11 月 17 日
Amazon S3 で、S3 Glacier Flexible Retrieval および S3 Glacier Deep Archive のより高い復元リクエストのレートをサポート	Amazon S3 は、S3 Glacier Flexible Retrieval および S3 Glacier Deep Archive ストレージクラスで、AWS アカウント ごとに、1 秒あたり最大 1,000 件のトランザクションの復元リクエストをサポートします。	2022 年 11 月 15 日

Amazon S3 on Outposts は、追加の S3 ライフサイクルアクションとフィルタをサポート	S3 on Outposts は、キャパシティ管理を最適化するための追加の S3 ライフサイクルルールをサポートしています。オブジェクトが古くなったり、新しいバージョンに置き換えられたりしたときに期限切れにすることができます。プレフィックス、オブジェクトタグ、オブジェクトサイズでフィルタリングすることで、バケット全体またはバケット内のオブジェクトのサブセットに対してライフサイクルルールを作成することができます。ライフサイクル設定の管理の詳細については、「Amazon S3 on Outposts バケットのライフサイクル設定を作成および管理する」を参照してください。	2022 年 11 月 2 日
SSE-C オブジェクトに対する S3 レプリケーションのサポート	カスタマー提供キーでサーバーサイド暗号化を使用して作成されたオブジェクトをレプリケートすることができます。暗号化されたオブジェクトのレプリケートについて詳しくは、「サーバー側の暗号化 (SSE-C、SSE-S3、SSE-KMS) で作成されたオブジェクトをレプリケートする」を参照してください。	2022 年 10 月 24 日

Amazon S3 on Outposts でアクセスポイントのエイリアスをサポート	S3 on Outposts では、Outposts バケット内の任意のオブジェクトにアクセスするにはアクセスポイントを使用する必要があります。バケットのアクセスポイントを作成するたびに、S3 on Outposts によってアクセスポイントのエイリアスが自動的に生成されます。このアクセスポイントエイリアスは、あらゆるデータプレーンオペレーションでアクセスポイント ARN の代わりに使用できます。詳細については、「Using a bucket-style alias for your S3 on Outposts bucket access point」(S3 on Outposts バケットアクセスポイントにバケット形式のエイリアスを使用する) を参照してください。	2022 年 10 月 21 日
S3 Object Lambda で `HeadObject` 、`ListObjects` 、および `ListObjectsV2` オペレーションをサポート	カスタムコードを使用して、標準の S3 `GET`、`LIST`、`HEAD` リクエストによって返されるデータを変更し、行のフィルタリング、画像の動的なサイズ変更、機密データの編集などを行うことができるようになりました。詳細については、「S3 Object Lambda を使用したオブジェクトの変換」を参照してください。	2022 年 10 月 4 日

Amazon S3 on Outposts で S3 バージョニングをサポート	S3 バージョニングを有効にすると、オブジェクトの複数の異なるコピーが同じバケット内に保存されます。S3 バージョニングを使用すると、Outposts バケットに保存されたあらゆるオブジェクトのあらゆるバージョンを保存、取得、復元できます。S3 バージョニングによって、意図しないユーザーアクションやアプリケーション障害から復旧できます。詳細については、「Managing S3 Versioning for your S3 on Outposts bucket」(S3 on Outposts バケットの S3 バージョニングの管理) を参照してください。	2022 年 9 月 21 日
Amazon S3 用 AWS Backup	AWS Backup は、Amazon S3 のデータを保護するための中央バックアップポリシーを定義するために使用できる、フルマネージド型のポリシーベースのサービスです。詳細については、「Amazon S3 用の AWS Backup の使用」を参照してください。	2022 年 2 月 18 日

S3 バッチレプリケーションを使用して既存のオブジェクトをレプリケートする	S3 バッチレプリケーションを使用すると、レプリケーション設定が実行される前に存在していたオブジェクトをレプリケートできます。既存のオブジェクトのレプリケートは、バッチオペレーションジョブを使用して行います。S3 バッチレプリケーションは、Amazon S3 バケット間で新しいオブジェクトを継続的かつ自動的にコピーするライブレプリケーションとは異なります。詳細については、「S3 バッチレプリケーションを使用した既存のオブジェクトをレプリケートする」を参照してください。	2022 年 2 月 8 日
S3 Glacier Flexible Retrieval の名前変更	Glacier ストレージクラスが S3 Glacier Flexible Retrieval に変更されました。この変更は API に影響を与えません。	2021 年 11 月 30 日

ACL を無効にする新しい S3 オブジェクトの所有権の設定	オブジェクト所有権のバケット所有者強制設定を適用すると、バケットとその中のオブジェクトの ACL を無効にして、バケット内のすべてのオブジェクトの所有権を取得できます。バケット所有者の強制設定により、Amazon S3 に保存されているデータのアクセス管理が簡単になります。詳細については、バケットのオブジェクト所有権のコントロールと ACL の無効化を参照してください。	2021 年 11 月 30 日
新しい S3 Intelligent-Tiering ストレージクラス	S3 Intelligent-Tiering のアーカイブインスタントアクセスは、S3 Intelligent-Tiering の下位にあるストレージクラスです。詳細については、「S3 Intelligent-Tiering の仕組み」を参照してください。	2021 年 11 月 30 日
新しい S3 Glacier Instant Retrieval ストレージクラス	S3 Glacier Instant Retrieval ストレージクラスに、オブジェクトを配置できるようになりました。このストレージクラスの詳細については、Amazon S3 ストレージクラス を参照してください。	2021 年 11 月 30 日

Amazon S3 用 AWS Backup プレビュー	AWS Backup は、Amazon S3 のデータを保護するための中央バックアップポリシーを定義するために使用できる、フルマネージド型のポリシーベースのサービスです。詳細については、「Amazon S3 用の AWS Backup の使用」を参照してください。	2021 年 11 月 30 日
Amazon S3 用 AWS Identity and Access Management Access Analyzer	IAM Access Analyzer は、IAM ポリシーの文法 および ベストプラクティス に対してポリシーチェックを行います。IAM Access Analyzer を使用したポリシーの検証の詳細については、IAM ユーザーガイドの IAM Access Analyzer のポリシーの検証を参照してください。	2021 年 11 月 30 日
新しいイベントタイプ	Amazon S3 イベント通知に追加されたイベントタイプ。Amazon S3 イベント通知を参照してください。	2021 年 11 月 29 日
バケットで Amazon EventBridge を有効にする	Amazon S3 バケットで EventBridge を有効にして Amazon EventBridge にイベントを送信できます。EventBridge を使用する を参照してください。	2021 年 11 月 29 日

新しい S3 ライフサイクルフィルタ	オブジェクトサイズに基づいてライフサイクルルールを作成したり、最新ではないオブジェクトバージョンをどれほど保持するかを指定したりできます。ライフサイクル設定についての詳細は、「S3 ライフサイクル設定の例」を参照してください。	2021 年 11 月 23 日
Amazon S3 ストレージレンズのメトリクスを Amazon CloudWatch にパブリッシュする	S3 Storage Lens の使用状況とアクティビティのメトリクスを Amazon CloudWatch に公開して、CloudWatch ダッシュボード で運用状態の統一ビューを作成できます。また、アラームやトリガーアクション、メトリクス計算、異常検出などの CloudWatch 機能を使用して、S3 Storage Lens メトリクスをモニタリングして対処することができます。さらに、 CloudWatch API により、サードパーティープロバイダーを含むアプリケーションが S3 Storage Lens メトリクスにアクセスできるようになります。詳細については、Cloudwatch の S3 Storage Lens メトリクスのモニタリング を参照してください。	2021 年 11 月 22 日

マルチリージョンアクセスポイント	マルチリージョンアクセスポイントを使用して、アプリケーションが複数の AWS リージョン にある Amazon S3 バケットからのリクエストを実行するために使用できるグローバルエンドポイントを作成できます。このマルチリージョンアクセスポイントを使用して、レイテンシーが最も低いバケットにデータをルーティングできます。マルチリージョンアクセスポイントの詳細と使用方法については、「Amazon S3 のマルチリージョンアクセスポイント」を参照してください。	2021 年 9 月 2 日

Amazon S3 on Outposts に追加されたアプリケーションのダイレクトローカルアクセス	AWS Outposts 仮想プライベートクラウド (VPC) の外でアプリケーションを実行し、S3 on Outposts のデータにアクセスすることができます。オンプレミスネットワークから直接 S3 on Outposts オブジェクトにアクセスすることもできます。お客様所有の IP (CoIP) アドレスを使用して S3 on Outposts のエンドポイントを構成し、オンプレミスネットワークからローカルゲートウェイを作成してオブジェクトにアクセスする方法については、VPC 専用のアクセスポイントを使用した Amazon S3 on Outposts へのアクセスに関する記事を参照してください。	2021 年 7 月 29 日
Amazon S3 アクセスポイントエイリアス	アクセスポイントを作成すると、Amazon S3 はデータアクセス用のバケット名の代わりに使用できるエイリアスを自動的に生成します。このアクセスポイントエイリアスは、あらゆるアクセスポイントのデータプレーンオペレーションにおいて、Amazon リソースネーム (ARN) の代わりに使用することができます。詳細については、「アクセスポイントにバケット形式のエイリアスを使用する」を参照してください。	2021 年 7 月 26 日

Amazon S3 インベントリと S3 バッチオペレーションでは、S3 バケットキーのステータスがサポートされています	Amazon S3 インベントリおよびバッチオペレーションでは、S3 バケットキーを使用した既存のオブジェクトの識別とコピーがサポートされています。S3 バケットキーは、既存のオブジェクトのサーバー側の暗号化コストの削減を加速します。詳細については、「Amazon S3 Inventory」および「バッチオペレーションによるオブジェクトのコピー」を参照してください。	2021 年 6 月 3 日
Amazon S3 ストレージレンズメトリクスアカウントのスナップショット	S3 Storage Lens アカウントのスナップショットは、デフォルトのダッシュボードからメトリクスを要約して、S3 コンソールホーム ([Buckets] (バケット)) ページに、ストレージ合計、オブジェクト数、および平均オブジェクトサイズを表示します。詳細については、S3 Storage Lens メトリクスアカウントのスナップショットを参照してください。	2021 年 5 月 5 日
強化された Amazon S3 on Outposts のエンドポイントサポート	S3 on Outposts では、Outposts ごとに最大 100 個のエンドポイントがサポートされるようになりました。詳細については、S3 on Outposts のネットワーク制限を参照してください。	2021 年 4 月 29 日

Amazon CloudWatch Events での Amazon S3 on Outposts イベント通知	CloudWatch Events を使用して、S3 on Outposts の API イベントをキャプチャし、サポートされているすべての CloudWatch ターゲットを通じて通知を受け取るためのルールを作成できます。詳細については、CloudWatch Events を使用した S3 on Outposts イベント通知の受信を参照してください。	2021 年 4 月 19 日
S3 Object Lambda	S3 Object Lambda を使用すると、Amazon S3 GET リクエストに独自のコードを追加して、データがアプリケーションに返されるときにそのデータを変更および処理できます。カスタムコードを使用すると、標準 S3 GET リクエストによって返されるデータを変更し、行のフィルタリング、画像の動的なサイズ変更、機密データの編集などを行うことができます。詳細については、「オブジェクトの変換」を参照してください。	2021 年 3 月 18 日

AWS PrivateLink	AWS PrivateLink for Amazon S3 を使用すると、インターネット経由で接続する代わりに、仮想プライベートクラウド (VPC) のインターフェイスエンドポイントを使用して S3 に直接接続できます。インターフェイスエンドポイントは、オンプレミスまたは別の AWS リージョン にあるアプリケーションから直接アクセスできます。詳細については、「AWS PrivateLinkAmazon S3」を参照してください。	2021 年 2 月 2 日
次を使用した Amazon S3 on Outposts キャパシティーの管理AWS CloudTrail	S3 on Outposts 管理イベントは、CloudTrail ログを通してご利用いただけます。詳細については、CloudTrail を使用した S3 on Outposts キャパシティーの管理を参照してください。	2020 年 12 月 21 日

強力な整合性	Amazon S3 には、すべての AWS リージョン にある Amazon S3 バケットの、オブジェクトの PUT および DELETE リクエストに関する、書き込み後読み取りの強力な整合性があります。さらに、Amazon S3 Select、Amazon S3 アクセスコントロールリスト、Amazon S3 オブジェクトタグ、オブジェクトメタデータ (HEAD オブジェクトなど) での読み込みオペレーションには強力な整合性があります。詳細については、「Amazon S3 のデータ整合性モデル」を参照してください。	2020 年 12 月 1 日
Amazon S3 レプリカ変更の同期	Amazon S3 レプリカ変更を同期することにより、ソースオブジェクトとレプリカとを同期する際に、タグ、ACL、オブジェクトロック設定などのオブジェクトメタデータを維持できます。この機能を有効にすると、Amazon S3 は、ソースオブジェクトまたはレプリカコピーのいずれかに対して行われたメタデータの変更を、レプリケートします。詳細については、「レプリカ変更の同期を使用してメタデータの変更をレプリケートする」を参照してください。	2020 年 12 月 1 日

Amazon S3 バケットキー	Amazon S3 バケットキーは、AWS Key Management Service (SSE-KMS) を使用した Amazon S3 サーバー側の暗号化のコストを削減します。サーバー側の暗号化でこの新しいバケットレベルキーを使用すると、Amazon S3 から AWS KMS へのリクエストトラフィックを減らすことにより、AWS KMS リクエストコストを最大 99% 削減できます。詳細については、「S3 バケットキーを使用した SSE-KMS のコストの削減」を参照してください。	2020 年 12 月 1 日

Amazon S3 Storage Lens	S3 ストレージレンズはメトリクスを集約し、Amazon S3 コンソールの [Buckets] (バケット) ページの [Account snapshot] (アカウントスナップショット) セクションにこの情報を表示します。S3 Storage Lens は、インサイトと傾向を可視化したり、外れ値にフラグ付けしたり、ストレージコストの最適化やデータ保護のベストプラクティスの適用に関するレコメンデーション事項を受け取ったりするために使用できるインタラクティブダッシュボードも提供します。ダッシュボードには、組織、アカウント、AWS リージョン、ストレージクラス、バケット、プレフィックス、またはストレージレンズのグループレベルでインサイトを生成して可視化できる、ドリルダウンオプションが用意されています。1 日 1 回のメトリクスのエクスポートを CSV 形式または Parquet 形式で S3 バケットに送信することもできます。詳細については、「S3 Storage Lens を使用したストレージのアクティビティと使用状況の評価」を参照してください。	2020 年 11 月 18 日

次を使用した S3 リクエストのトレースAWS X-Ray	Amazon S3 は X-Ray と統合して、トレースコンテキストを伝達し、アップストリームノードとダウンストリームノードを持つ 1 つのリクエストチェーンを提供します。詳細については、「X-Ray を使用したリクエストのトレース」を参照してください。	2020 年 11 月 16 日
S3 レプリケーションメトリクス	S3 レプリケーションメトリクスは、レプリケーション設定のレプリケーションルールの詳細なメトリクスを提供します。詳細については、「レプリケーションメトリクスと Amazon S3 イベント通知」を参照してください。	2020 年 11 月 9 日
S3 Intelligent-Tiering のアーカイブアクセスとディープアーカイブアクセス	S3 Intelligent-Tiering のアーカイブアクセスとディープアーカイブアクセスは、S3 Intelligent-Tiering の下位にあるストレージ層です。詳細については、「アクセスが頻繁なオブジェクトと頻繁ではないオブジェクトを自動的に最適化するストレージクラス」を参照してください。	2020 年 11 月 9 日

削除マーカーレプリケーション	削除マーカーのレプリケーションを使用すると、レプリケーションルールの送信先のバケットに、削除マーカーを確実にコピーできます。詳細については、「削除マーカーレプリケーションの使用」を参照してください。	2020 年 11 月 9 日
S3 オブジェクトの所有権	オブジェクト所有権は、バケットにアップロードされる新しいオブジェクトの所有権を制御するために使用できる S3 バケット設定です。詳細については、「S3 オブジェクト所有権の使用」を参照してください。	2020 年 10 月 2 日
Amazon S3 on Outposts	Amazon S3 on Outposts を使用すると、AWS Outposts リソースで S3 バケットを作成し、ローカルデータアクセス、ローカルデータ処理、データレジデンシーを必要とするアプリケーション用に、オンプレミスのオブジェクトを簡単に保存および取得できます。AWS Management Console、AWS CLI、AWS SDK、または REST API を使用して S3 on Outposts を使用できます。詳細については、Amazon S3 on Outposts の使用を参照してください。	2020 年 9 月 30 日

バケット所有者条件	Amazon S3 バケット所有者条件を使用すると、S3 オペレーションで使用するバケットが、正しい AWS アカウント に属していることを確認できます。詳細については、「バケット所有者条件」を参照してください。	2020 年 9 月 11 日
オブジェクトロック保持のための S3 バッチオペレーションサポート	バッチ操作と S3 オブジェクトロックを使用して、多くの Amazon S3 オブジェクトに一括で保持設定を適用できます。詳細については、「Setting S3 Object Lock Retention dates with S3 Batch Operations」(S3 バッチオペレーションを使用した S3 オブジェクトロック保持日の設定) を参照してください。	2020 年 5 月 4 日
オブジェクトロックのリーガルホールドのための S3 バッチオペレーションサポート	バッチオペレーションと S3 オブジェクトロックを使用して、多数の Amazon S3 オブジェクトに一括でリーガルホールドを追加できるようになりました。詳細については、「S3 オブジェクトロックの法的保留の設定への S3 バッチオペレーションの使用」を参照してください。	2020 年 5 月 4 日

S3 バッチオペレーションのジョブタグ	S3 バッチオペレーションジョブにタグを追加して、それらのジョブを制御およびラベル付けできます。詳細については、「Tags for S3 Batch Operations jobs」(S3 バッチオペレーションジョブのタグ) を参照してください。	2020 年 3 月 16 日
Amazon S3 アクセスポイント	Amazon S3 アクセスポイントは、S3 の共有データセットへの大規模なデータアクセスの管理を簡素化します。アクセスポイントは、バケットにアタッチされた名前付きのネットワークエンドポイントで、S3 オブジェクトのオペレーションを実行するために使用できます。詳細については、「Amazon S3 アクセスポイントによるデータアクセスの管理」を参照してください。	2019 年 12 月 2 日
Access Analyzer for Amazon S3	Access Analyzer for Amazon S3 は、インターネットの任意のユーザーや他の AWS アカウント (組織外のアカウントを含む) にアクセスを許可するように設定されている S3 バケットに関して警告します。詳細については、「Access Analyzer for Amazon S3 の使用」を参照してください。	2019 年 12 月 2 日

S3 Replication Time Control (S3 RTC)	S3 Replication Time Control (S3 RTC) では、Amazon S3 に「アップロードする」ほとんどのオブジェクトを数秒で、また 99.99% のオブジェクトを 15 分以内でレプリケートします。詳細については、「S3 Replication Time Control (S3 RTC) によるオブジェクトのレプリケーション」を参照してください。	2019 年 11 月 20 日
同一リージョンレプリケーション	同じ AWS リージョン 内の Amazon S3 バケット間でオブジェクトをコピーするには、同一リージョンレプリケーション (SRR) を使用します。クロスリージョンレプリケーション (CRR) および同一リージョンレプリケーションの詳細については、「レプリケーション」を参照してください。	2019 年 9 月 18 日
S3 オブジェクトロックのクロスリージョンレプリケーションのサポート	クロスリージョンレプリケーションはオブジェクトロックをサポートするようになりました。詳細については、「Amazon S3 がレプリケートするもの」を参照してください。	2019 年 5 月 28 日

S3 バッチオペレーション	S3 バッチオペレーションを使用することで、Amazon S3 のオブジェクトに対して大規模なバッチオペレーションを実行できます。S3 バッチオペレーションでは、指定したオブジェクトのリストに対して、1 つのオペレーションを実行できます。1 つのジョブで、エクサバイトのデータを含む数十億ものオブジェクトに対して、指定されたオペレーションを実行できます。詳細については、「S3 バッチオペレーションの実行」を参照してください。	2019 年 4 月 30 日
アジアパシフィック (香港) リージョン	Amazon S3 が、アジアパシフィック (香港) リージョンで使用できるようになりました。Amazon S3 リージョンおよびエンドポイントの詳細については、「AWS 全般のリファレンス」の「リージョンとエンドポイント」を参照してください。	2019 年 4 月 24 日
サーバーアクセスログに新しいフィールドを追加しました	Amazon S3 のサーバーアクセスログに次の新しいフィールドが追加されました: TLS (Transport Layer Security (TLS)) バージョン。詳細については、「サーバーアクセスログの形式」を参照してください。	2019 年 3 月 28 日

新しいアーカイブストレージクラス	Amazon S3 で、アクセス頻度の低いオブジェクトの保存用に、新しいアーカイブストレージクラス「S3 Glacier Deep Archive (DEEP_ARCHIVE)」を利用できるようになりました。詳細については、「ストレージクラス」を参照してください。	2019 年 3 月 27 日
新しいフィールドをサーバーアクセスログに追加しました	Amazon S3 では、次の新しいフィールドをサーバーアクセスログに追加しました: ホスト ID、署名バージョン、暗号スイート、認証タイプ、ホストヘッダー 詳細については、「サーバーアクセスログの形式」を参照してください。	2019 年 3 月 5 日
Parquet 形式の Amazon S3 インベントリファイルのサポート	Simple Storage Service (Amazon S3) では、Apache optimized row columnar (ORC)およびインベントリ出力ファイルのカンマ区切り値 (CSV) ファイル形式に加えて、Apache Parquet (Parquet) 形式をサポートします。詳細については、「インベントリ」を参照してください。	2018 年 12 月 4 日

S3 オブジェクトロック	Amazon S3 で、Amazon S3 オブジェクトへの Write Once Read Many (WORM) 保護を提供するオブジェクトロック機能を利用できるようになりました。詳細については、「オブジェクトのロック」を参照してください。	2018 年 11 月 26 日
復元速度のアップグレード	Amazon S3 の復元速度のアップグレードを使用すると、S3 Glacier Flexible Retrieval ストレージクラスで復元速度を変更できるため、復元が進行中であっても速度をより速くできます。詳細については、「アーカイブされたオブジェクトの復元」を参照してください。	2018 年 11 月 26 日
イベント通知の復元	Amazon S3 イベント通知では、オブジェクトを S3 Glacier Flexible Retrieval ストレージクラスから復元する際の開始イベントと完了イベントがサポートされるようになりました。詳細については、「イベント通知」を参照してください。	2018 年 11 月 26 日

S3 Glacier Flexible Retrieval ストレージクラスへの PUT ディレクトリ	Amazon S3 PUT オペレーションで、オブジェクトを作成する際に S3 Glacier Flexible Retrieval をストレージクラスとして指定できるようになりました。以前は、オブジェクトを別の Amazon S3 ストレージクラスから S3 Glacier Flexible Retrieval ストレージクラスに移行する必要がありました。さらに S3 クロスリージョンレプリケーション (CRR) を使用することで、S3 Glacier Flexible Retrieval をレプリケートされたオブジェクトのストレージクラスとして指定することもできるようになりました。S3 Glacier Flexible Retrieval ストレージクラスの詳細については、「ストレージクラス」を参照してください。レプリケートされたオブジェクトのストレージクラスを指定する方法の詳細については、「レプリケーション設定の概要」を参照してください。S3 Glacier Flexible Retrieval REST API 変更への PUT ディレクトリについての詳細は、ドキュメント履歴: S3 Glacier Flexible Retrieval への PUT ディレクトリを参照してください。	2018 年 11 月 26 日

新しいストレージクラス	Amazon S3 では、S3 Intelligent-Tiering (`INTELLIGENT_TIERING`) という名前のストレージクラスの提供を開始しました。このストレージクラスは、アクセスパターンが変化する、または未知で、長期間使用するデータ用に設計されています。詳細については、「ストレージクラス」を参照してください。	2018 年 11 月 26 日
Amazon S3 パブリックアクセスブロック	Amazon S3 にバケット単位またはアカウント全体でバケットとオブジェクトへのパブリックアクセスをブロックする機能が追加されました。詳細については、「Amazon S3 パブリックアクセスのブロックの使用」を参照してください。	2018 年 11 月 15 日

クロスリージョンレプリケーション (CRR) ルールのフィルタ処理機能の強化	CRR ルール設定では、オブジェクトフィルタを指定して、ルールを適用するオブジェクトのサブセットを選択できます。これまでは、オブジェクトキープレフィックスでのみフィルタを適用できました。今回のリリースにより、オブジェクトキープレフィックス、1 つ以上のオブジェクトタグ、またはその両方でフィルタを適用できるようになりました。詳細については、「CRR セットアップ: レプリケーション設定の概要」を参照してください。	2018 年 9 月 19 日
Amazon S3 Select の新機能	Amazon S3 Select では、Apache Parquet 入力、ネストされた JSON オブジェクトでのクエリ、および 2 つの新しい Amazon CloudWatch モニタリングメトリクス (`SelectScannedBytes` と `SelectReturnedBytes`) がサポートされるようになりました。	2018 年 9 月 5 日
更新を RSS で今すぐ入手可能	RSS フィードにサブスクライブすると、Amazon S3 ユーザーガイドの更新に関する通知を受け取ることができます。	2018 年 6 月 19 日

以前の更新

次の表に、2018 年 6 月 19 日以前の Amazon S3 ユーザーガイドの各リリースにおける重要な変更点が記されています。

変更	説明	日付
コード例の更新	コード例の更新: • C#—タスクベースの非同期パターンを使用するようにすべての例を更新しました。詳細については、AWS SDK for .NET デベロッパーガイドの「Amazon Web Services Asynchronous APIs for .NET」(.NET の Amazon Web Services 非同期 API) を参照してください。コード例は、バージョン 3 の AWS SDK for .NET に準拠するようになりました。 • Java—クライアントビルダーモデルを使用するようにすべての例を更新しました。クライアントビルダーモデルの詳細については、「サービスクライアントの作成」を参照してください。 • PHP – AWS SDK for PHP 3.0 を使用するようにすべての例を更新しました。AWS SDK for PHP 3.0 の詳細については、「AWS SDK for PHP」を参照してください。 • Ruby – サンプルコードを更新し、例が AWS SDK for Ruby バージョン 3 で動作するようにしました。	2018 年 30 月 4 日
Amazon S3 は、S3 Glacier Flexible Retrieval および `ONEZONE_IA` ストレージクラスを Amazon CloudWatch Logs ストレージメト	これらのストレージメトリクスには、実際のバイト数の報告に加えて、該当するストレージクラス (`ONEZONE_IA` 、`STANDARD_IA` 、S3 Glacier Flexible Retrieval) のオブジェクトごとのオーバーヘッドバイト数も含まれます。 • `ONEZONE_IA` および `STANDARD_IA` ストレージクラスオブジェクトの場合、Amazon S3 は 128 KB より小さいオブジェクトを 128 KB と報告します。詳細について	2018 年 30 月 4 日

変更	説明	日付
リクスに報告するようになりました。	は、「Amazon S3 ストレージクラスの理解と管理」を参照してください。 • S3 Glacier Flexible Retrieval ストレージクラスオブジェクトの場合、ストレージメトリクスは次のオーバーヘッドを報告します。 • オブジェクトあたり 32 KB のオーバーヘッド、S3 Glacier Flexible Retrieval ストレージクラスの料金で請求 • オブジェクトあたり 8 KB のオーバーヘッド、STANDARD ストレージクラスの料金で請求 詳細については、「Amazon S3 ライフサイクルを使用したオブジェクトの移行」を参照してください。 ストレージメトリクスの詳細については、「Amazon CloudWatch によるメトリクスのモニタリング」を参照してください。	
新しいストレージクラス	Amazon S3 では、オブジェクトを保存するための新しいストレージクラスである STANDARD_IA (IA は少頻度アクセスを意味します) の提供が開始されました。このストレージクラスは、存続時間が長く、アクセス頻度の低いデータに最適化されています。詳細については、「Amazon S3 ストレージクラスの理解と管理」を参照してください。	2018 年 4 月 4 日
Amazon S3 Select	a>Amazon S3 は、SQL 式に基づいたオブジェクトのコンテンツの取得をサポートするようになりました。詳細については、「Amazon S3 Select で所定のデータをクエリする」を参照してください。	2018 年 4 月 4 日

変更	説明	日付
アジアパシフィック (大阪: ローカル) リージョン	Amazon S3 が、アジアパシフィック (大阪ローカル) リージョンで使用できるようになりました。Amazon S3 リージョンおよびエンドポイントの詳細については、「AWS 全般のリファレンス」の「リージョンとエンドポイント」を参照してください。 **Important** アジアパシフィック (大阪ローカル) リージョンは、アジアパシフィック (東京) リージョンと組み合わせてのみ使用できます。アジアパシフィック (大阪ローカル) リージョンへのアクセスをリクエストするには、販売担当者にお問い合わせください。	2018 年 2 月 12 日
Amazon S3 インベントリ作成のタイムスタンプ	Amazon S3 インベントリには、Amazon S3 インベントリレポートの作成日と作成開始時刻のタイムスタンプが含まれるようになりました。このタイムスタンプを使用して、インベントリレポートの作成開始時刻以降の Amazon S3 ストレージの変更を判断できます。	2018 年 1 月 16 日
欧州 (パリ) リージョン	Amazon S3 が欧州 (パリ) リージョンで利用可能になりました。Amazon S3 リージョンおよびエンドポイントの詳細については、「AWS 全般のリファレンス」の「リージョンとエンドポイント」を参照してください。	2017 年 18 月 12 日
中国 (寧夏) リージョン	Amazon S3 が中国 (寧夏) リージョンで利用可能になりました。Amazon S3 リージョンおよびエンドポイントの詳細については、「AWS 全般のリファレンス」の「リージョンとエンドポイント」を参照してください。	2017 年 11 月 29 日

変更	説明	日付
ORC 形式の Amazon S3 インベントリファイルのサポート	Amazon S3 は、インベントリ出力ファイルにカンマ区切り値 (CSV) ファイル形式に加えて Apache 最適化行列 (ORC) 形式をサポートするようになりました。また、Amazon S3 インベントリをクエリする際に、Amazon Athena、Amazon Redshift Spectrum、およびその他のツール (Presto、Apache Hive、Apache Spark など) で標準の SQL を使用できるようになりました。詳細については、「S3 インベントリを使用したデータのカタログ化と分析」を参照してください。	2017 年 11 月 17 日
S3 バケットのデフォルトの暗号化	Amazon S3 のデフォルトの暗号化により、S3 バケットのデフォルト暗号化の動作を設定できます。バケットにデフォルト暗号化を設定して、バケットに保存される際すべてのオブジェクトが暗号化されるようにします。オブジェクトは、Amazon S3 マネージドキー (SSE-S3) と AWS マネージドキー (SSE-KMS) のいずれかで、サーバー側の暗号化を使って暗号化されます。詳細については、「Amazon S3 バケット向けのサーバー側のデフォルトの暗号化動作の設定」を参照してください。	2017 年 11 月 06 日
Amazon S3 インベントリの暗号化ステータス	Amazon S3 が Amazon S3 インベントリでの暗号化ステータスをサポートするようになったため、オブジェクトが保管時にどのようにコンプライアンス監査などの目的で暗号化されているかを確認できます。また、Amazon S3 インベントリをサーバー側暗号化 (SSE) または SSE-KMS で暗号化するように設定でき、すべてのインベントリファイルはそれに応じて暗号化されます。詳細については、「S3 インベントリを使用したデータのカタログ化と分析」を参照してください。	2017 年 11 月 06 日

変更	説明	日付
クロスリージョンレプリケーション (CRR) の機能強化	クロスリージョンレプリケーションは以下をサポートするようになりました。 • クロスアカウントのシナリオでは、CRR の設定を追加してレプリカの所有権を、送信先バケットを所有する AWS アカウント に変更できます。詳細については、「レプリカ所有者の変更」を参照してください。 • デフォルトでは、Amazon S3 は AWS KMS に保存されたキーでサーバー側の暗号化を使用して作成されたソースバケット内のオブジェクトをレプリケートしません。CRR 設定で、これらのオブジェクトをレプリケートするよう Amazon S3 に指示できるようになりました。詳細については、「暗号化されたオブジェクトのレプリケート (SSE-S3、SSE-KMS、DSSE-KMS、SSE-C)」を参照してください。	2017 年 11 月 06 日
欧州 (ロンドン) リージョン	Amazon S3 が欧州 (ロンドン) リージョンで利用可能になりました。Amazon S3 リージョンおよびエンドポイントの詳細については、「AWS 全般のリファレンス」の「リージョンとエンドポイント」を参照してください。	2016 年 12 月 13 日
カナダ (中部) リージョン	Amazon S3 がカナダ (中部) リージョンで使用可能になりました。Amazon S3 リージョンおよびエンドポイントの詳細については、「AWS 全般のリファレンス」の「リージョンとエンドポイント」を参照してください。	2016 年 12 月 8 日

変更	説明	日付
オブジェクトのタグ付け	Amazon S3 では、オブジェクトのタグ付けがサポートされるようになりました。オブジェクトのタグ付けによりストレージを分類できます。オブジェクトキー名のプレフィックスによってもストレージを分類でき、オブジェクトのタグ付けによって別のディメンションが追加されます。 タグ付けには他のメリットもあります。具体的には次のとおりです。 • オブジェクトタグにより、アクセス許可を細かくアクセスコントロールできます (たとえば、特定のタグが付いたオブジェクトのみ読み取るアクセス許可を IAM ユーザーに付与できます)。 • ライフサイクル設定を指定する際の細かいコントロール。ライフサイクルルールが適用されるオブジェクトのサブセットを選択するタグを指定できます。 • クロスリージョンレプリケーション (CRR) を設定している場合、Amazon S3 はタグをレプリケートできます。オブジェクトを自動的にレプリケートできるように、Amazon S3 に作成された IAM ロールに必要なアクセス許可を付与する必要があります。 • CloudWatch メトリクスと CloudTrail イベントをカスタマイズして、特定のタグフィルタごとに情報を表示することもできます。 詳細については、「タグを使用してストレージを分類する」を参照してください。	2016 年 11 月 29 日

変更	説明	日付
Amazon S3 ライフサイクルでタグベースのフィルタのサポートを開始	Amazon S3 では、ライフサイクル設定におけるタグベースのフィルタリングがサポートされるようになりました。キープレフィックス、1 つ以上のオブジェクトタグ、または両方の組み合わせを指定できるライフサイクルルールを指定して、ライフサイクルルールが適用されるオブジェクトのサブセットを選択できるようになりました。詳細については、「オブジェクトのライフサイクルの管理」を参照してください。	2016 年 11 月 29 日
バケットの CloudWatch リクエストメトリクス	Amazon S3 では、バケットで行われたリクエストの CloudWatch メトリクスがサポートされるようになりました。バケットでこれらのメトリクスを有効にすると、メトリクスが 1 分ごとに報告されます。これらのリクエストメトリクスを報告するバケット内のオブジェクトを設定することもできます。詳細については、「Amazon CloudWatch によるメトリクスのモニタリング」を参照してください。	2016 年 11 月 29 日
Amazon S3 インベントリ	Amazon S3 では、ストレージインベントリがサポートされるようになりました。Amazon S3 インベントリは、S3 バケットまたは共有プレフィックスに関して、オブジェクトのフラットファイル出力と対応するメタデータを毎日または毎週生成します (つまり、名前の先頭が共通文字列のオブジェクト)。 詳細については、「S3 インベントリを使用したデータのカタログ化と分析」を参照してください。	2016 年 11 月 29 日

変更	説明	日付
Amazon S3 分析 – ストレージクラス分析	新しい Amazon S3 分析 – ストレージクラスの分析機能は、アクセス頻度の低い STANDARD ストレージをいつ STANDARD_IA (IA: 小頻度アクセス) ストレージクラスに移行すべきかを判断できるように、データアクセスパターンを確認します。ストレージクラス分析が、フィルタリングされたデータセットの低頻度アクセスパターンを一定期間監視すると、分析結果を使用してライフサイクル設定を改善できます。この機能には、S3 バケットにエクスポートできる指定したバケット、プレフィックス、またはタグのレベルに応じたストレージ使用状況の毎日の詳細な分析も含まれています。	2016 年 11 月 29 日
アーカイブされたオブジェクトを S3 Glacier から復元する際の新しい緊急データ取得と一括データ取得	Amazon S3 では、S3 Glacier にアーカイブされたオブジェクトを復元する際に、標準取得に加えて緊急データ取得と一括データ取得がサポートされるようになりました。詳細については、「アーカイブされたオブジェクトの復元」を参照してください。	2016 年 11 月 21 日
CloudTrail オブジェクト記録	CloudTrail では、GetObject 、PutObject 、DeleteObject など、Amazon S3 オブジェクトレベルの API オペレーションのログ記録がサポートされます。オブジェクトレベルの API オペレーションが口グ記録されるように、イベントセレクターを設定できます。詳細については、「AWS CloudTrail を使用した Amazon S3 API コールのログ記録」を参照してください。	2016 年 11 月 21 日
米国東部 (オハイオ) リージョン	Amazon S3 が米国東部 (オハイオ) リージョンで利用可能になりました。Amazon S3 リージョンおよびエンドポイントの詳細については、「AWS 全般のリファレンス」の「リージョンとエンドポイント」を参照してください。	2016 年 10 月 17 日

変更	説明	日付
Amazon S3 Transfer Acceleration 向けの IPv6 サポート	Amazon S3 は、Amazon S3 Transfer Acceleration 向けのインターネットプロトコルバージョン 6 (IPv6) をサポートするようになりました。Transfer Acceleration エンドポイントの新しいデュアルスタックを使用することで、IPv6 を使って Amazon S3 に接続できます。詳細については、「Amazon S3 Transfer Acceleration の開始方法」を参照してください。	2016 年 10 月 6 日
IPv6 サポート	Amazon S3 がインターネットプロトコルのバージョン 6 (IPv6) をサポートするようになりました。デュアルスタックのエンドポイントを使用して IPv6; で Amazon S3 にアクセスできます。詳細については、「Amazon S3 API リファレンス」の「IPv6 経由で Amazon S3 へのリクエストを行う」を参照してください。	2016 年 8 月 11 日
アジアパシフィック (ムンバイ) リージョン	Amazon S3 が、アジアパシフィック (ムンバイ) リージョンで使用できるようになりました。Amazon S3 リージョンおよびエンドポイントの詳細については、「AWS 全般のリファレンス」の「リージョンとエンドポイント」を参照してください。	2016 年 6 月 27 日
Amazon S3 Transfer Acceleration	Amazon S3 Transfer Acceleration によって、クライアントと S3 バケットの長距離間でファイルを高速、簡単、安全に転送できます。Transfer Acceleration は、Amazon CloudFront の世界中に点在するエッジロケーションを利用します。 詳細については、「Amazon S3 Transfer Acceleration を使用した高速かつ安全なファイル転送の設定」を参照してください。	2016 年 4 月 19 日
期限切れオブジェクト削除マーカーを削除するライフサイクルのサポート	ライフサイクル設定の `Expiration` アクションで、バージョニング管理されたバケット内の期限切れオブジェクトの削除マーカーを削除するように Amazon S3 に指示できるようになりました。詳細については、「ライフサイクルアクションを記述する要素」を参照してください。	2016 年 3 月 16 日

変更	説明	日付
バケットのライフサイクル設定での完了していないマルチパートアップロードを中止するアクションのサポート	バケットのライフサイクル設定で、AbortIncompleteMultipartUpload アクションがサポートされるようになりました。このアクションを使用すると、開始後に指定された日数以内に完了していないマルチパートアップロードを中止するように Amazon S3 に指示できます。マルチパートアップロードが中止オペレーションの対象になると、Amazon S3 はアップロードされたパートをすべて削除し、マルチパートアップロードを中止します。 概念的な情報については、Amazon S3 ユーザーガイドの以下のトピックを参照してください。 • マルチパートアップロードの中止 • ライフサイクルアクションを記述する要素 次の API オペレーションが更新され、新しいアクションがサポートされるようになりました。 • PUT Bucket lifecycle – XML 設定で、ライクサイクル設定ルールに AbortIncompleteMultipartUpload アクションを指定できるようになりました。 • パートの一覧表示とマルチパートアップロードの開始 – バケットに x-amz-abort-date アクションを指定しているライフサイクルルールがある場合、これらの 2 つの API オペレーションは追加の 2 つのレスポンスヘッダー (x-amz-abort-rule-id と AbortIncompleteMultipartUpload) を返すようになりました。レスポインスのこれらのヘッダーは、開始されたマルチパートアップロードがいつ中止オペレーションの対象になり、どのライフサイクルルールが適用されるかを示します。	2016 年 3 月 16 日

変更	説明	日付
アジアパシフィック (ソウル) リージョン	Amazon S3 が、アジアパシフィック (ソウル) リージョンで使用できるようになりました。Amazon S3 リージョンおよびエンドポイントの詳細については、「AWS 全般のリファレンス」の「リージョンとエンドポイント」を参照してください。	2016 年 1 月 6 日
新しい条件キーとマルチパートアップロードの変更	IAM ポリシーが、Amazon S3 `s3:x-amz-storage-class` 条件キーをサポートするようになりました。詳細については、「条件キーを使用したバケットポリシーの例」を参照してください。 パートをアップロードしてアップロードを完了するために、マルチパートアップロードのイニシエータになる必要がなくなりました。詳細については、「マルチパートアップロード API とアクセス許可」を参照してください。	2015 年 12 月 14 日
米国スタンダードリージョンの名前を変更しました	「米国スタンダード」から「米国東部 (バージニア北部)」にリージョン名文字列を変更しました。これはリージョン名の更新のみであり、機能に変更はありません。	2015 年 12 月 11 日

変更	説明	日付
新しいストレージクラス	Amazon S3 では、オブジェクトを保存するための新しいストレージクラスである STANDARD_IA (IA、少頻度アクセス) の提供が開始されました。このストレージクラスは、存続時間が長く、アクセス頻度の低いデータに最適化されています。詳細については、「Amazon S3 ストレージクラスの理解と管理」を参照してください。 ライフサイクル設定機能の更新により、STANDARD_IA ストレージクラスにオブジェクトを移行できるようになりました。詳細については、「オブジェクトのライフサイクルの管理」を参照してください。 これまでは、クロスリージョンレプリケーション機能では、オブジェクトのレプリカにソースオブジェクトのストレージクラスが使用されました。現在は、クロスリージョンのレプリケーションを設定するときに、送信先バケットで作成されたオブジェクトレプリカ用にストレージクラスを指定することができます。詳細については、「リージョン内およびリージョン間でのオブジェクトのレプリケート」を参照してください。	2015 年 9 月 16 日
AWS CloudTrail の統合	新しい AWS CloudTrail の統合により、Amazon S3 API 操作を S3 バケットに記録できるようになりました。CloudTrail を使用して、S3 バケットの作成または削除、アクセス制御の変更、またはライフサイクル設定の変更を追跡できます。詳細については、「AWS CloudTrail を使用した Amazon S3 API コールのログ記録」を参照してください。	2015 年 9 月 1 日

変更	説明	日付
バケット制限の引き上げ	Amazon S3 でバケット制限の引き上げがサポートされるようになりました。デフォルトでは、AWS アカウント で作成できるバケットの数は最大で 100 個です。追加のバケットを必要とする場合は、サービスの制限の引き上げを申請することで制限を引き上げることができます。バケットの制限を引き上げる方法については、AWS 全般リファレンスの「AWS のサービス クォータ」を参照してください。詳細については、「AWS SDKs の使用」および「汎用バケットのクォータ、制限、制約」を参照してください。	2015 年 8 月 4 日
整合性モデルの更新	Amazon S3 が、米国東部 (バージニア北部) リージョンで Amazon S3 に追加された新しいオブジェクトの read-after-write 整合性をサポートするようになりました。この更新の前は、米国東部 (バージニア北部) 以外のすべてのリージョンが、Amazon S3 にアップロードされた新しいオブジェクトの「read-after-write」整合性をサポートしていました。この機能強化により、Amazon S3 は、すべてのリージョンについて、Amazon S3 に追加された新しいオブジェクトの「read-after-write」整合性をサポートするようになりました。「Read-after-write」整合性により、Amazon S3 でオブジェクトを作成した直後にオブジェクトを取得できます。詳細については、「リージョン」を参照してください。	2015 年 8 月 4 日
イベント通知	Amazon S3 のイベント通知が更新されており、オブジェクトが削除されたときの通知が追加され、プレフィックスおよびサフィックスの一致によるオブジェクト名のフィルタリングが追加されました。詳細については、「Amazon S3 イベント通知」を参照してください。	2015 年 7 月 28 日

変更	説明	日付
Amazon CloudWatch との統合	新しい Amazon CloudWatch 統合により、Amazon S3 の CloudWatch メトリクスを使用して、Amazon S3 の使用状況に関するアラームを監視および設定できます。サポートされているメトリクスには、標準ストレージの合計バイト数、低冗長化ストレージの合計バイト数、特定の S3 バケットのオブジェクトの合計数などがあります。詳細については、「Amazon CloudWatch によるメトリクスのモニタリング」を参照してください。	2015 年 7 月 28 日
空ではないバケットの削除とバケットを空にするサポート	Amazon S3 は、空ではないバケットの削除とバケットを空にするサポートができるようになりました。詳細については、「汎用バケットを空にする」を参照してください。	2015 年 7 月 16 日
Amazon VPC エンドポイントのバケットポリシー	Amazon S3 では、仮想プライベートクラウド (VPC) エンドポイントのバケットポリシーのサポートが追加されました。S3 バケットポリシーを使用して、特定の VPC エンドポイントまたは特定の VPC からバケットへのアクセスを制御できます。VPC エンドポイントは設定が簡単で信頼性が高く、ゲートウェイまたは NAT インスタンスを必要とすることなく、Amazon S3 に安全に接続できます。詳細については、「バケットポリシーを使用した VPC エンドポイントからのアクセスコントロール」を参照してください。	2015 年 4 月 29 日
イベント通知	Amazon S3 イベント通知は、AWS Lambda 関数のリソースベースの許可への切り替えをサポートするように更新されました。詳細については、「Amazon S3 イベント通知」を参照してください。	2015 年 4 月 9 日
クロスリージョンレプリケーション	Amazon S3 がクロスリージョンレプリケーションをサポートするようになりました。クロスリージョンレプリケーションは、異なる AWS リージョンにあるバケット間でオブジェクトを自動的に非同期コピーする機能です。詳細については、「リージョン内およびリージョン間でのオブジェクトのレプリケート」を参照してください。	2015 年 3 月 24 日

変更	説明	日付
イベント通知	Amazon S3 では、バケットの通知設定で、新しいイベントタイプと宛先がサポートされるようになりました。このリリース以前の Amazon S3 では、s3:ReducedRedundancyLostObject イベントタイプおよびその宛先として Amazon SNS トピックのみがサポートされていました。新しいイベントタイプの詳細については、「Amazon S3 イベント通知」を参照してください。	2014 年 11 月 13 日
お客様が用意した暗号化キーを使用したサーバー側の暗号化	AWS Key Management Service (AWS KMS) キー (SSE-KMS) によるサーバー側の暗号化 Amazon S3 で、AWS KMS を使用したサーバー側暗号化がサポートされるようになりました。この機能により、AWS KMS を介してエンベロープキーを管理できます。また、Amazon S3 は AWS KMS を呼び出して、設定された許可内のエンベロープキーにアクセスできます。 AWS KMS のサーバー側の暗号化の詳細については、「AWS Key Management Service でのサーバー側の暗号化を使用したデータの保護」を参照してください。	2014 年 11 月 12 日
欧州 (フランクフルト) リージョン	Amazon S3 が欧州 (フランクフルト) リージョンで利用可能になりました。	2014 年 10 月 23 日

変更	説明	日付
お客様が用意した暗号化キーを使用したサーバー側の暗号化	Amazon S3 で、お客様が用意した暗号化キーによるサーバー側の暗号化 (SSE-C)がサポートされるようになりました。サーバー側の暗号化によって、保管時のデータの暗号化を Amazon S3 にリクエストすることができます。SSE-C を使用する場合、Amazon S3 はお客様が用意した独自の暗号化キーを使用してオブジェクトを暗号化します。Amazon S3 によって暗号化が実行されるため、独自の暗号化コードを作成または実行するコストをかけずに、独自の暗号化キーを使用できるというメリットがあります。 SSE-C の詳細については、「お客様が用意した暗号化キーによるサーバー側の暗号化 (SSE-C) を使用したデータの保護」を参照してください。	2014 年 6 月 12 日
バージョニングのライフサイクルのサポート	以前のリリースでは、ライフサイクルの設定は、バージョニングが設定されていないバケットでのみサポートされていました。このリリースでは、バージョニング対応および非対応の両方のバケットでライフサイクルを設定できます。詳細については、「オブジェクトのライフサイクルの管理」を参照してください。	2014 年 5 月 20 日
アクセスコントロールのトピックを改訂	Amazon S3 アクセスコントロールのドキュメントが改訂されました。詳細については、「Amazon S3 用 Identity and Access Management」を参照してください。	2014 年 4 月 15 日
サーバーアクセスの口グ記録に関するトピックが改訂されました。	改訂後の、サーバーアクセスログ記録のドキュメント。詳細については、「サーバーアクセスログによるリクエストの口グ記録」を参照してください。	2013 年 11 月 26 日
.NET SDK サンプルがバージョン 2.0 に更新	このガイドの .NET SDK サンプルがバージョン 2.0 に準拠しました。	2013 年 11 月 26 日

変更	説明	日付
HTTP 経由での SOAP のサポートが廃止される	SOAP のサポートは HTTP 経由では廃止されましたが、HTTPS 経由では引き続き利用可能です。SOAP では、Amazon S3 の新機能がサポートされなくなります。REST API か AWS SDK を使用することをお勧めします。	2013 年 9 月 20 日
IAM ポリシー変数のサポート	IAM ポリシー言語では、変数がサポートされるようになりました。ポリシーが評価されると、認証ユーザーのセッションの文脈ベースの情報から得られた値によって、ポリシー変数が置換されます。ポリシー変数を使用すれば、ポリシーのすべての構成要素を明示的にリストしなくても、汎用的なポリシーを定義できます。ポリシー変数の詳細については、IAM ユーザーガイドの「IAM ポリシー変数の概要」を参照してください。 Amazon S3 のポリシー変数の例については、「Amazon S3 のアイデンティティベースのポリシー例」を参照してください。	2013 年 3 月 4 日
コンソールでのリクエスタ支払いのサポート	Amazon S3 コンソールで、バケットをリクエスタ支払い用に設定できるようになりました。詳細については、「ストレージの転送と使用にリクエスタ支払い汎用バケットを使用する」を参照してください。	2012 年 12 月 31 日

変更	説明	日付
ウェブサイトホスティングでのルートドメインのサポート	Amazon S3 が、ルートドメインでの静的ウェブサイトのホスティングをサポートするようになりました。ウェブサイトにアクセスする訪問者がブラウザにウェブアドレスを入力する際、「www」を省略できます (例えば、www.example.com ではなく example.com を使用できます)。既に Amazon S3 上でホスティングされている静的ウェブサイトの多くが、www サブドメイン (例: www.example.com) からアクセスするようになっています。これまでは、ルートドメインアクセスをサポートするには、ルートドメインへのリクエストをブラウザから Amazon S3 上のウェブサイトに中継するためのウェブサーバーを独自に運用することが必要でした。リクエストを中継するためのウェブサーバー運用には、コストや運用の負担の増加が伴うだけではなく、障害点となりうるものが増えるおそれがあります。現在では、Amazon S3 の可用性と耐久性の高さを、「www」とルートドメインの両方のアドレスに活用できます。詳細については、「Amazon S3 を使用して静的ウェブサイトをホスティングする」を参照してください。	2012 年 12 月 27 日
コンソールの修正	Amazon S3 コンソールが更新されました。ドキュメントのトピックのうち、コンソールに言及している部分も、これに従って修正されています。	2012 年 12 月 14 日

変更	説明	日付
S3 Glacier へのデータのアーカイブのサポート	Amazon S3 で、データのアーカイブに S3 Glacier の低コストなストレージサービスを使用する新しいストレージオプションがサポートされるようになりました。オブジェクトをアーカイブするには、オブジェクト、および Amazon S3 でこれらのオブジェクトを S3 Glacier にアーカイブする期間を特定するためのアーカイブルールを定義します。Amazon S3 コンソールを使用して、あるいは Amazon S3 API または AWS SDK を使用したプログラミングによって、バケット上にルールを簡単に設定できます。 詳細については、「オブジェクトのライフサイクルの管理」を参照してください。	2012 年 11 月 13 日
ウェブサイトページのリダイレクトのサポート	Amazon S3 では、バケットがウェブサイトとして設定されている場合、オブジェクトに対するリクエストを同じバケット内の別のオブジェクトまたは外部 URL にリダクレクトできるようになりました。詳細については、「(オプション) ウェブページリダイレクトの設定」を参照してください。 ウェブサイトのホスティングについては、Amazon S3 を使用して静的ウェブサイトをホスティングする を参照してください。	2012 年 10 月 4 日

変更	説明	日付
Cross-Origin Resource Sharing (CORS) のサポート	Amazon S3 で Cross Origin Resource Sharing (CORS) がサポートされるようになりました。CORS は、あるドメインにロードされたクライアントウェブアプリケーションが、異なるドメイン内のリソースと通信またはアクセスする方法を定義します。Amazon S3 で CORS がサポートされたことにより、Amazon S3 を基盤とする機能豊富なクライアント側ウェブアプリケーションを構築し、Amazon S3 リソースに対するクロスドメインアクセスを選択的に許可することができます。詳細については、「Cross-Origin Resource Sharing (CORS) の使用」を参照してください。	2012 年 8 月 31 日
コスト割り当てタグのサポート	Amazon S3 でコスト割り当てタグがサポートされました。S3 バケットにラベルを付けることができるため、プロジェクトやその他の条件に照らして、それらのコストを簡単に追跡できます。バケットのタグの使用に関する詳細については、「S3 バケットタグでのコスト配分タグの使用」を参照してください。	2012 年 8 月 21 日
バケットポリシーでの MFA で保護された API アクセスのサポート	Amazon S3 で、MFA で保護された API アクセスがサポートされました。これにより、Amazon S3 リソースへのアクセス時に AWS Multi-Factor Authentication を適用してセキュリティを強化できます。このセキュリティ機能では、有効な MFA コードを入力して MFA デバイスを物理的に所有していることを証明することがユーザーに要求されます。詳細については、「AWS 多要素認証」を参照してください。Amazon S3 リソースへのすべてのアクセスリクエストに対して、MFA 認証を要求できるようになりました。 MFA 認証を適用するために、Amazon S3 がバケットポリシーで `aws:MultiFactorAuthAge` キーがサポートされるようになりました。バケットポリシーの例については、「MFA が必要」を参照してください。	2012 年 7 月 10 日

変更	説明	日付
オブジェクトの有効期限のサポート	オブジェクトの有効期限を使用して、設定した期間を経過後にデータを自動削除するよう設定できます。オブジェクトの有効期限を設定するには、バケットにライフサイクル設定を追加します。	2011 年 12 月 27 日
新しくサポートされるリージョン	Amazon S3 で、南米 (サンパウロ) リージョンがサポートされるようになりました。詳細については、「Amazon S3 汎用バケットへのアクセス」を参照してください。	2011 年 12 月 14 日
Multi-Object Delete	Amazon S3 で、単一のリクエストで複数のオブジェクトを削除できるマルチオブジェクト削除 API がサポートされるようになりました。この機能を使用して、複数の個別の DELETE リクエストを使用するよりもすばやく多数のオブジェクトを Amazon S3 から削除できます。詳細については、「Amazon S3 オブジェクトの削除」を参照してください。	2011 年 12 月 7 日
新しくサポートされるリージョン	Amazon S3 で、米国西部 (オレゴン) リージョンがサポートされるようになりました。詳細については、「バケットとリージョン」を参照してください。	2011 年 11 月 8 日
ドキュメントの更新	ドキュメントのバグの修正。	2011 年 11 月 8 日
ドキュメントの更新	ドキュメントのバグの修正に加えて、このリリースには、次の機能強化が含まれています。 • AWS SDK for PHP と AWS SDK for Ruby (「Amazon S3 マネージドキーによるサーバー側の暗号化 (SSE-S3) の指定」を参照) を使用した新しいサーバー側の暗号化セクション。	2011 年 10 月 17 日

変更	説明	日付
サーバー側暗号化のサポート	Amazon S3 で、サーバー側暗号化がサポートされるようになりました。これにより、Amazon S3 に保存時にデータを暗号化する、つまり、Amazon S3 がそのデータセンター内のディスクにオブジェクトデータを書き込むときに、データを暗号化するようにリクエストできます。REST API の更新に加えて、AWS SDK for Java および .NET には、サーバー側の暗号化をリクエストするために必要な機能が備わっています。さらに、AWS Management Console を使用して、オブジェクトのアップロード時に、サーバー側暗号化をリクエストすることもできます。データ暗号化の詳細については、「暗号化を使用したデータの保護」を参照してください。	2011 年 10 月 4 日
ドキュメントの更新	ドキュメントのバグの修正に加えて、このリリースには、次の機能強化が含まれています。 • 「Amazon S3 API リファレンス」の「リクエストの作成」セクションに Ruby と PHP サンプルを追加しました。 • 署名付き URL の生成および使用方法を説明するセクションが追加されました。詳細については、「署名付き URL を使用したオブジェクトの共有」および「署名付き URL を使用したオブジェクトの共有」を参照してください。 • Eclipse および Visual Studio 用の AWS Explorer を紹介する既存のセクションが更新されました。詳細については、「Amazon S3 API リファレンス」の「AWS SDK を使用した Amazon S3 での開発」を参照してください。	2011 年 9 月 22 日

変更	説明	日付
一時的なセキュリティ認証情報を使用したリクエスト送信のサポート	AWS アカウントおよび IAM ユーザーセキュリティ証明書を使用して認証済みリクエストを Amazon S3 に送信することに加え、AWS Identity and Access Management (IAM) から取得する一時セキュリティ認証情報を使用してリクエストを送信できるようになりました。AWS Security Token Service API または AWS SDK ラッパーライブラリを使用して、一時的な認証情報を IAM でリクエストできます。これらの一時セキュリティ証明書は、自身で使用するためにリクエストするか、フェデレーティッドユーザーおよびアプリケーションに渡すことができます。この機能により、AWS の外部でユーザーを管理し、それらのユーザーに AWS リソースにアクセスするための一時セキュリティ証明書を提供できます。 詳細については、「Amazon S3 API リファレンス」の「リクエストの実行」を参照してください。 一時的なセキュリティ認証情報の IAM によるサポートの詳細については、IAM ユーザーガイドの「IAM の一時的なセキュリティ認証情報」を参照してください。	2011 年 8 月 3 日
マルチパートアップロード API 拡張による最大 5 TB のオブジェクトのコピー	このリリース以前、Amazon S3 API では5 GB までのサイズのオブジェクトのコピーをサポートしていました。5 GB 以上のオブジェクトをコピーできるようにするため、Amazon S3 で新しいオペレーション `Upload Part (Copy)` が加えられて、マルチパートアップロード API が拡張されました。このマルチパートアップロード操作を使用して、最大 5 TB のサイズのオブジェクトをコピーできます。詳細については、「オブジェクトのコピー、移動、名前の変更」を参照してください。 マルチパートアップロード API の概念については、Amazon S3 でのマルチパートアップロードを使用したオブジェクトのアップロードとコピー を参照してください。	2011 年 21 月 6 日

変更	説明	日付
HTTP を介した SOAP API 呼び出しの無効化	セキュリティの向上のため、HTTP を介した SOAP API 呼び出しが無効になりました。認証済みおよび匿名 SOAP リクエストは SSL を使用して、Amazon S3 に送信される必要があります。	2011 年 6 月 6 日
IAM によるクロスアカウント委任の有効化	これまでは、Amazon S3 リソースにアクセスするには、IAM ユーザーは親 AWS アカウントと Amazon S3 リソース所有者の両方からの許可が必要でした。アカウント間のアクセスによって、IAM ユーザーは所有者アカウントからのアクセス許可のみが必要になりました。つまり、リソース所有者が AWS アカウントへのアクセス許可を付与した場合、その AWS アカウントは IAM ユーザーにこれらのリソースへのアクセス許可を付与できるようになりました。 詳細については、IAM ユーザーガイドの「IAM ユーザーにアクセス許可を委任するロールの作成」を参照してください。 バケットポリシーでのプリンシパルの指定については、バケットポリシーのプリンシパル を参照してください。	2011 年 6 月 6 日
新しいリンク	このサービスのエンドポイント情報は、現在、AWS 全般のリファレンスで参照できます。詳細については、AWS の全般的なリファレンスの「リージョンとエンドポイント」を参照してください。	2011 年 3 月 1 日

変更	説明	日付
Amazon S3 での静的ウェブサイトのホストのサポート	Amazon S3 に、静的ウェブサイトをホストするための拡張サポートが導入されました。これには、インデックスドキュメントとカスタムエラードキュメントのサポートが含まれます。これらの機能を使用すると、バケットのルートまたはサブフォルダへのリクエスト (例えば `http://mywebsite.com/subfolder`) は、バケット内のオブジェクトのリストの代わりに、インデックスドキュメントを返します。エラーが検出されると、Amazon S3 は Amazon S3 エラーメッセージの代わりにカスタムエラーメッセージを返します。詳細については、「Amazon S3 を使用して静的ウェブサイトをホスティングする」を参照してください。	2011 年 6 月 6 日
このサービスのエンドポイント情報は、現在、AWS 全般のリファレンスで参照できます。詳細については、AWS の全般的なリファレンスの「リージョンとエンドポイント」を参照してください。	2011 年 3 月 1 日	

変更	説明	日付
Amazon S3 での静的ウェブサイトのホストのサポート	Amazon S3 に、静的ウェブサイトをホストするための拡張サポートが導入されました。これには、インデックスドキュメントとカスタムエラードキュメントのサポートが含まれます。これらの機能を使用すると、バケットのルートまたはサブフォルダへのリクエスト (例えば `http://mywebsite.com/subfolder`) は、バケット内のオブジェクトのリストの代わりに、インデックスドキュメントを返します。エラーが検出されると、Amazon S3 は Amazon S3 エラーメッセージの代わりにカスタムエラーメッセージを返します。詳細については、「Amazon S3 を使用して静的ウェブサイトをホスティングする」を参照してください。	2011 年 2 月 17 日
レスポンスヘッダー API のサポート	GET Object REST API により、各リクエストの REST GET Object リクエストのレスポンスヘッダーを変更できるようになりました。つまり、オブジェクト自体を変更せずに、レスポンスのオブジェクトメタデータを変更できます。詳細については、「オブジェクトのダウンロード」を参照してください。	2011 年 1 月 14 日
大容量オブジェクトのサポート	Amazon S3 で S3 バケットに保存できるオブジェクトの最大サイズが5 GB から5 TB に増加しました。REST API を使用する場合、単一の PUT 操作で、最大 5 GB のオブジェクトをアップロードできます。これよりも大きなオブジェクトは、マルチパートアップロード REST API を使用して、オブジェクトを分割してアップロードする必要があります。詳細については、「Amazon S3 でのマルチパートアップロードを使用したオブジェクトのアップロードとコピー」を参照してください。	2010 年 12 月 9 日

変更	説明	日付
マルチパートアップロード	マルチパートアップロードにより、Amazon S3 に高速で柔軟にアップロードできます。一連のパーツとして、単一のオブジェクトをアップロードできます。詳細については、「Amazon S3 でのマルチパートアップロードを使用したオブジェクトのアップロードとコピー」を参照してください。	2010 年 11 月 10 日
バケットポリシーでの正規化 ID のサポート	バケットポリシーで正規化 ID を指定できるようになりました。詳細については、バケットポリシーのプリンシパルを参照してください。	2010 年 9 月 17 日
Amazon S3 の IAM との連携	このサービスが AWS Identity and Access Management (IAM) と連動するようになりました。詳細については、IAM ユーザーガイドの「IAM と連携する AWS のサービス」を参照してください。	2010 年 9 月 2 日
通知	Amazon S3 通知機能により、Amazon S3 がバケットで主要イベントを検出した場合に、Amazon Simple Notification Service (Amazon SNS) トピックにメッセージを公開するように、バケットを設定できます。詳細については、「Amazon S3 イベント通知の設定」を参照してください。	2010 年 7 月 14 日
バケットポリシー	バケットポリシーは、バケット、オブジェクト、一連のオブジェクト間でアクセス許可を設定するために使用するアクセス管理システムです。この機能は、アクセスコントロールリストを補完し、多くの場合に置き換わるものです。詳細については、「Amazon S3 のバケットポリシー」を参照してください。	2010 年 7 月 6 日
すべてのリージョンで使用可能なパススタイル構文	Amazon S3 では、米国クラシックリージョンの、またはバケットがリクエストのエンドポイントと同じリージョンにある場合、すべてのバケットでパススタイル構文をサポートするようになりました。詳細については、「バケットの仮想ホスティング」を参照してください。	2010 年 6 月 9 日

変更	説明	日付
欧州 (アイルランド) の新しいエンドポイント	Amazon S3 は、欧州 (アイルランド) のエンドポイントを提供するようになりました: `http://s3-eu-west-1.amazonaws.com` 。	2010 年 6 月 9 日
コンソール	AWS Management Console 経由で、Amazon S3 を使用できるようになりました。Amazon Simple Storage Service ユーザーガイドで、コンソールのすべての Amazon S3 機能について読むことができます。	2010 年 6 月 9 日
低冗長化	低冗長化ストレージに Amazon S3 のオブジェクトを格納することにより、Amazon S3 でストレージコストの削減を実現できます。詳細については、「低冗長化ストレージ」を参照してください。	2010 年 5 月 12 日
新しくサポートされるリージョン	Amazon S3 でアジアパシフィック (シンガポール) リージョンがサポートされるようになりました。詳細については、「バケットとリージョン」を参照してください。	2010 年 4 月 28 日
オブジェクトのバージョニング	本リリースでオブジェクトバージョニングが導入されました。すべてのオブジェクトはキーとバージョンを持つことができます。バケットのバージョニングを有効にすると、Amazon S3 はバケットに追加されたすべてのオブジェクトに一意のバージョン ID を与えます。この機能により、意図しない上書きと削除からの復元が可能です。詳細については、「バージョニング」と「バージョニングの使用」を参照してください。	2010 年 2 月 8 日
新しくサポートされるリージョン	Amazon S3 で米国西部 (北カリフォルニア) リージョンがサポートされるようになりました。このリージョンへのリクエストのための新しいエンドポイントは、`s3-us-west-1.amazonaws.com` です。詳細については、「バケットとリージョン」を参照してください。	2009 年 12 月 2 日

変更	説明	日付
AWS SDK for .NET	AWS では、REST や SOAP の代わりに、.NET 言語固有の API オペレーションを使用してアプリケーションを構築することを好むソフトウェアデベロッパー向けに、ライブラリ、サンプルコード、チュートリアル、その他のリソースを提供するようになりました。これらのライブラリはリクエスト認証、リクエストの再試行、エラー処理などの基本機能 (REST または SOAP API に含まれない) を提供しているため、簡単に開始できます。言語固有のライブラリとリソースの詳細については、「Amazon S3リファレンス」の「AWS SDK を使用した Amazon S3 での開発」を参照してください。	2009 年 11 月 11 日