S3

概要

オブジェクトストレージ

オブジェクト形式でデータを保存

安価且つ高い耐久性をもつ

Sinple Strage Service（S3）

特徴

高い耐久性

安価なストレージ　１GB　＝　2.5円　月額

スケーラブルで安定した性能

暗号化可能

データ保存形式

バケット

フォルダ的な扱い

オブジェクト

バケット下に保存される

各オブジェクトにURLが付与される

データサイズ

０KB~5TB

オブジェクト構成

Key　主キー

Value　データそのもの

バージョンID　バージョン管理用

メタデータ

サブリソース

バケット作成はリージョンに配置

その下にオブジェクトがある

ストレージ

STANDARD　標準的なやつ

STANDARD-IA 低頻度アクセスストレージ(IA)

One-Zone-IA　アクセス頻度が低い　必要に応じて取り出すデータ向け

複数AZにまたがらない構成

RRS 非推奨ストレージ　耐久性低い　値段も高い

Amazon Glacier 最安のアーカイブストレージ

中長期データ保存用　あまり使わないデータ

ボールとロックでデータを保持

S3　Intelligent teiring

高頻度アクセス層にデフォルトでは保存

低頻度アクセスのもの(30d)を自動的に低頻度アクセス層に移動する

アクセス後は高頻度アクセスに戻る

アクセス頻度が分からない頻度のものも最低コストで実現可能

アクセス管理

IAMポリシー

S3の操作権限を設定

バケットポリシー

S3内の各バケットに対して細かい設定する

高度なアクセス管理(IPアドレスなど)が可能

JSON形式

ACL

XML設定

オブジェクトに対して管理

署名付きURL

一時的にIAMユーザ以外に見せるときなどに使う

インターネットからパブリックアクセス可能

パブリックアクセス権限

デフォルトオフ設定

S3の暗号化

SSE-S3 S3に入れた後S3側で暗号化

ユーザが意識する必要なし

SSE-KMS 別サービスで鍵を作成

クライアント独自の暗号化も可能

SSE-C SDKなどを介して自分で鍵を作れる

アプリケーション上で構築するなど応用的な技術

CSE S3に送信前に暗号化する

KMSで作成したキーも使える

SSE　サーバサイド暗号化　CSE　カスタマーサイド暗号化

S3アクセスポイント

アクセスポイントの作成

アクセス制限設定

ＶＰＣアクセス制限設定

アクセス管理の実行

Ｓ３アクセスアナライザー

不正なアクセスが発生していないかアクセスポリシーを監視する

バケットポリシー、ＡＣＬのモニタリング

バケットのアクセス状況を確認できる

アクセスポリシーが間違っていないか確認もできる

ライフサイクル管理機能

効率的なデータ保存が可能になる

アーカイブや安価な場所への移動を自動化できる

レプリケーション

デフォルトの複数ＡＺだけでなく、リージョンに跨いでも冗長構成が出来る

データの同期がリージョン間をまたいでできる

バージョン管理をして同期していく

トリガー：オブジェクト作成、更新、削除

バージョン管理

誤操作でデータ削除などが発生してもバージョンから復元できる

データ復活！！！！

データ保護を強化していく

データの容量を食うデメリットがあるのでライフサイクル管理で古いバージ

ョンを削除していく対応をとること

バックアップ

アーカイブ

ライフサイクル管理によりGlacierに移動させる

リストア

S3の分析

アクセスパターンの簡易可視化

CSV出力可能

バケット内の分析を実施

S3のイベント通知

SNS

SQS

Lambdaに通知設定が可能

データ解析

S3 Select　 Ｓ３内部にある簡易検索機能

Amazon　Athena　 外部サービス

機械学習による推論も可能

S3のデータ分析に使う

Amazon　Macie 機密データ検出や調査

コンプライアンスチェックなどに使う

Amazon　Redshift　Spectrum　Redshiftから直接クエリを実行できる

CORS

クロスオリジンリソースシェアリング

マルチパートアップロード

大容量オブジェクトをいくつかにわけてアップロードする機能

バッチオペレーション

大量データに対して一括処理を実行することが可能

ジョブとマニュフェストがある

用途

コンテンツ配信　保管

ログ・バッチを保管する場所

バックアップ/ディザスタリカバリ

WEBの性的なホスティング　WEBサイトとして機能させる

データレイク

IoTなどを使う際のデータ蓄積　 RedshiftとＳ３を組み合わせて使う

C:\Users\miyak>aws s3 cp --recursive s3://udemy-test-20211217 s3://udemy-aws-replication-test-20211215

S3バケット内にあるもともとのデータコピー

レプリケーションルールはお互いに作成しないと共有が出来ない

出来ると同じバケットをリージョンを跨いで共有が出来る

AWS　Storage Gateway

オンプレ側からS3の利点を生かした運用が出来る

Storage Gatewayタイプ

ファイルゲートウェイ

オブジェクトとして格納

S3の利点を全部生かせる

ボリュームゲートウェイ

SnapshotとしてS3上に取得

Disaster Recoveryを実現

長期のバックアップとして利用

テープゲートウェイ

仮想テープライブラリ

VTL　Virtual Tape Library

低コストで運用可能

S3　Transfer　Acceleration

世界中からアップロードされるときに使うと効果的に早いやり取りができる

Snowball

物理ストレージデバイス

ＡＷＳから借りる

物理的に格納してデータセンターへもっていってもらう

Glacier

バックアップ保存用の安価なストレージ

耐久性はS3と同じ　速度が遅い

40TBまでのサイズ

オブジェクト単位はアーカイブ

ボールト≒バケット

アーカイブ≒オブジェクト

AES256　暗号化手法　S3と同じ

アップロード操作はできない

CLIやプログラムでアップロード実行可能

ジョブ

Glacier　Selectクエリを実行したりアーカイブを取得したりする実行単位

データを一時的にアーカイブして暫く経ったらボールトに保存

アクセス管理

IAMポリシー

ボールトポリシー≒バケットポリシー

データ取得ポリシー　 データ取り出しに対して制限できる

例）無料枠超過しないように

コスト管理

ボールトロックポリシー　ボールトの変更禁止

コンプライアンス強固になる

署名

Glacierコスト

保存はS3より安い

取り出しは高い　リクエストでも金とる