aws

Panduan Pengguna

Aplikasi Cost Profiler

Aplikasi Cost Profiler: Panduan Pengguna

Table of Contents

AWS Profiler Biaya Aplikasi akan dihentikan pada 30 September 2024 dan tidak lagi menerima pelanggan baru.

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.

ApaAWSAplikasi Cost Profiler?

AWSAplikasi Biaya Profiler membantu Anda memisahkanAWSpenagihan dan biaya oleh penyewa layanan Anda. SEBUAHpenyewabisa menjadi pengguna, sekelompok pengguna, atau proyek.

SEBUAHsumber dayaadalah entitas yang dapat digunakan oleh penggunaAWS, misalnya Amazon Elastic Compute Cloud (Amazon EC2). Pastikan bahwa Anda dapat mengidentifikasi penggunaan sumber daya Anda oleh penyewa yang Anda pilih.

KhasAWSpenggunaan sumber daya mencakup layanan bersama yang mendukung beberapa penyewa dalam organisasi Anda. Sumber daya tertentu menggunakan dimensi berbasis waktu. Untuk mendapatkan informasi biaya dan penagihan oleh penyewa daripada penggunaan per jam untuk sumber daya, Anda dapat mengintegrasikan sumber daya Anda dengan Application Cost Profiler. Dengan pendekatan granular ini, Anda dapat memahami bagaimanaAWSsumber daya dikonsumsi di seluruh solusi perangkat lunak bersama.

Sumber daya berikut yang dapat menggunakan dimensi berbasis waktu atau penggunaan per jam diaktifkan untuk Application Cost Profiler:

- Instans Amazon EC2 (hanya berdasarkan permintaan dan instans spot)
- Antrean Amazon Simple Queue Service (Amazon SQS)
- Topik Amazon Simple Notification Service (Amazon SNS)
- Amazon DynamoDB membaca dan menulis

> **Note**
>
> Penggunaan Amazon SQS, Amazon SNS, dan DynamoDB tidak dikenai biaya berdasarkan waktu, tidak seperti sebagian besar sumber daya. Dalam kasus mereka, penggunaan selama satu jam (misalnya, sejumlah membaca dan menulis di DynamoDB), dikategorikan berdasarkan persentase jam yang Anda alokasikan untuk penyewa yang berbeda, terlepas dari kapan membaca atau menulis terjadi selama satu jam.

Anda mengintegrasikan layanan Anda dengan Application Cost Profiler dalam tiga langkah:

1. Aktifkan laporan- Langkah ini mendefinisikan apa yang Anda inginkan output akhir Anda terlihat seperti.

2. Kirim data penggunaan penyewa ke Application Cost Profiler— Langkah ini memerlukan kode dalam layanan Anda untuk membuat data penggunaan yang menghubungkan penyewa dengan waktu mereka menggunakan sumber daya Anda, dan kemudian mengirim data penggunaan ke Application Cost Profiler.
3. Dapatkan laporan— Aplikasi Cost Profiler memberikan laporan pada irama yang Anda tentukan dalam konfigurasi laporan Anda. Laporan menunjukkan biaya yang terkait dengan penggunaan masing-masing penyewa, memberi Anda tampilan terperinci tentang penagihan Anda.

Untuk informasi selengkapnya tentang langkah-langkahnya, lihatMemulai.

Memulai dengan Profiler Biaya Aplikasi

AWS Profiler Biaya Aplikasi membantu Anda mendapatkan informasi biaya tentang AWS sumber daya Anda dengan melaporkan penggunaan sumber daya oleh penyewa, bukan untuk sumber daya secara keseluruhan. Penyewa dapat berupa pengguna, sekelompok pengguna, atau proyek. Pastikan bahwa Anda dapat mengidentifikasi penggunaan sumber daya Anda oleh penyewa yang Anda pilih. Untuk mendapatkan laporan biaya tentang penggunaan penyewa, Anda mengonfigurasi laporan dan mengirim data penggunaan ke Profiler Biaya Aplikasi. Bagian ini membahas prasyarat yang harus Anda selesaikan sebelum menggunakan Application Cost Profiler.

Topik

Mendaftar untuk Akun AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka https://portal.aws.amazon.com/billing/signup.
2. Ikuti petunjuk online.

   Bagian dari prosedur pendaftaran melibatkan tindakan menerima panggilan telepon dan memasukkan kode verifikasi di keypad telepon.

   Saat Anda mendaftar untuk sebuah Akun AWS, sebuah Pengguna root akun AWSdibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan tugas yang memerlukan akses pengguna root.

AWS mengirimi Anda email konfirmasi setelah proses pendaftaran selesai. Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan mengunjungi https://aws.amazon.com/ dan memilih Akun Saya.

Buat pengguna dengan akses administratif

Setelah Anda mendaftar Akun AWS, amankan Pengguna root akun AWS, aktifkan AWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Amankan Anda Pengguna root akun AWS

1. Masuk ke AWS Management Consolesebagai pemilik akun dengan memilih pengguna Root dan memasukkan alamat Akun AWS email Anda. Di laman berikutnya, masukkan kata sandi.

   Untuk bantuan masuk dengan menggunakan pengguna root, lihat Masuk sebagai pengguna root di AWS Sign-In Panduan Pengguna.
2. Mengaktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

   Untuk petunjuk, lihat Mengaktifkan perangkat MFA virtual untuk pengguna Akun AWS root (konsol) Anda di Panduan Pengguna IAM.

Buat pengguna dengan akses administratif

1. Aktifkan Pusat Identitas IAM.

   Untuk mendapatkan petunjuk, silakan lihat Mengaktifkan AWS IAM Identity Center di Panduan Pengguna AWS IAM Identity Center .
2. Di Pusat Identitas IAM, berikan akses administratif ke pengguna.

   Untuk tutorial tentang menggunakan Direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat Mengkonfigurasi akses pengguna dengan default Direktori Pusat Identitas IAM di Panduan AWS IAM Identity Center Pengguna.

Masuk sebagai pengguna dengan akses administratif

- Untuk masuk dengan pengguna Pusat Identitas IAM, gunakan URL masuk yang dikirim ke alamat email saat Anda membuat pengguna Pusat Identitas IAM.

Untuk bantuan masuk menggunakan pengguna Pusat Identitas IAM, lihat Masuk ke portal AWS akses di Panduan AWS Sign-In Pengguna.

Tetapkan akses ke pengguna tambahan

1. Di Pusat Identitas IAM, buat set izin yang mengikuti praktik terbaik menerapkan izin hak istimewa paling sedikit.

   Untuk petunjuknya, lihat Membuat set izin di Panduan AWS IAM Identity Center Pengguna.
2. Tetapkan pengguna ke grup, lalu tetapkan akses masuk tunggal ke grup.

   Untuk petunjuk, lihat Menambahkan grup di Panduan AWS IAM Identity Center Pengguna.

Memberikan akses programatis

Pengguna membutuhkan akses terprogram jika mereka ingin berinteraksi dengan AWS luar. AWS Management Console Cara untuk memberikan akses terprogram tergantung pada jenis pengguna yang mengakses AWS.

Untuk memberi pengguna akses programatis, pilih salah satu opsi berikut.

Pengguna mana yang membutuhkan akses programatis?	Untuk	Oleh
Identitas tenaga kerja (Pengguna yang dikelola di Pusat Identitas IAM)	Gunakan kredenal sementara untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDK, atau API. AWS	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. • Untuk AWS CLI, lihat Mengkonfigurasi yang akan AWS CLI digunakan AWS IAM Identity Center dalam Panduan AWS Command Line Interface Pengguna. • Untuk AWS SDK, alat, dan AWS API, lihat autentika

Pengguna mana yang membutuhkan akses programatis?	Untuk	Oleh
		si Pusat Identitas IAM di Panduan Referensi AWS SDK dan Alat.
IAM	Gunakan kredenal sementara untuk menandatangani permintaan terprogram ke AWS CLI, AWS SDK, atau API. AWS	Mengikuti petunjuk dalam Menggunakan kredensil sementara dengan AWS sumber daya di Panduan Pengguna IAM.
IAM	(Tidak direkomendasikan) Gunakan kredensil jangka panjang untuk menandata ngani permintaan terprogram ke AWS CLI, AWS SDK, atau API. AWS	Mengikuti petunjuk untuk antarmuka yang ingin Anda gunakan. • Untuk mengetahui AWS CLI, lihat Mengautentikasi menggunakan kredensil pengguna IAM di Panduan Pengguna.AWS Command Line Interface • Untuk AWS SDK dan alat bantu, lihat Mengautentikasi menggunakan kredensil jangka panjang di Panduan Referensi AWS SDK dan Alat. • Untuk AWS API, lihat Mengelola kunci akses untuk pengguna IAM di Panduan Pengguna IAM.

Prasyarat khusus Profiler Biaya Aplikasi

Sebelum Anda memulai dengan Application Cost Profiler, Anda harus menyelesaikan prasyarat berikut:

- Aktifkan Cost Explorer

  Aktifkan AWS Cost Explorer untuk AWS akun Anda. Menyiapkan akun dengan Cost Explorer dapat memakan waktu hingga 24 jam. Anda harus menyelesaikan penyiapan Cost Explorer sebelum Application Cost Profiler dapat menghasilkan laporan harian dan bulanan Anda.

  Untuk informasi selengkapnya, lihat Mengaktifkan Cost Explorer di Panduan AWS Billing and Cost Management Pengguna.

- Buat ember S3

  Buat setidaknya dua bucket Amazon Simple Storage Service (Amazon S3). Profiler Biaya Aplikasi menggunakan satu bucket S3 untuk memberikan laporan kepada Anda. Anda menggunakan bucket S3 lainnya untuk mengunggah data penggunaan ke Application Cost Profiler. Biasanya, Anda hanya memerlukan satu bucket S3 untuk mengunggah data penggunaan. Namun, Anda mungkin ingin memiliki lebih dari satu bucket S3 sehingga Anda dapat menyimpan penggunaan untuk layanan yang berbeda di bucket S3 terpisah dengan izin yang berbeda, jika diperlukan untuk keamanan Anda. Anda harus memberikan izin Application Cost Profiler ke bucket S3 ini.

  Untuk informasi selengkapnya tentang menyiapkan bucket Amazon S3 untuk Application Cost Profiler, lihat. Menyiapkan bucket Amazon S3 untuk Profiler Biaya Aplikasi

- Aktifkan tag

  Untuk melaporkan penggunaan berdasarkan tag, bukan berdasarkan sumber daya, Anda harus mengaktifkan tag tersebut di AWS Billing and Cost Management konsol.

  Untuk informasi selengkapnya tentang mengaktifkan tag AWS yang dihasilkan, lihat Mengaktifkan Tag Alokasi Biaya AWS yang Dihasilkan di Panduan Pengguna.AWS Billing and Cost Management Untuk informasi selengkapnya tentang mengaktifkan tag yang ditentukan pengguna, lihat Mengaktifkan Tag Alokasi Biaya yang Ditentukan Pengguna di Panduan Pengguna.AWS Billing and Cost Management

Langkah selanjutnya

Setelah Anda menyelesaikan prasyarat ini, Anda dapat:

- Konfigurasikan laporan Anda dan kirim data penggunaan ke Application Cost Profiler. Untuk informasi selengkapnya, lihat Membuat laporan Anda.
- Dapatkan dan analisis laporan yang Anda hasilkan. Untuk informasi selengkapnya, lihat Laporan Cost Profiler Aplikasi.

Menyiapkan bucket Amazon S3 untuk Profiler Biaya Aplikasi

Untuk mengirim data penggunaan ke dan menerima laporan dariAWSProfiler Biaya, Anda harus memiliki setidaknya satu ember Amazon Simple Storage Service (Amazon S3) di AndaAkun AWSuntuk menyimpan data dan satu bucket S3 untuk menerima laporan Anda.

> **Note**
>
> Untuk penggunaAWS Organizations, ember Amazon S3 dapat berupa di akun manajemen atau di akun anggota individu. Data dalam ember S3 yang dimiliki oleh akun manajemen dapat digunakan untuk menghasilkan laporan untuk seluruh organisasi. Dalam akun anggota individu, data dalam bucket S3 hanya dapat digunakan untuk menghasilkan laporan untuk akun anggota tersebut.

Ember S3 yang Anda buat dimiliki olehAkun AWSbahwa Anda membuat mereka di. Bucket S3 ditagih dengan tarif standar Amazon S3. Untuk informasi selengkapnya tentang cara membuat bucket Amazon S3, lihatMembuat bucketdiPanduan Pengguna Amazon Simple Storage.

Agar Profiler Biaya Aplikasi menggunakan ember S3, Anda harus melampirkan kebijakan ke ember yang memberikan izin Application Cost Profiler untuk membaca dan/atau menulis ke bucket. Jika Anda mengubah kebijakan setelah laporan diatur, Anda dapat mencegah Aplikasi Cost Profiler tidak dapat membaca data penggunaan Anda atau menyampaikan laporan Anda.

Topik berikut menunjukkan cara mengatur izin pada bucket Amazon S3 Anda setelah Anda membuatnya. Selain kemampuan untuk membaca dan menulis objek, jika Anda mengenkripsi ember, Aplikasi Biaya Profiler harus memiliki akses keAWS Key Management Service(AWS KMS) kunci untuk setiap ember.

Topik

Memberikan akses Profiler Biaya Aplikasi ke ember S3 pengiriman laporan Anda

Bucket S3 yang Anda konfigurasikan untuk Application Cost Profiler untuk menyampaikan laporan Anda harus memiliki kebijakan yang dilampirkan yang memungkinkan Application Cost Profiler untuk membuat objek laporan. Selain itu, bucket S3 harus dikonfigurasi untuk mengaktifkan enkripsi.

> **Note**
>
> Saat Anda membuat bucket Anda, Anda harus memilih untuk mengenkripsi. Anda dapat memilih untuk mengenkripsi bucket Anda dengan kunci yang dikelola Amazon S3 (SSE-S3) atau dengan kunci Anda sendiri yang dikelola olehAWS KMS(SSE-KMS). Jika Anda telah membuat bucket Anda tanpa enkripsi, Anda harus mengedit bucket Anda untuk menambahkan enkripsi.

Untuk memberikan akses Application Cost Profiler ke bucket S3 pengiriman laporan Anda

1. Pergi keKonsol Amazon S3dan masuk
2. PilihBucketdari navigasi kiri, dan kemudian pilih bucket Anda dari daftar.
3. PilihIzintab, kemudian, di sampingKebijakan bucket, pilihMengedit.
4. DiKebijakanbagian, masukkan kebijakan berikut. Ganti*<bucket_name>*dengan nama ember Anda, dan*<Akun AWS>*dengan IDAkun AWS.

```
{
      "Version":"2008-10-17",
      "Statement":[
        {
          "Effect":"Allow",
          "Principal":{
            "Service":"application-cost-profiler.amazonaws.com"
          },
```

```
            "Action":[
              "s3:PutObject*",
              "s3:GetEncryptionConfiguration"
            ],
            "Resource": [
              "arn:aws:s3:::<bucket-name>",
              "arn:aws:s3:::<bucket-name>/*"
            ],
            "Condition": {
              "StringEquals": {
                "aws:SourceAccount": "<Akun AWS>"
              },
              "ArnEquals": {
                "aws:SourceArn": "arn:aws:application-cost-profiler:us-east-1:<Akun
AWS>:*"
              }
            }
          }
        ]
    }
```

Dalam kebijakan ini Anda memberikan prinsipal layanan Application Cost Profiler (`application-cost-profiler.amazonaws.com`) akses untuk mengirimkan laporan ke bucket yang ditentukan. Ini melakukan ini atas nama Anda, dan termasuk header dengan AndaAkun AWSdan ARN khusus untuk ember pengiriman laporan Anda. Untuk memastikan bahwa Application Cost Profiler mengakses bucket Anda hanya ketika bertindak atas nama Anda,`Condition`memeriksa header tersebut.

5. MemiilihSimpan perubahanuntuk menyimpan kebijakan Anda, melekat pada ember Anda.

   Jika Anda telah membuat bucket Anda menggunakan enkripsi SSE-S3, maka Anda sudah selesai. Jika Anda menggunakan enkripsi SSE-KMS, maka langkah-langkah berikut diperlukan untuk memberikan akses Application Cost Profiler ke bucket Anda.

6. (Opsional) PilihPropertitab untuk ember Anda, dan di bawahEnkripsi Default, pilih Amazon Resource Name (ARN) untuk AndaAWS KMSkunci. Tindakan ini menampilkanAWS Key Management Servicekonsol dan menunjukkan kunci Anda.

7. (Opsional) Tambahkan kebijakan untuk memberikan akses Profiler Biaya Aplikasi keAWS KMSkunci. Untuk petunjuk tentang cara menambahkan kebijakan ini, lihat[Memberikan akses Profiler Biaya Aplikasi ke bucket S3 terenkripsi SSE-KMS](#).

Memberikan Aplikasi Cost Profiler akses ke data penggunaan Anda S3 bucket

Bucket S3 yang Anda konfigurasikan untuk Application Cost Profiler untuk membaca data penggunaan Anda harus memiliki kebijakan yang dilampirkan untuk memungkinkan Application Cost Profiler membaca objek data penggunaan.

> **Note**
>
> Dengan memberikan akses Application Cost Profiler ke data penggunaan Anda, Anda setuju bahwa kami dapat menyalin sementara objek data penggunaan tersebut ke AS Timur (Virginia Utara)Wilayah AWSsaat memproses laporan. Data ini akan disimpan di Wilayah AS Timur (N. Virginia) sampai generasi laporan bulanan selesai.

Untuk memberikan akses Application Cost Profiler ke data penggunaan Anda S3 bucket

1. Pergi keKonsol Amazon S3dan masuk
2. PilihBucketdari navigasi kiri, dan kemudian pilih bucket Anda dari daftar.
3. PilihIzintab, kemudian, di sampingKebijakan bucket, pilihMengedit.
4. DiKebijakanbagian, masukkan kebijakan berikut. Ganti*<bucket-name>*dengan nama ember Anda, dan*<Akun AWS>*dengan IDAkun AWS.

```
{
      "Version":"2008-10-17",
      "Statement":[
        {
          "Effect":"Allow",
          "Principal":{
            "Service":"application-cost-profiler.amazonaws.com"
          },
          "Action":[
            "s3:GetObject*"
          ],
          "Resource": [
            "arn:aws:s3:::<bucket-name>",
            "arn:aws:s3:::<bucket-name>/*"
          ],
          "Condition": {
```

```
            "StringEquals": {
              "aws:SourceAccount": "<Akun AWS>"
            },
            "ArnEquals": {
              "aws:SourceArn": "arn:aws:application-cost-profiler:us-east-1:<Akun
AWS>:*"
            }
          }
        }
      ]
    }
```

Dalam kebijakan ini Anda memberikan prinsipal layanan Application Cost Profiler (`application-cost-profiler.amazonaws.com`) akses untuk mendapatkan data dari ember yang ditentukan. Ini melakukan ini atas nama Anda, dan termasuk header dengan AndaAkun AWSdan ARN khusus untuk bucket penggunaan Anda. Untuk memastikan bahwa Application Cost Profiler mengakses bucket Anda hanya ketika bertindak atas nama Anda,`Condition`memeriksa header tersebut.

5. MemiilihSimpan perubahanuntuk menyimpan kebijakan Anda, melekat pada ember Anda.

Jika bucket Anda dienkripsiAWS KMSkunci terkelola, maka Anda harus memberikan akses Application Cost Profiler ke bucket Anda dengan mengikuti prosedur di bagian berikutnya.

Memberikan akses Profiler Biaya Aplikasi ke bucket S3 terenkripsi SSE-KMS

Jika Anda mengenkripsi bucket S3 yang Anda konfigurasikan untuk Application Cost Profiler (diperlukan untuk ember laporan) dengan kunci yang tersimpanAWS KMS(SSE-KMS), Anda juga harus memberikan izin untuk Application Cost Profiler untuk mendekripsi mereka. Anda melakukan ini dengan memberikan akses keAWS KMSkunci yang digunakan untuk mengenkripsi data.

> **Note**
>
> Jika bucket Anda dienkripsi dengan kunci terkelola Amazon S3, maka Anda tidak perlu menyelesaikan prosedur ini.

Memberikan akses Profiler Biaya AplikasiAWS KMSuntuk ember S3 terenkripsi

1. Pergi keAWS KMSkonsoldan masuk
2. PilihKunci yang dikelola pelanggandari navigasi kiri, dan kemudian pilih kunci yang digunakan untuk mengenkripsi bucket Anda dari daftar.
3. PilihBeralih ke Tampilan Kebijakan, lalu pilihMengedit.
4. DiKebijakanbagian, masukkan pernyataan kebijakan berikut.

```
{
  "Effect": "Allow",
  "Principal": {
      "Service": "application-cost-profiler.amazonaws.com"
  },
  "Action": [
      "kms:Decrypt",
      "kms:GenerateDataKey*"
  ],
  "Resource": "*",
        "Condition": {
          "StringEquals": {
            "aws:SourceAccount": "<Akun AWS>"
          },
          "ArnEquals": {
            "aws:SourceArn": "arn:aws:application-cost-profiler:us-east-1:<Akun
AWS>:*"
          }
 }
```

5. MemiilihSimpan perubahanuntuk menyimpan kebijakan Anda, melekat pada kunci Anda.
6. Ulangi untuk setiap kunci yang mengenkripsi bucket S3 yang perlu diakses Application Cost Profiler.

> **Note**
>
> Data disalin dari bucket S3 Anda yang diimpor ke dalam bucket yang dikelola Application Cost Profiler (yang dienkripsi). Jika Anda mencabut akses ke kunci, Application Cost Profiler tidak dapat mengambil objek baru dari bucket. Namun, setiap data yang sudah diimpor masih dapat digunakan untuk menghasilkan laporan.

Membuat laporan Anda

Setelah memenuhi prasyarat, Anda siap untuk mengkonfigurasi laporan untuk AndaAkun AWS dan mengirim data penggunaan Anda keAWS Application Cost Profiler. Bagian ini menjelaskan cara mengkonfigurasi laporan dan cara mengirim data penggunaan ke Application Cost Profiler.

Mengonfigurasi laporan Cost Profiler Aplikasi Anda

Prosedur berikut menunjukkan cara mengonfigurasi laporan yang ingin Anda hasilkan berdasarkan tanggal penggunaan Anda. Anda mengonfigurasi detail seperti frekuensi laporan yang dihasilkan.

> **Note**
>
> Jika AndaAkun AWS adalah bagian dariAWS organisasi, Anda dapat mengonfigurasi laporan menggunakan akun manajemen atau akun anggota individual. Laporan yang dikonfigurasi untuk akun individual hanya berisi data untuk akun tersebut. Laporan yang dikonfigurasi menggunakan akun manajemen dapat mencakup data untuk seluruh organisasi.
> Bucket Amazon S3 yang digunakan untuk keluaran laporan harus termasuk dalam akun yang membuat konfigurasi laporan.

Cara mengonfigurasi laporan Profiler Biaya Aplikasi

1. Buka peramban web dan masuk ke konsol Cost Profiler Aplikasi.
2. Pilih Mulai sekarang untuk mengonfigurasi atau memodifikasi laporan.
3. Masukkan Nama Laporan dan Deskripsi Laporan untuk laporan Anda.
4. Masukkan nama bucket S3 Anda di kolom nama bucket Enter S3 dan masukkan awalan S3 di bidang awalan Enter S3. Untuk informasi selengkapnya tentang membuat bucket S3 dan memberikan izin Application Cost Profiler, lihatMenyiapkan bucket Amazon S3 untuk Profiler Biaya Aplikasi.
5. Pilih opsi yang Anda inginkan agar laporan Anda miliki:

   - Frekuensi Waktu - Pilih apakah laporan dihasilkan pada irama Harian atau Bulanan, atau Keduanya.
   - Format Output Laporkan — Pilih jenis file yang akan dibuat dalam bucket Amazon S3 Anda. Jika Anda memilih CSV, Application Cost Profiler membuat file teks nilai yang dipisahkan

koma dengan kompresi gzip untuk laporan. Jika Anda memilih Parket, file Parket dihasilkan untuk laporan.

6. Pilih Konfigurasi untuk menyimpan konfigurasi laporan Anda.

> **Note**
>
> Anda juga dapat menggunakan AWSApplication Cost Profiler API untuk mengonfigurasi laporan.

Verifikasi pengaturan laporan dengan memilih Mulai sekarang untuk melihat konfigurasi laporan saat ini.

> **Note**
>
> Anda hanya dapat mengonfigurasi satu laporan. Kembali ke halaman konfigurasi akan mengedit laporan Anda yang ada.

Setelah Anda mengonfigurasi laporan, konsumsi data diaktifkan. Anda dapat mengintegrasikan layanan Anda dengan Application Cost Profiler untuk menyediakan data penggunaan untuk sumber daya Anda.

Melaporkan data penggunaan penyewa dari layanan Anda

Setelah mengonfigurasi laporan, Anda siap mengirim data penggunaan penyewa dari sumber daya atau layanan di akun Anda. Anda harus memberi tahu Profiler Biaya Aplikasi saat sumber daya Anda digunakan untuk penyewa tertentu. Misalnya, jika layanan Anda menerima panggilan API dari penyewa yang berbeda, Anda merekam waktu mulai dan berakhir untuk setiap penyewa saat Anda memulai dan mengakhiri panggilan API dari penyewa tersebut. Aplikasi Biaya Profiler menggunakan data tersebut untuk menghasilkan laporan tentang biaya layanan Anda, dengan jumlah waktu yang dihabiskan untuk bekerja untuk setiap penyewa.

Untuk memberikan data Cost Profiler Aplikasi, Anda melakukan hal berikut:

- Siapkan data penggunaan sumber daya - Buat tabel yang menjelaskan kapan sumber daya digunakan untuk penyewa tertentu.

- Unggah data penggunaan — Unggah tabel ke bucket Amazon S3 yang telah Anda berikan izin Application Cost Profiler untuk mengakses.
- Data penggunaan impor - Panggil operasi`ImportApplicationUsage` API untuk memberi tahu Application Cost Profiler bahwa data siap diproses.

Bagian berikut menjelaskan masing-masing langkah ini secara lebih mendetail.

Topik

Langkah 1: Mempersiapkan data penggunaan sumber daya Anda

Sebagai sumber daya yang digunakan dalam layanan Anda, Anda melacak penyewa mana yang menggunakannya. Rekam data ini ke dalam tabel yang nantinya dapat Anda unggah untuk Profiler Biaya Aplikasi untuk diimpor. Setiap baris dalam tabel menggambarkan sumber daya, penyewa yang menggunakan sumber daya, dan waktu mulai dan akhir penggunaan itu. Contoh sumber daya adalah instans Amazon Elastic Compute Cloud (Amazon EC2) yang sedang digunakan.

Langkah ini mengharuskan Anda mengintegrasikan kode ke layanan Anda untuk menampilkan informasi yang benar tentang penggunaan.

Bidang yang ada dalam tabel penggunaan sumber daya tercantum dalam tabel berikut.

Bidang	Deskripsi
ApplicationId	Mengidentifikasi aplikasi atau produk dalam sistem Anda yang sedang digunakan. Mendefinisikan ruang lingkup metadata penyewa.
TenantId	Pengenal dalam sistem Anda untuk penyewa yang mengkonsumsi sumber daya yang ditentukan. Aplikasi Biaya Profiler agregat ke tingkat ini dalam ApplicationId.

Bidang	Deskripsi
TenantDesc	(Opsional) Data tambahan tentang penyewa untuk pelaporan tambahan Anda sendiri.
UsageAccountId	Akun tempat sumber daya berjalan (penting untuk akun yang merupakan bagian dari organisasi).
StartTime	Stempel waktu (dalam milidetik dan mikrodetik) dari Epoch, di UTC. Menunjukkan waktu mulai periode untuk penggunaan oleh penyewa yang ditentukan.
EndTime	Stempel waktu (dalam milidetik dan mikrodetik) dari Epoch, di UTC. Menunjukkan waktu akhir periode untuk penggunaan oleh penyewa yang ditentukan.
ResourceId	Amazon Resource Name (ARN) untuk sumber daya yang digunakan.
Nama	(Opsional) Sebagai alternatif untuk menentuka n ResourceId, Anda dapat menentukan tag sumber daya Nama untuk mengaitkan biaya ke sekumpulan sumber daya (bidang harus menyertakan nilai yang ingin Anda gunakan untuk tag Nama). Tag sumber daya diaktifka n sebagai bagian dari Cost and Usage Report Anda. Untuk informasi selengkapnya tentang tag sumber daya, lihat Rincian tag sumber daya di Panduan Pengguna Laporan Biaya dan Penggunaan.

Output harus dalam file comma-separated values (.csv) yang menyertakan baris judul, seperti yang ditunjukkan dalam contoh berikut.

```
ApplicationId,TenantId,TenantDesc,UsageAccountId,StartTime,EndTime,ResourceId
```

```
MyApp,Tenant1,,123456789012,1613681437032.9001,1613681437041.5312,arn:aws:ec2:us-
east-1:123456789012:instance/1234-abcd-example-1234
MyApp,Tenant2,,123456789012,1613681245531.4426,1613681245551.1323,arn:aws:ec2:us-
east-1:123456789012:instance/1234-abcd-example-1234
MyApp,Tenant1,,123456789012,1613681904815.3381,1613681904930.0972,arn:aws:ec2:us-
east-1:123456789012:instance/1234-abcd-example-1234
MyApp,Tenant2,,123456789012,1613681904765.1956,1613681904946.574,arn:aws:ec2:us-
east-1:123456789012:instance/1234-abcd-example-1234
```

Simpan data sebagai file, dengan ekstensi.csv (atau .csv.gzip jika dikompresi dengan gzip). Saat Anda mengunggah data ini ke Application Cost Profiler, setiap kali potongan ditetapkan ke penyewa terkait. Dalam contoh ini, laporan tersebut menyertakan potongan waktu biaya instans Amazon EC2 untuk penyewa tersebut. Hanya untuk instans Amazon EC2, irisan yang tidak terkait dengan penyewa tertentu ditambahkan ke penyewa yang tidak dikaitkan. Irisan waktu yang tumpang tindih dihitung beberapa kali. Anda bertanggung jawab untuk memastikan bahwa data dalam tabel penggunaan Anda akurat.

> **Note**
>
> File Anda harus mewakili satu jam waktu. Jika sumber daya digunakan selama beberapa jam, akhiri penggunaan pada jam, dan miliki catatan baru di file berikutnya yang dimulai pada waktu yang bersamaan.
>
> Anda harus mengirimkan satu file yang berisi data satu jam penuh. Jika beberapa file dikirimkan untuk data jam yang sama, Application Cost Profiler hanya mempertimbangkan data dalam file terbaru.

Misalnya, tabel berikut menunjukkan bagaimana Application Cost Profiler menghitung penggunaan untuk tiga penyewa, lebih dari satu jam (3.600.000 milidetik), berdasarkan potongan waktu yang disediakan.

Penyewa	Irisan waktu yang disediakan	Dihitung persen dari biaya per jam
Penyewa1	1,200.000 ms	33,34%
Penyewa2	600.000 nona	16,66%
<unattributed>		50,00%

Dalam contoh ini, Tenant1 ditugaskan sepertiga jam dan Tenant2 ditugaskan seperenam jam. Setengah jam tersisa (1.800.000 ms) tidak dikaitkan dengan salah satu klien, yaitu 50% dari jam.

Saat ini, sumber daya berikut diaktifkan untuk Application Cost Profiler:

- Instans Amazon EC2 (hanya berdasarkan permintaan dan instans spot)
- Fungsi Lambda (Jika Anda mengirim data untuk fungsi Lambda, Anda harus mengirim ARN Sumber Daya Tidak Berkualifikasi sebagai`ResourceId`.)
- Instans Amazon Elastic Container Service (Amazon ECS)
- Antrean Amazon Simple Queue Service (Amazon SQS)
- Topik Amazon Simple Notification Service (Amazon SNS)
- Amazon DynamoDB membaca dan menulis

> **Note**
>
> Amazon SQS, Amazon SNS, dan penggunaan DynamoDB tidak dikenai waktu, tidak seperti kebanyakan sumber daya. Dalam kasus mereka, penggunaan selama satu jam (misalnya, sejumlah baca dan tulis di DynamoDB), dikategorikan berdasarkan persentase jam yang Anda alokasikan ke penyewa yang berbeda, terlepas dari kapan pembacaan atau penulisan terjadi selama satu jam.

Langkah 2: Mengunggah penggunaan sumber Anda

Setelah Anda memiliki file penggunaan oleh penyewa, unggah file data Anda ke Amazon S3 dan pastikan bahwa Application Cost Profiler memiliki izin untuk mengaksesnya.

Untuk mempelajari selengkapnya tentang membuat bucket S3, lihatPrasyarat khusus Profiler Biaya Aplikasi.

Anda harus memastikan bahwa Application Cost Profiler memiliki akses ke bucket S3 Anda. Ini hanya perlu dilakukan sekali per bucket S3 (Anda dapat menggunakan kembali bucket yang sama untuk mengunggah beberapa file penggunaan). Untuk informasi tentang memberikan akses ke bucket, lihatMemberikan Aplikasi Cost Profiler akses ke data penggunaan Anda S3 bucket. Jika bucket dienkripsi, lihatMemberikan akses Profiler Biaya Aplikasi ke bucket S3 terenkripsi SSE-KMS.

> **Note**
>
> Anda tidak perlu mengenkripsi bucket S3 yang Anda gunakan untuk data penggunaan.

Unggah data Anda ke bucket S3 sebagai file, dengan ekstensi.csv (atau .csv.gzip jika dikompresi dengan gzip), pada interval per jam. Setelah Anda mengunggah file baru, Anda harus memberi tahu Application Cost Profiler bahwa Anda telah mengunggahnya sehingga file tersebut dapat diimpor ke laporan Anda.

> **Note**
>
> Dengan memberikan akses Application Cost Profiler ke data penggunaan Anda, Anda setuju bahwa kami dapat menyalin sementara objek data penggunaan tersebut ke AS Timur (Virginia Utara)Wilayah AWS saat memproses laporan. Objek data ini akan disimpan di Wilayah Timur AS (N. Virginia) sampai pembuatan laporan bulanan selesai.

Langkah 3: Mengimpor data penggunaan ke Aplikasi Biaya Profiler

Setelah Anda mengunggah data penggunaan ke bucket Amazon S3 yang dapat diakses oleh Profiler Biaya Aplikasi, beri tahu Profiler Biaya Aplikasi bahwa data tersebut ada dan untuk mengimpornya ke laporan akhir Anda. Anda melakukan ini dengan menggunakan`ImportApplicationUsage` operasi di Application Cost Profiler API.

Untuk informasi tentangAWS Application Cost Profiler API, termasuk`ImportApplicationUsage` operasi, lihat ReferensiAWS Application Cost Profiler API.

Contoh berikut menunjukkan cara menelepon`ImportApplicationUsage`. Ganti *`teks input dalam tanda kurung`* dengan nilai untuk bucket S3 Anda dan objek yang diunggah.

```
POST /ImportApplicationUsage HTTP/1.1
Content-type: application/json

{
    "sourceS3Location" : {
        "bucket": "<bucket-name>",
        "key": "<object-key>",
        "region": "<region-id>"
```

```
    }
}
```

> **Note**
>
> `region`Parameter hanya diperlukan jika bucket Anda berada diWilayah AWS yang dinonaktifkan secara default. Untuk informasi selengkapnya, lihat MengelolaWilayah AWS di bagian Referensi Umum AWS.

Application Cost Profiler menghasilkan laporan baru pada frekuensi yang Anda minta saat mengonfigurasi laporan, menggunakan data yang Anda impor`ImportApplicationUsage`.

Setelah mengonfigurasi laporan dan mengimpor data penggunaan secara otomatis ke Application Cost Profiler, Anda siap untuk melihat laporan yang dihasilkan. Untuk informasi selengkapnya tentang laporan, lihatLaporan Cost Profiler Aplikasi.

Laporan Cost Profiler Aplikasi

Setelah Anda mengintegrasikan data penggunaan Anda denganAWSAplikasi Biaya Profiler dan mengirimkan data secara per jam, Aplikasi Biaya Profiler secara otomatis menghasilkan laporan Anda.

Laporan dihasilkan baik setiap hari atau bulanan, berdasarkan opsi yang Anda pilih saatmengonfigurasi laporan Anda. Laporan terkirim ke bucket Amazon Simple Storage Service (Amazon S3) yang Anda pilih saat mengonfigurasi laporan.

Laporan harian yang dihasilkan pada hari pertama bulan memiliki data bulan sebelumnya.

Data tersedia dalam laporan Application Cost Profiler

Kolom yang dibuat dalam laporan penggunaan ditunjukkan dalam tabel berikut.

Nama kolom	Deskripsi
PayerAccountId	ID akun manajemen dalam organisasi, atau ID akun jika akun bukan bagian dariAWS Organizations.
UsageAccountId	ID akun untuk akun dengan penggunaan.
LineItemType	Jenis catatan. SelaluUsage.
UsageStartTime	Timestamp (dalam milidetik) dari Epoch, di UTC. Menunjukkan waktu mulai periode untuk penggunaan oleh penyewa yang ditentukan.
UsageEndTime	Timestamp (dalam milidetik) dari Epoch, di UTC. Menunjukkan waktu akhir periode untuk penggunaan oleh penyewa yang ditentukan.
ApplicationIdentifier	ParameterApplicationIdditentukan dalam data penggunaan yang dikirim ke Application Cost Profiler.

Nama kolom	Deskripsi
Tenantidentifier	ParameterTenanTidditentukan dalam data penggunaan yang dikirim ke Application Cost Profiler. Data tanpa catatan dalam data penggunaan dikumpulkanunattributed .
Penyewa Deskripsi	ParameterTenantDesc ditentukan dalam data penggunaan yang dikirim ke Application Cost Profiler.
ProductCode	ParameterAWSproduk yang ditagih (misalnya ,AmazonEC2).
UsageType	Jenis penggunaan yang ditagih (misalnya ,BoxUsage:c5.large).
Operasi	Operasi yang ditagih (misalnya,RunInstances).
ResourceId	ID sumber daya atau Amazon Resource Name (ARN) untuk sumber daya yang ditagih.
ScaleFactor	Jika sumber daya dialokasikan lebih dari satu jam, misalnya, data penggunaan yang dilaporkan sama dengan 2 jam, bukan 1 jam, faktor skala diterapkan untuk membuat total sama dengan jumlah yang ditagih aktual (dalam hal ini, 0.5). Kolom ini melaporkan faktor skala yang digunakan untuk sumber daya tertentu untuk jam itu. Faktor skala selalu lebih besar dari nol (0) dan kurang dari atau sama dengan 1.
TenantAttributionPercent	Persentase penggunaan dikaitkan dengan penyewa yang ditentukan (antara nol (0) dan 1).

Nama kolom	Deskripsi
UsageAmount	Jumlah penggunaan dikaitkan dengan penyewa yang ditentukan.
CurrencyCode	Mata uang yang nilai dan biaya dalam (misalnya,USD).
Laju	Tingkat penagihan untuk penggunaan, per unit.
TenantCost	Total biaya untuk sumber daya untuk penyewa yang ditentukan.
Wilayah	ParameterAWSWilayah sumber daya.
Nama	Jika Anda membuat tag sumber daya untuk sumber daya Anda pada laporan Biaya dan Penggunaan, atau melalui data penggunaan sumber daya, makaNamatag ditampilkan di sini. Untuk informasi selengkapnya tentang tag sumber daya, lihatRincian tag sumber dayadiPanduan Pengguna Laporan Biaya dan Penggunaan.

Berikut ini adalah contoh laporan output untuk satu sumber daya selama dua jam.

```
PayerAccountId,UsageAccountId,LineItemType,UsageStartTime,UsageEndTime,ApplicationIdentifier,Te
123456789012,123456789012,Usage,2021-02-01T00:00:00.000Z,2021-02-01T00:30:00.000Z,Canary,unattr
east-1,test-tag
123456789012,123456789012,Usage,2021-02-01T00:30:00.000Z,2021-02-01T01:00:00.000Z,Canary,Tenant
east-1,test-tag
123456789012,123456789012,Usage,2021-02-01T01:00:00.000Z,2021-02-01T02:00:00.000Z,Canary,Tenant
east-1,test-tag
123456789012,123456789012,Usage,2021-02-01T01:00:00.000Z,2021-02-01T02:00:00.000Z,Canary,Tenant
east-1,test-tag
123456789012,123456789012,Usage,2021-02-01T01:00:00.000Z,2021-02-01T02:00:00.000Z,Canary,Tenant
east-1,test-tag
123456789012,123456789012,Usage,2021-02-01T01:00:00.000Z,2021-02-01T02:00:00.000Z,Canary,Tenant
east-1,test-tag
```

Dalam contoh ini, jam pertama dialokasikan untuk`Tenant1`untuk setengah dari waktu. Setengah jam tetapu`nattributed`. Pada jam kedua, empat penyewa semuanya dialokasikan satu jam penuh. Dalam hal ini, faktor skala skala mereka semua turun sebesar 0,25, dan semuanya dialokasikan seperempat jam. Anda dapat melihat biaya akhir di`TenantCost`kolom.

AWSAplikasi Cost Profiler Quota

Akun AWS Anda memiliki kuota default, yang sebelumnya disebut sebagai batas, untuk setiap layanan AWS. Kecuali dinyatakan lain, masing-masing kuota adalahAWSWilayah khusus. Anda dapat meminta peningkatan untuk beberapa kuota dan kuota lainnya tidak dapat ditingkatkan.

Tabel berikut mencantumkan kuota layanan per akun danAWSTitik akhir wilayah untuk Aplikasi Biaya Profiler.

Kuota layanan

Sumber daya	Nilai default	Deskripsi
Permintaan tarif `PutReportDefinition`	5	Jumlah maksimum`PutReportDefinition` permintaan per detik per akun
Permintaan tarif `UpdateReportDefinition`	5	Jumlah maksimum`UpdateReportDefinition` permintaan per detik per akun
Permintaan tarif `GetReportDefinition`	5	Jumlah maksimum`GetReportDefinition` permintaan per detik per akun
Permintaan tarif `DeleteReportDefinition`	5	Jumlah maksimum`DeleteReportDefinition` permintaan per detik per akun
Permintaan tarif `ListReportDefinitions`	5	Jumlah maksimum`ListReportDefinitions` permintaan per detik per akun

Sumber daya	Nilai default	Deskripsi
Permintaan tarif `ImportApplicationUsage`	5	Jumlah maksimum `ImportApplicationUsage` permintaan per detik per akun
Ukuran maksimum file data penggunaan	10 MB	Ukuran maksimum file data penggunaan per jam.

Titik akhir layanan

Aplikasi Cost Profiler adalah layanan global. Semua panggilan API harus dilakukan ke titik akhir US East (N. Virginia).

- AS Timur (Virginia Utara) – `application-cost-profiler.us-east-1.amazonaws.com`

Keamanan dalamAWSAplikasi Cost Profiler

Keamanan cloud di AWS merupakan prioritas tertinggi. Sebagai pelanggan AWS, Anda akan mendapatkan manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara AWS dan Anda. Model tanggung jawab bersama menjelaskan hal ini sebagai keamanan cloud dan keamanan dalam cloud:

- Keamanan cloud – AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan layanan AWS di Cloud AWS. AWS juga menyediakan layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga menguji dan memverifikasi efektivitas keamanan kami secara berkala sebagai bagian dari Program Kepatuhan AWS. Untuk mempelajari program kepatuhan yang berlaku di Aplikasi Cost Profiler, lihatAWS dalam Lingkup oleh Program Kepatuhan.
- Keamanan dalam cloud – Tanggung jawab Anda ditentukan oleh layanan AWS yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, mencakup kepekaan data Anda, persyaratan perusahaan, serta peraturan perundangan yang berlaku

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakanAWSAplikasi Cost Profiler. Dokumentasi ini juga menunjukkan cara mengonfigurasi Aplikasi Cost Profiler untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga belajar cara menggunakan lainnyaAWSlayanan yang membantu Anda memantau dan mengamankan sumber daya Cost Profiler Aplikasi Anda.

Konten

Perlindungan data dalam Profiler Biaya AWS Aplikasi

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di Profiler Biaya AWS Aplikasi. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi

infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Lihat informasi yang lebih lengkap tentang privasi data dalam Pertanyaan Umum Privasi Data. Lihat informasi tentang perlindungan data di Eropa di pos blog Model Tanggung Jawab Bersama dan GDPR AWS di Blog Keamanan AWS .

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensyal dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan sumber daya. AWS Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi yang lebih lengkap tentang titik akhir FIPS yang tersedia di Standar Pemrosesan Informasi Federal (FIPS) 140-2.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan Application Cost Profiler atau lainnya Layanan AWS menggunakan konsol, API AWS CLI, atau AWS SDK. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

Enkripsi diam

AWS Application Cost Profiler selalu mengenkripsi semua data yang disimpan dalam layanan saat istirahat tanpa memerlukan konfigurasi tambahan. Enkripsi ini otomatis ketika Anda menggunakan Application Cost Profiler.

Untuk bucket Amazon S3 yang Anda berikan, Anda harus mengenkripsi bucket laporan, dan dapat mengenkripsi bucket data penggunaan dan memberikan akses kepada Application Cost Profiler. Untuk informasi selengkapnya, lihat Menyiapkan bucket Amazon S3 untuk Profiler Biaya Aplikasi.

Enkripsi bergerak

AWS Profiler Biaya Aplikasi menggunakan Transport Layer Security (TLS) dan enkripsi sisi klien untuk enkripsi dalam perjalanan. Komunikasi dengan Application Cost Profiler selalu dilakukan melalui HTTPS sehingga data Anda selalu dienkripsi saat transit. Enkripsi ini dikonfigurasi secara default saat Anda menggunakan Application Cost Profiler.

Manajemen identitas dan akses untuk AWS Application Cost Profiler

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya Application Cost Profiler. IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

- Audiens
- Mengautentikasi dengan identitas
- Mengelola akses menggunakan kebijakan
- Bagaimana Profiler Biaya AWS Aplikasi bekerja dengan IAM
- AWS Contoh kebijakan berbasis identitas Profiler Biaya Aplikasi
- Pemecahan Masalah AWS Identitas dan akses Profiler Biaya Aplikasi

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan di Application Cost Profiler.

Pengguna layanan — Jika Anda menggunakan layanan Application Cost Profiler untuk melakukan pekerjaan Anda, maka administrator Anda memberi Anda kredensi dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak fitur Application Cost Profiler untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara akses dikelola dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di Application Cost Profiler, lihatPemecahan Masalah AWS Identitas dan akses Profiler Biaya Aplikasi.

Administrator layanan — Jika Anda bertanggung jawab atas sumber daya Profiler Biaya Aplikasi di perusahaan Anda, Anda mungkin memiliki akses penuh ke Profiler Biaya Aplikasi. Tugas Anda adalah menentukan fitur dan sumber daya Application Cost Profiler mana yang harus diakses pengguna layanan Anda. Kemudian, Anda harus mengirimkan permintaan kepada administrator IAM untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep Basic IAM. Untuk mempelajari lebih lanjut tentang bagaimana perusahaan Anda dapat menggunakan IAM dengan Application Cost Profiler, lihat. Bagaimana Profiler Biaya AWS Aplikasi bekerja dengan IAM

Administrator IAM - Jika Anda seorang administrator IAM, Anda mungkin ingin mempelajari detail tentang cara menulis kebijakan untuk mengelola akses ke Application Cost Profiler. Untuk melihat contoh kebijakan berbasis identitas Profiler Biaya Aplikasi yang dapat Anda gunakan di IAM, lihat. AWS Contoh kebijakan berbasis identitas Profiler Biaya Aplikasi

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensyal identitas Anda. Anda harus diautentikasi (masuk ke AWS) sebagai Pengguna root akun AWS, sebagai pengguna IAM, atau dengan mengasumsikan peran IAM.

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensil yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (IAM Identity Center), autentikasi masuk tunggal perusahaan Anda, dan kredensi Google atau Facebook Anda adalah contoh identitas federasi. Saat Anda masuk sebagai identitas terfederasi, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan peran IAM. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

Bergantung pada jenis pengguna Anda, Anda dapat masuk ke AWS Management Console atau portal AWS akses. Untuk informasi selengkapnya tentang masuk AWS, lihat Cara masuk ke Panduan AWS Sign-In Pengguna Anda Akun AWS.

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensil Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Untuk informasi selengkapnya tentang penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, lihat Menandatangani permintaan AWS API di Panduan Pengguna IAM.

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari selengkapnya, lihat Autentikasi multi-faktor dalam Panduan Pengguna AWS IAM Identity Center dan Menggunakan autentikasi multi-faktor (MFA) dalam AWS dalam Panduan Pengguna IAM.

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya di akun. Identitas ini disebut pengguna Akun AWS root dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat Tugas yang memerlukan kredensial pengguna root dalam Panduan Pengguna IAM.

Pengguna dan grup IAM

Pengguna IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, kami merekomendasikan untuk mengandalkan kredensial sementara, bukan membuat pengguna IAM yang memiliki kredensial jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan tertentu yang memerlukan kredensial jangka panjang dengan pengguna IAM, kami merekomendasikan Anda merotasi kunci akses. Untuk informasi selengkapnya, lihat Merotasi kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang dalam Panduan Pengguna IAM.

Grup IAM adalah identitas yang menentukan sekumpulan pengguna IAM. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat memiliki grup yang bernama IAMAdmins dan memberikan izin ke grup tersebut untuk mengelola sumber daya IAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari selengkapnya, lihat Kapan harus membuat pengguna IAM (bukan peran) dalam Panduan Pengguna IAM.

Peran IAM

Peran IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Peran ini mirip dengan pengguna IAM, tetapi tidak terkait dengan orang tertentu. Anda dapat mengambil peran IAM untuk sementara AWS Management Console dengan beralih peran. Anda dapat mengambil peran dengan memanggil operasi AWS CLI atau AWS API atau dengan menggunakan URL kustom. Untuk informasi selengkapnya tentang cara menggunakan peran, lihat Menggunakan peran IAM dalam Panduan Pengguna IAM.

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat Membuat peran untuk Penyedia Identitas pihak ketiga dalam Panduan Pengguna IAM. Jika menggunakan Pusat Identitas IAM, Anda harus mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas tersebut diautentikasi, Pusat Identitas IAM akan mengorelasikan set izin ke peran dalam IAM. Untuk informasi tentang set izin, lihat Set izin dalam Panduan Pengguna AWS IAM Identity Center .
- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM guna mendapatkan berbagai izin secara sementara untuk tugas tertentu.
- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (prinsipal tepercaya) di akun lain untuk mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan peran sebagai

proxy). Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM.

- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Sebagai contoh, ketika Anda memanggil suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.
  - Sesi akses teruskan (FAS) — Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses maju.
  - Peran layanan – Peran layanan adalah peran IAM yang dijalankan oleh layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Membuat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.
  - Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke peran layanan. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.
- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan peran IAM untuk mengelola kredensi sementara untuk aplikasi yang berjalan pada instans EC2 dan membuat atau permintaan API. AWS CLI AWS Cara ini lebih dianjurkan daripada menyimpan kunci akses dalam instans EC2. Untuk menetapkan AWS peran ke instans EC2 dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instans berisi peran dan memungkinkan program yang berjalan di instans EC2 mendapatkan kredensial sementara. Untuk informasi selengkapnya, lihat Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan dalam instans Amazon EC2 dalam Panduan Pengguna IAM.

Untuk mempelajari apakah kita harus menggunakan peran IAM atau pengguna IAM, lihat Kapan harus membuat peran IAM (bukan pengguna) dalam Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izinnya. AWS mengevaluasi kebijakan ini ketika prinsipal (pengguna, pengguna root, atau sesi peran) membuat permintaan. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang struktur dan isi dokumen kebijakan JSON, lihat Gambaran umum kebijakan JSON dalam Panduan Pengguna IAM.

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

Kebijakan IAM mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk melakukan operasinya. Misalnya, anggaplah Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan tersebut bisa mendapatkan informasi peran dari AWS Management Console, API AWS CLI, atau AWS API.

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan yang dikelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran dalam. Akun AWS Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan yang

dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan yang dikelola atau kebijakan inline, lihat Memilih antara kebijakan yang dikelola dan kebijakan inline dalam Panduan Pengguna IAM.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Kebijakan berbasis sumber daya merupakan kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola dari IAM dalam kebijakan berbasis sumber daya.

Daftar kontrol akses (ACL)

Daftar kontrol akses (ACL) mengendalikan prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis sumber daya, meskipun kebijakan tersebut tidak menggunakan format dokumen kebijakan JSON.

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung ACL. Untuk mempelajari ACL selengkapnya, lihat Gambaran umum daftar kontrol akses (ACL) dalam Panduan Developer Amazon Simple Storage Service.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang kurang umum. Jenis-jenis kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda oleh jenis kebijakan yang lebih umum.

- Batasan izin – Batasan izin adalah fitur lanjutan tempat Anda mengatur izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas ke entitas IAM (pengguna IAM atau peran IAM). Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian

izin. Untuk informasi selengkapnya tentang batasan izin, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.

- Kebijakan kontrol layanan (SCP) — SCP adalah kebijakan JSON yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di. AWS Organizations AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur di organisasi, Anda dapat menerapkan kebijakan kontrol layanan (SCP) ke salah satu atau semua akun Anda. SCP membatasi izin untuk entitas di akun anggota, termasuk masing-masing. Pengguna root akun AWS Untuk informasi selengkapnya tentang Organisasi dan SCP, lihat Cara kerja SCP dalam Panduan Pengguna AWS Organizations .
- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya, lihat Kebijakan sesi dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat Logika evaluasi kebijakan di Panduan Pengguna IAM.

Bagaimana Profiler Biaya AWS Aplikasi bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke Application Cost Profiler, Anda harus memahami fitur IAM apa yang tersedia untuk digunakan dengan Application Cost Profiler. Untuk mendapatkan tampilan tingkat tinggi tentang cara kerja Application Cost Profiler dan AWS layanan lainnya dengan IAM, lihat AWS Layanan yang Bekerja dengan IAM di Panduan Pengguna IAM.

Topik

- Kebijakan berbasis identitas Profiler Biaya Aplikasi
- Kebijakan berbasis sumber daya Profiler Biaya Aplikasi
- Otorisasi berdasarkan tag Profiler Biaya Aplikasi
- Peran IAM Profiler Biaya Aplikasi

Kebijakan berbasis identitas Profiler Biaya Aplikasi

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan tindakan dan sumber daya yang diizinkan atau ditolak selain kondisi di mana tindakan diizinkan atau ditolak. Profiler Biaya Aplikasi mendukung tindakan tertentu. Untuk mempelajari semua elemen yang Anda gunakan dalam kebijakan JSON, lihat Referensi Elemen Kebijakan JSON IAM dalam Panduan Pengguna IAM.

Tindakan

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Tindakan kebijakan biasanya memiliki nama yang sama dengan operasi AWS API terkait. Ada beberapa pengecualian, misalnya tindakan hanya izin yang tidak memiliki operasi API yang cocok. Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

Menyertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Tindakan kebijakan di Application Cost Profiler menggunakan awalan berikut sebelum tindakan:. `application-cost-profiler:` Misalnya, untuk memberikan izin kepada seseorang untuk melihat detail definisi laporan Profiler Biaya Aplikasi Anda, Anda menyertakan `application-cost-profiler:GetReportDefinition` tindakan tersebut dalam kebijakan mereka. Pernyataan kebijakan harus memuat elemen `Action` atau `NotAction`. Application Cost Profiler mendefinisikan serangkaian tindakannya sendiri yang menggambarkan tugas yang dapat Anda lakukan dengan layanan ini.

Untuk menentukan beberapa tindakan dalam satu pernyataan, pisahkan tindakan dengan koma seperti berikut:

```
"Action": [
      "application-cost-profiler:ListReportDefinitions",
      "application-cost-profiler:GetReportDefinition"
```

Berikut ini adalah tindakan yang tersedia di Application Cost Profiler. Masing-masing memungkinkan aksi API dengan nama yang sama. Untuk informasi selengkapnya tentang Application Cost Profiler API, lihat Referensi API AWS Application Cost Profiler.

- `application-cost-profiler:ListReportDefinitions`— Memungkinkan daftar definisi laporan untuk AWS akun Anda, jika ada.
- `application-cost-profiler:GetReportDefinition`— Memungkinkan mendapatkan rincian definisi laporan untuk laporan Profiler Biaya Aplikasi Anda.
- `application-cost-profiler:PutReportDefinition`— Memungkinkan membuat definisi laporan baru.
- `application-cost-profiler:UpdateReportDefinition`— Memungkinkan memperbarui definisi laporan.
- `application-cost-profiler:DeleteReportDefinition`— Memungkinkan menghapus laporan (hanya tersedia melalui Application Cost Profiler API).
- `application-cost-profiler:ImportApplicationUsage`— Memungkinkan meminta Application Cost Profiler mengimpor data penggunaan dari bucket Amazon S3 yang ditentukan.

Sumber daya

Application Cost Profiler tidak mendukung penetapan nama sumber daya Amazon Resource Names (ARN) dalam kebijakan.

Kunci syarat

Profiler Biaya Aplikasi tidak menyediakan kunci kondisi khusus layanan apa pun, tetapi mendukung penggunaan beberapa kunci kondisi global. Untuk melihat semua kunci kondisi AWS global, lihat Kunci Konteks Kondisi AWS Global di Panduan Pengguna IAM.

Contoh

Untuk melihat contoh kebijakan berbasis identitas Application Cost Profiler, lihat. AWS Contoh kebijakan berbasis identitas Profiler Biaya Aplikasi

Kebijakan berbasis sumber daya Profiler Biaya Aplikasi

Profiler Biaya Aplikasi tidak mendukung kebijakan berbasis sumber daya.

Otorisasi berdasarkan tag Profiler Biaya Aplikasi

Profiler Biaya Aplikasi tidak mendukung penandaan sumber daya atau mengontrol akses berdasarkan tag.

Peran IAM Profiler Biaya Aplikasi

Peran IAM adalah entitas dalam AWS akun Anda yang memiliki izin tertentu.

Menggunakan kredensyal sementara dengan Application Cost Profiler

Anda dapat menggunakan kredensial sementara untuk masuk dengan gabungan, menjalankan IAM role, atau menjalankan peran lintas akun. Anda memperoleh kredensil keamanan sementara dengan memanggil operasi AWS STS API seperti AssumeRoleatau. GetFederationToken

Profiler Biaya Aplikasi mendukung penggunaan kredensyal sementara.

Peran terkait layanan

Peran terkait AWS layanan memungkinkan layanan mengakses sumber daya di layanan lain untuk menyelesaikan tindakan atas nama Anda. Peran tertaut layanan muncul di akun IAM Anda dan dimiliki oleh layanan tersebut. Administrator dapat melihat tetapi tidak dapat mengedit izin untuk peran yang terkait dengan layanan.

Application Cost Profiler tidak mendukung peran terkait layanan.

Peran layanan

Fitur ini memungkinkan layanan untuk menerima peran layanan atas nama Anda. Peran ini mengizinkan layanan untuk mengakses sumber daya di layanan lain untuk menyelesaikan tindakan atas nama Anda. Peran layanan muncul di akun IAM Anda dan dimiliki oleh akun tersebut. Ini berarti bahwa administrator dapat mengubah izin untuk peran ini. Namun, melakukannya mungkin merusak fungsi layanan.

Profiler Biaya Aplikasi tidak mendukung peran layanan.

AWS Contoh kebijakan berbasis identitas Profiler Biaya Aplikasi

Secara default, pengguna dan peran IAM tidak memiliki izin untuk membuat atau memodifikasi sumber daya AWS Application Cost Profiler. Mereka juga tidak dapat melakukan tugas menggunakan AWS Management Console, AWS Command Line Interface (AWS CLI), atau AWS API. Administrator harus membuat kebijakan IAM yang memberikan izin kepada pengguna dan peran untuk melakukan operasi API tertentu yang mereka butuhkan. Administrator kemudian harus melampirkan kebijakan tersebut ke pengguna IAM atau grup yang memerlukan izin tersebut.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM menggunakan contoh dokumen kebijakan JSON ini, lihat Membuat Kebijakan pada Tab JSON dalam Panduan Pengguna IAM.

Topik

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya Profiler Biaya Aplikasi di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat Kebijakan yang dikelola AWS atau Kebijakan yang dikelola AWS untuk fungsi tugas dalam Panduan Pengguna IAM.
- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat Kebijakan dan izin dalam IAM dalam Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Kondisi dalam Panduan Pengguna IAM.
- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah

ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat Validasi kebijakan IAM Access Analyzer dalam Panduan Pengguna IAM.

- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Anda, Akun AWS aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Mengonfigurasi akses API yang dilindungi MFA dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat Praktik terbaik keamanan dalam IAM dalam Panduan Pengguna IAM.

Menggunakan konsol Application Cost Profiler

Untuk mengakses konsol AWS Application Cost Profiler, Anda harus memiliki seperangkat izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang sumber daya Profiler Biaya Aplikasi di akun Anda AWS . Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tersebut tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna IAM atau peran) dengan kebijakan tersebut.

Untuk memastikan bahwa entitas tersebut dapat menggunakan konsol Application Cost Profiler untuk melihat definisi laporan Application Cost Profiler untuk AWS akun Anda, lampirkan izin berikut ke entitas.

```
application-cost-profiler:ListReportDefinitions
application-cost-profiler:GetReportDefinition
```

Misalnya, Anda dapat membuat kebijakan berikut untuk pengguna hanya-baca.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "application-cost-profiler:ListReportDefinitions",
```

```
            "application-cost-profiler:GetReportDefinition"
         ],
         "Resource":"*"
      }
   ]
}
```

Untuk informasi selengkapnya, lihat Menambahkan Izin ke Pengguna dalam Panduan Pengguna IAM.

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebagai alternatif, hanya izinkan akses ke tindakan yang cocok dengan operasi API yang sedang Anda coba lakukan.

Izinkan para pengguna untuk melihat izin mereka sendiri

Contoh ini menunjukkan cara membuat kebijakan yang mengizinkan pengguna IAM melihat kebijakan inline dan terkelola yang dilampirkan ke identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau menggunakan API atau secara terprogram. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
```

```
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Mengakses satu bucket Amazon S3

Dalam contoh ini, Anda ingin memberi pengguna IAM di AWS akun Anda akses ke salah satu bucket Amazon S3 Anda,. `examplebucket` Anda juga ingin mengizinkan pengguna untuk menambah, memperbarui, dan menghapus objek.

Selain memberikan izin `s3:PutObject`, `s3:GetObject`, dan `s3:DeleteObject` bagi pengguna, kebijakan tersebut juga memberikan izin `s3:ListAllMyBuckets`, `s3:GetBucketLocation`, dan `s3:ListBucket`. Izin-izin tersebut adalah izin tambahan yang diperlukan oleh konsol tersebut. Selain itu, tindakan `s3:PutObjectAcl` dan `s3:GetObjectAcl` diperlukan untuk dapat menyalin, memotong, dan menempel objek di konsol. Untuk contoh panduan yang memberikan izin kepada pengguna dan mengujinya menggunakan konsol, lihat Contoh Panduan: Menggunakan kebijakan pengguna untuk mengontrol akses ke bucket Anda.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"ListBucketsInConsole",
         "Effect":"Allow",
         "Action":[
            "s3:ListAllMyBuckets"
         ],
         "Resource":"arn:aws:s3:::*"
      },
      {
         "Sid":"ViewSpecificBucketInfo",
         "Effect":"Allow",
         "Action":[
            "s3:ListBucket",
```

```
            "s3:GetBucketLocation"
         ],
         "Resource":"arn:aws:s3:::examplebucket"
      },
      {
         "Sid":"ManageBucketContents",
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:PutObjectAcl",
            "s3:GetObject",
            "s3:GetObjectAcl",
            "s3:DeleteObject"
         ],
         "Resource":"arn:aws:s3:::examplebucket/*"
      }
   ]
}
```

Pemecahan Masalah AWS Identitas dan akses Profiler Biaya Aplikasi

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan AWS Application Cost Profiler dan AWS Identity and Access Management (IAM).

Topik

- Saya Tidak Berwenang Melakukan Tindakan dalam Profiler Biaya Aplikasi
- Saya Tidak Berwenang untuk Melakukan iam: PassRole
- Saya Ingin Mengizinkan Orang Di Luar AWS Akun Saya Mengakses Sumber Daya Profiler Biaya Aplikasi Saya

Saya Tidak Berwenang Melakukan Tindakan dalam Profiler Biaya Aplikasi

Jika AWS Management Console memberitahu Anda bahwa Anda tidak berwenang untuk melakukan suatu tindakan, maka Anda harus menghubungi administrator Anda untuk bantuan. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Contoh kesalahan berikut terjadi ketika pengguna `mateojackson` IAM mencoba menggunakan konsol untuk melihat detail tentang laporan Application Cost Profiler tetapi tidak memiliki `application-cost-profiler:ListReportDefinitions` izin.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 application-cost-profiler:ListReportDefinitions on resource: Report Definition
```

Dalam hal ini, Mateo meminta administratornya untuk memperbarui kebijakannya untuk memungkinkannya mengakses sumber definisi laporan menggunakan `application-cost-profiler:ListReportDefinitions` tindakan tersebut.

Saya Tidak Berwenang untuk Melakukan iam: PassRole

Jika Anda menerima kesalahan bahwa Anda tidak berwenang untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran ke Profiler Biaya Aplikasi.

Beberapa Layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika pengguna IAM bernama `marymajor` mencoba menggunakan konsol untuk melakukan tindakan di Application Cost Profiler. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

Jika Anda memerlukan bantuan, hubungi AWS administrator Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Saya Ingin Mengizinkan Orang Di Luar AWS Akun Saya Mengakses Sumber Daya Profiler Biaya Aplikasi Saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACL), Anda dapat menggunakan kebijakan tersebut untuk memberi orang akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mengetahui apakah Application Cost Profiler mendukung fitur-fitur ini, lihatBagaimana Profiler Biaya AWS Aplikasi bekerja dengan IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat Menyediakan akses ke pengguna IAM di pengguna lain Akun AWS yang Anda miliki di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat Menyediakan akses ke pengguna terautentikasi eksternal (federasi identitas) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM.

Validasi kepatuhan untuk AWS Profiler Biaya Aplikasi

Untuk mempelajari apakah an Layanan AWS berada dalam lingkup program kepatuhan tertentu, lihat Layanan AWS di Lingkup oleh Program Kepatuhan Layanan AWS dan pilih program kepatuhan yang Anda minati. Untuk informasi umum, lihat Program AWS Kepatuhan Program AWS .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Mengunduh Laporan di AWS Artifact .

Tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- Panduan Memulai Cepat Keamanan dan Kepatuhan — Panduan penerapan ini membahas pertimbangan arsitektur dan memberikan langkah-langkah untuk menerapkan lingkungan dasar AWS yang berfokus pada keamanan dan kepatuhan.
- Arsitektur untuk Keamanan dan Kepatuhan HIPAA di Amazon Web Services — Whitepaper ini menjelaskan bagaimana perusahaan dapat menggunakan AWS untuk membuat aplikasi yang memenuhi syarat HIPAA.

> **Note**
>
> Tidak semua memenuhi Layanan AWS syarat HIPAA. Untuk informasi selengkapnya, lihat Referensi Layanan yang Memenuhi Syarat HIPAA.

- AWS Sumber Daya AWS — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- AWS Panduan Kepatuhan Pelanggan - Memahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan Layanan AWS dan memetakan panduan untuk kontrol keamanan di berbagai kerangka kerja (termasuk Institut Standar dan Teknologi Nasional (NIST), Dewan Standar Keamanan Industri Kartu Pembayaran (PCI), dan Organisasi Internasional untuk Standardisasi (ISO)).
- Mengevaluasi Sumber Daya dengan Aturan dalam Panduan AWS Config Pengembang — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub— Ini Layanan AWS memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS. Security Hub menggunakan kontrol keamanan untuk sumber daya AWS Anda serta untuk memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat Referensi kontrol Security Hub.
- Amazon GuardDuty — Ini Layanan AWS mendeteksi potensi ancaman terhadap beban kerja Akun AWS, kontainer, dan data Anda dengan memantau lingkungan Anda untuk aktivitas mencurigakan dan berbahaya. GuardDuty dapat membantu Anda mengatasi berbagai persyaratan kepatuhan, seperti PCI DSS, dengan memenuhi persyaratan deteksi intrusi yang diamanatkan oleh kerangka kerja kepatuhan tertentu.
- AWS Audit ManagerIni Layanan AWS membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

Ketahanan diAWSAplikasi Cost Profiler

Infrastruktur global AWS dibangun di sekitar Wilayah AWS dan Availability Zone. Wilayah menyediakan beberapa Availability Zone yang terpisah dan terisolasi secara fisik, yang terhubung melalui jaringan latensi rendah, throughput tinggi, dan sangat redundan. Dengan Availability Zone, Anda dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis

mengalami failover antar zona tanpa gangguan. Availability Zone lebih tersedia, memiliki toleransi kesalahan, dan dapat diskalakan dibandingkan dengan satu atau beberapa infrastruktur pusat data tradisional.

Untuk informasi selengkapnya tentang Wilayah AWS dan Availability Zone, lihat Infrastruktur Global AWS.

Keamanan infrastruktur diAWSProfiler Biaya Aplikasi

Sebagai layanan terkelola,AWSAplikasi Biaya Profiler dilindungi olehAWSkeamanan jaringan global. Untuk informasi tentangAWSlayanan keamanan dan bagaimanaAWSmelindungi infrastruktur, lihatAWSKeamanan Cloud. Untuk mendesainAWSlingkungan menggunakan praktik terbaik untuk keamanan infrastruktur, lihatPerlindungan InfrastrukturdiPilar KeamananAWSKerangka Kerja yang Diarsiteksikan.

Anda menggunakanAWSpanggilan API yang diterbitkan untuk mengakses Application Cost Profiler melalui jaringan. Klien harus mendukung hal berikut:

- Transport Layer Security (TLS). Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Suite cipher dengan kerahasiaan maju sempurna (PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan sistem yang lebih baru mendukung mode ini.

Selain itu, permintaan harus ditandatangani menggunakan access key ID dan secret access key yang terkait dengan principal IAM. Atau Anda bisa menggunakan AWS Security Token Service (AWS STS) untuk membuat kredensial keamanan sementara guna menandatangani permintaan.

Peristiwa Cost Profiler EventBridge

Anda dapat menggunakan Amazon EventBridge untuk mengotomatiskanAWSlayanan dan merespons peristiwa sistem secara otomatis seperti masalah ketersediaan aplikasi atau perubahan sumber daya. Peristiwa dariAWSlayanan dikirimkan ke EventBridge dalam waktu dekat. Anda dapat menuliskan aturan sederhana untuk menunjukkan peristiwa mana yang sesuai kepentingan Anda, dan tindakan otomatis mana yang diambil ketika suatu peristiwa sesuai dengan suatu aturan. Untuk informasi selengkapnya, lihatAmazon EventBridge Panduan Pengguna.

Anda dapat memonitorAWSperistiwa Cost Profiler EventBridge. EventBridge merutekan data ke target sepertiAWS Lambdadan Amazon Simple Notification Service (Amazon SNS). Peristiwa ini sama dengan yang muncul di Amazon CloudWatch Acara, yang memberikan near-real-time aliran peristiwa sistem yang menjelaskan perubahanAWSsumber daya.

Memiilih pembuatan laporan dengan EventBridge

Dengan EventBridgeAnda dapat membuat aturan yang menentukan tindakan yang akan diambil ketika Applist Profiler mengirimkan pemberitahuan laporan yang dihasilkan. Misalnya, Anda dapat membuat aturan yang mengirimkan pesan email kapan pun laporan dibuat.

Memonitor pembuatan laporan

1. Masuk keAWSmenggunakan akun yang memiliki izin untuk menggunakan keduanya EventBridge dan aplikasi Cost Profiler.
2. Buka Amazon EventBridge konsol dihttps://console.aws.amazon.com/events/.
3. Menggunakan nilai-nilai berikut, membuat EventBridge aturan yang memantau peristiwa yang dibuat saat laporan dibuat:

   - UntukJenis aturan, pilihMemiilih pola peristiwa.
   - UntukSumber peristiwa, pilihLainnya.
   - DiPola peristiwabagian, pilihPola kustom (editor JSON), dan kemudian paste pola peristiwa berikut ke area teks:

     ```
     {
       "source": ["aws.application-cost-profiler"],
       "detail-type": ["Application Cost Profiler Report Generated"]
     }
     ```

- UntukJenis target, pilihAWSlayanan, dan untukPilih target, pilihAWSlayanan yang Anda ingin bertindak kapan EventBridge mendeteksi peristiwa dari jenis yang dipilih. Target terpicu saat peristiwa diterima yang sesuai dengan pola peristiwa yang ditentukan dalam aturan.

Untuk detail tentang membuat aturan, lihatMembuat Amazon EventBridge aturan yang bereaksi terhadap peristiwadi dalamAmazon EventBridge Panduan Pengguna.

Contoh peristiwa Laporan yang Dihasilkan

Peristiwa ini memberi tahu Anda saat laporan dibuat dan siap untuk Anda ambil. Parametermessagebidang memberi Anda bucket Amazon Simple Storage Service (Amazon S3) untuk objek Amazon S3 tempat laporan disimpan.

```
{
   "version": "0",
   "id": "01234567-EXAMPLE",
   "detail-type": "Application Cost Profiler Report Generated",
   "source": "aws.application-cost-profiler",
   "account": "123456789012",
   "time": "2021-03-31T10:23:43Z",
   "region": "us-east-1",
   "resources": [],
   "detail": {
     "message": "Application Cost Profiler report delivered in bucket: SampleBucket,
 key: SampleReport-112233445566"
   }
}
```

Riwayat dokumen

Tabel berikut menjelaskan rilis dokumentasi untukAWSProfiler Biaya Aplikasi.

Perubahan	Deskripsi	Tanggal
Pemberitahuan penghentian layanan	AWSProfiler Biaya Aplikasi akan dihentikan pada 30 September 2024 dan tidak lagi menerima pelanggan baru.	Agustus 11, 2023
Memantau peristiwa	Karena perubahan padaEvent Bridgeconsole, cara Anda membuat aturan untuk memantau peristiwa Applicati on Cost Profiler berubah. Untuk informasi lebih lanjut lihat,Memantau peristiwa Profiler Biaya Aplikasi diEventBridge.	Juli 5, 2022
Pembaruan untuk contoh kebijakan bucket S3	Pembaruan khusus dokumentasi ke contoh kebijakan bucket S3. Untuk informasi lebih lanjut, lihatMenyiapkan bucket Amazon S3 untuk Profiler Biaya Aplikasi.	Desember 6, 2021
Ketersediaan umum	Rilis publik awal Application Cost Profiler.	13 Mei 2021