aws

Amazon EMR pada Panduan Pengembangan EKS

Amazon EMR

Amazon EMR: Amazon EMR pada Panduan Pengembangan EKS

Table of Contents

Apa itu Amazon EMR di EKS?

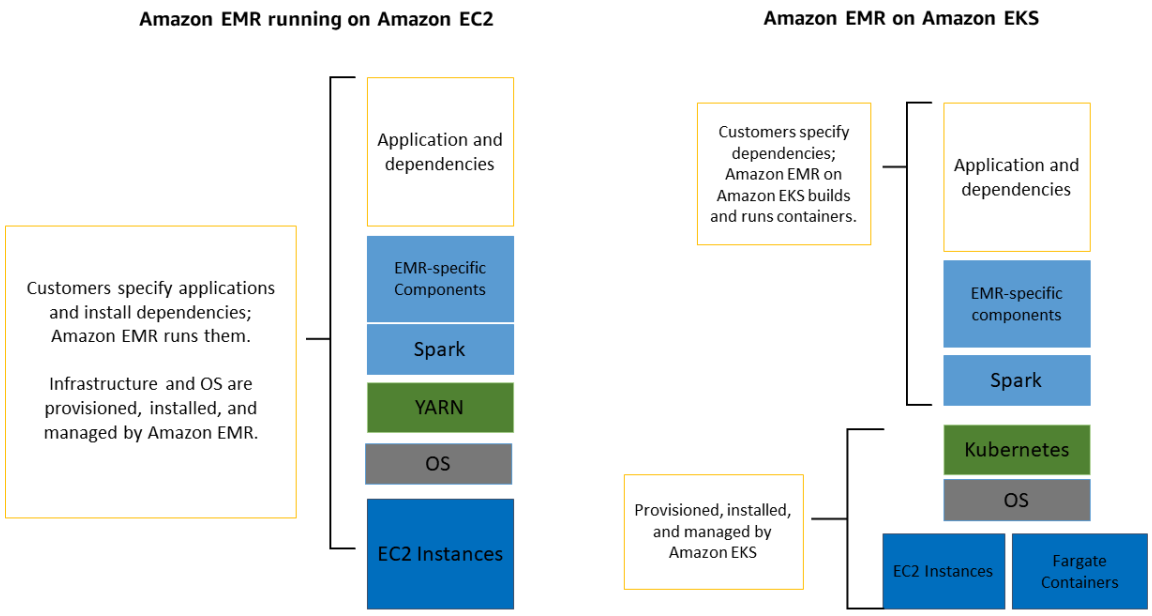
Amazon EMR di EKS menyediakan opsi penyebaran untuk Amazon EMR yang memungkinkan Anda untuk menjalankan kerangka kerja big data sumber terbuka di Amazon Elastic Kubernetes Service (Amazon EKS). Dengan opsi penyebaran ini, Anda dapat fokus pada menjalankan beban kerja analitik sementara Amazon EMR di EKS membangun, mengonfigurasi, dan mengelola kontainer untuk aplikasi sumber terbuka.

Jika Anda sudah menggunakan Amazon EMR, Anda sekarang dapat menjalankan aplikasi berbasis Amazon EMR dengan jenis aplikasi lain pada klaster Amazon EKS yang sama. Opsi penyebaran ini juga meningkatkan pemanfaatan sumber daya dan menyederhanakan manajemen infrastruktur di beberapa Availability Zones. Jika Anda sudah menjalankan kerangka kerja big data di Amazon EKS, Anda sekarang dapat menggunakan Amazon EMR untuk mengotomatisasi penyediaan dan manajemen, dan menjalankan Apache Spark lebih cepat.

Amazon EMR di EKS memungkinkan tim Anda untuk berkolaborasi lebih efisien dan memproses sejumlah besar data dengan lebih mudah dan hemat biaya:

- Anda dapat menjalankan aplikasi pada kolam umum sumber daya tanpa harus menyediakan infrastruktur. Anda dapat menggunakanAmazon EMR StudiodanAWSSDK atauAWS CLIuntuk mengembangkan, mengirimkan, dan mendiagnosis aplikasi analitik yang berjalan di klaster EKS. Anda dapat menjalankan tugas terjadwal di Amazon EMR di EKS menggunakan Apache Airflow terkelola mandiri atau Amazon Managed Workflows for Apache Airflow (MWAA).
- Tim infrastruktur dapat mengelola platform komputasi umum secara terpusat untuk mengkonsolidasikan beban kerja Amazon EMR dengan aplikasi berbasis kontainer lainnya. Anda dapat menyederhanakan manajemen infrastruktur dengan alat umum Amazon EKS dan memanfaatkan klaster bersama untuk beban kerja yang membutuhkan versi kerangka kerja sumber terbuka yang berbeda. Anda juga dapat mengurangi overhead operasional dengan manajemen klaster Kubernetes otomatis dan patching OS. Dengan Amazon EC2 dan AWS Fargate, Anda dapat mengaktifkan beberapa sumber daya komputasi untuk memenuhi persyaratan performa, operasional, atau keuangan.

Diagram berikut menunjukkan dua model penyebaran yang berbeda untuk Amazon EMR.



Topik

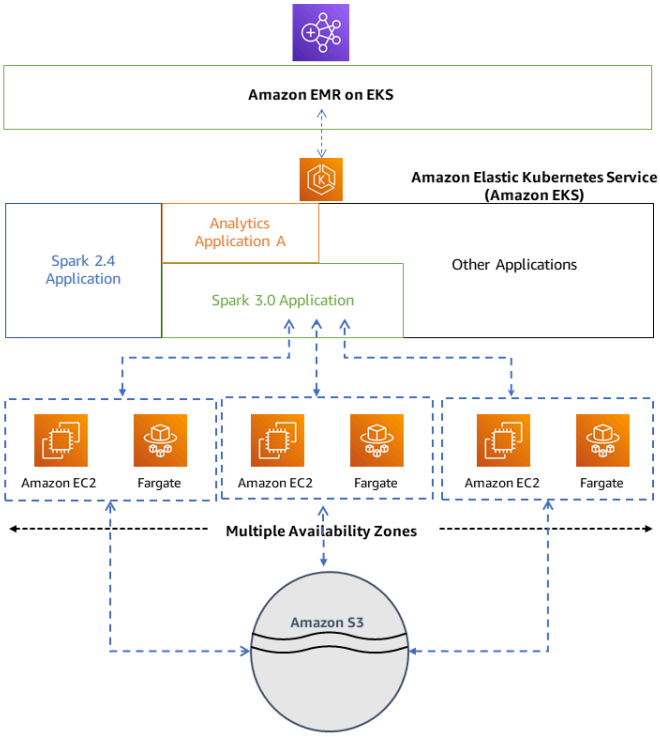
- Arsitektur
- Konsep
- Bagaimana komponen bekerja sama

Arsitektur

Amazon EMR di EKS menggabungkan dengan longgar aplikasi untuk infrastruktur tempat aplikasi berjalan. Setiap lapisan infrastruktur menyediakan orkestrasi untuk lapisan berikutnya. Ketika Anda mengirimkan tugas ke Amazon EMR, definisi tugas Anda berisi semua parameter khusus aplikasi. Amazon EMR menggunakan parameter ini untuk menginstruksikan Amazon EKS tentang yang pod dan kontainer mana yang disebarkan. Amazon EKS kemudian membuat online sumber daya komputasi dari Amazon EC2 dan AWS Fargate diperlukan untuk menjalankan tugas.

Dengan penggabungan longgar layanan, Anda dapat menjalankan beberapa tugas yang terisolasi dengan aman secara bersamaan. Anda juga dapat mengukur tugas yang sama dengan backend komputasi yang berbeda atau menyebarkan tugas Anda di beberapa Availability Zones yang sama untuk meningkatkan ketersediaan.

Diagram berikut menggambarkan cara Amazon EMR di EKS bekerja dengan layanan AWS lainnya.



Konsep

Namespace Kubernetes

Amazon EKS menggunakan namespace Kubernetes untuk membagi sumber daya klaster antara beberapa pengguna dan aplikasi. Namespace ini adalah dasar untuk lingkungan multi-penyewa. Sebuah namespace Kubernetes dapat memiliki baik Amazon EC2 atau AWS Fargate sebagai penyedia komputasi. Fleksibilitas ini memberi Anda pilihan performa dan biaya yang berbeda untuk dijalankan pada tugas Anda.

Klaster virtual

Sebuah klaster virtual adalah namespace Kubernetes tempat Amazon EMR terdaftar. Amazon EMR menggunakan klaster virtual untuk menjalankan tugas dan meng-host titik akhir. Beberapa klaster virtual dapat didukung oleh klaster fisik yang sama. Namun, setiap klaster virtual memetakan ke satu namespace pada klaster EKS. Klaster virtual tidak membuat sumber daya aktif apa pun yang berkontribusi pada tagihan Anda atau yang memerlukan manajemen siklus hidup di luar layanan.

Tugas berjalan

Sebuah tugas berjalan adalah unit kerja, seperti Spark jar, PySpark skrip, atau kueri SparkSQL, yang Anda kirimkan ke Amazon EMR di EKS. Satu tugas dapat memiliki beberapa tugas berjalan. Ketika Anda mengirimkan tugas berjalan, Anda menyertakan informasi berikut:

- Sebuah klaster virtual di mana tugas harus berjalan.
- Sebuah nama tugas untuk mengidentifikasi tugas.
- Peran eksekusi — IAM role tercakup yang menjalankan tugas dan memungkinkan Anda untuk menentukan sumber daya mana yang dapat diakses oleh tugas.
- Label rilis Amazon EMR yang menentukan versi aplikasi sumber terbuka untuk digunakan.
- Artefak yang digunakan saat mengirimkan tugas Anda, seperti parameter spark-submit.

Secara default, log diunggah ke server Riwayat Spark dan dapat diakses dari AWS Management Console. Anda juga dapat mendorong log peristiwa, log eksekusi, dan metrik ke Amazon S3 C3 dan Amazon C3 dan Amazon CloudWatch.

Kontainer Amazon EMR

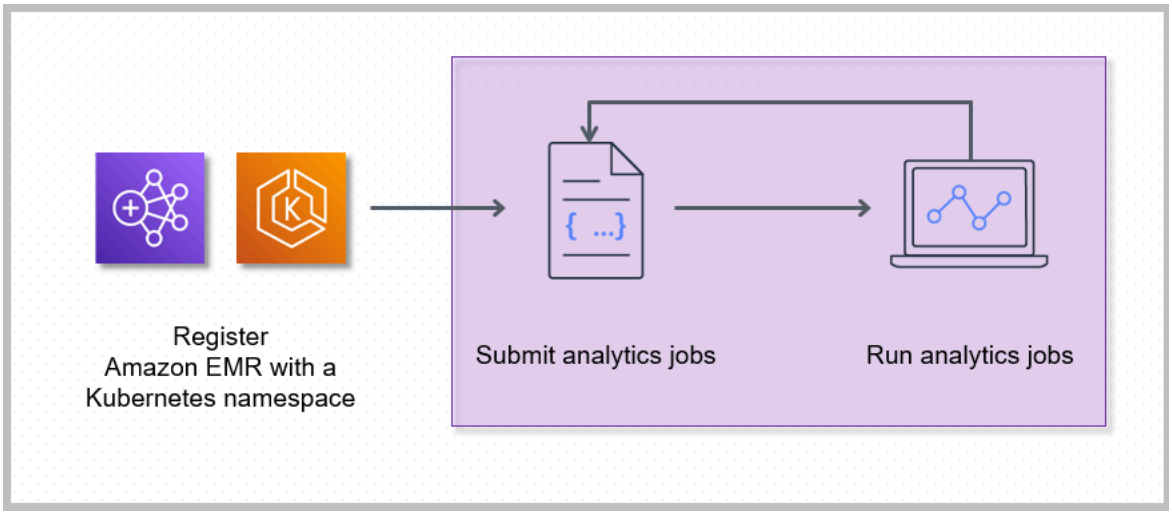
Kontainer Amazon EMR adalah Nama API untuk Amazon EMR di EKS. Prefiks `emr-containers` digunakan dalam skenario berikut:

- Ini adalah prefiks dalam perintah CLI untuk Amazon EMR di EKS. Sebagai contoh, `aws emr-containers start-job-run`.
- Ini adalah prefiks sebelum tindakan kebijakan IAM untuk Amazon EMR di EKS. Sebagai contoh, `"Action": [ "emr-containers:StartJobRun"]`. Untuk informasi selengkapnya, lihat Tindakan kebijakan untuk Amazon EMR di EKS.
- Ini adalah prefiks yang digunakan di Amazon EMR pada titik akhir layanan EKS. Sebagai contoh, `emr-containers.us-east-1.amazonaws.com`. Untuk informasi selengkapnya, lihat Amazon EMR pada Titik Akhir Layanan EKS.

Bagaimana komponen bekerja sama

Langkah-langkah dan diagram berikut menggambarkan alur kerja Amazon EMR di EKS:

- Menggunakan klaster Amazon EKS yang ada atau membuat klaster dengan menggunakan utilitas baris perintah eksctl atau konsol Amazon EKS.
- Buat klaster virtual dengan mendaftarkan Amazon EMR dengan namespace pada klaster EKS.
- Kirimkan tugas Anda ke klaster virtual menggunakan AWS CLI atau SDK.



Mendaftarkan Amazon EMR dengan namespace Kubernetes pada Amazon EKS membuat klaster virtual. Amazon EMR kemudian dapat menjalankan beban kerja analitik pada namespace tersebut. Saat Anda menggunakan Amazon EMR di EKS untuk mengirimkan tugas Spark ke klaster virtual, Amazon EMR di EKS meminta penjadwal Kubernetes di Amazon EKS untuk menjadwalkan pod.

Untuk setiap tugas yang Anda jalankan, Amazon EMR di EKS menciptakan sebuah kontainer dengan gambar dasar Amazon Linux 2, Apache Spark, dan dependensi terkait. Setiap tugas berjalan dalam pod yang mengunduh kontainer dan mulai menjalankannya. Pod berakhir setelah tugas berakhir. Jika gambar kontainer sebelumnya telah disebarkan ke simpul, maka gambar yang di-cache digunakan dan unduhan dilewati. Kontainer sidecar, seperti penerus log atau metrik, dapat disebarkan ke pod. Setelah tugas berakhir, Anda masih dapat melakukan debug menggunakan UI aplikasi Spark di konsol Amazon EMR.

Mulai

Topik ini membantu Anda memulai menggunakan Amazon EMR di EKS dengan menyebarkan aplikasi Spark park park park park park park park park park park park park park park park park park park park park park park park park park park park park park park park park park park park park park Sebelum memulai, pastikan bahwa Anda telah menyelesaikan langkah-langkah dalam Menyiapkan Amazon EMR di EKS. Untuk template lain yang dapat membantu Anda memulai, lihat Panduan Praktik Terbaik Kontainer EMR kami di GitHub.

Anda memerlukan informasi berikut dari langkah-langkah penyiapan:

- ID klaster virtual untuk klaster Amazon EKS dan namespace Kubernetes terdaftar dengan Amazon EMR

  > **Important**
  >
  > Ketika membuat klaster EKS, pastikan untuk menggunakan m5.xlarge sebagai tipe instans, atau tipe instans lainnya dengan CPU dan memori yang lebih tinggi. Menggunakan jenis instans dengan CPU atau memori yang lebih rendah daripada m5.xlarge dapat menyebabkan kegagalan pekerjaan karena sumber daya yang tidak mencukupi yang tersedia di klaster.

- Nama IAM role yang digunakan untuk eksekusi tugas
- Label rilis untuk rilis Amazon EMR (misalnya, `emr-6.4.0-latest`)
- Target tujuan untuk pencatatan dan pemantauan:
  - Nama grup Amazon CloudWatch log dan prefiks stream log
  - Lokasi Amazon S3 untuk menyimpan peristiwa dan log kontainer

> **Important**
>
> Amazon EMR pada pekerjaan EKS menggunakan Amazon CloudWatch dan Amazon S3 sebagai target tujuan untuk pemantauan dan pencatatan log. Anda dapat memantau kemajuan pekerjaan dan memecahkan masalah kegagalan dengan melihat log pekerjaan yang dikirim ke tujuan ini. Untuk mengaktifkan pencatatan, kebijakan IAM yang terkait dengan IAM role untuk pelaksanaan tugas harus memiliki izin yang diperlukan untuk mengakses sumber daya target. Jika kebijakan IAM tidak memiliki izin yang diperlukan, Anda harus

mengikuti langkah-langkah yang diuraikan dalamPerbarui kebijakan kepercayaan dari peran eksekusi tugas, Mengonfigurasi tugas berjalan untuk menggunakan log Amazon S3, dan Mengonfigurasi tugas berjalan untuk menggunakan CloudWatch Log sebelum menjalankan tugas sampel ini.

Jalankan aplikasi Spark park park park park park park

Ambil langkah-langkah berikut untuk menjalankan aplikasi Spark park park park park park park park park park park park park park park park park park park park park park park park park park park park park `entryPointFile` aplikasi untuk aplikasi Spark Python terletak di`s3://REGION.elasticmapreduce/emr-containers/samples/wordcount/scripts/wordcount.py`. *`REGION`* adalah Wilayah tempat klaster virtual Amazon EMR pada EKS Anda berada, seperti *`us-timur-1`*.

1. Perbarui kebijakan IAM untuk peran eksekusi pekerjaan dengan izin yang diperlukan, seperti yang ditunjukkan oleh pernyataan kebijakan berikut.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadFromLoggingAndInputScriptBuckets",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::*.elasticmapreduce",
                "arn:aws:s3:::*.elasticmapreduce/*",
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET-OUTPUT",
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET-OUTPUT/*",
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET-LOGGING",
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET-LOGGING/*"
            ]
        },
        {
            "Sid": "WriteToLoggingAndOutputDataBuckets",
            "Effect": "Allow",
            "Action": [
```

```
                "s3:PutObject",
                "s3:DeleteObject"
            ],
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET-OUTPUT/*",
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET-LOGGING/*"
            ]
        },
        {
            "Sid": "DescribeAndCreateCloudwatchLogStream",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:DescribeLogGroups",
                "logs:DescribeLogStreams"
            ],
            "Resource": [
                "arn:aws:logs:*:*:*"
            ]
        },
        {
            "Sid": "WriteToCloudwatchLogs",
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:my_log_group_name:log-
stream:my_log_stream_prefix/*"
            ]
        }
    ]
}
```

- Pernyataan pertama`ReadFromLoggingAndInputScriptBuckets` dalam kebijakan ini memberikan`ListBucket` dan`GetObjects` akses ke bucket Amazon S3 berikut:
  - *REGION*`.elasticmapreduce`- ember tempat`entryPoint` file aplikasi berada.
  - *DOC-EXAMPLE-BUCKET-OUTPUT* - bucket yang Anda tentukan untuk data keluaran Anda.
  - *DOC-EXAMPLE-BUCKET-LOGGING* - bucket yang Anda tentukan untuk data logging Anda.
- Pernyataan kedua`WriteToLoggingAndOutputDataBuckets` dalam kebijakan ini memberikan izin pekerjaan untuk menulis data ke output dan mencatat bucket masing-masing.

- Pernyataan ketigaDescribeAndCreateCloudwatchLogStream memberikan pekerjaan dengan izin untuk menggambarkan dan membuat CloudWatch Log Amazon.
- Pernyataan keempatWriteToCloudwatchLogs memberikan izin untuk menulis log ke grup CloudWatch log Amazon yang diberi nama *my_log_group_name*di bawah aliran log bernama *my_log_stream_prefix*.

2. Untuk menjalankan aplikasi Spark Python, gunakan perintah berikut. Ganti semua nilai *miring merah* yang dapat diganti dengan nilai yang sesuai. *REGION* adalah Wilayah tempat klaster virtual Amazon EMR pada EKS Anda berada, seperti *us-timur-1*.

```
aws emr-containers start-job-run \
--virtual-cluster-id cluster_id \
--name sample-job-name \
--execution-role-arn execution-role-arn \
--release-label emr-6.4.0-latest \
--job-driver '{
  "sparkSubmitJobDriver": {
    "entryPoint": "s3://REGION.elasticmapreduce/emr-containers/samples/wordcount/
scripts/wordcount.py",
    "entryPointArguments": ["s3://DOC-EXAMPLE-BUCKET-OUTPUT/wordcount_output"],
    "sparkSubmitParameters": "--conf spark.executor.instances=2 --
conf spark.executor.memory=2G --conf spark.executor.cores=2 --conf
 spark.driver.cores=1"
  }
}' \
--configuration-overrides '{
  "monitoringConfiguration": {
    "cloudWatchMonitoringConfiguration": {
      "logGroupName": "my_log_group_name",
      "logStreamNamePrefix": "my_log_stream_prefix"
    },
    "s3MonitoringConfiguration": {
       "logUri": "s3://DOC-EXAMPLE-BUCKET-LOGGING"
    }
  }
}'
```

Data output dari pekerjaan ini akan tersedia dis3://*DOC-EXAMPLE-BUCKET-OUTPUT*/wordcount_output.

Anda juga dapat membuat file JSON dengan parameter tertentu untuk menjalankan tugas Anda. Kemudian jalankan perintah `start-job-run` dengan jalur ke file JSON. Untuk informasi selengkapnya, lihat Kirim pekerjaan yang dijalankan dengan `StartJobRun`. Untuk detail lebih lanjut tentang mengonfigurasi parameter untuk menjalankan tugas, lihat Pilihan untuk mengonfigurasi tugas berjalan.

3. Untuk menjalankan aplikasi Spark park SQL SQL SQL, gunakan perintah berikut. Ganti semua nilai *miring merah* dengan nilai yang sesuai. *REGION* adalah Wilayah tempat klaster virtual Amazon EMR pada EKS Anda berada, seperti *us-timur-1*.

```
aws emr-containers start-job-run \
--virtual-cluster-id cluster_id \
--name sample-job-name \
--execution-role-arn execution-role-arn \
--release-label emr-6.7.0-latest \
--job-driver '{
  "sparkSqlJobDriver": {
    "entryPoint": "s3://query-file.sql",
    "sparkSqlParameters": "--conf spark.executor.instances=2 --
conf spark.executor.memory=2G --conf spark.executor.cores=2 --conf
 spark.driver.cores=1"
  }
}' \
--configuration-overrides '{
  "monitoringConfiguration": {
    "cloudWatchMonitoringConfiguration": {
      "logGroupName": "my_log_group_name",
      "logStreamNamePrefix": "my_log_stream_prefix"
    },
    "s3MonitoringConfiguration": {
       "logUri": "s3://DOC-EXAMPLE-BUCKET-LOGGING"
    }
  }
}'
```

Contoh file query SQL ditampilkan di bawah ini. Anda harus memiliki penyimpanan file eksternal, seperti S3, tempat data untuk tabel disimpan.

```
CREATE DATABASE demo;
CREATE EXTERNAL TABLE IF NOT EXISTS demo.amazonreview( marketplace string,
 customer_id string, review_id  string, product_id  string, product_parent  string,
```

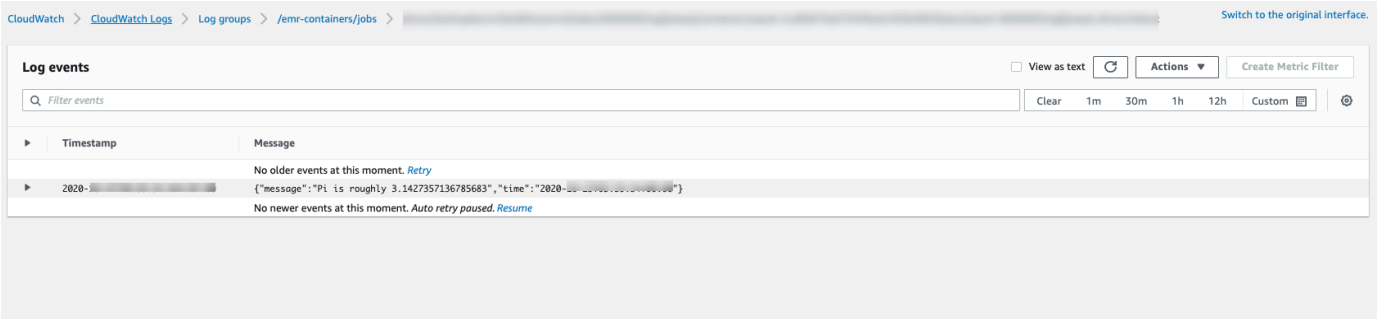
```
 product_title  string, star_rating  integer, helpful_votes  integer, total_votes
  integer, vine  string, verified_purchase  string, review_headline  string,
 review_body  string, review_date  date, year  integer) STORED AS PARQUET LOCATION
 's3://URI to parquet files';
SELECT count(*) FROM demo.amazonreview;
SELECT count(*) FROM demo.amazonreview WHERE star_rating = 3;
```

Output untuk pekerjaan ini akan tersedia di log stdout driver di S3 atau CloudWatch, tergantung pada`monitoringConfiguration` yang dikonfigurasi.

4. Anda juga dapat membuat file JSON dengan parameter tertentu untuk menjalankan tugas Anda. Kemudian jalankan start-job-run perintah dengan jalur ke file JSON. Untuk informasi selengkapnya, lihat Kirim tugas berjalan. Untuk detail lebih lanjut tentang mengonfigurasi parameter untuk menjalankan tugas berjalan, lihat Opsi untuk mengonfigurasi tugas berjalan.

   Untuk memantau kemajuan tugas atau kegagalan debug, Anda dapat memeriksa log yang diunggah ke Amazon S3, CloudWatch Logs, Logs, atau keduanya. Lihat jalur log di Amazon S3 di Konfigurasi tugas berjalan untuk menggunakan log S3 dan untuk Cloudwatch logs di Konfigurasi tugas berjalan untuk menggunakan CloudWatch Log. Untuk melihat log di CloudWatch Log, ikuti petunjuk di bawah ini.

   - Buka CloudWatch konsol di https://console.aws.amazon.com/cloudwatch/.
   - Di panel Navigasi, pilih Log. Lalu pilih Grup log.
   - Pilih grup log untuk Amazon EMR di EKS kemudian lihat log acara yang diunggah.



Important

Pekerjaan memiliki kebijakan coba ulang yang dikonfigurasi secara default. Untuk informasi tentang cara mengubah atau menonaktifkan konfigurasi, lihat Menggunakan kebijakan coba ulang pekerjaan.

Tautan ke Amazon EMR pada panduan praktik terbaik EKS GitHub

Kami telah membangun Amazon EMR pada Panduan Praktik Terbaik EKS menggunakan kolaborasi komunitas open source sehingga kami dapat melakukan iterasi dengan cepat dan memberikan rekomendasi untuk berbagai kasus penggunaan. Kami menyarankan Anda menggunakan panduan praktik terbaik Amazon EMR on EKS untuk bagian tersebut. Pilih tautan di setiap bagian untuk pergi ke GitHub situs.

Keamanan

> **Note**
>
> Untuk informasi lebih lanjut tentang keamanan dengan Amazon EMR di EKS, lihatPraktik terbaik keamanan Amazon EMR di EKS.

Praktik terbaik enkripsi: cara menggunakan enkripsi untuk data at rest dan transit.

Mengelola keamanan jaringan menjelaskan cara mengonfigurasi grup keamanan untuk Pod untuk Amazon EMR di EKS saat Anda terhubung ke sumber data yang dihosting Layanan AWS seperti Amazon RDS dan Amazon Redshift.

Menggunakan manajer AWS rahasia untuk menyimpan rahasia.

tugas Pyspark tugas Pyspark

Pengiriman pekerjaan Pyspark: menentukan berbagai jenis kemasan untuk aplikasi PySpark menggunakan format kemasan seperti zip, telur, roda, dan pex.

Penyimpanan

Menggunakan volume EBS:: cara menggunakan penyediaan statis dan dinamis untuk pekerjaan yang membutuhkan volume EBS.

Menggunakan volume Amazon FSx for Lustre: cara menggunakan penyediaan statis dan dinamis untuk pekerjaan yang membutuhkan volume Amazon FSx for Luster.

Menggunakan volume penyimpanan Instance: cara menggunakan volume penyimpanan instans untuk pemrosesan pekerjaan.

Integrasi Metastore

Menggunakan Hive metastore: menawarkan cara yang berbeda untuk menggunakan metastore Hive.

Menggunakan AWS Glue: menawarkan berbagai cara untuk mengkonfigurasi katalog AWS Glue.

Debugging

Menggunakan debugging Spark: cara mengubah level log.

Menghubungkan ke Spark UI pada pod driver.

Cara menggunakan server riwayat Spark yang di-host sendiri dengan Amazon EMR di EKS.

Memecahkan Masalah Masalah Masalah Amazon EMR di EKS

Pemecahan masalah.

penempatan simpul simpul simpul

Menggunakan selektor node Kubernetes untuk `single-az` dan kasus penggunaan lainnya.

Menggunakan penempatan simpul Fargate.

Performa

Menggunakan Dynamic Resource Allocation (DRA).

Praktik terbaik EKS untuk plugin Amazon VPC Container Network Interface (CNI), Cluster Autoscaler, dan Core DNS.

Optimalisasi biaya

Menggunakan instans spot: Praktik terbaik instans spot Amazon EC2 dan cara menggunakan fitur dekomisi node Spark.

Menggunakan AWS Outposts

Jalankan Amazon EMR di EKS menggunakan Amazon EMR di EKS menggunakan AWS Outposts

Menyesuaikan gambar Docker untuk Amazon EMR di EKS

Anda dapat menggunakan gambar Docker yang disesuaikan dengan Amazon EMR di EKS. Menyesuaikan Amazon EMR pada gambar waktu aktif EKS memberikan manfaat sebagai berikut:

- Menggabungkan ketergantungan aplikasi dan lingkungan waktu aktif menjadi kontainer tetap tunggal yang mempromosikan portabilitas dan menyederhanakan manajemen ketergantungan untuk setiap beban kerja.
- Menginstal dan mengkonfigurasi paket yang dioptimalkan untuk beban kerja Anda. Paket ini mungkin tidak tersedia secara luas dalam distribusi publik dari waktu aktif Amazon EMR.
- Integrasikan Amazon EMR pada EKS dengan proses membangun, menguji, dan penyebaran yang ada saat ini dalam organisasi Anda, termasuk pengembangan dan pengujian lokal.
- Terapkan proses keamanan yang telah ditetapkan, seperti pemindaian gambar, yang memenuhi persyaratan kepatuhan dan tata kelola dalam organisasi Anda.

Topik

Cara menyesuaikan gambar Docker

Ambil langkah-langkah berikut untuk menyesuaikan gambar Docker untuk Amazon EMR di EKS.

Berikut adalah opsi lain yang mungkin ingin Anda pertimbangkan saat menyesuaikan gambar Docker:

- Sesuaikan gambar Docker untuk titik akhir interaktif
- Bekerja dengan gambar multi-arsitektur

Prasyarat

- Selesaikan Menyiapkan Amazon EMR di EKS langkah-langkah untuk Amazon EMR di EKS.
- Instal Docker di lingkungan Anda. Untuk informasi lebih lanjut, lihat Get Docker.

Langkah 1: Ambil gambar dasar dari Amazon Elastic Container Registry (Amazon ECR)

Gambar dasar berisi runtime Amazon EMR dan konektor yang digunakan untuk mengakses layanan lain. AWS Untuk Amazon EMR 6.9.0 dan yang lebih tinggi, Anda bisa mendapatkan gambar dasar dari Galeri Publik Amazon ECR. Jelajahi galeri untuk menemukan tautan gambar dan tarik gambar ke ruang kerja lokal Anda. Misalnya, untuk rilis Amazon EMR 7.0.0, `docker pull` perintah berikut memberi Anda gambar dasar standar terbaru. Anda dapat mengganti `emr-7.0.0:latest` dengan `emr-7.0.0-spark-rapids:latest` untuk mengambil gambar yang memiliki akselerator Nvidia RAPIDS. Anda juga dapat mengganti `emr-7.0.0:latest` dengan `emr-7.0.0-java11:latest` untuk mengambil gambar dengan runtime Java 11.

```
docker pull public.ecr.aws/emr-on-eks/spark/emr-7.0.0:latest
```

Jika Anda ingin mengambil gambar dasar untuk Amazon EMR 6.9.0 atau rilis ealier, atau jika Anda lebih suka mengambil dari akun registri Amazon ECR di setiap Wilayah, gunakan langkah-langkah berikut:

1. Pilih URI gambar dasar. URI gambar mengikuti format ini, *ECR-registry-account*`.dkr.ecr.`*Region*`.amazonaws.com/spark/`*container-image-tag*, seperti yang ditunjukkan contoh berikut.

   ```
   895885662937.dkr.ecr.us-west-2.amazonaws.com/spark/emr-6.6.0:latest
   ```

   Untuk memilih gambar dasar di Wilayah Anda, lihat Cara memilih URI gambar dasar.
2. Masuk ke repositori Amazon ECR di mana gambar dasar disimpan. Ganti *895885662937* dan *us-west-2* dengan akun registri Amazon ECR dan Wilayah AWS yang telah Anda pilih.

```
aws ecr get-login-password --region us-west-2 | docker login --username AWS --
password-stdin 895885662937.dkr.ecr.us-west-2.amazonaws.com
```

3. Tarik gambar dasar ke Workspace lokal Anda. Ganti *emr-6.6.0: latest* dengan tag gambar kontainer yang telah Anda pilih.

```
docker pull 895885662937.dkr.ecr.us-west-2.amazonaws.com/spark/emr-6.6.0:latest
```

Langkah 2: Sesuaikan gambar dasar

Lakukan langkah-langkah berikut untuk menyesuaikan gambar dasar yang telah Anda tarik dari Amazon ECR.

1. Buat `Dockerfile` baru di Workspace lokal Anda.
2. Edit `Dockerfile` yang baru saja Anda buat dan tambahkan konten berikut. `Dockerfile` ini menggunakan gambar kontainer yang telah Anda tarik dari `895885662937.dkr.ecr.us-west-2.amazonaws.com/spark/emr-6.6.0:latest`.

```
FROM 895885662937.dkr.ecr.us-west-2.amazonaws.com/spark/emr-6.6.0:latest
USER root
### Add customization commands here ####
USER hadoop:hadoop
```

3. Tambahkan perintah di `Dockerfile` untuk menyesuaikan gambar dasar. Sebagai contoh, tambahkan perintah untuk menginstal pustaka Python, seperti yang ditunjukkan `Dockerfile` berikut.

```
FROM 895885662937.dkr.ecr.us-west-2.amazonaws.com/spark/emr-6.6.0:latest
USER root
RUN pip3 install --upgrade boto3 pandas numpy // For python 3
USER hadoop:hadoop
```

4. Dari direktori yang sama di mana `Dockerfile` dibuat, jalankan perintah berikut untuk membangun gambar Docker. Berikan nama untuk gambar Docker, misalnya, *emr6.6_custom*.

```
docker build -t emr6.6_custom .
```

Langkah 3: (Opsional tapi disarankan) Validasi gambar kustom

Kami menyarankan Anda menguji kompatibilitas gambar kustom Anda sebelum menerbitkannya. Anda dapat menggunakan EMR Amazon pada CLI gambar khusus EKS untuk memeriksa apakah gambar Anda memiliki struktur file yang diperlukan dan konfigurasi yang benar untuk berjalan di Amazon EMR di EKS.

> **Note**
>
> Amazon EMR pada CLI gambar khusus EKS tidak dapat mengonfirmasi bahwa gambar Anda bebas dari kesalahan. Berhati-hatilah saat menghapus dependensi dari gambar dasar.

Ambil langkah-langkah berikut untuk memvalidasi gambar kustom Anda.

1. Unduh dan instal Amazon EMR pada CLI gambar khusus EKS. Untuk informasi selengkapnya, lihat Amazon EMR di Panduan Instalasi CLI gambar khusus EKS.
2. Jalankan perintah berikut untuk menguji instalasi.

   ```
   emr-on-eks-custom-image --version
   ```

   Berikut ini menunjukkan contoh output.

   ```
   Amazon EMR on EKS Custom Image CLI
   Version: x.xx
   ```

3. Jalankan perintah berikut untuk memvalidasi gambar kustom Anda.

   ```
   emr-on-eks-custom-image validate-image -i image_name -r release_version [-
   t image_type]
   ```

   - `-i`menentukan URI gambar lokal yang perlu divalidasi. Ini bisa berupa URI gambar, nama atau tag apa pun yang Anda tentukan untuk gambar Anda.
   - `-r`menentukan versi rilis yang tepat untuk gambar dasar, misalnya,`emr-6.6.0-latest`.
   - `-t`menentukan jenis gambar. Jika ini adalah gambar Spark, masukan`spark`. Nilai default-nya adalah `spark`. EMR Amazon saat ini pada versi CLI gambar khusus EKS hanya mendukung gambar runtime Spark.

Jika Anda menjalankan perintah dengan sukses dan gambar kustom memenuhi semua konfigurasi dan struktur file yang diperlukan, output yang dikembalikan menampilkan hasil dari semua pengujian, seperti contoh berikut menunjukkan.

```
Amazon EMR on EKS Custom Image Test
Version: x.xx
... Checking if docker cli is installed
... Checking Image Manifest
[INFO] Image ID: xxx
[INFO] Created On: 2021-05-17T20:50:07.986662904Z
[INFO] Default User Set to hadoop:hadoop : PASS
[INFO] Working Directory Set to /home/hadoop : PASS
[INFO] Entrypoint Set to /usr/bin/entrypoint.sh : PASS
[INFO] SPARK_HOME is set with value: /usr/lib/spark : PASS
[INFO] JAVA_HOME is set with value: /etc/alternatives/jre : PASS
[INFO] File Structure Test for spark-jars in /usr/lib/spark/jars: PASS
[INFO] File Structure Test for hadoop-files in /usr/lib/hadoop: PASS
[INFO] File Structure Test for hadoop-jars in /usr/lib/hadoop/lib: PASS
[INFO] File Structure Test for bin-files in /usr/bin: PASS
... Start Running Sample Spark Job
[INFO] Sample Spark Job Test with local:///usr/lib/spark/examples/jars/spark-
examples.jar : PASS
----------------------------------------------------------------
Overall Custom Image Validation Succeeded.
----------------------------------------------------------------
```

Jika gambar kustom tidak memenuhi konfigurasi atau struktur file yang diperlukan, pesan kesalahan akan terjadi. Output yang dikembalikan memberikan informasi tentang konfigurasi atau struktur file yang salah.

Langkah 4: Publikasikan gambar khusus

Publikasikan gambar Docker baru ke registri Amazon ECR Anda.

1. Jalankan perintah berikut untuk membuat repositori Amazon ECR untuk menyimpan gambar Docker Anda. *Berikan nama untuk repositori Anda, misalnya, emr6.6_custom_repo.* Ganti *us-west-2* dengan Wilayah Anda.

```
aws ecr create-repository \
```

```
    --repository-name emr6.6_custom_repo \
    --image-scanning-configuration scanOnPush=true \
    --region us-west-2
```

Untuk informasi lebih lanjut, lihat Membuat repositori dalam Panduan Pengguna Amazon ECR.

2. Jalankan perintah berikut untuk mengautentikasi ke registri default Anda.

```
aws ecr get-login-password --region us-west-2 | docker login --username AWS --
password-stdin aws_account_id.dkr.ecr.us-west-2.amazonaws.com
```

Untuk informasi selengkapnya, lihat Autentikasi ke registri default Anda di Panduan Pengguna Amazon ECR.

3. Tandai dan publikasikan gambar ke repositori Amazon ECR yang Anda buat.

Tandai gambar.

```
docker tag emr6.6_custom aws_account_id.dkr.ecr.us-
west-2.amazonaws.com/emr6.6_custom_repo
```

Tekan gambar.

```
docker push aws_account_id.dkr.ecr.us-west-2.amazonaws.com/emr6.6_custom_repo
```

Untuk informasi selengkapnya, lihat Menekan gambar ke Amazon ECR di Panduan Pengguna Amazon ECR.

Langkah 5: Kirim beban kerja Spark di Amazon EMR menggunakan gambar khusus

Setelah gambar kustom dibangun dan diterbitkan, Anda dapat mengirimkan tugas Amazon EMR di EKS menggunakan gambar kustom.

Pertama, buat start-job-run-request file.json dan tentukan `spark.kubernetes.container.image` parameter untuk referensi gambar kustom, seperti contoh file JSON berikut menunjukkan.

> **Note**
>
> Anda dapat menggunakan `local://` skema untuk merujuk ke file yang tersedia dalam gambar kustom seperti yang ditunjukkan dengan `entryPoint` argumen dalam cuplikan JSON di bawah ini. Anda juga dapat menggunakan `local://` skema untuk merujuk ke dependensi aplikasi. Semua file dan dependensi yang dirujuk menggunakan `local://` skema harus sudah ada di jalur yang ditentukan dalam gambar kustom.

```
{
    "name": "spark-custom-image",
    "virtualClusterId": "virtual-cluster-id",
    "executionRoleArn": "execution-role-arn",
    "releaseLabel": "emr-6.6.0-latest",
    "jobDriver": {
      "sparkSubmitJobDriver": {
        "entryPoint": "local:///usr/lib/spark/examples/jars/spark-examples.jar",
        "entryPointArguments": [
                  "10"
             ],
         "sparkSubmitParameters": "--class org.apache.spark.examples.SparkPi --conf
 spark.kubernetes.container.image=123456789012.dkr.ecr.us-west-2.amazonaws.com/
emr6.6_custom_repo"
       }
    }
}
```

Anda juga dapat mereferensikan gambar kustom dengan `applicationConfiguration` properti seperti contoh berikut menunjukkan.

```
{
    "name": "spark-custom-image",
    "virtualClusterId": "virtual-cluster-id",
    "executionRoleArn": "execution-role-arn",
    "releaseLabel": "emr-6.6.0-latest",
    "jobDriver": {
      "sparkSubmitJobDriver": {
        "entryPoint": "local:///usr/lib/spark/examples/jars/spark-examples.jar",
```

```
        "entryPointArguments": [
                  "10"
              ],
         "sparkSubmitParameters": "--class org.apache.spark.examples.SparkPi"
       }
    },
    "configurationOverrides": {
        "applicationConfiguration": [
            {
                "classification": "spark-defaults",
                "properties": {
                    "spark.kubernetes.container.image": "123456789012.dkr.ecr.us-
west-2.amazonaws.com/emr6.6_custom_repo"
                }
            }
        ]
    }
}
```

Kemudian jalankan perintah `start-job-run` untuk mengirimkan tugas.

```
aws emr-containers start-job-run --cli-input-json file://./start-job-run-request.json
```

Dalam contoh JSON di atas, ganti *`emr-6.6.0-latest dengan`* versi rilis Amazon EMR Anda. Kami sangat menyarankan Anda menggunakan versi `-latest` rilis untuk memastikan bahwa versi yang dipilih berisi pembaruan keamanan terbaru. Untuk informasi selengkapnya tentang versi rilis Amazon EMR dan tag gambarnya, lihat. Cara memilih URI gambar dasar

> **Note**
>
> Anda dapat menggunakan `spark.kubernetes.driver.container.image` dan `spark.kubernetes.executor.container.image` untuk menentukan gambar yang berbeda untuk driver dan pod eksekutor.

Sesuaikan gambar Docker untuk titik akhir interaktif

Anda juga dapat menyesuaikan gambar Docker untuk titik akhir interaktif sehingga Anda dapat menjalankan gambar kernel dasar yang disesuaikan. Ini membantu Anda memastikan bahwa Anda memiliki dependensi yang Anda butuhkan saat menjalankan beban kerja interaktif dari EMR Studio.

1. Ikuti Langkah 1-4 yang diuraikan di atas untuk menyesuaikan gambar Docker. Untuk rilis Amazon EMR 6.9.0 dan yang lebih baru, Anda bisa mendapatkan URI gambar dasar dari Galeri Publik Amazon ECR. Untuk rilis sebelum Amazon EMR 6.9.0, Anda bisa mendapatkan gambar di akun Amazon ECR Registry di masing-masing akunWilayah AWS, dan satu-satunya perbedaan adalah URI gambar dasar di Dockerfile Anda. URI gambar dasar mengikuti format:

```
ECR-registry-account.dkr.ecr.Region.amazonaws.com/notebook-spark/container-image-tag
```

Anda perlu menggunakan `notebook-spark` URI gambar dasar, bukan`spark`. Gambar dasar berisi runtime Spark dan kernel notebook yang berjalan dengannya. Untuk informasi selengkapnya tentang memilih tag gambar Wilayah dan kontainer, lihatCara memilih URI gambar dasar.

> **Note**
>
> Saat ini hanya penggantian gambar dasar yang didukung dan memperkenalkan kernel yang sama sekali baru dari jenis lain selain yang AWS disediakan gambar dasar tidak didukung.

2. Buat endpoint interaktif yang dapat digunakan dengan gambar kustom.

Pertama, buat file JSON yang disebut `custom-image-managed-endpoint.json` dengan konten berikut.

```
{
    "name": "endpoint-name",
    "virtualClusterId": "virtual-cluster-id",
    "type": "JUPYTER_ENTERPRISE_GATEWAY",
    "releaseLabel": "emr-6.6.0-latest",
    "executionRoleArn": "execution-role-arn",
    "certificateArn": "certificate-arn",
    "configurationOverrides": {
        "applicationConfiguration": [
            {
                "classification": "jupyter-kernel-overrides",
                "configurations": [
                    {
                        "classification": "python3",
                        "properties": {
```

```
                            "container-image": "123456789012.dkr.ecr.us-
west-2.amazonaws.com/custom-notebook-python:latest"
                        }
                    },
                    {
                        "classification": "spark-python-kubernetes",
                        "properties": {
                            "container-image": "123456789012.dkr.ecr.us-
west-2.amazonaws.com/custom-notebook-spark:latest"
                        }
                    }
                ]
            }
        ]
    }
}
```

Selanjutnya, buat endpoint interaktif menggunakan konfigurasi yang ditentukan dalam file JSON, seperti contoh berikut menunjukkan.

```
aws emr-containers create-managed-endpoint --cli-input-json custom-image-managed-
endpoint.json
```

Untuk informasi selengkapnya, lihat Membuat titik akhir interaktif untuk klaster virtual Anda.

3. Connect ke endpoint interaktif melalui EMR Studio. Untuk informasi selengkapnya, lihat Menghubungkan dari Studio.

Bekerja dengan gambar multi-arsitektur

Amazon EMR di EKS mendukung gambar kontainer multi-arsitektur untuk Amazon Elastic Container Registry (Amazon ECR) Registry ECR). Untuk informasi selengkapnya, lihat Memperkenalkan gambar kontainer multi-arsitektur untuk Amazon ECR.

Amazon EMR pada gambar khusus EKS mendukung instans EC2 berbasis AWS Graviton dan instans EC2 berbasis non-Graviton. Gambar berbasis Graviton disimpan dalam repositori gambar yang sama di Amazon ECR sebagai gambar berbasis non-Graviton.

Misalnya, untuk memeriksa daftar manifes Docker untuk gambar 6.6.0, jalankan perintah berikut.

```
docker manifest inspect 895885662937.dkr.ecr.us-west-2.amazonaws.com/spark/
emr-6.6.0:latest
```

Berikut adalah outputnya. `arm64`Arsitekturnya untuk contoh Graviton. `amd64`Ini untuk contoh non-Graviton.

```
{
   "schemaVersion": 2,
   "mediaType": "application/vnd.docker.distribution.manifest.list.v2+json",
   "manifests": [
      {
         "mediaType": "application/vnd.docker.distribution.manifest.v2+json",
         "size": 1805,
         "digest":
 "xxx123:6b971cb47d11011ab3d45fff925e9442914b4977ae0f9fbcdcf5cfa99a7593f0",
         "platform": {
            "architecture": "arm64",
            "os": "linux"
         }
      },
      {
         "mediaType": "application/vnd.docker.distribution.manifest.v2+json",
         "size": 1805,
         "digest":
 "xxx123:6f2375582c9c57fa9838c1d3a626f1b4fc281e287d2963a72dfe0bd81117e52f",
         "platform": {
            "architecture": "amd64",
            "os": "linux"
         }
      }
   ]
}
```

Ambil langkah-langkah berikut untuk membuat gambar multi-arsitektur:

1. Buat `Dockerfile` dengan konten berikut sehingga Anda dapat menarik `arm64` gambar.

   ```
   FROM --platform=arm64 895885662937.dkr.ecr.us-west-2.amazonaws.com/spark/
   emr-6.6.0:latest
   USER root

   RUN pip3 install boto3 // install customizations here
   ```

```
USER hadoop:hadoop
```

2. Ikuti petunjuk di Memperkenalkan gambar wadah multi-arsitektur untuk Amazon ECR untuk membuat gambar multi-arsitektur.

> **Note**
>
> Anda harus membuat `arm64` gambar pada `arm64` instance. Demikian pula, Anda harus membangun `amd64` gambar pada `amd64` instance.

   Anda juga dapat membuat gambar multi-arsitektur tanpa membangun setiap jenis instance tertentu dengan perintah Docker`buildx`. Untuk informasi selengkapnya, lihat Memanfaatkan dukungan arsitektur multi-CPU.

3. Setelah Anda membangun gambar multi-arsitektur, Anda dapat mengirimkan pekerjaan dengan `spark.kubernetes.container.image` parameter yang sama dan mengarahkannya ke gambar. Dalam cluster heterogen dengan instance EC2 AWS berbasis Graviton dan non-Graviton, instance menentukan gambar arsitektur yang benar berdasarkan arsitektur instance yang menarik gambar.

Cara memilih URI gambar dasar

> **Note**
>
> Untuk rilis Amazon EMR 6.9.0 dan yang lebih baru, Anda dapat mengambil gambar dasar dari Galeri Publik Amazon ECR, jadi Anda tidak perlu membuat URI gambar dasar sebagai petunjuk langsung pada halaman ini. Untuk menemukan tag gambar kontainer untuk gambar dasar Anda, lihat halaman catatan rilis untuk rilis Amazon EMR yang sesuai di EKS.

Gambar Docker dasar yang dapat Anda pilih disimpan di Amazon Elastic Container Registry (Amazon ECR). URI gambar mengikuti format ini:*ECR-registry-account*`.dkr.ecr.`*Region*`.amazonaws.com/spark/`*container-image-tag*, seperti contoh berikut menunjukkan.

```
895885662937.dkr.ecr.us-west-2.amazonaws.com/spark/emr-7.0.0:latest
```

URI gambar untuk endpoint interaktif mengikuti format ini:*ECR-registry-account*.dkr.ecr.*Region*.amazonaws.com/notebook-spark/*container-image-tag*, seperti contoh berikut menunjukkan. Anda perlu menggunakan `notebook-spark` URI gambar dasar, bukan`spark`.

```
895885662937.dkr.ecr.us-west-2.amazonaws.com/notebook-spark/emr-7.0.0:latest
```

Demikian pula, untuk `python3` gambar non-Spark untuk titik akhir interaktif, URI gambar adalah. *ECR-registry-account*.dkr.ecr.*Region*.amazonaws.com/notebook-python/*container-image-tag* Contoh URI berikut diformat dengan benar:

```
895885662937.dkr.ecr.us-west-2.amazonaws.com/notebook-python/emr-7.0.0:latest
```

Untuk menemukan tag gambar kontainer untuk gambar dasar Anda, lihat halaman catatan rilis untuk rilis Amazon EMR yang sesuai di EKS.

Akun registri Amazon ECR berdasarkan Wilayah

Untuk menghindari latensi jaringan yang tinggi, tarik gambar dasar dari yang terdekatWilayah AWS. Pilih akun registri Amazon ECR yang sesuai dengan Wilayah tempat Anda menarik gambar berdasarkan tabel berikut.

Wilayah	Akun registri Amazon ECR
ap-northeast-1	059004520145
ap-northeast-2	996579266876
ap-south-1	235914868574
ap-southeast-1	671219180197
ap-southeast-2	038297999601
ca-central-1	351826393999
eu-central-1	107292555468
eu-north-1	830386416364

Wilayah	Akun registri Amazon ECR	
eu-west-1	483788554619	
eu-west-2	118780647275	
eu-west-3	307523725174	
sa-east-1	052806832358	
us-east-1	755674844232	
us-east-2	711395599931	
us-west-1	608033475327	
us-west-2	895885662937	

Pertimbangan-pertimbangan

Saat Anda menyesuaikan gambar Docker, Anda dapat memilih runtime yang tepat untuk pekerjaan Anda pada tingkat granular. Ikuti praktik terbaik ini saat Anda menggunakan fitur ini:

- Keamanan menjadi tanggung jawab bersama antara AWS dan Anda. Anda bertanggung jawab atas keamanan menambal binari yang Anda tambahkan ke gambar. Ikuti Praktik terbaik keamanan Amazon EMR di EKS, terutama Dapatkan pembaruan keamanan terbaru untuk gambar kustom dan Terapkan prinsip hak istimewa paling rendah.
- Saat Anda menyesuaikan gambar dasar, Anda harus mengubah pengguna Docker `hadoop:hadoop` agar pekerjaan tidak berjalan dengan pengguna root.
- Amazon EMR di EKS memasang file di atas konfigurasi untuk gambar, seperti, saat dijalankan`spark-defaults.conf`. Untuk mengganti file konfigurasi ini, kami sarankan Anda menggunakan `applicationOverrides` parameter selama pengiriman pekerjaan dan tidak secara langsung memodifikasi file dalam gambar kustom.
- Amazon EMR di EKS memasang folder tertentu saat dijalankan. Modifikasi apa pun yang Anda buat pada folder ini tidak tersedia di wadah. Jika Anda ingin menambahkan aplikasi atau dependensinya untuk gambar kustom, kami sarankan Anda memilih direktori yang bukan bagian dari jalur yang telah ditentukan berikut:

  - `/var/log/fluentd`
  - `/var/log/spark/user`
  - `/var/log/spark/apps`
  - `/mnt`
  - `/tmp`
  - `/home/hadoop`
- Anda dapat mengunggah gambar yang disesuaikan ke repositori yang kompatibel dengan Docker, seperti Amazon ECR, Docker Hub, atau repositori perusahaan swasta. Untuk informasi selengkapnya tentang cara mengonfigurasi otentikasi klaster Amazon EKS dengan repositori Docker yang dipilih, lihat Tarik Gambar dari Registri Pribadi.

Menjalankan pekerjaan Flink dengan Amazon EMR di EKS

Amazon EMR merilis 6.13.0 dan lebih tinggi mendukung Amazon EMR di EKS dengan Apache Flink, atau operator Flink Kubernetes, sebagai model pengiriman pekerjaan untuk Amazon EMR di EKS. Dengan Amazon EMR di EKS dengan Apache Flink, Anda dapat menerapkan dan mengelola aplikasi Flink dengan runtime rilis Amazon EMR di kluster Amazon EKS Anda sendiri. Setelah Anda menerapkan operator Flink Kubernetes di cluster Amazon EKS Anda, Anda dapat langsung mengirimkan aplikasi Flink dengan operator. Operator mengelola siklus hidup aplikasi Flink.

Topik

Operator Flink Kubernetes

Halaman-halaman berikut menjelaskan cara mengatur dan menggunakan operator Flink Kubernetes untuk menjalankan pekerjaan Flink dengan Amazon EMR di EKS.

Topik

Menyiapkan operator Flink Kubernetes untuk Amazon EMR di EKS

Selesaikan tugas-tugas berikut untuk menyiapkan sebelum Anda menginstal operator Flink Kubernetes di Amazon EKS. Jika Anda sudah mendaftar untuk Amazon Web Services (AWS) dan

telah menggunakan Amazon EKS, Anda hampir siap untuk menggunakan Amazon EMR di EKS. Selesaikan tugas-tugas berikut untuk menyiapkan operator Flink di Amazon EKS. Jika Anda telah menyelesaikan salah satu prasyarat, Anda dapat melewatinya dan melanjutkan ke yang berikutnya.

- Instal AWS CLI— Jika Anda sudah menginstalAWS CLI, konfirmasikan bahwa Anda memiliki versi terbaru.
- Instal eksctl - eksctl adalah alat baris perintah yang Anda gunakan untuk berkomunikasi dengan Amazon EKS.
- Instal Helm — Manajer paket Helm untuk Kubernetes membantu Anda menginstal dan mengelola aplikasi di klaster Kubernetes Anda.
- Siapkan cluster Amazon EKS — Ikuti langkah-langkah untuk membuat cluster Kubernetes baru dengan node di Amazon EKS.
- Pilih label rilis EMR Amazon (rilis 6.13.0 atau lebih tinggi) — operator Flink Kubernetes didukung dengan Amazon EMR rilis 6.13.0 dan yang lebih tinggi.
- Aktifkan Peran IAM untuk Akun Layanan (IRSA) di klaster Amazon EKS.
- Buat peran eksekusi pekerjaan.
- Perbarui kebijakan kepercayaan dari peran eksekusi pekerjaan.
- Buat peran eksekusi operator. Langkah ini opsional. Anda dapat menggunakan peran yang sama untuk pekerjaan dan operator Flink. Jika Anda ingin memiliki peran IAM yang berbeda untuk operator Anda, Anda dapat membuat peran terpisah.
- Perbarui kebijakan kepercayaan dari peran eksekusi operator. Anda harus secara eksplisit menambahkan satu entri kebijakan kepercayaan untuk peran yang ingin Anda gunakan untuk akun layanan operator Amazon EMR Flink Kubernetes. Anda dapat mengikuti format contoh ini:

```
{
   "Version": "2012-10-17",
   "Statement": [
       {
           "Effect": "Allow",
           "Principal": {
               "Federated": "arn:aws:iam::ACCOUNT_ID:oidc-provider/OIDC_PROVIDER"
           },
           "Action": "sts:AssumeRoleWithWebIdentity",
           "Condition": {
               "StringLike": {
                   "OIDC_PROVIDER:sub": "system:serviceaccount:NAMESPACE:emr-
containers-sa-flink-operator"
```

```
                }
            }
        }
    ]
}
```

Memulai dengan operator Flink Kubernetes untuk Amazon EMR di EKS

Topik ini membantu Anda mulai menggunakan operator Flink Kubernetes di Amazon EKS dengan menerapkan penerapan Flink.

Menginstal operator

Gunakan langkah-langkah berikut untuk menginstal operator Kubernetes untuk Apache Flink.

1. Jika Anda belum melakukannya, selesaikan langkah-langkahnyathe section called “Menyiapkan”.
2. Instal *cert-manager* (sekali per Amazon EKS cluster) untuk mengaktifkan penambahan komponen webhook.

   ```
   kubectl apply -f https://github.com/cert-manager/cert-manager/releases/download/
   v1.12.0/cert-manager.yaml
   ```

3. Instal bagan Helm.

   ```
   export VERSION=7.0.0 # The Amazon EMR release version
   export NAMESPACE=The Kubernetes namespace to deploy the operator

   helm install flink-kubernetes-operator-demo \
   oci://public.ecr.aws/emr-on-eks/flink-kubernetes-operator \
   --version $VERSION \
   --namespace $NAMESPACE
   ```

   Contoh output:

   ```
   NAME: flink-kubernetes-operator-demo
   LAST DEPLOYED: Tue May 31 17:38:56 2022
   NAMESPACE: $NAMESPACE
   STATUS: deployed
   REVISION: 1
   TEST SUITE: None
   ```

4. Tunggu hingga penerapan selesai dan verifikasi instalasi bagan.

```
kubectl wait deployment flink-kubernetes-operator-demo --namespace $NAMESPACE --for
 condition=Available=True --timeout=30s
```

5. Anda akan melihat pesan berikut saat penerapan selesai.

```
deployment.apps/flink-kubernetes-operator-demo condition met
```

6. Gunakan perintah berikut untuk melihat operator yang digunakan.

```
helm list --namespace $NAMESPACE
```

Berikut ini menunjukkan contoh keluaran, di mana versi aplikasi `x.y.z-amzn-n` akan sesuai dengan versi operator Flink untuk EMR Amazon Anda pada rilis EKS. Untuk informasi selengkapnya, lihat Rilis yang didukung untuk Amazon EMR di EKS dengan Apache Flink.

```
NAME                            NAMESPACE    REVISION    UPDATED
               STATUS      CHART                                  APP VERSION

flink-kubernetes-operator-demo    $NAMESPACE   1           2023-02-22
 16:43:45.24148 -0500 EST    deployed    flink-kubernetes-operator-emr-7.0.0
 x.y.z-amzn-n
```

Menjalankan aplikasi Flink

Dengan Amazon EMR 6.13.0 dan yang lebih tinggi, Anda dapat menjalankan aplikasi Flink dengan operator Flink Kubernetes dalam mode Aplikasi di Amazon EMR di EKS. Dengan Amazon EMR 6.15.0 dan yang lebih tinggi, Anda juga dapat menjalankan aplikasi Flink dalam mode Sesi. Halaman ini menjelaskan kedua metode yang dapat Anda gunakan untuk menjalankan aplikasi Flink dengan Amazon EMR di EKS.

> **Note**
>
> Anda harus memiliki bucket Amazon S3 yang dibuat untuk menyimpan metadata ketersediaan tinggi saat mengirimkan pekerjaan Flink Anda. Jika Anda tidak ingin menggunakan fitur ini, Anda dapat menonaktifkannya. Ini diaktifkan secara default.

Prasyarat — Sebelum Anda dapat menjalankan aplikasi Flink dengan operator Flink Kubernetes, selesaikan langkah-langkah di dan. the section called “Menyiapkan” the section called “Menginstal operator”

Application mode

Dengan Amazon EMR 6.13.0 dan yang lebih tinggi, Anda dapat menjalankan aplikasi Flink dengan operator Flink Kubernetes dalam mode Aplikasi di Amazon EMR di EKS.

1. Buat `FlinkDeployment` file definisi file `basic-example-app-cluster.yaml` dengan contoh konten berikut:

```
apiVersion: flink.apache.org/v1beta1
kind: FlinkDeployment
metadata:
  name: basic-example-app-cluster
spec:
  flinkConfiguration:
    taskmanager.numberOfTaskSlots: "2"
    state.checkpoints.dir: CHECKPOINT_S3_STORAGE_PATH
    state.savepoints.dir: SAVEPOINT_S3_STORAGE_PATH
  flinkVersion: v1_17
  executionRoleArn: JOB_EXECUTION_ROLE_ARN
  emrReleaseLabel: "emr-5.36.1-flink-latest" // 6.13 or higher
  jobManager:
    storageDir: HIGH_AVAILABILITY_STORAGE_PATH
    resource:
      memory: "2048m"
      cpu: 1
  taskManager:
    resource:
      memory: "2048m"
      cpu: 1
  job:
    # if you have your job jar in S3 bucket you can use that path as well
    jarURI: local:///opt/flink/examples/streaming/StateMachineExample.jar
    parallelism: 2
    upgradeMode: savepoint
    savepointTriggerNonce: 0
  monitoringConfiguration:
    cloudWatchMonitoringConfiguration:
       logGroupName: LOG_GROUP_NAME
```

2. Kirim penyebaran Flink dengan perintah berikut. Ini juga akan membuat `FlinkDeployment` objek bernama`basic-example-app-cluster`.

```
kubectl create -f example.yaml -n <NAMESPACE>
```

3. Akses UI Flink.

```
kubectl port-forward deployments/basic-example-app-cluster 8081 -n NAMESPACE
```

4. Buka `localhost:8081` untuk melihat pekerjaan Flink Anda secara lokal.
5. Bersihkan pekerjaan. Ingatlah untuk membersihkan artefak S3 yang dibuat untuk pekerjaan ini, seperti checkpointing, ketersediaan tinggi, metadata savepointing, dan log. CloudWatch

Untuk informasi selengkapnya tentang mengirimkan aplikasi ke Flink melalui operator Flink Kubernetes, lihat contoh operator Flink Kubernetes di folder di. `apache/flink-kubernetes-operator` GitHub

Session mode

Dengan Amazon EMR 6.15.0 dan yang lebih tinggi, Anda dapat menjalankan aplikasi Flink dengan operator Flink Kubernetes dalam mode Session di Amazon EMR di EKS.

1. Buat `FlinkDeployment` file definisi file `basic-example-session-cluster.yaml` dengan contoh konten berikut:

```
apiVersion: flink.apache.org/v1beta1
kind: FlinkDeployment
metadata:
  name: basic-example-session-cluster
spec:
  flinkConfiguration:
    taskmanager.numberOfTaskSlots: "2"
    state.checkpoints.dir: CHECKPOINT_S3_STORAGE_PATH
    state.savepoints.dir: SAVEPOINT_S3_STORAGE_PATH
  flinkVersion: v1_17
  executionRoleArn: JOB_EXECUTION_ROLE_ARN
  emrReleaseLabel: "emr-5.36.1-flink-latest"
  jobManager:
    storageDir: HIGH_AVAILABILITY_S3_STORAGE_PATH
```

```
    resource:
      memory: "2048m"
      cpu: 1
  taskManager:
    resource:
      memory: "2048m"
      cpu: 1
  monitoringConfiguration:
    s3MonitoringConfiguration:
       logUri:
    cloudWatchMonitoringConfiguration:
       logGroupName: LOG_GROUP_NAME
```

2. Kirim penyebaran Flink dengan perintah berikut. Ini juga akan membuat `FlinkDeployment` objek bernama`basic-example-session-cluster`.

```
kubectl create -f example.yaml -n NAMESPACE
```

3. Gunakan perintah berikut untuk mengonfirmasi bahwa cluster sesi `LIFECYCLE` adalah`STABLE`:

```
kubectl get flinkdeployments.flink.apache.org basic-example-session-cluster -
n NAMESPACE
```

Outputnya harus mirip dengan contoh berikut:

```
NAME                              JOB STATUS   LIFECYCLE STATE
basic-example-session-cluster                          STABLE
```

4. Buat file sumber daya definisi `FlinkSessionJob` khusus `basic-session-job.yaml` dengan contoh konten berikut:

```
apiVersion: flink.apache.org/v1beta1
kind: FlinkSessionJob
metadata:
  name: basic-session-job
spec:
  deploymentName: basic-session-deployment
  job:
    # If you have your job jar in an S3 bucket you can use that path.
    # To use jar in S3 bucket, set
```

```
    # OPERATOR_EXECUTION_ROLE_ARN (--set emrContainers.operatorExecutionRoleArn=
$OPERATOR_EXECUTION_ROLE_ARN)
    # when you install Spark operator
    jarURI: https://repo1.maven.org/maven2/org/apache/flink/flink-examples-
streaming_2.12/1.16.1/flink-examples-streaming_2.12-1.16.1-TopSpeedWindowing.jar
    parallelism: 2
    upgradeMode: stateless
```

5. Kirim pekerjaan sesi Flink dengan perintah berikut. Ini akan membuat `FlinkSessionJob` objek`basic-session-job`.

```
kubectl apply -f basic-session-job.yaml -n $NAMESPACE
```

6. Gunakan perintah berikut untuk mengonfirmasi bahwa cluster sesi `LIFECYCLE` adalah`STABLE`, dan `JOB STATUS` adalah`RUNNING`:

```
kubectl get flinkdeployments.flink.apache.org basic-example-session-cluster -
n NAMESPACE
```

   Outputnya harus mirip dengan contoh berikut:

```
NAME                              JOB STATUS   LIFECYCLE STATE
basic-example-session-cluster     RUNNING      STABLE
```

7. Akses UI Flink.

```
kubectl port-forward deployments/basic-example-session-cluster 8081 -n NAMESPACE
```

8. Buka `localhost:8081` untuk melihat pekerjaan Flink Anda secara lokal.
9. Bersihkan pekerjaan. Ingatlah untuk membersihkan artefak S3 yang dibuat untuk pekerjaan ini, seperti checkpointing, ketersediaan tinggi, metadata savepointing, dan log. CloudWatch

Keamanan

RBAC

Untuk menerapkan operator dan menjalankan pekerjaan Flink, kita harus membuat dua peran Kubernetes: satu operator dan satu peran pekerjaan. Amazon EMR membuat dua peran secara default saat Anda menginstal operator.

Peran operator

Kami menggunakan peran operator untuk mengelola `flinkdeployments` untuk membuat dan mengelola JobManager untuk setiap pekerjaan Flink dan sumber daya lainnya, seperti layanan.

Nama default peran operator adalah `emr-containers-sa-flink-operator` dan memerlukan izin berikut.

```
rules:
- apiGroups:
  - ""
  resources:
  - pods
  - services
  - events
  - configmaps
  - secrets
  - serviceaccounts
  verbs:
  - '*'
- apiGroups:
  - rbac.authorization.k8s.io
  resources:
  - roles
  - rolebindings
  verbs:
  - '*'
- apiGroups:
  - apps
  resources:
  - deployments
  - deployments/finalizers
  - replicasets
  verbs:
  - '*'
- apiGroups:
  - extensions
  resources:
  - deployments
  - ingresses
  verbs:
  - '*'
- apiGroups:
```

```
  - flink.apache.org
  resources:
  - flinkdeployments
  - flinkdeployments/status
  - flinksessionjobs
  - flinksessionjobs/status
  verbs:
  - '*'
- apiGroups:
  - networking.k8s.io
  resources:
  - ingresses
  verbs:
  - '*'
- apiGroups:
  - coordination.k8s.io
  resources:
  - leases
  verbs:
  - '*'
```

Peran Job

JobManager Menggunakan peran pekerjaan untuk membuat dan mengelola TaskManagers dan ConfigMaps untuk setiap pekerjaan.

```
rules:
- apiGroups:
  - ""
  resources:
  - pods
  - configmaps
  verbs:
  - '*'
- apiGroups:
  - apps
  resources:
  - deployments
  - deployments/finalizers
  verbs:
  - '*'
```

Menghapus instalasi operator Flink Kubernetes untuk Amazon EMR di EKS

Ikuti langkah-langkah berikut untuk menghapus instalasi operator Flink Kubernetes.

1. Hapus operator.

```
helm uninstall flink-kubernetes-operator-demo -n <NAMESPACE>
```

2. Hapus sumber daya Kubernetes yang tidak dihapus Helm.

```
kubectl delete serviceaccounts, roles, rolebindings -l emr-
containers.amazonaws.com/component=flink.operator --namespace <namespace>
kubectl delete crd flinkdeployments.flink.apache.org
 flinksessionjobs.flink.apache.org
```

3. (Opsional) Hapus cert-manager.

```
kubectl delete -f https://github.com/jetstack/cert-manager/releases/download/
v1.12.0/cert-manager.yaml
```

Kubernetes Asli

Amazon EMR merilis 6.13.0 dan dukungan yang lebih tinggi Flink Native Kubernetes sebagai alat baris perintah yang dapat Anda gunakan untuk mengirimkan dan menjalankan aplikasi Flink ke EMR Amazon di klaster EKS.

Topik

- Menyiapkan Flink Native Kubernetes untuk Amazon EMR di EKS
- Memulai dengan Kubernetes asli Flink untuk Amazon EMR di EKS
- Persyaratan keamanan akun JobManager layanan Flink untuk Native Kubernetes

Menyiapkan Flink Native Kubernetes untuk Amazon EMR di EKS

Selesaikan tugas-tugas berikut untuk menyiapkan sebelum Anda dapat menjalankan aplikasi dengan Flink CLI di Amazon EMR di EKS. Jika Anda sudah mendaftar untuk Amazon Web Services (AWS) dan telah menggunakan Amazon EKS, Anda hampir siap untuk menggunakan Amazon EMR di EKS.

Jika Anda telah menyelesaikan salah satu prasyarat, Anda dapat melewatinya dan melanjutkan ke yang berikutnya.

- Instal AWS CLI— Jika Anda sudah menginstalAWS CLI, konfirmasikan bahwa Anda memiliki versi terbaru.
- Siapkan cluster Amazon EKS — Ikuti langkah-langkah untuk membuat cluster Kubernetes baru dengan node di Amazon EKS.
- Pilih URI image dasar EMR Amazon (rilis 6.13.0 atau lebih tinggi) — perintah Flink Kubernetes didukung dengan Amazon EMR rilis 6.13.0 dan yang lebih tinggi.
- Konfirmasikan bahwa akun JobManager layanan memiliki izin yang sesuai untuk membuat dan menonton TaskManager pod. Untuk informasi selengkapnya, lihat persyaratan keamanan akun JobManager layanan Flink untuk Kubernetes Asli.
- Siapkan profil AWSkredensial lokal Anda.
- Buat atau perbarui file kubeconfig untuk cluster Amazon EKS tempat Anda ingin menjalankan aplikasi Flink.

Memulai dengan Kubernetes asli Flink untuk Amazon EMR di EKS

Jalankan aplikasi Flink

Amazon EMR 6.13.0 dan yang lebih tinggi mendukung Flink Native Kubernetes untuk menjalankan aplikasi Flink di cluster Amazon EKS. Untuk menjalankan aplikasi Flink, ikuti langkah-langkah berikut:

1. Sebelum Anda dapat menjalankan aplikasi Flink dengan perintah Flink Native Kubernetes, selesaikan langkah-langkahnya. the section called “Menyiapkan”
2. Tetapkan nilai untuk variabel lingkungan berikut.

```
export FLINK_HOME=
export NAMESPACE=flink
export CLUSTER_ID=flink-application-cluster
export IMAGE=<123456789012.dkr.ecr.sample-Wilayah AWS-.amazonaws.com/flink/
emr-6.13.0-flink:latest>
export FLINK_SERVICE_ACCOUNT=emr-containers-sa-flink
export FLINK_CLUSTER_ROLE_BINDING=emr-containers-crb-flink
```

3. Buat akun layanan untuk mengelola sumber daya Kubernetes.

```
kubectl create serviceaccount $FLINK_SERVICE_ACCOUNT -n $NAMESPACE
```

```
kubectl create clusterrolebinding $FLINK_CLUSTER_ROLE_BINDING --clusterrole=edit --
serviceaccount=$NAMESPACE:$FLINK_SERVICE_ACCOUNT
```

4. Jalankan `run-application` perintah CLI.

```
$FLINK_HOME/bin/flink run-application \
    --target kubernetes-application \
    -Dkubernetes.namespace=$NAMESPACE \
    -Dkubernetes.cluster-id=$CLUSTER_ID \
    -Dkubernetes.container.image.ref=$IMAGE \
    -Dkubernetes.service-account=$FLINK_SERVICE_ACCOUNT \
    local:///opt/flink/examples/streaming/Iteration.jar
2022-12-29 21:13:06,947 INFO  org.apache.flink.kubernetes.utils.KubernetesUtils
            [] - Kubernetes deployment requires a fixed port. Configuration
 blob.server.port will be set to 6124
2022-12-29 21:13:06,948 INFO  org.apache.flink.kubernetes.utils.KubernetesUtils
            [] - Kubernetes deployment requires a fixed port. Configuration
 taskmanager.rpc.port will be set to 6122
2022-12-29 21:13:07,861 WARN
 org.apache.flink.kubernetes.KubernetesClusterDescriptor      [] - Please note that
 Flink client operations(e.g. cancel, list, stop, savepoint, etc.) won't work from
 outside the Kubernetes cluster since 'kubernetes.rest-service.exposed.type' has
 been set to ClusterIP.
2022-12-29 21:13:07,868 INFO
 org.apache.flink.kubernetes.KubernetesClusterDescriptor      [] - Create flink
 application cluster flink-application-cluster successfully, JobManager Web
 Interface: http://flink-application-cluster-rest.flink:8081
```

5. Periksa sumber daya Kubernetes yang dibuat.

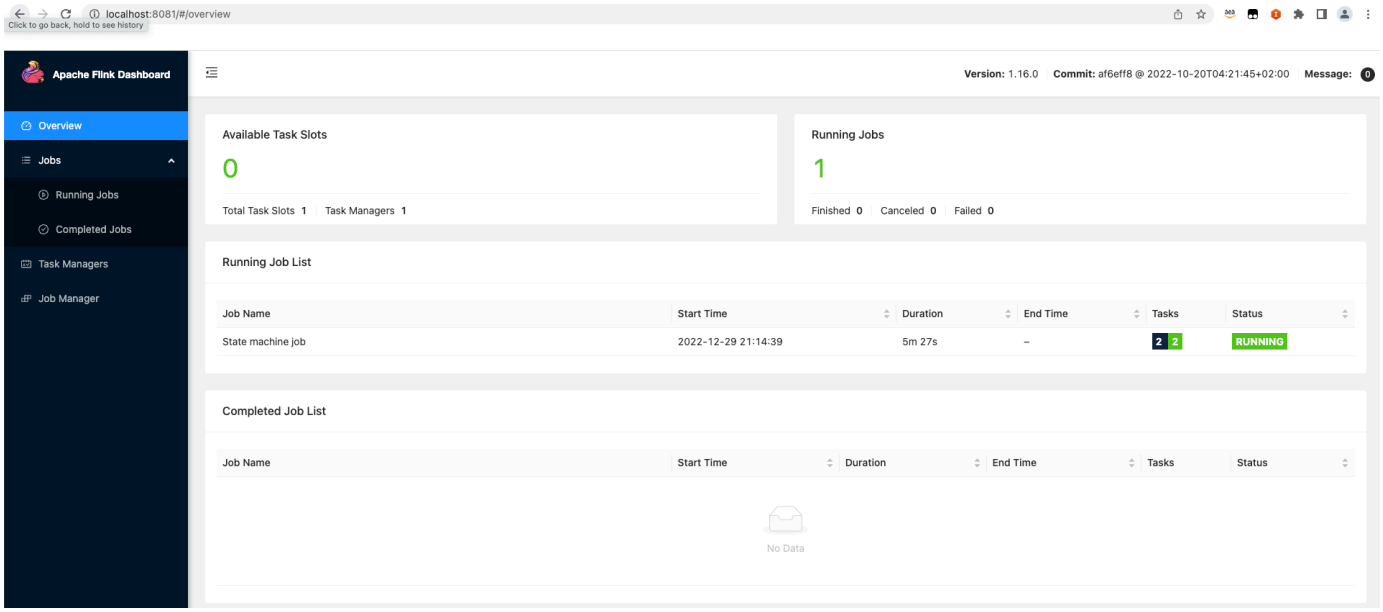
```
kubectl get all -n <namespace>
NAME READY STATUS RESTARTS AGE
pod/flink-application-cluster-546687cb47-w2p2z 1/1 Running 0 3m37s
pod/flink-application-cluster-taskmanager-1-1 1/1 Running 0 3m24s

NAME TYPE CLUSTER-IP EXTERNAL-IP PORT(S) AGE
service/flink-application-cluster ClusterIP None <none> 6123/TCP,6124/TCP 3m38s
service/flink-application-cluster-rest ClusterIP 10.100.132.158 <none> 8081/TCP
 3m38s

NAME READY UP-TO-DATE AVAILABLE AGE
deployment.apps/flink-application-cluster 1/1 1 1 3m38s
```

```
NAME DESIRED CURRENT READY AGE
replicaset.apps/flink-application-cluster-546687cb47 1 1 1 3m38s
```

6. Port maju ke 8081.

```
kubectl port-forward service/flink-application-cluster-rest 8081 -n <namespace>
Forwarding from 127.0.0.1:8081 -> 8081
```

7. Akses UI Flink secara lokal.



8. Hapus aplikasi Flink.

```
kubectl delete deployment.apps/flink-application-cluster -n <namespace>
deployment.apps "flink-application-cluster" deleted
```

Untuk informasi selengkapnya tentang mengirimkan aplikasi ke Flink, lihat Native Kubernetes di dokumentasi Apache Flink.

Persyaratan keamanan akun JobManager layanan Flink untuk Native Kubernetes

JobManager Pod Flink menggunakan akun layanan Kubernetes untuk mengakses server API Kubernetes untuk membuat dan menonton pod. TaskManager JobManager akun layanan harus memiliki izin yang sesuai untuk membuat/menghapus TaskManager pod dan memungkinkan

pemimpin TaskManager to watch ConfigMaps untuk mengambil alamat dan di klaster Anda. JobManager ResourceManager

Aturan berikut berlaku untuk akun layanan ini.

```
rules:
- apiGroups:
  - ""
  resources:
  - pods
  verbs:
  - "*"
- apiGroups:
  - ""
  resources:
  - services
  verbs:
  - "*"
- apiGroups:
  - ""
  resources:
  - configmaps
  verbs:
  - "*"
```

Memantau pekerjaan operator Flink Kubernetes dan Flink

Bagian ini menjelaskan beberapa cara agar Anda dapat memantau pekerjaan Flink Anda dengan Amazon EMR di EKS.

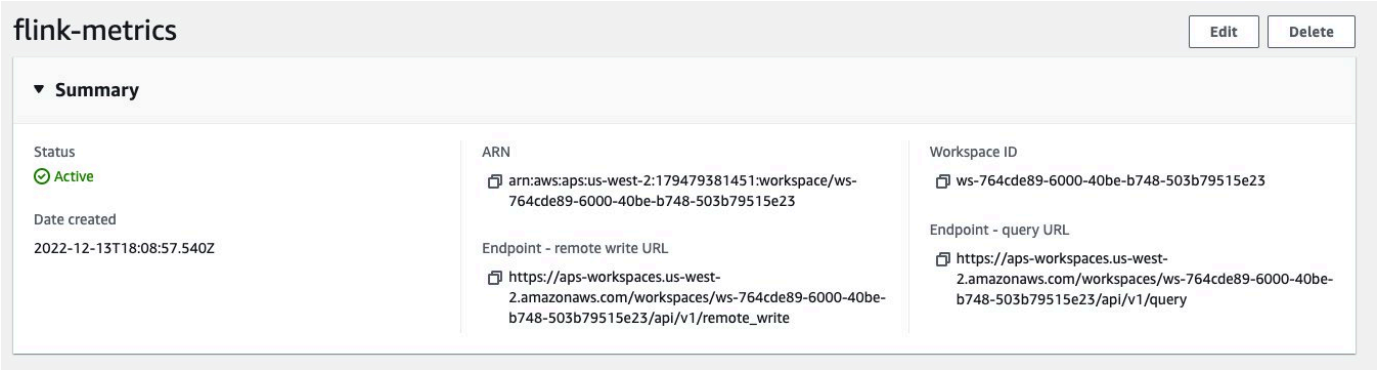
Topik

- Menggunakan Amazon Managed Service untuk Prometheus untuk memantau pekerjaan Flink
- Menggunakan UI Flink untuk memantau pekerjaan Flink
- Menggunakan konfigurasi pemantauan untuk memantau operator Flink Kubernetes dan pekerjaan Flink

Menggunakan Amazon Managed Service untuk Prometheus untuk memantau pekerjaan Flink

Anda dapat mengintegrasikan Apache Flink dengan Amazon Managed Service untuk Prometheus (portal manajemen). Layanan Terkelola Amazon untuk Prometheus mendukung pengambilan metrik dari Amazon Managed Service untuk server Prometheus dalam cluster yang berjalan di Amazon EKS. Layanan Terkelola Amazon untuk Prometheus bekerja sama dengan server Prometheus yang sudah berjalan di cluster Amazon EKS Anda. Menjalankan Amazon Managed Service untuk integrasi Prometheus dengan operator Amazon EMR Flink akan secara otomatis menerapkan dan mengonfigurasi server Prometheus untuk diintegrasikan dengan Amazon Managed Service untuk Prometheus.

1. Buat Layanan Terkelola Amazon untuk Prometheus Workspace. Ruang kerja ini berfungsi sebagai titik akhir konsumsi. Anda akan memerlukan URL tulis jarak jauh nanti.



2. Siapkan peran IAM untuk akun layanan.

   Untuk metode orientasi ini, gunakan peran IAM untuk akun layanan di klaster Amazon EKS tempat server Prometheus berjalan. Peran ini juga disebut peran layanan.

   Jika Anda belum memiliki peran, siapkan peran layanan untuk menelan metrik dari kluster Amazon EKS.

   Sebelum Anda melanjutkan, buat peran IAM yang disebut`amp-iamproxy-ingest-role`.
3. Instal Operator Flink EMR Amazon dengan Amazon Managed Service untuk Prometheus.

Sekarang setelah Anda memiliki Layanan Terkelola Amazon untuk ruang kerja Prometheus, peran IAM khusus untuk Layanan Terkelola Amazon untuk Prometheus, dan izin yang diperlukan, Anda dapat menginstal operator Amazon EMR Flink. Teruskan parameter `prometheus.install=true` dan tingkatkan untuk menunjuk ke Layanan Terkelola Amazon untuk instance Prometheus.

Ini secara otomatis menginstal reporter Prometheus di operator pada port 9999. Any future `FlinkDeployment` juga mengekspos `metrics` port di 9249.

- Metrik operator Flink muncul di Prometheus di bawah label. `flink_k8soperator_`
- Metrik Flink Task Manager muncul di Prometheus di bawah label. `flink_taskmanager_`
- Metrik Manajer Job Flink muncul di Prometheus di bawah label. `flink_jobmanager_`

Gunakan `Helm Install --set`perintah untuk meneruskan penggantian ke bagan. `flink-kubernetes-operator`

```
helm install flink-kubernetes-operator-demo -n namespace \
 ~/workplace/helm/flink-kubernetes-operator \
 --set prometheus.install=true
```

Menggunakan UI Flink untuk memantau pekerjaan Flink

Untuk memantau kesehatan dan kinerja aplikasi Flink yang sedang berjalan, gunakan Flink Web Dashboard. Dasbor ini memberikan informasi tentang status pekerjaan, jumlah TaskManagers, dan metrik serta log untuk pekerjaan itu. Ini juga memungkinkan Anda melihat dan memodifikasi konfigurasi pekerjaan Flink, dan berinteraksi dengan cluster Flink untuk mengirimkan atau membatalkan pekerjaan.

Untuk mengakses Flink Web Dashboard untuk aplikasi Flink yang sedang berjalan di Kubernetes:

1. Gunakan `kubectl port-forward` perintah untuk meneruskan port lokal ke port tempat Flink Web Dashboard berjalan di pod aplikasi TaskManager Flink. Secara default, port ini adalah 8081. Ganti *`deployment-name dengan nama`* penerapan aplikasi Flink dari atas.

   ```
   kubectl get deployments -n namespace
   ```

   Contoh output:

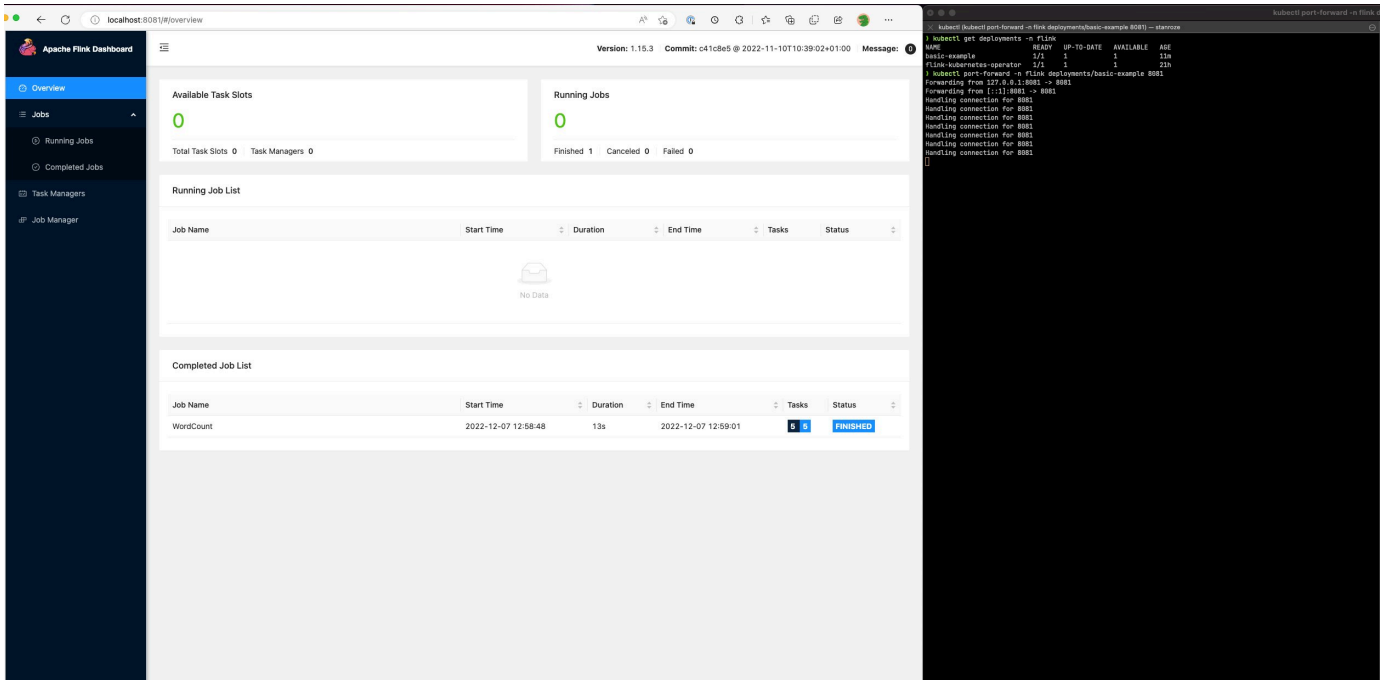
   ```
   kubectl get deployments -n flink-namespace
   NAME                        READY   UP-TO-DATE   AVAILABLE   AGE
   basic-example               1/1       1            1           11m
   flink-kubernetes-operator   1/1       1            1           21h
   ```

```
kubectl port-forward deployments/deployment-name 8081 -n namespace
```

2. Jika Anda ingin menggunakan port yang berbeda secara lokal, gunakan parameter *local-port:8081*.

```
kubectl port-forward -n flink deployments/basic-example 8080:8081
```

3. Di browser web, navigasikan ke `http://localhost:8081` (atau `http://localhost:local-port` jika Anda menggunakan port lokal khusus) untuk mengakses Dasbor Web Flink. Dasbor ini menampilkan informasi tentang aplikasi Flink yang sedang berjalan, seperti status pekerjaan, jumlah TaskManagers, dan metrik serta log untuk pekerjaan tersebut.



Menggunakan konfigurasi pemantauan untuk memantau operator Flink Kubernetes dan pekerjaan Flink

Konfigurasi pemantauan memungkinkan Anda dengan mudah mengatur pengarsipan log aplikasi Flink dan log operator Anda ke S3 dan/atau CloudWatch (Anda dapat memilih salah satu atau keduanya). Melakukan hal itu menambahkan sidecar FluentD ke JobManager Anda TaskManager dan pod dan selanjutnya meneruskan log komponen ini ke sink yang dikonfigurasi.

> **Note**
>
> Anda harus mengatur Peran IAM untuk akun layanan untuk operator Flink Anda dan pekerjaan Flink Anda (Akun Layanan) untuk dapat menggunakan fitur ini, karena memerlukan interaksi dengan yang lain. Layanan AWS Anda harus mengatur ini menggunakan IRSA di[Menyiapkan operator Flink Kubernetes untuk Amazon EMR di EKS](#).

Log aplikasi Flink

Anda dapat menentukan konfigurasi ini dengan cara berikut.

```
apiVersion: flink.apache.org/v1beta1
kind: FlinkDeployment
metadata:
  name: basic-example
spec:
  image: FLINK IMAGE TAG
  imagePullPolicy: Always
  flinkVersion: v1_17
  flinkConfiguration:
    taskmanager.numberOfTaskSlots: "2"
  executionRoleArn: JOB EXECUTION ROLE
  jobManager:
    resource:
      memory: "2048m"
      cpu: 1
  taskManager:
    resource:
      memory: "2048m"
      cpu: 1
  job:
    jarURI: local:///opt/flink/examples/streaming/StateMachineExample.jar
  monitoringConfiguration:
    s3MonitoringConfiguration:
      logUri: S3 BUCKET
    cloudWatchMonitoringConfiguration:
      logGroupName: LOG GROUP NAME
      logStreamNamePrefix: LOG GROUP STREAM PREFIX
    sideCarResources:
      limits:
        cpuLimit: 500m
```

```
        memoryLimit: 250Mi
    containerLogRotationConfiguration:
        rotationSize: 2Gb
        maxFilesToKeep: 10
```

Berikut ini adalah opsi konfigurasi.

- `s3MonitoringConfiguration`— Kunci konfigurasi untuk mengatur penerusan ke S3
  - `logUri`(wajib) — jalur bucket S3 tempat Anda ingin menyimpan log Anda.
  - Jalur di S3 setelah log diunggah akan terlihat seperti berikut.
    - Tidak ada rotasi log yang diaktifkan:

      ```
      s3://${logUri}/${POD NAME}/STDOUT or STDERR.gz
      ```

    - Rotasi log diaktifkan. Anda dapat menggunakan file yang diputar dan file saat ini (satu tanpa cap tanggal).

      ```
      s3://${logUri}/${POD NAME}/STDOUT or STDERR.gz
      ```

      Format berikut adalah angka yang bertambah.

      ```
      s3://${logUri}/${POD NAME}/stdout_YYYYMMDD_index.gz
      ```

  - Izin IAM berikut diperlukan untuk menggunakan forwarder ini.

    ```
    {
        "Effect": "Allow",
        "Action": [
            "s3:PutObject"
        ],
        "Resource": [
           "S3_BUCKET_URI/*",
           "S3_BUCKET_URI"
        ]
    }
    ```

- `cloudWatchMonitoringConfiguration`— kunci konfigurasi untuk mengatur penerusan ke. CloudWatch
  - `logGroupName`(wajib) — nameof grup CloudWatch log yang ingin Anda kirimi log (secara otomatis membuat grup jika tidak ada).

- `logStreamNamePrefix`(opsional) — nama aliran log yang ingin Anda kirim log ke. Nilai default adalah string kosong. Formatnya adalah sebagai berikut:

  ```
  ${logStreamNamePrefix}/${POD NAME}/STDOUT or STDERR
  ```

- Izin IAM berikut diperlukan untuk menggunakan forwarder ini.

  ```
  {
      "Effect": "Allow",
      "Action": [
          "logs:CreateLogStream",
          "logs:CreateLogGroup",
          "logs:PutLogEvents"
      ],
      "Resource": [
          "arn:aws:logs:REGION:ACCOUNT-ID:log-group:{YOUR_LOG_GROUP_NAME}:*",
          "arn:aws:logs:REGION:ACCOUNT-ID:log-group:{YOUR_LOG_GROUP_NAME}"
      ]
  }
  ```

- `sideCarResources`(opsional) — kunci konfigurasi untuk menetapkan batas sumber daya pada wadah sidecar Fluentbit yang diluncurkan.
  - `memoryLimit`(opsional) - nilai default adalah 512Mi. Sesuaikan sesuai dengan kebutuhan Anda.
  - `cpuLimit`(opsional) — opsi ini tidak memiliki default. Sesuaikan sesuai dengan kebutuhan Anda.
- `containerLogRotationConfiguration`(opsional) — mengontrol perilaku rotasi log kontainer. Agen tidak diaktifkan secara default.
  - `rotationSize`(wajib) - menentukan ukuran file untuk rotasi log. Kisaran nilai yang mungkin adalah dari 2KB hingga 2GB. Bagian unit numerik dari parameter RotationSize dilewatkan sebagai bilangan bulat. Karena nilai desimal tidak didukung, Anda dapat menentukan ukuran rotasi 1,5GB, misalnya, dengan nilai 1500MB. Defaultnya adalah 2GB.
  - `maxFilesToKeep`(wajib) — menentukan jumlah maksimum file untuk disimpan dalam wadah setelah rotasi telah terjadi. Nilai minimum adalah 1, dan nilai maksimum adalah 50. Default-nya adalah 10.

Log operator Flink

Kami juga dapat mengaktifkan pengarsipan log untuk operator dengan menggunakan opsi berikut dalam `values.yaml` file di instalasi bagan helm Anda. Anda dapat mengaktifkan S3, CloudWatch, atau keduanya.

```
monitoringConfiguration:
  s3MonitoringConfiguration:
    logUri: "S3-BUCKET"
    totalFileSize: "1G"
    uploadTimeout: "1m"
  cloudWatchMonitoringConfiguration:
    logGroupName: "flink-log-group"
    logStreamNamePrefix: "example-job-prefix-test-2"
  sideCarResources:
    limits:
      cpuLimit: 1
      memoryLimit: 800Mi
  memoryBufferLimit: 700M
```

Berikut ini adalah opsi konfigurasi yang tersedia di bawah`monitoringConfiguration`.

- `s3MonitoringConfiguration`— atur opsi ini untuk mengarsipkan ke S3.
- `logUri`(wajib) - Jalur bucket S3 tempat Anda ingin menyimpan log Anda.
- Berikut ini adalah format seperti apa jalur bucket S3 setelah log diunggah.
  - Tidak ada rotasi log yang diaktifkan.

    ```
    s3://${logUri}/${POD NAME}/OPERATOR or WEBHOOK/STDOUT or STDERR.gz
    ```

  - Rotasi log diaktifkan. Anda dapat menggunakan file yang diputar dan file saat ini (satu tanpa cap tanggal).

    ```
    s3://${logUri}/${POD NAME}/OPERATOR or WEBHOOK/STDOUT or STDERR.gz
    ```

    Indeks format berikut adalah angka yang bertambah.

    ```
    s3://${logUri}/${POD NAME}/OPERATOR or WEBHOOK/stdout_YYYYMMDD_index.gz
    ```

- `cloudWatchMonitoringConfiguration`— kunci konfigurasi untuk mengatur penerusan ke. CloudWatch

  - `logGroupName`(wajib) — nama grup CloudWatch log yang ingin Anda kirimi log. Grup secara otomatis akan dibuat jika tidak ada.
  - `logStreamNamePrefix`(opsional) — nama aliran log yang ingin Anda kirim log ke. Nilai default adalah string kosong. Formatnya CloudWatch adalah sebagai berikut:

    ```
    ${logStreamNamePrefix}/${POD NAME}/STDOUT or STDERR
    ```

- `sideCarResources`(opsional) — kunci konfigurasi untuk menetapkan batas sumber daya pada wadah sidecar Fluentbit yang diluncurkan.
  - `memoryLimit`(opsional) — batas memori. Sesuaikan sesuai dengan kebutuhan Anda. Defaultnya adalah 512Mi.
  - `cpuLimit`— batas CPU. Sesuaikan sesuai dengan kebutuhan Anda. Tidak ada nilai default.
- `containerLogRotationConfiguration`(opsional): — mengontrol perilaku rotasi log kontainer. Agen tidak diaktifkan secara default.
  - `rotationSize`(wajib) - menentukan ukuran file untuk rotasi log. Kisaran nilai yang mungkin adalah dari 2KB hingga 2GB. Bagian unit numerik dari parameter RotationSize dilewatkan sebagai bilangan bulat. Karena nilai desimal tidak didukung, Anda dapat menentukan ukuran rotasi 1,5GB, misalnya, dengan nilai 1500MB. Defaultnya adalah 2GB.
  - `maxFilesToKeep`(wajib) — menentukan jumlah maksimum file untuk disimpan dalam wadah setelah rotasi telah terjadi. Nilai minimum adalah 1, dan nilai maksimum adalah 50. Default-nya adalah 10.

Ketahanan Job

Bagian berikut menguraikan cara membuat pekerjaan Flink Anda lebih andal dan sangat tersedia.

Topik

- Menggunakan ketersediaan tinggi (HA) untuk Operator Flink dan Aplikasi Flink
- Mengoptimalkan waktu restart pekerjaan Flink untuk pemulihan tugas dan operasi penskalaan dengan Amazon EMR di EKS
- Penonaktifan Instans Spot yang anggun dengan Flink di Amazon EMR di EKS

Menggunakan ketersediaan tinggi (HA) untuk Operator Flink dan Aplikasi Flink

Operator Flink ketersediaan tinggi

Kami mengaktifkan ketersediaan tinggi untuk Operator Flink sehingga kami dapat gagal ke Operator Flink siaga untuk meminimalkan waktu henti di loop kontrol operator jika terjadi kegagalan. Ketersediaan tinggi diaktifkan secara default dan jumlah default replika operator awal adalah 2. Anda dapat mengonfigurasi bidang replika di `values.yaml` file Anda untuk bagan helm.

Bidang berikut dapat disesuaikan:

- `replicas`(opsional, defaultnya adalah 2): Menyetel nomor ini menjadi lebih besar dari 1 membuat Operator siaga lainnya dan memungkinkan pemulihan pekerjaan Anda lebih cepat.
- `highAvailabilityEnabled`(opsional, defaultnya benar): Mengontrol apakah Anda ingin mengaktifkan HA. Menentukan parameter ini sebagai true memungkinkan dukungan penyebaran multi AZ, serta menetapkan parameter yang benar`flink-conf.yaml`.

Anda dapat menonaktifkan HA untuk operator Anda dengan mengatur konfigurasi berikut di `values.yaml` file Anda.

```
...
imagePullSecrets: []

replicas: 1

# set this to false if you don't want HA
highAvailabilityEnabled: false
...
```

Penyebaran multi AZ

Kami membuat pod operator di beberapa Availability Zone. Ini adalah kendala lunak, dan pod operator Anda akan dijadwalkan di AZ yang sama jika Anda tidak memiliki cukup sumber daya di AZ yang berbeda.

Menentukan replika pemimpin

Jika HA diaktifkan, replika menggunakan sewa untuk menentukan JM mana yang menjadi pemimpin dan menggunakan Sewa K8 untuk pemilihan pemimpin. Anda dapat menjelaskan Sewa dan melihat bidang Identitas .Spec.Holder untuk menentukan pemimpin saat ini

```
kubectl describe lease <Helm Install Release Name>-<NAMESPACE>-lease -n <NAMESPACE> |
 grep "Holder Identity"
```

Interaksi Flink-S3

Mengkonfigurasi kredenal akses

Pastikan Anda telah mengonfigurasi IRSA dengan izin IAM yang sesuai untuk mengakses bucket S3.

Mengambil stoples pekerjaan dari mode Aplikasi S3

Operator Flink juga mendukung pengambilan stoples aplikasi dari S3. Anda hanya menyediakan lokasi S3 untuk JarUri dalam spesifikasi Anda FlinkDeployment .

Anda juga dapat menggunakan fitur ini untuk mengunduh artefak lain seperti PyFlink skrip. Skrip Python yang dihasilkan dijatuhkan di bawah jalur. `/opt/flink/usrlib/`

Contoh berikut menunjukkan bagaimana menggunakan fitur ini untuk PyFlink pekerjaan. Perhatikan bidang JarUri dan args.

```
apiVersion: flink.apache.org/v1beta1
kind: FlinkDeployment
metadata:
  name: python-example
spec:
  image: <YOUR CUSTOM PYFLINK IMAGE>
  emrReleaseLabel: "emr-6.12.0-flink-latest"
  flinkVersion: v1_16
  flinkConfiguration:
    taskmanager.numberOfTaskSlots: "1"
  serviceAccount: flink
  jobManager:
    highAvailabilityEnabled: false
    replicas: 1
    resource:
      memory: "2048m"
      cpu: 1
  taskManager:
```

```
    resource:
      memory: "2048m"
      cpu: 1
  job:
    jarURI: "s3://<S3-BUCKET>/scripts/pyflink.py" # Note, this will trigger the
 artifact download process
    entryClass: "org.apache.flink.client.python.PythonDriver"
    args: ["-pyclientexec", "/usr/local/bin/python3", "-py", "/opt/flink/usrlib/
pyflink.py"]
    parallelism: 1
    upgradeMode: stateless
```

Konektor Flink S3

Flink dikemas dengan dua konektor S3 (tercantum di bawah). Bagian berikut membahas kapan harus menggunakan konektor mana.

Checkpointing: Konektor Presto S3

- Setel skema S3 ke s3p://
- Konektor yang disarankan untuk digunakan ke pos pemeriksaan ke s3.

Contoh FlinkDeployment spesifikasi:

```
apiVersion: flink.apache.org/v1beta1
kind: FlinkDeployment
metadata:
  name: basic-example
spec:
  flinkConfiguration:
    taskmanager.numberOfTaskSlots: "2"
    state.checkpoints.dir: s3p://<UCKET-NAME>/flink-checkpoint/
```

- Atur skema S3 ke `s3://` atau () `s3a://`
- Konektor yang direkomendasikan untuk membaca dan menulis file dari S3 (hanya konektor S3 yang mengimplementasikan antarmuka Flinks Filesystem).
- Secara default, kami mengatur `flink-conf.yaml` file `fs.s3a.aws.credentials.provider` dalam, yaitu`com.amazonaws.auth.WebIdentityTokenCredentialsProvider`. Jika Anda mengganti d efault `flink-conf` sepenuhnya dan Anda berinteraksi dengan S3, pastikan untuk menggunakan penyedia ini.

Contoh FlinkDeployment spesifikasi

```
apiVersion: flink.apache.org/v1beta1
kind: FlinkDeployment
metadata:
  name: basic-example
spec:
  job:
    jarURI: local:///opt/flink/examples/streaming/WordCount.jar
    args: [ "--input", "s3a://<INPUT BUCKET>/PATH", "--output", "s3a://<OUTPUT BUCKET>/
PATH" ]
    parallelism: 2
    upgradeMode: stateless
```

Manajer Pekerjaan Flink

Ketersediaan Tinggi (HA) untuk Penerapan Flink memungkinkan pekerjaan terus membuat kemajuan bahkan jika kesalahan sementara ditemukan dan crash Anda. JobManager Pekerjaan akan dimulai ulang tetapi dari pos pemeriksaan terakhir yang berhasil dengan HA diaktifkan. Tanpa HA diaktifkan, Kubernetes akan memulai ulang pekerjaan Anda JobManager, tetapi pekerjaan Anda akan dimulai sebagai pekerjaan baru dan akan kehilangan kemajuannya. Setelah mengonfigurasi HA, kami dapat memberi tahu Kubernetes untuk menyimpan metadata HA dalam penyimpanan persisten untuk referensi jika terjadi kegagalan sementara di JobManager dan kemudian melanjutkan pekerjaan kami dari pos pemeriksaan terakhir yang berhasil.

HA diaktifkan secara default untuk pekerjaan Flink Anda (jumlah replika disetel ke 2, yang mengharuskan Anda menyediakan lokasi penyimpanan S3 agar metadata HA tetap ada).

Konfigurasi HA

```
apiVersion: flink.apache.org/v1beta1
kind: FlinkDeployment
metadata:
  name: basic-example
spec:
  flinkConfiguration:
    taskmanager.numberOfTaskSlots: "2"
  executionRoleArn: "<JOB EXECUTION ROLE ARN>"
  emrReleaseLabel: "emr-6.13.0-flink-latest"
  jobManager:
    resource:
```

```
      memory: "2048m"
      cpu: 1
    replicas: 2
    highAvailabilityEnabled: true
    storageDir: "s3://<S3 PERSISTENT STORAGE DIR>"
  taskManager:
    resource:
      memory: "2048m"
      cpu: 1
```

Berikut ini adalah deskripsi untuk konfigurasi HA di atas di Job Manager (didefinisikan di bawah.spec.jobManager):

- `highAvailabilityEnabled`(opsional, default adalah true): Setel ini ke `false` jika Anda tidak ingin HA diaktifkan dan tidak ingin menggunakan konfigurasi HA yang disediakan. Anda masih dapat memanipulasi bidang “replika” untuk mengonfigurasi HA secara manual.
- `replicas`(opsional, defaultnya adalah 2): Menyetel nomor ini menjadi lebih besar dari 1 membuat siaga lainnya JobManagers dan memungkinkan pemulihan pekerjaan Anda lebih cepat. Jika Anda menonaktifkan HA, Anda harus mengatur jumlah replika ke 1, atau Anda akan terus mendapatkan kesalahan validasi (hanya 1 replika yang didukung jika HA tidak diaktifkan).
- `storageDir`(required): Karena kami menggunakan jumlah replika sebagai 2 secara default, kami harus menyediakan StorageDir persisten. Saat ini bidang ini hanya menerima jalur S3 sebagai lokasi penyimpanan.

Lokalitas pod

Jika Anda mengaktifkan HA, kami juga mencoba mengkolokasi pod di AZ yang sama, yang mengarah pada peningkatan kinerja (mengurangi latensi jaringan dengan memiliki pod di AZ yang sama). Ini adalah proses upaya terbaik, artinya jika Anda tidak memiliki cukup sumber daya di AZ di mana sebagian besar Pod Anda dijadwalkan, Pod yang tersisa masih akan dijadwalkan tetapi mungkin berakhir pada node di luar AZ ini.

Menentukan replika pemimpin

Jika HA diaktifkan, replika menggunakan sewa untuk menentukan JM mana yang menjadi pemimpin dan menggunakan K8s Configmap sebagai datastore untuk menyimpan metadata ini. Jika Anda ingin menentukan pemimpin, Anda dapat melihat konten Configmap dan melihat kunci di `org.apache.flink.k8s.leader.restserver` bawah data untuk menemukan pod K8s dengan alamat IP. Anda juga dapat menggunakan perintah bash berikut.

```
ip=$(kubectl get configmap -n <NAMESPACE> <JOB-NAME>-cluster-config-map -o json | jq -
r ".data[\"org.apache.flink.k8s.leader.restserver\"]" | awk -F: '{print $2}' | awk -F
 '/' '{print $3}')
kubectl get pods -n NAMESPACE  -o json | jq -r ".items[] | select(.status.podIP ==
 \"$ip\") | .metadata.name"
```

Pekerjaan Flink - Kubernetes asli

Amazon EMR 6.13.0 dan yang lebih tinggi mendukung Kubernetes asli Flink untuk menjalankan aplikasi Flink dalam mode ketersediaan tinggi pada cluster Amazon EKS.

> **Note**
>
> Anda harus memiliki bucket Amazon S3 yang dibuat untuk menyimpan metadata ketersediaan tinggi saat mengirimkan pekerjaan Flink Anda. Jika Anda tidak ingin menggunakan fitur ini, Anda dapat menonaktifkannya. Ini diaktifkan secara default.

Untuk mengaktifkan fitur ketersediaan tinggi Flink, berikan parameter Flink berikut saat Anda menjalankan perintah CLI `run-application`. Parameter didefinisikan di bawah contoh.

```
-Dhigh-availability.type=kubernetes \
-Dhigh-availability.storageDir=S3://DOC-EXAMPLE-STORAGE-BUCKET \
-
Dfs.s3a.aws.credentials.provider="com.amazonaws.auth.WebIdentityTokenCredentialsProvider"
 \
-Dkubernetes.jobmanager.replicas=3 \
-Dkubernetes.cluster-id=example-cluster
```

- **`Dhigh-availability.storageDir`**- Bucket Amazon S3 tempat Anda ingin menyimpan metadata ketersediaan tinggi untuk pekerjaan Anda.

  `Dkubernetes.jobmanager.replicas`— Jumlah pod Job Manager yang akan dibuat sebagai bilangan bulat lebih besar dari1.

  `Dkubernetes.cluster-id`— ID unik yang mengidentifikasi cluster Flink.

Mengoptimalkan waktu restart pekerjaan Flink untuk pemulihan tugas dan operasi penskalaan dengan Amazon EMR di EKS

Ketika tugas gagal atau ketika operasi penskalaan terjadi, Flink mencoba untuk mengeksekusi kembali tugas dari pos pemeriksaan terakhir selesai. Proses restart bisa memakan waktu satu menit atau lebih lama untuk dijalankan, tergantung pada ukuran status pos pemeriksaan dan jumlah tugas paralel. Selama periode restart, tugas backlog dapat menumpuk untuk pekerjaan itu. Ada beberapa cara, bahwa Flink mengoptimalkan kecepatan pemulihan dan memulai ulang grafik eksekusi untuk meningkatkan stabilitas pekerjaan.

Halaman ini menjelaskan beberapa cara Amazon EMR Flink dapat meningkatkan waktu restart pekerjaan selama pemulihan tugas atau operasi penskalaan.

Topik

Tugas-pemulihan lokal

> **Note**
>
> Pemulihan tugas-lokal didukung dengan Flink di Amazon EMR di EKS 6.14.0 dan lebih tinggi.

Dengan pos pemeriksaan Flink, setiap tugas menghasilkan snapshot statusnya yang ditulis Flink ke penyimpanan terdistribusi seperti Amazon S3. Dalam kasus pemulihan, tugas mengembalikan keadaan mereka dari penyimpanan terdistribusi. Penyimpanan terdistribusi memberikan toleransi kesalahan dan dapat mendistribusikan kembali status selama penskalaan ulang karena dapat diakses oleh semua node.

Namun, toko terdistribusi jarak jauh juga memiliki kelemahan: semua tugas harus membaca statusnya dari lokasi terpencil melalui jaringan. Hal ini dapat mengakibatkan waktu pemulihan yang lama untuk negara bagian besar selama pemulihan tugas atau operasi penskalaan.

Masalah waktu pemulihan yang lama ini diselesaikan dengan pemulihan tugas-lokal. Tugas menulis status mereka di pos pemeriksaan ke dalam penyimpanan sekunder yang bersifat lokal untuk tugas, seperti pada disk lokal. Mereka juga menyimpan status mereka di penyimpanan utama, atau Amazon S3 dalam kasus kami. Selama pemulihan, penjadwal menjadwalkan tugas pada Task Manager yang sama di mana tugas berjalan lebih awal sehingga mereka dapat pulih dari penyimpanan status lokal alih-alih membaca dari penyimpanan status jarak jauh. Untuk informasi selengkapnya, lihat Task-Local Recovery di Dokumentasi Apache Flink.

Tes benchmark kami dengan pekerjaan sampel telah menunjukkan bahwa waktu pemulihan telah dikurangi dari menit menjadi beberapa detik dengan pemulihan tugas-lokal diaktifkan.

Untuk mengaktifkan pemulihan tugas-lokal, atur konfigurasi berikut di file Anda. `flink-conf.yaml` Tentukan nilai interval checkpointing dalam milidetik.

```
state.backend.local-recovery: true
state.backend: hasmap or rocksdb
state.checkpoints.dir: s3://STORAGE-BUCKET-PATH/checkpoint
execution.checkpointing.interval: 15000
```

Pemulihan tugas-lokal dengan pemasangan volume Amazon EBS

> **Note**
>
> Pemulihan tugas-lokal oleh Amazon EBS didukung dengan Flink di Amazon EMR di EKS 6.15.0 dan lebih tinggi.

Dengan Flink di Amazon EMR di EKS, Anda dapat secara otomatis menyediakan volume Amazon EBS ke pod untuk pemulihan TaskManager tugas lokal. Mount overlay default dilengkapi dengan volume 10 GB, yang cukup untuk pekerjaan dengan status lebih rendah. Pekerjaan dengan status besar dapat mengaktifkan opsi pemasangan volume EBS otomatis. TaskManagerPod secara otomatis dibuat dan dipasang selama pembuatan pod dan dihapus selama penghapusan pod.

Gunakan langkah-langkah berikut untuk mengaktifkan pemasangan volume EBS otomatis untuk Flink di Amazon EMR di EKS:

1. Ekspor nilai untuk variabel berikut yang akan Anda gunakan dalam langkah mendatang.

   ```
   export AWS_REGION=aa-example-1
   ```

```
export FLINK_EKS_CLUSTER_NAME=my-cluster
export AWS_ACCOUNT_ID=111122223333
```

2. Buat atau perbarui file `kubeconfig` YAMM untuk klaster Anda.

```
aws eks update-kubeconfig --name $FLINK_EKS_CLUSTER_NAME --region $AWS_REGION
```

3. Buat akun layanan IAM untuk driver Amazon EBS Container Storage Interface (CSI) di cluster Amazon EKS Anda.

```
eksctl create iamserviceaccount \
   --name ebs-csi-controller-sa \
   --namespace kube-system \
   --region $AWS_REGION \
   --cluster $FLINK_EKS_CLUSTER_NAME\
   --role-name TLR_${AWS_REGION}_${FLINK_EKS_CLUSTER_NAME} \
   --role-only \
   --attach-policy-arn arn:aws:iam::aws:policy/service-role/
AmazonEBSCSIDriverPolicy \
   --approve
```

4. Buat driver Amazon EBS CSI dengan perintah berikut:

```
eksctl create addon \
   --name aws-ebs-csi-driver \
   --region $AWS_REGION \
   --cluster $FLINK_EKS_CLUSTER_NAME \
   --service-account-role-arn arn:aws:iam::${AWS_ACCOUNT_ID}:role/TLR_
${AWS_REGION}_${FLINK_EKS_CLUSTER_NAME}
```

5. Buat kelas penyimpanan Amazon EBS dengan perintah berikut:

```
cat # EOF # storage-class.yaml
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ebs-sc
provisioner: ebs.csi.aws.com
volumeBindingMode: WaitForFirstConsumer
EOF
```

Dan kemudian terapkan kelas:

```
kubectl apply -f storage-class.yaml
```

6. Helm instal operator Amazon EMR Flink Kubernetes dengan opsi untuk membuat akun layanan. Ini menciptakan `emr-containers-sa-flink` untuk digunakan dalam penerapan Flink.

```
helm install flink-kubernetes-operator flink-kubernetes-operator/ \
   --set jobServiceAccount.create=true \
   --set rbac.jobRole.create=true \
   --set rbac.jobRoleBinding.create=true
```

7. Untuk mengirimkan pekerjaan Flink dan mengaktifkan penyediaan otomatis volume EBS untuk pemulihan tugas-lokal, atur konfigurasi berikut di file Anda. `flink-conf.yaml` Sesuaikan batas ukuran untuk ukuran status pekerjaan. Atur `serviceAccount` menjadi `emr-containers-sa-flink`. Tentukan nilai interval checkpointing dalam milidetik. Dan hilangkan. `executionRoleArn`

```
flinkConfiguration:
    task.local-recovery.ebs.enable: true
    kubernetes.taskmanager.local-recovery.persistentVolumeClaim.sizeLimit: 10Gi
    state.checkpoints.dir: s3://BUCKET-PATH/checkpoint
    state.backend.local-recovery: true
    state.backend: hasmap or rocksdb
    state.backend.incremental: "true"
    execution.checkpointing.interval: 15000
  serviceAccount: emr-containers-sa-flink
```

Saat Anda siap untuk menghapus plugin driver Amazon EBS CSI, gunakan perintah berikut:

```
  # Detach Attached Policy
  aws iam detach-role-policy --role-name TLR_${$AWS_REGION}_${FLINK_EKS_CLUSTER_NAME}
 --policy-arn arn:aws:iam::aws:policy/service-role/AmazonEBSCSIDriverPolicy
  # Delete the created Role
  aws iam delete-role --role-name TLR_${$AWS_REGION}_${FLINK_EKS_CLUSTER_NAME}
  # Delete the created service account
  eksctl delete iamserviceaccount --name ebs-csi-controller-sa --namespace kube-system
 --cluster $FLINK_EKS_CLUSTER_NAME --region $AWS_REGION
  # Delete Addon
  eksctl delete addon --name aws-ebs-csi-driver --cluster $FLINK_EKS_CLUSTER_NAME --
region $AWS_REGION
  # Delete the EBS storage class
```

```
kubectl delete -f storage-class.yaml
```

Pos pemeriksaan inkremental berbasis log generik

> **Note**
>
> Pemeriksaan inkremental berbasis log generik didukung dengan Flink di Amazon EMR di EKS 6.14.0 dan yang lebih tinggi.

Checkpointing inkremental berbasis log generik ditambahkan di Flink 1.16 untuk meningkatkan kecepatan pos pemeriksaan. Interval pos pemeriksaan yang lebih cepat sering mengakibatkan pengurangan pekerjaan pemulihan karena lebih sedikit peristiwa yang perlu diproses ulang setelah pemulihan. Untuk informasi selengkapnya, lihat Meningkatkan kecepatan dan stabilitas pos pemeriksaan dengan pos pemeriksaan inkremental berbasis log generik di Blog Apache Flink.

Dengan pekerjaan sampel, tes benchmark kami telah menunjukkan bahwa waktu pos pemeriksaan berkurang dari menit menjadi beberapa detik dengan pos pemeriksaan inkremental berbasis log generik.

Untuk mengaktifkan pos pemeriksaan inkremental berbasis log generik, atur konfigurasi berikut di file Anda. `flink-conf.yaml` Tentukan nilai interval checkpointing dalam milidetik.

```
state.backend.changelog.enabled: true
state.backend.changelog.storage: filesystem
dstl.dfs.base-path: s3://bucket-path/changelog
state.backend.local-recovery: true
state.backend: rocksdb
state.checkpoints.dir: s3://bucket-path/checkpoint
execution.checkpointing.interval: 15000
```

Pemulihan berbutir halus

> **Note**
>
> Dukungan pemulihan berbutir halus untuk penjadwal default didukung dengan Flink di Amazon EMR di EKS 6.14.0 dan yang lebih tinggi. Dukungan pemulihan berbutir halus dalam penjadwal adaptif tersedia dengan Flink di Amazon EMR di EKS 6.15.0 dan lebih tinggi.

Ketika tugas gagal selama eksekusi, Flink mengatur ulang seluruh grafik eksekusi dan memicu eksekusi ulang lengkap dari pos pemeriksaan terakhir yang diselesaikan. Ini lebih mahal daripada hanya menjalankan kembali tugas yang gagal. Pemulihan berbutir halus hanya memulai kembali komponen yang terhubung dengan pipa dari tugas yang gagal. Dalam contoh berikut, grafik pekerjaan memiliki 5 simpul (AkeE). Semua koneksi antara simpul disalurkan dengan distribusi pointwise, dan `parallelism.default` untuk pekerjaan diatur ke. 2

```
A # B # C # D # E
```

Untuk contoh ini, ada total 10 tugas yang berjalan. Pipeline pertama (a1toe1) berjalan pada a TaskManager (TM1), dan pipeline kedua (a2toe2) berjalan pada yang lain TaskManager (TM2).

```
a1 # b1 # c1 # d1 # e1
a2 # b2 # c2 # d2 # e2
```

Ada dua komponen yang terhubung dengan pipa:`a1 # e1`, dana`2 # e2`. Jika salah satu TM1 atau TM2 gagal, kegagalan hanya berdampak pada 5 tugas dalam pipeline tempat TaskManager sedang berjalan. Strategi restart hanya memulai komponen pipelined yang terpengaruh.

Pemulihan berbutir halus hanya berfungsi dengan pekerjaan Flink paralel sempurna. Ini tidak didukung dengan `keyBy()` atau `redistribute()` operasi. Untuk informasi selengkapnya, lihat FLIP-1: Pemulihan Berbutir Halus dari Kegagalan Tugas dalam proyek Jira Proposal Peningkatan Flink.

Untuk mengaktifkan pemulihan berbutir halus, atur konfigurasi berikut di file Anda. `flink-conf.yaml`

```
jobmanager.execution.failover-strategy: region
restart-strategy: exponential-delay or fixed-delay
```

Mekanisme restart gabungan dalam penjadwal adaptif

> **Note**
>
> Mekanisme restart gabungan dalam penjadwal adaptif didukung dengan Flink di Amazon EMR di EKS 6.15.0 dan lebih tinggi.

Penjadwal adaptif dapat menyesuaikan paralelisme pekerjaan berdasarkan slot yang tersedia. Ini secara otomatis mengurangi paralelisme jika tidak cukup slot yang tersedia agar sesuai dengan paralelisme pekerjaan yang dikonfigurasi. Jika slot baru tersedia, pekerjaan ditingkatkan lagi ke paralelisme pekerjaan yang dikonfigurasi. Penjadwal adaptif menghindari waktu henti di tempat kerja ketika tidak ada cukup sumber daya yang tersedia. Ini adalah penjadwal yang didukung untuk Flink Autoscaler. Kami merekomendasikan penjadwal adaptif dengan Amazon EMR Flink karena alasan ini. Namun, penjadwal adaptif mungkin melakukan beberapa restart dalam waktu singkat, satu restart untuk setiap sumber daya baru yang ditambahkan. Hal ini dapat menyebabkan penurunan kinerja dalam pekerjaan.

Dengan Amazon EMR 6.15.0 dan yang lebih tinggi, Flink memiliki mekanisme restart gabungan dalam penjadwal adaptif yang membuka jendela restart ketika sumber daya pertama ditambahkan, dan kemudian menunggu hingga interval jendela yang dikonfigurasi dari default 1 menit. Ini melakukan restart tunggal ketika ada sumber daya yang cukup tersedia untuk menjalankan pekerjaan dengan paralelisme yang dikonfigurasi atau ketika interval waktu habis.

Dengan contoh pekerjaan, pengujian benchmark kami menunjukkan bahwa fitur ini memproses 10% rekaman lebih banyak daripada perilaku default saat Anda menggunakan adaptive scheduler dan Flink autoscaler.

Untuk mengaktifkan mekanisme restart gabungan, atur konfigurasi berikut di `flink-conf.yaml` file Anda.

```
jobmanager.adaptive-scheduler.combined-restart.enabled: true
jobmanager.adaptive-scheduler.combined-restart.window-interval: 1m
```

Penonaktifan Instans Spot yang anggun dengan Flink di Amazon EMR di EKS

Flink dengan Amazon EMR di EKS dapat meningkatkan waktu restart pekerjaan selama pemulihan tugas atau operasi penskalaan.

Gambaran Umum

Amazon EMR di EKS merilis 6.15.0 dan yang lebih tinggi mendukung penonaktifan Manajer Tugas di Instans Spot di Amazon EMR di EKS dengan Apache Flink. Sebagai bagian dari fitur ini, Amazon EMR di EKS dengan Flink menyediakan kemampuan berikut:

- ust-in-time Checkpointing J — Pekerjaan streaming Flink dapat merespons interupsi Instans Spot, melakukan pos pemeriksaan just-in-time (JIT) dari pekerjaan yang sedang berjalan, dan mencegah penjadwalan tugas tambahan pada Instans Spot ini. Pos pemeriksaan JIT didukung dengan penjadwal default dan adaptif.
- Mekanisme restart gabungan — Mekanisme restart gabungan melakukan upaya terbaik untuk memulai kembali pekerjaan setelah mencapai paralelisme sumber daya target atau akhir jendela yang dikonfigurasi saat ini. Ini juga mencegah restart pekerjaan berturut-turut yang mungkin disebabkan oleh beberapa penghentian Instans Spot. Mekanisme restart gabungan hanya tersedia dengan penjadwal adaptif.

Kemampuan ini memberikan manfaat sebagai berikut:

- Anda dapat memanfaatkan Instans Spot untuk menjalankan Manajer Tugas dan mengurangi pengeluaran klaster.
- Peningkatan keaktifan untuk Spot Instance Task Manager menghasilkan ketahanan yang lebih tinggi dan penjadwalan pekerjaan yang lebih efisien.
- Pekerjaan Flink Anda akan memiliki lebih banyak uptime karena akan ada lebih sedikit restart dari penghentian Instans Spot.

Cara kerjanya

Pertimbangkan contoh berikut: Anda menyediakan EMR Amazon di klaster EKS yang menjalankan Apache Flink, dan Anda menentukan node Sesuai Permintaan untuk Job Manager, dan node Instans Spot untuk Task Manager. Dua menit sebelum penghentian, Task Manager menerima pemberitahuan gangguan.

Dalam skenario ini, Job Manager akan menangani sinyal interupsi Instans Spot, memblokir penjadwalan tugas tambahan pada Instans Spot, dan memulai pemeriksaan JIT untuk pekerjaan streaming.

Kemudian, Job Manager akan memulai ulang grafik pekerjaan hanya setelah ada ketersediaan sumber daya baru yang cukup untuk memenuhi paralelisme pekerjaan saat ini di jendela interval restart saat ini. Interval jendela restart ditentukan berdasarkan durasi penggantian Instans Spot, pembuatan pod Task Manager baru, dan pendaftaran dengan Job Manager.

Prasyarat

Untuk menggunakan dekomisi gracefull, buat dan jalankan pekerjaan streaming di Amazon EMR di kluster EKS yang menjalankan Apache Flink. Aktifkan Penjadwal Adaptif dan Manajer Tugas yang dijadwalkan pada setidaknya satu Instance Spot, seperti yang ditunjukkan pada contoh berikut. Anda harus menggunakan node On-Demand untuk Job Manager, dan Anda dapat menggunakan node On-Demand untuk Task Manager selama setidaknya ada satu Instance Spot juga.

```
apiVersion: flink.apache.org/v1beta1
kind: FlinkDeployment
metadata:
  name: deployment_name
spec:
  flinkVersion: v1_17
  flinkConfiguration:
    taskmanager.numberOfTaskSlots: "2"
    cluster.taskmanager.graceful-decommission.enabled: "true"
    execution.checkpointing.interval: "240s"
    jobmanager.adaptive-scheduler.combined-restart.enabled: "true"
    jobmanager.adaptive-scheduler.combined-restart.window-interval : "1m"
  serviceAccount: flink
  jobManager:
    resource:
      memory: "2048m"
      cpu: 1
  taskManager:
    resource:
      memory: "2048m"
      cpu: 1
  job:
    jarURI: flink_job_jar_path
```

Konfigurasi

Bagian ini mencakup sebagian besar konfigurasi yang dapat Anda tentukan untuk kebutuhan penonaktifan Anda.

Key	Deskripsi	Nilai default	Nilai yang dapat diterima
`cluster.taskmanager.graceful-decommission.enabled`	Aktifkan penonaktifan Task Manager yang anggun.	`true`	`true`, `false`
`jobmanager.adaptive-scheduler.combined-restart.enabled`	Aktifkan mekanisme restart gabungan di Adaptive Scheduler.	`false`	`true`, `false`
`jobmanager.adaptive-scheduler.combined-restart.window-interval`	Interval jendela restart gabungan untuk melakukan restart gabungan untuk pekerjaan tersebut. Sebuah integer tanpa unit ditafsirkan sebagai milidetik.	`1m`	Contoh:`30`,`60s`,`3m`, `1h`

Menggunakan Autoscaler untuk aplikasi Flink

Autoscaler operator dapat membantu meringankan tekanan balik dengan mengumpulkan metrik dari pekerjaan Flink dan secara otomatis menyesuaikan paralelisme pada tingkat titik pekerjaan. Berikut ini adalah contoh seperti apa konfigurasi Anda:

```
apiVersion: flink.apache.org/v1beta1
kind: FlinkDeployment
metadata:
  ...
spec:
  ...
```

```
  flinkVersion: v1_17
  flinkConfiguration:
    kubernetes.operator.job.autoscaler.enabled: "true"
    kubernetes.operator.job.autoscaler.stabilization.interval: 1m
    kubernetes.operator.job.autoscaler.metrics.window: 5m
    kubernetes.operator.job.autoscaler.target.utilization: "0.6"
    kubernetes.operator.job.autoscaler.target.utilization.boundary: "0.2"
    kubernetes.operator.job.autoscaler.restart.time: 2m
    kubernetes.operator.job.autoscaler.catch-up.duration: 5m
    pipeline.max-parallelism: "720"
  ...
```

Berikut ini adalah opsi konfigurasi untuk autoscaler.

- `kubernetes.operator.job.autoscaler.scaling.enabled`— menentukan apakah akan mengaktifkan tindakan autoscaler. Default ke false untuk mendukung mode pasif/metrik saja di mana autoscaler hanya mengumpulkan dan mengevaluasi metrik kinerja terkait penskalaan tetapi tidak memicu peningkatan pekerjaan apa pun. Ini dapat digunakan untuk mendapatkan kepercayaan pada modul tanpa berdampak pada aplikasi yang sedang berjalan.
- `kubernetes.operator.job.autoscaler.stabilization.interval`— periode stabilisasi di mana tidak ada penskalaan baru yang akan dieksekusi. Default adalah 5 menit.
- `kubernetes.operator.job.autoscaler.metrics.window`— ukuran jendela agregasi metrik penskalaan. Semakin besar jendela, semakin halus dan stabil, tetapi autoscaler mungkin lebih lambat untuk bereaksi terhadap perubahan beban mendadak. Default adalah 10 menit. Kami menyarankan Anda bereksperimen dengan menggunakan nilai antara 3 hingga 60 menit.
- `kubernetes.operator.job.autoscaler.target.utilization`— pemanfaatan simpul target untuk memberikan kinerja pekerjaan yang stabil dan beberapa buffer untuk fluktuasi beban. Defaultnya `0.7` menargetkan 70% pemanfaatan/pemuatan untuk simpul pekerjaan.
- `kubernetes.operator.job.autoscaler.target.utilization.boundary`— batas pemanfaatan simpul target yang berfungsi sebagai buffer ekstra untuk menghindari penskalaan langsung pada fluktuasi beban. Defaultnya adalah`0.4`, yang berarti 40% deviasi dari pemanfaatan target diperbolehkan sebelum memicu tindakan penskalaan.
- `kubernetes.operator.job.autoscaler.restart.time`— waktu yang diharapkan untuk me-restart aplikasi. Default adalah 3 menit.
- `kubernetes.operator.job.autoscaler.catch-up.duration`— waktu yang diharapkan untuk catch up, yang berarti sepenuhnya memproses setiap backlog setelah operasi penskalaan

selesai. Default adalah 5 menit. Dengan menurunkan durasi catch-up, autoscaler harus memesan lebih banyak kapasitas ekstra untuk tindakan penskalaan.

- `pipeline.max-parallelism`— paralelisme maksimum yang dapat digunakan autoscaler. Autoscaler mengabaikan batas ini jika lebih tinggi dari paralelisme maks yang dikonfigurasi dalam konfigurasi Flink atau langsung pada setiap operator. Defaultnya adalah 200. Perhatikan bahwa autoscaler menghitung paralelisme sebagai pembagi bilangan paralelisme maks oleh karena itu disarankan untuk memilih pengaturan paralelisme maks yang memiliki banyak pembagi daripada mengandalkan default yang disediakan Flink. Kami merekomendasikan penggunaan kelipatan 60 untuk konfigurasi ini, seperti 120, 180, 240, 360, 720 dll.

Untuk halaman referensi konfigurasi yang lebih detail, lihat Konfigurasi Autoscaler.

Pemeliharaan dan pemecahan masalah

Bagian berikut akan menguraikan cara mempertahankan pekerjaan Flink Anda yang sudah berjalan lama, dan memberikan panduan tentang cara memecahkan masalah umum.

Migrasi aplikasi Flink

Aplikasi Flink biasanya dirancang untuk berjalan dalam jangka waktu yang lama seperti minggu, bulan, atau bahkan bertahun-tahun. Seperti semua layanan yang berjalan lama, aplikasi streaming Flink perlu dipertahankan. Ini termasuk perbaikan bug, peningkatan, dan migrasi ke cluster Flink versi yang lebih baru.

Ketika spesifikasi berubah `FlinkDeployment` dan `FlinkSessionJob` sumber daya, Anda perlu memutakhirkan aplikasi yang sedang berjalan. Untuk melakukan ini, operator menghentikan pekerjaan yang sedang berjalan (kecuali sudah ditangguhkan) dan menerapkannya kembali dengan spesifikasi terbaru dan, untuk aplikasi stateful, status dari proses sebelumnya.

Pengguna mengontrol cara mengelola status saat aplikasi stateful berhenti dan memulihkan dengan `upgradeMode` pengaturan. `JobSpec`

Mode upgrade

Pengenalan opsional

Tanpa kewarganegaraan

Peningkatan aplikasi stateless dari status kosong.

Keadaan terakhir

Peningkatan cepat dalam keadaan aplikasi apa pun (bahkan untuk pekerjaan yang gagal), tidak memerlukan pekerjaan yang sehat karena selalu menggunakan pos pemeriksaan terbaru yang berhasil. Pemulihan manual mungkin diperlukan jika metadata HA hilang. Untuk membatasi waktu pekerjaan mungkin mundur saat mengambil pos pemeriksaan terbaru yang dapat Anda konfigurasikan`kubernetes.operator.job.upgrade.last-state.max.allowed.checkpoint.age`. Jika pos pemeriksaan lebih tua dari nilai yang dikonfigurasi, savepoint akan diambil sebagai gantinya untuk pekerjaan yang sehat. Ini tidak didukung dalam mode Sesi.

Savepoint

Gunakan savepoint untuk upgrade, memberikan keamanan maksimal dan kemungkinan untuk berfungsi sebagai backup/fork point. Savepoint akan dibuat selama proses upgrade. Perhatikan bahwa pekerjaan Flink harus dijalankan untuk memungkinkan savepoint dibuat. Jika pekerjaan dalam keadaan tidak sehat, pos pemeriksaan terakhir akan digunakan (kecuali kubernetes.operator.job.upgrade. last-state-fallback.enabled disetel ke false). Jika pos pemeriksaan terakhir tidak tersedia, peningkatan pekerjaan akan gagal.

Pemecahan Masalah

Bagian ini menjelaskan cara memecahkan masalah dengan Amazon EMR di EKS. Untuk informasi tentang cara memecahkan masalah umum dengan Amazon EMR, lihat Memecahkan masalah klaster di Panduan Manajemen EMR Amazon.

- Pekerjaan pemecahan masalah yang menggunakan PersistentVolumeClaims (PVC)
- Memecahkan masalah Amazon EMR pada penskalaan otomatis vertikal EKS
- Memecahkan masalah Amazon EMR pada operator EKS

Memecahkan masalah Apache Flink di Amazon EMR di EKS

Pemetaan sumber daya tidak ditemukan saat menginstal bagan Helm

Anda mungkin menemukan pesan galat berikut saat menginstal bagan Helm.

```
Error: INSTALLATION FAILED: pulling from host 1234567890.dkr.ecr.us-
west-2.amazonaws.com failed with status code [manifests 6.13.0]: 403 Forbidden Error:
```

```
 INSTALLATION FAILED: unable to build kubernetes objects from release manifest:
 [resource mapping not found for name: "flink-operator-serving-cert" namespace: "<the
 namespace to install your operator>" from "": no matches for kind "Certificate" in
 version "cert-manager.io/v1"

ensure CRDs are installed first, resource mapping not found for name: "flink-operator-
selfsigned-issuer" namespace: "<the namespace to install your operator>" " from "": no
 matches for kind "Issuer" in version "cert-manager.io/v1"

ensure CRDs are installed first].
```

Untuk mengatasi kesalahan ini, instal cert-manager untuk mengaktifkan penambahan komponen webhook. Anda harus menginstal cert-manager ke setiap cluster Amazon EKS yang Anda gunakan.

```
kubectl apply -f https://github.com/cert-manager/cert-manager/releases/download/v1.12.0
```

Layanan AWSakses ditolak kesalahan

Jika Anda melihat access denied kesalahan, konfirmasikan bahwa peran IAM untuk `operatorExecutionRoleArn` dalam `values.yaml` file bagan Helm memiliki izin yang benar. Pastikan juga peran IAM `executionRoleArn` di bawah `FlinkDeployment` spesifikasi Anda memiliki izin yang benar.

`FlinkDeployment`macet

Jika Anda `FlinkDeployment` terhenti dalam keadaan tertangkap, gunakan langkah-langkah berikut untuk menghapus paksa penyebaran:

1. Edit proses penerapan.

   ```
   kubectl edit -n Flink Namespace flinkdeployments/App Name
   ```

2. Hapus finalizer ini.

   ```
   finalizers:
     - flinkdeployments.flink.apache.org/finalizer
   ```

3. Hapus penyebaran.

   ```
   kubectl delete -n Flink Namespace flinkdeployments/App Name
   ```

Rilis yang didukung untuk Amazon EMR di EKS dengan Apache Flink

Apache Flink tersedia dengan EMR Amazon berikut pada rilis EKS. Untuk informasi tentang semua rilis yang tersedia, lihatAmazon EMR pada rilis EKS.

Label rilis	Java	Flink	Operator Flink
emr-7.0.0-flink-latest	11	1.18.0	-
emr-7.0.0-flink-k8s-operator-latest	11	1.18.0	1.6.1
emr-6.15.0-flink-latest	11	1.17.1	-
emr-6.15.0-flink-k8s-operator-latest	11	1.17.1	1.6.0
emr-6.14.0-flink-latest	11	1.17.1	-
emr-6.14.0-flink-k8s-operator-latest	11	1.17.1	1.6.0
emr-6.13.0-flink-latest	11	1.17.0	-
emr-6.13.0-flink-k8s-operator-latest	11	1.17.0	1.5.0

Menjalankan pekerjaan dengan Amazon EMR di EKS

Job run adalah unit kerja, seperti jar Spark, PySpark skrip, atau kueri SparkSQL, yang Anda kirimkan ke Amazon EMR di EKS. Topik ini memberikan gambaran umum tentang mengelola tugas berjalan menggunakan AWS CLI, melihat tugas berjalan menggunakan konsol Amazon EMR, dan memecahkan masalah umum kesalahan tugas berjalan.

> **Note**
>
> Sebelum Anda mengirimkan pekerjaan dengan Amazon EMR di EKS, Anda harus menyelesaikan langkah-langkahnya. Menyiapkan Amazon EMR di EKS

Topik

Menjalankan pekerjaan Spark dengan `StartJobRun`

Topik

Menyiapkan Amazon EMR di EKS

Selesaikan tugas-tugas berikut untuk menyiapkan Amazon EMR di EKS. Jika Anda telah mendaftar untuk Amazon Web Services (AWS) dan telah menggunakan Amazon EKS, Anda hampir siap untuk menggunakan Amazon EMR di EKS. Lewati salah satu tugas yang telah Anda selesaikan.

> **Note**
>
> Anda juga dapat mengikuti Amazon EMR di EKS Workshop untuk mengatur semua sumber daya yang diperlukan untuk menjalankan pekerjaan Spark di Amazon EMR di EKS. Lokakarya ini juga menyediakan otomatisasi dengan menggunakan CloudFormation template untuk membuat sumber daya yang diperlukan bagi Anda untuk memulai. Untuk templat dan praktik terbaik lainnya, lihat Panduan Praktik Terbaik Kontainer EMR kami diGitHub.

1. Instal AWS CLI
2. Instal `eksctl`
3. Atur klaster Amazon EKS
4. Aktifkan akses klaster untuk Amazon EMR di EKS
5. Aktifkan IAM Role untuk Akun Layanan (IRSA) di klaster EKS
6. Untuk membuat peran eksekusi tugas
7. Perbarui kebijakan kepercayaan dari peran eksekusi tugas
8. Memberikan pengguna akses ke Amazon EMR di EKS
9. Daftarkan klaster Amazon EKS dengan Amazon EMR

Instal AWS CLI

Anda dapat menginstal versi terbaru dari AWS CLI untuk macOS, Linux, atau Windows.

> **Important**
>
> Untuk mengatur Amazon EMR di EKS, Anda harus memiliki versi terbaru AWS CLI diinstal.

Untuk menginstal atau memperbarui AWS CLI untuk macOS

1. Jika saat ini Anda memiliki AWS CLI terinstal, tentukan versi mana yang telah Anda instal.

   ```
   aws --version
   ```

2. Jika Anda memiliki versi sebelumnya dari AWS CLI, maka gunakan perintah berikut untuk menginstal AWS CLI versi 2 terbaru. Untuk opsi instalasi lainnya, atau untuk meningkatkan versi 2 yang saat ini diinstal, lihat Meningkatkan AWS CLI versi 2 di macOS.

   ```
   curl "https://awscli.amazonaws.com/AWSCLIV2.pkg" -o "AWSCLIV2.pkg"
   sudo installer -pkg AWSCLIV2.pkg -target /
   ```

   Jika Anda tidak dapat menggunakan AWS CLI versi 2, maka pastikan bahwa Anda memiliki versi terbaru dari AWS CLI versi 1 yang diinstal menggunakan perintah berikut.

   ```
   pip3 install awscli --upgrade --user
   ```

Untuk menginstal atau memperbarui AWS CLI untuk Linux

1. Jika saat ini Anda memiliki AWS CLI terinstal, tentukan versi mana yang telah Anda instal.

   ```
   aws --version
   ```

2. Jika Anda memiliki versi sebelumnya dari AWS CLI, maka gunakan perintah berikut untuk menginstal AWS CLI versi 2 terbaru. Untuk opsi instalasi lainnya, atau untuk meningkatkan versi 2 yang saat ini diinstal, lihat Meningkatkan AWS CLI versi 2 di Linux.

   ```
   curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip"
   unzip awscliv2.zip
   sudo ./aws/install
   ```

   Jika Anda tidak dapat menggunakan AWS CLI versi 2, maka pastikan bahwa Anda memiliki versi terbaru dari AWS CLI versi 1 yang diinstal menggunakan perintah berikut.

   ```
   pip3 install --upgrade --user awscli
   ```

Untuk menginstal atau memperbarui AWS CLI untuk Windows

1. Jika saat ini Anda memiliki AWS CLI terinstal, tentukan versi mana yang telah Anda instal.

   ```
   aws --version
   ```

2. Jika Anda memiliki versi sebelumnya dari AWS CLI, maka gunakan perintah berikut untuk menginstal AWS CLI versi 2 terbaru. Untuk opsi instalasi lainnya, atau untuk meningkatkan versi 2 yang saat ini diinstal, lihat Meningkatkan AWS CLI versi 2 di Windows.

   1. Unduh penginstal AWS CLI MSI untuk Windows (64-bit) di https://awscli.amazonaws.com/2.msi AWSCLIV
   2. Jalankan penginstal MSI yang diunduh dan ikuti instruksi di layar. Secara default, AWS CLI instalasi keC:\Program Files\Amazon\AWSCLIV2.

   Jika Anda tidak dapat menggunakan AWS CLI versi 2, maka pastikan bahwa Anda memiliki versi terbaru dari AWS CLI versi 1 yang diinstal menggunakan perintah berikut.

   ```
   pip3 install --user --upgrade awscli
   ```

Konfigurasi kredensial AWS CLI Anda

Baik eksctl dan AWS CLI mengharuskan Anda memiliki kredensial AWS yang terkonfigurasi di lingkungan Anda. Perintah `aws configure` adalah cara tercepat untuk mengatur instalasi AWS CLI Anda untuk penggunaan umum.

```
$ aws configure
AWS Access Key ID [None]: <AKIAIOSFODNN7EXAMPLE>
AWS Secret Access Key [None]: <wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY>
Default region name [None]: <region-code>
Default output format [None]: <json>
```

Ketika Anda mengetik perintah ini, AWS CLI meminta Anda untuk empat bagian informasi: Access key, secret access key, Wilayah AWS, dan format output. Informasi ini disimpan dalam profil (kumpulan pengaturan) bernama `default`. Profil ini digunakan saat Anda menjalankan perintah kecuali Anda menentukan perintah lain. Untuk informasi lebih lanjut, lihat Mengonfigurasi AWS CLI di AWS Command Line Interface Panduan Pengguna.

Instal `eksctl`

Instal versi terbaru utilitas baris `eksctl` perintah di macOS, Linux, atau Windows. Untuk informasi lebih lanjut, lihat https://eksctl.io/.

> **Important**
>
> Untuk mengatur Amazon EMR di EKS, Anda harus memiliki `eksctl` versi 0.34.0 atau yang lebih baru. Kami menyarankan Anda mengunduh eksctl terbaru, karena beberapa fungsi di Amazon EMR di EKS memerlukan versi yang lebih baru. Untuk informasi selengkapnya, lihat Instal `eksctl`.

Untuk menginstal atau meningkatkan eksctl di macOS menggunakan Homebrew

Cara termudah untuk memulai dengan Amazon EKS dan macOS adalah dengan menginstal eksctl dengan Homebrew. Resep eksctl Homebrew menginstal eksctl dan dependensi lain yang diperlukan untuk Amazon EKS, seperti kubectl. Resep juga menginstal aws-iam-authenticator, yang diperlukan jika Anda tidak memiliki AWS CLI versi 1.16.156 atau yang lebih baru diinstal.

1. Jika Anda belum menginstal Homebrew di macOS, instal dengan perintah berikut.

   ```
   /bin/bash -c "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/
   master/install.sh)"
   ```

2. Instal tap Weaveworks Homebrew.

   ```
   brew tap weaveworks/tap
   ```

3. 1. Menginstal atau meningkatkan eksctl.
      - Instal `eksctl` dengan perintah berikut.

        ```
        brew install weaveworks/tap/eksctl
        ```

      - Jika `eksctl` telah diinstal, jalankan perintah berikut untuk meningkatkan.

        ```
        brew upgrade eksctl & brew link --overwrite eksctl
        ```

   2. Uji apakah instalasi Anda berhasil dengan perintah berikut. Anda harus memiliki `eksctl` versi 0.34.0 atau lebih baru.

```
eksctl version
```

Untuk menginstal atau meningkatkan **`eksctl`** di Linux menggunakan **`curl`**

1. Unduh dan ekstrak rilis terbaru dari eksctl dengan perintah berikut.

```
curl --silent --location "https://github.com/weaveworks/eksctl/releases/latest/
download/eksctl_$(uname -s)_amd64.tar.gz" | tar xz -C /tmp
```

2. Pindahkan biner yang diekstrak ke /usr/local/bin.

```
sudo mv /tmp/eksctl /usr/local/bin
```

3. Uji apakah instalasi Anda berhasil dengan perintah berikut. Anda harus memiliki `eksctl` versi 0.34.0 atau lebih baru.

```
eksctl version
```

Untuk menginstal atau meningkatkan **`eksctl`** pada Windows menggunakan Chocolatey

1. Jika Anda belum menginstal Chocolatey pada sistem Windows Anda, lihat Menginstal Chocolatey.
2. Pasang atau tingkatkan `eksctl`.
   - Instal biner dengan perintah berikut.

```
chocolatey install -y eksctl
```

   - Jika biner telah diinstal, jalankan perintah berikut untuk meningkatkan:

```
chocolatey upgrade -y eksctl
```

3. Uji apakah instalasi Anda berhasil dengan perintah berikut. Anda harus memiliki `eksctl` versi 0.34.0 atau lebih baru.

```
eksctl version
```

Atur klaster Amazon EKS

Amazon EKS adalah sebuah layanan terkelola yang memudahkan Anda menjalankan Kubernetes AWS tanpa perlu menginstal, mengoperasikan, dan mengelola bidang kontrol atau simpul Kubernetes Anda sendiri. Ikuti langkah-langkah yang diuraikan di bawah ini untuk membuat klaster Kubernetes baru dengan node di Amazon EKS.

Prasyarat

> **Important**
>
> Sebelum Anda membuat klaster Amazon EKS, lengkapi persyaratan dan pertimbangan Amazon EKS VPC dan subnet dalam Panduan Pengguna Amazon EKS untuk memastikan bahwa klaster Amazon EKS Anda berfungsi dan menskalakan seperti yang diharapkan.

Anda harus menginstal dan mengkonfigurasi alat dan sumber daya berikut yang Anda butuhkan untuk membuat dan mengelola klaster Amazon EKS:

- Versi terbaru dariAWS CLI.
- `kubectl`versi 1.20 atau yang lebih baru.
- Versi terbaru dari`eksctl`.

Untuk informasi lebih lanjut, lihatInstal AWS CLI, Instalasi `kubectl`, danInstal `eksctl`.

Membuat klaster Amazon EKS menggunakan **`eksctl`**

Ambil langkah-langkah berikut untuk membuat klaster Amazon EKS menggunakan`eksctl`.

> **Important**
>
> Untuk memulai dengan cepat, Anda dapat membuat klaster EKS dan node dengan pengaturan default. Namun untuk penggunaan produksi, kami sarankan Anda menyesuaikan pengaturan untuk klaster dan node untuk memenuhi kebutuhan spesifik Anda. Untuk daftar semua pengaturan dan opsi, jalankan perintah`eksctl create cluster -h`. Untuk informasi selengkapnya, lihat Membuat dan Mengelola Kluster dalam `eksctl` dokumentasi.

1. Buat pasangan kunci Amazon EC2.

   Jika Anda tidak memiliki pasangan kunci yang ada, Anda dapat menjalankan perintah berikut untuk membuat pasangan kunci baru. Ganti `us-west-2` dengan Region tempat Anda ingin membuat klaster Anda.

   ```
   aws ec2 create-key-pair --region us-west-2 --key-name myKeyPair
   ```

   Simpan output yang dikembalikan dalam file di komputer lokal Anda. Untuk informasi selengkapnya, lihat Membuat atau mengimpor pasangan kunci dalam Panduan Pengguna Amazon EC2 untuk instans Linux.

   > **Note**
   >
   > Pasangan kunci tidak diperlukan untuk membuat klaster EKS. Tetapi menentukan pasangan kunci memungkinkan Anda untuk SSH ke node setelah mereka dibuat. Anda dapat menentukan pasangan kunci hanya ketika Anda membuat grup node.

2. Buat cluster EKS.

   Jalankan perintah berikut untuk membuat cluster EKS dan node. Ganti *cluster saya* dan *myKeyPair*dengan nama cluster dan nama pasangan kunci Anda sendiri. Ganti *us-west-2* dengan Region tempat Anda ingin membuat klaster Anda. Untuk informasi selengkapnya tentang Wilayah yang didukung Amazon EKS, lihat titik akhir dan kuota Amazon Elastic Kubernetes Service.

   ```
   eksctl create cluster \
   --name my-cluster \
   --region us-west-2 \
   --with-oidc \
   --ssh-access \
   --ssh-public-key myKeyPair \
   --instance-types=m5.xlarge \
   --managed
   ```

   > **Important**
   >
   > Saat membuat klaster EKS, gunakan m5.xlarge sebagai jenis instance, atau jenis instans lainnya dengan CPU dan memori yang lebih tinggi. Menggunakan jenis instans

dengan CPU atau memori yang lebih rendah dibandingkan dengan m5.xlarge dapat menyebabkan kegagalan pekerjaan karena sumber daya yang tidak mencukupi yang tersedia di klaster. Untuk melihat semua sumber daya yang dibuat, lihat stack bernama `eksctl-my-cluster-cluster` di konsol AWS Cloud Formation.

Proses pembuatan cluster dan node membutuhkan waktu beberapa menit. Anda akan melihat beberapa baris output ketika cluster dan node dibuat. Contoh berikut menunjukkan baris terakhir dari output.

```
...
[#]  EKS cluster "my-cluster" in "us-west-2" region is ready
```

`eksctl`membuat file `kubectl` konfigurasi `~/.kube` atau menambahkan konfigurasi cluster baru dalam file konfigurasi yang ada di. `~/.kube`

3. Melihat dan memvalidasi sumber daya

   Jalankan perintah berikut untuk melihat node cluster Anda.

   ```
   kubectl get nodes -o wide
   ```

   Berikut ini menunjukkan contoh output.

   ```
   Amazon EC2 node output

   NAME                                           STATUS   ROLES    AGE    VERSION
             INTERNAL-IP      EXTERNAL-IP     OS-IMAGE         KERNEL-VERSION
            CONTAINER-RUNTIME
   ip-192-168-12-49.us-west-2.compute.internal    Ready    none     6m7s
    v1.18.9-eks-d1db3c   192.168.12.49    52.35.116.65    Amazon Linux 2
    4.14.209-160.335.amzn2.x86_64   docker://19.3.6
   ip-192-168-72-129.us-west-2.compute.internal   Ready    none     6m4s
    v1.18.9-eks-d1db3c   192.168.72.129   44.242.140.21   Amazon Linux 2
    4.14.209-160.335.amzn2.x86_64   docker://19.3.6
   ```

   Untuk informasi selengkapnya, lihat Melihat node.

   Gunakan perintah berikut untuk melihat beban kerja yang berjalan di klaster Anda.

```
kubectl get pods --all-namespaces -o wide
```

Berikut ini menunjukkan contoh output.

```
Amazon EC2 output

NAMESPACE     NAME                       READY   STATUS    RESTARTS   AGE     IP
               NODE                                                NOMINATED NODE
 READINESS GATES
kube-system   aws-node-6ctpm             1/1     Running   0          7m43s
 192.168.72.129   ip-192-168-72-129.us-west-2.compute.internal   none
 none
kube-system   aws-node-cbntg             1/1     Running   0          7m46s
 192.168.12.49    ip-192-168-12-49.us-west-2.compute.internal    none
 none
kube-system   coredns-559b5db75d-26t47   1/1     Running   0          14m
 192.168.78.81    ip-192-168-72-129.us-west-2.compute.internal   none
 none
kube-system   coredns-559b5db75d-9rvnk   1/1     Running   0          14m
 192.168.29.248   ip-192-168-12-49.us-west-2.compute.internal    none
 none
kube-system   kube-proxy-l8pbd           1/1     Running   0          7m46s
 192.168.12.49    ip-192-168-12-49.us-west-2.compute.internal    none
 none
kube-system   kube-proxy-zh85h           1/1     Running   0          7m43s
 192.168.72.129   ip-192-168-72-129.us-west-2.compute.internal   none
 none
```

Untuk informasi selengkapnya tentang apa yang Anda lihat di sini, lihat Lihat beban kerja.

Buat klaster EKS menggunakan AWS Management Console dan AWS CLI

Anda juga dapat menggunakan AWS Management Console dan AWS CLI untuk membuat klaster EKS. Ikuti langkah-langkah di Memulai dengan Amazon EKS — AWS Management Console dan AWS CLI. Dengan cara ini memberi Anda visibilitas tentang bagaimana setiap sumber daya dibuat untuk klaster EKS dan bagaimana sumber daya berinteraksi satu sama lain.

> **Important**
>
> Saat membuat node untuk klaster EKS, gunakan m5.xlarge sebagai jenis instance, atau jenis instance lainnya dengan CPU dan memori yang lebih tinggi.

Buat klaster EKS dengan AWS Fargate

Kamu juga dapat membuat klaster EKS dengan Pod yang sedang berjalan. AWS Fargate

1. Untuk membuat klaster EKS dengan Pod yang berjalan di Fargate, ikuti langkah-langkah yang diuraikan pada Getting Started dengan AWS Fargate menggunakan Amazon EKS.

   > **Note**
   >
   > Amazon EMR pada EKS membutuhkan CoreDNS untuk menjalankan pekerjaan di klaster EKS. Jika kamu ingin menjalankan Pod kamu hanya di Fargate, kamu harus mengikuti langkah-langkah di Update CoreDNS.

2. Jalankan perintah berikut untuk melihat node cluster Anda.

   ```
   kubectl get nodes -o wide
   ```

   Berikut ini menunjukkan contoh output Fargate.

   ```
   Fargate node output

   NAME                                                  STATUS   ROLES    AGE
      VERSION              INTERNAL-IP       EXTERNAL-IP   OS-IMAGE         KERNEL-
   VERSION                   CONTAINER-RUNTIME
   fargate-ip-192-168-141-147.us-west-2.compute.internal   Ready    none
    8m3s    v1.18.8-eks-7c9bda   192.168.141.147   none          Amazon Linux 2
    4.14.209-160.335.amzn2.x86_64   containerd://1.3.2
   fargate-ip-192-168-164-53.us-west-2.compute.internal    Ready    none
    7m30s   v1.18.8-eks-7c9bda   192.168.164.53    none          Amazon Linux 2
    4.14.209-160.335.amzn2.x86_64   containerd://1.3.2
   ```

   Untuk informasi selengkapnya, lihat Melihat node.

3. Jalankan perintah berikut untuk melihat beban kerja yang berjalan di klaster Anda.

```
kubectl get pods --all-namespaces -o wide
```

Berikut ini menunjukkan contoh output Fargate.

```
Fargate output

NAMESPACE     NAME                          READY   STATUS    RESTARTS   AGE   IP
           NODE                                                    NOMINATED NODE
 READINESS GATES
kube-system   coredns-69dfb8f894-9z95l   1/1     Running   0          18m
 192.168.164.53    fargate-ip-192-168-164-53.us-west-2.compute.internal    none
         none
kube-system   coredns-69dfb8f894-c8v66   1/1     Running   0          18m
 192.168.141.147   fargate-ip-192-168-141-147.us-west-2.compute.internal   none
         none
```

Untuk informasi selengkapnya, lihat Melihat beban kerja.

Aktifkan akses klaster untuk Amazon EMR di EKS

Anda harus mengizinkan akses Amazon EMR di EKS ke namespace tertentu di klaster Anda dengan mengambil tindakan berikut: membuat peran Kubernetes, mengikat peran ke pengguna Kubernetes, dan memetakan pengguna Kubernetes dengan peran terkait layanan `AWSServiceRoleForAmazonEMRContainers`. Tindakan ini diotomatiskan di `eksctl` ketika perintah pemetaan identitas IAM digunakan dengan `emr-containers` sebagai nama layanan. Anda dapat melakukan operasi ini dengan mudah menggunakan perintah berikut.

```
eksctl create iamidentitymapping \
    --cluster my_eks_cluster \
    --namespace kubernetes_namespace \
    --service-name "emr-containers"
```

Ganti *`my_eks_cluster`* dengan nama klaster Amazon EKS Anda dan ganti *`kubernetes_namespace`* dengan namespace Kubernetes yang dibuat untuk menjalankan beban kerja Amazon EMR.

> **Important**
>
> Anda harus mengunduh eksctl terbaru menggunakan langkah Instal `eksctl` sebelumnya untuk menggunakan fungsi ini.

Langkah manual untuk mengaktifkan akses klaster untuk Amazon EMR di EKS

Anda juga dapat menggunakan langkah manual berikut untuk mengaktifkan akses klaster untuk Amazon EMR di EKS.

1. Membuat peran Kubernetes dalam namespace tertentu

   Amazon EKS 1.22 - 1.27

   Dengan Amazon EKS 1.22 - 1.27, jalankan perintah berikut untuk membuat peran Kubernetes dalam namespace tertentu. Peran ini memberikan izin RBAC yang diperlukan untuk Amazon EMR di EKS.

```
namespace=my-namespace
cat - >>EOF | kubectl apply -f - >>namespace "${namespace}"
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  name: emr-containers
  namespace: ${namespace}
rules:
  - apiGroups: [""]
    resources: ["namespaces"]
    verbs: ["get"]
  - apiGroups: [""]
    resources: ["serviceaccounts", "services", "configmaps", "events", "pods",
 "pods/log"]
    verbs: ["get", "list", "watch", "describe", "create", "edit", "delete",
 "deletecollection", "annotate", "patch", "label"]
  - apiGroups: [""]
    resources: ["secrets"]
    verbs: ["create", "patch", "delete", "watch"]
  - apiGroups: ["apps"]
    resources: ["statefulsets", "deployments"]
    verbs: ["get", "list", "watch", "describe", "create", "edit", "delete",
 "annotate", "patch", "label"]
```

```
  - apiGroups: ["batch"]
    resources: ["jobs"]
    verbs: ["get", "list", "watch", "describe", "create", "edit", "delete",
 "annotate", "patch", "label"]
  - apiGroups: ["extensions", "networking.k8s.io"]
    resources: ["ingresses"]
    verbs: ["get", "list", "watch", "describe", "create", "edit", "delete",
 "annotate", "patch", "label"]
  - apiGroups: ["rbac.authorization.k8s.io"]
    resources: ["roles", "rolebindings"]
    verbs: ["get", "list", "watch", "describe", "create", "edit", "delete",
 "deletecollection", "annotate", "patch", "label"]
  - apiGroups: [""]
    resources: ["persistentvolumeclaims"]
    verbs: ["get", "list", "watch", "describe", "create", "edit", "delete",
 "annotate", "patch", "label"]
EOF
```

Amazon EKS 1.21 and below

Dengan Amazon EKS 1.21 ke bawah, jalankan perintah berikut untuk membuat peran Kubernetes dalam namespace tertentu. Peran ini memberikan izin RBAC yang diperlukan untuk Amazon EMR di EKS.

```
namespace=my-namespace
cat - >>EOF | kubectl apply -f - >>namespace "${namespace}"
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  name: emr-containers
  namespace: ${namespace}
rules:
  - apiGroups: [""]
    resources: ["namespaces"]
    verbs: ["get"]
  - apiGroups: [""]
    resources: ["serviceaccounts", "services", "configmaps", "events", "pods",
 "pods/log"]
    verbs: ["get", "list", "watch", "describe", "create", "edit", "delete",
 "deletecollection", "annotate", "patch", "label"]
  - apiGroups: [""]
    resources: ["secrets"]
```

```
    verbs: ["create", "patch", "delete", "watch"]
  - apiGroups: ["apps"]
    resources: ["statefulsets", "deployments"]
    verbs: ["get", "list", "watch", "describe", "create", "edit", "delete",
 "annotate", "patch", "label"]
  - apiGroups: ["batch"]
    resources: ["jobs"]
    verbs: ["get", "list", "watch", "describe", "create", "edit", "delete",
 "annotate", "patch", "label"]
  - apiGroups: ["extensions"]
    resources: ["ingresses"]
    verbs: ["get", "list", "watch", "describe", "create", "edit", "delete",
 "annotate", "patch", "label"]
  - apiGroups: ["rbac.authorization.k8s.io"]
    resources: ["roles", "rolebindings"]
    verbs: ["get", "list", "watch", "describe", "create", "edit", "delete",
 "deletecollection", "annotate", "patch", "label"]
  - apiGroups: [""]
    resources: ["persistentvolumeclaims"]
    verbs: ["get", "list", "watch", "describe", "create", "edit", "delete",
 "annotate", "patch", "label"]
EOF
```

2. Membuat role binding Kubernetes yang tercakup pada namespace

   Jalankan perintah berikut untuk membuat peran mengikat Kubernetes mengikat di namespace yang diberikan. Pengikatan peran ini memberikan izin yang ditetapkan dalam peran yang dibuat di langkah sebelumnya ke pengguna bernama `emr-containers`. Pengguna ini mengidentifikasi peran terkait layanan untuk Amazon EMR di EKS dan dengan demikian memungkinkan Amazon EMR di EKS untuk melakukan tindakan seperti yang didefinisikan oleh peran yang Anda buat.

```
namespace=my-namespace

cat - <<EOF | kubectl apply -f - --namespace "${namespace}"
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: emr-containers
  namespace: ${namespace}
subjects:
- kind: User
```

```
  name: emr-containers
  apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: Role
  name: emr-containers
  apiGroup: rbac.authorization.k8s.io
EOF
```

3. Memperbarui peta konfigurasi Kubernetes **`aws-auth`**

   Anda dapat menggunakan salah satu opsi berikut untuk memetakan Amazon EMR di EKS peran terkait layanan dengan pengguna `emr-containers` yang terikat dengan peran Kubernetes pada langkah sebelumnya.

   Opsi 1: Menggunakan **`eksctl`**

   Jalankan perintah `eksctl` berikut untuk memetakan peran terkait layanan EMR Amazon di EKS dengan pengguna `emr-containers`.

   ```
   eksctl create iamidentitymapping \
       --cluster my-cluster-name \
       --arn "arn:aws:iam::my-account-id:role/AWSServiceRoleForAmazonEMRContainers" \
       --username emr-containers
   ```

   Opsi 2: Tanpa menggunakan eksctl

   1. Jalankan perintah berikut untuk membuka peta konfigurasi `aws-auth` dalam editor teks.

      ```
      kubectl edit -n kube-system configmap/aws-auth
      ```

      > **Note**
      >
      > Jika Anda menerima kesalahan yang menyatakan`Error from server (NotFound): configmaps "aws-auth" not found`, lihat langkah-langkah dalam Menambahkan peran pengguna di Panduan Pengguna Amazon EKS untuk menerapkan stokConfigMap.

   2. Tambahkan detail peran terkait Amazon EMR di EKS ke bagian `mapRoles` dari `ConfigMap`, di bawah `data`. Tambahkan bagian ini jika belum ada dalam file. Bagian `mapRoles` yang diperbarui di bawah data terlihat seperti contoh berikut.

```
apiVersion: v1
data:
  mapRoles: |
    - rolearn: arn:aws:iam::<your-account-id>:role/
AWSServiceRoleForAmazonEMRContainers
      username: emr-containers
    - ... <other previously existing role entries, if there's any>.
```

3. Simpan file , dan tutup editor teks Anda.

Aktifkan IAM Role untuk Akun Layanan (IRSA) di klaster EKS

IAM role untuk fitur akun layanan tersedia di Amazon EKS versi 1.14 dan yang lebih baru dan untuk klaster EKS yang diperbarui ke versi 1.13 atau yang lebih baru pada atau setelah 3 September 2019. Untuk menggunakan fitur ini, Anda dapat memperbarui klaster EKS yang ada ke versi 1.14 atau yang lebih baru. Untuk informasi lebih lanjut, lihat Memperbarui versi Kubernetes klaster Amazon EKS.

Jika klaster Anda mendukung IAM role untuk akun layanan, klaster Anda memiliki URL penerbit Connect OpenID yang terkait dengannya. Anda dapat melihat URL ini di konsol Amazon EKS, atau Anda dapat menggunakan perintah AWS CLI berikut untuk mengambilnya.

> **Important**
>
> Anda harus menggunakan versi terbaru dari AWS CLI untuk menerima output yang tepat dari perintah ini.

```
aws eks describe-cluster --name cluster_name --query "cluster.identity.oidc.issuer" --
output text
```

Output yang diharapkan adalah sebagai berikut.

```
https://oidc.eks.<region-code>.amazonaws.com/id/EXAMPLED539D4633E53DE1B716D3041E
```

Untuk menggunakan IAM role untuk akun layanan di klaster Anda, Anda harus membuat penyedia identitas OIDC menggunakan baik eksctl atau AWS Management Console.

Untuk membuat penyedia identitas IAM OIDC untuk klaster Anda dengan **`eksctl`**

Periksa versi `eksctl` Anda dengan perintah berikut. Prosedur ini mengasumsikan bahwa Anda telah menginstal `eksctl` dan bahwa `eksctl` versi 0.32.0 atau yang lebih baru.

```
eksctl version
```

Untuk informasi selengkapnya tentang menginstal atau meningkatkan eksctl, lihat Menginstal atau meningkatkan eksctl.

Buat penyedia identitas OIDC Anda untuk klaster Anda dengan perintah berikut. Ganti *`cluster_name`* dengan nilai Anda sendiri.

```
eksctl utils associate-iam-oidc-provider --cluster cluster_name --approve
```

Untuk membuat penyedia identitas IAM OIDC untuk klaster Anda dengan AWS Management Console

Ambil URL penerbit OIDC dari deskripsi konsol Amazon EKS dari klaster Anda, atau gunakan perintah AWS CLI berikut.

Gunakan perintah berikut untuk mengambil URL penerbit OIDC dari AWS CLI.

```
aws eks describe-cluster --name <cluster_name> --query "cluster.identity.oidc.issuer"
 --output text
```

Gunakan langkah-langkah berikut untuk mengambil URL penerbit OIDC dari konsol Amazon EKS.

1. Buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, pilih Penyedia Identitas, lalu pilih Buat Penyedia.
    1. Untuk Jenis Penyedia, pilih Pilih jenis penyedia, lalu pilih OpenID Connect.
    2. Untuk Penyedia URL, tempelkan URL penerbit OIDC untuk klaster Anda.
    3. Untuk Audiens, ketik sts.amazonaws.com dan pilih Langkah Selanjutnya.
3. Verifikasi bahwa informasi penyedia sudah benar, kemudian pilih Buat untuk membuat penyedia identitas Anda.

Untuk membuat peran eksekusi tugas

Untuk menjalankan beban kerja di Amazon EMR di EKS, Anda perlu membuat peran IAM. Kami menyebut peran ini sebagai peran eksekusi tugas dalam dokumentasi ini. Untuk informasi selengkapnya tentang cara membuat peran IAM, lihat Membuat peran IAM di Panduan Pengguna IAM.

Anda juga harus membuat kebijakan IAM yang menentukan izin untuk peran eksekusi pekerjaan dan kemudian melampirkan kebijakan IAM ke peran eksekusi pekerjaan.

Kebijakan berikut untuk peran eksekusi pekerjaan memungkinkan akses ke target sumber daya, Amazon S3, dan. CloudWatch Izin ini diperlukan untuk memantau tugas dan log akses. Untuk mengikuti proses yang sama menggunakanAWS CLI, Anda juga dapat mengatur peran Anda menggunakan langkah-langkah di bagian Buat Peran IAM untuk eksekusi pekerjaan di Amazon EMR on EKS Workshop.

> **Note**
>
> Akses harus dicakup dengan tepat, tidak diberikan ke semua objek S3 dalam peran eksekusi pekerjaan.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": "arn:aws:s3:::example-bucket"
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents",
                "logs:CreateLogStream",
                "logs:DescribeLogGroups",
                "logs:DescribeLogStreams"
```

```
            ],
            "Resource": [
                "arn:aws:logs:*:*:*"
            ]
        }
    ]
}
```

Untuk informasi selengkapnya, lihat Menggunakan peran eksekusi pekerjaan, Mengkonfigurasi pekerjaan yang dijalankan untuk menggunakan log S3, dan Mengkonfigurasi pekerjaan yang dijalankan untuk menggunakan CloudWatch Log.

Perbarui kebijakan kepercayaan dari peran eksekusi tugas

Ketika Anda menggunakan IAM Role untuk Akun Layanan (IRSA) untuk menjalankan tugas di namespace Kubernetes, administrator harus membuat hubungan kepercayaan antara peran eksekusi tugas dan identitas akun layanan terkelola EMR. Hubungan kepercayaan dapat dibuat dengan memperbarui kebijakan kepercayaan dari peran pelaksanaan tugas. Perhatikan bahwa akun layanan terkelola EMR secara otomatis dibuat pada pengiriman tugas, dicakup ke namespace di mana tugas dikirimkan.

Jalankan perintah berikut untuk memperbarui kebijakan kepercayaan.

```
aws emr-containers update-role-trust-policy \
      --cluster-name cluster \
      --namespace namespace \
      --role-name iam_role_name_for_job_execution
```

Untuk informasi selengkapnya, lihat Menggunakan peran eksekusi tugas dengan Amazon EMR di EKS.

> **Important**
>
> Operator yang menjalankan perintah di atas harus memiliki izin berikut: `eks:DescribeCluster`, `iam:GetRole`, `iam:UpdateAssumeRolePolicy`.

Memberikan pengguna akses ke Amazon EMR di EKS

Untuk setiap tindakan yang Anda lakukan di Amazon EMR di EKS, Anda memerlukan izin IAM yang sesuai untuk tindakan itu. Anda harus membuat kebijakan IAM yang memungkinkan Anda untuk melakukan tindakan Amazon EMR di EKS dan melampirkan kebijakan pada pengguna atau peran IAM yang Anda gunakan.

Topik ini menyediakan langkah-langkah untuk membuat kebijakan baru dan melampirkannya ke pengguna. Hal ini juga mencakup izin dasar yang Anda butuhkan untuk mengatur lingkungan Amazon EMR di EKS Anda. Sebaiknya Anda menyempurnakan izin ke sumber daya tertentu bila memungkinkan berdasarkan kebutuhan bisnis Anda.

Membuat kebijakan IAM baru dan melampirkannya ke pengguna di konsol IAM

Buat kebijakan IAM baru

1. Masuk ke AWS Management Console dan buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi kiri konsol IAM, pilih Kebijakan.
3. Pada halaman Kebijakan, pilih Buat Kebijakan.
4. Di jendela Buat Kebijakan, navigasikan ke tab Edit JSON. Buat dokumen kebijakan dengan satu atau lebih pernyataan JSON seperti yang ditunjukkan dalam contoh prosedur berikut ini. Selanjutnya, pilih Tinjau kebijakan.
5. Pada layar Tinjau Kebijakan, masukkan Nama kebijakanAnda, misalnya `AmazonEMROnEKSPolicy`. Masukkan deskripsi opsional, lalu pilih Buat kebijakan.

Melampirkan kebijakan ke pengguna atau peran

1. Masuk ke AWS Management Console dan buka konsol IAM di https://console.aws.amazon.com/iam/
2. Di panel navigasi, pilih Kebijakan.
3. Dalam daftar kebijakan, pilih kotak centang di samping kebijakan yang dibuat dalam bagian sebelumnya. Anda bisa memakai menu Filter dan kotak pencarian untuk memfilter daftar kebijakan.
4. Pilih Tindakan kebijakan, lalu pilih Lampirkan.

5. Pilih pengguna atau peran untuk melampirkan kebijakan. Anda bisa memakai menu Filter dan kotak pencarian untuk memfilter daftar entitas prinsipiel. Setelah memilih pengguna atau peran untuk melampirkan kebijakan, pilih Lampirkan kebijakan.

Izin untuk mengelolaklaster virtual

Untuk mengelola klaster virtual di akun AWS Anda, buat kebijakan IAM dengan izin berikut. Izin ini memungkinkan Anda untuk membuat, mendaftar, menjelaskan, dan menghapus klaster virtual di akun AWS Anda.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "emr-containers.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "emr-containers:CreateVirtualCluster",
                "emr-containers:ListVirtualClusters",
                "emr-containers:DescribeVirtualCluster",
                "emr-containers:DeleteVirtualCluster"
            ],
            "Resource": "*"
        }
    ]
}
```

Saat operasi `CreateVirtualCluster` dipanggil untuk pertama kalinya dari sebuah akun AWS, Anda juga memerlukan izin `CreateServiceLinkedRole` untuk membuat peran terkait layanan

untuk Amazon EMR di EKS. Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan untuk Amazon EMR di EKS.

Izin untuk mengirimkan tugas

Untuk mengirimkan tugas pada klaster virtual di akun AWS Anda, buat kebijakan IAM dengan izin berikut. Izin ini memungkinkan Anda untuk memulai, mendaftar, menjelaskan, dan membatalkan klaster virtual di akun Anda. Anda harus mempertimbangkan menambahkan izin untuk membuat daftar atau menjelaskan klaster virtual, yang memungkinkan Anda untuk memeriksa keadaan klaster virtual sebelum mengirimkan tugas.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "emr-containers:StartJobRun",
                "emr-containers:ListJobRuns",
                "emr-containers:DescribeJobRun",
                "emr-containers:CancelJobRun"
            ],
            "Resource": "*"
        }
    ]
}
```

Izin untuk melakukan debug dan pemantauan

Untuk mendapatkan akses ke log yang didorong ke Amazon S3 danCloudWatch, atau untuk melihat log peristiwa aplikasi di konsol Amazon EMR, buat kebijakan IAM dengan izin berikut. Sebaiknya Anda menyempurnakan izin ke sumber daya tertentu bila memungkinkan berdasarkan kebutuhan bisnis Anda.

> **Important**
>
> Jika Anda belum membuat bucket Amazon S3, Anda perlu menambahkan izin `s3:CreateBucket` pada pernyataan kebijakan. Jika Anda belum membuat grup log, Anda perlu menambahkan `logs:CreateLogGroup` pada pernyataan kebijakan.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "emr-containers:DescribeJobRun",
                "elasticmapreduce:CreatePersistentAppUI",
                "elasticmapreduce:DescribePersistentAppUI",
                "elasticmapreduce:GetPersistentAppUIPresignedURL"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:Get*",
                "logs:DescribeLogGroups",
                "logs:DescribeLogStreams"
            ],
            "Resource": "*"
        }
    ]
}
```

Untuk informasi selengkapnya tentang cara mengonfigurasi pekerjaan yang dijalankan untuk mendorong log ke Amazon S3 danCloudWatch, lihat Mengonfigurasi pekerjaan yang dijalankan untuk menggunakan log S3 dan Mengkonfigurasi pekerjaan yang dijalankan untuk menggunakan CloudWatch Log.

Daftarkan klaster Amazon EKS dengan Amazon EMR

Mendaftarkan klaster Anda adalah langkah terakhir yang diperlukan untuk mengatur Amazon EMR di EKS untuk menjalankan beban kerja.

Gunakan perintah berikut untuk membuat klaster virtual dengan nama pilihan Anda untuk klaster Amazon EKS dan namespace yang Anda atur dalam langkah-langkah sebelumnya.

> **Note**
>
> Setiap cluster virtual harus memiliki nama unik di semua cluster EKS. Jika dua cluster virtual memiliki nama yang sama, proses penyebaran akan gagal bahkan jika kedua cluster virtual milik cluster EKS yang berbeda.

```
aws emr-containers create-virtual-cluster \
--name virtual_cluster_name \
--container-provider '{
    "id": "cluster_name",
    "type": "EKS",
    "info": {
        "eksInfo": {
            "namespace": "namespace_name"
        }
    }
}'
```

Atau, Anda dapat membuat file JSON yang mencakup parameter yang diperlukan untuk klaster virtual dan kemudian jalankan perintah `create-virtual-cluster` dengan jalur ke file JSON. Untuk informasi selengkapnya, lihat Mengelola klaster virtual.

> **Note**
>
> Untuk memvalidasi keberhasilan pembuatan klaster virtual, lihat status klaster virtual menggunakan operasi `list-virtual-clusters` atau dengan masuk ke halaman Klaster Virtual di konsol Amazon EMR.

Kirim pekerjaan yang dijalankan dengan `StartJobRun`

Untuk mengirimkan pekerjaan yang dijalankan dengan file JSON dengan parameter tertentu

1. Buat file `start-job-run-request.json` dan tentukan parameter yang diperlukan untuk menjalankan tugas Anda, seperti contoh yang ditunjukkan file JSON berikut. Untuk informasi tentang parameter, lihat Pilihan untuk mengonfigurasi tugas berjalan.

```
{
  "name": "myjob",
  "virtualClusterId": "123456",
  "executionRoleArn": "iam_role_name_for_job_execution",
  "releaseLabel": "emr-6.2.0-latest",
  "jobDriver": {
    "sparkSubmitJobDriver": {
      "entryPoint": "entryPoint_location",
      "entryPointArguments": ["argument1", "argument2", ...],
       "sparkSubmitParameters": "--class <main_class> --conf
 spark.executor.instances=2 --conf spark.executor.memory=2G --conf
 spark.executor.cores=2 --conf spark.driver.cores=1"
    }
  },
  "configurationOverrides": {
    "applicationConfiguration": [
      {
        "classification": "spark-defaults",
        "properties": {
          "spark.driver.memory":"2G"
         }
      }
    ],
    "monitoringConfiguration": {
      "persistentAppUI": "ENABLED",
      "cloudWatchMonitoringConfiguration": {
        "logGroupName": "my_log_group",
        "logStreamNamePrefix": "log_stream_prefix"
      },
      "s3MonitoringConfiguration": {
        "logUri": "s3://my_s3_log_location"
      }
    }
  }
```

```
}
```

2. Gunakan `start-job-run` perintah dengan path ke `start-job-run-request.json` file yang disimpan secara lokal.

```
aws emr-containers start-job-run \
--cli-input-json file://./start-job-run-request.json
```

Untuk memulai tugas berjalan menggunakan perintah **`start-job-run`**

1. Pasokan semua parameter yang ditentukan dalam perintah `StartJobRun`, seperti yang ditunjukkan contoh berikut.

```
aws emr-containers start-job-run \
--virtual-cluster-id 123456 \
--name myjob \
--execution-role-arn execution-role-arn \
--release-label emr-6.2.0-latest \
--job-driver '{"sparkSubmitJobDriver": {"entryPoint": "entryPoint_location",
 "entryPointArguments": ["argument1", "argument2", ...], "sparkSubmitParameters":
 "--class <main_class> --conf spark.executor.instances=2 --conf
 spark.executor.memory=2G --conf spark.executor.cores=2 --conf
 spark.driver.cores=1"}}' \
--configuration-overrides '{"applicationConfiguration": [{"classification":
 "spark-defaults", "properties": {"spark.driver.memory": "2G"}}],
 "monitoringConfiguration": {"cloudWatchMonitoringConfiguration":
 {"logGroupName": "log_group_name", "logStreamNamePrefix": "log_stream_prefix"},
 "persistentAppUI":"ENABLED",  "s3MonitoringConfiguration": {"logUri":
 "s3://my_s3_log_location" }}}'
```

2. Untuk Spark SQL, sediakan semua parameter yang ditentukan dalam `StartJobRun` perintah, seperti yang ditunjukkan contoh berikut.

```
aws emr-containers start-job-run \
--virtual-cluster-id 123456 \
--name myjob \
--execution-role-arn execution-role-arn \
--release-label emr-6.7.0-latest \
--job-driver '{"sparkSqlJobDriver": {"entryPoint": "entryPoint_location",
 "sparkSqlParameters": "--conf spark.executor.instances=2 --conf
```

```
 spark.executor.memory=2G --conf spark.executor.cores=2 --conf
 spark.driver.cores=1"}}' \
--configuration-overrides '{"applicationConfiguration": [{"classification":
 "spark-defaults", "properties": {"spark.driver.memory": "2G"}}],
 "monitoringConfiguration": {"cloudWatchMonitoringConfiguration":
 {"logGroupName": "log_group_name", "logStreamNamePrefix": "log_stream_prefix"},
 "persistentAppUI":"ENABLED",  "s3MonitoringConfiguration": {"logUri":
 "s3://my_s3_log_location" }}}'
```

Menjalankan pekerjaan Spark dengan operator Spark

Amazon EMR merilis 6.10.0 dan lebih tinggi mendukung operator Kubernetes untuk Apache Spark, atau operator Spark, sebagai model pengiriman pekerjaan untuk Amazon EMR di EKS. Dengan operator Spark, Anda dapat menerapkan dan mengelola aplikasi Spark dengan runtime rilis Amazon EMR di kluster Amazon EKS Anda sendiri. Setelah Anda menyebarkan operator Spark di cluster Amazon EKS Anda, Anda dapat langsung mengirimkan aplikasi Spark dengan operator. Operator mengelola siklus hidup aplikasi Spark.

> **Note**
>
> Amazon EMR menghitung harga di Amazon EKS berdasarkan vCPU dan sumber daya memori yang Anda gunakan dari pod operator sejak Anda mulai mengunduh gambar aplikasi Amazon EMR hingga pod Amazon EKS berakhir, dibulatkan ke detik terdekat.

Topik

- Menyiapkan operator Spark untuk Amazon EMR di EKS
- Memulai dengan operator Spark untuk Amazon EMR di EKS
- Menggunakan penskalaan otomatis vertikal dengan operator Spark untuk Amazon EMR di EKS
- Menghapus instalasi operator Spark untuk Amazon EMR di EKS
- Keamanan dan operator Spark dengan Amazon EMR di EKS

Menyiapkan operator Spark untuk Amazon EMR di EKS

Selesaikan tugas-tugas berikut untuk menyiapkan sebelum Anda menginstal operator Spark di Amazon EKS. Jika Anda sudah mendaftar untuk Amazon Web Services (AWS) dan telah

menggunakan Amazon EKS, Anda hampir siap untuk menggunakan Amazon EMR di EKS. Selesaikan tugas-tugas berikut untuk menyiapkan operator Spark di Amazon EKS. Jika Anda telah menyelesaikan salah satu prasyarat, Anda dapat melewatinya dan melanjutkan ke yang berikutnya.

- Instal AWS CLI— Jika Anda sudah menginstalAWS CLI, konfirmasikan bahwa Anda memiliki versi terbaru.
- Instal eksctl - eksctl adalah alat baris perintah yang Anda gunakan untuk berkomunikasi dengan Amazon EKS.
- Instal Helm — Manajer paket Helm untuk Kubernetes membantu Anda menginstal dan mengelola aplikasi di klaster Kubernetes Anda.
- Siapkan cluster Amazon EKS — Ikuti langkah-langkah untuk membuat cluster Kubernetes baru dengan node di Amazon EKS.
- Pilih URI gambar dasar EMR Amazon (rilis 6.10.0 atau lebih tinggi) — operator Spark didukung dengan rilis Amazon EMR 6.10.0 dan yang lebih tinggi.

Memulai dengan operator Spark untuk Amazon EMR di EKS

Topik ini membantu Anda mulai menggunakan operator Spark di Amazon EKS dengan menerapkan aplikasi Spark dan aplikasi Schedule Spark.

Instal operator Spark

Gunakan langkah-langkah berikut untuk menginstal operator Kubernetes untuk Apache Spark.

1. Jika Anda belum melakukannya, selesaikan langkah-langkahnyaMenyiapkan operator Spark untuk Amazon EMR di EKS.
2. Otentikasi klien Helm Anda ke registri Amazon ECR. Dalam perintah berikut, ganti nilai *region-id* dengan pilihan AndaWilayah AWS, dan nilai akun *ECR-Registry-Account* yang sesuai untuk Wilayah dari halaman. Akun registri Amazon ECR berdasarkan Wilayah

   ```
   aws ecr get-login-password \
   --region region-id | helm registry login \
   --username AWS \
   --password-stdin ECR-registry-account.dkr.ecr.region-id.amazonaws.com
   ```

3. Instal operator Spark dengan perintah berikut.

Untuk `--version` parameter bagan Helm, gunakan label rilis Amazon EMR Anda dengan awalan dan `emr-` akhiran tanggal dihapus. Misalnya, dengan `emr-6.12.0-java17-latest` rilis, tentukan`6.12.0-java17`. Contoh dalam perintah berikut menggunakan `emr-7.0.0-latest` rilis, sehingga menentukan `7.0.0` bagan Helm. `--version`

```
helm install spark-operator-demo \
  oci://895885662937.dkr.ecr.region-id.amazonaws.com/spark-operator \
  --set emrContainers.awsRegion=region-id \
  --version 7.0.0 \
  --namespace spark-operator \
  --create-namespace
```

Secara default, perintah membuat akun layanan `emr-containers-sa-spark-operator` untuk operator Spark. Untuk menggunakan akun layanan yang berbeda, berikan argumennya`serviceAccounts.sparkoperator.name`. Sebagai contoh:

```
--set serviceAccounts.sparkoperator.name my-service-account-for-spark-operator
```

Jika Anda ingin menggunakan penskalaan otomatis vertikal dengan operator Spark, tambahkan baris berikut ke perintah instalasi untuk mengizinkan webhook untuk operator:

```
--set webhook.enable=true
```

4. Verifikasi bahwa Anda menginstal bagan Helm dengan `helm list` perintah:

```
helm list --namespace spark-operator -o yaml
```

`helm list`Perintah harus mengembalikan informasi rilis bagan Helm yang baru Anda gunakan:

```
app_version: v1beta2-1.3.8-3.1.1
chart: spark-operator-7.0.0
name: spark-operator-demo
namespace: spark-operator
revision: "1"
status: deployed
updated: 2023-03-14 18:20:02.721638196 +0000 UTC
```

5. Instalasi lengkap dengan opsi tambahan apa pun yang Anda butuhkan. Untuk informasi lebih lanjut, lihat `spark-on-k8s-operator`dokumentasi di GitHub.

Jalankan aplikasi Spark

Operator Spark didukung dengan Amazon EMR 6.10.0 atau lebih tinggi. Ketika Anda menginstal operator Spark, itu membuat akun layanan `emr-containers-sa-spark` untuk menjalankan aplikasi Spark secara default. Gunakan langkah-langkah berikut untuk menjalankan aplikasi Spark dengan operator Spark di Amazon EMR di EKS 6.10.0 atau lebih tinggi.

1. Sebelum Anda dapat menjalankan aplikasi Spark dengan operator Spark, selesaikan langkah-langkah di Menyiapkan operator Spark untuk Amazon EMR di EKS dan. Instal operator Spark
2. Buat file `SparkApplication` definisi `spark-pi.yaml` dengan isi contoh berikut:

```
apiVersion: "sparkoperator.k8s.io/v1beta2"
kind: SparkApplication
metadata:
  name: spark-pi
  namespace: spark-operator
spec:
  type: Scala
  mode: cluster
  image: "895885662937.dkr.ecr.us-west-2.amazonaws.com/spark/emr-6.10.0:latest"
  imagePullPolicy: Always
  mainClass: org.apache.spark.examples.SparkPi
  mainApplicationFile: "local:///usr/lib/spark/examples/jars/spark-examples.jar"
  sparkVersion: "3.3.1"
  restartPolicy:
    type: Never
  volumes:
    - name: "test-volume"
      hostPath:
        path: "/tmp"
        type: Directory
  driver:
    cores: 1
    coreLimit: "1200m"
    memory: "512m"
    labels:
      version: 3.3.1
    serviceAccount: emr-containers-sa-spark
    volumeMounts:
      - name: "test-volume"
        mountPath: "/tmp"
  executor:
```

```
    cores: 1
    instances: 1
    memory: "512m"
    labels:
      version: 3.3.1
    volumeMounts:
      - name: "test-volume"
        mountPath: "/tmp"
```

3. Sekarang, kirimkan aplikasi Spark dengan perintah berikut. Ini juga akan membuat `SparkApplication` objek bernama`spark-pi`:

```
kubectl apply -f spark-pi.yaml
```

4. Periksa peristiwa untuk `SparkApplication` objek dengan perintah berikut:

```
kubectl describe sparkapplication spark-pi --namespace spark-operator
```

Untuk informasi selengkapnya tentang mengirimkan aplikasi ke Spark melalui operator Spark, lihat Menggunakan a `SparkApplication` dalam dokumentasi pada. `spark-on-k8s-operator` GitHub

Menggunakan penskalaan otomatis vertikal dengan operator Spark untuk Amazon EMR di EKS

Amazon EMR pada penskalaan otomatis vertikal EKS menyederhanakan manajemen sumber daya. Ini secara otomatis menyetel memori dan sumber daya CPU untuk beradaptasi dengan kebutuhan beban kerja yang Anda sediakan untuk aplikasi Amazon EMR Spark. Untuk informasi selengkapnya, lihat Menggunakan penskalaan otomatis vertikal dengan pekerjaan Amazon EMR Spark .

Bagian ini menjelaskan cara mengkonfigurasi operator Spark untuk menggunakan penskalaan otomatis vertikal.

Prasyarat

Sebelum melanjutkan, pastikan untuk menyelesaikan pengaturan berikut:

- Selesaikan langkah-langkah dalam Menyiapkan operator Spark untuk Amazon EMR di EKS.
- Selesaikan langkah-langkah dalam Instal operator Spark. Pada langkah 3, tambahkan baris berikut ke perintah instalasi untuk mengizinkan webhook untuk operator:

```
--set webhook.enable=true
```

Jalankan pekerjaan dengan penskalaan otomatis vertikal pada operator Spark

Sebelum Anda dapat menjalankan aplikasi Spark dengan operator Spark, Anda harus menyelesaikan langkah-langkahnya. Prasyarat

Untuk menggunakan penskalaan otomatis vertikal dengan operator Spark, ada beberapa konfigurasi yang diperlukan untuk ditambahkan ke aplikasi Anda. Anda dapat menemukan contoh di bawah daftar ini.

Konfigurasi driver

Tambahkan anotasi berikut ke konfigurasi driver Anda:

```
emr-containers.amazonaws.com/dynamic.sizing.signature: "YOUR_JOB_SIGNATURE"
```

Tambahkan label berikut ke konfigurasi aplikasi Anda:

```
emr-containers.amazonaws.com/dynamic.sizing: "true"
```

Konfigurasi pelaksana

Tambahkan label berikut ke konfigurasi eksekutor Anda:

```
emr-containers.amazonaws.com/dynamic.sizing.signature: "YOUR_JOB_SIGNATURE"
```

Tentukan variabel lingkungan berikut untuk konfigurasi pelaksana Anda:

```
- name: DYNAMIC_SIZING_ENABLED
        value: "true" # true, not set otherwise
- name: OVERHEAD_FACTOR
        value: "0.1" # value of spark.kubernetes.memoryOverheadFactor
                     # or spark.driver.memoryOverheadFactor, not set otherwise
- name: PYSPARK_MEM
        value: "0.1" # value of spark.executor.pyspark.memory, not set otherwise
- name: EXEC_POD_CPU_REQUEST
        valueFrom:
          resourceFieldRef:
```

```
            containerName: spark-kubernetes-executor
            resource: requests.cpu
            divisor: 1
- name: EXEC_POD_CPU_LIMIT
        valueFrom:
          resourceFieldRef:
            containerName: spark-kubernetes-executor
            resource: limits.cpu
            divisor: 1
- name: EXEC_POD_MEM_REQUEST
        valueFrom:
          resourceFieldRef:
            containerName: spark-kubernetes-executor
            resource: requests.memory
            divisor: 1
- name: EXEC_POD_MEM_LIMIT
        valueFrom:
          resourceFieldRef:
            containerName: spark-kubernetes-executor
            resource: limits.memory
            divisor: 1
```

Contoh berikut menunjukkan file `SparkApplication` definisi `spark-pi.yaml` dengan konfigurasi yang diperlukan untuk menggunakan penskalaan otomatis vertikal:

```
apiVersion: "sparkoperator.k8s.io/v1beta2"
kind: SparkApplication
metadata:
  name: spark-pi
  namespace: spark-operator
spec:
  type: Scala
  mode: cluster
  image: "895885662937.dkr.ecr.us-west-2.amazonaws.com/spark/emr-6.10.0:latest"
  imagePullPolicy: Always
  mainClass: org.apache.spark.examples.SparkPi
  mainApplicationFile: "local:///usr/lib/spark/examples/jars/spark-examples.jar"
  arguments:
    - "10000"
  sparkVersion: "3.3.1"
  sparkConf:
    spark.kubernetes.executor.deleteOnTermination: "true"
```

```
  restartPolicy:
    type: Never
  volumes:
    - name: "test-volume"
      hostPath:
        path: "/tmp"
        type: Directory
  driver:
    cores: 1
    coreLimit: "1200m"
    memory: "512m"
    annotations:
       emr-containers.amazonaws.com/dynamic.sizing.signature: "my-signature"
    labels:
       emr-containers.amazonaws.com/dynamic.sizing: "true"
       version: 3.3.1
    serviceAccount: emr-containers-sa-spark
    volumeMounts:
       - name: "test-volume"
         mountPath: "/tmp"
  executor:
    cores: 1
    instances: 1
    memory: "512m"
    labels:
      emr-containers.amazonaws.com/dynamic.sizing.signature: "my-signature"
      version: 3.3.1
    volumeMounts:
      - name: "test-volume"
        mountPath: "/tmp"
    env:
      - name: "DYNAMIC_SIZING_ENABLED"
        value: "true" # true, not set otherwise
      - name: "EXEC_POD_CPU_REQUEST"
        valueFrom:
          resourceFieldRef:
            containerName: "spark-kubernetes-executor"
            resource: "requests.cpu"
            divisor: "1"
      - name: "EXEC_POD_CPU_LIMIT"
        valueFrom:
          resourceFieldRef:
            containerName: "spark-kubernetes-executor"
            resource: "limits.cpu"
```

```
            divisor: "1"
      - name: "EXEC_POD_MEM_REQUEST"
        valueFrom:
          resourceFieldRef:
            containerName: "spark-kubernetes-executor"
            resource: "requests.memory"
            divisor: "1"
      - name: "EXEC_POD_MEM_LIMIT"
        valueFrom:
          resourceFieldRef:
            containerName: "spark-kubernetes-executor"
            resource: "limits.memory"
            divisor: "1"
```

Sekarang, kirimkan aplikasi Spark dengan perintah berikut. Ini juga akan membuat `SparkApplication` objek bernama`spark-pi`:

```
kubectl apply -f spark-pi.yaml
```

Untuk informasi selengkapnya tentang mengirimkan aplikasi ke Spark melalui operator Spark, lihat Menggunakan a `SparkApplication` dalam dokumentasi pada. `spark-on-k8s-operator` GitHub

Memverifikasi fungsionalitas penskalaan otomatis vertikal

Untuk memverifikasi bahwa penskalaan otomatis vertikal berfungsi dengan benar untuk pekerjaan yang dikirimkan, gunakan kubectl untuk mendapatkan sumber daya `verticalpodautoscaler` kustom dan melihat rekomendasi penskalaan Anda.

```
kubectl get verticalpodautoscalers --all-namespaces \
-l=emr-containers.amazonaws.com/dynamic.sizing.signature=my-signature
```

Output dari kueri ini harus menyerupai yang berikut:

```
NAMESPACE        NAME                                                        MODE
 CPU    MEM         PROVIDED   AGE
spark-operator   ds-p73j6mkosvc4xeb3gr7x4xol2bfcw5evqimzqojrlysvj3giozuq-vpa   Off
     580026651   True       15m
```

Jika output Anda tidak terlihat serupa atau berisi kode kesalahan, lihat langkah-langkah Memecahkan masalah Amazon EMR pada penskalaan otomatis vertikal EKS untuk membantu menyelesaikan masalah.

Menghapus instalasi operator Spark untuk Amazon EMR di EKS

Gunakan langkah-langkah berikut untuk menghapus instalan operator Spark.

1. Hapus operator Spark menggunakan namespace yang benar. Untuk contoh ini, namespace adalah. `spark-operator-demo`

```
helm uninstall spark-operator-demo -n spark-operator
```

2. Hapus akun layanan operator Spark:

```
kubectl delete sa emr-containers-sa-spark-operator -n spark-operator
```

3. Hapus operator Spark `CustomResourceDefinitions` (CRD):

```
kubectl delete crd sparkapplications.sparkoperator.k8s.io
kubectl delete crd scheduledsparkapplications.sparkoperator.k8s.io
```

Keamanan dan operator Spark dengan Amazon EMR di EKS

Topik

- Menyiapkan izin akses cluster dengan kontrol akses berbasis peran (RBAC)
- Menyiapkan izin akses klaster dengan peran IAM untuk akun layanan (IRSA)

Menyiapkan izin akses cluster dengan kontrol akses berbasis peran (RBAC)

Untuk menyebarkan operator Spark, Amazon EMR di EKS membuat dua peran dan akun layanan untuk operator Spark dan aplikasi Spark.

Topik

- Akun dan peran layanan operator
- Akun dan peran layanan Spark

Akun dan peran layanan operator

Amazon EMR di EKS membuat akun layanan operator dan peran `SparkApplications` untuk mengelola pekerjaan Spark dan sumber daya lain seperti layanan.

Nama default untuk akun layanan ini adalah`emr-containers-sa-spark-operator`.

Aturan berikut berlaku untuk peran layanan ini:

```
 rules:
- apiGroups:
  - ""
  resources:
  - pods
  verbs:
  - "*"
- apiGroups:
  - ""
  resources:
  - services
  - configmaps
  - secrets
  verbs:
  - create
  - get
  - delete
  - update
- apiGroups:
  - extensions
  - networking.k8s.io
  resources:
  - ingresses
  verbs:
  - create
  - get
  - delete
- apiGroups:
  - ""
  resources:
  - nodes
  verbs:
  - get
- apiGroups:
  - ""
```

```
  resources:
  - events
  verbs:
  - create
  - update
  - patch
- apiGroups:
  - ""
  resources:
  - resourcequotas
  verbs:
  - get
  - list
  - watch
- apiGroups:
  - apiextensions.k8s.io
  resources:
  - customresourcedefinitions
  verbs:
  - create
  - get
  - update
  - delete
- apiGroups:
  - admissionregistration.k8s.io
  resources:
  - mutatingwebhookconfigurations
  - validatingwebhookconfigurations
  verbs:
  - create
  - get
  - update
  - delete
- apiGroups:
  - sparkoperator.k8s.io
  resources:
  - sparkapplications
  - sparkapplications/status
  - scheduledsparkapplications
  - scheduledsparkapplications/status
  verbs:
  - "*"
  {{- if .Values.batchScheduler.enable }}
  # required for the `volcano` batch scheduler
```

```
- apiGroups:
  - scheduling.incubator.k8s.io
  - scheduling.sigs.dev
  - scheduling.volcano.sh
  resources:
  - podgroups
  verbs:
  - "*"
  {{- end }}
  {{ if .Values.webhook.enable }}
- apiGroups:
  - batch
  resources:
  - jobs
  verbs:
  - delete
  {{- end }}
```

Akun dan peran layanan Spark

Pod driver Spark membutuhkan akun layanan Kubernetes di namespace yang sama dengan pod. Akun layanan ini membutuhkan izin untuk membuat, mendapatkan, membuat daftar, menambal, dan menghapus pod pelaksana, dan untuk membuat layanan tanpa kepala Kubernetes untuk driver. Driver gagal dan keluar tanpa akun layanan kecuali akun layanan default di namespace pod memiliki izin yang diperlukan.

Nama default untuk akun layanan ini adalah`emr-containers-sa-spark`.

Aturan berikut berlaku untuk peran layanan ini:

```
 rules:
- apiGroups:
  - ""
  resources:
  - pods
  verbs:
  - "*"
- apiGroups:
  - ""
  resources:
  - services
  verbs:
  - "*"
```

```
- apiGroups:
  - ""
  resources:
  - configmaps
  verbs:
  - "*"
- apiGroups:
  - ""
  resources:
  - persistentvolumeclaims
  verbs:
  - "*"
```

Menyiapkan izin akses klaster dengan peran IAM untuk akun layanan (IRSA)

Bagian ini menggunakan contoh untuk menunjukkan cara mengonfigurasi akun layanan Kubernetes untuk mengambil peran. AWS Identity and Access Management Pod yang menggunakan akun layanan kemudian dapat mengakses AWS layanan apa pun yang perannya memiliki izin untuk diakses.

Contoh berikut menjalankan aplikasi Spark untuk menghitung kata-kata dari file di Amazon S3. Untuk melakukan ini, Anda dapat mengatur peran IAM untuk akun layanan (IRSA) untuk mengautentikasi dan mengotorisasi akun layanan Kubernetes.

> **Note**
>
> Contoh ini menggunakan namespace “spark-operator” untuk operator Spark dan untuk namespace tempat Anda mengirimkan aplikasi Spark.

Prasyarat

Sebelum Anda mencoba contoh di halaman ini, lengkapi prasyarat berikut:

- Siapkan untuk operator Spark.
- Instal operator Spark.
- Buat bucket Amazon S3.
- Simpan puisi favorit Anda dalam file teks bernama`poem.txt`, dan unggah file ke bucket S3 Anda. Aplikasi Spark yang Anda buat di halaman ini akan membaca isi file teks. Untuk informasi

selengkapnya tentang mengunggah file ke S3, lihat Mengunggah objek ke bucket di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Konfigurasikan akun layanan Kubernetes untuk mengambil peran IAM

Gunakan langkah-langkah berikut untuk mengonfigurasi akun layanan Kubernetes untuk mengambil peran IAM yang dapat digunakan pod untuk mengakses AWS layanan yang memiliki izin untuk diakses oleh peran tersebut.

1. Setelah menyelesaikanPrasyarat, gunakan AWS Command Line Interface untuk membuat `example-policy.json` file yang memungkinkan akses hanya-baca ke file yang Anda unggah ke Amazon S3:

```
cat >example-policy.json <<EOF
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::my-pod-bucket",
                "arn:aws:s3:::my-pod-bucket/*"
            ]
        }
    ]
}
EOF
```

2. Kemudian, buat kebijakan `example-policy` IAM:

```
aws iam create-policy --policy-name example-policy --policy-document file://
example-policy.json
```

3. Selanjutnya, buat peran IAM `example-role` dan kaitkan dengan akun layanan Kubernetes untuk driver Spark:

```
eksctl create iamserviceaccount --name driver-account-sa --namespace spark-operator
 \
--cluster my-cluster --role-name "example-role" \
--attach-policy-arn arn:aws:iam::111122223333:policy/example-policy --approve
```

4. Buat file yaml dengan binding peran cluster yang diperlukan untuk akun layanan driver Spark:

```
cat >spark-rbac.yaml <<EOF
apiVersion: v1
kind: ServiceAccount
metadata:
  name: driver-account-sa
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: spark-role
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: edit
subjects:
  - kind: ServiceAccount
    name: driver-account-sa
    namespace: spark-operator
EOF
```

5. Menerapkan konfigurasi pengikatan peran cluster:

```
kubectl apply -f spark-rbac.yaml
```

Perintah kubectl harus mengonfirmasi keberhasilan pembuatan akun:

```
serviceaccount/driver-account-sa created
clusterrolebinding.rbac.authorization.k8s.io/spark-role configured
```

Menjalankan aplikasi dari operator Spark

Setelah Anda mengkonfigurasi akun layanan Kubernetes, Anda dapat menjalankan aplikasi Spark yang menghitung jumlah kata dalam file teks yang Anda unggah sebagai bagian dari. Prasyarat

1. Buat file baru`word-count.yaml`, dengan `SparkApplication` definisi untuk aplikasi penghitungan kata Anda.

```
cat >word-count.yaml <<EOF
apiVersion: "sparkoperator.k8s.io/v1beta2"
kind: SparkApplication
metadata:
  name: word-count
  namespace: spark-operator
spec:
  type: Java
  mode: cluster
  image: "895885662937.dkr.ecr.us-west-2.amazonaws.com/spark/emr-6.10.0:latest"
  imagePullPolicy: Always
  mainClass: org.apache.spark.examples.JavaWordCount
  mainApplicationFile: local:///usr/lib/spark/examples/jars/spark-examples.jar
  arguments:
    - s3://my-pod-bucket/poem.txt
  hadoopConf:
   # EMRFS filesystem
    fs.s3.customAWSCredentialsProvider:
 com.amazonaws.auth.WebIdentityTokenCredentialsProvider
    fs.s3.impl: com.amazon.ws.emr.hadoop.fs.EmrFileSystem
    fs.AbstractFileSystem.s3.impl: org.apache.hadoop.fs.s3.EMRFSDelegate
    fs.s3.buffer.dir: /mnt/s3
    fs.s3.getObject.initialSocketTimeoutMilliseconds: "2000"

 mapreduce.fileoutputcommitter.algorithm.version.emr_internal_use_only.EmrFileSystem:
 "2"
    mapreduce.fileoutputcommitter.cleanup-
failures.ignored.emr_internal_use_only.EmrFileSystem: "true"
  sparkConf:
    # Required for EMR Runtime
    spark.driver.extraClassPath: /usr/lib/hadoop-lzo/lib/*:/usr/lib/hadoop/
hadoop-aws.jar:/usr/share/aws/aws-java-sdk/*:/usr/share/aws/emr/emrfs/conf:/usr/
share/aws/emr/emrfs/lib/*:/usr/share/aws/emr/emrfs/auxlib/*:/usr/share/aws/emr/
security/conf:/usr/share/aws/emr/security/lib/*:/usr/share/aws/hmclient/lib/aws-
glue-datacatalog-spark-client.jar:/usr/share/java/Hive-JSON-Serde/hive-openx-
serde.jar:/usr/share/aws/sagemaker-spark-sdk/lib/sagemaker-spark-sdk.jar:/home/
hadoop/extrajars/*
    spark.driver.extraLibraryPath: /usr/lib/hadoop/lib/native:/usr/lib/hadoop-lzo/
lib/native:/docker/usr/lib/hadoop/lib/native:/docker/usr/lib/hadoop-lzo/lib/native
```

```
    spark.executor.extraClassPath: /usr/lib/hadoop-lzo/lib/*:/usr/lib/hadoop/
hadoop-aws.jar:/usr/share/aws/aws-java-sdk/*:/usr/share/aws/emr/emrfs/conf:/usr/
share/aws/emr/emrfs/lib/*:/usr/share/aws/emr/emrfs/auxlib/*:/usr/share/aws/emr/
security/conf:/usr/share/aws/emr/security/lib/*:/usr/share/aws/hmclient/lib/aws-
glue-datacatalog-spark-client.jar:/usr/share/java/Hive-JSON-Serde/hive-openx-
serde.jar:/usr/share/aws/sagemaker-spark-sdk/lib/sagemaker-spark-sdk.jar:/home/
hadoop/extrajars/*
    spark.executor.extraLibraryPath: /usr/lib/hadoop/lib/native:/usr/lib/hadoop-
lzo/lib/native:/docker/usr/lib/hadoop/lib/native:/docker/usr/lib/hadoop-lzo/lib/
native
  sparkVersion: "3.3.1"
  restartPolicy:
    type: Never
  driver:
    cores: 1
    coreLimit: "1200m"
    memory: "512m"
    labels:
      version: 3.3.1
    serviceAccount: my-spark-driver-sa
  executor:
    cores: 1
    instances: 1
    memory: "512m"
    labels:
      version: 3.3.1
EOF
```

2. Kirim aplikasi Spark.

```
kubectl apply -f word-count.yaml
```

Perintah kubectl harus mengembalikan konfirmasi bahwa Anda berhasil membuat objek yang `SparkApplication` dipanggil. `word-count`

```
sparkapplication.sparkoperator.k8s.io/word-count configured
```

3. Untuk memeriksa peristiwa untuk `SparkApplication` objek, jalankan perintah berikut:

```
kubectl describe sparkapplication word-count -n spark-operator
```

Perintah kubectl harus mengembalikan deskripsi `SparkApplication` dengan peristiwa:

```
Events:
  Type     Reason                                Age                    From
    Message
  ----     ------                                ----                   ----
    -------
  Normal   SparkApplicationSpecUpdateProcessed  3m2s (x2 over 17h)     spark-
operator  Successfully processed spec update for SparkApplication word-count
  Warning  SparkApplicationPendingRerun         3m2s (x2 over 17h)     spark-
operator  SparkApplication word-count is pending rerun
  Normal   SparkApplicationSubmitted            2m58s (x2 over 17h)    spark-
operator  SparkApplication word-count was submitted successfully
  Normal   SparkDriverRunning                   2m56s (x2 over 17h)    spark-
operator  Driver word-count-driver is running
  Normal   SparkExecutorPending                 2m50s                  spark-
operator  Executor [javawordcount-fdd1698807392c66-exec-1] is pending
  Normal   SparkExecutorRunning                 2m48s                  spark-
operator  Executor [javawordcount-fdd1698807392c66-exec-1] is running
  Normal   SparkDriverCompleted                2m31s (x2 over 17h)    spark-
operator  Driver word-count-driver completed
  Normal   SparkApplicationCompleted            2m31s (x2 over 17h)    spark-
operator  SparkApplication word-count completed
  Normal   SparkExecutorCompleted               2m31s (x2 over 2m31s)  spark-
operator  Executor [javawordcount-fdd1698807392c66-exec-1] completed
```

Aplikasi ini sekarang menghitung kata-kata dalam file S3 Anda. Untuk menemukan jumlah kata, lihat file log untuk driver Anda:

```
kubectl logs pod/word-count-driver -n spark-operator
```

Perintah kubectl harus mengembalikan isi file log dengan hasil aplikasi hitungan kata Anda.

```
INFO DAGScheduler: Job 0 finished: collect at JavaWordCount.java:53, took 5.146519 s
               Software: 1
```

Untuk informasi selengkapnya tentang cara mengirimkan aplikasi ke Spark melalui operator Spark, lihat dokumentasi Using a SparkApplication in the Kubernetes Operator for Apache Spark (8s-operator). spark-on-k GitHub

Menjalankan pekerjaan Spark dengan spark-submit

Amazon EMR merilis 6.10.0 dan dukungan yang lebih tinggi `spark-submit` sebagai alat baris perintah yang dapat Anda gunakan untuk mengirimkan dan menjalankan aplikasi Spark ke EMR Amazon di kluster EKS.

> **Note**
>
> Amazon EMR menghitung harga di Amazon EKS berdasarkan vCPU dan sumber daya memori yang Anda gunakan dari pod operator sejak Anda mulai mengunduh gambar aplikasi Amazon EMR hingga pod Amazon EKS berakhir, dibulatkan ke detik terdekat.

Topik

Menyiapkan spark-submit untuk Amazon EMR di EKS

Selesaikan tugas-tugas berikut untuk menyiapkan sebelum Anda dapat menjalankan aplikasi dengan spark-submit di Amazon EMR di EKS. Jika Anda sudah mendaftar untuk Amazon Web Services (AWS) dan telah menggunakan Amazon EKS, Anda hampir siap untuk menggunakan Amazon EMR di EKS. Jika Anda telah menyelesaikan salah satu prasyarat, Anda dapat melewatinya dan melanjutkan ke yang berikutnya.

- Instal AWS CLI— Jika Anda sudah menginstalAWS CLI, konfirmasikan bahwa Anda memiliki versi terbaru.
- Instal eksctl - eksctl adalah alat baris perintah yang Anda gunakan untuk berkomunikasi dengan Amazon EKS.
- Siapkan cluster Amazon EKS — Ikuti langkah-langkah untuk membuat cluster Kubernetes baru dengan node di Amazon EKS.
- Pilih URI gambar dasar EMR Amazon (rilis 6.10.0 atau lebih tinggi) — `spark-submit` perintah ini didukung dengan rilis Amazon EMR 6.10.0 dan yang lebih tinggi.

- Konfirmasikan bahwa akun layanan driver memiliki izin yang sesuai untuk membuat dan menonton pod pelaksana. Untuk informasi selengkapnya, lihat Persyaratan keamanan akun layanan driver Spark untuk pengiriman spark.
- Siapkan profil AWSkredensial lokal Anda.
- Dapatkan titik akhir cluster Amazon EKS.

Memulai dengan spark-submit untuk Amazon EMR di EKS

Jalankan aplikasi Spark

Amazon EMR 6.10.0 dan yang lebih tinggi mendukung spark-submit untuk menjalankan aplikasi Spark di cluster Amazon EKS. Untuk menjalankan aplikasi Spark, ikuti langkah-langkah berikut:

1. Sebelum Anda dapat menjalankan aplikasi Spark dengan `spark-submit` perintah, selesaikan langkah-langkahnya. Menyiapkan spark-submit untuk Amazon EMR di EKS
2. Tetapkan nilai untuk variabel lingkungan berikut:

```
export SPARK_HOME=spark-home
export MASTER_URL=k8s://Amazon EKS-cluster-endpoint
```

3. Sekarang, kirimkan aplikasi Spark dengan perintah berikut:

```
$SPARK_HOME/bin/spark-submit \
 --class org.apache.spark.examples.SparkPi \
 --master $MASTER_URL \
 --conf spark.kubernetes.container.image=895885662937.dkr.ecr.us-
west-2.amazonaws.com/spark/emr-6.10.0:latest \
 --conf spark.kubernetes.authenticate.driver.serviceAccountName=spark \
 --deploy-mode cluster \
 --conf spark.kubernetes.namespace=spark-operator \
 local:///usr/lib/spark/examples/jars/spark-examples.jar 20
```

Untuk informasi selengkapnya tentang mengirimkan aplikasi ke Spark, lihat Mengirimkan aplikasi dalam dokumentasi Apache Spark.

> **Important**
>
> `spark-submit`hanya mendukung mode cluster sebagai mekanisme pengiriman.

Persyaratan keamanan akun layanan driver Spark untuk pengiriman spark

Pod driver Spark menggunakan akun layanan Kubernetes untuk mengakses server API Kubernetes untuk membuat dan menonton pod pelaksana. Akun layanan driver harus memiliki izin yang sesuai untuk membuat daftar, membuat, mengedit, menambal, dan menghapus pod di klaster Anda. Anda dapat memverifikasi bahwa Anda dapat mencantumkan sumber daya ini dengan menjalankan perintah berikut:

```
kubectl auth can-i list|create|edit|delete|patch pods
```

Aturan berikut berlaku untuk peran layanan ini:

```
 rules:
- apiGroups:
  - ""
  resources:
  - pods
  verbs:
  - "*"
- apiGroups:
  - ""
  resources:
  - services
  verbs:
  - "*"
- apiGroups:
  - ""
  resources:
  - configmaps
  verbs:
  - "*"
- apiGroups:
  - ""
  resources:
  - persistentvolumeclaims
  verbs:
```

```
  - "*"
```

Mengelola Amazon EMR pada pekerjaan EKS

Bagian berikut mencakup topik yang membantu Anda mengelola Amazon EMR Anda di EKS pekerjaan berjalan.

Topik

Mengelola pekerjaan berjalan denganAWS CLI

Halaman ini mencakup cara mengelola pekerjaan berjalan denganAWS Command Line Interface(AWS CLI).

Pilihan untuk mengonfigurasi tugas berjalan

Gunakan opsi berikut untuk mengonfigurasi parameter tugas berjalan:

- `--execution-role-arn`: Anda harus menyediakan IAM role yang digunakan untuk menjalankan tugas. Untuk informasi selengkapnya, lihat Menggunakan peran eksekusi tugas dengan Amazon EMR di EKS.
- `--release-label`: Anda dapat menyebarkan Amazon EMR di EKS dengan Amazon EMR versi 5.32.0 dan 6.2.0 dan lebih baru. Amazon EMR di EKS tidak didukung dalam versi rilis Amazon EMR sebelumnya. Untuk informasi selengkapnya, lihat Amazon EMR pada rilis EKS.
- `--job-driver`: Driver tugas digunakan untuk memberikan input pada tugas utama. Ini adalah bidang jenis serikat di mana Anda hanya dapat meloloskan salah satu nilai untuk jenis tugas yang ingin Anda jalankan. Jenis tugas yang didukung meliputi:
  - Tugas Spark submit - Digunakan untuk menjalankan perintah melalui Spark submit. Anda dapat menggunakan jenis pekerjaan ini untuk menjalankan Scala,PySpark, SparKr, SparkSQL dan pekerjaan lain yang didukung melalui Spark Submit. Tugas ini memiliki parameter berikut:

    - Entrypoint - Ini adalah referensi HCFS (Hadoop sistem file yang kompatibel) ke file jar/py file utama yang ingin Anda jalankan.
    - EntryPointArguments- Ini adalah array argumen yang ingin Anda sampaikan ke file jar/py utama Anda. Anda harus menangani membaca parameter ini menggunakan kode entrypoint Anda. Setiap argumen dalam array harus dipisahkan dengan koma. EntryPointArgumentstidak dapat berisi tanda kurung atau tanda kurung, seperti (), {}, atau [].
    - SparkSubmitParameters- Ini adalah parameter percikan tambahan yang ingin Anda kirim ke pekerjaan. Gunakan parameter ini untuk menimpa properti default Spark seperti memori driver atau jumlah pelaksana seperti —conf atau —class. Untuk informasi tambahan, lihat Peluncuran Aplikasi dengan spark-submit.
  - Spark SQL jobs - Digunakan untuk menjalankan file query SQL melalui Spark SQL. Anda dapat menggunakan jenis pekerjaan ini untuk menjalankan pekerjaan SparkSQL. Tugas ini memiliki parameter berikut:
    - Entrypoint - ini adalah HCFS (Hadoop sistem file yang kompatibel) referensi ke file query SQL Anda ingin menjalankan.

      Untuk daftar parameter Spark tambahan yang dapat Anda gunakan untuk pekerjaan Spark SQL, lihatMenjalankan skrip Spark SQL melaluiStartJobRunAPI.
- `--configuration-overrides`: Anda dapat menimpa konfigurasi default untuk aplikasi dengan menyediakan objek konfigurasi. Anda dapat menggunakan sintaks singkatan untuk menyediakan konfigurasi atau Anda dapat mereferensikan objek konfigurasi dalam file JSON. Objek konfigurasi terdiri dari klasifikasi, properti, dan konfigurasi bersarang opsional. Properti terdiri dari pengaturan yang ingin Anda timpa dalam file tersebut. Anda dapat menentukan beberapa klasifikasi untuk beberapa aplikasi dalam objek JSON tunggal. Klasifikasi konfigurasi yang tersedia bervariasi berdasarkan versi rilis Amazon EMR. Untuk daftar klasifikasi konfigurasi yang tersedia untuk setiap versi rilis Amazon EMR, lihat Amazon EMR pada rilis EKS.

  Jika Anda melewati konfigurasi yang sama dalam penimpaan aplikasi dan di parameter kirim Spark, parameter kirim Spark diutamakan. Daftar prioritas konfigurasi lengkap mengikuti, dalam urutan prioritas tertinggi ke prioritas terendah.
  - Konfigurasi disediakan saat membuat `SparkSession`.
  - Konfigurasi disediakan sebagai bagian dari `sparkSubmitParameters` menggunakan `–conf`.
  - Konfigurasi disediakan sebagai bagian dari penimpaan aplikasi.
  - Konfigurasi yang dioptimalkan dipilih oleh Amazon EMR untuk rilisan.
  - Konfigurasi sumber terbuka default untuk aplikasi.

Untuk memantau pekerjaan yang berjalan menggunakan AmazonCloudWatchatau Amazon S3, Anda harus memberikan detail konfigurasi untukCloudWatch. Untuk informasi selengkapnya, lihat Mengonfigurasi pekerjaan yang dijalankan untuk menggunakan log Amazon S3 dan Mengonfigurasi pekerjaan yang dijalankan untuk menggunakan AmazonCloudWatchLog. Jika ember S3 atauCloudWatchgrup log tidak ada, lalu Amazon EMR membuatnya sebelum mengunggah log ke bucket.

- Untuk daftar tambahan opsi konfigurasi Kubernetes, lihat Properti Spark di Kubernetes.

  Konfigurasi Spark berikut tidak didukung.

  - `spark.kubernetes.authenticate.driver.serviceAccountName`
  - `spark.kubernetes.authenticate.executor.serviceAccountName`
  - `spark.kubernetes.namespace`
  - `spark.kubernetes.driver.pod.name`
  - `spark.kubernetes.container.image.pullPolicy`
  - `spark.kubernetes.container.image`

  > **Note**
  >
  > Anda dapat menggunakan`spark.kubernetes.container.image`untuk gambar Docker yang disesuaikan. Untuk informasi selengkapnya, lihat Menyesuaikan gambar Docker untuk Amazon EMR di EKS.

Mengonfigurasi pekerjaan yang dijalankan untuk menggunakan log Amazon S3

Untuk dapat memantau kemajuan pekerjaan dan memecahkan masalah kegagalan, Anda harus mengkonfigurasi pekerjaan Anda untuk mengirim informasi log ke Amazon S3, AmazonCloudWatchLog, atau keduanya. Topik ini membantu Anda memulai penerbitan log aplikasi ke Amazon S3 pada pekerjaan Anda yang diluncurkan dengan Amazon EMR di EKS.

S3 log kebijakan IAM

Sebelum tugas Anda dapat mengirim data log ke Amazon S3, izin berikut harus disertakan dalam kebijakan perizinan untuk peran eksekusi tugas. Ganti*DOC-CONTOH-EMBER-LOGGING*dengan nama bucket logging Anda.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET-LOGGING",
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET-LOGGING/*",
            ]
        }
    ]
}
```

> **Note**
>
> Amazon EMR di EKS juga dapat membuat bucket Amazon S3. Jika bucket Amazon S3 tidak tersedia, sertakan`"s3:CreateBucket"`izin dalam kebijakan IAM.

Setelah Anda memberikan peran eksekusi izin yang tepat untuk mengirim log ke Amazon S3, data log Anda akan dikirim ke lokasi Amazon S3 berikut saats3MonitoringConfigurationdilewatkan dimonitoringConfigurationbagian daristart-job-runpermintaan, seperti yang ditunjukkan padaMengelola pekerjaan berjalan denganAWS CLI.

- Log Pengontrol -/*LogURI*/*virtual-cluster-id*/pekerjaan/*id pekerjaan*/wadah/*nama pod*/ (stderr.gz/stdout.gz)
- Log Pengemudi -/*LogURI*/*virtual-cluster-id*/pekerjaan/*id pekerjaan*/wadah/*spark-application-id*/percikan api -*id pekerjaan*-driver/ (stderr.gz/stdout.gz)
- Log Pelaksana -/*LogURI*/*virtual-cluster-id*/pekerjaan/*id pekerjaan*/wadah/*spark-application-id*/*executor-pod-name*/(stderr.gz/stdout.gz)

Mengonfigurasi pekerjaan yang dijalankan untuk menggunakan AmazonCloudWatchLog

Untuk memantau kemajuan pekerjaan dan memecahkan masalah kegagalan, Anda harus mengonfigurasi pekerjaan Anda untuk mengirim informasi log ke Amazon S3, AmazonCloudWatchLog, atau keduanya. Topik ini membantu Anda mulai menggunakanCloudWatchLog pada pekerjaan Anda yang diluncurkan dengan Amazon EMR di EKS. Untuk informasi lebih lanjut tentangCloudWatchLog, lihatMemantau File Logdi AmazonCloudWatchPanduan Pengguna.

CloudWatchLog kebijakan IAM

Agar pekerjaan Anda dapat mengirim data log keCloudWatchLog, izin berikut harus disertakan dalam kebijakan izin untuk peran eksekusi pekerjaan. Ganti*my_log_group_name*dan*my_log_stream_prefiks*dengan nama-namaCloudWatchlog kelompok dan log nama aliran, masing-masing. Amazon EMR di EKS menciptakan grup log dan stream log jika mereka tidak ada selama peran eksekusi ARN memiliki izin yang sesuai.

```
{
     "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:DescribeLogGroups",
                "logs:DescribeLogStreams"
            ],
            "Resource": [
                "arn:aws:logs:*:*:*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:my_log_group_name:log-
stream:my_log_stream_prefix/*"
            ]
        }
```

```
    ]
}
```

> **Note**
>
> Amazon EMR di EKS juga dapat membuat aliran log. Jika aliran log tidak ada, kebijakan IAM harus menyertakan`"logs:CreateLogGroup"`izin.

Setelah Anda memberikan peran eksekusi izin yang tepat, aplikasi Anda akan mengirimkan data lognya keCloudWatchLog saat`cloudWatchMonitoringConfiguration`dilewatkan di`monitoringConfiguration`bagian dari`start-job-run`permintaan, seperti yang ditunjukkan padaMengelola pekerjaan berjalan denganAWS CLI.

Dalam`StartJobRun`API,*`log_group_name`*adalah nama grup log untukCloudWatch, dan*`log_stream_prefiks`*adalah awalan nama aliran log untukCloudWatch. Anda dapat melihat dan mencari log ini di AWS Management Console.

- Log pengontrol -*`LogGroup`*/*`logStreamPrefix`*/*`virtual-cluster-id`*/pekerjaan/*`id pekerjaan`*/wadah/*`nama pod`*/(stderr/stdout)
- Log driver -*`LogGroup`*/*`logStreamPrefix`*/*`virtual-cluster-id`*/pekerjaan/*`id pekerjaan`*/wadah/*`spark-application-id`*/percikan api -*`id pekerjaan`*-driver/ (stderrstdout)
- Log pelaksana -*`LogGroup`*/*`logStreamPrefix`*/*`virtual-cluster-id`*/pekerjaan/*`id pekerjaan`*/wadah/*`spark-application-id`*/*`executor-pod-name`*/(stderr/stdout)

Daftar tugas berjalan

Anda dapat menjalankan `list-job-run` untuk menunjukkan keadaan tugas berjalan, seperti yang ditunjukkan contoh berikut.

```
aws emr-containers list-job-runs --virtual-cluster-id <cluster-id>
```

Jelaskan tugas berjalan

Anda dapat menjalankan `describe-job-run` untuk mendapatkan detail lebih lanjut tentang tugas, seperti status tugas, detail tugas, dan nama tugas, seperti yang ditunjukkan contoh berikut.

```
aws emr-containers describe-job-run --virtual-cluster-id cluster-id --id job-run-id
```

Membatalkan tugas berjalan

Anda dapat menjalankan `cancel-job-run` untuk membatalkan tugas berjalan, seperti yang ditunjukkan contoh berikut.

```
aws emr-containers cancel-job-run --virtual-cluster-id cluster-id --id job-run-id
```

Menjalankan skrip Spark SQL melaluiStartJobRunAPI

Amazon EMR pada rilis EKS 6.7.0 dan yang lebih tinggi menyertakan driver pekerjaan Spark SQL sehingga Anda dapat menjalankan skrip Spark SQL melalui`StartJobRun`API. Anda dapat menyediakan file entry-point SQL untuk langsung menjalankan kueri Spark SQL di Amazon EMR di EKS dengan`StartJobRun`API, tanpa modifikasi pada skrip SQL Spark yang ada. Tabel berikut mencantumkan parameter Spark yang didukung untuk pekerjaan Spark SQL melaluiStartJobRunAPI.

Anda dapat memilih dari parameter Spark berikut untuk dikirim ke pekerjaan Spark SQL. Gunakan parameter ini untuk mengganti properti Spark default.

Opsi	Deskripsi
--nama NAMA	Nama Aplikasi
-guci	Daftar dipisahkan koma guci untuk disertakan dengan driver dan mengeksekusi classpath.
--paket	Daftar dipisahkan koma koordinat maven guci untuk memasukkan pada driver dan classpaths pelaksana.
--exclude-paket	Daftar grup yang dipisahkan koma: artifactI d, untuk dikecualikan saat menyelesaikan dependensi yang disediakan dalam —packages untuk menghindari konflik ketergant ungan.
--repositori	Daftar dipisahkan koma dari repositori jarak jauh tambahan untuk mencari koordinat maven yang diberikan dengan —packages.

Opsi	Deskripsi
-file FILE	Daftar file yang dipisahkan koma untuk ditempatkan di direktori kerja masing-masing pelaksana.
--conf PROP = NILAI	Properti konfigurasi percikan.
--properti-berkas BERKAS	Path ke file dari mana untuk memuat properti tambahan.
-driver-memori MEM	Memori untuk pengemudi. Default 1024MB.
--driver-java-options	Opsi Java tambahan untuk diteruskan ke pengemudi.
--driver-library-path	Ekstra entri jalur perpustakaan untuk diteruskan ke pengemudi.
--driver-class-path	Entri classpath ekstra untuk diteruskan ke pengemudi.
--executor-memori MEM	Memori per pelaksana. Default 1GB.
-driver-core NUM	Jumlah core yang digunakan oleh pengemudi.
--total-executor-coresNUM	Total core untuk semua pelaksana.
--executor-core NUM	Jumlah core yang digunakan oleh masing-ma sing pelaksana.
-num-pelaksana NUM	Jumlah pelaksana yang akan diluncurkan.
-hivevar <key=nilai>	Substitusi variabel untuk diterapkan pada perintah Hive, misalnya,`-hivevar A=B`
-hiveconf <properti = nilai>	Nilai yang digunakan untuk properti yang diberikan.

Untuk pekerjaan Spark SQL, buatstart-job-run-request.json mengajukan dan menentukan parameter yang diperlukan untuk menjalankan pekerjaan Anda, seperti dalam contoh berikut:

```
{
  "name": "myjob",
  "virtualClusterId": "123456",
  "executionRoleArn": "iam_role_name_for_job_execution",
  "releaseLabel": "emr-6.7.0-latest",
  "jobDriver": {
    "sparkSqlJobDriver": {
      "entryPoint": "entryPoint_location",
       "sparkSqlParameters": "--conf spark.executor.instances=2 --conf
 spark.executor.memory=2G --conf spark.executor.cores=2 --conf spark.driver.cores=1"
    }
  },
  "configurationOverrides": {
    "applicationConfiguration": [
      {
        "classification": "spark-defaults",
        "properties": {
          "spark.driver.memory":"2G"
         }
      }
    ],
    "monitoringConfiguration": {
      "persistentAppUI": "ENABLED",
      "cloudWatchMonitoringConfiguration": {
        "logGroupName": "my_log_group",
        "logStreamNamePrefix": "log_stream_prefix"
      },
      "s3MonitoringConfiguration": {
        "logUri": "s3://my_s3_log_location"
      }
    }
  }
}
```

Status tugas berjalan

Ketika Anda mengirimkan tugas berjalan ke antrean tugas Amazon EMR di EKS, tugas berjalan memasuki status `PENDING`. Kemudian melewati status-status berikut sampai berhasil (keluar dengan kode `0`) atau gagal (keluar dengan kode bukan nol).

Tugas berjalan dapat memiliki status berikut:

- `PENDING` - Status tugas awal saat tugas berjalan dikirimkan ke Amazon EMR di EKS. Tugas sedang menunggu untuk dikirimkan ke klaster virtual, dan Amazon EMR di EKS sedang bekerja untuk mengirimkan tugas ini.
- `SUBMITTED` - Tugas berjalan yang telah berhasil dikirimkan ke klaster virtual. Penjadwal klaster kemudian mencoba untuk menjalankan tugas ini di cluster.
- `RUNNING` - Tugas berjalan yang berjalan di klaster virtual. Dalam aplikasi Spark, ini berarti bahwa proses driver Spark ada di status `running`.
- `FAILED` - Tugas berjalan yang gagal untuk dikirimkan ke klaster virtual atau yang gagal diselesaikan. LihatlahStateDetailsdanFailureReasonuntuk menemukan informasi tambahan tentang kegagalan pekerjaan ini.
- `COMPLETED` - Tugas berjalan yang telah berhasil diselesaikan.
- `CANCEL_PENDING` - Tugas berjalan telah diminta untuk pembatalan. Amazon EMR di EKS sedang mencoba untuk membatalkan tugas pada klaster virtual.
- `CANCELLED` - Tugas berjalan yang berhasil dibatalkan.

Melihat tugas di konsol Amazon EMR

Untuk melihat pekerjaan di konsol Amazon EMR, lakukan langkah-langkah berikut.

1. Di menu kiri konsol Amazon EMR, di bawah Amazon EMR di EKS, pilihCluster virtual.
2. Dari daftar cluster virtual, pilih cluster virtual yang ingin Anda lihat pekerjaan.
3. Pada tabel Tugas berjalan, pilih Lihat log untuk melihat detail tugas.

> **Note**
>
> Dukungan untuk pengalaman satu klik diaktifkan secara default. Ini dapat dimatikan dengan mengatur `persistentAppUI` ke `DISABLED` dalam `monitoringConfiguration` selama pengiriman tugas. Untuk informasi selengkapnya, lihat Melihat Antarmuka Pengguna Aplikasi Persisten.

Kesalahan umum saat menjalankan tugas

Kesalahan berikut dapat terjadi ketika Anda menjalankan API `StartJobRun`.

Pesan Kesalahan	Kondisi Kesalahan	Langkah Selanjutnya yang Disarankan
kesalahan: argumen –*argumen* diperlukan	Parameter yang diperlukan hilang.	Tambahkan argumen yang hilang ke permintaan API.
Terjadi galat (AccessDeniedException) saat memanggilStartJobRunoperasi: Pengguna:*ARN*tidak berwenang untuk melakukan: emr-kontainer:StartJobRun	Peran eksekusi hilang.	Lihat Menggunakan Menggunakan peran eksekusi tugas dengan Amazon EMR di EKS.
Terjadi galat (AccessDeniedException) saat memanggilStartJobRunoperasi: Pengguna:*ARN*tidak berwenang untuk melakukan: emr-kontainer:StartJobRun	Pemanggil tidak memiliki izin untuk peran eksekusi [format valid / tidak valid] melalui kunci kondisi.	Lihat Menggunakan peran eksekusi tugas dengan Amazon EMR di EKS.
Terjadi galat (AccessDeniedException) saat memanggilStartJobRunoperasi: Pengguna:*ARN*tidak berwenang untuk melakukan: emr-kontainer:StartJobRun	Pengirim tugas dan Peran eksekusi ARN berasal dari akun yang berbeda.	Pastikan bahwa pengirim tugas dan peran eksekusi ARN adalah dari akun AWS yang sama.
1 kesalahan validasi terdeteksi: Nilai*Peran*di 'executionRoleArn'gagal memenuhi pola ekspresi reguler ARN: ^arn: (aws [a-za-Z0-9-] *) :iam:: (\ d {12})? : (peran ((\ u002f) | (\ u002f [\ u0021-\	Pemanggil memiliki izin untuk peran eksekusi melalui kunci kondisi, tetapi peran tidak memenuhi batasan format ARN.	Berikan peran eksekusi mengikuti format ARN berikut. Lihat Menggunakan peran eksekusi tugas dengan Amazon EMR di EKS.

Pesan Kesalahan	Kondisi Kesalahan	Langkah Selanjutnya yang Disarankan
u007f] +\ u002f)) [\ w+=, .@-] +)		
Terjadi galat (Resource NotFoundException) saat memanggilStartJobR unoperasi: Cluster virtual*ID Klaster Virtual*tidak ada.	ID klaster virtual tidak ditemukan.	Menyediakan klaster virtual ID terdaftar dengan Amazon EMR di EKS.
Terjadi galat (Validati onException) saat memanggil StartJobRunoperasi: Status cluster virtual*negara*tidak valid untuk membuat sumber dayaJobRun.	Klaster virtual tidak siap untuk melaksanakan tugas.	Lihat Status klaster virtual.
Terjadi galat (Resource NotFoundException) saat memanggilStartJobR unOperasi: Rilis*MELEPASKA N* tidak ada.	Rilis yang ditentukan dalam pengiriman tugas tidak benar.	Lihat Amazon EMR pada rilis EKS.

Pesan Kesalahan	Kondisi Kesalahan	Langkah Selanjutnya yang Disarankan
Terjadi galat (AccessDeniedException) saat memanggilStartJobRunoperasi: Pengguna:*ARN*tidak berwenang untuk melakukan: emr-kontainer:StartJobRunpada sumber daya:*ARN*dengan penolakan eksplisit. Terjadi galat (AccessDeniedException) saat memanggilStartJobRunoperasi: Pengguna:*ARN*tidak berwenang untuk melakukan: emr-kontainer:StartJobRunpada sumber daya:*ARN*	Pengguna tidak berwenang untuk meneleponStartJobRun.	Lihat Menggunakan peran eksekusi tugas dengan Amazon EMR di EKS.
Terjadi galat (ValidationException) saat memanggil StartJobRunoperasi: ConfigurationOverrides.MonitoringConfiguration.S3MonitoringConfiguration.logUri gagal memenuhi kendala: %s	Jalur S3 sintaks URI tidak valid.	logURI harus dalam format s3://...

Kesalahan berikut dapat terjadi ketika Anda menjalankan API `DescribeJobRun` sebelum tugas berjalan.

Pesan Kesalahan	Kondisi Kesalahan	Langkah Selanjutnya yang Disarankan
StateDetails:JobRunpengajuan gagal.	Parameter diStartJobRuntidak valid.	Lihat Amazon EMR pada rilis EKS.

Pesan Kesalahan	Kondisi Kesalahan	Langkah Selanjutnya yang Disarankan
Klasifikasi *klasifikasi* tidak didukung. failureReason: VALIDATIO N_ERROR status: GAGAL.		
stateDetails: Klaster *ID Klaster EKS* tidak ada. failureReason: CLUSTER_U NAVAILABLE status: GAGAL	Klaster EKS tidak tersedia.	Periksa apakah klaster EKS ada dan memiliki izin yang tepat. Untuk informasi selengkapnya, lihat Menyiapka n Amazon EMR di EKS.
stateDetails: Klaster *ID Klaster EKS* tidak memiliki izin yang cukup. failureReason: CLUSTER_U NAVAILABLE status: GAGAL	Amazon EMR tidak memiliki izin untuk mengakses klaster EKS.	Verifikasi bahwa izin diatur untuk Amazon EMR pada namespace terdaftar. Untuk informasi selengkapnya, lihat Menyiapkan Amazon EMR di EKS.
stateDetails: Klaster *ID Klaster EKS* saat ini tidak dapat dijangkau. failureReason: CLUSTER_U NAVAILABLE status: GAGAL	Klaster EKS tidak dapat dijangkau.	Periksa apakah Klaster EKS ada dan memiliki izin yang tepat. Untuk informasi selengkapnya, lihat Menyiapka n Amazon EMR di EKS.

Pesan Kesalahan	Kondisi Kesalahan	Langkah Selanjutnya yang Disarankan
StateDetails:JobRunpengajuan gagal karena kesalahan internal. failureReason: INTERNAL_ERROR status: GAGAL	Kesalahan internal telah terjadi dengan klaster EKS.	N/A
stateDetails: Klaster *ID Klaster EKS* tidak memiliki sumber daya yang cukup. failureReason: USER_ERROR status: GAGAL	Ada sumber daya yang tidak mencukupi di klaster EKS untuk menjalankan tugas.	Tambahkan lebih banyak kapasitas ke grup simpul EKS atau atur EKS Autoscaler. Untuk informasi lebih lanjut, lihat Klaster Autoscaler.

Kesalahan berikut dapat terjadi ketika Anda menjalankan API `DescribeJobRun` setelah tugas berjalan.

Pesan Kesalahan	Kondisi Kesalahan	Langkah Selanjutnya yang Disarankan
StateDetails: Kesulitan memonitorJobRun. Klaster *ID Klaster EKS* tidak ada. failureReason: CLUSTER_UNAVAILABLE status: GAGAL	Klaster EKS tidak ada.	Periksa apakah Klaster EKS ada dan memiliki izin yang tepat. Untuk informasi selengkapnya, lihat Menyiapkan Amazon EMR di EKS.

Pesan Kesalahan	Kondisi Kesalahan	Langkah Selanjutnya yang Disarankan
StateDetails: Kesulitan memonitorJobRun. Klaster *ID Klaster EKS* tidak memiliki izin yang cukup. failureReason: CLUSTER_UNAVAILABLE status: GAGAL	Amazon EMR tidak memiliki izin untuk mengakses klaster EKS.	Verifikasi bahwa izin diatur untuk Amazon EMR pada namespace terdaftar. Untuk informasi selengkapnya, lihat Menyiapkan Amazon EMR di EKS.
StateDetails: Kesulitan memonitorJobRun. Klaster *ID Klaster EKS* saat ini tidak dapat dijangkau. failureReason: CLUSTER_UNAVAILABLE status: GAGAL	Klaster EKS tidak dapat dijangkau.	Periksa apakah Klaster EKS ada dan memiliki izin yang tepat. Untuk informasi selengkapnya, lihat Menyiapkan Amazon EMR di EKS.
StateDetails: Kesulitan memonitorJobRunkarena kesalahan internal failureReason: INTERNAL_ERROR status: GAGAL	Kesalahan internal telah terjadi dan mencegahJobRunpemantauan.	T/A

Kesalahan berikut dapat terjadi ketika pekerjaan tidak dapat dimulai dan pekerjaan menunggu dalam keadaan DIKIRIM selama 15 menit. Hal ini dapat disebabkan oleh kurangnya sumber daya cluster.

Pesan Kesalahan	Kondisi Kesalahan	Langkah Selanjutnya yang Disarankan
batas waktu klaster	Pekerjaan telah di negara diserahkan selama 15 menit atau lebih.	Anda dapat mengganti pengaturan default 15 menit untuk parameter ini dengan penggantian konfigurasi yang ditunjukkan di bawah ini.

Gunakan konfigurasi berikut untuk mengubah pengaturan batas waktu klaster menjadi 30 menit. Perhatikan bahwa Anda memberikan yang baru`job-start-timeout`nilai dalam detik:

```
{
"configurationOverrides": {
  "applicationConfiguration": [{
      "classification": "emr-containers-defaults",
      "properties": {
          "job-start-timeout":"1800"
      }
  }]
}
```

Menggunakan klasifikasi pengirim pekerjaan

Gambaran Umum

Amazon EMR di EKS`StartJobRun`permintaan menciptakan*pengirim pekerjaan*pod (juga dikenal sebagai*pekerjaan-pelari*pod) untuk menelurkan driver Spark. Kamu dapat mengonfigurasi selektor node untuk pod submitter pekerjaanmu dengan`emr-job-submitter`klasifikasi.

Pengaturan berikut tersedia di bawah`emr-job-submitter`klasifikasi:

`jobsubmitter.node.selector.[`*`labelKey`*`]`

Menambahkan ke pemilih node dari pod submitter pekerjaan, dengan kunci*`labelKey`*dan nilai sebagai nilai konfigurasi untuk konfigurasi. Misalnya, Anda dapat mengatur`jobsubmitter.node.selector.identifier`kepada`myIdentifier`dan pod

job submitter akan memiliki pemilih node dengan nilai pengenal kuncimy`Identifier`. Untuk menambahkan beberapa kunci pemilih node, atur beberapa konfigurasi dengan awalan ini.

Sebagai praktik terbaik, kami merekomendasikan bahwa pod pengirim pekerjaan memilikipenempatan node pada Instans On Demanddan bukan pada Instans Spot. Hal ini dikarenakan suatu pekerjaan akan gagal jika Pod submitter job mengalami interupsi Spot Instance. Anda juga bisatempatkan pod pengirim pekerjaan dalam satu Availability Zone, ataumenggunakan label Kubernetes yang diterapkan pada node.

Contoh klasifikasi pengirim pekerjaan

Dalam bagian ini

- StartJobRunrequest dengan penempatan Node On-Demand untuk pod job submitter
- StartJobRunrequest dengan penempatan node Single-AZ untuk pod job submitter
- StartJobRunpermintaan dengan penempatan tipe instans Single-AZ dan Amazon EC2 untuk pod pengirim pekerjaan

`StartJobRun`request dengan penempatan Node On-Demand untuk pod job submitter

```
cat >spark-python-in-s3-nodeselector-job-submitter.json << EOF
{
  "name": "spark-python-in-s3-nodeselector",
  "virtualClusterId": "virtual-cluster-id",
  "executionRoleArn": "execution-role-arn",
  "releaseLabel": "emr-6.11.0-latest",
  "jobDriver": {
    "sparkSubmitJobDriver": {
      "entryPoint": "s3://S3-prefix/trip-count.py",
       "sparkSubmitParameters": "--conf spark.driver.cores=5  --conf
 spark.executor.memory=20G --conf spark.driver.memory=15G --conf
 spark.executor.cores=6"
    }
  },
  "configurationOverrides": {
    "applicationConfiguration": [
      {
        "classification": "spark-defaults",
        "properties": {
          "spark.dynamicAllocation.enabled":"false"
```

```
         }
      },
      {
        "classification": "emr-job-submitter",
        "properties": {
            "jobsubmitter.node.selector.eks.amazonaws.com/capacityType": "ON_DEMAND"
        }
      }
    ],
    "monitoringConfiguration": {
      "cloudWatchMonitoringConfiguration": {
        "logGroupName": "/emr-containers/jobs",
        "logStreamNamePrefix": "demo"
      },
      "s3MonitoringConfiguration": {
        "logUri": "s3://joblogs"
      }
    }
  }
}
EOF
aws emr-containers start-job-run --cli-input-json file:///spark-python-in-s3-
nodeselector-job-submitter.json
```

StartJobRunrequest dengan penempatan node Single-AZ untuk pod job submitter

```
cat >spark-python-in-s3-nodeselector-job-submitter-az.json << EOF
{
  "name": "spark-python-in-s3-nodeselector",
  "virtualClusterId": "virtual-cluster-id",
  "executionRoleArn": "execution-role-arn",
  "releaseLabel": "emr-6.11.0-latest",
  "jobDriver": {
    "sparkSubmitJobDriver": {
      "entryPoint": "s3://S3-prefix/trip-count.py",
       "sparkSubmitParameters": "--conf spark.driver.cores=5  --conf
 spark.executor.memory=20G --conf spark.driver.memory=15G --conf
 spark.executor.cores=6"
    }
  },
  "configurationOverrides": {
    "applicationConfiguration": [
      {
```

```
        "classification": "spark-defaults",
        "properties": {
          "spark.dynamicAllocation.enabled":"false"
         }
      },
      {
        "classification": "emr-job-submitter",
        "properties": {
            "jobsubmitter.node.selector.topology.kubernetes.io/zone": "Availability
 Zone"
        }
      }
    ],
    "monitoringConfiguration": {
      "cloudWatchMonitoringConfiguration": {
        "logGroupName": "/emr-containers/jobs",
        "logStreamNamePrefix": "demo"
      },
      "s3MonitoringConfiguration": {
        "logUri": "s3://joblogs"
      }
    }
  }
}
EOF
aws emr-containers start-job-run --cli-input-json file:///spark-python-in-s3-
nodeselector-job-submitter-az.json
```

StartJobRunpermintaan dengan penempatan tipe instans Single-AZ dan Amazon EC2 untuk pod pengirim pekerjaan

```
{
  "name": "spark-python-in-s3-nodeselector",
  "virtualClusterId": "virtual-cluster-id",
  "executionRoleArn": "execution-role-arn",
  "releaseLabel": "emr-6.11.0-latest",
  "jobDriver": {
    "sparkSubmitJobDriver": {
      "entryPoint": "s3://S3-prefix/trip-count.py",
       "sparkSubmitParameters": "--conf spark.driver.cores=5  --conf
 spark.kubernetes.pyspark.pythonVersion=3 --conf spark.executor.memory=20G
 --conf spark.driver.memory=15G --conf spark.executor.cores=6 --conf
 spark.sql.shuffle.partitions=1000"
```

```
    }
  },
  "configurationOverrides": {
    "applicationConfiguration": [
      {
        "classification": "spark-defaults",
        "properties": {
          "spark.dynamicAllocation.enabled":"false",
         }
      },
      {
        "classification": "emr-job-submitter",
        "properties": {
            "jobsubmitter.node.selector.topology.kubernetes.io/zone": "Availability
 Zone",
            "jobsubmitter.node.selector.node.kubernetes.io/instance-type":"m5.4xlarge"
        }
      }
    ],
    "monitoringConfiguration": {
      "cloudWatchMonitoringConfiguration": {
        "logGroupName": "/emr-containers/jobs",
        "logStreamNamePrefix": "demo"
      },
      "s3MonitoringConfiguration": {
        "logUri": "s3://joblogs"
      }
    }
  }
}
```

Menggunakan templat pekerjaan

Template pekerjaan menyimpan nilai yang dapat dibagikan`StartJobRun`Pemanggilan API saat memulai pekerjaan. Ini mendukung dua kasus penggunaan:

- Untuk mencegah berulang berulang`StartJobRun`Nilai permintaan API.
- Untuk menegakkan aturan bahwa nilai-nilai tertentu harus disediakan melalui`StartJobRun`Permintaan API.

Template pekerjaan memungkinkan Anda untuk menentukan template yang dapat digunakan kembali untuk pekerjaan berjalan untuk menerapkan kustomisasi tambahan, misalnya:

- Mengkonfigurasi kapasitas komputasi pelaksana dan driver
- Menetapkan properti keamanan dan tata kelola seperti peran IAM
- Menyesuaikan image buruh pelabuhan untuk digunakan di beberapa aplikasi dan pipeline data

Membuat dan menggunakan template pekerjaan untuk memulai pekerjaan

Bagian ini menjelaskan pembuatan template pekerjaan dan menggunakan template untuk memulai pekerjaan yang dijalankan denganAWS Command Line Interface(AWS CLI).

Untuk membuat template pekerjaan

1. Buat`create-job-template-request.json`file dan menentukan parameter yang diperlukan untuk template pekerjaan Anda, seperti yang ditunjukkan dalam contoh file JSON berikut. Untuk informasi tentang semua parameter yang tersedia, lihatCreateJobTemplateAPI.

   Sebagian besar nilai yang diperlukan untuk`StartJobRun`API juga diperlukan untuk`jobTemplateData`. Jika Anda ingin menggunakan placeholder untuk parameter apa pun dan memberikan nilai saat memohonStartJobRunmenggunakan template pekerjaan, silakan lihat bagian berikutnya pada parameter template pekerjaan.

```
{
   "name": "mytemplate",
   "jobTemplateData": {
        "executionRoleArn": "iam_role_arn_for_job_execution",
        "releaseLabel": "emr-6.7.0-latest",
        "jobDriver": {
            "sparkSubmitJobDriver": {
                "entryPoint": "entryPoint_location",
                "entryPointArguments": [ "argument1","argument2",...],
                "sparkSubmitParameters": "--class <main_class> --conf
 spark.executor.instances=2 --conf spark.executor.memory=2G --conf
 spark.executor.cores=2 --conf spark.driver.cores=1"
            }
       },
       "configurationOverrides": {
            "applicationConfiguration": [
                {
```

```
                    "classification": "spark-defaults",
                    "properties": {
                         "spark.driver.memory":"2G"
                    }
                }
            ],
            "monitoringConfiguration": {
                "persistentAppUI": "ENABLED",
                "cloudWatchMonitoringConfiguration": {
                    "logGroupName": "my_log_group",
                    "logStreamNamePrefix": "log_stream_prefix"
                },
                "s3MonitoringConfiguration": {
                    "logUri": "s3://my_s3_log_location/"
                }
            }
        }
    }
}
```

2. Gunakan`create-job-template`perintah dengan path ke`create-job-template-request.json`file yang disimpan secara lokal.

```
aws emr-containers create-job-template \
--cli-input-json file://./create-job-template-request.json
```

Untuk memulai pekerjaan yang dijalankan menggunakan template pekerjaan

Menyediakan id cluster virtual, id template pekerjaan, dan nama pekerjaan di`StartJobRun`perintah, seperti yang ditunjukkan pada contoh berikut.

```
aws emr-containers start-job-run \
--virtual-cluster-id 123456 \
--name myjob \
--job-template-id 1234abcd
```

Mendefinisikan parameter template pekerjaan

Parameter template pekerjaan memungkinkan Anda untuk menentukan variabel dalam template pekerjaan. Nilai untuk variabel parameter ini perlu ditentukan saat memulai pekerjaan yang dijalankan menggunakan template pekerjaan itu. Parameter template pekerjaan ditentukan

dalam`${parameterName}`format. Anda dapat memilih untuk menentukan nilai apa pun dalam`jobTemplateData`lapangan sebagai parameter template pekerjaan. Untuk masing-masing variabel parameter template pekerjaan, tentukan tipe datanya (`STRING`atau`NUMBER`) dan opsional nilai default. Contoh di bawah ini menunjukkan bagaimana Anda dapat menentukan parameter template pekerjaan untuk lokasi titik masuk, kelas utama, dan nilai lokasi log S3.

Untuk menentukan lokasi titik masuk, kelas utama, dan lokasi log Amazon S3 sebagai parameter template pekerjaan

1. Buat`create-job-template-request.json`file dan menentukan parameter yang diperlukan untuk template pekerjaan Anda, seperti yang ditunjukkan dalam contoh file JSON berikut. Untuk informasi lebih lanjut tentang parameter, lihatCreateJobTemplateAPI.

```
{
   "name": "mytemplate",
   "jobTemplateData": {
        "executionRoleArn": "iam_role_arn_for_job_execution",
        "releaseLabel": "emr-6.7.0-latest",
        "jobDriver": {
            "sparkSubmitJobDriver": {
                "entryPoint": "${EntryPointLocation}",
                "entryPointArguments": [ "argument1","argument2",...],
                "sparkSubmitParameters": "--class ${MainClass} --conf
 spark.executor.instances=2 --conf spark.executor.memory=2G --conf
 spark.executor.cores=2 --conf spark.driver.cores=1"
            }
        },
        "configurationOverrides": {
            "applicationConfiguration": [
                {
                    "classification": "spark-defaults",
                    "properties": {
                         "spark.driver.memory":"2G"
                    }
                }
            ],
            "monitoringConfiguration": {
                "persistentAppUI": "ENABLED",
                "cloudWatchMonitoringConfiguration": {
                    "logGroupName": "my_log_group",
                    "logStreamNamePrefix": "log_stream_prefix"
                },
```

```
                "s3MonitoringConfiguration": {
                    "logUri": "${LogS3BucketUri}"
                }
            }
        },
        "parameterConfiguration": {
            "EntryPointLocation": {
                "type": "STRING"
            },
            "MainClass": {
                "type": "STRING",
                "defaultValue":"Main"
            },
            "LogS3BucketUri": {
                "type": "STRING",
                "defaultValue":"s3://my_s3_log_location/"
            }
        }
    }
}
```

2. Gunakan perintah `create-job-template` dengan jalur ke file `create-job-template-request.json` yang disimpan secara lokal atau di Amazon S3.

```
aws emr-containers create-job-template \
--cli-input-json file://./create-job-template-request.json
```

Untuk memulai menjalankan pekerjaan menggunakan template pekerjaan dengan parameter template pekerjaan

Untuk memulai pekerjaan yang dijalankan dengan template pekerjaan yang berisi parameter template pekerjaan, tentukan id template pekerjaan serta nilai untuk parameter template pekerjaan di`StartJobRun`Permintaan API seperti yang ditunjukkan di bawah ini.

```
aws emr-containers start-job-run \
--virtual-cluster-id 123456 \
--name myjob \
--job-template-id 1234abcd \
--job-template-parameters '{"EntryPointLocation": "entry_point_location","MainClass":
 "ExampleMainClass","LogS3BucketUri": "s3://example_s3_bucket/"}'
```

Mengontrol akses ke templat pekerjaan

`StartJobRun`kebijakan memungkinkan Anda menegakkan bahwa pengguna atau peran hanya dapat menjalankan pekerjaan menggunakan template pekerjaan yang Anda tentukan dan tidak dapat dijalankan`StartJobRun`operasi tanpa menggunakan template pekerjaan yang ditentukan. Untuk mencapai hal ini, pertama pastikan bahwa Anda memberikan pengguna atau peran izin baca untuk template pekerjaan tertentu seperti yang ditunjukkan di bawah ini.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "emr-containers:DescribeJobTemplate",
            "Resource": [
                "job_template_1_arn",
                "job_template_2_arn",
                ...
            ]
        }
    ]
}
```

Untuk menegakkan bahwa pengguna atau peran dapat memohon`StartJobRun`operasi hanya ketika menggunakan template pekerjaan tertentu, Anda dapat menetapkan berikut`StartJobRun`izin kebijakan untuk pengguna atau peran tertentu.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "emr-containers:StartJobRun",
            "Resource": [
                "virtual_cluster_arn",
            ],
            "Condition": [
                "StringEquals": {
                    "emr-containers:JobTemplateArn": [
                        "job_template_1_arn",
                        "job_template_2_arn",
                        ...
```

```
                    ]
                }
                ]
            }
        }
    ]
}
```

Jika template pekerjaan menentukan parameter template pekerjaan di dalam bidang peran eksekusi ARN, maka pengguna akan dapat memberikan nilai untuk parameter ini dan dengan demikian dapat memanggil`StartJobRun`menggunakan peran eksekusi sewenang-wenang. Untuk membatasi peran eksekusi yang dapat diberikan pengguna, lihatMengontrol akses ke peran eksekusidi[Menggunakan peran eksekusi tugas dengan Amazon EMR di EKS](#).

Jika tidak ada kondisi yang ditentukan di atas`StartJobRun`kebijakan tindakan untuk pengguna tertentu atau peran, pengguna atau peran akan diizinkan untuk memohon`StartJobRun`tindakan pada cluster virtual yang ditentukan menggunakan template pekerjaan sewenang-wenang bahwa mereka telah membaca akses ke atau menggunakan peran eksekusi sewenang-wenang.

Menggunakan templat pod

Dimulai dengan Amazon EMR versi 5.33.0 atau 6.3.0, Amazon EMR di EKS mendukung fitur templat pod Spark. Sebuah pod adalah sekelompok satu atau lebih kontainer, dengan penyimpanan bersama dan sumber daya jaringan, dan spesifikasi cara menjalankan kontainer. Templat pod adalah spesifikasi yang menentukan cara menjalankan setiap pod. Anda dapat menggunakan file templat pod untuk menentukan konfigurasi driver atau pelaksana pod yang tidak didukung konfigurasi Spark. Untuk informasi selengkapnya tentang fitur templat pod Spark, lihat Templat Pod.

> **Note**
>
> Fitur templat pod hanya bekerja dengan driver dan pelaksana pod. Anda tidak dapat mengonfigurasi pod pengendali tugas menggunakan templat pod.

Skenario umum

Anda dapat menentukan cara menjalankan tugas Spark di klaster EKS yang dibagikan dengan menggunakan templat pod dengan Amazon EMR di EKS dan menghemat biaya dan meningkatkan pemanfaatan sumber daya dan performa.

- Untuk mengurangi biaya, Anda dapat menjadwalkan tugas driver Spark untuk dijalankan di Instans Sesuai Permintaan Amazon EC2 sambil menjadwalkan tugas pelaksana Spark untuk dijalankan di Instans Spot Amazon EC2.
- Untuk meningkatkan pemanfaatan sumber daya, Anda dapat mendukung beberapa tim yang menjalankan beban kerja mereka pada klaster EKS yang sama. Setiap tim akan mendapatkan grup simpul Amazon EC2 yang ditunjuk untuk tempat menjalankan beban kerja mereka. Anda dapat menggunakan templat pod untuk menerapkan toleransi yang sesuai untuk beban kerja mereka.
- Untuk meningkatkan pemantauan, Anda dapat menjalankan kontainer pencatatan terpisah untuk meneruskan log pada aplikasi pemantauan yang ada.

Sebagai contoh, file templat pod berikut menunjukkan skenario penggunaan umum.

```
apiVersion: v1
kind: Pod
spec:
  volumes:
    - name: source-data-volume
      emptyDir: {}
    - name: metrics-files-volume
      emptyDir: {}
  nodeSelector:
    eks.amazonaws.com/nodegroup: emr-containers-nodegroup
  containers:
  - name: spark-kubernetes-driver # This will be interpreted as driver Spark main
 container
    env:
      - name: RANDOM
        value: "random"
    volumeMounts:
      - name: shared-volume
        mountPath: /var/data
      - name: metrics-files-volume
        mountPath: /var/metrics/data
  - name: custom-side-car-container # Sidecar container
    image: <side_car_container_image>
    env:
      - name: RANDOM_SIDECAR
        value: random
    volumeMounts:
      - name: metrics-files-volume
        mountPath: /var/metrics/data
```

```
    command:
      - /bin/sh
      - '-c'
      -  <command-to-upload-metrics-files>
  initContainers:
  - name: spark-init-container-driver # Init container
    image: <spark-pre-step-image>
    volumeMounts:
      - name: source-data-volume # Use EMR predefined volumes
        mountPath: /var/data
    command:
      - /bin/sh
      - '-c'
      -  <command-to-download-dependency-jars>
```

Templat pod menyelesaikan tugas berikut:

- Tambahkan kontainer initbaru yang dieksekusi sebelum kontainer utama Spark dimulai. Kontainer init berbagiEmptyDirvolumedisebut`source-data-volume`dengan wadah utama Spark. Anda dapat meminta kontainer init Anda menjalankan langkah inisialisasi, seperti mengunduh dependensi atau menghasilkan data input. Kemudian kontainer utama Spark mengkonsumsi data.
- Tambahkan kontainer sidecar lain yang dieksekusi bersama dengan kontainer utama Spark. Kedua kontainer berbagi volume `EmptyDir` lain yang disebut `metrics-files-volume`. Tugas Spark Anda dapat menghasilkan metrik, seperti metrik Prometheus. Kemudian tugas Spark dapat menempatkan metrik ke dalam file dan meminta kontainer sidecar mengunggah file ke sistem BI Anda sendiri untuk analisis di masa mendatang.
- Tambahkan variabel lingkungan baru ke kontainer utama Spark. Anda dapat meminta tugas Anda mengkonsumsi variabel lingkungan.
- Definisikan sebuah simpul pemilih, sehingga pod hanya dijadwalkan pada grup simpul `emr-containers-nodegroup`. Hal ini membantu untuk mengisolasi sumber daya komputasi di seluruh tugas dan tim.

Mengaktifkan templat pod dengan Amazon EMR di EKS

Untuk mengaktifkan fitur templat pod dengan Amazon EMR pada EKS, konfigurasi properti Spark `spark.kubernetes.driver.podTemplateFile` dan `spark.kubernetes.executor.podTemplateFile` untuk menunjuk ke file templat pod di

Amazon S3. Spark kemudian mengunduh file templat pod dan menggunakannya untuk membangun driver dan pod pelaksana.

> **Note**
>
> Spark menggunakan peran eksekusi tugas untuk memuat templat pod, sehingga peran eksekusi pekerjaan harus memiliki izin untuk mengakses Amazon S3 untuk memuat templat pod. Untuk informasi selengkapnya, lihat Untuk membuat peran eksekusi tugas.

Anda dapat menggunakan `SparkSubmitParameters` untuk menentukan jalur Amazon S3 ke templat pod, seperti yang ditunjukkan file tugas berjalan JSON berikut.

```
{
  "name": "myjob",
  "virtualClusterId": "123456",
  "executionRoleArn": "iam_role_name_for_job_execution",
  "releaseLabel": "release_label",
  "jobDriver": {
    "sparkSubmitJobDriver": {
      "entryPoint": "entryPoint_location",
      "entryPointArguments": ["argument1", "argument2", ...],
       "sparkSubmitParameters": "--class <main_class> \
         --conf
 spark.kubernetes.driver.podTemplateFile=s3://path_to_driver_pod_template \
         --conf
 spark.kubernetes.executor.podTemplateFile=s3://path_to_executor_pod_template \
         --conf spark.executor.instances=2 \
         --conf spark.executor.memory=2G \
         --conf spark.executor.cores=2 \
         --conf spark.driver.cores=1"
    }
  }
}
```

Atau, Anda dapat menggunakan `configurationOverrides` untuk menentukan jalur Amazon S3 ke templat pod, seperti yang ditunjukkan file tugas berjalan JSON berikut.

```
{
  "name": "myjob",
  "virtualClusterId": "123456",
```

```
  "executionRoleArn": "iam_role_name_for_job_execution",
  "releaseLabel": "release_label",
  "jobDriver": {
    "sparkSubmitJobDriver": {
      "entryPoint": "entryPoint_location",
      "entryPointArguments": ["argument1", "argument2", ...],
       "sparkSubmitParameters": "--class <main_class> \
         --conf spark.executor.instances=2 \
         --conf spark.executor.memory=2G \
         --conf spark.executor.cores=2 \
         --conf spark.driver.cores=1"
    }
  },
  "configurationOverrides": {
    "applicationConfiguration": [
      {
        "classification": "spark-defaults",
        "properties": {
          "spark.driver.memory":"2G",
          "spark.kubernetes.driver.podTemplateFile":"s3://path_to_driver_pod_template",

 "spark.kubernetes.executor.podTemplateFile":"s3://path_to_executor_pod_template"
         }
      }
    ]
  }
}
```

> **Note**
>
> 1. Anda harus mengikuti pedoman keamanan saat menggunakan fitur templat pod dengan Amazon EMR di EKS, seperti mengisolasi kode aplikasi yang tidak dipercaya. Untuk informasi selengkapnya, lihat Praktik terbaik keamanan Amazon EMR di EKS.
> 2. Anda tidak dapat mengubah nama kontainer utama Spark dengan menggunakan `spark.kubernetes.driver.podTemplateContainerName` dan `spark.kubernetes.executor.podTemplateContainerName`, karena nama-nama ini di-hardcode sebagai `spark-kubernetes-driver` dan `spark-kubernetes-executors`. Jika Anda ingin menyesuaikan kontainer utama Spark, Anda harus menentukan kontainer dalam templat pod dengan nama-nama di-hardcode ini.

Bidang templat pod

Pertimbangkan pembatasan bidang berikut ketika mengonfigurasi templat pod dengan Amazon EMR di EKS.

- Amazon EMR di EKS hanya mengizinkan bidang-bidang berikut dalam templat pod untuk mengaktifkan penjadwalan tugas yang tepat.

  Ini adalah bidang tingkat pod yang diizinkan:

  - `apiVersion`
  - `kind`
  - `metadata`
  - `spec.activeDeadlineSeconds`
  - `spec.affinity`
  - `spec.containers`
  - `spec.enableServiceLinks`
  - `spec.ephemeralContainers`
  - `spec.hostAliases`
  - `spec.hostname`
  - `spec.imagePullSecrets`
  - `spec.initContainers`
  - `spec.nodeName`
  - `spec.nodeSelector`
  - `spec.overhead`
  - `spec.preemptionPolicy`
  - `spec.priority`
  - `spec.priorityClassName`
  - `spec.readinessGates`
  - `spec.runtimeClassName`
  - `spec.schedulerName`
  - `spec.subdomain`
  - `spec.terminationGracePeriodSeconds`

- `spec.tolerations`
- `spec.topologySpreadConstraints`
- `spec.volumes`

Ini adalah bidang tingkat kontainer utama Spark yang diizinkan:

- `env`
- `envFrom`
- `name`
- `lifecycle`
- `livenessProbe`
- `readinessProbe`
- `resources`
- `startupProbe`
- `stdin`
- `stdinOnce`
- `terminationMessagePath`
- `terminationMessagePolicy`
- `tty`
- `volumeDevices`
- `volumeMounts`
- `workingDir`

Saat Anda menggunakan bidang yang tidak diizinkan dalam templat pod, Spark melempar pengecualian dan tugas gagal. Contoh berikut menunjukkan pesan kesalahan dalam log pengendali Spark karena bidang tidak diizinkan.

```
Executor pod template validation failed.
Field container.command in Spark main container not allowed but specified.
```

- Amazon EMR di EKS menentukan terlebih dahulu parameter berikut dalam templat pod. Bidang yang Anda tentukan dalam templat pod tidak boleh tumpang tindih dengan bidang ini.

  Ini adalah nama volume yang telah ditetapkan:

  - `emr-container-communicate`

- `config-volume`
- `emr-container-application-log-dir`
- `emr-container-event-log-dir`
- `temp-data-dir`
- `mnt-dir`
- `home-dir`
- `emr-container-s3`

Ini adalah pemasangan volume yang telah ditetapkan yang hanya berlaku untuk kontainer utama Spark:

- Nama:`emr-container-communicate`;MountPath:`/var/log/fluentd`
- Nama:`emr-container-application-log-dir`;MountPath:`/var/log/spark/user`
- Nama:`emr-container-event-log-dir`;MountPath:`/var/log/spark/apps`
- Nama:`mnt-dir`;MountPath:`/mnt`
- Nama:`temp-data-dir`;MountPath:`/tmp`
- Nama:`home-dir`;MountPath:`/home/hadoop`

Ini adalah variabel lingkungan yang telah ditetapkan yang hanya berlaku untuk kontainer utama Spark:

- `SPARK_CONTAINER_ID`
- `K8S_SPARK_LOG_URL_STDERR`
- `K8S_SPARK_LOG_URL_STDOUT`
- `SIDECAR_SIGNAL_FILE`

> **Note**
>
> Anda masih dapat menggunakan volume standar yang telah ditentukan ini dan memasangnya ke kontainer sidecar tambahan Anda. Misalnya, Anda dapat menggunakan `emr-container-application-log-dir` dan memasangnya ke kontainer sidecar Anda sendiri yang didefinisikan dalam templat pod.

Jika bidang yang Anda tentukan bertentangan dengan salah satu bidang yang telah ditetapkan dalam templat pod, Spark melempar pengecualian dan tugas gagal. Contoh berikut menunjukkan

pesan kesalahan dalam log aplikasi Spark karena bertentangan dengan bidang yang telah ditentukan.

```
Defined volume mount path on main container must not overlap with reserved mount
 paths: [<reserved-paths>]
```

Pertimbangan kontainer sidecar

Amazon EMR mengendalikan siklus hidup pod yang disediakan oleh Amazon EMR di EKS. Kontainer sidecar harus mengikuti siklus hidup yang sama dengan kontainer utama Spark. Jika Anda menyuntikkan kontainer sidecar tambahan ke pod Anda, kami sarankan Anda mengintegrasikan dengan manajemen siklus hidup pod yang didefinisikan Amazon EMR sehingga kontainer sidecar dapat berhenti sendiri ketika kontainer utama Spark keluar.

Untuk mengurangi biaya, sebaiknya Anda menerapkan proses yang mencegah driver pod dengan kontainer sidecar terus berjalan setelah tugas Anda selesai. Driver Spark menghapus pod pelaksana saat pelaksana selesai. Namun, ketika program driver selesai, kontainer sidecar tambahan terus berjalan. Pod ditagihkan sampai Amazon EMR di EKS membersihkan pod driver, biasanya kurang dari satu menit setelah kontainer utama driver Spark selesai. Untuk mengurangi biaya, Anda dapat mengintegrasikan kontainer sidecar tambahan Anda dengan mekanisme manajemen siklus hidup yang didefinisikan Amazon EMR di EKS untuk driver dan pelaksana pod, seperti yang dijelaskan pada bagian berikut.

Kontainer utama Spark dalam driver dan pelaksana pod mengirimkan `heartbeat` ke `/var/log/fluentd/main-container-terminated` file setiap dua detik. Dengan menambahkan Amazon EMR yang telah ditetapkan `emr-container-communicate` pemasangan volume ke kontainer sidecar Anda, Anda dapat menentukan sub-proses kontainer sidecar Anda untuk secara berkala melacak waktu terakhir diubah untuk file ini. Sub-proses kemudian berhenti sendiri jika menemukan bahwa kontainer utama Spark menghentikan `heartbeat` untuk durasi yang lebih lama.

Contoh berikut menunjukkan sub-proses yang melacak file detak jantung dan berhenti sendiri. Ganti *`your_volume_mount`* dengan jalur di mana anda memasang volume yang telah ditentukan sebelumnya. Script dipaketkan di dalam gambar yang digunakan oleh kontainer sidecar. Dalam file templat pod, Anda dapat menentukan kontainer sidecar dengan perintah `sub_process_script.sh` dan `main_command` berikut.

```
MOUNT_PATH="your_volume_mount"
FILE_TO_WATCH="$MOUNT_PATH/main-container-terminated"
```

```
INITIAL_HEARTBEAT_TIMEOUT_THRESHOLD=60
HEARTBEAT_TIMEOUT_THRESHOLD=15
SLEEP_DURATION=10

function terminate_main_process() {
  # Stop main process
}

# Waiting for the first heartbeat sent by Spark main container
echo "Waiting for file $FILE_TO_WATCH to appear..."
start_wait=$(date +%s)
while ! [[ -f "$FILE_TO_WATCH" ]]; do
    elapsed_wait=$(expr $(date +%s) - $start_wait)
    if [ "$elapsed_wait" -gt "$INITIAL_HEARTBEAT_TIMEOUT_THRESHOLD" ]; then
        echo "File $FILE_TO_WATCH not found after $INITIAL_HEARTBEAT_TIMEOUT_THRESHOLD
 seconds; aborting"
        terminate_main_process
        exit 1
    fi
    sleep $SLEEP_DURATION;
done;
echo "Found file $FILE_TO_WATCH; watching for heartbeats..."

while [[ -f "$FILE_TO_WATCH" ]]; do
    LAST_HEARTBEAT=$(stat -c %Y $FILE_TO_WATCH)
    ELAPSED_TIME_SINCE_AFTER_HEARTBEAT=$(expr $(date +%s) - $LAST_HEARTBEAT)
    if [ "$ELAPSED_TIME_SINCE_AFTER_HEARTBEAT" -gt "$HEARTBEAT_TIMEOUT_THRESHOLD" ];
 then
        echo "Last heartbeat to file $FILE_TO_WATCH was more than
 $HEARTBEAT_TIMEOUT_THRESHOLD seconds ago at $LAST_HEARTBEAT; terminating"
        terminate_main_process
        exit 0
    fi
    sleep $SLEEP_DURATION;
done;
echo "Outside of loop, main-container-terminated file no longer exists"

# The file will be deleted once the fluentd container is terminated

echo "The file $FILE_TO_WATCH doesn't exist any more;"
terminate_main_process
exit 0
```

Menggunakan kebijakan coba ulang pekerjaan

Di Amazon EMR pada EKS versi 6.9.0 dan yang lebih baru, Anda dapat menetapkan kebijakan coba ulang untuk pekerjaan Anda berjalan. Coba lagi kebijakan menyebabkan pod driver pekerjaan dimulai ulang secara otomatis jika gagal atau dihapus. Ini membuat pekerjaan streaming Spark yang berjalan lama lebih tahan terhadap kegagalan.

Menetapkan kebijakan coba ulang untuk suatu pekerjaan

Untuk mengonfigurasi kebijakan coba ulang, Anda menyediakan`RetryPolicyConfiguration`bidang menggunakan[StartJobRun](#)API. Contoh`retryPolicyConfiguration`ditampilkan di sini:

```
aws emr-containers start-job-run \
--virtual-cluster-id cluster_id \
--name sample-job-name \
--execution-role-arn execution-role-arn \
--release-label emr-6.9.0-latest \
--job-driver '{
  "sparkSubmitJobDriver": {
    "entryPoint": "local:///usr/lib/spark/examples/src/main/python/pi.py",
    "entryPointArguments": [ "2" ],
    "sparkSubmitParameters": "--conf spark.executor.instances=2 --conf
 spark.executor.memory=2G --conf spark.executor.cores=2 --conf spark.driver.cores=1"
  }
}' \
--retry-policy-configuration '{
    "maxAttempts": 5
  }' \
--configuration-overrides '{
  "monitoringConfiguration": {
    "cloudWatchMonitoringConfiguration": {
      "logGroupName": "my_log_group_name",
      "logStreamNamePrefix": "my_log_stream_prefix"
    },
    "s3MonitoringConfiguration": {
       "logUri": "s3://DOC-EXAMPLE-BUCKET-LOGGING"
    }
  }
}'
```

> **Note**
>
> `retryPolicyConfiguration`hanya tersedia dariAWS CLI1.27.68 versi dan seterusnya. Untuk memperbaruiAWS CLIke versi terbaru, lihatMenginstal atau memperbarui versi terbaru dariAWS CLI

KonfigurasikanmaxAttemptsfield dengan jumlah maksimum yang kamu inginkan agar pod driver job di-restart jika gagal atau dihapus. Interval eksekusi antara dua upaya coba ulang pengemudi pekerjaan adalah interval percobaan ulang eksponensial (10 detik, 20 detik, 40 detik...) yang dibatasi pada 6 menit, seperti yang dijelaskan dalamDokumentasi Kubernetes.

> **Note**
>
> Setiap eksekusi pengemudi pekerjaan tambahan akan ditagih sebagai pekerjaan lain, dan akan dikenakanAmazon EMR pada harga EKS.

Coba lagi nilai konfigurasi kebijakan

- Kebijakan coba ulang default untuk suatu pekerjaan: `StartJobRun`menyertakan kebijakan coba lagi yang ditetapkan ke 1 upaya maksimum secara default. Anda dapat mengonfigurasi kebijakan coba lagi sesuai keinginan.

  > **Note**
  >
  > JikamaxAttemptsdariretryPolicyConfigurationdiatur ke 1, itu berarti tidak ada percobaan ulang yang akan dilakukan untuk memunculkan pod driver pada kegagalan.

- Menonaktifkan kebijakan coba lagi untuk suatu pekerjaan:Untuk menonaktifkan kebijakan coba lagi, tetapkan nilai upaya maks diretryPolicyConfigurationuntuk 1.

  ```
  "retryPolicyConfiguration": {
      "maxAttempts": 1
  }
  ```

- Tetapkan MaxUpaya untuk pekerjaan dalam rentang yang valid: `StartJobRun`panggilan akan gagal jikamaxAttemptsnilai berada di luar rentang yang valid. Yang validmaxAttemptsRentang adalah dari 1 hingga 2.147.483.647 (32-bit integer), rentang yang didukung untuk Kubernetes

'`backOffLimit`pengaturan konfigurasi. Untuk informasi lebih lanjut, lihatKebijakan kegagalan Pod backoffdalam dokumentasi Kubernetes. Jika`maxAttempts`nilai tidak valid, pesan galat berikut dikembalikan:

```
{
 "message": "Retry policy configuration's parameter value of maxAttempts is invalid"
}
```

Mengambil status kebijakan percobaan ulang untuk suatu pekerjaan

Anda dapat melihat status upaya percobaan ulang untuk pekerjaan dengan`ListJobRuns`dan`DescribeJobRun`API. Setelah Anda meminta pekerjaan dengan konfigurasi kebijakan coba ulang yang diaktifkan,`ListJobRun`dan`DescribeJobRun`tanggapan akan berisi status kebijakan coba lagi di`RetryPolicyExecution`bidang. Selain itu,`DescribeJobRun`respon akan berisi`RetryPolicyConfiguration`yang masukan di`StartJobRun`permintaan untuk pekerjaan itu.

Respons sampel

ListJobRuns response

```
{
  "jobRuns": [
    ...
    ...
    "retryPolicyExecution" : {
      "currentAttemptCount": 2
    }
    ...
    ...
  ]
}
```

DescribeJobRun response

```
{
  ...
  ...
  "retryPolicyConfiguration": {
    "maxAttempts": 5
```

```
    },
    "retryPolicyExecution" : {
     "currentAttemptCount": 2
   },
   ...
   ...
}
```

Bidang ini tidak akan terlihat ketika kebijakan coba lagi dinonaktifkan dalam pekerjaan, seperti yang dijelaskan di bawah ini diCoba lagi nilai konfigurasi kebijakan.

Memantau pekerjaan dengan kebijakan coba lagi

Saat Anda mengaktifkan kebijakan coba ulang, aCloudWatchacara yang dihasilkan untuk setiap driver pekerjaan yang dibuat. Untuk berlangganan acara ini, siapkanCloudWatchaturan acara menggunakan perintah berikut:

```
aws events put-rule \
--name cwe-test \
--event-pattern '{"detail-type": ["EMR Job Run New Driver Attempt"]}'
```

Acara ini akan mengembalikan informasi tentang`newDriverPodName`,`newDriverCreatedAt`stempel waktu,`previousDriverFailureMessage`, dan`currentAttemptCount`dari pengemudi pekerjaan. Peristiwa ini tidak akan dibuat jika kebijakan coba lagi dinonaktifkan.

Untuk informasi lebih lanjut tentang cara memantau pekerjaan Anda denganCloudWatchperistiwa, lihatMemantau tugas dengan Amazon CloudWatch Events.

Menemukan log untuk driver dan pelaksana

Nama pod driver mengikuti format`spark-<job id>-driver-<random-suffix>`. Sama`random-suffix`ditambahkan ke nama pod pelaksana yang dihasilkan pengemudi. Bila Anda menggunakan ini`random-suffix`, Anda dapat menemukan log untuk driver dan pelaksana terkait. Yang`random-suffix`hanya hadir jikakebijakan coba lagi diaktifkanuntuk pekerjaan; jika tidak,`random-suffix`tidak ada.

Untuk informasi selengkapnya tentang cara mengonfigurasi pekerjaan dengan konfigurasi pemantauan untuk pencatatan, lihatJalankan aplikasi Spark park park park park park park.

Menggunakan rotasi log peristiwa Spark

Dengan Amazon EMR 6.3.0 dan versi lebih baru, Anda dapat mengaktifkan fitur rotasi log peristiwa Spark untuk Amazon EMR di EKS. Alih-alih menghasilkan file log peristiwa tunggal, fitur ini merotasikan file berdasarkan interval waktu terkonfigurasi Anda dan menghapus file log peristiwa terlama.

Merotasi log peristiwa Spark dapat membantu Anda menghindari potensi masalah dengan file log peristiwa Spark besar yang dihasilkan untuk tugas yang dijalankan atau di-stream dalam jangka panjang. Misalnya, Anda memulai tugas Spark berjangka panjang dengan log peristiwa yang diaktifkan dengan parameter `persistentAppUI`. Driver Spark menghasilkan file log peristiwa. Jika tugas berjalan selama berjam-jam atau berhari-hari dan ada ruang disk terbatas pada simpul Kubernetes, file log peristiwa dapat mengkonsumsi semua ruang disk yang tersedia. Mengaktifkan fitur rotasi log peristiwa Spark memecahkan masalah dengan membelah file log ke beberapa file dan menghapus file terlama.

> **Note**
>
> Fitur ini hanya berfungsi dengan Amazon EMR di EKS. Amazon EMR yang berjalan di Amazon EC2 tidak mendukung rotasi log peristiwa Spark.

Untuk mengaktifkan fitur rotasi log peristiwa Spark, konfigurasi parameter Spark berikut:

- `spark.eventLog.rotation.enabled` - menyalakan rotasi log. Ini dinonaktifkan secara default dalam file konfigurasi Spark. Atur ke betul untuk mengaktifkan fitur ini.
- `spark.eventLog.rotation.interval` - menentukan interval waktu untuk rotasi log. Nilai minimum adalah 60 detik. Nilai default adalah 300 detik.
- `spark.eventLog.rotation.minFileSize` - menentukan ukuran file minimum untuk merotasikan file log. Nilai minimum dan default adalah 1 MB.
- `spark.eventLog.rotation.maxFilesToRetain` - menentukan berapa banyak dile log yang dirotasikan untuk disimpan selama pembersihan. Rentang validnya adalah 1 hingga 10. Nilai default adalah 2.

Anda dapat menentukan parameter ini dalam bagian `sparkSubmitParameters` dari API `StartJobRun`, seperti yang ditunjukkan contoh berikut.

```
"sparkSubmitParameters": "--class org.apache.spark.examples.SparkPi --conf
 spark.eventLog.rotation.enabled=true --conf spark.eventLog.rotation.interval=300 --
conf spark.eventLog.rotation.minFileSize=1m --conf
 spark.eventLog.rotation.maxFilesToRetain=2"
```

Menggunakan rotasi log kontainer Spark

Dengan Amazon EMR 6.11.0 dan versi lebih baru, Anda dapat mengaktifkan fitur rotasi log kontainer Spark untuk Amazon EMR di EKS. Alih-alih menghasilkan satu`stdout`atau`stderr`log file, fitur ini memutar file berdasarkan ukuran rotasi Anda dikonfigurasi dan menghapus file log tertua dari wadah.

Memutar log kontainer Spark dapat membantu Anda menghindari potensi masalah dengan file log Spark besar yang dihasilkan untuk pekerjaan yang berjalan lama atau streaming. Misalnya, Anda mungkin memulai pekerjaan Spark yang berjalan lama, dan driver Spark menghasilkan file log kontainer. Jika pekerjaan berjalan selama berjam-jam atau hari dan ada ruang disk terbatas pada node Kubernetes, file log kontainer dapat menggunakan semua ruang disk yang tersedia. Saat mengaktifkan rotasi log kontainer Spark, Anda membagi file log menjadi beberapa file, dan menghapus file terlama.

Untuk mengaktifkan fitur rotasi log kontainer Spark, konfigurasikan parameter Spark berikut:

`containerLogRotationConfiguration`

Sertakan parameter ini di`monitoringConfiguration`untuk mengaktifkan rotasi log. Ini dinonaktifkan secara default. Anda harus menggunakan`containerLogRotationConfiguration`selain`s3MonitoringConfiguration`.

`rotationSize`

Yang`rotationSize`parameter menentukan ukuran file untuk rotasi log. Kisaran nilai yang mungkin adalah dari`2KB`kepada`2GB`. Bagian satuan numerik dari`rotationSize`parameter dilewatkan sebagai integer. Karena nilai desimal tidak didukung, Anda dapat menentukan ukuran rotasi 1,5GB, misalnya, dengan nilai`1500MB`.

`maxFilesToKeep`

Yang`maxFilesToKeep`parameter menentukan jumlah maksimum file untuk mempertahankan dalam wadah setelah rotasi telah terjadi. Nilai minimum adalah 1, dan nilai maksimumnya adalah 50.

Anda dapat menentukan parameter ini dalam bagian `monitoringConfiguration` dari API `StartJobRun`, seperti yang ditunjukkan contoh berikut. Dalam contoh ini, dengan`rotationSize = "10 MB"`dan`maxFilesToKeep = 3`, Amazon EMR di EKS memutar log Anda pada 10 MB, menghasilkan file log baru, dan kemudian membersihkan file log tertua setelah jumlah file log mencapai 3.

```
{
  "name": "my-long-running-job",
  "virtualClusterId": "123456",
  "executionRoleArn": "iam_role_name_for_job_execution",
  "releaseLabel": "emr-6.11.0-latest",
  "jobDriver": {
    "sparkSubmitJobDriver": {
      "entryPoint": "entryPoint_location",
      "entryPointArguments": ["argument1", "argument2", ...],
       "sparkSubmitParameters": "--class main_class --conf spark.executor.instances=2
 --conf spark.executor.memory=2G --conf spark.executor.cores=2 --conf
 spark.driver.cores=1"
    }
  },
  "configurationOverrides": {
    "applicationConfiguration": [
      {
        "classification": "spark-defaults",
        "properties": {
          "spark.driver.memory":"2G"
         }
      }
    ],
    "monitoringConfiguration": {
      "persistentAppUI": "ENABLED",
      "cloudWatchMonitoringConfiguration": {
        "logGroupName": "my_log_group",
        "logStreamNamePrefix": "log_stream_prefix"
      },
      "s3MonitoringConfiguration": {
        "logUri": "s3://my_s3_log_location"
      },
      "containerLogRotationConfiguration": {
        "rotationSize":"10MB",
        "maxFilesToKeep":"3"
      }
    }
```

```
  }
}
```

Untuk memulai pekerjaan yang dijalankan dengan rotasi log kontainer Spark, sertakan jalur ke file json yang Anda konfigurasikan dengan parameter ini di`StartJobRun`perintah.

```
aws emr-containers start-job-run \
--cli-input-json file://path-to-json-request-file
```

Menggunakan penskalaan otomatis vertikal dengan pekerjaan Amazon EMR Spark

Amazon EMR pada penskalaan otomatis vertikal EKS secara otomatis menyetel memori dan sumber daya CPU untuk beradaptasi dengan kebutuhan beban kerja yang Anda berikan untuk aplikasi Amazon EMR Spark. Ini menyederhanakan manajemen sumber daya.

Untuk melacak pemanfaatan sumber daya real-time dan historis dari aplikasi Amazon EMR Spark Anda, penskalaan otomatis vertikal memanfaatkan KubernetesAutoscaler Pod Vertikal (VPA). Kemampuan autoscaling vertikal menggunakan data yang dikumpulkan VPA untuk secara otomatis menyetel memori dan sumber daya CPU yang ditetapkan ke aplikasi Spark Anda. Proses yang disederhanakan ini meningkatkan keandalan dan mengoptimalkan biaya.

Topik

- Menyiapkan penskalaan otomatis vertikal untuk Amazon EMR di EKS
- Memulai dengan penskalaan otomatis vertikal untuk Amazon EMR di EKS
- Mengonfigurasi penskalaan otomatis vertikal untuk Amazon EMR di EKS
- Memantau penskalaan otomatis vertikal untuk Amazon EMR di EKS
- Copot pemasangan Amazon EMR pada operator penskalaan otomatis vertikal EKS

Menyiapkan penskalaan otomatis vertikal untuk Amazon EMR di EKS

Topik ini membantu Anda menyiapkan klaster Amazon EKS Anda untuk mengirimkan pekerjaan Amazon EMR Spark dengan penskalaan otomatis vertikal. Proses penyiapan mengharuskan Anda untuk mengonfirmasi atau menyelesaikan tugas di bagian berikut:

Topik

Prasyarat

Selesaikan tugas-tugas berikut sebelum kamu menginstal operator Kubernetes autoscaling vertikal pada klaster kamu. Jika Anda telah menyelesaikan salah satu prasyarat, Anda dapat melewatkannya dan beralih ke yang berikutnya.

- Instal AWS CLI- Jika Anda sudah menginstalAWS CLI, konfirmasikan bahwa Anda memiliki versi terbaru.
- Instal kubectl— kubectl adalah sebuah command line tool yang kamu gunakan untuk berkomunikasi dengan Kubernetes API server. Kamu perlu kubectl untuk menginstal dan memantau artefak terkait autoscaling vertikal pada klaster Amazon EKS kamu.
- Instal Operator SDK— Amazon EMR on EKS menggunakan Operator SDK sebagai manajer paket untuk masa pakai operator penskalaan otomatis vertikal yang Anda instal di klaster Anda.
- Instal Docker— Anda memerlukan akses ke Docker CLI untuk mengautentikasi dan mengambil gambar Docker terkait autoscaling vertikal untuk dipasang di klaster Amazon EKS Anda.
- Atur klaster Amazon EKS(versi 1.24 atau lebih tinggi)- Penskalaan otomatis vertikal didukung dengan Amazon EKS versi 1.24 dan yang lebih tinggi. Setelah Anda membuat klaster,mendaftarkannya untuk digunakan dengan Amazon EMR.
- Pilih URI gambar dasar Amazon EMR(rilis 6.10.0 atau lebih tinggi)— Penskalaan otomatis vertikal didukung dengan rilis Amazon EMR 6.10.0 dan yang lebih tinggi.

Instal Operator Lifecycle Manager (OLM) di klaster Amazon EKS

Gunakan Operator SDK CLI untuk menginstal Operator Lifecycle Manager (OLM) pada klaster Amazon EMR di EKS tempat Anda ingin menyiapkan penskalaan otomatis vertikal, seperti yang ditunjukkan pada contoh berikut. Setelah Anda mengaturnya, Anda dapat menggunakan OLM untuk menginstal dan mengelola siklus hidupOperator penskalaan otomatis vertikal Amazon EMR.

```
operator-sdk olm install
```

Untuk memvalidasi instalasi, jalankan`olm status`perintah:

```
operator-sdk olm status
```

Verifikasi bahwa perintah mengembalikan hasil yang sukses, mirip dengan contoh output berikut:

```
INFO[0007] Successfully got OLM status for version X.XX
```

Jika penginstalan Anda tidak berhasil, lihatMemecahkan masalah Amazon EMR pada penskalaan otomatis vertikal EKS.

Instal Amazon EMR pada operator penskalaan otomatis vertikal EKS

Gunakan langkah-langkah berikut untuk menginstal operator penskalaan otomatis vertikal di klaster Amazon EKS Anda:

1. Siapkan variabel lingkungan berikut yang akan Anda gunakan untuk menyelesaikan instalasi:
   - **$REGION**poin keWilayah AWSuntuk cluster Anda. Sebagai contoh, `us-west-2`.
   - **$ACCOUNT_ID**menunjuk ke ID akun Amazon ECR untuk Wilayah Anda. Untuk informasi selengkapnya, lihat Akun registri Amazon ECR berdasarkan Wilayah.
   - **$RELEASE**menunjuk ke rilis Amazon EMR yang ingin Anda gunakan untuk klaster Anda. Dengan penskalaan otomatis vertikal, Anda harus menggunakan Amazon EMR release 6.10.0 atau yang lebih tinggi.
2. Selanjutnya, dapatkan token otentikasi keRegistri Amazon ECRuntuk operator.

   ```
   aws ecr get-login-password \
    --region region-id | docker login \
    --username AWS \
    --password-stdin $ACCOUNT_ID.dkr.ecr.region-id.amazonaws.com
   ```
3. Instal Amazon EMR pada operator penskalaan otomatis vertikal EKS dengan perintah berikut:

   ```
   ECR_URL=$ACCOUNT_ID.dkr.ecr.$REGION.amazonaws.com && \
   REPO_DEST=dynamic-sizing-k8s-operator-olm-bundle && \
   BUNDLE_IMG=emr-$RELEASE-dynamic-sizing-k8s-operator && \
   operator-sdk run bundle \
   $ECR_URL/$REPO_DEST/$BUNDLE_IMG\:latest
   ```

   Ini akan membuat rilis operator penskalaan otomatis vertikal di namespace default klaster Amazon EKS Anda. Gunakan perintah ini untuk menginstal di namespace yang berbeda:

```
operator-sdk run bundle \
$ACCOUNT_ID.dkr.ecr.$REGION.amazonaws.com/dynamic-sizing-k8s-operator-olm-bundle/
emr-$RELEASE-dynamic-sizing-k8s-operator:latest \
-n operator-namespace
```

> **Note**
>
> Jika namespace yang Anda tentukan tidak ada, OLM tidak akan menginstal operator. Untuk informasi selengkapnya, lihat Namespace Kubernetes tidak ditemukan.

4. Pastikan kamu berhasil menginstal operator dengan command-line tool kubectl Kubernetes.

```
kubectl get csv -n operator-namespace
```

Yang`kubectl`perintah harus mengembalikan operator autoscaler vertikal Anda yang baru dikerahkan denganFasestatusBerhasil. Jika Anda mengalami masalah dengan instalasi atau penyiapan, lihatMemecahkan masalah Amazon EMR pada penskalaan otomatis vertikal EKS.

Memulai dengan penskalaan otomatis vertikal untuk Amazon EMR di EKS

Mengirimkan pekerjaan Spark dengan autoscaling vertikal

Ketika Anda mengirimkan pekerjaan melaluiStartJobRunAPI, tambahkan dua konfigurasi berikut ke driver untuk pekerjaan Spark Anda untuk mengaktifkan autoscaling vertikal:

```
"spark.kubernetes.driver.label.emr-containers.amazonaws.com/dynamic.sizing":"true",
"spark.kubernetes.driver.annotation.emr-containers.amazonaws.com/
dynamic.sizing.signature":"YOUR_JOB_SIGNATURE"
```

Pada kode di atas, baris pertama memungkinkan kemampuan autoscaling vertikal. Baris berikutnya adalah konfigurasi tanda tangan yang diperlukan yang memungkinkan Anda memilih tanda tangan untuk pekerjaan Anda.

Untuk informasi selengkapnya tentang konfigurasi ini dan nilai parameter yang dapat diterima, lihatMengonfigurasi penskalaan otomatis vertikal untuk Amazon EMR di EKS. Secara default, pekerjaan Anda diserahkan dalam pemantauan sajaOffmodus autoscaling vertikal. Status pemantauan ini memungkinkan Anda menghitung dan melihat rekomendasi sumber daya tanpa

melakukan penskalaan otomatis. Untuk informasi selengkapnya, lihat Mode penskalaan otomatis vertikal.

Contoh berikut menunjukkan bagaimana untuk menyelesaikan sampel`start-job-run`perintah dengan autoscaling vertikal:

```
aws emr-containers start-job-run \
--virtual-cluster-id $VIRTUAL_CLUSTER_ID \
--name $JOB_NAME \
--execution-role-arn $EMR_ROLE_ARN \
--release-label emr-6.10.0-latest \
--job-driver '{
  "sparkSubmitJobDriver": {
     "entryPoint": "local:///usr/lib/spark/examples/src/main/python/pi.py"
   }
 }' \
--configuration-overrides '{
    "applicationConfiguration": [{
        "classification": "spark-defaults",
        "properties": {
          "spark.kubernetes.driver.label.emr-containers.amazonaws.com/dynamic.sizing":
 "true",
          "spark.kubernetes.driver.annotation.emr-containers.amazonaws.com/
dynamic.sizing.signature": "test-signature"
        }
    }]
  }'
```

Memverifikasi fungsi autoscaling vertikal

Untuk memverifikasi bahwa autoscaling vertikal berfungsi dengan benar untuk pekerjaan yang diajukan, gunakan kubectl untuk mendapatkan`verticalpodautoscaler`sumber daya khusus dan lihat rekomendasi penskalaan Anda. Misalnya, perintah berikut query untuk rekomendasi pada contoh pekerjaan dariMengirimkan pekerjaan Spark dengan autoscaling vertikalbagian:

```
kubectl get verticalpodautoscalers --all-namespaces \
-l=emr-containers.amazonaws.com/dynamic.sizing.signature=test-signature
```

Output dari query ini harus menyerupai berikut ini:

```
NAME                                                    MODE   CPU         MEM
 PROVIDED   AGE
```

```
ds-jceyefkxnhrvdzw6djum3naf2abm6o63a6dvjkkedqtkhlrf25eq-vpa   Off    3304504865  True
        87m
```

Jika output Anda tidak terlihat serupa atau berisi kode kesalahan, lihatMemecahkan masalah Amazon EMR pada penskalaan otomatis vertikal EKSuntuk langkah-langkah untuk membantu menyelesaikan masalah.

Mengonfigurasi penskalaan otomatis vertikal untuk Amazon EMR di EKS

Anda dapat mengonfigurasi penskalaan otomatis vertikal saat mengirimkan pekerjaan Amazon EMR Spark melaluiStartJobRunAPI. Tetapkan parameter konfigurasi terkait autoscaling pada Pod driver Spark seperti yang ditunjukkan pada contohMengirimkan pekerjaan Spark dengan autoscaling vertikal.

Operator autoscaling vertikal Amazon EMR pada EKS mendengarkan pod driver yang memiliki autoscaling, kemudian mengatur integrasi dengan Kubernetes Vertical Pod Autoscaler (VPA) dengan pengaturan pada pod driver. Ini memfasilitasi pelacakan sumber daya dan autoscaling dari Pod pelaksana Spark.

Bagian berikut menjelaskan parameter yang dapat Anda gunakan saat mengonfigurasi penskalaan otomatis vertikal untuk klaster Amazon EKS Anda.

> **Note**
>
> Konfigurasikan parameter toggle fitur sebagai label, dan konfigurasikan parameter yang tersisa sebagai anotasi pada pod driver Spark. Parameter autoscaling milikiemr-containers.amazonaws.com/domain dan memilikidynamic.sizingawalan.

Parameter yang dibutuhkan

Anda harus menyertakan dua parameter berikut pada driver pekerjaan Spark ketika Anda mengirimkan pekerjaan Anda:

Key	Deskripsi	Nilai yang diterima	Nilai default	Tipe	Parameter percikan[1]
dynamic.sizing	Fitur beralih	true, false	tidak diatur	label	spark.kubernetes.d

Key	Deskripsi	Nilai yang diterima	Nilai default	Tipe	Parameter percikan[1]
					`river.label.emr-containers.amazonaws.com/dynamic.sizing`
`dynamic.sizing.signature`	Tanda tangan pekerjaan	tali	tidak diatur	anotasi	`spark.kubernetes.driver.annotation.emr-containers.amazonaws.com/dynamic.sizing.signature`

[1]Gunakan parameter ini sebagai`SparkSubmitParameter`atau`ConfigurationOverride`di dalam`StartJobRun`API.

- **`dynamic.sizing`**- Anda dapat mengaktifkan dan mematikan autoscaling vertikal dengan`dynamic.sizing`label. Untuk mengaktifkan penskalaan otomatis vertikal, setel`dynamic.sizing`kepada`true`pada pod driver Spark. Jika Anda menghilangkan label ini atau mengaturnya ke nilai selain`true`, autoscaling vertikal dimatikan.
- **`dynamic.sizing.signature`**- Tetapkan tanda tangan pekerjaan dengan`dynamic.sizing.signature`anotasi pada pod driver. Penskalaan otomatis vertikal menggabungkan data penggunaan sumber daya Anda di berbagai proses pekerjaan Amazon EMR Spark untuk mendapatkan rekomendasi sumber daya. Anda memberikan pengenal unik untuk mengikat pekerjaan bersama.

> **Note**
>
> Jika pekerjaan Anda berulang pada interval tetap seperti harian atau mingguan, maka tanda tangan pekerjaan Anda harus tetap sama untuk setiap contoh pekerjaan baru. Hal ini memastikan bahwa autoscaling vertikal dapat menghitung dan mengumpulkan rekomendasi di berbagai pekerjaan.

[1]Gunakan parameter ini sebagai`SparkSubmitParameter`atau`ConfigurationOverride`di dalam`StartJobRun`API.

Parameter opsional

Autoscaling vertikal juga mendukung parameter opsional berikut. Atur mereka sebagai anotasi pada pod driver.

Key	Deskripsi	Nilai yang diterima	Nilai default	Tipe	Parameter percikan[1]
dynamic.sizing.mode	Mode penskalaan otomatis vertikal	`Off`, `Initial`, `Auto`	`Off`	anotasi	`spark.kubernetes.driver.label.emr-containers.amazonaws.com/dynamic.sizing.mode`
dynamic.sizing.scale.memory	Memungkinkan penskalaan memori	*`true`*, *`false`*	`true`	anotasi	`spark.kubernetes.driver.label.emr-containers.amazonaws.com/dynamic.sizin`

Key	Deskripsi	Nilai yang diterima	Nilai default	Tipe	Parameter percikan[1]
					`g.scale.memory`
`dynamic.sizing.scale.cpu`	Mengaktifkan atau menonaktifkan penskalaan CPU	*`true`*, *`false`*	`false`	anotasi	`spark.kubernetes.driver.label.emr-containers.amazonaws.com/dynamic.sizing.scale.cpu`
`dynamic.sizing.scale.memory.min`	Batas minumum untuk penskalaan memori	tali,Kuantitas sumber daya K8smantan: `1G`	tidak diatur	anotasi	`spark.kubernetes.driver.label.emr-containers.amazonaws.com/dynamic.sizing.scale.memory.min`

Key	Deskripsi	Nilai yang diterima	Nilai default	Tipe	Parameter percikan[1]
dynamic.sizing.scale.memory.max	Batas maksimum untuk penskalaan memori	tali,Kuantitas sumber daya K8smantan: 4G	tidak diatur	anotasi	spark.kubernetes.driver.label.emr-containers.amazonaws.com/dynamic.sizing.scale.memory.max
dynamic.sizing.scale.cpu.min	Batas minimum untuk penskalaan CPU	tali,Kuantitas sumber daya K8smantan: 1	tidak diatur	anotasi	spark.kubernetes.driver.label.emr-containers.amazonaws.com/dynamic.sizing.scale.cpu.min
dynamic.sizing.scale.cpu.max	Batas maksimum untuk penskalaan CPU	tali,Kuantitas sumber daya K8smantan: 2	tidak diatur	anotasi	spark.kubernetes.driver.label.emr-containers.amazonaws.com/dynamic.sizing.scale.cpu.max

Mode penskalaan otomatis vertikal

Yang`mode`parameter peta ke mode autoscaling yang berbeda yang didukung VPA. Gunakan`dynamic.sizing.mode`anotasi pada pod driver untuk mengatur mode. Nilai berikut didukung untuk parameter ini:

- Off- Mode lari kering di mana Anda dapat memantau rekomendasi, tetapi penskalaan otomatis tidak dilakukan. Ini adalah mode default untuk autoscaling vertikal. Dalam mode ini, sumber daya vertical pod autoscaler terkait menghitung rekomendasi, dan kamu dapat memantau rekomendasinya melalui alat seperti kubectl, Prometheus, dan Grafana.
- Awal— Dalam mode ini, VPA autoscale sumber daya ketika pekerjaan dimulai jika rekomendasi tersedia berdasarkan pekerjaan bersejarah, seperti dalam kasus pekerjaan berulang.
- Otomatis— Dalam mode ini, VPA mengusir Pod pelaksana Spark, dan menskalakannya secara otomatis dengan pengaturan sumber daya yang direkomendasikan saat Pod driver Spark memulai ulang Pod tersebut. Terkadang, VPA mengusir menjalankan Pod pelaksana Spark, sehingga dapat mengakibatkan latensi tambahan saat mencoba ulang pelaksana yang terputus.

Penskalaan sumber daya

Saat mengatur penskalaan otomatis vertikal, Anda dapat memilih apakah akan menskalakan sumber daya CPU dan memori.
Mengaturd`ynamic.sizing.scale.cpu`dan`dynamic.sizing.scale.memory`anotasi k`etrue`ataufalse. Secara default, penskalaan CPU diatur k`efalse`, dan penskalaan memori diatur k`etrue`.

Minimum sumber daya dan maksimum (Batas)

Secara opsional, Anda juga dapat menetapkan batasan pada sumber daya CPU dan memori. Pilih nilai minimum dan maksimum untuk sumber daya ini dengan`dynamic.sizing.[memory/cpu].[min/max]`anotasi saat Anda mengaktifkan penskalaan otomatis. Secara default, sumber daya tidak memiliki batasan. Tetapkan anotasi sebagai nilai string yang merepresentasikan kuantitas sumber daya Kubernetes. Misalnya, set`dynamic.sizing.memory.max`kepada`4G`untuk mewakili 4 GB.

Memantau penskalaan otomatis vertikal untuk Amazon EMR di EKS

Kamu dapat menggunakan command line tool kubectl Kubernetes untuk mencantumkan rekomendasi yang berhubungan dengan autoscaling-vertikal yang aktif pada klaster kamu. Anda

juga dapat melihat tanda tangan pekerjaan yang dilacak, dan membersihkan sumber daya yang tidak dibutuhkan yang terkait dengan tanda tangan.

Buat daftar rekomendasi autoscaling vertikal untuk klaster Anda

Gunakan kubectl untuk mendapatkan`verticalpodautoscalers`sumber daya, dan melihat status saat ini dan rekomendasi. Contoh kueri berikut menampilkan semua sumber daya aktif di klaster Amazon EKS Anda.

```
kubectl get verticalpodautoscalers \
-o custom-columns="NAME:.metadata.name,"\
"SIGNATURE:.metadata.labels.emr-containers\.amazonaws\.com/dynamic\.sizing
\.signature,"\
"MODE:.spec.updatePolicy.updateMode,"\
"MEM:.status.recommendation.containerRecommendations[0].target.memory" \
--all-namespaces
```

Output dari query ini menyerupai berikut ini:

```
NAME                  SIGNATURE              MODE      MEM
ds-example-id-1-vpa   job-signature-1        Off       none
ds-example-id-2-vpa   job-signature-2        Initial   12936384283
```

Kueri dan hapus rekomendasi autoscaling vertikal untuk klaster Anda

Saat Anda menghapus sumber daya yang dijalankan oleh pekerjaan penskalaan otomatis vertikal Amazon EMR, secara otomatis akan menghapus objek VPA terkait yang melacak dan menyimpan rekomendasi.

Contoh berikut menggunakan kubectl untuk membersihkan rekomendasi untuk pekerjaan yang diidentifikasi dengan tanda tangan:

```
kubectl delete jobrun -n emr -l=emr-containers\.amazonaws\.com/dynamic\.sizing
\.signature=integ-test
jobrun.dynamicsizing.emr.services.k8s.aws "ds-job-signature" deleted
```

Jika Anda tidak tahu tanda tangan pekerjaan tertentu, atau ingin membersihkan semua sumber daya pada klaster, Anda dapat menggunakan`--all`atau`--all-namespaces`dalam perintah Anda, bukan ID pekerjaan unik, seperti yang ditunjukkan pada contoh berikut:

```
kubectl delete jobruns --all --all-namespaces
jobrun.dynamicsizing.emr.services.k8s.aws "ds-example-id" deleted
```

Copot pemasangan Amazon EMR pada operator penskalaan otomatis vertikal EKS

Jika Anda ingin menghapus operator penskalaan otomatis vertikal dari klaster Amazon EKS Anda, gunakan`cleanup`perintah dengan Operator SDK CLI seperti yang ditunjukkan pada contoh berikut. Ini juga menghapus dependensi upstream yang diinstal dengan operator, seperti Vertical Pod Autoscaler.

```
operator-sdk cleanup emr-dynamic-sizing
```

Jika ada pekerjaan yang berjalan di cluster ketika Anda menghapus operator, pekerjaan tersebut terus berjalan tanpa autoscaling vertikal. Jika Anda mengirimkan pekerjaan pada klaster setelah Anda menghapus operator, Amazon EMR pada EKS akan mengabaikan parameter terkait autoscaling vertikal yang mungkin telah Anda tetapkan selamakonfigurasi.

Menjalankan beban kerja interaktif di Amazon EMR di EKS

Endpoint interaktif adalah gateway yang menghubungkan Amazon EMR Studio ke Amazon EMR di EKS sehingga Anda dapat menjalankan beban kerja interaktif. Anda dapat menggunakan endpoint interaktif dengan EMR Studio untuk menjalankan analisis interaktif dengan kumpulan data di penyimpanan data seperti Amazon S3 dan Amazon DynamoDB.

Kasus penggunaan

- Buat skrip ETL dengan pengalaman EMR Studio IDE. IDE menyerap data lokal dan menyimpannya di Amazon S3 setelah transformasi untuk analisis selanjutnya.
- Gunakan buku catatan untuk menjelajahi kumpulan data dan melatih model pembelajaran mesin untuk mendeteksi anomali dalam kumpulan data.
- Buat skrip yang menghasilkan laporan harian untuk aplikasi analitik seperti dasbor bisnis.

Topik

Ikhtisar titik akhir interaktif

Endpoint interaktif menyediakan kemampuan untuk klien interaktif seperti Amazon EMR Studio untuk terhubung ke Amazon EMR pada kluster EKS untuk menjalankan beban kerja interaktif. Endpoint interaktif didukung oleh Jupyter Enterprise Gateway yang menyediakan kemampuan manajemen siklus hidup kernel jarak jauh yang dibutuhkan klien interaktif. Kernel adalah proses khusus bahasa yang berinteraksi dengan klien Amazon EMR Studio berbasis Jupyter untuk menjalankan beban kerja interaktif.

Endpoint interaktif mendukung kernel berikut:

- Python 3
- PySpark di Kubernetes
- Apache Spark dengan Scala

> **Note**
>
> Amazon EMR pada harga EKS berlaku untuk titik akhir dan kernel interaktif. Untuk informasi lebih lanjut, lihat halaman harga Amazon EMR di EKS.

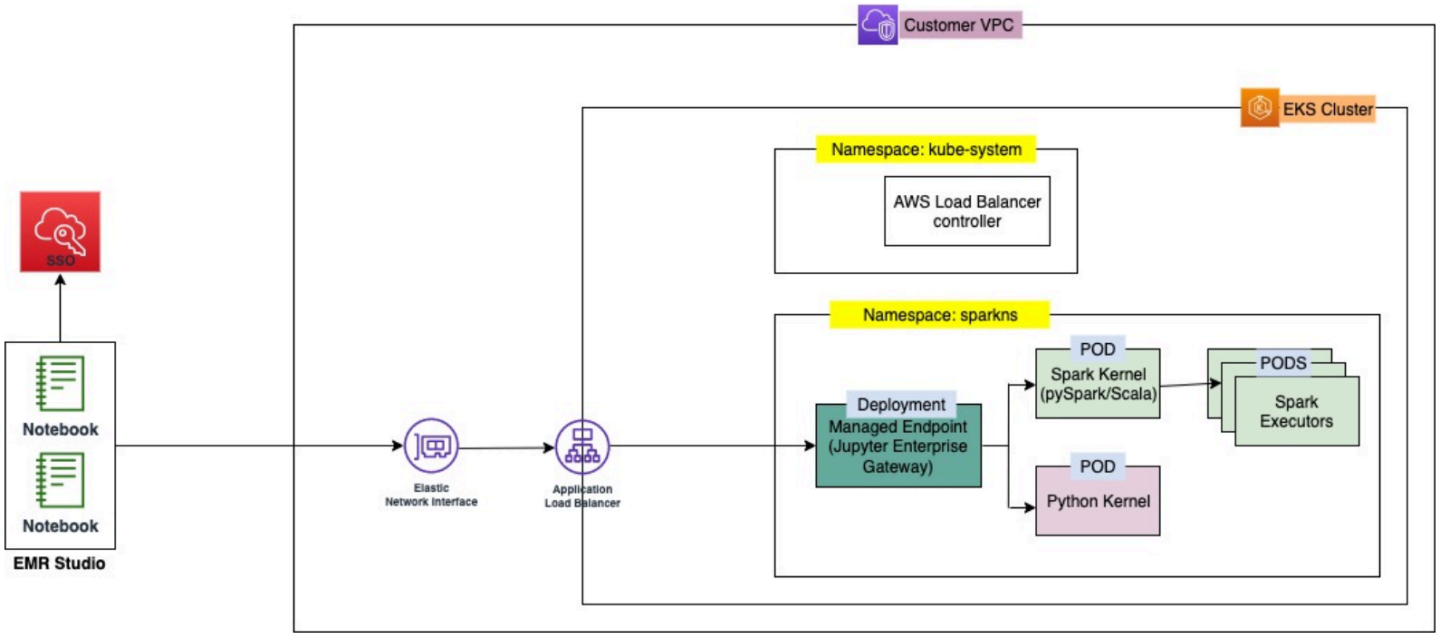
Entitas berikut diperlukan agar EMR Studio terhubung dengan Amazon EMR di EKS.

- Amazon EMR di kluster virtual EKS — Cluster virtual adalah namespace Kubernetes tempat Anda mendaftarkan EMR Amazon. Amazon EMR menggunakan klaster virtual untuk menjalankan tugas dan meng-host titik akhir. Anda dapat mendukung beberapa cluster virtual dengan cluster fisik yang sama. Namun, setiap cluster virtual memetakan ke satu namespace di cluster Amazon EKS. Cluster virtual tidak membuat sumber daya aktif apa pun yang berkontribusi pada tagihan Anda atau yang memerlukan manajemen siklus hidup di luar layanan.
- Amazon EMR pada titik akhir interaktif EKS - Titik akhir interaktif adalah titik akhir HTTPS tempat pengguna EMR Studio dapat menghubungkan ruang kerja. Anda hanya dapat mengakses titik akhir HTTPS dari EMR Studio Anda, dan Anda membuatnya di subnet pribadi Amazon Virtual Private Cloud (Amazon VPC) untuk kluster Amazon EKS Anda.

  Kernel Python, PySpark, dan Spark Scala menggunakan izin yang ditentukan dalam EMR Amazon Anda pada peran eksekusi pekerjaan EKS untuk memanggil yang lain. Layanan AWS Semua kernel dan pengguna yang terhubung ke endpoint interaktif menggunakan peran yang Anda tentukan saat membuat endpoint. Kami menyarankan Anda membuat titik akhir terpisah untuk pengguna yang berbeda, dan bahwa pengguna memiliki peran AWS Identity and Access Management (IAM) yang berbeda.
- AWSPengontrol Application Load Balancer — Pengontrol AWS Application Load Balancer mengelola Elastic Load Balancing untuk klaster Amazon EKS Kubernetes. Controller menyediakan Application Load Balancer (ALB) saat Anda membuat resource Kubernetes Ingress. ALB mengekspos layanan Kubernetes, seperti endpoint interaktif, di luar klaster Amazon EKS tetapi dalam VPC Amazon yang sama. Saat Anda membuat titik akhir interaktif, sumber daya Ingress juga digunakan yang mengekspos titik akhir interaktif melalui ALB untuk terhubung dengan klien

interaktif. Anda hanya perlu menginstal satu AWS Application Load Balancer controller untuk setiap cluster Amazon EKS.

Diagram berikut menggambarkan arsitektur endpoint interaktif di Amazon EMR di EKS. Cluster Amazon EKS terdiri dari komputasi untuk menjalankan beban kerja analitik, dan titik akhir interaktif. Pengontrol Application Load Balancer berjalan di `kube-system` namespace; beban kerja dan titik akhir interaktif berjalan di namespace yang Anda tentukan saat Anda membuat cluster virtual. Saat Anda membuat titik akhir interaktif, EMR Amazon pada bidang kontrol EKS membuat penerapan titik akhir interaktif di klaster Amazon EKS. Selain itu, instance dari ingress penyeimbang beban aplikasi dibuat oleh pengontrol penyeimbang AWS beban. Penyeimbang beban aplikasi menyediakan antarmuka eksternal untuk klien seperti EMR Studio untuk terhubung ke cluster EMR Amazon dan menjalankan beban kerja interaktif.



Prasyarat untuk membuat titik akhir interaktif di Amazon EMR di EKS

Bagian ini menjelaskan prasyarat untuk menyiapkan titik akhir interaktif yang dapat digunakan EMR Studio untuk terhubung ke EMR Amazon di kluster EKS dan menjalankan beban kerja interaktif.

AWS CLI

Ikuti langkah-langkah Instal AWS CLI untuk menginstal versi terbaru dari AWS Command Line Interface (AWS CLI).

Instalasi eksctl

Ikuti langkah-langkah Instal `eksctl` untuk menginstal versi terbaru eksctl. Jika Anda menggunakan Kubernetes versi 1.22 atau yang lebih baru untuk klaster Amazon EKS Anda, gunakan versi eksctl yang lebih besar dari 0.117.0.

Klaster Amazon EKS

Buat klaster Amazon EKS. Daftarkan cluster sebagai cluster virtual dengan Amazon EMR di EKS. Berikut ini adalah persyaratan dan pertimbangan untuk cluster ini:

- Cluster harus berada di Amazon Virtual Private Cloud (VPC) yang sama dengan EMR Studio Anda.
- Cluster harus memiliki setidaknya satu subnet pribadi untuk mengaktifkan endpoint interaktif, untuk menautkan repositori berbasis Git, dan untuk meluncurkan Application Load Balancer dalam mode pribadi.
- Harus ada minimal satu subnet privat yang sama antara EMR Studio Anda dan klaster Amazon EKS yang Anda gunakan untuk mendaftarkan klaster virtual Anda. Ini memastikan bahwa endpoint interaktif Anda muncul sebagai opsi di ruang kerja Studio Anda, dan mengaktifkan konektivitas dari Studio ke Application Load Balancer.

  Ada dua metode yang dapat Anda pilih untuk menghubungkan Studio dan kluster Amazon EKS Anda:

  - Buat klaster Amazon EKS dan kaitkan dengan subnet milik EMR Studio Anda.
  - Atau, buat EMR Studio dan tentukan subnet pribadi untuk klaster Amazon EKS Anda.
- Amazon EKS dioptimalkan ARM Amazon Linux AMI tidak didukung untuk Amazon EMR pada titik akhir interaktif EKS.
- Endpoint interaktif bekerja dengan kluster Amazon EKS yang menggunakan versi Kubernetes hingga 1,27.
- Hanya grup simpul terkelola Amazon EKS yang didukung.

Berikan akses Cluster untuk Amazon EMR di EKS

Gunakan langkah-langkah dalam Grant Cluster Access untuk Amazon EMR di EKS untuk memberikan Amazon EMR di EKS akses ke namespace tertentu di cluster Anda.

Aktifkan IRSA di kluster Amazon EKS

Untuk mengaktifkan peran IAM untuk Akun Layanan (IRSA) di klaster Amazon EKS, ikuti langkah-langkah di Aktifkan Peran IAM untuk Akun Layanan (IRSA).

Buat peran eksekusi pekerjaan IAM

Anda harus membuat peran IAM untuk menjalankan beban kerja di Amazon EMR pada titik akhir interaktif EKS. Kami menyebut peran IAM ini sebagai peran eksekusi pekerjaan dalam dokumentasi ini. Peran IAM ini akan ditetapkan ke wadah endpoint interaktif dan kontainer eksekusi aktual yang dibuat saat Anda mengirimkan pekerjaan dengan EMR Studio. Anda memerlukan Nama Sumber Daya Amazon (ARN) dari peran eksekusi pekerjaan Anda untuk Amazon EMR di EKS. Ada dua langkah yang diperlukan untuk ini:

- Buat peran IAM untuk eksekusi pekerjaan.
- Perbarui kebijakan kepercayaan dari peran eksekusi pekerjaan.

Memberikan pengguna akses ke Amazon EMR di EKS

Entitas IAM (pengguna atau peran) yang membuat permintaan untuk membuat titik akhir interaktif juga harus memiliki Amazon `emr-containers` EC2 dan izin berikut. Ikuti langkah-langkah yang dijelaskan Memberikan pengguna akses ke Amazon EMR di EKS untuk memberikan izin ini yang memungkinkan Amazon EMR di EKS membuat, mengelola, dan menghapus grup keamanan yang membatasi lalu lintas masuk ke penyeimbang beban titik akhir interaktif Anda.

`emr-containers`Izin berikut memungkinkan pengguna untuk melakukan operasi endpoint interaktif dasar:

```
"ec2:CreateSecurityGroup",
"ec2:DeleteSecurityGroup",
"ec2:AuthorizeSecurityGroupEgress",
"ec2:AuthorizeSecurityGroupIngress",
"ec2:RevokeSecurityGroupEgress",
"ec2:RevokeSecurityGroupIngress"

"emr-containers:CreateManagedEndpoint",
"emr-containers:ListManagedEndpoints",
"emr-containers:DescribeManagedEndpoint",
"emr-containers:DeleteManagedEndpoint"
```

Daftarkan klaster Amazon EKS dengan Amazon EMR

Siapkan cluster virtual dan petakan ke namespace di klaster Amazon EKS tempat Anda ingin menjalankan pekerjaan Anda. Untuk cluster AWS Fargate -only, gunakan namespace yang sama untuk EMR Amazon di klaster virtual EKS dan profil Fargate.

Untuk informasi tentang pengaturan EMR Amazon di kluster virtual EKS, lihat. Daftarkan klaster Amazon EKS dengan Amazon EMR

Menerapkan AWS Load Balancer Controller ke klaster Amazon EKS

AWSApplication Load Balancer diperlukan untuk klaster Amazon EKS Anda. Anda hanya perlu menyiapkan satu pengontrol Application Load Balancer per kluster Amazon EKS. Untuk informasi tentang cara menyiapkan pengontrol AWS Application Load Balancer, lihat Menginstal add-on Load AWS Balancer Controller di Panduan Pengguna Amazon EKS.

Membuat endpoint interaktif untuk klaster virtual Anda

Halaman ini menjelaskan cara membuat endpoint interaktif menggunakan AWS Command Line Interface (AWS CLI).

Buat endpoint interaktif dengan perintah **`create-managed-endpoint`**

Tentukan parameter dalam `create-managed-endpoint` perintah sebagai berikut. Amazon EMR di EKS mendukung pembuatan endpoint interaktif dengan Amazon EMR rilis 6.7.0 dan yang lebih tinggi.

```
aws emr-containers create-managed-endpoint \
--type JUPYTER_ENTERPRISE_GATEWAY \
--virtual-cluster-id 1234567890abcdef0xxxxxxx \
--name example-endpoint-name \
--execution-role-arn arn:aws:iam::444455556666:role/JobExecutionRole \
--release-label emr-6.9.0-latest \
--configuration-overrides '{
    "applicationConfiguration": [{
        "classification": "spark-defaults",
        "properties": {
            "spark.driver.memory": "2G"
        }
    }],
    "monitoringConfiguration": {
```

```
        "cloudWatchMonitoringConfiguration": {
            "logGroupName": "log_group_name",
            "logStreamNamePrefix": "log_stream_prefix"
        },
        "persistentAppUI": "ENABLED",
        "s3MonitoringConfiguration": {
            "logUri": "s3://my_s3_log_location"
        }
    }
}'
```

Untuk informasi selengkapnya, lihat Parameter untuk membuat endpoint interaktif.

Buat endpoint interaktif dengan parameter tertentu dalam file JSON

1. Buat `create-managed-endpoint-request.json` file dan tentukan parameter yang diperlukan untuk titik akhir Anda, seperti yang ditunjukkan pada file JSON berikut:

```
{
    "name": "MY_TEST_ENDPOINT",
    "virtualClusterId": "MY_CLUSTER_ID",
    "type": "JUPYTER_ENTERPRISE_GATEWAY",
    "releaseLabel": "emr-6.9.0-latest",
    "executionRoleArn": "arn:aws:iam::444455556666:role/JobExecutionRole",
    "configurationOverrides":
    {
        "applicationConfiguration":
        [
            {
                "classification": "spark-defaults",
                "properties":
                {
                    "spark.driver.memory": "8G"
                }
            }
        ],
        "monitoringConfiguration":
        {
            "persistentAppUI": "ENABLED",
            "cloudWatchMonitoringConfiguration":
            {
                "logGroupName": "my_log_group",
                "logStreamNamePrefix": "log_stream_prefix"
```

```
            },
            "s3MonitoringConfiguration":
            {
                "logUri": "s3://my_s3_log_location"
            }
        }
    }
}
```

2. Gunakan `create-managed-endpoint` perintah dengan jalur ke `create-managed-endpoint-request.json` file yang disimpan secara lokal atau di Amazon S3.

```
aws emr-containers create-managed-endpoint \
--cli-input-json  file://./create-managed-endpoint-request.json --region AWS-Region
```

Output dari membuat endpoint interaktif

Anda akan melihat output berikut di terminal. Outputnya mencakup nama dan pengenal titik akhir interaktif baru Anda:

```
{
    "id": "1234567890abcdef0",
    "name": "example-endpoint-name",
    "arn": "arn:aws:emr-containers:us-west-2:111122223333:/
virtualclusters/444455556666/endpoints/444455556666",
    "virtualClusterId": "111122223333xxxxxxxx"
}
```

Running `aws emr-containers create-managed-endpoint` membuat sertifikat yang ditandatangani sendiri yang memungkinkan komunikasi HTTPS antara EMR Studio dan server endpoint interaktif.

Jika Anda menjalankan `create-managed-endpoint` dan belum menyelesaikan prasyarat, Amazon EMR mengembalikan pesan kesalahan dengan tindakan yang harus Anda ambil untuk melanjutkan.

Parameter untuk membuat endpoint interaktif

Topik

- Parameter yang diperlukan untuk titik akhir interaktif

Parameter yang diperlukan untuk titik akhir interaktif

Anda harus menentukan parameter berikut saat membuat endpoint interaktif:

`--type`

Gunakan `JUPYTER_ENTERPRISE_GATEWAY`. Ini adalah satu-satunya jenis yang didukung.

`--virtual-cluster-id`

Pengidentifikasi cluster virtual yang Anda daftarkan dengan Amazon EMR di EKS.

`--name`

Nama deskriptif untuk endpoint interaktif yang membantu pengguna EMR Studio memilihnya dari daftar dropdown.

`--execution-role-arn`

Nama Sumber Daya Amazon (ARN) dari peran eksekusi pekerjaan IAM Anda untuk Amazon EMR di EKS yang dibuat sebagai bagian dari prasyarat.

`--release-label`

Label rilis rilis EMR Amazon untuk digunakan untuk titik akhir. Sebagai contoh, `emr-6.9.0-latest`. Amazon EMR di EKS mendukung endpoint interaktif dengan Amazon EMR rilis 6.7.0 dan lebih tinggi.

Parameter opsional untuk titik akhir interaktif

Secara opsional, Anda juga dapat menentukan parameter berikut saat membuat endpoint interaktif:

`--configuration-overrides`

Untuk mengganti konfigurasi default untuk aplikasi, berikan objek coonfiguration. Anda dapat menggunakan sintaks singkatan untuk menyediakan konfigurasi, atau Anda dapat mereferensikan objek konfigurasi dalam file JSON.

Objek konfigurasi terdiri dari klasifikasi, properti, dan konfigurasi bersarang opsional. Properti terdiri dari pengaturan yang ingin Anda timpa dalam file itu. Anda dapat menentukan beberapa klasifikasi

untuk beberapa aplikasi dalam objek JSON tunggal. Klasifikasi konfigurasi yang tersedia bervariasi menurut Amazon EMR pada rilis EKS. Untuk daftar klasifikasi konfigurasi yang tersedia untuk setiap rilis Amazon EMR di EKS, lihat. Amazon EMR pada rilis EKS Selain klasifikasi konfigurasi yang terdaftar untuk setiap rilis, titik akhir interaktif membawa klasifikasi tambahan. `jeg-config` Untuk informasi selengkapnya, lihat Opsi konfigurasi Jupyter Enterprise Gateway (JEG).

Mengkonfigurasi pengaturan untuk titik akhir interaktif

Lowongan kerja Monitoring Spark

Agar Anda dapat memantau dan memecahkan masalah kegagalan, konfigurasikan titik akhir interaktif Anda sehingga pekerjaan yang dimulai dengan titik akhir dapat mengirim informasi log ke Amazon S3, Amazon Log, atau keduanya. CloudWatch Bagian berikut menjelaskan cara mengirim log aplikasi Spark ke Amazon S3 untuk pekerjaan Spark yang Anda luncurkan dengan Amazon EMR di titik akhir interaktif EKS.

Konfigurasikan kebijakan IAM untuk log Amazon S3

Sebelum kernel Anda dapat mengirim data log ke Amazon S3, kebijakan izin untuk peran eksekusi pekerjaan harus menyertakan izin berikut. Ganti *DOC-EXAMPLE-BUCKET-LOGGING dengan nama bucket logging* Anda.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET-LOGGING",
                "arn:aws:s3:::DOC-EXAMPLE-BUCKET-LOGGING/*",
            ]
        }
    ]
}
```

> **Note**
>
> Amazon EMR di EKS juga dapat membuat bucket S3. Jika bucket S3 tidak tersedia, sertakan `s3:CreateBucket` izin tersebut dalam kebijakan IAM.

Setelah Anda memberikan izin pada peran eksekusi yang diperlukan untuk mengirim log ke bucket S3, data log Anda akan dikirim ke lokasi Amazon S3 berikut. Ini terjadi ketika `s3MonitoringConfiguration` diteruskan di `monitoringConfiguration` bagian `create-managed-endpoint` permintaan.

- Log driver — `logUri/virtual-cluster-id/endpoints/endpoint-id/containers/spark-application-id/spark-application-id-driver/(stderr.gz/stdout.gz)`
- Log pelaksana — `logUri/virtual-cluster-id/endpoints/endpoint-id/containers/spark-application-id/executor-pod-name-exec-<Number>/(stderr.gz/stdout.gz)`

> **Note**
>
> Amazon EMR di EKS tidak mengunggah log titik akhir ke bucket S3 Anda.

Menentukan template pod kustom dengan endpoint interaktif

Anda dapat membuat endpoint interaktif di mana Anda menentukan template pod kustom untuk driver dan pelaksana. Template Pod adalah spesifikasi yang menentukan cara menjalankan setiap pod. Anda dapat menggunakan file template pod untuk menentukan konfigurasi driver atau pod pelaksana yang tidak didukung oleh konfigurasi Spark. Template Pod saat ini didukung di Amazon EMR rilis 6.3.0 dan yang lebih baru.

Untuk informasi selengkapnya tentang template pod, lihat Menggunakan templat pod di Amazon EMR on EKS Development Guide.

Contoh berikut menunjukkan cara membuat endpoint interaktif dengan template pod:

```
aws emr-containers create-managed-endpoint \
    --type JUPYTER_ENTERPRISE_GATEWAY \
    --virtual-cluster-id virtual-cluster-id \
```

```
    --name example-endpoint-name \
    --execution-role-arn arn:aws:iam::aws-account-id:role/EKSClusterRole \
    --release-label emr-6.9.0-latest \
    --configuration-overrides '{
        "applicationConfiguration": [
        {
            "classification": "spark-defaults",
            "properties": {
                "spark.kubernetes.driver.podTemplateFile": "path/to/driver/
template.yaml",
                "spark.kubernetes.executor.podTemplateFile": "path/to/executor/
template.yaml"
            }
        }]
    }'
```

Menerapkan pod JEG ke grup node

Penempatan pod JEG (Jupyter Enterprise Gateway) adalah fitur yang memungkinkan Anda untuk menerapkan endpoint interaktif pada grup node tertentu. Dengan fitur ini, Anda dapat mengonfigurasi pengaturan seperti `instance type` untuk titik akhir interaktif.

Mengaitkan pod JEG ke grup node terkelola

Properti konfigurasi berikut memungkinkan Anda menentukan nama grup node terkelola di klaster Amazon EKS tempat pod JEG akan di-deploy.

```
//payload
--configuration-overrides '{
      "applicationConfiguration": [
            {
                "classification": "endpoint-configuration",
                "properties": {
                    "managed-nodegroup-name": NodeGroupName
                }
            }
        ]
    }'
```

Sebuah grup node harus memiliki label Kubernetes yang `for-use-with-emr-containers-managed-endpoint-ng=`*NodeGroupName* melekat pada semua node yang merupakan bagian dari

grup node. Untuk membuat daftar semua node dari grup node yang memiliki tag ini, gunakan perintah berikut:

```
kubectl get nodes --show-labels | grep for-use-with-emr-containers-managed-endpoint-ng=NodeGroupName
```

Jika output dari perintah di atas tidak mengembalikan node yang merupakan bagian dari grup node terkelola Anda, maka tidak ada node dalam grup node yang memiliki label `for-use-with-emr-containers-managed-endpoint-ng=`*`NodeGroupName`* Kubernetes terpasang. Dalam hal ini, ikuti langkah-langkah di bawah ini untuk melampirkan label tersebut ke node di grup node Anda.

1. Gunakan perintah berikut untuk menambahkan label `for-use-with-emr-containers-managed-endpoint-ng=`*`NodeGroupName`* Kubernetes ke semua node dalam grup node terkelola: *`NodeGroupName`*

   ```
   kubectl label nodes --selector eks:nodegroup-name=NodeGroupName for-use-with-emr-containers-managed-endpoint-ng=NodeGroupName
   ```

2. Verifikasi bahwa node diberi label dengan benar menggunakan perintah berikut:

   ```
   kubectl get nodes --show-labels | grep for-use-with-emr-containers-managed-endpoint-ng=NodeGroupName
   ```

Grup node terkelola harus dikaitkan dengan grup keamanan klaster Amazon EKS, yang biasanya terjadi jika Anda membuat cluster dan grup node terkelola menggunakan`eksctl`. Anda dapat memverifikasi ini di AWS konsol menggunakan langkah-langkah berikut.

1. Buka cluster Anda di konsol Amazon EKS.
2. Buka tab jaringan cluster Anda dan catat grup keamanan cluster.
3. Buka tab komputasi klaster Anda dan klik pada nama grup node terkelola.
4. Di bawah tab Detail grup node terkelola, verifikasi bahwa grup keamanan klaster yang Anda catat sebelumnya terdaftar di bawah Grup keamanan.

Jika grup node terkelola tidak dilampirkan ke grup keamanan klaster Amazon EKS, Anda harus melampirkan `for-use-with-emr-containers-managed-endpoint-sg=`*`ClusterName`*`/`*`NodeGroupName`* tag ke grup keamanan grup node. Gunakan langkah-langkah di bawah ini untuk melampirkan tag ini.

1. Buka konsol Amazon EC2 dan klik grup keamanan di panel navigasi kiri.
2. Pilih grup keamanan grup node terkelola Anda dengan mengklik kotak centang.
3. Di bawah tab Tag, tambahkan tag `for-use-with-emr-containers-managed-endpoint-sg=`*`ClusterName`*`/`*`NodeGroupName`* menggunakan tombol Kelola tag.

Mengaitkan pod JEG ke grup node yang dikelola sendiri

Properti konfigurasi berikut memungkinkan Anda menentukan nama grup node yang dikelola sendiri atau tidak dikelola di klaster Amazon EKS tempat pod JEG akan di-deploy.

```
//payload
--configuration-overrides '{
      "applicationConfiguration": [
            {
                "classification": "endpoint-configuration",
                "properties": {
                    "self-managed-nodegroup-name": NodeGroupName
                }
            }
        ]
    }'
```

Grup node harus memiliki label `for-use-with-emr-containers-managed-endpoint-ng=`*`NodeGroupName`* Kubernetes yang melekat pada semua node yang merupakan bagian dari grup node. Untuk membuat daftar semua node dari grup node yang memiliki tag ini, gunakan perintah berikut:

```
kubectl get nodes --show-labels | grep for-use-with-emr-containers-managed-endpoint-ng=NodeGroupName
```

Jika output dari perintah di atas tidak mengembalikan node yang merupakan bagian dari grup node yang dikelola sendiri, maka tidak ada node di grup node yang memiliki label `for-use-with-emr-containers-managed-endpoint-ng=`*`NodeGroupName`* Kubernetes yang terpasang. Dalam hal ini, ikuti langkah-langkah di bawah ini untuk melampirkan label tersebut ke node di grup node Anda.

1. Jika Anda membuat grup node yang dikelola sendiri menggunakan`eksctl`, maka gunakan perintah berikut untuk menambahkan label `for-use-with-emr-containers-managed-endpoint-ng=`*`NodeGroupName`* Kubernetes ke semua node dalam grup node yang dikelola sendiri sekaligus. *`NodeGroupName`*

```
kubectl label nodes --selector alpha.eksctl.io/nodegroup-name=NodeGroupName for-use-with-emr-containers-managed-endpoint-ng=NodeGroupName
```

Jika Anda tidak menggunakannya `eksctl` untuk membuat grup node yang dikelola sendiri, maka Anda perlu mengganti pemilih pada perintah di atas ke label Kubernetes yang berbeda yang dilampirkan ke semua node dari grup node.

2. Gunakan perintah berikut untuk memverifikasi bahwa node diberi label dengan benar:

```
kubectl get nodes --show-labels | grep for-use-with-emr-containers-managed-endpoint-ng=NodeGroupName
```

Grup keamanan untuk grup node yang dikelola sendiri harus memiliki `for-use-with-emr-containers-managed-endpoint-sg=`*`ClusterName`*`/`*`NodeGroupName` tag yang dilampirkan. Gunakan langkah-langkah berikut untuk melampirkan tag ke grup keamanan dariAWS Management Console.

1. Arahkan ke konsol Amazon EC2. Pilih Grup keamanan di panel navigasi kiri.
2. Pilih kotak centang di samping grup keamanan untuk grup node yang dikelola sendiri.
3. Di bawah tab Tag, gunakan tombol Kelola tag untuk menambahkan tag`for-use-with-emr-containers-managed-endpoint-sg=`*`ClusterName`*`/`*`NodeGroupName`*. Ganti *`ClusterName`* dan *`NodeGroupName`* dengan nilai yang sesuai.

Mengaitkan pod JEG ke grup node terkelola dengan instans On-Demand

Anda juga dapat menentukan label tambahan, yang dikenal sebagai pemilih label Kubernetes, untuk menentukan batasan atau batasan tambahan untuk menjalankan titik akhir interaktif pada node atau grup node tertentu. Contoh berikut menunjukkan cara menggunakan instans Amazon EC2 On-Demand untuk pod JEG.

```
--configuration-overrides '{
      "applicationConfiguration": [
            {
                "classification": "endpoint-configuration",
                "properties": {
                    "managed-nodegroup-name": NodeGroupName,
                    "node-labels": "eks.amazonaws.com/capacityType:ON_DEMAND"
```

```
            }
        }
    ]
}'
```

> **Note**
>
> Anda hanya dapat menggunakan `node-labels` properti dengan `self-managed-nodegroup-name` properti `managed-nodegroup-name` atau properti.

Opsi konfigurasi Jupyter Enterprise Gateway (JEG)

Amazon EMR di EKS menggunakan Jupyter Enterprise Gateway (JEG) untuk mengaktifkan endpoint interaktif. Anda dapat mengatur nilai berikut untuk konfigurasi JEG yang diizinkan saat Anda membuat titik akhir.

- **`RemoteMappingKernelManager.cull_idle_timeout`**— Timeout dalam hitungan detik (integer), setelah itu kernel dianggap idle dan siap untuk dimusnahkan. Nilai `0` atau lebih rendah menonaktifkan pemusnahan. Batas waktu yang singkat dapat mengakibatkan kernel dimusnahkan untuk pengguna dengan koneksi jaringan yang buruk.
- **`RemoteMappingKernelManager.cull_interval`**— Interval dalam detik (integer) untuk memeriksa kernel idle yang melebihi nilai batas waktu pemusnahan.

Memodifikasi PySpark parameter sesi

Dimulai dengan Amazon EMR pada rilis EKS 6.9.0, di Amazon EMR Studio Anda dapat menyesuaikan konfigurasi Spark yang terkait dengan PySpark sesi dengan menjalankan perintah `%%configure` ajaib di sel notebook EMR.

Contoh berikut menunjukkan payload sampel yang dapat Anda gunakan untuk memodifikasi memori, core, dan properti lainnya untuk driver dan eksekutor Spark. Untuk `conf` pengaturan, Anda dapat mengonfigurasi konfigurasi Spark apa pun yang disebutkan dalam dokumentasi konfigurasi Apache Spark.

```
%%configure -f
{
  "driverMemory": "16G",
```

```
  "driverCores" 4,
  "executorMemory" : "32G"
  "executorCores": 2,
  "conf": {
     "spark.dynamicAllocation.maxExecutors" : 10,
     "spark.dynamicAllocation.minExecutors": 1
  }
}
```

Contoh berikut menunjukkan contoh payload yang dapat Anda gunakan untuk menambahkan file, PyFiles, dan dependensi jar ke runtime Spark.

```
%%configure -f
{
  "files": "s3://test-bucket-emr-eks/sample_file.txt",
  "pyFiles": : "path-to-python-files",
  "jars" : "path-to-jars
}
```

Gambar kernel kustom dengan endpoint interaktif

Untuk memastikan bahwa Anda memiliki dependensi yang benar untuk aplikasi saat menjalankan beban kerja interaktif dari Amazon EMR Studio, Anda dapat menyesuaikan gambar Docker untuk titik akhir interaktif dan menjalankan image kernel dasar yang disesuaikan. Untuk membuat endpoint interaktif dan menghubungkannya dengan image Docker kustom, lakukan langkah-langkah berikut.

> **Note**
>
> Anda hanya dapat mengganti gambar dasar. Anda tidak dapat menambahkan jenis gambar kernel baru.

1. Buat dan publikasikan gambar Docker yang disesuaikan. Gambar dasar berisi runtime Spark dan kernel notebook yang berjalan dengannya. Untuk membuat gambar, Anda dapat mengikuti langkah 1 hingga 4 inCara menyesuaikan gambar Docker. Pada langkah 1, URI gambar dasar dalam file Docker Anda harus digunakan `notebook-spark` sebagai pengganti. `spark`

   ```
   ECR-registry-account.dkr.ecr.Region.amazonaws.com/notebook-spark/container-image-tag
   ```

Untuk informasi selengkapnya tentang cara memilih Wilayah AWS dan menampung tag gambar, lihatCara memilih URI gambar dasar.

2. Buat endpoint interaktif yang dapat digunakan dengan gambar kustom.

   a. Buat file JSON `custom-image-managed-endpoint.json` dengan konten berikut. Contoh ini menggunakan Amazon EMR rilis 6.9.0.

      Example

```
{
    "name": "endpoint-name",
    "virtualClusterId": "virtual-cluster-id",
    "type": "JUPYTER_ENTERPRISE_GATEWAY",
    "releaseLabel": "emr-6.9.0-latest",
    "executionRoleArn": "execution-role-arn",
    "configurationOverrides": {
        "applicationConfiguration": [
            {
                "classification": "jupyter-kernel-overrides",
                "configurations": [
                    {
                        "classification": "python3",
                        "properties": {
                            "container-image": "123456789012.dkr.ecr.us-
west-2.amazonaws.com/custom-notebook-python:latest"
                        }
                    },
                    {
                        "classification": "spark-python-kubernetes",
                        "properties": {
                            "container-image": "123456789012.dkr.ecr.us-
west-2.amazonaws.com/custom-notebook-spark:latest"
                        }
                    }
                ]
            }
        ]
    }
}
```

b. Buat endpoint interaktif dengan konfigurasi yang ditentukan dalam file JSON seperti yang ditunjukkan pada contoh berikut. Untuk informasi selengkapnya, lihat Buat endpoint interaktif dengan perintah `create-managed-endpoint`.

```
aws emr-containers create-managed-endpoint --cli-input-json custom-image-
managed-endpoint.json
```

3. Connect ke endpoint interaktif melalui EMR Studio. Untuk informasi selengkapnya dan langkah-langkah yang harus diselesaikan, lihat Menghubungkan dari Studio di bagian Amazon EMR di EKS pada dokumen AWS Workshop Studio.

Memantau titik akhir interaktif

Dengan Amazon EMR di EKS versi 6.10 dan yang lebih baru, titik akhir interaktif memancarkan metrik CloudWatch Amazon untuk memantau dan memecahkan masalah operasi siklus hidup kernel. Metrik dipicu oleh klien interaktif, seperti EMR Studio atau notebook Jupyter yang dihosting sendiri. Setiap operasi yang didukung oleh endpoint interaktif memiliki metrik yang terkait dengannya. Operasi dimodelkan sebagai dimensi untuk setiap metrik, seperti yang ditunjukkan pada tabel di bawah ini. Metrik yang dipancarkan oleh titik akhir interaktif terlihat di bawah namespace khusus, EMRContainers, di akun Anda.

Metrik	Deskripsi	Unit
RequestCount	Jumlah kumulatif permintaan operasi yang diproses oleh endpoint interaktif.	Hitungan
RequestLatency	Waktu dari ketika permintaan tiba di titik akhir interaktif dan respons dikirim oleh titik akhir interaktif.	Milidetik
4XXError	Dipancarkan ketika permintaan untuk operasi menghasilkan kesalahan 4xx selama pemrosesan.	Hitungan

Metrik	Deskripsi	Unit
5XXError	Dipancarkan saat permintaan operasi menghasilkan kesalahan sisi server 5Xxx.	Hitungan
KernelLaunchSuccess	Hanya berlaku untuk CreateKernel operasi. Ini menunjukkan jumlah kumulatif peluncuran kernel yang berhasil hingga dan termasuk permintaan ini.	Hitungan
KernelLaunchFailure	Hanya berlaku untuk CreateKernel operasi. Ini menunjukkan jumlah kumulatif kegagalan peluncuran kernel hingga dan termasuk permintaan ini.	Hitungan

Setiap metrik endpoint interaktif memiliki dimensi berikut yang melekat padanya:

- **`ManagedEndpointId`**— Pengidentifikasi untuk titik akhir interaktif
- **`OperationName`**— Operasi yang dipicu oleh klien interaktif

Nilai yang mungkin untuk **`OperationName`**dimensi ditunjukkan pada tabel berikut:

`operationName`	Deskripsi operasi
`CreateKernel`	Minta endpoint interaktif memulai kernel.
`ListKernels`	Minta agar titik akhir interaktif mencantumkan kernel yang sebelumnya telah dimulai menggunakan token sesi yang sama.

operationName	Deskripsi operasi
`GetKernel`	Minta agar endpoint interaktif mendapatkan detail tentang kernel tertentu yang telah dimulai sebelumnya.
`ConnectKernel`	Minta endpoint interaktif membangun konektivitas antara klien notebook dan kernel.
`ConfigureKernel`	Publikasikan `%%configure magic request` pada kernel pyspark.
`ListKernelSpecs`	Minta agar titik akhir interaktif mencantumkan spesifikasi kernel yang tersedia.
`GetKernelSpec`	Minta agar endpoint interaktif mendapatkan spesifikasi kernel dari kernel yang telah diluncurkan sebelumnya.
`GetKernelSpecResource`	Minta agar endpoint interaktif mendapatkan sumber daya spesifik yang terkait dengan spesifikasi kernel yang telah diluncurkan sebelumnya.

Contoh

Untuk mengakses jumlah kernel yang diluncurkan untuk titik akhir interaktif pada hari tertentu:

1. Pilih namespace kustom: `EMRContainers`
2. Pilih Anda`ManagedEndpointId`, `OperationName - CreateKernel`
3. `RequestCount`metrik dengan statistik `SUM` dan periode `1 day` akan memberikan semua permintaan peluncuran kernel yang dibuat dalam 24 jam terakhir.
4. KernelLaunchSuccess metrik dengan statistik `SUM` dan periode `1 day` akan memberikan semua permintaan peluncuran kernel yang berhasil dibuat dalam 24 jam terakhir.

Untuk mengakses jumlah kegagalan kernel untuk endpoint interaktif pada hari tertentu:

1. Pilih namespace kustom: EMRContainers
2. Pilih Anda`ManagedEndpointId`, `OperationName - CreateKernel`
3. `KernelLaunchFailure`metrik dengan statistik `SUM` dan periode `1 day` akan memberikan semua permintaan peluncuran kernel gagal yang dibuat dalam 24 jam terakhir. Anda juga dapat memilih `5XXError` metrik `4XXError` dan untuk mengetahui jenis kegagalan peluncuran kernel yang terjadi.

Menggunakan notebook Jupyter yang dihosting sendiri

Anda dapat meng-host dan mengelola Jupyter atau JupyterLab notebook di instans Amazon EC2 atau di cluster Amazon EKS Anda sendiri sebagai notebook Jupyter yang dihosting sendiri. Anda kemudian dapat menjalankan beban kerja interaktif dengan notebook Jupyter yang dihosting sendiri. Bagian berikut berjalan melalui proses untuk menyiapkan dan menerapkan notebook Jupyter yang dihosting sendiri di cluster Amazon EKS.

Membuat notebook Jupyter yang dihosting sendiri di cluster EKS

- Membuat grup keamanan
- Buat EMR Amazon di titik akhir interaktif EKS
- Ambil URL server gateway dari titik akhir interaktif Anda
- Ambil token autentikasi untuk terhubung ke titik akhir interaktif
- Contoh: Menyebarkan buku catatan JupyterLab
- Menghapus buku catatan Jupyter yang dihosting sendiri

Membuat grup keamanan

Sebelum Anda dapat membuat endpoint interaktif dan menjalankan Jupyter atau JupyterLab notebook yang dihosting sendiri, Anda harus membuat grup keamanan untuk mengontrol lalu lintas antara buku catatan Anda dan titik akhir interaktif. Untuk menggunakan konsol Amazon EC2 atau Amazon EC2 SDK untuk membuat grup keamanan, lihat langkah-langkah dalam Membuat grup keamanan di Panduan Pengguna Amazon EC2 untuk Instans Linux. Anda harus membuat grup keamanan di VPC tempat Anda ingin menyebarkan server notebook Anda.

Untuk mengikuti contoh dalam panduan ini, gunakan VPC yang sama dengan cluster Amazon EKS Anda. Jika Anda ingin meng-host notebook Anda di VPC yang berbeda dari VPC untuk cluster Amazon EKS Anda, Anda mungkin perlu membuat koneksi peering antara kedua VPC tersebut. Untuk langkah-langkah untuk membuat koneksi peering antara dua VPC, lihat Membuat koneksi peering VPC di Panduan Memulai VPC Amazon.

Anda memerlukan ID untuk grup keamanan untuk membuat EMR Amazon di titik akhir interaktif EKS di langkah berikutnya.

Buat EMR Amazon di titik akhir interaktif EKS

Setelah Anda membuat grup keamanan untuk buku catatan Anda, gunakan langkah-langkah yang disediakan Membuat endpoint interaktif untuk klaster virtual Anda untuk membuat titik akhir interaktif. Anda harus memberikan ID grup keamanan yang Anda buat untuk buku catatan AndaMembuat grup keamanan.

Masukkan ID keamanan sebagai pengganti *your-notebook-security-group-id* dalam pengaturan penggantian konfigurasi berikut:

```
--configuration-overrides '{
    "applicationConfiguration": [
        {
            "classification": "endpoint-configuration",
            "properties": {
                "notebook-security-group-id": "your-notebook-security-group-id"
            }
        }
    ],
    "monitoringConfiguration": {
    ...'
```

Ambil URL server gateway dari titik akhir interaktif Anda

Setelah Anda membuat endpoint interaktif, ambil URL server gateway dengan `describe-managed-endpoint` perintah di. AWS CLI Anda memerlukan URL ini untuk menghubungkan buku catatan Anda ke titik akhir. URL server gateway adalah titik akhir pribadi.

```
aws emr-containers describe-managed-endpoint \
--region region \
--virtual-cluster-id virtualClusterId \
```

```
--id endpointId
```

Awalnya, titik akhir Anda ada di CREATINGnegara bagian. Setelah beberapa menit, ia beralih ke ACTIVEnegara. Ketika titik akhir ACTIVE, itu siap digunakan.

Perhatikan `serverUrl` atribut yang dikembalikan `aws emr-containers describe-managed-endpoint` perintah dari endpoint aktif. Anda memerlukan URL ini untuk menghubungkan buku catatan Anda ke titik akhir saat Anda menerapkan Jupyter atau notebook yang dihosting sendiri. JupyterLab

Ambil token autentikasi untuk terhubung ke titik akhir interaktif

Untuk terhubung ke endpoint interaktif dari Jupyter atau JupyterLab notebook, Anda harus membuat token sesi dengan API. `GetManagedEndpointSessionCredentials` Token bertindak sebagai bukti otentikasi untuk terhubung ke server endpoint interaktif.

Perintah berikut dijelaskan secara lebih rinci dengan contoh output di bawah ini.

```
aws emr-containers get-managed-endpoint-session-credentials \
--endpoint-identifier endpointArn \
--virtual-cluster-identifier virtualClusterArn \
--execution-role-arn executionRoleArn \
--credential-type "TOKEN" \
--duration-in-seconds durationInSeconds \
--region region
```

endpointArn

ARN dari titik akhir Anda. Anda dapat menemukan ARN dalam hasil panggilan`describe-managed-endpoint`.

virtualClusterArn

ARN dari cluster virtual.

executionRoleArn

ARN dari peran eksekusi.

durationInSeconds

Durasi dalam detik dimana token valid. Durasi default adalah 15 menit (`900`), dan maksimum adalah 12 jam (`43200`).

region

Wilayah yang sama dengan titik akhir Anda.

Output Anda harus menyerupai contoh berikut. Catat *session-token* nilai yang akan Anda gunakan saat menerapkan Jupyter atau notebook yang dihosting sendiri. JupyterLab

```
{
    "id": "credentialsId",
    "credentials": {
        "token": "session-token"
    },
    "expiresAt": "2022-07-05T17:49:38Z"
}
```

Contoh: Menyebarkan buku catatan JupyterLab

Setelah Anda menyelesaikan langkah-langkah di atas, Anda dapat mencoba prosedur contoh ini untuk menyebarkan JupyterLab notebook ke cluster Amazon EKS dengan endpoint interaktif Anda.

1. Buat namespace untuk menjalankan server notebook.
2. Buat file secara lokal,`notebook.yaml`, dengan konten berikut. Isi file dijelaskan di bawah ini.

```
apiVersion: v1
kind: Pod
metadata:
  name: jupyter-notebook
  namespace: namespace
spec:
  containers:
  - name: minimal-notebook
    image: jupyter/all-spark-notebook:lab-3.1.4 # open source image
    ports:
    - containerPort: 8888
    command: ["start-notebook.sh"]
    args: ["--LabApp.token=''"]
    env:
    - name: JUPYTER_ENABLE_LAB
      value: "yes"
    - name: KERNEL_LAUNCH_TIMEOUT
      value: "400"
```

```
    - name: JUPYTER_GATEWAY_URL
      value: "serverUrl"
    - name: JUPYTER_GATEWAY_VALIDATE_CERT
      value: "false"
    - name: JUPYTER_GATEWAY_AUTH_TOKEN
      value: "session-token"
```

Jika Anda menerapkan notebook Jupyter ke cluster khusus Fargate, beri label pada pod Jupyter dengan label seperti yang ditunjukkan pada contoh berikut: `role`

```
...
metadata:
  name: jupyter-notebook
  namespace: default
  labels:
    role: example-role-name-label
spec:
            ...
```

namespace

Namespace Kubernetes yang digunakan notebook.

serverUrl

`serverUrl`Atribut yang dikembalikan `describe-managed-endpoint` perintahAmbil URL server gateway dari titik akhir interaktif Anda .

session-token

`session-token`Atribut yang dikembalikan `get-managed-endpoint-session-credentials` perintahAmbil token autentikasi untuk terhubung ke titik akhir interaktif.

KERNEL_LAUNCH_TIMEOUT

Jumlah waktu dalam hitungan detik titik akhir interaktif menunggu kernel muncul. RUNNING Pastikan waktu yang cukup untuk menyelesaikan peluncuran kernel dengan mengatur batas waktu peluncuran kernel ke nilai yang sesuai (maksimum 400 detik).

KERNEL_EXTRA_SPARK_OPTS

Secara opsional, Anda dapat meneruskan konfigurasi Spark tambahan untuk kernel Spark. Tetapkan variabel lingkungan ini dengan nilai-nilai sebagai properti konfigurasi Spark seperti yang ditunjukkan pada contoh berikut:

```
- name: KERNEL_EXTRA_SPARK_OPTS
  value: "--conf spark.driver.cores=2
          --conf spark.driver.memory=2G
          --conf spark.executor.instances=2
          --conf spark.executor.cores=2
          --conf spark.executor.memory=2G
          --conf spark.dynamicAllocation.enabled=true
          --conf spark.dynamicAllocation.shuffleTracking.enabled=true
          --conf spark.dynamicAllocation.minExecutors=1
          --conf spark.dynamicAllocation.maxExecutors=5
          --conf spark.dynamicAllocation.initialExecutors=1
          "
```

3. Menerapkan spesifikasi pod ke cluster Amazon EKS Anda:

```
kubectl apply -f notebook.yaml -n namespace
```

Ini akan memulai JupyterLab notebook minimal yang terhubung ke EMR Amazon Anda di titik akhir interaktif EKS. Tunggu sampai pod itu RUNNING. Anda dapat memeriksa statusnya dengan perintah berikut:

```
kubectl get pod jupyter-notebook -n namespace
```

Ketika pod siap, `get pod` perintah mengembalikan output yang mirip dengan ini:

```
NAME              READY   STATUS    RESTARTS   AGE
jupyter-notebook  1/1     Running   0          46s
```

4. Lampirkan grup keamanan notebook ke node tempat notebook dijadwalkan.

   a. Pertama, identifikasi node tempat `jupyter-notebook` pod dijadwalkan dengan `describe` pod perintah.

   ```
   kubectl describe pod jupyter-notebook -n namespace
   ```

b. Buka konsol Amazon EKS di https://console.aws.amazon.com/eks/home#/clusters.

c. Arahkan ke tab Compute untuk cluster Amazon EKS Anda dan pilih node yang diidentifikasi oleh `describe pod` perintah. Pilih ID instance untuk node.

d. Dari menu Tindakan, pilih Keamanan > Ubah grup keamanan untuk melampirkan grup keamanan yang Anda buatMembuat grup keamanan.

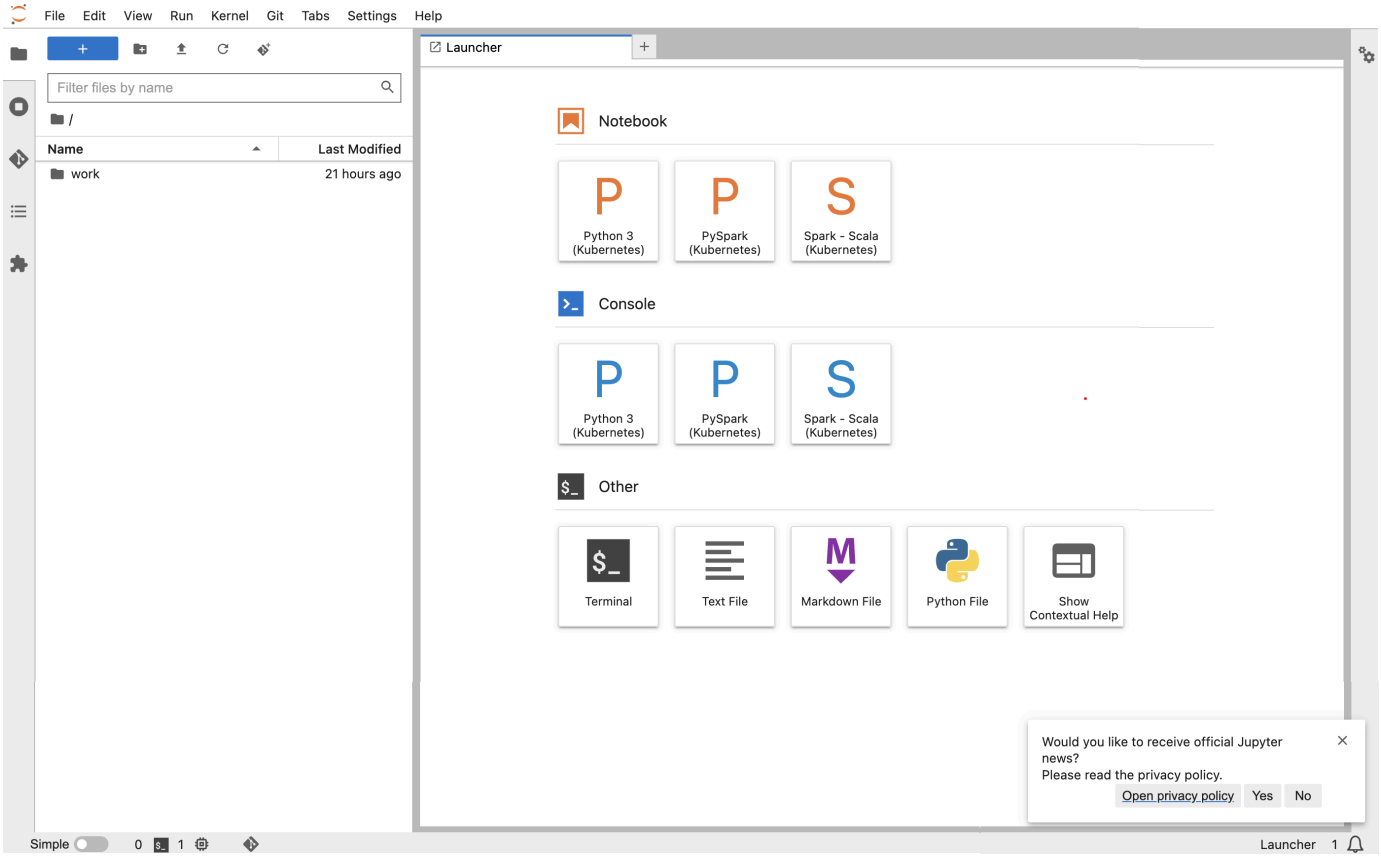
e. Jika Anda menerapkan pod notebook JupyterAWS Fargate, buat a `SecurityGroupPolicy`to apply ke pod notebook Jupyter dengan label peran:

```
cat >my-security-group-policy.yaml <<EOF
apiVersion: vpcresources.k8s.aws/v1beta1
kind: SecurityGroupPolicy
metadata:
  name: example-security-group-policy-name
  namespace: default
spec:
  podSelector:
    matchLabels:
      role: example-role-name-label
  securityGroups:
    groupIds:
      - your-notebook-security-group-id
EOF
```

5. Sekarang, port-forward sehingga Anda dapat mengakses antarmuka secara lokal: JupyterLab

```
kubectl port-forward jupyter-notebook 8888:8888 -n namespace
```

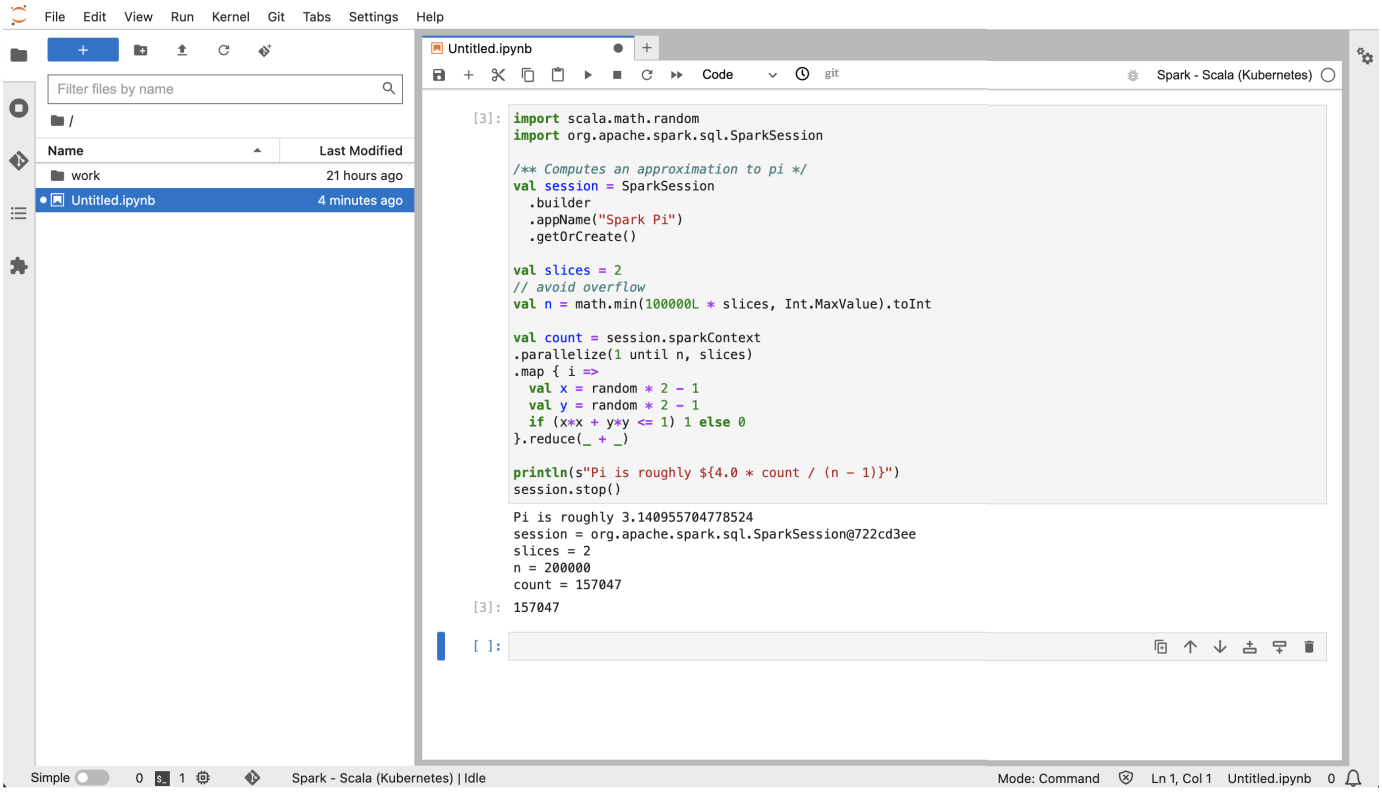
Setelah berjalan, navigasikan ke browser lokal Anda dan kunjungi `localhost:8888` untuk melihat JupyterLab antarmuka:



6. Dari JupyterLab, buat notebook Scala baru. Berikut adalah contoh cuplikan kode yang dapat Anda jalankan untuk memperkirakan nilai Pi:

```
import scala.math.random
import org.apache.spark.sql.SparkSession

/** Computes an approximation to pi */
val session = SparkSession
  .builder
  .appName("Spark Pi")
  .getOrCreate()

val slices = 2
// avoid overflow
val n = math.min(100000L * slices, Int.MaxValue).toInt

val count = session.sparkContext
.parallelize(1 until n, slices)
.map { i =>
  val x = random * 2 - 1
  val y = random * 2 - 1
```

```
  if (x*x + y*y <= 1) 1 else 0
}.reduce(_ + _)

println(s"Pi is roughly ${4.0 * count / (n - 1)}")
session.stop()
```



Menghapus buku catatan Jupyter yang dihosting sendiri

Saat Anda siap untuk menghapus buku catatan yang dihosting sendiri, Anda juga dapat menghapus titik akhir interaktif dan grup keamanan juga. Lakukan tindakan dengan urutan sebagai berikut:

1. Gunakan perintah berikut untuk menghapus `jupyter-notebook` pod:

   ```
   kubectl delete pod jupyter-notebook -n namespace
   ```

2. Kemudian, hapus endpoint interaktif Anda dengan `delete-managed-endpoint` perintah. Untuk langkah-langkah menghapus titik akhir interaktif, lihatHapus titik akhir interaktif. Awalnya, titik akhir Anda akan berada di TERMINATINGnegara bagian. Setelah semua sumber daya dibersihkan, ia beralih ke TERMINATEDnegara bagian.

3. Jika Anda tidak berencana untuk menggunakan grup keamanan notebook yang Anda buat Membuat grup keamanan untuk penerapan notebook Jupyter lainnya, Anda dapat menghapusnya. Lihat Menghapus grup keamanan di Panduan Pengguna Amazon EC2 untuk informasi selengkapnya.

Operasi lain pada titik akhir interaktif

Topik ini mencakup operasi yang didukung pada titik akhir interaktif selain `create-managed-endpoint`.

Ambil detail titik akhir interaktif

Setelah Anda membuat endpoint interaktif, Anda dapat mengambil detailnya menggunakan perintah. `describe-managed-endpoint` AWS CLI Masukkan nilai Anda sendiri untuk *`managed-endpoint-id`*, *`virtual-cluster-id`*, dan *`wilayah`*:

```
aws emr-containers describe-managed-endpoint --id managed-endpoint-id \
 --virtual-cluster-id virtual-cluster-id --region region
```

Outputnya terlihat mirip dengan berikut ini, dengan titik akhir yang ditentukan, seperti ARN, ID, dan nama.

```
{
   "id": "as3ys2xxxxxxx",
   "name": "endpoint-name",
    "arn": "arn:aws:emr-containers:us-east-1:1828xxxxxxxx:/virtualclusters/
lbhl6kwwyoxxxxxxxxxxxxxxx/endpoints/as3ysxxxxxxxx",
    "virtualClusterId": "lbhl6kwwyoxxxxxxxxxxxxxxx",
    "type": "JUPYTER_ENTERPRISE_GATEWAY",
    "state": "ACTIVE",
    "releaseLabel": "emr-6.9.0-latest",
   "executionRoleArn": "arn:aws:iam::1828xxxxxxxx:role/RoleName",
    "certificateAuthority": {
        "certificateArn": "arn:aws:acm:us-east-1:1828xxxxxxxx:certificate/zzzzzzzz-
e59b-4ed0-aaaa-bbbbbbbbbbbb",
        "certificateData": "certificate-data"
    },
    "configurationOverrides": {
        "applicationConfiguration": [
            {
```

```
                "classification": "spark-defaults",
                "properties": {
                    "spark.driver.memory": "8G"
                }
            }
        ],
        "monitoringConfiguration": {
            "persistentAppUI": "ENABLED",
            "cloudWatchMonitoringConfiguration": {
                "logGroupName": "log-group-name",
                "logStreamNamePrefix": "log-stream-name-prefix"
            },
            "s3MonitoringConfiguration": {
                "logUri": "s3-bucket-name"
            }
        }
    },
   "serverUrl": "https://internal-k8s-namespace-ingressa-aaaaaaaaaa-
zzzzzzzzzz.us-east-1.elb.amazonaws.com:18888 (https://internal-k8s-nspluto-
ingressa-51e860abbd-1620715833.us-east-1.elb.amazonaws.com:18888/)",
    "createdAt": "2022-09-19T12:37:49+00:00",
    "securityGroup": "sg-aaaaaaaaaaaaaa",
    "subnetIds": [
        "subnet-11111111111",
        "subnet-22222222222",
        "subnet-33333333333"
    ],
    "stateDetails": "Endpoint created successfully. It took 3 Minutes 15 Seconds",
    "tags": {}
 }
```

Buat daftar semua titik akhir interaktif yang terkait dengan cluster virtual

Gunakan `list-managed-endpoints` AWS CLI perintah untuk mengambil daftar semua endpoint interaktif yang terkait dengan cluster virtual tertentu. Ganti `virtual-cluster-id` dengan ID cluster virtual Anda.

```
aws emr-containers list-managed-endpoints --virtual-cluster-id virtual-cluster-id
```

Output dari `list-managed-endpoint` perintah ditunjukkan di bawah ini:

```
{
```

```
    "endpoints": [{
        "id": "as3ys2xxxxxxx",
        "name": "endpoint-name",
        "arn": "arn:aws:emr-containers:us-east-1:1828xxxxxxxx:/virtualclusters/
lbhl6kwwyoxxxxxxxxxxxxxx/endpoints/as3ysxxxxxxxx",
        "virtualClusterId": "lbhl6kwwyoxxxxxxxxxxxxxx",
        "type": "JUPYTER_ENTERPRISE_GATEWAY",
        "state": "ACTIVE",
        "releaseLabel": "emr-6.9.0-latest",
        "executionRoleArn": "arn:aws:iam::1828xxxxxxxx:role/RoleName",
        "certificateAuthority": {
            "certificateArn": "arn:aws:acm:us-east-1:1828xxxxxxxx:certificate/zzzzzzzz-
e59b-4ed0-aaaa-bbbbbbbbbbbb",
            "certificateData": "certificate-data"
        },
        "configurationOverrides": {
            "applicationConfiguration": [{
                "classification": "spark-defaults",
                "properties": {
                    "spark.driver.memory": "8G"
                }
            }],
            "monitoringConfiguration": {
                "persistentAppUI": "ENABLED",
                "cloudWatchMonitoringConfiguration": {
                    "logGroupName": "log-group-name",
                    "logStreamNamePrefix": "log-stream-name-prefix"
                },
                "s3MonitoringConfiguration": {
                    "logUri": "s3-bucket-name"
                }
            }
        },
        "serverUrl": "https://internal-k8s-namespace-ingressa-aaaaaaaaaa-
zzzzzzzzzz.us-east-1.elb.amazonaws.com:18888 (https://internal-k8s-nspluto-
ingressa-51e860abbd-1620715833.us-east-1.elb.amazonaws.com:18888/)",
        "createdAt": "2022-09-19T12:37:49+00:00",
        "securityGroup": "sg-aaaaaaaaaaaaa",
        "subnetIds": [
            "subnet-11111111111",
            "subnet-22222222222",
            "subnet-33333333333"
        ],
        "stateDetails": "Endpoint created successfully. It took 3 Minutes 15 Seconds",
```

```
        "tags": {}
    }]
}
```

Hapus titik akhir interaktif

Untuk menghapus titik akhir interaktif yang terkait dengan EMR Amazon di kluster virtual EKS, gunakan `delete-managed-endpoint` AWS CLI perintah. Saat Anda menghapus titik akhir interaktif, Amazon EMR di EKS menghapus grup keamanan default yang dibuat untuk titik akhir tersebut.

Tentukan nilai untuk parameter berikut ke perintah:

- --id: Pengidentifikasi titik akhir interaktif yang ingin Anda hapus.
- -- virtual-cluster-id — Pengidentifikasi cluster virtual yang terkait dengan titik akhir interaktif yang ingin Anda hapus. Ini adalah ID cluster virtual yang sama yang ditentukan ketika endpoint interaktif dibuat.

```
aws emr-containers delete-managed-endpoint --id managed-endpoint-id --virtual-cluster-
id virtual-cluster-id
```

Perintah mengembalikan output yang mirip dengan berikut ini untuk mengonfirmasi bahwa Anda menghapus titik akhir interaktif:

```
{
    "id":"8gai4l4exxxxx",
    "virtualClusterId":"0b0qvauoy3ch1nqodxxxxxxxx"
}
```

Pemantauan tugas

Topik

Memantau tugas dengan Amazon CloudWatch Events

Amazon EMR di EKS menyiarkan peristiwa ketika keadaan tugas berjalan berubah. Setiap peristiwa memberikan informasi, seperti tanggal dan waktu ketika peristiwa terjadi, bersama dengan detail lebih lanjut tentang peristiwa, seperti ID klaster virtual dan ID tugas berjalan yang terpengaruh.

Anda dapat menggunakan peristiwa untuk melacak aktivitas dan kesehatan tugas yang Anda jalankan pada klaster virtual. Anda juga dapat menggunakan Amazon CloudWatch Events untuk menentukan tindakan yang akan dilakukan saat tugas berjalan menghasilkan peristiwa yang cocok dengan pola yang Anda tentukan. Peristiwa berguna untuk memantau kejadian tertentu selama siklus hidup dari tugas berjalan. Misalnya, Anda dapat memantau saat status tugas berjalan berubah dari `submitted` ke `running`. Untuk informasi selengkapnya tentang CloudWatch Acara, lihat Panduan Pengguna CloudWatch Acara Amazon.

Tabel berikut mencantumkan peristiwa Amazon EMR di EKS, bersama dengan status atau perubahan status yang ditunjukkan peristiwa, tingkat kepelikan peristiwa, dan pesan peristiwa. Setiap peristiwa direpresentasikan sebagai objek JSON yang dikirim secara otomatis ke alur kejadian. Objek JSON mencakup detail lebih lanjut tentang peristiwa tersebut. Objek JSON sangat penting ketika Anda mengatur aturan untuk pengolahan CloudWatch peristiwa menggunakan Events karena aturan berusaha untuk mencocokkan pola dalam objek JSON. Untuk informasi selengkapnya, lihat Pola Acara dan Peristiwa serta Amazon EMR pada Acara EKS di Panduan Pengguna CloudWatch Acara Amazon.

Peristiwa perubahan status tugas berjalan

Status	Kepelikan	Pesan
DIKIRIMKAN	INFO	Job Run *JobRunId*(*JobRunName*) berhasil diserahkan ke klaster virtual *VirtualClusterId* di *Time* UTC.
BERJALAN	INFO	Job Run *JobRunId*(*JobRunName*) di cluster virtual *VirtualClusterId* mulai berjalan di *Time*.
DISELESAIKAN	INFO	Job Run *jobRunId*(*JobRunName*) di cluster virtual *VirtualClusterId* selesai pada *Waktu*. Tugas Berjalan mulai berjalan pada *Waktu* dan memakan waktu *Num* menit untuk diselesaikan.
DIBATALKAN	PERINGATAN	Permintaan pembatalan telah berhasil untuk Job Run *JobRunId*(*JobRunName*) di cluster virtual *VirtualClusterId* di *Time* dan Job Run sekarang dibatalkan.
GAGAL	ERROR	Job Run *JobRunId*(*JobRunName*) di cluster virtual *VirtualClusterId* gagal pada *Waktu*.

Otomatiskan Amazon EMR di EKS dengan CloudWatch Events

Anda dapat menggunakan Amazon CloudWatch Events untuk mengotomatiskanAWS layanan Anda untuk merespons peristiwa sistem seperti masalah ketersediaan aplikasi atau perubahan sumber daya. Kejadian dariAWS layanan dikirimkan ke CloudWatch Events dalam hampir waktu nyata. Anda dapat menuliskan aturan sederhana untuk menunjukkan peristiwa mana yang sesuai kepentingan Anda, dan tindakan otomatis yang diambil ketika suatu peristiwa sesuai dengan suatu aturan. Tindakan yang dapat dipicu secara otomatis meliputi hal berikut:

- Mengambil fungsi AWS Lambda
- Meminta Perintah Amazon EC2 Run

- Mengirim peristiwa ke Amazon Kinesis Data Streams
- Mengaktifkan mesin keadaan AWS Step Functions
- Memberi tahu topikAmazon Simple Notification Service (SNS) atau antreanAmazon Simple Queue Service (SQS)

Beberapa contoh penggunaan CloudWatch Events dengan Amazon EMR di EKS adalah sebagai berikut:

- Mengaktifkan fungsi Lambda ketika tugas berjalan berhasil
- Memberi tahu topik Amazon SNS saat pekerjaan berjalan gagal

CloudWatch Acara untuk "`detail-type:`" "`EMR Job Run State Change`" "dihasilkan oleh Amazon EMR di EKS untuk`SUBMITTED`,`RUNNING`,`CANCELLED`,`FAILED` dan perubahan`COMPLETED` status.

Contoh: Mengatur aturan yang memanggil Lambda

Gunakan langkah-langkah berikut untuk menyiapkan aturan CloudWatch Acara yang memanggil Lambda ketika ada acara “Perubahan Status Jalankan Job EMR”.

```
aws events put-rule \
--name cwe-test \
--event-pattern '{"detail-type": ["EMR Job Run State Change"]}'
```

Tambahkan fungsi Lambda yang Anda miliki sebagai target baru dan berikan izin CloudWatch Kejadian untuk memanggil fungsi Lambda seperti berikut. Ganti *123456789012* ID akun Anda.

```
aws events put-targets \
--rule cwe-test \
--targets Id=1,Arn=arn:aws:lambda:us-east-1:123456789012:function:MyFunction
```

```
aws lambda add-permission \
--function-name MyFunction \
--statement-id MyId \
--action 'lambda:InvokeFunction' \
--principal events.amazonaws.com
```

> **Note**
>
> Anda tidak dapat menulis program yang tergantung pada urutan keberadaan atau notifikasi peristiwa, karena program tersebut mungkin tidak berurutan atau hilang. Peristiwa dipancarkan atas dasar upaya terbaik.

Pantau pod driver pekerjaan dengan kebijakan coba lagi menggunakan Amazon CloudWatch Events

Dengan menggunakan CloudWatch event, kamu dapat memantau Pod driver yang telah dibuat dalam pekerjaan yang memiliki kebijakan percobaan ulang. Untuk informasi lain, lihat Memantau pekerjaan dengan kebijakan coba lagi dalam panduan ini.

Mengelola klaster virtual

Sebuah klaster virtual adalah namespace Kubernetes tempat Amazon EMR terdaftar. Anda dapat menciptakan, menggambarkan, membuat daftar, dan menghapus klaster virtual. Mereka tidak mengonsumsi sumber daya tambahan apa pun dalam sistem Anda. Sebuah klaster virtual tunggal memetakan ke satu namespace Kubernetes. Mengingat hubungan ini, Anda dapat memodelkan klaster virtual dengan cara yang sama Anda memodelkan namespace Kubernetes untuk memenuhi persyaratan Anda. Lihat kemungkinan kasus penggunaan di dokumentasi Gambaran Umum Konsep Kubernetes.

Untuk mendaftar Amazon EMR dengan namespace Kubernetes pada klaster Amazon EKS, Anda perlu nama klaster EKS dan namespace yang telah diatur untuk menjalankan beban kerja Anda. Klaster terdaftar tersebut di Amazon EMR disebut klaster virtual karena mereka tidak mengelola komputasi atau penyimpanan fisik tetapi menunjuk ke namespace Kubernetes di mana beban kerja Anda dijadwalkan.

> **Note**
>
> Sebelum membuat klaster virtual, Anda harus terlebih dahulu menyelesaikan langkah 1-8 di Menyiapkan Amazon EMR di EKS.

Topik

Membuat klaster virtual

Jalankan perintah berikut untuk membuat klaster virtual dengan mendaftarkan Amazon EMR dengan namespace pada klaster EKS. Ganti *virtual_cluster_name* dengan nama yang Anda berikan untuk klaster virtual Anda. Ganti *eks_cluster_name* dengan nama klaster EKS. Ganti *namespace_name* dengan namespace yang ingin Anda daftarkan dengan Amazon EMR.

```
aws emr-containers create-virtual-cluster \
--name virtual_cluster_name \
--container-provider '{
    "id": "eks_cluster_name",
    "type": "EKS",
    "info": {
        "eksInfo": {
            "namespace": "namespace_name"
        }
    }
}'
```

Atau, Anda dapat membuat file JSON yang mencakup parameter yang diperlukan untuk klaster virtual, seperti yang ditunjukkan contoh berikut.

```
{
    "name": "virtual_cluster_name",
    "containerProvider": {
        "type": "EKS",
        "id": "eks_cluster_name",
        "info": {
            "eksInfo": {
                "namespace": "namespace_name"
            }
        }
    }
}
```

Kemudian jalankan perintah `create-virtual-cluster` berikut dengan jalur ke file JSON.

```
aws emr-containers create-virtual-cluster \
--cli-input-json file://./create-virtual-cluster-request.json
```

> **Note**
>
> Untuk memvalidasi keberhasilan pembuatan klaster virtual, lihat status klaster virtual dengan menjalankan perintah `list-virtual-clusters` atau dengan masuk ke halaman Klaster virtual di konsol Amazon EMR.

Daftar klaster virtual

Jalankan perintah berikut untuk menampilkan status klaster virtual.

```
aws emr-containers list-virtual-clusters
```

Gambarkan klaster virtual

Jalankan perintah berikut untuk mendapatkan detail lebih lanjut tentang klaster virtual, seperti namespace, status, dan tanggal terdaftar. Ganti *123456* dengan ID klaster virtual Anda.

```
aws emr-containers describe-virtual-cluster --id 123456
```

Menghapus klaster virtual

Jalankan perintah berikut untuk menghapus klaster virtual. Ganti *123456* dengan ID klaster virtual Anda.

```
aws emr-containers delete-virtual-cluster --id 123456
```

Status klaster virtual

Tabel berikut menjelaskan empat kemungkinan status klaster virtual.

State	Deskripsi
RUNNING	Klaster virtual berada dalam status RUNNING.
TERMINATING	Penghentian klaster virtual yang diminta sedang berlangsung.
TERMINATED	Penghentian yang diminta selesai.
ARRESTED	Penghentian yang diminta gagal karena izin yang tidak mencukupi.

Tutorial untuk Amazon EMR di EKS

Bagian ini menjelaskan kasus penggunaan umum saat Anda bekerja dengan Amazon EMR pada aplikasi EKS.

Topik

Menggunakan Delta Lake dengan Amazon EMR di EKS

Menggunakan Delta Lake dengan Amazon EMR di EKS

1. Saat Anda memulai pekerjaan untuk mengirimkan pekerjaan Spark dalam konfigurasi aplikasi, sertakan file Delta Lake JAR:

```
--job-driver '{"sparkSubmitJobDriver" : {
      "sparkSubmitParameters" : "--jars local:///usr/share/aws/delta/lib/delta-
core.jar,local:///usr/share/aws/delta/lib/delta-storage.jar,local:///usr/share/aws/
delta/lib/delta-storage-s3-dynamodb.jar"}}'
```

2. Sertakan konfigurasi tambahan Delta Lake dan gunakan Katalog Data AWS Glue sebagai metastore Anda.

```
--configuration-overrides '{
        "applicationConfiguration": [
        {
          "classification" : "spark-defaults",
          "properties" : {
            "spark.sql.extensions" : "io.delta.sql.DeltaSparkSessionExtension",

 "spark.sql.catalog.spark_catalog":"org.apache.spark.sql.delta.catalog.DeltaCatalog",
"spark.hadoop.hive.metastore.client.factory.class":"com.amazonaws.glue.catalog.metastore.AW
```

```
          }
        }]}'
```

Menggunakan Apache Iceberg EMR di EKS

Menggunakan Apache Iceberg EMR di EKS

1. Saat Anda memulai pekerjaan untuk mengirimkan pekerjaan Spark dalam konfigurasi aplikasi, sertakan file JAR runtime Iceberg spark:

```
--job-driver '{"sparkSubmitJobDriver" : {"sparkSubmitParameters" : "--jars
 local:///usr/share/aws/iceberg/lib/iceberg-spark3-runtime.jar"}}'
```

2. Sertakan konfigurasi tambahan Iceberg:

```
--configuration-overrides '{
    "applicationConfiguration": [
    "classification" : "spark-defaults",
    "properties" : {
        "spark.sql.catalog.dev.warehouse" : "s3://DOC-EXAMPLE-BUCKET/EXAMPLE-
PREFIX/ ",
        "spark.sql.extensions ":"
 org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions ",
        "spark.sql.catalog.dev" : "org.apache.iceberg.spark.SparkCatalog",
        "spark.sql.catalog.dev.catalog-impl" :
 "org.apache.iceberg.aws.glue.GlueCatalog",
        "spark.sql.catalog.dev.io-impl": "org.apache.iceberg.aws.s3.S3FileIO"
        }
    ]
}'
```

Untuk mempelajari lebih lanjut tentang versi rilis Apache Iceberg dari EMR, lihat riwayat rilis Iceberg.

Menggunakan RAPIDS Accelerator untuk Apache Spark dengan Amazon EMR di EKS

Dengan Amazon EMR di EKS, Anda dapat menjalankan pekerjaan untuk Nvidia RAPIDS Accelerator untuk Apache Spark. Tutorial ini mencakup cara menjalankan pekerjaan Spark menggunakan RAPIDS pada tipe instans unit pemrosesan grafis EC2 (GPU). Tutorial menggunakan versi berikut:

- Amazon EMR di EKS versi 6.9.0 dan versi yang lebih tinggi
- Apache Spark 3.x

Anda dapat mempercepat Spark dengan jenis instans GPU Amazon EC2 dengan menggunakan plugin Nvidia RAPIDS Accelerator for Apache Spark. Ketika Anda menggunakan teknologi ini bersama-sama, Anda mempercepat jaringan pipa ilmu data Anda tanpa harus membuat perubahan kode. Ini mengurangi waktu berjalan yang diperlukan untuk pemrosesan data dan pelatihan model. Dengan menyelesaikan lebih banyak dalam waktu yang lebih singkat, Anda menghabiskan lebih sedikit biaya infrastruktur.

Sebelum memulai, pastikan Anda memiliki sumber daya berikut.

- Amazon EMR pada klaster virtual EKS
- Klaster Amazon EKS dengan grup node yang diaktifkan GPU

Klaster virtual Amazon EKS adalah handel terdaftar untuk namespace Kubernetes pada klaster Amazon EKS, dan dikelola oleh Amazon EMR pada EKS. Handel ini memungkinkan Amazon EMR menggunakan namespace Kubernetes sebagai tujuan untuk menjalankan pekerjaan. Untuk informasi lebih lanjut tentang cara mengatur klaster virtual, lihat Menyiapkan Amazon EMR di EKS di panduan ini.

Anda harus mengonfigurasi klaster virtual Amazon EKS dengan grup node yang memiliki instans GPU. Anda harus mengkonfigurasi node dengan plugin perangkat Nvidia. Lihat grup node terkelola untuk mempelajari lebih lanjut.

Untuk mengonfigurasi klaster Amazon EKS Anda agar menambahkan grup node berkemampuan GPU, lakukan prosedur berikut:

Untuk menambahkan grup node yang diaktifkan GPU

1. Buat grup node berkemampuan GPU dengan perintah create-nodegroup berikut. Pastikan untuk mengganti parameter yang benar untuk klaster Amazon EKS Anda. Gunakan jenis instans yang mendukung Spark RAPIDS, seperti P4, P3, G5 atau G4dn.

```
aws eks create-nodegroup \
 --cluster-name EKS_CLUSTER_NAME \
 --nodegroup-name NODEGROUP_NAME \
 --scaling-config minSize=0,maxSize=5,desiredSize=2 CHOOSE_APPROPRIATELY \
 --ami-type AL2_x86_64_GPU \
 --node-role NODE_ROLE \
 --subnets SUBNETS_SPACE_DELIMITED  \
 --remote-access ec2SshKey= SSH_KEY \
 --instance-types GPU_INSTANCE_TYPE \
 --disk-size DISK_SIZE \
 --region AWS_REGION
```

2. Instal plugin perangkat Nvidia di klaster Anda untuk memancarkan jumlah GPU pada setiap node klaster Anda dan untuk menjalankan kontainer berkemampuan GPU di klaster Anda. Jalankan kode berikut untuk menginstal plugin:

```
kubectl apply -f https://raw.githubusercontent.com/NVIDIA/k8s-device-plugin/v0.9.0/
nvidia-device-plugin.yml
```

3. Untuk memvalidasi berapa banyak GPU tersedia pada setiap node klaster Anda, jalankan perintah berikut ini:

```
kubectl get nodes  "-o=custom-
columns=NAME:.metadata.name,GPU:.status.allocatable.nvidia\.com/gpu"
```

Untuk menjalankan pekerjaan Spark RAPIDS

1. Kirim tugas Spark RAPIDS untuk Amazon EMR pada klaster EKS. Kode berikut menunjukkan contoh perintah untuk memulai pekerjaan. Pertama kali Anda menjalankan pekerjaan, mungkin perlu beberapa menit untuk men-download gambar dan cache pada node.

```
aws emr-containers start-job-run \
--virtual-cluster-id VIRTUAL_CLUSTER_ID \
--execution-role-arn JOB_EXECUTION_ROLE \
```

```
--release-label emr-6.9.0-spark-rapids-latest \
--job-driver '{"sparkSubmitJobDriver": {"entryPoint": "local:///usr/lib/
spark/examples/jars/spark-examples.jar","entryPointArguments":  ["10000"],
 "sparkSubmitParameters":"--class org.apache.spark.examples.SparkPi "}}' \
---configuration-overrides '{"applicationConfiguration": [{"classification":
 "spark-defaults","properties": {"spark.executor.instances":
 "2","spark.executor.memory": "2G"}}],"monitoringConfiguration":
 {"cloudWatchMonitoringConfiguration": {"logGroupName": "LOG_GROUP
 _NAME"},"s3MonitoringConfiguration": {"logUri": "LOG_GROUP_STREAM"}}}'
```

2. Untuk memvalidasi bahwa Akselerator Spark RAPIDS diaktifkan, periksa log driver Spark. Log ini disimpan di dalam CloudWatch atau di lokasi S3 yang Anda tentukan saat menjalankan `start-job-run` perintah. Contoh berikut umumnya menunjukkan apa garis log terlihat seperti:

```
22/11/15 00:12:44 INFO RapidsPluginUtils: RAPIDS Accelerator build:
 {version=22.08.0-amzn-0, user=release, url=, date=2022-11-03T03:32:45Z, revision=,
 cudf_version=22.08.0, branch=}
22/11/15 00:12:44 INFO RapidsPluginUtils: RAPIDS Accelerator JNI build:
 {version=22.08.0, user=, url=https://github.com/NVIDIA/spark-rapids-jni.git,
 date=2022-08-18T04:14:34Z, revision=a1b23cd_sample, branch=HEAD}
22/11/15 00:12:44 INFO RapidsPluginUtils: cudf build: {version=22.08.0,
 user=, url=https://github.com/rapidsai/cudf.git, date=2022-08-18T04:14:34Z,
 revision=a1b23ce_sample, branch=HEAD}
22/11/15 00:12:44 WARN RapidsPluginUtils: RAPIDS Accelerator 22.08.0-amzn-0 using
 cudf 22.08.0.
22/11/15 00:12:44 WARN RapidsPluginUtils:
 spark.rapids.sql.multiThreadedRead.numThreads is set to 20.
22/11/15 00:12:44 WARN RapidsPluginUtils: RAPIDS Accelerator is enabled, to disable
 GPU support set `spark.rapids.sql.enabled` to false.
22/11/15 00:12:44 WARN RapidsPluginUtils: spark.rapids.sql.explain is set to
 `NOT_ON_GPU`. Set it to 'NONE' to suppress the diagnostics logging about the query
 placement on the GPU.
```

3. Untuk melihat operasi yang akan dijalankan pada GPU, lakukan langkah-langkah berikut untuk mengaktifkan pencatatan ekstra. Catatan "`spark.rapids.sql.explain : ALL`" config.

```
aws emr-containers start-job-run \
--virtual-cluster-id VIRTUAL_CLUSTER_ID \
--execution-role-arn JOB_EXECUTION_ROLE \
--release-label emr-6.9.0-spark-rapids-latest \
--job-driver '{"sparkSubmitJobDriver": {"entryPoint": "local:///usr/lib/
spark/examples/jars/spark-examples.jar","entryPointArguments":  ["10000"],
 "sparkSubmitParameters":"--class org.apache.spark.examples.SparkPi "}}' \
```

```
---configuration-overrides '{"applicationConfiguration":
 [{"classification": "spark-defaults","properties":
 {"spark.rapids.sql.explain":"ALL","spark.executor.instances":
 "2","spark.executor.memory": "2G"}}],"monitoringConfiguration":
 {"cloudWatchMonitoringConfiguration": {"logGroupName":
 "LOG_GROUP_NAME"},"s3MonitoringConfiguration": {"logUri": "LOG_GROUP_STREAM"}}}'
```

Perintah sebelumnya adalah contoh pekerjaan yang menggunakan GPU. Outputnya akan terlihat seperti contoh di bawah ini. Lihat kunci ini untuk membantu memahami output:

- *- menandai operasi yang bekerja pada GPU
- !- menandai operasi yang tidak dapat berjalan pada GPU
- @- menandai operasi yang bekerja pada GPU, tetapi tidak akan bisa berjalan karena ada di dalam rencana yang tidak dapat dijalankan pada GPU

```
22/11/15 01:22:58 INFO GpuOverrides: Plan conversion to the GPU took 118.64 ms
22/11/15 01:22:58 INFO GpuOverrides: Plan conversion to the GPU took 4.20 ms
22/11/15 01:22:58 INFO GpuOverrides: GPU plan transition optimization took 8.37 ms
22/11/15 01:22:59 WARN GpuOverrides:
   *Exec <ProjectExec> will run on GPU
     *Expression <Alias> substring(cast(date#149 as string), 0, 7) AS month#310
will run on GPU
       *Expression <Substring> substring(cast(date#149 as string), 0, 7) will run
on GPU
         *Expression <Cast> cast(date#149 as string) will run on GPU
     *Exec <SortExec> will run on GPU
       *Expression <SortOrder> date#149 ASC NULLS FIRST will run on GPU
       *Exec <ShuffleExchangeExec> will run on GPU
         *Partitioning <RangePartitioning> will run on GPU
           *Expression <SortOrder> date#149 ASC NULLS FIRST will run on GPU
         *Exec <UnionExec> will run on GPU
           !Exec <ProjectExec> cannot run on GPU because not all expressions can
be replaced
             @Expression <AttributeReference> customerID#0 could run on GPU
             @Expression <Alias> Charge AS kind#126 could run on GPU
               @Expression <Literal> Charge could run on GPU
             @Expression <AttributeReference> value#129 could run on GPU
             @Expression <Alias> add_months(2022-11-15, cast(-(cast(_we0#142 as
bigint) + last_month#128L) as int)) AS date#149 could run on GPU
```

```
                ! <AddMonths> add_months(2022-11-15, cast(-
(cast(_we0#142 as bigint) + last_month#128L) as int)) cannot run
 on GPU because GPU does not currently support the operator class
 org.apache.spark.sql.catalyst.expressions.AddMonths
                  @Expression <Literal> 2022-11-15 could run on GPU
                  @Expression <Cast> cast(-(cast(_we0#142 as bigint) +
 last_month#128L) as int) could run on GPU
                    @Expression <UnaryMinus> -(cast(_we0#142 as bigint) +
 last_month#128L) could run on GPU
                      @Expression <Add> (cast(_we0#142 as bigint) +
 last_month#128L) could run on GPU
                        @Expression <Cast> cast(_we0#142 as bigint) could run on
 GPU
                          @Expression <AttributeReference> _we0#142 could run on
 GPU
                        @Expression <AttributeReference> last_month#128L could run
 on GPU
```

Menggunakan integrasi Amazon Redshift untuk Apache Spark di Amazon EMR di EKS

Dengan rilis Amazon EMR 6.9.0 dan versi lebih baru, setiap gambar rilis menyertakan konektor antara Apache Spark dan Amazon Redshift. Dengan cara ini, Anda dapat menggunakan Spark di Amazon EMR di EKS untuk memproses data yang disimpan di Amazon Redshift. Integrasi didasarkan pada konektor `spark-redshift`open-source. Untuk Amazon EMR di EKS, integrasi Amazon Redshift untuk Apache Spark disertakan sebagai integrasi asli.

Topik

- Meluncurkan aplikasi Spark menggunakan integrasi Amazon Redshift untuk Apache Spark
- Mengautentikasi dengan integrasi Amazon Redshift untuk Apache Spark
- Membaca dan menulis dari dan ke Amazon Redshift
- Pertimbangan dan batasan saat menggunakan konektor Spark

Meluncurkan aplikasi Spark menggunakan integrasi Amazon Redshift untuk Apache Spark

Untuk menggunakan integrasi, Anda harus meneruskan dependensi Spark Redshift yang diperlukan dengan pekerjaan Spark Anda. Anda harus menggunakan `--jars` untuk menyertakan pustaka terkait konektor Redshift. Untuk melihat lokasi file lain yang didukung oleh `--jars` opsi, lihat bagian Manajemen Ketergantungan Lanjutan pada dokumentasi Apache Spark.

- `spark-redshift.jar`
- `spark-avro.jar`
- `RedshiftJDBC.jar`
- `minimal-json.jar`

Untuk meluncurkan aplikasi Spark dengan integrasi Amazon Redshift untuk Apache Spark di Amazon EMR pada rilis EKS 6.9.0 atau yang lebih baru, gunakan perintah contoh berikut. Perhatikan bahwa jalur yang terdaftar dengan `--conf spark.jars` opsi adalah jalur default untuk file JAR.

```
aws emr-containers start-job-run \

--virtual-cluster-id cluster_id \
--execution-role-arn arn \
--release-label emr-6.9.0-latest\
--job-driver '{
    "sparkSubmitJobDriver": {
        "entryPoint": "s3://script_path",
            "sparkSubmitParameters":
            "--conf spark.kubernetes.file.upload.path=s3://upload_path
             --conf spark.jars=
                /usr/share/aws/redshift/jdbc/RedshiftJDBC.jar,
                /usr/share/aws/redshift/spark-redshift/lib/spark-redshift.jar,
                /usr/share/aws/redshift/spark-redshift/lib/spark-avro.jar,
                /usr/share/aws/redshift/spark-redshift/lib/minimal-json.jar"
                            }
            }'
```

Mengautentikasi dengan integrasi Amazon Redshift untuk Apache Spark

Gunakan AWS Secrets Manager untuk mengambil kredensi dan terhubung ke Amazon Redshift

Anda dapat menyimpan kredensi di Secrets Manager untuk mengautentikasi secara aman ke Amazon Redshift. Anda dapat meminta pekerjaan Spark Anda memanggil `GetSecretValue` API untuk mengambil kredensialnya:

```
from pyspark.sql import SQLContextimport boto3

sc = # existing SparkContext
sql_context = SQLContext(sc)

secretsmanager_client = boto3.client('secretsmanager',
 region_name=os.getenv('AWS_REGION'))
secret_manager_response = secretsmanager_client.get_secret_value(
    SecretId='string',
    VersionId='string',
    VersionStage='string'
)
username = # get username from secret_manager_response
password = # get password from secret_manager_response
url = "jdbc:redshift://redshifthost:5439/database?user=" + username + "&password="
 + password

# Access to Redshift cluster using Spark
```

Gunakan otentikasi berbasis IAM dengan Amazon EMR pada peran eksekusi pekerjaan EKS

Dimulai dengan Amazon EMR pada rilis EKS 6.9.0, driver Amazon Redshift JDBC versi 2.1 atau lebih tinggi dikemas ke dalam lingkungan. Dengan driver JDBC 2.1 dan lebih tinggi, Anda dapat menentukan URL JDBC dan tidak termasuk username mentah dan password. Sebaliknya, Anda dapat menentukan `jdbc:redshift:iam://` skema. Ini memerintahkan driver JDBC untuk menggunakan Amazon EMR Anda pada peran eksekusi pekerjaan EKS untuk mengambil kredensi secara otomatis.

Lihat Mengkonfigurasi koneksi JDBC atau ODBC untuk menggunakan kredensi IAM di Panduan Manajemen Amazon Redshift untuk informasi selengkapnya.

Contoh URL berikut menggunakan `jdbc:redshift:iam://` skema.

```
jdbc:redshift:iam://examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com:5439/
dev
```

Izin berikut diperlukan untuk peran eksekusi pekerjaan Anda ketika memenuhi ketentuan yang disediakan.

Izin	Kondisi bila diperlukan untuk peran eksekusi pekerjaan
`redshift:GetClusterCredentials`	Diperlukan untuk driver JDBC untuk mengambil kredensi dari Amazon Redshift
`redshift:DescribeCluster`	Diperlukan jika Anda menentukan klaster Amazon Redshift dan Wilayah AWS di URL JDBC, bukan titik akhir
`redshift-serverless:GetCredentials`	Diperlukan bagi driver JDBC untuk mengambil kredensi dari Amazon Redshift Tanpa Server
`redshift-serverless:GetWorkgroup`	Diperlukan jika Anda menggunakan Amazon Redshift Tanpa Server dan Anda menentukan URL dalam hal nama grup kerja dan Wilayah

Kebijakan peran eksekusi pekerjaan Anda harus memiliki izin berikut.

```
{
            "Effect": "Allow",
            "Action": [
                "redshift:GetClusterCredentials",
                "redshift:DescribeCluster",
                "redshift-serverless:GetCredentials",
                "redshift-serverless:GetWorkgroup"
            ],
            "Resource": [

 "arn:aws:redshift:AWS_REGION:ACCOUNT_ID:dbname:CLUSTER_NAME/DATABASE_NAME",
```

```
            "arn:aws:redshift:AWS_REGION:ACCOUNT_ID:dbuser:DATABASE_NAME/USER_NAME"
        ]
    }
```

Otentikasi ke Amazon Redshift dengan driver JDBC

Mengatur username dan password di dalam URL JDBC

Untuk mengautentikasi tugas Spark ke klaster Amazon Redshift, Anda dapat menentukan nama database dan kata sandi Amazon Redshift di URL JDBC.

> **Note**
>
> Jika Anda meneruskan kredensi database di URL, siapa pun yang memiliki akses ke URL juga dapat mengakses kredensialnya. Metode ini umumnya tidak direkomendasikan karena ini bukan opsi yang aman.

Jika keamanan bukan masalah untuk aplikasi Anda, Anda dapat menggunakan format berikut untuk mengatur nama pengguna dan kata sandi di URL JDBC:

```
jdbc:redshift://redshifthost:5439/database?user=username&password=password
```

Membaca dan menulis dari dan ke Amazon Redshift

Contoh kode berikut digunakan PySpark untuk membaca dan menulis data sampel dari dan ke database Amazon Redshift dengan API sumber data dan dengan SparkSQL.

Data source API

Gunakan PySpark untuk membaca dan menulis data sampel dari dan ke database Amazon Redshift dengan API sumber data.

```
import boto3
from pyspark.sql import SQLContext

sc = # existing SparkContext
sql_context = SQLContext(sc)

url = "jdbc:redshift:iam://redshifthost:5439/database"
```

```
aws_iam_role_arn = "arn:aws:iam::accountID:role/roleName"

df = sql_context.read \
    .format("io.github.spark_redshift_community.spark.redshift") \
    .option("url", url) \
    .option("dbtable", "tableName") \
    .option("tempdir", "s3://path/for/temp/data") \
    .option("aws_iam_role", "aws_iam_role_arn") \
    .load()

df.write \
    .format("io.github.spark_redshift_community.spark.redshift") \
    .option("url", url) \
    .option("dbtable", "tableName_copy") \
    .option("tempdir", "s3://path/for/temp/data") \
    .option("aws_iam_role", "aws_iam_role_arn") \
    .mode("error") \
    .save()
```

SparkSQL

Gunakan PySpark untuk membaca dan menulis data sampel dari dan ke database Amazon Redshift menggunakan SparkSQL.

```
import boto3
import json
import sys
import os
from pyspark.sql import SparkSession

spark = SparkSession \
    .builder \
    .enableHiveSupport() \
    .getOrCreate()

url = "jdbc:redshift:iam://redshifthost:5439/database"
aws_iam_role_arn = "arn:aws:iam::accountID:role/roleName"

bucket = "s3://path/for/temp/data"
tableName = "tableName" # Redshift table name

s = f"""CREATE TABLE IF NOT EXISTS {tableName} (country string, data string)
    USING io.github.spark_redshift_community.spark.redshift
```

```
    OPTIONS (dbtable '{tableName}', tempdir '{bucket}', url '{url}', aws_iam_role
 '{aws_iam_role_arn}' ); """

spark.sql(s)

columns = ["country" ,"data"]
data = [("test-country","test-data")]
df = spark.sparkContext.parallelize(data).toDF(columns)

# Insert data into table
df.write.insertInto(tableName, overwrite=False)
df = spark.sql(f"SELECT * FROM {tableName}")
df.show()
```

Pertimbangan dan batasan saat menggunakan konektor Spark

- Kami menyarankan Anda mengaktifkan SSL untuk koneksi JDBC dari Spark di Amazon EMR ke Amazon Redshift.
- Kami merekomendasikan Anda mengelola kredensi klaster Amazon Redshift AWS Secrets Manager sebagai praktik terbaik. Lihat Menggunakan AWS Secrets Manager untuk mengambil kredensi untuk menghubungkan ke Amazon Redshift sebagai contoh.
- Kami menyarankan Anda meneruskan peran IAM dengan parameter `aws_iam_role` untuk parameter autentikasi Amazon Redshift.
- Parameter `tempformat` saat ini tidak mendukung format Parket.
- `tempdir`URI menunjuk ke lokasi Amazon S3. Direktori temp ini tidak dibersihkan secara otomatis dan oleh karena itu dapat menambah biaya tambahan.
- Pertimbangkan rekomendasi berikut untuk Amazon Redshift:
  - Kami merekomendasikan Anda memblokir akses publik ke klaster Amazon Redshift.
  - Kami menyarankan Anda mengaktifkan pencatatan audit Amazon Redshift.
  - Sebaiknya aktifkan enkripsi saat istirahat Amazon Redshift.
- Pertimbangkan rekomendasi berikut untuk Amazon S3:
  - Kami merekomendasikan memblokir akses publik ke bucket Amazon S3.
  - Kami menyarankan Anda menggunakan enkripsi sisi server Amazon S3 untuk mengenkripsi bucket S3 yang Anda gunakan.

- Kami menyarankan Anda menggunakan kebijakan siklus hidup Amazon S3 untuk menentukan aturan penyimpanan untuk bucket S3.
- Amazon EMR selalu memverifikasi kode yang diimpor dari sumber terbuka ke dalam gambar. Demi keamanan, kami tidak mendukung kunci AWS akses pengkodean di `tempdir` URI sebagai metode autentikasi dari Spark ke Amazon S3.

Untuk informasi selengkapnya tentang penggunaan konektor dan parameter yang didukung, lihat sumber daya berikut:

- Integrasi Amazon Redshift untuk Apache Spark dalam Panduan Manajemen Amazon Redshift
- Repositori `spark-redshift` komunitas di Github

Menggunakan Volcano sebagai penjadwal khusus untuk Apache Spark di Amazon EMR di EKS

Dengan Amazon EMR di EKS, Anda dapat menggunakan operator Spark atau spark-submit untuk menjalankan pekerjaan Spark dengan penjadwal kustom Kubernetes. Tutorial ini mencakup cara menjalankan pekerjaan Spark dengan penjadwal Volcano pada antrian khusus.

Gambaran Umum

Volcano dapat membantu mengelola penjadwalan Spark dengan fungsi-fungsi lanjutan seperti penjadwalan antrian, penjadwalan fair-share, dan reservasi sumber daya. Untuk informasi lebih lanjut tentang manfaat Volcano, lihat Why Spark memilih Volcano sebagai penjadwal batch bawaan pada Kubernetes di blog CNCF The Linux Foundation.

Instal dan atur Volcano

1. Pilih salah satu perintah kubectl berikut untuk menginstal Volcano, tergantung pada kebutuhan arsitektur Anda:

```
# x86_64
kubectl apply -f https://raw.githubusercontent.com/volcano-sh/volcano/v1.5.1/
installer/volcano-development.yaml
# arm64:
kubectl apply -f https://raw.githubusercontent.com/volcano-sh/volcano/v1.5.1/
installer/volcano-development-arm64.yaml
```

2. Siapkan sampel antrian gunung berapi. Antrian adalah kumpulan. PodGroups Antrian mengadopsi FIFO dan merupakan dasar untuk divisi sumber daya.

```
cat << EOF > volcanoQ.yaml
apiVersion: scheduling.volcano.sh/v1beta1
kind: Queue
metadata:
  name: sparkqueue
spec:
  weight: 4
  reclaimable: false
  capability:
    cpu: 10
    memory: 20Gi
EOF

kubectl apply -f volcanoQ.yaml
```

3. Unggah PodGroup manifes sampel ke Amazon S3. PodGroupAdalah sekelompok polong dengan asosiasi yang kuat. Anda biasanya menggunakan penjadwalan PodGroup untuk batch. Kirimkan contoh berikut PodGroup ke antrean yang Anda tentukan di langkah sebelumnya.

```
cat << EOF > podGroup.yaml
apiVersion: scheduling.volcano.sh/v1beta1
kind: PodGroup
spec:
  # Set minMember to 1 to make a driver pod
  minMember: 1
  # Specify minResources to support resource reservation.
  # Consider the driver pod resource and executors pod resource.
  # The available resources should meet the minimum requirements of the Spark job
  # to avoid a situation where drivers are scheduled, but they can't schedule
  # sufficient executors to progress.
  minResources:
    cpu: "1"
    memory: "1Gi"
  # Specify the queue. This defines the resource queue that the job should be
 submitted to.
  queue: sparkqueue
EOF

aws s3 mv podGroup.yaml s3://bucket-name
```

Jalankan aplikasi Spark dengan penjadwal Volcano dengan operator Spark

1. Jika Anda belum melakukannya, selesaikan langkah-langkah di bagian berikut untuk menyiapkan:

   a. Instal dan atur Volcano

   b. Menyiapkan operator Spark untuk Amazon EMR di EKS

   c. Instal operator Spark

      Sertakan argumen berikut saat Anda menjalankan `helm install spark-operator-demo` perintah:

      ```
      --set batchScheduler.enable=true
      --set webhook.enable=true
      ```

2. Buat file `SparkApplication` definisi `spark-pi.yaml` dengan `batchScheduler` dikonfigurasi.

```
apiVersion: "sparkoperator.k8s.io/v1beta2"
kind: SparkApplication
metadata:
  name: spark-pi
  namespace: spark-operator
spec:
  type: Scala
  mode: cluster
  image: "895885662937.dkr.ecr.us-west-2.amazonaws.com/spark/emr-6.10.0:latest"
  imagePullPolicy: Always
  mainClass: org.apache.spark.examples.SparkPi
  mainApplicationFile: "local:///usr/lib/spark/examples/jars/spark-examples.jar"
  sparkVersion: "3.3.1"
  batchScheduler: "volcano"   #Note: You must specify the batch scheduler name as
 'volcano'
  restartPolicy:
    type: Never
  volumes:
    - name: "test-volume"
      hostPath:
        path: "/tmp"
        type: Directory
  driver:
```

```
    cores: 1
    coreLimit: "1200m"
    memory: "512m"
    labels:
      version: 3.3.1
    serviceAccount: emr-containers-sa-spark
    volumeMounts:
      - name: "test-volume"
        mountPath: "/tmp"
  executor:
    cores: 1
    instances: 1
    memory: "512m"
    labels:
      version: 3.3.1
    volumeMounts:
      - name: "test-volume"
        mountPath: "/tmp"
```

3. Kirimkan aplikasi Spark dengan perintah berikut. Ini juga menciptakan `SparkApplication` objek yang disebut`spark-pi`:

```
kubectl apply -f spark-pi.yaml
```

4. Periksa peristiwa untuk `SparkApplication` objek dengan perintah berikut:

```
kubectl describe pods spark-pi-driver --namespace spark-operator
```

Peristiwa pod pertama akan menunjukkan bahwa Volcano telah menjadwalkan Pod:

```
Type    Reason     Age   From               Message
----    ------     ----  ----               -------
Normal  Scheduled  23s   volcano            Successfully assigned default/spark-
pi-driver to integration-worker2
```

Jalankan aplikasi Spark dengan Volcano scheduler dengan **`spark-submit`**

1. Pertama, selesaikan langkah-langkah di Menyiapkan spark-submit untuk Amazon EMR di EKS bagian ini. Anda harus membangun `spark-submit` distribusi Anda dengan dukungan Volcano.

Untuk informasi selengkapnya, lihat bagian Build dari Using Volcano as Customized Scheduler for Spark on Kubernetes dalam dokumentasi Apache Spark.

2. Tetapkan nilai untuk variabel lingkungan berikut:

```
export SPARK_HOME=spark-home
export MASTER_URL=k8s://Amazon-EKS-cluster-endpoint
```

3. Kirimkan aplikasi Spark dengan perintah berikut:

```
$SPARK_HOME/bin/spark-submit \
 --class org.apache.spark.examples.SparkPi \
 --master $MASTER_URL \
 --conf spark.kubernetes.container.image=895885662937.dkr.ecr.us-
west-2.amazonaws.com/spark/emr-6.10.0:latest \
 --conf spark.kubernetes.authenticate.driver.serviceAccountName=spark \
 --deploy-mode cluster \
 --conf spark.kubernetes.namespace=spark-operator \
 --conf spark.kubernetes.scheduler.name=volcano \
 --conf spark.kubernetes.scheduler.volcano.podGroupTemplateFile=/path/to/podgroup-
template.yaml \
 --conf
 spark.kubernetes.driver.pod.featureSteps=org.apache.spark.deploy.k8s.features.VolcanoFeatu
 \
 --conf
 spark.kubernetes.executor.pod.featureSteps=org.apache.spark.deploy.k8s.features.VolcanoFea
 \
 local:///usr/lib/spark/examples/jars/spark-examples.jar 20
```

4. Periksa peristiwa untuk `SparkApplication` objek dengan perintah berikut:

```
kubectl describe pod spark-pi --namespace spark-operator
```

Peristiwa pod pertama akan menunjukkan bahwa Volcano telah menjadwalkan Pod:

```
Type    Reason     Age   From               Message
----    ------     ----  ----               -------
Normal  Scheduled  23s   volcano            Successfully assigned default/spark-
pi-driver to integration-worker2
```

Menggunakan YuniKorn sebagai penjadwal khusus untuk Apache Spark di Amazon EMR di EKS

Dengan Amazon EMR di EKS, Anda dapat menggunakan operator Spark atau spark-submit untuk menjalankan pekerjaan Spark dengan penjadwal kustom Kubernetes. Tutorial ini mencakup cara menjalankan pekerjaan Spark dengan YuniKorn penjadwal pada antrian kustom dan penjadwalan geng.

Gambaran Umum

Apache YuniKorn dapat membantu mengelola penjadwalan Spark dengan penjadwalan sadar aplikasi sehingga Anda dapat memiliki kontrol yang baik pada kuota dan prioritas sumber daya. Dengan penjadwalan geng, YuniKorn jadwalkan aplikasi hanya jika permintaan sumber daya minimal untuk aplikasi dapat dipenuhi. Untuk informasi lebih lanjut, lihat Apa itu penjadwalan geng di situs YuniKorn dokumentasi Apache.

Buat klaster Anda dan siapkan YuniKorn

Gunakan langkah-langkah berikut untuk menerapkan klaster Amazon EKS. Anda dapat mengubah Wilayah AWS (`region`) dan Availability Zones (`availabilityZones`).

1. Tentukan klaster Amazon EKS:

```
cat <<EOF >eks-cluster.yaml
---
apiVersion: eksctl.io/v1alpha5
kind: ClusterConfig

metadata:
  name: emr-eks-cluster
  region: eu-west-1

vpc:
  clusterEndpoints:
    publicAccess: true
    privateAccess: true

iam:
  withOIDC: true
```

```
nodeGroups:
  - name: spark-jobs
    labels: { app: spark }
    instanceType: m5.xlarge
    desiredCapacity: 2
    minSize: 2
    maxSize: 3
    availabilityZones: ["eu-west-1a"]
EOF
```

2. Buat klaster:

```
eksctl create cluster -f eks-cluster.yaml
```

3. Buat namespace `spark-job` tempat Anda akan mengeksekusi pekerjaan Spark:

```
kubectl create namespace spark-job
```

4. Selanjutnya, buat role dan role binding Kubernetes. Ini diperlukan untuk akun layanan yang digunakan oleh pekerjaan Spark.

   a. Tentukan akun layanan, peran, dan pengikatan peran untuk pekerjaan Spark.

```
cat <<EOF >emr-job-execution-rbac.yaml
---
apiVersion: v1
kind: ServiceAccount
metadata:
  name: spark-sa
  namespace: spark-job
automountServiceAccountToken: false
---
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  name: spark-role
  namespace: spark-job
rules:
  - apiGroups: ["", "batch","extensions"]
    resources: ["configmaps","serviceaccounts","events","pods","pods/
exec","pods/log","pods/
portforward","secrets","services","persistentvolumeclaims"]
    verbs: ["create","delete","get","list","patch","update","watch"]
```

```
---
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: spark-sa-rb
  namespace: spark-job
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: Role
  name: spark-role
subjects:
  - kind: ServiceAccount
    name: spark-sa
    namespace: spark-job
EOF
```

b. Terapkan definisi role dan role binding Kubernetes dengan perintah berikut:

```
kubectl apply -f emr-job-execution-rbac.yaml
```

Instal dan atur YuniKorn

1. Gunakan perintah kubectl berikut untuk membuat namespace untuk men-deploy penjadwal `yunikorn` Yunikorn:

```
kubectl create namespace yunikorn
```

2. Untuk menginstal scheduler, jalankan perintah Helm berikut:

```
helm repo add yunikorn https://apache.github.io/yunikorn-release
```

```
helm repo update
```

```
helm install yunikorn yunikorn/yunikorn --namespace yunikorn
```

Jalankan aplikasi Spark dengan YuniKorn scheduler dengan operator Spark

1. Jika Anda belum melakukannya, selesaikan langkah-langkah di bagian berikut untuk menyiapkan:

   a. Buat klaster Anda dan siapkan YuniKorn

   b. Instal dan atur YuniKorn

   c. Menyiapkan operator Spark untuk Amazon EMR di EKS

   d. Instal operator Spark

   Sertakan argumen berikut saat Anda menjalankan `helm install spark-operator-demo` perintah:

   ```
   --set batchScheduler.enable=true
   --set webhook.enable=true
   ```

2. Buat file `SparkApplication` definisi`spark-pi.yaml`.

   Untuk digunakan YuniKorn sebagai penjadwal untuk pekerjaan Anda, Anda harus menambahkan anotasi dan label tertentu ke definisi aplikasi Anda. Anotasi dan label menentukan antrian untuk pekerjaan Anda dan strategi penjadwalan yang ingin Anda gunakan.

   Pada contoh berikut, anotasi `schedulingPolicyParameters` mengatur penjadwalan geng untuk aplikasi. Kemudian, contoh membuat grup tugas, atau “geng” tugas, untuk menentukan kapasitas minimum yang harus tersedia sebelum menjadwalkan Pod untuk memulai eksekusi pekerjaan. Dan akhirnya, itu menentukan dalam definisi kelompok tugas untuk menggunakan kelompok simpul dengan `"app": "spark"` label, seperti yang didefinisikan dalam Buat klaster Anda dan siapkan YuniKorn bagian.

   ```
   apiVersion: "sparkoperator.k8s.io/v1beta2"
   kind: SparkApplication
   metadata:
     name: spark-pi
     namespace: spark-job
   spec:
     type: Scala
     mode: cluster
     image: "895885662937.dkr.ecr.us-west-2.amazonaws.com/spark/emr-6.10.0:latest"
     imagePullPolicy: Always
     mainClass: org.apache.spark.examples.SparkPi
   ```

```
  mainApplicationFile: "local:///usr/lib/spark/examples/jars/spark-examples.jar"
  sparkVersion: "3.3.1"
  restartPolicy:
    type: Never
  volumes:
    - name: "test-volume"
      hostPath:
        path: "/tmp"
        type: Directory
  driver:
    cores: 1
    coreLimit: "1200m"
    memory: "512m"
    labels:
      version: 3.3.1
    annotations:
      yunikorn.apache.org/schedulingPolicyParameters: "placeholderTimeoutSeconds=30
gangSchedulingStyle=Hard"
      yunikorn.apache.org/task-group-name: "spark-driver"
      yunikorn.apache.org/task-groups: |-
        [{
            "name": "spark-driver",
            "minMember": 1,
            "minResource": {
              "cpu": "1200m",
              "memory": "1Gi"
            },
            "nodeSelector": {
              "app": "spark"
            }
          },
          {
            "name": "spark-executor",
            "minMember": 1,
            "minResource": {
              "cpu": "1200m",
              "memory": "1Gi"
            },
            "nodeSelector": {
              "app": "spark"
            }
        }]
    serviceAccount: spark-sa
    volumeMounts:
```

```
      - name: "test-volume"
        mountPath: "/tmp"
  executor:
    cores: 1
    instances: 1
    memory: "512m"
    labels:
      version: 3.3.1
    annotations:
      yunikorn.apache.org/task-group-name: "spark-executor"
    volumeMounts:
      - name: "test-volume"
        mountPath: "/tmp"
```

3. Kirim aplikasi Spark dengan perintah berikut. Ini juga menciptakan `SparkApplication` objek yang disebut`spark-pi`:

```
kubectl apply -f spark-pi.yaml
```

4. Periksa peristiwa untuk `SparkApplication` objek dengan perintah berikut:

```
kubectl describe sparkapplication spark-pi --namespace spark-job
```

Peristiwa Pod pertama akan menunjukkan bahwa YuniKorn telah menjadwalkan Pod:

```
Type    Reason            Age   From                         Message
----    ------            ----  ----                         -------
Normal Scheduling        3m12s yunikorn   spark-operator/org-apache-spark-examples-
sparkpi-2a777a88b98b8a95-driver is queued and waiting for allocation
Normal GangScheduling    3m12s yunikorn   Pod belongs to the taskGroup spark-
driver, it will be scheduled as a gang member
Normal Scheduled         3m10s yunikorn   Successfully assigned spark
Normal PodBindSuccessful 3m10s yunikorn   Pod spark-operator/
Normal TaskCompleted     2m3s  yunikorn   Task spark-operator/
Normal Pulling           3m10s kubelet    Pulling
```

Jalankan aplikasi Spark dengan YuniKorn scheduler dengan `spark-submit`

1. Pertama, selesaikan langkah-langkah di Menyiapkan spark-submit untuk Amazon EMR di EKS bagian ini.
2. Tetapkan nilai untuk variabel lingkungan berikut:

```
export SPARK_HOME=spark-home
export MASTER_URL=k8s://Amazon-EKS-cluster-endpoint
```

3. Kirimkan aplikasi Spark dengan perintah berikut:

   Pada contoh berikut, anotasi `schedulingPolicyParameters` mengatur penjadwalan geng untuk aplikasi. Kemudian, contoh membuat grup tugas, atau “geng” tugas, untuk menentukan kapasitas minimum yang harus tersedia sebelum menjadwalkan Pod untuk memulai eksekusi pekerjaan. Dan akhirnya, itu menentukan dalam definisi kelompok tugas untuk menggunakan kelompok simpul dengan `"app": "spark"` label, seperti yang didefinisikan dalam Buat klaster Anda dan siapkan YuniKorn bagian.

```
$SPARK_HOME/bin/spark-submit \
 --class org.apache.spark.examples.SparkPi \
 --master $MASTER_URL \
 --conf spark.kubernetes.container.image=895885662937.dkr.ecr.us-
west-2.amazonaws.com/spark/emr-6.10.0:latest \
 --conf spark.kubernetes.authenticate.driver.serviceAccountName=spark-sa \
 --deploy-mode cluster \
 --conf spark.kubernetes.namespace=spark-job \
 --conf spark.kubernetes.scheduler.name=yunikorn \
 --conf spark.kubernetes.driver.annotation.yunikorn.apache.org/
schedulingPolicyParameters="placeholderTimeoutSeconds=30 gangSchedulingStyle=Hard"
 \
 --conf spark.kubernetes.driver.annotation.yunikorn.apache.org/task-group-
name="spark-driver" \
 --conf spark.kubernetes.executor.annotation.yunikorn.apache.org/task-group-
name="spark-executor" \
 --conf spark.kubernetes.driver.annotation.yunikorn.apache.org/task-groups='[{
            "name": "spark-driver",
            "minMember": 1,
            "minResource": {
              "cpu": "1200m",
              "memory": "1Gi"
```

```
            },
            "nodeSelector": {
              "app": "spark"
            }
          },
          {
            "name": "spark-executor",
            "minMember": 1,
            "minResource": {
              "cpu": "1200m",
              "memory": "1Gi"
            },
            "nodeSelector": {
              "app": "spark"
            }
        }]' \
 local:///usr/lib/spark/examples/jars/spark-examples.jar 20
```

4. Periksa peristiwa untuk `SparkApplication` objek dengan perintah berikut:

```
kubectl describe pod spark-driver-pod --namespace spark-job
```

Peristiwa Pod pertama akan menunjukkan bahwa YuniKorn telah menjadwalkan Pod:

```
Type    Reason           Age   From                          Message
----    ------           ----  ----                          -------
Normal Scheduling        3m12s yunikorn   spark-operator/org-apache-spark-examples-
sparkpi-2a777a88b98b8a95-driver is queued and waiting for allocation
Normal GangScheduling    3m12s yunikorn   Pod belongs to the taskGroup spark-
driver, it will be scheduled as a gang member
Normal Scheduled         3m10s yunikorn   Successfully assigned spark
Normal PodBindSuccessful 3m10s yunikorn   Pod spark-operator/
Normal TaskCompleted     2m3s  yunikorn   Task spark-operator/
Normal Pulling           3m10s kubelet    Pulling
```

Keamanan di Amazon EMR di EKS

Keamanan cloud di AWS merupakan prioritas tertinggi. Sebagai pelanggan AWS, Anda 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 menggambarkan ini sebagai keamanan dari cloud dan keamanan di dalam cloud:

- Keamanan cloud – AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan layanan–layanan AWS di dalam AWS Cloud. AWS juga memberikan Anda layanan yang dapat digunakan dengan aman. Auditor pihak ketiga menguji dan memverifikasi secara berkala efektivitas keamanan kami sebagai bagian dari AWSProgram Kepatuhan. Untuk mempelajari tentang program kepatuhan yang berlaku untuk Amazon EMR, lihat AWSLayanan dalam Lingkup berdasarkan AWS Layanan Program Kepatuhan dalam Lingkup oleh Program .
- Keamanan dalam cloud – Tanggung jawab Anda ditentukan oleh layanan AWS yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain termasuk sensitivitas data Anda, persyaratan perusahaan Anda, serta hukum dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan Amazon EMR di EKS. Topik berikut menunjukkan kepada Anda cara mengonfigurasi Amazon EMR di EKS untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga akan mempelajari cara menggunakan layanan AWS lain yang dapat membantu Anda memantau dan mengamankan sumber daya Amazon EMR di EKS Anda.

Topik

- Analisis konfigurasi dan kerentanan
- Connect ke Amazon EMR di EKS Menggunakan VPC endpoints
- Atur akses lintas akun untuk Amazon EMR di EKS

Praktik terbaik keamanan Amazon EMR di EKS

Amazon EMR di EKS menyediakan sejumlah fitur keamanan untuk dipertimbangkan ketika Anda mengembangkan dan menerapkan kebijakan keamanan Anda sendiri. Praktik terbaik berikut adalah pedoman umum dan tidak mewakili solusi keamanan yang lengkap. Karena praktik terbaik ini mungkin tidak sesuai atau cukup untuk lingkungan Anda, anggap praktik terbaik tersebut sebagai pertimbangan yang membantu dan bukan sebagai rekomendasi.

> **Note**
>
> Untuk praktik terbaik keamanan AmazonPraktik terbaik keamanan Amazon EMR di EKS.

Terapkan prinsip hak istimewa paling rendah

Amazon EMR di EKS menyediakan kebijakan akses granular untuk aplikasi menggunakan IAM role, seperti peran eksekusi. Peran eksekusi ini dipetakan ke akun layanan Kubernetes melalui kebijakan kepercayaan IAM role. Amazon EMR di EKS menciptakan pod dalam namespace Amazon EKS terdaftar yang mengeksekusi kode aplikasi yang disediakan pengguna. Pod tugas yang menjalankan kode aplikasi mengasumsikan peran eksekusi ketika menghubungkan ke layanan AWS lain. Kami merekomendasikan bahwa peran eksekusi diberikan hanya seperangkat minimum hak istimewa yang diperlukan oleh tugas, seperti mencakup aplikasi Anda dan akses ke tujuan log. Kami juga merekomendasikan mengaudit tugas untuk izin secara teratur dan pada setiap perubahan pada kode aplikasi.

Daftar kontrol akses untuk titik akhir

Titik akhir terkelola dapat dibuat hanya untuk klaster EKS yang telah dikonfigurasi untuk menggunakan setidaknya satu subnet privat di VPC Anda. Konfigurasi ini membatasi akses ke penyeimbang beban yang dibuat oleh titik akhir terkelola sehingga mereka hanya dapat diakses dari VPC Anda. Untuk lebih meningkatkan keamanan, kami sarankan Anda mengonfigurasi grup keamanan dengan penyeimbang beban ini sehingga mereka dapat membatasi lalu lintas masuk ke serangkaian alamat IP yang dipilih.

Dapatkan pembaruan keamanan terbaru untuk gambar kustom

Untuk menggunakan gambar kustom dengan Amazon EMR di EKS, Anda dapat menginstal biner dan perpustakaan pada gambar. Anda bertanggung jawab untuk patch keamanan biner yang Anda tambahkan ke gambar. Gambar Amazon EMR di EKS secara teratur di-patch dengan patch keamanan terbaru. Untuk mendapatkan gambar terbaru, Anda harus membangun kembali gambar kustom setiap kali ada versi gambar dasar baru dari rilis Amazon EMR. Untuk informasi lebih lanjut, lihat Amazon EMR pada rilis EKS dan Cara memilih URI gambar dasar.

Batasi akses kredensial pod

Kubernetes mendukung beberapa metode penetapan kredensial ke pod. Penyediaan beberapa penyedia kredensial dapat meningkatkan kompleksitas model keamanan Anda. Amazon EMR di EKS telah mengadopsi penggunaan IAM role untuk akun layanan (IRSA) sebagai penyedia kredensial standar dalam namespace EKS terdaftar. Metode lain tidak didukung, termasuk kube2iam, kiam dan menggunakan profil instans EC2 dari instans yang berjalan di klaster.

Mengisolasi kode aplikasi yang tidak tepercaya

Amazon EMR di EKS tidak memeriksa integritas kode aplikasi yang dikirimkan oleh pengguna sistem. Jika Anda menjalankan klaster virtual multi-tenanted yang dikonfigurasi menggunakan beberapa peran eksekusi yang dapat digunakan untuk mengirimkan tugas oleh penyewa tidak tepercaya yang menjalankan kode arbitrer, ada risiko aplikasi berbahaya meningkatkan hak istimewanya. Dalam situasi ini, pertimbangkan untuk mengisolasi peran eksekusi dengan hak istimewa yang sama ke klaster virtual yang berbeda.

Izin kontrol akses berbasis peran (RBAC)

Administrator harus mengontrol ketat izin kontrol akses berbasis peran (RBAC) untuk namespace terkelola Amazon EMR di EKS. Minimal, izin berikut tidak boleh diberikan kepada pengirim tugas di namespace terkelola Amazon EMR di EKS.

- Izin Kubernetes RBAC untuk memodifikasi configmap - karena Amazon EMR di EKS menggunakan configmap Kubernetes untuk menghasilkan templat pod terkelola yang memiliki nama akun layanan terkelola. Atribut ini seharusnya tidak bermutasi.
- Izin Kubernetes RBAC untuk exec ke pod Amazon EMR di EKS - untuk menghindari memberikan akses ke templat pod terkelola yang memiliki nama SA terkelola. Atribut ini seharusnya tidak bermutasi. Izin ini juga dapat memberikan akses ke token JWT dipasang ke pod yang kemudian dapat digunakan untuk mengambil kredensial peran eksekusi.

- Izin Kubernetes RBAC untuk membuat pod untuk mencegah pengguna membuat pod menggunakan Kubernetes ServiceAccount yang dapat dipetakan ke IAM role dengan keistimewaan lebih banyak dari pengguna. AWS
- Izin Kubernetes RBAC untuk menyebarkan webhook bermutasi - untuk mencegah pengguna menggunakan webhook bermutasi untuk memutasikan nama Kubernetes untuk pod yang dibuat oleh Amazon EMR di EKS. ServiceAccount
- Izin RBAC Kubernetes untuk membaca rahasia Kubernetes - untuk mencegah pengguna membaca data rahasia yang tersimpan dalam rahasia ini.

Membatasi akses ke nodegroup IAM role atau kredensial profil instans

- Kami menyarankan agar Anda menetapkan izin AWS minimum untuk nodegroup IAM role. Ini membantu untuk menghindari eskalasi hak istimewa dengan kode yang dapat dijalankan menggunakan kredensial profil instans dari simpul pekerja EKS.
- Untuk memblokir akses sepenuhnya ke kredensial profil isntans untuk semua pod yang berjalan di namespace terkelola Amazon EMR di EKS, kami sarankan Anda menjalankan perintah `iptables` pada simpul EKS. Untuk informasi lebih lanjut, lihat Membatasi akses ke kredensial profil instans Amazon EC2. Namun, penting untuk mencakup dengan benar IAM role akun layanan Anda sehingga pod Anda memiliki semua izin yang diperlukan. Sebagai contoh, IAM role simpul diberikan izin untuk menarik gambar kontainer dari Amazon ECR. Jika pod tidak ditugaskan izin tersebut, pod tidak dapat menarik gambar kontainer dari Amazon ECR. Plugin VPC CNI juga perlu diperbarui. Untuk informasi lebih lanjut, lihat Panduan: Memperbarui plugin VPC CNI untuk menggunakan IAM role untuk akun layanan.

Perlindungan data

AWS model tanggung jawab bersama diterapkan untuk perlindungan data di Amazon EMR di EKS. Sebagaimana diuraikan dalam model ini, AWS bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua CloudAWS. Anda bertanggung jawab untuk memelihara kontrol terhadap konten Anda yang di-hosting pada infrastruktur ini. Konten ini meliputi konfigurasi keamanan dan tugas manajemen untuk berbagai layanan AWS yang Anda gunakan. Untuk informasi selengkapnya tentang privasi data, lihat FAQ Privasi Data . Untuk informasi tentang perlindungan data di Eropa, lihat postingan blog Model Tanggung Jawab Bersama dan GDPR AWS di Blog Keamanan AWS.

Untuk tujuan perlindungan data, kami menyarankan agar Anda melindungi kredensyalAWS akun dan mengatur akun individu denganAWS Identity and Access Management (IAM). Dengan cara seperti itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugas mereka. Kami juga merekomendasikan agar Anda mengamankan data Anda dengan cara-cara berikut ini:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk melakukan komunikasi dengan sumber daya AWS. Kami merekomendasikan TLS 1.2 atau versi yang lebih baru.
- Siapkan API dan log aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi enkripsi AWS, bersama dengan semua kontrol keamanan default dalam layanan AWS.
- Gunakan layanan keamanan terkelola tingkat lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data pribadi yang disimpan di Amazon S3.
- Gunakan opsi enkripsi Amazon EMR di EKS pada opsi enkripsi untuk mengenkripsi data at rest dan transit.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 ketika mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Untuk informasi lebih lanjut tentang titik akhir FIPS yang tersedia, lihat Standar Pemrosesan Informasi Federal (FIPS) 140-2.

Kami sangat merekomendasikan agar Anda tidak memasukkan informasi identifikasi sensitif apapun, seperti nomor rekening pelanggan Anda, ke dalam kolom isian teks bebas seperti kolom Nama. Hal ini termasuk ketika Anda bekerja dengan Amazon EMR di EKS atau layanan AWS lainnya dengan menggunakan konsol, API, AWS CLI, atau SDK AWS. Data apa pun yang Anda masukkan ke dalam Amazon EMR di EKS atau layanan lain mungkin akan diambil untuk dimasukkan ke dalam log diagnostik. Saat Anda menyediakan URL ke peladen eksternal, jangan menyertakan informasi kredensial dalam URL untuk memvalidasi permintaan Anda ke peladen tersebut.

Enkripsi saat istirahat

Enkripsi data membantu mencegah pengguna yang tidak sah membaca data pada klaster dan sistem penyimpanan data terkait. Ini termasuk data yang disimpan ke media persisten, yang dikenal sebagai data at rest, dan data yang mungkin dicegat saat perjalanan jaringan, yang dikenal sebagai data dalam transit.

Enkripsi data memerlukan kunci dan sertifikat. Anda dapat memilih dari beberapa opsi, termasuk kunci yang dikelola oleh AWS Key Management Service, kunci yang dikelola oleh Amazon S3, dan kunci dan sertifikat dari penyedia kustom yang Anda suplai. Saat menggunakan AWS KMS sebagai penyedia kunci Anda, biaya berlaku untuk penyimpanan dan penggunaan kunci enkripsi. Untuk informasi lebih lanjut, lihat AWS KMS Harga.

Sebelum Anda menentukan opsi enkripsi, tentukan sistem manajemen kunci dan sertifikat yang ingin Anda gunakan. Kemudian buat kunci dan sertifikat untuk penyedia kustom yang Anda tentukan sebagai bagian dari pengaturan enkripsi.

Enkripsi saat istirahat untuk data EMRFS di Amazon S3

Enkripsi Amazon S3 bekerja dengan objek EMR File System (EMRFS) yang dibaca dari dan ditulis ke Amazon S3. Anda menentukan Amazon S3 server-side encryption (SSE) atau client-side encryption (CSE) sebagai Mode enkripsi default saat Anda mengaktifkan enkripsi saat istirahat. Secara opsional, Anda dapat menentukan metode enkripsi yang berbeda untuk setiap bucket menggunakan Per penimpaan enkripsi bucket. Keamanan Lapisan Pengangkutan (TLS) terlepas dari apakah enkripsi Amazon S3 diaktifkan, Keamanan Lapisan Pengangkutan (TLS) mengenkripsi objek EMRFS dalam transit antara simpul klaster EMR dan Amazon S3. Untuk informasi selengkapnya tentang enkripsi Amazon S3, lihat Melindungi Data Menggunakan Enkripsi di Panduan Developer Amazon Simple Storage Service.

> **Note**
>
> Saat Anda menggunakan AWS KMS, biaya berlaku untuk penyimpanan dan penggunaan kunci enkripsi. Untuk informasi lebih lanjut, lihat AWS KMS Harga.

Enkripsi sisi server Amazon S3

Saat Anda mengatur enkripsi sisi server Amazon S3, Amazon S3 akan mengenkripsi data pada tingkat objek saat menulis data ke disk dan mendekripsi data saat diakses. Untuk informasi selengkapnya, lihat Melindungi Data Menggunakan Enkripsi Sisi Server di Panduan Developer Amazon Simple Storage Service.

Anda dapat memilih antara dua sistem pengelolaan kunci yang berbeda ketika Anda menentukan SSE di Amazon EMR di EKS:

- SSE-S3 - Amazon S3 mengelola kunci untuk Anda.

- SSE-KMS - Anda menggunakan sebuahAWS KMS key untuk mengatur kebijakan yang cocok untuk Amazon EMR di EKS.

SSE dengan kunci yang disediakan pelanggan (SSE-C) tidak tersedia untuk digunakan dengan Amazon EMR di EKS.

Enkripsi di sisi klien Amazon S3

Dengan enkripsi sisi klien Amazon S3, enkripsi dan dekripsi Amazon S3 dilakukan di klien EMRFS pada klaster Anda. Objek dienkripsi sebelum diunggah ke Amazon S3 dan didekripsi setelah diunduh. Penyedia yang Anda tentukan menyediakan kunci enkripsi yang digunakan klien. Klien dapat menggunakan kunci yang disediakan melaluiAWS KMS (CSE-KMS) atau kelas Java khusus yang menyediakan kunci utama sisi klien (CSE-C). Spesifikasi enkripsi sedikit berbeda antara CSE-KMS dan CSE-C, tergantung pada penyedia yang ditentukan dan metadata objek yang didekripsi atau dienkripsi. Untuk informasi selengkapnya, tentang perbedaan ini, lihat Melindungi Data Menggunakan Enkripsi Di Sisi Klien di Panduan Developer Amazon Simple Storage Service.

> **Note**
>
> Amazon S3 CSE hanya memastikan bahwa data EMRFS yang dipertukarkan dengan Amazon S3 dienkripsi; tidak semua data pada volume instans klaster dienkripsi. Selain itu, karena Hue tidak menggunakan EMRFS, objek yang Hue S3 File Browser tulis ke Amazon S3 tidak dienkripsi.

Enkripsi disk lokal

Apache Spark mendukung mengenkripsi data sementara ditulis ke disk lokal. Ini mencakup file acak, spill acak, dan blok data yang disimpan pada disk untuk variabel baik caching maupun siaran. Ini tidak mencakup enkripsi data output yang dihasilkan oleh aplikasi dengan API seperti `saveAsHadoopFile` atau `saveAsTable`. Ini juga mungkin tidak mencakup file sementara yang dibuat secara eksplisit oleh pengguna. Untuk informasi selengkapnya, lihat Enkripsi Penyimpanan Lokal dalam dokumentasi Spark. Spark tidak mendukung data terenkripsi pada disk lokal, seperti data menengah yang ditulis ke disk lokal oleh proses eksekutor ketika data tidak cocok dalam memori. Data yang bertahan ke disk dicakup untuk waktu aktif tugas, dan kunci yang digunakan untuk mengenkripsi data dihasilkan secara dinamis oleh Spark untuk setiap tugas berjalan. Setelah pekerjaan Spark berakhir, tidak ada proses lain yang dapat mendekripsi data.

Untuk driver dan pod eksekutor, Anda mengenkripsi data at rest yang bertahan untuk volume terpasang. Ada tiga perbedaan pilihan penyimpanan asli AWS yang dapat Anda gunakan dengan Kubernetes: EBS, EFS, dan FSx for Lustre. Ketiganya menawarkan enkripsi at rest menggunakan kunci terkelola layanan atau kunci terkelola layanan atauAWS KMS key. Untuk informasi selengkapnya lihat Panduan Praktik Terbaik EKS. Dengan pendekatan ini, semua data yang disimpan ke volume terpasang dienkripsi.

Manajemen kunci

Anda dapat mengonfigurasi KMS untuk secara otomatis merotasi kunci KMS Anda. Ini merotasi kunci Anda setahun sekali sambil menyimpan kunci lama tanpa batas waktu sehingga data Anda masih dapat didekripsi. Untuk informasi tambahan, lihat MerotasiAWS KMS keys.

Enkripsi dalam transit

Beberapa mekanisme enkripsi diaktifkan dengan enkripsi dalam transit. Ini adalah fitur sumber daya terbuka, khusus aplikasi, dan dapat bervariasi dengan rilis Amazon EMR di EKS. Fitur enkripsi khusus aplikasi berikut dapat diaktifkan dengan Amazon EMR di EKS:

- Spark
  - Komunikasi RPC internal antara komponen Spark, seperti layanan transfer blok dan layanan shuffle eksternal, dienkripsi menggunakan cipher AES-256 di Amazon EMR versi 5.9.0 dan versi terbaru. Di rilis sebelumnya, komunikasi RPC internal dienkripsi menggunakan SASL dengan DIGEST-MD5 sebagai cipher.
  - Komunikasi protokol HTTP dengan antarmuka pengguna seperti Spark History Server dan server file HTTPS-enabled dienkripsi menggunakan konfigurasi SSL Spark. Untuk informasi lebih lanjut, lihat Konfigurasi SSL di dokumentasi Spark.

  Untuk informasi lebih lanjut, lihat Pengaturan keamanan Spark.
- Anda sebaiknya hanya mengizinkan koneksi terenkripsi melalui HTTPS (TLS) menggunakan SecureTransport kondisi aws: di kebijakan IAM bucket Amazon S3.
- Hasil kueri yang di-stream ke klien JDBC atau ODBC dienkripsi menggunakan TLS.

Manajemen Identitas dan Akses

(IAM) AWS Identity and Access Management adalah Layanan AWS yang membantu seorang administrator dalam mengendalikan akses ke sumber daya AWS secara aman. Administrator IAM

mengontrol siapa yang dapat diautentikasi (masuk) dan diotorisasi (memiliki izin) untuk menggunakan sumber daya Amazon EMR di EKS. IAM adalah sebuah layanan Layanan AWS yang dapat Anda gunakan tanpa dikenakan biaya tambahan.

Topik

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan di Amazon EMR di EKS.

Pengguna layanan – Jika Anda menggunakan layanan Amazon EMR di EKS untuk melakukan tugas Anda, administrator Anda akan memberikan kredensial dan izin yang dibutuhkan. Saat Anda menggunakan lebih banyak fitur Amazon EMR di EKS untuk melakukan pekerjaan, Anda mungkin memerlukan izin tambahan. Memahami bagaimana cara mengelola akses dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di Amazon EMR di EKS, lihat Memecahkan Masalah identitas dan akses Amazon EMR di EKS.

Administrator layanan – Jika Anda bertanggung jawab atas sumber daya Amazon EMR di EKS di perusahaan Anda, Anda mungkin memiliki akses penuh ke Amazon EMR di EKS. Tugas Anda adalah menentukan EMR Amazon mana pada fitur dan sumber daya EKS yang harus diakses pengguna layanan Anda. Kemudian, Anda harus mengirimkan permintaan kepada administrator IAM Anda untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep Basic IAM. Untuk mempelajari selengkapnya tentang cara perusahaan Anda dapat menggunakan IAM dengan Amazon EMR di EKS, lihat Bagaimana Amazon EMR di EKS bekerja dengan IAM.

Administrator IAM – Jika Anda adalah administrator IAM, Anda mungkin ingin belajar dengan lebih terperinci tentang cara Anda dapat menulis kebijakan untuk mengelola akses ke Amazon EMR di EKS. Untuk melihat contoh kebijakan berbasis identitas Amazon EMR di EKS yang dapat Anda gunakan di IAM, lihat Contoh kebijakan berbasis identitas untuk Amazon EMR di EKS.

Mengautentikasi menggunakan identitas

Autentikasi merupakan cara Anda untuk masuk ke AWS dengan menggunakan kredensial identitas Anda. Anda harus terautentikasi (masuk keAWS) sebagai Pengguna root akun AWS, sebagai pengguna IAM, atau dengan mengambil peran IAM.

Anda dapat masuk ke AWS sebagai identitas terfederasi dengan menggunakan kredensial yang disediakan melalui sumber identitas. AWS IAM Identity Center Para pengguna (Pusat Identitas IAM), otentikasi sign-on tunggal perusahaan Anda, dan kredensial Google atau Facebook Anda merupakan contoh identitas terfederasi. Saat Anda masuk sebagai identitas terfederasi, administrator Anda sebelumnya menyiapkan federasi identitas dengan menggunakan peran IAM. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil suatu peran.

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

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 kredensial Anda. Jika Anda tidak menggunakan peralatan AWS, maka Anda harus menandatangani sendiri permintaan tersebut. Untuk informasi selengkapnya tentang penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, silakan lihat Menandatangani permintaan API AWS di Panduan Pengguna IAM.

Terlepas dari metode autentikasi yang Anda gunakan, Anda mungkin juga diminta untuk menyediakan informasi keamanan tambahan. Sebagai contoh, AWS menyarankan supaya Anda menggunakan autentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari selengkapnya, silakan lihat Autentikasi multi-faktor di Panduan Pengguna AWS IAM Identity Center dan Menggunakan autentikasi multi-faktor (MFA) di AWS di Panduan Pengguna IAM.

Pengguna root Akun AWS

Ketika Anda membuat Akun AWS, Anda memulai dengan satu identitas masuk yang memiliki akses ke semua Layanan AWS dan sumber daya di akun tersebut. Identitas ini disebut pengguna root

Akun AWS dan diakses dengan cara masuk ke alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan 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, silakan lihat Tugas yang memerlukan kredensial pengguna root di Panduan Pengguna IAM.

Identitas terfederasi

Praktik terbaiknya berupa, mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS dengan menggunakan kredensial temporer.

Identitas terfederasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, dikenal sebagai AWS Directory Service, direktori Pusat Identitas, atau pengguna mana pun yang mengakses Layanan AWS dengan menggunakan kredensial yang disediakan melalui sumber identitas. Ketika identitas terfederasi mengakses Akun AWS, identitas tersebut mengambil peran, dan peran memberikan kredensial temporer.

Untuk pengelolaan akses terpusat, kami sarankan Anda menggunakanAWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat Identitas IAM, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua Akun AWS Anda dan aplikasi Anda. Untuk informasi tentang Pusat Identitas IAM, silakan lihat Apakah Pusat Identitas IAM itu? di User Guide AWS IAM Identity Center.

Pengguna dan Grup IAM

Pengguna IAM adalah identitas dalam Akun AWS Anda yang memiliki izin khusus untuk satu orang atau aplikasi. Apabila memungkinkan, kami menyarankan untuk mengandalkan pada kredensial temporer alih-alih membuat pengguna IAM yang memiliki kredensyal jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan khusus yang memerlukan kredensial jangka panjang dengan pengguna IAM, kami menyarankan Anda memutar kunci akses. Untuk informasi selengkapnya, silakan lihat Memutar kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang di Panduan Pengguna IAM.

Grup IAM adalah identitas yang menerangkan secara spesifik kumpulan pengguna IAM. Anda tidak dapat masuk sebagai kelompok. Anda dapat menggunakan grup untuk menerangkan secara spesifik izin untuk beberapa pengguna sekaligus. Grup membuat izin lebih mudah dikelola untuk

sekelompok besar pengguna. Sebagai contoh, Anda dapat memiliki grup yang diberi nama AdminIAM dan memberikan izin kepada grup tersebut untuk mengelola sumber daya IAM.

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

Peran IAM

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

IAM role dengan kredensial temporer berguna dalam situasi berikut:

- Akses pengguna gabungan – Untuk menetapkan izin ke sebuah identitas terfederasi, Anda harus membuat sebuah peran dan menentukan izin untuk peran tersebut. Ketika identitas gabungan terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberikan izin yang ditentukan oleh peran. Untuk informasi tentang peran-peran untuk federasi, silakan lihat Membuat sebuah peran untuk Penyedia Identitas pihak ketiga di Panduan Pengguna IAM. Jika Anda menggunakan Pusat Identitas IAM, Anda mengonfigurasi serangkain izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas tersebut diautentikasi, Pusat Identitas IAM mengkorelasikan izin yang diatur ke peran dalam IAM. Untuk informasi tentang rangkaian izin, silakan lihat Rangkaian izin di Panduan Pengguna AWS IAM Identity Center.
- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM untuk sementara mengambil izin berbeda untuk tugas tertentu.
- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (pengguna utama tepercaya) di akun berbeda untuk mengakses sumber daya yang ada di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, pada beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan suatu peran sebagai proksi). Untuk mempelajari perbedaan antara kebijakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, silakan lihat Bagaimana peran IAM role berbeda dari kebijakan berbasis sumber daya dalam Panduan Pengguna IAM.

- Akses lintas layanan – Sebagian Layanan AWS menggunakan fitur di Layanan AWS lainnya. Sebagai contoh, ketika Anda melakukan panggilan dalam suatu layanan, lazim pada layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Suatu layanan mungkin melakukan hal tersebut menggunakan izin pengguna utama panggilan, menggunakan peran layanan, atau peran tertaut layanan.
  - Sesi akses maju (FAS) – Ketika Anda menggunakan pengguna IAM atau peran IAM untuk melakukan tindakan-tindakan di AWS, Anda akan dianggap sebagai seorang pengguna utama. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian dilanjutkan oleh tindakan lain pada layanan yang berbeda. FAS menggunakan izin dari pengguna utama untuk memanggil Layanan AWS, yang dikombinasikan dengan Layanan AWS yang diminta untuk membuat pengajuan ke layanan hilir. Permintaan FAS hanya diajukan ketika sebuah layanan menerima pengajuan yang memerlukan interaksi dengan Layanan AWS lain atau sumber daya lain untuk diselesaikan. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, silakan lihat Meneruskan sesi akses.
  - Peran layanan – Sebuah peran layanan adalah sebuah peran IAM yang dijalankan oleh suatu layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, memodifikasi, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, silakan lihat Membuat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.
  - Peran tertaut layanan – Peran tertaut layanan adalah tipe peran layanan yang tertaut dengan Layanan AWS. Layanan tersebut dapat menjalankan peran untuk melakukan sebuah tindakan atas nama Anda. Peran tertaut layanan akan muncul di Akun AWS Anda dan dimiliki oleh layanan tersebut. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran tertaut layanan.
- Aplikasi yang berjalan di Amazon EC2 – Anda dapat menggunakan peran IAM untuk mengelola kredensial temporer untuk aplikasi yang berjalan di instans EC2 dan mengajukan permintaan AWS CLI atau API AWS. Cara ini lebih baik daripada menyimpan kunci akses dalam instans EC2. Untuk menugaskan sebuah peran AWS ke instans EC2 dan membuatnya tersedia untuk semua aplikasinya, Anda dapat membuat sebuah profil instans yang dilampirkan ke instans. Profil instans berisi peran dan memungkinkan program yang berjalan di instans EC2 untuk mendapatkan kredensial sementara. Untuk informasi selengkapnya, silakan lihat Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan di instans Amazon EC2 di Panduan Pengguna IAM.

Untuk mempelajari apakah kita harus menggunakan peran IAM atau pengguna IAM, silakan lihat Kapan harus membuat peran IAM (alih-alih pengguna) di Panduan Pengguna IAM.

Mengelola kebijakan menggunakan akses

Anda mengendalikan akses di AWS dengan membuat kebijakan dan melampirkannya ke identitas atau sumber daya AWS. Kebijakan adalah objek di AWS yang, ketika terkait dengan identitas atau sumber daya, akan menentukan izinnya. AWS mengevaluasi kebijakan-kebijakan tersebut ketika seorang pengguna utama (pengguna, root user, atau sesi peran) mengajukan permintaan. Izin dalam kebijakan menentukan apakah permintaan diberikan atau ditolak. Sebagian besar kebijakan disimpan di AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang struktur dan isi dokumen kebijakan JSON, silakan lihat Gambaran Umum kebijakan JSON di Panduan Pengguna IAM.

Administrator dapat menggunakan kebijakan JSON AWS untuk menentukan secara spesifik siapa yang memiliki akses pada apa. Yaitu, pengguna utama manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan syarat apa.

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

Kebijakan IAM mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk pengoperasiannya. Sebagai contoh, anggap saja Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole` . Pengguna dengan kebijakan tersebut dapat memperoleh informasi peran dari AWS Management Console, AWS CLI, atau APIAWS.

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, misalnya pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol apa yang pengguna tindakan dan peran dapat kerjakan, pada sumber daya mana, dan dalam keadaan apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, silakan lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan terkelola. Kebijakan inline ditanam secara langsung ke pengguna tunggal, grup, atau peran. Kebijakan terkelola adalah kebijakan yang berdiri sendiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran di Akun AWS Anda. Kebijakan terkelola mencakup kebijakan terkelola AWS dan kebijakan terkelola pelanggan. Untuk mempelajari cara memilih antara kebijakan terkelola

atau kebijakan inline, silakan lihat Memilih antara kebijakan terkelola dan kebijakan inline diPanduan Pengguna IAM.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan-kebijakan berbasis sumber daya adalah kebijakan terpercaya 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 yang dilampiri kebijakan, kebijakan tersebut menentkan tindakan apa yang dapat dilakukan oleh pengguna utama yang ditentukan di sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan pengguna utama dalam kebijakan berbasis sumber daya. Pengguna utama dapat mencakup akun, pengguna, peran, pengguna gabungan, atau Layanan AWS.

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

Daftar kontrol akses (ACL)

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

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh-contoh layanan yang mendukung ACL. Untuk mempelajari ACL selengkapnya, silakan lihat Gambaran umum daftar kontrol akses (ACL) di Panduan Pengembang Layanan Penyimpanan Ringkas Amazon.

Tipe-tipe kebijakan lain

AWS mendukung tipe kebijakan tambahan, yang kurang umum. Tipe-tipe kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda oleh tipe kebijakan yang lebih umum.

- Batasan izin – Batasan izin adalah fitur lanjutan tempat Anda mengatur izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada 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 batas 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 menindihi izin. Untuk informasi selengkapnya tentang batasan izin, silakan lihat Batasan izin untuk entitas IAM di Panduan Pengguna IAM.

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

Berbagai tipe kebijakan

Ketika beberapa tipe kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari bagaimana AWS menentukan apakah mengizinkan permintaan jika beberapa jenis kebijakan dilibatkan, lihat Logika evaluasi kebijakan dalam Panduan Pengguna IAM.

Bagaimana Amazon EMR di EKS bekerja dengan IAM

Sebelum menggunakan IAM untuk mengelola akses ke Amazon EMR di EKS, pelajari fitur IAM apa yang tersedia untuk digunakan dengan Amazon EMR di EKS.

Fitur IAM yang dapat Anda gunakan dengan Amazon EMR di EKS

Fitur IAM	Dukungan Amazon EMR di EKS
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
Kunci kondisi kebijakan	Ya

Fitur IAM	Dukungan Amazon EMR di EKS
ACL	Tidak
ABAC (tag dalam kebijakan)	Ya
Kredensial temporer	Ya
Izin-izin pengguna utama	Ya
Peran layanan	Tidak
Peran tertaut layanan	Ya

Untuk mendapatkan tampilan tingkat tinggi tentang cara Amazon EMR di EKS dan layanan AWS lainnya bekerja dengan sebagian besar fitur IAM, lihat AWS layanan yang bekerja dengan IAM dalam Panduan Pengguna IAM.

Kebijakan berbasis identitas untuk Amazon EMR di EKS

Mendukung kebijakan berbasis identitas	Ya

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, misalnya pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol apa yang pengguna tindakan dan peran dapat kerjakan, pada sumber daya mana, dan dalam keadaan apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, silakan lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta persyaratan yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. Anda tidak dapat menentukan secara spesifik pengguna utama dalam sebuah kebijakan berbasis identitas karena pengguna utama berlaku bagi pengguna atau peran yang melekat kepadanya. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan IAM JSON dalam Panduan Pengguna IAM.

Contoh kebijakan berbasis identitas untuk Amazon EMR di EKS

Untuk melihat contoh kebijakan berbasis identitas Amazon EMR di EKS, lihat Contoh kebijakan berbasis identitas untuk Amazon EMR di EKS.

Kebijakan berbasis sumber daya di dalam Amazon EMR di EKS

Mendukung kebijakan berbasis sumber daya	Tidak

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan-kebijakan berbasis sumber daya adalah kebijakan terpercaya 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 yang dilampiri kebijakan, kebijakan tersebut menentkan tindakan apa yang dapat dilakukan oleh pengguna utama yang ditentukan di sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan pengguna utama dalam kebijakan berbasis sumber daya. Pengguna utama dapat mencakup akun, pengguna, peran, pengguna gabungan, atau Layanan AWS.

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan secara spesifik seluruh akun atau entitas IAM di akun lain sebagai pengguna utama dalam kebijakan berbasis sumber daya. Menambahkan pengguna utama akun silang ke kebijakan berbasis sumber daya hanya setengah dari membangun hubungan kepercayaan. Ketika pengguna utama dan sumber daya berada dalam Akun AWS yang berbeda, Administrator IAM di akun tepercaya juga harus memberikan izin kepada entitas pengguna utama (pengguna atau peran) untuk mengakses sumber daya. Mereka memberikan izin melampirkan kebijakan berbasis identitas kepada entitas. Namun, jika kebijakan berbasis sumber daya memberikan akses kepada pengguna utama dalam akun yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi selengkapnya, lihat Bagaimana IAM role berbeda dengan kebijakan berbasis sumber daya di Panduan Pengguna IAM.

Tindakan kebijakan untuk Amazon EMR di EKS

Mendukung tindakan kebijakan	Ya

Administrator dapat menggunakan kebijakan JSON AWS untuk menentukan secara spesifik siapa yang memiliki akses pada apa. Yaitu, pengguna utama manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan syarat apa.

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

Sertakan tindakan dalam kebijakan untuk memberikan izin guna melakukan operasi terkait.

Untuk melihat daftar tindakan Amazon EMR di EKS, lihat Kunci tindakan, sumber daya, dan kondisi untuk Amazon EMR di EKS dalam Referensi Otorisasi Layanan.

Tindakan kebijakan di Amazon EMR di EKS menggunakan prefiks berikut sebelum tindakan:

```
emr-containers
```

Untuk menetapkan beberapa tindakan dalam satu pernyataan, pisahkan dengan koma.

```
"Action": [
      "emr-containers:action1",
      "emr-containers:action2"
         ]
```

Untuk melihat contoh kebijakan berbasis identitas Amazon EMR di EKS, lihat Contoh kebijakan berbasis identitas untuk Amazon EMR di EKS.

Sumber daya kebijakan untuk Amazon EMR di EKS

Mendukung sumber daya kebijakan	Ya

Administrator dapat menggunakan kebijakan JSON AWS untuk menentukan secara spesifik siapa yang memiliki akses pada apa. Yaitu, pengguna utama manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan syarat apa.

Elemen kebijakan JSON `Resource` menentukan objek atau objek-objek yang menjadi target penerapan tindakan. Pernyataan harus menyertakan entah elemen `Resource` atau `NotResource`.

Praktik terbaiknya, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Anda dapat melakukan ini untuk tindakan-tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin tingkat sumber daya, seperti operasi daftar, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan berlaku untuk semua sumber daya.

```
"Resource": "*"
```

Untuk melihat daftar jenis sumber daya Amazon EMR di EKS dan ARN mereka, lihat Sumber daya yang ditentukan oleh Amazon EMR di EKS dalam Referensi Otorisasi Layanan. Untuk mempelajari tindakan mana yang dapat Anda tentukan ARN setiap sumber daya, lihat Tindakan, sumber daya, dan kunci ketentuan untuk Amazon EMR di EKS.

Untuk melihat contoh kebijakan berbasis identitas Amazon EMR di EKS, lihat Contoh kebijakan berbasis identitas untuk Amazon EMR di EKS.

Kunci ketentuan kebijakan untuk Amazon EMR di EKS

Mendukung kunci-kunci persyaratan kebijakan spesifik layanan	Ya

Administrator dapat menggunakan kebijakan JSON AWS untuk menentukan secara spesifik siapa yang memiliki akses pada apa. Yaitu, pengguna utama manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan syarat apa.

Elemen `Condition` (atau blok `Condition`) akan memungkinkan Anda menentukan syarat yang menjadi dasar suatu pernyataan berlaku. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi bersyarat yang menggunakan operator syarat, misalnya sama dengan atau kurang dari, untuk mencocokkan syarat dalam kebijakan dengan nilai-nilai yang diminta.

Jika Anda menentukan beberapa elemen `Condition` dalam sebuah pernyataan, atau beberapa kunci dalam elemen `Condition` tunggal, maka AWS akan mengevaluasinya dengan menggunakan operasi `AND` yang logis. Jika Anda menentukan beberapa niilai untuk satu kunci persyaratan, maka AWS akan mengevaluasi syarat tersebut menggunakan operasi `OR` yang logis. Semua persyaratan harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan syarat. Sebagai contoh, Anda dapat memberikan izin kepada pengguna IAM untuk mengakses sumber daya hanya jika izin tersebut mempunyai tag yang sesuai dengan nama pengguna IAM mereka. Untuk informasi selengkapnya, silakan lihat Elemen kebijakan IAM: variabel dan tag di Panduan Pengguna IAM.

AWS mendukung kunci-kunci syarat global dan kunci-kunci syarat spesifik layanan. Untuk melihat semua kunci ketentuan global AWS, lihat kunci konteks ketentuan global AWS dalam Panduan Pengguna IAM.

Untuk melihat daftar kunci kondisi Amazon EMR di EKS dan untuk mempelajari tindakan dan sumber daya mana yang dapat Anda gunakan dengan kunci ketentuan, lihat Kunci tindakan, sumber daya, dan kondisi untuk Amazon EMR di EKS dalam Referensi Otorisasi Layanan.

Untuk melihat contoh kebijakan berbasis identitas Amazon EMR di EKS, lihat Contoh kebijakan berbasis identitas untuk Amazon EMR di EKS.

Daftar kontrol akses (ACLs) di Amazon EMR di EKS

Mendukung ACL	Tidak

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

Kontrol akses berbasis atribut (ABAC) dengan Amazon EMR di EKS

Mendukung ABAC (tanda dalam kebijakan)	Ya

Kontrol akses berbasis atribut (ABAC) adalah strategi otorisasi yang mendefinisikan izin berdasarkan atribut. Di AWS, atribut-atribut ini disebut tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke banyak sumber daya AWS. Pemberian tag ke entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian rancanglah kebijakan ABAC untuk mengizinkan operasi-operasi ketika tag milik pengguna utama cocok dengan tag yang ada di sumber daya yang ingin diakses.

ABAC sangat berguna di lingkungan yang berkembang dengan cepat dan berguna di situasi dimana pengelolaan kebijakan menjadi rumit.

Untuk mengendalikan akses berdasarkan tag, berikan informasi tentang tag di elemen syarat dari sebuh kebijakan dengan menggunakan kunci-kunci persyaratan `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci-kunci persyaratan untuk setiap jenis sumber daya, maka nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci persyaratan untuk hanya beberapa jenis sumber daya, maka nilainya adalah Parsial.

Untuk informasi selengkapnya tentang ABAC, silakan lihat Apa itu ABAC? di Panduan Pengguna IAM. Untuk melihat tutorial dengan langkah-langkah untuk mengatur ABAC, lihat Gunakan kontrol akses berbasis atribut (ABAC) di Panduan Pengguna IAM.

Menggunakan kredensial Sementara dengan Amazon EMR di EKS

Mendukung kredensial temporer	Ya

Beberapa Layanan AWS tidak berfungsi saat Anda masuk dengan menggunakan kredensial temporer. Sebagai informasi tambahan, termasuk tentang Layanan AWS mana saja yang berfungsi dengan kredensial temporer, silakan lihat Layanan AWS yang berfungsi dengan IAM di Panduan Pengguna IAM.

Anda menggunakan kredensial temporer jika Anda masuk ke AWS Management Console dengan menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Sebagai contoh, ketika Anda mengakses AWS dengan menggunakan tautan masuk tunggal (SSO) milik perusahaan Anda, proses itu secara otomatis akan membuat kredensial temporer. Anda juga akan secara otomatis membuat kredensial temporer ketika Anda masuk ke konsol sebagai seorang pengguna dan kemudian beralih peran. Untuk informasi selengkapnya tentang peralihan peran, silakan lihat Peralihan peran (konsol) di Panduan Pengguna IAM.

Anda dapat secara manual membuat kredensial temporer menggunakan AWS CLI atau API AWS. Anda kemudian dapat menggunakan kredensial temporer tersebut untuk mengakses AWS. AWS menyarankan agar Anda secara dinamis membuat kredensial temporer alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Menggunakan kredensial keamanan sementara di IAM.

Izin prinsipal lintas layanan untuk Amazon EMR di EKS

Mendukung sesi akses maju (FAS)	Ya

Saat Anda menggunakan pengguna IAM atau peran IAM untuk mengerjakan tindakan di AWS, Anda akan dianggap sebagai pengguna utama. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian dilanjutkan oleh tindakan lain pada layanan yang berbeda. FAS menggunakan izin dari pengguna utama untuk memanggil Layanan AWS, yang dikombinasikan dengan Layanan AWS yang diminta untuk membuat pengajuan ke layanan hilir. Permintaan FAS hanya diajukan ketika sebuah layanan menerima pengajuan yang memerlukan interaksi dengan Layanan AWS lain atau sumber daya lain untuk diselesaikan. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, silakan lihat Meneruskan sesi akses.

Peran layanan untuk Amazon EMR di EKS

Mendukung peran layanan	Tidak

Peran terkait layanan untuk Amazon EMR di EKS

Mendukung peran yang terhubung dengan layanan	Ya

Untuk informasi selengkapnya tentang cara membuat atau mengelola peran terkait layanan, lihat AWS layanan yang bekerja dengan IAM. Cari layanan dalam tabel yang memiliki `Yes` di kolom Service-linked role (Peran yang terhubung dengan layanan). Pilih tautan Ya untuk melihat dokumentasi peran tertaut layanan untuk layanan tersebut.

Menggunakan peran terkait layanan untuk Amazon EMR di EKS

Amazon EMR di EKS menggunakan AWS Identity and Access Management (IAM) peran terkait layanan. Peran terkait layanan adalah jenis IAM role unik yang terhubung langsung ke Amazon EMR di EKS. Peran tertaut layanan ditentukan sebelumnya oleh Amazon EMR di EKS dan mencakup semua izin yang diperlukan oleh layanan untuk menghubungi layanan AWS lainnya atas nama Anda.

Peran tertaut layanan mempermudah pengaturan Amazon EMR di EKS karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. Amazon EMR di EKS menentukan izin dari peran tertaut layanan, kecuali jika ditentukan lain, hanya Amazon EMR di EKS yang dapat mengambil perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, serta bahwa kebijakan izin tidak dapat dilampirkan ke entitas IAM lainnya.

Anda dapat menghapus peran yang terhubung dengan layanan hanya setelah menghapus sumber daya terkait terlebih dahulu. Ini melindungi sumber daya Amazon EMR di EKS Anda karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya.

Untuk informasi tentang layanan lain yang mendukung peran yang terhubung dengan layanan, lihat Layanan AWS yang Berfungsi dengan IAM dan cari layanan yang memiliki Ya di kolom Peran yang Terhubung dengan Layanan. Pilih Ya dengan tautan untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Izin peran terkait layanan untuk Amazon EMR di EKS

Amazon EMR di EKS menggunakan peran terkait layanan yang bernama AWSServiceRoleForAmazonEMRContainers.

`AWSServiceRoleForAmazonEMRContainers` peran terkait layanan memercayakan layanan berikut untuk menjalankan peran tersebut:

- `emr-containers.amazonaws.com`

Kebijakan izin peran `AmazonEMRContainersServiceRolePolicy` memungkinkan Amazon EMR di EKS untuk menyelesaikan serangkaian tindakan pada sumber daya yang ditentukan, seperti yang ditunjukkan pernyataan kebijakan berikut.

> **Note**
>
> Isi kebijakan terkelola berubah, sehingga kebijakan yang ditampilkan di sini mungkin out-of-date. Lihat up-to-date kebijakan paling AmazonEMRContainersServiceRolePolicy diAWS Management Console.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "eks:DescribeCluster",
                "eks:ListNodeGroups",
                "eks:DescribeNodeGroup",
```

```
                "ec2:DescribeRouteTables",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "elasticloadbalancing:DescribeInstanceHealth",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:DescribeTargetHealth"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "acm:ImportCertificate",
                "acm:AddTagsToCertificate"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/emr-container:endpoint:managed-certificate": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "acm:DeleteCertificate"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/emr-container:endpoint:managed-certificate":
 "true"
                }
            }
        }
    ]
}
```

Anda harus mengonfigurasi izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi lebih lanjut, lihat Izin Peran yang Terhubung dengan Layanan di Panduan Pengguna IAM.

Membuat Peran Terkait Layanan untuk Amazon EMR di EKS

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda membuat klaster virtual, Amazon EMR di EKS membuat peran terkait layanan bagi Anda.

Jika Anda menghapus peran terkait layanan ini, lalu ingin membuatnya lagi, Anda dapat menggunakan proses yang sama untuk membuat ulang peran tersebut di akun Anda. Saat Anda membuat klaster virtual, Amazon EMR di EKS membuat peran terkait layanan bagi Anda lagi.

Anda juga dapat menggunakan konsol IAM untuk membuat peran terkait layanan dengan kasus penggunaan Amazon EMR di EKS. Di AWS CLI atau API AWS, buat peran yang terhubung dengan layanan dengan nama layanan `emr-containers.amazonaws.com`. Untuk informasi lebih lanjut, lihat Membuat Peran yang Terhubung dengan Layanan di Panduan Pengguna IAM. Jika Anda menghapus peran yang terhubung dengan layanan ini, Anda dapat menggunakan proses yang sama untuk membuat ulang peran tersebut.

Mengedit peran terkait layanan untuk Amazon EMR di EKS

Amazon EMR di EKS tidak mengizinkan Anda untuk mengedit peran terkait layanan `AWSServiceRoleForAmazonEMRContainers`. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat mengedit penjelasan peran menggunakan IAM. Untuk informasi lebih lanjut, lihat Mengedit Peran yang Terhubung dengan Layanan di Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk Amazon EMR di EKS

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran terkait layanan, kami menyarankan Anda menghapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan yang tidak dipantau atau dipelihara secara aktif. Tetapi, Anda harus membersihkan sumber daya peran yang terhubung dengan layanan sebelum menghapusnya secara manual.

> **Note**
>
> Jika layanan Amazon EMR di EKS menggunakan peran tersebut ketika Anda mencoba menghapus sumber daya, penghapusan mungkin gagal. Jika hal itu terjadi, tunggu beberapa menit dan coba lagi.

Untuk menghapus sumber daya Amazon EMR di EKS yang digunakan oleh **`AWSServiceRoleForAmazonEMRContainers`**

1. Buka konsol Amazon EMR.
2. Pilih klaster virtual.
3. Pada halaman `Virtual Cluster` pilih Hapus.
4. Ulangi prosedur ini untuk setiap klaster virtual lainnya di akun Anda.

Untuk menghapus peran terkait layanan secara manual menggunakan IAM

Gunakan konsol IAM, AWS CLI, atau AWS API untuk menghapus peran terkait layanan `AWSServiceRoleForAmazonEMRContainers`. Untuk informasi lebih lanjut, lihat Menghapus Peran Tertaut Layanan dalam Panduan Pengguna IAM.

Wilayah yang Didukung untuk Peran Terkait Layanan Amazon EMR di EKS

Amazon EMR di EKS memberikan dukungan dengan peran terkait layanan di semua Wilayah tempat layanan tersedia. Untuk informasi selengkapnya, lihat Kuota layanan Amazon EMdi EKS.

Kebijakan terkelola untuk Amazon EMR di EKS

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk Amazon EMR di EKS sejak 1 Maret 2021.

Perubahan	Deskripsi	Tanggal
`AmazonEMRContainersServiceRolePolicy` - Menambahkan izin untuk mendeskripsikan dan mencantumkan nodegroup Amazon EKS, mendeskripsikan grup target penyeimbang beban, dan menjelaskan kesehatan target penyeimbang beban.	Izin berikut ditambahkan ke kebijakan:`eks:ListNodeGroups` ,, `eks:DescribeNodeGroup elasticloadbalancing:DescribeTargetGroups ,elasticloadbalancing:DescribeTargetHealth` .	Maret 13, 2023

Perubahan	Deskripsi	Tanggal
`AmazonEMRContainersServiceRolePolicy` - Menambahkan izin untuk mengimpor dan menghapus sertifikat diAWS Certificate Manager.	Izin berikut ditambahkan ke kebijakan:`acm:ImportCertificate` ,`acm:AddTagsToCertificate` ,`acm:DeleteCertificate` .	Desember 3, 2021
Amazon EMR di EKS mulai melacak perubahan	Amazon EMR di EKS mulai melacak perubahan untuk kebijakan yang AWS dikelola.	1 Maret 2021

Menggunakan peran eksekusi tugas dengan Amazon EMR di EKS

Untuk menggunakan perintah `StartJobRun` untuk mengirimkan tugas berjalan di klaster EKS, Anda harus terlebih dahulu mengorientasi peran eksekusi tugas yang akan digunakan dengan klaster virtual. Untuk informasi selengkapnya, lihat Untuk membuat peran eksekusi tugas di Menyiapkan Amazon EMR di EKS. Anda juga dapat mengikuti petunjuk di bagian Buat Peran IAM untuk pelaksanaan pekerjaan di Amazon EMR di EKS Workshop.

Izin berikut harus disertakan dalam kebijakan kepercayaan untuk peran eksekusi tugas.

```
{
"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Principal": {
      "Federated": "arn:aws:iam::AWS_ACCOUNT_ID:oidc-provider/OIDC_PROVIDER"
    },
    "Action": "sts:AssumeRoleWithWebIdentity",
    "Condition": {
      "StringLike": {
        "OIDC_PROVIDER:sub": "system:serviceaccount:NAMESPACE:emr-containers-sa-*-
*-AWS_ACCOUNT_ID-BASE36_ENCODED_ROLE_NAME"
      }
    }
  }
```

```
  ]
}
```

Kebijakan kepercayaan pada contoh sebelumnya hanya memberikan izin ke akun layanan Kubernetes yang dikelola EMR Amazon EMR dengan nama yang cocok dengan polanya. `emr-containers-sa-*-*-`*AWS_ACCOUNT_ID*`-`*BASE36_ENCODED_ROLE_NAME* Akun layanan dengan pola ini akan dibuat secara otomatis pada pengiriman pekerjaan, dan dicakup ke namespace tempat Anda mengirimkan pekerjaan. Kebijakan kepercayaan ini memungkinkan akun layanan ini untuk mengasumsikan peran eksekusi dan mendapatkan kredensial sementara peran eksekusi. Akun layanan dari kluster Amazon EKS yang berbeda atau dari namespace yang berbeda dalam kluster EKS yang sama dibatasi untuk mengasumsikan peran eksekusi.

Anda dapat menjalankan perintah berikut untuk memperbarui kebijakan kepercayaan secara otomatis dalam format yang diberikan di atas.

```
aws emr-containers update-role-trust-policy \
       --cluster-name cluster \
       --namespace namespace \
       --role-name iam_role_name_for_job_execution
```

Mengontrol akses ke peran eksekusi

Administrator untuk klaster Amazon EKS Anda dapat membuat EMR Amazon multi-tenant di kluster virtual EKS tempat administrator IAM dapat menambahkan beberapa peran eksekusi. Karena penyewa yang tidak tepercaya dapat menggunakan peran eksekusi ini untuk mengirimkan pekerjaan yang menjalankan kode arbitrer, Anda mungkin ingin membatasi penyewa tersebut sehingga mereka tidak dapat menjalankan kode yang mendapatkan izin yang ditetapkan ke satu atau beberapa peran eksekusi ini. Untuk membatasi kebijakan IAM yang dilampirkan pada identitas IAM, administrator IAM dapat menggunakan kunci kondisi Amazon Resource Name (ARN) opsional. `emr-containers:ExecutionRoleArn` Kondisi ini menerima daftar ARN peran eksekusi yang memiliki izin ke klaster virtual, seperti yang ditunjukkan oleh kebijakan izin berikut.

```
{
"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": "emr-containers:StartJobRun",
```

```
      "Resource": "arn:aws:emr-containers:REGION:AWS_ACCOUNT_ID:/
virtualclusters/VIRTUAL_CLUSTER_ID",
      "Condition": {
        "ArnEquals": {
          "emr-containers:ExecutionRoleArn": [
            "execution_role_arn_1",
            "execution_role_arn_2",
            ...
          ]
        }
      }
    }
  ]
}
```

Jika Anda ingin mengizinkan semua peran eksekusi yang dimulai dengan awalan tertentu, sepertiMyRole, Anda dapat mengganti operator kondisi `ArnEquals` dengan `ArnLike` operator, dan Anda dapat mengganti `execution_role_arn` nilai dalam kondisi dengan karakter wildcard`*`. Sebagai contoh, `arn:aws:iam::AWS_ACCOUNT_ID:role/MyRole*`. Semua kunci kondisi ARN lainnya juga didukung.

> **Note**
>
> Dengan Amazon EMR di EKS, Anda tidak dapat memberikan izin untuk peran eksekusi berdasarkan tag atau atribut. EMR Amazon di EKS tidak mendukung kontrol akses berbasis tag (TBAC) atau kontrol akses berbasis atribut (ABAC) untuk peran eksekusi.

Contoh kebijakan berbasis identitas untuk Amazon EMR di EKS

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi Amazon EMR pada sumber daya EKS. Pengguan dan peran tersebut juga tidak dapat melakukan tugas dengan menggunakan API AWS Management Console, AWS Command Line Interface (AWS CLI), atau AWS. Untuk mengabulkan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian akan dapat menambahkan kebijakan IAM ke peran, dan para pengguna dapat mengambil peran.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM menggunakan contoh dokumen kebijakan JSON ini, silakan lihat Membuat kebijakan IAM di Panduan Pengguna IAM.

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh Amazon EMR di EKS, termasuk format ARN untuk setiap jenis sumber daya, lihat Kunci tindakan, sumber daya, dan kondisi untuk Amazon EMR di EKS dalam Referensi Otorisasi Layanan.

Topik

- Praktik terbaik kebijakan
- Menggunakan konsol Amazon EMR di EKS
- Perbolehkan pengguna untuk melihat izin mereka sendiri

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus Amazon EMR pada sumber daya EKS di akun Anda. Tindakan ini mengenakan biaya kepada Anda Akun AWS. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan terkelola AWS dan beralih ke izin dengan hak akses paling rendah – Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan terkelola AWS yang memberikan izin untuk banyak kasus penggunaan umum. Kebijakan tedapat di Akun AWS Anda. Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola pelanggan AWS yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, silakan lihat kebijakan-kebijakan terkelola AWS atau kebijakan-kebijakan terkelola AWS untuk fungsi tugas di 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 melakukan ini dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan pengguna IAM untuk mengajukan izin, silakan lihat Kebijakan dan izin di IAM di Panduan Pengguna IAM.
- Gunakan syarat dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu syarat ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis syarat kebijakan untuk menentukan bahwa semua pengajuan harus dikirim menggunakan SSL. Anda juga dapat menggunakan syarat untuk memberi akses ke tindakan layanan jika digunakan melalui Layanan AWS yang spesifk, sepertiAWS CloudFormation. Untuk informasi selengkapnya, silakan lihat Elemen kebijakan JSON IAM: Syarat di Panduan Pengguna IAM.

- Gunakan Analizer Akses IAM untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – Analizer Akses IAM memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. Analizer Akses IAM menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, silakan lihat validasi kebijakan Analizer Akses IAM di Panduan Pengguna IAM.
- Memerlukan autentikasi multi-faktor (MFA) – Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Akun AWS Anda, aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA ketika operasi API dipanggil, tambahkan syarat MFA pada kebijakan Anda. Untuk informasi selengkapnya, silakan lihat Mengonfigurasi akses API yang diproteksi MFA di Panduan Pengguna IAM.

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

Menggunakan konsol Amazon EMR di EKS

Untuk mengakses konsol Amazon EMR di EKS, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang Amazon EMR pada sumber daya EKS di Anda. Akun AWS Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna atau peran) dengan kebijakan tersebut.

Anda tidak perlu meloloskan izin konsol minimum bagi pengguna yang hanya melakukan panggilan ke API AWS CLI atau AWS. Jika tidak, akses hanya diizinkan ke tindakan-tindakan yang sesuai dengan operasi API yang sedang mereka coba lakukan.

Untuk memastikan bahwa pengguna dan peran masih dapat menggunakan konsol Amazon EMR di EKS, juga melampirkan kebijakan terkelola Amazon EMR di EKS `ConsoleAccess` atau `ReadOnly` AWS pada entitas. Untuk informasi selengkapnya, lihat Menambahkan izin ke pengguna dalam Panduan Pengguna IAM.

Perbolehkan pengguna untuk melihat izin mereka sendiri

Contoh ini menunjukkan cara Anda dapat membuat kebijakan yang mengizinkan para pengguna IAM untuk melihat kebijakan inline dan terkelola yang dilampirkan ke identitas pengguna mereka.

Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini pada konsol atau secara terprogram menggunakan AWS CLI atau API 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": "*"
        }
    ]
}
```

Kebijakan untuk kendali akses berbasis tanda

Anda dapat menggunakan kondisi di kebijakan berbasis identitas Anda untuk mengontrol akses ke klaster virtual dan tugas berjalan berbasis tanda. Untuk informasi lebih lanjut tentang penandaan, lihat Menandai Sumber Daya Amazon EMR di EKS Anda.

Contoh berikut menunjukkan skenario yang berbeda dan cara untuk menggunakan operator syarat dengan kunci syarat Amazon EMR di EKS. Pernyataan kebijakan IAM ini dimaksudkan untuk tujuan demonstrasi saja dan tidak boleh digunakan di lingkungan produksi. Ada beberapa cara untuk menggabungkan pernyataan kebijakan untuk memberikan dan menolak izin sesuai dengan kebutuhan Anda. Untuk informasi selengkapnya tentang perencanaan dan pengujian kebijakan IAM, lihat Panduan pengguna IAM.

> **Important**
>
> Secara eksplisit menolak izin untuk tindakan penandaan adalah pertimbangan penting. Hal ini mencegah pengguna dari penandaan sumber daya dan dengan demikian memberikan sendiri izin yang tidak ingin Anda berikan. Jika tindakan penandaan untuk sumber daya tidak ditolak, pengguna dapat memodifikasi tanda dan menghindari maksud kebijakan berbasis tanda. Untuk contoh kebijakan yang menolak tindakan penandaan, lihat Tolak akses untuk menambah dan menghapus tanda.

Contoh di bawah menunjukkan kebijakan izin berbasis identitas yang digunakan untuk mengontrol tindakan yang diizinkan dengan klaster virtual Amazon EMR di EKS.

Izinkan tindakan hanya pada sumber daya dengan nilai tanda tertentu

Dalam contoh kebijakan berikut, operator StringEquals kondisi mencoba mencocokkan dev dengan nilai untuk departemen tag. Jika departemen tanda belum ditambahkan ke klaster virtual, atau tidak mengandung dev nilai, kebijakan tersebut tidak berlaku, dan tindakan tersebut tidak diizinkan oleh kebijakan ini. Jika tidak ada pernyataan kebijakan lain mengizinkan tindakan, pengguna hanya dapat bekerja dengan klaster virtual yang memiliki tanda ini dengan nilai ini.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```
      "Action": [
        "emr-containers:DescribeVirtualCluster"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/department": "dev"
        }
      }
    }
  ]
}
```

Anda juga dapat menentukan beberapa nilai tanda menggunakan operator syarat. Misalnya, untuk mengizinkan tindakan pada klaster virtual di mana tanda `department` berisi nilai `dev` atau `test`, Anda bisa mengganti blok syarat di contoh sebelumnya dengan berikut ini.

```
"Condition": {
        "StringEquals": {
          "aws:ResourceTag/department": ["dev", "test"]
        }
      }
```

Memerlukan penandaan ketika sumber daya dibuat

Pada contoh di bawah ini, tanda perlu diterapkan saat membuat klaster virtual.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "emr-containers:CreateVirtualCluster"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/department": "dev"
        }
      }
    }
```

```
  ]
}
```

Pernyataan kebijakan berikut mengizinkan pengguna untuk membuat klaster virtual hanya jika klaster memiliki tanda `department`, yang dapat berisi nilai apa pun.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "emr-containers:CreateVirtualCluster"
      ],
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:RequestTag/department": "false"
        }
      }
    }
  ]
}
```

Tolak akses untuk menambah dan menghapus tanda

Efek dari kebijakan ini adalah untuk menolak izin pengguna untuk menambah atau menghapus tanda apa pun pada klaster virtual yang ditandai dengan tanda `department` yang berisi nilai `dev`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "emr-containers:TagResource",
        "emr-containers:UntagResource"
      ],
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:ResourceTag/department": "dev"
```

```
        }
      }
    }
  ]
}
```

Memecahkan Masalah identitas dan akses Amazon EMR di EKS

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan mengatasi masalah umum yang mungkin Anda temui saat bekerja menggunakan Amazon EMR di EKS dan IAM.

Topik

- Saya tidak berwenang untuk melakukan tindakan di Amazon EMR di EKS
- Saya tidak berwenang untuk melakukan iam: PassRole
- Saya ingin mengizinkan orang di luar akun AWS saya untuk mengakses sumber daya Amazon EMR di EKS saya

Saya tidak berwenang untuk melakukan tindakan di Amazon EMR di EKS

Jika AWS Management Console memberi tahu bahwa Anda tidak berwenang untuk melakukan tindakan, Anda harus menghubungi administrator untuk mendapatkan bantuan. Administrator adalah orang yang memberikan nama pengguna dan kata sandi Anda untuk Anda.

Contoh kesalahan berikut terjadi ketika `mateojackson` pengguna mencoba menggunakan konsol untuk melihat detail tentang *`my-example-widget`* sumber daya fiksi tetapi tidak memiliki izin `emr-containers:`*`GetWidget`* fiksi.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform: emr-
containers:GetWidget on resource: my-example-widget
```

Dalam hal ini, Mateo meminta administratornya untuk memperbarui kebijakannya untuk memungkinkannya mengakses sumber daya *`my-example-widget`* dengan menggunakan tindakan `emr-containers:`*`GetWidget`*.

Saya tidak berwenang untuk melakukan iam: PassRole

Jika Anda menerima kesalahan bahwa Anda tidak diizinkan untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran ke Amazon EMR di EKS.

Sebagian Layanan AWS mengizinkan Anda untuk memberikan peran yang sudah ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran tertaut-layanan. Untuk melakukan tindakan tersebut, Anda harus memiliki izin untuk memberikan peran pada layanan tersebut.

Contoh kesalahan berikut terjadi ketika pengguna IAM bernama `marymajor` mencoba menggunakan konsol untuk melakukan tindakan di Amazon EMR di EKS. 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 membutuhkan bantuan, hubungi administrator AWS Anda. Administrator Anda adalah orang yang memberikan kredensial masuk Anda.

Saya ingin mengizinkan orang di luar akun AWS saya untuk mengakses sumber daya Amazon EMR di EKS saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun atau orang lain di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa 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 akses kepada orang ke sumber daya Anda.

Untuk mempelajari selengkapnya, lihat hal berikut:

- Untuk mempelajari apakah Amazon EMR di EKS mendukung fitur ini, lihat Bagaimana Amazon EMR di EKS bekerja dengan IAM.
- Untuk mempelajari cara memberikan akses ke sumber daya di seluruh Akun AWS yang Anda miliki, silakan lihat Menyediakan akses ke pengguna IAM di Akun AWS lainnya yang Anda miliki di Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses ke sumber daya Anda ke pihak ketiga Akun AWS, silakan lihat Menyediakan akses ke akun Akun AWS yang dimiliki oleh pihak ketiga dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, silakan lihat Menyediakan akses ke pengguna terautentikasi eksternal (gabungan identitas) di Panduan Pengguna IAM .

- Untuk mempelajari perbedaan antara penggunaan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Perbedaan IAM role dan kebijakan berbasis sumber daya di Panduan Pengguna IAM.

Pencatatan dan pemantauan

Untuk mendeteksi insiden, menerima peringatan ketika insiden terjadi, dan menanggapinya, gunakan opsi ini dengan Amazon EMR di EKS:

- Pantau Amazon EMR di EKS dengan AWS CloudTrail - AWS CloudTrail menyediakan rekaman tindakan yang diambil oleh pengguna, peran, atau layanan AWS di Amazon EMR di EKS. Ini menangkap panggilan dari konsol Amazon EMR dan panggilan kode ke operasi API Amazon EMR di EKS sebagai peristiwa. Ini memungkinkan Anda untuk menentukan permintaan yang diajukan ke Amazon EMR di EKS, alamat IP dari mana permintaan dibuat, siapa yang mengajukan permintaan, kapan dibuat, dan detail tambahan. Untuk informasi selengkapnya, lihat Pencatatan panggilan API Amazon EMR di EKS menggunakan AWS CloudTrail.
- Gunakan CloudWatch Events dengan Amazon EMR di EKS - CloudWatch Events memberikan stream sistem hampir secara waktu nyata yang menguraikan perubahan dalam sumber daya AWS. CloudWatch Events menjadi sadar akan perubahan operasional saat terjadi, meresponsnya, dan mengambil tindakan korektif seperlunya, dengan mengirim pesan untuk merespons lingkungan, mengaktifkan fungsi, membuat perubahan, dan menangkap informasi status. Untuk menggunakan CloudWatch Events dengan Amazon EMR di EKS, buat aturan yang memicu panggilan API Amazon EMR di EKS melalui CloudTrail. Untuk informasi selengkapnya, lihat Memantau tugas dengan Amazon CloudWatch Events.

Pencatatan panggilan API Amazon EMR di EKS menggunakan AWS CloudTrail

Amazon EMR di EKS terintegrasi dengan AWS CloudTrail, sebuah layanan yang menyediakan catatan tindakan yang dilakukan oleh pengguna, peran, atau layanan AWS dalam Amazon EMR di EKS. CloudTrail menangkap semua panggilan API untuk Amazon EMR di EKS sebagai peristiwa. Panggilan yang direkam mencakup panggilan dari konsol Amazon EMR di EKS dan panggilan kode ke operasi API Amazon EMR di EKS. Jika membuat jejak, Anda dapat mengaktifkan pengiriman peristiwa CloudTrail berkelanjutan ke bucket Amazon S3, termasuk peristiwa untuk Amazon EMR di EKS. Jika Anda tidak dapat mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru dalam konsol CloudTrail di Riwayat peristiwa. Menggunakan informasi yang dikumpulkan oleh CloudTrail,

Anda dapat menentukan permintaan yang dibuat ke Amazon EMR di EKS, alamat IP asal permintaan tersebut dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail lainnya.

Untuk mempelajari selengkapnya tentang CloudTrail, lihat AWS CloudTrail Panduan Pengguna.

Informasi Amazon EMR di EKS di CloudTrail

CloudTrail diaktifkan pada akun AWS Anda saat Anda membuat akun tersebut. Ketika aktivitas terjadi di Amazon EMR di EKS, aktivitas tersebut dicatat di peristiwa CloudTrail bersama peristiwa layanan AWS lainnya di Riwayat peristiwa. Anda dapat melihat, mencari, dan mengunduh peristiwa terbaru di akun AWS Anda. Untuk informasi lebih lanjut, lihat Melihat peristiwa dengan riwayat CloudTrail Event.

Untuk catatan peristiwa yang sedang berlangsung di akun AWS Anda, termasuk peristiwa untuk Amazon EMR di EKS, buatlah jejak. Jejak memungkinkan CloudTrail untuk mengirim berkas log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di dalam konsol tersebut, jejak diterapkan ke semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di partisi AWS dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi layanan AWS lainnya untuk menganalisis lebih lanjut dan bertindak berdasarkan data peristiwa yang dikumpulkan di log CloudTrail. Untuk informasi selengkapnya, lihat yang berikut:

- Gambaran umum untuk membuat jejak
- Layanan dan integrasi yang didukung CloudTrail
- Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail
- Menerima file log CloudTrail dari beberapa wilayah dan Menerima file log CloudTrail dari beberapa akun

Semua tindakan Amazon EMR di EKS dicatat oleh CloudTrail dan didokumentasikan dalam Dokumentasi API Amazon EMR di EKS. Misalnya, panggilan untuk tindakan `CreateVirtualCluster`, `StartJobRun` dan `ListJobRuns` menghasilkan entri di berkas log CloudTrail.

Setiap entri peristiwa atau log berisi informasi tentang orang yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan hal berikut:

- Bahwa permintaan dibuat dengan kredensial pengguna root atau pengguna AWS Identity and Access Management (IAM).
- Bahwa permintaan tersebut dibuat dengan kredensial keamanan sementara untuk peran atau pengguna gabungan.

- Apakah permintaan dibuat oleh layanan AWS lain.

Untuk informasi selengkapnya, lihat Elemen identitas pengguna CloudTrail.

Memahami entri file log Amazon EMR di EKS

Jejak adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai berkas log ke bucket Amazon S3 yang telah Anda tentukan. File log CloudTrail berisi satu atau beberapa entri log. Peristuwa mewakili satu permintaan dari sumber apa pun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. Berkas log CloudTrail bukanlah pelacakan tumpukan terurut dari panggilan API publik, sehingga tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan entri log CloudTrail yang menunjukkan tindakan `ListJobRuns`.


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE:admin",
    "arn": "arn:aws:sts::012345678910:assumed-role/Admin/admin",
    "accountId": "012345678910",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn": "arn:aws:iam::012345678910:role/Admin",
        "accountId": "012345678910",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2020-11-04T21:49:36Z"
      }
    }
  },
  "eventTime": "2020-11-04T21:52:58Z",
  "eventSource": "emr-containers.amazonaws.com",
  "eventName": "ListJobRuns",
  "awsRegion": "us-east-1",
```

```
  "sourceIPAddress": "203.0.113.1",
  "userAgent": "aws-cli/1.11.167 Python/2.7.10 Darwin/16.7.0 botocore/1.7.25",
  "requestParameters": {
    "virtualClusterId": "1K48XXXXXXHCB"
  },
  "responseElements": null,
  "requestID": "890b8639-e51f-11e7-b038-EXAMPLE",
  "eventID": "874f89fa-70fc-4798-bc00-EXAMPLE",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "recipientAccountId": "012345678910"
}
```


Menggunakan Hibah Akses Amazon S3 dengan Amazon EMR di EKS

Ikhtisar Hibah Akses S3 untuk Amazon EMR di EKS

Dengan Amazon EMR rilis 6.15.0 dan yang lebih tinggi, Amazon S3 Access Grants menyediakan solusi kontrol akses yang dapat diskalakan yang dapat Anda gunakan untuk menambah akses ke data Amazon S3 Anda dari Amazon EMR di EKS. Jika Anda memiliki konfigurasi izin yang kompleks atau besar untuk data S3, Anda dapat menggunakan Access Grants untuk menskalakan izin data S3 untuk pengguna, peran, dan aplikasi.

Gunakan S3 Access Grants untuk menambah akses ke data Amazon S3 di luar izin yang diberikan oleh peran runtime atau peran IAM yang dilampirkan ke identitas dengan akses ke Amazon EMR Anda di klaster EKS.

Untuk informasi selengkapnya, lihat Mengelola akses dengan Hibah Akses S3 untuk Amazon EMR di Panduan Manajemen EMR Amazon dan Mengelola akses dengan Hibah Akses S3 di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Halaman ini menjelaskan persyaratan untuk menjalankan pekerjaan Spark di Amazon EMR di EKS dengan integrasi S3 Access Grants. Dengan Amazon EMR di EKS, S3 Access Grants memerlukan pernyataan kebijakan IAM tambahan dalam peran eksekusi untuk pekerjaan Anda, dan konfigurasi penggantian tambahan untuk API. `StartJobRun` Untuk langkah-langkah menyiapkan Hibah Akses S3 dengan penerapan EMR Amazon lainnya, lihat dokumentasi berikut:

- Menggunakan Hibah Akses S3 dengan Amazon EMR

- Menggunakan Hibah Akses S3 dengan EMR Tanpa Server

Luncurkan Amazon EMR di klaster EKS dengan S3 Access Grants untuk manajemen data

Anda dapat mengaktifkan S3 Access Grants di Amazon EMR di EKS dan meluncurkan pekerjaan Spark. Saat aplikasi Anda membuat permintaan untuk data S3, Amazon S3 menyediakan kredenal sementara yang dicakup ke bucket, awalan, atau objek tertentu.

1. Siapkan peran eksekusi pekerjaan untuk EMR Amazon Anda di klaster EKS. Sertakan izin IAM yang diperlukan yang Anda perlukan untuk menjalankan pekerjaan Spark, dan: `s3:GetDataAccess` `s3:GetAccessGrantsInstanceForPrefix`

```
{
    "Effect": "Allow",
    "Action": [
    "s3:GetDataAccess",
    "s3:GetAccessGrantsInstanceForPrefix"
    ],
    "Resource": [     //LIST ALL INSTANCE ARNS THAT THE ROLE IS ALLOWED TO QUERY
         "arn:aws_partition:s3:Region:account-id1:access-grants/default",
         "arn:aws_partition:s3:Region:account-id2:access-grants/default"
    ]
}
```

> **Note**
>
> Jika Anda menentukan peran IAM yang untuk eksekusi pekerjaan yang memiliki izin tambahan untuk mengakses S3 secara langsung, maka pengguna mungkin dapat mengakses data terlepas dari izin yang Anda tentukan di S3 Access Grants

2. Kirimkan pekerjaan ke EMR Amazon Anda di kluster EKS dengan label rilis Amazon EMR 6,15 atau lebih tinggi dan `emrfs-site` klasifikasi, seperti yang ditunjukkan contoh berikut. Ganti nilai *red text* dengan nilai yang sesuai untuk skenario penggunaan Anda.

```
{
  "name": "myjob",
  "virtualClusterId": "123456",
  "executionRoleArn": "iam_role_name_for_job_execution",
```

```
  "releaseLabel": "emr-7.0.0-latest",
  "jobDriver": {
    "sparkSubmitJobDriver": {
      "entryPoint": "entryPoint_location",
      "entryPointArguments": ["argument1", "argument2"],
       "sparkSubmitParameters": "--class main_class"
    }
  },
  "configurationOverrides": {
    "applicationConfiguration": [
      {
        "classification": "emrfs-site",
        "properties": {
          "fs.s3.s3AccessGrants.enabled": "true",
          "fs.s3.s3AccessGrants.fallbackToIAM": "false"
         }
      }
    ],
  }
}
```

Akses S3 Memberikan pertimbangan dengan Amazon EMR di EKS

Untuk informasi dukungan, kompatibilitas, dan perilaku penting saat Anda menggunakan Hibah Akses Amazon S3 dengan Amazon EMR di EKS, lihat pertimbangan Hibah Akses S3 dengan Amazon EMR di Panduan Manajemen EMR Amazon.

Validasi kepatuhan untuk Amazon EMR di EKS

Auditor pihak ketiga menilai keamanan dan kepatuhan Amazon EMR di EKS sebagai bagian dari beberapa program kepatuhan AWS. Program ini mencakup SOC, PCI, FedRAMP, HIPAA, dan lainnya.

Ketahanan di Amazon EMR di EKS

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

mengalami kegagalan di antara 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 AWS Wilayah dan Availability Zone, lihat AWS Infrastruktur Global.

Selain infrastruktur global AWS, Amazon EMR di EKS menawarkan integrasi dengan Amazon S3 melalui EMRFS untuk membantu mendukung ketahanan data dan kebutuhan pencadangan Anda.

Keamanan infrastruktur dalam Amazon EMR di EKS

Sebagai layanan terkelola, Amazon EMR on EKS dilindungi olehAWSprosedur keamanan jaringan global yang dijelaskan dalamAmazon Web Services: Whitepaper Ikhtisar Proses Keamanan.

Anda menggunakan panggilan API yang dipublikasikan AWS untuk mengakses Amazon EMR di EKS melalui jaringan. Klien harus mendukung Transport Layer Security (TLS) 1.0 atau versi yang lebih baru. Kami merekomendasikan TLS 1.2 atau versi yang lebih baru. Klien juga harus mendukung suite cipher dengan perfect forward secrecy (PFS) seperti Ephemeral Diffie-Hellman (DHE) atau Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). 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.

Analisis konfigurasi dan kerentanan

AWS menangani tugas-tugas keamanan dasar seperti sistem operasi tamu (OS) dan patching basis data, konfigurasi firewall, dan pemulihan bencana. Prosedur ini telah ditinjau dan disertifikasi oleh pihak ketiga yang sesuai. Untuk detail selengkapnya, lihat sumber daya berikut:

- Validasi kepatuhan untuk Amazon EMR di EKS
- Model Tanggung Jawab Bersama
- Amazon Web Services: Ikhtisar Proses Keamanan (kertas putih)

Connect ke Amazon EMR di EKS Menggunakan VPC endpoints

Anda dapat terhubung langsung ke Amazon EMR di EKS menggunakan VPC endpoints AWS PrivateLink Ketika Anda menggunakan VPC endpoint antarmuka, komunikasi antara VPC dan Amazon EMR di EKS dilakukan sepenuhnya dalam jaringan AWS. Masing-masing VPC endpoint diwakili oleh satu Antarmuka jaringan elastis (ENI) dengan alamat IP privat di subnet VPC Anda.

Antarmuka VPC endpoint menghubungkan VPC Anda langsung ke Amazon EMR di EKS tanpa gateway internet, perangkat NAT, koneksi VPN, atau Koneksi Direct Connect AWS. Instans dalam VPC Anda tidak memerlukan alamat IP publik untuk berkomunikasi dengan API Amazon EMR di EKS.

Anda dapat membuat VPC endpoint antarmuka untuk terhubung ke Amazon EMR di EKS menggunakan perintah AWS Management Console atau AWS Command Line Interface (AWS CLI). Untuk informasi selengkapnya, lihat Membuat Titik Akhir Antarmuka.

Setelah Anda membuat antarmuka VPC endpoint, jika Anda mengaktifkan nama host DNS privat untuk titik akhir, titik akhir Amazon EMR di EKS default menyelesaikan ke VPC endpoint Anda. Titik akhir nama layanan default untuk Amazon EMR di EKS adalah dalam format berikut.

```
emr-containers.Region.amazonaws.com
```

Jika Anda tidak mengaktifkan nama host DNS privat, Amazon VPC menyediakan nama titik akhir DNS yang dapat Anda gunakan dalam format berikut.

```
VPC_Endpoint_ID.emr-containers.Region.vpce.amazonaws.com
```

Untuk informasi selengkapnya, lihat Antarmuka (AWSPrivateLink) di Panduan Pengguna Amazon VPC. Amazon EMR di EKS mendukung panggilan ke semua Tindakan API di dalam VPC Anda.

Anda dapat melampirkan kebijakan VPC endpoint ke VPC endpoint untuk mengontrol akses untuk prinsipal IAM. Anda juga dapat mengasosiasi grup keamanan dengan VPC endpoint untuk mengontrol akses masuk dan keluar berdasarkan asal dan tujuan lalu lintas jaringan, seperti rentang alamat IP. Untuk informasi selengkapnya, lihat Mengontrol Akses ke Layanan dengan VPC Endpoints.

Buat Kebijakan VPC Endpoint untuk Amazon EMR di EKS

Anda dapat membuat kebijakan untuk Amazon VPC endpoint untuk Amazon EMR di EKS untuk menentukan hal berikut:

- Prinsip-prinsip yang dapat atau tidak dapat melakukan tindakan
- Tindakan yang dapat dilakukan
- Sumber daya yang dapat digunakan untuk mengambil tindakan

Untuk informasi selengkapnya, lihat Mengontrol Akses ke Layanan dengan VPC Endpoint dalam Panduan Pengguna Amazon VPC.

Example Kebijakan VPC Endpoint untuk Menolak Semua Akses dari Akun AWS Tertentu

Kebijakan VPC endpoint berikut mneolak akun AWS *123456789012* semua akses ke sumber daya menggunakan titik akhir.

```
{
    "Statement": [
        {
            "Action": "*",
            "Effect": "Allow",
            "Resource": "*",
            "Principal": "*"
        },
        {
            "Action": "*",
            "Effect": "Deny",
            "Resource": "*",
            "Principal": {
                "AWS": [
                    "123456789012"
                ]
            }
        }
    ]
}
```

Example Kebijakan VPC Endpoint untuk Mengizinkan Akses VPC Hanya ke Prinsipal IAM (Pengguna) Tertentu

Kebijakan VPC endpoint berikut memungkinkan akses penuh hanya ke pengguna IAM *lijuan* di akun AWS *123456789012*. Semua prinsipal IAM lain ditolak aksesnya menggunakan titik akhir.

```
{
    "Statement": [
        {
            "Action": "*",
            "Effect": "Allow",
            "Resource": "*",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::123456789012:user/lijuan"
                ]
            }
        }
    ]
}
```

Example Kebijakan VPC Endpoint untuk Mengizinkan Operasi Read-Only Amazon EMR di EKS

Kebijakan VPC endpoint berikut hanya mengizinkan akun AWS *123456789012* untuk melakukan tindakan Amazon EMR di EKS khusus.

Tindakan yang ditentukan memberikan akses setara dengan read-only untuk Amazon EMR di EKS. Semua tindakan lain pada VPC ditolak untuk akun yang ditentukan. Semua akun lain ditolak akses apa pun. Untuk daftar tindakan Amazon EMR di EKS, lihat Kunci Tindakan, Sumber Daya, dan Kondisi untuk Amazon EMR di EKS.

```
{
    "Statement": [
        {
            "Action": [
                "emr-containers:DescribeJobRun",
                "emr-containers:DescribeVirtualCluster",
                "emr-containers:ListJobRuns",
                "emr-containers:ListTagsForResource",
                "emr-containers:ListVirtualClusters"
            ],
            "Effect": "Allow",
```

```
            "Resource": "*",
            "Principal": {
                "AWS": [
                    "123456789012"
                ]
            }
        }
    ]
}
```

Example Kebijakan VPC Endpoint Menolak Akses ke Klaster Virtual Tertentu

Kebijakan VPC endpoint berikut memungkinkan akses penuh untuk semua akun dan prinsipal, namun menolak akses apa pun untuk akun AWS *123456789012* untuk tindakan yang dilakukan pada klaster virtual dengan ID klaster *A1B2CD34EF5G*. Amazon EMR lainnya pada tindakan EKS yang tidak mendukung izin tingkat sumber daya untuk klaster virtual masih diizinkan. Untuk daftar tindakan Amazon EMR di EKS dan jenis sumber daya terkait, lihat Kunci Tindakan, Sumber Daya, dan Kondisi untuk Amazon EMR di EKS - di AWS Identity and Access ManagementPanduan Pengguna.

```
{
    "Statement": [
        {
            "Action": "*",
            "Effect": "Allow",
            "Resource": "*",
            "Principal": "*"
        },
        {
            "Action": "*",
            "Effect": "Deny",
            "Resource": "arn:aws:emr-containers:us-west-2:123456789012:/
virtualclusters/A1B2CD34EF5G",
            "Principal": {
                "AWS": [
                    "123456789012"
                ]
            }
        }
    ]
}
```

Atur akses lintas akun untuk Amazon EMR di EKS

Anda dapat mengatur akses lintas-akun untuk Amazon EMR di EKS. Akses lintas akun memungkinkan pengguna dari satu akun AWS untuk menjalankan tugas Amazon EMR di EKS dan mengakses data yang mendasari milik akun AWS lain.

Prasyarat

Untuk menyiapkan akses lintas-akun untuk Amazon EMR di EKS, Anda akan menyelesaikan tugas saat masuk ke akun AWS:

- `AccountA` - Sebuah akun AWS di mana Anda telah membuat klaster virtual Amazon EMR di EKS dengan mendaftarkan Amazon EMR dengan namespace pada klaster EKS.
- `AccountB` - Sebuah akun AWS yang berisi bucket Amazon S3 atau tabel DynamoDB yang Anda inginkan untuk diakses tugas Amazon EMR di EKS.

Anda harus menyiapkan hal berikut dalam akun AWS Anda mengatur akses lintas akun:

- Klaster virtual Amazon EMR di EKS di `AccountA` di mana Anda ingin menjalankan tugas.
- Peran eksekusi tugas di `AccountA` yang memiliki izin yang diperlukan untuk menjalankan tugas di klaster virtual. Untuk informasi lebih lanjut, lihat Untuk membuat peran eksekusi tugas dan Menggunakan peran eksekusi tugas dengan Amazon EMR di EKS.

Cara mengakses bucket Amazon S3 lintas akun atau tabel DynamoDB

Untuk mengatur akses lintas-akun untuk Amazon EMR di EKS, selesaikan langkah-langkah berikut.

1. Buat bucket Amazon S3, `cross-account-bucket`, di `AccountB`. Untuk informasi lebih lanjut, lihat Membuat bucket. Jika Anda ingin memiliki akses lintas-akun ke DynamoDB, Anda juga dapat membuat tabel DynamoDB di `AccountB`. Untuk informasi selengkapnya, lihat Membuat tabel DynamoDB.
2. Buat IAM role `Cross-Account-Role-B` dalam `AccountB` yang dapat mengakses `cross-account-bucket`.
    1. Masuklah ke konsol IAM.
    2. Pilih Peran dan buat peran baru: `Cross-Account-Role-B`. Untuk informasi selengkapnya tentang cara membuat IAM role, lihat Membuat IAM role dalam Panduan Pengguna IAM.

3. Buat kebijakan IAM yang menentukan izin untuk `Cross-Account-Role-B` untuk mengakses S3 bucket `cross-account-bucket`, seperti yang ditunjukkan pernyataan kebijakan berikut. Kemudian lampirkan kebijakan IAM ke `Cross-Account-Role-B`. Untuk informasi selengkapnya, lihat Membuat Kebijakan Baru dalam Panduan Pengguna IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::cross-account-bucket",
                "arn:aws:s3:::cross-account-bucket/*"
            ]
        }
    ]
}
```

Jika akses DynamoDB diperlukan, buat kebijakan IAM yang menentukan izin untuk mengakses tabel DynamoDB lintas akun. Kemudian lampirkan kebijakan IAM ke `Cross-Account-Role-B`. Untuk informasi selengkapnya, lihat Buat tabel DynamoDB dalam Panduan Pengguna IAM.

Berikut ini adalah kebijakan untuk mengakses tabel DynamoDB, `CrossAccountTable`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "dynamodb:*",
            "Resource": "arn:aws:dynamodb:MyRegion:AccountB:table/
CrossAccountTable"
        }
    ]
}
```

3. Cara mengedit hubungan kepercayaan untuk peran `Cross-Account-Role-B`.

1. Untuk mengonfigurasi hubungan kepercayaan untuk peran, pilih tab Hubungan Kepercayaan di konsol IAM untuk peran yang dibuat di langkah 2: `Cross-Account-Role-B`.
2. Pilih Edit Hubungan Kepercayaan.
3. Tambahkan dokumen kebijakan berikut, yang memungkinkan `Job-Execution-Role-A` dalam `AccountA` untuk mengasumsikan peran `Cross-Account-Role-B` ini.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::AccountA:role/Job-Execution-Role-A"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

4. Berikan `Job-Execution-Role-A` `AccountA` dengan - STS Asumsikan izin peran untuk mengasumsikan`Cross-Account-Role-B`.
   1. Dalam konsol IAM untuk akun AWS `AccountA`, pilih `Job-Execution-Role-A`.
   2. Tambahkan pernyataan kebijakan berikut pada `Job-Execution-Role-A` untuk mengizinkan tindakan `AssumeRole` di peran `Cross-Account-Role-B`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::AccountB:role/Cross-Account-Role-B"
        }
    ]
}
```

5. Untuk akses Amazon S3, atur parameter `spark-submit` berikut (`spark conf`) saat mengirimkan tugas ke Amazon EMR di EKS.

> **Note**
>
> Secara default, EMRFS menggunakan peran eksekusi tugas untuk mengakses bucket S3 dari tugas. Tapi saat `customAWSCredentialsProvider` diatur ke `AssumeRoleAWSCredentialsProvider`, EMRFS menggunakan peran yang sesuai yang Anda tentukan dengan `ASSUME_ROLE_CREDENTIALS_ROLE_ARN` bukan dari `Job-Execution-Role-A` untuk akses Amazon S3.

- `--conf spark.hadoop.fs.s3.customAWSCredentialsProvider=com.amazonaws.emr.AssumeRol`
- `--conf spark.kubernetes.driverEnv.ASSUME_ROLE_CREDENTIALS_ROLE_ARN=arn:aws:iam::Ac Cross-Account-Role-B \`
- `--conf spark.executorEnv.ASSUME_ROLE_CREDENTIALS_ROLE_ARN=arn:aws:iam::AccountB:ro Cross-Account-Role-B \`

> **Note**
>
> Anda harus menetapkan `ASSUME_ROLE_CREDENTIALS_ROLE_ARN` baik untuk pelaksana maupun driver `env` dalam konfigurasi tugas spark.

Untuk akses lintas akun DynamoDB, Anda harus mengatur `--conf spark.dynamodb.customAWSCredentialsProvider=com.amazonaws.emr.AssumeRoleAWSCr`

6. Jalankan Amazon EMR pada tugas EKS dengan akses lintas-akun, seperti yang ditunjukkan contoh berikut.

```
aws emr-containers start-job-run \
--virtual-cluster-id 123456 \
--name myjob \
--execution-role-arn execution-role-arn \
--release-label emr-6.2.0-latest \
--job-driver '{"sparkSubmitJobDriver": {"entryPoint": "entryPoint_location",
 "entryPointArguments": ["arguments_list"], "sparkSubmitParameters": "--class
```

```
 <main_class> --conf spark.executor.instances=2 --conf spark.executor.memory=2G
 --conf spark.executor.cores=2 --conf spark.driver.cores=1 --conf
 spark.hadoop.fs.s3.customAWSCredentialsProvider=com.amazonaws.emr.AssumeRoleAWSCredentials
 --conf
 spark.kubernetes.driverEnv.ASSUME_ROLE_CREDENTIALS_ROLE_ARN=arn:aws:iam::AccountB:role/
Cross-Account-Role-B --conf
 spark.executorEnv.ASSUME_ROLE_CREDENTIALS_ROLE_ARN=arn:aws:iam::AccountB:role/
Cross-Account-Role-B"}} ' \
--configuration-overrides '{"applicationConfiguration": [{"classification":
 "spark-defaults", "properties": {"spark.driver.memory": "2G"}}],
 "monitoringConfiguration": {"cloudWatchMonitoringConfiguration":
 {"logGroupName": "log_group_name", "logStreamNamePrefix": "log_stream_prefix"},
 "persistentAppUI":"ENABLED",  "s3MonitoringConfiguration": {"logUri": "s3://
my_s3_log_location" }}}'
```

Menandai Sumber Daya Amazon EMR di EKS Anda

Untuk membantu Anda mengelola Amazon EMR di EKS, Anda dapat menetapkan metadata Anda sendiri ke setiap sumber daya menggunakan tanda. Topik ini memberikan gambaran umum dari fungsi tanda dan menunjukkan kepada Anda cara membuat tanda.

Topik

Dasar tanda

Tanda adalah sebuah label yang Anda tetapkan ke sebuah sumber daya AWS. Setiap tanda terdiri atas sebuah kunci dan sebuah nilai opsional, yang keduanya Anda tentukan.

Tanda memungkinkan Anda untuk mengategorikan sumber daya AWS dengan atribut seperti tujuan, pemilik, atau lingkungan. Saat Anda memiliki banyak sumber daya dengan jenis yang sama, Anda dapat dengan cepat mengidentifikasi sumber daya tertentu berdasarkan tanda yang telah Anda tetapkan. Misalnya, Anda dapat menentukan serangkaian tanda untuk Amazon EMR Anda pada klaster EKS untuk membantu Anda melacak setiap pemilik dan tingkat tumpukan klaster. Kami menyarankan agar Anda merancang serangkaian konsisten kunci tanda untuk setiap jenis sumber daya. Kemudian Anda dapat mencari dan memfilter sumber daya berdasarkan tanda yang Anda tambahkan.

Tanda tidak secara otomatis ditetapkan ke sumber daya Anda. Setelah Anda menambahkan sebuah tanda, Anda dapat mengedit kunci serta nilai tanda atau menghilangkan tanda dari sumber daya kapanpun yang Anda mau. Jika Anda menghapus sebuah sumber daya, tag apa pun untuk sumber daya tersebut juga dihapus.

Tanda tidak memiliki makna semantik pada Amazon EMR di EKS dan diterjemahkan sebagai serangkaian karakter saja.

Nilai tanda bisa berupa string kosong, tapi tidak null. Kunci tanda tidak bisa berupa string kosong. Jika Anda menambahkan tanda yang memiliki kunci yang sama dengan tanda yang ada pada sumber daya tersebut, nilai yang baru akan menimpa nilai sebelumnya.

Jika Anda menggunakan AWS Identity and Access Management (IAM), Anda dapat mengontrol pengguna mana dalam akun AWS Anda yang memiliki izin untuk mengelola tanda.

Untuk contoh kebijakan kontrol akses berbasis tanda, lihat Kebijakan untuk kendali akses berbasis tanda.

Beri tanda pada sumber daya Anda

Anda dapat menandai klaster virtual dan tugas berjalan baru atau yang sudah ada yang berada dalam status aktif. Status aktif untuk tugas berjalan meliputi: `PENDING`, `SUBMITTED`, `RUNNING`, dan `CANCEL_PENDING`. Status aktif untuk klaster virtual meliputi: `RUNNING`, `TERMINATING` dan `ARRESTED`. Untuk informasi lebih lanjut, lihat Status tugas berjalan dan Status klaster virtual.

Ketika klaster virtual dihentikan, tanda dibersihkan dan tidak lagi dapat diakses.

Jika Anda menggunakan API Amazon EMR di EKS, AWS CLI, atau SDK AWS, Anda dapat memasang tanda ke sumber daya baru menggunakan parameter tanda pada tindakan API yang relevan. Anda dapat memasang tanda ke sumber daya yang ada menggunakan tindakan API `TagResource`.

Anda dapat menggunakan beberapa tindakan penciptaan sumber daya untuk menentukan tanda untuk sumber daya saat sumber daya diciptakan. Dalam kasus ini, jika tanda tidak dapat diterapkan saat sumber daya sedang dibuat, sumber daya gagal untuk dibuat. Mekanisme ini memastikan bahwa sumber daya yang Anda inginkan untuk ditandai pada penciptaan dibuat dengan tanda tertentu atau tidak dibuat sama sekali. Jika Anda menandai sumber daya pada saat penciptaan, Anda tidak perlu untuk menjalankan skrip penandaan khusus setelah penciptaan sumber daya.

Tabel berikut menjelaskan sumber daya Amazon EMR di EKS yang dapat ditandai.

Sumber Daya	Mendukung tanda	Propagasi dukungan tanda	Dukungan penandaan pada penciptaan (API Amazon EMR di EKS, AWS CLI, dan SDK AWS)	API untuk pembuatan (tanda dapat ditambahkan selama pembuatan)
Klaster virtual	Ya	Tidak. Tanda yang terkait	Ya	CreateVirtualCluster

Sumber Daya	Mendukung tanda	Propagasi dukungan tanda	Dukungan penandaan pada penciptaan (API Amazon EMR di EKS, AWS CLI, dan SDK AWS)	API untuk pembuatan (tanda dapat ditambahkan selama pembuatan)
		dengan klaster virtual tidak menyebarkan ke tugas berjalan yang dikirimkan ke cluster virtual tersebut.		
Tugas berjalan	Ya	Tidak	Ya	StartJobRun

Batasan tag

Batasan dasar berikut berlaku untuk tag:

- Jumlah maksimum tanda per sumber daya – 50
- Untuk setiap sumber daya, setiap kunci tag harus unik, dan setiap kunci tag hanya dapat memiliki satu nilai.
- Panjang kunci maksimum – 128 karakter Unicode dalam UTF-8
- Panjang nilai maksimum – 256 karakter Unicode dalam UTF-8
- Jika skema penandaan Anda digunakan di beberapa layanan dan sumber daya AWS, ingatlah bahwa layanan lain mungkin memiliki pembatasan pada karakter yang diizinkan. Karakter yang secara umum diperbolehkan adalah huruf, angka, spasi yang dapat diwakili dalam UTF-8, serta karakter berikut: + - = . _ : / @.
- Kunci dan nilai tag peka huruf besar dan kecil.
- Nilai tanda bisa berupa string kosong, tapi tidak null. Kunci tanda tidak bisa berupa string kosong.
- Jangan gunakan `aws:`, `AWS:`, atau kombinasi huruf besar atau kecil seperti prefiks baik untuk kunci atau nilai. Ini hanya diperuntukkan bagi penggunaan AWS.

Bkerja dengan tanda menggunakan AWS CLI dan API Amazon EMR di EKS

Gunakan perintah AWS CLI berikut atau operasi API Amazon EMR di EKS untuk menambahkan, memperbarui, membuat daftar, dan menghapus tanda untuk sumber daya Anda.

Tugas	AWS CLI	Tindakan API
Penambahan atau penimpaan satu tag atau lebih	tag-resource	TagResource
Daftar tanda untuk sumber daya	list-tags-for-resource	ListTagsForResource
Penghapusan satu tag atau lebih	untag-resource	UntagResource

Contoh berikut menunjukkan cara menandai atau menghapus tanda pada sumber daya menggunakan AWS CLI.

Contoh 1: Menandai klaster virtual yang ada

Perintah berikut memberi tanda klaster virtual yang ada.

```
aws emr-containers tag-resource --resource-arn resource_ARN --tags team=devs
```

Contoh 2: Untag klaster virtual yang ada

Perintah berikut menghapus tanda dari klaster virtual yang ada.

```
aws emr-containers untag-resource --resource-arn resource_ARN --tag-keys tag_key
```

Contoh 3: Daftar tanda untuk sumber daya

Perintah berikut membuat daftar tanda yang terkait dengan sumber daya yang ada.

```
aws emr-containers list-tags-for-resource --resource-arn resource_ARN
```

Memecahkan masalah Amazon EMR di EKS

Bagian ini menjelaskan cara memecahkan masalah dengan Amazon EMR di EKS. Untuk informasi tentang cara memecahkan masalah umum dengan Amazon EMR, lihat Memecahkan masalah klaster di Panduan Manajemen Amazon EMR.

Topik

Pekerjaan pemecahan masalah yang menggunakan PersistentVolumeClaims (PVC)

Jika kamu perlu membuat, mencantumkan, atau menghapus PersistentVolumeClaims (PVC) untuk sebuah job tetapi tidak menambahkan izin PVC ke role emr-container Kubernetes default, maka pekerjaan akan gagal saat kamu mengirimkannya. Tanpa izin ini, peran emr-container tidak dapat membuat peran yang diperlukan untuk driver Spark atau klien Spark. Tidak cukup menambahkan izin ke driver Spark atau peran klien, seperti yang disarankan oleh pesan kesalahan. Peran utama emr-container harus menyertakan izin yang diperlukan juga. Bagian ini menjelaskan cara menambahkan izin yang diperlukan ke peran utama emr-container.

Verifikasi

Untuk memverifikasi apakah peran emr-container Anda memiliki izin yang diperlukan atau tidak, setel variabel NAMESPACE dengan nilai Anda sendiri dan kemudian jalankan perintah berikut:

```
export NAMESPACE=YOUR_VALUE
kubectl describe role emr-containers -n ${NAMESPACE}
```

Selain itu, untuk memverifikasi apakah peran Spark dan klien memiliki izin yang diperlukan, jalankan perintah berikut:

```
kubectl describe role emr-containers-role-spark-driver -n ${NAMESPACE}
kubectl describe role emr-containers-role-spark-client -n ${NAMESPACE}
```

Jika izin tidak ada, lanjutkan dengan tambalan, sebagai berikut.

Patch

1. Jika pekerjaan tanpa izin sedang berjalan, hentikan pekerjaan ini.
2. Buat file bernama RBAC_Patch.py sebagai berikut:

```
import os
import subprocess as sp
import tempfile as temp
import json
import argparse
import uuid

def delete_if_exists(dictionary: dict, key: str):
    if dictionary.get(key, None) is not None:
        del dictionary[key]

def doTerminalCmd(cmd):
    with temp.TemporaryFile() as f:
        process = sp.Popen(cmd, stdout=f, stderr=f)
        process.wait()
        f.seek(0)
        msg = f.read().decode()
    return msg

def patchRole(roleName, namespace, extraRules, skipConfirmation=False):
    cmd = f"kubectl get role {roleName} -n {namespace} --output json".split(" ")
    msg = doTerminalCmd(cmd)
    if "(NotFound)" in msg and "Error" in msg:
        print(msg)
        return False
    role = json.loads(msg)
    rules = role["rules"]
    rulesToAssign = extraRules[::]
    passedRules = []
    for rule in rules:
        apiGroups = set(rule["apiGroups"])
        resources = set(rule["resources"])
        verbs = set(rule["verbs"])
        for extraRule in extraRules:
            passes = 0
            apiGroupsExtra = set(extraRule["apiGroups"])
```

```
            resourcesExtra = set(extraRule["resources"])
            verbsExtra = set(extraRule["verbs"])
            passes += len(apiGroupsExtra.intersection(apiGroups)) >=
len(apiGroupsExtra)
            passes += len(resourcesExtra.intersection(resources)) >=
len(resourcesExtra)
            passes += len(verbsExtra.intersection(verbs)) >= len(verbsExtra)
            if passes >= 3:
                if extraRule not in passedRules:
                    passedRules.append(extraRule)
                    if extraRule in rulesToAssign:
                        rulesToAssign.remove(extraRule)
                break
    prompt_text = "Apply Changes?"
    if len(rulesToAssign) == 0:
        print(f"The role {roleName} seems to already have the necessary
permissions!")
        prompt_text = "Proceed anyways?"
    for ruleToAssign in rulesToAssign:
        role["rules"].append(ruleToAssign)
    delete_if_exists(role, "creationTimestamp")
    delete_if_exists(role, "resourceVersion")
    delete_if_exists(role, "uid")
    new_role = json.dumps(role, indent=3)
    uid = uuid.uuid4()
    filename = f"Role-{roleName}-New_Permissions-{uid}-TemporaryFile.json"
    try:
        with open(filename, "w+") as f:
            f.write(new_role)
            f.flush()
        prompt = "y"
        if not skipConfirmation:
            prompt = input(
                doTerminalCmd(f"kubectl diff -f {filename}".split(" ")) +
f"\n{prompt_text} y/n: "
            ).lower().strip()
            while prompt != "y" and prompt != "n":
                prompt = input("Please make a valid selection. y/n:
").lower().strip()
        if prompt == "y":
            print(doTerminalCmd(f"kubectl apply -f {filename}".split(" ")))
    except Exception as e:
        print(e)
    os.remove(f"./{filename}")
```

```
if __name__ == '__main__':
    parser = argparse.ArgumentParser()
    parser.add_argument("-n", "--namespace",
                        help="Namespace of the Role. By default its the
 VirtualCluster's namespace",
                        required=True,
                        dest="namespace"
                        )

    parser.add_argument("-p", "--no-prompt",
                        help="Applies the patches without asking first",
                        dest="no_prompt",
                        default=False,
                        action="store_true"
                        )
    args = parser.parse_args()

    emrRoleRules = [
        {
            "apiGroups": [""],
            "resources": ["persistentvolumeclaims"],
            "verbs": ["list", "create", "delete"]
         }

    ]

    driverRoleRules = [
        {
            "apiGroups": [""],
            "resources": ["persistentvolumeclaims"],
            "verbs": ["list", "create", "delete"]
        },
        {
            "apiGroups": [""],
            "resources": ["services"],
            "verbs": ["get", "list", "describe", "create", "delete", "watch"]
        }
    ]

    clientRoleRules = [
        {
            "apiGroups": [""],
            "resources": ["persistentvolumeclaims"],
```

```
            "verbs": ["list", "create", "delete"]
        }
    ]

    patchRole("emr-containers", args.namespace, emrRoleRules, args.no_prompt)
    patchRole("emr-containers-role-spark-driver", args.namespace, driverRoleRules,
 args.no_prompt)
    patchRole("emr-containers-role-spark-client", args.namespace, clientRoleRules,
 args.no_prompt)
```

3. Jalankan skrip Python:

```
python3 RBAC_Patch.py -n ${NAMESPACE}
```

4. Perbedaan kubectl antara izin baru dan yang lama akan muncul. Tekan y untuk menambal peran.
5. Verifikasi tiga peran dengan izin tambahan sebagai berikut:

```
kubectl describe role -n ${NAMESPACE}
```

6. Jalankan skrip python:

```
python3 RBAC_Patch.py -n ${NAMESPACE}
```

7. Setelah menjalankan perintah, ia akan menampilkan perbedaan kubectl antara izin baru dan yang lama. Tekan y untuk menambal peran.
8. Verifikasi tiga peran dengan izin tambahan:

```
kubectl describe role -n ${NAMESPACE}
```

9. Kirimkan pekerjaan lagi.

Tambalan manual

Jika izin yang diperlukan aplikasi Anda berlaku untuk sesuatu selain aturan PVC, Anda dapat secara manual menambahkan izin Kubernetes untuk klaster virtual Amazon EMR Anda sesuai kebutuhan.

> **Note**
>
> Peran emr-kontainer adalah peran utama. Ini berarti bahwa ia harus menyediakan semua izin yang diperlukan sebelum Anda dapat mengubah peran driver atau klien yang mendasarinya.

1. Unduh izin saat ini ke file yaml dengan menjalankan perintah di bawah ini:

```
kubectl get role -n ${NAMESPACE} emr-containers -o yaml >> emr-containers-role-patch.yaml
kubectl get role -n ${NAMESPACE} emr-containers-role-spark-driver -o yaml >> driver-role-patch.yaml
kubectl get role -n ${NAMESPACE} emr-containers-role-spark-client -o yaml >> client-role-patch.yaml
```

2. Berdasarkan izin yang dibutuhkan aplikasi Anda, edit setiap file dan tambahkan aturan tambahan seperti berikut ini:

   - emr-containers-role-patch.yaml

```
- apiGroups:
  - ""
  resources:
  - persistentvolumeclaims
  verbs:
  - list
  - create
  - delete
```

   - driver-role-patch.yaml

```
- apiGroups:
  - ""
  resources:
  - persistentvolumeclaims
  verbs:
  - list
  - create
  - delete
- apiGroups:
  - ""
  resources:
```

```
  - services
  verbs:
  - get
  - list
  - describe
  - create
  - delete
  - watch
```

- client-role-patch.yaml

```
- apiGroups:
  - ""
  resources:
  - persistentvolumeclaims
  verbs:
  - list
  - create
  - delete
```

3. Hapus atribut berikut dengan nilainya. Ini diperlukan untuk menerapkan pembaruan.
   - KreasiTimestamp
   - ResourceVersion
   - uid
4. Akhirnya, jalankan tambalan:

```
kubectl apply -f emr-containers-role-patch.yaml
kubectl apply -f driver-role-patch.yaml
kubectl apply -f client-role-patch.yaml
```

Memecahkan masalah Amazon EMR pada penskalaan otomatis vertikal EKS

Lihat bagian berikut jika Anda mengalami masalah saat menyiapkan Amazon EMR pada operator penskalaan otomatis vertikal EKS pada klaster Amazon EKS dengan Operator Lifecycle Manager. Untuk informasi lebih lanjut termasuk langkah-langkah untuk menyelesaikan instalasi, lihatMenggunakan penskalaan otomatis vertikal dengan pekerjaan Amazon EMR Spark .

403 Dilarang

Jika Anda mengikuti langkah-langkahInstal Operator Lifecycle Manager (OLM) di klaster Amazon EKS, menjalankan `olm status` perintah, dan mengembalikan `403 Forbidden` kesalahan seperti di bawah ini, Anda mungkin tidak memperoleh token otentikasi ke repositori Amazon ECR untuk operator.

Untuk mengatasi masalah ini, ulangi langkah Instal Amazon EMR pada operator penskalaan otomatis vertikal EKS untuk mendapatkan token. Kemudian, coba instalasi lagi.

```
Error: FATA[0002] Failed to run bundle: pull bundle image: error pulling image IMAGE.
error resolving name : unexpected status code [manifests latest]: 403 Forbidden
```

Namespace Kubernetes tidak ditemukan

Saat Anda mengatur Amazon EMR pada operator penskalaan otomatis vertikal EKS pada klaster Amazon EKS, Anda mungkin mendapatkan `namespaces not found` kesalahan seperti yang ditunjukkan di sini:

```
FATA[0020] Failed to run bundle: create catalog: error creating catalog source:
 namespaces "NAME" not found.
```

Jika namespace yang Anda tentukan tidak ada, OLM tidak akan menginstal operator autoscaling vertikal. Untuk mengatasi masalah ini, gunakan perintah berikut untuk membuat namespace. Kemudian, coba instalasi lagi.

```
kubectl create namespace NAME
```

Galat saat menyimpan kredensi Docker

Untuk mengatur penskalaan otomatis vertikal, Anda harus mengautentikasi dan mengambil Amazon EMR pada gambar Docker terkait autoscaling vertikal EKS. Ketika Anda melakukan ini, Anda mungkin mendapatkan kesalahan seperti yang berikut jika Docker tidak berjalan:

```
aws ecr get-login-password \
 --region $REGION | docker login \
 --username AWS \
 --password-stdin $ACCOUNT_ID.dkr.ecr.$REGION.amazonaws.com
```

```
Error saving credentials: error storing credentials - err: exit status 1
out: 'Post "http://ipc/registry/credstore-updated": dial unix backend.sock: connect: no
 such file or directory'
```

Untuk mengatasi masalah ini, konfirmasikan bahwa Docker sedang berjalan atau membuka Docker Desktop. Kemudian, coba simpan kredensialmu lagi.

Memecahkan masalah Amazon EMR pada operator EKS

Lihat bagian berikut jika Anda mengalami masalah dengan Amazon EMR pada operator EKS Spark. Untuk informasi lebih lanjut termasuk langkah-langkah untuk menyelesaikan instalasi, lihatMenjalankan pekerjaan Spark dengan operator Spark.

Kesalahan pada instalasi bagan Helm

Jika Anda mengikuti langkah-langkah Instal operator Spark dan mengembalikan `INSTALLATION FAILED` kesalahan seperti yang di bawah ini ketika Anda mencoba menginstal atau memverifikasi bagan Helm, Anda mungkin tidak memperoleh token otentikasi ke repositori Amazon ECR untuk operator.

Untuk mengatasi masalah ini, ulangi langkah di Instal operator Spark untuk autentikasi Helm client Anda ke registrasi Amazon ECR. Kemudian, coba langkah instalasi lagi.

```
Error: INSTALLATION FAILED: Kubernetes cluster unreachable: the server has asked for
 the client to provide credentials
```

UnsupportedFileSystemException: Tidak FileSystem untuk skema “s3"

Anda mungkin menemukan pengecualian berikut di thread “main”:

```
org.apache.hadoop.fs.UnsupportedFileSystemException: No FileSystem for scheme "s3"
```

Jika ini terjadi, tambahkan pengecualian berikut ke `SparkApplication` spesifikasi:

```
 hadoopConf:
   # EMRFS filesystem
   fs.s3.customAWSCredentialsProvider:
 com.amazonaws.auth.WebIdentityTokenCredentialsProvider
```

```
    fs.s3.impl: com.amazon.ws.emr.hadoop.fs.EmrFileSystem
    fs.AbstractFileSystem.s3.impl: org.apache.hadoop.fs.s3.EMRFSDelegate
    fs.s3.buffer.dir: /mnt/s3
    fs.s3.getObject.initialSocketTimeoutMilliseconds: "2000"
    mapreduce.fileoutputcommitter.algorithm.version.emr_internal_use_only.EmrFileSystem:
 "2"
    mapreduce.fileoutputcommitter.cleanup-
failures.ignored.emr_internal_use_only.EmrFileSystem: "true"
 sparkConf:
    # Required for EMR Runtime
    spark.driver.extraClassPath: /usr/lib/hadoop-lzo/lib/*:/usr/lib/hadoop/hadoop-
aws.jar:/usr/share/aws/aws-java-sdk/*:/usr/share/aws/emr/emrfs/conf:/usr/share/aws/
emr/emrfs/lib/*:/usr/share/aws/emr/emrfs/auxlib/*:/usr/share/aws/emr/security/conf:/
usr/share/aws/emr/security/lib/*:/usr/share/aws/hmclient/lib/aws-glue-datacatalog-
spark-client.jar:/usr/share/java/Hive-JSON-Serde/hive-openx-serde.jar:/usr/share/aws/
sagemaker-spark-sdk/lib/sagemaker-spark-sdk.jar:/home/hadoop/extrajars/*
    spark.driver.extraLibraryPath: /usr/lib/hadoop/lib/native:/usr/lib/hadoop-lzo/lib/
native:/docker/usr/lib/hadoop/lib/native:/docker/usr/lib/hadoop-lzo/lib/native
    spark.executor.extraClassPath: /usr/lib/hadoop-lzo/lib/*:/usr/lib/hadoop/hadoop-
aws.jar:/usr/share/aws/aws-java-sdk/*:/usr/share/aws/emr/emrfs/conf:/usr/share/aws/
emr/emrfs/lib/*:/usr/share/aws/emr/emrfs/auxlib/*:/usr/share/aws/emr/security/conf:/
usr/share/aws/emr/security/lib/*:/usr/share/aws/hmclient/lib/aws-glue-datacatalog-
spark-client.jar:/usr/share/java/Hive-JSON-Serde/hive-openx-serde.jar:/usr/share/aws/
sagemaker-spark-sdk/lib/sagemaker-spark-sdk.jar:/home/hadoop/extrajars/*
    spark.executor.extraLibraryPath: /usr/lib/hadoop/lib/native:/usr/lib/hadoop-lzo/lib/
native:/docker/usr/lib/hadoop/lib/native:/docker/usr/lib/hadoop-lzo/lib/native
```

Kuota layanan Amazon EMdi EKS

Berikut ini adalah titik akhir layanan dan kuota layanan untuk Amazon EMR di EKS. Untuk menghubungkan secara programatis ke layanan AWS, Anda menggunakan titik akhir. Selain titik akhir AWS standar, beberapa layanan AWS menawarkan titik akhir FIPS di Wilayah terpilih. Untuk informasi selengkapnya, lihat AWS titik akhir layanan. Kuota layanan, juga disebut sebagai batasan, adalah jumlah maksimum sumber daya layanan atau operasi untuk AWS akun Anda. Untuk informasi lebih lanjut, lihat AWS kuota layanan.

Titik akhir layanan

Wilayah AWS nama	Code	Titik akhir	Protokol
AS Timur (N. Virginia)	us-east-1	`emr-containers.us-east-1.amazonaws.com`	HTTPS
US East (Ohio)	us-east-2	`emr-containers.us-east-2.amazonaws.com`	HTTPS
US West (N. Californi a)	us-west-1	`emr-containers.us-west-1.amazonaws.com`	HTTPS
US West (Oregon)	us-west-2	`emr-containers.us-west-2.amazonaws.com`	HTTPS
Asia Pacific (Tokyo)	ap-northe ast-1	`emr-containers.ap-northeast-1.amazonaws.com`	HTTPS
Asia Pacific (Seoul)	ap-northe ast-2	`emr-containers.ap-northeast-2.amazonaws.com`	HTTPS
Asia Pacific (Mumbai)	ap-south-1	`emr-containers.ap-south-1.amazonaws.com`	HTTPS
Asia Pacific (Singapor e)	ap-southe ast-1	`emr-containers.ap-southeast-1.amazonaws.com`	HTTPS

Wilayah AWS nama	Code	Titik akhir	Protokol
Asia Pacific (Sydney)	ap-southeast-2	`emr-containers.ap-southeast-2.amazonaws.com`	HTTPS
Asia Pacific (Hong Kong)	ap-east-1	`emr-containers.ap-east-1.amazonaws.com`	HTTPS
Canada (Central)	ca-central-1	`emr-containers.ca-central-1.amazonaws.com`	HTTPS
Europe (Frankfurt)	eu-central-1	`emr-containers.eu-central-1.amazonaws.com`	HTTPS
Europe (Ireland)	eu-west-1	`emr-containers.eu-west-1.amazonaws.com`	HTTPS
Europe (London)	eu-west-2	`emr-containers.eu-west-2.amazonaws.com`	HTTPS
Europe (Stockholm)	eu-north-1	`emr-containers.eu-north-1.amazonaws.com`	HTTPS
South America (Sao Paulo)	sa-east-1	`emr-containers.sa-east-1.amazonaws.com`	HTTPS
Middle East (Bahrain)	me-south-1	`emr-containers.me-south-1.amazonaws.com`	HTTPS
AWSGovCloud(AS-timur)	us-gov-east-1	`emr-containers.us-gov-east-1.amazonaws.com`	HTTPS
AWSGovCloud(AS-Barat)	us-gov-west-1	`emr-containers.us-gov-west-1.amazonaws.com`	HTTPS

Kuota layanan

Amazon EMR di EKS melakukan throttling permintaan API berikut untuk setiap akun AWS secara per Wilayah. Untuk informasi selengkapnya tentang cara throttling diterapkan, lihat Throttling Permintaan

API dalam Referensi API Amazon EC2. Anda dapat meminta penambahan kuota throttling API untuk akun AWS Anda.

Tindakan API	Kapasitas maksimum bucket	Tingkat isi ulang bucket (per detik)
CancelJobRun	25	1
CreateManagedEndpoint	25	1
CreateVirtualCluster	25	1
DeleteManagedEndpoint	25	1
DeleteVirtualCluster	25	1
DescribeJobRun	25	1
DescribeVirtualCluster	25	1
ListJobRun	25	1
ListManagedEndpoint	25	1
ListVirtualCluster	25	1
StartJobRun	25	1
At the AWS account level, the bucket maximum capacity and refill rate for the sum of all API actions listed in this table	50	7

Amazon EMR pada rilis EKS

Rilis Amazon EMR adalah seperangkat aplikasi sumber terbuka dari ekosistem big data. Setiap rilis terdiri dari aplikasi, komponen, dan fitur big data yang berbeda yang Anda pilih untuk meminta Amazon EMR di EKS menyebarkan dan mengonfigurasi ketika Anda menjalankan tugas berjalan Anda.

Dimulai dengan Amazon EMR rilis 5.32.0 dan 6.2.0, Anda dapat menerapkan Amazon EMR di EKS. Opsi deployment ini tidak tersedia dengan versi rilis Amazon EMR sebelumnya. Anda harus menentukan versi rilis yang didukung ketika Anda mengirimkan tugas Anda.

Amazon EMR di EKS menggunakan bentuk berikut dari label rilis: `emr-x.x.x-latest` atau `emr-x.x.x-yyyymmdd` dengan tanggal rilis tertentu. Misalnya, `emr-7.0.0-latest` atau `emr-7.0.0-20210129`. Saat Anda menggunakan `-latest` akhiran, Anda memastikan bahwa versi EMR Amazon Anda selalu menyertakan pembaruan keamanan terbaru.

> **Note**
>
> Untuk perbandingan antara Amazon EMR di EKS dan Amazon EMR yang berjalan di EC2, lihat FAQ Amazon EMR di situs web. AWS

Topik

- Amazon EMR pada rilis EKS 6.5.0
- Amazon EMR pada rilis EKS 6.4.0
- Amazon EMR pada rilis EKS 6.3.0
- Amazon EMR pada rilis EKS 6.2.0
- Amazon EMR pada rilis EKS 5.36.0
- Amazon EMR pada rilis EKS 5.35.0
- Amazon EMR pada rilis EKS 5.34.0
- Amazon EMR pada rilis EKS 5.33.0
- Amazon EMR pada rilis EKS 5.32.0

Amazon EMR pada rilis EKS 7.0.0

Halaman ini menjelaskan fungsionalitas baru dan yang diperbarui untuk Amazon EMR yang khusus untuk EMR Amazon pada penerapan EKS. Untuk detail tentang Amazon EMR yang berjalan di Amazon EC2 dan tentang rilis Amazon EMR 7.0.0 secara umum, lihat Amazon EMR 7.0.0 di Panduan Rilis Amazon EMR.

Amazon EMR pada rilis EKS 7.0

Rilis Amazon EMR 7.0.0 berikut tersedia untuk Amazon EMR di EKS. Pilih rilis EMR-7.0.0-XXXX tertentu untuk melihat detail selengkapnya seperti tag gambar kontainer terkait.

Flink releases

Rilis Amazon EMR 7.0.0 berikut tersedia untuk Amazon EMR di EKS saat Anda menjalankan aplikasi Flink.

- emr-7.0.0-flink-terbaru
- emr-7.0.0-batu pipi-20231211

Spark releases

Rilis Amazon EMR 7.0.0 berikut tersedia untuk Amazon EMR di EKS saat Anda menjalankan aplikasi Spark.

- emr-7.0.0-terbaru

- emr-7.0.0-20231211
- emr-7.0.0-spark-rapids-latest
- emr-7.0.0-spark-rapids-20231211
- emr-7.0.0-java11-latest
- emr-7.0.0-java11-20231211
- emr-7.0.0-java8-latest
- emr-7.0.0-java8-20231211
- emr-7.0.0-spark-rapids-java8-latest
- emr-7.0.0-spark-rapids-java8-20231211
- notebook-spark/emr-7.0.0-latest
- notebook-spark/emr-7.0.0-20231211
- notebook-spark/emr-7.0.0-spark-rapids-latest
- notebook-spark/emr-7.0.0-spark-rapids-20231211
- notebook-spark/emr-7.0.0-java11-latest
- notebook-spark/emr-7.0.0-java11-20231211
- notebook-spark/emr-7.0.0-java8-latest
- notebook-spark/emr-7.0.0-java8-20231211
- notebook-spark/emr-7.0.0-spark-rapids-java8-latest
- notebook-spark/emr-7.0.0-spark-rapids-java8-20231211
- notebook-python/emr-7.0.0-latest
- notebook-python/emr-7.0.0-20231211
- notebook-python/emr-7.0.0-spark-rapids-latest
- notebook-python/emr-7.0.0-spark-rapids-20231211
- notebook-python/emr-7.0.0-java11-latest
- notebook-python/emr-7.0.0-java11-20231211
- notebook-python/emr-7.0.0-java8-latest
- notebook-python/emr-7.0.0-java8-20231211
- notebook-python/emr-7.0.0-spark-rapids-java8-latest
- notebook-python/emr-7.0.0-spark-rapids-java8-20231211

Catatan perilisan

Catatan rilis untuk Amazon EMR di EKS 7.0.0

- Aplikasi yang didukung - AWS SDK for Java 2.20.160-amzn-0 and 1.12.595, Apache Spark 3.5.0-amzn-0, Apache Flink 1.18.0-amzn-0, Flink Operator 1.6.1, Apache Hudi 0.14.0-amzn-1, Apache Iceberg 1.4.2-amzn-0, Delta 3.0.0, Apache Spark RAPIDS 23.10.0-amzn-0, Jupyter Enterprise Gateway 2.6.0
- Komponen yang didukung - `aws-sagemaker-spark-sdkemr-ddb`,`emr-goodies`,,`emr-s3-select`,`emrfs`,`hadoop-client`,`hudi`,`hudi-spark`,`iceberg`,`spark-kubernetes`.
- Klasifikasi konfigurasi yang didukung

  Untuk digunakan dengan StartJobRundan CreateManagedEndpointAPI:

Klasifikasi	Deskripsi
`core-site`	Ubah nilai dalam file `core-site.xml` Hadoop.
`emrfs-site`	Ubah pengaturan EMRFS.
`spark-metrics`	Ubah nilai dalam file `metrics.properties` Spark.
`spark-defaults`	Ubah nilai dalam file `spark-defaults.conf` Spark.
`spark-env`	Ubah nilai di lingkungan Spark.
`spark-hive-site`	Ubah nilai dalam file `hive-site.xml` Spark.
`spark-log4j2`	Ubah nilai dalam file `log4j2.properties` Spark.
`emr-job-submitter`	Konfigurasi untuk pod pengirim pekerjaan.

  Untuk digunakan secara khusus dengan CreateManagedEndpointAPI:

Klasifikasi	Deskripsi
`jeg-config`	Ubah nilai dalam file Jupyter Enterprise Gatewayjupyter_enterprise_gateway_config.py .
`jupyter-kernel-overrides`	Ubah nilai untuk Gambar Kernel di file Spesifikasi Kernel Jupyter.

Klasifikasi konfigurasi memungkinkan Anda menyesuaikan aplikasi. Ini sering kali bersesuaian dengan file XML konfigurasi untuk aplikasi, seperti `spark-hive-site.xml`. Untuk informasi selengkapnya, lihat Mengkonfigurasi Aplikasi.

Fitur penting

Fitur-fitur berikut disertakan dengan rilis 7.0 Amazon EMR di EKS.

- Peningkatan aplikasi - Amazon EMR pada peningkatan aplikasi EKS 7.0.0 termasuk Spark 3.5, Flink 1.18, dan Flink Operator 1.6.1.
- Penyetelan otomatis parameter Flink Autoscaler — Parameter default yang digunakan Flink Autoscaler untuk perhitungan penskalaannya mungkin bukan nilai optimal untuk pekerjaan tertentu. Amazon EMR di EKS 7.0.0 menggunakan tren historis metrik tertentu yang diambil untuk menghitung parameter optimal yang disesuaikan untuk pekerjaan tersebut.

Perubahan

Perubahan berikut disertakan dengan rilis 7.0 Amazon EMR di EKS.

- Amazon Linux 2023 - Dengan Amazon EMR di EKS 7.0.0 dan yang lebih tinggi, semua gambar kontainer didasarkan pada Amazon Linux 2023.
- Spark menggunakan Java 17 sebagai runtime default - Amazon EMR di EKS 7.0.0 Spark menggunakan Java 17 sebagai runtime default. Jika perlu, Anda dapat beralih untuk menggunakan Java 8 atau Java 11 dengan label rilis yang sesuai seperti yang disediakan dalam Amazon EMR pada rilis EKS 7.0 daftar.

Masalah yang diketahui

Masalah yang diketahui berikut telah diidentifikasi untuk rilis 7.0 Amazon EMR di EKS.

- Kami telah menemukan kemungkinan masalah korupsi data saat Anda menjalankan pekerjaan Spark `emr-7.0.0` karena masalah mendasar di JDK 17. Ketika Anda mengirimkan pekerjaan Spark dengan konfigurasi default, itu menetapkan opsi `-XX:UseAVX=2` Java secara default dan tidak terpengaruh oleh masalah ini. Jika Anda menyesuaikan opsi Spark Java Anda, Anda harus memastikan `-XX:UseAVX=2` itu disertakan. Misalnya, jika Anda mengonfigurasi milik Anda sendiri`spark.executor.defaultJavaOptions`, Anda harus menyertakan tanda ini saat mengirimkan pekerjaan Anda. Amazon EMR akan memperbaiki masalah ini di pembaruan di masa mendatang.

emr-7.0.0-terbaru

Catatan rilis: `emr-7.0.0-latest` saat ini menunjuk ke `emr-7.0.0-20231211`.

Wilayah: `emr-7.0.0-latest` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-7.0.0:latest`

emr-7.0.0-20231211

Catatan rilis: `7.0.0-20231211` dirilis pada bulan Desember 2023. Ini adalah rilis awal Amazon EMR 7.0.0 (Spark).

Wilayah: `emr-7.0.0-20231211` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-7.0.0:20231211`

emr-7.0.0-flink-terbaru

Catatan rilis: `emr-7.0.0-flink-latest` saat ini menunjuk ke `emr-7.0.0-flink-20231211`.

Wilayah: `emr-7.0.0-flink-latest` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-7.0.0-flink:latest`

emr-7.0.0-batu pipi-20231211

Catatan rilis: `7.0.0-flink-20231211` dirilis pada Desember 2023. Ini adalah rilis awal Amazon EMR 7.0.0 (Flink).

Wilayah: `emr-7.0.0-flink-20231211` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-7.0.0-flink:20231211`

Amazon EMR pada rilis EKS 6.15.0

Halaman ini menjelaskan fungsionalitas baru dan yang diperbarui untuk Amazon EMR yang khusus untuk EMR Amazon pada penerapan EKS. Untuk detail tentang Amazon EMR yang berjalan di Amazon EC2 dan tentang rilis Amazon EMR 6.15.0 secara umum, lihat Amazon EMR 6.15.0 di Panduan Rilis Amazon EMR.

Amazon EMR pada rilis EKS 6.15

Rilis Amazon EMR 6.15.0 berikut tersedia untuk Amazon EMR di EKS. Pilih rilis EMR-6.15.0-XXXX tertentu untuk melihat detail selengkapnya seperti tag gambar kontainer terkait.

Flink releases

Rilis Amazon EMR 6.15.0 berikut tersedia untuk Amazon EMR di EKS saat Anda menjalankan aplikasi Flink.

- emr-6.15.0-flink-terbaru
- emr-6.15.0-batu pipi-20231109

Spark releases

Rilis Amazon EMR 6.15.0 berikut tersedia untuk Amazon EMR di EKS saat Anda menjalankan aplikasi Spark.

- emr-6.15.0-terbaru
- emr-6.15.0-20231109
- emr-6.15.0-spark-rapids-latest

- emr-6.15.0-spark-rapids-20231109
- emr-6.15.0-java11-latest
- emr-6.15.0-java11-20231109
- emr-6.15.0-java17-latest
- emr-6.15.0-java17-20231109
- emr-6.15.0-java17-al2023-latest
- emr-6.15.0-java17-al2023-20231109
- emr-6.15.0-spark-rapids-java17-latest
- emr-6.15.0-spark-rapids-java17-20231109
- emr-6.15.0-spark-rapids-java17-al2023-latest
- emr-6.15.0-spark-rapids-java17-al2023-20231109
- notebook-spark/emr-6.15.0-latest
- notebook-spark/emr-6.15.0-20231109
- notebook-spark/emr-6.15.0-spark-rapids-latest
- notebook-spark/emr-6.15.0-spark-rapids-20231109
- notebook-spark/emr-6.15.0-java11-latest
- notebook-spark/emr-6.15.0-java11-20231109
- notebook-spark/emr-6.15.0-java17-latest
- notebook-spark/emr-6.15.0-java17-20231109
- notebook-spark/emr-6.15.0-java17-al2023-latest
- notebook-spark/emr-6.15.0-java17-al2023-20231109
- notebook-python/emr-6.15.0-latest
- notebook-python/emr-6.15.0-20231109
- notebook-python/emr-6.15.0-spark-rapids-latest
- notebook-python/emr-6.15.0-spark-rapids-20231109
- notebook-python/emr-6.15.0-java11-latest
- notebook-python/emr-6.15.0-java11-20231109
- notebook-python/emr-6.15.0-java17-latest
- notebook-python/emr-6.15.0-java17-20231109

- notebook-python/emr-6.15.0-java17-al2023-latest
- notebook-python/emr-6.15.0-java17-al2023-20231109

Catatan perilisan

Catatan rilis untuk Amazon EMR di EKS 6.15.0

- Aplikasi yang didukung - AWS SDK for Java 1.12.543, Apache Spark 3.4.1-amzn-2, Apache Flink 1.17.1-amzn-1, Apache Hudi 0.14.0-amzn-0, Apache Iceberg 1.4.0-amzn-0, Delta 2.4.0, Apache Spark RAPIDS 23.08.01-amzn-0, Jupyter Enterprise Gateway 2.6.0
- Komponen yang didukung - `aws-sagemaker-spark-sdkemr-ddb`,`emr-goodies`,,`emr-s3-select`,`emrfs`,`hadoop-client`,`hudi`,`hudi-spark`,`iceberg`,`spark-kubernetes`.
- Klasifikasi konfigurasi yang didukung

  Untuk digunakan dengan StartJobRundan CreateManagedEndpointAPI:

Klasifikasi	Deskripsi
`core-site`	Ubah nilai dalam file `core-site.xml` Hadoop.
`emrfs-site`	Ubah pengaturan EMRFS.
`spark-metrics`	Ubah nilai dalam file `metrics.properties` Spark.
`spark-defaults`	Ubah nilai dalam file `spark-defaults.conf` Spark.
`spark-env`	Ubah nilai di lingkungan Spark.
`spark-hive-site`	Ubah nilai dalam file `hive-site.xml` Spark.
`spark-log4j2`	Ubah nilai dalam file `log4j2.properties` Spark.
`emr-job-submitter`	Konfigurasi untuk pod pengirim pekerjaan.

Untuk digunakan secara khusus dengan CreateManagedEndpointAPI:

Klasifikasi	Deskripsi
`jeg-config`	Ubah nilai dalam file Jupyter Enterprise Gatewayjupyter_enterprise_gateway_config.py .
`jupyter-kernel-overrides`	Ubah nilai untuk Gambar Kernel di file Spesifikasi Kernel Jupyter.

Klasifikasi konfigurasi memungkinkan Anda menyesuaikan aplikasi. Ini sering kali bersesuaian dengan file XML konfigurasi untuk aplikasi, seperti `spark-hive-site.xml`. Untuk informasi selengkapnya, lihat Mengkonfigurasi Aplikasi.

Fitur penting

Fitur-fitur berikut disertakan dengan rilis 6.15 Amazon EMR di EKS.

- Amazon EMR di EKS dengan Apache Flink - Dengan Amazon EMR di EKS 6.15.0, Anda dapat menjalankan aplikasi berbasis Apache Flink bersama dengan jenis aplikasi lain di cluster Amazon EKS yang sama. Ini membantu meningkatkan pemanfaatan sumber daya dan menyederhanakan manajemen infrastruktur. Anda dapat memanfaatkan Instans Spot di aplikasi Flink dengan penonaktifan yang anggun, dan mencapai waktu restart yang lebih cepat dengan pemulihan berbutir halus dan pemulihan lokal tugas dengan Amazon EBS. Fitur aksesibilitas dan pemantauan mencakup kemampuan untuk meluncurkan aplikasi Flink dengan toples yang disimpan di Amazon S3, akses ke Katalog Data AWS Glue, pemantauan integrasi dengan Amazon S3 dan CloudWatch Amazon, dan rotasi log kontainer.

emr-6.15.0-terbaru

Catatan rilis: `emr-6.15.0-latest` saat ini menunjuk ke `emr-6.15.0-20231109`.

Wilayah: `emr-6.15.0-latest` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.15.0:latest`

emr-6.15.0-20231109

Catatan rilis: `6.15.0-20231109` dirilis pada 17 November 2023. Ini adalah rilis awal Amazon EMR 6.15.0.

Wilayah: `emr-6.15.0-20231109` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.15.0:20231109`

emr-6.15.0-flink-terbaru

Catatan rilis: `emr-6.15.0-flink-latest` saat ini menunjuk ke `emr-6.15.0-flink-20231109`.

Wilayah: `emr-6.15.0-flink-latest` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.15.0-flink:latest`

emr-6.15.0-batu pipi-20231109

Catatan rilis: `6.15.0-flink-20231109` dirilis pada 17 November 2023. Ini adalah rilis awal Amazon EMR 6.15.0.

Wilayah: `emr-6.15.0-flink-20231109` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.15.0-flink:20231109`

Amazon EMR pada rilis EKS 6.14.0

Halaman ini menjelaskan fungsionalitas baru dan yang diperbarui untuk Amazon EMR yang khusus untuk EMR Amazon pada penerapan EKS. Untuk detail tentang Amazon EMR yang berjalan di Amazon EC2 dan tentang rilis Amazon EMR 6.14.0 secara umum, lihat Amazon EMR 6.14.0 di Panduan Rilis Amazon EMR.

Amazon EMR pada rilis EKS 6.14

Rilis Amazon EMR 6.14.0 berikut tersedia untuk Amazon EMR di EKS. Pilih rilis EMR-6.14.0-XXXX tertentu untuk melihat detail selengkapnya seperti tag gambar kontainer terkait.

- emr-6.14.0-terbaru
- emr-6.14.0-20231005
- emr-6.14.0-spark-rapids-latest
- emr-6.14.0-spark-rapids-20231005
- emr-6.14.0-java11-latest
- emr-6.14.0-java11-20231005
- emr-6.14.0-java17-latest
- emr-6.14.0-java17-20231005
- emr-6.14.0-java17-al2023-latest
- emr-6.14.0-java17-al2023-20231005
- emr-6.14.0-spark-rapids-java17-latest
- emr-6.14.0-spark-rapids-java17-20231005
- emr-6.14.0-spark-rapids-java17-al2023-latest
- emr-6.14.0-spark-rapids-java17-al2023-20231005
- notebook-spark/emr-6.14.0-latest
- notebook-spark/emr-6.14.0-20231005
- notebook-spark/emr-6.14.0-spark-rapids-latest
- notebook-spark/emr-6.14.0-spark-rapids-20231005
- notebook-spark/emr-6.14.0-java11-latest
- notebook-spark/emr-6.14.0-java11-20231005
- notebook-spark/emr-6.14.0-java17-latest
- notebook-spark/emr-6.14.0-java17-20231005
- notebook-spark/emr-6.14.0-java17-al2023-latest
- notebook-spark/emr-6.14.0-java17-al2023-20231005
- notebook-python/emr-6.14.0-latest
- notebook-python/emr-6.14.0-20231005
- notebook-python/emr-6.14.0-spark-rapids-latest
- notebook-python/emr-6.14.0-spark-rapids-20231005
- notebook-python/emr-6.14.0-java11-latest

- notebook-python/emr-6.14.0-java11-20231005
- notebook-python/emr-6.14.0-java17-latest
- notebook-python/emr-6.14.0-java17-20231005
- notebook-python/emr-6.14.0-java17-al2023-latest
- notebook-python/emr-6.14.0-java17-al2023-20231005

Catatan perilisan

Catatan rilis untuk Amazon EMR di EKS 6.14.0

- Aplikasi yang didukung - AWS SDK for Java 1.12.543, Apache Spark 3.4.1-amzn-1, Apache Hudi 0.13.1-amzn-2, Apache Iceberg 1.3.0-amzn-0, Delta 2.4.0, Apache Spark RAPIDS 23.06.0-amzn-2, Jupyter Enterprise Gateway 2.7.0
- Komponen yang didukung - `aws-sagemaker-spark-sdkemr-ddb`,`emr-goodies`,,`emr-s3-select`,`emrfs`,`hadoop-client`,`hudi`,`hudi-spark`,`iceberg`,`spark-kubernetes`.
- Klasifikasi konfigurasi yang didukung

  Untuk digunakan dengan StartJobRundan CreateManagedEndpointAPI:

Klasifikasi	Deskripsi
`core-site`	Ubah nilai dalam file `core-site.xml` Hadoop.
`emrfs-site`	Ubah pengaturan EMRFS.
`spark-metrics`	Ubah nilai dalam file `metrics.properties` Spark.
`spark-defaults`	Ubah nilai dalam file `spark-defaults.conf` Spark.
`spark-env`	Ubah nilai di lingkungan Spark.
`spark-hive-site`	Ubah nilai dalam file `hive-site.xml` Spark.

Klasifikasi	Deskripsi
`spark-log4j2`	Ubah nilai dalam file `log4j2.properties` Spark.
`emr-job-submitter`	Konfigurasi untuk pod pengirim pekerjaan.

Untuk digunakan secara khusus dengan CreateManagedEndpointAPI:

Klasifikasi	Deskripsi
`jeg-config`	Ubah nilai dalam file Jupyter Enterpris e Gateway`jupyter_enterprise _gateway_config.py` .
`jupyter-kernel-overrides`	Ubah nilai untuk Gambar Kernel di file Spesifikasi Kernel Jupyter.

Klasifikasi konfigurasi memungkinkan Anda menyesuaikan aplikasi. Ini sering kali bersesuaian dengan file XML konfigurasi untuk aplikasi, seperti `spark-hive-site.xml`. Untuk informasi selengkapnya, lihat Mengkonfigurasi Aplikasi.

Fitur penting

Fitur-fitur berikut disertakan dengan rilis 6.14 Amazon EMR di EKS.

- Dukungan Apache Livy - Amazon EMR di EKS sekarang mendukung Apache Livy dengan. `spark-submit`

emr-6.14.0-terbaru

Catatan rilis: `emr-6.14.0-latest` saat ini menunjuk ke `emr-6.14.0-20231005`.

Wilayah: `emr-6.14.0-latest` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.14.0:latest`

emr-6.14.0-20231005

Catatan rilis: `6.14.0-20231005` dirilis pada 17 Oktober 2023. Ini adalah rilis awal Amazon EMR 6.14.0.

Wilayah: `emr-6.14.0-20231005` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.14.0:20231005`

Amazon EMR pada rilis EKS 6.13.0

Halaman ini menjelaskan fungsionalitas baru dan yang diperbarui untuk Amazon EMR yang khusus untuk EMR Amazon pada penerapan EKS. Untuk detail tentang Amazon EMR yang berjalan di Amazon EC2 dan tentang rilis Amazon EMR 6.13.0 secara umum, lihat Amazon EMR 6.13.0 di Panduan Rilis Amazon EMR.

Amazon EMR pada rilis EKS 6.13

Rilis Amazon EMR 6.13.0 berikut tersedia untuk Amazon EMR di EKS. Pilih rilis EMR-6.13.0-XXXX tertentu untuk melihat detail selengkapnya seperti tag gambar kontainer terkait.

- emr-6.13.0-terbaru
- emr-6.13.0-20230814
- emr-6.13.0-spark-rapids-latest
- emr-6.13.0-spark-rapids-20230814
- emr-6.13.0-java11-latest
- emr-6.13.0-java11-20230814
- emr-6.13.0-java17-latest
- emr-6.13.0-java17-20230814
- emr-6.13.0-java17-al2023-latest
- emr-6.13.0-java17-al2023-20230814
- emr-6.13.0-spark-rapids-java17-latest
- emr-6.13.0-spark-rapids-java17-20230814
- emr-6.13.0-spark-rapids-java17-al2023-latest

- emr-6.13.0-spark-rapids-java17-al2023-20230814
- notebook-spark/emr-6.13.0-latest
- notebook-spark/emr-6.13.0-20230814
- notebook-spark/emr-6.13.0-spark-rapids-latest
- notebook-spark/emr-6.13.0-spark-rapids-20230814
- notebook-spark/emr-6.13.0-java11-latest
- notebook-spark/emr-6.13.0-java11-20230814
- notebook-spark/emr-6.13.0-java17-latest
- notebook-spark/emr-6.13.0-java17-20230814
- notebook-spark/emr-6.13.0-java17-al2023-latest
- notebook-spark/emr-6.13.0-java17-al2023-20230814
- notebook-python/emr-6.13.0-latest
- notebook-python/emr-6.13.0-20230814
- notebook-python/emr-6.13.0-spark-rapids-latest
- notebook-python/emr-6.13.0-spark-rapids-20230814
- notebook-python/emr-6.13.0-java11-latest
- notebook-python/emr-6.13.0-java11-20230814
- notebook-python/emr-6.13.0-java17-latest
- notebook-python/emr-6.13.0-java17-20230814
- notebook-python/emr-6.13.0-java17-al2023-latest
- notebook-python/emr-6.13.0-java17-al2023-20230814

Catatan perilisan

Catatan rilis untuk Amazon EMR di EKS 6.13.0

- Aplikasi yang didukung - AWS SDK for Java 1.12.513, Apache Spark 3.4.1-amzn-0, Apache Hudi 0.13.1-amzn-0, Apache Iceberg 1.3.0-amzn-0, Delta 2.4.0, Apache Spark RAPIDS 23.06.0-amzn-1, Jupyter Enterprise Gateway 2.6.0.amzn
- Komponen yang didukung - `aws-sagemaker-spark-sdkemr-ddb`,`emr-goodies`,,`emr-s3-select`,`emrfs`,`hadoop-client`,`hudi`,`hudi-spark`,`iceberg`,`spark-kubernetes`.
- Klasifikasi konfigurasi yang didukung

Untuk digunakan dengan StartJobRundan CreateManagedEndpointAPI:

Klasifikasi	Deskripsi
`core-site`	Ubah nilai dalam file `core-site.xml` Hadoop.
`emrfs-site`	Ubah pengaturan EMRFS.
`spark-metrics`	Ubah nilai dalam file `metrics.properties` Spark.
`spark-defaults`	Ubah nilai dalam file `spark-defaults.conf` Spark.
`spark-env`	Ubah nilai di lingkungan Spark.
`spark-hive-site`	Ubah nilai dalam file `hive-site.xml` Spark.
`spark-log4j2`	Ubah nilai dalam file `log4j2.properties` Spark.
`emr-job-submitter`	Konfigurasi untuk pod pengirim pekerjaan.

Untuk digunakan secara khusus dengan CreateManagedEndpointAPI:

Klasifikasi	Deskripsi
`jeg-config`	Ubah nilai dalam file Jupyter Enterprise Gateway`jupyter_enterprise_gateway_config.py` .
`jupyter-kernel-overrides`	Ubah nilai untuk Gambar Kernel di file Spesifikasi Kernel Jupyter.

Klasifikasi konfigurasi memungkinkan Anda menyesuaikan aplikasi. Ini sering kali bersesuaian dengan file XML konfigurasi untuk aplikasi, seperti `spark-hive-site.xml`. Untuk informasi selengkapnya, lihat Mengkonfigurasi Aplikasi.

Fitur penting

Fitur-fitur berikut disertakan dengan rilis 6.13 Amazon EMR di EKS.

- Amazon Linux 2023 - Dengan Amazon EMR di EKS 6.13 dan lebih tinggi, Anda dapat meluncurkan Spark dengan AL2023 sebagai sistem operasi bersama dengan runtime Java 17. Untuk melakukan ini, gunakan label rilis `al2023` dengan namanya. Sebagai contoh: `emr-6.13.0-java17-al2023-latest`. Kami menyarankan Anda memvalidasi dan menjalankan pengujian kinerja sebelum memindahkan beban kerja produksi ke AL2023 dan Java 17.
- Amazon EMR di EKS dengan Apache Flink (pratinjau publik) - Amazon EMR di EKS merilis 6.13 dan dukungan yang lebih tinggi Apache Flink, tersedia di pratinjau publik. Dengan peluncuran ini, Anda dapat menjalankan aplikasi berbasis Apache Flink Anda bersama dengan jenis aplikasi lain di cluster Amazon EKS yang sama. Ini membantu meningkatkan pemanfaatan sumber daya dan menyederhanakan manajemen infrastruktur. Jika Anda sudah menjalankan kerangka kerja data besar di Amazon EKS, Anda sekarang dapat membiarkan Amazon EMR mengotomatiskan penyediaan dan manajemen Anda.

emr-6.13.0-terbaru

Catatan rilis: `emr-6.13.0-latest` saat ini menunjuk ke `emr-6.13.0-20230814`.

Wilayah: `emr-6.13.0-latest` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.13.0:latest`

emr-6.13.0-20230814

Catatan rilis: `6.13.0-20230814` dirilis pada 7 September 2023. Ini adalah rilis awal Amazon EMR 6.13.0.

Wilayah: `emr-6.13.0-20230814` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.13.0:20230814`

Amazon EMR pada rilis EKS 6.12.0

Halaman ini menjelaskan fungsionalitas baru dan yang diperbarui untuk Amazon EMR yang khusus untuk EMR Amazon pada penerapan EKS. Untuk detail tentang Amazon EMR yang berjalan di Amazon EC2 dan tentang rilis Amazon EMR 6.12.0 secara umum, lihat Amazon EMR 6.12.0 di Panduan Rilis Amazon EMR.

Amazon EMR pada rilis EKS 6.12

Rilis Amazon EMR 6.12.0 berikut tersedia untuk Amazon EMR di EKS. Pilih rilis EMR-6.12.0-XXXX tertentu untuk melihat detail selengkapnya seperti tag gambar kontainer terkait.

- emr-6.12.0-terbaru
- emr-6.12.0-20230701
- emr-6.12.0- spark-rapids-latest
- emr-6.12.0-spark-cepat-20230701
- emr-6.12.0-java11-terbaru
- emr-6.12.0-java11-20230701
- emr-6.12.0-java17-terbaru
- emr-6.12.0-java17-20230701
- emr-6.12.0- 17-terbaru spark-rapids-java
- emr-6.12.0- 17-20230701 spark-rapids-java
- notebook-spark/emr-6.12.0-terbaru
- notebook-spark/emr-6.12.0-20230701
- notebook-spark/emr-6.12.0- spark-rapids-latest
- notebook-spark/emr-6.12.0-spark-rapids-20230701
- notebook-python/emr-6.12.0-terbaru
- notebook-python/emr-6.12.0-20230701
- notebook-python/emr-6.12.0- spark-rapids-latest
- notebook-python/emr-6.12.0-spark-rapids-20230701

Catatan perilisan

Catatan rilis untuk Amazon EMR di EKS 6.12.0

- Aplikasi yang didukung - AWS SDK for Java 1.12.490, Apache Spark 3.4.0-amzn-0, Apache Hudi 0.13.1-amzn-0, Apache Iceberg 1.3.0-amzn-0, Delta 2.4.0, Apache Spark RAPIDS 23.06.0-amzn-0, Jupyter Enterprise Gateway 2.6.0
- Komponen yang didukung - `aws-sagemaker-spark-sdkemr-ddb`,`emr-goodies`,,`emr-s3-select`,`emrfs`,`hadoop-client`,`hudi`,`hudi-spark`,`iceberg`,`spark-kubernetes`.
- Klasifikasi konfigurasi yang didukung

  Untuk digunakan dengan StartJobRundan CreateManagedEndpointAPI:

Klasifikasi	Deskripsi
`core-site`	Ubah nilai dalam file `core-site.xml` Hadoop.
`emrfs-site`	Ubah pengaturan EMRFS.
`spark-metrics`	Ubah nilai dalam file `metrics.properties` Spark.
`spark-defaults`	Ubah nilai dalam file `spark-defaults.conf` Spark.
`spark-env`	Ubah nilai di lingkungan Spark.
`spark-hive-site`	Ubah nilai dalam file `hive-site.xml` Spark.
`spark-log4j2`	Ubah nilai dalam file `log4j2.properties` Spark.
`emr-job-submitter`	Konfigurasi untuk pod pengirim pekerjaan.

  Untuk digunakan secara khusus dengan CreateManagedEndpointAPI:

Klasifikasi	Deskripsi
`jeg-config`	Ubah nilai dalam file Jupyter Enterprise Gatewayjupyter_enterprise_gateway_config.py .
`jupyter-kernel-overrides`	Ubah nilai untuk Gambar Kernel di file Spesifikasi Kernel Jupyter.

Klasifikasi konfigurasi memungkinkan Anda menyesuaikan aplikasi. Ini sering kali bersesuaian dengan file XML konfigurasi untuk aplikasi, seperti `spark-hive-site.xml`. Untuk informasi selengkapnya, lihat Mengkonfigurasi Aplikasi.

Fitur penting

Fitur-fitur berikut disertakan dengan rilis 6.12 Amazon EMR di EKS.

- Java 17 - Dengan Amazon EMR di EKS 6.12 dan lebih tinggi, Anda dapat meluncurkan Spark dengan runtime Java 17. Untuk melakukan ini, berikan `emr-6.12.0-java17-latest` sebagai label rilis. Kami menyarankan Anda memvalidasi dan menjalankan pengujian kinerja sebelum memindahkan beban kerja produksi dari versi sebelumnya dari gambar Java ke gambar Java 17.

emr-6.12.0-terbaru

Catatan rilis: `emr-6.12.0-latest` saat ini menunjuk ke `emr-6.12.0-20230701`.

Wilayah: `emr-6.12.0-latest` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.12.0:latest`

emr-6.12.0-20230701

Catatan rilis: `6.12.0-20230701` dirilis pada 1 Juli 2023. Ini adalah rilis awal Amazon EMR 6.12.0.

Wilayah: `emr-6.12.0-20230701` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.12.0:20230701`

Amazon EMR pada rilis EKS 6.11.0

Halaman ini menjelaskan fungsionalitas baru dan yang diperbarui untuk Amazon EMR yang khusus untuk EMR Amazon pada penerapan EKS. Untuk detail tentang Amazon EMR yang berjalan di Amazon EC2 dan tentang rilis Amazon EMR 6.11.0 secara umum, lihat Amazon EMR 6.11.0 di Panduan Rilis Amazon EMR.

Amazon EMR pada rilis EKS 6.11

Rilis Amazon EMR 6.11.0 berikut tersedia untuk Amazon EMR di EKS. Pilih rilis EMR-6.11.0-XXXX tertentu untuk melihat detail selengkapnya seperti tag gambar kontainer terkait.

- emr-6.11.0-terbaru
- emr-6.11.0-20230509

- emr-6.11.0- spark-rapids-latest
- emr-6.11.0-spark-cepat-20230509
- emr-6.11.0-java11-terbaru
- emr-6.11.0-java11-20230509
- notebook-spark/emr-6.11.0-terbaru
- notebook-spark/emr-6.11.0-20230509
- notebook-python/emr-6.11.0-terbaru
- notebook-python/emr-6.11.0-20230509

Catatan perilisan

Catatan rilis untuk Amazon EMR di EKS 6.11.0

- Aplikasi yang didukung - AWS SDK for Java 1.12.446, Apache Spark 3.3.2-amzn-0, Apache Hudi 0.13.0-amzn-0, Apache Iceberg 1.2.0-amzn-0, Delta 2.2.0, Apache Spark RAPIDS 23.02.0-amzn-0, Jupyter Enterprise Gateway 2.6.0
- Komponen yang didukung - `aws-sagemaker-spark-sdkemr-ddb`,`emr-goodies`,,`emr-s3-select`,`emrfs`,`hadoop-client`,`hudi`,`hudi-spark`,`iceberg`,`spark-kubernetes`.

- Klasifikasi konfigurasi yang didukung

  Untuk digunakan dengan StartJobRundan CreateManagedEndpointAPI:

Klasifikasi	Deskripsi
`core-site`	Ubah nilai dalam file `core-site.xml` Hadoop.
`emrfs-site`	Ubah pengaturan EMRFS.
`spark-metrics`	Ubah nilai dalam file `metrics.properties` Spark.
`spark-defaults`	Ubah nilai dalam file `spark-defaults.conf` Spark.
`spark-env`	Ubah nilai di lingkungan Spark.
`spark-hive-site`	Ubah nilai dalam file `hive-site.xml` Spark.
`spark-log4j`	Ubah nilai dalam file `log4j.properties` Spark.

  Untuk digunakan secara khusus dengan CreateManagedEndpointAPI:

Klasifikasi	Deskripsi
`jeg-config`	Ubah nilai dalam file Jupyter Enterprise Gateway`jupyter_enterprise_gateway_config.py` .
`jupyter-kernel-overrides`	Ubah nilai untuk Gambar Kernel di file Spesifikasi Kernel Jupyter.

Klasifikasi konfigurasi memungkinkan Anda menyesuaikan aplikasi. Ini sering kali bersesuaian dengan file XML konfigurasi untuk aplikasi, seperti `spark-hive-site.xml`. Untuk informasi selengkapnya, lihat Mengkonfigurasi Aplikasi.

Fitur penting

Fitur-fitur berikut disertakan dengan rilis 6.11 Amazon EMR di EKS.

- Amazon EMR pada gambar dasar EKS di Galeri Publik Amazon ECR — Jika Anda menggunakan kemampuan gambar khusus, gambar dasar kami menyediakan toples, konfigurasi, dan pustaka penting untuk berinteraksi dengan Amazon EMR di EKS. Anda sekarang dapat menemukan gambar dasar di Galeri Publik Amazon ECR.
- Rotasi log kontainer percikan - Amazon EMR di EKS 6.11 mendukung rotasi log kontainer Spark. Anda dapat mengaktifkan kemampuan dengan `containerLogRotationConfiguration` dalam `MonitoringConfiguration` pengoperasian `StartJobRun` API. Anda dapat mengonfigurasi `rotationSize` dan `maxFilestoKeep` menentukan jumlah dan ukuran file log yang Anda inginkan Amazon EMR di EKS untuk disimpan di driver Spark dan pod pelaksana. Untuk informasi selengkapnya, lihat Menggunakan rotasi log kontainer Spark.
- Dukungan gunung berapi di operator Spark dan spark-submit — Amazon EMR di EKS 6.11 mendukung menjalankan pekerjaan Spark dengan Volcano sebagai penjadwal kustom Kubernetes di operator Spark dan spark-submit. Anda dapat menggunakan fitur seperti penjadwalan geng, manajemen antrian, preemption, dan penjadwalan berbagi adil untuk mencapai throughput penjadwalan yang tinggi dan kapasitas yang dioptimalkan. Untuk informasi selengkapnya, lihat Menggunakan Volcano sebagai penjadwal khusus untuk Apache Spark di Amazon EMR di EKS.

emr-6.11.0-terbaru

Catatan rilis: `emr-6.11.0-latest` saat ini menunjuk ke `emr-20230509`.

Wilayah: `emr-6.11.0-latest` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.11.0:latest`

emr-6.11.0-20230509

Catatan rilis: `6.11.0-20230509` dirilis pada 9 Mei 2023. Ini adalah rilis awal Amazon EMR 6.11.0.

Wilayah: `emr-6.11.0-20230509` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.11.0:20230509`

Amazon EMR pada rilis EKS 6.10.0

Rilis Amazon EMR 6.10.0 berikut tersedia untuk Amazon EMR di EKS. Pilih rilis EMR-6.10.0-XXXX tertentu untuk melihat detail selengkapnya seperti tag gambar kontainer terkait.

- emr-6.10.0-terbaru
- emr-6.10.0-20230624
- emr-6.10.0-20230421
- emr-6.10.0-20230403
- emr-6.10.0-20230220
- emr-6.10.0- spark-rapids-latest
- emr-6.10.0-spark-cepat-20230624
- emr-6.10.0-spark-cepat-20230220
- emr-6.10.0-java11-terbaru
- emr-6.10.0-java11-20230624
- emr-6.10.0-java11-20230220
- notebook-spark/emr-6.10.0-terbaru
- notebook-spark/emr-6.10.0-20230624
- notebook-spark/emr-6.10.0-20230220
- notebook-python/emr-6.10.0-terbaru
- notebook-python/emr-6.10.0-20230624
- notebook-python/emr-6.10.0-20230220

Catatan rilis untuk Amazon EMR 6.10.0

- Aplikasi yang didukung - AWS SDK for Java 1.12.397, Spark 3.3.1-amzn-0, Hudi 0.12.2-amzn-0, Iceberg 1.1.0-amzn-0, Delta 2.2.0.
- Komponen yang didukung - `aws-sagemaker-spark-sdkemr-ddb`,`emr-goodies`,,`emr-s3-select`,`emrfs`,`hadoop-client`,`hudi`,`hudi-spark`,`iceberg`,`spark-kubernetes`.
- Klasifikasi konfigurasi yang didukung:

  Untuk digunakan dengan StartJobRundan CreateManagedEndpointAPI:

Klasifikasi	Deskripsi
`core-site`	Ubah nilai dalam file Hadoop. `core-site.xml`
`emrfs-site`	Ubah pengaturan EMRFS.
`spark-metrics`	Ubah nilai dalam `metrics.properties` file Spark.
`spark-defaults`	Ubah nilai dalam `spark-defaults.conf` file Spark.
`spark-env`	Ubah nilai di lingkungan Spark.
`spark-hive-site`	Ubah nilai dalam `hive-site.xml` file Spark.
`spark-log4j`	Ubah nilai dalam `log4j.properties` file Spark.

  Untuk digunakan secara khusus dengan CreateManagedEndpointAPI:

Klasifikasi	Deskripsi
`jeg-config`	Ubah nilai dalam file Jupyter Enterprise Gateway`jupyter_enterprise_gateway_config.py` .

Klasifikasi	Deskripsi
`jupyter-kernel-overrides`	Ubah nilai untuk Gambar Kernel di file Spesifikasi Kernel Jupyter.

Klasifikasi konfigurasi memungkinkan Anda menyesuaikan aplikasi. Ini sering kali bersesuaian dengan file XML konfigurasi untuk aplikasi, seperti `spark-hive-site.xml`. Untuk informasi selengkapnya, lihat Mengkonfigurasi Aplikasi.

Fitur penting

- Operator Spark - Dengan Amazon EMR di EKS 6.10.0 dan yang lebih tinggi, Anda dapat menggunakan operator Kubernetes untuk Apache Spark, atau operator Spark, untuk menyebarkan dan mengelola aplikasi Spark dengan runtime rilis Amazon EMR di kluster Amazon EKS Anda sendiri. Untuk informasi selengkapnya, lihat Menjalankan pekerjaan Spark dengan operator Spark.
- Java 11 - Dengan Amazon EMR di EKS 6.10 dan yang lebih tinggi, Anda dapat meluncurkan Spark dengan runtime Java 11. Untuk melakukan ini, berikan `emr-6.10.0-java11-latest` sebagai label rilis. Sebaiknya Anda memvalidasi dan menjalankan pengujian kinerja sebelum memindahkan beban kerja produksi dari gambar Java 8 ke gambar Java 11.
- Untuk integrasi Amazon Redshift untuk Apache Spark, Amazon EMR di EKS 6.10.0 menghapus dependensi`minimal-json.jar`, dan secara otomatis menambahkan jar terkait yang `spark-redshift` diperlukan ke jalur kelas pelaksana untuk Spark:,, dan. `spark-redshift.jar` `spark-avro.jar` `RedshiftJDBC.jar`

Perubahan

- EMRFS S3 committer yang dioptimalkan sekarang diaktifkan secara default untuk parket, ORC, dan format berbasis teks (termasuk CSV dan JSON).

emr-6.10.0-terbaru

Catatan rilis: `emr-6.10.0-latest` saat ini menunjuk ke `emr-6.10.0-20230624`.

Wilayah: `emr-6.10.0-latest` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.10.0:latest`

emr-6.10.0-20230624

Catatan rilis: `6.10.0-20230624` dirilis pada 7 Juli 2023. Dibandingkan dengan rilis sebelumnya, versi ini telah diperbarui dengan paket Amazon Linux yang baru diperbarui dan perbaikan kritis.

Wilayah: `emr-6.10.0-20230624` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.10.0:20230624`

emr-6.10.0-20230421

Catatan rilis: `6.10.0-20230421` dirilis pada 28 April 2023. Dibandingkan dengan rilis sebelumnya, versi ini telah diperbarui dengan paket Amazon Linux yang baru diperbarui dan perbaikan kritis.

Wilayah: `emr-6.10.0-20230421` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.10.0:20230421`

emr-6.10.0-20230403

Catatan rilis: `6.10.0-20230403` dirilis pada 12 April 2023. Dibandingkan dengan rilis sebelumnya, versi ini telah diperbarui dengan paket Amazon Linux yang baru diperbarui dan perbaikan kritis.

Wilayah: `emr-6.10.0-20230403` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.10.0:20230403`

emr-6.10.0-20230220

Catatan rilis: `emr-6.10.0-20230220` dirilis pada 20 Februari 2023. Ini adalah rilis awal Amazon EMR 6.10.0.

Wilayah: `emr-6.10.0-20230220` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.10.0:20230220`

Amazon EMR pada rilis EKS 6.9.0

Rilis Amazon EMR 6.9.0 berikut tersedia untuk Amazon EMR di EKS. Pilih rilis EMR-6.9.0-XXXX tertentu untuk melihat detail selengkapnya seperti tag gambar kontainer terkait.

- emr-6.9.0-terbaru
- emr-6.9.0-20230912
- emr-6.9.0-20230624
- emr-6.9.0-20221108
- emr-6.9.0- spark-rapids-latest
- emr-6.9.0-spark-cepat-20230624
- emr-6.9.0-spark-cepat-20221108
- notebook-spark/emr-6.9.0-terbaru
- notebook-spark/emr-6.9.0-20230624
- notebook-spark/emr-6.9.0-20221108
- notebook-python/emr-6.9.0-terbaru
- notebook-python/emr-6.9.0-20230624
- notebook-python/emr-6.9.0-20221108

Catatan rilis untuk Amazon EMR 6.9.0

- Aplikasi yang didukung - AWS SDK for Java 1.12.331, Spark 3.3.0-amzn-1, Hudi 0.12.1-amzn-0, Iceberg 0.14.1-amzn-0, Delta 2.1.0.
- Komponen yang didukung - `aws-sagemaker-spark-sdkemr-ddb`,`emr-goodies`,,`emr-s3-select`,`emrfs`,`hadoop-client`,`hudi`,`hudi-spark`,`iceberg`,`spark-kubernetes`.
- Klasifikasi konfigurasi yang didukung:

  Untuk digunakan dengan StartJobRundan CreateManagedEndpointAPI:

Klasifikasi	Deskripsi
`core-site`	Ubah nilai dalam file core-site.xml Hadoop.
`emrfs-site`	Ubah pengaturan EMRFS.

Klasifikasi	Deskripsi
`spark-metrics`	Ubah nilai dalam file metrics.properties Spark.
`spark-defaults`	Ubah nilai dalam file spark-defaults.conf Spark.
`spark-env`	Ubah nilai di lingkungan Spark.
`spark-hive-site`	Ubah nilai dalam file hive-site.xml Spark.
`spark-log4j`	Ubah nilai dalam file log4j.properties Spark.

Untuk digunakan secara khusus dengan CreateManagedEndpointAPI:

Klasifikasi	Deskripsi
`jeg-config`	Ubah nilai dalam file Jupyter Enterpris e Gateway`jupyter_enterprise _gateway_config.py` .
`jupyter-kernel-overrides`	Ubah nilai untuk Gambar Kernel di file Spesifikasi Kernel Jupyter.

Klasifikasi konfigurasi memungkinkan Anda menyesuaikan aplikasi. Ini sering kali bersesuaian dengan file XML konfigurasi untuk aplikasi, seperti `spark-hive-site.xml`. Untuk informasi selengkapnya, lihat Mengkonfigurasi Aplikasi.

Fitur penting

- Akselerator Nvidia RAPIDS untuk Apache Spark - Amazon EMR di EKS untuk mempercepat Spark menggunakan tipe instans unit pemrosesan grafis (GPU) EC2. Untuk menggunakan gambar Spark dengan RAPIDS Accelerator, tentukan label rilis sebagai emr-6.9.0-. spark-rapids-latest Kunjungi halaman dokumentasi untuk mempelajari lebih lanjut.
- Konektor Spark-Redshift - Integrasi Amazon Redshift untuk Apache Spark disertakan dalam rilis Amazon EMR 6.9.0 dan yang lebih baru. Sebelumnya alat open-source, integrasi asli adalah

konektor Spark yang dapat Anda gunakan untuk membangun aplikasi Apache Spark yang membaca dan menulis ke data di Amazon Redshift dan Amazon Redshift Serverless. Untuk informasi selengkapnya, lihat Menggunakan integrasi Amazon Redshift untuk Apache Spark di Amazon EMR di EKS.

- Delta Lake - Delta Lake adalah format penyimpanan sumber terbuka yang memungkinkan pembangunan danau data dengan konsistensi transaksional, definisi kumpulan data yang konsisten, perubahan evolusi skema, dan dukungan mutasi data. Kunjungi Menggunakan Danau Delta untuk mempelajari lebih lanjut.
- Ubah PySpark parameter - Titik akhir interaktif sekarang mendukung modifikasi parameter Spark yang terkait dengan PySpark sesi di Notebook EMR Studio Jupyter. Kunjungi Memodifikasi parameter PySpark sesi untuk mempelajari lebih lanjut.

Masalah terselesaikan

- Saat Anda menggunakan konektor DynamoDB dengan Spark di Amazon EMR versi 6.6.0, 6.7.0, dan 6.8.0, semua pembacaan dari tabel Anda mengembalikan hasil kosong, meskipun pemisahan input mereferensikan data yang tidak kosong. Amazon EMR rilis 6.9.0 memperbaiki masalah ini.
- Amazon EMR di EKS 6.8.0 salah mengisi hash build dalam metadata file Parquet yang dihasilkan menggunakan Apache Spark. Masalah ini dapat menyebabkan alat yang mengurai string versi metadata dari file Parket yang dihasilkan oleh Amazon EMR di EKS 6.8.0 gagal.

Masalah yang diketahui

- Jika Anda menggunakan integrasi Amazon Redshift untuk Apache Spark dan memiliki waktu, jadwal, stempel waktu, atau timestamptz dengan presisi mikrodetik dalam format Parket, konektor membulatkan nilai waktu ke nilai milidetik terdekat. Sebagai solusinya, gunakan parameter format pembongkaran teks. `unload_s3_format`

emr-6.9.0-terbaru

Catatan rilis: `emr-6.9.0-latest` saat ini menunjuk ke `emr-6.9.0-20230912`.

Wilayah: `emr-6.9.0-latest` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.9.0:latest`

emr-6.9.0-20230912

Catatan rilis:`emr-6.9.0-20230912`.

Wilayah: `emr-6.9.0-20230912` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.9.0:20230912`

emr-6.9.0-20230624

Catatan rilis: `emr-6.9.0-20230624` dirilis pada 7 Juli 2023.

Wilayah: `emr-6.9.0-20230624` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.9.0:20230624`

emr-6.9.0-20221108

Catatan rilis: `emr-6.9.0-20221108` dirilis pada 08 Desember 2022. Ini adalah rilis awal Amazon EMR 6.9.0.

Wilayah: `emr-6.9.0-20221108` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.9.0:20221108`

Amazon EMR pada rilis EKS 6.8.0

Rilis Amazon EMR 6.8.0 berikut tersedia untuk Amazon EMR di EKS. Pilih rilis EMR-6.8.0-XXXX tertentu untuk melihat detail selengkapnya seperti tag gambar kontainer terkait.

- emr-6.8.0-terbaru
- emr-6.8.0-20230624
- emr-6.8.0-20221219
- emr-6.8.0-20220802

Catatan rilis untuk Amazon EMR 6.8.0

- Aplikasi yang didukung - AWS SDK for Java 1.12.170, Spark 3.3.0-amzn-0, Hudi 0.11.1-amzn-0, Iceberg 0.14.0-amzn-0.
- Komponen yang didukung - `aws-sagemaker-spark-sdkemr-ddb`,`emr-goodies`,,`emr-s3-select`,`emrfs`,`hadoop-client`,`hudi`,`hudi-spark`,`iceberg`,`spark-kubernetes`.
- Klasifikasi konfigurasi yang didukung:

Klasifikasi	Deskripsi
`core-site`	Ubah nilai dalam file core-site.xml Hadoop.
`emrfs-site`	Ubah pengaturan EMRFS.
`spark-metrics`	Ubah nilai dalam file metrics.properties Spark.
`spark-defaults`	Ubah nilai dalam file spark-defaults.conf Spark.
`spark-env`	Ubah nilai di lingkungan Spark.
`spark-hive-site`	Ubah nilai dalam file hive-site.xml Spark.
`spark-log4j`	Ubah nilai dalam file log4j.properties Spark.

Klasifikasi konfigurasi memungkinkan Anda menyesuaikan aplikasi. Ini sering kali bersesuaian dengan file XML konfigurasi untuk aplikasi, seperti `spark-hive-site.xml`. Untuk informasi selengkapnya, lihat Mengkonfigurasi Aplikasi.

Fitur penting

- Spark3.3.0 - Amazon EMR di EKS 6.8 menyertakan Spark 3.3.0, yang mendukung penggunaan label pemilih node terpisah untuk pod pelaksana driver Spark. Label baru ini memungkinkan Anda untuk menentukan tipe node untuk driver dan pod eksekutor secara terpisah di StartJobRun API, tanpa menggunakan templat pod.
  - Properti pemilih node driver: spark.kubernetes.driver.node.selector. [LabelKey]
  - Properti pemilih node pelaksana: spark.kubernetes.executor.node.selector. [LabelKey]

- Pesan kegagalan pekerjaan yang disempurnakan - Rilis ini memperkenalkan konfigurasi `spark.stage.extraDetailsOnFetchFailures.enabled` dan `spark.stage.extraDetailsOnFetchFailures.maxFailuresToInclude` melacak kegagalan tugas karena kode pengguna. Detail ini akan digunakan untuk menyempurnakan pesan kegagalan yang ditampilkan di log driver saat tahap dibatalkan karena kegagalan pengambilan acak.

Nama properti	Nilai default	Arti	Sejak versi
`spark.stage.extraDetailsOnFetchFailures.enabled`	salah	Jika disetel ke`true`, properti ini digunakan untuk menyempurnakan pesan kegagalan pekerjaan yang ditampilkan di log driver saat tahap dibatalkan karena Kegagalan Pengambilan Aduk. Secara default, 5 kegagalan tugas terakhir yang disebabkan oleh kode pengguna dilacak, dan pesan kesalahan kegagalan ditambahkan di Log Driver. Untuk meningkatkan jumlah kegagalan tugas dengan pengecualian pengguna untuk dilacak, lihat konfigurasi`spark.stage.extraDetailsOnFetchFailures.maxFa`	emr-6.8

Nama properti	Nilai default	Arti	Sejak versi
		`iluresToI nclude` .	
`spark.sta ge.extraD etailsOnF etchFailu res.maxFa iluresToI nclude`	5	Jumlah kegagalan tugas untuk melacak per tahap dan upaya. Properti ini digunakan untuk menyempur nakan pesan kegagalan pekerjaan dengan pengecual ian pengguna yang ditampilkan di log driver saat tahap dibatalkan karena Kegagalan Pengambilan Aduk. Properti ini hanya berfungsi jika Config spark.stage. extraDetailsOnFetc hFailures.enabled disetel ke true.	emr-6.8

Untuk informasi selengkapnya lihat dokumentasi konfigurasi Apache Spark.

Masalah yang diketahui

- Amazon EMR di EKS 6.8.0 salah mengisi hash build dalam metadata file Parquet yang dihasilkan menggunakan Apache Spark. Masalah ini dapat menyebabkan alat yang mengurai string versi metadata dari file Parket yang dihasilkan oleh Amazon EMR di EKS 6.8.0 gagal. Pelanggan yang mengurai string versi dari metadata Parket dan bergantung pada hash build harus beralih ke versi EMR Amazon yang berbeda dan menulis ulang file.

Masalah terselesaikan

- Kemampuan Kernel interupsi untuk kernel PySpark - Beban kerja interaktif yang sedang berlangsung yang dipicu oleh mengeksekusi sel di notebook dapat dihentikan dengan menggunakan kemampuan tersebut. `Interrupt Kernel` Perbaikan telah diperkenalkan sehingga fungsi ini berfungsi untuk kernel PySpark. Ini juga tersedia di open source di Changes untuk menangani interupsi untuk PySpark Kubernetes Kernel #1115.

emr-6.8.0-terbaru

Catatan rilis: `emr-6.8.0-latest` saat ini menunjuk ke `emr-6.8.0-20230624`.

Wilayah: `emr-6.8.0-latest` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.8.0:latest`

emr-6.8.0-20230624

Catatan rilis: `emr-6.8.0-20230624` dirilis pada 7 Juli 2023. Dibandingkan dengan versi sebelumnya, versi ini telah diperbarui dengan Paket Amazon Linux yang baru diperbarui dan perbaikan kritis.

Wilayah: `emr-6.8.0-20230624` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.8.0:20230624`

emr-6.8.0-20221219

Catatan rilis: `emr-6.8.0-20221219` dirilis pada 19 Jan 2023. Dibandingkan dengan versi sebelumnya, versi ini telah diperbarui dengan Paket Amazon Linux yang baru diperbarui dan perbaikan kritis.

Wilayah: `emr-6.8.0-20221219` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.8.0:20221219`

emr-6.8.0-20220802

Catatan rilis: `emr-6.8.0-20220802` dirilis pada 27 Sep 2022. Ini adalah rilis awal Amazon EMR 6.8.0.

Wilayah: `emr-6.8.0-20220802` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.8.0:20220802`

Amazon EMR pada rilis EKS 6.7.0

Rilis Amazon EMR 6.7.0 berikut tersedia untuk Amazon EMR di EKS. Pilih rilis EMR-6.7.0-XXXX tertentu untuk melihat detail selengkapnya seperti tag gambar kontainer terkait.

- emr-6.7.0-terbaru
- emr-6.7.0-20230624
- emr-6.7.0-20221219
- emr-6.7.0-20220630

Catatan rilis untuk Amazon EMR 6.7.0

- Aplikasi yang didukung - Spark 3.2.1-amzn-0, Jupyter Enterprise Gateway 2.6, Hudi 0.11-amzn-0, Iceberg 0.13.1.
- Komponen yang didukung - `aws-hm-client` (Konektor Glue), `aws-sagemaker-spark-sdk`, `emr-s3-select`, `emrfs`, `emr-ddb`, `hudi-spark`.
- Dengan upgrade ke JEG 2.6, manajemen kernel sekarang asinkron, yang berarti bahwa JEG tidak memblokir transaksi ketika peluncuran kernel sedang berlangsung. Ini sangat meningkatkan pengalaman pengguna dengan memberikan yang berikut:
  - kemampuan untuk menjalankan perintah di notebook yang sedang berjalan saat peluncuran kernel lainnya sedang berlangsung
  - kemampuan untuk meluncurkan beberapa kernel secara bersamaan tanpa memengaruhi kernel yang sudah berjalan
- Klasifikasi konfigurasi yang didukung:

Klasifikasi	Deskripsi
`core-site`	Ubah nilai dalam file Hadoop`core-site.xml` .
`emrfs-site`	Ubah pengaturan EMRFS.
`spark-metrics`	Ubah nilai dalam `metrics.properties` file Spark.
`spark-defaults`	Ubah nilai dalam `spark-defaults.conf` file Spark.
`spark-env`	Ubah nilai di lingkungan Spark.
`spark-hive-site`	Ubah nilai dalam `hive-site.xml` file Spark.
`spark-log4j`	Ubah nilai dalam `log4j.properties` file Spark.

Klasifikasi konfigurasi memungkinkan Anda menyesuaikan aplikasi. Ini sering kali bersesuaian dengan file XML konfigurasi untuk aplikasi, seperti `spark-hive-site.xml`. Untuk informasi lebih lanjut, lihat Mengonfigurasi Aplikasi.

Masalah terselesaikan

- Amazon EMR di EKS 6.7 memperbaiki masalah di 6.6 saat menggunakan fungsionalitas templat pod Apache Spark dengan titik akhir interaktif. Masalah ini hadir di Amazon EMR pada rilis EKS 6.4, 6.5 dan 6.6. Anda sekarang dapat menggunakan templat pod untuk menentukan bagaimana driver Spark dan pod pelaksana Anda dimulai saat menggunakan titik akhir interaktif untuk menjalankan analitik interaktif.
- Di Amazon EMR sebelumnya pada rilis EKS, Jupyter Enterprise Gateway akan memblokir transaksi saat peluncuran kernel sedang berlangsung, dan ini menghambat pelaksanaan sesi notebook yang sedang berjalan. Anda sekarang dapat menjalankan perintah di notebook yang sedang berjalan saat peluncuran kernel lainnya sedang berlangsung. Anda juga dapat

meluncurkan beberapa kernel secara bersamaan tanpa risiko kehilangan konektivitas ke kernel yang sudah berjalan.

emr-6.7.0-terbaru

Catatan rilis: `emr-6.7.0-latest` saat ini menunjuk ke `emr-6.7.0-20230624`.

Wilayah: `emr-6.7.0-latest` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.7.0:latest`

emr-6.7.0-20230624

Catatan rilis: `emr-6.7.0-20230624` dirilis pada 7 Juli 2023. Dibandingkan dengan versi sebelumnya, versi ini telah diperbarui dengan Paket Amazon Linux yang baru diperbarui dan perbaikan kritis.

Wilayah: `emr-6.7.0-20230624` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.7.0:20230624`

emr-6.7.0-20221219

Catatan rilis: `emr-6.7.0-20221219` dirilis pada 19 Januari 2023. Dibandingkan dengan versi sebelumnya, versi ini telah diperbarui dengan Paket Amazon Linux yang baru diperbarui dan perbaikan kritis.

Wilayah: `emr-6.7.0-20221219` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.7.0:20221219`

emr-6.7.0-20220630

Catatan rilis: `emr-6.7.0-20220630` dirilis pada 12 Juli 2022. Ini adalah rilis awal Amazon EMR 6.7.0.

Wilayah: `emr-6.7.0-20220630` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.7.0:20220630`

Amazon EMR pada rilis EKS 6.6.0

Rilis Amazon EMR 6.6.0 berikut tersedia untuk Amazon EMR di EKS. Pilih rilis EMR-6.6.0-XXXX tertentu untuk melihat detail selengkapnya seperti tag gambar kontainer terkait.

- emr-6.6.0-terbaru
- emr-6.6.0-20230624
- emr-6.6.0-20221219
- emr-6.6.0-20220411

Catatan rilis untuk Amazon EMR 6.6.0

- Aplikasi yang didukung - Spark 3.2.0-amzn-0, Jupyter Enterprise Gateway (titik akhir, pratinjau publik), Hudi 0.10.1-amzn-0, Iceberg 0.13.1.
- Komponen yang didukung - `aws-hm-client` (Konektor Glue), `aws-sagemaker-spark-sdk`, `emr-s3-select`, `emrfs`, `emr-ddb`, `hudi-spark`.
- Klasifikasi konfigurasi yang didukung:

Klasifikasi	Deskripsi
`core-site`	Ubah nilai dalam file core-site.xml Hadoop.
`emrfs-site`	Ubah pengaturan EMRFS.
`spark-metrics`	Ubah nilai dalam file metrics.properties Spark.
`spark-defaults`	Ubah nilai dalam file spark-defaults.conf Spark.
`spark-env`	Ubah nilai di lingkungan Spark.
`spark-hive-site`	Ubah nilai dalam file hive-site.xml Spark.

Klasifikasi	Deskripsi
`spark-log4j`	Ubah nilai dalam file log4j.properties Spark.

Klasifikasi konfigurasi memungkinkan Anda menyesuaikan aplikasi. Ini sering sesuai dengan file XHTML konfigurasi untuk aplikasi, spark-hive-site seperti.xml.xml. Untuk informasi lebih lanjut, lihat Mengonfigurasi Aplikasi.

Masalah yang diketahui

- Fungsionalitas template Spark pod dengan titik akhir interaktif tidak berfungsi di Amazon EMR pada rilis EKS 6.4, 6.5, dan 6.6.

Masalah terselesaikan

- Log endpoint interaktif diunggah ke Cloudwatch dan S3.

emr-6.6.0-terbaru

Catatan rilis: `emr-6.6.0-latest` saat ini menunjuk ke `emr-6.6.0-20230624`.

Wilayah: `emr-6.6.0-latest` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.6.0:latest`

emr-6.6.0-20230624

Catatan rilis: `emr-6.6.0-20230624` dirilis pada 27 Jan 2023. Dibandingkan dengan versi sebelumnya, versi ini telah diperbarui dengan Paket Amazon Linux yang baru diperbarui dan perbaikan kritis.

Wilayah: `emr-6.6.0-20230624` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.6.0:20230624`

emr-6.6.0-20221219

Catatan rilis: `emr-6.6.0-20221219` dirilis pada 27 Jan 2023. Dibandingkan dengan versi sebelumnya, versi ini telah diperbarui dengan Paket Amazon Linux yang baru diperbarui dan perbaikan kritis.

Wilayah: `emr-6.6.0-20221219` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.6.0:20221219`

emr-6.6.0-20220411

Catatan rilis: `emr-6.6.0-20220411` dirilis pada 20 Mei 2022. Ini adalah rilis awal Amazon EMR 6.6.0.

Wilayah: `emr-6.6.0-20220411` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.6.0:20220411`

Amazon EMR pada rilis EKS 6.5.0

Rilis Amazon EMR 6.5.0 berikut tersedia untuk Amazon EMR di EKS. Pilih rilis EMR-6.5.0-XXXX tertentu untuk melihat detail selengkapnya seperti tag gambar kontainer terkait.

- emr-6.5.0-terbaru
- emr-6.5.0-20221219
- emr-6.5.0-20220802
- emr-6.5.0-20211119

Catatan rilis untuk Amazon EMR 6.5.0

- Aplikasi yang didukung - Spark 3.1.2-amzn-1, Jupyter Enterprise Gateway (titik akhir, pratinjau publik).
- Komponen yang didukung - `aws-hm-client` (Konektor Glue), `aws-sagemaker-spark-sdk`, `emr-s3-select`, `emrfs`, `emr-ddb`, `hudi-spark`.

- Klasifikasi konfigurasi yang didukung:

Klasifikasi	Deskripsi
`core-site`	Ubah nilai dalam file core-site.xml Hadoop.
`emrfs-site`	Ubah pengaturan EMRFS.
`spark-metrics`	Ubah nilai dalam file metrics.properties Spark.
`spark-defaults`	Ubah nilai dalam file spark-defaults.conf Spark.
`spark-env`	Ubah nilai di lingkungan Spark.
`spark-hive-site`	Ubah nilai dalam file hive-site.xml Spark.
`spark-log4j`	Ubah nilai dalam file log4j.properties Spark.

  Klasifikasi konfigurasi memungkinkan Anda menyesuaikan aplikasi. Ini sering sesuai dengan file XHTML konfigurasi untuk aplikasi, spark-hive-site seperti.xml.xml. Untuk informasi lebih lanjut, lihat Mengonfigurasi Aplikasi.

Masalah yang Diketahui

- Fungsionalitas template Spark pod dengan titik akhir interaktif tidak berfungsi di Amazon EMR pada rilis EKS 6.4 dan 6.5.

emr-6.5.0-terbaru

Catatan rilis: `emr-6.5.0-latest` saat ini menunjuk ke `emr-6.5.0-20221219`.

Wilayah: `emr-6.5.0-latest` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.5.0:latest`

emr-6.5.0-20221219

Catatan rilis: `emr-6.5.0-20221219` dirilis pada 19 Jan 2023. Dibandingkan dengan versi sebelumnya, versi ini telah diperbarui dengan Paket Amazon Linux yang baru diperbarui dan perbaikan kritis.

Wilayah: `emr-6.5.0-20221219` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.5.0:20221219`

emr-6.5.0-20220802

Catatan rilis: `emr-6.5.0-20220802` dirilis pada 24 Agustus 2022. Dibandingkan dengan versi sebelumnya, versi ini telah diperbarui dengan Paket Amazon Linux yang baru diperbarui.

Wilayah: `emr-6.5.0-20220802` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.5.0:20220802`

emr-6.5.0-20211119

Catatan rilis: `emr-6.5.0-20211119` dirilis pada 20 Jan 2022. Ini adalah rilis awal Amazon EMR 6.5.0.

Wilayah: `emr-6.5.0-20211119` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.5.0:20211119`

Amazon EMR pada rilis EKS 6.4.0

Rilis Amazon EMR 6.4.0 berikut tersedia untuk Amazon EMR di EKS. Pilih rilis EMR-6.4.0-XXXX tertentu untuk melihat detail selengkapnya seperti tag gambar kontainer terkait.

- emr-6.4.0-terbaru
- emr-6.4.0-20221219
- emr-6.4.0-20210830

Catatan rilis untuk Amazon EMR 6.4.0

- Aplikasi yang didukung - Spark 3.1.2-amzn-0, Jupyter Enterprise Gateway (titik akhir, pratinjau publik).
- Komponen yang didukung - `aws-hm-client` (Konektor Glue), `aws-sagemaker-spark-sdk`, `emr-s3-select`, `emrfs`, `emr-ddb`, `hudi-spark`.
- Klasifikasi konfigurasi yang didukung:

Klasifikasi	Deskripsi
`core-site`	Ubah nilai dalam file core-site.xml Hadoop.
`emrfs-site`	Ubah pengaturan EMRFS.
`spark-metrics`	Ubah nilai dalam file metrics.properties Spark.
`spark-defaults`	Ubah nilai dalam file spark-defaults.conf Spark.
`spark-env`	Ubah nilai di lingkungan Spark.
`spark-hive-site`	Ubah nilai dalam file hive-site.xml Spark.
`spark-log4j`	Ubah nilai dalam file log4j.properties Spark.

  Klasifikasi konfigurasi memungkinkan Anda menyesuaikan aplikasi. Ini sering sesuai dengan file XHTML konfigurasi untuk aplikasi, spark-hive-site seperti.xml.xml. Untuk informasi lebih lanjut, lihat Mengonfigurasi Aplikasi.

Masalah yang diketahui

- Fungsionalitas template Spark pod dengan titik akhir interaktif tidak berfungsi di Amazon EMR pada rilis EKS 6.4.

emr-6.4.0-terbaru

Catatan rilis: `emr-6.4.0-latest` saat ini menunjuk ke `emr-6.4.0-20221219`.

Wilayah: `emr-6.4.0-latest` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.4.0:latest`

emr-6.4.0-20221219

Catatan rilis: `emr-6.4.0-20221219` dirilis pada 27 Jan 2023. Dibandingkan dengan versi sebelumnya, versi ini telah diperbarui dengan Paket Amazon Linux yang baru saja ditambahkan.

Wilayah: `emr-6.4.0-20221219` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.4.0:20221219`

emr-6.4.0-20210830

Catatan rilis: `emr-6.4.0-20210830` dirilis pada 9 Desember 2021. Ini adalah rilis awal Amazon EMR 6.4.0.

Wilayah: `emr-6.4.0-20210830` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.4.0:20210830`

Amazon EMR pada rilis EKS 6.3.0

Rilis Amazon EMR 6.3.0 berikut tersedia untuk Amazon EMR di EKS. Pilih rilis EMR-6.3.0-XXXX tertentu untuk melihat detail selengkapnya seperti tag gambar kontainer terkait.

- emr-6.3.0-terbaru
- emr-6.3.0-20220802
- emr-6.3.0-20211008
- emr-6.3.0-20210802
- emr-6.3.0-20210429

Catatan rilis untuk Amazon EMR 6.3.0

- Fitur baru - Dimulai dengan Amazon EMR 6.3.0 dalam seri rilis 6.x, Amazon EMR di EKS mendukung fitur templat pod Spark. Anda juga dapat mengaktifkan fitur rotasi Spark log peristiwa untuk Amazon EMR di EKS. Untuk informasi lebih lanjut, lihat Menggunakan templat pod dan Menggunakan rotasi log peristiwa Spark.
- Aplikasi yang didukung - Spark 3.1.1-amzn-0, Jupyter Enterprise Gateway (titik akhir, pratinjau publik).
- Komponen yang didukung - `aws-hm-client` (Konektor Glue), `aws-sagemaker-spark-sdk`, `emr-s3-select`, `emrfs`, `emr-ddb`, `hudi-spark`.
- Klasifikasi konfigurasi yang didukung:

Klasifikasi	Deskripsi
`core-site`	Ubah nilai dalam file core-site.xml Hadoop.
`emrfs-site`	Ubah pengaturan EMRFS.
`spark-metrics`	Ubah nilai dalam file metrics.properties Spark.
`spark-defaults`	Ubah nilai dalam file spark-defaults.conf Spark.
`spark-env`	Ubah nilai di lingkungan Spark.
`spark-hive-site`	Ubah nilai dalam file hive-site.xml Spark.
`spark-log4j`	Ubah nilai dalam file log4j.properties Spark.

Klasifikasi konfigurasi memungkinkan Anda menyesuaikan aplikasi. Ini sering sesuai dengan file XHTML konfigurasi untuk aplikasi, spark-hive-site seperti.xml.xml. Untuk informasi lebih lanjut, lihat Mengonfigurasi Aplikasi.

emr-6.3.0-terbaru

Catatan rilis: `emr-6.3.0-latest` saat ini menunjuk ke `emr-6.3.0-20220802`.

Wilayah: `emr-6.3.0-latest` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.3.0:latest`

emr-6.3.0-20220802

Catatan rilis: `emr-6.3.0-20220802` dirilis pada 27 Sep 2022. Dibandingkan dengan versi sebelumnya, versi ini telah diperbarui dengan Paket Amazon Linux yang baru diperbarui.

Wilayah: `emr-6.3.0-20220802` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.3.0:20220802`

emr-6.3.0-20211008

Catatan rilis: `emr-6.3.0-20211008` dirilis pada 9 Desember 2021. Dibandingkan dengan versi sebelumnya, versi ini berisi perbaikan masalah dan pembaruan keamanan.

Wilayah: `emr-6.3.0-20211008` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.3.0:20211008`

emr-6.3.0-20210802

Catatan rilis: `emr-6.3.0-20210802` dirilis pada 2 Agustus 2021. Dibandingkan dengan versi sebelumnya, versi ini berisi perbaikan masalah dan pembaruan keamanan.

Wilayah: `emr-6.3.0-20210802` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.3.0:20210802`

emr-6.3.0-20210429

Catatan rilis: `emr-6.3.0-20210429` dirilis pada tanggal 29 April 2021. Ini adalah rilis awal Amazon EMR 6.3.0.

Wilayah: `emr-6.3.0-20210429` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.3.0:20210429`

Amazon EMR pada rilis EKS 6.2.0

Rilis Amazon EMR 6.2.0 berikut tersedia untuk Amazon EMR di EKS. Pilih rilis EMR-6.2.0-XXXX tertentu untuk melihat detail selengkapnya seperti tag gambar kontainer terkait.

- emr-6.2.0-latest
- emr-6.2.0-20220802
- emr-6.2.0-20211008
- emr-6.2.0-20210802
- emr-6.2.0-20210615
- emr-6.2.0-20210129
- emr-6.2.0-20201218
- emr-6.2.0-20201201

Catatan rilis untuk Amazon EMR 6.2.0

- Aplikasi yang didukung - Spark 3.0.1-amzn-0, Jupyter Enterprise Gateway (titik akhir, pratinjau publik).
- Komponen yang didukung - `aws-hm-client` (Konektor Glue), `aws-sagemaker-spark-sdk`, `emr-s3-select`, `emrfs`, `emr-ddb`, `hudi-spark`.
- Klasifikasi konfigurasi yang didukung:

Klasifikasi	Deskripsi
`core-site`	Ubah nilai dalam file core-site.xml Hadoop.
`emrfs-site`	Ubah pengaturan EMRFS.
`spark-metrics`	Ubah nilai dalam file metrics.properties Spark.
`spark-defaults`	Ubah nilai dalam file spark-defaults.conf Spark.
`spark-env`	Ubah nilai di lingkungan Spark.

Klasifikasi	Deskripsi
`spark-hive-site`	Ubah nilai dalam file hive-site.xml Spark.
`spark-log4j`	Ubah nilai dalam file log4j.properties Spark.

Klasifikasi konfigurasi memungkinkan Anda menyesuaikan aplikasi. Ini sering sesuai dengan file XHTML konfigurasi untuk aplikasi, spark-hive-site seperti.xml.xml. Untuk informasi lebih lanjut, lihat Mengonfigurasi Aplikasi.

emr-6.2.0-latest

Catatan rilis: `emr-6.2.0-latest` saat ini menunjuk ke `emr-6.2.0-20220802`.

Wilayah: `emr-6.2.0-latest` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.2.0:20220802`

emr-6.2.0-20220802

Catatan rilis: `emr-6.2.0-20220802` dirilis pada 27 Sep 2022. Dibandingkan dengan versi sebelumnya, versi ini telah diperbarui dengan Paket Amazon Linux yang baru diperbarui.

Wilayah: `emr-6.2.0-20220802` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-6.2.0:20220802`

emr-6.2.0-20211008

Catatan rilis: `emr-6.2.0-20211008` dirilis pada 9 Desember 2021. Dibandingkan dengan versi sebelumnya, versi ini berisi perbaikan masalah dan pembaruan keamanan.

Wilayah: `emr-6.2.0-20211008` tersedia di Wilayah Berikut: US East (N. Virginia), US West (Oregon), Asia Pacific (Tokyo), Europe (Ireland), South America (Sao Paulo).

Tanda gambar kontainer: `emr-6.2.0:20211008`

emr-6.2.0-20210802

Catatan rilis: `emr-6.2.0-20210802` dirilis pada 2 Agustus 2021. Dibandingkan dengan versi sebelumnya, versi ini berisi perbaikan masalah dan pembaruan keamanan.

Wilayah: `emr-6.2.0-20210802` tersedia di Wilayah Berikut: US East (N. Virginia), US West (Oregon), Asia Pacific (Tokyo), Europe (Ireland), South America (Sao Paulo).

Tanda gambar kontainer: `emr-6.2.0:20210802`

emr-6.2.0-20210615

Catatan rilis: `emr-6.2.0-20210615` dirilis pada 15 Juni 2021. Dibandingkan dengan versi sebelumnya, versi ini berisi perbaikan masalah dan pembaruan keamanan.

Wilayah: `emr-6.2.0-20210615` tersedia di Wilayah Berikut: US East (N. Virginia), US West (Oregon), Asia Pacific (Tokyo), Europe (Ireland), South America (Sao Paulo).

Tanda gambar kontainer: `emr-6.2.0:20210615`

emr-6.2.0-20210129

Catatan rilis: `emr-6.2.0-20210129` dirilis pada tanggal 29 Januari 2021. Dibandingkan dengan `emr-6.2.0-20201218`, versi ini berisi perbaikan masalah dan pembaruan keamanan.

Wilayah: `emr-6.2.0-20210129` tersedia di Wilayah berikut: US East (N. Virginia), US West (Oregon), Asia Pacific (Tokyo), Europe (Ireland), South America (Sao Paulo).

Tanda gambar kontainer: `emr-6.2.0-20210129`

emr-6.2.0-20201218

Catatan rilis: `emr-6.2.0-20201218` dirilis pada tanggal 18 Desember 2020. Dibandingkan dengan `emr-6.2.0-20201201`, versi ini berisi perbaikan masalah dan pembaruan keamanan.

Wilayah: `emr-6.2.0-20201218` tersedia di Wilayah berikut: US East (N. Virginia), US West (Oregon), Asia Pacific (Tokyo), Europe (Ireland), South America (Sao Paulo).

Tanda gambar kontainer: `emr-6.2.0-20201218`

emr-6.2.0-20201201

Catatan rilis: `emr-6.2.0-20201201` dirilis pada tanggal 1 Desember 2020. Ini adalah rilis awal Amazon EMR 6.2.0.

Wilayah: `emr-6.2.0-20201201` tersedia di Wilayah Berikut: US East (N. Virginia), US West (Oregon), Asia Pacific (Tokyo), Europe (Ireland), South America (Sao Paulo).

Tanda gambar kontainer: `emr-6.2.0-20201201`

Amazon EMR pada rilis EKS 5.36.0

Rilis Amazon EMR 5.36.0 berikut tersedia untuk Amazon EMR di EKS. Pilih rilis EMR-5.36.0-XXXX tertentu untuk melihat detail selengkapnya seperti tag gambar kontainer terkait.

- emr-5.36.0-terbaru
- emr-5.36.0-20221219
- emr-5.36.0-20220620
- emr-5.36.0-20220525

Catatan rilis untuk Amazon EMR 5.36.0

- Memperbaiki masalah keamanan log4j2.
- Aplikasi yang didukung - Spark 2.4.8-amzn-2, Jupyter Enterprise Gateway (titik akhir, pratinjau publik; Kernel Scala tidak didukung), livy-0.7.1, fluentd-4.0.0.
- Komponen yang didukung - aws-hm-client,, emr-ddb aws-sagemaker-spark-sdk, emr-goodies, emr-kinesis, kerberos-server.
- Klasifikasi konfigurasi yang didukung:

Klasifikasi	Deskripsi
`core-site`	Ubah nilai dalam file core-site.xml Hadoop.
`emrfs-site`	Ubah pengaturan EMRFS.
`spark-metrics`	Ubah nilai dalam file metrics.properties Spark.

Klasifikasi	Deskripsi
`spark-defaults`	Ubah nilai dalam file spark-defaults.conf Spark.
`spark-env`	Ubah nilai di lingkungan Spark.
`spark-hive-site`	Ubah nilai dalam file hive-site.xml Spark.
`spark-log4j`	Ubah nilai dalam file log4j.properties Spark.

Klasifikasi konfigurasi memungkinkan Anda menyesuaikan aplikasi. Ini sering sesuai dengan file XHTML konfigurasi untuk aplikasi, spark-hive-site seperti.xml.xml. Untuk informasi lebih lanjut, lihat Mengonfigurasi Aplikasi.

emr-5.36.0-terbaru

Catatan rilis: `emr-5.36.0-latest` saat ini menunjuk ke `emr-5.36.0-20221219`.

Wilayah: `emr-5.36.0-latest` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-5.36.0:latest`

emr-5.36.0-20221219

Catatan rilis: `emr-5.36.0-20221219` dirilis pada 27 Jan 2023. Dibandingkan dengan versi sebelumnya, versi ini telah diperbarui dengan Paket Amazon Linux yang baru diperbarui.

Wilayah: `emr-5.36.0-20221219` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-5.36.0:20221219`

emr-5.36.0-20220620

Catatan rilis: `emr-5.36.0-20220620` dirilis pada 27 Juli 2022. Dibandingkan dengan versi sebelumnya, versi ini telah diperbarui dengan Paket Amazon Linux yang baru diperbarui.

Wilayah: `emr-5.36.0-20220620` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-5.36.0:20220620`

emr-5.36.0-20220525

Catatan rilis: `emr-5.36.0-20220525` dirilis pada 16 Juni 2022. Ini adalah rilis awal Amazon EMR 5.36.0.

Wilayah: `emr-5.36.0-20220525` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-5.36.0:20220525`

Amazon EMR pada rilis EKS 5.35.0

Rilis Amazon EMR 5.35.0 berikut tersedia untuk Amazon EMR di EKS. Pilih rilis EMR-5.35.0-XXXX tertentu untuk melihat detail selengkapnya seperti tag gambar kontainer terkait.

- emr-5.35.0-terbaru
- emr-5.35.0-20221219
- emr-5.35.0-20220802
- emr-5.35.0-20220307

Catatan rilis untuk Amazon EMR 5.35.0

- Memperbaiki masalah keamanan log4j2.
- Aplikasi yang didukung - Spark 2.4.8-amzn-1, Hudi 0.9.0-amzn-2, Jupyter Enterprise Gateway (titik akhir, pratinjau publik; Kernel Scala tidak didukung).
- Komponen yang didukung - aws-hm-client (Konektor Glue),, emr-s3-select aws-sagemaker-spark-sdk, emrfs, emr-ddb, hudi-spark.
- Klasifikasi konfigurasi yang didukung:

Klasifikasi	Deskripsi
`core-site`	Ubah nilai dalam file core-site.xml Hadoop.

Klasifikasi	Deskripsi
`emrfs-site`	Ubah pengaturan EMRFS.
`spark-metrics`	Ubah nilai dalam file metrics.properties Spark.
`spark-defaults`	Ubah nilai dalam file spark-defaults.conf Spark.
`spark-env`	Ubah nilai di lingkungan Spark.
`spark-hive-site`	Ubah nilai dalam file hive-site.xml Spark.
`spark-log4j`	Ubah nilai dalam file log4j.properties Spark.

Klasifikasi konfigurasi memungkinkan Anda menyesuaikan aplikasi. Ini sering sesuai dengan file XHTML konfigurasi untuk aplikasi, spark-hive-site seperti.xml.xml. Untuk informasi lebih lanjut, lihat Mengonfigurasi Aplikasi.

emr-5.35.0-terbaru

Catatan rilis: `emr-5.35.0-latest` saat ini menunjuk ke `emr-5.35.0-20221219`.

Wilayah: `emr-5.35.0-latest` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-5.35.0:latest`

emr-5.35.0-20221219

Catatan rilis: `emr-5.35.0-20221219` dirilis pada 27 Jan 2023. Dibandingkan dengan versi sebelumnya, versi ini telah diperbarui dengan Paket Amazon Linux yang baru diperbarui.

Wilayah: `emr-5.35.0-20221219` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-5.35.0:20221219`

emr-5.35.0-20220802

Catatan rilis: `emr-5.35.0-20220802` dirilis pada 27 Sep 2022. Dibandingkan dengan versi sebelumnya, versi ini telah diperbarui dengan Paket Amazon Linux yang baru diperbarui.

Wilayah: `emr-5.35.0-20220802` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-5.35.0:20220802`

emr-5.35.0-20220307

Catatan rilis: `emr-5.35.0-20220307` dirilis pada 30 Maret 2022. Dibandingkan dengan versi sebelumnya, versi ini telah diperbarui dengan Paket Amazon Linux yang baru diperbarui.

Wilayah: `emr-5.35.0-20220307` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-5.35.0:20220307`

Amazon EMR pada rilis EKS 5.34.0

Rilis Amazon EMR 5.34.0 berikut tersedia untuk Amazon EMR di EKS. Pilih rilis EMR-5.34.0-XXXX tertentu untuk melihat detail selengkapnya seperti tag gambar kontainer terkait.

- emr-5.34.0-terbaru
- emr-5.34.0-20220802

Catatan rilis untuk Amazon EMR 5.34.0

- Aplikasi yang didukung - Spark 2.4.8-amzn-0, Jupyter Enterprise Gateway (titik akhir, pratinjau publik; Kernel Scala tidak didukung).
- Komponen yang didukung - `aws-hm-client` (Konektor Glue), `aws-sagemaker-spark-sdk`, `emr-s3-select`, `emrfs`, `emr-ddb`, `hudi-spark`.
- Klasifikasi konfigurasi yang didukung:

Klasifikasi	Deskripsi
`core-site`	Ubah nilai dalam file core-site.xml Hadoop.
`emrfs-site`	Ubah pengaturan EMRFS.
`spark-metrics`	Ubah nilai dalam file metrics.properties Spark.
`spark-defaults`	Ubah nilai dalam file spark-defaults.conf Spark.
`spark-env`	Ubah nilai di lingkungan Spark.
`spark-hive-site`	Ubah nilai dalam file hive-site.xml Spark.
`spark-log4j`	Ubah nilai dalam file log4j.properties Spark.

Klasifikasi konfigurasi memungkinkan Anda menyesuaikan aplikasi. Ini sering sesuai dengan file XHTML konfigurasi untuk aplikasi, spark-hive-site seperti.xml.xml. Untuk informasi lebih lanjut, lihat Mengonfigurasi Aplikasi.

emr-5.34.0-terbaru

Catatan rilis: `emr-5.34.0-latest` saat ini menunjuk ke `emr-5.34.0-20220802`.

Wilayah: `emr-5.34.0-latest` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-5.34.0:latest`

emr-5.34.0-20220802

Catatan rilis: `emr-5.34.0-20220802` dirilis pada 24 Agustus 2022. Dibandingkan dengan versi sebelumnya, versi ini telah diperbarui dengan Paket Amazon Linux yang baru diperbarui.

Wilayah: `emr-5.34.0-20220802` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-5.34.0:20220802`

emr-5.34.0-20211208

Catatan rilis: `emr-5.34.0-20211208` dirilis pada 20 Jan 2022. Dibandingkan dengan versi sebelumnya, versi ini telah diperbarui dengan Paket Amazon Linux yang baru diperbarui.

Wilayah: `emr-5.34.0-20211208` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-5.34.0:20211208`

Amazon EMR pada rilis EKS 5.33.0

Rilis Amazon EMR 5.33.0 berikut tersedia untuk Amazon EMR di EKS. Pilih rilis EMR-5.33.0-XXXX tertentu untuk melihat detail selengkapnya seperti tag gambar kontainer terkait.

- emr-5.33.0-latest
- emr-5.33.0-20221219
- emr-5.33.0-20220802
- emr-5.33.0-20211008
- emr-5.33.0-20210802
- emr-5.33.0-20210615
- emr-5.33.0-20210323

Catatan rilis untuk Amazon EMR 5.33.0

- Fitur baru - Dimulai dengan Amazon EMR 5.33.0 dalam seri rilis 5.x, Amazon EMR di EKS mendukung fitur templat pod Spark. Untuk informasi selengkapnya, lihat Menggunakan templat pod.
- Aplikasi yang didukung - Spark 2.4.7-amzn-1, Jupyter Enterprise Gateway (titik akhir, pratinjau publik; Kernel Scala tidak didukung).
- Komponen yang didukung - `aws-hm-client` (Konektor Glue), `aws-sagemaker-spark-sdk`, `emr-s3-select`, `emrfs`, `emr-ddb`, `hudi-spark`.
- Klasifikasi konfigurasi yang didukung:

Klasifikasi	Deskripsi
`core-site`	Ubah nilai dalam file core-site.xml Hadoop.
`emrfs-site`	Ubah pengaturan EMRFS.
`spark-metrics`	Ubah nilai dalam file metrics.properties Spark.
`spark-defaults`	Ubah nilai dalam file spark-defaults.conf Spark.
`spark-env`	Ubah nilai di lingkungan Spark.
`spark-hive-site`	Ubah nilai dalam file hive-site.xml Spark.
`spark-log4j`	Ubah nilai dalam file log4j.properties Spark.

Klasifikasi konfigurasi memungkinkan Anda menyesuaikan aplikasi. Ini sering sesuai dengan file XHTML konfigurasi untuk aplikasi, spark-hive-site seperti.xml.xml. Untuk informasi lebih lanjut, lihat Mengonfigurasi Aplikasi.

emr-5.33.0-latest

Catatan rilis: `emr-5.33.0-latest` saat ini menunjuk ke `emr-5.33.0-20221219`.

Wilayah: `emr-5.33.0-latest` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-5.33.0:latest`

emr-5.33.0-20221219

Catatan rilis: `emr-5.33.0-20221219` dirilis pada 19 Jan 2023. Dibandingkan dengan versi sebelumnya, versi ini telah diperbarui dengan Paket Amazon Linux yang baru diperbarui dan perbaikan kritis.

Wilayah: `emr-5.33.0-20221219` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-5.33.0:20221219`

emr-5.33.0-20220802

Catatan rilis: `emr-5.33.0-20220802` dirilis pada 24 Agustus 2022. Dibandingkan dengan versi sebelumnya, versi ini telah diperbarui dengan Paket Amazon Linux yang baru diperbarui.

Wilayah: `emr-5.33.0-20220802` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-5.33.0:20220802`

emr-5.33.0-20211008

Catatan rilis: `emr-5.33.0-20211008` dirilis pada 9 Desember 2021. Dibandingkan dengan versi sebelumnya, versi ini berisi perbaikan masalah dan pembaruan keamanan.

Wilayah: `emr-5.33.0-20211008` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-5.33.0:20211008`

emr-5.33.0-20210802

Catatan rilis: `emr-5.33.0-20210802` dirilis pada 2 Agustus 2021. Dibandingkan dengan versi sebelumnya, versi ini berisi perbaikan masalah dan pembaruan keamanan.

Wilayah: `emr-5.33.0-20210802` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-5.33.0:20210802`

emr-5.33.0-20210615

Catatan rilis: `emr-5.33.0-20210615` dirilis pada 15 Juni 2021. Dibandingkan dengan versi sebelumnya, versi ini berisi perbaikan masalah dan pembaruan keamanan.

Wilayah: `emr-5.33.0-20210615` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-5.33.0:20210615`

emr-5.33.0-20210323

Catatan rilis: `emr-5.33.0-20210323` dirilis pada tanggal 23 Maret 2021. Ini adalah rilis awal Amazon EMR 5.33.0.

Wilayah: `emr-5.33.0-20210323` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-5.33.0-20210323`

Amazon EMR pada rilis EKS 5.32.0

Rilis Amazon EMR 5.32.0 berikut tersedia untuk Amazon EMR di EKS. Pilih rilis EMR-5.32.0-XXXX tertentu untuk melihat detail selengkapnya seperti tag gambar kontainer terkait.

- emr-5.32.0-latest
- emr-5.32.0-20220802
- emr-5.32.0-20211008
- emr-5.32.0-20210802
- emr-5.32.0-20210615
- emr-5.32.0-20210129
- emr-5.32.0-20201218
- emr-5.32.0-20201201

Catatan rilis untuk Amazon EMR 5.32.0

- Aplikasi yang didukung - Spark 2.4.7-amzn-0, Jupyter Enterprise Gateway (titik akhir, pratinjau publik; Kernel Scala tidak didukung).
- Komponen yang didukung - `aws-hm-client` (Konektor Glue), `aws-sagemaker-spark-sdk`, `emr-s3-select`, `emrfs`, `emr-ddb`, `hudi-spark`.
- Klasifikasi konfigurasi yang didukung:

Klasifikasi	Deskripsi
`core-site`	Ubah nilai dalam file core-site.xml Hadoop.

Klasifikasi	Deskripsi
`emrfs-site`	Ubah pengaturan EMRFS.
`spark-metrics`	Ubah nilai dalam file metrics.properties Spark.
`spark-defaults`	Ubah nilai dalam file spark-defaults.conf Spark.
`spark-env`	Ubah nilai di lingkungan Spark.
`spark-hive-site`	Ubah nilai dalam file hive-site.xml Spark.
`spark-log4j`	Ubah nilai dalam file log4j.properties Spark.

Klasifikasi konfigurasi memungkinkan Anda menyesuaikan aplikasi. Ini sering sesuai dengan file XHTML konfigurasi untuk aplikasi, spark-hive-site seperti.xml.xml. Untuk informasi lebih lanjut, lihat Mengonfigurasi Aplikasi.

emr-5.32.0-latest

Catatan rilis: `emr-5.32.0-latest` saat ini menunjuk ke `emr-5.32.0-20220802`.

Wilayah: `emr-5.32.0-latest` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-5.32.0:latest`

emr-5.32.0-20220802

Catatan rilis: `emr-5.32.0-20220802` dirilis pada 24 Agustus 2022. Dibandingkan dengan versi sebelumnya, versi ini telah diperbarui dengan Paket Amazon Linux yang baru diperbarui.

Wilayah: `emr-5.32.0-20220802` tersedia di semua Wilayah yang didukung oleh Amazon EMR di EKS. Untuk informasi selengkapnya, lihat titik akhir layanan Amazon EMR di EKS.

Tanda gambar kontainer: `emr-5.32.0:20220802`

emr-5.32.0-20211008

Catatan rilis: `emr-5.32.0-20211008` dirilis pada 9 Desember 2021. Dibandingkan dengan versi sebelumnya, versi ini berisi perbaikan masalah dan pembaruan keamanan.

Wilayah: `emr-5.32.0-20211008` tersedia di Wilayah Berikut: US East (N. Virginia), US West (Oregon), Asia Pacific (Tokyo), Europe (Ireland), South America (Sao Paulo).

Tanda gambar kontainer: `emr-5.32.0:20211008`

emr-5.32.0-20210802

Catatan rilis: `emr-5.32.0-20210802` dirilis pada 2 Agustus 2021. Dibandingkan dengan versi sebelumnya, versi ini berisi perbaikan masalah dan pembaruan keamanan.

Wilayah: `emr-5.32.0-20210802` tersedia di Wilayah Berikut: US East (N. Virginia), US West (Oregon), Asia Pacific (Tokyo), Europe (Ireland), South America (Sao Paulo).

Tanda gambar kontainer: `emr-5.32.0:20210802`

emr-5.32.0-20210615

Catatan rilis: `emr-5.32.0-20210615` dirilis pada 15 Juni 2021. Dibandingkan dengan versi sebelumnya, versi ini berisi perbaikan masalah dan pembaruan keamanan.

Wilayah: `emr-5.32.0-20210615` tersedia di Wilayah Berikut: US East (N. Virginia), US West (Oregon), Asia Pacific (Tokyo), Europe (Ireland), South America (Sao Paulo).

Tanda gambar kontainer: `emr-5.32.0:20210615`

emr-5.32.0-20210129

Catatan rilis: `emr-5.32.0-20210129` dirilis pada tanggal 29 Januari 2021. Dibandingkan dengan `emr-5.32.0-20201218`, versi ini berisi perbaikan masalah dan pembaruan keamanan.

Wilayah: `emr-5.32.0-20210129` tersedia di Wilayah berikut: US East (N. Virginia), US West (Oregon), Asia Pacific (Tokyo), Europe (Ireland), South America (Sao Paulo).

Tanda gambar kontainer: `emr-5.32.0-20210129`

emr-5.32.0-20201218

Catatan rilis: `5.32.0-20201218` dirilis pada tanggal 18 Desember 2020. Dibandingkan dengan `5.32.0-20201201`, versi ini berisi perbaikan masalah dan pembaruan keamanan.

Wilayah: `emr-5.32.0-20201218` tersedia di Wilayah berikut: US East (N. Virginia), US West (Oregon), Asia Pacific (Tokyo), Europe (Ireland), South America (Sao Paulo).

Tanda gambar kontainer: `emr-5.32.0-20201218`

emr-5.32.0-20201201

Catatan rilis: `5.32.0-20201201` dirilis pada tanggal 1 Desember 2020. Ini adalah rilis awal Amazon EMR 5.32.0.

Wilayah: `5.32.0-20201201d` tersedia di Wilayah berikut: US East (N. Virginia), US West (Oregon), Asia Pacific (Tokyo), Europe (Ireland), South America (Sao Paulo).

Tanda gambar kontainer: `emr-5.32.0-20201201`

Riwayat dokumen

Tabel berikut menjelaskan perubahan penting pada dokumentasi sejak rilis terakhir Amazon EMR di EKS. Untuk informasi lebih lanjut tentang pembaruan dokumentasi ini, Anda dapat berlangganan umpan RSS.

Perubahan	Deskripsi	Tanggal
Rilis baru	Amazon EMR pada rilis EKS 7.0.0	Desember 22, 2023
Rilis baru	Amazon EMR pada rilis EKS 6.15.0	17 November 2023
Rilis baru	Amazon EMR pada rilis EKS 6.14.0	17 Oktober 2023
Perbarui konten	Ubah nama “titik akhir terkelola” menjadi titik akhir interaktif; Ketersediaan umum titik akhir interaktif	September 29, 2023
Rilis baru	Amazon EMR pada rilis EKS 6.13.0, dan dokumen pratinjau publik untuk Menjalankan pekerjaan Flink dengan Amazon EMR di EKS	12 September 2023
Rilis baru	Amazon EMR pada rilis EKS 6.12.0	Juli 21, 2023
Konten baru	Ditambahkan Menggunakan Volcano sebagai penjadwal khusus untuk Apache Spark di Amazon EMR di EKS	13 Juni 2023
Konten baru	Ditambahkan Menggunakan Volcano sebagai penjadwal khusus untuk Apache Spark di Amazon EMR di EKS	13 Juni 2023
Konten baru	Ditambahkan Menggunakan rotasi log kontainer Spark	12 Juni 2023
Perbarui konten	Memperbarui dokumentasi gambar khusus untuk menemukan informasi	8 Juni 2023

Perubahan	Deskripsi	Tanggal
	gambar dasar di Galeri Publik Amazon ECR.	
Rilis baru	Amazon EMR pada rilis EKS 6.11.0	8 Juni 2023
Konten baru	Menambahkan Menjalankan pekerjaan Spark dengan operator Spark dan mengatur ulang bagian Job Runs di bawahMenjalankan pekerjaan dengan Amazon EMR di EKS.	Juni 5, 2023
Konten baru	Ditambahkan dua bagian: Menggunakan penskalaan otomatis vertikal dengan pekerjaan Amazon EMR Spark dan Menggunakan notebook Jupyter yang dihosting sendiri	4 Mei 2023
Halaman riwayat dokumen	Membuat halaman riwayat dokumen untuk Amazon EMR di EKS.	Maret 13, 2023
Halaman kebijakan terkelola	Membuat halaman kebijakan terkelola untuk Amazon EMR di EKS.	Maret 13, 2023

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