Panduan Implementasi

# Penemuan Beban Kerja di AWS

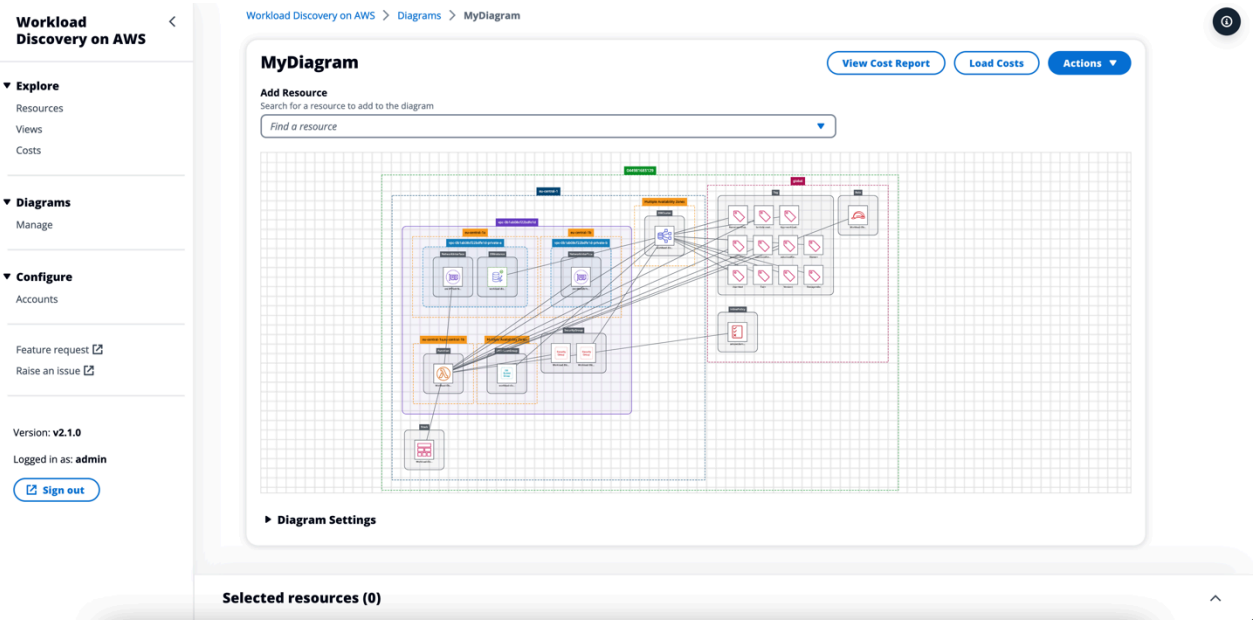
# Penemuan Beban Kerja di AWS: Panduan Implementasi

# Table of Contents

# Menerapkan alat visualisasi yang secara otomatis menghasilkan diagram arsitektur beban kerja AWS Cloud

Memantau beban kerja Cloud Amazon Web Services (AWS) Anda adalah kunci untuk menjaga kesehatan dan efisiensi operasional. Namun, melacak sumber daya AWS dan hubungan di antara keduanya bisa menjadi tantangan. Workload Discovery on AWS adalah alat visualisasi yang secara otomatis menghasilkan diagram arsitektur beban kerja Anda di AWS. Anda dapat menggunakan solusi ini untuk membangun, menyesuaikan, dan berbagi visualisasi beban kerja terperinci berdasarkan data langsung dari AWS.

Solusi ini berfungsi dengan memelihara inventaris sumber daya AWS di seluruh akun dan Wilayah Anda, memetakan hubungan di antara keduanya, dan menampilkannya dalam antarmuka pengguna web (UI web). Saat membuat perubahan pada sumber daya, Workload Discovery di AWS menghemat waktu Anda dengan menyediakan tautan ke sumber daya di AWS Management Console.




Contoh diagram arsitektur yang dihasilkan oleh Workload Discovery di AWS

Panduan implementasi ini menjelaskan pertimbangan arsitektur dan langkah-langkah konfigurasi untuk menerapkan Workload Discovery di AWS di AWS Cloud. Ini mencakup tautan ke CloudFormation templat AWS yang meluncurkan dan mengonfigurasi layanan AWS yang diperlukan untuk menerapkan solusi ini menggunakan praktik terbaik AWS untuk keamanan dan ketersediaan.

Audiens yang dituju untuk menerapkan solusi Workload Discovery on AWS di lingkungan mereka mencakup arsitek solusi, pengambil keputusan bisnis, DevOps insinyur, ilmuwan data, dan profesional cloud.

Gunakan tabel navigasi ini untuk menemukan jawaban atas pertanyaan-pertanyaan ini dengan cepat:

| Jika kau mau. | Baca. |
| --- | --- |
| Ketahui biaya untuk menjalankan solusi ini.<br><br>Perkiraan biaya untuk menjalankan solusi ini di Wilayah AS Timur (Virginia N.) adalah USD $425.19 per bulan. | Biaya |
| Memahami pertimbangan keamanan untuk solusi ini. | Keamanan |
| Ketahui cara merencanakan kuota untuk solusi ini. | Kuota |
| Ketahui Wilayah AWS mana yang mendukung solusi ini. | Wilayah AWS yang Didukung |
| Lihat atau unduh CloudFormation templat AWS yang disertakan dalam solusi ini untuk secara otomatis menerapkan sumber daya infrastru ktur (“tumpukan”) untuk solusi ini. | CloudFormation Templat AWS |
| Akses kode sumber. | GitHub repositori |

# Fitur dan manfaat

Workload Discovery di AWS menyediakan fitur-fitur berikut:

Buat diagram arsitektur menggunakan data mendekati waktu nyata

Workload Discovery di AWS memindai akun Anda setiap 15 menit untuk memastikan bahwa diagram yang Anda buat adalah representasi beban kerja Anda yang akurat dan terkini.

Lihat sumber daya dari beberapa akun dan Wilayah di satu tempat

Solusi ini menyimpan inventaris sumber daya AWS di seluruh akun AWS dan Wilayah Anda dalam database grafik terpusat, memungkinkan Anda menjelajahi beberapa akun dan Wilayah serta hubungannya satu sama lain dalam satu UI.

Integrasi AWS Organizations

Saat menerapkan solusi dengan AWS Organizations, Workload Discovery on AWS akan secara otomatis menemukan semua sumber daya yang didukung di organisasi Anda. Dalam konfigurasi ini, tidak perlu secara langsung mengelola penyebaran CloudFormation templat khusus akun untuk membuat akun ini tersedia untuk ditemukan.

Menyusun data biaya di seluruh beban kerja Anda

Saat diaktifkan, fitur biaya memungkinkan Anda untuk mencari sumber daya di akun Anda berdasarkan biaya dan menambahkan sumber daya yang Anda temukan ke diagram. Anda juga dapat menambahkan data biaya ke diagram yang sudah ada.

Ekspor ke diagrams.net (sebelumnya draw.io)

Workload Discovery di AWS dapat mengekspor diagram Anda sehingga Anda dapat membuat anotasi lebih lanjut menggunakan perangkat lunak gambar pihak ketiga ini.

Integrasi dengan AWS Service Catalog AppRegistry dan Application Manager, kemampuan AWS Systems Manager

Solusi ini mencakup AppRegistry sumber daya Service Catalog untuk mendaftarkan CloudFormation template solusi dan sumber daya dasarnya sebagai aplikasi di Service Catalog AppRegistry dan Application Manager. Dengan integrasi ini, Anda dapat mengelola sumber daya solusi secara terpusat dan mengaktifkan tindakan pencarian, pelaporan, dan manajemen aplikasi.

# Kasus penggunaan

Ulasan desain dan keamanan

Gunakan solusi ini untuk menghasilkan diagram arsitektur untuk memvalidasi bahwa implementasi beban kerja sesuai dengan desain yang diusulkan.

Jelajahi dan dokumentasikan beban kerja yang ada

Buat diagram arsitektur untuk mengeksplorasi beban kerja di mana ada sedikit dokumentasi atau yang digunakan secara manual tanpa infrastruktur sebagai kode.

Visualisasikan biaya

Buat laporan biaya untuk diagram arsitektur Anda yang berisi ikhtisar perkiraan biaya.

## Konsep dan definisi

Bagian ini menjelaskan konsep-konsep kunci dan mendefinisikan terminologi khusus untuk solusi ini:

sumber daya

Sumber daya AWS, seperti bucket Amazon Simple Storage Service (Amazon S3) atau fungsi AWS Lambda.

hubungan

Tautan antara dua sumber daya, seperti peran AWS Identity and Access Management (IAM) dan fungsi AWS Lambda terkait.

jenis sumber daya

Kategori klasifikasi sumber daya. Selalu mengikuti konvensi CloudFormation penamaan, seperti`AWS::Lambda::Function`.

penemuan

Proses yang dimulai solusi untuk memetakan sumber daya dan hubungannya di akun dan Wilayah AWS Anda.

mode penemuan akun

Metode menemukan akun dan menambahkannya ke solusi: dikelola sendiri melalui Workload Discovery di AWS UI atau didelegasikan ke AWS Organizations.

> **Note**
>
> Untuk referensi umum istilah AWS, lihat Daftar Istilah AWS.

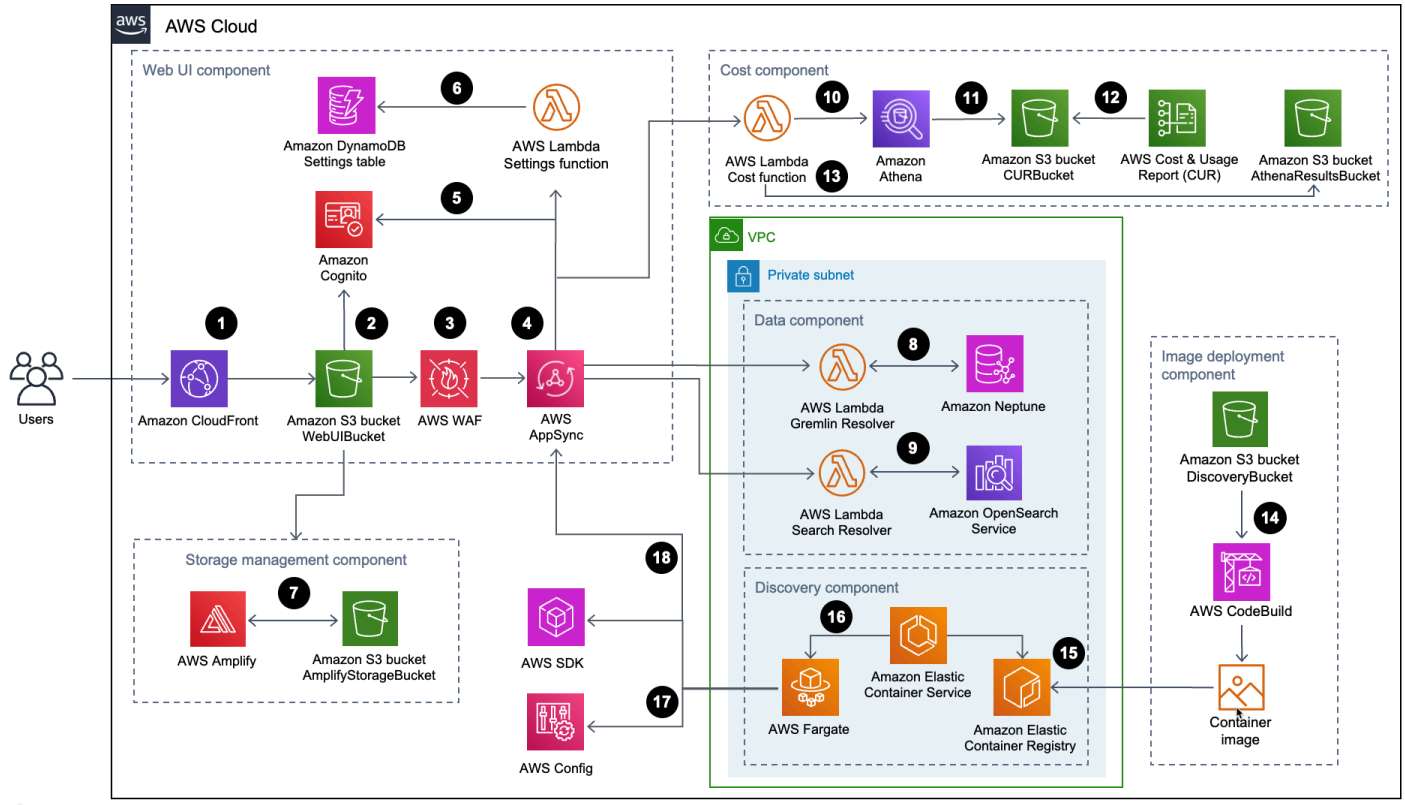
# Gambaran umum arsitektur

Bagian ini menyediakan diagram arsitektur implementasi referensi untuk komponen yang digunakan dengan solusi ini.

## Diagram arsitektur

Menerapkan solusi ini dengan parameter default membangun lingkungan berikut di AWS Cloud.

Penemuan Beban Kerja pada arsitektur AWS




Alur proses tingkat tinggi untuk komponen solusi yang digunakan dengan CloudFormation template AWS adalah sebagai berikut:

1. HTTP Strict-Transport-Security (HSTS) menambahkan header keamanan untuk setiap respons dari distribusi Amazon CloudFront.
2. Bucket Amazon Simple Storage Service (Amazon S3) menghosting UI web, yang didistribusikan dengan Amazon. CloudFront Amazon Cognito mengautentikasi akses pengguna ke UI web.

3. AWS WAF melindungi AppSync API dari eksploitasi umum dan bot yang dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan.
4. AppSyncTitik akhir AWS memungkinkan komponen UI web untuk meminta data hubungan sumber daya, biaya kueri, mengimpor Wilayah AWS baru, dan memperbarui preferensi. AWS AppSync juga memungkinkan komponen penemuan untuk menyimpan data persisten dalam database solusi.
5. AWS AppSync menggunakan JSON Web Tokens (JWTs) yang disediakan oleh Amazon Cognito untuk mengautentikasi setiap permintaan.
6. Fungsi `Settings`AWS Lambda mempertahankan Wilayah yang diimpor dan konfigurasi lainnya ke Amazon DynamoDB.
7. Solusinya menerapkan AWS Amplify dan bucket Amazon S3 sebagai komponen manajemen penyimpanan untuk menyimpan preferensi pengguna dan diagram arsitektur yang disimpan.
8. Komponen data menggunakan fungsi `Gremlin Resolver` AWS Lambda untuk menanyakan dan mengembalikan data dari database Amazon Neptunus.
9. Komponen data menggunakan fungsi `Search Resolver` Lambda untuk menanyakan dan menyimpan data sumber daya ke dalam domain Layanan Amazon OpenSearch .
10. Fungsi `Cost` Lambda menggunakan Amazon Athena untuk menanyakan Laporan Biaya dan Penggunaan AWS (AWS CUR) untuk memberikan perkiraan data biaya ke UI web.
11. Amazon Athena menjalankan kueri di AWS CUR.
12. AWS CUR mengirimkan laporan ke bucket `CostAndUsageReportBucket` Amazon S3.
13. Fungsi `Cost` Lambda menyimpan hasil Amazon Athena di bucket Amazon `AthenaResultsBucket` S3.
14. AWS CodeBuild membangun image container komponen penemuan dalam komponen penerapan gambar.
15. Amazon Elastic Container Registry (Amazon ECR) berisi image Docker yang disediakan oleh komponen penyebaran gambar.
16. Amazon Elastic Container Service (Amazon ECS) mengelola tugas AWS Fargate dan menyediakan konfigurasi yang diperlukan untuk menjalankan tugas. AWS Fargate menjalankan tugas penampung setiap 15 menit untuk menyegarkan data inventaris dan sumber daya.
17. Panggilan AWS Config dan AWS SDK membantu komponen penemuan mempertahankan inventaris data sumber daya dari Wilayah yang diimpor, lalu menyimpan hasilnya dalam komponen data.

18.Tugas AWS Fargate mempertahankan hasil AWS Config dan AWS SDK panggilan ke database Amazon Neptune dan domain Layanan Amazon dengan panggilan API ke API. OpenSearch AppSync

# Pertimbangan desain AWS Well-Architected

Solusi ini menggunakan praktik terbaik dari AWS Well-Architected Framework yang membantu pelanggan merancang dan mengoperasikan beban kerja yang andal, aman, efisien, dan hemat biaya di cloud.

Bagian ini menjelaskan bagaimana prinsip-prinsip desain dan praktik terbaik dari Well-Architected Framework menguntungkan solusi ini.

## Keunggulan operasional

Kami merancang solusi ini menggunakan prinsip dan praktik terbaik dari pilar keunggulan operasional untuk mendapatkan manfaat dari solusi ini.

- Sumber daya didefinisikan sebagai infrastruktur sebagai penggunaan kode CloudFormation.
- Solusi ini mendorong metrik CloudWatch ke Amazon untuk memberikan observabilitas ke dalam infrastruktur, fungsi Lambda, tugas Amazon ECS, bucket AWS S3, dan komponen solusi lainnya.

## Keamanan

Kami merancang solusi ini menggunakan prinsip dan praktik terbaik dari pilar keamanan untuk mendapatkan manfaat dari solusi ini.

- Amazon Cognito mengautentikasi dan mengotorisasi pengguna aplikasi UI web.
- Semua peran yang digunakan oleh solusi mengikuti akses hak istimewa paling sedikit. Dengan kata lain, mereka hanya berisi izin minimum yang diperlukan sehingga layanan dapat berfungsi dengan baik.
- Data saat istirahat dan transit dienkripsi menggunakan kunci yang disimpan di AWS Key Management Service (AWS KMS) --penyimpanan manajemen kunci khusus.
- Kredensil memiliki kedaluwarsa singkat dan mengikuti kebijakan kata sandi yang kuat.
- Arahan GraphQL AppSync keamanan AWS memberikan kontrol halus atas operasi apa yang dapat dipanggil oleh frontend dan backend.

- Pencatatan, penelusuran, dan pembuatan versi diaktifkan jika berlaku.
- Penambalan otomatis (versi minor) dan pembuatan snapshot diaktifkan jika berlaku.
- Akses jaringan bersifat pribadi secara default dengan titik akhir Amazon Virtual Private Cloud (Amazon VPC) diaktifkan jika tersedia.

## Keandalan

Kami merancang solusi ini menggunakan prinsip dan praktik terbaik dari pilar keandalan untuk mendapatkan manfaat dari solusi ini.

- Solusinya menggunakan layanan tanpa server AWS sedapat mungkin untuk memastikan ketersediaan dan pemulihan yang tinggi dari kegagalan layanan.
- Semua pemrosesan komputasi menggunakan fungsi Lambda atau Amazon ECS di AWS Fargate.
- Semua kode kustom menggunakan AWS SDK dan permintaan dibatasi di sisi klien untuk mencegah tercapainya kuota tarif API.

## Efisiensi kinerja

Kami merancang solusi ini menggunakan prinsip dan praktik terbaik dari pilar efisiensi kinerja untuk mendapatkan manfaat dari solusi ini.

- Solusinya menggunakan arsitektur tanpa server AWS jika memungkinkan. Ini menghilangkan beban operasional mengelola server fisik.
- Solusi ini dapat diluncurkan di Wilayah mana pun yang mendukung layanan AWS yang digunakan dalam solusi ini seperti: AWS Lambda, Amazon Neptunus, AWS, AppSync Amazon S3, dan Amazon Cognito.
- Di Wilayah yang didukung, Amazon Neptunus tanpa server memungkinkan Anda menjalankan dan menskalakan beban kerja grafik secara instan, tanpa perlu mengelola dan mengoptimalkan kapasitas basis data.
- Solusi ini menggunakan layanan terkelola secara keseluruhan untuk mengurangi beban operasional penyediaan dan manajemen sumber daya.

## Optimalisasi biaya

Kami merancang solusi ini menggunakan prinsip dan praktik terbaik dari pilar pengoptimalan biaya untuk mendapatkan manfaat dari solusi ini.

- AWS ECS di AWS Fargate menggunakan fungsi Lambda secara eksklusif untuk komputasi dan hanya mengenakan biaya berdasarkan penggunaan.
- Amazon DynamoDB menskalakan kapasitas sesuai permintaan, jadi Anda hanya membayar untuk kapasitas yang Anda gunakan.

## Keberlanjutan

Kami merancang solusi ini menggunakan prinsip dan praktik terbaik dari pilar keberlanjutan untuk mendapatkan manfaat dari solusi ini.

- Solusinya menggunakan layanan terkelola dan tanpa server jika memungkinkan untuk meminimalkan dampak lingkungan dari layanan backend.

# Detail arsitektur

Bagian ini menjelaskan komponen dan layanan AWS yang membentuk solusi ini dan detail arsitektur tentang cara komponen ini bekerja sama.

## Mekanisme autentikasi

Workload Discovery di AWS menggunakan kumpulan pengguna Amazon Cognito untuk autentikasi UI dan AWS AppSync . Setelah diautentikasi, Amazon Cognito menyediakan Token Web JSON (JWT) ke UI web yang akan disediakan dengan semua permintaan API berikutnya. Jika JWT yang valid tidak disediakan, permintaan API akan gagal dan mengembalikan respons Terlarang HTTP 403.

## Sumber daya yang didukung

Untuk daftar jenis sumber daya AWS yang dapat ditemukan oleh Workload Discovery di AWS dalam akun dan Wilayah Anda, lihat sumber daya yang didukung.

## Penemuan Beban Kerja pada manajemen diagram arsitektur AWS

Anda dapat menyimpan Workload Discovery pada diagram arsitektur AWS menggunakan UI web tempat operasi membuat, membaca, memperbarui, dan menghapus (CRUD) dapat dilakukan. AWS Amplify storage API memungkinkan Workload Discovery di AWS menyimpan diagram arsitektur dalam bucket Amazon S3. Ada dua tingkat izin yang tersedia:

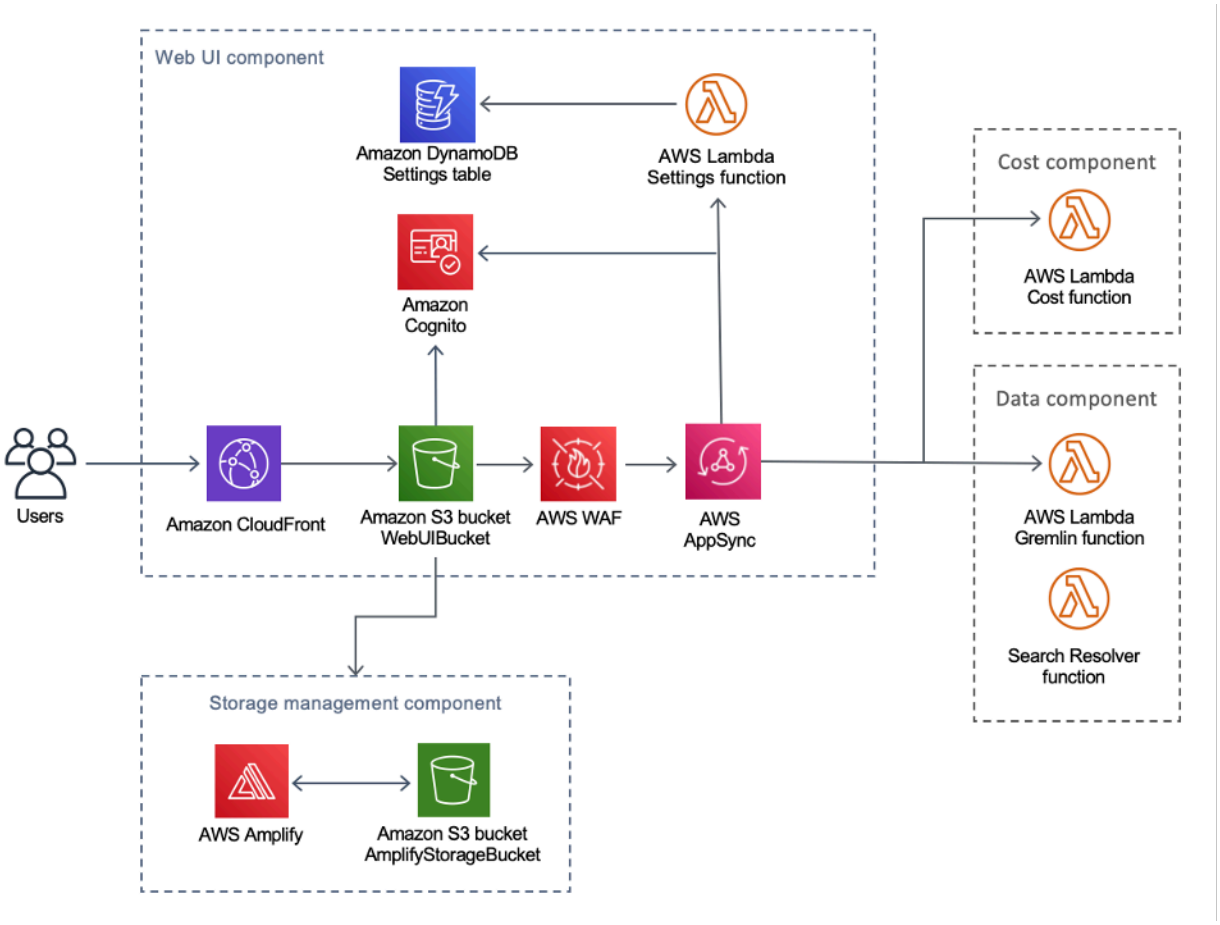
- Semua pengguna - Memungkinkan Penemuan Beban Kerja pada diagram arsitektur AWS terlihat oleh Workload Discovery pada pengguna AWS dalam penerapan Anda. Pengguna dapat mengunduh dan mengedit diagram ini.
- Anda - Memungkinkan Penemuan Beban Kerja pada diagram arsitektur AWS hanya dapat dilihat oleh pembuatnya. Pengguna lain tidak akan dapat melihatnya.

## UI Web dan manajemen penyimpanan

Kami mengembangkan UI web menggunakan React. UI web menyediakan konsol frontend untuk memungkinkan pengguna berinteraksi dengan Workload Discovery di AWS.

Amazon CloudFront dikonfigurasi untuk menambahkan header aman ke setiap permintaan HTTP ke UI web. Ini memberikan lapisan keamanan tambahan, melindungi terhadap serangan seperti cross-site scripting (XSS).

Penemuan Beban Kerja di UI web AWS dan komponen manajemen penyimpanan

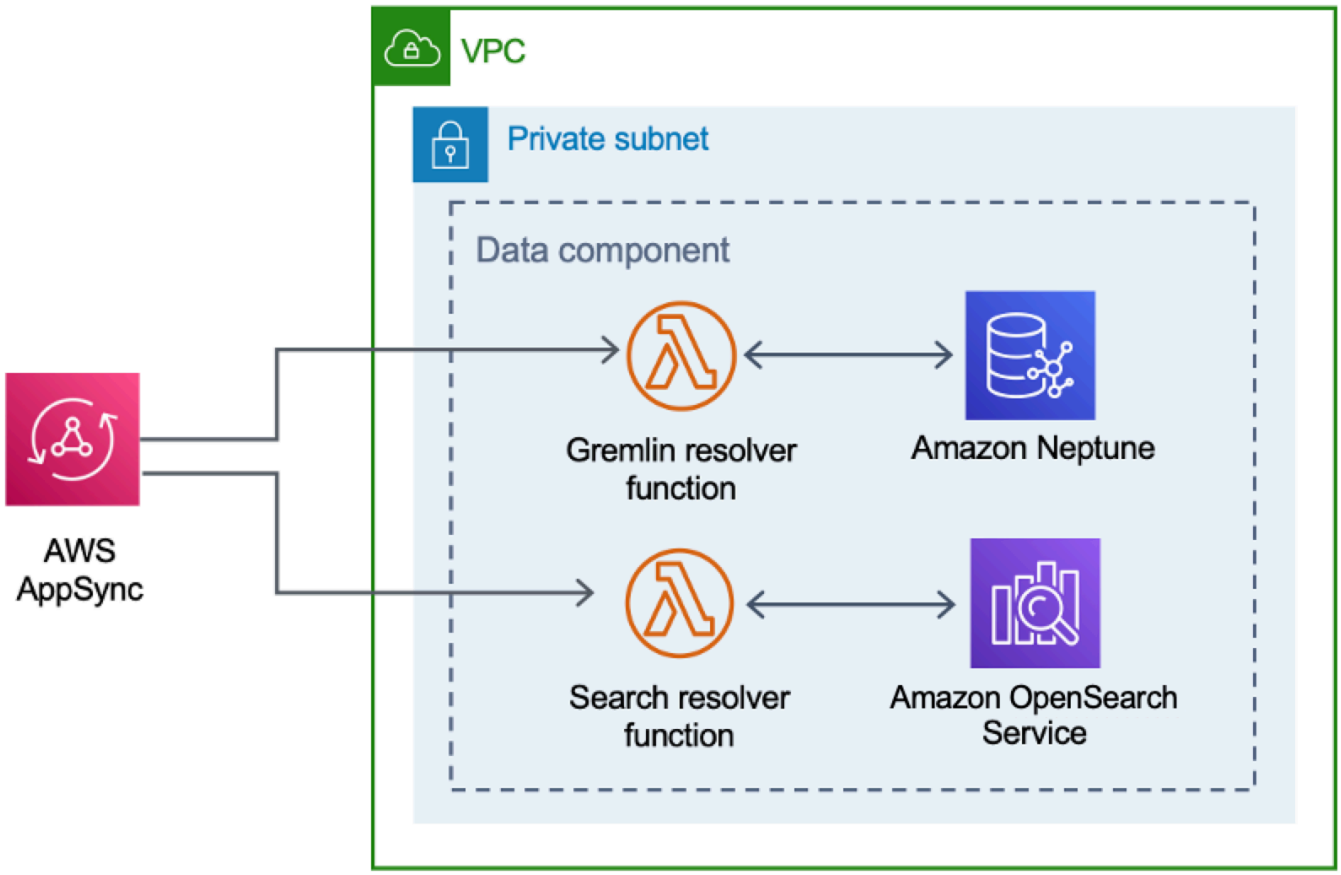



Sumber daya UI web di-host di bucket `WebUIBucket` Amazon S3 dan didistribusikan oleh Amazon. CloudFront AWS Amplify menyediakan lapisan abstraksi untuk menyederhanakan integrasi ke AWS dan Amazon S3. AppSync

Solusi ini menggunakan AWS AppSync untuk memfasilitasi interaksi dengan berbagai konfigurasi yang tersedia untuk Workload Discovery di AWS, termasuk mengelola Wilayah yang diimpor. AWS AppSync menggunakan fungsi `Settings` AWS Lambda untuk menangani permintaan seperti mengimpor akun atau Wilayah baru.

# Komponen data

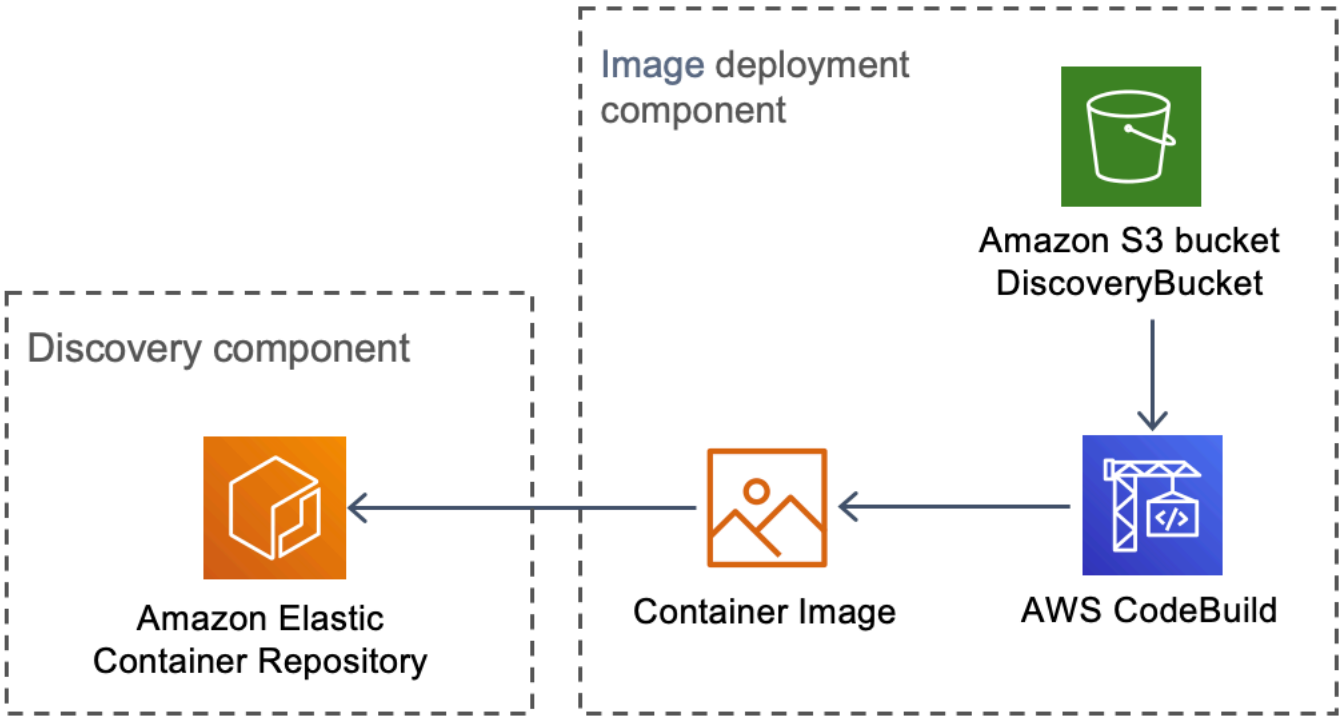
Penemuan Beban Kerja pada komponen data AWS




UI web mengirimkan permintaan ke AppSync API, yang memanggil fungsi `Gremlin Resolver` atau `Search Resolver` Lambda. Fungsi-fungsi ini memproses permintaan dan kueri Amazon Neptunus OpenSearch atau Layanan untuk mengambil data tentang sumber daya yang disediakan. AWS AppSync juga mendukung permintaan untuk data perkiraan biaya dari AWS CUR.

Komponen penemuan mengirimkan permintaan ke AppSync API untuk membaca dan menyimpan data di database Amazon OpenSearch Neptunus dan Layanan. API menerima permintaan dari tugas AWS Fargate dalam komponen penemuan. API kemudian diautentikasi menggunakan peran IAM yang menyediakan akses ke database.

# Komponen penyebaran gambar



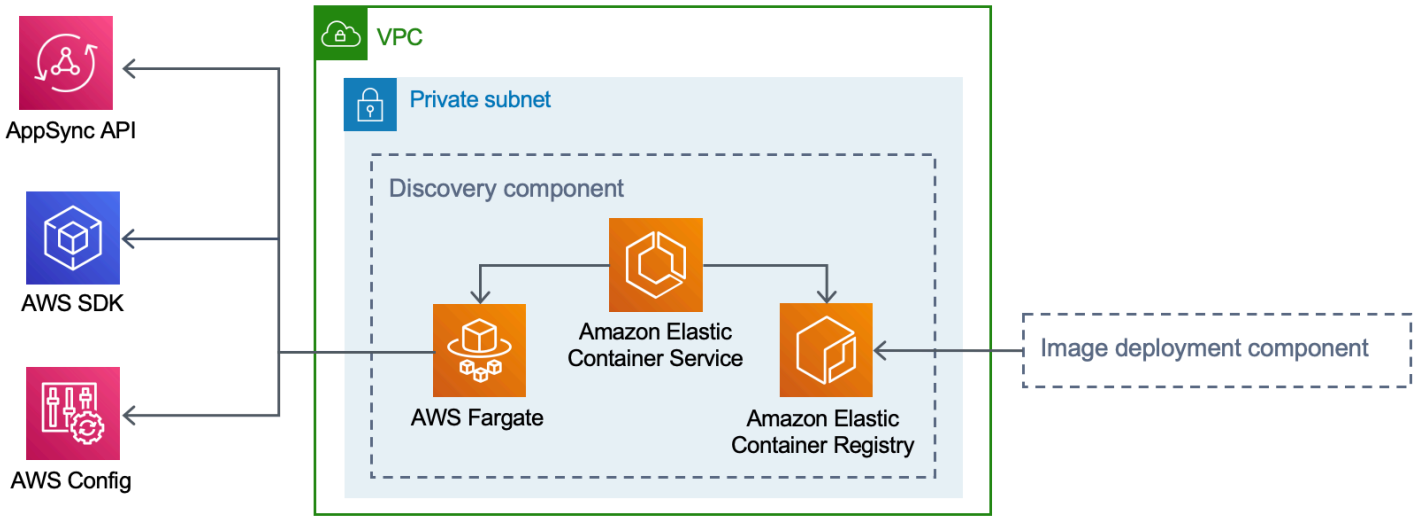

Penemuan Beban Kerja pada komponen penerapan gambar AWS

Komponen penerapan gambar membangun image kontainer yang digunakan komponen penemuan. Bucket Amazon S3 `DiscoveryBucket` dan Amazon S3 meng-host kode yang dapat diunduh pada saat penerapan oleh CodeBuild pekerjaan AWS yang membangun image kontainer dan mengunggahnya ke Amazon ECR.

# Komponen penemuan

Komponen penemuan adalah elemen pengumpulan data utama dari Workload Discovery pada arsitektur AWS. Ini bertanggung jawab untuk menanyakan AWS Config dan membuat panggilan API describe untuk memelihara inventaris sumber daya dan hubungannya antara satu sama lain.

Penemuan Beban Kerja pada komponen penemuan AWS



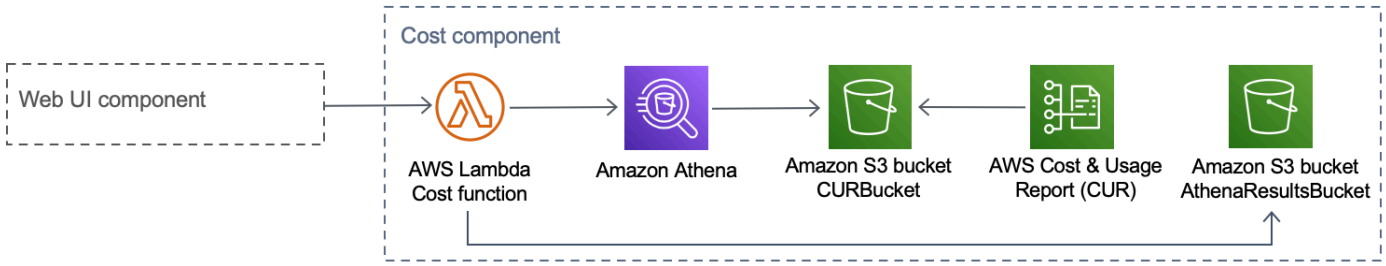

Solusi ini mengonfigurasi Amazon ECS untuk menjalankan tugas AWS Fargate menggunakan image container yang diunduh dari Amazon ECR. Tugas AWS Fargate dijadwalkan berjalan pada interval 15 menit. Data hubungan sumber daya yang dikumpulkan dimasukkan ke dalam database grafik Amazon Neptunus dan Layanan Amazon. OpenSearch

Alur kerja komponen penemuan terdiri dari tiga langkah berikut:

1. Amazon ECS memanggil tugas AWS Fargate dengan interval 15 menit.
2. Tugas Fargate mengumpulkan data sumber daya dari AWS Config, AWS API menjelaskan panggilan, dan dari database Amazon Neptunus.
3. Tugas Fargate menghitung perbedaan antara apa yang ada di database Amazon Neptunus dan apa yang diterimanya dari AWS Config dan panggilan deskripsikan.
4. Tugas Fargate mengirimkan permintaan ke AppSync API untuk mempertahankan perubahan sumber daya dan hubungan yang ditemukan ke Amazon Neptunus dan Amazon Service. OpenSearch

# Komponen biaya

Penemuan Beban Kerja pada komponen biaya AWS




Anda dapat membuat AWS CUR di AWS Billing and Cost Management dan Cost Management dan Cost Management. Ini menerbitkan file berformat Parket ke bucket Amazon S3`CostAndUsageReportBucket`. UI web membuat permintaan ke AppSync titik akhir AWS yang memanggil fungsi Cost Lambda. Fungsi ini mengirimkan kueri yang telah ditentukan sebelumnya ke Amazon Athena yang mengembalikan informasi perkiraan biaya dari AWS CUR.

Karena ukuran AWS CUR, respons dari Amazon Athena bisa sangat besar. Solusinya menyimpan hasilnya di bucket `AthenaResultsBucket` Amazon S3 dan memberi halaman hasilnya kembali ke UI web. Kebijakan siklus hidup yang dikonfigurasi pada bucket ini akan menghapus item yang berumur lebih dari tujuh hari.

## Layanan AWS dalam solusi ini

| AWS service | Deskripsi |
|---|---|
| AWS AppSync | Inti. Solusi ini digunakan AppSync untuk menyediakan API GraphQL tanpa server yang digunakan UI Web. |
| Amazon CloudFront | Inti. Solusi ini menggunakan CloudFront bucket Amazon S3 sebagai asalnya. Ini membatasi akses ke bucket Amazon S3 sehingga tidak dapat diakses publik dan mencegah akses langsung dari bucket. |
| AWS Config | Inti. Solusinya menggunakan AWS Config sebagai sumber data utama untuk sumber daya dan hubungan yang ditemukan solusi. |

| AWS service | Deskripsi |
| --- | --- |
| OpenSearch Layanan Amazon | Inti. Solusinya menggunakan OpenSearch Layanan Amazon untuk pemantauan aplikasi, analisis log, dan observabilitas. |
| Amazon DynamoDB | Inti. Solusi ini menggunakan DynamoDB untuk menyimpan data konfigurasi untuk solusinya. |
| Layanan Kontainer Elastis Amazon (ECS) | Inti. Solusi ini menggunakan Amazon ECS untuk mengatur menjalankan tugas yang menemukan sumber daya dan hubungan di akun AWS Anda. |
| AWS Fargate | Inti. Solusi ini menggunakan AWS Fargate di Amazon ECS sebagai lapisan komputasi untuk tugas penemuan. |
| AWS Lambda | Inti. Solusi ini menggunakan fungsi Lambda tanpa server, dengan runtime Node.js dan Python, untuk menangani panggilan API. |
| Amazon Neptune | Inti. Solusi ini menggunakan Neptunus sebagai datastore utama untuk sumber daya dan hubungan yang ditemukan solusi. |
| Layanan Penyimpanan Sederhana Amazon | Inti. Solusi ini menggunakan Amazon S3 untuk keperluan penyimpanan frontend dan backend. |
| Amazon CloudWatch | Mendukung. Solusi ini digunakan CloudWatch untuk mengumpulkan dan memvisualisasikan log waktu nyata, metrik, dan data peristiwa dalam kasus otomatis. Selain itu, Anda dapat memantau masalah penggunaan sumber daya dan kinerja solusi yang diterapkan. |

| AWS service | Deskripsi |
| --- | --- |
| AWS CodeBuild | Mendukung. Solusi ini digunakan CodeBuild untuk membangun wadah Docker yang berisi kode untuk tugas penemuan dan untuk menyebarkan aset untuk frontend ke Amazon S3. |
| Amazon Cognito | Mendukung. Solusi ini menggunakan kumpulan pengguna Cognito untuk mengautentikasi dan memberi wewenang kepada pengguna untuk mengakses UI web solusi. |
| AWS Systems Manager | Mendukung. Solusi ini menggunakan AWS Systems Manager untuk menyediakan pemantauan sumber daya tingkat aplikasi dan visualisasi operasi sumber daya dan data biaya. |
| Amazon Virtual Private Cloud | Mendukung. Solusi ini menggunakan VPC untuk meluncurkan Neptunus dan database di. OpenSearch |
| AWS WAF | Mendukung. Solusi ini menggunakan AWS WAF untuk melindungi AppSync API dari eksploitasi umum dan bot yang dapat memengaruhi ketersediaan, membahayakan keamanan, atau mengkonsumsi sumber daya yang berlebihan. |
| Amazon Athena | Opsional. Solusi ini menggunakan Athena untuk menanyakan Laporan Biaya dan Penggunaan jika fitur biaya diaktifkan. |

# Rencanakan penyebaran Anda

Bagian ini menjelaskan Wilayah, biaya, keamanan, dan pertimbangan lain sebelum menerapkan solusi.

## Wilayah AWS yang Didukung

Solusi ini menggunakan layanan Amazon Cognito, yang saat ini tidak tersedia di semua Wilayah AWS. Untuk ketersediaan terbaru layanan AWS menurut Wilayah, lihat Daftar Layanan Regional AWS.

Penemuan Beban Kerja di AWS tersedia di Wilayah AWS berikut:

| Nama wilayah | |
|---|---|
| AS Timur (Virginia Utara) | Kanada (Pusat) |
| AS Timur (Ohio) | Eropa (London) |
| AS Barat (Oregon) | Eropa (Frankfurt) |
| Asia Pasifik (Mumbai) | Eropa (Irlandia) |
| Asia Pasifik (Seoul) | Eropa (Paris) |
| Asia Pasifik (Singapura) | Eropa (Stockholm) |
| Asia Pasifik (Sydney) | Amerika Selatan (Sao Paulo) |
| Asia Pasifik (Tokyo) | |

Penemuan Beban Kerja di AWS tidak tersedia di Wilayah AWS berikut:

| Nama wilayah | Layanan Tidak Tersedia |
|---|---|
| AWS GovCloud (AS-Timur) | AWS AppSync |
| AWS GovCloud (AS-Barat) | AWS AppSync |

| Nama wilayah | Layanan Tidak Tersedia |
| --- | --- |
| Tiongkok (Beijing) | Amazon Cognito |
| Tiongkok (Ningxia) | Amazon Cognito |

# Biaya

Anda bertanggung jawab atas biaya layanan AWS yang disediakan saat menjalankan solusi ini. Pada revisi ini, biaya untuk menjalankan solusi ini menggunakan opsi penyebaran instance tunggal di Wilayah AS Timur (Virginia N.) adalah sekitar $0,58 per jam atau $425,19 per bulan.

> **Note**
>
> Biaya untuk menjalankan Workload Discovery di AWS di AWS Cloud bergantung pada konfigurasi penerapan yang Anda pilih. Contoh berikut memberikan rincian biaya untuk konfigurasi penerapan instance tunggal dan beberapa instance di Wilayah AS Timur (Virginia N.). Layanan AWS yang tercantum dalam contoh tabel di bawah ini ditagih setiap bulan.

Sebaiknya buat anggaran melalui AWS Cost Explorer untuk membantu mengelola biaya. Harga dapat berubah sewaktu-waktu. Untuk detail selengkapnya, lihat halaman web harga untuk setiap layanan AWS yang digunakan dalam solusi ini.

## Contoh tabel biaya

### Opsi 1: Penerapan instance tunggal (default)

Saat menerapkan solusi ini menggunakan CloudFormation templat AWS, modifikasi OpensearchMultiAzparameter untuk `No` menerapkan satu instance untuk domain OpenSearch Layanan, dan memodifikasi CreateNeptuneReplicaparameter untuk `No` menerapkan satu instance untuk penyimpanan data Neptunus. Opsi penerapan instans tunggal menimbulkan biaya yang lebih rendah, tetapi ini mengurangi ketersediaan Workload Discovery di AWS jika terjadi kegagalan Availability Zone.

| AWS service | Jenis instans | Biaya per jam [USD] | Biaya bulanan [USD] |
|---|---|---|---|
| Amazon Neptune | `db.r5.large` | $0,348 | $254,04 |
| OpenSearch Layanan Amazon | `m6g.large .search` | $0,18 | $93,44 |
| Amazon VPC (Gerbang NAT) | N/A | 0,090 USD | $65,7 |
| AWS Config | N/A | $0,003 per sumber daya | $0,003 per sumber daya |
| Amazon ECS (Tugas AWS Fargate) | N/A | $0,02 | $12,01 |
| Total | | $0,586 | $425,19 |

## Opsi 2: Penerapan beberapa instance

Saat menerapkan solusi ini menggunakan CloudFormation templat AWS, memodifikasi OpensearchMultiAzparameter untuk `Yes` menerapkan dua instance di dua Availability Zone untuk domain OpenSearch Layanan, dan memodifikasi CreateNeptuneReplicaparameter untuk `Yes` menerapkan dua instance di dua Availability Zone untuk penyimpanan data Neptunus. Opsi penerapan beberapa instans akan lebih mahal untuk dijalankan, tetapi ini meningkatkan ketersediaan Penemuan Beban Kerja di AWS jika terjadi kegagalan Availability Zone.

| AWS service | Jenis instans | Biaya per jam | Biaya bulanan [USD] |
|---|---|---|---|
| Amazon Neptune | `db.r5.large` | $0,696 | $508,08 |
| OpenSearch Layanan Amazon | `m6g.large .search` | $0,256 | $186,88 |
| Amazon VPC (Gerbang NAT) | N/A | 0,090 USD | $65,7 |

| AWS service | Jenis instans | Biaya per jam | Biaya bulanan [USD] |
|---|---|---|---|
| AWS Config | N/A | $0,003 per sumber daya | $0,003 per sumber daya |
| Amazon ECS (Tugas AWS Fargate) | N/A | $0,02 | $12,01 |
| Total | | $1,062 | $772,67 |

- Biaya akhir Anda bergantung pada jumlah sumber daya yang dideteksi AWS Config. $0,003 per item sumber daya yang direkam akan dikeluarkan selain jumlah yang disediakan dalam tabel.

> **Important**
>
> Biaya untuk Amazon Neptunus dan OpenSearch Amazon Service bervariasi, tergantung pada jenis instans yang Anda pilih.

# Keamanan

Saat Anda membangun sistem pada infrastruktur AWS, tanggung jawab keamanan dibagi antara Anda dan AWS. Model tanggung jawab bersama ini mengurangi beban operasional Anda karena AWS mengoperasikan, mengelola, dan mengontrol komponen termasuk sistem operasi host, lapisan virtualisasi, dan keamanan fisik fasilitas tempat layanan beroperasi. Untuk informasi selengkapnya tentang keamanan AWS, kunjungi Pusat Keamanan AWS.

## Akses sumber daya

### Peran IAM

Peran IAM memungkinkan pelanggan untuk menetapkan kebijakan akses terperinci dan izin ke layanan dan pengguna di AWS Cloud. Beberapa peran diperlukan untuk menjalankan Workload Discovery di AWS dan menemukan sumber daya di akun AWS.

### Amazon Cognito

Amazon Cognito digunakan untuk mengautentikasi akses dengan kredensyal yang berumur pendek dan kuat yang memberikan akses ke komponen yang dibutuhkan oleh Workload Discovery di AWS.

## Akses jaringan

### Amazon VPC

Workload Discovery di AWS diterapkan dalam VPC Amazon dan dikonfigurasi sesuai dengan praktik terbaik untuk memberikan keamanan dan ketersediaan tinggi. Untuk detail tambahan, lihat Praktik terbaik Keamanan untuk VPC Anda. Titik akhir VPC memungkinkan transit non-internet antar layanan dan dikonfigurasi jika tersedia.

Grup keamanan digunakan untuk mengontrol dan mengisolasi lalu lintas jaringan antara komponen yang diperlukan untuk menjalankan Workload Discovery di AWS.

Kami menyarankan Anda meninjau grup keamanan dan membatasi akses lebih lanjut sesuai kebutuhan setelah penerapan aktif dan berjalan.

### Amazon CloudFront

Solusi ini menerapkan UI konsol web yang dihosting di bucket Amazon S3 yang didistribusikan oleh Amazon. CloudFront Dengan menggunakan fitur identitas akses asal, konten bucket Amazon S3 ini hanya dapat diakses melalui. CloudFront Untuk informasi selengkapnya, lihat Membatasi akses ke asal Amazon S3 di Panduan Pengembang  CloudFront Amazon.

CloudFront mengaktifkan mitigasi keamanan tambahan untuk menambahkan header keamanan HTTP ke setiap respons penampil. Untuk detail tambahan, lihat Menambahkan atau menghapus header HTTP dalam CloudFront tanggapan.

Solusi ini menggunakan CloudFront sertifikat default yang memiliki protokol keamanan minimum yang didukung TLS v1.0. Untuk menegakkan penggunaan TLS v1.2 atau TLS v1.3, Anda harus menggunakan sertifikat SSL kustom alih-alih sertifikat default. CloudFront Untuk informasi lebih lanjut, lihat Bagaimana cara mengonfigurasi CloudFront distribusi saya untuk menggunakan sertifikat SSL/TLS.

## Konfigurasi aplikasi

### AWS AppSync

Penemuan Beban Kerja di AWS APIs GraphQL memiliki validasi permintaan yang disediakan oleh AWS AppSync sesuai dengan spesifikasi GraphQL. Selanjutnya, otentikasi dan otorisasi diimplementasikan menggunakan IAM dan Amazon Cognito, yang menggunakan JWT yang disediakan oleh Amazon Cognito ketika pengguna berhasil mengautentikasi di UI web.

### AWS Lambda

Secara default, fungsi Lambda dikonfigurasi dengan versi stabil terbaru dari runtime bahasa. Tidak ada data sensitif atau rahasia yang dicatat. Interaksi layanan dilakukan dengan hak istimewa yang paling tidak diperlukan. Peran yang menentukan hak istimewa ini tidak dibagi antar fungsi.

### OpenSearch Layanan Amazon

Domain OpenSearch Layanan Amazon dikonfigurasi dengan kebijakan akses yang membatasi akses untuk menghentikan permintaan yang tidak ditandatangani yang dibuat ke kluster Layanan. OpenSearch Ini terbatas pada satu fungsi Lambda.

Kluster OpenSearch Layanan dibangun dengan node-to-node enkripsi yang diaktifkan untuk menambahkan lapisan perlindungan data tambahan di atas fitur keamanan OpenSearch Layanan yang ada.

# Kuota

Service quotas, juga disebut batasan, adalah jumlah maksimum sumber daya layanan atau operasi untuk akun AWS Anda.

## Kuota untuk layanan AWS dalam solusi ini

Pastikan Anda memiliki kuota yang cukup untuk setiap layanan yang diterapkan dalam solusi ini. Untuk informasi lebih lanjut, lihat Service quotas AWS.

Gunakan tautan berikut untuk membuka halaman untuk layanan itu. Untuk melihat kuota layanan untuk semua layanan AWS dalam dokumentasi tanpa berpindah halaman, lihat informasi di titik akhir Layanan dan halaman kuota di PDF sebagai gantinya.

| | |
|---|---|
| Amplify | Amazon ECR |
| Athena | Lambda |
| CloudFront | OpenSearch Layanan |
| Cognito | Neptunus |
| Config | Amazon S3 |
| Amazon ECS | |

## CloudFormation Kuota AWS

Akun AWS Anda memiliki CloudFormation kuota AWS yang harus Anda ketahui saat meluncurkan tumpukan dalam solusi ini. Dengan memahami kuota ini, Anda dapat menghindari kesalahan pembatasan yang akan mencegah Anda menerapkan solusi ini dengan sukses. Untuk informasi selengkapnya, lihat CloudFormation kuota AWS di Panduan CloudFormation Pengguna AWS.

## Kuota AWS Lambda

Akun Anda memiliki kuota eksekusi bersamaan AWS Lambda sebesar 1000. Jika solusi digunakan di akun di mana ada beban kerja lain yang berjalan dan menggunakan Lambda, maka atur kuota ini ke nilai yang sesuai. Nilai ini dapat disesuaikan; untuk informasi selengkapnya, lihat kuota AWS Lambda di Panduan Pengguna AWS Lambda.

> **Note**
>
> Solusi ini membutuhkan 150 eksekusi dari kuota eksekusi bersamaan untuk tersedia di akun tempat solusi tersebut digunakan. Jika ada kurang dari 150 eksekusi yang tersedia di akun itu, CloudFormation penerapan akan gagal.

## Kuota Amazon VPC

Akun AWS Anda dapat berisi lima VPCs dan dua Elastic IPs (EIPs). Jika solusi digunakan di akun dengan yang lain VPCs atau EIPs, ini dapat mencegah Anda menerapkan solusi ini dengan sukses. Jika Anda berisiko mencapai kuota ini, Anda dapat memberikan VPC Anda sendiri untuk penerapan

dengan menyediakannya saat mengikuti langkah-langkah di bagian Luncurkan Tumpukan. Untuk informasi selengkapnya, lihat kuota Amazon VPC di Panduan Pengguna Amazon VPC.

## Memilih akun penerapan

Jika Anda menerapkan Workload Discovery di AWS ke AWS Organization, solusinya harus diinstal di akun admin yang didelegasikan tempat StackSetsdan kemampuan AWS Config Multi-wilayah telah diaktifkan.

Jika Anda tidak menggunakan AWS Organizations, sebaiknya Anda menerapkan Workload Discovery di AWS ke dalam akun AWS khusus yang dibuat khusus untuk solusi ini. Pendekatan ini berarti Workload Discovery di AWS diisolasi dari beban kerja Anda yang ada dan menyediakan satu lokasi untuk mengonfigurasi solusi, seperti menambahkan pengguna dan mengimpor Wilayah baru. Juga lebih mudah untuk melacak biaya yang dikeluarkan saat menjalankan solusi.

Setelah Workload Discovery di AWS diterapkan, Anda kemudian dapat mengimpor Wilayah dari akun apa pun yang telah Anda sediakan.

# Terapkan solusinya

Solusi ini menggunakan CloudFormation templat dan tumpukan AWS untuk mengotomatiskan penerapannya. CloudFormation Template menentukan sumber daya AWS yang disertakan dalam solusi ini dan propertinya. CloudFormation Tumpukan menyediakan sumber daya yang dijelaskan dalam template.

## Ikhtisar proses penyebaran

> **Note**
>
> Jika sebelumnya Anda menerapkan Workload Discovery di AWS dan ingin meningkatkan ke versi terbaru, lihat Perbarui solusinya.

Ikuti step-by-step petunjuk di bagian ini untuk mengonfigurasi dan menyebarkan solusi ke akun Anda.

Waktu untuk menyebarkan: Sekitar 30 menit

Sebelum Anda meluncurkan solusi, tinjau biaya, arsitektur, keamanan jaringan, dan pertimbangan lain yang dibahas dalam panduan ini.

> **Important**
>
> Solusi ini mencakup opsi untuk mengirim metrik operasional anonim ke AWS. Kami menggunakan data ini untuk lebih memahami bagaimana pelanggan menggunakan solusi ini dan layanan serta produk terkait. AWS memiliki data yang dikumpulkan melalui survei ini. Pengumpulan data tunduk pada Pemberitahuan Privasi AWS.

# Prasyarat

## Kumpulkan detail parameter penerapan

Sebelum menerapkan Workload Discovery di AWS, tinjau detail konfigurasi Anda untuk peran terkait OpenSearch layanan Amazon Service dan AWS Config.

## Verifikasi apakah Anda memiliki AWSService RoleForAmazonOpenSearchService peran

Penerapan membuat kluster OpenSearch Layanan Amazon di dalam Amazon Virtual Private Cloud (Amazon VPC). Template menggunakan peran terkait layanan untuk membuat kluster OpenSearch Service. Namun, jika Anda sudah memiliki peran yang dibuat di akun Anda, gunakan peran yang ada.

Untuk memeriksa apakah Anda sudah memiliki peran ini:

1. Masuk ke konsol Identity and Access Management (IAM) untuk akun yang Anda rencanakan untuk menerapkan solusi ini.
2. Di kotak Pencarian, masukkan`AWSServiceRoleForAmazonOpenSearchService`.
3. Jika pencarian Anda mengembalikan peran, pilih No CreateOpensearchServiceRoleparameter saat Anda meluncurkan tumpukan.

## Verifikasi AWS Config sudah disiapkan

Penemuan Beban Kerja di AWS menggunakan AWS Config untuk mengumpulkan sebagian besar konfigurasi sumber daya. Saat menerapkan solusi atau mengimpor Wilayah baru, Anda harus mengonfirmasi apakah AWS Config sudah disiapkan dan berfungsi seperti yang diharapkan. AlreadyHaveConfigSetup CloudFormation Parameter menginformasikan Workload Discovery di AWS apakah akan menyiapkan AWS Config.

Cuplikan berikut diambil dari AWS CLI Command Reference. Jalankan perintah di Wilayah yang ingin Anda gunakan Workload Discovery di AWS atau impor ke Workload Discovery di AWS.

Masukkan perintah berikut:

```
aws configservice get-status
```

Jika Anda menerima respons yang mirip dengan output, maka ada Perekam Konfigurasi dan Saluran Pengiriman yang berjalan di Wilayah itu. Pilih `Yes` untuk AlreadyHaveConfigSetup CloudFormation parameter.

Output:

```
Configuration Recorders:

name: default
```

```
recorder: ON
last status: SUCCESS

Delivery Channels:

name: default
last stream delivery status: SUCCESS
last history delivery status: SUCCESS
last snapshot delivery status: SUCCESS
```

Jika Anda mengonfigurasi AWS CloudFormation StackSets, maka Anda harus menyertakan Wilayah ini dalam kumpulan Wilayah yang sudah memiliki AWS Config yang dikonfigurasi.

### Verifikasi detail AWS Config Anda di akun Anda

Penerapan akan mencoba menyiapkan AWS Config. Jika Anda sudah menggunakan AWS Config di akun yang Anda rencanakan untuk diterapkan atau dibuat dapat ditemukan oleh Workload Discovery di AWS, pilih parameter yang relevan saat Anda menerapkan solusi ini. Selain itu, agar penerapan berhasil, pastikan Anda tidak membatasi sumber daya yang dipindai AWS Config.

Untuk memeriksa konfigurasi AWS Config Anda saat ini:

1. Masuk ke konsol AWS Config.
2. Pilih Pengaturan dan pastikan kotak Rekam semua sumber daya yang didukung di Wilayah ini dan Sertakan sumber daya global dipilih.

### Verifikasi konfigurasi VPC Anda

Jika menerapkan ke VPC yang ada, verifikasi subnet pribadi Anda dapat merutekan permintaan ke layanan AWS.

Jika Anda memilih opsi untuk menerapkan solusi di VPC yang ada, Anda harus memastikan bahwa Penemuan Beban Kerja pada AWS Lambda berfungsi dan tugas Amazon ECS yang berjalan di subnet pribadi VPC Anda dapat terhubung ke layanan AWS lainnya. Cara standar untuk mengaktifkan ini adalah dengan gateway NAT. Anda dapat mencantumkan gateway NAT di akun Anda seperti yang ditunjukkan pada contoh kode berikut.

```
aws ec2 describe-route-tables --filters Name=association.subnet-id,Values=<private-
subnet-id1>,<private-subnet-id2> --query 'RouteTables[].Routes[].NatGatewayId'
```

Output:

```
[
    "nat-1111111111111111",
    "nat-2222222222222222"
]
```

> **Note**
>
> Jika kurang dari dua hasil kembali, subnet tidak memiliki jumlah gateway NAT yang benar.

Jika VPC Anda tidak memiliki gateway NAT, Anda harus menyediakannya atau memastikan bahwa Anda memiliki titik akhir VPC untuk semua layanan AWS yang tercantum di bagian AWS. APIs

## CloudFormation Templat AWS

Solusi ini menggunakan AWS CloudFormation untuk mengotomatiskan penerapan Workload Discovery di AWS di AWS Cloud. Ini termasuk CloudFormation template berikut, yang dapat Anda unduh sebelum penerapan:

View template

workload-discovery-on-aws.template - Gunakan template ini untuk meluncurkan solusi dan semua komponen terkait. Konfigurasi default menerapkan solusi inti dan pendukung yang ditemukan di layanan AWS di bagian solusi ini, tetapi Anda dapat menyesuaikan template untuk memenuhi kebutuhan spesifik Anda.

> **Note**
>
> Anda dapat menyesuaikan template untuk memenuhi kebutuhan spesifik Anda; Namun, setiap perubahan yang Anda buat dapat memengaruhi proses peningkatan.

# Luncurkan tumpukan

CloudFormation Template AWS otomatis ini menerapkan Workload Discovery di AWS di AWS Cloud. Anda harus mengumpulkan detail parameter penerapan sebelum meluncurkan tumpukan. Untuk detailnya, lihat Prasyarat.

Waktu untuk menyebarkan: Sekitar 30 menit

1. Masuk ke AWS Management Console dan pilih tombol untuk meluncurkan CloudFormation template `workload-discovery-on-aws.template` AWS.


2. Template diluncurkan di Wilayah AS Timur (Virginia N.) secara default. Untuk meluncurkan solusi di Wilayah AWS yang berbeda, gunakan pemilih Wilayah di bilah navigasi konsol.

> **Note**
>
> Solusi ini menggunakan layanan yang tidak tersedia di semua Wilayah AWS. Lihat Wilayah AWS yang Didukung untuk daftar Wilayah AWS yang didukung.

3. Pada halaman Buat tumpukan, verifikasi bahwa URL templat yang benar ada di kotak teks URL Amazon S3, dan pilih Berikutnya.
4. Pada halaman Tentukan detail tumpukan, tetapkan nama ke tumpukan solusi Anda. Untuk informasi tentang batasan penamaan karakter, lihat kuota IAM dan AWS STS di Panduan Pengguna AWS Identity and Access Management.
5. Di bawah Parameter, tinjau parameter untuk templat solusi ini dan modifikasi sesuai kebutuhan. Solusi ini menggunakan nilai default berikut.

| Parameter | Default | Deskripsi |
| --- | --- | --- |
| AdminUserEmailAddress | *<Requires input>* | Alamat email untuk membuat pengguna pertama. Kredensi sementara akan dikirim ke alamat email ini. |

| Parameter | Default | Deskripsi |
| --- | --- | --- |
| AlreadyHaveConfigSetup | `No` | Konfirmasi apakah Anda sudah menyiapkan AWS Config di akun penerapan atau belum. Untuk detailnya, lihat Prasyarat. |
| AthenaWorkgroup | `primary` | Workgroup yang akan digunakan untuk mengeluar kan kueri Athena saat fitur Cost diaktifkan. |
| ApiAllowListedRanges | `0.0.0.0/1,128.0.0.0/1` | Daftar dipisahkan koma CIDRs untuk mengelola akses ke AppSync GraphQL API. Untuk mengizinkan seluruh internet, gunakan 0.0.0.0/1,128.0.0.0/1. Jika membatasi akses ke spesifik CIDRs, Anda juga harus menyertakan alamat IP (dan subnet mask dari/32) dari gateway NAT yang memungkinkan tugas ECS proses penemuan berjalan di subnet pribadiny a untuk mengakses internet. CATATAN: Daftar izin ini tidak mengatur akses ke WebUI, hanya GraphQL API. |

| Parameter | Default | Deskripsi |
| --- | --- | --- |
| CreateNeptuneReplica | No | Pilih apakah akan membuat replika baca untuk Neptunus di Availability Zone terpisah. Memilih Yes meningkatkan ketahanan tetapi meningkatkan biaya solusi ini. |
| CreateOpenSearchServiceRole | Yes | Konfirmasi apakah Anda sudah memiliki peran terkait layanan untuk Layanan Amazon OpenSearch atau belum. Untuk detailnya, lihat Prasyarat. |
| NeptuneInstanceClass | db.r5.large | Jenis instans yang digunakan untuk meng-host database Amazon Neptunus. Apa yang Anda pilih di sini memengaruhi biaya menjalankan solusi ini. |
| OpensearchInstanceType | m6g.large.search | Jenis instans yang digunakan untuk node data OpenSearch Service Anda. Pilihan Anda memengaruhi biaya menjalankan solusi. |
| OpensearchMultiAz | No | Pilih apakah akan membuat kluster OpenSearch Layanan yang mencakup beberapa Availability Zone. Memilih Yes meningkatkan ketahanan tetapi meningkatkan biaya solusi ini. |

| Parameter | Default | Deskripsi |
| --- | --- | --- |
| CrossAccountDiscovery | `SELF_MANAGED` | Pilih apakah Workload Discovery di AWS atau AWS Organizations mengelola pengimporan akun. Nilai dapat berupa `SELF_MANAGED` atau `AWS_ORGANIZATIONS`. |
| OrganizationUnitId | <Optional input> | ID unit organisasi root. Parameter ini hanya digunakan ketika CrossAccountDiscoverydiatur ke`AWS_ORGANIZATIONS`. |
| AccountType | `DELEGATED_ADMIN` | Jenis akun AWS Organizations untuk menginstal Workload Discovery di AWS di. Parameter ini hanya digunakan ketika CrossAccountDiscoverydiatur ke`AWS_ORGANIZATIONS`. Untuk detailnya, lihat Memilih akun penerapan. |

| Parameter | Default | Deskripsi |
| --- | --- | --- |
| ConfigAggregatorName | <Optional input> | Agregator AWS Organizat ion-wide Config untuk digunakan. Anda harus menginstal solusi di akun dan Wilayah yang sama dengan agregator ini. Jika Anda membiarkan parameter ini kosong, agregator baru akan dibuat. Parameter ini hanya digunakan ketika CrossAccountDiscoverydiatur keAWS;_ORGANIZATIONS . |
| CpuUnits | 1 vCPU | Jumlah yang CPUs dialokasi kan untuk tugas Fargate tempat proses penemuan berjalan. |
| Memori | 2048 | Jumlah memori yang dialokasikan untuk tugas Fargate tempat proses penemuan berjalan. |
| DiscoveryTaskFrequency | 15mins | Interval waktu antara setiap proses penemuan tugas ECS. |

| Parameter | Default | Deskripsi |
| --- | --- | --- |
| Min NCUs | 1 | Unit Kapasitas Neptunus Minimum NCUs () yang akan ditetapkan pada cluster Neptunus (harus kurang dari atau sama dengan Max). NCUs Diperlukan jika DBInstance jenisnya`db.serverless` . |
| Maks NCUs | 128 | Maksimum NCUs yang akan ditetapkan pada gugus Neptunus (harus lebih besar dari atau sama dengan Min). NCUs Diperlukan jika DBInstance jenisnya`db.serverless` . |
| VpcId | <Optional input> | ID VPC yang ada untuk solusi yang akan digunakan. Jika Anda membiarkan parameter ini kosong, VPC baru akan disediakan. |
| VpcCidrBlock | <Optional input> | Blok VPC CIDR dari VPC direferensikan oleh parameter . VpcId Parameter ini hanya digunakan jika VpcIdparameter diatur. |
| PrivateSubnet0 | <Optional input> | Subnet pribadi yang ingin Anda gunakan. Parameter ini hanya digunakan jika VpcIdparameter diatur. |

| Parameter | Default | Deskripsi |
| --- | --- | --- |
| PrivateSubnet1 | <Optional input> | Subnet pribadi yang ingin Anda gunakan. Parameter ini hanya digunakan jika VpcIdparameter diatur. |
| UsesCustomIdentity | No | Konfirmasi apakah Anda tidak akan menggunakan penyedia identitas khusus, seperti SAMP atau OIDC. |
| CognitoCustomDomain | <Optional input> | Awalan domain untuk domain kustom Amazon Cognito yang menghosting halaman pendaftaran dan login untuk aplikasi Anda. Biarkan kosong jika Anda tidak menggunakan iDP kustom, jika tidak harus menyertakan hanya huruf kecil, angka, dan tanda hubung. |
| CognitoAttributeMapping | <Optional input> | Pemetaan atribut iDP ke atribut kumpulan pengguna Cognito standar dan kustom. Biarkan kosong jika Anda tidak menggunakan iDP kustom, jika tidak harus string JSON yang valid. |
| IdentityType | <Optional input> | Jenis Penyedia Identitas yang akan digunakan (`Google`,`SAML`, atau`OIDC`). Biarkan kosong jika Anda tidak menggunakan iDP kustom. |

| Parameter | Default | Deskripsi |
| --- | --- | --- |
| ProviderName | <Optional input> | Nama untuk Penyedia Identitas. Biarkan kosong jika Anda tidak menggunakan iDP kustom. |
| GoogleClientId | <Optional input> | ID Klien Google yang akan digunakan. Parameter hanya digunakan ketika IdentityT ypediatur ke`Google`. |
| GoogleClientSecret | <Optional input> | Rahasia klien Google untuk digunakan. Parameter hanya digunakan ketika IdentityT ypediatur ke`Google`. |
| SAMLMetadataURL | <Optional input> | URL metadata untuk Penyedia Identitas SAMP. Parameter hanya digunakan ketika IdentityTypediatur ke SAMP. |
| OIDCClientId | <Optional input> | ID klien OIDC untuk digunakan. Parameter hanya digunakan ketika IdentityT ypediatur ke`OIDC`. |
| OIDCClientRahasia | <Optional input> | Rahasia klien OIDC untuk digunakan. Parameter hanya digunakan ketika IdentityT ypediatur ke`OIDC`. |
| OIDCIssuerURL | <Optional input> | URL penerbit OIDC untuk digunakan. Parameter hanya digunakan ketika IdentityT ypediatur ke`OIDC`. |

| Parameter | Default | Deskripsi |
| --- | --- | --- |
| OIDCAttributeRequestMethod | `GET` | Metode permintaan atribut OIDC untuk digunakan. Harus salah satu `GET` atau `POST` (lihat penyedia OIDC atau gunakan nilai default). Parameter hanya digunakan ketika IdentityTypediatur ke`OIDC`. |

6. Pilih Berikutnya.
7. Pada halaman Konfigurasikan opsi tumpukan, pilih Berikutnya.
8. Pada halaman Tinjau dan buat, tinjau dan konfirmasikan pengaturan. Pilih kotak yang mengakui bahwa template membuat sumber daya IAM dan memerlukan kemampuan tertentu.
9. Pilih Kirim untuk menyebarkan tumpukan.

   Anda dapat melihat status tumpukan di AWS CloudFormation Console di kolom Status. Anda akan menerima status CREATE_COMPLETE dalam waktu sekitar 30 menit.

> **Note**
>
> Jika dihapus, tumpukan ini menghapus semua sumber daya. Jika tumpukan diperbarui, ia mempertahankan kumpulan pengguna Amazon Cognito untuk memastikan bahwa pengguna yang dikonfigurasi tidak hilang.

# Tugas konfigurasi pasca-penerapan

Setelah Workload Discovery di AWS berhasil diterapkan, selesaikan tugas konfigurasi pasca-penerapan berikut.

## Aktifkan keamanan tingkat lanjut di Amazon Cognito

Untuk mengaktifkan fitur keamanan lanjutan untuk Amazon Cognito, ikuti petunjuk tentang Menambahkan keamanan lanjutan ke kumpulan pengguna di Panduan Pengembang Amazon Cognito.

> **Note**
>
> Ada biaya tambahan untuk mengaktifkan keamanan tingkat lanjut di Amazon Cognito.

## Buat pengguna Amazon Cognito

Workload Discovery di AWS menggunakan Amazon Cognito untuk mengelola semua pengguna dan otentikasi. Ini menciptakan pengguna untuk Anda selama penyebaran dan mengirim email di alamat yang disediakan dalam AdminUserEmailAddress parameter dengan kredensi sementara.

### Untuk membuat pengguna tambahan:

1. Masuk ke konsol AWS Cognito.
2. Pilih Kelola Kolam Pengguna.
3. Pilih WDCognitoUserPool-*<ID-string>*.
4. Di panel navigasi, di bawah Pengaturan Umum, pilih Pengguna dan grup.
5. Pada tab Pengguna, pilih Buat pengguna.
6. Pada kotak Buat pengguna, masukkan nilai untuk semua bidang wajib.

| Bidang Formulir | Wajib? | Deskripsi |
| --- | --- | --- |
| nama pengguna | Ya | Nama pengguna yang akan Anda gunakan untuk masuk |

| Bidang Formulir | Wajib? | Deskripsi |
| --- | --- | --- |
| | | ke Workload Discovery di AWS. |
| Kirim undangan | Ya (hanya email) | Saat dipilih, kirim pemberita huan sebagai pengingat kata sandi sementara. Pilih Email saja. Jika Anda memilih SMS (default), pesan kesalahan ditampilkan, tetapi pengguna masih dibuat. |
| Kata Sandi Sementara | Ya | Masukkan kata sandi sementara. Pengguna dipaksa untuk mengubah ini saat mereka masuk ke Workload Discovery di AWS untuk pertama kalinya. |
| Nomor Telepon | Tidak | Masukkan nomor telepon dalam format internasional, misalnya,\+44. Pastikan nomor telepon Tandai sebagai terverifikasi? kotak dipilih. |
| Email | Ya | Masukkan alamat email yang valid. Pastikan bahwa email Tandai sebagai terverifikasi? kotak dipilih. |

7. Pilih Create user (Buat pengguna).

Ulangi proses ini untuk membuat pengguna sebanyak yang Anda butuhkan.

> **Note**
>
> Setiap pengguna akan memiliki tingkat akses yang sama ke sumber daya yang ditemukan. Kami merekomendasikan penyediaan penerapan terpisah Workload Discovery di AWS untuk akun yang berisi beban kerja atau data sensitif. Ini memungkinkan Anda untuk membatasi akses hanya ke pengguna yang membutuhkannya.

## Masuk ke Workload Discovery di AWS

Setelah solusi berhasil diterapkan, tentukan URL untuk CloudFront distribusi Amazon yang melayani UI web solusi.

1. Masuk ke CloudFormation konsol AWS.
2. Pilih Lihat bersarang untuk menampilkan tumpukan bersarang yang membentuk penerapan. Bergantung pada preferensi Anda, tumpukan bersarang mungkin sudah ditampilkan.
3. Pilih Workload Discovery utama di AWS stack.
4. Pilih tab Output dan pilih URL di kolom Nilai yang terkait dengan WebUiUrlkunci.
5. Pada layar Masuk ke, masukkan kredenal masuk yang Anda terima melalui email. Kemudian lakukan tindakan berikut:
   a. Ikuti petunjuk untuk mengubah kata sandi Anda.
   b. Gunakan kode verifikasi yang dikirim ke email Anda untuk menyelesaikan pemulihan akun.

## Impor Wilayah

> **Note**
>
> Bagian berikut hanya berlaku jika mode penemuan akun solusi dikelola sendiri. Untuk informasi tentang cara kerja penemuan akun dalam mode AWS Organizations, lihat bagian Mode Penemuan Akun AWS Organizations.

Mengimpor Wilayah membutuhkan infrastruktur tertentu untuk dikerahkan. Infrastruktur ini terdiri dari sumber daya Global dan Regional:

Global — Sumber daya yang digunakan sekali dalam akun dan digunakan kembali untuk setiap Wilayah yang diimpor.

- Peran IAM () WorkloadDiscoveryRole

Regional — Sumber daya yang digunakan di setiap Wilayah yang diimpor.

- Saluran Pengiriman AWS Config
- Bucket Amazon S3 untuk AWS Config
- Peran IAM () ConfigRole

Ada dua opsi untuk menerapkan infrastruktur ini:

- AWS CloudFormation StackSets (disarankan)
- AWS CloudFormation

## Impor Wilayah

Langkah-langkah ini memandu Anda dalam mengimpor Wilayah dan menerapkan templat CloudFormation AWS.

1. Masuk ke Workload Discovery di AWS. Lihat Masuk ke Workload Discovery di AWS untuk URL.
2. Di menu navigasi, pilih Akun.
3. Pilih Impor.
4. Pilih metode impor:
   a. Tambahkan Akun & Wilayah menggunakan file CSV.
   b. Tambahkan Akun & Wilayah menggunakan formulir.

### File CSV

Berikan file Comma Separated Value (CSV) yang berisi Wilayah yang akan diimpor dalam format berikut.

```
"accountId","accountName","region"
123456789012,"test-account-1",eu-west-2
123456789013,"test-account-2",eu-west-1
```

```
123456789013,"test-account-2",eu-west-2
123456789014,"test-account-3",eu-west-3
```

1. Pilih Unggah CSV.
2. Temukan dan buka file CSV Anda.
3. Tinjau tabel Regions, lalu pilih Impor.
4. Dalam dialog modal, unduh templat sumber daya global dan templat Sumber Daya Regional.
5. Terapkan CloudFormation templat di akun yang relevan (lihat bagian Menerapkan CloudFormation templat AWS).
6. Setelah templat sumber daya global dan regional telah digunakan, pilih kedua kotak untuk mengonfirmasi bahwa penginstalan selesai dan pilih Impor.

### Formulir

Berikan Wilayah untuk diimpor menggunakan formulir:

1. Untuk ID Akun, masukkan ID akun 12 digit atau pilih ID akun yang ada.
2. Untuk nama Akun, masukkan nama akun atau gunakan nilai yang telah diisi sebelumnya saat memilih ID akun yang ada.
3. Pilih Wilayah yang akan diimpor.
4. Pilih Tambahkan untuk mengisi Wilayah pada tabel Wilayah di bawah ini.
5. Tinjau tabel Regions, lalu pilih Impor.
6. Dalam dialog modal, unduh templat sumber daya global dan templat Sumber Daya Regional.
7. Terapkan CloudFormation templat di akun yang relevan (lihat bagian Menerapkan CloudFormation templat AWS).
8. Setelah templat sumber daya global dan regional telah digunakan, pilih kedua kotak untuk mengonfirmasi penginstalan selesai dan pilih Impor.

## Menerapkan templat AWS CloudFormation

Sumber daya global harus digunakan sekali per akun. Jangan gunakan templat ini saat mengimpor Wilayah dari akun yang berisi Wilayah yang sudah diimpor ke Workload Discovery di AWS. Jika Wilayah telah diimpor, ikuti petunjuk di Menyebarkan tumpukan untuk menyediakan sumber daya Regional.

# Gunakan CloudFormation StackSets untuk menyediakan sumber daya Global di seluruh akun

> **Important**
>
> Pertama, selesaikan Prasyarat untuk operasi set tumpukan untuk diaktifkan StackSets di akun target Anda.

1. Di akun administrator, masuk ke CloudFormation konsol AWS.
2. Dari menu navigasi, pilih StackSets.
3. Pilih Buat StackSet.
4. Pada halaman Pilih templat, di bawah Izin:
   a. Jika Anda menggunakan AWS Organizations, pilih izin terkelola Layanan atau izin layanan Mandiri. Untuk detailnya, lihat Menggunakan StackSets di Organisasi AWS.
   b. Jika Anda tidak menggunakan AWS Organizations, masukkan nama peran jalankan IAM yang digunakan saat mengikuti langkah-langkah StackSets prasyarat. Untuk detailnya, lihat Berikan izin yang dikelola sendiri.
5. Di bawah Tentukan templat, pilih Unggah file templat. Pilih `global-resources.template` file (diunduh sebelumnya saat Anda mengimpor Region baik dengan file CSV atau formulir), dan pilih Berikutnya.
6. Pada halaman Tentukan StackSet detail, tetapkan nama untuk Anda StackSet. Untuk informasi tentang batasan penamaan karakter, lihat kuota IAM dan AWS STS di Panduan Pengguna AWS Identity and Access Management.
7. Di bawah Parameter, tinjau parameter untuk templat solusi ini dan modifikasi sesuai kebutuhan. Solusi ini menggunakan nilai default berikut.

| Nama Bidang | Default | Deskripsi |
| --- | --- | --- |
| AccountId | ID akun penerapan | ID akun dari akun penerapan asli. Anda harus meninggalkan nilai ini sebagai default. |

1. Pilih Berikutnya.
2. Pada halaman Configure StackSet options, pilih Next.
3. Pada halaman Setel opsi penyebaran, di bawah Akun, masukkan akun IDs untuk menerapkan peran akun di kotak Nomor akun.
4. Di bawah Tentukan wilayah, pilih Wilayah untuk menginstal tumpukan.
5. Di bawah Opsi penyebaran, pilih Paralel, lalu pilih Berikutnya.
6. Pada halaman Tinjauan, centang kotak yang mengakui bahwa AWS CloudFormation mungkin membuat sumber daya IAM dengan nama khusus.
7. Pilih Kirim.

## Gunakan CloudFormation StackSets untuk menyediakan sumber daya Regional

> **Important**
>
> Pertama, selesaikan Prasyarat untuk operasi set tumpukan untuk diaktifkan StackSets di akun target Anda.
> Jika Anda memiliki beberapa Wilayah dengan AWS Config yang diinstal dan beberapa tanpa, Anda harus melakukan dua StackSet operasi, satu untuk Wilayah dengan AWS Config diinstal dan satu untuk yang tidak.

1. Di akun administrator, masuk ke CloudFormation konsol AWS.
2. Dari menu navigasi, pilih StackSets.
3. Pilih Buat StackSet.
4. Pada halaman Pilih templat, di bawah Izin:
   a. Jika Anda menggunakan AWS Organizations, pilih izin terkelola Layanan atau izin layanan Mandiri. Untuk detailnya, lihat Menggunakan StackSets di Organisasi AWS.
   b. Jika Anda tidak menggunakan AWS Organizations, masukkan nama peran jalankan IAM yang digunakan saat mengikuti langkah-langkah StackSets prasyarat. Untuk detailnya, lihat Berikan izin yang dikelola sendiri.
5. Di bawah Tentukan templat, pilih Unggah file templat. Pilih `regional-resources.template` file (diunduh sebelumnya saat Anda mengimpor Region baik dengan file CSV atau formulir), dan pilih Berikutnya.

6. Pada halaman Tentukan StackSet detail, tetapkan nama untuk Anda StackSet. Untuk informasi tentang batasan penamaan karakter, lihat kuota IAM dan AWS STS di Panduan Pengguna AWS Identity and Access Management.
7. Di bawah Parameter, tinjau parameter untuk templat solusi ini dan modifikasi sesuai kebutuhan. Solusi ini menggunakan nilai default berikut.

| Nama Bidang | Default | Deskripsi |
| --- | --- | --- |
| AccountId | ID akun penerapan | ID akun dari akun penerapan asli. Anda harus meninggalkan nilai ini sebagai default. |
| AggregationRegion | Wilayah penyebaran | Wilayah yang awalnya dikerahkan ke. Anda harus meninggalkan nilai ini sebagai default. |
| AlreadyHaveConfigSetup | `No` | Konfirmasi apakah Wilayah sudah menginstal AWS Config. Setel ke Ya jika AWS Config sudah diinstal di Wilayah ini. |

1. Pilih Berikutnya.
2. Pada halaman Configure StackSet options, pilih Next.
3. Pada halaman Setel opsi penyebaran, di bawah Akun, masukkan akun IDs untuk menerapkan peran akun di kotak Nomor akun.
4. Di bawah Tentukan wilayah, pilih Wilayah untuk menginstal tumpukan. Ini menginstal tumpukan di Wilayah ini di semua akun yang dimasukkan pada langkah 6.
5. Di bawah Opsi penyebaran, pilih Paralel, lalu pilih Berikutnya.
6. Pada halaman Tinjauan, centang kotak yang mengakui bahwa AWS CloudFormation mungkin membuat sumber daya IAM dengan nama khusus.
7. Pilih Kirim.

# Menyebarkan tumpukan untuk menyediakan sumber daya Global menggunakan CloudFormation

Sumber daya global harus digunakan sekali per akun. Jangan gunakan templat ini saat mengimpor Wilayah dari akun yang berisi Wilayah yang sudah diimpor ke Workload Discovery di AWS.

1. Masuk ke _CloudFormation konsol AWS.
2. Pilih Buat tumpukan, lalu pilih Dengan sumber daya baru (standar).
3. Pada halaman Buat tumpukan, di bagian Tentukan templat, pilih Unggah file templat.
4. Pilih Pilih file dan pilih `global-resources.template` file yang (diunduh lebih awal saat Anda mengimpor Wilayah baik dengan file atau formulir CSV), dan pilih Berikutnya.
5. Pada halaman Tentukan detail tumpukan, tetapkan nama ke tumpukan solusi Anda. Untuk informasi tentang batasan penamaan karakter, lihat kuota IAM dan AWS STS di _AWS Identity and Access Management _User Guide.
6. Di bawah Parameter, tinjau parameter untuk templat solusi ini dan modifikasi sesuai kebutuhan. Solusi ini menggunakan nilai default berikut.

| Nama Bidang | Default | Deskripsi |
|---|---|---|
| Nama tumpukan | `workload-discovery` | Nama CloudFormation tumpukan AWS ini. |
| AccountId | ID akun penerapan | ID akun dari akun penerapan asli. Anda harus meninggalkan nilai ini sebagai default. |

1. Pilih Berikutnya.
2. Pilih kotak yang mengakui bahwa AWS CloudFormation mungkin membuat sumber daya IAM dengan nama khusus.
3. Pilih Buat tumpukan.

Wilayah baru akan dipindai selama proses penemuan berikutnya, yang berjalan pada interval 15 menit, misalnya: 15:00, 15:15, 15:30, 15:45.

# Menyebarkan tumpukan untuk menyediakan sumber daya Regional menggunakan CloudFormation

1. Masuk ke CloudFormation konsol AWS.
2. Pilih Buat tumpukan, lalu pilih Dengan sumber daya baru (standar).
3. Pada halaman Buat tumpukan, di bagian Tentukan templat, pilih Unggah file templat.
4. Pilih Pilih file dan pilih `regional-resources.template` file (diunduh lebih awal saat Anda mengimpor Wilayah baik dengan file atau formulir CSV), dan pilih Berikutnya.
5. Pada halaman Tentukan detail tumpukan, tetapkan nama ke tumpukan solusi Anda. Untuk informasi tentang batasan penamaan karakter, lihat kuota IAM dan AWS STS di Panduan Pengguna AWS Identity and Access Management.
6. Di bawah Parameter, tinjau parameter untuk templat solusi ini dan modifikasi sesuai kebutuhan. Solusi ini menggunakan nilai default berikut.

| Nama Bidang | Default | Deskripsi |
|---|---|---|
| AccountId | ID akun penerapan solusi | ID akun dari akun penerapan asli. Harus dibiarkan sebagai default. |
| AggregationRegion | Wilayah penyebaran solusi | Wilayah yang awalnya dikerahkan ke. Harus dibiarkan sebagai default. |
| AlreadyHaveConfigSetup | No | Konfirmasi apakah Wilayah sudah menginstal AWS Config. Setel ke Yes jika AWS Config sudah diinstal di Wilayah ini. |

1. Pilih Berikutnya.
2. Pilih kotak yang mengakui bahwa AWS CloudFormation mungkin membuat sumber daya IAM dengan nama khusus.
3. Pilih Buat tumpukan.

Wilayah baru akan dipindai selama proses penemuan berikutnya, yang berjalan pada interval 15 menit, misalnya, 15:00, 15:15, 15:30, 15:45.

### Verifikasi Wilayah telah diimpor dengan benar

1. Masuk ke UI web solusi (atau segarkan halaman jika sudah dimuat). Lihat Masuk ke Workload Discovery di AWS untuk URL.
2. Dari panel navigasi kiri, di bawah Pengaturan, pilih Wilayah yang Diimpor.

Wilayah, nama akun, dan ID akun muncul di tabel. Kolom Terakhir Dipindai menunjukkan sumber daya terakhir yang ditemukan di Wilayah itu.

> **Note**
>
> Jika kolom Last Scanned tetap kosong selama lebih dari 30 menit, lihat Debugging komponen penemuan.

## Siapkan fitur biaya

Fitur biaya memerlukan penyiapan laporan Biaya dan Penggunaan AWS (CUR) secara manual. Mengikuti instruksi di bawah ini Anda akan:

1. Siapkan CUR terjadwal.
2. Siapkan replikasi Amazon S3 (saat CURs berada di luar akun penerapan)

### Membuat Laporan Biaya dan Penggunaan AWS di akun penerapan

1. Masuk ke konsol Penagihan akun tempat Anda ingin mengumpulkan data biaya.
2. Di menu navigasi, di bawah Penagihan, pilih Laporan biaya & penggunaan.
3. Pilih Buat Laporan.
4. Gunakan `workload-discovery-cost-and-usage-` *`<your-workload-discovery-deployment-account-ID>`* sebagai nama laporan.

> **Note**
>
> Anda harus mengikuti konvensi penamaan ini karena sejumlah kecil infrastruktur akan digunakan untuk memfasilitasi kueri. CURs

5. Pilih IDs kotak Sertakan sumber daya.

> **Note**
>
> Anda harus memilih IDs kotak Sertakan sumber daya untuk melihat data biaya. ID ini harus sesuai dengan sumber daya yang ditemukan oleh Workload Discovery di AWS.

6. Pilih Berikutnya.
7. Pada halaman Opsi pengiriman, pilih Konfigurasi 0
8. Pilih bucket *<stack-name>* `-s3buc-costandusagereportbucket-` *<ID-string>* Amazon S3 untuk menyimpan CUR. Pilih Berikutnya.
9. Tinjau kebijakan, pilih kotak konfirmasi, dan pilih Simpan.
10. Setel jalur awalan Laporan ke`aws-perspective`.
11. Pilih Harian untuk perincian waktu.
12. Di bawah Aktifkan integrasi data laporan untuk, pilih Amazon Athena.
13. Pilih Berikutnya.
14. Pilih Review dan Selesaikan.

Untuk memverifikasi bahwa laporan telah diatur dengan benar, periksa bucket Amazon S3 untuk file pengujian.

> **Note**
>
> Diperlukan waktu hingga 24 jam untuk laporan diunggah ke bucket Anda.

## Membuat Laporan Biaya dan Penggunaan AWS di akun eksternal

1. Masuk ke konsol Penagihan akun tempat Anda ingin mengumpulkan data biaya.

2. Di menu navigasi, di bawah Manajemen Biaya, pilih Laporan biaya & penggunaan.
3. Pilih Buat Laporan.
4. Gunakan `workload-discovery-cost-and-usage-` *`<your-external-account-ID>`* sebagai nama laporan.

> **Note**
>
> Anda harus mengikuti konvensi penamaan ini karena sejumlah kecil infrastruktur akan digunakan untuk memfasilitasi kueri. CURs

5. Centang IDs kotak Sertakan sumber daya.

> **Note**
>
> Anda harus memilih IDs kotak Sertakan sumber daya untuk melihat data biaya. ID ini diperlukan agar sesuai dengan sumber daya yang ditemukan oleh Workload Discovery di AWS.

6. Pilih Berikutnya.
7. Pada halaman Opsi pengiriman, pilih Konfigurasi 0
8. Buat bucket Amazon S3 baru untuk menyimpan. CURs
9. Tinjau kebijakan, pilih kotak konfirmasi, dan pilih Simpan.
10. Setel jalur awalan Laporan ke`aws-perspective`.
11. Pilih Harian untuk perincian waktu.
12. Di bawah Aktifkan integrasi data laporan untuk, pilih Amazon Athena.
13. Pilih Berikutnya.
14. Pilih Review dan Selesaikan. Untuk memverifikasi bahwa laporan telah diatur dengan benar, periksa bucket Amazon S3 untuk file pengujian.

> **Note**
>
> Diperlukan waktu hingga 24 jam untuk laporan diunggah ke bucket Anda.

Selanjutnya, atur replikasi ke akun penerapan.

# Mengatur replikasi

Siapkan replikasi ke dalam bucket Amazon S3 yang dibuat selama penerapan. Bucket Amazon S3 mengikuti format berikut:. *<stack-name>* `-s3buc-costandusagereportbucket-` *<ID-string>* Ini memungkinkan solusi untuk menanyakan ember dengan Amazon Athena.

1. Masuk ke akun AWS di konsol Amazon S3 yang berisi CUR yang dibuat yang perlu direplikasi.
2. Pilih bucket Amazon S3 yang dibuat saat mengonfigurasi CUR Anda. Untuk informasi selengkapnya, lihat Langkah 8 Membuat dan menjadwalkan Laporan Biaya dan Penggunaan AWS.
3. Pilih tab Manajemen.
4. Di bawah Aturan replikasi, pilih Buat aturan replikasi.
5. Di bawah Konfigurasi aturan replikasi, di kotak Nama aturan replikasi, masukkan ID aturan deskriptif.
6. Di bawah bucket Source, pilih Terapkan ke semua objek di bucket untuk mengonfigurasi cakupan aturan.
7. Di bawah Tujuan, konfigurasikan hal berikut:
   a. Pilih Tentukan bucket di akun lain.
   b. Masukkan ID akun.
   c. Masukkan nilai untuk nama Bucket yang dibuat selama penerapan Workload Discovery di AWS. Anda dapat menemukannya dengan mengikuti petunjuk di Menemukan sumber daya penerapan, menggunakan ID logis `CostAndUsageReportBucket` dan nama tumpukan yang Anda tentukan saat pertama kali menerapkan Workload Discovery di AWS.
   d. Pilih kotak untuk Ubah kepemilikan objek menjadi pemilik bucket tujuan.
8. Di bawah peran IAM, pilih Buat peran baru.

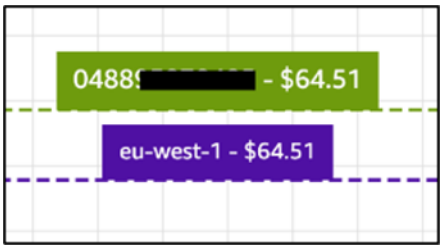
> **Note**
>
> Peran replikasi mungkin sudah ada. Anda dapat memilihnya dan memastikan bahwa ia memiliki tindakan peran replikasi S3 yang diperlukan.

9. Pilih Simpan.
10. Masuk ke AWS Management Console tempat CUR diinstal, buka halaman layanan S3 dan pilih bucket `CostAndUsageReportBucket` S3. Untuk detailnya, lihat Menemukan sumber daya penerapan.

11. Pilih tab Manajemen.
12. Di bawah Aturan replikasi, dari menu tarik-turun Tindakan, pilih Terima objek yang direplikasi.
13. Di bawah pengaturan akun bucket Sumber:
    a. Masukkan ID akun bucket sumber.
    b. Pilih Buat kebijakan.
    c. Di bawah Kebijakan, pilih lihat kebijakan bucket.
    d. Pilih Sertakan izin untuk mengubah kepemilikan objek menjadi pemilik bucket tujuan.
    e. Pilih Terapkan pengaturan. Ini memberinya akses untuk menyalin objek ke sana. Lihat kebijakan replikasi Cost Bucket untuk contoh kebijakan bucket S3.

> **Note**
>
> Saat mereplikasi CURs dari beberapa akun AWS. Anda perlu memastikan kebijakan bucket pada bucket tujuan (dalam Workload Discovery on AWS account) memiliki ARN untuk setiap Peran IAM yang Anda gunakan dari setiap akun. Lihat kebijakan replikasi Cost Bucket untuk detail selengkapnya.

Saat laporan ada di akun, data biaya muncul di kotak pembatas dan sumber daya individu.




## Edit kebijakan siklus hidup bucket S3

Selama penerapan, solusi mengonfigurasi kebijakan siklus hidup pada dua bucket:

- `CostAndUsageReportBucket`
- `AccessLogsBucket`

**Important**

Kebijakan siklus hidup ini menghapus data dari bucket ini setelah 90 hari. Anda dapat mengedit siklus hidup agar sesuai dengan kebijakan internal yang Anda miliki.

# Memantau solusinya

Solusi ini menggunakan MyApplications dan CloudWatch AppInsightsmemungkinkan Anda memantau Workload Discovery pada penerapan AWS.

## MyApplications

MyApplications adalah perpanjangan dari Console Home yang membantu Anda mengelola dan memantau biaya, kesehatan, postur keamanan, dan kinerja aplikasi Anda di AWS. Anda dapat mengakses semua aplikasi di akun Anda, metrik utama di semua aplikasi, dan ikhtisar metrik biaya, keamanan, dan operasi serta wawasan dari beberapa konsol layanan dari satu tampilan di AWS Management Console.

Untuk melihat dasbor MyApplications untuk Workload Discovery di AWS:

1. Masuk ke AWS Management Console.
2. Di bilah sisi kiri, pilih MyApplications.
3. Ketik `workload-discovery` ke dalam searchbar untuk menemukan aplikasi.
4. Pilih aplikasi.

## CloudWatch AppInsights

CloudWatch Application Insights membantu Anda memantau aplikasi Anda dengan mengidentifikasi dan menyiapkan metrik utama, log, dan alarm di seluruh sumber daya aplikasi dan tumpukan teknologi Anda. Ini terus memantau metrik dan log untuk mendeteksi dan mengkorelasikan anomali dan kesalahan. Untuk membantu pemecahan masalah, Wawasan Aplikasi ini akan membuat dasbor otomatis untuk masalah yang terdeteksi, yang mencakup anomali metrik terkorelasi dan kesalahan log, bersama dengan wawasan tambahan untuk menunjukkan akar masalah yang mungkin menjadi penyebabnya.

Untuk melihat CloudWatch AppInsights dasbor untuk Workload Discovery di AWS:

1. Masuk ke konsol CloudWatch tersebut.
2. Di sidebar kiri, pilih Insights, Application Insights.
3. Pilih tab Aplikasi.

4. Ketik `workload-discovery` ke dalam bilah pencarian untuk menemukan dasbor.
5. Pilih dasbor.
6. Pilih aplikasi.

# Perbarui solusinya

> **Important**
>
> Memperbarui dari v1.xx ke v2.xx dari Workload Discovery di AWS tidak didukung. Kami menyarankan Anda untuk menghapus v1.x.x dari solusi ini sebelum menginstal v2.xx.

Untuk memperbarui dari penerapan 2.xx, ikuti langkah-langkah ini.

1. Unduh CloudFormation templat AWS solusi.
2. Masuk ke CloudFormation konsol AWS.
3. Pilih tumpukan dengan nama yang diberikan selama penerapan dan pilih Perbarui.
4. Pada halaman Perbarui tumpukan, pilih Ganti templat saat ini, lalu pilih Unggah file templat, dan unggah file yang diunduh di langkah 1.
5. Pilih Berikutnya.
6. Pada halaman Tentukan detail tumpukan, di bawah Parameter, tinjau parameter dan modifikasi sesuai kebutuhan.
7. Pilih Berikutnya.
8. Pada halaman Configure stack options, di bawah Stack failure options, pastikan tombol Behavior on provisioning failure radio disetel ke Rollback all stack resource.
9. pilih Berikutnya.
10. Pada halaman Ulasan, tinjau dan konfirmasikan pengaturan. Pilih kotak yang mengakui bahwa template membuat sumber daya IAM dan membutuhkan kemampuan tertentu.
11. Pilih Perbarui tumpukan untuk menyebarkan tumpukan.

> **Note**
>
> Jika Anda menerapkan solusi dalam mode penemuan akun yang dikelola sendiri, Anda harus memperbarui sumber daya global yang Anda gunakan saat mengikuti langkah-langkah di bagian Impor Wilayah.

# Pemecahan Masalah

Resolusi masalah yang diketahui memberikan instruksi untuk mengurangi kesalahan yang diketahui. Jika petunjuk ini tidak mengatasi masalah Anda, lihat bagian Hubungi AWS Support untuk petunjuk cara membuka kasus AWS Support untuk solusi ini.

## Resolusi masalah yang diketahui

Selama penerapan Workload Discovery di AWS dan pada fase pasca-penerapan, beberapa kesalahan konfigurasi umum dapat terjadi:

> **Note**
>
> Untuk membantu mempermudah pemecahan masalah, sebaiknya nonaktifkan fitur rollback on failure di template AWS. CloudFormation Anda juga dapat menemukan bantuan pemecahan masalah tambahan dalam dokumentasi konfigurasi pasca-penerapan Workload Discovery pada AWS.

### Kesalahan Saluran Pengiriman Config

Masalah: Kesalahan berikut terjadi saat menerapkan CloudFormation template AWS utama:

```
Failed to put delivery channel '<stack-name>-DiscoveryImport-<ID-string>-
DeliveryChannel-<ID-string>' because the maximum number of delivery channels:
 1 is reached. (Service: AmazonConfig; Status Code: 400; Error Code:
 MaxNumberOfDeliveryChannelsExceededException; Request ID: 4edc54bc-8c85-4925-
b99d-7ef9c73215b3; Proxy: null)
```

Alasan: Solusi sedang diterapkan ke wilayah yang sudah mengaktifkan AWS Config.

Resolusi: Ikuti instruksi di bagian prasyarat dan gunakan solusi dengan parameter yang disetel ke CloudFormation . AlreadyHaveConfigSetupYes

## Cari Resolver Stack Deployment Times Habis Saat Menyebarkan Ke VPC yang Ada

Masalah: Tumpukan bersarang yang menyediakan sumber daya khusus untuk membuat indeks di waktu OpenSearch cluster habis dengan kesalahan berikut:

```
Embedded stack arn:aws:cloudformation:<region>::stack/<stack-name>-
SearchResolversStack-<ID-string>/<guid> was not successfullycreated: Stack creation
 time exceeded the specified timeout
```

Alasan: Subnet pribadi yang disediakan sebagai CloudFormation parameter tidak memiliki kemampuan untuk merutekan ke S3 (sumber daya khusus harus menulis hasil eksekusi mereka ke bucket S3 menggunakan URL yang telah ditentukan sebelumnya). Umumnya ada dua alasan untuk ini:

1. Subnet pribadi tidak memiliki gateway NAT yang terkait dengannya sehingga tidak ada akses ke internet.
2. Subnet pribadi menggunakan titik akhir VPC alih-alih gateway NAT dan titik akhir gateway S3 tidak dikonfigurasi dengan benar.

Resolusi:

1. Menyediakan gateway NAT di VPC untuk memungkinkan tugas yang berjalan di subnet pribadi untuk mengakses internet, baik menggunakan atau CloudFormation AWS CLI sesuai dokumentasi.
2. Pastikan bahwa tabel rute untuk subnet telah diperbarui untuk titik akhir VPC S3 sesuai dokumentasi.

## Sumber Daya Tidak Ditemukan Setelah Akun Diimpor

Masalah: Akun telah diimpor melalui UI Web tetapi tidak ada sumber daya yang ditemukan setelah proses penemuan berjalan.

Alasan: Alasan yang paling mungkin adalah sebagai berikut,

1. Ketika CrossAccountDiscovery CloudFormation parameter disetel ke`SELF_MANAGED`, CloudFormation template sumber daya global belum digunakan.

2. Ketika CrossAccountDiscovery CloudFormation parameter disetel ke`AWS_ORGANIZATIONS`: satu atau beberapa akun tidak ditemukan dan kolom Status Peran memiliki entri Tidak Diterapkan. Ini berarti ada masalah dengan penerapan otomatis template sumber daya global menggunakan StackSets.
3. Proses penemuan tugas ECS kehabisan memori. Ini terjadi ketika mengimpor sejumlah besar akun atau sumber daya. Kolom Terakhir Ditemukan di UI akan memiliki nilai yang lebih besar dari yang ditentukan dalam DiscoveryTaskFrequency CloudFormation parameter (nilai default adalah 15 menit) dan akan ada kesalahan kehabisan memori di konsol ECS.

Resolusi:

1. Terapkan templat sumber daya global di akun yang diperlukan, sesuai dokumentasi.
2. Buka WdGlobalResources StackSet di wilayah tempat Workload Discovery telah digunakan dan periksa kesalahan dalam instance tumpukan yang gagal diterapkan.
3. Perbarui CloudFormation parameter Memori ke nilai yang lebih besar: mulai dengan ganda dan terus meningkat hingga kesalahan berhenti.

> **Note**
>
> Hanya kombinasi tertentu dari unit CPU dan nilai memori yang valid sehingga Anda mungkin harus memperbarui CpuUnits CloudFormation parameter juga. Daftar lengkap kombinasi tercantum dalam dokumentasi ECS.

## Hanya Sumber Daya Konfigurasi Non-AWS yang Ditemukan Di Akun Tertentu

Masalah: Satu-satunya jenis sumber daya yang ditemukan solusi adalah yang tercantum dalam tabel di bagian Sumber daya yang didukung.

Alasan: Penyebab paling umum dari masalah ini adalah,

1. Ketika CrossAccountDiscovery CloudFormation parameter diatur ke`SELF_MANAGED`, CloudFormation template sumber daya regional belum digunakan di wilayah setiap akun yang akan ditemukan.

2. Saat CrossAccountDiscovery CloudFormation parameter disetel ke`SELF_MANAGED`, CloudFormation templat sumber daya regional telah diterapkan di wilayah sejumlah akun yang tidak mengaktifkan Config tetapi CloudFormation AlreadyHaveConfigSetupparameternya salah disetel ke. `Yes`
3. Saat CrossAccountDiscovery CloudFormation parameter disetel ke`AWS_ORGANIZATIONS`, AWS Config tidak diaktifkan di wilayah setiap akun yang akan ditemukan. Dalam `AWS_ORGANIZATIONS` mode, Anda bertanggung jawab untuk mengaktifkan Config sesuai kebijakan organisasi Anda.

Resolusi:

1. Terapkan templat sumber daya regional di akun yang diperlukan, sesuai dokumentasi.
2. Hapus tumpukan sumber daya regional yang diterapkan sebelumnya (AWS Config akan berada dalam keadaan tidak konsisten jika tidak) dan terapkan ulang dengan parameter yang disetel ke. CloudFormation AlreadyHaveConfigSetupNo
3. Aktifkan AWS Config di wilayah setiap akun yang akan ditemukan.

# Hubungi AWS Support

Jika Anda memiliki AWS Developer Support, AWS Business Support, atau AWS Enterprise Support, Anda dapat menggunakan Support Center untuk mendapatkan bantuan ahli terkait solusi ini. Bagian berikut memberikan petunjuk.

## Buat kasus

1. Masuk ke Support Center.
2. Pilih Buat kasus.

## Bagaimana kami bisa membantu?

1. Pilih Teknis.
2. Untuk Layanan, pilih Solusi.
3. Untuk Kategori, pilih Solusi Lain.
4. Untuk Keparahan, pilih opsi yang paling cocok dengan kasus penggunaan Anda.

5. Saat Anda memasukkan Layanan, Kategori, dan Tingkat Keparahan, antarmuka akan mengisi tautan ke pertanyaan pemecahan masalah umum. Jika Anda tidak dapat menyelesaikan pertanyaan Anda dengan tautan ini, pilih Langkah selanjutnya: Informasi tambahan.

## Informasi tambahan

1. Untuk Subjek, masukkan teks yang merangkum pertanyaan atau masalah Anda.
2. Untuk Deskripsi, jelaskan masalah ini secara rinci.
3. Pilih Lampirkan file.
4. Lampirkan informasi yang dibutuhkan AWS Support untuk memproses permintaan.

## Bantu kami menyelesaikan kasus Anda lebih cepat

1. Masukkan informasi yang diminta.
2. Pilih Langkah selanjutnya: Selesaikan sekarang atau hubungi kami.

## Selesaikan sekarang atau hubungi kami

1. Tinjau solusi Selesaikan sekarang.
2. Jika Anda tidak dapat menyelesaikan masalah Anda dengan solusi ini, pilih Hubungi kami, masukkan informasi yang diminta, dan pilih Kirim.

# Copot pemasangan solusinya

Untuk menghapus instalan solusi, gunakan AWS Management Console atau AWS Command Line Interface (AWS CLI). Pertama, hentikan semua tugas yang berjalan dari cluster Amazon ECS. Jika tidak, penghapusan tumpukan bisa gagal.

## Menggunakan Konsol Manajemen AWS

1. Masuk ke CloudFormation konsol AWS.
2. Pilih tumpukan dengan nama yang diberikan selama penerapan.
3. Pilih Hapus tumpukan.

## Menggunakan AWS Command Line Interface

Tentukan apakah AWS CLI tersedia di lingkungan Anda. Untuk petunjuk penginstalan, lihat Apa itu Antarmuka Baris Perintah AWS di Panduan Pengguna AWS CLI.

Setelah mengonfirmasi bahwa AWS CLI tersedia, jalankan perintah berikut:

```
$ aws cloudformation delete-stack --stack-name <customer-defined-stack-name>
```

# Panduan pengembang

Bagian ini menyediakan kode sumber untuk solusi dan penyesuaian tambahan.

## Kode sumber

Kunjungi Workload Discovery di AWS GitHub repositori untuk mengunduh templat dan skrip untuk solusi ini, dan untuk membagikan penyesuaian Anda dengan orang lain.

## Menemukan sumber daya penyebaran

Ikuti langkah-langkah ini untuk menemukan sumber daya yang diterapkan ke akun Anda.

1. Masuk ke CloudFormation konsol AWS.
2. Pilih Wilayah tempat Anda menerapkan solusi.

   Bergantung pada penggunaan akun ini, mungkin berisi beberapa tumpukan untuk beban kerja yang berbeda. Akan ada tumpukan utama dengan nama yang diberikan selama penerapan dan beberapa tumpukan bersarang di bawahnya.
3. Pilih setiap tumpukan untuk mengakses sumber daya yang digunakan menggunakan templat itu.
4. Pilih tab Sumber Daya dan pilih tautan ID Fisik untuk sumber daya yang relevan untuk melihat sumber daya di konsol layanan masing-masing.

   Jika Anda mengetahui ID Logis sumber daya, Anda juga dapat mencari menggunakan bilah pencarian di atas tabel.

## Sumber daya yang didukung

Solusi ini mendukung semua jenis sumber daya yang didukung AWS Config, seperti yang tercantum di sini. Tabel berikut berisi sumber daya yang didukung yang ditemukan oleh Workload Discovery di AWS yang tidak didukung oleh AWS Config. Detail disediakan dalam daftar dokumentasi AWS terkait.

| Jenis sumber daya | Sumber | Deskripsi |
| --- | --- | --- |
| AWS::APIGateway::Authorizer | SDK | GetAuthorizers |

| Jenis sumber daya | Sumber | Deskripsi |
| --- | --- | --- |
| AWS::ApiGateway::Resource | SDK | GetResource |
| AWS::ApiGateway::Method | SDK | GetMethod |
| AWS::Cognito::UserPool | SDK | describeUserPool |
| AWS::ECS::Task | SDK | jelaskan tugas-tugas |
| AWS::EKS::Nodegroup | SDK | DescribenodeGroup |
| AWS::DynamoDB::Stream | SDK | DescribStream |
| AWS: :IAM:: Kebijakan AWSManaged | SDK | getAccountAuthorizationDetail |
| AWS::ElasticLoadBalancingV2 ::TargetGroup | SDK | describeTargetGroups |
| AWS::EC2::Spot | SDK | describeSpotInstancePermintaan |
| AWS::EC2::SpotFleet | SDK | describeSpotFleetPermintaan |

## Mode penemuan akun AWS Organizations

Saat Workload Discovery di AWS diterapkan di AWS Organization, penemuan akun tidak lagi dikelola melalui UI web solusi. Dalam hal ini, Anda tidak perlu mengelola penyebaran CloudFormation templat untuk menemukan akun.

Sebagai gantinya, solusinya menggunakan agregator AWS Config di seluruh Organisasi AWS untuk menemukan sumber daya di semua akun di organisasi yang mengaktifkan AWS Config.

Untuk jenis sumber daya yang tidak didukung oleh AWS Config, solusi secara otomatis menerapkan peran IAM di setiap akun di organisasi yang menggunakan AWS. CloudFormation StackSets Peran ini memungkinkan proses penemuan untuk melakukan panggilan SDK di semua akun organisasi untuk menemukan sumber daya tambahan ini.

Ini StackSet dikonfigurasi untuk secara otomatis menerapkan peran di akun baru apa pun yang ditambahkan ke organisasi dan menghapus peran dari akun apa pun yang dihapus dari organisasi.

> **Note**
>
> Tidak mungkin bagi a StackSet untuk menerapkan instance tumpukan ke akun Manajemen. Jika Anda ingin Workload Discovery menemukan akun ini, Anda harus menerapkan templat sumber daya global menggunakan metode CloudFormation penerapan AWS standar yang dijelaskan di bagian Menerapkan tumpukan untuk menyediakan sumber daya Global menggunakan bagian. CloudFormation

## Tindakan peran replikasi Amazon S3

Peran IAM yang digunakan untuk melakukan replikasi harus memiliki tindakan berikut:

| |
|---|
| s3: ReplicateObject |
| s3: ReplicateDelete |
| s3: ReplicateTags |
| s3: ObjectOwnerOverrideToBucketOwner |
| s3: ListBucket |
| s3: GetReplicationConfiguration |
| s3: GetObjectVersionForReplication |
| s3: GetObjectVersionAcl |
| s3: GetObjectVersionTagging |
| s3: GetObjectRetention |
| s3: GetObjectLegalHold |

Untuk memverifikasi peran memiliki tindakan peran replikasi:

1. Salin nama nama peran di wizard Replikasi S3.
2. Masuk ke Konsol IAM di dalam akun tempat Anda menyiapkan replikasi.
3. Tempelkan nama peran ke dalam kotak Cari IAM.
4. Pilih item teratas dari daftar. Ini adalah peran IAM yang akan digunakan.
5. Di bawah kebijakan Izin, perluas kebijakan Terkelola.
6. Pastikan bahwa kebijakan memiliki tindakan yang dirinci dalam tabel sebelumnya.

## Kebijakan bucket S3

Di bawah ini adalah contoh kebijakan bucket S3 yang memungkinkan CURs untuk diunggah ke bucket bersama dengan izin untuk mengizinkan akun eksternal mereplikasi objek ke dalamnya. Anda perlu menambahkan Peran IAM dari setiap akun AWS eksternal ke kebijakan ini untuk memberikan izin agar replikasi berlangsung.

```
   {
      "Version":"2012-10-17",
      "Id":"",
      "Statement":[
          {
            "Sid":"Set permissions for objects"
            "Effect":"Allow",
            "Principal":{
                "AWS":"arn-of-role-selected-in-replication-setup-in-source-account"
          },
      "Action":["s3:ReplicateObject",
      "s3:ReplicateDelete"],
"s3:ObjectOwnerOverrideToBucketOwner",
        "Resource":"arn:aws:s3:::destination-bucket-name/*"
      },
      {
          "Sid":"Set permissions on bucket",
          "Effect":"Allow",
          "Principal":{
                "AWS":"arn-of-role-selected-in-replication-setup-in-source-account"
      },

      "Action":["s3:GetBucketVersioning",
"s3:PutBucketVersioning"],
        "Resource":"arn:aws:s3:::destination-bucket-name "
```

```
    },
    {
        "Sid": "Stmt1335892150622",
        "Effect": "Allow",
        "Principal": {
            "Service": "billingreports.amazonaws.com"
        },
        "Action": [
            "s3:GetBucketAcl",
            "s3:GetBucketPolicy"
         ],
        "Resource": "arn:aws:s3:::destination-bucket-name"
    },
    {

        "Sid": "Stmt1335892526596",
        "Effect": "Allow",
        "Principal": {
            "Service": "billingreports.amazonaws.com"
        },
        "Action": "s3:PutObject",
        "Resource": "arn:aws:s3:::destination-bucket-name/*"

      }
   ]
}
```

# AWS APIs

Sebagaimana dirinci dalam prasyarat, jika Anda menerapkan solusi ke VPC yang ada, layanan berikut harus dapat diakses dari subnet pribadi Anda.

## API Gateway

- GetAuthorizers
- GetIntegration
- GetMethod
- GetResources
- GetRestApis

## Cognito

- DescribeUserPool

## Config

- BatchGetAggregateResourceConfig
- DescribeConfigurationAggregators
- ListAggregateDiscoveredResources
- SelectAggregateResourceConfig

## DynamoDB Streams

- DescribeStream

## Amazon EC2

- DescribeInstances
- DescribeSpotFleetRequests
- DescribeSpotInstanceRequests
- DescribeTransitGatewayAttachments

## Amazon Elastic Load Balancer

- DescribeLoadBalancers
- DescribeListeners
- DescribeTargetGroups
- DescribeTargetHealth

## Amazon Elastic Kubernetes Service

- DescribeNodegroup
- ListNodegroups

## IAM

- GetAccountAuthorizationDetails
- ListPolicies

## Lambda

- GetFunction
- GetFunctionConfiguration
- ListEventSourceMappings

## OpenSearch Layanan

- DescribeDomains
- ListDomainNames

## Organizations

- ListAccounts
- ListAccountsForParent
- ListOrganizationalUnitsForParent
- ListRoots

## Amazon Simple Notification Service

- ListSubscriptions

## Layanan Token Keamanan Amazon

- AssumeRole

# Referensi

Bagian ini mencakup informasi tentang fitur opsional untuk mengumpulkan metrik unik untuk solusi ini dan daftar pembangun yang berkontribusi pada solusi ini.

## Pengumpulan data anonim

Solusi ini mencakup opsi untuk mengirim metrik operasional anonim ke AWS. Kami menggunakan data ini untuk lebih memahami bagaimana pelanggan menggunakan solusi ini dan layanan serta produk terkait. Saat diaktifkan, informasi berikut dikumpulkan dan dikirim ke AWS:

- ID Solusi - Pengidentifikasi solusi AWS
- Unique ID (UUID) - Pengidentifikasi unik yang dibuat secara acak untuk setiap penerapan
- Timestamp - Stempel waktu pengumpulan data
- Fitur Biaya Diaktifkan - Informasi tentang apakah pengguna menggunakan fitur biaya
- Jumlah Akun - Jumlah akun yang telah dionboard pengguna dalam penerapannya
- Jumlah Diagram - Jumlah diagram yang dibuat di setiap penyebaran
- Jumlah Sumber Daya - Jumlah sumber daya yang ditemukan di semua akun onboard

AWS memiliki data yang dikumpulkan melalui survei ini. Pengumpulan data tunduk pada Pemberitahuan Privasi. Untuk memilih keluar dari fitur ini, selesaikan langkah-langkah berikut sebelum meluncurkan CloudFormation template AWS.

1. Unduh CloudFormation template AWS ke hard drive lokal Anda.
2. Buka CloudFormation template AWS dengan editor teks.
3. Ubah bagian pemetaan CloudFormation template AWS dari:

```
Mappings:
  Solution:
    Metrics:
      CollectAnonymizedUsageMetrics: 'true'
```

ke:

```
Mappings:
```

```
  Solution:
    Metrics:
      CollectAnonymizedUsageMetrics: 'false'
```

1. Masuk ke CloudFormation konsol AWS.
2. Pilih Buat tumpukan.
3. Pada halaman Buat tumpukan, Tentukan templat bagian, pilih Unggah file templat.
4. Di bawah Unggah file templat, pilih Pilih file dan pilih templat yang diedit dari drive lokal Anda.
5. Pilih Berikutnya dan ikuti langkah-langkah dalam Luncurkan tumpukan.

# Kontributor

- Mohsan Jaffery
- Bola Matthew
- Stefano Vozza
- Connor Kirkpatrick
- Chris Deigan
- Nick Lee
- Tim Mekari

# Revisi

Tanggal publikasi: September 2020. Untuk pembaruan, lihat file ChangelOG.md di repositori. GitHub

Lihat file ChangeLog.md di repositori. GitHub

# Pemberitahuan

Pelanggan bertanggung jawab untuk membuat penilaian independen mereka sendiri atas informasi dalam dokumen ini. Dokumen ini: (a) hanya untuk tujuan informasi, (b) mewakili penawaran dan praktik produk AWS saat ini, yang dapat berubah tanpa pemberitahuan, dan (c) tidak membuat komitmen atau jaminan apa pun dari AWS dan afiliasinya, pemasok, atau pemberi lisensinya. Produk atau layanan AWS disediakan “sebagaimana adanya” tanpa jaminan, pernyataan, atau ketentuan dalam bentuk apa pun, baik tersurat maupun tersirat. Tanggung jawab dan kewajiban AWS kepada pelanggannya dikendalikan oleh perjanjian AWS, dan dokumen ini bukan bagian dari, juga tidak mengubah, perjanjian apa pun antara AWS dan pelanggannya.

Solusinya dilisensikan berdasarkan ketentuan Lisensi Apache, Versi 2.0.

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