Panduan Pengguna

AWS Hub Ketahanan

AWS Hub Ketahanan: Panduan Pengguna

Table of Contents

Apa itu AWS Resilience Hub?

AWS Resilience Hub adalah lokasi sentral bagi Anda untuk mengelola dan meningkatkan postur ketahanan aplikasi Anda. AWS AWS Resilience Hub memungkinkan Anda untuk menentukan tujuan ketahanan Anda, menilai postur ketahanan Anda terhadap tujuan tersebut, dan menerapkan rekomendasi untuk perbaikan berdasarkan Kerangka Kerja Well-Architected. AWS Di dalamnya AWS Resilience Hub, Anda juga dapat membuat dan menjalankan eksperimen Amazon Fault Injection Service, yang meniru gangguan kehidupan nyata pada aplikasi Anda untuk membantu Anda lebih memahami dependensi dan mengungkap potensi kelemahan. AWS Resilience Hub menyediakan tempat sentral dengan semua AWS layanan dan alat yang Anda butuhkan untuk terus memperkuat postur ketahanan Anda. AWS Resilience Hub bekerja dengan layanan lain untuk memberikan rekomendasi dan membantu Anda mengelola sumber daya aplikasi Anda. Untuk informasi selengkapnya, lihat Bekerja dengan layanan yang lain.

Tabel berikut menyediakan tautan dokumentasi dari semua layanan ketahanan terkait.

Layanan AWS dan referensi ketahanan terkait

AWS layanan ketahanan	Tautan dokumentasi
AWS Elastic Disaster Recovery	Apa itu Pemulihan Bencana Elastis
AWS Backup	Apa itu AWS Backup
Pengontrol Pemulihan Aplikasi Amazon Route 53 (Route 53ARC)	Apa itu Pengontrol Pemulihan Aplikasi Amazon Route 53

Topik

- AWS Resilience Hub — Manajemen ketahanan
- AWS Resilience Hub - Pengujian ketahanan
- AWS Resilience Hub konsep
- AWS Resilience Hub persona
- AWS Resilience Hub sumber daya yang didukung

AWS Resilience Hub — Manajemen ketahanan

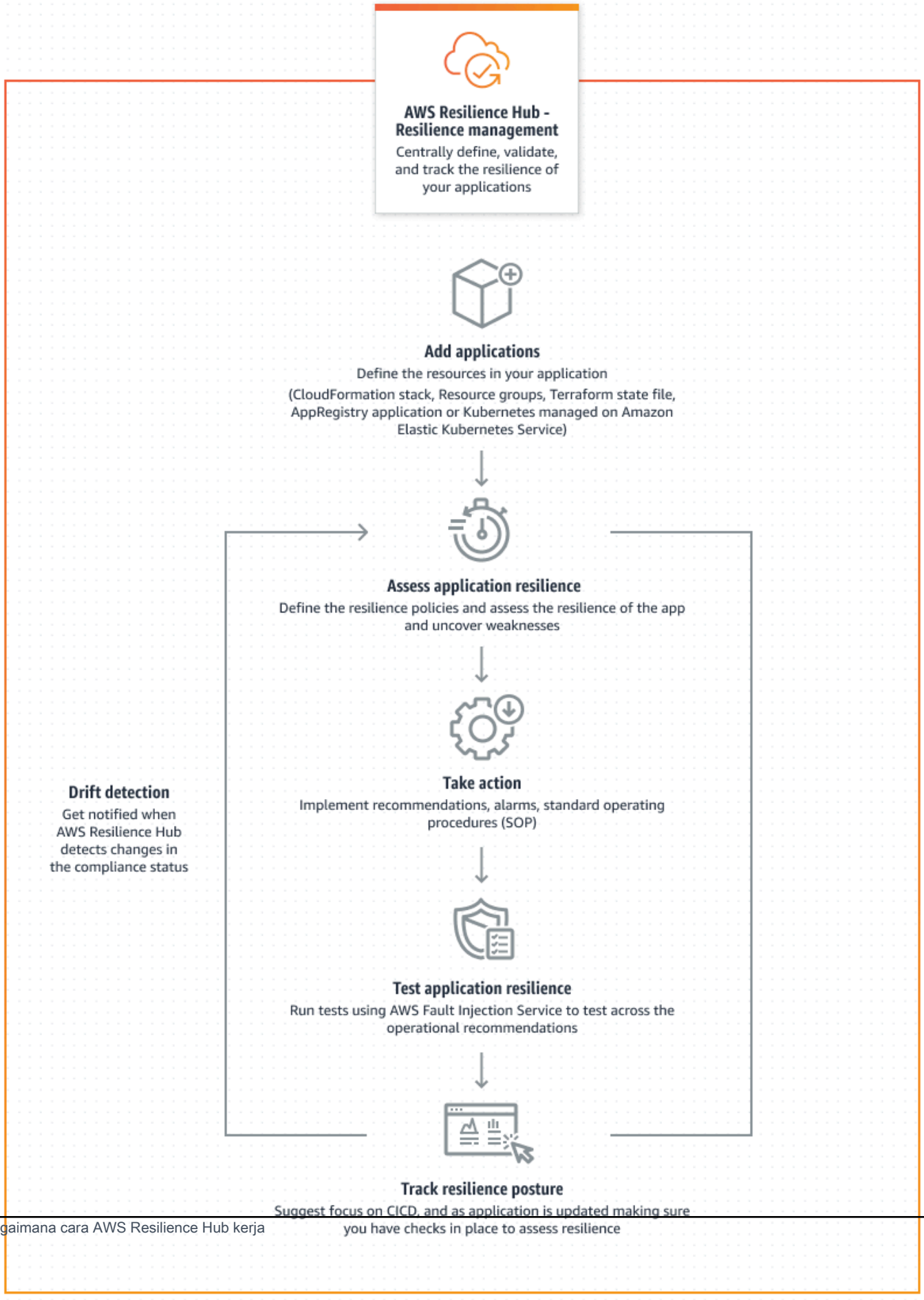
AWS Resilience Hub memberi Anda tempat sentral untuk mendefinisikan, memvalidasi, dan melacak ketahanan aplikasi Anda. AWS AWS Resilience Hub membantu Anda melindungi aplikasi Anda dari gangguan, dan mengurangi biaya pemulihan untuk mengoptimalkan kelangsungan bisnis guna membantu memenuhi persyaratan kepatuhan dan peraturan. Anda dapat menggunakan AWS Resilience Hub untuk melakukan hal berikut:

- Analisis infrastruktur Anda dan dapatkan rekomendasi untuk meningkatkan ketahanan aplikasi Anda. Selain panduan arsitektur untuk meningkatkan ketahanan aplikasi Anda, rekomendasi menyediakan kode untuk memenuhi kebijakan ketahanan Anda, menerapkan pengujian, alarm, dan prosedur operasi standar (SOPs) yang dapat Anda terapkan dan jalankan dengan aplikasi Anda dalam pipeline integrasi dan pengiriman (CI/CD) Anda.
- Mengevaluasi target target target waktu pemulihan (RTO) dan tujuan titik pemulihan (RPO) dalam kondisi yang berbeda.
- Optimalkan kelangsungan bisnis sekaligus mengurangi biaya pemulihan.
- Identifikasi dan selesaikan masalah sebelum terjadi dalam produksi.

Setelah menerapkan aplikasi ke dalam produksi, Anda dapat menambahkan AWS Resilience Hub ke pipeline CI/CD untuk memvalidasi setiap build sebelum dirilis ke produksi.

Bagaimana cara AWS Resilience Hub kerja

Diagram berikut memberikan garis besar tingkat tinggi tentang cara AWS Resilience Hub kerja.


AWS Resilience Hub - Resilience management
Centrally define, validate, and track the resilience of your applications
Add applications
Define the resources in your application (CloudFormation stack, Resource groups, Terraform state file, AppRegistry application or Kubernetes managed on Amazon Elastic Kubernetes Service)
Assess application resilience
Define the resilience policies and assess the resilience of the app and uncover weaknesses
Take action
Implement recommendations, alarms, standard operating procedures (SOP)
Test application resilience
Run tests using AWS Fault Injection Service to test across the operational recommendations
Track resilience posture
Suggest focus on CICD, and as application is updated making sure you have checks in place to assess resilience
Drift detection
Get notified when AWS Resilience Hub detects changes in the compliance status

Jelaskan

Jelaskan aplikasi Anda dengan mengimpor sumber daya dari AWS CloudFormation tumpukan, file status Terraform, AWS Resource Groups, kluster Amazon Elastic Kubernetes Service, atau Anda dapat memilih dari aplikasi yang sudah ditentukan. AWS Service Catalog AppRegistry

Mendefinisikan

Tentukan kebijakan ketahanan untuk aplikasi Anda. Kebijakan ini mencakup RTO dan RPO menargetkan gangguan aplikasi, infrastruktur, Availability Zone, dan Region. Target ini digunakan untuk memperkirakan apakah aplikasi memenuhi kebijakan ketahanan.

Menilai

Setelah Anda menjelaskan aplikasi Anda dan melampirkan kebijakan ketahanan padanya, jalankan penilaian ketahanan. AWS Resilience Hub Penilaian menggunakan praktik terbaik dari AWS Well-Architected Framework untuk menganalisis komponen aplikasi dan mengungkap kelemahan ketahanan potensial. Kelemahan ini dapat disebabkan oleh penyiapan infrastruktur yang tidak lengkap, kesalahan konfigurasi, atau situasi di mana perbaikan konfigurasi tambahan diperlukan. Untuk meningkatkan ketahanan, perbarui aplikasi dan kebijakan ketahanan Anda sesuai dengan rekomendasi dari laporan penilaian. Rekomendasi termasuk konfigurasi komponen, alarm, tes, dan pemulihan. SOPs Kemudian, Anda dapat menjalankan penilaian lain dan membandingkan hasilnya dengan laporan sebelumnya untuk melihat seberapa besar peningkatan ketahanan. Ulangi proses ini sampai perkiraan beban kerja dan perkiraan beban kerja RPO memenuhi target RTO dan target Anda. RTO RPO

Validasi

Jalankan pengujian untuk mengukur ketahanan AWS sumber daya Anda dan jumlah waktu yang diperlukan untuk memulihkan dari aplikasi, infrastruktur, Availability Zone, dan Wilayah AWS insiden. Untuk mengukur ketahanan, tes ini mensimulasikan pemadaman sumber daya Anda. AWS Contoh pemadaman termasuk kesalahan jaringan yang tidak tersedia, kegagalan, proses yang dihentikan, pemulihan RDS boot Amazon, dan masalah dengan Availability Zone Anda.

Lihat dan lacak

Setelah Anda menerapkan AWS aplikasi ke dalam produksi, Anda dapat menggunakan AWS Resilience Hub untuk terus melacak postur ketahanan aplikasi. Jika terjadi pemadaman, operator dapat melihat pemadaman AWS Resilience Hub dan meluncurkan proses pemulihan terkait.

AWS Resilience Hub - Pengujian ketahanan

AWS Resilience Hub memungkinkan Anda melakukan pengujian dan eksperimen Amazon Fault Injection Service (AWS FIS) pada AWS beban kerja Anda serta mempertahankan ketahanan optimal. Tes ini menekankan aplikasi dengan membuat peristiwa yang mengganggu sehingga Anda dapat mengamati bagaimana aplikasi Anda merespons. AWS FIS menyediakan beberapa skenario pra-bangun dan banyak pilihan tindakan yang menghasilkan gangguan. Selain itu, ini juga mencakup kontrol dan pagar pembatas yang Anda butuhkan untuk menjalankan eksperimen dalam produksi. Kontrol dan pagar pembatas mencakup opsi untuk melakukan putaran balik otomatis atau menghentikan percobaan jika kondisi tertentu terpenuhi. Untuk mulai menggunakan eksperimen AWS FIS untuk menjalankan dari AWS Resilience Hub konsol, lengkapi prasyarat yang ditentukan di bagian. the section called “Prasyarat”

Tabel berikut mencantumkan semua AWS FIS opsi yang tersedia dari panel navigasi dan tautan ke AWS FIS dokumentasi terkait yang berisi prosedur untuk mulai menggunakan AWS FIS pengujian dari AWS Resilience Hub konsol.

AWS FIS pilihan menu navigasi dan referensi

AWS FIS pilihan menu navigasi	AWS FIS dokumentasi
Pengujian ketahanan	Buat template eksperimen
Pustaka skenario	AWS FIS perpustakaan
Template percobaan	Template percobaan untuk AWS FIS

Tabel berikut mencantumkan semua AWS FIS opsi yang tersedia dari menu tarik-turun di bagian pengujian Ketahanan dan tautan ke AWS FIS dokumentasi terkait yang berisi prosedur untuk mulai menggunakan AWS FIS pengujian dari konsol. AWS Resilience Hub

AWS FIS pilihan menu dropdown dan referensi

AWS FIS pilihan menu dropdown	AWS FIS dokumentasi
Buat template eksperimen	Buat template eksperimen
Buat eksperimen dari skenario	Menggunakan skenario

AWS Resilience Hub konsep

Konsep-konsep ini dapat membantu Anda lebih memahami pendekatan untuk membantu meningkatkan ketahanan aplikasi dan mencegah pemadaman aplikasi. AWS Resilience Hub

Ketahanan

Kemampuan untuk menjaga ketersediaan dan memulihkan dari perangkat lunak dan gangguan operasional dalam kerangka waktu yang ditentukan.

Tujuan titik pemulihan (RPO)

Jumlah waktu maksimum yang dapat diterima sejak titik pemulihan data terakhir. Ini menentukan apa yang dianggap sebagai hilangnya data yang dapat diterima antara titik pemulihan terakhir dan gangguan layanan.

Tujuan waktu pemulihan (RTO)

Penundaan maksimum yang dapat diterima antara gangguan layanan dan pemulihan layanan. Ini menentukan apa yang dianggap sebagai jendela waktu yang dapat diterima ketika layanan tidak tersedia.

Perkiraan tujuan waktu pemulihan beban kerja

Perkiraan tujuan waktu pemulihan beban kerja (estimasi beban kerjaRTO) adalah RTO bahwa aplikasi Anda diperkirakan memenuhi berdasarkan definisi aplikasi yang diimpor dan kemudian menjalankan penilaian.

Perkiraan tujuan titik pemulihan beban kerja

Tujuan titik pemulihan beban kerja yang diperkirakan (estimasi beban kerjaRPO) adalah RPO bahwa aplikasi Anda diperkirakan memenuhi berdasarkan definisi aplikasi yang diimpor dan kemudian menjalankan penilaian.

Aplikasi

AWS Resilience Hub Aplikasi adalah kumpulan sumber daya yang AWS didukung yang terus dipantau dan dinilai untuk mengelola postur ketahanannya.

Komponen Aplikasi

Sekelompok AWS sumber daya terkait yang bekerja dan gagal sebagai satu kesatuan. Misalnya, jika Anda memiliki basis data primer dan replika, maka kedua database milik Komponen Aplikasi yang sama ()AppComponent.

AWS Resilience Hub menentukan AWS sumber daya mana yang dapat dimiliki oleh jenis AppComponent. Misalnya, `DBInstance` bisa menjadi milik `AWS::ResilienceHub::DatabaseAppComponent` tetapi bukan milik`AWS::ResilienceHub::ComputeAppComponent`.

Status kepatuhan aplikasi

AWS Resilience Hub melaporkan jenis status kepatuhan berikut untuk aplikasi Anda.

Kebijakan terpenuhi

Aplikasi ini diperkirakan memenuhi RTO dan RPO target yang ditentukan dalam kebijakan. Semua komponennya memenuhi tujuan kebijakan yang ditetapkan. Misalnya, Anda memilih RTO dan RPO target 24 jam untuk gangguan di seluruh AWS Wilayah. AWS Resilience Hub dapat melihat bahwa cadangan Anda disalin ke Wilayah fallback Anda. Anda masih diharapkan untuk mempertahankan pemulihan dari prosedur operasi standar cadangan (SOP), dan untuk menguji dan mengatur waktu itu. Ini ada dalam rekomendasi operasional dan bagian dari skor ketahanan Anda secara keseluruhan.

Kebijakan dilanggar

Aplikasi tidak dapat diperkirakan memenuhi RTO dan RPO target yang ditentukan dalam kebijakan. Satu atau lebih dari itu AppComponents tidak memenuhi tujuan kebijakan. Misalnya, Anda memilih RTO dan RPO target 24 jam untuk gangguan di seluruh AWS Wilayah, tetapi konfigurasi database Anda tidak menyertakan metode pemulihan Lintas wilayah apa pun, seperti replikasi global dan salinan cadangan.

Tidak dinilai

Aplikasi ini membutuhkan penilaian. Saat ini tidak dinilai atau dilacak.

Perubahan terdeteksi

Ada versi aplikasi baru yang diterbitkan yang belum dinilai.

Deteksi drift

AWS Resilience Hub menjalankan pemberitahuan drift saat menjalankan penilaian untuk aplikasi Anda untuk memeriksa apakah perubahan AppComponent konfigurasi telah memengaruhi status kepatuhan aplikasi Anda. Selain itu, ia juga memeriksa dan mendeteksi perubahan seperti penambahan atau penghapusan sumber daya dalam sumber input aplikasi dan memberi tahu tentang hal yang sama. Sebagai perbandingan, AWS Resilience Hub gunakan penilaian sebelumnya di mana komponen aplikasi memenuhi kebijakan. AWS Resilience Hub mendeteksi jenis drift berikut:

- Pergeseran kebijakan aplikasi — Jenis drift ini mengidentifikasi semua AppComponents yang sesuai dengan kebijakan dalam penilaian sebelumnya tetapi gagal mematuhi penilaian saat ini.
- Application resource drift — Jenis drift ini mengidentifikasi semua resource drifted dalam versi aplikasi saat ini.

Penilaian ketahanan

AWS Resilience Hub menggunakan daftar kesenjangan dan solusi potensial untuk mengukur efektivitas kebijakan yang dipilih untuk memulihkan dan melanjutkan dari bencana. Ini mengevaluasi setiap Komponen Aplikasi atau status kepatuhan aplikasi dengan kebijakan. Laporan ini mencakup rekomendasi pengoptimalan biaya dan referensi untuk masalah potensial.

Skor ketahanan

AWS Resilience Hub menghasilkan skor yang menunjukkan seberapa dekat aplikasi Anda mengikuti rekomendasi kami untuk memenuhi kebijakan ketahanan aplikasi, alarm, prosedur operasi standar (SOPs), dan pengujian.

Jenis gangguan

AWS Resilience Hub membantu Anda menilai ketahanan terhadap jenis pemadaman berikut:

Aplikasi

Infrastrukturnya sehat, tetapi tumpukan aplikasi atau perangkat lunak tidak beroperasi sesuai kebutuhan. Hal ini dapat terjadi setelah penerapan kode baru, perubahan konfigurasi, kerusakan data, atau kerusakan dependensi hilir.

Infrastruktur Cloud

Infrastruktur cloud tidak berfungsi seperti yang diharapkan karena pemadaman. Pemadaman dapat terjadi karena kesalahan lokal pada satu atau lebih komponen. Dalam kebanyakan kasus, jenis pemadaman ini diselesaikan dengan me-reboot, mendaur ulang, atau memuat ulang komponen yang salah.

Gangguan AZ Infrastruktur Cloud

Satu atau beberapa Availability Zone tidak tersedia. Jenis pemadaman ini dapat diatasi dengan beralih ke Availability Zone yang berbeda.

Insiden Wilayah Infrastruktur Cloud

Satu atau lebih Wilayah tidak tersedia. Jenis insiden ini dapat diselesaikan dengan beralih ke yang berbeda Wilayah AWS.

Eksperimen injeksi kesalahan

AWS Resilience Hub merekomendasikan tes untuk memverifikasi ketahanan aplikasi terhadap berbagai jenis pemadaman. Pemadaman ini termasuk aplikasi, infrastruktur, Availability Zones (AZ), atau Wilayah AWS insiden Komponen Aplikasi.

Eksperimen ini memungkinkan Anda melakukan hal berikut:

- Menyuntikkan kegagalan.
- Verifikasi bahwa alarm dapat mendeteksi pemadaman.
- Verifikasi bahwa prosedur pemulihan, atau prosedur operasi standar (SOPs), berfungsi dengan benar untuk memulihkan aplikasi dari pemadaman.

Pengujian untuk SOPs mengukur perkiraan beban kerja RTO dan perkiraan beban kerjaRPO. Anda dapat menguji konfigurasi aplikasi yang berbeda dan mengukur apakah output RTO dan RPO memenuhi tujuan yang ditentukan dalam kebijakan Anda.

SOP

Prosedur operasi standar (SOP) adalah serangkaian langkah preskriptif yang dirancang untuk memulihkan aplikasi Anda secara efisien jika terjadi pemadaman atau alarm. Berdasarkan penilaian aplikasi, AWS Resilience Hub rekomendasikan satu set SOPs dan disarankan untuk menyiapkan, menguji, dan mengukur SOPs terlebih dahulu gangguan untuk memastikan pemulihan tepat waktu.

AWS Resilience Hub persona

Membangun aplikasi perusahaan membutuhkan upaya kolaboratif dari tim lintas fungsi yang berbeda seperti infrastruktur, kelangsungan bisnis, pemilik aplikasi, dan pemangku kepentingan lainnya yang bertanggung jawab untuk memantau aplikasi. Persona yang berbeda dari tim yang berbeda berkontribusi dalam membangun dan mengelola aplikasi AWS Resilience Hub, masing-masing memiliki peran dan tanggung jawab yang berbeda. Untuk mempelajari lebih lanjut tentang izin kisi-kisi ke persona yang berbeda, lihat. the section called “AWS Resilience Hub referensi persona dan IAM izin”

Untuk memulai membuat aplikasi dan menjalankan penilaian di AWS Resilience Hub, kami sarankan Anda untuk membuat persona berikut:

- Manajer aplikasi infrastruktur — Pengguna dengan persona ini bertanggung jawab untuk menyiapkan, mengonfigurasi, dan memelihara infrastruktur dan sumber daya aplikasi, memastikan keandalan dan keamanan aplikasi. Tanggung jawab mereka meliputi:
  - Memastikan bahwa aplikasi dikerahkan dan diperbarui secara berkala
  - Memantau kinerja sistem
  - Memecahkan masalah
  - Menerapkan rencana cadangan dan pemulihan bencana
- Manajer kontinuitas bisnis — Pengguna dengan persona ini bertanggung jawab untuk mendikte kebijakan aplikasi dan menentukan kekritisan bisnis aplikasi. Tanggung jawab mereka meliputi:
  - Mengambil keputusan penting dalam menetapkan kebijakan
  - Menilai kekritisan bisnis
  - Mengalokasikan sumber daya untuk aplikasi penting
  - Menilai dan mengelola risiko
- Pemilik aplikasi — Pengguna dengan persona ini bertanggung jawab untuk memastikan aplikasi yang sangat tersedia dan andal. Tanggung jawab mereka meliputi:
  - Mendefinisikan pengidentifikasi kinerja utama untuk mengukur dan memantau kinerja aplikasi dan mengidentifikasi kemacetan
  - Menyelenggarakan pelatihan untuk berbagai pemangku kepentingan
  - Memastikan bahwa dokumentasi berikut adalah up-to-date:
    - Arsitektur aplikasi
    - Proses penyebaran

    - Konfigurasi pemantauan
    - Teknik pengoptimalan kinerja
- Akses hanya-baca - Pengguna dengan persona ini dibatasi untuk izin hanya-baca. Tanggung jawab mereka termasuk menjaga visibilitas dan pengawasan kinerja dan kesehatan aplikasi dengan memantau skor ketahanan, rekomendasi operasional, dan rekomendasi ketahanan. Selain itu, mereka juga bertanggung jawab untuk mengidentifikasi masalah, tren, dan area untuk perbaikan untuk memastikan bahwa aplikasi memenuhi tujuan organisasi.

AWS Resilience Hub sumber daya yang didukung

Sumber daya yang memengaruhi kinerja aplikasi jika terjadi gangguan didukung sepenuhnya oleh sumber daya AWS Resilience Hub tingkat atas seperti `AWS::RDS::DBInstance` dan. `AWS::RDS::DBCluster`

Untuk mempelajari lebih lanjut tentang izin yang diperlukan AWS Resilience Hub untuk menyertakan sumber daya dari semua layanan yang didukung dalam penilaian Anda, lihatthe section called “AWSResilienceHubAsssessmentExecutionPolicy”.

AWS Resilience Hub mendukung sumber daya dari AWS layanan berikut:

- Hitung
    - Amazon Elastic Compute Cloud (AmazonEC2)

      > **Note**
      >
      > AWS Resilience Hub tidak mendukung format Amazon Resource Name (ARN) lama untuk mengakses EC2 sumber daya Amazon. ARNFormat baru menggunakan ID AWS akun Anda dan memungkinkan kemampuan yang disempurnakan untuk menandai sumber daya di klaster Anda, dan juga melacak biaya layanan dan tugas yang berjalan di klaster Anda.
      >
      > - Format lama (usang) - `arn:aws:ec2:<region>::instance/<instance-id>`
      > - Format baru - `arn:aws:ec2:<region>:<account-id>:instance/<instance-id>`
      >
      > Untuk informasi selengkapnya tentang ARN format baru, lihat Memigrasi ECS penyebaran Amazon Anda ke format ID baru ARN dan sumber daya.

    - AWS Lambda

  - Amazon Elastic Kubernetes Service (Amazon) EKS
  - Layanan Kontainer Elastis Amazon (AmazonECS)
  - AWS Step Functions
- Basis Data
  - Amazon Relational Database Service (AmazonRDS)
  - Amazon DynamoDB
  - Amazon DocumentDB
- Jaringan dan Pengiriman Konten
  - Amazon Route 53
  - Penyeimbang Beban Elastis
  - Terjemahan Alamat Jaringan (NAT)
- Penyimpanan
  - Toko Blok Elastis Amazon (AmazonEBS)
  - Amazon Elastic File System (AmazonEFS)
  - Amazon Simple Storage Service (Amazon S3)
  - Amazon FSx untuk Server File Windows
- Lainnya
  - APIGerbang Amazon
  - Pengontrol Pemulihan Aplikasi Amazon Route 53 (Amazon Route 53ARC)
  - Amazon Simple Notification Service
  - Amazon Simple Queue Service
  - AWS Auto Scaling
  - AWS Backup
  - AWS Pemulihan Bencana Elastis

> **Note**
>
> - AWS Resilience Hub memberikan transparansi tambahan untuk sumber daya aplikasi Anda dengan memungkinkan Anda melihat instance yang didukung dari setiap sumber daya. Selain itu, AWS Resilience Hub memberikan rekomendasi ketahanan yang lebih akurat dengan mengidentifikasi contoh unik dari setiap sumber daya sambil menemukan

contoh sumber daya selama proses penilaian. Untuk informasi selengkapnya tentang menambahkan instance resource ke aplikasi Anda, lihatMengedit sumber daya AWS Resilience Hub aplikasi.

- AWS Resilience Hub mendukung Amazon EKS dan Amazon ECS di AWS Fargate.
- AWS Resilience Hub mendukung penilaian AWS Backup sumber daya sebagai bagian dari layanan berikut:
  - Amazon EBS
  - Amazon EFS
  - Amazon S3
  - Basis Data Global Amazon Aurora
  - Amazon DynamoDB
  - RDSLayanan Amazon
  - Amazon FSx untuk Server File Windows
- Amazon Route 53 ARC hanya AWS Resilience Hub menilai Amazon DynamoDB global, Elastic Load Balancing, Amazon, dan grup. RDS AWS Auto Scaling
- AWS Resilience Hub Untuk menilai sumber daya Lintas wilayah, kelompokkan sumber daya di bawah satu Komponen Aplikasi. Untuk informasi selengkapnya tentang sumber daya yang didukung oleh masing-masing Komponen AWS Resilience Hub Aplikasi dan sumber daya pengelompokan, lihatMengelompokkan sumber daya dalam Komponen Aplikasi.
- Saat ini, AWS Resilience Hub tidak mendukung penilaian lintas wilayah untuk EKS klaster Amazon jika EKS kluster Amazon berada atau jika aplikasi dibuat di Wilayah yang diaktifkan keikutsertaan. AWS
- Saat ini, hanya AWS Resilience Hub menilai tipe sumber daya Kubernetes berikut:
  - Deployment
  - ReplicaSets
  - Pod

AWS Resilience Hub mengabaikan jenis sumber daya berikut:

- Sumber daya yang tidak memengaruhi perkiraan beban kerja RTO atau perkiraan beban kerja RPO — Sumber daya seperti`AWS::RDS::DBParameterGroup`, yang tidak memengaruhi perkiraan beban kerja RTO atau perkiraan beban kerjaRPO, diabaikan oleh. AWS Resilience Hub

- Sumber daya tingkat non-top — AWS Resilience Hub hanya mengimpor sumber daya tingkat atas, karena mereka dapat memperoleh properti lain dengan menanyakan properti sumber daya tingkat atas. Misalnya, `AWS::ApiGateway::RestApi` dan `AWS::ApiGatewayV2::Api` merupakan sumber daya yang didukung untuk Amazon API Gateway. Namun, `AWS::ApiGatewayV2::Stage` bukan sumber daya tingkat atas. Oleh karena itu, tidak diimpor oleh AWS Resilience Hub.

> **Note**
>
> Sumber daya yang tidak didukung
>
> - Anda tidak dapat mengidentifikasi beberapa sumber daya dengan menggunakan AWS Resource Groups (Amazon Route 53 RecordSets dan API -GWHTTP) dan sumber daya Amazon Aurora Global. Jika Anda ingin menganalisis sumber daya ini sebagai bagian dari penilaian Anda, Anda harus menambahkan sumber daya secara manual ke aplikasi. Namun, saat Anda menambahkan sumber daya Amazon Aurora Global untuk penilaian, sumber daya tersebut harus dikelompokkan dengan Komponen Aplikasi RDS instans Amazon. Untuk informasi selengkapnya tentang mengedit sumber daya, lihatthe section called “Mengedit sumber daya aplikasi”.
> - Sumber daya ini dapat mempengaruhi pemulihan aplikasi, tetapi mereka tidak sepenuhnya didukung oleh AWS Resilience Hub saat ini. AWS Resilience Hub berusaha memperingatkan pengguna tentang sumber daya yang tidak didukung jika aplikasi didukung oleh AWS CloudFormation tumpukan, file status Terraform AWS Resource Groups, atau aplikasi. AppRegistry

Memulai

Bagian ini menjelaskan cara mulai menggunakan AWS Resilience Hub. Ini termasuk membuat izin AWS Identity and Access Management (IAM) untuk akun.

Topik

Prasyarat

Sebelum Anda dapat menggunakan AWS Resilience Hub, Anda harus menyelesaikan prasyarat berikut:

- AWS akun — Buat satu atau beberapa AWS akun untuk setiap jenis akun (akun primer/sekunder/sumber daya) yang ingin Anda gunakan. AWS Resilience Hub Untuk informasi selengkapnya tentang membuat dan mengelola AWS akun, lihat berikut ini:
  - AWS Pengguna pertama kali - Memulai: Apakah Anda AWS pengguna pertama kali?
  - Mengelola AWS akun - https://docs.aws.amazon.com/accounts/latest/reference/managing-accounts.html
- AWS Identity and Access Management Izin (IAM) — Setelah membuat AWS akun, Anda harus mengonfigurasi peran dan izin IAM yang diperlukan untuk setiap akun yang telah Anda buat. Misalnya, jika Anda telah membuat AWS akun untuk mengakses sumber daya aplikasi, Anda harus menyiapkan peran baru dan mengonfigurasi izin IAM yang diperlukan AWS Resilience Hub untuk mengakses sumber daya aplikasi dari akun Anda. Untuk mempelajari lebih lanjut tentang izin IAM, lihat the section called “Cara AWS kerja Resilience Hub IAM” dan untuk informasi selengkapnya tentang menambahkan kebijakan ke peran, lihat. the section called “Mendefinisikan kebijakan kepercayaan menggunakan file JSON”

  Untuk memulai dengan cepat dengan menambahkan izin IAM ke pengguna, grup, dan peran, Anda dapat menggunakan kebijakan AWS terkelola kami ()the section called “AWS kebijakan terkelola”. Lebih mudah menggunakan kebijakan AWS terkelola untuk mencakup kasus penggunaan umum yang tersedia di Anda Akun AWS daripada menulis kebijakan sendiri. AWS Resilience Hub menambahkan izin tambahan ke kebijakan AWS terkelola untuk memperluas dukungan ke AWS layanan lain dan menyertakan fitur baru. Oleh karena itu:

- Jika Anda adalah pelanggan yang sudah ada dan jika Anda ingin aplikasi Anda menggunakan perangkat tambahan terbaru dalam penilaian Anda, Anda harus menerbitkan versi baru aplikasi dan kemudian menjalankan penilaian baru. Untuk informasi selengkapnya, lihat topik berikut.
  - the section called “Publikasikan versi aplikasi baru”
  - the section called “Menjalankan penilaian ketahanan”
- Jika Anda tidak menggunakan kebijakan AWS terkelola untuk menetapkan izin IAM yang sesuai kepada pengguna, grup, dan peran, Anda harus mengonfigurasi izin ini secara manual. Untuk informasi selengkapnya tentang kebijakan AWS terkelola, lihatthe section called “AWSResilienceHubAsssessmentExecutionPolicy”.

Tambahkan aplikasi ke AWS Resilience Hub

AWS Resilience Hub menawarkan penilaian ketahanan dan validasi yang terintegrasi ke dalam siklus hidup pengembangan perangkat lunak Anda. AWS Resilience Hub membantu Anda secara proaktif mempersiapkan dan melindungi AWS aplikasi Anda dari gangguan dengan:

- Mengungkap kelemahan ketahanan.
- Memperkirakan apakah target waktu pemulihan target Anda (RTO) dan tujuan titik pemulihan (RPO) dapat dipenuhi.
- Menyelesaikan masalah sebelum dilepaskan ke produksi.

Bagian ini memandu Anda dengan menambahkan aplikasi. Anda mengumpulkan sumber daya dari aplikasi yang ada, AWS CloudFormation tumpukan AWS Resource Groups, atau AppRegistry dan membuat kebijakan ketahanan yang sesuai. Setelah menjelaskan aplikasi, Anda dapat mempublikasikannya AWS Resilience Hub, dan membuat laporan penilaian tentang ketahanan aplikasi Anda. Anda kemudian dapat menggunakan rekomendasi dari penilaian untuk meningkatkan ketahanan. Anda dapat menjalankan penilaian lain, membandingkan hasil, dan kemudian mengulang hingga perkiraan beban kerja RTO dan perkiraan beban kerja RPO mencapai target Anda. RTO RPO

Topik

- Langkah 1: Memulai dengan menambahkan aplikasi
- Langkah 2: Bagaimana aplikasi Anda dikelola?
- Langkah 3: Tambahkan sumber daya ke AWS Resilience Hub aplikasi Anda
- Langkah 4: Set RTO dan RPO

Langkah 1: Memulai dengan menambahkan aplikasi

Mulailah AWS Resilience Hub dengan menjelaskan detail AWS aplikasi Anda dan menjalankan laporan untuk menilai ketahanan.

Untuk memulai, pada AWS Resilience Hub halaman beranda di bawah Memulai, pilih Tambahkan aplikasi.

Untuk mempelajari lebih lanjut tentang biaya dan penagihan yang terkait AWS Resilience Hub, lihat AWS Resilience Hub harga.

Jelaskan detail aplikasi Anda di AWS Resilience Hub

Bagian ini menunjukkan kepada Anda bagaimana mendeskripsikan detail AWS aplikasi Anda yang ada di AWS Resilience Hub.

Untuk menjelaskan detail aplikasi Anda

1. Masukkan nama untuk aplikasi.
2. (Opsional) Masukkan deskripsi untuk aplikasi.

Selanjutnya

Langkah 2: Bagaimana aplikasi Anda dikelola?

Langkah 2: Bagaimana aplikasi Anda dikelola?

Selain AWS CloudFormation tumpukan, AppRegistry aplikasi AWS Resource Groups, dan file status Terraform, Anda dapat menambahkan sumber daya yang terletak di kluster Amazon

Elastic Kubernetes Service (Amazon). EKS Artinya, AWS Resilience Hub memungkinkan Anda menambahkan sumber daya yang terletak di EKS kluster Amazon Anda sebagai sumber daya opsional. Bagian ini menyediakan opsi berikut, yang membantu Anda menentukan lokasi sumber daya aplikasi Anda.

- Koleksi sumber daya - Pilih opsi ini jika Anda ingin menemukan sumber daya dari salah satu koleksi sumber daya. Koleksi sumber daya mencakup AWS CloudFormation tumpukan,, AppRegistry aplikasi AWS Resource Groups, dan file status Terraform.

  Jika Anda memilih opsi ini, Anda harus menyelesaikan salah satu prosedur dithe section called "Tambahkan koleksi sumber daya".
- EKShanya — Pilih opsi ini jika Anda ingin menemukan sumber daya dari ruang nama dalam kluster AmazonEKS.

  Jika Anda memilih opsi ini, Anda harus menyelesaikan prosedur di the section called "Tambahkan EKS cluster"
- Koleksi sumber daya & EKS — Pilih opsi ini jika Anda ingin menemukan sumber daya dari salah satu koleksi sumber daya dan EKS kluster Amazon.

  Jika Anda memilih opsi ini, selesaikan salah satu prosedur the section called "Tambahkan koleksi sumber daya" dan kemudian selesaikan prosedur dithe section called "Tambahkan EKS cluster".

> **Note**
>
> Untuk informasi tentang jumlah sumber daya yang didukung per aplikasi, lihat Service Quotas.

Selanjutnya

Langkah 3: Tambahkan sumber daya ke AWS Resilience Hub aplikasi Anda

Langkah 3: Tambahkan sumber daya ke AWS Resilience Hub aplikasi Anda

Bagian ini membahas opsi berikut yang dapat Anda gunakan untuk membentuk dasar struktur aplikasi Anda:

- the section called "Tambahkan koleksi sumber daya"

- the section called “Tambahkan EKS cluster”

Tambahkan koleksi sumber daya

Bagian ini membahas metode berikut yang Anda gunakan untuk membentuk dasar struktur aplikasi Anda:

- Menggunakan AWS CloudFormation tumpukan
- Menggunakan AWS Resource Groups
- Menggunakan AppRegistry aplikasi
- Menggunakan file status Terraform
- Menggunakan AWS Resilience Hub aplikasi yang ada

Menggunakan AWS CloudFormation tumpukan

Pilih AWS CloudFormation tumpukan yang berisi sumber daya yang ingin Anda gunakan dalam aplikasi yang Anda gambarkan. Tumpukan dapat dari Akun AWS yang Anda gunakan untuk menggambarkan aplikasi, atau mereka dapat dari akun yang berbeda atau Wilayah yang berbeda.

Untuk menemukan sumber daya yang membentuk dasar struktur aplikasi Anda

1. Pilih CloudFormation tumpukan untuk menemukan sumber daya berbasis tumpukan Anda.
2. Pilih tumpukan dari daftar tarik-turun Pilih tumpukan yang terkait dengan Anda dan Wilayah. Akun AWS

   Untuk menggunakan tumpukan yang berada di Wilayah berbeda Akun AWS, berbeda, atau keduanya, masukkan Nama Sumber Daya Amazon (ARN) tumpukan di kotak Tambah tumpukan di luar AWS Wilayah, lalu pilih Tambah tumpukan ARN. Untuk informasi selengkapnyaARNs, lihat Amazon Resource Names (ARNs) di Referensi AWS Umum.

Menggunakan AWS Resource Groups

Pilih AWS Resource Groups yang berisi sumber daya yang ingin Anda gunakan dalam aplikasi yang Anda gambarkan.

Untuk menemukan sumber daya yang membentuk dasar struktur aplikasi Anda

1. Pilih Grup sumber daya untuk menemukan AWS Resource Groups yang berisi sumber daya.

2. Pilih sumber daya dari Pilih daftar dropdown grup sumber daya.

   Untuk menggunakan AWS Resource Groups yang berada di Region berbeda Akun AWS, atau keduanya, masukkan Amazon Resource Name (ARN) dari tumpukan di ARN kotak Resource Group, lalu pilih Tambah Grup Sumber Daya ARN. Untuk informasi selengkapnyaARNs, lihat Amazon Resource Names (ARNs) di Referensi AWS Umum.

Menggunakan AppRegistry aplikasi

Anda hanya dapat menambahkan satu AppRegistry aplikasi dalam satu waktu.

Pilih AppRegistry aplikasi yang berisi sumber daya yang ingin Anda gunakan dalam aplikasi yang Anda gambarkan.

Untuk menemukan sumber daya yang membentuk dasar struktur aplikasi Anda

1. Pilih AppRegistryuntuk memilih dari daftar aplikasi yang dibuat di AppRegistry.
2. Pilih aplikasi, yang dibuat di AppRegistry, dari daftar dropdown Pilih aplikasi. Anda hanya dapat memilih satu aplikasi dalam satu waktu.

Menggunakan file status Terraform

Pilih file status Terraform yang berisi sumber daya bucket S3 yang ingin Anda gunakan dalam aplikasi yang Anda gambarkan. Anda dapat menavigasi ke lokasi file status Terraform Anda atau memberikan tautan ke file status Terraform yang dapat Anda akses yang terletak di Wilayah lain.

> **Note**
>
> AWS Resilience Hub mendukung versi file status Terraform `0.12` dan yang lebih baru.

Untuk menemukan sumber daya yang membentuk dasar struktur aplikasi Anda

1. Pilih file status Terraform untuk menemukan sumber daya bucket S3 Anda.
2. Dari bagian Pilih file status, pilih Jelajahi S3 untuk menavigasi ke lokasi file status Terraform Anda.

   Untuk menggunakan file status Terraform yang terletak di Wilayah lain, berikan tautan ke lokasi file status Terraform di URL bidang S3, dan pilih Tambahkan S3. URL

Batas untuk file status Terraform adalah 4 megabyte (MB).

3. Pilih bucket S3 Anda dari bagian Bucket.
4. Dari bagian Objek, pilih tombol, dan pilih Pilih.

Menggunakan AWS Resilience Hub aplikasi yang ada

Untuk memulai, gunakan aplikasi yang ada.

Untuk menemukan sumber daya yang membentuk dasar struktur aplikasi Anda

1. Pilih aplikasi yang ada untuk membangun aplikasi Anda dari aplikasi yang ada.
2. Pilih aplikasi dari daftar dropdown Pilih aplikasi yang ada.

Tambahkan EKS cluster

Bagian ini membahas tentang penggunaan EKS klaster Amazon untuk membentuk dasar struktur aplikasi Anda.

> **Note**
>
> Anda harus memiliki EKS izin Amazon dan IAM peran tambahan untuk terhubung ke EKS klaster Amazon. Untuk informasi selengkapnya tentang menambahkan EKS izin Amazon akun tunggal dan lintas akun serta IAM peran tambahan untuk terhubung ke klaster, lihat topik berikut:
>
> - AWS Resilience Hub referensi izin akses
> - the section called “Mengaktifkan AWS Resilience Hub akses ke klaster Amazon EKS Anda”

Pilih EKS klaster Amazon dan ruang nama yang berisi sumber daya yang ingin Anda gunakan dalam aplikasi yang Anda gambarkan. EKSCluster Amazon dapat berasal dari Akun AWS yang Anda gunakan untuk menggambarkan aplikasi, atau mereka dapat dari akun yang berbeda atau Wilayah yang berbeda.

> **Note**
>
> AWS Resilience Hub Untuk menilai EKS kluster Amazon Anda, Anda harus menambahkan ruang nama yang relevan secara manual ke setiap kluster Amazon di EKS bagian EKS cluster dan ruang nama. Nama namespace harus sama persis dengan nama namespace di cluster Amazon Anda. EKS

Untuk menambahkan EKS cluster Amazon

1. Pilih EKS kluster Amazon dari daftar tarik-turun Pilih EKS klaster yang terkait dengan Anda dan Wilayah. Akun AWS
2. Untuk menggunakan EKS kluster Amazon yang berada di Wilayah berbeda Akun AWS, berbeda, atau keduanya, masukkan Nama Sumber Daya Amazon (ARN) tumpukan di kotak Lintas akun atau Wilayah, lalu pilih Tambah EKS ARN. Untuk informasi selengkapnyaARNs, lihat Amazon Resource Names (ARNs) di Referensi AWS Umum.

   Untuk informasi selengkapnya tentang menambahkan izin untuk mengakses klaster Amazon Elastic Kubernetes Service lintas wilayah, lihat. the section called “Mengaktifkan AWS Resilience Hub akses ke klaster Amazon EKS Anda”

Untuk menambahkan ruang nama dari kluster Amazon yang dipilih EKS

1. Di bagian Tambahkan ruang nama, dari tabel EKScluster dan ruang nama, pilih tombol radio yang terletak di sebelah kiri nama EKS cluster Amazon, lalu pilih Perbarui ruang nama.

   Anda dapat mengidentifikasi EKS kluster Amazon dengan yang berikut:

   - EKSnama cluster - Menunjukkan nama EKS kluster Amazon yang dipilih.
   - # Ruang nama - Menunjukkan jumlah ruang nama yang dipilih di kluster Amazon. EKS
   - Status - Menunjukkan apakah AWS Resilience Hub telah menyertakan ruang nama dari EKS kluster Amazon yang dipilih dalam aplikasi Anda. Anda dapat mengidentifikasi status menggunakan opsi berikut:
     - Diperlukan namespace - Menunjukkan bahwa Anda belum menyertakan ruang nama apa pun dari klaster Amazon. EKS
     - Ruang nama ditambahkan - Menunjukkan bahwa Anda telah menyertakan satu atau beberapa ruang nama dari klaster Amazon. EKS

2. Untuk menambahkan namespace, di kotak dialog Perbarui namespace, pilih Tambahkan namespace baru.

   Kotak dialog Perbarui ruang nama menampilkan semua ruang nama yang telah Anda pilih dari EKS kluster Amazon, sebagai opsi yang dapat diedit.

3. Dalam kotak dialog Perbarui ruang nama, Anda memiliki opsi edit berikut:

   - Untuk menambahkan namespace baru, pilih Tambahkan namespace baru, lalu masukkan nama namespace di kotak namespace.

     Nama namespace harus sama persis dengan nama namespace di cluster Amazon Anda. EKS
   - Untuk menghapus namespace, pilih Hapus yang terletak di sebelah namespace.
   - Untuk menerapkan ruang nama yang dipilih ke semua kluster Amazon, pilih Terapkan ruang nama ke semua EKS cluster. EKS

     Jika Anda memilih opsi ini, pemilihan namespace sebelumnya di EKS kluster Amazon lainnya akan diganti dengan pemilihan namespace saat ini.

4. Untuk menyertakan ruang nama yang diperbarui dalam aplikasi Anda, pilih Perbarui.

Selanjutnya

Langkah 4: Set RTO dan RPO

Langkah 4: Set RTO dan RPO

Anda dapat menentukan kebijakan ketahanan baru dengan RPO target Anda sendiriRTO, atau Anda dapat memilih kebijakan ketahanan yang ada dengan target yang telah ditentukan sebelumnya. RTO RPO Jika Anda ingin menggunakan salah satu kebijakan ketahanan yang ada, pilih Pilih opsi kebijakan yang ada dan pilih aplikasi target yang ada dari daftar drop-down item Opsi.

Untuk menentukan RPO target RTO Anda sendiri

1. Pilih Buat opsi kebijakan ketahanan baru.
2. Masukkan nama untuk kebijakan ketahanan.
3. (Opsional) Masukkan deskripsi untuk kebijakan ketahanan.
4. TentukanRTO/Anda RPO di bagian RTO/RPOtarget.

> **Note**
>
> - Kami telah mengisi default RTO dan RPO untuk aplikasi Anda. Anda dapat mengubah RTO dan RPO sekarang, atau setelah Anda menilai aplikasi.
> - AWS Resilience Hub memungkinkan Anda memasukkan nilai nol di RTOdan RPObidang kebijakan ketahanan Anda. Namun, saat menilai aplikasi Anda, hasil penilaian serendah mungkin mendekati nol. Oleh karena itu, jika Anda memasukkan nilai nol di RPObidang RTOdan, perkiraan beban kerja RTO dan perkiraan RPO hasil beban kerja akan mendekati nol dan status Kepatuhan untuk aplikasi Anda akan disetel ke Kebijakan yang dilanggar.

5. Untuk menentukanRTO/RPOuntuk infrastruktur dan AZ Anda, pilih panah kanan untuk memperluas Infrastruktur RTO dan RPO bagian.
6. Di RTO/RPOtarget, masukkan nilai numerik di dalam kotak dan kemudian pilih satuan waktu yang diwakili oleh nilai untuk keduanya RTOdan RPO.

   Ulangi entri ini untuk Infrastruktur dan Availability Zone di Infrastruktur RTO dan RPO bagian.
7. (Opsional) Jika Anda memiliki aplikasi Multi-region dan jika Anda ingin menentukan Region RTO danRPO, aktifkan Region - Opsional.

   Di RTOdan RPO, masukkan nilai numerik di dalam kotak dan kemudian pilih satuan waktu yang diwakili oleh nilai untuk keduanya RTOdan RPO.

Selanjutnya

the section called “Langkah 5: Siapkan penilaian terjadwal dan pemberitahuan drift”

Langkah 5: Siapkan penilaian terjadwal dan pemberitahuan drift

AWS Resilience Hub memungkinkan Anda untuk mengatur penilaian terjadwal dan pemberitahuan drift untuk menilai aplikasi Anda setiap hari dan mendapatkan pemberitahuan ketika drift terdeteksi.

Untuk mengatur notifikasi drift

1. Untuk menilai aplikasi Anda setiap hari, aktifkan Secara otomatis menilai setiap hari.

   Jika opsi ini dihidupkan, jadwal penilaian harian dimulai hanya setelah yang berikut:

- Aplikasi dinilai secara manual berhasil untuk pertama kalinya.
- Aplikasi dikonfigurasi dengan IAM peran yang sesuai.
- Jika aplikasi Anda dikonfigurasi dengan izin IAM pengguna saat ini, Anda harus membuat `AWSResilienceHubAsssessmentExecutionPolicy`

  peran menggunakan prosedur yang tepat dithe section called “Cara AWS kerja Resilience Hub IAM”.

2. Untuk mendapatkan pemberitahuan saat AWS Resilience Hub mendeteksi penyimpangan apa pun dari kebijakan ketahanan, atau ketika sumber dayanya telah hanyut, aktifkan Dapatkan pemberitahuan saat aplikasi melayang.

   Jika opsi ini diaktifkan, untuk menerima pemberitahuan drift, Anda harus menentukan topik Amazon Simple Notification Service (AmazonSNS). Untuk menyediakan SNS topik Amazon, di bagian Menyediakan SNS Topik, pilih Pilih opsi SNS topik dan pilih SNS topik Amazon dari daftar tarik-turun Pilih SNS topik.

   > **Note**
   >
   > - Untuk mengaktifkan AWS Resilience Hub untuk mempublikasikan pemberitahuan ke SNS topik Amazon Anda, SNS topik Amazon Anda harus dikonfigurasi dengan izin yang sesuai. Untuk informasi selengkapnya tentang mengonfigurasi izin, lihat. the section called “Mengaktifkan AWS Resilience Hub untuk mempublikasikan ke topik Amazon SNS Anda”
   > - Penilaian harian dapat berdampak pada kuota lari Anda. Untuk informasi lebih lanjut tentang kuota, lihat AWS Resilience Hub titik akhir dan kuota di Referensi Umum.AWS

   Untuk menggunakan SNS topik Amazon yang berada di Wilayah yang berbeda Akun AWS atau berbeda, atau keduanya, pilih Masukkan SNS topik ARN dan masukkan Nama Sumber Daya Amazon (ARN) dari SNS topik Amazon di kotak Berikan SNS topik. Untuk informasi selengkapnyaARNs, lihat Amazon Resource Names (ARNs) di Referensi AWS Umum.

Selanjutnya

Langkah 6: Pengaturan izin

Langkah 6: Pengaturan izin

AWS Resilience Hub memungkinkan Anda mengonfigurasi izin yang diperlukan untuk akun Primer dan akun Sekunder untuk menemukan dan menilai sumber daya. Namun, Anda harus menjalankan prosedur secara terpisah untuk mengonfigurasi izin untuk setiap akun.

Untuk mengonfigurasi IAM peran dan IAM izin

1. Untuk memilih IAM peran yang ada yang akan digunakan untuk mengakses sumber daya di akun saat ini, pilih IAM peran dari daftar tarik-turun Pilih IAM peran.

   > **Note**
   >
   > Untuk penyiapan lintas akun, jika Anda tidak menentukan Nama Sumber Daya Amazon (ARNs) IAM peran dalam ARN kotak Masukkan IAM peran, AWS Resilience Hub akan menggunakan IAM peran yang telah Anda pilih dari daftar tarik-turun Pilih IAM peran untuk semua akun.

   Jika tidak ada IAM peran yang melekat pada akun Anda, Anda dapat membuat IAM peran dengan menggunakan salah satu opsi berikut:

   - AWS IAMkonsol — Jika Anda memilih opsi ini, Anda harus menyelesaikan prosedur di Untuk membuat peran hub AWS Ketahanan Anda di IAM konsol.
   - AWS CLI— Jika Anda memilih opsi ini, Anda harus menyelesaikan semua langkah masuk AWS CLI.
   - CloudFormation template — Jika Anda memilih opsi ini, tergantung pada jenis akun (Akun utama atau Akun Sekunder), Anda harus membuat peran menggunakan AWS CloudFormation templat yang sesuai.
2. Pilih panah kanan untuk memperluas Tambahkan IAM peran dari akun silang - Bagian opsional.
3. Untuk memilih IAM peran dari akun silang, masukkan ARNs IAM peran di Masukkan ARN kotak IAM peran. Pastikan bahwa ARNs IAM peran yang Anda masukkan bukan milik akun saat ini.
4. Jika Anda ingin menggunakan IAM pengguna saat ini untuk menemukan sumber daya aplikasi Anda, pilih panah kanan untuk memperluas Gunakan bagian izin IAM pengguna saat ini dan pilih Saya mengerti bahwa saya harus mengonfigurasi izin secara manual untuk mengaktifkan fungsionalitas yang diperlukan di dalamnya. AWS Resilience Hub

Jika Anda memilih opsi ini, beberapa AWS Resilience Hub fitur (seperti pemberitahuan drift) mungkin tidak berfungsi seperti yang diharapkan dan input yang Anda berikan di Langkah 1 dan Langkah 3 akan diabaikan.

Selanjutnya

Langkah 7: Konfigurasikan parameter konfigurasi aplikasi

Langkah 7: Konfigurasikan parameter konfigurasi aplikasi

Bagian ini memungkinkan Anda untuk memberikan rincian dukungan failover lintas wilayah Anda menggunakan. AWS Elastic Disaster Recovery AWS Resilience Hub akan menggunakan informasi ini untuk memberikan rekomendasi ketahanan.

Untuk informasi selengkapnya tentang parameter konfigurasi aplikasi, lihatParameter konfigurasi aplikasi.

Untuk menambahkan parameter konfigurasi aplikasi (Opsional)

1. Untuk memperluas bagian Parameter konfigurasi aplikasi, pilih panah kanan.
2. Masukkan ID akun failover di kotak ID Akun. Secara default, kami telah mengisi bidang ini dengan ID akun Anda yang digunakan untuk AWS Resilience Hub, yang dapat diubah.
3. Pilih Wilayah failover dari daftar dropdown Wilayah.

> **Note**
>
> Jika Anda ingin menonaktifkan fitur ini, pilih "—" dari daftar dropdown.

Selanjutnya

Langkah 8: Tambahkan tag

Langkah 8: Tambahkan tag

Tetapkan tag atau label ke AWS sumber daya untuk mencari dan memfilter sumber daya Anda, atau melacak AWS biaya Anda.

(Opsional) Untuk menambahkan tag ke aplikasi Anda, pilih Tambahkan tag baru jika Anda ingin mengaitkan satu atau beberapa tag dengan aplikasi. Untuk informasi selengkapnya tentang tag, lihat Menandai sumber daya di Referensi AWS Umum.

Pilih Tambahkan aplikasi untuk membuat aplikasi Anda.

Selanjutnya

Langkah 9: Tinjau dan publikasikan AWS Resilience Hub aplikasi Anda

Langkah 9: Tinjau dan publikasikan AWS Resilience Hub aplikasi Anda

Setelah menerbitkan, Anda masih dapat meninjau aplikasi dan mengedit sumber dayanya. Setelah selesai, pilih Publikasikan untuk mempublikasikan aplikasi.

Untuk informasi selengkapnya tentang meninjau aplikasi dan mengedit sumber dayanya, lihat berikut ini:

- the section called “Melihat ringkasan aplikasi”
- the section called “Mengedit sumber daya aplikasi”

Selanjutnya

Langkah 10: Jalankan penilaian AWS Resilience Hub aplikasi Anda

Langkah 10: Jalankan penilaian AWS Resilience Hub aplikasi Anda

Aplikasi yang Anda terbitkan tercantum di halaman Ringkasan.

Setelah Anda mempublikasikan AWS Resilience Hub aplikasi Anda, Anda diarahkan ke halaman ringkasan aplikasi di mana Anda dapat menjalankan penilaian ketahanan. Penilaian mengevaluasi konfigurasi aplikasi Anda terhadap kebijakan ketahanan yang dilampirkan pada aplikasi Anda. Laporan penilaian dibuat yang menunjukkan bagaimana tindakan aplikasi Anda terhadap tujuan dalam kebijakan ketahanan Anda.

Untuk menjalankan penilaian ketahanan

1. Pada halaman ringkasan Aplikasi, pilih Menilai ketahanan.
2. Dalam dialog Jalankan penilaian ketahanan, masukkan nama unik untuk laporan atau gunakan nama yang dihasilkan di kotak Nama laporan.

3. Pilih Jalankan.
4. Setelah Anda diberi tahu bahwa laporan penilaian telah dibuat, pilih tab Penilaian dan penilaian Anda untuk melihat laporan.
5. Pilih tab Tinjau untuk melihat laporan penilaian aplikasi Anda.

Menggunakan AWS Resilience Hub

AWS Resilience Hub membantu Anda meningkatkan ketahanan aplikasi Anda AWS dan mengurangi waktu pemulihan jika terjadi pemadaman aplikasi.

Topik:

AWS Resilience Hub dasbor

Dasbor memberikan pandangan komprehensif tentang status ketahanan portofolio aplikasi Anda. Dasbor menggabungkan dan mengatur peristiwa ketahanan (misalnya, database yang tidak tersedia atau validasi ketahanan yang gagal), peringatan, dan wawasan dari layanan seperti dan Amazon Fault Injection Service (). CloudWatch AWS FIS

Dasbor juga menghasilkan skor ketahanan untuk setiap aplikasi yang dinilai. Skor ini menunjukkan seberapa baik kinerja aplikasi Anda saat dinilai berdasarkan kebijakan ketahanan yang direkomendasikan, alarm, prosedur operasi standar pemulihan (SOP), dan pengujian. Anda dapat menggunakan skor ini untuk mengukur peningkatan ketahanan dari waktu ke waktu.

Untuk melihat AWS Resilience Hub dasbor, pilih Dasbor dari menu navigasi. Halaman Dashboard menampilkan bagian-bagian berikut:

Status aplikasi

Status aplikasi menunjukkan apakah aplikasi telah dinilai sesuai dengan kebijakan ketahanan terlampir atau tidak. Selain itu, setelah penilaian selesai, status juga menunjukkan apakah sumber

input aplikasi Anda telah dimodifikasi atau tidak. Pilih nomor di bawah masing-masing status berikut untuk melihat semua aplikasi yang memiliki status yang sama di halaman Aplikasi:

- Aplikasi dalam kebijakan - Menunjukkan semua aplikasi yang mematuhi kebijakan ketahanan terlampir mereka.
- Kebijakan pelanggaran aplikasi - Menunjukkan semua aplikasi yang tidak mematuhi kebijakan ketahanan terlampir mereka.
- Aplikasi tidak dinilai — Menunjukkan semua aplikasi yang kepatuhannya belum dinilai atau dilacak.
- Aplikasi hanyut - Menunjukkan semua aplikasi yang telah hanyut dari kebijakan ketahanan mereka atau jika sumber dayanya telah hanyut.

Skor ketahanan aplikasi dari waktu ke waktu

Dengan skor ketahanan aplikasi dari waktu ke waktu, Anda dapat melihat grafik ketahanan aplikasi Anda selama 30 hari terakhir. Sementara menu dropdown dapat mencantumkan 10 aplikasi Anda, AWS Resilience Hub hanya menampilkan grafik hingga empat aplikasi sekaligus. Untuk informasi lebih lanjut tentang skor ketahanan, lihat. Memahami skor ketahanan

> **Note**
>
> AWS Resilience Hub tidak menjalankan penilaian terjadwal pada saat yang sama. Akibatnya, Anda mungkin perlu kembali ke skor ketahanan dari grafik waktu di lain waktu untuk melihat penilaian harian aplikasi Anda.

AWS Resilience Hub juga menggunakan Amazon CloudWatch untuk menghasilkan grafik ini. Pilih Lihat metrik CloudWatch untuk membuat dan melihat informasi lebih terperinci tentang ketahanan aplikasi Anda di dasbor Anda. CloudWatch Untuk informasi selengkapnya CloudWatch, lihat Menggunakan dasbor di Panduan CloudWatch Pengguna Amazon.

Alarm yang diterapkan

Bagian ini mencantumkan semua alarm yang telah Anda atur di Amazon CloudWatch untuk memantau semua aplikasi. Untuk informasi lebih lanjut, lihatMelihat alarm.

Eksperimen yang diimplementasikan

Bagian ini mencantumkan semua eksperimen injeksi kesalahan yang telah Anda terapkan di semua aplikasi. Untuk informasi selengkapnya, lihat Melihat eksperimen injeksi kesalahan.

Menjelaskan dan mengelola Aplikasi AWS Resilience Hub

AWS Resilience Hub Aplikasi adalah kumpulan AWS sumber daya yang terstruktur untuk mencegah dan memulihkan gangguan AWS aplikasi.

Untuk mendeskripsikan AWS Resilience Hub aplikasi, Anda memberikan nama aplikasi, sumber daya dari satu AWS CloudFormation tumpukan atau lebih, dan kebijakan ketahanan yang sesuai. Anda juga dapat menggunakan AWS Resilience Hub aplikasi apa pun yang ada sebagai templat untuk menggambarkan aplikasi Anda.

Setelah Anda menjelaskan suatu AWS Resilience Hub aplikasi, Anda harus mempublikasikannya sehingga Anda dapat menjalankan penilaian ketahanan di atasnya. Anda kemudian dapat menggunakan rekomendasi dari penilaian untuk meningkatkan ketahanan dengan menjalankan penilaian lain, membandingkan hasil, dan kemudian mengulangi proses hingga perkiraan beban kerja dan perkiraan beban kerja memenuhi target RTO dan target Anda. RPO RTO RPO

Untuk melihat halaman Aplikasi, pilih Aplikasi dari panel navigasi. Anda dapat mengidentifikasi aplikasi Anda di halaman Aplikasi dengan yang berikut:

- Nama — Nama aplikasi yang Anda berikan saat mendefinisikannya. AWS Resilience Hub
- Deskripsi — Deskripsi aplikasi yang Anda berikan saat mendefinisikannya. AWS Resilience Hub
- Status kepatuhan - AWS Resilience Hub menetapkan status aplikasi sebagai Dinilai, Tidak dinilai, Kebijakan dilanggar, atau Perubahan terdeteksi.
  - Dinilai - AWS Resilience Hub telah menilai aplikasi Anda.
  - Tidak dinilai - AWS Resilience Hub belum menilai aplikasi Anda.
  - Kebijakan dilanggar - AWS Resilience Hub telah menentukan aplikasi Anda tidak memenuhi tujuan kebijakan ketahanan Anda untuk Tujuan Waktu Pemulihan (RTO) dan Tujuan Titik Pemulihan (). RPO Tinjau dan gunakan rekomendasi yang diberikan oleh AWS Resilience Hub sebelum menilai kembali aplikasi Anda untuk ketahanan. Untuk informasi lebih lanjut tentang rekomendasi, lihatTambahkan aplikasi ke AWS Resilience Hub.
  - Perubahan terdeteksi - AWS Resilience Hub telah mendeteksi perubahan yang dibuat pada kebijakan ketahanan yang terkait dengan aplikasi Anda. Anda harus menilai kembali aplikasi

Anda AWS Resilience Hub untuk menentukan apakah aplikasi Anda memenuhi tujuan kebijakan ketahanan Anda.

- Penilaian terjadwal — Jenis sumber daya mengidentifikasi sumber daya komponen untuk aplikasi Anda. Untuk informasi selengkapnya tentang penilaian terjadwal, lihatKetahanan aplikasi.
  - Aktif - Ini menunjukkan aplikasi Anda secara otomatis dinilai setiap hari oleh AWS Resilience Hub.
  - Dinonaktifkan - Ini menunjukkan aplikasi Anda tidak dinilai secara otomatis setiap hari oleh AWS Resilience Hub dan Anda harus menilai aplikasi Anda secara manual.
- Status drift - Menunjukkan apakah aplikasi Anda telah hanyut atau tidak dari penilaian sebelumnya yang berhasil dan menetapkan salah satu status berikut:
  - Drifted - Menunjukkan bahwa aplikasi, yang sesuai dengan kebijakan ketahanannya dalam penilaian sukses sebelumnya, kini telah melanggar kebijakan ketahanan dan aplikasi berisiko. Selain itu, ini juga menunjukkan apakah sumber daya dalam sumber input, yang termasuk dalam versi aplikasi saat ini, ditambahkan atau dihapus.
  - Tidak hanyut - Menunjukkan bahwa aplikasi masih diperkirakan memenuhi RPO target RTO dan target yang ditentukan dalam kebijakan. Selain itu, ini juga menunjukkan bahwa sumber daya dalam sumber input, yang termasuk dalam versi aplikasi saat ini, tidak ditambahkan atau dihapus.
- Perkiraan beban kerja RTO - Menunjukkan perkiraan beban kerja RTO maksimum aplikasi Anda. Nilai ini adalah perkiraan beban kerja maksimum RTO dari semua jenis gangguan dari penilaian terakhir yang berhasil.
- Perkiraan beban kerja RPO - Menunjukkan perkiraan beban kerja RPO maksimum aplikasi Anda. Nilai ini adalah perkiraan beban kerja maksimum RTO dari semua jenis gangguan dari penilaian terakhir yang berhasil.
- Waktu penilaian terakhir - Menunjukkan tanggal dan waktu aplikasi Anda terakhir dinilai dengan sukses.
- Waktu pembuatan - Tanggal dan waktu aplikasi dibuat.
- ARN— Nama Sumber Daya Amazon (ARN) aplikasi Anda. Untuk informasi selengkapnyaARNs, lihat Amazon Resource Names (ARNs) di Referensi AWS Umum.

> **Note**
>
> AWS Resilience Hub dapat sepenuhnya menilai ketahanan sumber daya Amazon lintas wilayah hanya jika Anda menggunakan ECS ECR Amazon untuk repositori gambar.

Selain itu, Anda juga dapat memfilter daftar aplikasi dengan menggunakan salah satu opsi berikut di halaman Aplikasi:

- Temukan aplikasi — Masukkan nama aplikasi Anda untuk memfilter hasil dengan nama aplikasi Anda.
- Filter waktu penilaian terakhir berdasarkan tanggal dan rentang waktu - Untuk menerapkan filter ini, pilih ikon kalender dan pilih salah satu opsi berikut untuk memfilter berdasarkan hasil yang cocok dengan rentang waktu:
  - Rentang relatif - Pilih salah satu opsi yang tersedia dan pilih Terapkan.

    Jika Anda memilih opsi Rentang yang disesuaikan, masukkan durasi di Masukkan durasi kotak dan pilih satuan waktu yang sesuai dari daftar tarik-turun Satuan waktu, lalu pilih Terapkan.
  - Rentang absolut - Untuk menentukan rentang tanggal dan waktu, berikan waktu mulai dan waktu akhir, lalu pilih Terapkan.

Topik berikut menunjukkan pendekatan yang berbeda untuk menggambarkan AWS Resilience Hub aplikasi dan cara mengelolanya.

Topik

Melihat ringkasan AWS Resilience Hub aplikasi

Halaman ringkasan aplikasi di AWS Resilience Hub konsol memberikan ikhtisar informasi aplikasi dan kesehatan ketahanan Anda.

Untuk melihat ringkasan aplikasi

1. Pilih Aplikasi dari panel navigasi.
2. Pada halaman Aplikasi, pilih nama aplikasi yang ingin Anda lihat.

Halaman ringkasan aplikasi memiliki bagian berikut.

Topik

Ringkasan Penilaian

Bagian ini memberikan ringkasan penilaian terakhir yang berhasil dan menyoroti rekomendasi penting sebagai wawasan yang dapat ditindaklanjuti. AWS Resilience Hub menggunakan kemampuan AI generatif Amazon Bedrock untuk membantu memfokuskan pengguna pada rekomendasi ketahanan paling penting yang disediakan oleh. AWS Resilience Hub Dengan berfokus pada item penting, Anda dapat fokus pada rekomendasi paling penting yang meningkatkan postur ketahanan aplikasi Anda. Pilih rekomendasi untuk melihat ringkasannya dan pilih Lihat detail untuk melihat detail selengkapnya tentang rekomendasi di bagian yang relevan dari laporan penilaian. Untuk informasi lebih lanjut tentang meninjau laporan penilaian, lihatthe section called “Meninjau laporan penilaian”.

> **Note**
>
> - Ringkasan penilaian ini hanya tersedia di Wilayah AS Timur (Virginia N.).
> - Ringkasan penilaian yang dihasilkan oleh model bahasa besar (LLMs) di Amazon Bedrock hanyalah saran. Tingkat teknologi AI generatif saat ini tidak sempurna dan LLMs tidak

sempurna. Bias dan jawaban yang salah, meskipun jarang, harus diharapkan. Tinjau setiap rekomendasi dalam ringkasan Penilaian sebelum Anda menggunakan output dari fileLLM.

Ringkasan

Bagian ini memberikan ringkasan aplikasi yang dipilih di bagian berikut:

- Info aplikasi — Bagian ini memberikan informasi berikut tentang aplikasi yang dipilih:
  - Status aplikasi - Menunjukkan status aplikasi.
  - Deskripsi — Deskripsi aplikasi.
  - Versi - Menunjukkan versi aplikasi yang saat ini dinilai.
  - Kebijakan ketahanan - Menunjukkan kebijakan ketahanan yang dilampirkan aplikasi. Untuk informasi selengkapnya tentang kebijakan ketahanan, lihat. Mengelola kebijakan ketahanan
- Application drifts — Bagian ini menyoroti drift yang terdeteksi saat menjalankan penilaian untuk aplikasi yang dipilih untuk memeriksa apakah aplikasi tersebut sesuai dengan kebijakan ketahanannya. Selain itu, ia juga memeriksa apakah ada sumber daya yang telah ditambahkan atau dihapus sejak terakhir kali versi aplikasi diterbitkan. Bagian ini menampilkan informasi berikut:
  - Pergeseran kebijakan — Pilih nomor di bawah ini untuk melihat semua Komponen Aplikasi yang sesuai dengan kebijakan dalam penilaian sebelumnya tetapi gagal mematuhi penilaian saat ini.
  - Penyimpangan sumber daya — Pilih nomor di bawah ini untuk melihat semua sumber daya yang hanyut dalam penilaian terbaru.

Ketahanan aplikasi

Metrik yang ditampilkan di bagian Skor Ketahanan berasal dari penilaian ketahanan aplikasi terbaru.

Skor ketahanan

Skor ketahanan membantu Anda mengukur kesiapan Anda untuk menangani potensi gangguan. Skor ini mencerminkan seberapa dekat aplikasi Anda telah mengikuti AWS Resilience Hub rekomendasi untuk memenuhi kebijakan ketahanan aplikasi, alarm, prosedur operasi standar (SOPs), dan pengujian.

Skor ketahanan maksimum yang dapat dicapai aplikasi Anda adalah 100%. Skor mewakili semua tes yang direkomendasikan yang berjalan dalam periode waktu yang telah ditentukan. Ini menunjukkan bahwa tes memulai alarm yang benar, dan alarm memulai yang benar. SOP

Misalnya, anggaplah itu AWS Resilience Hub merekomendasikan satu tes dengan satu alarm dan satuSOP. Ketika tes berjalan, alarm memulai yang terkaitSOP, dan kemudian berjalan dengan sukses. Untuk informasi lebih lanjut tentang skor ketahanan, lihat. Memahami skor ketahanan

Alarm yang diterapkan

Ringkasan aplikasi Bagian alarm yang diterapkan mencantumkan alarm yang Anda atur di Amazon CloudWatch untuk memantau aplikasi. Untuk informasi selengkapnya tentang alarm, lihatMengelola alarm-alarm.

Eksperimen yang diterapkan

Ringkasan aplikasi Bagian eksperimen injeksi kesalahan menunjukkan daftar eksperimen injeksi kesalahan. Untuk informasi lebih lanjut tentang eksperimen injeksi kesalahan, lihatMengelola eksperimen Layanan Injeksi Kesalahan Amazon.

Mengedit sumber daya AWS Resilience Hub aplikasi

Untuk menerima penilaian ketahanan yang akurat dan bermanfaat, pastikan deskripsi aplikasi Anda diperbarui dan sesuai dengan aplikasi dan sumber daya Anda yang sebenarnya AWS . Laporan penilaian, validasi, dan rekomendasi didasarkan pada sumber daya yang terdaftar. Jika Anda menambah atau menghapus sumber daya dari AWS aplikasi, Anda harus mencerminkan perubahan tersebut AWS Resilience Hub.

AWS Resilience Hub memberikan transparansi tentang sumber aplikasi Anda. Anda dapat mengidentifikasi dan mengedit sumber daya dan sumber aplikasi dalam aplikasi Anda.

> **Note**
>
> Mengedit sumber daya hanya memodifikasi AWS Resilience Hub referensi aplikasi Anda. Tidak ada perubahan yang dilakukan pada sumber daya Anda yang sebenarnya.

Anda dapat menambahkan sumber daya yang hilang, memodifikasi sumber daya yang ada, atau menghapus sumber daya yang tidak Anda butuhkan. Sumber daya dikelompokkan ke dalam Komponen Aplikasi logis (AppComponents). Anda dapat mengedit AppComponents untuk lebih mencerminkan struktur aplikasi Anda.

Tambahkan atau perbarui sumber daya aplikasi Anda dengan mengedit versi draf aplikasi Anda dan memublikasikan perubahan ke versi (rilis) baru. AWS Resilience Hub menggunakan versi rilis (yang mencakup sumber daya yang diperbarui) aplikasi Anda untuk menjalankan penilaian ketahanan.

Untuk menilai ketahanan aplikasi Anda

1. Pada panel navigasi, pilih Aplikasi.
2. Pada halaman Aplikasi, pilih nama aplikasi yang ingin Anda edit.
3. Dari menu Tindakan, pilih Menilai ketahanan.
4. Dalam dialog Jalankan penilaian ketahanan, masukkan nama unik untuk laporan atau gunakan nama yang dihasilkan di kotak Nama laporan.
5. Pilih Jalankan.
6. Setelah Anda diberi tahu bahwa laporan penilaian telah dibuat, pilih tab Penilaian dan penilaian Anda untuk melihat laporan.
7. Pilih tab Tinjau untuk melihat laporan penilaian aplikasi Anda.

Untuk mengaktifkan penilaian terjadwal

1. Pada panel navigasi, pilih Aplikasi.
2. Pada halaman Aplikasi, pilih aplikasi yang ingin Anda aktifkan penilaian terjadwal.
3. Aktifkan Secara otomatis menilai setiap hari.

Untuk menonaktifkan penilaian terjadwal

1. Pada panel navigasi, pilih Aplikasi.
2. Pada halaman Aplikasi, pilih aplikasi yang ingin Anda aktifkan penilaian terjadwal.
3. Matikan Secara otomatis menilai setiap hari.

> **Note**
>
> Menonaktifkan penilaian terjadwal akan menonaktifkan pemberitahuan drift.

4. Pilih Matikan.

Untuk mengaktifkan pemberitahuan drift untuk aplikasi Anda

1. Pada panel navigasi, pilih Aplikasi.
2. Pada halaman Aplikasi, pilih aplikasi yang ingin Anda aktifkan pemberitahuan drift atau edit pengaturan notifikasi drift.
3. Anda dapat mengedit notifikasi drift dengan memilih salah satu opsi berikut:
   - Dari Tindakan, pilih Aktifkan pemberitahuan drift.
   - Pilih Aktifkan pemberitahuan di bagian Application drifts.
4. Selesaikan langkah-langkahnyaLangkah 5: Siapkan penilaian terjadwal dan pemberitahuan drift, lalu kembali ke prosedur ini.
5. Pilih Aktifkan.

   Mengaktifkan pemberitahuan drift juga akan memungkinkan penilaian terjadwal.

Untuk mengedit notifikasi drift untuk aplikasi Anda

> **Note**
>
> Prosedur ini berlaku jika Anda telah mengaktifkan penilaian terjadwal (Secara otomatis menilai setiap hari diaktifkan) dan pemberitahuan drift.

1. Pada panel navigasi, pilih Aplikasi.
2. Pada halaman Aplikasi, pilih aplikasi yang ingin Anda aktifkan pemberitahuan drift atau edit pengaturan notifikasi drift.
3. Anda dapat mengedit notifikasi drift dengan memilih salah satu opsi berikut:
   - Dari Tindakan, pilih Edit notifikasi drift.
   - Pilih Edit notifikasi di bagian Application drifts.
4. Selesaikan langkah-langkahnyaLangkah 5: Siapkan penilaian terjadwal dan pemberitahuan drift, lalu kembali ke prosedur ini.
5. Pilih Simpan.

Untuk memperbarui izin keamanan aplikasi Anda

1. Pada panel navigasi, pilih Aplikasi.
2. Pada halaman Aplikasi, pilih aplikasi yang ingin Anda perbarui izin keamanannya.
3. Dari Tindakan, pilih Perbarui izin.
4. Untuk memperbarui izin keamanan, selesaikan langkah-langkahnyaLangkah 6: Pengaturan izin, lalu kembali ke prosedur ini.
5. Pilih Simpan dan perbarui.

Untuk melampirkan kebijakan ketahanan ke aplikasi Anda

1. Pada panel navigasi, pilih Aplikasi.
2. Pada halaman Aplikasi, pilih nama aplikasi yang ingin Anda edit.
3. Dari menu Tindakan, pilih Lampirkan kebijakan ketahanan.
4. Dalam dialog Lampirkan kebijakan, pilih kebijakan ketahanan dari Pilih daftar tarik-turun kebijakan ketahanan.
5. Pilih Lampirkan.

Untuk mengedit sumber input, sumber daya, dan AppComponents aplikasi Anda

1. Pada panel navigasi, pilih Aplikasi.
2. Pada halaman Aplikasi, pilih nama aplikasi yang ingin Anda edit.
3. Pilih tab Struktur aplikasi.
4. Pilih tanda plus + sebelum Versi, lalu pilih versi aplikasi dengan status Draft.
5. Untuk mengedit sumber input, sumber daya, dan AppComponents aplikasi Anda, selesaikan langkah-langkah dalam prosedur berikut.

Untuk mengedit sumber masukan aplikasi Anda

1. Untuk mengedit sumber input aplikasi Anda, pilih tab Sumber input.

   Bagian Sumber input mencantumkan semua sumber input sumber daya aplikasi Anda. Anda dapat mengidentifikasi sumber input dengan yang berikut:

- Nama sumber — Nama sumber input. Pilih nama sumber untuk melihat detailnya di aplikasi masing-masing. Untuk sumber input yang ditambahkan secara manual, tautan tidak akan tersedia. Misalnya, jika Anda memilih nama sumber yang diimpor dari AWS CloudFormation tumpukan, Anda akan diarahkan ke halaman detail tumpukan di AWS CloudFormation konsol.
- Sumber ARN — Nama Sumber Daya Amazon (ARN) dari sumber input. Pilih ARN untuk melihat detailnya di aplikasi masing-masing. Untuk sumber input yang ditambahkan secara manual, tautan tidak akan tersedia. Misalnya, jika Anda memilih ARN yang diimpor dari AWS CloudFormation tumpukan, Anda akan diarahkan ke halaman detail tumpukan di konsol. AWS CloudFormation
- Jenis Sumber — Jenis sumber input. Sumber input termasuk kluster Amazon EKS, AWS CloudFormation tumpukan, AppRegistry aplikasi, file status Terraform AWS Resource Groups, dan sumber daya yang ditambahkan secara manual.
- Sumber daya terkait — Jumlah sumber daya yang terkait dengan sumber input. Pilih nomor untuk melihat semua sumber daya terkait dari sumber input di tab Sumber Daya.

2. Untuk menambahkan sumber input ke aplikasi Anda, dari bagian Sumber input, pilih Tambahkan sumber input. Untuk informasi selengkapnya tentang menambahkan sumber input, lihatthe section called “Langkah 3: Tambahkan sumber daya ke AWS Resilience Hub aplikasi Anda”.
3. Untuk mengedit sumber input, pilih sumber input dan pilih salah satu opsi berikut dari Tindakan:

   - Impor ulang sumber input (hingga 5) - Mengimpor ulang hingga lima sumber input yang dipilih.
   - Hapus sumber input — Menghapus sumber input yang dipilih.

     Untuk mempublikasikan aplikasi, itu harus berisi minimal satu sumber input. Jika Anda menghapus semua sumber input, Publikasikan versi baru akan dinonaktifkan.

Untuk mengedit sumber daya aplikasi Anda

1. Untuk mengedit sumber daya aplikasi Anda, pilih tab Sumber Daya.

> **Note**
>
> Untuk melihat daftar sumber daya yang belum dinilai, pilih Lihat sumber daya yang belum dinilai.

Bagian Sumber daya mencantumkan sumber daya dari aplikasi yang Anda pilih untuk digunakan sebagai templat untuk deskripsi aplikasi Anda. Untuk meningkatkan pengalaman pencarian Anda, AWS Resilience Hub telah mengelompokkan sumber daya berdasarkan beberapa kriteria pencarian. Kriteria pencarian ini mencakup AppComponent tipe, Sumber daya yang tidak didukung, dan sumber daya yang dikecualikan. Untuk memfilter sumber daya berdasarkan kriteria pencarian di tabel Sumber daya, pilih nomor di bawah masing-masing kriteria pencarian.

Anda dapat mengidentifikasi sumber daya dengan yang berikut:

- Logical ID - ID logis adalah nama yang digunakan untuk mengidentifikasi sumber daya di AWS CloudFormation tumpukan Anda, file status Terraform, aplikasi yang ditambahkan secara manual, AppRegistry aplikasi, atau. AWS Resource Groups

  > **Note**
  >
  > - Terraform memungkinkan Anda menggunakan nama yang sama untuk jenis sumber daya yang berbeda. Oleh karena itu, Anda melihat "- tipe sumber daya" di akhir ID logis untuk sumber daya yang memiliki nama yang sama.
  > - Untuk melihat contoh semua sumber daya aplikasi, pilih tanda plus (+) sebelum ID Logis. Untuk melihat semua contoh sumber daya aplikasi, pilih tanda plus (+) sebelum ID Logis dari setiap sumber daya.
  >
  >   Untuk informasi selengkapnya tentang sumber daya yang didukung, lihatthe section called “ AWS Resilience Hub Sumber daya yang didukung”.

- Jenis sumber daya — Jenis sumber daya mengidentifikasi sumber daya komponen untuk aplikasi Anda. Misalnya, `AWS::EC2::Instance` mendeklarasikan instans Amazon EC2. Untuk informasi selengkapnya tentang pengelompokan AppComponent sumber daya, lihatMengelompokkan sumber daya dalam Komponen Aplikasi.
- Nama sumber — Nama sumber input. Pilih nama sumber untuk melihat detailnya di aplikasi masing-masing. Untuk sumber input yang ditambahkan secara manual, tautan tidak akan tersedia. Misalnya, jika Anda memilih nama sumber yang diimpor dari AWS CloudFormation tumpukan, Anda akan diarahkan ke halaman detail tumpukan di AWS CloudFormation halaman.

- Jenis Sumber — Jenis sumber input. Sumber input termasuk AWS CloudFormation tumpukan, AppRegistry aplikasi,, file status Terraform AWS Resource Groups, dan sumber daya yang ditambahkan secara manual.

  > **Note**
  >
  > Untuk mengedit kluster Amazon EKS Anda, selesaikan langkah-langkah di Untuk mengedit sumber input prosedur AWS Resilience Hub aplikasi Anda.

- Source stack — AWS CloudFormation Tumpukan yang berisi sumber daya. Kolom ini tergantung pada jenis struktur aplikasi yang Anda pilih.
- ID fisik — Pengenal yang ditetapkan sebenarnya untuk sumber daya tersebut, seperti ID instans Amazon EC2 atau nama bucket S3.
- Termasuk - Ini menunjukkan apakah AWS Resilience Hub termasuk sumber daya ini dalam aplikasi.
- Dapat dinilai — Ini menunjukkan apakah AWS Resilience Hub akan menilai sumber daya Anda untuk ketahanan.
- AppComponents— AWS Resilience Hub Komponen yang ditugaskan ke sumber daya ini ketika struktur aplikasinya ditemukan.
- Nama — Nama sumber daya aplikasi.
- Akun — AWS Akun yang memiliki sumber daya fisik.

2. Untuk menemukan sumber daya yang tidak terdaftar, masukkan ID logis sumber daya di kotak pencarian.
3. Untuk menghapus sumber daya dari aplikasi Anda, pilih sumber daya, lalu pilih Kecualikan sumber daya dari Tindakan.
4. Untuk menyelesaikan sumber daya pada aplikasi Anda, pilih Refresh resource.
5. Untuk memodifikasi sumber daya aplikasi yang ada, selesaikan langkah-langkah berikut:

   a. Pilih sumber daya, lalu pilih Perbarui tumpukan dari Tindakan.

   b. Di halaman Perbarui tumpukan, untuk memperbarui sumber daya Anda, selesaikan prosedur yang sesuaiLangkah 3: Tambahkan sumber daya ke AWS Resilience Hub aplikasi Anda, lalu kembali ke prosedur ini.

   c. Pilih Simpan.

6. Untuk menambahkan sumber daya ke aplikasi Anda, dari Tindakan, pilih Tambahkan sumber daya dan selesaikan langkah-langkah berikut:

    a. Pilih jenis sumber daya dari daftar dropdown Jenis sumber daya.

    b. Pilih AppComponent dari daftar AppComponentdropdown.

    c. Masukkan ID logis sumber daya di kotak Nama sumber daya.

    d. Masukkan ID sumber daya fisik, atau nama sumber daya, atau ARN sumber daya di kotak Pengenal sumber daya.

    e. Pilih Tambahkan.

7. Untuk mengedit nama sumber daya, pilih sumber daya, pilih Edit nama sumber daya dari Tindakan, lalu selesaikan langkah-langkah berikut:

    a. Masukkan ID logis sumber daya di kotak Nama sumber daya.

    b. Pilih Simpan.

8. Untuk mengedit pengenal sumber daya, pilih sumber daya, pilih Edit pengenal sumber daya dari Tindakan, lalu selesaikan langkah-langkah berikut:

    a. Masukkan ID sumber daya fisik, atau nama sumber daya, atau ARN sumber daya di kotak Pengenal sumber daya.

    b. Pilih Simpan.

9. Untuk mengubah AppComponent, pilih sumber daya, pilih Ubah AppComponent dari Tindakan, dan selesaikan langkah-langkah berikut:

    a. Pilih AppComponent dari daftar AppComponentdropdown.

    b. Pilih Tambahkan.

10. Untuk menghapus sumber daya, pilih sumber daya, lalu pilih Hapus sumber daya dari Tindakan.

11. Untuk menyertakan sumber daya, pilih sumber daya, lalu pilih Sertakan sumber daya dari Tindakan.

Untuk mengedit aplikasi Anda AppComponents

1. Untuk mengedit aplikasi Anda, pilih AppComponentstab. AppComponents

> **Note**
>
> Untuk informasi selengkapnya tentang pengelompokan AppComponent sumber daya, lihatMengelompokkan sumber daya dalam Komponen Aplikasi.

AppComponentsBagian ini mencantumkan semua komponen logis tempat sumber daya dikelompokkan. Anda dapat mengidentifikasi AppComponents dengan yang berikut:

- AppComponent Nama — Nama AWS Resilience Hub komponen yang ditugaskan ke sumber daya ini ketika struktur aplikasinya ditemukan.
- AppComponent Jenis — Jenis AWS Resilience Hub komponen.
- Nama sumber — Nama sumber input. Pilih nama sumber untuk melihat detailnya di aplikasi masing-masing. Misalnya, jika Anda memilih nama sumber yang diimpor dari AWS CloudFormation tumpukan, Anda akan diarahkan ke halaman detail tumpukan di AWS CloudFormation halaman.
- Jumlah sumber daya — Jumlah sumber daya yang terkait dengan sumber input. Pilih nomor untuk melihat semua sumber daya terkait dari sumber input di tab Sumber Daya.

2. Untuk membuat AppComponent, dari menu Tindakan, pilih Buat baru AppComponent dan selesaikan langkah-langkah berikut:

   a. Masukkan nama untuk AppComponent di kotak AppComponentnama. Sebagai referensi, kami telah mengisi bidang ini dengan nama sampel.

   b. Pilih jenis AppComponent dari daftar dropdown AppComponenttipe.

   c. Pilih Simpan.

3. Untuk mengedit AppComponent, pilih AppComponent, lalu pilih Edit AppComponent dari Tindakan.
4. Untuk menghapus AppComponent, pilih AppComponent, lalu pilih Hapus AppComponent dari Tindakan.

Setelah Anda membuat perubahan pada daftar sumber daya Anda, Anda akan menerima peringatan yang menunjukkan bahwa perubahan telah dilakukan pada versi draf aplikasi Anda. Untuk menjalankan penilaian ketahanan yang akurat, Anda harus mempublikasikan versi baru aplikasi Anda. Untuk informasi selengkapnya tentang cara mempublikasikan versi baru, lihatMenerbitkan versi AWS Resilience Hub aplikasi baru.

Mengelola Komponen Aplikasi

Komponen Aplikasi (AppComponent) adalah sekelompok AWS sumber daya terkait yang bekerja dan gagal sebagai satu unit. Misalnya, jika Anda memiliki basis data primer dan replika, kedua database milik yang sama. AppComponent AWS Resilience Hub memiliki aturan yang mengatur AWS sumber daya mana yang dapat dimiliki oleh AppComponent tipe mana. Misalnya, `DBInstance` bisa menjadi milik `AWS::ResilienceHub::DatabaseAppComponent` dan bukan milik`AWS::ResilienceHub::ComputeAppComponent`.

AWS Resilience Hub AppComponents Dukungan sumber daya berikut:

- `AWS::ResilienceHub::ComputeAppComponent`
  - `AWS::ApiGateway::RestApi`
  - `AWS::ApiGatewayV2::Api`
  - `AWS::AutoScaling::AutoScalingGroup`
  - `AWS::EC2::Instance`
  - `AWS::ECS::Service`
  - `AWS::EKS::Deployment`
  - `AWS::EKS::ReplicaSet`
  - `AWS::EKS::Pod`
  - `AWS::Lambda::Function`
  - `AWS::StepFunctions::StateMachine`
- `AWS::ResilienceHub::DatabaseAppComponent`
  - `AWS::DocDB::DBCluster`
  - `AWS::DynamoDB::Table`
  - `AWS::RDS::DBCluster`
  - `AWS::RDS::DBInstance`
- `AWS::ResilienceHub::NetworkingAppComponent`
  - `AWS::EC2::NatGateway`
  - `AWS::ElasticLoadBalancing::LoadBalancer`
  - `AWS::ElasticLoadBalancingV2::LoadBalancer`
  - `AWS::Route53::RecordSet`
- `AWS:ResilienceHub::NotificationAppComponent`

  - `AWS::SNS::Topic`
- `AWS::ResilienceHub::QueueAppComponent`
  - `AWS::SQS::Queue`
- `AWS::ResilienceHub::StorageAppComponent`
  - `AWS::Backup::BackupPlan`
  - `AWS::EC2::Volume`
  - `AWS::EFS::FileSystem`
  - `AWS::FSx::FileSystem`

    > **Note**
    >
    > Saat ini, hanya AWS Resilience Hub mendukung Amazon FSx untuk Windows File Server.

  - `AWS::S3::Bucket`

Topik

- Mengelompokkan sumber daya dalam Komponen Aplikasi

Mengelompokkan sumber daya dalam Komponen Aplikasi

Ketika aplikasi diimpor AWS Resilience Hub bersama dengan sumber dayanya, AWS Resilience Hub membuat upaya terbaik untuk mengelompokkan sumber daya terkait ke dalam hal yang sama AppComponent, tetapi mungkin tidak selalu 100 persen akurat. Selain itu, AWS Resilience Hub lakukan aktivitas berikut setelah aplikasi Anda dan sumber dayanya berhasil diimpor:

- Memindai sumber daya Anda untuk memeriksa apakah mereka dapat dikelompokkan ulang menjadi baru AppComponents untuk meningkatkan akurasi penilaian.
- Jika AWS Resilience Hub mengidentifikasi sumber daya yang dapat dikelompokkan ulang menjadi baru AppComponents, itu menampilkan hal yang sama seperti rekomendasi dan memungkinkan Anda untuk menerima, memodifikasi (menambah atau menghapus), atau menolak yang sama. Pada tahun AWS Resilience Hub, tingkat kepercayaan yang ditetapkan untuk rekomendasi pengelompokan menunjukkan tingkat kepastian dengan mana sumber daya harus dikelompokkan bersama berdasarkan atribut dan metadata mereka. Tingkat kepercayaan yang tinggi menunjukkan bahwa AWS Resilience Hub memiliki tingkat kepercayaan 90% atau di atas bahwa sumber daya

dalam kelompok itu terkait dan harus dikelompokkan bersama. Tingkat kepercayaan sedang menunjukkan bahwa AWS Resilience Hub memiliki tingkat kepercayaan antara 70% dan 90% bahwa sumber daya dalam kelompok itu terkait dan harus dikelompokkan bersama.

> **Note**
>
> AWS Resilience Hub memerlukan pengelompokan yang benar sehingga dapat menghitung perkiraan beban kerja RTO dan perkiraan beban kerja untuk menghasilkan rekomendasiRPO.

Berikut ini adalah contoh pengelompokan yang benar:

- Kelompokkan basis data utama dan replika di bawah satu. AppComponent
- Kelompokkan bucket Amazon S3 dan replikasi targetnya di bawah satu ember. AppComponent
- Kelompokkan EC2 instans Amazon yang menjalankan aplikasi yang sama di bawah satu AppComponent.
- Kelompokkan SQS antrian Amazon dan antrian huruf mati di bawah satu. AppComponent
- Kelompokkan ECS layanan Amazon di satu Wilayah dan failover ECS layanan Amazon di Wilayah lain di bawah satu AppComponent Wilayah.

Untuk informasi selengkapnya tentang meninjau dan menyertakan rekomendasi pengelompokan sumber daya berdasarkan AWS Resilience Hub, lihat topik berikut:

- AWS Resilience Hub rekomendasi pengelompokan sumber daya
- Mengelompokkan sumber daya secara manual menjadi AppComponent

AWS Resilience Hub rekomendasi pengelompokan sumber daya

Bagian ini menjelaskan cara membuat dan meninjau rekomendasi pengelompokan sumber daya di AWS Resilience Hub.

> **Note**
>
> Anda dapat memberikan IAM izin yang diperlukan yang diperlukan untuk bekerja AWS Resilience Hub dengan menggunakan kebijakan

`AWSResilienceHubAsssessmentExecutionPolicy` AWS terkelola.
Untuk informasi selengkapnya tentang kebijakan AWS terkelola,
lihatAWSResilienceHubAsssessmentExecutionPolicy.

Untuk melihat rekomendasi pengelompokan sumber daya

1. Pada panel navigasi, pilih Aplikasi.
2. Pilih Tambahkan halaman aplikasi, pilih nama aplikasi yang ingin Anda tinjau rekomendasi pengelompokan sumber daya.
3. Pilih tab Struktur aplikasi.
4. Jika AWS Resilience Hub menampilkan peringatan informasi, pilih Tinjau rekomendasi untuk melihat semua rekomendasi pengelompokan sumber daya. Jika tidak, selesaikan langkah-langkah berikut untuk menghasilkan rekomendasi pengelompokan sumber daya secara manual:

   a. Pilih Sumber daya.

   b. Pilih Dapatkan rekomendasi pengelompokan dari menu Tindakan.

      AWS Resilience Hub memindai sumber daya Anda untuk memeriksa bagaimana mereka dapat dikelompokkan dengan cara terbaik menjadi relevan AppComponents untuk meningkatkan akurasi penilaian. Jika AWS Resilience Hub mengetahui bahwa sumber daya Anda dapat dikelompokkan bersama, ini akan menampilkan peringatan informasi untuk hal yang sama.

   c. Jika peringatan informasi ditampilkan, pilih Tinjau rekomendasi untuk melihat semua rekomendasi pengelompokan sumber daya.

   Anda dapat mengidentifikasi AppComponents di bagian rekomendasi pengelompokan sumber daya ulasan menggunakan yang berikut ini:

   - AppComponent nama — Nama AppComponent di mana sumber daya akan dikelompokkan.
   - Tingkat kepercayaan - Menunjukkan tingkat kepercayaan AWS Resilience Hub dalam rekomendasi pengelompokan.
   - Jumlah sumber daya - Menunjukkan jumlah sumber daya yang akan dikelompokkan dalam. AppComponent
   - AppComponent type — Menunjukkan jenis AppComponent.

Untuk melihat sumber daya yang akan dikelompokkan AppComponents

1. Selesaikan langkah-langkah dalam Untuk melihat rekomendasi pengelompokan sumber dayaprosedur dan kemudian kembali ke prosedur ini.
2. Di bagian rekomendasi pengelompokan sumber daya ulasan, pilih kotak centang (berdekatan dengan AppComponent nama) untuk melihat semua sumber daya yang akan dikelompokkan bersama dalam yang dipilih. AppComponent Jika Anda memilih beberapa kotak centang, AWS Resilience Hub menampilkan bagian pilihan rekomendasi yang dihasilkan secara dinamis yang mengelompokkan yang dipilih AppComponents di bawah AppComponent jenisnya masing-masing. Pilih nomor di bawah setiap AppComponent jenis untuk melihat semua sumber daya yang akan dikelompokkan bersama dalam yang dipilih AppComponent.

   Anda dapat mengidentifikasi sumber daya yang akan dikelompokkan dalam yang dipilih AppComponent di bagian Sumber daya menggunakan yang berikut ini:

   - Logical ID — Menunjukkan ID logis dari sumber daya. ID logis adalah nama yang digunakan untuk mengidentifikasi sumber daya di AWS CloudFormation tumpukan Anda, file status Terraform, aplikasi yang ditambahkan secara manual, AppRegistry aplikasi, atau. AWS Resource Groups
   - ID fisik — Pengidentifikasi aktual yang ditetapkan untuk sumber daya, seperti ID EC2 instans Amazon atau nama bucket Amazon S3.
   - Jenis - Menunjukkan jenis sumber daya.
   - Wilayah — AWS Wilayah di mana sumber daya berada.

Untuk menerima rekomendasi pengelompokan sumber daya

1. Selesaikan langkah-langkah dalam Untuk melihat rekomendasi pengelompokan sumber dayaprosedur dan kemudian kembali ke prosedur ini.
2. Di bagian Tinjau rekomendasi pengelompokan sumber daya, pilih semua kotak centang yang berdekatan dengan AppComponentnama. Untuk menemukan yang spesifik AppComponent, masukkan AppComponent nama di AppComponents kotak Temukan.

   > **Note**
   >
   > Secara default, AWS Resilience Hub menampilkan semua rekomendasi pengelompokan sumber daya. Untuk memfilter tabel dengan rekomendasi pengelompokan sumber

daya yang ditolak sebelumnya, pilih Sebelumnya ditolak dari menu tarik-turun yang berdekatan dengan kotak Temukan. AppComponents

3. Pilih Terima.
4. Pilih Terima dalam dialog Terima rekomendasi pengelompokan sumber daya.

   AWS Resilience Hub menampilkan peringatan informasi jika pengelompokan sumber daya berhasil. Jika Anda hanya menerima sebagian dari rekomendasi pengelompokan sumber daya, bagian rekomendasi pengelompokan sumber daya akan menampilkan semua rekomendasi pengelompokan sumber daya yang belum Anda terima.

Untuk menolak rekomendasi pengelompokan sumber daya

1. Selesaikan langkah-langkah dalam Untuk melihat rekomendasi pengelompokan sumber dayaprosedur dan kemudian kembali ke prosedur ini.
2. Di bagian Rekomendasi pengelompokan sumber daya ulasan, pilih semua kotak centang yang berdekatan dengan AppComponentnama. Untuk menemukan yang spesifik AppComponent, masukkan AppComponent nama di AppComponents kotak Temukan.

   > **Note**
   >
   > Secara default, AWS Resilience Hub menampilkan semua rekomendasi pengelompokan sumber daya. Untuk memfilter tabel dengan rekomendasi pengelompokan sumber daya yang ditolak sebelumnya, pilih Sebelumnya ditolak dari menu tarik-turun yang berdekatan dengan kotak Temukan. AppComponents

3. Pilih Tolak.
4. Pilih salah satu alasan untuk menolak rekomendasi pengelompokan sumber daya dan kemudian pilih Tolak dalam dialog Tolak rekomendasi pengelompokan sumber daya.

   AWS Resilience Hub menampilkan peringatan informasi yang mengonfirmasi hal yang sama. Jika Anda hanya menolak sebagian dari rekomendasi pengelompokan sumber daya, bagian rekomendasi pengelompokan sumber daya akan menampilkan semua rekomendasi pengelompokan sumber daya yang belum Anda terima.

Mengelompokkan sumber daya secara manual menjadi AppComponent

Bagian ini menjelaskan cara mengelompokkan sumber daya secara manual ke dalam AppComponent dan menetapkan yang berbeda AppComponent ke sumber daya di AWS Resilience Hub.

Untuk mengelompokkan sumber daya

1. Pada panel navigasi, pilih Aplikasi.
2. Pada halaman Aplikasi, pilih nama aplikasi yang berisi sumber daya yang ingin Anda kelompokkan.
3. Pilih tab Struktur aplikasi.
4. Di bawah tab Versi, pilih versi aplikasi dengan status Draf.
5. Pilih tab Sumber Daya.
6. Pilih kotak centang yang berdekatan dengan Logical ID untuk memilih semua sumber daya yang ingin Anda kelompokkan.

   > **Note**
   >
   > Anda tidak dapat memilih sumber daya yang ditambahkan secara manual.

7. Pilih Tindakan, lalu pilih Sumber daya grup.
8. Pilih AppComponent dari daftar AppComponent tarik-turun Pilih tempat Anda ingin mengelompokkan sumber daya.
9. Pilih Simpan.
10. PilihPublikasikan versi baru.
11. Pilih tab Struktur aplikasi.
12. Untuk melihat versi aplikasi Anda yang dipublikasikan, selesaikan langkah-langkah berikut:
    a. Di bawah tab Versi, pilih versi aplikasi dengan status rilis saat ini.
    b. Pilih tab Sumber Daya.

Untuk menetapkan sumber daya ke AppComponent

1. Pada panel navigasi, pilih Aplikasi.

2. Pada halaman Aplikasi, pilih nama aplikasi yang berisi sumber daya yang ingin Anda kumpulkan kembali.
3. Pilih tab Struktur aplikasi.
4. Di bawah Versi, pilih versi aplikasi dengan status Draft.
5. Pilih tab Sumber Daya.
6. Pilih kotak centang yang berdekatan dengan Logical ID untuk memilih sumber daya.
7. Pilih Ubah AppComponent dari menu Tindakan.
8. Untuk menghapus arus AppComponent dari AppComponentbagian, pilih X di sudut kanan atas label yang menampilkan nama Anda saat ini. AppComponent
9. Untuk mengelompokkan sumber daya dalam yang berbeda AppComponent, pilih yang berbeda AppComponent dari daftar AppComponent dropdown Pilih.
10. Pilih Tambahkan.
11. Hapus semua yang kosong AppComponents dari AppComponentstab.
12. PilihPublikasikan versi baru.
13. Pilih tab Struktur aplikasi.
14. Untuk melihat versi aplikasi Anda yang dipublikasikan, selesaikan langkah-langkah berikut:

    a. Di bawah tab Versi, pilih versi aplikasi dengan status rilis saat ini.

    b. Pilih tab Sumber Daya.

Menerbitkan versi AWS Resilience Hub aplikasi baru

Setelah Anda membuat perubahan pada sumber daya AWS Resilience Hub aplikasi seperti yang dijelaskan dalamMengedit sumber daya AWS Resilience Hub aplikasi, Anda harus mempublikasikan versi baru aplikasi Anda untuk menjalankan penilaian ketahanan yang akurat. Selain itu, Anda mungkin perlu mempublikasikan versi baru aplikasi Anda jika Anda menambahkan alarm baru yang direkomendasikanSOPs, dan pengujian ke aplikasi Anda.

Untuk mempublikasikan versi baru aplikasi Anda

1. Pada panel navigasi, pilih Aplikasi.
2. Pada halaman Aplikasi, pilih nama aplikasi.
3. Pilih tab Struktur aplikasi.
4. PilihPublikasikan versi baru.

5. Dalam dialog Publikasikan versi, di kotak Nama, masukkan nama untuk versi aplikasi atau Anda dapat menggunakan nama default yang disarankan oleh AWS Resilience Hub.
6. Pilih Terbitkan.

   Saat Anda memublikasikan versi baru aplikasi Anda, ini menjadi versi yang dinilai saat Anda menjalankan penilaian ketahanan. Juga, versi draf akan identik dengan versi yang dirilis sampai Anda membuat perubahan apa pun.

Setelah Anda menerbitkan versi baru aplikasi Anda, kami sarankan Anda untuk menjalankan laporan penilaian ketahanan baru untuk mengonfirmasi aplikasi Anda masih memenuhi kebijakan ketahanan Anda. Untuk informasi tentang menjalankan penilaian, lihatMenjalankan dan mengelola AWS Resilience Hub penilaian ketahanan.

Melihat semua versi AWS Resilience Hub aplikasi

Untuk membantu melacak perubahan aplikasi, AWS Resilience Hub menampilkan versi aplikasi Anda sebelumnya sejak aplikasi dibuat AWS Resilience Hub.

Untuk melihat semua versi aplikasi Anda

1. Pada panel navigasi, pilih Aplikasi.
2. Pada halaman Aplikasi, pilih nama aplikasi.
3. Pilih tab Struktur aplikasi.
4. Untuk melihat semua versi aplikasi Anda sebelumnya, pilih tanda tambah (+) sebelum Lihat semua versi. AWS Resilience Hub menunjukkan versi draf dan versi aplikasi Anda yang baru saja dirilis menggunakan status rilis Draft dan Current, masing-masing. Anda dapat memilih versi aplikasi apa pun untuk melihat sumber dayanya AppComponent, sumber input, dan informasi terkait lainnya.

   Selain itu, Anda juga dapat memfilter daftar dengan menggunakan salah satu opsi berikut:

   - Filter berdasarkan nama versi — Masukkan nama untuk memfilter hasil dengan nama versi aplikasi Anda.
   - Filter berdasarkan tanggal dan rentang waktu - Untuk menerapkan filter ini, pilih ikon kalender dan pilih salah satu opsi berikut untuk memfilter berdasarkan hasil yang cocok dengan rentang waktu:
     - Rentang relatif - Pilih salah satu opsi yang tersedia dan pilih Terapkan.

Jika Anda memilih Rentang kustom pilihan, masukkan durasi di Masukkan durasi kotak dan pilih unit waktu yang sesuai dari daftar dropdown Satuan waktu, lalu pilih Terapkan.

- Rentang relatif - Untuk menentukan rentang tanggal dan waktu, berikan waktu mulai dan waktu akhir, lalu pilih Terapkan.

Melihat sumber daya AWS Resilience Hub aplikasi

Untuk melihat sumber daya aplikasi Anda

1. Pada panel navigasi, pilih Aplikasi.
2. Pada halaman Aplikasi, pilih aplikasi yang ingin Anda perbarui izin keamanannya.
3. Dari Tindakan, pilih Lihat sumber daya.

   Di tab Sumber Daya, Anda dapat mengidentifikasi sumber daya dalam tabel Sumber daya dengan cara berikut:

   - Logical ID - ID logis adalah nama yang digunakan untuk mengidentifikasi sumber daya di AWS CloudFormation tumpukan Anda, file status Terraform, aplikasi yang ditambahkan secara manual, AppRegistry aplikasi, atau. AWS Resource Groups

     > **Note**
     >
     > - Terraform memungkinkan Anda menggunakan nama yang sama untuk jenis sumber daya yang berbeda. Oleh karena itu, Anda melihat "- tipe sumber daya" di akhir ID logis untuk sumber daya yang memiliki nama yang sama.
     > - Untuk melihat contoh semua sumber daya aplikasi, pilih tanda plus (+) sebelum ID Logis. Untuk melihat semua contoh sumber daya aplikasi, pilih tanda plus (+) sebelum ID Logis dari setiap sumber daya.
     >
     > Untuk informasi selengkapnya tentang sumber daya yang didukung, lihatthe section called “ AWS Resilience Hub Sumber daya yang didukung”.

   - Status — Ini menunjukkan apakah AWS Resilience Hub akan menilai sumber daya Anda untuk ketahanan.
   - Jenis sumber daya — Jenis sumber daya mengidentifikasi sumber daya komponen untuk aplikasi Anda. Misalnya, `AWS::EC2::Instance` mendeklarasikan EC2 instance Amazon.

Untuk informasi selengkapnya tentang pengelompokan AppComponent sumber daya, lihatMengelompokkan sumber daya dalam Komponen Aplikasi.

- Nama sumber — Nama sumber input. Pilih nama sumber untuk melihat detailnya di aplikasi masing-masing. Untuk sumber input yang ditambahkan secara manual, tautan tidak akan tersedia. Misalnya, jika Anda memilih nama sumber yang diimpor dari AWS CloudFormation tumpukan, Anda akan diarahkan ke halaman detail tumpukan di AWS CloudFormation halaman.
- Jenis sumber — Jenis sumber input.
- AppComponent Jenis — Jenis sumber input. Sumber input termasuk AWS CloudFormation tumpukan, AppRegistry aplikasi,, file status Terraform AWS Resource Groups, dan sumber daya yang ditambahkan secara manual.

> **Note**
>
> Untuk mengedit EKS kluster Amazon Anda, selesaikan langkah-langkah di Untuk mengedit sumber input prosedur AWS Resilience Hub aplikasi Anda.

- ID fisik — Pengenal yang ditetapkan sebenarnya untuk sumber daya tersebut, seperti ID EC2 instans Amazon atau nama bucket S3.
- Termasuk - Ini menunjukkan apakah AWS Resilience Hub termasuk sumber daya ini dalam aplikasi.
- AppComponents— AWS Resilience Hub Komponen yang ditugaskan ke sumber daya ini ketika struktur aplikasinya ditemukan.
- Nama — Nama sumber daya aplikasi.
- Akun — AWS Akun yang memiliki sumber daya fisik.

4. Pilih Simpan dan perbarui.

Menghapus aplikasi AWS Resilience Hub

Setelah Anda mencapai maksimal sepuluh batas aplikasi, Anda harus menghapus satu atau lebih aplikasi sebelum Anda dapat menambahkan lebih banyak.

Untuk menghapus aplikasi

1. Pada panel navigasi, pilih Aplikasi.
2. Pada halaman Aplikasi, pilih aplikasi yang ingin Anda hapus.

3. Pilih Tindakan, dan kemudian pilih Hapus aplikasi.
4. Untuk mengonfirmasi penghapusan, masukkan Hapus di kotak Hapus, dan pilih Hapus.

Parameter konfigurasi aplikasi

AWS Resilience Hub menyediakan mekanisme input untuk mengumpulkan informasi tambahan tentang sumber daya yang terkait dengan aplikasi Anda. Dengan informasi ini, AWS Resilience Hub akan mendapatkan pemahaman yang lebih dalam tentang sumber daya Anda dan memberikan rekomendasi ketahanan yang lebih baik.

Bagian Parameter konfigurasi aplikasi mencantumkan semua parameter konfigurasi dukungan failover lintas wilayah Anda. AWS Elastic Disaster Recovery Anda dapat mengidentifikasi parameter konfigurasi dengan yang berikut:

- Topik - Menunjukkan area aplikasi Anda yang dikonfigurasi. Misalnya, konfigurasi failover.
- Tujuan — Menunjukkan alasan mengapa AWS Resilience Hub meminta informasi.
- Parameter — Menunjukkan detail yang spesifik untuk area aplikasi, yang AWS Resilience Hub akan digunakan untuk memberikan rekomendasi untuk aplikasi Anda. Saat ini, parameter ini menggunakan nilai kunci hanya satu Wilayah failover dan satu akun terkait.

Memperbarui parameter konfigurasi aplikasi

Bagian ini memungkinkan Anda untuk memperbarui parameter konfigurasi Anda AWS Elastic Disaster Recovery dan mempublikasikan aplikasi untuk menyertakan parameter yang diperbarui untuk penilaian ketahanan.

Untuk memperbarui parameter konfigurasi aplikasi

1. Pada panel navigasi, pilih Aplikasi.
2. Pada halaman Aplikasi, pilih nama aplikasi yang ingin Anda edit.
3. Pilih tab Parameter konfigurasi aplikasi.
4. Pilih Perbarui.
5. Masukkan ID akun failover di kotak ID Akun.
6. Pilih Wilayah failover dari daftar dropdown Wilayah.

> **Note**
>
> Jika Anda ingin menonaktifkan fitur ini, pilih "—" dari daftar dropdown.

7. Pilih Perbarui dan terbitkan.

Mengelola kebijakan ketahanan

Bagian ini menjelaskan cara membuat kebijakan ketahanan untuk aplikasi Anda. Menetapkan kebijakan ketahanan dengan benar memungkinkan Anda memahami postur ketahanan aplikasi Anda. Kebijakan ketahanan berisi informasi dan tujuan yang Anda gunakan untuk menilai apakah aplikasi Anda diperkirakan pulih dari jenis gangguan, seperti perangkat lunak, perangkat keras, Availability Zone, atau Region. AWS Kebijakan ini tidak mengubah atau memengaruhi aplikasi yang sebenarnya. Beberapa aplikasi dapat memiliki kebijakan ketahanan yang sama.

Ketika Anda membuat kebijakan ketahanan, Anda menentukan tujuan target: tujuan waktu pemulihan (RTO) dan tujuan titik pemulihan (RPO). Tujuan menentukan apakah aplikasi memenuhi kebijakan ketahanan. Lampirkan kebijakan ke aplikasi Anda dan jalankan penilaian ketahanan. Anda dapat membuat kebijakan yang berbeda untuk berbagai jenis aplikasi dalam portofolio Anda. Misalnya, aplikasi perdagangan real-time akan memiliki kebijakan ketahanan yang berbeda dari aplikasi pelaporan bulanan.

> **Note**
>
> AWS Resilience Hub memungkinkan Anda memasukkan nilai nol di bidang RTO dan RPO dari kebijakan ketahanan Anda. Namun, saat menilai aplikasi Anda, hasil penilaian serendah mungkin mendekati nol. Oleh karena itu, jika Anda memasukkan nilai nol di bidang RTO dan RPO, estimasi beban kerja RTO dan perkiraan hasil RPO beban kerja akan mendekati nol dan status Kepatuhan untuk aplikasi Anda akan diatur ke Kebijakan yang dilanggar.

Penilaian mengevaluasi konfigurasi aplikasi Anda terhadap kebijakan ketahanan terlampir. Di akhir proses, AWS Resilience Hub berikan penilaian tentang bagaimana tindakan aplikasi Anda terhadap target pemulihan dalam kebijakan ketahanan Anda.

Anda dapat membuat kebijakan ketahanan di Aplikasi, dan juga dalam kebijakan Ketahanan. Anda dapat mengakses detail yang relevan tentang kebijakan Anda, dan juga memodifikasi dan menghapusnya.

AWS Resilience Hub menggunakan target RTO dan RPO Anda untuk mengukur ketahanan untuk jenis gangguan potensial ini:

- Aplikasi — Kehilangan layanan atau proses perangkat lunak yang diperlukan.
- Infrastruktur cloud — Kehilangan perangkat keras, seperti instans EC2.
- Availability Zone (AZ) infrastruktur cloud — Satu atau beberapa Availability Zone tidak tersedia.
- Wilayah infrastruktur cloud — Satu atau beberapa Wilayah tidak tersedia.

AWS Resilience Hub memungkinkan Anda membuat kebijakan ketahanan yang disesuaikan atau menggunakan kebijakan ketahanan standar terbuka yang kami rekomendasikan. Saat Anda membuat kebijakan yang disesuaikan, beri nama dan jelaskan kebijakan Anda dan pilih tingkat atau tingkatan yang sesuai yang menentukan kebijakan Anda. Tingkatan ini meliputi: Layanan inti TI dasar, Misi kritis, Kritis, Penting, dan Non-kritis.

Pilih tingkat yang sesuai untuk kelas aplikasi Anda. Misalnya, Anda mungkin mengklasifikasikan sistem perdagangan real-time sebagai kritis, sementara Anda mungkin mengklasifikasikan aplikasi pelaporan bulanan sebagai tidak kritis. Saat Anda menggunakan kebijakan standar kami, Anda dapat memilih kebijakan ketahanan dengan tingkat dan nilai yang telah dikonfigurasi sebelumnya untuk target RTO dan RPO berdasarkan jenis gangguan. Jika perlu, Anda dapat mengubah tingkat dan target RTO dan RPO.

Anda dapat membuat kebijakan ketahanan dalam kebijakan Ketahanan, atau saat Anda mendeskripsikan aplikasi baru.

Membuat kebijakan ketahanan

Di AWS Resilience Hub, Anda dapat membuat kebijakan ketahanan. Kebijakan ketahanan berisi informasi dan tujuan yang Anda gunakan untuk menilai apakah aplikasi Anda dapat pulih dari jenis gangguan, seperti perangkat lunak, perangkat keras, Availability Zone, atau Region. AWS Kebijakan ini tidak mengubah atau memengaruhi aplikasi yang sebenarnya. Beberapa aplikasi dapat memiliki kebijakan ketahanan yang sama.

Saat Anda membuat kebijakan ketahanan, Anda menentukan target tujuan waktu pemulihan (RTO) dan tujuan titik pemulihan (RPO). Saat Anda menjalankan penilaian, AWS Resilience Hub tentukan apakah aplikasi diperkirakan memenuhi tujuan yang ditentukan dalam kebijakan ketahanan.

Penilaian mengevaluasi konfigurasi aplikasi Anda terhadap kebijakan ketahanan terlampir. Di akhir proses, AWS Resilience Hub berikan penilaian tentang bagaimana tindakan aplikasi Anda terhadap tujuan dalam kebijakan ketahanan Anda.

> **Note**
>
> AWS Resilience Hub memungkinkan Anda memasukkan nilai nol di bidang RTO dan RPO dari kebijakan ketahanan Anda. Namun, saat menilai aplikasi Anda, hasil penilaian serendah mungkin mendekati nol. Oleh karena itu, jika Anda memasukkan nilai nol di bidang RTO dan RPO, estimasi beban kerja RTO dan perkiraan hasil RPO beban kerja akan mendekati nol dan status Kepatuhan untuk aplikasi Anda akan diatur ke Kebijakan yang dilanggar.

Anda dapat membuat kebijakan ketahanan di Aplikasi, dan juga dalam kebijakan Ketahanan. Anda dapat mengakses detail yang relevan tentang kebijakan Anda, dan juga memodifikasi dan menghapusnya.

Untuk membuat kebijakan ketahanan dalam Aplikasi

1. Di menu navigasi kiri, pilih Aplikasi.
2. Selesaikan prosedur dari the section called “Langkah 1: Memulai dengan menambahkan aplikasi” melaluithe section called “Langkah 8: Tambahkan tag ke aplikasi Anda ”.
3. Di bagian Kebijakan Ketahanan, pilih Buat kebijakan ketahanan.

   Halaman kebijakan Create resiliency ditampilkan.
4. Di bagian Pilih metode pembuatan, pilih Buat kebijakan.
5. Masukkan nama untuk kebijakan.
6. (Opsional) Masukkan deskripsi untuk kebijakan.
7. Pilih salah satu dari daftar dropdown Tier berikut:

   - Layanan inti TI dasar
   - Misi kritis
   - Kritis

- Penting
- Tidak kritis

8. Untuk target RTO dan RPO, di bawah RTO Aplikasi Pelanggan dan RPO, masukkan nilai numerik di kotak, lalu pilih satuan waktu yang diwakili oleh nilai tersebut.

   Ulangi entri ini di bawah Infrastruktur RTO dan RPO untuk Infrastruktur dan Availability Zone.

9. (Opsional) Jika Anda memiliki aplikasi Multi-region, Anda mungkin ingin menentukan target RTO dan RPO Region.

   Wilayah Nyalakan. Untuk target Region RTO dan RPO, di bawah Customer Application RTO dan RPO, masukkan nilai numerik di kotak, lalu pilih satuan waktu yang diwakili oleh nilai tersebut.

10. (Opsional) Jika ingin menambahkan tag, Anda dapat melakukannya nanti saat melanjutkan pembuatan kebijakan. Untuk informasi selengkapnya tentang tag, lihat Menandai sumber daya di Referensi AWS Umum.
11. Untuk membuat kebijakan, pilih Buat.

Membuat kebijakan ketahanan dalam kebijakan Ketahanan

1. Di menu navigasi kiri, pilih Kebijakan.
2. Di bagian Kebijakan Ketahanan, pilih Buat kebijakan ketahanan.

   Halaman kebijakan Create resiliency ditampilkan.

3. Masukkan nama untuk kebijakan.
4. (Opsional) Masukkan deskripsi untuk kebijakan.
5. Pilih salah satu dari yang berikut dari Tier:

   - Layanan inti TI dasar
   - Misi kritis
   - Kritis
   - Penting
   - Tidak kritis

6. Untuk target RTO dan RPO, di bawah RTO Aplikasi Pelanggan dan RPO, masukkan nilai numerik di kotak dan kemudian pilih satuan waktu yang diwakili oleh nilai tersebut.

   Ulangi entri ini di bawah Infrastruktur RTO dan RPO untuk Infrastruktur dan Availability Zone.

7. (Opsional) Jika Anda memiliki aplikasi Multi-region, Anda mungkin ingin menentukan target RTO dan RPO Region.

   Wilayah Nyalakan. Untuk target RTO dan RPO, di bawah RTO Aplikasi Pelanggan dan RPO, masukkan nilai numerik di kotak dan kemudian pilih satuan waktu yang diwakili oleh nilai tersebut.

8. (Opsional) Jika ingin menambahkan tag, Anda dapat melakukannya nanti saat melanjutkan pembuatan kebijakan. Untuk informasi selengkapnya tentang tag, lihat Menandai sumber daya di Referensi AWS Umum.
9. Untuk membuat kebijakan, pilih Buat.

Untuk membuat kebijakan ketahanan berdasarkan kebijakan yang disarankan

1. Di menu navigasi kiri, pilih Kebijakan.
2. Di bagian Pilih metode pembuatan, pilih Pilih kebijakan berdasarkan kebijakan yang disarankan.
3. Di bagian Kebijakan Ketahanan, pilih Buat kebijakan ketahanan.

   Halaman kebijakan Create resiliency ditampilkan.
4. Masukkan nama untuk kebijakan ketahanan.
5. (Opsional) Masukkan deskripsi untuk kebijakan.
6. Di bagian Kebijakan ketahanan yang disarankan, lihat dan pilih salah satu tingkatan kebijakan ketahanan yang telah ditentukan berikut ini:

   - Aplikasi non-kritis
   - Aplikasi Penting
   - Aplikasi Kritis
   - Aplikasi Kritis Global
   - Aplikasi Kritis Misi
   - Aplikasi Kritis Misi Global
   - Layanan Inti Dasar
7. Untuk membuat kebijakan ketahanan, pilih Buat kebijakan.

Mengakses detail kebijakan ketahanan

Saat Anda membuka kebijakan ketahanan, Anda melihat detail penting tentang kebijakan tersebut. Anda juga dapat mengedit atau menghapus ketahanan.

Rincian kebijakan ketahanan terdiri dari dua pandangan utama: Ringkasan dan Tag.

Ringkasan

Informasi dasar

Memberikan informasi berikut tentang kebijakan ketahanan: Nama, Deskripsi, Tingkat, Tingkat Biaya, dan Tanggal Dibuat.

Perkiraan beban kerja RTO dan perkiraan beban kerja RPO

Menunjukkan estimasi beban kerja RTO dan estimasi jenis gangguan RPO beban kerja yang terkait dengan kebijakan ketahanan ini.

Tanda

Gunakan tampilan ini untuk mengelola, menambah, dan menghapus tag internal aplikasi ini.

Mengedit kebijakan ketahanan dalam rincian kebijakan Ketahanan

1. Di menu navigasi kiri, pilih Kebijakan.
2. Dalam kebijakan Ketahanan, buka kebijakan ketahanan.
3. Pilih Edit. Masukkan perubahan yang sesuai di bidang Info Dasar, dan RTO dan RPO. Lalu pilih Simpan Perubahan.

Mengedit kebijakan ketahanan dalam kebijakan Ketahanan

1. Di menu navigasi kiri, pilih Kebijakan.
2. Dalam kebijakan Ketahanan, pilih kebijakan ketahanan.
3. Pilih Tindakan, lalu pilih Edit.
4. Masukkan perubahan yang sesuai di bidang Info Dasar, dan RTO dan RPO. Lalu pilih Simpan Perubahan.

Untuk menghapus kebijakan ketahanan dalam rincian kebijakan Ketahanan

1. Di menu navigasi kiri, pilih Kebijakan.
2. Dalam kebijakan Ketahanan, buka kebijakan ketahanan.
3. Pilih Hapus. Konfirmasikan penghapusan Anda, lalu pilih Hapus.

Untuk menghapus kebijakan ketahanan dalam kebijakan Ketahanan

1. Di menu navigasi kiri, pilih Kebijakan.
2. Dalam kebijakan Ketahanan, pilih kebijakan ketahanan.
3. Pilih Tindakan, lalu pilih Hapus.
4. Konfirmasikan penghapusan Anda, lalu pilih Hapus.

Menjalankan dan mengelola AWS Resilience Hub penilaian ketahanan

Ketika aplikasi Anda berubah, Anda harus menjalankan penilaian ketahanan. Penilaian membandingkan setiap konfigurasi Komponen Aplikasi dengan kebijakan dan membuat alarm,SOP, dan rekomendasi pengujian. Rekomendasi konfigurasi ini dapat meningkatkan kecepatan prosedur pemulihan.

Rekomendasi alarm membantu Anda mengatur alarm yang mendeteksi pemadaman. SOPrekomendasi menyediakan skrip yang mengelola proses pemulihan umum, seperti pemulihan dari cadangan. Rekomendasi pengujian menawarkan saran untuk memverifikasi konfigurasi Anda berfungsi dengan baik. Misalnya, Anda dapat menguji apakah aplikasi pulih selama proses pemulihan otomatis, seperti penskalaan otomatis atau penyeimbangan beban karena masalah jaringan. Anda dapat menguji apakah alarm aplikasi dipicu saat sumber daya mencapai batasnya. Anda juga dapat menguji seberapa baik SOPs bekerja dalam kondisi yang Anda tunjukkan.

Menjalankan penilaian ketahanan

Anda dapat menjalankan laporan penilaian ketahanan dari beberapa lokasi di. AWS Resilience Hub Untuk informasi selengkapnya tentang aplikasi Anda, lihatthe section called “Mengelola aplikasi”.

Untuk menjalankan penilaian ketahanan dari menu Tindakan

1. Di menu navigasi kiri, pilih Aplikasi.

2. Pilih aplikasi dari tabel Aplikasi.
3. Pilih Menilai ketahanan dari menu Tindakan.
4. Dalam dialog Jalankan penilaian ketahanan, Anda dapat memasukkan nama unik atau menggunakan nama yang dihasilkan untuk penilaian.
5. Pilih Jalankan.

   Untuk meninjau laporan penilaian, pilih Penilaian dalam aplikasi Anda. Untuk informasi selengkapnya, lihat the section called “Meninjau laporan penilaian”.

Untuk menjalankan penilaian ketahanan dari tab Penilaian

Anda dapat menjalankan penilaian ketahanan baru saat aplikasi atau kebijakan ketahanan Anda berubah.

1. Di menu navigasi kiri, pilih Aplikasi.
2. Pilih aplikasi dari tabel Aplikasi.
3. Pilih tab Penilaian.
4. Pilih Jalankan penilaian ketahanan.
5. Dalam dialog Jalankan penilaian ketahanan, Anda dapat memasukkan nama unik atau menggunakan nama yang dihasilkan untuk penilaian.
6. Pilih Jalankan.

   Untuk meninjau laporan penilaian, pilih Penilaian dalam aplikasi Anda. Untuk informasi selengkapnya, lihat the section called “Meninjau laporan penilaian”.

Meninjau laporan penilaian

Anda menemukan laporan penilaian dalam tampilan Penilaian aplikasi Anda.

Untuk menemukan laporan penilaian

1. Di menu navigasi kiri, pilih Aplikasi.
2. Di Aplikasi, buka aplikasi.
3. Di tab Penilaian, pilih laporan penilaian dari tabel Penilaian Ketahanan.

Saat Anda membuka laporan, Anda melihat yang berikut:

- Gambaran keseluruhan dari laporan penilaian
- Rekomendasi untuk meningkatkan ketahanan.
- Rekomendasi untuk mengatur alarm,SOPs, dan tes
- Cara membuat dan mengelola tag untuk mencari dan memfilter AWS sumber daya Anda

Ulasan

Bagian ini memberikan gambaran umum tentang laporan penilaian. AWS Resilience Hub mencantumkan setiap jenis gangguan dan Komponen Aplikasi terkait. Ini juga mencantumkan aktual RTO dan RPO kebijakan Anda dan menentukan apakah Komponen Aplikasi dapat mencapai tujuan kebijakan.

Ikhtisar

Menunjukkan nama aplikasi, nama kebijakan ketahanan, dan tanggal pembuatan laporan.

Drift sumber daya yang terdeteksi

Bagian ini mencantumkan semua sumber daya yang ditambahkan atau dihapus setelah disertakan dalam versi terbaru aplikasi yang diterbitkan. Pilih Impor ulang sumber input untuk mengimpor ulang semua sumber input (yang berisi sumber daya hanyut) di tab Sumber input. Pilih Publikasikan dan nilai untuk memasukkan sumber daya yang diperbarui dalam aplikasi dan menerima penilaian ketahanan yang akurat.

Anda dapat mengidentifikasi sumber input yang hanyut menggunakan yang berikut ini:

- Logical ID — Menunjukkan ID logis dari sumber daya. ID logis adalah nama yang digunakan untuk mengidentifikasi sumber daya di AWS CloudFormation tumpukan Anda, file status Terraform, aplikasi yang ditambahkan secara manual, AppRegistry aplikasi, atau. AWS Resource Groups
- Ubah - Menunjukkan jika sumber daya masukan Ditambahkan atau Dihapus.
- Nama sumber - Menunjukkan nama sumber daya. Pilih nama sumber untuk melihat detailnya di aplikasi masing-masing. Untuk sumber input yang ditambahkan secara manual, tautan tidak akan tersedia. Misalnya, jika Anda memilih nama sumber yang diimpor dari AWS CloudFormation tumpukan, Anda akan diarahkan ke halaman detail tumpukan di AWS CloudFormation halaman.
- Jenis sumber daya - Menunjukkan jenis sumber daya.
- Akun — Menunjukkan AWS akun yang memiliki sumber daya fisik.
- Wilayah — Menunjukkan AWS Wilayah tempat sumber daya berada.

RTO

Menunjukkan representasi grafis apakah aplikasi diperkirakan memenuhi tujuan kebijakan ketahanan. Ini didasarkan pada jumlah waktu aplikasi dapat down tanpa menyebabkan kerusakan signifikan pada organisasi. Penilaian memberikan perkiraan beban kerjaRTO.

RPO

Menunjukkan representasi grafis apakah aplikasi diperkirakan memenuhi tujuan kebijakan ketahanan. Ini didasarkan pada jumlah waktu data dapat hilang sebelum kerugian yang signifikan terhadap bisnis terjadi. Penilaian memberikan perkiraan beban kerjaRPO.

Detail

Memberikan deskripsi terperinci dari setiap jenis gangguan menggunakan Semua hasil dan tab drift kepatuhan Aplikasi. Semua tab hasil menunjukkan semua gangguan termasuk penyimpangan kepatuhan, dan tab drift kepatuhan aplikasi hanya menampilkan penyimpangan kepatuhan. Jenis gangguan meliputi Aplikasi, infrastruktur cloud (Infrastruktur dan Zona Ketersediaan), dan Wilayah, dan memberikan informasi berikut tentangnya:

- AppComponent

  Sumber daya yang terdiri dari aplikasi. Misalnya, aplikasi Anda mungkin memiliki database atau komponen komputasi.

- Diperkirakan RTO

  Menunjukkan apakah konfigurasi kebijakan Anda selaras dengan persyaratan kebijakan Anda. Kami memberikan dua nilai, Estimasi RTO dan Target AndaRTO. Misalnya, jika Anda melihat nilai 2 jam di bawah Targeted RTO dan 40m di bawah Estimasi Beban Kerja RTO, ini menunjukkan bahwa kami menyediakan perkiraan beban kerja RTO 40 menit, sedangkan saat ini aplikasi Anda adalah RTO dua jam. Kami mendasarkan perkiraan RTO perhitungan beban kerja kami pada konfigurasi, bukan kebijakan. Akibatnya, database Zona Ketersediaan Multi akan memiliki perkiraan beban kerja yang sama RTO untuk kegagalan Availability Zone, apa pun kebijakan yang Anda pilih.
- RTOmelayang

  Menunjukkan durasi aplikasi Anda telah menyimpang dari perkiraan beban kerja penilaian RTO yang berhasil sebelumnya. Kami memberikan dua nilai, Estimasi RTO dan RTOdrift kami.

Misalnya, jika Anda melihat nilai 2 jam di bawah Estimasi RTO dan 40m di bawah RTOdrift, ini menunjukkan bahwa aplikasi Anda melayang dari perkiraan beban kerja penilaian yang berhasil sebelumnya RTO sebesar 40 menit.

- Diperkirakan RPO

  Menampilkan RPO kebijakan Estimasi Beban Kerja aktual yang AWS Resilience Hub memperkirakan, berdasarkan RPO kebijakan Target yang Anda tetapkan untuk setiap Komponen Aplikasi. Misalnya, Anda mungkin telah menetapkan RPO target dalam kebijakan ketahanan untuk kegagalan Availability Zone menjadi satu jam. Hasil estimasi dapat dihitung mendekati nol. Ini mengasumsikan bahwa Amazon Aurora, tempat kami melakukan setiap transaksi, berhasil dalam empat dari enam node, mencakup beberapa Availability Zone. Mungkin lima menit untuk point-in-time pemulihan.

  Satu-satunya RTO dan RPO target yang dapat Anda pilih untuk tidak memasok adalah Wilayah. Untuk beberapa aplikasi, sangat berguna untuk merencanakan pemulihan ketika ada ketergantungan penting pada AWS layanan, yang mungkin menjadi tidak tersedia di seluruh Wilayah.

  Jika Anda memilih opsi ini, seperti pengaturan RTO atau RPO target untuk Wilayah, Anda akan menerima perkiraan waktu pemulihan dan rekomendasi operasional untuk kegagalan tersebut.

- RPOmelayang

  Menunjukkan durasi aplikasi Anda telah menyimpang dari perkiraan beban kerja penilaian RPO yang berhasil sebelumnya. Kami memberikan dua nilai, Estimasi RPO dan RPOdrift kami. Misalnya, jika Anda melihat nilai 2 jam di bawah Estimasi RPO dan 40m di bawah RPOdrift, ini menunjukkan bahwa aplikasi Anda melayang dari perkiraan beban kerja penilaian yang berhasil sebelumnya RPO sebesar 40 menit.

Meninjau rekomendasi ketahanan

Rekomendasi ketahanan mengevaluasi Komponen Aplikasi dan merekomendasikan cara mengoptimalkan dengan perkiraan beban kerja RTO dan perkiraan beban kerjaRPO, biaya, dan perubahan minimal.

Dengan AWS Resilience Hub, Anda dapat mengoptimalkan ketahanan menggunakan salah satu opsi yang disarankan berikut di Mengapa Anda harus memilih opsi ini:

> **Note**
>
> - AWS Resilience Hub menyediakan hingga tiga opsi yang AWS Resilience Hub direkomendasikan.
> - Jika Anda menetapkan Regional RTO dan RPO target, AWS Resilience Hub menampilkan Optimalkan untuk WilayahRTO/RPOdalam opsi yang disarankan. Jika Regional RTO dan RPO target tidak ditetapkan, Optimalkan untuk Availability Zone (AZ)RTO/RPOditampilkan. Untuk informasi selengkapnya tentang menetapkan RegionalRTO/RPOtarget sambil membuat kebijakan ketahanan, lihat. Membuat kebijakan ketahanan
> - Perkiraan beban kerja RTO dan estimasi RPO nilai beban kerja untuk aplikasi dan konfigurasinya ditentukan dengan mempertimbangkan jumlah data dan individu. AppComponents Namun, nilai-nilai ini hanya perkiraan. Anda harus menggunakan pengujian Anda sendiri (seperti Amazon Fault Injection Service) untuk menguji aplikasi Anda untuk waktu pemulihan yang sebenarnya.

Optimalkan untuk Availability ZoneRTO/RPO

Perkiraan waktu pemulihan beban kerja serendah mungkin (RTO/RPO) selama gangguan Availability Zone (AZ). Jika konfigurasi Anda tidak dapat diubah secara memadai untuk memenuhi RPO target RTO dan target, Anda akan diberi tahu tentang perkiraan waktu pemulihan AZ beban kerja terendah untuk membuat konfigurasi Anda mendekati kemungkinan memenuhi kebijakan.

Optimalkan untuk WilayahRTO/RPO

Perkiraan waktu pemulihan beban kerja serendah mungkin (RTO/RPO) selama gangguan Regional. Jika konfigurasi Anda tidak dapat diubah secara memadai untuk memenuhi RPO target RTO dan target, Anda akan diberi tahu tentang perkiraan waktu pemulihan Wilayah beban kerja terendah untuk membuat konfigurasi Anda mendekati kemungkinan memenuhi kebijakan.

Optimalkan biaya

Biaya terendah yang dapat Anda keluarkan dan masih memenuhi kebijakan ketahanan Anda. Jika konfigurasi Anda tidak dapat diubah secara memadai untuk memenuhi sasaran pengoptimalan, Anda akan diberi tahu tentang biaya terendah yang dapat Anda keluarkan untuk membuat konfigurasi Anda mendekati kemungkinan memenuhi kebijakan.

Optimalkan untuk perubahan minimal

Perubahan minimum yang diperlukan untuk mencapai target kebijakan Anda. Jika konfigurasi Anda tidak dapat diubah secara memadai untuk memenuhi sasaran pengoptimalan, Anda akan diberi tahu tentang perubahan yang disarankan yang dapat membuat konfigurasi Anda mendekati kemungkinan memenuhi kebijakan.

Item berikut termasuk dalam rincian kategori optimasi:

- Deskripsi

  Menjelaskan konfigurasi yang disarankan oleh AWS Resilience Hub.

- Perubahan

  Daftar perubahan teks yang menggambarkan tugas yang diperlukan untuk beralih ke konfigurasi yang disarankan.

- Biaya dasar

  Perkiraan biaya terkait dengan perubahan yang disarankan.

  > **Note**
  >
  > Biaya dasar dapat bervariasi berdasarkan penggunaan dan tidak termasuk diskon atau penawaran apa pun dari Program Diskon Perusahaan (EDP).

- Perkiraan Beban Kerja RTO dan RPO

  Perkiraan beban kerja RTO dan perkiraan beban kerja RPO setelah perubahan.

AWSResilience Hub mengevaluasi apakah Komponen Aplikasi (AppComponent) dapat mematuhi kebijakan ketahanan. Jika AppComponent tidak mematuhi kebijakan ketahanan dan AWS Resilience Hub tidak dapat membuat rekomendasi apa pun untuk memfasilitasi kepatuhan, itu mungkin karena waktu pemulihan untuk yang dipilih AppComponent tidak dapat dipenuhi dalam batasan. AppComponent Contoh AppComponent kendala termasuk jenis sumber daya, ukuran penyimpanan, atau konfigurasi sumber daya.

Untuk memfasilitasi kepatuhan terhadap kebijakan ketahanan, ubah jenis sumber daya AppComponent atau perbarui kebijakan ketahanan agar selaras dengan apa yang dapat diberikan sumber daya. AppComponent

Meninjau rekomendasi operasional

Rekomendasi operasional berisi rekomendasi untuk mengatur alarm,SOPs, dan AWS FIS eksperimen melalui AWS CloudFormation templat.

AWS Resilience Hub menyediakan file AWS CloudFormation template bagi Anda untuk men-download dan mengelola infrastruktur aplikasi sebagai kode. Sebagai hasilnya, kami menyediakan rekomendasi AWS CloudFormation sehingga Anda dapat menambahkannya ke kode aplikasi Anda. Jika ukuran file AWS CloudFormation template lebih dari satu MB dan berisi lebih dari 500 sumber daya, AWS Resilience Hub menghasilkan lebih dari satu file AWS CloudFormation template di mana ukuran setiap file tidak lebih dari satu MB dan berisi hingga 500 sumber daya. Jika file AWS CloudFormation template dibagi menjadi beberapa file, nama file AWS CloudFormation template akan ditambahkan dengan`partXofY`, di mana `X` menunjukkan nomor file dalam urutan dan `Y` menunjukkan jumlah total file file AWS CloudFormation template dibagi menjadi. Misalnya, jika file template `big-app-template5-Alarm-104849185070-us-west-2.yaml` dibagi menjadi empat file, nama file akan menjadi sebagai berikut:

- `big-app-template5-Alarm-104849185070-us-west-2-part1of4.yaml`
- `big-app-template5-Alarm-104849185070-us-west-2-part2of4.yaml`
- `big-app-template5-Alarm-104849185070-us-west-2-part3of4.yaml`
- `big-app-template5-Alarm-104849185070-us-west-2-part4of4.yaml`

Namun, dalam kasus AWS CloudFormation template besar, Anda diminta untuk menyediakan Amazon Simple Storage Service URI alih-alih CLI API menggunakan/dengan file lokal sebagai input.

Di AWS Resilience Hub, Anda dapat melakukan tindakan berikut:

- Anda dapat menyediakan alarm yang dipilih,SOPs, dan AWS FIS eksperimen. Untuk menyediakan alarm,SOPs, dan AWS FIS eksperimen, pilih rekomendasi yang sesuai dan masukkan nama unik. AWS Resilience Hub membuat template berdasarkan rekomendasi yang Anda pilih. Di Template, Anda dapat mengakses template yang dibuat melalui Amazon Simple Storage Service (Amazon S3). URL
- Anda dapat menyertakan atau mengecualikan alarm yang dipilihSOPs, dan AWS FIS eksperimen yang direkomendasikan untuk aplikasi Anda kapan saja. Untuk informasi lebih lanjut lihat,the section called “Termasuk atau tidak termasuk rekomendasi operasional”.
- Anda juga dapat mencari, membuat, menambah, menghapus, dan mengelola tag, untuk aplikasi dan melihat semua tag yang terkait dengannya.

Termasuk atau tidak termasuk rekomendasi operasional

AWS Resilience Hub menyediakan opsi untuk menyertakan atau mengecualikan alarm,SOPs, dan AWS FIS eksperimen (tes) yang direkomendasikan untuk meningkatkan skor ketahanan aplikasi Anda kapan saja. Termasuk dan tidak termasuk rekomendasi operasional akan berdampak pada skor ketahanan aplikasi Anda hanya setelah Anda menjalankan penilaian baru. Oleh karena itu, kami menyarankan Anda untuk menjalankan penilaian untuk mendapatkan skor ketahanan yang diperbarui dan memahami dampaknya terhadap aplikasi Anda.

Untuk informasi selengkapnya tentang membatasi izin untuk menyertakan atau mengecualikan rekomendasi per aplikasi, lihat. the section called “Membatasi izin untuk menyertakan atau mengecualikan rekomendasi AWS Resilience Hub ”

Untuk memasukkan atau mengecualikan rekomendasi operasional dari aplikasi

1. Di menu navigasi kiri, pilih Aplikasi.
2. Di Aplikasi, buka aplikasi.
3. Pilih Penilaian dan pilih penilaian dari tabel Penilaian Ketahanan. Jika Anda tidak memiliki penilaian, selesaikan prosedur the section called “Menjalankan penilaian ketahanan” dan kemudian kembali ke langkah ini.
4. Pilih tab Rekomendasi operasional.
5. Untuk memasukkan atau mengecualikan rekomendasi operasional dari aplikasi Anda, lengkapi prosedur berikut:

Untuk menyertakan atau mengecualikan alarm yang disarankan dari aplikasi Anda

1. Untuk mengecualikan alarm, selesaikan langkah-langkah berikut:

    a. Di bawah tab Alarm, dari tabel Alarm, pilih semua alarm (dengan status Tidak diterapkan) yang ingin Anda kecualikan. Anda dapat mengidentifikasi status implementasi alarm saat ini dari kolom Negara.

    b. Dari Tindakan, pilih Kecualikan yang dipilih.

    c. Dari dialog Kecualikan rekomendasi, pilih salah satu alasan berikut (opsional), dan pilih Kecualikan dipilih untuk mengecualikan alarm yang dipilih dari aplikasi.

        - Sudah diterapkan — Pilih opsi ini jika Anda telah menerapkan alarm ini di AWS layanan seperti Amazon CloudWatch, atau penyedia layanan pihak ketiga lainnya.

- Tidak relevan — Pilih opsi ini jika alarm tidak sesuai dengan kebutuhan bisnis Anda.
- Terlalu rumit untuk diterapkan - Pilih opsi ini jika menurut Anda alarm ini terlalu rumit untuk diterapkan.
- Lainnya — Pilih opsi ini untuk menentukan alasan lain untuk mengecualikan rekomendasi.

2. Untuk menyertakan alarm, selesaikan langkah-langkah berikut:

   a. Di bawah tab Alarm, dari tabel Alarm, pilih semua alarm (dengan status Dikecualikan) yang ingin Anda sertakan. Anda dapat mengidentifikasi status implementasi alarm saat ini dari kolom Negara.

   b. Dari Tindakan, pilih Sertakan yang dipilih.

   c. Dari dialog Sertakan rekomendasi, pilih Sertakan yang dipilih untuk menyertakan semua alarm yang dipilih dalam aplikasi Anda.

Untuk memasukkan atau mengecualikan prosedur operasi standar yang direkomendasikan (SOPs) dari aplikasi Anda

1. Untuk mengecualikan yang disarankanSOPs, selesaikan langkah-langkah berikut:

   a. Di bawah tab Prosedur operasi standar, dari SOPstabel, pilih semua SOPs (dengan status Diimplementasikan atau Tidak diterapkan) yang ingin Anda kecualikan. Anda dapat mengidentifikasi status implementasi saat ini SOP dari kolom Negara.

   b. Dari Tindakan, pilih Kecualikan yang dipilih untuk mengecualikan yang dipilih SOPs dari aplikasi Anda.

   c. Dari dialog Kecualikan rekomendasi, pilih salah satu alasan berikut (opsional), dan pilih Kecualikan dipilih untuk mengecualikan yang dipilih SOPs dari aplikasi.

      - Sudah diterapkan — Pilih opsi ini jika Anda telah menerapkannya SOPs dalam suatu AWS layanan, atau penyedia layanan pihak ketiga lainnya.
      - Tidak relevan — Pilih opsi ini jika SOPs tidak sesuai dengan kebutuhan bisnis Anda.
      - Terlalu rumit untuk diterapkan - Pilih opsi ini jika menurut Anda SOPs ini terlalu rumit untuk diterapkan.
      - Tidak ada - Pilih opsi ini jika Anda tidak ingin menentukan alasannya.

2. Untuk memasukkanSOPs, selesaikan langkah-langkah berikut:

a. Di bawah tab Prosedur operasi standar, dari SOPstabel, pilih semua alarm (dengan status Dikecualikan) yang ingin Anda sertakan. Anda dapat mengidentifikasi status implementasi alarm saat ini dari kolom Negara.

b. Dari Tindakan, pilih Sertakan yang dipilih.

c. Dari dialog Sertakan rekomendasi, pilih Sertakan yang dipilih untuk menyertakan semua yang dipilih SOPs dalam aplikasi Anda.

Untuk menyertakan atau mengecualikan tes yang direkomendasikan dari aplikasi Anda

1. Untuk mengecualikan tes yang disarankan, selesaikan langkah-langkah berikut:

   a. Di bawah Tab templat eksperimen injeksi kesalahan, dari tabel templat eksperimen injeksi kesalahan, pilih semua pengujian (dengan status Diimplementasikan atau Tidak diterapkan) yang ingin Anda kecualikan. Anda dapat mengidentifikasi status implementasi pengujian saat ini dari kolom Negara.

   b. Dari Tindakan, pilih Kecualikan yang dipilih.

   c. Dari dialog Kecualikan rekomendasi, pilih salah satu alasan berikut (opsional), dan pilih Kecualikan dipilih untuk mengecualikan AWS FIS eksperimen yang dipilih dari aplikasi.

      - Sudah diterapkan — Pilih opsi ini jika Anda telah menerapkan pengujian ini dalam suatu AWS layanan, atau penyedia layanan pihak ketiga lainnya.
      - Tidak relevan — Pilih opsi ini jika tes tidak sesuai dengan kebutuhan bisnis Anda.
      - Terlalu rumit untuk diterapkan - Pilih opsi ini jika menurut Anda tes ini terlalu rumit untuk diterapkan.
      - Tidak ada - Pilih opsi ini jika Anda tidak ingin menentukan alasannya.

2. Untuk memasukkan tes yang direkomendasikan, selesaikan langkah-langkah berikut:

   a. Di bawah tab Templat eksperimen injeksi kesalahan, dari tabel templat eksperimen injeksi kesalahan, pilih semua pengujian (dengan status Dikecualikan) yang ingin Anda sertakan. Anda dapat mengidentifikasi status implementasi pengujian saat ini dari kolom Negara.

   b. Dari Tindakan, pilih Sertakan yang dipilih.

   c. Dari dialog Sertakan rekomendasi, pilih Sertakan yang dipilih untuk menyertakan semua tes yang dipilih dalam aplikasi Anda.

Menghapus penilaian ketahanan

Anda dapat menghapus penilaian ketahanan dalam tampilan Penilaian aplikasi Anda.

Untuk menghapus penilaian ketahanan

1. Di menu navigasi kiri, pilih Aplikasi.
2. Di Aplikasi, buka aplikasi.
3. Dalam Penilaian, pilih laporan penilaian dalam tabel penilaian Ketahanan.
4. Untuk mengonfirmasi penghapusan, pilih Hapus.

   Laporan tidak lagi muncul di tabel penilaian Ketahanan.

Mengelola alarm-alarm

Ketika Anda menjalankan penilaian ketahanan, sebagai bagian dari rekomendasi operasional, AWS Resilience Hub merekomendasikan pengaturan CloudWatch alarm Amazon untuk memantau ketahanan aplikasi Anda. Kami merekomendasikan alarm ini berdasarkan sumber daya dan komponen konfigurasi aplikasi Anda saat ini. Jika sumber daya dan komponen dalam aplikasi Anda berubah, Anda harus menjalankan penilaian ketahanan untuk memastikan Anda memiliki alarm yang benar untuk aplikasi yang diperbarui.

AWS Resilience Hub menyediakan file template (`README.md`) yang memungkinkan Anda membuat alarm yang direkomendasikan oleh AWS Resilience Hub dalam AWS (seperti Amazon CloudWatch) atau di luar AWS. Nilai default yang disediakan dalam alarm didasarkan pada praktik terbaik yang digunakan untuk membuat alarm ini.

Topik

Membuat alarm dari rekomendasi operasional

AWS Resilience Hub membuat AWS CloudFormation template yang berisi detail untuk membuat alarm yang dipilih di Amazon CloudWatch. Setelah template dibuat, Anda dapat mengaksesnya melalui Amazon S3URL, mengunduh yang sama dan menempatkannya di pipeline kode Anda atau membuat tumpukan melalui konsol. AWS CloudFormation

Untuk membuat alarm berdasarkan AWS Resilience Hub rekomendasi, Anda harus membuat AWS CloudFormation template untuk alarm yang direkomendasikan dan memasukkannya ke dalam basis kode Anda.

Untuk membuat alarm dalam rekomendasi operasional

1. Di menu navigasi kiri, pilih Aplikasi.
2. Di Aplikasi, pilih aplikasi Anda.
3. Pilih tab Penilaian.

   Dalam tabel penilaian Ketahanan, Anda dapat mengidentifikasi penilaian Anda menggunakan informasi berikut:

   - Nama — Nama penilaian yang Anda berikan pada saat pembuatan.
   - Status - Menunjukkan status eksekusi penilaian.
   - Status kepatuhan - Menunjukkan apakah penilaian sesuai dengan kebijakan ketahanan.
   - Status penyimpangan ketahanan - Menunjukkan apakah aplikasi Anda telah melayang atau tidak dari penilaian sukses sebelumnya.
   - Versi aplikasi - Versi aplikasi Anda.
   - Invoker — Menunjukkan peran yang memanggil penilaian.
   - Waktu mulai - Menunjukkan waktu mulai penilaian.
   - Waktu akhir - Menunjukkan waktu akhir penilaian.
   - ARN— Nama Sumber Daya Amazon (ARN) dari penilaian.
4. Pilih penilaian dari tabel penilaian Ketahanan. Jika Anda tidak memiliki penilaian, selesaikan prosedur the section called “Menjalankan penilaian ketahanan” dan kemudian kembali ke langkah ini.
5. Pilih Rekomendasi Operasional.
6. Jika tidak dipilih secara default, pilih tab Alarm.

   Di tabel Alarm, Anda dapat mengidentifikasi alarm yang disarankan menggunakan yang berikut ini:

   - Nama — Nama alarm yang telah Anda tetapkan untuk aplikasi Anda.
   - Deskripsi — Menjelaskan tujuan alarm.
   - Status - Menunjukkan status implementasi CloudWatch alarm Amazon saat ini.

Kolom ini menampilkan salah satu nilai berikut:

- Diimplementasikan - Menunjukkan bahwa alarm yang direkomendasikan oleh AWS Resilience Hub diimplementasikan dalam aplikasi Anda. Memilih nomor di bawah ini akan memfilter tabel Alarm untuk menampilkan semua alarm yang direkomendasikan yang diterapkan dalam aplikasi Anda.
- Tidak diimplementasikan - Menunjukkan bahwa alarm yang direkomendasikan oleh AWS Resilience Hub disertakan tetapi tidak diimplementasikan dalam aplikasi Anda. Memilih nomor di bawah ini akan memfilter tabel Alarm untuk menampilkan semua alarm yang direkomendasikan yang tidak diterapkan dalam aplikasi Anda.
- Dikecualikan - Menunjukkan bahwa alarm yang direkomendasikan oleh AWS Resilience Hub dikecualikan dari aplikasi Anda. Memilih nomor di bawah ini akan memfilter tabel Alarm untuk menampilkan semua alarm yang disarankan yang dikecualikan dari aplikasi Anda. Untuk informasi selengkapnya tentang memasukkan dan mengecualikan alarm yang direkomendasikan, lihat Menyertakan atau mengecualikan rekomendasi operasional.
- Tidak Aktif — Menunjukkan bahwa alarm disebarkan ke Amazon CloudWatch, tetapi statusnya disetel ke _ INSUFFICIENTdi DATA Amazon. CloudWatch Memilih nomor di bawah ini akan memfilter tabel Alarm untuk menampilkan semua alarm yang diterapkan dan tidak aktif.

- Konfigurasi - Menunjukkan jika ada dependensi konfigurasi yang tertunda yang perlu ditangani.
- Jenis - Menunjukkan jenis alarm.
- AppComponent— Menunjukkan Komponen Aplikasi (AppComponents) yang terkait dengan alarm ini.
- ID Referensi - Menunjukkan pengenal logis dari peristiwa AWS CloudFormation tumpukan di AWS CloudFormation.
- ID Rekomendasi - Menunjukkan pengenal logis sumber daya AWS CloudFormation tumpukan di AWS CloudFormation.

7. Di tab Alarm, untuk memfilter rekomendasi alarm di tabel Alarm berdasarkan status tertentu, pilih nomor di bawah yang sama.
8. Pilih alarm yang disarankan yang ingin Anda atur untuk aplikasi Anda, dan pilih Buat CloudFormation template.

9. Di Buat CloudFormation templat dialog, Anda dapat menggunakan nama yang dibuat secara otomatis, atau Anda dapat memasukkan nama untuk AWS CloudFormation templat di kotak nama CloudFormation templat.
10. Pilih Buat. Ini bisa memakan waktu hingga beberapa menit untuk membuat AWS CloudFormation template.

    Selesaikan prosedur berikut untuk memasukkan rekomendasi dalam basis kode Anda.

Untuk menyertakan AWS Resilience Hub rekomendasi basis kode Anda

1. Pilih tab Template untuk melihat template yang baru saja Anda buat. Anda dapat mengidentifikasi template Anda menggunakan yang berikut ini:
   - Nama — Nama penilaian yang Anda berikan pada saat pembuatan.
   - Status - Menunjukkan status eksekusi penilaian.
   - Jenis - Menunjukkan jenis rekomendasi operasional.
   - Format - Menunjukkan format (JSON/teks) di mana template dibuat.
   - Waktu mulai - Menunjukkan waktu mulai penilaian.
   - Waktu akhir - Menunjukkan waktu akhir penilaian.
   - ARN— Template ARN
2. Di bawah Detail templat, pilih tautan di bawah Template S3 Path untuk membuka objek template di konsol Amazon S3.
3. Di konsol Amazon S3, dari tabel Objects, pilih tautan SOP folder.
4. Untuk menyalin jalur Amazon S3, pilih kotak centang di depan JSON file dan pilih Salin. URL
5. Buat AWS CloudFormation tumpukan dari AWS CloudFormation konsol. Untuk informasi selengkapnya tentang membuat AWS CloudFormation tumpukan, lihathttps://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-console-create-stack.html.

   Saat membuat AWS CloudFormation tumpukan, Anda harus menyediakan jalur Amazon S3 yang Anda salin dari langkah sebelumnya.

Melihat alarm

Anda dapat melihat semua alarm aktif yang telah Anda atur untuk memantau ketahanan aplikasi Anda. AWS Resilience Hub menggunakan AWS CloudFormation template untuk menyimpan detail

alarm yang pada gilirannya digunakan untuk membuat alarm di Amazon. CloudWatch Anda dapat mengakses AWS CloudFormation template menggunakan Amazon S3URL, dan dapat mengunduh serta menempatkannya ke dalam pipeline kode Anda atau membuat tumpukan melalui konsol. AWS CloudFormation

Untuk melihat alarm dari dasbor, pilih Dasbor dari menu navigasi kiri. Dalam tabel alarm yang diterapkan, Anda dapat mengidentifikasi alarm yang diterapkan menggunakan informasi berikut:

- Application impacted — Nama aplikasi yang telah menerapkan alarm ini.
- Alarm aktif — Menunjukkan jumlah alarm aktif yang dipicu dari aplikasi.
- FISsedang berlangsung — Menunjukkan AWS FIS eksperimen yang sedang berjalan untuk aplikasi Anda.

Untuk melihat alarm yang diterapkan dalam aplikasi Anda

1. Di menu navigasi kiri, pilih Aplikasi.
2. Pilih aplikasi dari tabel Aplikasi.
3. Di halaman ringkasan aplikasi, tabel alarm yang diterapkan menampilkan semua alarm yang direkomendasikan yang diterapkan dalam aplikasi Anda.

   Untuk menemukan alarm tertentu di tabel Alarm yang diterapkan, di kotak Temukan alarm berdasarkan teks, properti, atau nilai, pilih salah satu bidang berikut, pilih operasi, lalu ketik nilai.

   - Nama alarm — Nama alarm yang telah Anda atur untuk aplikasi Anda.
   - Deskripsi — Menjelaskan tujuan alarm.
   - Status - Menunjukkan status implementasi CloudWatch alarm Amazon saat ini.

     Kolom ini menampilkan salah satu nilai berikut:

     - Diimplementasikan - Menunjukkan bahwa alarm yang direkomendasikan oleh AWS Resilience Hub diimplementasikan dalam aplikasi Anda. Pilih nomor di bawah ini untuk melihat semua alarm yang direkomendasikan dan diterapkan di tab Rekomendasi operasional.
     - Tidak diimplementasikan - Menunjukkan bahwa alarm yang direkomendasikan oleh AWS Resilience Hub disertakan tetapi tidak diimplementasikan dalam aplikasi Anda. Pilih nomor di bawah ini untuk melihat semua alarm yang direkomendasikan dan tidak diterapkan di tab Rekomendasi operasional.

    - Dikecualikan - Menunjukkan bahwa alarm yang direkomendasikan oleh AWS Resilience Hub dikecualikan dari aplikasi Anda. Pilih nomor di bawah ini untuk melihat semua alarm yang direkomendasikan dan dikecualikan di tab Rekomendasi operasional. Untuk informasi selengkapnya tentang memasukkan dan mengecualikan alarm yang direkomendasikan, lihat Menyertakan atau mengecualikan rekomendasi operasional.
    - Tidak Aktif — Menunjukkan bahwa alarm disebarkan ke Amazon CloudWatch, tetapi statusnya disetel ke _ INSUFFICIENTdi DATA Amazon. CloudWatch Pilih nomor di bawah ini untuk melihat semua alarm yang diterapkan dan tidak aktif di tab Rekomendasi operasional.
- Template sumber - Menyediakan Nama Sumber Daya Amazon (ARN) AWS CloudFormation tumpukan yang berisi detail alarm.
- Sumber Daya - Menampilkan sumber daya yang dilampirkan dan diimplementasikan untuk alarm ini.
- Metrik - Menampilkan CloudWatch metrik Amazon yang ditetapkan untuk alarm. Untuk informasi selengkapnya tentang CloudWatch metrik Amazon, lihat CloudWatch Metrik Amazon.
- Perubahan terakhir - Menampilkan tanggal dan waktu alarm terakhir diubah.

Untuk melihat alarm yang direkomendasikan dari penilaian

1. Di menu navigasi kiri, pilih Aplikasi.
2. Pilih aplikasi dari tabel Aplikasi.

   Untuk menemukan aplikasi, masukkan nama aplikasi di kotak Temukan aplikasi.
3. Pilih tab Penilaian.

   Dalam tabel penilaian Ketahanan, Anda dapat mengidentifikasi penilaian Anda menggunakan informasi berikut:

   - Nama — Nama penilaian yang Anda berikan pada saat pembuatan.
   - Status - Menunjukkan status eksekusi penilaian.
   - Status kepatuhan - Menunjukkan apakah penilaian sesuai dengan kebijakan ketahanan.
   - Status penyimpangan ketahanan - Menunjukkan apakah aplikasi Anda telah melayang atau tidak dari penilaian sukses sebelumnya.
   - Versi aplikasi - Versi aplikasi Anda.

- Invoker — Menunjukkan peran yang memanggil penilaian.
- Waktu mulai - Menunjukkan waktu mulai penilaian.
- Waktu akhir - Menunjukkan waktu akhir penilaian.
- ARN— Nama Sumber Daya Amazon (ARN) dari penilaian.

4. Pilih penilaian dari tabel penilaian Ketahanan.
5. Pilih tab Rekomendasi Operasional.
6. Jika tidak dipilih secara default, pilih tab Alarm.

   Di tabel Alarm, Anda dapat mengidentifikasi alarm yang disarankan menggunakan yang berikut ini:

   - Nama — Nama alarm yang telah Anda tetapkan untuk aplikasi Anda.
   - Deskripsi — Menjelaskan tujuan alarm.
   - Status - Menunjukkan status implementasi CloudWatch alarm Amazon saat ini.

     Kolom ini menampilkan salah satu nilai berikut:

     - Diimplementasikan - Menunjukkan bahwa alarm diimplementasikan dalam aplikasi Anda. Memilih nomor di bawah ini akan memfilter tabel Alarm untuk menampilkan semua alarm yang direkomendasikan yang diterapkan dalam aplikasi Anda.
     - Tidak diimplementasikan - Menunjukkan bahwa alarm tidak diimplementasikan atau disertakan dalam aplikasi Anda. Memilih nomor di bawah ini akan memfilter tabel Alarm untuk menampilkan semua alarm yang direkomendasikan yang tidak diterapkan dalam aplikasi Anda.
     - Dikecualikan - Menunjukkan bahwa alarm dikecualikan dari aplikasi. Memilih nomor di bawah ini akan memfilter tabel Alarm untuk menampilkan semua alarm yang disarankan yang dikecualikan dari aplikasi Anda. Untuk informasi selengkapnya tentang memasukkan dan mengecualikan alarm yang disarankan, lihat. the section called “Termasuk atau tidak termasuk rekomendasi operasional”
     - Tidak Aktif — Menunjukkan bahwa alarm disebarkan ke Amazon CloudWatch, tetapi statusnya disetel ke _ INSUFFICIENTdi DATA Amazon. CloudWatch Memilih nomor di bawah ini akan memfilter tabel Alarm untuk menampilkan semua alarm yang diterapkan dan tidak aktif.

   - Konfigurasi - Menunjukkan jika ada dependensi konfigurasi yang tertunda yang perlu ditangani.

- Jenis - Menunjukkan jenis alarm.
- AppComponent— Menunjukkan Komponen Aplikasi (AppComponents) yang terkait dengan alarm ini.
- ID Referensi - Menunjukkan pengenal logis dari peristiwa AWS CloudFormation tumpukan di AWS CloudFormation.
- ID Rekomendasi - Menunjukkan pengenal logis sumber daya AWS CloudFormation tumpukan di AWS CloudFormation.

Mengelola prosedur operasi standar

Prosedur operasi standar (SOP) adalah serangkaian langkah preskriptif yang dirancang untuk memulihkan aplikasi Anda secara efisien jika terjadi pemadaman atau alarm. Persiapkan, uji, dan ukur SOP Anda terlebih dahulu untuk memastikan pemulihan tepat waktu jika terjadi pemadaman operasional.

Berdasarkan Komponen Aplikasi Anda, AWS Resilience Hub rekomendasikan SOP yang harus Anda persiapkan. AWS Resilience Hub Bekerja dengan Systems Manager untuk mengotomatiskan langkah-langkah SOP Anda dengan menyediakan sejumlah dokumen SSM yang dapat Anda gunakan sebagai dasar untuk SOP tersebut.

Misalnya, AWS Resilience Hub dapat merekomendasikan SOP untuk menambahkan ruang disk berdasarkan dokumen SSM Automation yang ada. Untuk menjalankan dokumen SSM ini, Anda memerlukan peran IAM tertentu dengan izin yang benar. AWS Resilience Hub membuat metadata dalam aplikasi Anda yang menunjukkan dokumen otomatisasi SSM mana yang akan dijalankan jika terjadi kekurangan disk, dan peran IAM mana yang diperlukan untuk menjalankan dokumen SSM tersebut. Metadata ini kemudian disimpan dalam parameter SSM.

Selain mengonfigurasi otomatisasi SSM, ini juga merupakan praktik terbaik untuk mengujinya dengan eksperimen AWS FIS . Oleh karena itu, AWS Resilience Hub juga menyediakan AWS FIS eksperimen yang memanggil dokumen otomatisasi SSM - dengan cara ini, Anda dapat secara proaktif menguji aplikasi Anda untuk memastikan SOP yang Anda buat melakukan pekerjaan yang diinginkan.

AWS Resilience Hub memberikan rekomendasinya dalam bentuk AWS CloudFormation templat yang dapat Anda tambahkan ke basis kode aplikasi Anda. Template ini menyediakan:

- Peran IAM dengan izin yang diperlukan untuk menjalankan SOP.

- AWS FIS Eksperimen yang dapat Anda gunakan untuk menguji SOP.
- Parameter SSM yang berisi metadata aplikasi yang menunjukkan dokumen SSM mana dan peran IAM mana yang akan dijalankan sebagai SOP, dan sumber daya mana. Misalnya: `$(DocumentName) for SOP $(HandleCrisisA) on $(ResourceA)`.

Membuat SOP mungkin memerlukan beberapa trial and error. Menjalankan penilaian ketahanan terhadap aplikasi Anda dan membuat AWS CloudFormation templat dari AWS Resilience Hub rekomendasi adalah awal yang baik. Gunakan AWS CloudFormation template untuk menghasilkan AWS CloudFormation tumpukan, lalu gunakan parameter SSM dan nilai defaultnya di SOP Anda. Jalankan SOP dan lihat penyempurnaan apa yang perlu Anda lakukan.

Karena semua aplikasi memiliki persyaratan yang berbeda, daftar default dokumen SSM yang AWS Resilience Hub menyediakan tidak akan cukup untuk semua kebutuhan Anda. Namun, Anda dapat menyalin dokumen SSM default dan menggunakannya sebagai dasar untuk membuat dokumen kustom Anda sendiri yang disesuaikan untuk aplikasi Anda. Anda juga dapat membuat dokumen SSM Anda sendiri yang sama sekali baru. Jika Anda membuat dokumen SSM Anda sendiri alih-alih memodifikasi default, Anda harus mengaitkannya dengan parameter SSM, sehingga dokumen SSM yang benar dipanggil ketika SOP berjalan.

Ketika Anda telah menyelesaikan SOP Anda dengan membuat dokumen SSM yang diperlukan dan memperbarui parameter dan asosiasi dokumen yang diperlukan, tambahkan dokumen SSM langsung ke basis kode Anda, dan buat perubahan atau penyesuaian berikutnya di sana. Dengan begitu, setiap kali Anda menerapkan aplikasi Anda, Anda juga akan menerapkan SOP terbanyak up-to-date .

Topik

Membangun SOP berdasarkan rekomendasi AWS Resilience Hub

Untuk membangun SOP berdasarkan AWS Resilience Hub rekomendasi, Anda memerlukan AWS Resilience Hub aplikasi dengan kebijakan ketahanan yang melekat padanya, dan Anda

harus menjalankan penilaian ketahanan terhadap aplikasi itu. Penilaian ketahanan menghasilkan rekomendasi untuk SOP Anda.

Untuk membangun SOP berdasarkan AWS Resilience Hub rekomendasi, Anda harus membuat AWS CloudFormation template untuk SOP yang direkomendasikan dan memasukkannya ke dalam basis kode Anda.

Buat AWS CloudFormation template untuk rekomendasi SOP

1. Buka AWS Resilience Hub konsol.
2. Pada panel navigasi, pilih Aplikasi.
3. Dari daftar aplikasi, pilih aplikasi yang ingin Anda buat SOP.
4. Pilih tab Penilaian.
5. Pilih penilaian dari tabel penilaian Ketahanan. Jika Anda tidak memiliki penilaian, selesaikan prosedur the section called “Menjalankan penilaian ketahanan” dan kemudian kembali ke langkah ini.
6. Di bawah rekomendasi Operasional, pilih Prosedur operasi standar.
7. Pilih semua rekomendasi SOP yang ingin Anda sertakan.
8. Pilih Buat CloudFormation template. Ini bisa memakan waktu hingga beberapa menit untuk membuat AWS CloudFormation template.

   Selesaikan prosedur berikut untuk menyertakan rekomendasi SOP di basis kode Anda.

Untuk menyertakan AWS Resilience Hub rekomendasi dalam basis kode Anda

1. Dalam Rekomendasi operasional, pilih Template.
2. Dalam daftar template, pilih nama template SOP yang baru saja Anda buat.

   Anda dapat mengidentifikasi SOP yang diterapkan dalam aplikasi Anda menggunakan informasi berikut:

   - Nama SOP — Nama SOP yang telah Anda tetapkan untuk aplikasi Anda.
   - Deskripsi — Menjelaskan tujuan SOP.
   - Dokumen SSM — URL Amazon S3 dari dokumen SSM yang berisi definisi SOP.
   - Uji coba — URL Amazon S3 dari dokumen yang berisi hasil pengujian terbaru.

- Template sumber - Menyediakan Nama Sumber Daya Amazon (ARN) dari AWS CloudFormation tumpukan yang berisi detail SOP.

3. Di bawah Detail templat, pilih tautan di Template S3 Path untuk membuka objek template di konsol Amazon S3.
4. Di konsol Amazon S3, dari tabel Objects, pilih tautan folder SOP.
5. Untuk menyalin jalur Amazon S3, pilih kotak centang di depan file JSON dan pilih Salin URL.
6. Buat AWS CloudFormation tumpukan dari AWS CloudFormation konsol. Untuk informasi selengkapnya tentang membuat AWS CloudFormation tumpukan, lihathttps://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-console-create-stack.html.

   Saat membuat AWS CloudFormation tumpukan, Anda harus menyediakan jalur Amazon S3 yang Anda salin dari langkah sebelumnya.

Membuat dokumen SSM kustom

Untuk sepenuhnya mengotomatiskan pemulihan aplikasi Anda, Anda mungkin perlu membuat dokumen SSM khusus untuk SOP Anda di konsol Systems Manager. Anda dapat memodifikasi dokumen SSM yang ada sebagai basis, atau Anda dapat membuat dokumen SSM baru.

Untuk informasi rinci tentang penggunaan Systems Manager untuk membuat dokumen SSM, lihat Panduan: Menggunakan Pembuat Dokumen untuk membuat buku runbook kustom.

Untuk informasi tentang sintaks dokumen SSM, lihat sintaks dokumen SSM.

Untuk informasi tentang mengotomatiskan tindakan dokumen SSM, lihat referensi tindakan otomatisasi Systems Manager.

Menggunakan dokumen SSM kustom, bukan default

Untuk mengganti dokumen SSM yang AWS Resilience Hub disarankan untuk SOP Anda dengan dokumen khusus yang telah Anda buat, kerjakan langsung di basis kode Anda. Selain menambahkan dokumen otomatisasi SSM kustom baru Anda, Anda juga akan:

1. Tambahkan izin IAM yang diperlukan untuk menjalankan otomatisasi.
2. Tambahkan AWS FIS eksperimen untuk menguji dokumen SSM Anda.
3. Tambahkan parameter SSM yang menunjuk ke dokumen otomatisasi yang ingin Anda gunakan sebagai SOP.

Umumnya, paling efisien untuk bekerja dengan nilai default yang disarankan AWS Resilience Hub dan menyesuaikannya seperlunya. Misalnya, tambahkan atau hapus izin yang diperlukan untuk peran IAM, ubah penyiapan AWS FIS eksperimen untuk menunjuk ke dokumen SSM baru, atau mengubah parameter SSM untuk menunjuk ke dokumen SSM baru Anda.

Menguji SOP

Seperti disebutkan sebelumnya, praktik terbaik adalah menambahkan AWS FIS eksperimen ke saluran CI/CD Anda untuk menguji SOP Anda secara teratur; ini memastikan mereka siap untuk pergi jika terjadi pemadaman.

Uji SOP AWS Resilience Hub-provided dan custom.

Melihat prosedur operasi standar

Untuk melihat SOP yang diimplementasikan dari aplikasi

1. Di menu navigasi kiri, pilih Aplikasi.
2. Di Aplikasi, buka aplikasi.
3. Pilih tab Prosedur Operasi Standar.

   Di bagian ringkasan prosedur operasi standar, tabel prosedur operasi standar yang diterapkan menampilkan daftar SOP yang dihasilkan dari rekomendasi SOP.

   Anda dapat mengidentifikasi SOP Anda dengan yang berikut:

   - Nama SOP — Nama SOP yang telah Anda tetapkan untuk aplikasi Anda.
   - Dokumen SSM — URL S3 dari dokumen Amazon EC2 Systems Manager yang berisi definisi SOP.
   - Deskripsi — Menjelaskan tujuan SOP.
   - Uji coba — URL S3 dari dokumen yang berisi hasil tes terbaru.
   - ID Referensi — Pengidentifikasi rekomendasi SOP yang direferensikan.
   - Resource ID — Pengidentifikasi sumber daya yang rekomendasi SOP diimplementasikan.

Untuk melihat SOP yang direkomendasikan dari penilaian

1. Di menu navigasi kiri, pilih Aplikasi.
2. Pilih aplikasi dari tabel Aplikasi.

Untuk menemukan aplikasi, masukkan nama aplikasi di kotak Temukan aplikasi.

3. Pilih tab Penilaian.

   Dalam tabel penilaian Ketahanan, Anda dapat mengidentifikasi penilaian Anda menggunakan informasi berikut:

   - Nama — Nama penilaian yang Anda berikan pada saat pembuatan.
   - Status - Menunjukkan status eksekusi penilaian.
   - Status kepatuhan - Menunjukkan apakah penilaian sesuai dengan kebijakan ketahanan.
   - Status penyimpangan ketahanan - Menunjukkan apakah aplikasi Anda telah melayang atau tidak dari penilaian sukses sebelumnya.
   - Versi aplikasi - Versi aplikasi Anda.
   - Invoker — Menunjukkan peran yang memanggil penilaian.
   - Waktu mulai - Menunjukkan waktu mulai penilaian.
   - Waktu akhir - Menunjukkan waktu akhir penilaian.
   - ARN — Nama Sumber Daya Amazon (ARN) dari penilaian.
4. Pilih penilaian dari tabel penilaian Ketahanan.
5. Pilih tab Rekomendasi Operasional.
6. Pilih tab Prosedur Operasi Standar.

   Dalam tabel prosedur operasi Standar, Anda dapat memahami lebih lanjut tentang SOP yang direkomendasikan menggunakan informasi berikut:

   - Nama — Nama SOP yang direkomendasikan.
   - Deskripsi — Menjelaskan tujuan SOP.
   - Negara - Menunjukkan status implementasi SOP saat ini. Yaitu, Diimplementasikan, Tidak diimplementasikan, dan Dikecualikan.
   - Konfigurasi - Menunjukkan jika ada dependensi konfigurasi yang tertunda yang perlu ditangani.
   - Jenis - Menunjukkan jenis SOP.
   - AppComponent— Menunjukkan Komponen Aplikasi (AppComponents) yang terkait dengan SOP ini. Untuk informasi selengkapnya tentang dukungan AppComponents, lihat Mengelompokkan sumber daya dalam file AppComponent.

- ID Referensi - Menunjukkan pengidentifikasi logis dari peristiwa AWS CloudFormation tumpukan di AWS CloudFormation.
- ID Rekomendasi - Menunjukkan pengenal logis sumber daya AWS CloudFormation tumpukan di AWS CloudFormation.

Mengelola eksperimen Layanan Injeksi Kesalahan Amazon

Bagian ini menjelaskan cara membuat dan menjalankan eksperimen Amazon Fault Injection Service (AWS FIS) di AWS Resilience Hub. Anda menjalankan AWS FIS eksperimen untuk mengukur ketahanan AWS sumber daya Anda dan jumlah waktu yang diperlukan untuk memulihkan dari aplikasi, infrastruktur, zona ketersediaan, dan Wilayah AWS insiden.

Untuk mengukur ketahanan, AWS FIS eksperimen ini mensimulasikan gangguan pada sumber daya Anda. AWS Contoh gangguan termasuk kesalahan jaringan yang tidak tersedia, kegagalan, proses yang dihentikan di Amazon EC2 atau AWS ASG, pemulihan boot di Amazon RDS, dan masalah dengan Availability Zone Anda. Ketika AWS FIS percobaan selesai, Anda dapat memperkirakan apakah aplikasi dapat pulih dari jenis pemadaman yang ditentukan dalam target RTO dari kebijakan ketahanan.

Semua eksperimen AWS Resilience Hub dibangun menggunakan AWS FIS dan mereka melakukan AWS FIS tindakan. Sebagian besar AWS FIS eksperimen menggunakan tindakan otomatisasi Systems Manager untuk melakukan gangguan dan memantau alarm, dan AWS FIS eksperimen lain hanya menggunakan tindakan AWS FIS otomatisasi yang disesuaikan dengan AWS layanan tertentu (seperti tindakan Amazon EKS). Untuk informasi selengkapnya tentang AWS FIS tindakan, lihat referensi AWS FIS tindakan.

Anda dapat menggunakan AWS FIS eksperimen dalam status default atau menyesuaikannya berdasarkan kebutuhan Anda. AWS FIS eksperimen dapat diakses dari AWS Resilience Hub (the section called “Melihat eksperimen injeksi kesalahan”) atau AWS FIS console (AWS FIS).

Topik

- Membuat AWS FIS eksperimen dari rekomendasi operasional
- Menjalankan AWS FIS eksperimen dari AWS Resilience Hub
- Melihat eksperimen injeksi kesalahan
- Kegagalan eksperimen/pemeriksaan status Layanan Injeksi Kesalahan Amazon

Membuat AWS FIS eksperimen dari rekomendasi operasional

AWS Resilience Hub merekomendasikan agar Anda menguji aplikasi Anda setelah Anda menjalankan laporan penilaian. Anda dapat mengakses dan menjalankan eksperimen ini dari laporan Penilaian aplikasi Anda.

AWS Resilience Hub menyediakan daftar AWS FIS eksperimen, yang merupakan dokumen Systems Manager dengan parameter pengujian. Saat Anda memilih AWS FIS eksperimen dari daftar, AWS Resilience Hub buat AWS CloudFormation templat dengan parameter yang Anda tentukan dalam dokumen Systems Manager. Setelah pembuatan AWS CloudFormation tumpukan, Anda dapat melihat AWS FIS eksperimen yang disediakan untuk aplikasi Anda.

AWS CloudFormation Template terdiri dari peran IAM untuk setiap dokumen Systems Manager, dengan izin minimum yang diperlukan untuk menjalankan.

Untuk membuat AWS FIS eksperimen berdasarkan AWS Resilience Hub rekomendasi, Anda harus membuat AWS CloudFormation templat untuk pengujian yang direkomendasikan dan memasukkannya ke dalam basis kode Anda.

Untuk membuat AWS CloudFormation template untuk AWS FIS percobaan

1. Buka AWS Resilience Hub konsol.
2. Pada panel navigasi, pilih Aplikasi.
3. Dari daftar aplikasi, pilih aplikasi yang ingin Anda uji.
4. Pilih tab Penilaian.
5. Pilih penilaian dari tabel penilaian Ketahanan. Jika Anda tidak memiliki penilaian, selesaikan prosedur the section called “Menjalankan penilaian ketahanan” dan kemudian kembali ke langkah ini.
6. Di bawah rekomendasi Operasional, pilih Eksperimen injeksi kesalahan.
7. Pilih semua tes yang ingin Anda sertakan.
8. Pilih Buat CloudFormation template. Ini bisa memakan waktu hingga beberapa menit untuk membuat AWS CloudFormation template.
9. Pilih Template.

   Anda dapat melihat AWS CloudFormation template yang baru dibuat di tabel Template.

   Selesaikan prosedur berikut untuk memasukkan rekomendasi dalam basis kode Anda.

Untuk menyertakan AWS Resilience Hub rekomendasi dalam basis kode Anda

1. Dalam Rekomendasi operasional, pilih Template.
2. Dalam daftar template, pilih nama template AWS FIS percobaan yang baru saja Anda buat.

   Anda dapat mengidentifikasi tes yang diterapkan dalam aplikasi Anda menggunakan informasi berikut:

   - Nama uji — Nama tes yang telah Anda buat untuk aplikasi Anda.
   - Deskripsi — Menjelaskan tujuan tes.
   - Status - Menunjukkan status implementasi pengujian saat ini.

     Kolom ini menampilkan salah satu nilai berikut:

     - Diimplementasikan - Menunjukkan bahwa pengujian diimplementasikan dalam aplikasi Anda.
     - Tidak diimplementasikan - Menunjukkan bahwa pengujian tidak diimplementasikan atau disertakan dalam aplikasi Anda.
     - Dikecualikan - Menunjukkan bahwa tes dikecualikan dari aplikasi.
     - Tidak aktif - Menunjukkan bahwa pengujian diterapkan ke AWS FIS, tetapi belum berjalan dalam 30 hari terakhir.
   - Uji coba — URL Amazon S3 dari dokumen yang berisi hasil pengujian terbaru.
   - Template sumber - Menyediakan Nama Sumber Daya Amazon (ARN) AWS CloudFormation tumpukan yang berisi detail eksperimen.
3. Di bawah Detail templat, pilih tautan di Template S3 Path untuk membuka objek template di konsol Amazon S3.
4. Di konsol Amazon S3, dari tabel Objects, pilih tautan folder uji.
5. Untuk menyalin jalur Amazon S3, pilih kotak centang di depan file JSON dan pilih Salin URL.
6. Buat AWS CloudFormation tumpukan dari AWS CloudFormation konsol. Untuk informasi selengkapnya tentang membuat AWS CloudFormation tumpukan, lihathttps://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-console-create-stack.html.

   Saat membuat AWS CloudFormation tumpukan, Anda harus menyediakan jalur Amazon S3 yang Anda salin dari langkah sebelumnya.

Menjalankan AWS FIS eksperimen dari AWS Resilience Hub

Dalam aplikasi Anda, Anda harus terlebih dahulu membuat template AWS FIS eksperimen dari rekomendasi operasional sebelum AWS Resilience Hub dapat menjalankan AWS FIS eksperimen.

Untuk memulai AWS FIS percobaan

1. Di menu navigasi kiri, pilih Aplikasi.
2. Dari tabel Aplikasi, buka aplikasi.
3. Pilih tab Eksperimen injeksi kesalahan.
4. Pilih tombol radio sebelum templat eksperimen yang digunakan untuk membuat eksperimen yang ingin Anda jalankan dari tabel Templat eksperimen, lalu pilih Mulai eksperimen.

Untuk menghentikan AWS FIS percobaan

1. Di menu navigasi kiri, pilih Aplikasi.
2. Dari tabel Aplikasi, buka aplikasi.
3. Pilih tab Eksperimen injeksi kesalahan.
4. Pilih tombol radio sebelum percobaan dari tabel Eksperimen, lalu pilih Hentikan eksperimen.

Melihat eksperimen injeksi kesalahan

Di AWS Resilience Hub, lihat AWS FIS eksperimen yang Anda siapkan untuk mengukur ketahanan AWS sumber daya Anda dan jumlah waktu yang diperlukan untuk memulihkan dari aplikasi, infrastruktur, zona ketersediaan, dan Wilayah AWS insiden.

Untuk melihat AWS FIS eksperimen dari dasbor, pilih Dasbor dari menu navigasi kiri. Dalam tabel Eksperimen, Anda dapat mengidentifikasi AWS FIS eksperimen yang diterapkan menggunakan informasi berikut:

- ID Eksperimen — Pengidentifikasi AWS FIS percobaan.
- ID templat eksperimen — Pengidentifikasi template AWS FIS eksperimen yang digunakan untuk membuat AWS FIS eksperimen.
- Template sumber - Menyediakan Nama Sumber Daya Amazon (ARN) AWS CloudFormation tumpukan yang berisi detail eksperimen. AWS FIS
- Status - Menunjukkan apakah AWS FIS percobaan berhasil diselesaikan atau tidak.

Untuk melihat AWS FIS eksperimen yang diterapkan dari aplikasi

1. Di menu navigasi kiri, pilih Aplikasi.
2. Dari tabel Aplikasi, buka aplikasi.
3. Pilih Eksperimen injeksi kesalahan.
4. Pilih tab Eksperimen.

   Di tab Eksperimen, Anda dapat melihat daftar AWS FIS eksperimen aktif di tabel Eksperimen.

   Dalam tabel Eksperimen, Anda dapat mengidentifikasi AWS FIS eksperimen yang diterapkan menggunakan informasi berikut:

   - Nama pengujian — Nama pengujian yang direkomendasikan oleh AWS Resilience Hub yang digunakan untuk membuat eksperimen. AWS FIS
   - ID Eksperimen — Pengidentifikasi AWS FIS percobaan.
   - Deskripsi — Menjelaskan tujuan AWS FIS percobaan.
   - Waktu pembuatan — Tanggal dan waktu saat AWS FIS percobaan dibuat.
   - Waktu pembaruan terakhir - Tanggal dan waktu AWS FIS percobaan terakhir diperbarui.
   - Template sumber - Menyediakan Nama Sumber Daya Amazon (ARN) AWS CloudFormation tumpukan yang berisi detail eksperimen. AWS FIS

Untuk melihat eksperimen yang direkomendasikan dari penilaian

1. Di menu navigasi kiri, pilih Aplikasi.
2. Pilih aplikasi dari tabel Aplikasi.

   Untuk menemukan aplikasi, masukkan nama aplikasi di kotak Temukan aplikasi.
3. Pilih tab Penilaian.

   Dalam tabel penilaian Ketahanan, Anda dapat mengidentifikasi penilaian Anda menggunakan informasi berikut:

   - Nama — Nama penilaian yang Anda berikan pada saat pembuatan.
   - Status - Menunjukkan status eksekusi penilaian.
   - Status kepatuhan - Menunjukkan apakah penilaian sesuai dengan kebijakan ketahanan.

- Status resiliency drift — Menunjukkan apakah aplikasi Anda telah hanyut atau tidak dari penilaian sukses sebelumnya.
- Versi aplikasi - Versi aplikasi Anda.
- Invoker — Menunjukkan peran yang memanggil penilaian.
- Waktu mulai - Menunjukkan waktu mulai penilaian.
- Waktu akhir - Menunjukkan waktu akhir penilaian.
- ARN — Nama Sumber Daya Amazon (ARN) dari penilaian.

4. Pilih penilaian dari tabel penilaian Ketahanan.
5. Pilih tab Rekomendasi Operasional.
6. Pilih tab Eksperimen injeksi kesalahan.

   Dalam tabel template eksperimen injeksi kesalahan, Anda dapat memahami lebih lanjut tentang tes yang direkomendasikan menggunakan informasi berikut:

   - Nama — Nama tes yang direkomendasikan.
   - Deskripsi — Menjelaskan tujuan tes.
   - Status - Menunjukkan status implementasi pengujian saat ini.

     Kolom ini menampilkan salah satu nilai berikut:

     - Diimplementasikan - Menunjukkan bahwa pengujian diimplementasikan dalam aplikasi Anda.
     - Tidak diimplementasikan - Menunjukkan bahwa pengujian tidak diimplementasikan atau disertakan dalam aplikasi Anda.
     - Dikecualikan - Menunjukkan bahwa tes dikecualikan dari aplikasi.
     - Tidak aktif - Menunjukkan bahwa pengujian diterapkan ke AWS FIS, tetapi belum berjalan dalam 30 hari terakhir.
   - Konfigurasi - Menunjukkan jika ada dependensi konfigurasi yang tertunda yang perlu ditangani.
   - Jenis - Menunjukkan jenis tes.
   - AppComponent— Menunjukkan Komponen Aplikasi (AppComponents) yang terkait dengan tes ini. Untuk informasi selengkapnya tentang dukungan AppComponents, lihat Mengelompokkan sumber daya dalam file AppComponent.

- Risiko — Menunjukkan tingkat risiko kegagalan tes. Tingkat risiko diindikasikan menggunakan Tinggi, Sedang, dan Rendah untuk menunjukkan tingkat risiko tinggi, sedang, dan rendah, masing-masing.
- ID Referensi - Menunjukkan pengidentifikasi logis dari peristiwa AWS CloudFormation tumpukan di AWS CloudFormation.
- ID Rekomendasi - Menunjukkan pengenal logis sumber daya AWS CloudFormation tumpukan di AWS CloudFormation.

Kegagalan eksperimen/pemeriksaan status Layanan Injeksi Kesalahan Amazon

AWS Resilience Hub memungkinkan Anda melacak status eksperimen yang telah Anda mulai. Untuk informasi selengkapnya, lihat Untuk melihat eksperimen yang direkomendasikan dari prosedur penilaian dithe section called “Melihat eksperimen injeksi kesalahan”.

Topik

- Menganalisis eksekusi AWS FIS eksperimen menggunakan AWS Systems Manager
- AWS FIS kegagalan percobaan saat menguji pod Kubernetes yang berjalan di klaster Amazon Elastic Kubernetes Service

Menganalisis eksekusi AWS FIS eksperimen menggunakan AWS Systems Manager

Setelah menjalankan AWS FIS eksperimen, Anda dapat melihat detail eksekusi di AWS Systems Manager.

1. Pergi ke CloudTrail> Riwayat Acara.
2. Filter peristiwa berdasarkan Nama pengguna menggunakan ID percobaan.
3. Lihat StartAutomationExecution entri. ID Permintaan adalah ID otomatisasi SSM.
4. Pergi ke AWS Systems Manager > Automation.
5. Filter berdasarkan ID Eksekusi menggunakan ID otomatisasi SSM dan lihat detail otomatisasi.

   Anda dapat menganalisis eksekusi dengan otomatisasi Systems Manager apa pun. Untuk informasi selengkapnya, lihat panduan pengguna AWS Systems Manager Automation. Parameter input eksekusi muncul di bagian Parameter input dari Detail Eksekusi dan menyertakan parameter opsional yang tidak muncul dalam AWS FIS percobaan.

Anda dapat menemukan informasi tentang status langkah dan detail langkah lainnya dengan menelusuri langkah-langkah spesifik dalam langkah-langkah Eksekusi.

Kegagalan umum

Berikut ini adalah kegagalan umum yang dihadapi saat menjalankan laporan penilaian:

- Template alarm tidak digunakan sebelum percobaan test/SOP dijalankan. Ini menyebabkan pesan kesalahan selama langkah otomatisasi.
  - Pesan kegagalan: `The following parameters were not found: [/ResilienceHub/Alarm/3dee49a1-9877-452a-bb0c-a958479a8ef2/nat-gw-alarm-bytes-out-to-source-2020-09-21_nat-02ad9bc4fbd4e6135]. Make sure all the SSM parameters in automation document are created in SSM Parameter Store.`
  - Remediasi: Pastikan untuk membuat alarm yang relevan dan menyebarkan template yang dihasilkan sebelum menjalankan kembali eksperimen injeksi kesalahan.
- Izin yang hilang dalam peran eksekusi. Pesan kesalahan ini terjadi jika peran eksekusi yang diberikan tidak memiliki izin dan muncul dalam detail langkah.
  - Pesan kegagalan:`An error occurred (Unauthorized Operation) when calling the DescribeInstanceStatus operation: You are not authorized to perform this operation. Please Refer to Automation Service Troubleshooting Guide for more diagnosis details.`
  - Remediasi: Verifikasi bahwa Anda memberikan peran eksekusi yang benar. Jika ini dilakukan, tambahkan izin yang diperlukan dan jalankan kembali penilaian.
- Eksekusi berhasil tetapi tidak memiliki hasil yang diharapkan. Ini adalah hasil dari parameter yang salah atau masalah otomatisasi internal.
  - Pesan kegagalan: Eksekusi berhasil, jadi tidak ada pesan kesalahan yang ditampilkan.
  - Remediasi: Periksa parameter input dan lihat langkah-langkah yang dijalankan seperti yang dijelaskan dalam Analisis eksekusi AWS FIS eksperimen sebelum memeriksa langkah-langkah individu untuk input dan output yang diharapkan.

AWS FIS kegagalan percobaan saat menguji pod Kubernetes yang berjalan di klaster Amazon Elastic Kubernetes Service

Berikut ini adalah kegagalan Amazon Elastic Kubernetes Service (Amazon EKS) yang umum ditemui saat menguji pod Kubernetes yang berjalan di cluster Amazon EKS Anda:

- Konfigurasi peran IAM yang salah untuk AWS FIS eksperimen atau akun layanan Kubernetes.
  - Pesan kegagalan:
    - `Error resolving targets. Kubernetes API returned ApiException with error code 401.`
    - `Error resolving targets. Kubernetes API returned ApiException with error code 403.`
    - `Unable to inject AWS FIS Pod: Kubernetes API returned status code 403. Check Amazon EKS logs for more details.`
  - Remediasi: Verifikasi hal berikut.
    - Pastikan Anda telah mengikuti instruksi di Gunakan AWS FIS`aws:eks:pod` tindakan.
    - Pastikan Anda telah membuat dan mengonfigurasi Akun Layanan Kubernetes dengan izin RBAC yang diperlukan dan namespace yang benar.
    - Pastikan Anda telah memetakan peran IAM yang disediakan (lihat output dari AWS CloudFormation tumpukan pengujian) ke pengguna Kubernetes.
- Tidak dapat memulai AWS FIS Pod: Kontainer sespan yang gagal tercapai. Ini biasanya terjadi ketika memori tidak cukup untuk menjalankan wadah AWS FIS sespan.
  - Pesan kegagalan:`Unable to heartbeat FIS Pod: Max failed sidecar containers reached.`
  - Remediasi: Salah satu opsi untuk menghindari kesalahan ini adalah dengan mengurangi persentase beban target agar selaras dengan memori atau CPU yang tersedia.
- Pernyataan alarm gagal pada awal percobaan. Kesalahan ini terjadi karena alarm terkait tidak memiliki titik data.
  - Pesan kegagalan:`Assertion failed for the following alarms`. Daftar semua alarm yang pernyataannya gagal.
  - Remediasi: Pastikan Wawasan Kontainer dipasang dengan benar untuk alarm dan alarm tidak dihidupkan (dalam `ALARM` status).

Memahami skor ketahanan

Bagian ini menjelaskan bagaimana AWS Resilience Hub mengukur kesiapan aplikasi dari skenario gangguan yang berbeda.

AWS Resilience Hub memberikan skor ketahanan yang mewakili postur ketahanan aplikasi. Skor ini mencerminkan seberapa dekat aplikasi mengikuti rekomendasi kami untuk memenuhi kebijakan ketahanan aplikasi, alarm, prosedur operasi standar (SOPs), dan pengujian. Berdasarkan jenis sumber daya yang digunakan aplikasi, AWS Resilience Hub merekomendasikan alarmSOPs, dan serangkaian tes untuk setiap jenis gangguan.

Skor ketahanan teratas adalah 100 poin. Untuk mencapai skor terbaik atau skor teratas, Anda harus menerapkan semua alarm yang disarankan,SOPs, dan tes dalam aplikasi Anda. Misalnya, AWS Resilience Hub merekomendasikan satu tes dengan satu alarm dan satuSOP. Tes berjalan dan menyalakan alarm dan memulai yang terkaitSOP. Jika mereka berhasil dan jika aplikasi memenuhi kebijakan ketahanan, ia menerima skor ketahanan mendekati atau sama dengan 100 poin.

Setelah menjalankan penilaian pertama, AWS Resilience Hub berikan opsi untuk mengecualikan rekomendasi operasional dari aplikasi Anda. Untuk memahami dampak rekomendasi yang dikecualikan pada skor ketahanan, Anda harus menjalankan penilaian baru. Namun, Anda selalu dapat memasukkan rekomendasi yang dikecualikan dalam aplikasi Anda dan menjalankan penilaian baru. Untuk informasi selengkapnya tentang memasukkan dan mengecualikan alarmSOP, dan rekomendasi pengujian, lihatthe section called “Termasuk atau tidak termasuk rekomendasi operasional”.

Mengakses skor Ketahanan aplikasi Anda

Anda dapat melihat skor Ketahanan aplikasi Anda dengan memilih Dasbor atau Aplikasi dari menu navigasi.

Mengakses skor Ketahanan dari Dasbor

1. Di menu navigasi kiri, pilih Dasbor.
2. Dalam Skor ketahanan aplikasi dari waktu ke waktu, pilih satu atau beberapa aplikasi dalam daftar dropdown Pilih hingga 4 aplikasi.
3. Bagan skor Ketahanan menampilkan skor ketahanan untuk semua aplikasi yang dipilih.

Mengakses skor Ketahanan dari Aplikasi

1. Di menu navigasi kiri, pilih Aplikasi.
2. Di Aplikasi, buka aplikasi.
3. Pilih Ringkasan.

   Grafik skor Ketahanan menampilkan tren skor ketahanan aplikasi Anda hingga satu tahun. AWS Resilience Hub menampilkan item tindakan, pelanggaran kebijakan ketahanan, dan rekomendasi operasional yang perlu ditangani untuk meningkatkan dan mencapai skor ketahanan semaksimal mungkin menggunakan yang berikut:

   - Untuk melihat item tindakan yang perlu diselesaikan untuk meningkatkan dan mencapai skor ketahanan maksimum yang mungkin, pilih tab Item tindakan. Saat dipilih, AWS Resilience Hub menampilkan yang berikut ini:
     - RTO/RPO— Menunjukkan jumlah waktu pemulihan (RTO/RPOs) yang perlu diperbaiki untuk menyelesaikan pelanggaran dalam kebijakan ketahanan aplikasi Anda. Pilih nilai untuk melihat RTO RPO /detail dalam laporan penilaian aplikasi Anda.
     - Alarm - Menunjukkan jumlah CloudWatch alarm Amazon yang direkomendasikan yang perlu diimplementasikan dalam aplikasi Anda. Pilih nilai untuk melihat CloudWatch alarm Amazon yang perlu diperbaiki dalam laporan penilaian aplikasi Anda.
     - SOPs— Menunjukkan jumlah rekomendasi SOPs yang perlu diimplementasikan dalam aplikasi Anda. Pilih nilai untuk melihat SOPs yang perlu diperbaiki dalam laporan penilaian aplikasi Anda.
     - FIS— Menunjukkan jumlah tes yang direkomendasikan yang perlu diimplementasikan dalam aplikasi Anda. Pilih nilai untuk melihat tes yang perlu diperbaiki dalam laporan penilaian aplikasi Anda.
   - Untuk melihat skor setiap komponen yang memengaruhi skor ketahanan Anda, pilih Rincian skor. Saat dipilih, AWS Resilience Hub menampilkan yang berikut ini:
     - RTO/RPOkepatuhan — Menunjukkan seberapa patuh Komponen Aplikasi (AppComponents) dengan perkiraan waktu pemulihan beban kerja, dan waktu pemulihan target yang ditentukan dalam kebijakan ketahanan aplikasi Anda. Pilih nilai untuk melihatRTO/RPOestimasi dalam laporan penilaian aplikasi Anda.
     - Alarm diterapkan - Menunjukkan kontribusi aktual dari CloudWatch alarm Amazon yang diterapkan dibandingkan dengan kontribusi maksimum yang mungkin terhadap skor ketahanan aplikasi Anda. Pilih nilai untuk melihat CloudWatch alarm Amazon yang diterapkan dalam laporan penilaian aplikasi Anda.

- SOPsdiimplementasikan — Menunjukkan kontribusi aktual dari implementasi SOPs dibandingkan dengan kontribusi maksimum yang mungkin terhadap skor ketahanan aplikasi Anda. Pilih nilai untuk melihat implementasi SOPs dalam laporan penilaian aplikasi Anda.
- FISeksperimen dilaksanakan - Menunjukkan kontribusi aktual dari tes yang diterapkan dibandingkan dengan kontribusi maksimum yang mungkin terhadap skor ketahanan aplikasi Anda. Pilih nilai untuk melihat tes yang diterapkan dalam laporan penilaian aplikasi Anda.

- Untuk melihat pelanggaran kebijakan ketahanan dan rekomendasi operasional, pilih panah kanan untuk memperluas bagian pelanggaran Kebijakan dan rincian rekomendasi operasional. Saat diperluas, AWS Resilience Hub menampilkan yang berikut:
  - Pelanggaran kebijakan ketahanan - Menunjukkan jumlah Komponen Aplikasi yang melanggar kebijakan ketahanan aplikasi Anda. Pilih nilai di samping RTO/RPOuntuk melihat detail di tab Rekomendasi Ketahanan pada laporan penilaian aplikasi Anda.
  - Rekomendasi operasional — Menunjukkan rekomendasi operasional yang belum diterapkan atau dijalankan untuk meningkatkan ketahanan aplikasi Anda menggunakan tab Luar Biasa dan Dikecualikan. Rekomendasi operasional mencakup semua rekomendasi yang tidak aktif dan yang belum dilaksanakan.

    Untuk melihat rekomendasi operasional yang perlu diimplementasikan, pilih tab Luar Biasa. Saat dipilih, AWS Resilience Hub menampilkan yang berikut ini:
    - Alarm - Menunjukkan jumlah CloudWatch alarm Amazon yang direkomendasikan yang perlu diimplementasikan.
    - SOPs— Menunjukkan jumlah rekomendasi SOPs yang perlu diimplementasikan.
    - FIS— Menunjukkan jumlah tes yang direkomendasikan yang perlu diimplementasikan.

    Untuk melihat rekomendasi operasional yang dikecualikan dari aplikasi Anda, pilih tab Dikecualikan. Ketika dipilih AWS Resilience Hub menampilkan yang berikut:
    - Alarm - Menunjukkan jumlah CloudWatch alarm Amazon yang direkomendasikan yang dikecualikan dari aplikasi Anda.
    - SOPs— Menunjukkan jumlah rekomendasi SOPs yang dikecualikan dari aplikasi Anda.
    - FIS— Menunjukkan jumlah tes yang direkomendasikan yang dikecualikan dari aplikasi Anda.

Menghitung skor ketahanan

Tabel di bagian ini menjelaskan rumus yang digunakan AWS Resilience Hub untuk menentukan komponen penilaian dari setiap jenis rekomendasi dan skor ketahanan aplikasi Anda. Semua nilai yang dihasilkan ditentukan oleh AWS Resilience Hub untuk komponen penilaian dari setiap jenis rekomendasi dan skor ketahanan aplikasi Anda dibulatkan ke titik terdekat. Misalnya, jika dua dari tiga alarm diterapkan, skornya akan menjadi 13,33 ((2/3) * 20) poin. Nilai ini akan dibulatkan menjadi 13 poin. Untuk informasi lebih lanjut tentang bobot yang digunakan dalam rumus dalam tabel, lihat the section called “Bobot AppComponents dan jenis gangguan” bagian.

Beberapa komponen penilaian hanya dapat diperoleh melalui. `ScoringComponentResiliencyScore` API Untuk informasi lebih lanjut tentang iniAPI, lihat ScoringComponentResiliencyScore.

Tabel

Tabel berikut menjelaskan rumus yang digunakan oleh AWS Resilience Hub untuk menghitung komponen penilaian dari setiap jenis rekomendasi.

Rumus untuk menghitung komponen penilaian dari setiap jenis rekomendasi

Komponen penilaian	Deskripsi	Rumus .	Contoh
Cakupan uji (T)	Skor yang dinormalisasi (0 -100 poin) berdasarkan jumlah tes yang berhasil dilaksanakan dan dikecualikan, dari jumlah total tes yang AWS Resilience Hub direkomendasikan.	`T = ((Total number of tests implemented) + (Total number of tests excluded)) / (Total number of tests recommended)` Bagian dari rumus adalah sebagai berikut:	Jika Anda telah menerapkan 10 dan mengecualikan 5 tes dari 20 tes yang AWS Resilience Hub direkomendasikan, cakupan pengujian dihitung sebagai berikut:

Komponen penilaian	Deskripsi	Rumus .	Contoh
	Note Untuk menghitung skor ketahanan, tes yang direkomendasikan harus berjalan dengan sukses dalam 30 hari terakhir AWS Resilience Hub untuk mempertimbangkannya sebagai diterapkan.	• Jumlah total pengujian yang dikonfigurasi - Menunjukkan jumlah total pengujian yang dikonfigurasi saat AWS CloudFormation templat dibuat dan diunggah di AWS CloudFormation konsol. • Jumlah total tes yang direkomendasikan - Menunjukkan pengujian yang direkomendasikan AWS Resilience Hub berdasarkan sumber daya aplikasi. • Jumlah total tes yang dikecualikan - Menunjukkan jumlah tes yang direkomendasikan yang telah Anda kecualikan dari aplikasi.	`T = (10 + 5) / 20` Itu adalah, `T = .75 or 75 points`

Komponen penilaian	Deskripsi	Rumus .	Contoh
Cakupan alarm () `A`	Skor yang dinormalisasi (0 -100 poin) berdasarkan jumlah CloudWatch alarm Amazon yang berhasil diterapkan dan dikecualikan, dari jumlah total alarm AWS Resilience Hub Amazon yang direkomendasikan. CloudWatch **Note** Untuk menghitung skor ketahanan, alarm yang direkomendasikan harus dalam keadaan Siap untuk mempertimbangkannya sebagai AWS Resilience Hub diterapkan.	`A = ((Total number of alarms implemented) + (Total number of alarms excluded)) / (Total number of alarms recommended)` Bagian dari rumus adalah sebagai berikut: • Jumlah total alarm yang dikonfigurasi - Menunjukkan jumlah total CloudWatch alarm Amazon yang dikonfigurasi saat AWS CloudFormation template dibuat dan diunggah di konsol. AWS CloudFormation • Jumlah total alarm yang direkomendasikan - Menunjukkan CloudWatch alarm Amazon yang direkomendasikan AWS Resilience Hub berdasarkan sumber daya aplikasi. • Jumlah total alarm yang dikecualikan - Menunjukkan jumlah CloudWatch alarm Amazon yang direkomen	Jika Anda telah menerapkan 10 dan mengecualikan 5 CloudWatch alarm Amazon dari 20 CloudWatch alarm Amazon yang AWS Resilience Hub direkomendasikan, cakupan CloudWatch alarm Amazon dihitung sebagai berikut: `A = (10 + 5) / 20` Itu adalah, `A = .75 or 75 points`

Komponen penilaian	Deskripsi	Rumus .	Contoh
		dasikan yang telah Anda kecualikan dari aplikasi.	

Komponen penilaian	Deskripsi	Rumus .	Contoh
SOPcakupan (S)	Skor yang dinormalisasi (0 -100 poin) berdasark an jumlah SOPs yang berhasil diterapkan dan dikeluarkan, dari jumlah AWS Resilience Hub total yang direkomendasikan. SOPs	`S = ((Total number of SOPs implement ed) + (Total number of SOPs excluded) ) / (Total number of SOPs recommend ed)` Bagian dari rumus adalah sebagai berikut: • Jumlah total SOPs konfigurasi - Menunjukk an jumlah total yang SOPs dikonfigurasi saat AWS CloudForm ation templat dibuat dan diunggah di AWS CloudFormation konsol. • Jumlah total yang SOPs direkomen dasikan - Menunjukk an SOPs rekomenda si AWS Resilience Hub berdasarkan sumber daya aplikasi. • Jumlah total yang SOPs dikecualikan - Menunjukkan jumlah rekomendasi yang telah SOPs Anda kecualikan dari aplikasi.	Jika Anda telah menerapkan 10 dan mengecual ikan 5 SOPs dari 20 yang AWS Resilience Hub direkomendasik anSOPs, SOP cakupan dihitung sebagai berikut: `S = (10 + 5) / 20` Itu adalah, `S = .75 or 75 points`

Komponen penilaian	Deskripsi	Rumus .	Contoh

RTO/RPOkepatuhan (P)	Skor yang dinormalisasi (0 -100 poin) berdasarkan aplikasi yang memenuhi kebijakan ketahanannya.	`P = Total weights of disruption types meeting the application's resiliency policy / Total weights of all disruption types .`	Jika kebijakan ketahanan aplikasi Anda hanya memenuhi jenis gangguan Availability Zone (AZ) dan Infrastruktur, skor kebijakan ketahanan (P) dihitung sebagai berikut:
			• Jika Anda telah menetapkan Regional RTO dan RPO target, P dihitung sebagai berikut:
			`P = (20 + 30)/ 100`
			Itu adalah, `P = .5 or 50 points`
			• Jika Anda belum menetapkan Regional RTO dan RPO target, P dihitung sebagai berikut:
			`P = (22.22 + 33.33)/ 99.9`

Komponen penilaian	Deskripsi	Rumus .	Contoh
			Itu adalah, `P = .55 or 55 points`

Tabel berikut menjelaskan rumus yang digunakan AWS Resilience Hub untuk menghitung skor ketahanan untuk seluruh aplikasi Anda.

Rumus untuk menghitung skor Ketahanan

Komponen penilaian	Deskripsi	Rumus .	Contoh
Skor ketahanan untuk aplikasi () `RS`	Skor ketahanan yang dinormalisasi (0 -100 poin) berdasarkan aplikasi Anda yang memenuhi kebijakan ketahanan nya. Skor ketahanan per aplikasi adalah rata-rata tertimbang dari semua jenis rekomendasi. Itu adalah: `RS = Weighted Average (T, A, S, P)`	Skor ketahanan per aplikasi dihitung menggunakan rumus berikut: `RS = (T * Weight(T) + A * Weight(A) + S * Weight(S) + P * Weight(P)) / (Weight(T) + Weight(A) + Weight(S) + Weight(P))`	Rumus untuk menghitung cakupan setiap tabel jenis rekomendasi adalah sebagai berikut: • `Test coverage (T) = .75` • `Alarms (A) = .75` • `SOPs (S) = .75` • `Meeting resiliency policy (P) = .5`

Komponen penilaian	Deskripsi	Rumus .	Contoh
			Skor ketahanan per aplikasi dihitung sebagai berikut: `RS = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 * .4)) /(.2 + .2 + .2 + .4)` Itu adalah, `RS = .65 or 65 points`

Tabel berikut menjelaskan rumus yang digunakan oleh AWS Resilience Hub untuk menghitung skor ketahanan untuk Komponen Aplikasi (AppComponents) dan jenis gangguan. Namun, Anda dapat memperoleh skor ketahanan AppComponents dan jenis gangguan hanya melalui Hub Ketahanan berikut: AWS APIs

- DescribeAppAssessmentuntuk mendapatkan `RSo`
- ListAppComponentCompliancesuntuk mendapatkan `RSao` dan `RSA`

Rumus untuk menghitung skor ketahanan dan jenis gangguan AppComponents

Komponen penilaian	Deskripsi	Rumus .	Contoh
Skor ketahanan per AppCompon ent dan per jenis	Skor yang dinormalisasi (0 -100 poin) berdasarkan AppCompon	Skor ketahanan per AppCompon ent dan per jenis gangguan dihitung menggunakan rumus berikut:	`RSao`asumsi untuk semua jenis rekomendasi adalah sebagai berikut:

Komponen penilaian	Deskripsi	Rumus .	Contoh
gangguan () RSao	ent pertemuan kebijakan ketahanan per jenis gangguan. Skor ketahanan per AppCompon ent dan per jenis gangguan adalah rata-rata tertimbang dari semua jenis rekomendasi. Itu adalah: RSao = Weighted Average (T, A, S, P) Nilai untuk T, A, S, P dihitung untuk semua pengujian yang direkomen dasikan, alarmSOPs, dan kebijakan ketahanan pertemuan dari AppCompon	RSao = (T * Weight(T) + A * Weight(A) + S * Weight(S) + P * Weight(P)) / (Weight(T) + Weight(A) + Weight(S) + Weight(P))	• Test coverage (T) = .75 • Alarms (A) = .75 • SOPs (S) = .75 • Meeting resiliency policy (P) = .5 Skor ketahanan per AppComponent dan jenis gangguan dihitung sebagai berikut: RSao = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 * .4)) / (.2 + .2 + .2 + .4) Itu adalah, RSao = .65 or 65 points

Komponen penilaian	Deskripsi	Rumus .	Contoh
	ent dan jenis gangguan.		

Komponen penilaian	Deskripsi	Rumus .	Contoh

Skor ketahanan per AppComponent () `RSa`	Skor yang dinormalisasi (0 -100 poin) berdasarkan pemenuhan kebijakan ketahanan nya. Skor ketahanan per AppComponent adalah rata-rata tertimbang dari semua jenis rekomendasi. Itu adalah: `RSa = Weighted Average (T, A, S, P)`
	
	Nilai untuk `T, A, S, P` dihitung untuk semua pengujian yang direkomendasikan, alarmSOPs, dan kebijakan ketahanan pertemuan. AppComponent
		Skor ketahanan per AppComponent dihitung menggunakan rumus berikut:
		
		`RSa = (T * Weight(T) +`
		
		`A * Weight(A) +`
		
		`S * Weight(S) +`
		
		`P * Weight(P)) /`
		
		`(Weight(T) + Weight(A) + Weight(S) + Weight(P))`
			`RSa`asumsi untuk semua jenis rekomendasi adalah sebagai berikut:
			
			• `Test coverage (T) = .75`
			• `Alarms (A) = .75`
			• `SOPs (S) = .75`
			• `Meeting resiliency policy (P) = .5`
			
			Skor ketahanan per AppComponent dihitung sebagai berikut:
			
			`RSa = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 * .4)) / (.2 + .2 + .2 + .4)`
			
			Itu adalah, `RSa = .65 or 65 points`

Komponen penilaian	Deskripsi	Rumus .	Contoh

Skor ketahanan per jenis gangguan () `RSo`	Skor yang dinormalisasi (0 -100 poin) berdasarkan pemenuhan kebijakan ketahanan nya. Skor ketahanan per jenis gangguan adalah rata-rata tertimbang dari semua jenis rekomendasi. Itu adalah: `RSo = Weighted Average (T, A, S, P)`
	
	Nilai untuk `T, A, S, P` dihitung untuk semua pengujian yang direkomen dasikan, alarmSOPs, dan kebijakan ketahanan pertemuan dari jenis gangguan.
		Skor ketahanan per jenis gangguan dihitung menggunakan rumus berikut:
		
		`RSo = (T * Weight(T) + A * Weight(A) +`
		
		`S * Weight(S) + P * Weight(P)) /`
		
		`(Weight(T) + Weight(A) + Weight(S) + Weight(P))`
			`RSo`asumsi untuk semua jenis rekomendasi adalah sebagai berikut:
			
			• `Test coverage (T) = .75`
			• `Alarms (A) = .75`
			• `SOPs (S) = .75`
			• `Meeting resiliency policy (P) = .5`
			
			Skor ketahanan per jenis gangguan dihitung sebagai berikut:
			
			`RSo = ((.75 * .2) + (.75 * .2) + (.75 * .2) + (.5 *.4)) /`
			
			`(.2 + .2 + .2 + .4)`
			
			Itu adalah, `RSo = .65 or 65 points`

Bobot

AWS Resilience Hub memberikan bobot untuk setiap jenis rekomendasi untuk skor ketahanan total.

Tabel berikut menunjukkan bobot untuk alarm, pengujianSOPs, kebijakan ketahanan rapat, dan jenis gangguan. Jenis gangguan termasuk Aplikasi, Infrastruktur, AZ, dan Wilayah.

> **Note**
>
> Jika Anda memilih untuk tidak menentukan Regional RTO atau RPO target untuk kebijakan Anda, bobot untuk jenis gangguan lainnya akan ditingkatkan sesuai seperti yang ditunjukkan pada kolom Berat saat Wilayah tidak ditentukan.

Bobot untuk alarm,, pengujianSOPs, target kebijakan

Jenis rekomendasi	Berat Badan
Alarm	20 poin
SOPs	20 poin
Tes	20 poin
Memenuhi kebijakan ketahanan	40 poin

Bobot untuk tipe gangguan

Jenis gangguan	Berat ketika Wilayah didefinisikan	Berat ketika Wilayah tidak ditentukan
Aplikasi	40 poin	44,44 poin
Infrastruktur	30 poin	33,33 poin
Zona Ketersediaan	20 poin	22,22 poin
Wilayah	10 poin	N/A

Mengintegrasikan rekomendasi operasional ke dalam aplikasi Anda dengan AWS CloudFormation

Setelah Anda memilih Buat CloudFormation templat di halaman Rekomendasi operasional, AWS Resilience Hub buat AWS CloudFormation templat yang menjelaskan alarm tertentu, prosedur operasi standar (SOP), atau AWS FIS eksperimen untuk aplikasi Anda. AWS CloudFormation Template disimpan dalam bucket Amazon S3, dan Anda dapat memeriksa jalur S3 ke templat di tab Detail templat di halaman Rekomendasi operasional.

Misalnya, daftar di bawah ini menunjukkan AWS CloudFormation templat JSON berformat -yang menjelaskan rekomendasi alarm yang diberikan oleh. AWS Resilience Hub Ini adalah Read Throttling Alarm untuk tabel DynamoDB yang disebut. `Employees`

`Resources`Bagian template menjelaskan `AWS::CloudWatch::Alarm` alarm yang diaktifkan ketika jumlah peristiwa throttle baca untuk tabel DynamoDB melebihi 1. Dan dua `AWS::SSM::Parameter` sumber daya menentukan metadata yang memungkinkan AWS Resilience Hub untuk mengidentifikasi sumber daya yang diinstal tanpa harus memindai aplikasi yang sebenarnya.

```
{
  "AWSTemplateFormatVersion" : "2010-09-09",
  "Parameters" : {
    "SNSTopicARN" : {
      "Type" : "String",
      "Description" : "The ARN of the Amazon SNS topic to which alarm status changes
 are to be sent. This must be in the same Region being deployed.",
      "AllowedPattern" : "^arn:(aws|aws-cn|aws-iso|aws-iso-[a-z]{1}|aws-us-gov):sns:
([a-z]{2}-((iso[a-z]{0,1}-)|(gov-)){0,1}[a-z]+-[0-9]):[0-9]{12}:[A-Za-z0-9/][A-Za-
z0-9:_/+=,@.-]{1,256}$"
    }
  },
  "Resources" : {

 "ReadthrottleeventsthresholdexceededEmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm" :
 {
      "Type" : "AWS::CloudWatch::Alarm",
      "Properties" : {
        "AlarmDescription" : "An Alarm by AWS Resilience Hub that alerts when the
 number of read-throttle events are greater than 1.",
        "AlarmName" : "ResilienceHub-ReadThrottleEventsAlarm-2020-04-01_Employees-ON-
DEMAND-0-DynamoDBTable-PXBZQYH3DCJ9",
        "AlarmActions" : [ {
```

```
          "Ref" : "SNSTopicARN"
        } ],
        "MetricName" : "ReadThrottleEvents",
        "Namespace" : "AWS/DynamoDB",
        "Statistic" : "Sum",
        "Dimensions" : [ {
          "Name" : "TableName",
          "Value" : "Employees-ON-DEMAND-0-DynamoDBTable-PXBZQYH3DCJ9"
        } ],
        "Period" : 60,
        "EvaluationPeriods" : 1,
        "DatapointsToAlarm" : 1,
        "Threshold" : 1,
        "ComparisonOperator" : "GreaterThanOrEqualToThreshold",
        "TreatMissingData" : "notBreaching",
        "Unit" : "Count"
      },
      "Metadata" : {
        "AWS::ResilienceHub::Monitoring" : {
          "recommendationId" : "dynamodb:alarm:health-read_throttle_events:2020-04-01"
        }
      }
    },

 "dynamodbalarmhealthreadthrottleevents20200401EmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm
 {
      "Type" : "AWS::SSM::Parameter",
      "Properties" : {
        "Name" : "/ResilienceHub/Alarm/3f904525-4bfa-430f-96ef-58ec9b19aa73/dynamodb-
alarm-health-read-throttle-events-2020-04-01_Employees-ON-DEMAND-0-DynamoDBTable-
PXBZQYH3DCJ9",
        "Type" : "String",
        "Value" : {
          "Fn::Sub" :
 "${ReadthrottleeventsthresholdexceededEmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm}"
        },
        "Description" : "SSM Parameter for identifying installed resources."
      }
    },

 "dynamodbalarmhealthreadthrottleevents20200401EmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm
 {
      "Type" : "AWS::SSM::Parameter",
      "Properties" : {
```

```
        "Name" : "/ResilienceHub/Info/Alarm/3f904525-4bfa-430f-96ef-58ec9b19aa73/
dynamodb-alarm-health-read-throttle-events-2020-04-01_Employees-ON-DEMAND-0-
DynamoDBTable-PXBZQYH3DCJ9",
        "Type" : "String",
        "Value" : {
          "Fn::Sub" : "{\"alarmName\":
\"${ReadthrottleeventsthresholdexceededEmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm}\",
\"referenceId\":\"dynamodb:alarm:health_read_throttle_events:2020-04-01\",
\"resourceId\":\"Employees-ON-DEMAND-0-DynamoDBTable-PXBZQYH3DCJ9\",\"relatedSOPs\":
[\"dynamodb:sop:update_provisioned_capacity:2020-04-01\"]}"
        },
        "Description" : "SSM Parameter for identifying installed resources."
      }
    }
  }
}
```

Memodifikasi template AWS CloudFormation

Cara termudah untuk mengintegrasikan alarm,SOP, atau AWS FIS sumber daya ke dalam aplikasi utama Anda adalah dengan menambahkannya sebagai sumber daya lain dalam template yang menjelaskan template aplikasi Anda. File JSON -format yang disediakan di bawah ini memberikan garis besar dasar tentang bagaimana tabel DynamoDB dijelaskan dalam template. AWS CloudFormation Aplikasi nyata cenderung menyertakan beberapa sumber daya lagi, seperti tabel tambahan.

```
{
   "AWSTemplateFormatVersion": "2010-09-09T00:00:00.000Z",
   "Description": "Application Stack with Employees Table",
   "Outputs": {
      "DynamoDBTable": {
         "Description": "The DynamoDB Table Name",
         "Value": {"Ref": "Employees"}
      }
   },
   "Resources": {
      "Employees": {
         "Type": "AWS::DynamoDB::Table",
         "Properties": {
            "BillingMode": "PAY_PER_REQUEST",
            "AttributeDefinitions": [
               {
```

```
                "AttributeName": "USER_ID",
                "AttributeType": "S"
            },
            {
                "AttributeName": "RANGE_ATTRIBUTE",
                "AttributeType": "S"
            }
        ],
        "KeySchema": [
            {
                "AttributeName": "USER_ID",
                "KeyType": "HASH"
            },
            {
                "AttributeName": "RANGE_ATTRIBUTE",
                "KeyType": "RANGE"
            }
        ],
        "PointInTimeRecoverySpecification": {
            "PointInTimeRecoveryEnabled": true
        },
        "Tags": [
            {
                "Key": "Key",
                "Value": "Value"
            }
        ],
        "LocalSecondaryIndexes": [
            {
                "IndexName": "resiliencehub-index-local-1",
                "KeySchema": [
                    {
                        "AttributeName": "USER_ID",
                        "KeyType": "HASH"
                    },
                    {
                        "AttributeName": "RANGE_ATTRIBUTE",
                        "KeyType": "RANGE"
                    }
                ],
                "Projection": {
                    "ProjectionType": "ALL"
                }
            }
```

```
            ],
            "GlobalSecondaryIndexes": [
               {
                  "IndexName": "resiliencehub-index-1",
                  "KeySchema": [
                     {
                        "AttributeName": "USER_ID",
                        "KeyType": "HASH"
                     }
                  ],
                  "Projection": {
                     "ProjectionType": "ALL"
                  }
               }
            ]
         }
      }
   }
}
```

Untuk memungkinkan sumber daya alarm disebarkan dengan aplikasi Anda, Anda sekarang perlu mengganti sumber daya hardcode dengan referensi dinamis di tumpukan aplikasi.

Jadi, dalam definisi `AWS::CloudWatch::Alarm` sumber daya, ubah yang berikut ini:

```
"Value" : "Employees-ON-DEMAND-0-DynamoDBTable-PXBZQYH3DCJ9"
```

ke bawah ini:

```
"Value" : {"Ref": "Employees"}
```

Dan di bawah definisi `AWS::SSM::Parameter` sumber daya, ubah yang berikut ini:

```
"Fn::Sub" : "{\"alarmName\":
\"${ReadthrottleeventsthresholdexceededDynamoDBEmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm
\"referenceId\":\"dynamodb:alarm:health_read_throttle_events:2020-04-01\",
\"resourceId\":\"Employees-ON-DEMAND-0-DynamoDBTable-PXBZQYH3DCJ9\",\"relatedSOPs\":
[\"dynamodb:sop:update_provisioned_capacity:2020-04-01\"]}"
```

ke bawah ini:

```
"Fn::Sub" : "{\"alarmName\":
\"${ReadthrottleeventsthresholdexceededEmployeesONDEMAND0DynamoDBTablePXBZQYH3DCJ9Alarm}\",
\"referenceId\":\"dynamodb:alarm:health_read_throttle_events:2020-04-01\",\"resourceId
\":\"${Employees}\",\"relatedSOPs\":
[\"dynamodb:sop:update_provisioned_capacity:2020-04-01\"]}"
```

Saat memodifikasi AWS CloudFormation template untuk SOPs dan AWS FIS eksperimen, Anda akan mengambil pendekatan yang sama, mengganti referensi hardcode IDs dengan referensi dinamis yang terus berfungsi bahkan setelah perubahan perangkat keras.

Dengan menggunakan referensi ke tabel DynamoDB, Anda AWS CloudFormation mengizinkan untuk melakukan hal berikut:

- Buat tabel database terlebih dahulu.
- Selalu gunakan ID aktual dari sumber daya yang dihasilkan di alarm, dan perbarui alarm secara dinamis jika AWS CloudFormation perlu mengganti sumber daya.

> **Note**
>
> Anda dapat memilih metode yang lebih canggih untuk mengelola sumber daya aplikasi Anda AWS CloudFormation seperti tumpukan bersarang atau merujuk ke output sumber daya dalam tumpukan terpisah. AWS CloudFormation (Tetapi jika Anda ingin memisahkan tumpukan rekomendasi dari tumpukan utama, Anda perlu mengonfigurasi cara untuk meneruskan informasi di antara dua tumpukan.)
> Selain itu, alat pihak ketiga, seperti Terraform by HashiCorp, juga dapat digunakan untuk menyediakan Infrastructure as Code (IAc).

Menggunakan AWS Resilience Hub APIs untuk mendeskripsikan dan mengelola aplikasi

Sebagai alternatif untuk mendeskripsikan dan mengelola aplikasi menggunakan AWS Resilience Hub konsol, AWS Resilience Hub memungkinkan Anda untuk mendeskripsikan dan mengelola aplikasi menggunakan AWS Resilience Hub APIs. Bab ini menjelaskan cara membuat aplikasi menggunakan AWS Resilience Hub APIs. Ini juga mendefinisikan urutan di mana Anda perlu mengeksekusi APIs dan nilai parameter yang harus Anda berikan dengan contoh yang sesuai. Untuk informasi selengkapnya, lihat topik berikut.

- the section called “Mempersiapkan aplikasi”
- the section called “Menjalankan dan menganalisis aplikasi”
- the section called “Ubah aplikasi Anda”

Langkah 1: Mempersiapkan aplikasi

Untuk menyiapkan aplikasi, Anda harus terlebih dahulu membuat aplikasi, menetapkan kebijakan ketahanan, dan kemudian mengimpor sumber daya aplikasi dari sumber input Anda. Untuk informasi lebih lanjut tentang AWS Resilience Hub APIs yang digunakan untuk menyiapkan aplikasi, lihat topik berikut:

- the section called “Membuat aplikasi”
- the section called “Buat kebijakan ketahanan”
- the section called “Impor sumber daya aplikasi dan pantau status impor”
- the section called “Publikasikan aplikasi Anda dan tetapkan kebijakan ketahanan”

Membuat aplikasi

Untuk membuat aplikasi baru AWS Resilience Hub, Anda harus memanggil `CreateApp` API dan memberikan nama aplikasi yang unik. Untuk informasi lebih lanjut tentang iniAPI, lihathttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateApp.html.

Contoh berikut menunjukkan cara membuat aplikasi baru `newApp` dalam AWS Resilience Hub menggunakan `CreateApp`API.

Permintaan

```
aws resiliencehub create-app --name newApp
```

Respons

```
{
    "app": {
        "appArn": "<App_ARN>",
        "name": "newApp",
        "creationTime": "2022-10-26T19:48:00.434000+03:00",
        "status": "Active",
        "complianceStatus": "NotAssessed",
        "resiliencyScore": 0.0,
        "tags": {},
        "assessmentSchedule": "Disabled"
    }
}
```

Menciptakan kebijakan ketahanan

Setelah membuat aplikasi, Anda harus membuat kebijakan ketahanan yang memungkinkan Anda memahami postur ketahanan aplikasi Anda menggunakan. `CreateResiliencyPolicy` API Untuk informasi lebih lanjut tentang iniAPI, lihathttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateResiliencyPolicy.html.

Contoh berikut menunjukkan cara membuat `newPolicy` untuk aplikasi Anda dalam AWS Resilience Hub menggunakan `CreateResiliencyPolicy`API.

Permintaan

```
aws resiliencehub create-resiliency-policy \
--policy-name newPolicy --tier NonCritical \
--policy '{"AZ": {"rtoInSecs": 172800,"rpoInSecs": 86400}, \
"Hardware": {"rtoInSecs": 172800,"rpoInSecs": 86400}, \
"Software": {"rtoInSecs": 172800,"rpoInSecs": 86400}}'
```

Respons

```
{
    "policy": {
```

```
        "policyArn": "<Policy_ARN>",
        "policyName": "newPolicy",
        "policyDescription": "",
        "dataLocationConstraint": "AnyLocation",
        "tier": "NonCritical",
        "estimatedCostTier": "L1",
        "policy": {
            "AZ": {
                "rtoInSecs": 172800,
                "rpoInSecs": 86400
            },
            "Hardware": {
                "rtoInSecs": 172800,
                "rpoInSecs": 86400
            },
            "Software": {
                "rtoInSecs": 172800,
                "rpoInSecs": 86400
            }
        },
        "creationTime": "2022-10-26T20:48:05.946000+03:00",
        "tags": {}
    }
}
```

Mengimpor sumber daya dari sumber input dan memantau status impor

AWS Resilience Hub menyediakan hal-hal berikut APIs untuk mengimpor sumber daya ke aplikasi Anda:

- `ImportResourcesToDraftAppVersion`— Ini API memungkinkan Anda untuk mengimpor sumber daya ke versi draf aplikasi Anda dari sumber input yang berbeda. Untuk informasi lebih lanjut tentang iniAPI, lihathttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_ImportResourcesToDraftAppVersion.html.
- `PublishAppVersion`— Ini API menerbitkan versi baru aplikasi bersama dengan yang diperbarui AppComponents. Untuk informasi lebih lanjut tentang iniAPI, lihathttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_PublishAppVersion.html.
- `DescribeDraftAppVersionResourcesImportStatus`— Ini API memungkinkan Anda untuk memantau status impor sumber daya Anda ke versi aplikasi. Untuk informasi lebih lanjut tentang iniAPI, lihathttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeDraftAppVersionResourcesImportStatus.html.

Contoh berikut menunjukkan cara mengimpor sumber daya ke aplikasi Anda saat AWS Resilience Hub menggunakan `ImportResourcesToDraftAppVersion`API.

Permintaan

```
aws resiliencehub import-resources-to-draft-app-version \
--app-arn <App_ARN> \
--terraform-sources '[{"s3StateFileUrl": <S3_URI>}]'
```

Respons

```
{
    "appArn": "<App_ARN>",
    "appVersion": "draft",
    "sourceArns": [],
    "status": "Pending",
    "terraformSources": [
        {
            "s3StateFileUrl": <S3_URI>
        }
    ]
}
```

Contoh berikut menunjukkan cara menambahkan sumber daya secara manual ke aplikasi Anda dalam AWS Resilience Hub menggunakan `CreateAppVersionResource`API.

Permintaan

```
aws resiliencehub create-app-version-resource \
--app-arn <App_ARN> \
--resource-name "backup-efs" \
--logical-resource-id '{"identifier": "backup-efs"}' \
--physical-resource-id '<Physical_resource_id_ARN>' \
--resource-type AWS::EFS::FileSystem \
--app-components '["new-app-component"]'
```

Respons

```
{
    "appArn": "<App_ARN>",
    "appVersion": "draft",
```

```
    "physicalResource": {
        "resourceName": "backup-efs",
        "logicalResourceId": {
            "identifier": "backup-efs"
        },
        "physicalResourceId": {
            "identifier": "<Physical_resource_id_ARN>",
            "type": "Arn"
        },
        "resourceType": "AWS::EFS::FileSystem",
        "appComponents": [
            {
                "name": "new-app-component",
                "type": "AWS::ResilienceHub::StorageAppComponent",
                "id": "new-app-component"
            }
        ]
    }
}
```

Contoh berikut menunjukkan cara memantau status impor sumber daya Anda dalam AWS Resilience Hub menggunakan `DescribeDraftAppVersionResourcesImportStatus`API.

Permintaan

```
aws resiliencehub describe-draft-app-version-resources-import-status \
--app-arn <App_ARN>
```

Respons

```
{
    "appArn": "<App_ARN>",
    "appVersion": "draft",
    "status": "Success",
    "statusChangeTime": "2022-10-26T19:55:18.471000+03:00"
}
```

Menerbitkan versi draf aplikasi Anda dan menetapkan kebijakan ketahanan

Sebelum menjalankan penilaian, Anda harus terlebih dahulu mempublikasikan versi draf aplikasi Anda dan menetapkan kebijakan ketahanan ke versi rilis aplikasi Anda.

Untuk mempublikasikan versi draf aplikasi Anda dan menetapkan kebijakan ketahanan

1. Untuk mempublikasikan versi draf aplikasi Anda, gunakan `PublishAppVersion`API. Untuk informasi lebih lanjut tentang iniAPI, lihathttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_PublishAppVersion.html.

   Contoh berikut menunjukkan cara mempublikasikan versi draf aplikasi yang sedang AWS Resilience Hub digunakan `PublishAppVersion`API.

   Permintaan

   ```
   aws resiliencehub publish-app-version \
    --app-arn <App_ARN>
   ```

   Respons

   ```
   {
       "appArn": "<App_ARN>",
       "appVersion": "release"
   }
   ```

2. Terapkan kebijakan ketahanan ke versi rilis aplikasi Anda yang digunakan. `UpdateApp` API Untuk informasi lebih lanjut tentang iniAPI, lihathttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_UpdateApp.html.

   Contoh berikut menunjukkan cara menerapkan kebijakan ketahanan ke versi rilis aplikasi yang digunakan. AWS Resilience Hub `UpdateApp` API

   Permintaan

   ```
   aws resiliencehub update-app \
   --app-arn <App_ARN> \
   --policy-arn <Policy_ARN>
   ```

   Respons

```
{
    "app": {
        "appArn": "<App_ARN>",
        "name": "newApp",
        "policyArn": "<Policy_ARN>",
        "creationTime": "2022-10-26T19:48:00.434000+03:00",
        "status": "Active",
        "complianceStatus": "NotAssessed",
        "resiliencyScore": 0.0,
        "tags": {
            "resourceArn": "<App_ARN>"
        },
        "assessmentSchedule": "Disabled"
    }
}
```

Langkah 2: Menjalankan dan mengelola AWS Resilience Hub penilaian ketahanan

Setelah Anda mempublikasikan versi baru aplikasi Anda, Anda harus menjalankan penilaian ketahanan baru dan menganalisis hasilnya untuk memastikan bahwa aplikasi Anda memenuhi perkiraan beban kerja RTO dan perkiraan RPO yang ditentukan dalam kebijakan ketahanan Anda. Penilaian membandingkan setiap konfigurasi Komponen Aplikasi dengan kebijakan dan membuat alarm,SOP, dan rekomendasi pengujian.

Untuk informasi selengkapnya, lihat topik berikut.

- the section called “Jalankan dan pantau penilaian ketahanan”
- the section called “Buat kebijakan ketahanan”

Menjalankan dan memantau AWS Resilience Hub penilaian ketahanan

Untuk menjalankan penilaian ketahanan AWS Resilience Hub dan memantau statusnya, Anda harus menggunakan yang berikut ini: APIs

- `StartAppAssessment`— Ini API menciptakan penilaian baru untuk aplikasi. Untuk informasi lebih lanjut tentang iniAPI, lihathttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_StartAppAssessment.html.
- `DescribeAppAssessment`— Ini API menjelaskan penilaian untuk aplikasi dan memberikan status penyelesaian penilaian. Untuk informasi lebih lanjut tentang iniAPI, lihathttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeAppAssessment.html.

Contoh berikut menunjukkan cara memulai menjalankan penilaian baru dalam AWS Resilience Hub menggunakan `StartAppAssessment`API.

Permintaan

```
aws resiliencehub start-app-assessment \
--app-arn <App_ARN> \
--app-version release \
--assessment-name first-assessment
```

Respons

```
{
    "assessment": {
        "appArn": "<App_ARN>",
        "appVersion": "release",
        "invoker": "User",
        "assessmentStatus": "Pending",
        "startTime": "2022-10-27T08:15:10.452000+03:00",
        "assessmentName": "first-assessment",
        "assessmentArn": "<Assessment_ARN>",
        "policy": {
            "policyArn": "<Policy_ARN>",
            "policyName": "newPolicy",
            "dataLocationConstraint": "AnyLocation",
            "policy": {
                "AZ": {
                    "rtoInSecs": 172800,
                    "rpoInSecs": 86400
                },
                "Hardware": {
                    "rtoInSecs": 172800,
                    "rpoInSecs": 86400
                },
```

```
                "Software": {
                    "rtoInSecs": 172800,
                    "rpoInSecs": 86400
                }
            }
        },
        "tags": {}
    }
}
```

Contoh berikut menunjukkan cara memantau status penilaian Anda dalam AWS Resilience Hub menggunakan `DescribeAppAssessment`API. Anda dapat mengekstrak status penilaian Anda dari `assessmentStatus` variabel.

Permintaan

```
aws resiliencehub describe-app-assessment \
--assessment-arn <Assessment_ARN>
```

Respons

```
{
    "assessment": {
        "appArn": "<App_ARN>",
        "appVersion": "release",
        "cost": {
            "amount": 0.0,
            "currency": "USD",
            "frequency": "Monthly"
        },
        "resiliencyScore": {
            "score": 0.27,
            "disruptionScore": {
                "AZ": 0.42,
                "Hardware": 0.0,
                "Region": 0.0,
                "Software": 0.38
            }
        },
        "compliance": {
            "AZ": {
                "achievableRtoInSecs": 0,
```

```
                "currentRtoInSecs": 4500,
                "currentRpoInSecs": 86400,
                "complianceStatus": "PolicyMet",
                "achievableRpoInSecs": 0
            },
            "Hardware": {
                "achievableRtoInSecs": 0,
                "currentRtoInSecs": 2595601,
                "currentRpoInSecs": 2592001,
                "complianceStatus": "PolicyBreached",
                "achievableRpoInSecs": 0
            },
            "Software": {
                "achievableRtoInSecs": 0,
                "currentRtoInSecs": 4500,
                "currentRpoInSecs": 86400,
                "complianceStatus": "PolicyMet",
                "achievableRpoInSecs": 0
            }
        },
        "complianceStatus": "PolicyBreached",
        "assessmentStatus": "Success",
        "startTime": "2022-10-27T08:15:10.452000+03:00",
        "endTime": "2022-10-27T08:15:31.883000+03:00",
        "assessmentName": "first-assessment",
        "assessmentArn": "<Assessment_ARN>",
        "policy": {
            "policyArn": "<Policy_ARN>",
            "policyName": "newPolicy",
            "dataLocationConstraint": "AnyLocation",
            "policy": {
                "AZ": {
                    "rtoInSecs": 172800,
                    "rpoInSecs": 86400
                },
                "Hardware": {
                    "rtoInSecs": 172800,
                    "rpoInSecs": 86400
                },
                "Software": {
                    "rtoInSecs": 172800,
                    "rpoInSecs": 86400
                }
            }
```

```
        },
        "tags": {}
    }
}
```

Memeriksa hasil penilaian

Setelah penilaian Anda selesai dengan sukses, Anda dapat memeriksa hasil penilaian menggunakan yang berikut iniAPIs.

- `DescribeAppAssessment`— Ini API memungkinkan Anda untuk melacak status aplikasi Anda saat ini terhadap kebijakan ketahanan. Selain itu, Anda juga dapat mengekstrak status kepatuhan dari `complianceStatus` variabel, dan skor ketahanan untuk setiap jenis gangguan dari struktur. `resiliencyScore` Untuk informasi lebih lanjut tentang iniAPI, lihathttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_DescribeAppAssessment.html.
- `ListAlarmRecommendations`— Ini API memungkinkan Anda untuk mendapatkan rekomendasi alarm menggunakan Amazon Resource Name (ARN) penilaian. Untuk informasi lebih lanjut tentang iniAPI, lihathttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_ListAlarmRecommendations.html.

> **Note**
>
> Untuk mendapatkan SOP dan FIS menguji rekomendasi, gunakan `ListSopRecommendations` dan `ListTestRecommendations`APIs.

Contoh berikut menunjukkan cara mendapatkan rekomendasi alarm menggunakan Amazon Resource Name (ARN) dari penilaian menggunakan `ListAlarmRecommendations`API.

> **Note**
>
> Untuk mendapatkan rekomendasi SOP dan FIS tes, ganti dengan salah satu `ListSopRecommendations` atau`ListTestRecommendations`.

Permintaan

```
aws resiliencehub list-alarm-recommendations \
```

```
--assessment-arn <Assessment_ARN>
```

Respons


```
{
    "alarmRecommendations": [
        {
            "recommendationId": "78ece7f8-c776-499e-baa8-b35f5e8b8ba2",
            "referenceId": "app_common:alarm:synthetic_canary:2021-04-01",
            "name": "AWSResilienceHub-SyntheticCanaryInRegionAlarm_2021-04-01",
            "description": "A monitor for the entire application, configured to
 constantly verify that the application API/endpoints are available",
            "type": "Metric",
            "appComponentName": "appcommon",
            "items": [
                {
                    "resourceId": "us-west-2",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ],
            "prerequisite": "Make sure Amazon CloudWatch Synthetics is setup to monitor
 the application (see the <a href=\"https://docs.aws.amazon.com/AmazonCloudWatch/
latest/monitoring/CloudWatch_Synthetics_Canaries.html\" target=\"_blank\">docs</a>).
 \nMake sure that the Synthetics Name passed in the alarm dimension matches the name of
 the Synthetic Canary. It Defaults to the name of the application.\n"
        },
        {
            "recommendationId": "d9c72c58-8c00-43f0-ad5d-0c6e5332b84b",
            "referenceId": "efs:alarm:percent_io_limit:2020-04-01",
            "name": "AWSResilienceHub-EFSHighIoAlarm_2020-04-01",
            "description": "An alarm by AWS Resilience Hub that reports when Amazon EFS
 I/O load is more than 90% for too much time",
            "type": "Metric",
            "appComponentName": "storageappcomponent-rlb",
            "items": [
                {
                    "resourceId": "fs-0487f945c02f17b3e",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
```

```
            ]
        },
        {
            "recommendationId": "09f340cd-3427-4f66-8923-7f289d4a3216",
            "referenceId": "efs:alarm:mount_failure:2020-04-01",
            "name": "AWSResilienceHub-EFSMountFailureAlarm_2020-04-01",
            "description": "An alarm by AWS Resilience Hub that reports when volume
 failed to mount to EC2 instance",
            "type": "Metric",
            "appComponentName": "storageappcomponent-rlb",
            "items": [
                {
                    "resourceId": "fs-0487f945c02f17b3e",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ],
            "prerequisite": "* Make sure Amazon EFS utils are installed(see the <a
 href=\"https://github.com/aws/efs-utils#installation\" target=\"_blank\">docs</a>).
\n* Make sure cloudwatch logs are enabled in efs-utils (see the <a href=\"https://
github.com/aws/efs-utils#step-2-enable-cloudwatch-log-feature-in-efs-utils-config-
file-etcamazonefsefs-utilsconf\" target=\"_blank\">docs</a>).\n* Make sure that
 you've configured `log_group_name` in `/etc/amazon/efs/efs-utils.conf`, for example:
 `log_group_name = /aws/efs/utils`.\n* Use the created `log_group_name` in the
 generated alarm. Find `LogGroupName: REPLACE_ME` in the alarm and make sure the
 `log_group_name` is used instead of REPLACE_ME.\n"
        },
        {
            "recommendationId": "b0f57d2a-1220-4f40-a585-6dab1e79cee2",
            "referenceId": "efs:alarm:client_connections:2020-04-01",
            "name": "AWSResilienceHub-EFSHighClientConnectionsAlarm_2020-04-01",
            "description": "An alarm by AWS Resilience Hub that reports when client
 connection number deviation is over the specified threshold",
            "type": "Metric",
            "appComponentName": "storageappcomponent-rlb",
            "items": [
                {
                    "resourceId": "fs-0487f945c02f17b3e",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
```

```
        },
        {
            "recommendationId": "15f49b10-9bac-4494-b376-705f8da252d7",
            "referenceId": "rds:alarm:health-storage:2020-04-01",
            "name": "AWSResilienceHub-RDSInstanceLowStorageAlarm_2020-04-01",
            "description": "Reports when database free storage is low",
            "type": "Metric",
            "appComponentName": "databaseappcomponent-hji",
            "items": [
                {
                    "resourceId": "terraform-20220623141426115800000001",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "c1906101-cea8-4f77-be7b-60abb07621f5",
            "referenceId": "rds:alarm:health-connections:2020-04-01",
            "name": "AWSResilienceHub-RDSInstanceConnectionSpikeAlarm_2020-04-01",
            "description": "Reports when database connection count is anomalous",
            "type": "Metric",
            "appComponentName": "databaseappcomponent-hji",
            "items": [
                {
                    "resourceId": "terraform-20220623141426115800000001",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "f169b8d4-45c1-4238-95d1-ecdd8d5153fe",
            "referenceId": "rds:alarm:health-cpu:2020-04-01",
            "name": "AWSResilienceHub-RDSInstanceOverUtilizedCpuAlarm_2020-04-01",
            "description": "Reports when database used CPU is high",
            "type": "Metric",
            "appComponentName": "databaseappcomponent-hji",
            "items": [
                {
                    "resourceId": "terraform-20220623141426115800000001",
                    "targetAccountId": "12345678901",
```

```
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "69da8459-cbe4-4ba1-a476-80c7ebf096f0",
            "referenceId": "rds:alarm:health-memory:2020-04-01",
            "name": "AWSResilienceHub-RDSInstanceLowMemoryAlarm_2020-04-01",
            "description": "Reports when database free memory is low",
            "type": "Metric",
            "appComponentName": "databaseappcomponent-hji",
            "items": [
                {
                    "resourceId": "terraform-20220623141426115800000001",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "67e7902a-f658-439e-916b-251a57b97c8a",
            "referenceId": "ecs:alarm:health-service_cpu_utilization:2020-04-01",
            "name": "AWSResilienceHub-ECSServiceHighCpuUtilizationAlarm_2020-04-01",
            "description": "An alarm by AWS Resilience Hub that triggers when CPU
utilization of ECS tasks of Service exceeds the threshold",
            "type": "Metric",
            "appComponentName": "computeappcomponent-nrz",
            "items": [
                {
                    "resourceId": "aws_ecs_service_terraform-us-east-1-demo",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "fb30cb91-1f09-4abd-bd2e-9e8ee8550eb0",
            "referenceId": "ecs:alarm:health-service_memory_utilization:2020-04-01",
            "name": "AWSResilienceHub-ECSServiceHighMemoryUtilizationAlarm_2020-04-01",
```

```
            "description": "An alarm by AWS Resilience Hub for Amazon ECS that
 indicates if the percentage of memory that is used in the service, is exceeding
 specified threshold limit",
            "type": "Metric",
            "appComponentName": "computeappcomponent-nrz",
            "items": [
                {
                    "resourceId": "aws_ecs_service_terraform-us-east-1-demo",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ]
        },
        {
            "recommendationId": "1bd45a8e-dd58-4a8e-a628-bdbee234efed",
            "referenceId": "ecs:alarm:health-service_sample_count:2020-04-01",
            "name": "AWSResilienceHub-ECSServiceSampleCountAlarm_2020-04-01",
            "description": "An alarm by AWS Resilience Hub for Amazon ECS that triggers
 if the count of tasks isn't equal Service Desired Count",
            "type": "Metric",
            "appComponentName": "computeappcomponent-nrz",
            "items": [
                {
                    "resourceId": "aws_ecs_service_terraform-us-east-1-demo",
                    "targetAccountId": "12345678901",
                    "targetRegion": "us-west-2",
                    "alreadyImplemented": false
                }
            ],
            "prerequisite": "Make sure the Container Insights on Amazon ECS is enabled:
 (see the <a href=\"https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/
deploy-container-insights-ECS-cluster.html\" target=\"_blank\">docs</a>)."
        }
    ]
}
```

Contoh berikut menunjukkan cara mendapatkan rekomendasi konfigurasi (rekomendasi tentang cara meningkatkan ketahanan Anda saat ini) menggunakan. `ListAppComponentRecommendations` API

Permintaan

```
aws resiliencehub list-app-component-recommendations \
--assessment-arn <Assessment_ARN>
```

Respons

```
{
    "componentRecommendations": [
        {
            "appComponentName": "computeappcomponent-nrz",
            "recommendationStatus": "MetCanImprove",
            "configRecommendations": [
                {
                    "cost": {
                        "amount": 0.0,
                        "currency": "USD",
                        "frequency": "Monthly"
                },
                    "appComponentName": "computeappcomponent-nrz",
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": " Estimated time to restore
cluster with volumes. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Based on the frequency of the
backups"
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": " Estimated time to restore
cluster with volumes. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Based on the frequency of the
backups"
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
```

```
                        "expectedRtoDescription": " Estimated time to restore
cluster with volumes. (Estimate is based on averages, real time restore may vary).",
                        "expectedRpoInSecs": 86400,
                        "expectedRpoDescription": "Based on the frequency of the
backups"
                    }
                },
                "optimizationType": "LeastCost",
                "description": "Current Configuration",
                "suggestedChanges": [],
                "haArchitecture": "BackupAndRestore",
                "referenceId": "original"
            },
            {
                "cost": {
                    "amount": 0.0,
                    "currency": "USD",
                    "frequency": "Monthly"
                },
                "appComponentName": "computeappcomponent-nrz",
                "recommendationCompliance": {
                    "AZ": {
                        "expectedComplianceStatus": "PolicyMet",
                        "expectedRtoInSecs": 1800,
                        "expectedRtoDescription": " Estimated time to restore
cluster with volumes. (Estimate is based on averages, real time restore may vary).",
                        "expectedRpoInSecs": 86400,
                        "expectedRpoDescription": "Based on the frequency of the
backups"
                    },
                    "Hardware": {
                        "expectedComplianceStatus": "PolicyMet",
                        "expectedRtoInSecs": 1800,
                        "expectedRtoDescription": " Estimated time to restore
cluster with volumes. (Estimate is based on averages, real time restore may vary).",
                        "expectedRpoInSecs": 86400,
                        "expectedRpoDescription": "Based on the frequency of the
backups"
                    },
                    "Software": {
                        "expectedComplianceStatus": "PolicyMet",
                        "expectedRtoInSecs": 1800,
                        "expectedRtoDescription": " Estimated time to restore
cluster with volumes. (Estimate is based on averages, real time restore may vary).",
```

```
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Based on the frequency of the
backups"
                        }
                    },
                    "optimizationType": "LeastChange",
                    "description": "Current Configuration",
                    "suggestedChanges": [],
                    "haArchitecture": "BackupAndRestore",
                    "referenceId": "original"
                },
                {
                    "cost": {
                        "amount": 14.74,
                        "currency": "USD",
                        "frequency": "Monthly"
                    },
                    "appComponentName": "computeappcomponent-nrz",
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 0,
                            "expectedRtoDescription": "No expected downtime. You're
launching using EC2, with DesiredCount > 1 in multiple AZs and CapacityProviders with
MinSize > 1",
                            "expectedRpoInSecs": 0,
                            "expectedRpoDescription": "ECS Service state is saved on
Amazon EFS file system. No data loss is expected as objects are be stored in multiple
AZs."
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 0,
                            "expectedRtoDescription": "No expected downtime. You're
launching using EC2, with DesiredCount > 1 and CapacityProviders with MinSize > 1",
                            "expectedRpoInSecs": 0,
                            "expectedRpoDescription": "ECS Service state is saved on
Amazon EFS file system. No data loss is expected as objects are be stored in multiple
AZs."
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
```

```
                            "expectedRtoDescription": " Estimated time to restore
cluster with volumes. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Based on the frequency of the
backups"
                        }
                    },
                    "optimizationType": "BestAZRecovery",
                    "description": "Stateful Amazon ECS service with launch type Amazon
EC2 and Amazon EFS storage, deployed in multiple AZs. AWS Backup is used to backup
Amazon EFS and copy snapshots in-Region.",
                    "suggestedChanges": [
                        "Add AWS Auto Scaling Groups and Capacity Providers in multiple
AZs",
                        "Change desired count of the setup",
                        "Remove Amazon EBS volume"
                    ],
                    "haArchitecture": "BackupAndRestore",
                    "referenceId": "ecs:config:ec2-multi_az-efs-backups:2022-02-16"
                }
            ]
        },
        {
            "appComponentName": "databaseappcomponent-hji",
            "recommendationStatus": "MetCanImprove",
            "configRecommendations": [
                {
                    "cost": {
                        "amount": 0.0,
                        "currency": "USD",
                        "frequency": "Monthly"
                    },
                    "appComponentName": "databaseappcomponent-hji",
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": "Estimated time to restore from
an RDS backup. (Estimates are averages based on size, real time may vary greatly from
estimate).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Estimate based on the backup
schedule. (Estimates are calculated from backup schedule, real time restore may
vary)."
```

```
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": "Estimated time to restore from
snapshot. (Estimates are averages based on size, real time may vary greatly from
estimate).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Estimate based on the backup
schedule. (Estimates are calculated from backup schedule, real time restore may
vary)."
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": "Estimated time to restore from
snapshot. (Estimates are averages based on size, real time may vary greatly from
estimate).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Estimate based on the backup
schedule. (Estimates are calculated from backup schedule, real time restore may
vary)."
                        }
                    },
                    "optimizationType": "LeastCost",
                    "description": "Current Configuration",
                    "suggestedChanges": [],
                    "haArchitecture": "BackupAndRestore",
                    "referenceId": "original"
                },
                {
                    "cost": {
                        "amount": 0.0,
                        "currency": "USD",
                        "frequency": "Monthly"
                    },
                    "appComponentName": "databaseappcomponent-hji",
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": "Estimated time to restore from
an RDS backup. (Estimates are averages based on size, real time may vary greatly from
estimate).",
```

```
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Estimate based on the backup
schedule. (Estimates are calculated from backup schedule, real time restore may
vary)."
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": "Estimated time to restore from
snapshot. (Estimates are averages based on size, real time may vary greatly from
estimate).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Estimate based on the backup
schedule. (Estimates are calculated from backup schedule, real time restore may
vary)."
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 1800,
                            "expectedRtoDescription": "Estimated time to restore from
snapshot. (Estimates are averages based on size, real time may vary greatly from
estimate).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Estimate based on the backup
schedule. (Estimates are calculated from backup schedule, real time restore may
vary)."
                        }
                    },
                    "optimizationType": "LeastChange",
                    "description": "Current Configuration",
                    "suggestedChanges": [],
                    "haArchitecture": "BackupAndRestore",
                    "referenceId": "original"
                },
                {
                    "cost": {
                        "amount": 76.73,
                        "currency": "USD",
                        "frequency": "Monthly"
                    },
                    "appComponentName": "databaseappcomponent-hji",
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
```

```
                            "expectedRtoInSecs": 120,
                            "expectedRtoDescription": "Estimated time to promote a
secondary instance.",
                            "expectedRpoInSecs": 0,
                            "expectedRpoDescription": "Aurora data is automatically
replicated across multiple Availability Zones in a Region."
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 120,
                            "expectedRtoDescription": "Estimated time to promote a
secondary instance.",
                            "expectedRpoInSecs": 0,
                            "expectedRpoDescription": "Aurora data is automatically
replicated across multiple Availability Zones in a Region."
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 900,
                            "expectedRtoDescription": "Estimate time to backtrack to a
stable state.",
                            "expectedRpoInSecs": 300,
                            "expectedRpoDescription": "Estimate for latest restorable
time for point in time recovery."
                        }
                    },
                    "optimizationType": "BestAZRecovery",
                    "description": "Aurora database cluster with one read replica, with
backtracking window of 24 hours.",
                    "suggestedChanges": [
                        "Add read replica in the same Region",
                        "Change DB instance to a supported class (db.t3.small)",
                        "Change to Aurora",
                        "Enable cluster backtracking",
                        "Enable instance backup with retention period 7"
                    ],
                    "haArchitecture": "WarmStandby",
                    "referenceId": "rds:config:aurora-backtracking"
                }
            ]
        },
        {
            "appComponentName": "storageappcomponent-rlb",
            "recommendationStatus": "BreachedUnattainable",
```

```
            "configRecommendations": [
                {
                    "cost": {
                        "amount": 0.0,
                        "currency": "USD",
                        "frequency": "Monthly"
                    },
                    "appComponentName": "storageappcomponent-rlb",
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 0,
                            "expectedRtoDescription": "No data loss in your system",
                            "expectedRpoInSecs": 0,
                            "expectedRpoDescription": "No data loss in your system"
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyBreached",
                            "expectedRtoInSecs": 2592001,
                            "expectedRtoDescription": "No recovery option configured",
                            "expectedRpoInSecs": 2592001,
                            "expectedRpoDescription": "No recovery option configured"
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 900,
                            "expectedRtoDescription": "Time to recover Amazon EFS from
backup. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Recovery Point Objective for
Amazon EFS from backups, derived from backup frequency"
                        }
                    },
                    "optimizationType": "BestAZRecovery",
                    "description": "Amazon EFS with backups configured",
                    "suggestedChanges": [
                        "Add additional availability zone"
                    ],
                    "haArchitecture": "MultiSite",
                    "referenceId": "efs:config:with_backups:2020-04-01"
                },
                {
                    "cost": {
                        "amount": 0.0,
```

```
                        "currency": "USD",
                        "frequency": "Monthly"
                    },
                    "appComponentName": "storageappcomponent-rlb",
                    "recommendationCompliance": {
                        "AZ": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 0,
                            "expectedRtoDescription": "No data loss in your system",
                            "expectedRpoInSecs": 0,
                            "expectedRpoDescription": "No data loss in your system"
                        },
                        "Hardware": {
                            "expectedComplianceStatus": "PolicyBreached",
                            "expectedRtoInSecs": 2592001,
                            "expectedRtoDescription": "No recovery option configured",
                            "expectedRpoInSecs": 2592001,
                            "expectedRpoDescription": "No recovery option configured"
                        },
                        "Software": {
                            "expectedComplianceStatus": "PolicyMet",
                            "expectedRtoInSecs": 900,
                            "expectedRtoDescription": "Time to recover Amazon EFS from
 backup. (Estimate is based on averages, real time restore may vary).",
                            "expectedRpoInSecs": 86400,
                            "expectedRpoDescription": "Recovery Point Objective for
 Amazon EFS from backups, derived from backup frequency"
                        }
                    },
                    "optimizationType": "BestAttainable",
                    "description": "Amazon EFS with backups configured",
                    "suggestedChanges": [
                        "Add additional availability zone"
                    ],
                    "haArchitecture": "MultiSite",
                    "referenceId": "efs:config:with_backups:2020-04-01"
                }
            ]
        }
    ]
}
```

Langkah 3: Memodifikasi aplikasi Anda

AWS Resilience Hub memungkinkan Anda untuk memodifikasi sumber daya aplikasi Anda dengan mengedit versi draf aplikasi Anda dan menerbitkan perubahan ke versi baru (diterbitkan). AWS Resilience Hub menggunakan versi aplikasi Anda yang dipublikasikan, yang mencakup sumber daya yang diperbarui, untuk menjalankan penilaian ketahanan.

Untuk informasi selengkapnya, lihat topik berikut.

- the section called “Tambahkan sumber daya secara manual”
- the section called “Mengelompokkan sumber daya ke dalam satu Komponen Aplikasi”
- the section called “Mengecualikan sumber daya dari AppComponent”

Menambahkan sumber daya secara manual ke aplikasi Anda

Jika sumber daya tidak digunakan sebagai bagian dari sumber input, AWS Resilience Hub memungkinkan Anda menambahkan sumber daya secara manual ke aplikasi Anda menggunakan `CreateAppVersionResource`API. Untuk informasi lebih lanjut tentang iniAPI, lihathttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_CreateAppVersionResource.html.

Anda harus memberikan parameter berikut untuk iniAPI:

- Nama Sumber Daya Amazon (ARN) dari aplikasi
- ID logis sumber daya
- ID fisik sumber daya
- AWS CloudFormation jenis

Contoh berikut menunjukkan cara menambahkan sumber daya secara manual ke aplikasi Anda dalam AWS Resilience Hub menggunakan `CreateAppVersionResource`API.

Permintaan

```
aws resiliencehub create-app-version-resource \
--app-arn <App_ARN> \
--resource-name "backup-efs" \
--logical-resource-id '{"identifier": "backup-efs"}' \
--physical-resource-id '<Physical_resource_id_ARN>' \
```

```
--resource-type AWS::EFS::FileSystem \
--app-components '["new-app-component"]'
```

Respons

```
{
    "appArn": "<App_ARN>",
    "appVersion": "draft",
    "physicalResource": {
        "resourceName": "backup-efs",
        "logicalResourceId": {
            "identifier": "backup-efs"
        },
        "physicalResourceId": {
            "identifier": "<Physical_resource_id_ARN>",
            "type": "Arn"
        },
        "resourceType": "AWS::EFS::FileSystem",
        "appComponents": [
            {
                "name": "new-app-component",
                "type": "AWS::ResilienceHub::StorageAppComponent",
                "id": "new-app-component"
            }
        ]
    }
}
```

Mengelompokkan sumber daya ke dalam satu Komponen Aplikasi

Komponen Aplikasi (AppComponent) adalah sekelompok AWS sumber daya terkait yang bekerja dan gagal sebagai satu unit. Misalnya, ketika Anda memiliki beban kerja lintas wilayah yang digunakan sebagai penerapan siaga. AWS Resilience Hub memiliki aturan yang mengatur AWS sumber daya mana yang dapat dimiliki oleh jenis. AppComponent AWS Resilience Hub memungkinkan Anda untuk mengelompokkan sumber daya menjadi satu AppComponent menggunakan manajemen sumber daya berikutAPIs.

- `UpdateAppVersionResource`— Ini API memperbarui detail sumber daya aplikasi. Untuk informasi lebih lanjut tentang iniAPI, lihat UpdateAppVersionResource.
- `DeleteAppVersionAppComponent`— Ini API menghapus AppComponent dari aplikasi. Untuk informasi lebih lanjut tentang iniAPI, lihat DeleteAppVersionAppComponent.

Contoh berikut menunjukkan cara memperbarui detail sumber daya aplikasi Anda dalam AWS Resilience Hub menggunakan `DeleteAppVersionAppComponent`API.

Permintaan

```
aws resiliencehub delete-app-version-app-component \
--app-arn <App_ARN> \
--id new-app-component
```

Respons

```
{
    "appArn": "<App_ARN>",
    "appVersion": "draft",
    "appComponent": {
        "name": "new-app-component",
        "type": "AWS::ResilienceHub::StorageAppComponent",
        "id": "new-app-component"
    }
}
```

Contoh berikut menunjukkan cara menghapus kosong AppComponent yang dibuat dalam contoh sebelumnya dalam AWS Resilience Hub menggunakan `UpdateAppVersionResource`API.

Permintaan

```
aws resiliencehub delete-app-version-app-component \
--app-arn <App_ARN> \
--id new-app-component
```

Respons

```
{
    "appArn": "<App_ARN>",
    "appVersion": "draft",
    "appComponent": {
        "name": "new-app-component",
        "type": "AWS::ResilienceHub::StorageAppComponent",
        "id": "new-app-component"
    }
```

```
}
```

Mengecualikan sumber daya dari AppComponent

AWS Resilience Hub memungkinkan Anda untuk mengecualikan sumber daya dari penilaian menggunakan `UpdateAppVersionResource`API. Sumber daya ini tidak akan dipertimbangkan saat menghitung ketahanan aplikasi Anda. Untuk informasi lebih lanjut tentang iniAPI, lihathttps://docs.aws.amazon.com/resilience-hub/latest/APIReference/API_UpdateAppVersionResource.html.

> **Note**
>
> Anda hanya dapat mengecualikan sumber daya yang diimpor dari sumber input.

Contoh berikut menunjukkan cara mengecualikan sumber daya aplikasi Anda dalam AWS Resilience Hub menggunakan `UpdateAppVersionResource`API.

Permintaan

```
aws resiliencehub update-app-version-resource \
--app-arn <App_ARN> \
--resource-name "ec2instance-nvz" \
--excluded
```

Respons

```
{
    "appArn": "<App_ARN>",
    "appVersion": "draft",
    "physicalResource": {
        "resourceName": "ec2instance-nvz",
        "logicalResourceId": {
            "identifier": "ec2",
            "terraformSourceName": "test.state.file"
        },
        "physicalResourceId": {
            "identifier": "i-0b58265a694e5ffc1",
            "type": "Native",
            "awsRegion": "us-west-2",
            "awsAccountId": "123456789101"
```

```
        },
        "resourceType": "AWS::EC2::Instance",
        "appComponents": [
            {
                "name": "computeappcomponent-nrz",
                "type": "AWS::ResilienceHub::ComputeAppComponent"
            }
        ]
    }
}
```

Keamanan di AWS Resilience Hub

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

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

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari Program AWS Kepatuhan Program AWS Kepatuhan . Untuk mempelajari tentang program kepatuhan yang berlaku AWS Resilience Hub, lihat AWS Layanan dalam Lingkup oleh AWS Layanan Program Kepatuhan .
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan AWS Resilience Hub. Topik berikut menunjukkan cara mengonfigurasi AWS Resilience Hub untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga belajar cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan AWS Resilience Hub sumber daya Anda.

Daftar Isi

Perlindungan data di AWS Resilience Hub

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di AWS Resilience Hub. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan

kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk AWS layanan yang Anda gunakan. Untuk informasi selengkapnya tentang privasi data, lihat Privasi Data FAQ. Untuk informasi tentang perlindungan data di Eropa, lihat Model Tanggung Jawab AWS Bersama dan posting GDPR blog di Blog AWS Keamanan.

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

- Gunakan otentikasi multi-faktor (MFA) dengan setiap akun.
- GunakanSSL/TLSuntuk berkomunikasi dengan AWS sumber daya. Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya AWS layanan.
- Gunakan layanan keamanan terkelola lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan FIPS 140-3 modul kriptografi yang divalidasi saat mengakses AWS melalui antarmuka baris perintah atau, gunakan titik akhir. API FIPS Untuk informasi selengkapnya tentang FIPS titik akhir yang tersedia, lihat Federal Information Processing Standard (FIPS) 140-3.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan Resilience Hub atau lainnya AWS layanan menggunakan konsol,, API AWS CLI, atau. AWS SDKs Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Jika Anda memberikan URL ke server eksternal, kami sangat menyarankan agar Anda tidak menyertakan informasi kredensyal dalam URL untuk memvalidasi permintaan Anda ke server tersebut.

Enkripsi diam

AWS Resilience Hub mengenkripsi data Anda saat istirahat. Data dalam AWS Resilience Hub dienkripsi saat istirahat menggunakan enkripsi sisi server transparan. Hal ini membantu mengurangi

beban operasional dan kompleksitas yang terlibat dalam melindungi data sensitif. Dengan enkripsi saat istirahat, Anda dapat membangun aplikasi yang sensitif terhadap keamanan yang memenuhi persyaratan kepatuhan enkripsi dan peraturan.

Enkripsi bergerak

AWS Resilience Hub mengenkripsi data dalam perjalanan antara layanan dan layanan terintegrasi AWS lainnya. Semua data yang melewati antara AWS Resilience Hub dan layanan terintegrasi dienkripsi menggunakan Transport Layer Security ()TLS. AWS Resilience Hub menyediakan tindakan yang telah dikonfigurasi sebelumnya untuk jenis target tertentu di seluruh AWS layanan, dan mendukung tindakan untuk sumber daya target.

Identity and Access Management untuk AWS Resilience Hub

AWS Identity and Access Management (IAM) adalah AWS layanan yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. IAMadministrator mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber AWS daya Resilience Hub. IAMadalah AWS layanan yang dapat Anda gunakan tanpa biaya tambahan.

Topik

- Audiens
- Mengautentikasi dengan identitas
- Mengelola akses menggunakan kebijakan
- Cara AWS kerja Resilience Hub IAM
- Menyiapkan IAM peran dan izin
- Memecahkan masalah identitas dan AWS akses Resilience Hub
- AWS Resilience Hub referensi izin akses
- AWS kebijakan terkelola untuk AWS Resilience Hub
- AWS Resilience Hub referensi persona dan IAM izin
- Mengimpor file status Terraform ke AWS Resilience Hub
- Mengaktifkan AWS Resilience Hub akses ke klaster Amazon Elastic Kubernetes Service
- Mengaktifkan AWS Resilience Hub untuk mempublikasikan ke topik Amazon Simple Notification Service

- Membatasi izin untuk menyertakan atau mengecualikan rekomendasi AWS Resilience Hub

Audiens

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

Pengguna layanan — Jika Anda menggunakan layanan AWS Resilience Hub untuk melakukan pekerjaan Anda, administrator Anda memberi Anda kredensyal dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak fitur AWS Resilience Hub untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara akses dikelola dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di AWS Resilience Hub, lihat. Memecahkan masalah identitas dan AWS akses Resilience Hub

Administrator layanan - Jika Anda bertanggung jawab atas sumber daya AWS Resilience Hub di perusahaan Anda, Anda mungkin memiliki akses penuh ke AWS Resilience Hub. Tugas Anda adalah menentukan fitur dan sumber AWS daya Resilience Hub mana yang harus diakses pengguna layanan Anda. Anda kemudian harus mengirimkan permintaan ke IAM administrator Anda untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep dasarIAM. Untuk mempelajari lebih lanjut tentang cara perusahaan Anda dapat menggunakan IAM AWS Resilience Hub, lihat. Cara AWS kerja Resilience Hub IAM

IAMadministrator - Jika Anda seorang IAM administrator, Anda mungkin ingin mempelajari detail tentang cara menulis kebijakan untuk mengelola akses ke AWS Resilience Hub. Untuk melihat contoh kebijakan berbasis identitas AWS Resilience Hub yang dapat Anda gunakan, lihat. IAM Contoh kebijakan berbasis identitas untuk Resilience Hub AWS

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensi identitas Anda. Anda harus diautentikasi (masuk ke AWS) sebagai Pengguna root akun AWS, sebagai IAM pengguna, atau dengan mengambil peranIAM.

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

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

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

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

Akun AWS pengguna root

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

Identitas gabungan

Sebagai praktik terbaik, mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses AWS layanan dengan menggunakan kredensyal sementara.

Identitas federasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, direktori Pusat Identitas AWS Directory Service, atau pengguna mana pun yang mengakses AWS layanan dengan menggunakan kredensil yang disediakan melalui sumber identitas. Ketika identitas federasi mengakses Akun AWS, mereka mengambil peran, dan peran memberikan kredensi sementara.

Untuk manajemen akses terpusat, kami sarankan Anda menggunakan AWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat IAM Identitas, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua aplikasi Akun AWS dan aplikasi Anda. Untuk informasi tentang Pusat IAM Identitas, lihat Apa itu Pusat IAM Identitas? dalam AWS IAM Identity Center User Guide.

Pengguna dan grup IAM

IAMPengguna adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, sebaiknya mengandalkan kredensi sementara daripada membuat IAM pengguna yang memiliki kredensi jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan khusus yang memerlukan kredensil jangka panjang dengan IAM pengguna, kami sarankan Anda memutar kunci akses. Untuk informasi selengkapnya, lihat Memutar kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensi jangka panjang di IAMPanduan Pengguna.

IAMGrup adalah identitas yang menentukan kumpulan IAM pengguna. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat memiliki grup bernama IAMAdminsdan memberikan izin grup tersebut untuk mengelola sumber dayaIAM.

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

IAMperan

IAMPeran adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Ini mirip dengan IAM pengguna, tetapi tidak terkait dengan orang tertentu. Anda dapat mengambil IAM peran sementara AWS Management Console dengan beralih peran. Anda dapat mengambil peran dengan memanggil AWS CLI atau AWS API operasi atau dengan menggunakan kustomURL. Untuk informasi selengkapnya tentang metode penggunaan peran, lihat Menggunakan IAM peran di Panduan IAM Pengguna.

IAMperan dengan kredensi sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat Membuat peran untuk Penyedia Identitas pihak ketiga di Panduan IAM Pengguna. Jika Anda menggunakan Pusat IAM Identitas, Anda mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah diautentikasi, Pusat IAM Identitas mengkorelasikan izin yang disetel ke peran. IAM Untuk informasi tentang set izin, lihat Set izin dalam Panduan Pengguna AWS IAM Identity Center .
- Izin IAM pengguna sementara — IAM Pengguna atau peran dapat mengambil IAM peran untuk sementara mengambil izin yang berbeda untuk tugas tertentu.
- Akses lintas akun — Anda dapat menggunakan IAM peran untuk memungkinkan seseorang (prinsipal tepercaya) di akun lain mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa AWS layanan, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM Panduan Pengguna. IAM
- Akses lintas layanan — Beberapa AWS layanan menggunakan fitur lain AWS layanan. Misalnya, saat Anda melakukan panggilan dalam suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.
  - Sesi akses teruskan (FAS) — Saat Anda menggunakan IAM pengguna atau peran untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FASmenggunakan izin dari pemanggilan utama AWS layanan, dikombinasikan dengan permintaan AWS layanan untuk membuat permintaan ke layanan hilir. FASPermintaan hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain AWS layanan atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan saat membuat FAS permintaan, lihat Meneruskan sesi akses.
  - Peran layanan — Peran layanan adalah IAMperan yang diasumsikan layanan untuk melakukan tindakan atas nama Anda. IAMAdministrator dapat membuat, memodifikasi, dan menghapus peran layanan dari dalamIAM. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke AWS layanan dalam IAMPanduan Pengguna.

  - Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke peran layanan. AWS layanan Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. IAMAdministrator dapat melihat, tetapi tidak mengedit izin untuk peran terkait layanan.
- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan IAM peran untuk mengelola kredensil sementara untuk aplikasi yang berjalan pada EC2 instance dan membuat AWS CLI atau AWS API meminta. Ini lebih baik untuk menyimpan kunci akses dalam EC2 instance. Untuk menetapkan AWS peran ke EC2 instance dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instance berisi peran dan memungkinkan program yang berjalan pada EC2 instance untuk mendapatkan kredensi sementara. Untuk informasi selengkapnya, lihat Menggunakan IAM peran untuk memberikan izin ke aplikasi yang berjalan di EC2 instans Amazon di IAMPanduan Pengguna.

Untuk mempelajari apakah akan menggunakan IAM peran atau IAM pengguna, lihat Kapan membuat IAM peran (bukan pengguna) di Panduan IAM Pengguna.

Mengelola akses menggunakan kebijakan

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

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

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

IAMkebijakan menentukan izin untuk tindakan terlepas dari metode yang Anda gunakan untuk melakukan operasi. Misalnya, anggaplah Anda memiliki kebijakan yang mengizinkan tindakan

`iam:GetRole`. Pengguna dengan kebijakan itu bisa mendapatkan informasi peran dari AWS Management Console, AWS CLI, atau AWS API.

Kebijakan berbasis identitas

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

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan yang dikelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran dalam. Akun AWS Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan terkelola atau kebijakan sebaris, lihat Memilih antara kebijakan terkelola dan kebijakan sebaris di IAMPanduan Pengguna.

Kebijakan berbasis sumber daya

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

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

Daftar kontrol akses (ACLs)

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLsmirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan. JSON

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung. ACLs Untuk mempelajari selengkapnyaACLs, lihat Ikhtisar daftar kontrol akses (ACL) di Panduan Pengembang Layanan Penyimpanan Sederhana Amazon.

Jenis-jenis kebijakan lain

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

- Batas izin — Batas izin adalah fitur lanjutan tempat Anda menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas (pengguna atau peran). IAM IAM Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batas izin, lihat Batas izin untuk IAM entitas di IAMPanduan Pengguna.
- Kebijakan kontrol layanan (SCPs) — SCPs adalah JSON kebijakan yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di AWS Organizations. AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur dalam suatu organisasi, maka Anda dapat menerapkan kebijakan kontrol layanan (SCPs) ke salah satu atau semua akun Anda. SCPMembatasi izin untuk entitas di akun anggota, termasuk masing-masing Pengguna root akun AWS. Untuk informasi selengkapnya tentang Organizations danSCPs, lihat Kebijakan kontrol layanan di Panduan AWS Organizations Pengguna.
- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan secara tegas dalam salah satu kebijakan ini membatalkan izin. Untuk informasi selengkapnya, lihat Kebijakan sesi di Panduan IAM Pengguna.

Berbagai jenis kebijakan

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

Cara AWS kerja Resilience Hub IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke AWS Resilience Hub, pelajari IAM fitur apa saja yang tersedia untuk digunakan dengan AWS Resilience Hub.

IAMfitur yang dapat Anda gunakan dengan AWS Resilience Hub

IAMfitur	AWS Dukungan Resilience Hub
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
kunci-kunci persyaratan kebijakan (spesifik layanan)	Ya
ACLs	Tidak
ABAC(tag dalam kebijakan)	Parsial
Kredensial sementara	Ya
Teruskan sesi akses (FAS)	Ya
Peran layanan	Ya

Untuk mendapatkan tampilan tingkat tinggi tentang cara kerja AWS Resilience Hub dan AWS layanan lainnya dengan sebagian besar IAM fitur, lihat AWS layanan yang berfungsi IAM di Panduan Pengguna. IAM

Kebijakan berbasis identitas untuk Resilience Hub AWS

Mendukung kebijakan berbasis identitas: Ya

Kebijakan berbasis identitas adalah dokumen kebijakan JSON izin yang dapat Anda lampirkan ke identitas, seperti pengguna, grup IAM pengguna, atau peran. Kebijakan ini mengontrol jenis tindakan

yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Membuat IAM kebijakan di Panduan Pengguna. IAM

Dengan kebijakan IAM berbasis identitas, Anda dapat menentukan tindakan dan sumber daya yang diizinkan atau ditolak serta kondisi di mana tindakan diizinkan atau ditolak. Anda tidak dapat menentukan secara spesifik prinsipal dalam sebuah kebijakan berbasis identitas karena prinsipal berlaku bagi pengguna atau peran yang melekat kepadanya. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam JSON kebijakan, lihat referensi elemen IAM JSON kebijakan di Panduan IAM Pengguna.

Contoh kebijakan berbasis identitas untuk Resilience Hub AWS

Untuk melihat contoh kebijakan berbasis identitas AWS Resilience Hub, lihat. Contoh kebijakan berbasis identitas untuk Resilience Hub AWS

Kebijakan berbasis sumber daya dalam Resilience Hub AWS

Mendukung kebijakan berbasis sumber daya: Tidak

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

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan seluruh akun atau IAM entitas di akun lain sebagai prinsipal dalam kebijakan berbasis sumber daya. Menambahkan prinsipal akun silang ke kebijakan berbasis sumber daya hanya setengah dari membangun hubungan kepercayaan. Ketika prinsipal dan sumber daya berbeda Akun AWS, IAM administrator di akun tepercaya juga harus memberikan izin entitas utama (pengguna atau peran) untuk mengakses sumber daya. Mereka memberikan izin dengan melampirkan kebijakan berbasis identitas kepada entitas. Namun, jika kebijakan berbasis sumber daya memberikan akses ke prinsipal dalam akun yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun IAM di Panduan IAM Pengguna.

Tindakan kebijakan untuk AWS Resilience Hub

Mendukung tindakan kebijakan: Ya

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

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

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

Untuk melihat daftar tindakan AWS Resilience Hub, lihat Tindakan yang ditentukan oleh AWS Resilience Hub di Referensi Otorisasi Layanan.

Tindakan kebijakan di AWS Resilience Hub menggunakan awalan berikut sebelum tindakan:

```
resiliencehub
```

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan tersebut dengan koma.

```
"Action": [
      "resiliencehub:action1",
      "resiliencehub:action2"
         ]
```

Untuk melihat contoh kebijakan berbasis identitas AWS Resilience Hub, lihat. Contoh kebijakan berbasis identitas untuk Resilience Hub AWS

Sumber daya kebijakan untuk AWS Resilience Hub

Mendukung sumber daya kebijakan: Ya

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Elemen `Resource` JSON kebijakan menentukan objek atau objek yang tindakan tersebut berlaku. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Sebagai praktik terbaik, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, misalnya operasi pencantuman, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

```
"Resource": "*"
```

Untuk melihat daftar jenis sumber daya AWS Resilience Hub dan jenisnyaARNs, lihat Sumber Daya yang ditentukan oleh AWS Resilience Hub di Referensi Otorisasi Layanan. Untuk mempelajari tindakan yang dapat Anda tentukan ARN dari setiap sumber daya, lihat Tindakan yang ditentukan oleh AWS Resilience Hub.

Untuk melihat contoh kebijakan berbasis identitas AWS Resilience Hub, lihat. Contoh kebijakan berbasis identitas untuk Resilience Hub AWS

Kunci kondisi kebijakan untuk AWS Resilience Hub

Mendukung kunci kondisi kebijakan khusus layanan: Ya

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen `Condition` (atau blok `Condition`) akan memungkinkan Anda menentukan kondisi yang menjadi dasar suatu pernyataan berlaku. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi bersyarat yang menggunakan operator kondisi, misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi 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 menggunakan operasi

AND logis. Jika Anda menentukan beberapa nilai untuk satu kunci kondisi, AWS mengevaluasi kondisi menggunakan 0R operasi logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Misalnya, Anda dapat memberikan izin IAM pengguna untuk mengakses sumber daya hanya jika ditandai dengan nama IAM pengguna mereka. Untuk informasi selengkapnya, lihat elemen IAM kebijakan: variabel dan tag di Panduan IAM Pengguna.

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan IAM Pengguna.

Untuk melihat daftar kunci kondisi AWS Resilience Hub, lihat Kunci kondisi untuk AWS Resilience Hub di Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat Tindakan yang ditentukan oleh AWS Resilience Hub.

Untuk melihat contoh kebijakan berbasis identitas AWS Resilience Hub, lihat. Contoh kebijakan berbasis identitas untuk Resilience Hub AWS

ACLsdi AWS Resilience Hub

MendukungACLs: Tidak

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLsmirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan. JSON

ABACdengan AWS Resilience Hub

Mendukung ABAC (tag dalam kebijakan): Sebagian

Attribute-based access control (ABAC) adalah strategi otorisasi yang mendefinisikan izin berdasarkan atribut. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tag ke IAM entitas (pengguna atau peran) dan ke banyak AWS sumber daya. Menandai entitas dan sumber daya adalah langkah pertama dari. ABAC Kemudian Anda merancang ABAC kebijakan untuk mengizinkan operasi ketika tag prinsipal cocok dengan tag pada sumber daya yang mereka coba akses.

ABACmembantu dalam lingkungan yang berkembang pesat dan membantu dengan situasi di mana manajemen kebijakan menjadi rumit.

Untuk mengendalikan akses berdasarkan tag, berikan informasi tentang tag di elemen kondisi dari kebijakan menggunakan kunci kondisi `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi untuk hanya beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi lebih lanjut tentangABAC, lihat Apa ituABAC? dalam IAMUser Guide. Untuk melihat tutorial dengan langkah-langkah penyiapanABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) di IAMPanduan Pengguna.

Menggunakan kredensil sementara dengan AWS Resilience Hub

Mendukung kredensi sementara: Ya

Beberapa AWS layanan tidak berfungsi saat Anda masuk menggunakan kredensil sementara. Untuk informasi tambahan, termasuk yang AWS layanan bekerja dengan kredensyal sementara, lihat AWS layanan yang berfungsi IAM di IAMPanduan Pengguna.

Anda menggunakan kredensi sementara jika Anda masuk AWS Management Console menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, ketika Anda mengakses AWS menggunakan link sign-on (SSO) tunggal perusahaan Anda, proses tersebut secara otomatis membuat kredensi sementara. Anda juga akan secara otomatis membuat kredensial sementara ketika Anda masuk ke konsol sebagai seorang pengguna lalu beralih peran. Untuk informasi selengkapnya tentang beralih peran, lihat Beralih ke peran (konsol) di Panduan IAM Pengguna.

Anda dapat secara manual membuat kredensil sementara menggunakan atau. AWS CLI AWS API Anda kemudian dapat menggunakan kredensil sementara tersebut untuk mengakses. AWS AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensi sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensi keamanan sementara di. IAM

Teruskan sesi akses untuk AWS Resilience Hub

Mendukung sesi akses maju (FAS): Ya

Saat Anda menggunakan IAM pengguna atau peran untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FASmenggunakan izin dari pemanggilan utama AWS layanan, dikombinasikan dengan permintaan AWS layanan untuk membuat permintaan ke layanan hilir. FASPermintaan hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain AWS layanan atau sumber daya untuk

menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan saat membuat FAS permintaan, lihat Meneruskan sesi akses.

Peran layanan untuk AWS Resilience Hub

Mendukung peran layanan: Ya

Peran layanan adalah IAMperan yang diasumsikan layanan untuk melakukan tindakan atas nama Anda. IAMAdministrator dapat membuat, memodifikasi, dan menghapus peran layanan dari dalamIAM. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke AWS layanan dalam IAMPanduan Pengguna.

> **Warning**
>
> Mengubah izin untuk peran layanan dapat merusak fungsionalitas AWS Resilience Hub. Edit peran layanan hanya jika AWS Resilience Hub memberikan panduan untuk melakukannya.

Contoh kebijakan berbasis identitas untuk Resilience Hub AWS

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber AWS daya Resilience Hub. Mereka juga tidak dapat melakukan tugas dengan menggunakan AWS Management Console, AWS Command Line Interface (AWS CLI), atau AWS API. Untuk memberikan izin kepada pengguna untuk melakukan tindakan pada sumber daya yang mereka butuhkan, IAM administrator dapat membuat IAM kebijakan. Administrator kemudian dapat menambahkan IAM kebijakan ke peran, dan pengguna dapat mengambil peran.

Untuk mempelajari cara membuat kebijakan IAM berbasis identitas menggunakan contoh dokumen kebijakan ini, lihat Membuat JSON IAM kebijakan di Panduan Pengguna. IAM

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh AWS Resilience Hub, termasuk format ARNs untuk setiap jenis sumber daya, lihat Kunci tindakan, sumber daya, dan kondisi untuk AWS Resilience Hub di Referensi Otorisasi Layanan.

Topik

- Praktik terbaik kebijakan
- Menggunakan konsol AWS Resilience Hub
- Mengizinkan pengguna melihat izin mereka sendiri
- Daftar AWS Resilience Hub aplikasi yang tersedia

- Memulai penilaian aplikasi
- Menghapus penilaian aplikasi
- Membuat template rekomendasi untuk aplikasi tertentu
- Menghapus template rekomendasi untuk aplikasi tertentu
- Memperbarui aplikasi dengan kebijakan ketahanan tertentu

Praktik terbaik kebijakan

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

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan terkelola AWS pelanggan yang spesifik untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat kebijakan AWSAWS terkelola atau kebijakan terkelola untuk fungsi pekerjaan di Panduan IAM Pengguna.
- Menerapkan izin hak istimewa paling sedikit — Saat Anda menetapkan izin dengan IAM kebijakan, berikan hanya izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang penggunaan IAM untuk menerapkan izin, lihat Kebijakan dan izin IAM di IAM Panduan Pengguna.
- Gunakan ketentuan dalam IAM kebijakan untuk membatasi akses lebih lanjut — Anda dapat menambahkan kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Misalnya, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakanSSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik AWS layanan, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat elemen IAM JSON kebijakan: Kondisi dalam Panduan IAM Pengguna.
- Gunakan IAM Access Analyzer untuk memvalidasi IAM kebijakan Anda guna memastikan izin yang aman dan fungsional — IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan mematuhi bahasa IAM kebijakan () JSON dan praktik terbaik. IAM

IAMAccess Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat Validasi kebijakan IAM Access Analyzer di IAMPanduan Pengguna.

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

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

Menggunakan konsol AWS Resilience Hub

Untuk mengakses konsol AWS Resilience Hub, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang sumber daya AWS Resilience Hub 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 mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau. AWS API Sebagai gantinya, izinkan akses hanya ke tindakan yang cocok dengan API operasi yang mereka coba lakukan.

Untuk memastikan bahwa pengguna dan peran masih dapat menggunakan konsol AWS Resilience Hub, lampirkan juga AWS Resilience Hub *ConsoleAccess* atau kebijakan *ReadOnly* AWS terkelola ke entitas. Untuk informasi selengkapnya, lihat Menambahkan izin ke pengguna di Panduan IAM Pengguna.

Kebijakan berikut memberi pengguna izin untuk mencantumkan dan melihat semua sumber daya di AWS Resilience Hub konsol, tetapi tidak untuk membuat, memperbarui, atau menghapusnya.

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Effect": "Allow",
             "Action": [
                 "resiliencehub:List*",
```

```
                "resiliencehub:Describe*"
            ],
            "Resource": "*"
        }
    ]
}
```

Mengizinkan pengguna melihat izin mereka sendiri

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

```
{
    "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": "*"
```

```
        }
    ]
}
```

Daftar AWS Resilience Hub aplikasi yang tersedia

Kebijakan berikut memberi pengguna izin untuk membuat daftar AWS Resilience Hub aplikasi yang tersedia.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
          "resiliencehub:ListApps"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Memulai penilaian aplikasi

Kebijakan berikut memberi pengguna izin untuk memulai penilaian untuk AWS Resilience Hub aplikasi tertentu.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
          "resiliencehub:StartAppAssessment"
      ],
      "Resource": [
        "arn:aws:resiliencehub:*:*:app/appId"
      ]
```

```
    }
  ]
}
```

Menghapus penilaian aplikasi

Kebijakan berikut memberi pengguna izin untuk menghapus penilaian untuk AWS Resilience Hub aplikasi tertentu.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
          "resiliencehub:DeleteAppAssessment"
      ],
      "Resource": [
        "arn:aws:resiliencehub:*:*:app/appId"
      ]
    }
  ]
}
```

Membuat template rekomendasi untuk aplikasi tertentu

Kebijakan berikut memberi pengguna izin untuk membuat templat rekomendasi untuk AWS Resilience Hub aplikasi tertentu.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
          "resiliencehub:CreateRecommendationTemplate"
      ],
      "Resource": [
        "arn:aws:resiliencehub:*:*:app/appId"
      ]
```

```
    }
  ]
}
```

Menghapus template rekomendasi untuk aplikasi tertentu

Kebijakan berikut memberi pengguna izin untuk menghapus templat rekomendasi untuk AWS Resilience Hub aplikasi tertentu.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
          "resiliencehub:DeleteRecommendationTemplate"
      ],
      "Resource": [
        "arn:aws:resiliencehub:*:*:app/appId"
      ]
    }
  ]
}
```

Memperbarui aplikasi dengan kebijakan ketahanan tertentu

Kebijakan berikut memberi pengguna izin untuk memperbarui AWS Resilience Hub aplikasi dengan kebijakan ketahanan tertentu.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PolicyExample",
      "Effect": "Allow",
      "Action": [
          "resiliencehub:UpdateApp"
      ],
      "Resource": [
        "arn:aws:resiliencehub:*:*:app/appId"
      ],
      "Condition": {
```

```
        "StringLike" : { "resiliencehub:policyArn" : "arn:aws:resiliencehub:us-
west-2:111122223333:resiliency-policy/*" }
      }
    }
  ]
}
```

Menyiapkan IAM peran dan izin

AWS Resilience Hub memungkinkan Anda mengonfigurasi IAM peran yang ingin Anda gunakan saat menjalankan penilaian untuk aplikasi Anda. Ada beberapa cara untuk mengonfigurasi AWS Resilience Hub untuk mendapatkan akses hanya-baca ke sumber daya aplikasi Anda. Namun, AWS Resilience Hub merekomendasikan cara-cara berikut:

- Akses berbasis peran — Peran ini didefinisikan dan digunakan dalam akun saat ini. AWS Resilience Hub akan mengambil peran ini untuk mengakses sumber daya aplikasi Anda.

  Untuk menyediakan akses berbasis peran, peran harus mencakup yang berikut:

  - Izin baca-saja untuk membaca sumber daya Anda (AWS Resilience Hub menyarankan Anda untuk menggunakan kebijakan `AWSResilienceHubAsssessmentExecutionPolicy` terkelola).
  - Kebijakan kepercayaan untuk mengambil peran ini, yang memungkinkan Principal AWS Resilience Hub Layanan untuk mengambil peran ini. Jika Anda tidak memiliki peran seperti itu dikonfigurasi di akun Anda, AWS Resilience Hub akan menampilkan petunjuk untuk membuat peran itu. Untuk informasi selengkapnya, lihat the section called “Langkah 6: Pengaturan izin”.

  > **Note**
  >
  > Jika Anda hanya memberikan nama peran pemanggil dan jika sumber daya Anda berada di akun lain, AWS Resilience Hub akan menggunakan nama peran ini di akun lain untuk mengakses sumber daya lintas akun. Secara opsional, Anda dapat mengonfigurasi peran ARNs untuk akun lain, yang akan digunakan sebagai pengganti nama peran pemanggil.

- Akses IAM pengguna saat ini — AWS Resilience Hub akan menggunakan IAM pengguna saat ini untuk mengakses sumber daya aplikasi Anda. Ketika sumber daya Anda berada di akun yang berbeda, AWS Resilience Hub akan mengambil IAM peran berikut untuk mengakses sumber daya:
  - `AwsResilienceHubAdminAccountRole`di akun saat ini
  - `AwsResilienceHubExecutorAccountRole`di akun lain

Selain itu, ketika Anda mengkonfigurasi penilaian terjadwal, AWS Resilience Hub akan mengambil `AwsResilienceHubPeriodicAssessmentRole` peran. Namun, penggunaan tidak `AwsResilienceHubPeriodicAssessmentRole` disarankan karena Anda harus mengonfigurasi peran dan izin secara manual, dan beberapa fungsi (seperti pemberitahuan Drift) mungkin tidak berfungsi seperti yang diharapkan.

Memecahkan masalah identitas dan AWS akses Resilience Hub

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan AWS Resilience Hub dan. IAM

Topik

- Saya tidak berwenang untuk melakukan tindakan di AWS Resilience Hub
- Saya tidak berwenang untuk melakukan iam: PassRole
- Saya ingin mengizinkan orang di luar saya Akun AWS mengakses sumber AWS daya Resilience Hub saya

Saya tidak berwenang untuk melakukan tindakan di AWS Resilience Hub

Jika Anda menerima pesan kesalahan bahwa Anda tidak memiliki otorisasi untuk melakukan tindakan, kebijakan Anda harus diperbarui agar Anda dapat melakukan tindakan tersebut.

Contoh kesalahan berikut terjadi ketika `mateojackson` IAM pengguna mencoba menggunakan konsol untuk melihat detail tentang *`my-example-widget`* sumber daya fiksi tetapi tidak memiliki izin `resiliencehub:`*`GetWidget`* fiksi.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 resiliencehub:GetWidget on resource: my-example-widget
```

Dalam hal ini, kebijakan untuk pengguna `mateojackson` harus diperbarui untuk mengizinkan akses ke sumber daya *`my-example-widget`* dengan menggunakan tindakan `resiliencehub:`*`GetWidget`*.

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

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 AWS Resilience Hub.

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

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

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

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

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

Saya ingin mengizinkan orang di luar saya Akun AWS mengakses sumber AWS daya Resilience Hub saya

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

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mengetahui apakah AWS Resilience Hub mendukung fitur-fitur ini, lihat. Cara AWS kerja Resilience Hub IAM
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat Menyediakan akses ke IAM pengguna lain Akun AWS yang Anda miliki di Panduan IAM Pengguna.

- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga dalam Panduan IAM Pengguna.
- Untuk mempelajari cara menyediakan akses melalui federasi identitas, lihat Menyediakan akses ke pengguna yang diautentikasi secara eksternal (federasi identitas) di Panduan Pengguna. IAM
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM Panduan Pengguna. IAM

AWS Resilience Hub referensi izin akses

Anda dapat menggunakan AWS Identity and Access Management (IAM) untuk mengelola akses ke sumber daya aplikasi dan membuat IAM kebijakan yang berlaku untuk pengguna, grup, atau peran.

Setiap AWS Resilience Hub aplikasi dapat dikonfigurasi untuk menggunakan the section called “Peran invoker” (IAMperan), atau menggunakan izin IAM pengguna saat ini (bersama dengan serangkaian peran yang telah ditentukan untuk penilaian lintas akun dan terjadwal). Dalam peran ini, Anda dapat melampirkan kebijakan yang menentukan izin yang diperlukan AWS Resilience Hub untuk mengakses AWS sumber daya atau sumber daya aplikasi lainnya. Peran invoker harus memiliki kebijakan kepercayaan yang ditambahkan ke Prinsipal AWS Resilience Hub Layanan.

Untuk mengelola izin untuk aplikasi Anda, kami sarankan untuk menggunakanthe section called “AWS kebijakan terkelola”. Anda dapat menggunakan kebijakan terkelola ini tanpa modifikasi apa pun, atau Anda dapat menggunakannya sebagai titik awal untuk menulis kebijakan pembatasan Anda sendiri. Kebijakan dapat membatasi izin pengguna di tingkat sumber daya untuk tindakan yang berbeda dengan menggunakan kondisi opsional tambahan.

Jika sumber daya aplikasi Anda berada di akun yang berbeda (akun sekunder/sumber daya), Anda harus menyiapkan peran baru di setiap akun yang berisi sumber daya aplikasi Anda.

Topik

- the section called “Menggunakan IAM peran”
- the section called “Menggunakan izin IAM pengguna saat ini”

Menggunakan IAM peran

AWS Resilience Hub akan menggunakan IAM peran yang telah ditentukan sebelumnya untuk mengakses sumber daya Anda di akun utama atau akun sekunder/sumber daya. Ini adalah opsi izin yang disarankan untuk mengakses sumber daya Anda.

Topik

- the section called “Peran invoker”
- the section called “Peran di AWS akun berbeda untuk akses lintas akun”

Peran invoker

Peran AWS Resilience Hub invoker adalah peran AWS Identity and Access Management (IAM) yang AWS Resilience Hub mengasumsikan untuk mengakses AWS layanan dan sumber daya. Misalnya, Anda dapat membuat peran invoker yang memiliki izin untuk mengakses CFN template Anda dan sumber daya yang dibuatnya. Halaman ini memberikan informasi tentang cara membuat, melihat, dan mengelola peran pemanggil aplikasi.

Saat Anda membuat aplikasi, Anda memberikan peran invoker. AWS Resilience Hub mengasumsikan peran ini untuk mengakses sumber daya Anda saat Anda mengimpor sumber daya atau memulai penilaian. AWS Resilience Hub Agar dapat mengambil peran invoker Anda dengan benar, kebijakan kepercayaan peran harus menentukan prinsip AWS Resilience Hub layanan (resiliencehub.amazonaws.com) sebagai layanan tepercaya.

Untuk melihat peran invoker aplikasi, pilih Aplikasi dari panel navigasi, lalu pilih Perbarui izin dari menu Tindakan di halaman Aplikasi.

Anda dapat menambahkan atau menghapus izin dari peran pemanggil aplikasi kapan saja, atau mengonfigurasi aplikasi Anda untuk menggunakan peran yang berbeda untuk mengakses sumber daya aplikasi.

Topik

- the section called “Membuat peran invoker di konsol IAM”
- the section called “Mengelola peran dengan IAM API”
- the section called “Mendefinisikan kebijakan kepercayaan menggunakan file JSON”

Membuat peran invoker di konsol IAM

AWS Resilience Hub Untuk mengaktifkan akses AWS layanan dan sumber daya, Anda harus membuat peran invoker di akun utama menggunakan IAM konsol. Untuk informasi selengkapnya tentang membuat peran menggunakan IAM konsol, lihat Membuat peran untuk AWS layanan (konsol).

Untuk membuat peran invoker di akun utama menggunakan konsol IAM

1. Buka konsol IAM di `https://console.aws.amazon.com/iam/`.
2. Dari panel navigasi, pilih Peran, lalu pilih Buat peran.
3. Pilih Kebijakan Kepercayaan Kustom, salin kebijakan berikut di jendela Kebijakan kepercayaan kustom, lalu pilih Berikutnya.

> **Note**
>
> Jika sumber daya Anda berada di akun yang berbeda, Anda harus membuat peran di masing-masing akun tersebut, dan menggunakan kebijakan kepercayaan akun sekunder untuk akun lainnya.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "resiliencehub.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

4. Di bagian Kebijakan izin di halaman Tambahkan izin, masukkan `AWSResilienceHubAsssessmentExecutionPolicy` di Filter kebijakan berdasarkan properti atau nama kebijakan, lalu tekan kotak enter.
5. Pilih kebijakan dan pilih Berikutnya.

6. Di bagian Rincian peran, masukkan nama peran unik (sepertiAWSResilienceHubAssessmentRole) di kotak Nama peran.

   Bidang ini hanya menerima karakter alfanumerik dan ". +=,.@-_/

7. (Opsional) Masukkan deskripsi tentang peran di kotak Deskripsi.
8. Pilih Buat Peran.

   Untuk mengedit kasus penggunaan dan izin, pada langkah 6, pilih tombol Edit yang terletak di sebelah kanan Langkah 1: Pilih entitas tepercaya atau Langkah 2: Tambahkan bagian izin.

Setelah membuat peran invoker dan peran sumber daya (jika ada), Anda dapat mengonfigurasi aplikasi Anda untuk menggunakan peran ini.

> **Note**
>
> Anda harus memiliki `iam:passRole` izin dalam IAM pengguna/peran Anda saat ini untuk peran invoker saat membuat atau memperbarui aplikasi. Namun, Anda tidak memerlukan izin ini untuk menjalankan penilaian.

Mengelola peran dengan IAM API

Kebijakan kepercayaan peran memberikan izin kepala sekolah yang ditentukan untuk mengambil peran tersebut. Untuk membuat peran menggunakan AWS Command Line Interface (AWS CLI), gunakan `create-role` perintah. Saat menggunakan perintah ini, Anda dapat menentukan kebijakan kepercayaan sebaris. Contoh berikut menunjukkan cara memberikan AWS Resilience Hub layanan izin utama untuk mengambil peran Anda.

> **Note**
>
> Persyaratan untuk menghindari tanda kutip (' ') dalam JSON string dapat bervariasi berdasarkan versi shell Anda.

Sampel **`create-role`**

```
aws iam create-role --role-name AWSResilienceHubAssessmentRole --assume-role-policy-
document '{
```

```
  "Version": "2012-10-17","Statement":
  [
    {
      "Effect": "Allow",
      "Principal": {"Service": "resiliencehub.amazonaws.com"},
      "Action": "sts:AssumeRole"
    }
  ]
}'
```

Mendefinisikan kebijakan kepercayaan menggunakan file JSON

Anda dapat menentukan kebijakan kepercayaan untuk peran menggunakan JSON file terpisah dan kemudian menjalankan `create-role` perintah. Dalam contoh berikut, **`trust-policy.json`**adalah file yang berisi kebijakan kepercayaan di direktori saat ini. Kebijakan ini dilampirkan ke peran dengan menjalankan **`create-role`**perintah. Output dari **`create-role`** perintah ditampilkan dalam Output Sampel. Untuk menambahkan izin ke peran, gunakan attach-policy-to-roleperintah dan Anda dapat memulai dengan menambahkan kebijakan `AWSResilienceHubAsssessmentExecutionPolicy` terkelola. Untuk informasi selengkapnya tentang kebijakan terkelola ini, lihatthe section called "AWSResilienceHubAsssessmentExecutionPolicy".

Sampel **`trust-policy.json`**

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Principal": {
            "Service": "resiliencehub.amazonaws.com"
        },
        "Action": "sts:AssumeRole"
    }]
}
```

Sampel **`create-role`**

```
aws iam create-role --role-name AWSResilienceHubAssessmentRole --assume-
role-policy-document file://trust-policy.json
```

Keluaran Sampel

```
{
```

```
    "Role": {
        "Path": "/",
        "RoleName": "AWSResilienceHubAssessmentRole",
        "RoleId": "AROAQFOXMPL6TZ6ITKWND",
        "Arn": "arn:aws:iam::123456789012:role/AWSResilienceHubAssessmentRole",
        "CreateDate": "2020-01-17T23:19:12Z",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [{
                "Effect": "Allow",
                "Principal": {
                    "Service": "resiliencehub.amazonaws.com"
                },
                "Action": "sts:AssumeRole"
            }]
        }
    }
}
```

Sampel **`attach-policy-to-role`**

```
aws iam attach-role-policy --role-name AWSResilienceHubAssessmentRole --
policy-arn arn:aws:iam::aws:policy/
AWSResilienceHubAsssessmentExecutionPolicy
```

Peran dalam AWS akun yang berbeda untuk akses lintas akun - opsional

Ketika sumber daya Anda berada di akun sekunder/sumber daya, Anda harus membuat peran di masing-masing akun ini AWS Resilience Hub agar dapat berhasil menilai aplikasi Anda. Prosedur pembuatan peran mirip dengan proses pembuatan peran invoker, kecuali untuk konfigurasi kebijakan kepercayaan.

> **Note**
>
> Anda harus membuat peran di akun sekunder tempat sumber daya berada.

Topik

- the section called “Membuat peran di IAM konsol untuk akun sekunder/sumber daya”
- the section called “Mengelola peran dengan IAM API”

- the section called “Mendefinisikan kebijakan kepercayaan menggunakan file JSON”

Membuat peran di IAM konsol untuk akun sekunder/sumber daya

AWS Resilience Hub Untuk mengaktifkan akses AWS layanan dan sumber daya di AWS akun lain, Anda harus membuat peran di masing-masing akun ini.

Untuk membuat peran di IAM konsol untuk akun sekunder/sumber daya menggunakan konsol IAM

1. Buka konsol IAM di `https://console.aws.amazon.com/iam/`.
2. Dari panel navigasi, pilih Peran, lalu pilih Buat peran.
3. Pilih Kebijakan Kepercayaan Kustom, salin kebijakan berikut di jendela Kebijakan kepercayaan kustom, lalu pilih Berikutnya.

> **Note**
>
> Jika sumber daya Anda berada di akun yang berbeda, Anda harus membuat peran di masing-masing akun tersebut dan menggunakan kebijakan kepercayaan akun sekunder untuk akun lainnya.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::primary_account_id:role/InvokerRoleName"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

4. Di bagian Kebijakan izin di halaman Tambahkan izin, masukkan `AWSResilienceHubAsssessmentExecutionPolicy` di Filter kebijakan berdasarkan properti atau nama kebijakan, lalu tekan kotak enter.

5. Pilih kebijakan dan pilih Berikutnya.
6. Di bagian Rincian peran, masukkan nama peran unik (sepertiAWSResilienceHubAssessmentRole) di kotak Nama peran.
7. (Opsional) Masukkan deskripsi tentang peran di kotak Deskripsi.
8. Pilih Buat Peran.

   Untuk mengedit kasus penggunaan dan izin, pada langkah 6, pilih tombol Edit yang terletak di sebelah kanan Langkah 1: Pilih entitas tepercaya atau Langkah 2: Tambahkan bagian izin.

Selain itu, Anda juga perlu menambahkan `sts:assumeRole` izin ke peran invoker untuk memungkinkannya mengambil peran di akun sekunder Anda.

Tambahkan kebijakan berikut ke peran invoker Anda untuk setiap peran sekunder yang Anda buat:

```
{
    "Effect": "Allow",
    "Resource": [
      "arn:aws:iam::secondary_account_id_1:role/RoleInSecondaryAccount_1",
      "arn:aws:iam::secondary_account_id_2:role/RoleInSecondaryAccount_2",
      ...
      ],
      "Action": [
        "sts:AssumeRole"
      ]
}
```

Mengelola peran dengan IAM API

Kebijakan kepercayaan peran memberikan izin kepala sekolah yang ditentukan untuk mengambil peran tersebut. Untuk membuat peran menggunakan AWS Command Line Interface (AWS CLI), gunakan `create-role` perintah. Saat menggunakan perintah ini, Anda dapat menentukan kebijakan kepercayaan sebaris. Contoh berikut menunjukkan cara memberikan izin kepada kepala AWS Resilience Hub layanan untuk mengambil peran Anda.

> **Note**
>
> Persyaratan untuk menghindari tanda kutip (`'  '`) dalam JSON string dapat bervariasi berdasarkan versi shell Anda.

Sampel **`create-role`**

```
aws iam create-role --role-name AWSResilienceHubAssessmentRole --assume-role-policy-
document '{"Version": "2012-10-17","Statement": [{"Effect": "Allow","Principal":
 {"AWS": ["arn:aws:iam::primary_account_id:role/InvokerRoleName"]},"Action":
 "sts:AssumeRole"}]}'
```

Anda juga dapat menentukan kebijakan kepercayaan untuk peran tersebut menggunakan JSON file terpisah. Dalam contoh berikut, `trust-policy.json` adalah file dalam direktori saat ini.

Mendefinisikan kebijakan kepercayaan menggunakan file JSON

Anda dapat menentukan kebijakan kepercayaan untuk peran menggunakan JSON file terpisah dan kemudian menjalankan `create-role` perintah. Dalam contoh berikut, **`trust-policy.json`**adalah file yang berisi kebijakan kepercayaan di direktori saat ini. Kebijakan ini dilampirkan ke peran dengan menjalankan **`create-role`**perintah. Output dari **`create-role`** perintah ditampilkan dalam Output Sampel. Untuk menambahkan izin ke peran, gunakan attach-policy-to-roleperintah dan Anda dapat memulai dengan menambahkan kebijakan `AWSResilienceHubAsssessmentExecutionPolicy` terkelola. Untuk informasi selengkapnya tentang kebijakan terkelola ini, lihatthe section called “AWSResilienceHubAsssessmentExecutionPolicy”.

Sampel **`trust-policy.json`**

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::primary_account_id:role/InvokerRoleName"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Sampel **`create-role`**

```
aws iam create-role --role-name AWSResilienceHubAssessmentRole --assume-role-policy-
document file://trust-policy.json
```

Keluaran Sampel

```
{
    "Role": {
        "Path": "/",
        "RoleName": "AWSResilienceHubAssessmentRole2",
        "RoleId": "AROAT2GICMEDJML6EVQRG",
        "Arn": "arn:aws:iam::262412591366:role/AWSResilienceHubAssessmentRole2",
        "CreateDate": "2023-08-02T07:49:23+00:00",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Principal": {
                        "AWS": [
                            "arn:aws:iam::262412591366:role/
AWSResilienceHubAssessmentRole"
                        ]
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        }
    }
}
```

Sampel **`attach-policy-to-role`**

`aws iam attach-role-policy --role-name AWSResilienceHubAssessmentRole --policy-arn arn:aws:iam::aws:policy/AWSResilienceHubAsssessmentExecutionPolicy`.

Menggunakan izin IAM pengguna saat ini

Gunakan metode ini jika Anda ingin menggunakan izin IAM pengguna saat ini untuk membuat dan menjalankan penilaian. Anda dapat melampirkan kebijakan `AWSResilienceHubAsssessmentExecutionPolicy` terkelola ke IAM pengguna atau Peran yang terkait dengan pengguna Anda.

Penyiapan akun tunggal

Menggunakan kebijakan terkelola yang disebutkan di atas sudah cukup untuk menjalankan penilaian pada aplikasi yang dikelola di akun yang sama dengan IAM pengguna.

Pengaturan penilaian terjadwal

Anda harus membuat peran baru `AwsResilienceHubPeriodicAssessmentRole` agar dapat AWS Resilience Hub melakukan tugas terkait penilaian terjadwal.

> **Note**
>
> - Saat menggunakan akses berbasis peran (dengan peran invoker yang disebutkan di atas) langkah ini tidak diperlukan.
> - Nama peran harus`AwsResilienceHubPeriodicAssessmentRole`.

Untuk memungkinkan AWS Resilience Hub untuk melakukan tugas terkait penilaian terjadwal

1. Lampirkan kebijakan yang `AWSResilienceHubAsssessmentExecutionPolicy` dikelola ke peran.
2. Tambahkan kebijakan berikut, di `primary_account_id` mana AWS akun tempat aplikasi didefinisikan dan akan menjalankan penilaian. Selain itu, Anda harus menambahkan kebijakan kepercayaan terkait untuk peran penilaian terjadwal, (`AwsResilienceHubPeriodicAssessmentRole`), yang memberikan izin bagi AWS Resilience Hub layanan untuk mengambil peran penilaian terjadwal.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetRole",
        "sts:AssumeRole"
      ],
      "Resource": "arn:aws:iam::primary_account_id:role/
AwsResilienceHubAdminAccountRole"
    },
```

```
    {
      "Effect": "Allow",
      "Action": [
        "sts:AssumeRole"
      ],
      "Resource": [
        "arn:aws:iam::primary_account_id:role/
AwsResilienceHubAssessmentEKSAccessRole"
      ]
    }
  ]
}
```

Kebijakan kepercayaan untuk peran penilaian terjadwal (**`AwsResilienceHubPeriodicAssessmentRole`**)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "resiliencehub.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Penyiapan lintas akun

Kebijakan IAM izin berikut diperlukan jika Anda menggunakan AWS Resilience Hub dengan beberapa akun. Setiap AWS akun mungkin memerlukan izin yang berbeda tergantung pada kasus penggunaan Anda. Saat menyiapkan AWS Resilience Hub akses lintas akun, akun dan peran berikut dipertimbangkan:

- Akun utama — AWS akun tempat Anda ingin membuat aplikasi dan menjalankan penilaian.
- Akun Sekunder/Sumber Daya — AWS akun tempat sumber daya berada.

> **Note**
>
> - Saat menggunakan akses berbasis peran (dengan peran invoker yang disebutkan di atas) langkah ini tidak diperlukan.
> - Untuk informasi selengkapnya tentang mengonfigurasi izin untuk mengakses Amazon Elastic Kubernetes Service, lihat. the section called “Mengaktifkan AWS Resilience Hub akses ke klaster Amazon EKS Anda”

Penyiapan akun utama

Anda harus membuat peran baru `AwsResilienceHubAdminAccountRole` di akun utama dan mengaktifkan AWS Resilience Hub akses untuk menganggapnya. Peran ini akan digunakan untuk mengakses peran lain di AWS akun Anda yang berisi sumber daya Anda. Seharusnya tidak memiliki izin untuk membaca sumber daya.

> **Note**
>
> - Nama peran harus`AwsResilienceHubAdminAccountRole`.
> - Itu harus dibuat di akun utama.
> - IAMPengguna/peran Anda saat ini harus memiliki `iam:assumeRole` izin untuk mengambil peran ini.
> - Ganti `secondary_account_id_1/2/...` dengan pengidentifikasi akun sekunder yang relevan.

Kebijakan berikut memberikan izin pelaksana untuk peran Anda untuk mengakses sumber daya di peran lain di akun Anda: AWS

```
{
  {
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Resource": [
        "arn:aws:iam::secondary_account_id_1:role/AwsResilienceHubExecutorAccountRole",
        "arn:aws:iam::secondary_account_id_2:role/AwsResilienceHubExecutorAccountRole",
```

```
        ...
      ],
      "Action": [
        "sts:AssumeRole"
      ]
    }
  ]
}
```

Kebijakan kepercayaan untuk peran admin (`AwsResilienceHubAdminAccountRole`) adalah sebagai berikut:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::primary_account_id:role/caller_IAM_role"
      },
      "Action": "sts:AssumeRole"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::primary_account_id:role/
AwsResilienceHubPeriodicAssessmentRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Pengaturan akun Sekunder/Sumber Daya

Di setiap akun sekunder, Anda harus membuat yang baru `AwsResilienceHubExecutorAccountRole` dan mengaktifkan peran admin yang dibuat di atas untuk mengambil peran ini. Karena peran ini akan digunakan oleh AWS Resilience Hub untuk memindai dan menilai sumber daya aplikasi Anda, itu juga akan memerlukan izin yang sesuai.

Namun, Anda harus melampirkan kebijakan `AWSResilienceHubAsssessmentExecutionPolicy` terkelola ke peran dan melampirkan kebijakan peran pelaksana.

Kebijakan kepercayaan peran pelaksana adalah sebagai berikut:

```
{
  {
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::primary_account_id:role/AwsResilienceHubAdminAccountRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

AWS kebijakan terkelola untuk AWS Resilience Hub

Kebijakan AWS terkelola adalah kebijakan mandiri yang dibuat dan dikelola oleh AWS. AWS Kebijakan terkelola dirancang untuk memberikan izin bagi banyak kasus penggunaan umum sehingga Anda dapat mulai menetapkan izin kepada pengguna, grup, dan peran.

Perlu diingat bahwa kebijakan AWS terkelola mungkin tidak memberikan izin hak istimewa paling sedikit untuk kasus penggunaan spesifik Anda karena tersedia untuk digunakan semua pelanggan. AWS Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola pelanggan yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ditentukan dalam kebijakan AWS terkelola. Jika AWS memperbarui izin yang ditentukan dalam kebijakan AWS terkelola, pembaruan akan memengaruhi semua identitas utama (pengguna, grup, dan peran) yang dilampirkan kebijakan tersebut. AWS kemungkinan besar akan memperbarui kebijakan AWS terkelola saat baru AWS layanan diluncurkan atau API operasi baru tersedia untuk layanan yang ada.

Untuk informasi selengkapnya, lihat kebijakan AWS terkelola di Panduan IAM Pengguna.

AWSResilienceHubAsssessmentExecutionPolicy

Anda dapat melampirkan `AWSResilienceHubAsssessmentExecutionPolicy` ke IAM identitas Anda. Saat menjalankan penilaian, kebijakan ini memberikan izin akses ke AWS layanan lain untuk menjalankan penilaian.

Detail izin

Kebijakan ini memberikan izin yang memadai untuk memublikasikan alarm, AWS FIS dan SOP templat ke bucket Amazon Simple Storage Service (Amazon S3). Nama bucket Amazon S3 harus dimulai dengan. `aws-resilience-hub-artifacts-` Jika Anda ingin mempublikasikan ke bucket Amazon S3 lain, Anda dapat melakukannya saat menelepon. `CreateRecommendationTemplate` API Untuk informasi lebih lanjut, lihat CreateRecommendationTemplate.

Kebijakan ini mencakup izin berikut:

- Amazon CloudWatch (CloudWatch) - Mendapatkan semua alarm yang diterapkan yang Anda atur di Amazon CloudWatch untuk memantau aplikasi. Selain itu, kami gunakan `cloudwatch:PutMetricData` untuk mempublikasikan CloudWatch metrik untuk skor ketahanan aplikasi di namespace. `ResilienceHub`
- Amazon Data Lifecycle Manager — Mendapat dan menyediakan `Describe` izin untuk sumber daya Amazon Data Lifecycle Manager yang terkait dengan akun Anda. AWS
- Amazon DevOps Guru - Mendaftar dan memberikan `Describe` izin untuk sumber daya Amazon DevOps Guru yang terkait dengan AWS akun Anda.
- Amazon DocumentDB — Daftar dan `Describe` menyediakan izin untuk sumber daya Amazon DocumentDB yang terkait dengan akun Anda. AWS
- Amazon DynamoDB (DynamoDB) - Mendaftar dan memberikan `Describe` izin untuk sumber daya Amazon DynamoDB yang terkait dengan akun Anda. AWS
- Amazon ElastiCache (ElastiCache) — Menyediakan `Describe` izin untuk ElastiCache sumber daya yang terkait dengan AWS akun Anda.
- Amazon Elastic Compute Cloud (AmazonEC2) - Mendaftar dan memberikan `Describe` izin untuk EC2 sumber daya Amazon yang terkait dengan akun Anda AWS .
- Amazon Elastic Container Registry (AmazonECR) - Menyediakan `Describe` izin untuk ECR sumber daya Amazon yang terkait dengan AWS akun Anda.
- Amazon Elastic Container Service (AmazonECS) - Menyediakan `Describe` izin untuk ECS sumber daya Amazon yang terkait dengan AWS akun Anda.

- Amazon Elastic File System (AmazonEFS) - Menyediakan `Describe` izin untuk EFS sumber daya Amazon yang terkait dengan AWS akun Anda.
- Amazon Elastic Kubernetes Service (EKSAmazon) - Mendaftar dan `Describe` memberikan izin untuk sumber daya EKS Amazon yang terkait dengan akun Anda. AWS
- Amazon EC2 Auto Scaling — Mendaftarkan dan memberikan `Describe` izin untuk sumber daya Amazon EC2 Auto Scaling yang terkait dengan akun Anda. AWS
- Amazon EC2 Systems Manager (SSM) — Menyediakan `Describe` izin untuk SSM sumber daya yang terkait dengan AWS akun Anda.
- Amazon Fault Injection Service (AWS FIS) - Mendaftar dan memberikan `Describe` izin untuk AWS FIS eksperimen dan templat eksperimen yang terkait dengan AWS akun Anda.
- Amazon FSx untuk Windows File Server (AmazonFSx) - Daftar dan menyediakan `Describe` izin untuk FSx sumber daya Amazon yang terkait dengan AWS akun Anda.
- Amazon RDS — Daftar dan memberikan `Describe` izin untuk RDS sumber daya Amazon yang terkait dengan AWS akun Anda.
- Amazon Route 53 (Route 53) - Mendaftar dan memberikan `Describe` izin untuk sumber daya Route 53 yang terkait dengan AWS akun Anda.
- Amazon Route 53 Resolver — Daftar dan memberikan `Describe` izin untuk Amazon Route 53 Resolver sumber daya yang terkait dengan AWS akun Anda.
- Amazon Simple Notification Service (AmazonSNS) — Daftar dan memberikan `Describe` izin untuk SNS sumber daya Amazon yang terkait dengan AWS akun Anda.
- Amazon Simple Queue Service (AmazonSQS) — Daftar dan memberikan `Describe` izin untuk SQS sumber daya Amazon yang terkait dengan akun Anda AWS .
- Amazon Simple Storage Service (Amazon S3) - Mendaftar dan `Describe` memberikan izin untuk sumber daya Amazon S3 yang terkait dengan akun Anda. AWS

> **Note**
>
> Saat menjalankan penilaian, jika ada izin yang hilang yang perlu diperbarui dari kebijakan Terkelola, penilaian AWS Resilience Hub akan berhasil menyelesaikan penilaian menggunakan izin s3:GetBucketLogging . Namun, AWS Resilience Hub akan menampilkan pesan peringatan yang mencantumkan izin yang hilang dan akan memberikan masa tenggang untuk menambahkan yang sama. Jika Anda tidak menambahkan izin yang hilang dalam masa tenggang yang ditentukan, penilaian akan gagal.

- AWS Backup — Daftar dan dapatkan `Describe` izin untuk sumber daya Amazon EC2 Auto Scaling yang terkait dengan AWS akun Anda.
- AWS CloudFormation — Daftar dan dapatkan `Describe` izin untuk sumber daya pada AWS CloudFormation tumpukan yang terkait dengan akun Anda AWS .
- AWS DataSync — Daftar dan memberikan `Describe` izin untuk AWS DataSync sumber daya yang terkait dengan AWS akun Anda.
- AWS Directory Service — Daftar dan memberikan `Describe` izin untuk AWS Directory Service sumber daya yang terkait dengan AWS akun Anda.
- AWS Elastic Disaster Recovery (Elastic Disaster Recovery) - Memberikan `Describe` izin untuk sumber daya Pemulihan Bencana Elastis yang terkait dengan AWS akun Anda.
- AWS Lambda (Lambda) — Daftar dan memberikan `Describe` izin untuk sumber daya Lambda yang terkait dengan akun Anda. AWS
- AWS Resource Groups (Resource Groups) — Daftar dan memberikan `Describe` izin untuk sumber daya Resource Groups yang terkait dengan AWS akun Anda.
- AWS Service Catalog (Service Catalog) — Daftar dan memberikan `Describe` izin untuk sumber daya Service Catalog yang terkait dengan AWS akun Anda.
- AWS Step Functions — Daftar dan memberikan `Describe` izin untuk AWS Step Functions sumber daya yang terkait dengan AWS akun Anda.
- Elastic Load Balancing — Daftar dan memberikan `Describe` izin untuk sumber daya Elastic Load Balancing yang terkait dengan akun Anda. AWS
- `ssm:GetParametersByPath`— Kami menggunakan izin ini untuk mengelola CloudWatch alarm, pengujian, atau SOPs yang dikonfigurasi untuk aplikasi Anda.

IAMKebijakan berikut diperlukan agar AWS akun dapat menambahkan izin bagi pengguna, grup pengguna, dan peran yang memberikan izin yang diperlukan bagi tim Anda untuk mengakses AWS layanan saat menjalankan penilaian.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSResilienceHubFullResourceStatement",
            "Effect": "Allow",
            "Action": [
                "application-autoscaling:DescribeScalableTargets",
                "autoscaling:DescribeAutoScalingGroups",
```

```
                "backup:DescribeBackupVault",
                "backup:GetBackupPlan",
                "backup:GetBackupSelection",
                "backup:ListBackupPlans",
                "backup:ListBackupSelections",
                "cloudformation:DescribeStacks",
                "cloudformation:ListStackResources",
                "cloudformation:ValidateTemplate",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:GetMetricData",
                "cloudwatch:GetMetricStatistics",
                "datasync:DescribeTask",
                "datasync:ListLocations",
                "datasync:ListTasks",
                "devops-guru:ListMonitoredResources",
                "dlm:GetLifecyclePolicies",
                "dlm:GetLifecyclePolicy",
                "docdb-elastic:GetCluster",
                "docdb-elastic:GetClusterSnapshot",
                "docdb-elastic:ListClusterSnapshots",
                "docdb-elastic:ListTagsForResource",
                "drs:DescribeJobs",
                "drs:DescribeSourceServers",
                "drs:GetReplicationConfiguration",
                "ds:DescribeDirectories",
                "dynamodb:DescribeContinuousBackups",
                "dynamodb:DescribeGlobalTable",
                "dynamodb:DescribeLimits",
                "dynamodb:DescribeTable",
                "dynamodb:ListGlobalTables",
                "dynamodb:ListTagsOfResource",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeFastSnapshotRestores",
                "ec2:DescribeFleets",
                "ec2:DescribeHosts",
                "ec2:DescribeInstances",
                "ec2:DescribeNatGateways",
                "ec2:DescribePlacementGroups",
                "ec2:DescribeRegions",
                "ec2:DescribeSnapshots",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeVolumes",
                "ec2:DescribeVpcEndpoints",
```

```
                "ecr:DescribeRegistry",
                "ecs:DescribeCapacityProviders",
                "ecs:DescribeClusters",
                "ecs:DescribeContainerInstances",
                "ecs:DescribeServices",
                "ecs:DescribeTaskDefinition",
                "ecs:ListContainerInstances",
                "ecs:ListServices",
                "eks:DescribeCluster",
                "eks:DescribeFargateProfile",
                "eks:DescribeNodegroup",
                "eks:ListFargateProfiles",
                "eks:ListNodegroups",
                "elasticache:DescribeCacheClusters",
                "elasticache:DescribeGlobalReplicationGroups",
                "elasticache:DescribeReplicationGroups",
                "elasticache:DescribeSnapshots",
                "elasticfilesystem:DescribeFileSystems",
                "elasticfilesystem:DescribeLifecycleConfiguration",
                "elasticfilesystem:DescribeMountTargets",
                "elasticfilesystem:DescribeReplicationConfigurations",
                "elasticloadbalancing:DescribeListeners",
                "elasticloadbalancing:DescribeLoadBalancers",
                "elasticloadbalancing:DescribeTargetGroups",
                "elasticloadbalancing:DescribeTargetHealth",
                "fis:GetExperimentTemplate",
                "fis:ListExperimentTemplates",
                "fis:ListExperiments",
                "fsx:DescribeFileSystems",
                "lambda:GetFunctionConcurrency",
                "lambda:GetFunctionConfiguration",
                "lambda:ListAliases",
                "lambda:ListEventSourceMappings",
                "lambda:ListFunctionEventInvokeConfigs",
                "lambda:ListVersionsByFunction",
                "rds:DescribeDBClusterSnapshots",
                "rds:DescribeDBClusters",
                "rds:DescribeDBInstanceAutomatedBackups",
                "rds:DescribeDBInstances",
                "rds:DescribeDBProxies",
                "rds:DescribeDBProxyTargets",
                "rds:DescribeDBSnapshots",
                "rds:DescribeGlobalClusters",
                "rds:ListTagsForResource",
```

```
                "resource-groups:GetGroup",
                "resource-groups:ListGroupResources",
                "route53-recovery-control-config:ListClusters",
                "route53-recovery-control-config:ListControlPanels",
                "route53-recovery-control-config:ListRoutingControls",
                "route53-recovery-readiness:GetReadinessCheckStatus",
                "route53-recovery-readiness:GetResourceSet",
                "route53-recovery-readiness:ListReadinessChecks",
                "route53:GetHealthCheck",
                "route53:ListHealthChecks",
                "route53:ListHostedZones",
                "route53:ListResourceRecordSets",
                "route53resolver:ListResolverEndpoints",
                "route53resolver:ListResolverEndpointIpAddresses",
                "s3:ListBucket",
                "servicecatalog:GetApplication",
                "servicecatalog:ListAssociatedResources",
                "sns:GetSubscriptionAttributes",
                "sns:GetTopicAttributes",
                "sns:ListSubscriptionsByTopic",
                "sqs:GetQueueAttributes",
                "sqs:GetQueueUrl",
                "ssm:DescribeAutomationExecutions",
                "states:DescribeStateMachine",
                "states:ListStateMachineVersions",
                "states:ListStateMachineAliases",
                "tag:GetResources"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AWSResilienceHubApiGatewayStatement",
            "Effect": "Allow",
            "Action": [
                "apigateway:GET"
            ],
            "Resource": [
                "arn:aws:apigateway:*::/apis/*",
                "arn:aws:apigateway:*::/restapis/*",
                "arn:aws:apigateway:*::/usageplans"
            ]
        },
        {
            "Sid": "AWSResilienceHubS3ArtifactStatement",
```

```
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:PutObject",
                "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:::aws-resilience-hub-artifacts-*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        },
        {
            "Sid": "AWSResilienceHubS3AccessStatement",
            "Effect": "Allow",
            "Action": [
                "s3:GetBucketLocation",
                "s3:GetBucketLogging",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketTagging",
                "s3:GetBucketVersioning",
                "s3:GetMultiRegionAccessPointRoutes",
                "s3:GetReplicationConfiguration",
                "s3:ListAllMyBuckets",
                "s3:ListMultiRegionAccessPoints"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        },
        {
            "Sid": "AWSResilienceHubCloudWatchStatement",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
```

```
                    "cloudwatch:namespace": "ResilienceHub"
                }
            }
        },
        {
            "Sid": "AWSResilienceHubSSMStatement",
            "Effect": "Allow",
            "Action": [
                "ssm:GetParametersByPath"
            ],
            "Resource": "arn:aws:ssm:*:*:parameter/ResilienceHub/*"
        }
    ]
}
```

AWS Resilience Hub pembaruan kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola AWS Resilience Hub sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan RSS feed di halaman Riwayat AWS Resilience Hub dokumen.

Perubahan	Deskripsi	Tanggal
AWSResilienceHubAssessmentExecutionPolicy—Ubah	AWS Resilience Hub diperbarui `AWSResilienceHubAsssessmentExecutionPolicy` untuk memberikan `Describe` izin agar Anda dapat mengakses sumber daya dan konfigurasi di Amazon DocumentDB, Elastic Load Balancing, dan saat menjalankan penilaian. AWS Lambda	Agustus 01, 2024
AWSResilienceHubAssessmentExecutionPolicy—Ubah	AWS Resilience Hub diperbarui `AWSResilienceHubAsssessment`	Maret 26, 2024

Perubahan	Deskripsi	Tanggal
	`ExecutionPolicy` untuk memberikan `Describe` izin agar Anda dapat membaca konfigurasi Amazon FSx untuk Windows File Server saat menjalankan penilaian.	
AWSResilienceHubAssessmentExecutionPolicy—Ubah	AWS Resilience Hub diperbarui `AWSResilienceHubAsssessment ExecutionPolicy` untuk memberikan `Describe` izin agar Anda dapat membaca AWS Step Functions konfigurasi saat menjalankan penilaian.	30 Oktober 2023
AWSResilienceHubAssessmentExecutionPolicy—Ubah	AWS Resilience Hub diperbarui `AWSResilienceHubAsssessment ExecutionPolicy` untuk memberikan `Describe` izin agar Anda dapat mengakses sumber daya di Amazon RDS saat menjalankan penilaian.	5 Oktober 2023
AWSResilienceHubAssessmentExecutionPolicy—Baru	AWS Resilience Hub Kebijakan ini menyediakan akses ke AWS layanan lain untuk menjalankan penilaian.	26 Juni 2023
AWS Resilience Hub mulai melacak perubahan	AWS Resilience Hub mulai melacak perubahan untuk kebijakan yang AWS dikelola.	15 Juni 2023

AWS Resilience Hub referensi persona dan IAM izin

Anda dapat memberikan IAM izin kepada persona yang diperlukan untuk bekerja AWS Resilience Hub dengan menggunakan kebijakan `AWSResilienceHubAsssessmentExecutionPolicy` AWS terkelola dan salah satu kebijakan khusus persona berikut. Untuk informasi selengkapnya tentang kebijakan AWS terkelola, lihatthe section called “AWSResilienceHubAsssessmentExecutionPolicy”.

Kebijakan untuk persona yang disarankan oleh AWS Resilience Hub:

- IAMizin untuk persona manajer aplikasi Infrastruktur
- IAMizin untuk persona manajer kontinuitas bisnis
- IAMizin untuk persona pemilik Aplikasi
- IAMizin untuk memberikan akses hanya-baca

IAMizin untuk persona manajer aplikasi Infrastruktur

Kebijakan berikut memberikan izin yang diperlukan untuk persona manajer aplikasi Infrastruktur.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "InfrastructureApplicationManager",
      "Effect": "Allow",
      "Action": [
        "resiliencehub:AddDraftAppVersionResourceMappings",
        "resiliencehub:CreateAppVersionAppComponent",
        "resiliencehub:CreateAppVersionResource",
        "resiliencehub:CreateRecommendationTemplate",
        "resiliencehub:DeleteAppAssessment",
        "resiliencehub:DeleteAppInputSource",
        "resiliencehub:DeleteAppVersionAppComponent",
        "resiliencehub:DeleteAppVersionResource",
        "resiliencehub:DeleteRecommendationTemplate",
        "resiliencehub:Describe*",
        "resiliencehub:List*",
        "resiliencehub:PublishAppVersion",
        "resiliencehub:PutDraftAppVersionTemplate",
        "resiliencehub:RemoveDraftAppVersionResourceMappings",
        "resiliencehub:ResolveAppVersionResources",
        "resiliencehub:StartAppAssessment",
```

```
        "resiliencehub:TagResource",
        "resiliencehub:UntagResource",
        "resiliencehub:UpdateAppVersion",
        "resiliencehub:UpdateAppVersionAppComponent",
        "resiliencehub:UpdateAppVersionResource"
      ],
      "Resource": "*"
    }
  ]
}
```

IAMizin untuk persona manajer kontinuitas bisnis

Kebijakan berikut memberikan izin yang diperlukan untuk persona manajer kontinuitas Bisnis.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "BusinessContinuityManager",
      "Effect": "Allow",
      "Action": [
        "resiliencehub:CreateResiliencyPolicy",
        "resiliencehub:DeleteResiliencyPolicy",
        "resiliencehub:Describe*",
        "resiliencehub:List*",
        "resiliencehub:ResolveAppVersionResources",
        "resiliencehub:TagResource",
        "resiliencehub:UntagResource",
        "resiliencehub:UpdateAppVersion",
        "resiliencehub:UpdateAppVersionAppComponent",
        "resiliencehub:UpdateAppVersionResource",
        "resiliencehub:UpdateResiliencyPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

IAMizin untuk persona pemilik Aplikasi

Kebijakan berikut memberikan izin yang diperlukan untuk persona pemilik Aplikasi.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ApplicationOwner",
      "Effect": "Allow",
      "Action": [
        "resiliencehub:AddDraftAppVersionResourceMappings",
        "resiliencehub:BatchUpdateRecommendationStatus",
        "resiliencehub:CreateApp",
        "resiliencehub:CreateAppVersionAppComponent",
        "resiliencehub:CreateAppVersionResource",
        "resiliencehub:CreateRecommendationTemplate",
        "resiliencehub:CreateResiliencyPolicy",
        "resiliencehub:DeleteApp",
        "resiliencehub:DeleteAppAssessment",
        "resiliencehub:DeleteAppInputSource",
        "resiliencehub:DeleteAppVersionAppComponent",
        "resiliencehub:DeleteAppVersionResource",
        "resiliencehub:DeleteRecommendationTemplate",
        "resiliencehub:DeleteResiliencyPolicy",
        "resiliencehub:Describe*",
        "resiliencehub:ImportResourcesToDraftAppVersion",
        "resiliencehub:List*",
        "resiliencehub:PublishAppVersion",
        "resiliencehub:PutDraftAppVersionTemplate",
        "resiliencehub:RemoveDraftAppVersionResourceMappings",
        "resiliencehub:ResolveAppVersionResources",
        "resiliencehub:StartAppAssessment",
        "resiliencehub:TagResource",
        "resiliencehub:UntagResource",
        "resiliencehub:UpdateApp",
        "resiliencehub:UpdateAppVersion",
        "resiliencehub:UpdateAppVersionAppComponent",
        "resiliencehub:UpdateAppVersionResource",
        "resiliencehub:UpdateResiliencyPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

IAMizin untuk memberikan akses hanya-baca

Kebijakan berikut memberikan izin yang diperlukan untuk akses hanya-baca.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReadOnly",
      "Effect": "Allow",
      "Action": [
        "resiliencehub:Describe*",
        "resiliencehub:List*",
        "resiliencehub:ResolveAppVersionResources"
      ],
      "Resource": "*"
    }
  ]
}
```

Mengimpor file status Terraform ke AWS Resilience Hub

AWS Resilience Hub mendukung pengimporan file status Terraform yang dienkripsi menggunakan enkripsi sisi server () dengan kunci terkelola Amazon Simple Storage Service (-S3SSE) atau dengan kunci terkelola SSE (-). AWS Key Management Service SSE KMS Jika file status Terraform Anda dienkripsi menggunakan kunci enkripsi yang disediakan pelanggan (SSE-C), Anda tidak akan dapat mengimpornya menggunakan. AWS Resilience Hub

Mengimpor file status Terraform ke dalam AWS Resilience Hub memerlukan IAM kebijakan berikut tergantung di mana file status Anda berada.

Mengimpor file status Terraform dari bucket Amazon S3 yang terletak di akun utama

Kebijakan dan IAM kebijakan bucket Amazon S3 berikut diperlukan untuk mengizinkan akses AWS Resilience Hub baca ke file status Terraform Anda yang terletak di bucket Amazon S3 di akun utama.

- Kebijakan Bucket — Kebijakan bucket pada bucket Amazon S3 target, yang terletak di akun utama. Untuk informasi selengkapnya, lihat contoh berikut.

  ```
  {
  ```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::<s3-bucket-name>/<path-to-state-file>"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::<s3-bucket-name>"
    }
  ]
}
```

- Kebijakan identitas — Kebijakan identitas terkait untuk peran Invoker yang ditentukan untuk aplikasi ini, atau IAM peran AWS saat ini AWS Resilience Hub di AWS akun utama. Untuk informasi selengkapnya, lihat contoh berikut.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::<s3-bucket-name>/<path-to-state-file>"
    },
    {
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::<s3-bucket-name>"
    }
  ]
}
```

> **Note**
>
> Jika Anda menggunakan kebijakan `AWSResilienceHubAsssessmentExecutionPolicy` terkelola, `ListBucket` izin tidak diperlukan.

> **Note**
>
> Jika file status Terraform Anda dienkripsi menggunakanKMS, Anda harus menambahkan izin berikut. `kms:Decrypt`

```
{
      "Effect": "Allow",
      "Action": [
              "kms:Decrypt",
      ],
      "Resource": "<arn_of_kms_key>"
}
```

Mengimpor file status Terraform dari bucket Amazon S3 yang terletak di akun sekunder

- Kebijakan Bucket — Kebijakan bucket pada bucket Amazon S3 target, yang terletak di salah satu akun sekunder. Untuk informasi selengkapnya, lihat contoh berikut.

```
 {
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::<bucket-with-statefile-in-secondary-account>/<path-
to-state-file>"
```

```
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::<bucket-with-statefile-in-secondary-account>"
    }
  ]
}
```

- Kebijakan identitas — Kebijakan identitas terkait untuk peran AWS akun, yang berjalan AWS Resilience Hub di AWS akun utama. Untuk informasi selengkapnya, lihat contoh berikut.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::<bucket-with-statefile-in-secondary-account>/<path-
to-state-file>"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<primary-account>:role/<invoker-role-or-current-iam-
role>"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::<bucket-with-statefile-in-secondary-account>"
    }
  ]
}
```

> **Note**
>
> Jika Anda menggunakan kebijakan `AWSResilienceHubAsssessmentExecutionPolicy` terkelola, `ListBucket` izin tidak diperlukan.

> **Note**
>
> Jika file status Terraform Anda dienkripsi menggunakanKMS, Anda harus menambahkan izin berikut. `kms:Decrypt`

```
{
      "Effect": "Allow",
      "Action": [
              "kms:Decrypt",
      ],
      "Resource": "<arn_of_kms_key>"
}
```

Mengaktifkan AWS Resilience Hub akses ke klaster Amazon Elastic Kubernetes Service

AWS Resilience Hub menilai ketahanan klaster Amazon Elastic Kubernetes Service EKS (Amazon) dengan menganalisis infrastruktur klaster Amazon Anda. EKS AWS Resilience Hub menggunakan konfigurasi access control (RBAC) berbasis peran Kubernetes untuk menilai beban kerja Kubernetes (K8s) lainnya, yang digunakan sebagai bagian dari klaster Amazon. EKS AWS Resilience Hub Untuk menanyakan EKS klaster Amazon Anda untuk menganalisis dan menilai beban kerja, Anda harus menyelesaikan yang berikut ini:

- Buat atau gunakan peran AWS Identity and Access Management (IAM) yang ada di akun yang sama dengan EKS klaster Amazon.
- Aktifkan akses IAM pengguna dan peran ke EKS klaster Amazon Anda dan berikan izin hanya-baca tambahan ke sumber daya K8s di dalam klaster Amazon. EKS Untuk informasi selengkapnya

tentang mengaktifkan akses IAM pengguna dan peran ke EKS klaster Amazon Anda, lihat Mengaktifkan akses IAM pengguna dan peran ke klaster Anda - Amazon. EKS

Akses ke EKS klaster Amazon Anda menggunakan IAM entitas diaktifkan oleh AWS IAMAuthenticator for Kubernetes, yang berjalan di bidang kontrol Amazon. EKS Authenticator memperoleh informasi konfigurasi dari. `aws-auth ConfigMap`

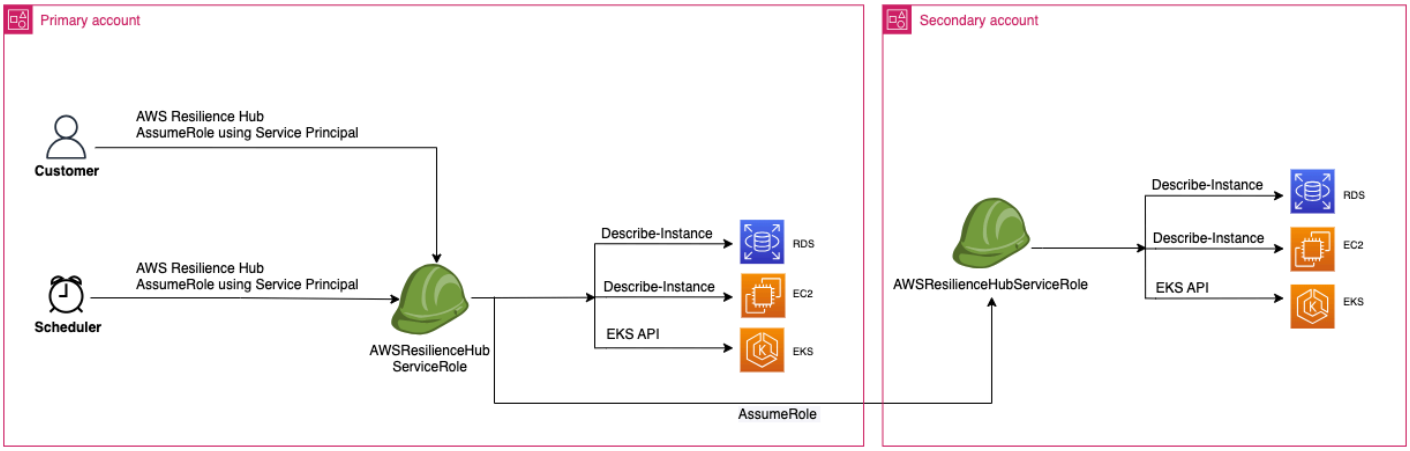
> **Note**
>
> - Untuk informasi selengkapnya tentang semua `aws-auth ConfigMap` pengaturan, lihat Format Konfigurasi Lengkap aktif GitHub.
> - Untuk informasi selengkapnya tentang IAM identitas yang berbeda, lihat Identitas (Pengguna, Grup, dan Peran) di IAM Panduan Pengguna.
> - Untuk informasi selengkapnya tentang konfigurasi access control (RBAC) berbasis peran Kubernetes, lihat Menggunakan Otorisasi. RBAC

AWS Resilience Hub kueri sumber daya di dalam EKS klaster Amazon Anda menggunakan IAM peran di akun Anda. AWS Resilience Hub Untuk mengakses sumber daya dalam EKS klaster Amazon Anda, IAM peran yang digunakan oleh AWS Resilience Hub harus dipetakan ke grup Kubernetes dengan izin hanya-baca yang memadai untuk sumber daya di dalam klaster Amazon Anda. EKS

AWS Resilience Hub memungkinkan untuk mengakses sumber daya EKS klaster Amazon Anda dengan menggunakan salah satu opsi IAM peran berikut:

- Jika aplikasi Anda dikonfigurasi untuk menggunakan akses berbasis peran untuk mengakses sumber daya, peran invoker atau peran akun sekunder yang diteruskan ke AWS Resilience Hub saat membuat aplikasi akan digunakan untuk mengakses klaster Amazon Anda selama penilaian. EKS

  Diagram konseptual berikut menunjukkan bagaimana AWS Resilience Hub mengakses EKS kluster Amazon ketika aplikasi dikonfigurasi sebagai aplikasi berbasis peran.



- Jika aplikasi Anda dikonfigurasi untuk menggunakan IAM pengguna saat ini untuk mengakses sumber daya, Anda harus membuat IAM peran baru dengan nama `AwsResilienceHubAssessmentEKSAccessRole` di akun yang sama dengan EKS klaster Amazon. IAMPeran ini kemudian akan digunakan untuk mengakses EKS cluster Amazon Anda.

  Diagram konseptual berikut menunjukkan cara AWS Resilience Hub mengakses EKS kluster Amazon yang diterapkan di akun utama Anda saat aplikasi dikonfigurasi untuk menggunakan izin pengguna saat ini. IAM

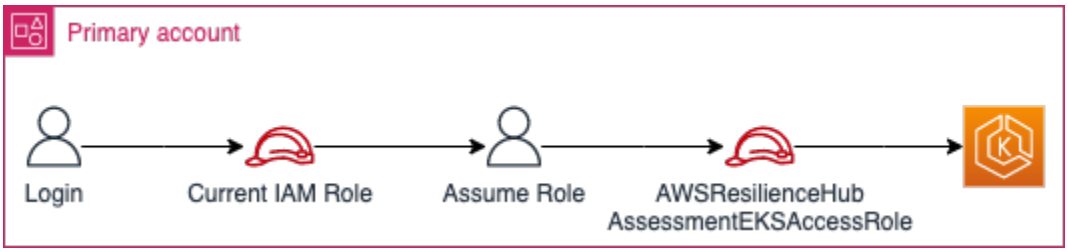
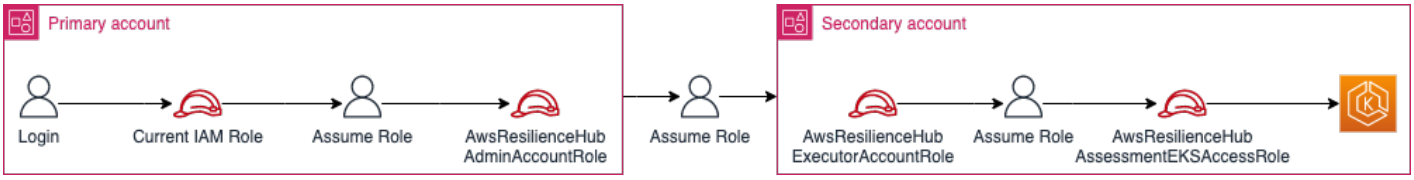


  Diagram konseptual berikut menunjukkan cara AWS Resilience Hub mengakses EKS kluster Amazon yang diterapkan pada akun sekunder saat aplikasi dikonfigurasi untuk menggunakan izin pengguna saat ini. IAM



Memberikan AWS Resilience Hub akses ke sumber daya di klaster Amazon EKS Anda

AWS Resilience Hub memungkinkan Anda mengakses sumber daya yang terletak di EKS kluster Amazon asalkan Anda telah mengonfigurasi izin yang diperlukan.

Untuk memberikan izin yang diperlukan AWS Resilience Hub untuk menemukan dan menilai sumber daya dalam klaster Amazon EKS

1. Konfigurasikan IAM peran untuk mengakses EKS klaster Amazon.

   Jika Anda telah mengonfigurasi aplikasi Anda menggunakan akses berbasis peran, Anda dapat melewati langkah ini dan melanjutkan ke langkah 2 dan menggunakan peran yang telah Anda gunakan untuk membuat aplikasi. Untuk informasi selengkapnya tentang cara AWS Resilience Hub menggunakan IAM peran, lihatthe section called “Cara AWS kerja Resilience Hub IAM”.

   Jika Anda telah mengonfigurasi aplikasi menggunakan izin IAM pengguna saat ini, Anda harus membuat `AwsResilienceHubAssessmentEKSAccessRole` IAM peran di akun yang sama dengan EKS klaster Amazon. IAMPeran ini kemudian akan digunakan saat mengakses EKS cluster Amazon Anda.

   Saat mengimpor dan menilai aplikasi Anda, AWS Resilience Hub gunakan IAM peran untuk mengakses sumber daya di klaster Amazon EKS Anda. Peran ini harus dibuat di akun yang sama dengan EKS cluster Amazon Anda dan akan dipetakan dengan grup Kubernetes yang menyertakan izin yang diperlukan untuk AWS Resilience Hub menilai klaster Amazon Anda. EKS

   Jika EKS klaster Amazon Anda berada di akun yang sama dengan akun AWS Resilience Hub panggilan, peran harus dibuat menggunakan kebijakan IAM kepercayaan berikut. Dalam kebijakan IAM kepercayaan `caller_IAM_role` ini, digunakan dalam akun saat ini APIs untuk memanggil AWS Resilience Hub.

   > **Note**
   >
   > `caller_IAM_role`Ini adalah peran yang terkait dengan akun AWS pengguna Anda.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::eks_cluster_account_id:role/caller_IAM_role"
      },
      "Action": "sts:AssumeRole"
    }
```

```
  ]
}
```

Jika EKS klaster Amazon Anda berada di akun silang (akun yang berbeda dari akun AWS Resilience Hub panggilan), Anda harus membuat `AwsResilienceHubAssessmentEKSAccessRole` IAM peran menggunakan kebijakan IAM kepercayaan berikut:

> **Note**
>
> Sebagai prasyarat, untuk mengakses EKS klaster Amazon yang digunakan di akun yang berbeda dari akun AWS Resilience Hub pengguna, Anda harus mengonfigurasi akses multi-akun. Untuk informasi selengkapnya, silakan lihat

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::eks_cluster_account_id:role/
AwsResilienceHubExecutorRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

2. Buat `ClusterRole` dan `ClusterRoleBinding` (atau`RoleBinding`) peran untuk AWS Resilience Hub aplikasi.

   Membuat `ClusterRole` dan `ClusterRoleBinding` akan memberikan izin hanya-baca yang diperlukan AWS Resilience Hub untuk menganalisis dan menilai sumber daya yang merupakan bagian dari ruang nama tertentu di klaster Amazon Anda. EKS

   AWS Resilience Hub memungkinkan Anda membatasi aksesnya ke ruang nama Anda untuk menghasilkan penilaian ketahanan dengan menyelesaikan salah satu dari berikut ini:

   a. Berikan akses baca di semua ruang nama ke AWS Resilience Hub aplikasi.

AWS Resilience Hub Untuk menilai ketahanan sumber daya di semua ruang nama dalam EKS klaster Amazon, Anda harus membuat berikut dan. `ClusterRole` `ClusterRoleBinding`

- `resilience-hub-eks-access-cluster-role`(`ClusterRole`) — Menentukan izin yang diperlukan oleh AWS Resilience Hub untuk menilai klaster Amazon EKS Anda.
- `resilience-hub-eks-access-cluster-role-binding`(`ClusterRoleBinding`) — Mendefinisikan grup bernama `resilience-hub-eks-access-group` di EKS klaster Amazon Anda yang memberikan penggunanya, izin yang diperlukan untuk menjalankan penilaian ketahanan di. AWS Resilience Hub

Template untuk memberikan akses baca di semua ruang nama ke AWS Resilience Hub aplikasi adalah sebagai berikut:

```
cat << EOF | kubectl apply -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: resilience-hub-eks-access-cluster-role
rules:
- apiGroups:
    - ""
  resources:
    - pods
    - replicationcontrollers
    - nodes
  verbs:
    - get
    - list
- apiGroups:
    - apps
  resources:
    - deployments
    - replicasets
  verbs:
    - get
    - list
- apiGroups:
    - policy
```

```
  resources:
    - poddisruptionbudgets
  verbs:
    - get
    - list
- apiGroups:
    - autoscaling.k8s.io
  resources:
    - verticalpodautoscalers
  verbs:
    - get
    - list
- apiGroups:
    - autoscaling
  resources:
    - horizontalpodautoscalers
  verbs:
    - get
    - list
- apiGroups:
    - karpenter.sh
  resources:
    - provisioners
    - nodepools
  verbs:
    - get
    - list
- apiGroups:
    - karpenter.k8s.aws
  resources:
    - awsnodetemplates
    - ec2nodeclasses
  verbs:
    - get
    - list
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: resilience-hub-eks-access-cluster-role-binding
subjects:
  - kind: Group
    name: resilience-hub-eks-access-group
    apiGroup: rbac.authorization.k8s.io
```

```
roleRef:
  kind: ClusterRole
  name: resilience-hub-eks-access-cluster-role
  apiGroup: rbac.authorization.k8s.io
---
EOF
```

b. Memberikan AWS Resilience Hub akses untuk membaca ruang nama tertentu.

Anda dapat membatasi AWS Resilience Hub untuk mengakses sumber daya dalam satu set ruang nama tertentu menggunakan. `RoleBinding` Untuk mencapai ini, Anda harus membuat peran berikut:

- `ClusterRole`— AWS Resilience Hub Untuk mengakses sumber daya di ruang nama tertentu dalam EKS klaster Amazon dan menilai ketahanannya, Anda harus membuat peran berikut. `ClusterRole`
  - `resilience-hub-eks-access-cluster-role`— Menentukan izin yang diperlukan untuk menilai sumber daya dalam ruang nama tertentu.
  - `resilience-hub-eks-access-global-cluster-role`— Menentukan izin yang diperlukan untuk menilai sumber daya dengan cakupan klaster, yang tidak terkait dengan namespace tertentu, dalam kluster Amazon Anda. EKS AWS Resilience Hub memerlukan izin untuk mengakses sumber daya dengan cakupan klaster (seperti node) di EKS klaster Amazon Anda untuk menilai ketahanan aplikasi Anda.

  Template untuk membuat `ClusterRole` peran adalah sebagai berikut:

```
cat << EOF | kubectl apply -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: resilience-hub-eks-access-cluster-role
rules:
  - apiGroups:
      - ""
    resources:
      - pods
      - replicationcontrollers
    verbs:
      - get
      - list
```

```
  - apiGroups:
      - apps
    resources:
      - deployments
      - replicasets
    verbs:
      - get
      - list
  - apiGroups:
      - policy
    resources:
      - poddisruptionbudgets
    verbs:
      - get
      - list
  - apiGroups:
      - autoscaling.k8s.io
    resources:
      - verticalpodautoscalers
    verbs:
      - get
      - list
  - apiGroups:
      - autoscaling
    resources:
      - horizontalpodautoscalers
    verbs:
      - get
      - list

---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: resilience-hub-eks-access-global-cluster-role
rules:
  - apiGroups:
      - ""
    resources:
      - nodes
    verbs:
      - get
      - list
  - apiGroups:
```

```
      - karpenter.sh
    resources:
      - provisioners
      - nodepools
    verbs:
      - get
      - list
  - apiGroups:
      - karpenter.k8s.aws
    resources:
      - awsnodetemplates
      - ec2nodeclasses
    verbs:
      - get
      - list

---
EOF
```

- `RoleBinding`peran — Peran ini memberikan izin yang diperlukan AWS Resilience Hub untuk mengakses sumber daya dalam ruang nama tertentu. Artinya, Anda harus membuat `RoleBinding` peran di setiap namespace AWS Resilience Hub untuk mengaktifkan akses sumber daya dalam namespace yang diberikan.

  > **Note**
  >
  > Jika Anda menggunakan `ClusterAutoscaler` untuk penskalaan otomatis, Anda juga harus membuat `RoleBinding` di. `kube-system` Ini diperlukan untuk menilai Anda`ClusterAutoscaler`, yang merupakan bagian dari `kube-system` namespace.
  > Dengan melakukan ini, Anda akan memberikan izin AWS Resilience Hub yang diperlukan untuk menilai sumber daya di dalam `kube-system` namespace saat menilai klaster Amazon Anda. EKS

  Template untuk membuat `RoleBinding` peran adalah sebagai berikut:

```
cat << EOF | kubectl apply -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
```

```
metadata:
  name: resilience-hub-eks-access-cluster-role-binding
  namespace: <namespace>
subjects:
  - kind: Group
    name: resilience-hub-eks-access-group
    apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: resilience-hub-eks-access-cluster-role
  apiGroup: rbac.authorization.k8s.io

---
EOF
```

- `ClusterRoleBinding`peran — Peran ini memberikan izin yang diperlukan untuk AWS Resilience Hub mengakses sumber daya dengan cakupan kluster.

  Template untuk membuat `ClusterRoleBinding` peran adalah sebagai berikut:

```
cat << EOF | kubectl apply -f -
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: resilience-hub-eks-access-global-cluster-role-binding
subjects:
  - kind: Group
    name: resilience-hub-eks-access-group
    apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: resilience-hub-eks-access-global-cluster-role
  apiGroup: rbac.authorization.k8s.io

---
EOF
```

3. Perbarui `aws-auth ConfigMap` untuk memetakan `resilience-hub-eks-access-group` dengan IAM peran yang digunakan untuk mengakses EKS klaster Amazon.

Langkah ini membuat pemetaan antara IAM peran yang digunakan pada langkah 1 dengan grup Kubernetes yang dibuat pada langkah 2. Pemetaan ini memberikan izin untuk IAM peran untuk mengakses sumber daya di dalam klaster Amazon. EKS

> **Note**
>
> - `ROLE-NAME`mengacu pada IAM peran yang digunakan untuk mengakses EKS cluster Amazon.
>   - Jika aplikasi Anda dikonfigurasi untuk menggunakan akses berbasis peran, peran tersebut harus berupa peran invoker atau peran akun sekunder yang diteruskan AWS Resilience Hub saat membuat aplikasi.
>   - Jika aplikasi Anda dikonfigurasi untuk menggunakan IAM pengguna saat ini untuk mengakses sumber daya, itu harus menjadi. `AwsResilienceHubAssessmentEKSAccessRole`
> - `ACCOUNT-ID`harus menjadi ID AWS akun EKS cluster Amazon.

Anda dapat membuat `aws-auth ConfigMap` menggunakan salah satu cara berikut:

- Menggunakan `eksctl`

  Gunakan perintah berikut untuk memperbarui `aws-authConfigMap`:

  ```
  eksctl create iamidentitymapping \
   --cluster <cluster-name> \
   --region=<region-code> \
   --arn arn:aws:iam::<ACCOUNT-ID>:role/<ROLE-NAME>\
   --group resilience-hub-eks-access-group \
   --username AwsResilienceHubAssessmentEKSAccessRole
  ```

- Anda dapat mengedit secara manual `aws-auth ConfigMap` dengan menambahkan detail IAM peran ke `mapRoles` bagian data di `ConfigMap` bawah. Gunakan perintah berikut untuk mengedit file `aws-authConfigMap`.

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

  `mapRoles`bagian terdiri dari parameter berikut:

- `rolearn`— Nama Sumber Daya Amazon (ARN) dari IAM peran yang akan ditambahkan.
  - ARNSintaks —`arn:aws:iam::<ACCOUNT-ID>:role/<ROLE-NAME>`.
- `username`— Nama pengguna dalam Kubernetes untuk dipetakan ke role (). IAM `AwsResilienceHubAssessmentEKSAccessRole`
- `groups`— Nama grup harus cocok dengan nama grup yang dibuat pada Langkah 2 (`resilience-hub-eks-access-group`).

> **Note**
>
> Jika `mapRoles` bagian tidak ada, Anda harus menambahkan bagian ini secara manual.

Gunakan templat berikut untuk menambahkan detail IAM peran ke `mapRoles` bagian data di `ConfigMap` bawah.

```
- groups:
  - resilience-hub-eks-access-group
  rolearn: arn:aws:iam::<ACCOUNT-ID>:role/<ROLE-NAME>
  username: AwsResilienceHubAssessmentEKSAccessRole
```

Mengaktifkan AWS Resilience Hub untuk mempublikasikan ke topik Amazon Simple Notification Service

Bagian ini menjelaskan tentang cara mengaktifkan AWS Resilience Hub untuk mempublikasikan pemberitahuan tentang aplikasi ke topik Amazon Simple Notification Service (AmazonSNS) Anda. Untuk mendorong notifikasi ke SNS topik Amazon, pastikan Anda memiliki yang berikut:

- AWS Resilience Hub Aplikasi aktif.
- SNSTopik Amazon yang ada yang AWS Resilience Hub harus mengirim pemberitahuan. Untuk informasi selengkapnya tentang membuat SNS topik Amazon, lihat Membuat SNS topik Amazon.

Untuk mengaktifkan AWS Resilience Hub untuk mempublikasikan notifikasi ke SNS topik Amazon Anda, Anda harus memperbarui kebijakan akses SNS topik Amazon dengan yang berikut:

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowResilienceHubPublish",
      "Effect": "Allow",
      "Principal": {
        "Service": "resiliencehub.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account-id:topic-name"
    }
  ]
}
```

> **Note**
>
> Bila digunakan AWS Resilience Hub untuk memublikasikan pesan dari Wilayah keikutsertaan ke topik yang terletak di Wilayah yang diaktifkan secara default, Anda harus mengubah kebijakan sumber daya yang dibuat untuk SNS topik Amazon. Ubah nilai prinsipal dari `resiliencehub.amazonaws.com` ke`resiliencehub.<opt-in-region>.amazonaws.com`.

Jika Anda menggunakan SNS topik SSE Amazon Terenkripsi Sisi Server (), Anda harus memastikan bahwa AWS Resilience Hub memiliki `Decrypt` dan `GenerateDataKey` * akses ke kunci SNS enkripsi Amazon.

Untuk menyediakan `Decrypt` dan `GenerateDataKey*` mengakses AWS Resilience Hub, Anda harus menyertakan izin berikut untuk AWS Key Management Service mengakses kebijakan.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowResilienceHubDecrypt",
      "Effect": "Allow",
      "Principal": {
        "Service": "resiliencehub.amazonaws.com"
      },
      "Action": [
        "kms:GenerateDataKey*",
```

```
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:region:account-id:key/key-id"
    }
  ]
}
```

Membatasi izin untuk menyertakan atau mengecualikan rekomendasi AWS Resilience Hub

AWS Resilience Hub memungkinkan Anda membatasi izin untuk menyertakan atau mengecualikan rekomendasi per aplikasi. Anda dapat membatasi izin untuk menyertakan atau mengecualikan rekomendasi per aplikasi menggunakan kebijakan IAM kepercayaan berikut. Dalam kebijakan IAM kepercayaan ini, `caller_IAM_role` (terkait dengan akun AWS pengguna Anda) digunakan di akun saat ini untuk menelepon AWS Resilience Hub. APIs

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "resiliencehub:BatchUpdateRecommendationStatus",
      "Resource": "arn:aws:resiliencehub:us-west-2:12345678900:app/0e6237b7-23ba-4103-
adb2-91811326b703"
    }
  ]
}
```

Keamanan infrastruktur di AWS Resilience Hub

Sebagai layanan terkelola, AWS Resilience Hub dilindungi oleh prosedur keamanan jaringan AWS global yang dijelaskan dalam white paper Amazon Web Services: Tinjauan Proses Keamanan.

Anda menggunakan API panggilan yang AWS dipublikasikan untuk mengakses AWS Resilience Hub melalui jaringan. Klien harus mendukung Transport Layer Security (TLS) 1.2 atau yang lebih baru. Kami merekomendasikan TLS 1.3 atau yang lebih baru. Klien juga harus mendukung cipher suite dengan perfect forward secrecy (PFS) seperti Ephemeral Diffie-Hellman () atau Elliptic Curve Ephemeral Diffie-Hellman (). DHE ECDHE Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani dengan menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan IAM prinsipal. Atau Anda bisa menggunakan AWS Security Token Service (AWS STS) untuk membuat kredensial keamanan sementara guna menandatangani permintaan.

Pemeriksaan Ketahanan untuk layanan AWS

Bab ini memberikan rincian berbagai pemeriksaan ketahanan yang dilakukan oleh AWS Resilience Hub untuk AWS layanan yang didukung untuk memastikan bahwa postur ketahanan aplikasi tidak terpengaruh. Pemeriksaan ini memperkirakan tujuan waktu pemulihan (RTO) dan tujuan titik pemulihan (RPO) terhadap nilai-nilai yang ditentukan dalam kebijakan ketahanan untuk setiap Komponen Aplikasi ()AppComponent. Penilaian mencakup berbagai jenis gangguan, yaitu, Aplikasi, kegagalan Infrastruktur, pemadaman AZ, dan kegagalan Regional. Namun, untuk menjalankan pemeriksaan ini, Anda harus memberikan IAM izin yang relevan AWS Resilience Hub untuk mengizinkannya mengakses sumber daya Anda. Untuk mempelajari lebih lanjut tentang IAM izin yang diperlukan AWS Resilience Hub untuk mengizinkan mengakses sumber daya Anda dan melakukan pemeriksaan ketahanan di Bab ini, lihat. AWS kebijakan terkelola untuk AWS Resilience Hub

AWS layanan

- Amazon Elastic File System
- Amazon Relational Database Service dan Amazon Aurora
- Amazon Simple Storage Service
- Amazon DynamoDB
- Amazon Elastic Compute Cloud
- Amazon EBS
- AWS Lambda
- Amazon Elastic Kubernetes Service
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- Amazon Elastic Container Service
- Penyeimbang Beban Elastis
- APIGerbang Amazon
- Amazon DocumentDB
- NATGerbang
- Amazon Route 53
- Pengendali Pemulihan Aplikasi Amazon Route 53

- Amazon FSx untuk Server File Windows
- AWS Step Functions

Amazon Elastic File System

Bagian ini mencantumkan semua pemeriksaan ketahanan dan rekomendasi yang khusus untuk Amazon Elastic File System.

Untuk informasi selengkapnya tentang Amazon Elastic File System, lihat dokumentasi Amazon Elastic File System.

Jenis filesystem

AWS Resilience Hub memeriksa jenis sistem file: Regional atau Satu Zona. Jenis sistem file memengaruhi ketahanannya jika terjadi gangguan Infrastruktur atau AZ. Untuk informasi selengkapnya tentang jenis sistem file, lihat Ketersediaan dan daya tahan sistem file Amazon EFS.

Cadangan Sistem File

AWS Resilience Hub memeriksa apakah AWS Backup rencana ditentukan untuk sistem file yang diterapkan. Selain itu, ini memverifikasi apakah opsi `Cross-Region` cadangan diaktifkan, memastikan cakupan untuk gangguan tingkat Wilayah jika diperlukan oleh kebijakan pelanggan.

Replikasi Data

AWS Resilience Hub memeriksa apakah replikasi EFS data Amazon In-region atau Lintas wilayah ditentukan untuk sistem file yang diterapkan. Replikasi EFS data Amazon membantu meningkatkan perkiraan RTO dan perkiraan RPO pada tingkat Aplikasi, Infrastruktur, AZ, dan Wilayah. Selain itu, AWS Resilience Hub periksa apakah digabungkan dengan In-region AWS Backup untuk mengaktifkan ketahanan sistem file jika terjadi gangguan aplikasi.

Amazon Relational Database Service dan Amazon Aurora

Bagian ini mencantumkan semua pemeriksaan ketahanan dan rekomendasi yang spesifik untuk Amazon Relational Database Service dan Amazon Aurora.

Untuk informasi selengkapnya tentang Amazon Relational Database Service dan Amazon Aurora, lihat dokumentasi Amazon Relational Database Service.

Penyebaran AZ tunggal

AWS Resilience Hub memeriksa apakah database digunakan sebagai satu contoh dan jika ditentukan, ini menunjukkan bahwa itu tidak mendukung instance sekunder dan replika baca.

Deployment Multi-AZ

AWS Resilience Hub memeriksa apakah database digunakan baik dengan instance sekunder atau replika baca. Jika database digunakan dengan replika baca, AWS Resilience Hub validasi jika digunakan di AZ yang berbeda untuk memungkinkan failover jika terjadi gangguan AZ.

Cadangan

AWS Resilience Hub memeriksa apakah kemampuan cadangan berikut diterapkan pada instance database yang digunakan.

- AWS Backup rencanakan dengan opsi pencadangan otomatis
- AWS Backup rencanakan dengan salinan cadangan lintas wilayah jika diperlukan oleh kebijakan pelanggan
- Cuplikan manual untuk sistem cadangan pihak ke-3

Kegagalan Lintas Wilayah

AWS Resilience Hub pemeriksaan RTO dan RPO target yang ditetapkan dalam kebijakan ketahanan untuk pulih dari gangguan Regional. Selain itu, AWS Resilience Hub dapat mengidentifikasi arsitektur lintas wilayah berikut untuk menutupi gangguan Regional:

- Pencadangan dalam wilayah dengan salinan snapshot Lintas wilayah
- Replika baca di Wilayah lain
- Database global Amazon Aurora dengan cluster sekunder di Wilayah lain
- Database global Amazon Aurora dengan cluster sekunder tanpa kepala di Wilayah lain

Failover di wilayah yang lebih cepat

AWS Resilience Hub pemeriksaan RTO dan RPO target yang ditentukan dalam kebijakan ketahanan selama gangguan infrastruktur atau AZ. Selain itu, AWS Resilience Hub dapat mengidentifikasi arsitektur In-region berikut untuk menutupi gangguan Aplikasi, Infrastruktur, dan AZ:

- Cadangan In-Region
- Replika baca di AZ yang berbeda
- Cluster Aurora dengan replika baca di AZ lain
- Instans Multi-AZ dari Amazon Relational Database Service (Amazon) RDS
- Kluster RDS Multi-AZ Amazon
- Satu contoh Amazon RDS dengan replika baca di AZ lain

Amazon Simple Storage Service

Bagian ini mencantumkan semua pemeriksaan ketahanan dan rekomendasi yang khusus untuk Amazon Simple Storage Service (Amazon S3).

Untuk informasi selengkapnya tentang Amazon S3, lihat dokumentasi Amazon S3.

Penentuan Versi

AWS Resilience Hub memverifikasi apakah bucket Amazon S3 dikonfigurasi dengan versi diaktifkan.

Pencadangan terjadwal

AWS Resilience Hub memeriksa apakah AWS Backup paket ditentukan untuk bucket Amazon Simple Storage Service (Amazon S3) yang di-deploy. Selain itu, ia juga memeriksa apakah opsi pencadangan lintas wilayah diaktifkan jika kebijakan Anda memerlukan cakupan untuk gangguan tingkat Wilayah.

oint-in-time Pemulihan P

Replikasi data

AWS Resilience Hub jika Same Region Replication (SRR) dan Cross Region Replication (CRR) ditentukan untuk bucket Amazon S3 yang digunakan.

Replikasi data Amazon S3 meningkatkan estimasi beban kerja RTO dan perkiraan beban kerja RPO di tingkat Aplikasi, Infrastruktur, AZ, dan Wilayah. Selain itu, ini juga melindungi dari penghapusan fisik objek karena penghapusan versi objek tidak direplikasi ke bucket Amazon S3 target. Selain itu, berdasarkan RTO target yang ditentukan dalam kebijakan ketahanan Anda, AWS Resilience Hub periksa apakah Kontrol Waktu Replikasi Amazon S3 (RTCS3) harus diaktifkan atau tidak. Fitur yang dapat ditagih ini mereplikasi 99,99 persen objek bucket sumber dalam waktu 15 menit.

- AWS Backup rencanakan dengan opsi pencadangan otomatis
- AWS Backup rencanakan dengan salinan cadangan lintas wilayah jika diperlukan oleh kebijakan pelanggan
- Cuplikan manual untuk sistem cadangan pihak ke-3

Amazon DynamoDB

Bagian ini mencantumkan semua pemeriksaan ketahanan dan rekomendasi yang khusus untuk Amazon DynamoDB.

Untuk informasi selengkapnya tentang Amazon DynamoDB, lihat dokumentasi Amazon DynamoDB.

Pencadangan terjadwal

AWS Resilience Hub memeriksa apakah cadangan sudah ditentukan untuk tabel yang digunakan. Selain itu, ia juga memeriksa apakah cadangan lintas wilayah harus dikonfigurasi untuk kebijakan Anda jika memerlukan cakupan untuk gangguan tingkat Wilayah.

oint-in-time Pemulihan P

AWS Resilience Hub memeriksa apakah point-in-time recovery (PITR) diperlukan sesuai dengan target kebijakan ketahanan Anda. RPO Namun, cadangan lintas wilayah tidak didukung untukPITR. Oleh karena itu, Anda menggunakan AWS Backup rencana terjadwal yang ada dengan opsi pencadangan lintas wilayah diaktifkan, atau membuat yang baru.

Tabel global

Amazon Elastic Compute Cloud

Bagian ini mencantumkan semua pemeriksaan ketahanan dan rekomendasi khusus untuk Amazon Elastic Compute Cloud.

Untuk informasi selengkapnya tentang Amazon Elastic Compute Cloud, lihat dokumentasi Amazon Elastic Compute Cloud.

Contoh stateful

AWS Resilience Hub mengidentifikasi instance Amazon sebagai EC2 instance stateful jika salah satu kriteria berikut terpenuhi:

- Jika `DeleteOnTermination` atribut disetel ke false untuk setidaknya satu volume Amazon Elastic Block Store (AmazonEBS) yang dilampirkan ke instance ini.
- Jika Amazon Data Lifecycle Manager atau AWS Backup paket dilampirkan ke EC2 instans Amazon atau setidaknya satu volume Amazon. EBS
- Jika AWS Elastic Disaster Recovery digunakan untuk mereplikasi volume penyimpanan EC2 instans Amazon Anda.

> **Note**
>
> Jika EC2 instans Amazon tidak memenuhi salah satu kriteria di atas, perlakukan sebagai AWS Resilience Hub EC2 instans Amazon tanpa kewarganegaraan.

Grup Auto Scaling

AWS Resilience Hub memeriksa sekelompok EC2 instance Amazon tanpa kewarganegaraan. Jika ditemukan, disarankan untuk mengatur hal yang sama menggunakan grup Auto Scaling () ASG dengan konfigurasi Multi-AZ.

Jika yang sudah ASG ada diidentifikasi, ARH akan memverifikasi apakah itu dikonfigurasi di beberapa Availability Zone. Jika juga ASG didefinisikan hanya menggunakan EC2 instans Amazon spot, disarankan untuk menambah kapasitasnya dengan instans EC2 Amazon sesuai permintaan untuk meningkatkan ketahanan

ketika EC2 instans Amazon spot tidak tersedia.

EC2Armada Amazon

AWS Resilience Hub mengidentifikasi EC2 Armada Amazon dan memverifikasi apakah itu didefinisikan sebagai penyebaran multi-AZ dan juga jika hanya menggunakan instans Amazon spot. EC2

Mendefinisikan EC2 Armada Amazon sebagai penyebaran Multi-AZ akan meningkatkan ketahanannya jika terjadi gangguan AZ.

Menambah EC2 Armada Amazon dengan instans sesuai permintaan akan meningkatkan ketahanannya saat instans spot tidak tersedia.

Amazon EBS

Bagian ini mencantumkan semua pemeriksaan ketahanan dan rekomendasi yang khusus untuk Amazon. EBS

Untuk informasi selengkapnya tentang AmazonEBS, lihat EBSdokumentasi Amazon.

Pencadangan terjadwal

AWS Resilience Hub memeriksa apakah salah satu atau kedua hal berikut ini ditentukan untuk EBS volume Amazon Anda.

- Aturan cadangan untuk EBS volume Amazon tertentu yang dilampirkan ke EC2 instans Amazon Anda.
- Aturan pencadangan untuk membuat Amazon yang EBS didukung AMI ke EC2 instans Amazon Anda.
- Cuplikan manual untuk sistem cadangan pihak ke-3.

Selain itu, jika kebijakan Anda memerlukan cakupan untuk gangguan tingkat Wilayah, AWS Resilience Hub periksa apakah aturan pencadangan Anda mengaktifkan opsi pencadangan lintas wilayah.

Pencadangan dan replikasi data

AWS Resilience Hub mengidentifikasi EBS volume Amazon dianggap sebagai volume stateful jika salah satu kriteria berikut terpenuhi:

- Jika `DeleteOnTermination` atribut disetel ke false untuk EBS volume Amazon ini.
- Jika Amazon Data Lifecycle Manager atau AWS Backup paket dikaitkan dengan volume Amazon ini EBS atau EC2 instans Amazon yang dilampirkan.
- Jika AWS Elastic Disaster Recovery digunakan untuk mereplikasi volume penyimpanan EC2 instans Amazon Anda.

AWS Lambda

Bagian ini mencantumkan semua pemeriksaan ketahanan dan rekomendasi yang khusus untuk. AWS Lambda

Untuk informasi selengkapnya AWS Lambda, lihat AWS Lambda dokumentasi.

VPCAkses Amazon Pelanggan

AWS Resilience Hub mengidentifikasi AWS Lambda fungsi yang terhubung ke pelangganVPC. Menghubungkan AWS Lambda ke subnet di Amazon Anda yang berbeda AZs VPC memungkinkan ketahanan fungsi jika terjadi gangguan AZ.

Antrian surat mati

AWS Resilience Hub memeriksa apakah suatu AWS Lambda fungsi memiliki antrian huruf mati (DLQ) yang dilampirkan padanya untuk menyimpan permintaan yang gagal. Melampirkan AWS Lambda fungsi DLQ ke memungkinkan untuk mencegah hilangnya data permintaan dan mencoba lagi untuk memproses permintaan yang gagal pada tahap selanjutnya.

Amazon Elastic Kubernetes Service

Bagian ini mencantumkan semua pemeriksaan ketahanan dan rekomendasi yang khusus untuk Amazon Elastic Kubernetes Service (Amazon). EKS

Untuk informasi selengkapnya tentang AmazonEKS, lihat EKSdokumentasi Amazon.

Deployment Multi-AZ

AWS Resilience Hub mengidentifikasi apakah penerapan pod berjalan pada beberapa node pekerja dalam beberapa. AZs

EKSCluster Amazon tambahan di Wilayah lain diperlukan jika kebijakan ketahanan Anda memerlukan cakupan jika terjadi gangguan Regional. EKSCluster Amazon tambahan ini juga diverifikasi untuk penerapan pod yang didistribusikan di antara beberapa node pekerja dalam beberapa. AZs

Penerapan vs. ReplicaSet

AWS Resilience Hub memeriksa apakah Anda menggunakan objek ReplicaSets atau pod alih-alih penerapan. Mengganti objek ReplicaSets atau pod dengan deployment menyederhanakan pembaruan pod ke versi baru perangkat lunak dan menyertakan fitur berguna lainnya.

Pemeliharaan penyebaran

AWS Resilience Hub memeriksa apakah praktik terbaik berikut digunakan untuk penerapan:

- Menggunakan Pod Disruption Budget (PDB) — Menggunakan PDB Pod Disruption Budget () memungkinkan untuk meningkatkan ketersediaan dengan menetapkan batas jumlah pod dalam beban kerja yang dapat terganggu pada waktu tertentu.
- Mengganti grup node yang dikelola sendiri dengan grup node EKS terkelola Amazon — Penggantian ini menyederhanakan pembaruan gambar node pekerja selama pemeliharaan.
- Mendukung permintaan dinamis CPU dan memori per penerapan — Permintaan ini membantu Kubernetes untuk memilih node yang sesuai dengan kebutuhan sebuah pod.
- Mengonfigurasi probe keaktifan dan kesiapan untuk semua kontainer — Mengonfigurasi probe keaktifan membantu meningkatkan ketahanan dengan memulai ulang pod yang tidak berfungsi. Mengkonfigurasi probe kesiapan memungkinkan untuk meningkatkan ketersediaan dengan mengalihkan lalu lintas dari pod yang sibuk.
- Mengonfigurasi Karpenter, Cluster Autoscaler, atau — Konfigurasi AWS Fargate ini memungkinkan infrastruktur EKS klaster Amazon tumbuh dan memenuhi tuntutan beban kerja.
- Mengonfigurasi Horizontal Pod Autoscaler — Konfigurasi ini membantu EKS klaster Amazon untuk secara otomatis menskalakan beban kerja untuk memenuhi permintaan pemrosesan permintaan.

Amazon Simple Notification Service

Bagian ini mencantumkan semua pemeriksaan ketahanan dan rekomendasi yang khusus untuk Amazon Simple Notification Service (AmazonSNS).

Untuk informasi selengkapnya tentang AmazonSNS, lihat SNSdokumentasi Amazon.

Langganan topik

AWS Resilience Hub memeriksa apakah SNS topik Amazon memiliki setidaknya 1 langganan yang dilampirkan padanya untuk memastikan bahwa pesan masuk tidak hilang.

Amazon Simple Queue Service

Bagian ini mencantumkan semua pemeriksaan ketahanan dan rekomendasi yang khusus untuk Amazon Simple Queue Service (Amazon). SQS

Untuk informasi selengkapnya tentang AmazonSQS, lihat SQSdokumentasi Amazon.

Antrian surat mati

AWS Resilience Hub memeriksa apakah SQS antrian Amazon memiliki yang DLQ terkait dengannya untuk menangani pesan yang tidak dapat dikirim ke pelanggan dengan sukses.

Amazon Elastic Container Service

Bagian ini mencantumkan semua pemeriksaan ketahanan dan rekomendasi yang khusus untuk Amazon Elastic Container Service (AmazonECS).

Untuk informasi selengkapnya tentang AmazonECS, lihat ECSdokumentasi Amazon.

Deployment Multi-AZ

AWS Resilience Hub memeriksa apakah ECS tugas atau layanan Amazon berjalan dalam beberapa AZs berdasarkan Amazon EC2 atau jenis AWS Fargate peluncuran. ECSCluster Amazon tambahan di Wilayah lain diperlukan jika kebijakan Anda memerlukan cakupan untuk gangguan Regional. Cluster tambahan juga diverifikasi untuk pelaksanaan tugas atau layanan dalam beberapaAZs.

Penyeimbang Beban Elastis

Bagian ini mencantumkan semua pemeriksaan ketahanan dan rekomendasi yang khusus untuk Elastic Load Balancing.

Untuk informasi selengkapnya tentang Elastic Load Balancing, lihat dokumentasi Elastic Load Balancing.

Deployment Multi-AZ

AWS Resilience Hub memeriksa apakah Elastic Load Balancing berjalan dalam beberapa. AZs

Elastic Load Balancing tambahan di Wilayah yang berbeda diperlukan jika polis Anda memerlukan pertanggungan untuk gangguan Regional. Elastic Load Balancing tambahan, yang terletak di Wilayah yang berbeda, juga diverifikasi untuk penerapannya dalam beberapa. AZs

APIGerbang Amazon

Bagian ini mencantumkan semua pemeriksaan ketahanan dan rekomendasi yang khusus untuk Amazon API Gateway.

Untuk informasi selengkapnya tentang Amazon API Gateway, lihat dokumentasi Amazon API Gateway.

Penyebaran Lintas Wilayah

Jika kebijakan Anda perlu mempertimbangkan gangguan Regional, AWS Resilience Hub akan memeriksa apakah ada penerapan tambahan API sumber daya Amazon API Gateway di Wilayah lain.

Penerapan API Multi-AZ pribadi

AWS Resilience Hub memeriksa apakah Anda API didefinisikan sebagai pribadi dalam Amazon API Gateway. Private APIs harus menerima lalu lintas melalui titik akhir VPC antarmuka Amazon yang digunakan ke beberapa. AZs

Amazon DocumentDB

Bagian ini mencantumkan semua pemeriksaan dan rekomendasi yang khusus untuk Amazon DocumentDB.

Untuk informasi selengkapnya tentang Amazon DocumentDB, lihat dokumentasi Amazon DocumentDB.

Deployment Multi-AZ

AWS Resilience Hub memeriksa apakah klaster Amazon DocumentDB digunakan dalam beberapa. AZs Cluster Amazon DocumentDB sekunder tambahan diperlukan di Wilayah lain jika kebijakan Anda memerlukan cakupan untuk gangguan Regional. Cluster Amazon DocumentDB tambahan, yang terletak di Wilayah yang berbeda, juga diverifikasi untuk pelaksanaannya dalam beberapa. AZs

Kluster elastis dan penyebaran Multi-AZ

AWS Resilience Hub memeriksa apakah pecahan klaster Amazon DocumentDB Elastic menggunakan replika baca yang digunakan di berbagai jenis. AZs

Cluster elastis dan snapshot Manual

AWS Resilience Hub memeriksa apakah snapshot manual dibuat secara teratur untuk cluster Amazon DocumentDB Elastic. Snapshot manual memungkinkan persistensi yang lebih lama dan

memberikan fleksibilitas dalam mengatur frekuensi snapshot agar sesuai dengan kebutuhan bisnis Anda.

NATGerbang

Bagian ini mencantumkan semua pemeriksaan dan rekomendasi yang khusus untuk NAT Gateway. Untuk informasi selengkapnya tentang NAT Gateway, lihat NAT Gateways.

Deployment Multi-AZ

AWS Resilience Hub memeriksa apakah NAT Gateway digunakan dalam beberapaAZs.

Penerapan NAT Gateway tambahan diperlukan di Wilayah lain jika kebijakan Anda memerlukan cakupan untuk gangguan Regional. NATGateway tambahan, yang terletak di Wilayah yang berbeda, juga diverifikasi untuk penerapannya di beberapaAZs.

Amazon Route 53

Bagian ini mencantumkan semua pemeriksaan dan rekomendasi yang khusus untuk Amazon Route 53.

Untuk informasi selengkapnya tentang Amazon Route 53, lihat dokumentasi Amazon Route 53.

Deployment Multi-AZ

AWS Resilience Hub memeriksa apakah catatan zona yang dihosting Amazon Route 53 ditentukan dengan beberapa target di Wilayah yang sama dan jika target ini diterapkan dalam beberapaAZs. Jika kebijakan Anda memerlukan cakupan untuk gangguan Regional, AWS Resilience Hub periksa apakah catatan zona yang dihosting Amazon Route 53 ditentukan di beberapa Wilayah dengan beberapa target per Wilayah, dan apakah target ini diterapkan di beberapa wilayah. AZs

Pengendali Pemulihan Aplikasi Amazon Route 53

Bagian ini mencantumkan semua pemeriksaan dan rekomendasi yang khusus untuk Amazon Route 53 Application Recovery Controller (Route 53ARC).

Untuk informasi selengkapnya tentang Route 53ARC, lihat ARCdokumentasi Route 53.

Deployment Multi-AZ

AWS Resilience Hub memeriksa apakah sumber daya serupa digunakan di beberapa Wilayah dan merekomendasikan sebagai praktik terbaik untuk menentukan pemeriksaan ARC kesiapan Route 53 untuk meningkatkan ketersediaan dan kesiapannya jika terjadi gangguan Regional. Anda akan diberi tahu bahwa Anda akan dikenakan biaya tambahan per jam.

Amazon FSx untuk Server File Windows

Bagian ini mencantumkan semua pemeriksaan dan rekomendasi yang khusus untuk Amazon FSx untuk Windows File Server. Untuk informasi selengkapnya tentang Amazon FSx untuk Windows File Server, lihat dokumentasi Amazon FSx untuk Windows File Server.

Jenis filesystem

AWS Resilience Hub memeriksa jenis sistem file: atau. `Regional` `One Zone` Jenis sistem file mempengaruhi ketahanannya jika terjadi gangguan Infrastruktur atau AZ. Untuk informasi selengkapnya tentang jenis sistem file, lihat Amazon. EFS

Cadangan Sistem File

AWS Resilience Hub memeriksa apakah AWS Backup didefinisikan untuk sistem file yang diterapkan. Selain itu, ia juga memeriksa apakah `cross-Region backup` opsi diaktifkan jika kebijakan Anda memerlukan pertanggungan untuk gangguan tingkat Wilayah.

Replikasi Data

AWS Resilience Hub memeriksa apakah tugas replikasi AWS DataSync data terjadwal In-region atau Cross-region ditentukan untuk sistem file yang diterapkan.

AWS DataSync tugas replikasi data terjadwal dapat meningkatkan perkiraan beban kerja RTO dan perkiraan beban kerja RPO di tingkat Infrastruktur, AZ, dan Wilayah. Selain itu, dapat dikombinasikan dengan In-region AWS Backup untuk pulih jika terjadi gangguan aplikasi.

AWS Step Functions

Bagian ini mencantumkan semua pemeriksaan dan rekomendasi yang khusus untuk AWS Step Functions.

Untuk informasi selengkapnya AWS Step Functions, lihat AWS Step Functions dokumentasi.

Versi dan alias

AWS Resilience Hub memeriksa apakah AWS Step Functions alur kerja menggunakan versi dan alias untuk meningkatkan waktu penerapan ulang.

Penyebaran Lintas Wilayah

AWS Resilience Hub memeriksa apakah AWS Step Functions alur kerja dari jenis alur kerja yang sama diterapkan di Wilayah yang berbeda untuk dipulihkan jika terjadi gangguan Regional.

Bekerja dengan layanan yang lain

Bagian ini menjelaskan AWS layanan yang berinteraksi dengan AWS Resilience Hub.

Topik

- AWS CloudFormation
- AWS CloudTrail
- AWS Systems Manager
- AWS Trusted Advisor

AWS CloudFormation

AWS Resilience Hub terintegrasi dengan AWS CloudFormation, yaitu layanan yang membantu Anda membuat model dan mengatur sumber daya AWS agar Anda dapat menghemat waktu untuk membuat dan mengelola sumber daya dan infrastruktur Anda. Anda membuat template yang menjelaskan semua AWS sumber daya yang Anda inginkan (seperti AWS::ResilienceHub:::ResiliencyPolicy dan AWS::ResilienceHub:::App), dan AWS CloudFormation ketentuan serta mengonfigurasi sumber daya tersebut untuk Anda.

Saat menggunakan AWS CloudFormation, Anda dapat menggunakan kembali templat Anda untuk menyiapkan sumber daya AWS Resilience Hub secara konsisten dan berulang kali. Jelaskan sumber daya Anda satu kali, lalu berikan sumber daya yang sama berulang kali di beberapa AWS akun dan Wilayah.

Templat AWS Resilience Hub dan AWS CloudFormation

Untuk menyediakan dan mengonfigurasi sumber daya untuk AWS Resilience Hub dan layanan terkait, Anda harus memahami templat AWS CloudFormation. Templat adalah file teks dengan format JSON atau YAML. Templat ini menjelaskan sumber daya yang ingin Anda sediakan di tumpukan AWS CloudFormation Anda. Jika Anda tidak terbiasa dengan JSON atau YAML, Anda dapat menggunakan AWS CloudFormation Designer untuk membantu Anda memulai dengan templat AWS CloudFormation. Untuk informasi selengkapnya, lihat Apa yang dimaksud dengan AWS CloudFormation Designer? dalam Panduan Pengguna AWS CloudFormation.

AWS Resilience Hubmendukung pembuatan AWS::ResilienceHub:::ResiliencyPolicy dan AWS::ResilienceHub:::App masukAWS CloudFormation. Untuk informasi selengkapnya,

termasuk contoh template JSON dan YAMAL untuk AWS::ResilienceHub:::ResiliencyPolicy dan AWS::ResilienceHub:::App, lihat referensi jenis AWS Resilience Hub sumber daya di AWS CloudFormationPanduan Pengguna.

Anda dapat menggunakan AWS CloudFormation tumpukan untuk menentukan AWS Resilience Hub aplikasi. Tumpukan memungkinkan Anda mengelola sumber daya terkait sebagai satu unit. Tumpukan dapat berisi semua sumber daya yang Anda butuhkan untuk menjalankan aplikasi web, seperti server web atau aturan jaringan.

Pelajari selengkapnya tentang AWS CloudFormation

Untuk informasi selengkapnyaAWS CloudFormation, lihat sumber daya berikut:

- AWS CloudFormation
- Panduan Pengguna AWS CloudFormation
- AWS CloudFormationReferensi API
- AWS CloudFormationPanduan Pengguna Antarmuka Baris Perintah

AWS CloudTrail

AWS Resilience Hub terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di AWS Resilience Hub. CloudTrail menangkap semua panggilan API untuk AWS Resilience Hub sebagai peristiwa. Panggilan yang ditangkap termasuk panggilan dari AWS Resilience Hub konsol dan panggilan kode ke operasi AWS Resilience Hub API. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara berkelanjutan ke bucket Amazon S3, termasuk acara untuk. AWS Resilience Hub Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat AWS Resilience Hub, alamat IP dari mana permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Untuk informasi selengkapnya CloudTrail, lihat Panduan AWS CloudTrail Pengguna.

AWS Systems Manager

AWS Resilience Hub Bekerja dengan Systems Manager untuk mengotomatiskan langkah-langkah SOP Anda dengan menyediakan sejumlah dokumen SSM yang dapat Anda gunakan sebagai dasar untuk SOP tersebut.

AWS Resilience Hub menyediakan AWS CloudFormation template yang berisi peran IAM yang diperlukan untuk menjalankan dokumen Systems Manager yang berbeda, satu peran per dokumen dengan izin yang diperlukan untuk dokumen tertentu. Setelah membuat tumpukan dengan AWS CloudFormation template, itu akan mengatur peran IAM dan menyimpan metadata dalam parameter Systems Manager untuk dokumen otomatisasi Systems Manager untuk menjalankan prosedur pemulihan yang berbeda.

Untuk informasi selengkapnya tentang penggunaan SOP, lihatMengelola prosedur operasi standar.

AWS Trusted Advisor

AWS Trusted Advisor adalah rumah terpusat dari rekomendasi praktik AWS terbaik yang membantu Anda mengidentifikasi, memprioritaskan, dan mengoptimalkan penerapan Anda. AWS AWS Trusted Advisor memeriksa AWS lingkungan Anda, dan kemudian membuat rekomendasi melalui pemeriksaan ketika ada peluang untuk menghemat uang, meningkatkan ketersediaan dan kinerja sistem, atau membantu menutup kesenjangan keamanan. Pemeriksaan ini dibagi menjadi beberapa kategori berdasarkan tujuannya. Untuk informasi selengkapnya tentang berbagai kategori pemeriksaan AWS Trusted Advisor, lihat Panduan AWS SupportPengguna.

AWS Trusted Advisor memberikan beberapa rekomendasi ketahanan tingkat tinggi melalui pemeriksaan ketahanan untuk setiap aplikasi di AWS Resilience Hub bawah kategori toleransi Kesalahan. Kategori toleransi kesalahan mencantumkan semua pemeriksaan yang menguji aplikasi Anda untuk menentukan ketahanan dan keandalannya. Pemeriksaan ini mengingatkan Anda ketika ada AppComponent kegagalan dan pelanggaran kebijakan yang dapat menyebabkan risiko ketahanan dan memengaruhi ketersediaan aplikasi untuk kelangsungan bisnis. Ini juga memberikan rekomendasi ketahanan yang akan meningkatkan peluang untuk mengurangi risiko ini di bawah bagian Tindakan yang Direkomendasikan, yang perlu ditangani. AWS Resilience Hub Untuk wawasan lebih lanjut tentang rekomendasi untuk setiap aplikasi di AWS Trusted Advisor, kami sarankan Anda untuk melihat rekomendasi terperinci yang disediakan di AWS Resilience Hub.

AWS Trusted Advisor memberikan pemeriksaan berikut untuk setiap aplikasi di AWS Resilience Hub:

- AWS Resilience Hub skor ketahanan aplikasi - Memeriksa skor ketahanan aplikasi Anda dari penilaian terbaru mereka AWS Resilience Hub dan memberi tahu Anda jika skor ketahanannya di bawah nilai tertentu.

  Kriteria peringatan

  - Hijau — Menunjukkan bahwa aplikasi Anda memiliki skor ketahanan 70 ke atas.

- Kuning — Menunjukkan bahwa aplikasi Anda memiliki skor ketahanan antara 40 dan 69.
- Merah - Menunjukkan bahwa aplikasi Anda memiliki skor ketahanan kurang dari 40.

Tindakan yang disarankan

Untuk meningkatkan postur ketahanan dan mendapatkan skor ketahanan terbaik untuk aplikasi Anda, jalankan penilaian dengan versi terbaru dari sumber daya aplikasi Anda dan jika berlaku, terapkan rekomendasi operasional yang disarankan. Untuk informasi selengkapnya tentang menjalankan, meninjau, dan menerapkan penilaian, meninjau dan menyertakan/mengecualikan rekomendasi operasional, dan menerapkan hal yang sama, lihat topik berikut:

- the section called “Menjalankan penilaian ketahanan”
- the section called “Meninjau laporan penilaian”
- the section called “Meninjau rekomendasi ketahanan”
- the section called “Termasuk atau tidak termasuk rekomendasi operasional”

- AWS Resilience Hub kebijakan aplikasi dilanggar — Memeriksa apakah AWS Resilience Hub aplikasi memenuhi target RTO dan RPO yang telah Anda tetapkan untuk aplikasi dan memberi tahu Anda jika aplikasi tidak memenuhi target RTO dan RPO.

  Kriteria peringatan

  - Hijau — Menunjukkan bahwa aplikasi memiliki kebijakan dan perkiraan beban kerja RTO dan perkiraan beban kerja RPO memenuhi target RTO dan RPO.
  - Kuning — Menunjukkan bahwa aplikasi memiliki kebijakan dan belum dinilai.
  - Merah — Menunjukkan bahwa aplikasi memiliki kebijakan dan perkiraan beban kerja RTO dan perkiraan beban kerja RPO tidak memenuhi target RTO dan RPO.

  Tindakan yang disarankan

  Untuk memastikan bahwa perkiraan beban kerja RTO dan perkiraan beban kerja RPO aplikasi Anda masih memenuhi target RTO dan RPO yang ditentukan, jalankan penilaian secara teratur dengan versi terbaru dari sumber daya aplikasi Anda. Selain itu, jika Anda ingin memastikan bahwa kebijakan ketahanan aplikasi Anda tidak dilanggar, kami sarankan Anda untuk meninjau laporan penilaian dan menerapkan rekomendasi ketahanan yang disarankan. Untuk informasi selengkapnya tentang AWS Resilience Hub memungkinkan menjalankan penilaian setiap hari atas nama Anda, menjalankan penilaian, meninjau rekomendasi ketahanan, dan menerapkan hal yang sama, lihat topik berikut:

  - the section called “Mengedit sumber daya aplikasi”(AWS Resilience Hub Untuk mengaktifkan menjalankan penilaian setiap hari atas nama Anda, selesaikan langkah-langkah di Untuk mengedit pengaturan pemberitahuan drift prosedur aplikasi Anda untuk memilih kotak centang otomatis menilai harian.)
  - the section called “Menjalankan penilaian ketahanan”
  - the section called “Meninjau laporan penilaian”
  - the section called “Meninjau rekomendasi ketahanan”
  - the section called “Termasuk atau tidak termasuk rekomendasi operasional”
- AWS Resilience Hub usia penilaian aplikasi - Memeriksa terakhir kali sejak Anda menjalankan penilaian untuk setiap aplikasi Anda di AWS Resilience Hub. Ini memberi tahu Anda jika Anda belum menjalankan penilaian untuk jumlah hari yang ditentukan.

  Kriteria peringatan

  - Hijau - Menunjukkan bahwa Anda telah menjalankan penilaian untuk aplikasi Anda dalam 30 hari terakhir.
  - Kuning — Menunjukkan bahwa Anda belum menjalankan penilaian untuk aplikasi Anda dalam 30 hari terakhir.

  Tindakan yang disarankan

  Jalankan penilaian secara teratur untuk mengelola dan meningkatkan postur ketahanan aplikasi Anda. AWS Jika Anda AWS Resilience Hub ingin menilai aplikasi Anda setiap hari atas nama Anda, Anda dapat mengaktifkan hal yang sama dengan memilih kotak centang Secara otomatis menilai aplikasi ini setiap hari dalam pemberitahuan AWS Resilience Hub drift. Untuk memilih Secara otomatis menilai aplikasi ini setiap hari kotak centang, lengkapi To edit drift notifikasi prosedur aplikasi Anda di???.

  > **Note**
  >
  > Pemeriksaan ini menentukan usia penilaian hanya aplikasi yang telah dinilai setidaknya sekali. AWS Resilience Hub

- AWS Resilience Hub pemeriksaan komponen aplikasi — Memeriksa apakah Komponen Aplikasi (AppComponent) dalam aplikasi Anda tidak dapat dipulihkan. Artinya, jika ini AppComponent tidak pulih jika terjadi gangguan, Anda mungkin mengalami kehilangan data yang tidak diketahui dan

downtime sistem. Jika kriteria peringatan diatur ke Merah, ini menunjukkan bahwa tidak dapat AppComponent dipulihkan.

Tindakan yang disarankan

Untuk memastikan bahwa Anda dapat AppComponent dipulihkan, tinjau dan terapkan rekomendasi ketahanan, dan kemudian jalankan penilaian baru. Untuk informasi lebih lanjut tentang meninjau rekomendasi ketahanan, lihat. the section called “Meninjau rekomendasi ketahanan”

Untuk informasi selengkapnya tentang penggunaan AWS Trusted Advisor, lihat Panduan AWS Support Pengguna.

Riwayat dokumen untuk Panduan AWS Resilience Hub Pengguna

Tabel berikut menjelaskan dokumentasi untuk rilis ini AWS Resilience Hub.

- APIversi: terbaru
- Pembaruan dokumentasi terbaru: 01 Agustus 2024

Perubahan	Deskripsi	Tanggal
AWS Resilience Hub memperkenalkan rekomendasi pengelompokan	AWS Resilience Hub memperkenalkan opsi pengelompokan cerdas baru untuk mengelompokkan sumber daya ke dalam Komponen Aplikasi (AppComponents) saat melakukan onboarding aplikasi Anda. Saat Anda menjalankan penilaian ketahanan AWS Resilience Hub, penting agar sumber daya Anda dikelompokkan secara akurat menjadi sesuai AppComponents untuk menerima rekomendasi yang dioptimalkan dan dapat ditindaklanjuti. Opsi ini sangat ideal untuk aplikasi kompleks atau lintas wilayah untuk mengurangi waktu yang dibutuhkan untuk onboard aplikasi Anda, dan ini melengkapi alur kerja orientasi aplikasi yang ada yang tersedia saat ini.	Agustus 1, 2024

Untuk informasi selengkapnya, lihat topik berikut.

- the section called “Mengelola Komponen Aplikasi”
- the section called “AWS Resilience Hub rekomendasi pengelompokan sumber daya”

AWS Resilience Hub memperkenalkan widget ringkasan penilaian baru	AWS Resilience Hub memperkenalkan widget ringkasan penilaian baru yang menggunakan kemampuan AI generatif Amazon Bedrock untuk mengubah data ketahanan kompleks menjadi wawasan yang sangat dapat ditindaklanjuti. Ringkasan penilaian ini mengekstrak temuan penting, memprioritaskan risiko, dan merekomendasikan langkah-langkah untuk meningkat kan ketahanan. Dengan berfokus pada elemen yang paling berdampak, Anda dapat memahami penilaian dengan lebih mudah, yang membantu Anda dengan informasi berdampak tinggi yang berfokus pada elemen paling penting dari postur ketahanan Anda. Untuk informasi selengkap nya, lihat the section called “Ringkasan Penilaian”.	Agustus 1, 2024

AWS Resilience Hub memperluas dukungan untuk Amazon DocumentDB	AWS Resilience Hub Kebijakan ini memungkinkan Anda memberikan `Describe` izin agar Anda dapat mengakses sumber daya dan konfigurasi di Amazon DocumentDB, Elastic Load Balancing, dan saat menjalankan penilaian. AWS Lambda Untuk informasi selengkapnya tentang kebijakan AWS terkelola, lihatthe section called “AWSResilienceHubAsssessmentExecutionPolicy”.	Agustus 1, 2024

AWS Resilience Hub memperluas kemampuan deteksi drift ketahanan aplikasi	AWS Resilience Hub telah memperluas kemampuan deteksi drift dengan memperkenalkan tipe baru deteksi drift — Application resource drift. Peningkatan ini mendeteksi perubahan, seperti penambahan atau penghapus an sumber daya dalam sumber input aplikasi. Anda dapat mengaktifkan penilaian AWS Resilience Hub terjadwal dan layanan pemberitahuan drift dan diberi tahu setiap kali terjadi penyimpangan. Penilaian ketahanan terbaru mengidentifikasi penyimpan gan dan menyajikan tindakan remediasi untuk mengembal ikan aplikasi sesuai dengan kebijakan ketahanan Anda. Untuk informasi selengkapnya, lihat topik berikut. • the section called “Deteksi drift” • the section called “Langkah 5: Siapkan penilaian terjadwal dan pemberita huan drift”	8 Mei 2024

AWS Trusted Advisor perangkat tambahan	AWS Resilience Hub telah memperluas dukungan AWS Trusted Advisor dengan menambahkan cek untuk mengidentifikasi Komponen Aplikasi () yang tidak dapat dipulihkan. AppComponents Untuk informasi selengkapnya, lihat the section called “AWS Trusted Advisor”.	Maret 28, 2024
AWS Resilience Hub memperluas dukungan untuk alarm yang direkomendasikan	AWS Resilience Hub telah memperbarui file `README.md` template dengan nilai yang memungkinkan Anda membuat alarm yang direkomendasikan oleh AWS Resilience Hub dalam AWS (seperti Amazon CloudWatch) atau di luar AWS. Untuk informasi selengkap nya, lihat the section called “Mengelola alarm-alarm”.	Maret 26, 2024

AWS Resilience Hub memperluas dukungan untuk Amazon FSx untuk Windows File Server	AWS Resilience Hub memperluas dukungan penilaian untuk Amazon FSx untuk sumber daya Windows File Server sambil menilai ketahanan aplikasi Anda. Untuk aplikasi yang menggunakan Amazon FSx untuk Windows File Server, AWS Resilience Hub menyediakan serangkaian rekomendasi ketahanan baru, yang mencakup penyebaran Availability Zone (AZ) dan multi-AZ, dan rencana cadangan, serta replikasi data. AWS Resilience Hub mendukung Amazon FSx untuk Windows File Server, termasuk ketergantungan sistem file pada Microsoft Active Directory, untuk penyebaran In-region dan Cross-region. Untuk informasi selengkapnya, lihat topik berikut. • the section called “ AWS Resilience Hub Sumber daya yang didukung” • the section called “AWSResilienceHubAsssessmentExecutionPolicy” • the section called “Mengelompokkan sumber	Maret 26, 2024

	daya dalam Komponen Aplikasi”	
AWS Resilience Hub memberikan informasi tambahan tentang skor Ketahanan	AWS Resilience Hub telah memperbarui pengalaman pengguna skor Ketahanan untuk membantu Anda menavigasi dan memahami tindakan yang diperlukan untuk meningkatkan postur ketahanan aplikasi Anda dengan mudah. Untuk informasi selengkap nya, lihat the section called “Memahami skor ketahanan”.	9 November 2023
AWS Resilience Hub memperluas dukungan untuk aplikasi yang menyertakan sumber daya Amazon Elastic Kubernetes Service (Amazon) EKS	AWS Resilience Hub memperluas dukungan untuk aplikasi yang mencakup EKS sumber daya Amazon untuk menyertakan rekomenda si operasional baru. Saat menjalankan penilaian yang mencakup sumber daya dari EKS kluster Amazon, kami sekarang akan merekomen dasikan pengujian dan alarm untuk dijalankan untuk membantu meningkatkan postur ketahanan aplikasi. Untuk informasi selengkap nya, lihat the section called “Mengelola eksperimen Layanan Injeksi Kesalahan Amazon”.	9 November 2023

AWS Resilience Hub memberikan informasi tambahan di tingkat aplikasi	AWS Resilience Hub memberikan informasi tambahan di tingkat aplikasi tentang perkiraan beban kerja RTO dan perkiraan beban kerjaRPO. Informasi tambahan ini menunjukk an perkiraan beban kerja maksimum yang mungkin RTO dan perkiraan beban kerja aplikasi Anda RPO dari penilaian sukses terbaru. Nilai ini adalah perkiraan beban kerja maksimum RTO dan perkiraan beban kerja RPO dari semua jenis gangguan. Untuk informasi selengkap nya, lihat the section called “Mengelola aplikasi”.	30 Oktober 2023

AWS Resilience Hub memperluas dukungan penilaian untuk sumber daya AWS Step Functions	AWS Resilience Hub memperluas dukungan penilaian untuk AWS Step Functions sumber daya sambil menilai ketahanan aplikasi Anda. AWS Resilience Hub menganalisis AWS Step Functions konfigurasi termasuk jenis mesin status (baik alur kerja Standar atau Ekspres). Selain itu, juga AWS Resilience Hub akan memberikan rekomendasi yang membantu Anda untuk memenuhi perkiraan beban kerja Recovery Time Objectives (RTO) dan perkiraan beban kerja Recovery Point Objectives (RPO). Untuk menilai aplikasi termasuk AWS Step Functions sumber daya, Anda harus menyiapkan izin yang diperlukan, baik dengan menggunakan kebijakan AWS terkelola atau dengan menambahkan izin khusus secara manual AWS Resilience Hub untuk mengizinkan membaca AWS Step Functions konfigurasi. Untuk informasi selengkapnya tentang izin terkait, lihatthe section called “AWSResilienceHubAsssessmentExecutionPolicy”.	30 Oktober 2023

AWS Resilience Hub memungkinkan Mengecualikan Rekomendasi Operasional	AWS Resilience Hub menambahkan kemampuan bagi Anda untuk mengecualikan rekomendasi operasional termasuk alarm, prosedur operasi standar (SOPs), dan Amazon Fault Injection Service (AWS FIS) pengujian. Saat menjalankan penilaian AWS Resilience Hub, Anda diberikan perkiraan waktu pemulihan dan rekomendasi tentang cara-cara untuk meningkatkan ketahanan aplikasi yang dinilai. Dengan menggunakan alur kerja rekomendasi pengecualian, Anda sekarang akan memiliki kemampuan untuk mengecualikan alarm yang disarankan,SOPs, dan AWS FIS tes yang tidak relevan untuknya. Alur kerja pengecualian bermanfaat jika Anda menggunakan platform di luar yang disarankan, atau telah menerapkan rekomendasi dalam metode alternatif. Untuk informasi selengkapnya, lihat topik berikut. • the section called “Termasuk atau tidak termasuk rekomendasi operasional”	9 Agustus 2023

	• the section called “Membatasi izin untuk menyertakan atau mengecualikan rekomendasi AWS Resilience Hub ”	
Meningkatkan desain izin untuk AWS Resilience Hub	AWS Resilience Hub memperkenalkan desain izin baru untuk memberikan fleksibilitas saat mengonfig urasi peran AWS Identity and Access Management (IAM) untuk. AWS Resilienc e Hub Ini juga menggabun gkan izin ke dalam satu peran, dengan kemampuan untuk membuat nama peran khusus yang berarti bagi Anda dan tim Anda. Kebijakan terkelola baru AWS Resilience Hub akan memungkinkan Anda memiliki izin yang sesuai untuk layanan yang didukung. Jika Anda merasa nyaman dengan metode pengatura n izin saat ini, kami akan terus mendukung konfigurasi manual. Untuk informasi selengkap nya tentang kebijakan AWS terkelola, lihatthe section called “AWSResilienceHubA sssessmentExecutionPolicy”.	2 Agustus 2023

Deteksi Drift Ketahanan Aplikasi dengan AWS Resilience Hub	AWS Resilience Hub memungkinkan Anda untuk secara proaktif mendeteksi dan memahami tindakan yang diperlukan untuk menyelesaikan ketahanan aplikasi. Mengaktifkan Amazon Simple Notification Service (AmazonSNS) untuk menerima notifikasi ketika estimasi target waktu pemulihan beban kerja (RTO) atau estimasi target titik pemulihan beban kerja (RPO) telah berubah dari memenuhi target menjadi tidak lagi memenuhi tujuan bisnis organisasi Anda. Beralih dari menemukan masalah ketahanan secara reaktif saat menjalankan penilaian secara manual menjadi diberitahukan secara proaktif melalui SNS topik Amazon akan memungkinkan Anda untuk mengantisipasi potensi gangguan lebih awal, dan memberikan keyakinan tambahan bahwa tujuan pemulihan akan tercapai. Untuk informasi selengkapnya, lihat topik berikut. • the section called “Langkah 5: Siapkan penilaian	2 Agustus 2023

terjadwal dan pemberita huan drift”

- the section called “Mengedit sumber daya aplikasi”

AWS Resilience Hub meningkatkan dukungan untuk Amazon Relational Database Service dan Amazon Aurora	AWS Resilience Hub memperluas dukungan penilaian untuk proxy Amazon Relational Database Service, serta konfigurasi database Headless dan Amazon Aurora DB. Selain itu, saat menilai aplikasi yang menyertakan AmazonRDS, kami sekarang akan membedakan antara mesin database yang berbeda untuk memberikan perkiraan waktu pemulihan beban kerja yang lebih tepat (RTOs). AWS Resilience Hub juga akan memberikan tindakan tambahan untuk menerapka n praktik terbaik ketahanan dalam lingkungan Anda AWS . Praktik terbaik dapat mencakup wawasan kinerja dengan DevOps Guru untuk AmazonRDS, pemantauan yang disempurnakan, dan otomatisasi penyebaran biru/ hijau pada mesin basis data yang didukung. Untuk mempelajari lebih lanjut tentang izin yang diperlukan AWS Resilience Hub untuk menyertakan sumber daya dari semua layanan yang didukung dalam penilaian Anda, lihatthe section called	2 Agustus 2023

	“AWSResilienceHubAsssessmentExecutionPolicy”.	
AWS Resilience Hub memperluas dukungan untuk snapshot Amazon Elastic Block Store	AWS Resilience Hub memperluas dukungan penilaian untuk Amazon Elastic Block Store (AmazonEBS) untuk mengenali EBS snapshot Amazon, yang diambil dalam EBS Wilayah Amazon yang sama menggunakan langsung. APIs Dukungan yang diperluas merupakan tambahan dukungan saat ini untuk pelanggan yang menggunakan Amazon Data Lifecycle Manager (Amazon Data Lifecycle Manager) atau Backup. AWS Untuk informasi selengkapnya, lihat Amazon Elastic Block Store (AmazonEBS).	2 Agustus 2023

Peningkatan Amazon Elastic Compute Cloud	AWS Resilience Hub telah memperluas dukungan untuk Amazon Elastic Compute Cloud (AmazonEC2). Untuk Aplikasi dengan ukuran berbeda, AWS memungkin kan pelanggannya yang menggunakan Amazon EC2 untuk memilih konfigurasi yang sesuai untuk kasus penggunaannya. AWS Resilience Hub mendukung penilaian pada EC2 konfigura si Amazon berikut: • Contoh sesuai permintaan. • Instans cadangan oleh AWS Backup dan AWS Elastic Disaster Recovery. • Support untuk grup auto-scaling dengan Amazon Route 53 Application Recovery Controller (Route 53) ARC Ke depan, dukungan penilaian akan diperluas untuk mencakup instans spot, host khusus, instans khusus, grup penempatan, dan armada. Untuk informasi selengkapnya, lihat the section called “AWS Resilience Hub referensi izin akses”.	Juni 27, 2023

AWS pembaruan kebijakan terkelola	Menambahkan kebijakan baru yang menyediakan akses ke AWS layanan lain untuk menjalankan penilaian. Untuk informasi selengkap nya, lihat the section called “AWSResilienceHubA sssessmentExecutionPolicy”.	26 Juni 2023
Alarm rekomendasi operasion al Amazon DynamoDB baru	Untuk aplikasi yang menggunakan Amazon DynamoDB AWS Resilienc e Hub , kini menyediakan serangkaian alarm baru yang mengingatkan Anda akan risiko ketahanan untuk mode kapasitas sesuai permintaa n dan penyediaan serta tabel global. Untuk mengakses alarm baru, Anda mungkin perlu memperbarui kebijakan AWS Identity and Access Management (IAM) peran yang Anda gunakan. Untuk informasi selengkapnya, lihat the section called “AWS Resilience Hub referensi izin akses”.	2 Mei 2023

AWS Trusted Advisor perangkat tambahan	AWS Resilience Hub telah memperluas dukungan untuk AWS Trusted Advisor dan aplikasi menggunak an Amazon DynamoDB. Saat Anda menggunak annya AWS Trusted Advisor AWS Resilience Hub, Anda sekarang dapat menerima pemberitahuan ketika aplikasi belum dinilai dalam 30 hari sebelumnya. Pemberita huan ini meminta Anda untuk menilai kembali aplikasi untuk memahami apakah ada perubahan yang akan memengaruhi ketahanannya. Untuk informasi lebih lanjut tentang pemeriksaan usia AWS Resilience Hub penilaian , lihatthe section called “AWS Trusted Advisor”.	2 Mei 2023

Dukungan tambahan untuk Amazon Simple Storage Service	Selain dukungan saat ini dari Amazon Simple Storage Service (Amazon S3) Simple Storage S3) Replikasi Lintas Wilayah (Amazon S3CRR) /Amazon S3 Same-Region Replication SRR (), pembuatan versi, dan AWS Backup, sekarang akan AWS Resilience Hub menilai Amazon S3 untuk jalur akses Multi-wilayah, Kontrol Waktu Replikasi Amazon S3 (Amazon S3), dan konfigurasi Backup recovery (). RTC AWS point-in-time PITR Untuk informasi selengkapnya, lihat topik berikut. • the section called “AWS Resilience Hub referensi izin akses” • Mengelola penyimpanan Amazon S3 Anda	21 Maret 2023

Dukungan tambahan untuk Amazon Elastic Kubernetes Service	AWS Resilience Hub telah menambahkan EKS klaster Amazon sebagai sumber daya yang didukung untuk mendefinisikan, memvalida si, dan melacak ketahanan aplikasi. Pelanggan dapat menambahkan EKS klaster Amazon ke aplikasi baru atau yang sudah ada, dan menerima penilaian dan rekomendasi untuk meningkat kan ketahanan. Pelanggan dapat menambahkan sumber daya aplikasi menggunak an AWS CloudFormation, Terraform, AWS Resource Groups, dan. AppRegist ry Selain itu, pelanggan dapat menambahkan satu atau beberapa EKS kluster Amazon secara langsung di satu atau beberapa Wilayah dengan satu atau lebih ruang nama di setiap cluster. Hal ini memungkinkan AWS Resilienc e Hub untuk memberikan penilaian dan rekomendasi tunggal dan lintas wilayah. Selain memeriksa penerapan , Replika, dan Pod Replicati onControllers, AWS Resilienc e Hub akan menganalisis ketahanan klaster secara keseluruhan. AWS Resilience Hub mendukung beban kerja	21 Maret 2023

	EKS klaster Amazon stateless . Kemampuan baru tersedia di semua AWS Wilayah di mana AWS Resilience Hub didukung. Untuk informasi selengkapnya, lihat topik berikut. • the section called “Langkah 2: Kelola sumber daya aplikasi Anda” • the section called “Tambahkan EKS cluster” • the section called “AWS Resilience Hub referensi izin akses” • AWS Layanan Regional	
Dukungan tambahan untuk Amazon Elastic File System	Selain dukungan saat ini untuk cadangan Amazon Elastic File System (AmazonEFS), sekarang AWS Resilience Hub akan menilai Amazon EFS untuk EFS replikasi Amazon dan konfigurasi AZ. Untuk informasi selengkapnya, lihat topik berikut. • the section called “ AWS Resilience Hub Sumber daya yang didukung” • Apa itu Amazon Elastic File System?	21 Maret 2023

Support untuk sumber input aplikasi	AWS Resilience Hub sekarang memberikan transparansi tentang sumber aplikasi Anda. Ini membantu Anda untuk menambahkan, menghapus , dan mengimpor kembali sumber input aplikasi Anda, dan menerbitkan versi aplikasi baru. Untuk informasi selengkap nya, lihat the section called “Mengedit sumber daya aplikasi”.	21 Februari 2023

Support untuk parameter konfigurasi aplikasi	AWS Resilience Hub sekarang menyediakan mekanisme masukan untuk mengumpulkan informasi tambahan tentang sumber daya yang terkait dengan aplikasi Anda. Dengan informasi ini, AWS Resilience Hub akan mendapatkan pemahaman yang lebih dalam tentang sumber daya Anda dan memberikan rekomendasi ketahanan yang lebih baik. Untuk informasi selengkapnya, lihat topik berikut. • the section called “Parameter konfigurasi aplikasi” • the section called “Langkah 7: Konfigurasikan parameter konfigurasi aplikasi” • the section called “Memperbarui parameter konfigurasi aplikasi”	21 Februari 2023

Dukungan tambahan untuk Amazon Elastic Block Store	Selain dukungan volume Amazon Elastic Block Store (AmazonEBS) saat ini, sekarang AWS Resilience Hub akan menilai EBS snapshot Amazon oleh Amazon Data Lifecycle Manager dan EBS Amazon fast snapshot restore (). FSR Untuk informasi selengkapnya, lihat topik berikut. • the section called “AWS Resilience Hub referensi izin akses” • Toko Blok Elastis Amazon (AmazonEBS)	21 Februari 2023

Integrasi dengan AWS Trusted Advisor	AWS Trusted Advisor pengguna akan dapat melihat aplikasi yang terkait dengan akun mereka yang telah dinilai oleh AWS Resilience Hub. AWS Trusted Advisor menunjukkan skor ketahanan terbaru dan memberikan status yang menunjukkan apakah kebijakan ketahanan yang ditargetkan (RTOdanRPO) telah terpenuhi atau tidak. Setiap kali penilaian dijalankan, AWS Resilience Hub update AWS Trusted Advisor dengan hasil terbaru. AWS Trusted Advisor adalah layanan yang terus menganalisis AWS akun Anda dan memberikan rekomendasi untuk membantu Anda mengikuti praktik AWS terbaik dan pedoman AWS Well-Architected. Untuk informasi selengkapnya, lihat the section called “AWS Trusted Advisor”.	18 November 2022

Support untuk Amazon Simple Notification Service (AmazonSNS)	AWS Resilience Hub sekarang menilai aplikasi yang menggunakan Amazon SNS dengan menganalisis SNS konfigurasi Amazon, termasuk pelanggan, dan memberikan rekomendasi untuk memenuhi perkiraan tujuan pemulihan beban kerja organisasi (perkiraan beban kerja RTO dan perkiraan beban kerjaRPO) untuk aplikasi. Amazon SNS adalah layanan terkelola yang mengirimkan pesan dari penerbit (produsen) ke pelanggan (konsumen). Untuk informasi selengkapnya, lihat topik berikut. • the section called “ AWS Resilience Hub Sumber daya yang didukung” • the section called “Identity and Access Management” • the section called “Mengelompokkan sumber daya dalam Komponen Aplikasi”	16 November 2022

Support Tambahan untuk Amazon Route 53 Application Recovery Controller (Amazon Route 53ARC)	AWS Resilience Hub sekarang menilai Amazon Route 53 ARC untuk Elastic Load Balancing dan Amazon Relational Database Service (RDSAmazon), yang mencakup memberi saran kapan Amazon Route 53 ARC akan bermanfaat. Memperlua s AWS Resilience Hub, dukungan ARC penilaian Amazon Route 53 di luar AWS Auto Scaling Group AWS ASG () dan Amazon DynamoDB. Amazon Route 53 ARC menyediakan ketersedi aan tinggi untuk aplikasi Anda, memungkinkan Anda untuk dengan cepat failover seluruh aplikasi Anda ke Wilayah failover. Untuk informasi selengkapnya, lihat topik berikut. • the section called “ AWS Resilience Hub Sumber daya yang didukung” • the section called “Identity and Access Management”	16 November 2022

Support Tambahan untuk AWS Backup	AWS Resilience Hub sekarang menilai Amazon Route 53 ARC untuk Elastic Load Balancing dan Amazon Relational Database Service (RDSAmazon), yang mencakup memberi saran kapan Amazon Route 53 ARC akan bermanfaat. Memperlua s AWS Resilience Hub, dukungan ARC penilaian Amazon Route 53 di luar AWS Auto Scaling Group AWS ASG () dan Amazon DynamoDB. Amazon Route 53 ARC menyediakan ketersedi aan tinggi untuk aplikasi Anda, memungkinkan Anda untuk dengan cepat failover seluruh aplikasi Anda ke Wilayah failover. Untuk informasi selengkapnya, lihat topik berikut. • the section called “ AWS Resilience Hub Sumber daya yang didukung” • the section called “Identity and Access Management”	16 November 2022
Konten yang diperbarui: Menambahkan sumber daya Komponen Aplikasi baru	Menambahkan Route53 dan AWS Backup ke daftar sumber daya Komponen Aplikasi yang didukung di bagian AppComponent pengelomp okan.	1 Juli 2022

Konten baru: Konsep status kepatuhan aplikasi	Ditambahkan Perubahan terdeteksi jenis status.	2 Juni 2022
Memperkenalkan AWS Resilience Hub	AWS Resilience Hub sekarang tersedia. Panduan ini menjelaskan AWS Resilienc e Hub cara menggunakan infrastruktur Anda, mendapatk an rekomendasi untuk meningkatkan ketahanan AWS aplikasi Anda, meninjau skor ketahanan, dan banyak lagi.	November 10, 2021

Daftar istilah AWS

Untuk terminologi AWS terbaru, lihat Daftar istilah AWS di Referensi Glosarium AWS.

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