Menerapkan kebijakan untuk izin hak istimewa paling rendah untuk AWS CloudFormation

AWS Bimbingan Preskriptif

AWS Bimbingan Preskriptif: Menerapkan kebijakan untuk izin hak istimewa paling rendah untuk AWS CloudFormation

Table of Contents

Menerapkan kebijakan untuk izin hak istimewa paling rendah untuk AWS CloudFormation

Nima Fotouhi dan Moumita Saha, Amazon Web Services ()AWS

Mei 2023 (riwayat dokumen)

AWS CloudFormationadalah layanan infrastruktur sebagai kode (IAc) yang membantu Anda meningkatkan skala pengembangan infrastruktur cloud Anda dengan menyediakan sumber daya. AWS Ini juga membantu Anda mengelola sumber daya tersebut sepanjang siklus hidupnya, di seluruh Akun AWS dan. Wilayah AWS Di CloudFormation, Anda mendefinisikan template, yang bertindak sebagai cetak biru untuk satu set sumber daya. Anda kemudian menyediakan sumber daya tersebut dengan membuat dan menerapkan tumpukan, yang merupakan sekelompok sumber daya terkait yang Anda kelola sebagai satu unit. Anda juga dapat menggunakan CloudFormation untuk menyebarkan kumpulan tumpukan, yang merupakan grup tumpukan yang dapat Anda buat, perbarui, dan hapus di beberapa akun dan Wilayah AWS dengan satu operasi. Panduan ini memberikan gambaran umum tentang bagaimana Anda dapat menerapkan izin hak istimewa paling sedikit untuk AWS CloudFormation dan sumber daya yang disediakan. CloudFormation

Anda dapat menerapkan CloudFormation tumpukan atau set tumpukan dengan melakukan salah satu hal berikut:

- Akses langsung AWS lingkungan melalui prinsipal AWS Identity and Access Management (IAM) dan gunakan tumpukan CloudFormation .
- Dorong CloudFormation tumpukan dalam pipeline penerapan dan mulai penyebaran tumpukan melalui pipeline. Pipa mengakses AWS lingkungan melalui prinsip IAM dan menyebarkan tumpukan. Pendekatan ini adalah praktik terbaik yang direkomendasikan.

Untuk salah satu dari pendekatan ini, izin diperlukan untuk menyebarkan tumpukan CloudFormation . Misalnya, pertimbangkan pengguna yang berencana menggunakannya CloudFormation untuk membuat instance Amazon Elastic Compute Cloud (Amazon EC2). Contoh itu akan membutuhkan profil instance IAM untuk mengakses yang lain Layanan AWS. Prinsip IAM yang digunakan untuk menyebarkan CloudFormation tumpukan akan memerlukan izin berikut:

- Izin untuk mengakses CloudFormation
- Izin untuk membuat tumpukan di CloudFormation

- Izin untuk membuat instance di Amazon EC2
- Izin untuk membuat profil instans IAM yang diperlukan

Apa itu hak istimewa yang paling tidak?

Keistimewaan paling sedikit adalah praktik keamanan terbaik untuk memberikan izin minimum yang diperlukan untuk melakukan tugas. Prinsip hak istimewa terkecil adalah bagian dari pilar Keamanan dalam Kerangka AWS Well-Architected. Ketika Anda menerapkan praktik terbaik ini, ini dapat membantu melindungi AWS lingkungan Anda dari risiko eskalasi hak istimewa, mengurangi permukaan serangan, meningkatkan keamanan data, dan mencegah kesalahan pengguna (seperti salah konfigurasi atau menghapus sumber daya secara tidak sengaja).

Untuk menerapkan hak istimewa paling sedikit untuk AWS sumber daya Anda, Anda mengonfigurasi kebijakan, seperti kebijakan berbasis identitas di AWS Identity and Access Management (IAM). Kebijakan ini menentukan izin dan menentukan kondisi akses. Organizations mungkin memulai dengan kebijakan AWS terkelola, tetapi kemudian mereka biasanya membuat kebijakan khusus yang membatasi ruang lingkup izin hanya untuk tindakan yang diperlukan untuk beban kerja atau kasus penggunaan.

Izin hak istimewa paling sedikit untuk CloudFormation layanan ini merupakan pertimbangan keamanan yang penting. Karena pengguna dan pengembang yang berinteraksi CloudFormation dapat memiliki kemampuan untuk dengan cepat membuat, memodifikasi, atau menghapus sumber daya dalam skala besar, hak istimewa paling sedikit sangat penting. Namun, CloudFormation memerlukan izin yang diperlukan untuk membuat, memperbarui, dan memodifikasi sumber daya di Anda Akun AWS. Anda harus menyeimbangkan kebutuhan akan izin untuk beroperasi CloudFormation dengan prinsip hak istimewa paling sedikit.

Saat menerapkan prinsip hak istimewa paling sedikit CloudFormation, Anda perlu mempertimbangkan hal berikut:

- Izin untuk CloudFormation layanan — Pengguna mana yang memerlukan akses CloudFormation, tingkat akses apa yang mereka butuhkan, dan tindakan apa yang dapat mereka ambil untuk membuat, memperbarui, atau menghapus tumpukan?
- Izin untuk menyediakan sumber daya — Sumber daya apa yang dapat disediakan pengguna? CloudFormation
- Izin untuk sumber daya yang disediakan — Bagaimana Anda mengonfigurasi izin hak istimewa terkecil untuk sumber daya yang Anda sediakan? CloudFormation

Hasil bisnis yang ditargetkan

Dengan mengikuti praktik dan rekomendasi terbaik dalam panduan ini, Anda dapat:

- Tentukan pengguna mana di organisasi Anda yang memerlukan akses CloudFormation, lalu konfigurasikan izin hak istimewa paling sedikit untuk pengguna tersebut.
- Gunakan kebijakan tumpukan untuk membantu melindungi CloudFormation tumpukan dari pembaruan yang tidak diinginkan.
- Konfigurasikan izin hak istimewa paling sedikit untuk CloudFormation pengguna dan sumber daya untuk membantu mencegah eskalasi hak istimewa dan masalah wakil yang membingungkan.
- Gunakan AWS CloudFormation untuk menyediakan AWS sumber daya dengan izin hak istimewa paling sedikit. Ini membantu organisasi Anda mempertahankan postur keamanan yang lebih kuat.
- Secara proaktif mengurangi jumlah waktu, energi, dan uang yang dibutuhkan untuk menyelidiki dan mengurangi insiden keamanan.

Audiens yang dituju

Panduan ini ditujukan untuk Arsitek Infrastruktur Cloud, DevOps insinyur, dan insinyur keandalan situs (SREs) yang mengelola dan menyediakan sumber daya dengan menggunakan CloudFormation.

Menggunakan kebijakan akses untuk memberikan izin di AWS

Anda mengelola akses AWS dengan membuat kebijakan berbasis identitas dan melampirkannya ke prinsipal AWS Identity and Access Management (IAM), seperti peran atau pengguna, dan dengan membuat kebijakan berbasis sumber daya dan melampirkannya ke sumber daya. AWS AWS mengevaluasi kebijakan ini setiap kali permintaan dibuat. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak.

Untuk memahami cara mengonfigurasi akses hak istimewa paling sedikit dalam kebijakan, Anda perlu memahami berbagai jenis kebijakan, elemen dan struktur kebijakan, dan bagaimana kebijakan dievaluasi. Panduan ini hanya berfokus pada kebijakan berbasis identitas dan kebijakan berbasis sumber daya. Namun, AWS menyediakan jenis kebijakan lain, seperti kebijakan kontrol layanan (SCPs), batas izin, dan kebijakan sesi. Setiap jenis kebijakan berperan dalam menerapkan izin hak istimewa paling sedikit di Anda. Akun AWS Untuk informasi selengkapnya, lihat Kebijakan dan izin dan Menerapkan izin hak istimewa paling sedikit dalam dokumentasi IAM.

Mengonfigurasi izin hak istimewa paling sedikit untuk digunakan CloudFormation

Bab ini mengulas opsi untuk mengonfigurasi izin untuk mengakses dan menggunakan layanan. AWS CloudFormation

Ketika pengguna atau layanan menyediakan sumber AWS daya melalui CloudFormation, langkah pertama adalah melakukan panggilan ke CloudFormation layanan melalui AWS Identity and Access Management (IAM) prinsipal. Prinsipal IAM ini harus memiliki izin untuk membuat tumpukan. CloudFormation Selanjutnya, prinsipal IAM menggunakan salah satu pendekatan berikut untuk menyediakan sumber daya melalui CloudFormation:

- Jika prinsipal IAM tidak meneruskan operasi tumpukan ke peran CloudFormation layanan, CloudFormation gunakan kredensi prinsipal IAM untuk melakukan operasi tumpukan. Ini adalah default. Oleh karena itu, selain izin untuk melakukan operasi CloudFormation tumpukan, prinsipal IAM juga memerlukan izin untuk menyediakan sumber daya yang ditentukan dalam CloudFormation templat yang akan mereka gunakan. Misalnya, jika prinsipal IAM tidak memiliki izin untuk membuat instans Amazon Elastic Compute Cloud (Amazon EC2), maka mereka tidak dapat membuat CloudFormation tumpukan yang akan menyediakan instance Amazon. EC2
- Jika prinsipal IAM meneruskan operasi tumpukan ke peran CloudFormation layanan, maka CloudFormation gunakan peran layanan untuk melakukan operasi tumpukan dan menyediakan sumber daya dalam CloudFormation template. Peran CloudFormation layanan ini harus didefinisikan dengan izin untuk menyediakan Layanan AWS atas nama prinsipal IAM. Pendekatan ini menghindari pemberian izin langsung ke prinsipal IAM untuk menyediakan AWS sumber daya yang ditentukan dalam templat. CloudFormation Prinsipal IAM membutuhkan izin pembuatan CloudFormation tumpukan, dan CloudFormation menggunakan kebijakan peran layanan untuk melakukan panggilan alih-alih kebijakan prinsipal IAM.

Dengan menggunakan pendekatan peran layanan dan prinsip hak istimewa terkecil, Anda dapat membakukan penyediaan sumber daya di AWS lingkungan Anda dan mengharuskan pengguna menyediakan sumber daya sebagai IAc. CloudFormation Karena kebijakan yang dilampirkan pada prinsipal IAM tidak berisi izin untuk menyediakan AWS sumber daya secara langsung, pengguna harus menggunakannya untuk menyediakannya. CloudFormation

Bab ini mengulas mekanisme berikut untuk mengonfigurasi dan mengelola akses ke CloudFormation layanan dan CloudFormation tumpukan:

- Kebijakan berbasis identitas untuk CloudFormation— Gunakan jenis kebijakan ini untuk mengonfigurasi prinsipal IAM mana yang dapat diakses CloudFormation dan tindakan apa yang dapat mereka lakukan. CloudFormation
- Peran layanan untuk CloudFormation— Buat peran layanan yang memungkinkan CloudFormation untuk membuat, memperbarui, atau menghapus sumber daya tumpukan atas nama kepala IAM yang menyebarkan tumpukan. Peran layanan dibuat di IAM dan dapat dikaitkan dengan satu atau lebih tumpukan.
- CloudFormation kebijakan tumpukan— Gunakan jenis kebijakan ini untuk menentukan kapan tumpukan dapat diperbarui. Jenis kebijakan ini dapat membantu mencegah sumber daya tumpukan diperbarui atau dihapus secara tidak sengaja. Kebijakan tumpukan dibuat dan dikaitkan dengan tumpukan di CloudFormation.

Kebijakan berbasis identitas untuk CloudFormation

Pertimbangkan jenis pengguna yang membutuhkan akses AWS CloudFormation, dan pertimbangkan tindakan mana yang perlu dilakukan pengguna tersebut CloudFormation. Anda mengonfigurasi izin pengguna melalui kebijakan berbasis identitas, yang Anda lampirkan ke prinsipal AWS Identity and Access Management (IAM), seperti peran atau pengguna.

Saat Anda mengonfigurasi kebijakan berbasis identitas, elemen `Effect`, `Action`, dan `Resource` elemen diperlukan. Anda juga dapat mendefinisikan `Condition` elemen secara opsional. Untuk informasi selengkapnya tentang elemen-elemen ini, lihat referensi elemen kebijakan IAM JSON.

Bagian ini berisi topik berikut:

- Praktik terbaik untuk mengonfigurasi kebijakan berbasis identitas untuk akses hak istimewa paling sedikit CloudFormation
- Contoh kebijakan berbasis identitas untuk CloudFormation

Praktik terbaik untuk mengonfigurasi kebijakan berbasis identitas untuk akses hak istimewa paling sedikit CloudFormation

- Untuk kepala sekolah IAM yang memerlukan izin untuk mengakses CloudFormation, Anda harus menyeimbangkan kebutuhan izin untuk beroperasi CloudFormation dengan prinsip hak istimewa paling sedikit. Untuk membantu Anda mematuhi prinsip hak istimewa terkecil, kami sarankan Anda mendefinisikan identitas kepala sekolah IAM berdasarkan tindakan spesifik yang memungkinkan prinsipal melakukan hal berikut:
  - Buat, perbarui, dan hapus CloudFormation tumpukan.
  - Lulus satu atau beberapa peran layanan yang memiliki izin yang diperlukan untuk menyebarkan sumber daya yang ditentukan dalam templat. CloudFormation Hal ini memungkinkan CloudFormation untuk mengambil peran layanan dan menyediakan sumber daya dalam tumpukan atas nama prinsipal IAM.
- Eskalasi hak istimewa mengacu pada kemampuan pengguna dengan akses, untuk meningkatkan tingkat izin mereka dan membahayakan keamanan. Keistimewaan paling sedikit adalah praktik terbaik penting yang dapat membantu mencegah eskalasi hak istimewa. Karena CloudFormation mendukung penyediaan jenis sumber daya IAM, seperti kebijakan dan peran, prinsipal IAM dapat meningkatkan hak istimewa mereka melalui: CloudFormation
  - Menggunakan CloudFormation tumpukan untuk menyediakan prinsipal IAM dengan izin, kebijakan, atau kredensional yang sangat istimewa — Untuk membantu mencegah hal ini, sebaiknya gunakan pagar pembatas izin untuk membatasi tingkat akses bagi prinsipal IAM. Pagar pembatas izin menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada prinsipal IAM. Ini membantu mencegah eskalasi hak istimewa yang disengaja dan tidak disengaja. Anda dapat menggunakan jenis kebijakan berikut sebagai pagar pembatas izin:
    - Batas izin menentukan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada prinsipal IAM. Untuk informasi selengkapnya, lihat Batas izin untuk entitas IAM.
    - Di AWS Organizations, Anda dapat menggunakan kebijakan kontrol layanan (SCPs) untuk menentukan izin maksimum yang tersedia di tingkat organisasi. SCPs hanya memengaruhi peran IAM dan pengguna yang dikelola oleh akun di organisasi. Anda dapat melampirkan SCPs ke akun, unit organisasi, atau ke akar organisasi. Untuk informasi selengkapnya, lihat efek SCP pada izin.

- Membuat peran CloudFormation layanan yang menawarkan izin ekstensif — Untuk membantu mencegah hal ini, sebaiknya Anda menambahkan izin berbutir halus berikut ke kebijakan berbasis identitas untuk prinsipal IAM yang akan menggunakan: CloudFormation
  - Gunakan tombol `cloudformation:RoleARN` kondisi untuk mengontrol peran CloudFormation layanan mana yang dapat digunakan oleh prinsipal IAM.
  - Izinkan `iam:PassRole` tindakan hanya untuk peran CloudFormation layanan tertentu yang harus dilewati oleh kepala sekolah IAM.

  Untuk informasi selengkapnya, lihat Memberikan izin utama IAM untuk menggunakan peran layanan CloudFormation dalam panduan ini.
- Batasi izin dengan menggunakan pagar pembatas izin, seperti batas izin dan SCPs, dan berikan izin dengan menggunakan kebijakan berbasis identitas atau berbasis sumber daya.

Contoh kebijakan berbasis identitas untuk CloudFormation

Bagian ini berisi contoh kebijakan berbasis identitas yang menunjukkan cara memberikan dan menolak izin. CloudFormation Anda dapat menggunakan contoh kebijakan ini untuk mulai merancang kebijakan Anda sendiri yang mematuhi prinsip hak istimewa paling sedikit.

Untuk daftar tindakan dan kondisi CloudFormation tertentu, lihat Tindakan, sumber daya, dan kunci kondisi untuk AWS CloudFormation dan AWS CloudFormation kondisi. Untuk daftar jenis sumber daya yang akan digunakan dengan kondisi, lihat referensi jenis AWS sumber daya dan properti.

Bagian ini berisi contoh kebijakan berikut:

- Izinkan akses tampilan
- Izinkan pembuatan tumpukan berdasarkan template
- Tolak pembaruan atau penghapusan tumpukan

Izinkan akses tampilan

Akses tampilan adalah jenis akses yang paling tidak memiliki hak istimewa. CloudFormation Kebijakan semacam ini mungkin sesuai untuk para kepala sekolah IAM yang ingin melihat semua tumpukan di CloudFormation. Akun AWS Kebijakan contoh berikut memberikan izin untuk melihat detail CloudFormation tumpukan apa pun di akun.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStackResources"
      ],
      "Resource": "*"
    }
  ]
}
```

Izinkan pembuatan tumpukan berdasarkan template

Kebijakan contoh berikut memungkinkan prinsipal IAM untuk membuat tumpukan hanya dengan menggunakan CloudFormation templat yang disimpan di bucket Amazon Simple Storage Service (Amazon S3) tertentu. Nama bucket adalah`my-CFN-templates`. Anda dapat mengunggah templat yang disetujui ke bucket ini. Kunci `cloudformation:TemplateUrl` kondisi dalam kebijakan mencegah prinsipal IAM menggunakan templat lain untuk membuat tumpukan.

> **Important**
>
> Izinkan prinsipal IAM memiliki akses hanya-baca ke bucket S3 ini. Ini membantu mencegah prinsipal IAM menambahkan, menghapus, atau memodifikasi templat yang disetujui.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "cloudformation:TemplateUrl": "https:// my-CFN-templates.s3.amazonaws.com/*"
```

```
        }
      }
    }
  ]
}
```

Tolak pembaruan atau penghapusan tumpukan

Untuk membantu melindungi CloudFormation tumpukan tertentu yang menyediakan AWS sumber daya penting bisnis, Anda dapat membatasi tindakan pembaruan dan penghapusan untuk tumpukan tertentu. Anda dapat mengizinkan tindakan ini hanya untuk beberapa prinsip IAM tertentu dan menolaknya untuk prinsip IAM lainnya di lingkungan. Pernyataan kebijakan berikut ini menolak izin untuk memperbarui atau menghapus CloudFormation tumpukan tertentu dalam tumpukan tertentu Wilayah AWS dan. Akun AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "cloudformation:DeleteStack",
        "cloudformation:UpdateStack"
      ],
      "Resource": "arn:aws:cloudformation:us-east-1:123456789012:stack/
MyProductionStack/<stack_ID>"
    }
  ]
}
```

Pernyataan kebijakan ini menolak izin untuk memperbarui atau menghapus `MyProductionStack` CloudFormation tumpukan, yang ada di dalam `us-east-1` Wilayah AWS dan di. `123456789012` Akun AWS Anda dapat melihat ID tumpukan di CloudFormation konsol. Berikut ini adalah beberapa contoh bagaimana Anda dapat memodifikasi `Resource` elemen pernyataan ini untuk kasus penggunaan Anda:

- Anda dapat menambahkan beberapa CloudFormation tumpukan IDs dalam `Resource` elemen kebijakan ini.

- Anda dapat menggunakan `arn:aws:cloudformation:us-east-1:123456789012:stack/*` untuk mencegah prinsipal IAM memperbarui atau menghapus tumpukan apa pun yang ada di dalam dan di `us-east-1` Wilayah AWS akun. `123456789012`

Langkah penting adalah memutuskan kebijakan mana yang harus berisi pernyataan ini. Anda dapat menambahkan pernyataan ini ke kebijakan berikut:

- Kebijakan berbasis identitas yang dilampirkan pada prinsipal IAM — Menempatkan pernyataan dalam kebijakan ini membatasi prinsipal IAM tertentu untuk membuat atau menghapus tumpukan tertentu. CloudFormation
- Batas izin yang dilampirkan pada prinsipal IAM — Menempatkan pernyataan dalam kebijakan ini akan membuat pagar pembatas izin. Ini membatasi lebih dari satu prinsipal IAM untuk membuat atau menghapus CloudFormation tumpukan tertentu, tetapi tidak membatasi semua prinsip di lingkungan Anda.
- SCP yang dilampirkan ke akun, unit organisasi, atau organisasi — Menempatkan pernyataan dalam kebijakan ini akan membuat pagar pembatas izin. Ini membatasi semua prinsip IAM di akun target, unit organisasi, atau organisasi dari membuat atau menghapus tumpukan tertentu. CloudFormation

  Namun, jika Anda tidak mengizinkan setidaknya satu prinsipal IAM, prinsipal istimewa, untuk memperbarui atau menghapus CloudFormation tumpukan, maka Anda tidak akan dapat membuat perubahan apa pun, bila perlu, pada sumber daya yang disediakan melalui tumpukan ini. Pengguna atau pipeline pengembangan (disarankan) dapat mengasumsikan prinsipal istimewa ini. Jika Anda ingin menerapkan pembatasan sebagai SCP, maka kami merekomendasikan pernyataan kebijakan berikut sebagai gantinya.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "cloudformation:DeleteStack",
        "cloudformation:UpdateStack"
      ],
      "Resource": "arn:aws:cloudformation:us-east-1:123456789012:stack/
MyProductionStack/<stack_ID>",
      "Condition": {
```

```
        "ArnNotLike": {
          "aws:PrincipalARN": [
            "<ARN of the allowed privilege IAM principal>"
          ]
        }
      }
    }
  ]
}
```

Dalam pernyataan ini, `Condition` elemen mendefinisikan prinsip IAM yang dikecualikan dari SCP. Pernyataan ini menolak izin utama IAM untuk memperbarui atau menghapus CloudFormation tumpukan kecuali ARN dari prinsipal IAM cocok dengan ARN dalam elemen. `Condition` Kunci `aws:PrincipalARN` kondisi menerima daftar, yang berarti Anda dapat mengecualikan lebih dari satu prinsip IAM dari batasan, sebagaimana diperlukan untuk lingkungan Anda. Untuk SCP serupa yang mencegah modifikasi CloudFormation sumber daya, lihat SCP-CLOUDFORMATION-1 (). GitHub

Peran layanan untuk CloudFormation

Peran layanan adalah peran AWS Identity and Access Management (IAM) yang memungkinkan AWS CloudFormation untuk membuat, memperbarui, atau menghapus sumber daya tumpukan. Jika Anda tidak memberikan peran layanan, CloudFormation gunakan kredensil prinsipal IAM untuk melakukan operasi tumpukan. Jika Anda membuat peran layanan untuk CloudFormation dan menentukan peran layanan selama pembuatan tumpukan, CloudFormation gunakan kredensional peran layanan untuk melakukan operasi, bukan kredenal prinsipal IAM.

Saat menggunakan peran layanan, kebijakan berbasis identitas yang dilampirkan pada prinsipal IAM tidak memerlukan izin untuk menyediakan semua AWS sumber daya yang ditentukan dalam templat. CloudFormation Jika Anda tidak siap untuk menyediakan AWS sumber daya untuk operasi bisnis penting melalui pipa pengembangan (praktik terbaik yang AWS disarankan), menggunakan peran layanan dapat menambahkan lapisan perlindungan tambahan untuk manajemen sumber daya di AWS. Manfaat dari pendekatan ini adalah:

- Prinsipal IAM di organisasi Anda mengikuti model hak istimewa terkecil yang mencegah mereka membuat atau mengubah sumber daya secara manual di lingkungan Anda. AWS

- Untuk membuat, memperbarui, atau menghapus AWS sumber daya, prinsipal IAM harus menggunakan. CloudFormation Ini menstandarisasi penyediaan sumber daya melalui infrastruktur sebagai kode.

Misalnya, untuk membuat tumpukan yang berisi instans Amazon Elastic Compute Cloud (Amazon EC2), prinsipal IAM harus memiliki izin untuk membuat EC2 instance melalui kebijakan berbasis identitas mereka. Sebagai gantinya, CloudFormation dapat mengambil peran layanan yang memiliki izin untuk membuat EC2 instance atas nama kepala sekolah. Dengan pendekatan ini, prinsipal IAM dapat membuat tumpukan, dan Anda tidak perlu memberikan izin yang terlalu luas kepada prinsipal IAM untuk layanan yang seharusnya tidak mereka akses reguler.

Untuk menggunakan peran layanan untuk membuat CloudFormation tumpukan, kepala sekolah IAM harus memiliki izin untuk meneruskan peran layanan CloudFormation, dan kebijakan kepercayaan dari peran layanan harus memungkinkan untuk mengambil peran tersebut. CloudFormation

Bagian ini berisi topik berikut:

- Menerapkan hak istimewa paling sedikit untuk peran CloudFormation layanan
- Mengkonfigurasi peran layanan
- Memberikan izin utama IAM untuk menggunakan peran layanan CloudFormation
- Mengonfigurasi kebijakan kepercayaan untuk peran CloudFormation layanan
- Mengaitkan peran layanan dengan tumpukan

Menerapkan hak istimewa paling sedikit untuk peran CloudFormation layanan

Dalam peran layanan, Anda menentukan kebijakan izin yang secara eksplisit menentukan tindakan yang dapat dilakukan layanan. Ini mungkin bukan tindakan yang sama yang dapat dilakukan oleh kepala sekolah IAM. Kami menyarankan Anda bekerja mundur dari CloudFormation template Anda untuk membuat peran layanan yang mematuhi prinsip hak istimewa paling sedikit.

Mencakup kebijakan berbasis identitas dari kepala sekolah IAM dengan benar untuk hanya melewati peran layanan tertentu dan melingkupi kebijakan kepercayaan peran layanan untuk memungkinkan hanya kepala sekolah tertentu untuk mengambil peran membantu mencegah kemungkinan eskalasi hak istimewa melalui peran layanan.

Mengkonfigurasi peran layanan

> **Note**
>
> Peran layanan dikonfigurasi di IAM. Untuk membuat peran layanan, Anda harus memiliki izin untuk melakukannya. Prinsipal IAM dengan izin untuk membuat peran dan melampirkan kebijakan apa pun dapat meningkatkan izin mereka sendiri. AWS merekomendasikan membuat satu peran layanan untuk masing-masing Layanan AWS untuk setiap kasus penggunaan. Setelah membuat peran CloudFormation layanan untuk kasus penggunaan, Anda dapat mengizinkan pengguna untuk hanya meneruskan peran layanan yang disetujui CloudFormation. Untuk contoh kebijakan berbasis identitas yang memungkinkan pengguna membuat peran layanan, lihat Izin peran layanan dalam dokumentasi IAM.

Untuk petunjuk tentang cara membuat peran layanan, lihat Membuat peran untuk mendelegasikan izin ke. Layanan AWS Tentukan CloudFormation (`cloudformation.amazonaws.com`) sebagai layanan yang dapat mengasumsikan peran tersebut. Ini mencegah prinsipal IAM dari mengambil peran itu sendiri atau meneruskannya ke layanan lain. Saat Anda mengonfigurasi peran layanan`Effect`, elemen`Action`, dan `Resource` elemen diperlukan. Anda juga dapat mendefinisikan `Condition` elemen secara opsional.

Untuk informasi selengkapnya tentang elemen-elemen ini, lihat referensi elemen kebijakan IAM JSON. Untuk daftar lengkap tindakan, sumber daya, dan kunci kondisi, lihat Tindakan, sumber daya, dan kunci kondisi untuk Manajemen Identitas dan Akses.

Memberikan izin utama IAM untuk menggunakan peran layanan CloudFormation

Untuk menyediakan sumber daya CloudFormation melalui dengan menggunakan peran CloudFormation layanan, prinsipal IAM harus memiliki izin untuk lulus peran layanan. Anda dapat membatasi izin kepala sekolah IAM untuk hanya meneruskan peran tertentu dengan menentukan ARN peran dalam izin kepala sekolah. Untuk informasi selengkapnya, lihat Memberikan izin pengguna untuk meneruskan peran ke dokumentasi Layanan AWS IAM.

Pernyataan kebijakan berbasis identitas IAM berikut memungkinkan prinsipal untuk melewati peran, termasuk peran layanan, yang ada di jalurnya. `cfnroles` Kepala sekolah tidak dapat melewati peran yang berada di jalur yang berbeda.

```
{
"Sid": "AllowPassingAppRoles",
"Effect": "Allow",
"Action": "iam:PassRole",
"Resource": "arn:aws:iam::<account ID>:role/cfnroles/*"
}
```

Pendekatan lain untuk membatasi prinsipal pada peran tertentu adalah dengan menggunakan awalan untuk CloudFormation nama peran layanan. Pernyataan kebijakan berikut memungkinkan prinsipal IAM untuk hanya meneruskan peran yang memiliki awalan. `CFN-`

```
{
"Sid": "AllowPassingAppRoles",
"Effect": "Allow",
"Action": "iam:PassRole",
"Resource": "arn:aws:iam::<account ID>:role/CFN-*"
}
```

Selain pernyataan kebijakan sebelumnya, Anda dapat menggunakan kunci `cloudformation:RoleARN` kondisi untuk memberikan kontrol lebih lanjut dalam kebijakan berbasis identitas, untuk akses hak istimewa paling sedikit. Pernyataan kebijakan berikut memungkinkan prinsipal IAM untuk membuat, memperbarui, dan menghapus tumpukan hanya jika mereka melewati peran CloudFormation layanan tertentu. Sebagai variasi, Anda dapat menentukan lebih ARNs dari satu peran CloudFormation layanan dalam kunci kondisi.

```
{
  "Sid": "RestrictCloudFormationAccess",
  "Effect": "Allow",
  "Action": [
    "cloudformation:CreateStack",
    "cloudformation:DeleteStack",
    "cloudformation:UpdateStack"
  ],
  "Resource": "arn:aws:iam::<account ID>:role/CFN-*",
  "Condition": {
    "StringEquals": {
      "cloudformation:RoleArn": [
        "<ARN of the specific CloudFormation service role>"
      ]
    }
```

```
  }
}
```

Selain itu Anda juga dapat menggunakan kunci `cloudformation:RoleARN` kondisi untuk membatasi prinsipal IAM agar tidak melewati peran CloudFormation layanan yang sangat istimewa untuk operasi tumpukan. Satu-satunya perubahan yang diperlukan adalah di operator bersyarat, dari `StringEquals` ke`StringNotEquals`.

```
{
  "Sid": "RestrictCloudFormationAccess",
  "Effect": "Allow",
  "Action": [
    "cloudformation:CreateStack",
    "cloudformation:DeleteStack",
    "cloudformation:UpdateStack"
  ],
  "Resource": "arn:aws:iam::<account ID>:role/CFN-*",
  "Condition": {
    "StringNotEquals": {
      "cloudformation:RoleArn": [
        "<ARN of a privilege CloudFormation service role>"
      ]
    }
  }
}
```

Mengonfigurasi kebijakan kepercayaan untuk peran CloudFormation layanan

Kebijakan kepercayaan peran adalah kebijakan berbasis sumber daya wajib yang melekat pada peran IAM. Kebijakan kepercayaan mendefinisikan prinsip-prinsip IAM mana yang dapat mengambil peran tersebut. Dalam kebijakan kepercayaan, Anda dapat menentukan pengguna, peran, akun, atau layanan sebagai prinsipal. Untuk mencegah prinsipal IAM meneruskan peran layanan CloudFormation ke layanan lain, Anda dapat menentukan CloudFormation sebagai prinsipal dalam kebijakan kepercayaan peran.

Kebijakan kepercayaan berikut hanya memungkinkan CloudFormation layanan untuk mengambil peran layanan.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": {
      "Service": "cloudformation.amazonaws.com"
    },
    "Action": "sts:AssumeRole"
  }
}
```

Mengaitkan peran layanan dengan tumpukan

Setelah peran layanan dibuat, Anda dapat mengaitkannya dengan tumpukan saat membuat tumpukan. Untuk informasi selengkapnya, lihat Mengkonfigurasi opsi tumpukan. Sebelum Anda menentukan peran layanan, pastikan bahwa kepala sekolah IAM memiliki izin untuk meneruskannya. Untuk informasi selengkapnya, lihat Memberikan izin utama IAM untuk menggunakan peran layanan CloudFormation .

CloudFormation kebijakan tumpukan

Kebijakan tumpukan dapat membantu mencegah sumber daya tumpukan diperbarui atau dihapus secara tidak sengaja selama pembaruan tumpukan. Kebijakan tumpukan adalah dokumen JSON yang mendefinisikan tindakan pembaruan yang dapat dilakukan pada sumber daya yang ditentukan. Secara default, setiap prinsipal IAM dengan `cloudformation:UpdateStack` izin dapat memperbarui semua sumber daya dalam tumpukan. AWS CloudFormation Pembaruan dapat menyebabkan gangguan, atau mereka dapat sepenuhnya menghapus dan mengganti sumber daya. Anda dapat menggunakan kebijakan tumpukan untuk membantu mengonfigurasi izin hak istimewa terkecil. Kebijakan tumpukan dapat memberikan lapisan perlindungan tambahan.

Secara default, kebijakan tumpukan membantu melindungi semua sumber daya dalam tumpukan. Namun, manfaat utama dari kebijakan tumpukan adalah mereka menyediakan kontrol granular untuk setiap AWS sumber daya yang digunakan dalam tumpukan. CloudFormation Anda dapat menggunakan kebijakan tumpukan untuk membantu melindungi hanya sumber daya tertentu dalam tumpukan dan mengizinkan pembaruan atau penghapusan sumber daya lain dalam tumpukan yang sama. Untuk mengizinkan pembaruan sumber daya tertentu, Anda menyertakan `Allow` pernyataan eksplisit untuk sumber daya tersebut dalam kebijakan tumpukan Anda.

Kebijakan tumpukan memberikan kontrol preventif untuk CloudFormation tumpukan yang dilampirkan. Setiap tumpukan hanya dapat memiliki satu kebijakan tumpukan, tetapi Anda dapat

menggunakan kebijakan tumpukan itu untuk membantu melindungi semua sumber daya dalam tumpukan itu. Anda dapat menerapkan kebijakan tumpukan ke beberapa tumpukan.

Misalnya, bayangkan Anda memiliki pipeline yang menghasilkan artefak sensitif dan menyimpannya di bucket Amazon Simple Storage Service (Amazon S3) untuk sementara waktu untuk diproses lebih lanjut. Bucket S3 disediakan oleh CloudFormation, dan semua kontrol keamanan yang diperlukan sudah ada. Tanpa kebijakan tumpukan, pengembang mungkin sengaja atau tidak sengaja mengubah tujuan artefak pipeline menjadi bucket S3 yang kurang aman dan mengekspos data sensitif. Jika Anda memiliki kebijakan tumpukan yang diterapkan ke tumpukan, ini mencegah pengguna yang berwenang melakukan tindakan pembaruan atau penghapusan yang tidak diinginkan.

Bagian ini berisi topik berikut:

- Mengkonfigurasi kebijakan tumpukan
- Menyetel dan mengesampingkan kebijakan tumpukan
- Membatasi dan membutuhkan kebijakan tumpukan

Mengkonfigurasi kebijakan tumpukan

Saat Anda mengonfigurasi kebijakan tumpukan`Effect`, `Resource` elemen `ActionPrincipal`,,, dan diperlukan. Anda juga dapat mendefinisikan `Condition` elemen secara opsional.

Saat Anda membuat kebijakan tumpukan, secara default, kebijakan ini mencegah pembaruan untuk semua sumber daya di tumpukan. Anda menyesuaikan kebijakan tumpukan untuk menentukan tindakan mana yang diizinkan secara eksplisit. Jika ingin membalikkan kebijakan, Anda dapat menentukan `Allow` pernyataan yang mengizinkan semua tindakan, lalu menentukan pernyataan eksplisit `Deny` yang mencegah tindakan hanya pada sumber daya tertentu. Untuk referensi, lihat contoh kebijakan tumpukan ini dalam CloudFormation dokumentasi.

Untuk informasi selengkapnya tentang penggunaan elemen ini untuk membuat kebijakan tumpukan kustom dan kebijakan contoh lainnya, lihat Mendefinisikan kebijakan tumpukan dan Kebijakan tumpukan contoh lainnya dalam CloudFormation dokumentasi.

Menyetel dan mengesampingkan kebijakan tumpukan

Setelah Anda membuat kebijakan tumpukan, Anda mengaitkannya ke tumpukan. Jika Anda menetapkan kebijakan tumpukan ke tumpukan yang ada, Anda harus menggunakan AWS Command Line Interface (AWS CLI). Namun, jika Anda menetapkan kebijakan pada saat pembuatan tumpukan,

Anda dapat menggunakan CloudFormation konsol atau. AWS CLI Untuk petunjuk, lihat Menyetel kebijakan tumpukan dalam CloudFormation dokumentasi.

Saat Anda ingin mengizinkan pengguna memperbarui atau menghapus sumber daya di tumpukan, Anda perlu mengganti sementara kebijakan tumpukan. Penggantian ini memungkinkan Anda untuk melakukan tindakan yang ditolak pada sumber daya yang dilindungi di tumpukan itu. Untuk petunjuk, lihat Memperbarui sumber daya yang dilindungi dalam CloudFormation dokumentasi.

Membatasi dan membutuhkan kebijakan tumpukan

Sebagai praktik terbaik untuk izin hak istimewa terkecil, pertimbangkan untuk mewajibkan prinsipal IAM untuk menetapkan kebijakan tumpukan dan membatasi kebijakan tumpukan mana yang dapat ditetapkan oleh prinsip IAM. Banyak prinsipal IAM seharusnya tidak memiliki izin untuk membuat dan menetapkan kebijakan tumpukan khusus ke tumpukan mereka sendiri.

Setelah membuat kebijakan tumpukan, sebaiknya Anda mengunggahnya ke bucket S3.
Anda kemudian dapat mereferensikan kebijakan tumpukan ini dengan menggunakan kunci `cloudformation:StackPolicyUrl` kondisi dan menyediakan URL kebijakan tumpukan di bucket S3.

Memberikan izin untuk melampirkan kebijakan tumpukan

Sebagai praktik terbaik untuk izin hak istimewa terkecil, pertimbangkan untuk membatasi kebijakan tumpukan mana yang dapat dilampirkan oleh prinsip IAM ke tumpukan. CloudFormation Dalam kebijakan berbasis identitas untuk prinsipal IAM, Anda dapat menentukan kebijakan tumpukan mana yang memiliki izin untuk ditetapkan oleh prinsipal IAM. Ini mencegah prinsipal IAM melampirkan kebijakan tumpukan apa pun, yang dapat mengurangi risiko kesalahan konfigurasi.

Misalnya, sebuah organisasi mungkin memiliki tim yang berbeda dengan persyaratan yang berbeda. Dengan demikian, setiap tim membangun kebijakan tumpukan untuk tumpukan khusus tim CloudFormation mereka. Di lingkungan bersama, jika semua tim menyimpan kebijakan tumpukan mereka di bucket S3 yang sama, anggota tim mungkin melampirkan kebijakan tumpukan yang tersedia tetapi tidak ditujukan untuk CloudFormation tumpukan tim mereka. Untuk menghindari skenario ini, Anda dapat menentukan pernyataan kebijakan yang memungkinkan prinsipal IAM untuk melampirkan hanya kebijakan tumpukan tertentu.

Kebijakan sampel berikut memungkinkan prinsipal IAM untuk melampirkan kebijakan tumpukan yang disimpan dalam folder khusus tim dalam bucket S3. Anda dapat menyimpan kebijakan tumpukan yang disetujui di bucket ini.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:SetStackPolicy"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "cloudformation:StackPolicyUrl": "<Bucket URL>/<Team folder>/*"
        }
      }
    }
  ]
}
```

Pernyataan kebijakan ini tidak memerlukan prinsipal IAM untuk menetapkan kebijakan tumpukan ke setiap tumpukan. Bahkan jika prinsipal IAM memiliki izin untuk membuat tumpukan dengan kebijakan tumpukan tertentu, mereka dapat memilih untuk membuat tumpukan yang tidak memiliki kebijakan tumpukan.

Memerlukan kebijakan tumpukan

Untuk memastikan semua prinsipal IAM menetapkan kebijakan tumpukan ke tumpukan mereka, Anda dapat menentukan kebijakan kontrol layanan (SCP) atau batas izin sebagai pagar pembatas pencegahan.

Contoh kebijakan berikut menunjukkan bagaimana Anda dapat mengonfigurasi SCP yang memerlukan prinsipal IAM untuk menetapkan kebijakan tumpukan saat membuat tumpukan. Jika prinsipal IAM tidak melampirkan kebijakan tumpukan, mereka tidak dapat membuat tumpukan. Selain itu, kebijakan ini mencegah prinsipal IAM dengan izin pembaruan tumpukan menghapus kebijakan tumpukan selama pembaruan. kebijakan membatasi tindakan dengan menggunakan kunci kondisi. `cloudformation:UpdateStack` `cloudformation:StackPolicyUrl`

```
        {
  "Version": "2012-10-17",
  "Statement": [
```

```
    {
      "Effect": "Deny",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack"
      ],
      "Resource": "*",
      "Condition": {
        "Null": {
          "cloudformation:StackPolicyUrl": "true"
        }
      }
    }
  ]
}
```

Dengan menyertakan pernyataan kebijakan ini dalam SCP, bukan batas izin, Anda dapat menerapkan pagar pembatas ke semua akun di organisasi. Ini dapat melakukan hal berikut:

1. Kurangi upaya untuk melampirkan kebijakan secara individual ke beberapa prinsip IAM dalam sebuah. Akun AWS Batas izin dapat langsung dilampirkan hanya ke prinsipal IAM.
2. Kurangi upaya untuk membuat dan mengelola beberapa salinan batas izin untuk yang berbeda. Akun AWS Ini mengurangi risiko kesalahan konfigurasi di beberapa batas izin yang identik.

> **Note**
>
> SCPs dan batas izin adalah pagar pembatas izin yang menentukan izin maksimum yang tersedia untuk prinsipal IAM di akun atau organisasi. Kebijakan ini tidak memberikan izin kepada prinsipal IAM. Jika Anda ingin menstandarisasi persyaratan bahwa semua prinsipal IAM di akun atau organisasi Anda menetapkan kebijakan tumpukan, Anda harus menggunakan pagar pembatas izin dan kebijakan berbasis identitas.

Mengonfigurasi izin hak istimewa terkecil untuk sumber daya yang disediakan melalui CloudFormation

AWS CloudFormation memungkinkan Anda untuk menyediakan berbagai jenis AWS sumber daya. Sumber daya yang disediakan memerlukan set izin mereka sendiri untuk berfungsi sebagaimana dimaksud dan untuk mengonfigurasi siapa yang memiliki akses ke sumber daya tersebut. Bab sebelumnya meninjau opsi untuk mengonfigurasi izin untuk mengakses dan menggunakan layanan. CloudFormation Bab ini mengulas bagaimana Anda dapat menerapkan prinsip hak istimewa terkecil pada sumber daya yang disediakan. CloudFormation

Dalam panduan ini, praktis tidak mungkin untuk meninjau rekomendasi keamanan dan praktik terbaik untuk setiap jenis AWS sumber daya yang dapat disediakan. CloudFormation Jika Anda memiliki pertanyaan terkait dengan layanan tertentu, kami sarankan Anda meninjau dokumentasi untuk layanan tersebut. Sebagian besar Layanan AWS dokumen berisi bagian keamanan dan informasi tentang izin yang diperlukan untuk menggunakan layanan tersebut. Untuk daftar lengkap Layanan AWS dokumentasi, lihat AWS Dokumentasi.

Berikut ini adalah langkah-langkah agnostik layanan tingkat tinggi yang dapat Anda ambil untuk membuat CloudFormation templat yang mematuhi prinsip hak istimewa paling rendah:

1. Siapkan daftar sumber daya yang Anda rencanakan untuk disediakan dengan menggunakan CloudFormation.
2. Lihat AWS Dokumentasi untuk layanan terkait dan tinjau bagian tentang keamanan dan manajemen akses. Ini membantu Anda memahami persyaratan dan rekomendasi khusus layanan.
3. Gunakan informasi yang Anda kumpulkan di langkah sebelumnya untuk merancang CloudFormation templat dan kebijakan terkait yang hanya mengizinkan izin yang diperlukan dan menolak semua yang lain.

Selanjutnya, panduan ini mengulas contoh bagaimana Anda dapat menerapkan prinsip hak istimewa terkecil dalam CloudFormation templat, menggunakan kasus penggunaan dunia nyata.

Contoh: Bucket Amazon S3 untuk menyimpan artefak pipa

Contoh ini membuat bucket Amazon Simple Storage Service (Amazon S3) yang digunakan untuk AWS CodeBuildmenyimpan artefak proyek. AWS CodePipelinemenggunakan artefak yang disimpan

ini. Anda dapat mengizinkan CodeBuild dan CodePipeline mengakses bucket S3 ini melalui peran layanan, dan Anda mengontrol akses tersebut dengan menggunakan kebijakan bucket Amazon S3. Berikut ini adalah nama sumber daya yang digunakan dalam contoh ini:

- `Deployfiles_build`adalah nama CodeBuild proyek.
- `Deployment-Pipeline`adalah nama pipa di CodePipeline.

Tentukan bucket Amazon S3

Pertama, Anda menentukan bucket S3 dalam CloudFormation template, yang merupakan file teks berformat YAML.

```
amzn-s3-demo-bucket:
  Type: AWS::S3::Bucket
  Properties:
    PublicAccessBlockConfiguration:
        BlockPublicAcls: true
        BlockPublicPolicy: true
        IgnorePublicAcls: true
        RestrictPublicBuckets: true
```

Tentukan kebijakan bucket Amazon S3

Selanjutnya, di CloudFormation template, Anda membuat kebijakan bucket yang hanya mengizinkan `Deployfiles_build` proyek dan `Deployment-Pipeline` pipeline untuk mengakses bucket.

```
MyBucketPolicy:
  Type: AWS::S3::BucketPolicy
  Properties:
    Bucket: !Ref amzn-s3-demo-bucket
    PolicyDocument:
      Version: "2012-10-17"
      Statement:
      - Sid: "S3ArtifactRepoAccess"
        Effect: Allow
        Action:
          - ‘s3:GetObject'
          - ‘s3:GetObjectVersion'
          - ‘s3:PutObject'
          - ‘s3:GetBucketVersioning'
        Resource:
```

```
          - !Sub 'arn:aws:s3:::${amzn-s3-demo-bucket}'
          - !Sub 'arn:aws:s3:::${amzn-s3-demo-bucket}/*'
        Principal:
          Service:
            - codebuild.amazonaws.com
            - codepipeline.amazonaws.com
        Condition:
          StringLike:
            'aws:SourceArn':
              - !Sub 'arn:aws:codebuild:${AWS::Region}:${AWS::AccountId}:project/
Deployfiles_build'
              - !Sub 'arn:aws:codepipeline:${AWS::Region}:${AWS::AccountId}:Deployment-
Pipeline'
              - !Sub 'arn:aws:codepipeline:${AWS::Region}:${AWS::AccountId}:Deployment-
Pipeline/*'
```

Perhatikan hal berikut tentang kebijakan bucket ini:

- `Resource`Elemen ini mencantumkan dua jenis sumber daya yang menggunakan format Amazon Resource Name (ARN) berikut:
  - Format ARN dari objek S3 adalah. `arn:$`*`<Partition>`*`:s3:::$`*`<BucketName>`*`/$`*`<ObjectName>`*
  - Format ARN dari bucket S3 adalah. `arn:$`*`<Partition>`*`:s3:::$`*`<BucketName>`*

  `s3:GetObject`,`s3:GetObjectVersion`, dan `s3:PutObject` memerlukan tipe sumber daya objek S3, dan `s3:GetBucketVersioning` memerlukan tipe sumber daya bucket S3. Untuk informasi selengkapnya tentang jenis sumber daya yang diperlukan untuk setiap tindakan, lihat Tindakan, sumber daya, dan kunci kondisi untuk Amazon S3.
- `Principal`Elemen mencantumkan entitas yang diizinkan untuk melakukan tindakan Amazon S3 yang ditentukan dalam pernyataan. Dalam hal ini, hanya CodeBuild dan CodePipeline diizinkan untuk melakukan tindakan ini.
- `Condition`Elemen selanjutnya membatasi akses ke bucket S3 sehingga hanya `Deployfiles_build` CodeBuild proyek, `Deployment-Pipeline` CodePipeline pipeline, dan tindakan pipeline yang dapat mengakses bucket.

Buat peran layanan

Meskipun kebijakan bucket mengontrol akses ke bucket, kebijakan bucket tidak memberikan izin CodeBuild dan CodePipeline mengaksesnya. Untuk memberikan akses, Anda perlu membuat peran

layanan untuk setiap layanan dan menambahkan pernyataan berikut ke masing-masing layanan. Layanan berperan CodeBuild dan CodePipeline memungkinkan layanan mengakses bucket S3 dan objeknya.

```
Sid: "ViewAccessToS3ArtifactRepo"
Effect: Allow
Action:
  - ‘s3:GetObject'
  - ‘s3:GetObjectVersion'
  - ‘s3:PutObject'
  - ‘s3:GetBucketVersioning'
Resource:
  - !Sub ‘arn:aws:s3:::${BuildArtifactsBucket}'
  - !Sub ‘arn:aws:s3:::${BuildArtifactsBucket}/*'
```

Praktik terbaik untuk izin hak istimewa paling sedikit untuk AWS CloudFormation

Panduan ini meninjau berbagai pendekatan dan beberapa jenis kebijakan yang dapat Anda gunakan untuk mengonfigurasi akses hak istimewa AWS CloudFormation dan sumber daya yang disediakan. CloudFormation Panduan ini berfokus pada konfigurasi akses ke CloudFormation melalui prinsip-prinsip IAM, peran layanan, dan kebijakan tumpukan. Rekomendasi dan praktik terbaik yang disertakan dirancang untuk membantu melindungi akun Anda dan menumpuk sumber daya dari tindakan yang tidak diinginkan oleh pengguna yang berwenang dan dari aktor jahat yang mungkin mengeksploitasi izin berlebihan.

Berikut ini adalah ringkasan dari praktik terbaik yang dijelaskan dalam panduan ini. Praktik terbaik ini dapat membantu Anda mematuhi prinsip hak istimewa paling sedikit saat mengonfigurasi izin untuk digunakan CloudFormation dan sumber daya yang disediakan melalui: CloudFormation

- Tentukan tingkat akses yang dibutuhkan pengguna dan tim untuk menggunakan CloudFormation layanan, dan berikan hanya akses minimum yang diperlukan. Misalnya, berikan akses tampilan ke magang dan auditor, dan jangan izinkan jenis pengguna ini membuat, memperbarui, atau menghapus tumpukan.
- Untuk prinsipal IAM yang perlu menyediakan beberapa jenis AWS sumber daya melalui CloudFormation tumpukan, pertimbangkan untuk menggunakan peran layanan CloudFormation untuk memungkinkan penyediaan sumber daya atas nama kepala sekolah, alih-alih mengonfigurasi akses ke yang ada Layanan AWS dalam kebijakan berbasis identitas kepala sekolah.
- Dalam kebijakan berbasis identitas untuk prinsipal IAM, gunakan kunci `cloudformation:RoleARN` kondisi untuk mengontrol peran layanan mana yang dapat diteruskan. CloudFormation
- Untuk membantu mencegah eskalasi hak istimewa, lakukan hal berikut:
  - Pantau secara ketat semua kepala sekolah IAM yang memiliki akses ke CloudFormation layanan dan tingkat akses yang mereka miliki.
  - Pantau secara ketat pengguna mana yang dapat mengakses prinsipal IAM ini.
  - Pantau aktivitas prinsipal IAM yang dapat meneruskan peran layanan istimewa ke. CloudFormation Meskipun mereka mungkin tidak memiliki izin untuk membuat sumber daya IAM

melalui kebijakan berbasis identitas mereka, peran layanan yang dapat mereka lewati dapat membuat sumber daya IAM.

- Tentukan kebijakan tumpukan setiap kali Anda membuat tumpukan yang memiliki sumber daya penting. Ini dapat membantu melindungi sumber daya tumpukan penting dari pembaruan yang tidak disengaja yang dapat menyebabkan sumber daya tersebut terganggu atau diganti.
- Untuk sumber daya yang disediakan melalui CloudFormation, lihat rekomendasi manajemen akses dan praktik terbaik keamanan untuk layanan tersebut.
- Untuk melengkapi rekomendasi dalam panduan ini untuk kebijakan berbasis identitas dan kebijakan berbasis sumber daya, pertimbangkan untuk menerapkan kontrol keamanan tambahan untuk izin hak istimewa terkecil, seperti kebijakan kontrol layanan () dan batas izin. SCPs Untuk informasi selengkapnya, lihat Langkah berikutnya.

CloudFormation Dokumentasi berisi Praktik Terbaik dan praktik terbaik Keamanan tambahan yang dapat membantu Anda menggunakan dengan CloudFormation lebih efektif dan aman. Selain itu, lihat Praktik terbaik untuk mengonfigurasi kebijakan berbasis identitas untuk akses hak istimewa paling sedikit CloudFormation di panduan ini.

Langkah berikutnya

Anda dapat menggunakan informasi dan contoh dalam panduan ini untuk mulai menerapkan prinsip hak istimewa paling sedikit di organisasi Anda. Kami menyarankan Anda meninjau sumber daya tambahan di Sumber daya bagian ini, yang berisi referensi dokumentasi dan alat yang dapat membantu Anda menyempurnakan kebijakan Anda.

Panduan ini dimaksudkan untuk membantu Anda mulai menerapkan akses hak istimewa paling sedikit untuk. AWS CloudFormation Namun, ada jenis kebijakan tambahan yang dapat membantu Anda memperkuat prinsip hak istimewa paling sedikit di organisasi Anda. Berdasarkan lingkungan dan persyaratan bisnis Anda, Anda mungkin ingin menerapkan kontrol tambahan yang tidak dibahas dalam panduan ini. Sebagai langkah berikutnya dan untuk informasi lebih lanjut, kami sarankan Anda meninjau topik berikut yang terkait dengan hak istimewa paling sedikit dan mengonfigurasi akses dan izin:

- Batasan Izin untuk Entitas IAM
- Kebijakan kontrol layanan (SCP)
- Peran untuk akses lintas akun
- Federasi Identitas
- Melihat informasi terakhir yang diakses untuk IAM

Alat-alat berikut dapat membantu Anda memantau akses dan izin dengan hak istimewa paling rendah untuk: CloudFormation

- AWS Identity and Access Management Access Analyzer
- Anda dapat menggunakan tab Access Advisor di konsol AWS Identity and Access Management (IAM) untuk mengidentifikasi izin berlebihan untuk identitas IAM. Sebagai contoh, lihat Mengetatkan izin S3 untuk pengguna dan peran IAM Anda menggunakan riwayat akses tindakan S3 (AWS posting blog).
- Anda dapat menggunakan alat linting, seperti cfn-policy-validator(GitHub), untuk membantu mengidentifikasi izin yang berlebihan.

Ketika Anda merasa nyaman dengan membuat dan mengelola CloudFormation izin, Anda disarankan untuk menggunakan pipeline continuous integration dan continuous delivery (CI/CD)

untuk menyebarkan template Anda. CloudFormation Ini mengurangi risiko kesalahan manusia dan mempercepat proses penyebaran Anda.

Sumber daya

AWS CloudFormation dokumentasi

- Mengontrol akses dengan AWS Identity and Access Management
- AWS referensi jenis sumber daya dan properti
- Mengatur opsi AWS CloudFormation tumpukan
- AWS CloudFormation peran layanan

AWS Identity and Access Management Dokumentasi (IAM)

- Kebijakan dan izin di IAM
- Referensi elemen kebijakan IAM JSON
- Logika evaluasi kebijakan
- Layanan AWS yang bekerja dengan IAM
- Membuat peran untuk mendelegasikan izin ke Layanan AWS
- Masalah wakil yang membingungkan
- Praktik terbaik keamanan di IAM

AWS Referensi lainnya

- Tindakan, sumber daya, dan kunci kondisi untuk Layanan AWS (Referensi Otorisasi Layanan)
- Berikan akses hak istimewa paling sedikit (AWS Well-Architected Framework)
- Teknik untuk menulis kebijakan IAM dengan hak istimewa paling sedikit (AWS posting blog)

Riwayat dokumen

Tabel berikut menjelaskan perubahan signifikan pada panduan ini. Jika Anda ingin diberi tahu tentang pembaruan masa depan, Anda dapat berlangganan umpan RSS.

Perubahan	Deskripsi	Tanggal
Pembaruan signifikan	Kami secara signifikan merevisi dan menyempur nakan pedoman dan contoh pernyataan kebijakan untuk mengatasi kasus penggunaan organisasi yang umum.	5 Mei 2023
Publikasi awal	—	9 Maret 2023

AWS Glosarium Panduan Preskriptif

Berikut ini adalah istilah yang umum digunakan dalam strategi, panduan, dan pola yang disediakan oleh Panduan AWS Preskriptif. Untuk menyarankan entri, silakan gunakan tautan Berikan umpan balik di akhir glosarium.

Nomor

7 Rs

Tujuh strategi migrasi umum untuk memindahkan aplikasi ke cloud. Strategi ini dibangun di atas 5 Rs yang diidentifikasi Gartner pada tahun 2011 dan terdiri dari yang berikut:

- Refactor/Re-Architect — Memindahkan aplikasi dan memodifikasi arsitekturnya dengan memanfaatkan sepenuhnya fitur cloud-native untuk meningkatkan kelincahan, kinerja, dan skalabilitas. Ini biasanya melibatkan porting sistem operasi dan database. Contoh: Migrasikan database Oracle lokal Anda ke Amazon Aurora PostgreSQL Compatible Edition.
- Replatform (angkat dan bentuk ulang) — Pindahkan aplikasi ke cloud, dan perkenalkan beberapa tingkat pengoptimalan untuk memanfaatkan kemampuan cloud. Contoh: Memigrasikan database Oracle lokal Anda ke Amazon Relational Database Service (Amazon RDS) untuk Oracle di. AWS Cloud
- Pembelian kembali (drop and shop) - Beralih ke produk yang berbeda, biasanya dengan beralih dari lisensi tradisional ke model SaaS. Contoh: Migrasikan sistem manajemen hubungan pelanggan (CRM) Anda ke Salesforce.com.
- Rehost (lift dan shift) — Pindahkan aplikasi ke cloud tanpa membuat perubahan apa pun untuk memanfaatkan kemampuan cloud. Contoh: Migrasikan database Oracle lokal Anda ke Oracle pada instance EC2 di. AWS Cloud
- Relokasi (hypervisor-level lift and shift) — Pindahkan infrastruktur ke cloud tanpa membeli perangkat keras baru, menulis ulang aplikasi, atau memodifikasi operasi yang ada. Anda memigrasikan server dari platform lokal ke layanan cloud untuk platform yang sama. Contoh: Migrasikan Microsoft Hyper-V aplikasi ke AWS.
- Pertahankan (kunjungi kembali) - Simpan aplikasi di lingkungan sumber Anda. Ini mungkin termasuk aplikasi yang memerlukan refactoring besar, dan Anda ingin menunda pekerjaan itu sampai nanti, dan aplikasi lama yang ingin Anda pertahankan, karena tidak ada pembenaran bisnis untuk memigrasikannya.

- Pensiun — Menonaktifkan atau menghapus aplikasi yang tidak lagi diperlukan di lingkungan sumber Anda.

A

ABAC

Lihat kontrol akses berbasis atribut.

layanan abstrak

Lihat layanan terkelola.

ASAM

Lihat atomisitas, konsistensi, isolasi, daya tahan.

migrasi aktif-aktif

Metode migrasi database di mana database sumber dan target tetap sinkron (dengan menggunakan alat replikasi dua arah atau operasi penulisan ganda), dan kedua database menangani transaksi dari menghubungkan aplikasi selama migrasi. Metode ini mendukung migrasi dalam batch kecil yang terkontrol alih-alih memerlukan pemotongan satu kali. Ini lebih fleksibel tetapi membutuhkan lebih banyak pekerjaan daripada migrasi aktif-pasif.

migrasi aktif-pasif

Metode migrasi database di mana database sumber dan target disimpan dalam sinkron, tetapi hanya database sumber yang menangani transaksi dari menghubungkan aplikasi sementara data direplikasi ke database target. Basis data target tidak menerima transaksi apa pun selama migrasi.

fungsi agregat

Fungsi SQL yang beroperasi pada sekelompok baris dan menghitung nilai pengembalian tunggal untuk grup. Contoh fungsi agregat meliputi `SUM` dan`MAX`.

AI

Lihat kecerdasan buatan.

AIOps

Lihat operasi kecerdasan buatan.

anonimisasi

Proses menghapus informasi pribadi secara permanen dalam kumpulan data. Anonimisasi dapat membantu melindungi privasi pribadi. Data anonim tidak lagi dianggap sebagai data pribadi.

anti-pola

Solusi yang sering digunakan untuk masalah berulang di mana solusinya kontra-produktif, tidak efektif, atau kurang efektif daripada alternatif.

kontrol aplikasi

Pendekatan keamanan yang memungkinkan penggunaan hanya aplikasi yang disetujui untuk membantu melindungi sistem dari malware.

portofolio aplikasi

Kumpulan informasi rinci tentang setiap aplikasi yang digunakan oleh organisasi, termasuk biaya untuk membangun dan memelihara aplikasi, dan nilai bisnisnya. Informasi ini adalah kunci untuk penemuan portofolio dan proses analisis dan membantu mengidentifikasi dan memprioritaskan aplikasi yang akan dimigrasi, dimodernisasi, dan dioptimalkan.

kecerdasan buatan (AI)

Bidang ilmu komputer yang didedikasikan untuk menggunakan teknologi komputasi untuk melakukan fungsi kognitif yang biasanya terkait dengan manusia, seperti belajar, memecahkan masalah, dan mengenali pola. Untuk informasi lebih lanjut, lihat Apa itu Kecerdasan Buatan?

operasi kecerdasan buatan (AIOps)

Proses menggunakan teknik pembelajaran mesin untuk memecahkan masalah operasional, mengurangi insiden operasional dan intervensi manusia, dan meningkatkan kualitas layanan. Untuk informasi selengkapnya tentang cara AIOps digunakan dalam strategi AWS migrasi, lihat panduan integrasi operasi.

enkripsi asimetris

Algoritma enkripsi yang menggunakan sepasang kunci, kunci publik untuk enkripsi dan kunci pribadi untuk dekripsi. Anda dapat berbagi kunci publik karena tidak digunakan untuk dekripsi, tetapi akses ke kunci pribadi harus sangat dibatasi.

atomisitas, konsistensi, isolasi, daya tahan (ACID)

Satu set properti perangkat lunak yang menjamin validitas data dan keandalan operasional database, bahkan dalam kasus kesalahan, kegagalan daya, atau masalah lainnya.

kontrol akses berbasis atribut (ABAC)

Praktik membuat izin berbutir halus berdasarkan atribut pengguna, seperti departemen, peran pekerjaan, dan nama tim. Untuk informasi selengkapnya, lihat ABAC untuk AWS dokumentasi AWS Identity and Access Management (IAM).

sumber data otoritatif

Lokasi di mana Anda menyimpan versi utama data, yang dianggap sebagai sumber informasi yang paling dapat diandalkan. Anda dapat menyalin data dari sumber data otoritatif ke lokasi lain untuk tujuan pemrosesan atau modifikasi data, seperti menganonimkan, menyunting, atau membuat nama samaran.

Availability Zone

Lokasi berbeda di dalam Wilayah AWS yang terisolasi dari kegagalan di Availability Zone lainnya dan menyediakan konektivitas jaringan latensi rendah yang murah ke Availability Zone lainnya di Wilayah yang sama.

AWS Kerangka Adopsi Cloud (AWS CAF)

Kerangka pedoman dan praktik terbaik AWS untuk membantu organisasi mengembangkan rencana yang efisien dan efektif untuk bergerak dengan sukses ke cloud. AWS CAF mengatur panduan ke dalam enam area fokus yang disebut perspektif: bisnis, orang, tata kelola, platform, keamanan, dan operasi. Perspektif bisnis, orang, dan tata kelola fokus pada keterampilan dan proses bisnis; perspektif platform, keamanan, dan operasi fokus pada keterampilan dan proses teknis. Misalnya, perspektif masyarakat menargetkan pemangku kepentingan yang menangani sumber daya manusia (SDM), fungsi kepegawaian, dan manajemen orang. Untuk perspektif ini, AWS CAF memberikan panduan untuk pengembangan, pelatihan, dan komunikasi orang untuk membantu mempersiapkan organisasi untuk adopsi cloud yang sukses. Untuk informasi lebih lanjut, lihat situs web AWS CAF dan whitepaper AWS CAF.

AWS Kerangka Kualifikasi Beban Kerja (AWS WQF)

Alat yang mengevaluasi beban kerja migrasi database, merekomendasikan strategi migrasi, dan memberikan perkiraan kerja. AWS WQF disertakan dengan AWS Schema Conversion Tool ()AWS SCT. Ini menganalisis skema database dan objek kode, kode aplikasi, dependensi, dan karakteristik kinerja, dan memberikan laporan penilaian.

B

bot buruk

Bot yang dimaksudkan untuk mengganggu atau membahayakan individu atau organisasi.

BCP

Lihat perencanaan kontinuitas bisnis.

grafik perilaku

Pandangan interaktif yang terpadu tentang perilaku dan interaksi sumber daya dari waktu ke waktu. Anda dapat menggunakan grafik perilaku dengan Amazon Detective untuk memeriksa upaya logon yang gagal, panggilan API yang mencurigakan, dan tindakan serupa. Untuk informasi selengkapnya, lihat Data dalam grafik perilaku di dokumentasi Detektif.

sistem big-endian

Sistem yang menyimpan byte paling signifikan terlebih dahulu. Lihat juga endianness.

klasifikasi biner

Sebuah proses yang memprediksi hasil biner (salah satu dari dua kelas yang mungkin). Misalnya, model ML Anda mungkin perlu memprediksi masalah seperti “Apakah email ini spam atau bukan spam?” atau “Apakah produk ini buku atau mobil?”

filter mekar

Struktur data probabilistik dan efisien memori yang digunakan untuk menguji apakah suatu elemen adalah anggota dari suatu himpunan.

deployment biru/hijau

Strategi penyebaran tempat Anda membuat dua lingkungan yang terpisah namun identik. Anda menjalankan versi aplikasi saat ini di satu lingkungan (biru) dan versi aplikasi baru di lingkungan lain (hijau). Strategi ini membantu Anda dengan cepat memutar kembali dengan dampak minimal.

bot

Aplikasi perangkat lunak yang menjalankan tugas otomatis melalui internet dan mensimulasikan aktivitas atau interaksi manusia. Beberapa bot berguna atau bermanfaat, seperti perayap web yang mengindeks informasi di internet. Beberapa bot lain, yang dikenal sebagai bot buruk, dimaksudkan untuk mengganggu atau membahayakan individu atau organisasi.

botnet

Jaringan bot yang terinfeksi oleh malware dan berada di bawah kendali satu pihak, yang dikenal sebagai bot herder atau operator bot. Botnet adalah mekanisme paling terkenal untuk skala bot dan dampaknya.

cabang

Area berisi repositori kode. Cabang pertama yang dibuat dalam repositori adalah cabang utama. Anda dapat membuat cabang baru dari cabang yang ada, dan Anda kemudian dapat mengembangkan fitur atau memperbaiki bug di cabang baru. Cabang yang Anda buat untuk membangun fitur biasanya disebut sebagai cabang fitur. Saat fitur siap dirilis, Anda menggabungkan cabang fitur kembali ke cabang utama. Untuk informasi selengkapnya, lihat Tentang cabang (GitHub dokumentasi).

akses break-glass

Dalam keadaan luar biasa dan melalui proses yang disetujui, cara cepat bagi pengguna untuk mendapatkan akses ke Akun AWS yang biasanya tidak memiliki izin untuk mengaksesnya. Untuk informasi lebih lanjut, lihat indikator Implementasikan prosedur kaca pecah dalam panduan Well-Architected AWS .

strategi brownfield

Infrastruktur yang ada di lingkungan Anda. Saat mengadopsi strategi brownfield untuk arsitektur sistem, Anda merancang arsitektur di sekitar kendala sistem dan infrastruktur saat ini. Jika Anda memperluas infrastruktur yang ada, Anda dapat memadukan strategi brownfield dan greenfield.

cache penyangga

Area memori tempat data yang paling sering diakses disimpan.

kemampuan bisnis

Apa yang dilakukan bisnis untuk menghasilkan nilai (misalnya, penjualan, layanan pelanggan, atau pemasaran). Arsitektur layanan mikro dan keputusan pengembangan dapat didorong oleh kemampuan bisnis. Untuk informasi selengkapnya, lihat bagian Terorganisir di sekitar kemampuan bisnis dari Menjalankan layanan mikro kontainer di whitepaper. AWS

perencanaan kelangsungan bisnis (BCP)

Rencana yang membahas dampak potensial dari peristiwa yang mengganggu, seperti migrasi skala besar, pada operasi dan memungkinkan bisnis untuk melanjutkan operasi dengan cepat.

C

KAFE

Lihat Kerangka Adopsi AWS Cloud.

penyebaran kenari

Rilis versi yang lambat dan bertahap untuk pengguna akhir. Ketika Anda yakin, Anda menyebarkan versi baru dan mengganti versi saat ini secara keseluruhan.

CCoE

Lihat Cloud Center of Excellence.

CDC

Lihat mengubah pengambilan data.

ubah pengambilan data (CDC)

Proses melacak perubahan ke sumber data, seperti tabel database, dan merekam metadata tentang perubahan tersebut. Anda dapat menggunakan CDC untuk berbagai tujuan, seperti mengaudit atau mereplikasi perubahan dalam sistem target untuk mempertahankan sinkronisasi.

rekayasa kekacauan

Sengaja memperkenalkan kegagalan atau peristiwa yang mengganggu untuk menguji ketahanan sistem. Anda dapat menggunakan AWS Fault Injection Service (AWS FIS) untuk melakukan eksperimen yang menekankan AWS beban kerja Anda dan mengevaluasi responsnya.

CI/CD

Lihat integrasi berkelanjutan dan pengiriman berkelanjutan.

klasifikasi

Proses kategorisasi yang membantu menghasilkan prediksi. Model ML untuk masalah klasifikasi memprediksi nilai diskrit. Nilai diskrit selalu berbeda satu sama lain. Misalnya, model mungkin perlu mengevaluasi apakah ada mobil dalam gambar atau tidak.

Enkripsi sisi klien

Enkripsi data secara lokal, sebelum target Layanan AWS menerimanya.

Pusat Keunggulan Cloud (CCoE)

Tim multi-disiplin yang mendorong upaya adopsi cloud di seluruh organisasi, termasuk mengembangkan praktik terbaik cloud, memobilisasi sumber daya, menetapkan jadwal migrasi, dan memimpin organisasi melalui transformasi skala besar. Untuk informasi selengkapnya, lihat posting CCo E di Blog Strategi AWS Cloud Perusahaan.

komputasi cloud

Teknologi cloud yang biasanya digunakan untuk penyimpanan data jarak jauh dan manajemen perangkat IoT. Cloud computing umumnya terhubung ke teknologi edge computing.

model operasi cloud

Dalam organisasi TI, model operasi yang digunakan untuk membangun, mematangkan, dan mengoptimalkan satu atau lebih lingkungan cloud. Untuk informasi selengkapnya, lihat Membangun Model Operasi Cloud Anda.

tahap adopsi cloud

Empat fase yang biasanya dilalui organisasi ketika mereka bermigrasi ke AWS Cloud:

- Proyek — Menjalankan beberapa proyek terkait cloud untuk bukti konsep dan tujuan pembelajaran
- Foundation — Melakukan investasi dasar untuk meningkatkan adopsi cloud Anda (misalnya, membuat landing zone, mendefinisikan CCo E, membuat model operasi)
- Migrasi — Migrasi aplikasi individual
- Re-invention — Mengoptimalkan produk dan layanan, dan berinovasi di cloud

Tahapan ini didefinisikan oleh Stephen Orban dalam posting blog The Journey Toward Cloud-First & the Stages of Adoption di blog Strategi Perusahaan. AWS Cloud Untuk informasi tentang bagaimana kaitannya dengan strategi AWS migrasi, lihat panduan kesiapan migrasi.

CMDB

Lihat database manajemen konfigurasi.

repositori kode

Lokasi di mana kode sumber dan aset lainnya, seperti dokumentasi, sampel, dan skrip, disimpan dan diperbarui melalui proses kontrol versi. Repositori cloud umum termasuk GitHub atau. Bitbucket Cloud Setiap versi kode disebut cabang. Dalam struktur layanan mikro, setiap repositori

dikhususkan untuk satu bagian fungsionalitas. Pipa CI/CD tunggal dapat menggunakan beberapa repositori.

cache dingin

Cache buffer yang kosong, tidak terisi dengan baik, atau berisi data basi atau tidak relevan. Ini mempengaruhi kinerja karena instance database harus membaca dari memori utama atau disk, yang lebih lambat daripada membaca dari cache buffer.

data dingin

Data yang jarang diakses dan biasanya historis. Saat menanyakan jenis data ini, kueri lambat biasanya dapat diterima. Memindahkan data ini ke tingkat penyimpanan atau kelas yang berkinerja lebih rendah dan lebih murah dapat mengurangi biaya.

visi komputer (CV)

Bidang AI yang menggunakan pembelajaran mesin untuk menganalisis dan mengekstrak informasi dari format visual seperti gambar dan video digital. Misalnya, Amazon SageMaker AI menyediakan algoritma pemrosesan gambar untuk CV.

konfigurasi drift

Untuk beban kerja, konfigurasi berubah dari status yang diharapkan. Ini dapat menyebabkan beban kerja menjadi tidak patuh, dan biasanya bertahap dan tidak disengaja.

database manajemen konfigurasi (CMDB)

Repositori yang menyimpan dan mengelola informasi tentang database dan lingkungan TI, termasuk komponen perangkat keras dan perangkat lunak dan konfigurasinya. Anda biasanya menggunakan data dari CMDB dalam penemuan portofolio dan tahap analisis migrasi.

paket kesesuaian

Kumpulan AWS Config aturan dan tindakan remediasi yang dapat Anda kumpulkan untuk menyesuaikan kepatuhan dan pemeriksaan keamanan Anda. Anda dapat menerapkan paket kesesuaian sebagai entitas tunggal di Akun AWS dan Wilayah, atau di seluruh organisasi, dengan menggunakan templat YAMM. Untuk informasi selengkapnya, lihat Paket kesesuaian dalam dokumentasi. AWS Config

integrasi berkelanjutan dan pengiriman berkelanjutan (CI/CD)

Proses mengotomatiskan sumber, membangun, menguji, pementasan, dan tahap produksi dari proses rilis perangkat lunak. CI/CD biasanya digambarkan sebagai pipa. CI/CD dapat membantu

Anda mengotomatiskan proses, meningkatkan produktivitas, meningkatkan kualitas kode, dan memberikan lebih cepat. Untuk informasi lebih lanjut, lihat Manfaat pengiriman berkelanjutan. CD juga dapat berarti penerapan berkelanjutan. Untuk informasi selengkapnya, lihat Continuous Delivery vs Continuous Deployment.

CV

Lihat visi komputer.

D

data saat istirahat

Data yang stasioner di jaringan Anda, seperti data yang ada di penyimpanan.

klasifikasi data

Proses untuk mengidentifikasi dan mengkategorikan data dalam jaringan Anda berdasarkan kekritisan dan sensitivitasnya. Ini adalah komponen penting dari setiap strategi manajemen risiko keamanan siber karena membantu Anda menentukan perlindungan dan kontrol retensi yang tepat untuk data. Klasifikasi data adalah komponen pilar keamanan dalam AWS Well-Architected Framework. Untuk informasi selengkapnya, lihat Klasifikasi data.

penyimpangan data

Variasi yang berarti antara data produksi dan data yang digunakan untuk melatih model ML, atau perubahan yang berarti dalam data input dari waktu ke waktu. Penyimpangan data dapat mengurangi kualitas, akurasi, dan keadilan keseluruhan dalam prediksi model ML.

data dalam transit

Data yang aktif bergerak melalui jaringan Anda, seperti antara sumber daya jaringan.

jala data

Kerangka arsitektur yang menyediakan kepemilikan data terdistribusi dan terdesentralisasi dengan manajemen dan tata kelola terpusat.

minimalisasi data

Prinsip pengumpulan dan pemrosesan hanya data yang sangat diperlukan. Mempraktikkan minimalisasi data di dalamnya AWS Cloud dapat mengurangi risiko privasi, biaya, dan jejak karbon analitik Anda.

perimeter data

Satu set pagar pembatas pencegahan di AWS lingkungan Anda yang membantu memastikan bahwa hanya identitas tepercaya yang mengakses sumber daya tepercaya dari jaringan yang diharapkan. Untuk informasi selengkapnya, lihat Membangun perimeter data pada AWS.

prapemrosesan data

Untuk mengubah data mentah menjadi format yang mudah diuraikan oleh model ML Anda. Preprocessing data dapat berarti menghapus kolom atau baris tertentu dan menangani nilai yang hilang, tidak konsisten, atau duplikat.

asal data

Proses melacak asal dan riwayat data sepanjang siklus hidupnya, seperti bagaimana data dihasilkan, ditransmisikan, dan disimpan.

subjek data

Individu yang datanya dikumpulkan dan diproses.

gudang data

Sistem manajemen data yang mendukung intelijen bisnis, seperti analitik. Gudang data biasanya berisi sejumlah besar data historis, dan biasanya digunakan untuk kueri dan analisis.

bahasa definisi database (DDL)

Pernyataan atau perintah untuk membuat atau memodifikasi struktur tabel dan objek dalam database.

bahasa manipulasi basis data (DHTML)

Pernyataan atau perintah untuk memodifikasi (memasukkan, memperbarui, dan menghapus) informasi dalam database.

DDL

Lihat bahasa definisi database.

ansambel yang dalam

Untuk menggabungkan beberapa model pembelajaran mendalam untuk prediksi. Anda dapat menggunakan ansambel dalam untuk mendapatkan prediksi yang lebih akurat atau untuk memperkirakan ketidakpastian dalam prediksi.

pembelajaran mendalam

Subbidang ML yang menggunakan beberapa lapisan jaringan saraf tiruan untuk mengidentifikasi pemetaan antara data input dan variabel target yang diinginkan.

defense-in-depth

Pendekatan keamanan informasi di mana serangkaian mekanisme dan kontrol keamanan dilapisi dengan cermat di seluruh jaringan komputer untuk melindungi kerahasiaan, integritas, dan ketersediaan jaringan dan data di dalamnya. Saat Anda mengadopsi strategi ini AWS, Anda menambahkan beberapa kontrol pada lapisan AWS Organizations struktur yang berbeda untuk membantu mengamankan sumber daya. Misalnya, defense-in-depth pendekatan mungkin menggabungkan otentikasi multi-faktor, segmentasi jaringan, dan enkripsi.

administrator yang didelegasikan

Di AWS Organizations, layanan yang kompatibel dapat mendaftarkan akun AWS anggota untuk mengelola akun organisasi dan mengelola izin untuk layanan tersebut. Akun ini disebut administrator yang didelegasikan untuk layanan itu. Untuk informasi selengkapnya dan daftar layanan yang kompatibel, lihat Layanan yang berfungsi dengan AWS Organizations AWS Organizations dokumentasi.

deployment

Proses pembuatan aplikasi, fitur baru, atau perbaikan kode tersedia di lingkungan target. Deployment melibatkan penerapan perubahan dalam basis kode dan kemudian membangun dan menjalankan basis kode itu di lingkungan aplikasi.

lingkungan pengembangan

Lihat lingkungan.

kontrol detektif

Kontrol keamanan yang dirancang untuk mendeteksi, mencatat, dan memperingatkan setelah suatu peristiwa terjadi. Kontrol ini adalah garis pertahanan kedua, memperingatkan Anda tentang peristiwa keamanan yang melewati kontrol pencegahan di tempat. Untuk informasi selengkapnya, lihat Kontrol Detektif dalam Menerapkan kontrol keamanan pada. AWS

pemetaan aliran nilai pengembangan (DVSM)

Sebuah proses yang digunakan untuk mengidentifikasi dan memprioritaskan kendala yang mempengaruhi kecepatan dan kualitas dalam siklus hidup pengembangan perangkat lunak. DVSM memperluas proses pemetaan aliran nilai yang awalnya dirancang untuk praktik

manufaktur ramping. Ini berfokus pada langkah-langkah dan tim yang diperlukan untuk menciptakan dan memindahkan nilai melalui proses pengembangan perangkat lunak.

kembar digital

Representasi virtual dari sistem dunia nyata, seperti bangunan, pabrik, peralatan industri, atau jalur produksi. Kembar digital mendukung pemeliharaan prediktif, pemantauan jarak jauh, dan optimalisasi produksi.

tabel dimensi

Dalam skema bintang, tabel yang lebih kecil yang berisi atribut data tentang data kuantitatif dalam tabel fakta. Atribut tabel dimensi biasanya bidang teks atau angka diskrit yang berperilaku seperti teks. Atribut ini biasanya digunakan untuk pembatasan kueri, pemfilteran, dan pelabelan set hasil.

musibah

Peristiwa yang mencegah beban kerja atau sistem memenuhi tujuan bisnisnya di lokasi utama yang digunakan. Peristiwa ini dapat berupa bencana alam, kegagalan teknis, atau akibat dari tindakan manusia, seperti kesalahan konfigurasi yang tidak disengaja atau serangan malware.

pemulihan bencana (DR)

Strategi dan proses yang Anda gunakan untuk meminimalkan downtime dan kehilangan data yang disebabkan oleh bencana. Untuk informasi selengkapnya, lihat Disaster Recovery of Workloads on AWS: Recovery in the Cloud in the AWS Well-Architected Framework.

DML~

Lihat bahasa manipulasi basis data.

desain berbasis domain

Pendekatan untuk mengembangkan sistem perangkat lunak yang kompleks dengan menghubungkan komponennya ke domain yang berkembang, atau tujuan bisnis inti, yang dilayani oleh setiap komponen. Konsep ini diperkenalkan oleh Eric Evans dalam bukunya, Domain-Driven Design: Tackling Complexity in the Heart of Software (Boston: Addison-Wesley Professional, 2003). Untuk informasi tentang cara menggunakan desain berbasis domain dengan pola gambar pencekik, lihat Memodernisasi layanan web Microsoft ASP.NET (ASMX) lama secara bertahap menggunakan container dan Amazon API Gateway.

DR

Lihat pemulihan bencana.

deteksi drift

Melacak penyimpangan dari konfigurasi dasar. Misalnya, Anda dapat menggunakan AWS CloudFormation untuk mendeteksi penyimpangan dalam sumber daya sistem, atau Anda dapat menggunakannya AWS Control Tower untuk mendeteksi perubahan di landing zone yang mungkin memengaruhi kepatuhan terhadap persyaratan tata kelola.

DVSM

Lihat pemetaan aliran nilai pengembangan.

E

EDA

Lihat analisis data eksplorasi.

EDI

Lihat pertukaran data elektronik.

komputasi tepi

Teknologi yang meningkatkan daya komputasi untuk perangkat pintar di tepi jaringan IoT. Jika dibandingkan dengan komputasi awan, komputasi tepi dapat mengurangi latensi komunikasi dan meningkatkan waktu respons.

pertukaran data elektronik (EDI)

Pertukaran otomatis dokumen bisnis antar organisasi. Untuk informasi selengkapnya, lihat Apa itu Pertukaran Data Elektronik.

enkripsi

Proses komputasi yang mengubah data plaintext, yang dapat dibaca manusia, menjadi ciphertext.

kunci enkripsi

String kriptografi dari bit acak yang dihasilkan oleh algoritma enkripsi. Panjang kunci dapat bervariasi, dan setiap kunci dirancang agar tidak dapat diprediksi dan unik.

endianness

Urutan byte disimpan dalam memori komputer. Sistem big-endian menyimpan byte paling signifikan terlebih dahulu. Sistem little-endian menyimpan byte paling tidak signifikan terlebih dahulu.

titik akhir

Lihat titik akhir layanan.

layanan endpoint

Layanan yang dapat Anda host di cloud pribadi virtual (VPC) untuk dibagikan dengan pengguna lain. Anda dapat membuat layanan endpoint dengan AWS PrivateLink dan memberikan izin kepada prinsipal lain Akun AWS atau ke AWS Identity and Access Management (IAM). Akun atau prinsipal ini dapat terhubung ke layanan endpoint Anda secara pribadi dengan membuat titik akhir VPC antarmuka. Untuk informasi selengkapnya, lihat Membuat layanan titik akhir di dokumentasi Amazon Virtual Private Cloud (Amazon VPC).

perencanaan sumber daya perusahaan (ERP)

Sistem yang mengotomatiskan dan mengelola proses bisnis utama (seperti akuntansi, MES, dan manajemen proyek) untuk suatu perusahaan.

enkripsi amplop

Proses mengenkripsi kunci enkripsi dengan kunci enkripsi lain. Untuk informasi selengkapnya, lihat Enkripsi amplop dalam dokumentasi AWS Key Management Service (AWS KMS).

lingkungan

Sebuah contoh dari aplikasi yang sedang berjalan. Berikut ini adalah jenis lingkungan yang umum dalam komputasi awan:

- Development Environment — Sebuah contoh dari aplikasi yang berjalan yang hanya tersedia untuk tim inti yang bertanggung jawab untuk memelihara aplikasi. Lingkungan pengembangan digunakan untuk menguji perubahan sebelum mempromosikannya ke lingkungan atas. Jenis lingkungan ini kadang-kadang disebut sebagai lingkungan pengujian.
- lingkungan yang lebih rendah — Semua lingkungan pengembangan untuk aplikasi, seperti yang digunakan untuk build awal dan pengujian.
- lingkungan produksi — Sebuah contoh dari aplikasi yang berjalan yang pengguna akhir dapat mengakses. Dalam sebuah CI/CD pipeline, lingkungan produksi adalah lingkungan penyebaran terakhir.

- lingkungan atas — Semua lingkungan yang dapat diakses oleh pengguna selain tim pengembangan inti. Ini dapat mencakup lingkungan produksi, lingkungan praproduksi, dan lingkungan untuk pengujian penerimaan pengguna.

epik

Dalam metodologi tangkas, kategori fungsional yang membantu mengatur dan memprioritaskan pekerjaan Anda. Epik memberikan deskripsi tingkat tinggi tentang persyaratan dan tugas implementasi. Misalnya, epos keamanan AWS CAF mencakup manajemen identitas dan akses, kontrol detektif, keamanan infrastruktur, perlindungan data, dan respons insiden. Untuk informasi selengkapnya tentang epos dalam strategi AWS migrasi, lihat panduan implementasi program.

ERP

Lihat perencanaan sumber daya perusahaan.

analisis data eksplorasi (EDA)

Proses menganalisis dataset untuk memahami karakteristik utamanya. Anda mengumpulkan atau mengumpulkan data dan kemudian melakukan penyelidikan awal untuk menemukan pola, mendeteksi anomali, dan memeriksa asumsi. EDA dilakukan dengan menghitung statistik ringkasan dan membuat visualisasi data.

F

tabel fakta

Tabel tengah dalam skema bintang. Ini menyimpan data kuantitatif tentang operasi bisnis. Biasanya, tabel fakta berisi dua jenis kolom: kolom yang berisi ukuran dan yang berisi kunci asing ke tabel dimensi.

gagal cepat

Filosofi yang menggunakan pengujian yang sering dan bertahap untuk mengurangi siklus hidup pengembangan. Ini adalah bagian penting dari pendekatan tangkas.

batas isolasi kesalahan

Dalam AWS Cloud, batas seperti Availability Zone, Wilayah AWS, control plane, atau data plane yang membatasi efek kegagalan dan membantu meningkatkan ketahanan beban kerja. Untuk informasi selengkapnya, lihat Batas Isolasi AWS Kesalahan.

cabang fitur

Lihat cabang.

fitur

Data input yang Anda gunakan untuk membuat prediksi. Misalnya, dalam konteks manufaktur, fitur bisa berupa gambar yang diambil secara berkala dari lini manufaktur.

pentingnya fitur

Seberapa signifikan fitur untuk prediksi model. Ini biasanya dinyatakan sebagai skor numerik yang dapat dihitung melalui berbagai teknik, seperti Shapley Additive Explanations (SHAP) dan gradien terintegrasi. Untuk informasi lebih lanjut, lihat Interpretabilitas model pembelajaran mesin dengan. AWS

transformasi fitur

Untuk mengoptimalkan data untuk proses ML, termasuk memperkaya data dengan sumber tambahan, menskalakan nilai, atau mengekstrak beberapa set informasi dari satu bidang data. Hal ini memungkinkan model ML untuk mendapatkan keuntungan dari data. Misalnya, jika Anda memecah tanggal “2021-05-27 00:15:37" menjadi “2021", “Mei”, “Kamis”, dan “15", Anda dapat membantu algoritme pembelajaran mempelajari pola bernuansa yang terkait dengan komponen data yang berbeda.

beberapa tembakan mendorong

Menyediakan LLM dengan sejumlah kecil contoh yang menunjukkan tugas dan output yang diinginkan sebelum memintanya untuk melakukan tugas serupa. Teknik ini adalah aplikasi pembelajaran dalam konteks, di mana model belajar dari contoh (bidikan) yang tertanam dalam petunjuk. Beberapa bidikan dapat efektif untuk tugas-tugas yang memerlukan pemformatan, penalaran, atau pengetahuan domain tertentu. Lihat juga bidikan nol.

FGAC

Lihat kontrol akses berbutir halus.

kontrol akses berbutir halus (FGAC)

Penggunaan beberapa kondisi untuk mengizinkan atau menolak permintaan akses.

migrasi flash-cut

Metode migrasi database yang menggunakan replikasi data berkelanjutan melalui pengambilan data perubahan untuk memigrasikan data dalam waktu sesingkat mungkin, alih-alih

menggunakan pendekatan bertahap. Tujuannya adalah untuk menjaga downtime seminimal mungkin.

FM

Lihat model pondasi.

model pondasi (FM)

Jaringan saraf pembelajaran mendalam yang besar yang telah melatih kumpulan data besar-besaran data umum dan tidak berlabel. FMs mampu melakukan berbagai tugas umum, seperti memahami bahasa, menghasilkan teks dan gambar, dan berbicara dalam bahasa alami. Untuk informasi selengkapnya, lihat Apa itu Model Foundation.

G

AI generatif

Subset model AI yang telah dilatih pada sejumlah besar data dan yang dapat menggunakan prompt teks sederhana untuk membuat konten dan artefak baru, seperti gambar, video, teks, dan audio. Untuk informasi lebih lanjut, lihat Apa itu AI Generatif.

pemblokiran geografis

Lihat pembatasan geografis.

pembatasan geografis (pemblokiran geografis)

Di Amazon CloudFront, opsi untuk mencegah pengguna di negara tertentu mengakses distribusi konten. Anda dapat menggunakan daftar izinkan atau daftar blokir untuk menentukan negara yang disetujui dan dilarang. Untuk informasi selengkapnya, lihat Membatasi distribusi geografis konten Anda dalam dokumentasi. CloudFront

Alur kerja Gitflow

Pendekatan di mana lingkungan bawah dan atas menggunakan cabang yang berbeda dalam repositori kode sumber. Alur kerja Gitflow dianggap warisan, dan alur kerja berbasis batang adalah pendekatan modern yang lebih disukai.

gambar emas

Sebuah snapshot dari sistem atau perangkat lunak yang digunakan sebagai template untuk menyebarkan instance baru dari sistem atau perangkat lunak itu. Misalnya, di bidang manufaktur,

gambar emas dapat digunakan untuk menyediakan perangkat lunak pada beberapa perangkat dan membantu meningkatkan kecepatan, skalabilitas, dan produktivitas dalam operasi manufaktur perangkat.

strategi greenfield

Tidak adanya infrastruktur yang ada di lingkungan baru. Saat mengadopsi strategi greenfield untuk arsitektur sistem, Anda dapat memilih semua teknologi baru tanpa batasan kompatibilitas dengan infrastruktur yang ada, juga dikenal sebagai brownfield. Jika Anda memperluas infrastruktur yang ada, Anda dapat memadukan strategi brownfield dan greenfield.

pagar pembatas

Aturan tingkat tinggi yang membantu mengatur sumber daya, kebijakan, dan kepatuhan di seluruh unit organisasi ()OUs. Pagar pembatas preventif menegakkan kebijakan untuk memastikan keselarasan dengan standar kepatuhan. Mereka diimplementasikan dengan menggunakan kebijakan kontrol layanan dan batas izin IAM. Detective guardrails mendeteksi pelanggaran kebijakan dan masalah kepatuhan, dan menghasilkan peringatan untuk remediasi. Mereka diimplementasikan dengan menggunakan AWS Config, AWS Security Hub, Amazon GuardDuty AWS Trusted Advisor, Amazon Inspector, dan pemeriksaan khusus AWS Lambda .

H

HA

Lihat ketersediaan tinggi.

migrasi database heterogen

Memigrasi database sumber Anda ke database target yang menggunakan mesin database yang berbeda (misalnya, Oracle ke Amazon Aurora). Migrasi heterogen biasanya merupakan bagian dari upaya arsitektur ulang, dan mengubah skema dapat menjadi tugas yang kompleks. AWS menyediakan AWS SCT yang membantu dengan konversi skema.

ketersediaan tinggi (HA)

Kemampuan beban kerja untuk beroperasi terus menerus, tanpa intervensi, jika terjadi tantangan atau bencana. Sistem HA dirancang untuk gagal secara otomatis, secara konsisten memberikan kinerja berkualitas tinggi, dan menangani beban dan kegagalan yang berbeda dengan dampak kinerja minimal.

modernisasi sejarawan

Pendekatan yang digunakan untuk memodernisasi dan meningkatkan sistem teknologi operasional (OT) untuk melayani kebutuhan industri manufaktur dengan lebih baik. Sejarawan adalah jenis database yang digunakan untuk mengumpulkan dan menyimpan data dari berbagai sumber di pabrik.

data penahanan

Sebagian dari data historis berlabel yang ditahan dari kumpulan data yang digunakan untuk melatih model pembelajaran mesin. Anda dapat menggunakan data penahanan untuk mengevaluasi kinerja model dengan membandingkan prediksi model dengan data penahanan.

migrasi database homogen

Memigrasi database sumber Anda ke database target yang berbagi mesin database yang sama (misalnya, Microsoft SQL Server ke Amazon RDS for SQL Server). Migrasi homogen biasanya merupakan bagian dari upaya rehosting atau replatforming. Anda dapat menggunakan utilitas database asli untuk memigrasi skema.

data panas

Data yang sering diakses, seperti data real-time atau data translasi terbaru. Data ini biasanya memerlukan tingkat atau kelas penyimpanan berkinerja tinggi untuk memberikan respons kueri yang cepat.

perbaikan terbaru

Perbaikan mendesak untuk masalah kritis dalam lingkungan produksi. Karena urgensinya, perbaikan terbaru biasanya dibuat di luar alur kerja DevOps rilis biasa.

periode hypercare

Segera setelah cutover, periode waktu ketika tim migrasi mengelola dan memantau aplikasi yang dimigrasi di cloud untuk mengatasi masalah apa pun. Biasanya, periode ini panjangnya 1-4 hari. Pada akhir periode hypercare, tim migrasi biasanya mentransfer tanggung jawab untuk aplikasi ke tim operasi cloud.

I

IAc

Lihat infrastruktur sebagai kode.

kebijakan berbasis identitas

Kebijakan yang dilampirkan pada satu atau beberapa prinsip IAM yang mendefinisikan izin mereka dalam lingkungan. AWS Cloud

aplikasi idle

Aplikasi yang memiliki penggunaan CPU dan memori rata-rata antara 5 dan 20 persen selama periode 90 hari. Dalam proyek migrasi, adalah umum untuk menghentikan aplikasi ini atau mempertahankannya di tempat.

IIoT

Lihat Internet of Things industri.

infrastruktur yang tidak dapat diubah

Model yang menyebarkan infrastruktur baru untuk beban kerja produksi alih-alih memperbarui, menambal, atau memodifikasi infrastruktur yang ada. Infrastruktur yang tidak dapat diubah secara inheren lebih konsisten, andal, dan dapat diprediksi daripada infrastruktur yang dapat berubah. Untuk informasi selengkapnya, lihat praktik terbaik Deploy using immutable infrastructure di AWS Well-Architected Framework.

masuk (masuknya) VPC

Dalam arsitektur AWS multi-akun, VPC yang menerima, memeriksa, dan merutekan koneksi jaringan dari luar aplikasi. Arsitektur Referensi AWS Keamanan merekomendasikan pengaturan akun Jaringan Anda dengan inbound, outbound, dan inspeksi VPCs untuk melindungi antarmuka dua arah antara aplikasi Anda dan internet yang lebih luas.

migrasi inkremental

Strategi cutover di mana Anda memigrasikan aplikasi Anda dalam bagian-bagian kecil alih-alih melakukan satu cutover penuh. Misalnya, Anda mungkin hanya memindahkan beberapa layanan mikro atau pengguna ke sistem baru pada awalnya. Setelah Anda memverifikasi bahwa semuanya berfungsi dengan baik, Anda dapat secara bertahap memindahkan layanan mikro atau pengguna tambahan hingga Anda dapat menonaktifkan sistem lama Anda. Strategi ini mengurangi risiko yang terkait dengan migrasi besar.

Industri 4.0

Sebuah istilah yang diperkenalkan oleh Klaus Schwab pada tahun 2016 untuk merujuk pada modernisasi proses manufaktur melalui kemajuan dalam konektivitas, data real-time, otomatisasi, analitik, dan AI/ML.

infrastruktur

Semua sumber daya dan aset yang terkandung dalam lingkungan aplikasi.

infrastruktur sebagai kode (IAc)

Proses penyediaan dan pengelolaan infrastruktur aplikasi melalui satu set file konfigurasi. IAc dirancang untuk membantu Anda memusatkan manajemen infrastruktur, menstandarisasi sumber daya, dan menskalakan dengan cepat sehingga lingkungan baru dapat diulang, andal, dan konsisten.

Internet of Things industri (IIoT)

Penggunaan sensor dan perangkat yang terhubung ke internet di sektor industri, seperti manufaktur, energi, otomotif, perawatan kesehatan, ilmu kehidupan, dan pertanian. Untuk informasi lebih lanjut, lihat Membangun strategi transformasi digital Internet of Things (IIoT) industri.

inspeksi VPC

Dalam arsitektur AWS multi-akun, VPC terpusat yang mengelola inspeksi lalu lintas jaringan antara VPCs (dalam yang sama atau berbeda Wilayah AWS), internet, dan jaringan lokal. Arsitektur Referensi AWS Keamanan merekomendasikan pengaturan akun Jaringan Anda dengan inbound, outbound, dan inspeksi VPCs untuk melindungi antarmuka dua arah antara aplikasi Anda dan internet yang lebih luas.

Internet untuk Segala (IoT)

Jaringan objek fisik yang terhubung dengan sensor atau prosesor tertanam yang berkomunikasi dengan perangkat dan sistem lain melalui internet atau melalui jaringan komunikasi lokal. Untuk informasi selengkapnya, lihat Apa itu IoT?

interpretasi

Karakteristik model pembelajaran mesin yang menggambarkan sejauh mana manusia dapat memahami bagaimana prediksi model bergantung pada inputnya. Untuk informasi lebih lanjut, lihat Interpretabilitas model pembelajaran mesin dengan. AWS

IoT

Lihat Internet of Things.

Perpustakaan informasi TI (ITIL)

Serangkaian praktik terbaik untuk memberikan layanan TI dan menyelaraskan layanan ini dengan persyaratan bisnis. ITIL menyediakan dasar untuk ITSM.

Manajemen layanan TI (ITSM)

Kegiatan yang terkait dengan merancang, menerapkan, mengelola, dan mendukung layanan TI untuk suatu organisasi. Untuk informasi tentang mengintegrasikan operasi cloud dengan alat ITSM, lihat panduan integrasi operasi.

ITIL

Lihat perpustakaan informasi TI.

ITSM

Lihat manajemen layanan TI.

L

kontrol akses berbasis label (LBAC)

Implementasi kontrol akses wajib (MAC) di mana pengguna dan data itu sendiri masing-masing secara eksplisit diberi nilai label keamanan. Persimpangan antara label keamanan pengguna dan label keamanan data menentukan baris dan kolom mana yang dapat dilihat oleh pengguna.

landing zone

Landing zone adalah AWS lingkungan multi-akun yang dirancang dengan baik yang dapat diskalakan dan aman. Ini adalah titik awal dari mana organisasi Anda dapat dengan cepat meluncurkan dan menyebarkan beban kerja dan aplikasi dengan percaya diri dalam lingkungan keamanan dan infrastruktur mereka. Untuk informasi selengkapnya tentang zona pendaratan, lihat Menyiapkan lingkungan multi-akun AWS yang aman dan dapat diskalakan.

model bahasa besar (LLM)

Model AI pembelajaran mendalam yang dilatih sebelumnya pada sejumlah besar data. LLM dapat melakukan beberapa tugas, seperti menjawab pertanyaan, meringkas dokumen, menerjemahkan teks ke dalam bahasa lain, dan menyelesaikan kalimat. Untuk informasi lebih lanjut, lihat Apa itu LLMs.

migrasi besar

Migrasi 300 atau lebih server.

LBAC

Lihat kontrol akses berbasis label.

hak istimewa paling sedikit

Praktik keamanan terbaik untuk memberikan izin minimum yang diperlukan untuk melakukan tugas. Untuk informasi selengkapnya, lihat Menerapkan izin hak istimewa terkecil dalam dokumentasi IAM.

angkat dan geser

Lihat 7 Rs.

sistem endian kecil

Sebuah sistem yang menyimpan byte paling tidak signifikan terlebih dahulu. Lihat juga endianness.

LLM

Lihat model bahasa besar.

lingkungan yang lebih rendah

Lihat lingkungan.

M

pembelajaran mesin (ML)

Jenis kecerdasan buatan yang menggunakan algoritma dan teknik untuk pengenalan pola dan pembelajaran. ML menganalisis dan belajar dari data yang direkam, seperti data Internet of Things (IoT), untuk menghasilkan model statistik berdasarkan pola. Untuk informasi selengkapnya, lihat Machine Learning.

cabang utama

Lihat cabang.

malware

Perangkat lunak yang dirancang untuk membahayakan keamanan atau privasi komputer. Malware dapat mengganggu sistem komputer, membocorkan informasi sensitif, atau mendapatkan akses yang tidak sah. Contoh malware termasuk virus, worm, ransomware, Trojan horse, spyware, dan keyloggers.

layanan terkelola

Layanan AWS yang AWS mengoperasikan lapisan infrastruktur, sistem operasi, dan platform, dan Anda mengakses titik akhir untuk menyimpan dan mengambil data. Amazon Simple Storage Service (Amazon S3) dan Amazon DynamoDB adalah contoh layanan terkelola. Ini juga dikenal sebagai layanan abstrak.

sistem eksekusi manufaktur (MES)

Sistem perangkat lunak untuk melacak, memantau, mendokumentasikan, dan mengendalikan proses produksi yang mengubah bahan baku menjadi produk jadi di lantai toko.

PETA

Lihat Program Percepatan Migrasi.

mekanisme

Proses lengkap di mana Anda membuat alat, mendorong adopsi alat, dan kemudian memeriksa hasilnya untuk melakukan penyesuaian. Mekanisme adalah siklus yang memperkuat dan meningkatkan dirinya sendiri saat beroperasi. Untuk informasi lebih lanjut, lihat Membangun mekanisme di AWS Well-Architected Framework.

akun anggota

Semua Akun AWS selain akun manajemen yang merupakan bagian dari organisasi di AWS Organizations. Sebuah akun hanya dapat menjadi anggota satu organisasi dalam satu waktu.

MES

Lihat sistem eksekusi manufaktur.

Transportasi Telemetri Antrian Pesan (MQTT)

Protokol komunikasi ringan machine-to-machine (M2M), berdasarkan pola terbitkan/berlangganan, untuk perangkat IoT yang dibatasi sumber daya.

layanan mikro

Layanan kecil dan independen yang berkomunikasi melalui definisi yang jelas APIs dan biasanya dimiliki oleh tim kecil yang mandiri. Misalnya, sistem asuransi mungkin mencakup layanan mikro yang memetakan kemampuan bisnis, seperti penjualan atau pemasaran, atau subdomain, seperti pembelian, klaim, atau analitik. Manfaat layanan mikro termasuk kelincahan, penskalaan yang fleksibel, penyebaran yang mudah, kode yang dapat digunakan kembali, dan ketahanan. Untuk informasi selengkapnya, lihat Mengintegrasikan layanan mikro dengan menggunakan layanan tanpa AWS server.

arsitektur microservices

Pendekatan untuk membangun aplikasi dengan komponen independen yang menjalankan setiap proses aplikasi sebagai layanan mikro. Layanan mikro ini berkomunikasi melalui antarmuka yang terdefinisi dengan baik dengan menggunakan ringan. APIs Setiap layanan mikro dalam arsitektur ini dapat diperbarui, digunakan, dan diskalakan untuk memenuhi permintaan fungsi tertentu dari suatu aplikasi. Untuk informasi selengkapnya, lihat Menerapkan layanan mikro di AWS.

Program Percepatan Migrasi (MAP)

AWS Program yang menyediakan dukungan konsultasi, pelatihan, dan layanan untuk membantu organisasi membangun fondasi operasional yang kuat untuk pindah ke cloud, dan untuk membantu mengimbangi biaya awal migrasi. MAP mencakup metodologi migrasi untuk mengeksekusi migrasi lama dengan cara metodis dan seperangkat alat untuk mengotomatisasi dan mempercepat skenario migrasi umum.

migrasi dalam skala

Proses memindahkan sebagian besar portofolio aplikasi ke cloud dalam gelombang, dengan lebih banyak aplikasi bergerak pada tingkat yang lebih cepat di setiap gelombang. Fase ini menggunakan praktik dan pelajaran terbaik dari fase sebelumnya untuk mengimplementasikan pabrik migrasi tim, alat, dan proses untuk merampingkan migrasi beban kerja melalui otomatisasi dan pengiriman tangkas. Ini adalah fase ketiga dari strategi AWS migrasi.

pabrik migrasi

Tim lintas fungsi yang merampingkan migrasi beban kerja melalui pendekatan otomatis dan gesit. Tim pabrik migrasi biasanya mencakup operasi, analis dan pemilik bisnis, insinyur migrasi, pengembang, dan DevOps profesional yang bekerja di sprint. Antara 20 dan 50 persen portofolio aplikasi perusahaan terdiri dari pola berulang yang dapat dioptimalkan dengan pendekatan pabrik. Untuk informasi selengkapnya, lihat diskusi tentang pabrik migrasi dan panduan Pabrik Migrasi Cloud di kumpulan konten ini.

metadata migrasi

Informasi tentang aplikasi dan server yang diperlukan untuk menyelesaikan migrasi. Setiap pola migrasi memerlukan satu set metadata migrasi yang berbeda. Contoh metadata migrasi termasuk subnet target, grup keamanan, dan akun. AWS

pola migrasi

Tugas migrasi berulang yang merinci strategi migrasi, tujuan migrasi, dan aplikasi atau layanan migrasi yang digunakan. Contoh: Rehost migrasi ke Amazon EC2 dengan Layanan Migrasi AWS Aplikasi.

Penilaian Portofolio Migrasi (MPA)

Alat online yang menyediakan informasi untuk memvalidasi kasus bisnis untuk bermigrasi ke. AWS Cloud MPA menyediakan penilaian portofolio terperinci (ukuran kanan server, harga, perbandingan TCO, analisis biaya migrasi) serta perencanaan migrasi (analisis data aplikasi dan pengumpulan data, pengelompokan aplikasi, prioritas migrasi, dan perencanaan gelombang). Alat MPA (memerlukan login) tersedia gratis untuk semua AWS konsultan dan konsultan APN Partner.

Penilaian Kesiapan Migrasi (MRA)

Proses mendapatkan wawasan tentang status kesiapan cloud organisasi, mengidentifikasi kekuatan dan kelemahan, dan membangun rencana aksi untuk menutup kesenjangan yang diidentifikasi, menggunakan CAF. AWS Untuk informasi selengkapnya, lihat panduan kesiapan migrasi. MRA adalah tahap pertama dari strategi AWS migrasi.

strategi migrasi

Pendekatan yang digunakan untuk memigrasikan beban kerja ke file. AWS Cloud Untuk informasi lebih lanjut, lihat entri 7 Rs di glosarium ini dan lihat Memobilisasi organisasi Anda untuk mempercepat migrasi skala besar.

ML

Lihat pembelajaran mesin.

modernisasi

Mengubah aplikasi usang (warisan atau monolitik) dan infrastrukturnya menjadi sistem yang gesit, elastis, dan sangat tersedia di cloud untuk mengurangi biaya, mendapatkan efisiensi, dan memanfaatkan inovasi. Untuk informasi selengkapnya, lihat Strategi untuk memodernisasi aplikasi di. AWS Cloud

penilaian kesiapan modernisasi

Evaluasi yang membantu menentukan kesiapan modernisasi aplikasi organisasi; mengidentifikasi manfaat, risiko, dan dependensi; dan menentukan seberapa baik organisasi dapat mendukung keadaan masa depan aplikasi tersebut. Hasil penilaian adalah cetak biru arsitektur target, peta jalan yang merinci fase pengembangan dan tonggak untuk proses modernisasi, dan rencana aksi untuk mengatasi kesenjangan yang diidentifikasi. Untuk informasi lebih lanjut, lihat Mengevaluasi kesiapan modernisasi untuk aplikasi di. AWS Cloud

aplikasi monolitik (monolit)

Aplikasi yang berjalan sebagai layanan tunggal dengan proses yang digabungkan secara ketat. Aplikasi monolitik memiliki beberapa kelemahan. Jika satu fitur aplikasi mengalami lonjakan permintaan, seluruh arsitektur harus diskalakan. Menambahkan atau meningkatkan fitur aplikasi monolitik juga menjadi lebih kompleks ketika basis kode tumbuh. Untuk mengatasi masalah ini, Anda dapat menggunakan arsitektur microservices. Untuk informasi lebih lanjut, lihat Menguraikan monolit menjadi layanan mikro.

MPA

Lihat Penilaian Portofolio Migrasi.

MQTT

Lihat Transportasi Telemetri Antrian Pesan.

klasifikasi multiclass

Sebuah proses yang membantu menghasilkan prediksi untuk beberapa kelas (memprediksi satu dari lebih dari dua hasil). Misalnya, model ML mungkin bertanya “Apakah produk ini buku, mobil, atau telepon?” atau “Kategori produk mana yang paling menarik bagi pelanggan ini?”

infrastruktur yang bisa berubah

Model yang memperbarui dan memodifikasi infrastruktur yang ada untuk beban kerja produksi. Untuk meningkatkan konsistensi, keandalan, dan prediktabilitas, AWS Well-Architected Framework merekomendasikan penggunaan infrastruktur yang tidak dapat diubah sebagai praktik terbaik.

O

OAC

Lihat kontrol akses asal.

OAI

Lihat identitas akses asal.

OCM

Lihat manajemen perubahan organisasi.

migrasi offline

Metode migrasi di mana beban kerja sumber diturunkan selama proses migrasi. Metode ini melibatkan waktu henti yang diperpanjang dan biasanya digunakan untuk beban kerja kecil dan tidak kritis.

OI

Lihat integrasi operasi.

OLA

Lihat perjanjian tingkat operasional.

migrasi online

Metode migrasi di mana beban kerja sumber disalin ke sistem target tanpa diambil offline. Aplikasi yang terhubung ke beban kerja dapat terus berfungsi selama migrasi. Metode ini melibatkan waktu henti nol hingga minimal dan biasanya digunakan untuk beban kerja produksi yang kritis.

OPC-UA

Lihat Komunikasi Proses Terbuka - Arsitektur Terpadu.

Komunikasi Proses Terbuka - Arsitektur Terpadu (OPC-UA)

Protokol komunikasi machine-to-machine (M2M) untuk otomasi industri. OPC-UA menyediakan standar interoperabilitas dengan enkripsi data, otentikasi, dan skema otorisasi.

perjanjian tingkat operasional (OLA)

Perjanjian yang menjelaskan apa yang dijanjikan kelompok TI fungsional untuk diberikan satu sama lain, untuk mendukung perjanjian tingkat layanan (SLA).

Tinjauan Kesiapan Operasional (ORR)

Daftar pertanyaan dan praktik terbaik terkait yang membantu Anda memahami, mengevaluasi, mencegah, atau mengurangi ruang lingkup insiden dan kemungkinan kegagalan. Untuk informasi lebih lanjut, lihat Ulasan Kesiapan Operasional (ORR) dalam Kerangka Kerja Well-Architected AWS .

teknologi operasional (OT)

Sistem perangkat keras dan perangkat lunak yang bekerja dengan lingkungan fisik untuk mengendalikan operasi industri, peralatan, dan infrastruktur. Di bidang manufaktur, integrasi sistem OT dan teknologi informasi (TI) adalah fokus utama untuk transformasi Industri 4.0.

integrasi operasi (OI)

Proses modernisasi operasi di cloud, yang melibatkan perencanaan kesiapan, otomatisasi, dan integrasi. Untuk informasi selengkapnya, lihat panduan integrasi operasi.

jejak organisasi

Jejak yang dibuat oleh AWS CloudTrail itu mencatat semua peristiwa untuk semua Akun AWS dalam organisasi di AWS Organizations. Jejak ini dibuat di setiap Akun AWS bagian organisasi dan melacak aktivitas di setiap akun. Untuk informasi selengkapnya, lihat Membuat jejak untuk organisasi dalam CloudTrail dokumentasi.

manajemen perubahan organisasi (OCM)

Kerangka kerja untuk mengelola transformasi bisnis utama yang mengganggu dari perspektif orang, budaya, dan kepemimpinan. OCM membantu organisasi mempersiapkan, dan transisi ke, sistem dan strategi baru dengan mempercepat adopsi perubahan, mengatasi masalah transisi, dan mendorong perubahan budaya dan organisasi. Dalam strategi AWS migrasi, kerangka kerja ini disebut percepatan orang, karena kecepatan perubahan yang diperlukan dalam proyek adopsi cloud. Untuk informasi lebih lanjut, lihat panduan OCM.

kontrol akses asal (OAC)

Di CloudFront, opsi yang disempurnakan untuk membatasi akses untuk mengamankan konten Amazon Simple Storage Service (Amazon S3) Anda. OAC mendukung semua bucket S3 di semua Wilayah AWS, enkripsi sisi server dengan AWS KMS (SSE-KMS), dan dinamis dan permintaan ke bucket S3. `PUT` `DELETE`

identitas akses asal (OAI)

Di CloudFront, opsi untuk membatasi akses untuk mengamankan konten Amazon S3 Anda. Saat Anda menggunakan OAI, CloudFront buat prinsipal yang dapat diautentikasi oleh Amazon S3. Prinsipal yang diautentikasi dapat mengakses konten dalam bucket S3 hanya melalui distribusi tertentu. CloudFront Lihat juga OAC, yang menyediakan kontrol akses yang lebih terperinci dan ditingkatkan.

ORR

Lihat tinjauan kesiapan operasional.

OT

Lihat teknologi operasional.

keluar (jalan keluar) VPC

Dalam arsitektur AWS multi-akun, VPC yang menangani koneksi jaringan yang dimulai dari dalam aplikasi. Arsitektur Referensi AWS Keamanan merekomendasikan pengaturan akun Jaringan Anda dengan inbound, outbound, dan inspeksi VPCs untuk melindungi antarmuka dua arah antara aplikasi Anda dan internet yang lebih luas.

P

batas izin

Kebijakan manajemen IAM yang dilampirkan pada prinsipal IAM untuk menetapkan izin maksimum yang dapat dimiliki pengguna atau peran. Untuk informasi selengkapnya, lihat Batas izin dalam dokumentasi IAM.

Informasi Identifikasi Pribadi (PII)

Informasi yang, jika dilihat secara langsung atau dipasangkan dengan data terkait lainnya, dapat digunakan untuk menyimpulkan identitas individu secara wajar. Contoh PII termasuk nama, alamat, dan informasi kontak.

PII

Lihat informasi yang dapat diidentifikasi secara pribadi.

buku pedoman

Serangkaian langkah yang telah ditentukan sebelumnya yang menangkap pekerjaan yang terkait dengan migrasi, seperti mengirimkan fungsi operasi inti di cloud. Buku pedoman dapat berupa skrip, runbook otomatis, atau ringkasan proses atau langkah-langkah yang diperlukan untuk mengoperasikan lingkungan modern Anda.

PLC

Lihat pengontrol logika yang dapat diprogram.

PLM

Lihat manajemen siklus hidup produk.

kebijakan

Objek yang dapat menentukan izin (lihat kebijakan berbasis identitas), menentukan kondisi akses (lihat kebijakan berbasis sumber daya), atau menentukan izin maksimum untuk semua akun di organisasi (lihat kebijakan kontrol layanan). AWS Organizations

ketekunan poliglot

Secara independen memilih teknologi penyimpanan data microservice berdasarkan pola akses data dan persyaratan lainnya. Jika layanan mikro Anda memiliki teknologi penyimpanan data yang sama, mereka dapat menghadapi tantangan implementasi atau mengalami kinerja yang buruk. Layanan mikro lebih mudah diimplementasikan dan mencapai kinerja dan skalabilitas yang lebih baik jika mereka menggunakan penyimpanan data yang paling sesuai dengan kebutuhan mereka. Untuk informasi selengkapnya, lihat Mengaktifkan persistensi data di layanan mikro.

penilaian portofolio

Proses menemukan, menganalisis, dan memprioritaskan portofolio aplikasi untuk merencanakan migrasi. Untuk informasi selengkapnya, lihat Mengevaluasi kesiapan migrasi.

predikat

Kondisi kueri yang mengembalikan `true` atau`false`, biasanya terletak di `WHERE` klausa.

predikat pushdown

Teknik optimasi kueri database yang menyaring data dalam kueri sebelum transfer. Ini mengurangi jumlah data yang harus diambil dan diproses dari database relasional, dan meningkatkan kinerja kueri.

kontrol preventif

Kontrol keamanan yang dirancang untuk mencegah suatu peristiwa terjadi. Kontrol ini adalah garis pertahanan pertama untuk membantu mencegah akses tidak sah atau perubahan yang tidak diinginkan ke jaringan Anda. Untuk informasi selengkapnya, lihat Kontrol pencegahan dalam Menerapkan kontrol keamanan pada. AWS

principal

Entitas AWS yang dapat melakukan tindakan dan mengakses sumber daya. Entitas ini biasanya merupakan pengguna root untuk Akun AWS, peran IAM, atau pengguna. Untuk informasi selengkapnya, lihat Prinsip dalam istilah dan konsep Peran dalam dokumentasi IAM.

privasi berdasarkan desain

Pendekatan rekayasa sistem yang memperhitungkan privasi melalui seluruh proses pengembangan.

zona host pribadi

Container yang menyimpan informasi tentang bagaimana Anda ingin Amazon Route 53 merespons kueri DNS untuk domain dan subdomainnya dalam satu atau lebih. VPCs Untuk informasi selengkapnya, lihat Bekerja dengan zona yang dihosting pribadi di dokumentasi Route 53.

kontrol proaktif

Kontrol keamanan yang dirancang untuk mencegah penyebaran sumber daya yang tidak sesuai. Kontrol ini memindai sumber daya sebelum disediakan. Jika sumber daya tidak sesuai dengan kontrol, maka itu tidak disediakan. Untuk informasi selengkapnya, lihat panduan referensi Kontrol dalam AWS Control Tower dokumentasi dan lihat Kontrol proaktif dalam Menerapkan kontrol keamanan pada AWS.

manajemen siklus hidup produk (PLM)

Manajemen data dan proses untuk suatu produk di seluruh siklus hidupnya, mulai dari desain, pengembangan, dan peluncuran, melalui pertumbuhan dan kematangan, hingga penurunan dan penghapusan.

lingkungan produksi

Lihat lingkungan.

pengontrol logika yang dapat diprogram (PLC)

Di bidang manufaktur, komputer yang sangat andal dan mudah beradaptasi yang memantau mesin dan mengotomatiskan proses manufaktur.

rantai cepat

Menggunakan output dari satu prompt LLM sebagai input untuk prompt berikutnya untuk menghasilkan respons yang lebih baik. Teknik ini digunakan untuk memecah tugas yang kompleks menjadi subtugas, atau untuk secara iteratif memperbaiki atau memperluas respons awal. Ini membantu meningkatkan akurasi dan relevansi respons model dan memungkinkan hasil yang lebih terperinci dan dipersonalisasi.

pseudonimisasi

Proses penggantian pengenal pribadi dalam kumpulan data dengan nilai placeholder. Pseudonimisasi dapat membantu melindungi privasi pribadi. Data pseudonim masih dianggap sebagai data pribadi.

publish/subscribe (pub/sub)

Pola yang memungkinkan komunikasi asinkron antara layanan mikro untuk meningkatkan skalabilitas dan daya tanggap. Misalnya, dalam MES berbasis layanan mikro, layanan mikro dapat mempublikasikan pesan peristiwa ke saluran yang dapat berlangganan layanan mikro lainnya. Sistem dapat menambahkan layanan mikro baru tanpa mengubah layanan penerbitan.

Q

rencana kueri

Serangkaian langkah, seperti instruksi, yang digunakan untuk mengakses data dalam sistem database relasional SQL.

regresi rencana kueri

Ketika pengoptimal layanan database memilih rencana yang kurang optimal daripada sebelum perubahan yang diberikan ke lingkungan database. Hal ini dapat disebabkan oleh perubahan statistik, kendala, pengaturan lingkungan, pengikatan parameter kueri, dan pembaruan ke mesin database.

R

Matriks RACI

Lihat bertanggung jawab, akuntabel, dikonsultasikan, diinformasikan (RACI).

LAP

Lihat Retrieval Augmented Generation.

ransomware

Perangkat lunak berbahaya yang dirancang untuk memblokir akses ke sistem komputer atau data sampai pembayaran dilakukan.

Matriks RASCI

Lihat bertanggung jawab, akuntabel, dikonsultasikan, diinformasikan (RACI).

RCAC

Lihat kontrol akses baris dan kolom.

replika baca

Salinan database yang digunakan untuk tujuan read-only. Anda dapat merutekan kueri ke replika baca untuk mengurangi beban pada database utama Anda.

arsitek ulang

Lihat 7 Rs.

tujuan titik pemulihan (RPO)

Jumlah waktu maksimum yang dapat diterima sejak titik pemulihan data terakhir. Ini menentukan apa yang dianggap sebagai kehilangan 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.

refactor

Lihat 7 Rs.

Wilayah

Kumpulan AWS sumber daya di wilayah geografis. Masing-masing Wilayah AWS terisolasi dan independen dari yang lain untuk memberikan toleransi kesalahan, stabilitas, dan ketahanan. Untuk informasi selengkapnya, lihat Menentukan Wilayah AWS akun yang dapat digunakan.

regresi

Teknik ML yang memprediksi nilai numerik. Misalnya, untuk memecahkan masalah "Berapa harga rumah ini akan dijual?" Model ML dapat menggunakan model regresi linier untuk memprediksi harga jual rumah berdasarkan fakta yang diketahui tentang rumah (misalnya, luas persegi).

rehost

Lihat 7 Rs.

melepaskan

Dalam proses penyebaran, tindakan mempromosikan perubahan pada lingkungan produksi.

memindahkan

Lihat 7 Rs.

memplatform ulang

Lihat 7 Rs.

pembelian kembali

Lihat 7 Rs.

ketahanan

Kemampuan aplikasi untuk melawan atau pulih dari gangguan. Ketersediaan tinggi dan pemulihan bencana adalah pertimbangan umum ketika merencanakan ketahanan di. AWS Cloud Untuk informasi lebih lanjut, lihat AWS Cloud Ketahanan.

kebijakan berbasis sumber daya

Kebijakan yang dilampirkan ke sumber daya, seperti bucket Amazon S3, titik akhir, atau kunci enkripsi. Jenis kebijakan ini menentukan prinsipal mana yang diizinkan mengakses, tindakan yang didukung, dan kondisi lain yang harus dipenuhi.

matriks yang bertanggung jawab, akuntabel, dikonsultasikan, diinformasikan (RACI)

Matriks yang mendefinisikan peran dan tanggung jawab untuk semua pihak yang terlibat dalam kegiatan migrasi dan operasi cloud. Nama matriks berasal dari jenis tanggung jawab yang

didefinisikan dalam matriks: bertanggung jawab (R), akuntabel (A), dikonsultasikan (C), dan diinformasikan (I). Jenis dukungan (S) adalah opsional. Jika Anda menyertakan dukungan, matriks disebut matriks RASCI, dan jika Anda mengecualikannya, itu disebut matriks RACI.

kontrol responsif

Kontrol keamanan yang dirancang untuk mendorong remediasi efek samping atau penyimpangan dari garis dasar keamanan Anda. Untuk informasi selengkapnya, lihat Kontrol responsif dalam Menerapkan kontrol keamanan pada AWS.

melestarikan

Lihat 7 Rs.

pensiun

Lihat 7 Rs.

Retrieval Augmented Generation (RAG)

Teknologi AI generatif di mana LLM mereferensikan sumber data otoritatif yang berada di luar sumber data pelatihannya sebelum menghasilkan respons. Misalnya, model RAG mungkin melakukan pencarian semantik dari basis pengetahuan organisasi atau data kustom. Untuk informasi lebih lanjut, lihat Apa itu RAG.

rotasi

Proses memperbarui rahasia secara berkala untuk membuatnya lebih sulit bagi penyerang untuk mengakses kredensil.

kontrol akses baris dan kolom (RCAC)

Penggunaan ekspresi SQL dasar dan fleksibel yang telah menetapkan aturan akses. RCAC terdiri dari izin baris dan topeng kolom.

RPO

Lihat tujuan titik pemulihan.

RTO

Lihat tujuan waktu pemulihan.

buku runbook

Satu set prosedur manual atau otomatis yang diperlukan untuk melakukan tugas tertentu. Ini biasanya dibangun untuk merampingkan operasi berulang atau prosedur dengan tingkat kesalahan yang tinggi.

D

SAML 2.0

Standar terbuka yang digunakan oleh banyak penyedia identitas (IdPs). Fitur ini memungkinkan sistem masuk tunggal gabungan (SSO), sehingga pengguna dapat masuk ke AWS Management Console atau memanggil operasi AWS API tanpa Anda harus membuat pengguna di IAM untuk semua orang di organisasi Anda. Untuk informasi lebih lanjut tentang federasi berbasis SAMP 2.0, lihat Tentang federasi berbasis SAMP 2.0 dalam dokumentasi IAM.

PENIPUAN

Lihat kontrol pengawasan dan akuisisi data.

SCP

Lihat kebijakan kontrol layanan.

Rahasia

Dalam AWS Secrets Manager, informasi rahasia atau terbatas, seperti kata sandi atau kredensil pengguna, yang Anda simpan dalam bentuk terenkripsi. Ini terdiri dari nilai rahasia dan metadata-nya. Nilai rahasia dapat berupa biner, string tunggal, atau beberapa string. Untuk informasi selengkapnya, lihat Apa yang ada di rahasia Secrets Manager? dalam dokumentasi Secrets Manager.

keamanan dengan desain

Pendekatan rekayasa sistem yang memperhitungkan keamanan melalui seluruh proses pengembangan.

kontrol keamanan

Pagar pembatas teknis atau administratif yang mencegah, mendeteksi, atau mengurangi kemampuan pelaku ancaman untuk mengeksploitasi kerentanan keamanan. Ada empat jenis kontrol keamanan utama: preventif, detektif, responsif, dan proaktif.

pengerasan keamanan

Proses mengurangi permukaan serangan untuk membuatnya lebih tahan terhadap serangan. Ini dapat mencakup tindakan seperti menghapus sumber daya yang tidak lagi diperlukan, menerapkan praktik keamanan terbaik untuk memberikan hak istimewa paling sedikit, atau menonaktifkan fitur yang tidak perlu dalam file konfigurasi.

sistem informasi keamanan dan manajemen acara (SIEM)

Alat dan layanan yang menggabungkan sistem manajemen informasi keamanan (SIM) dan manajemen acara keamanan (SEM). Sistem SIEM mengumpulkan, memantau, dan menganalisis data dari server, jaringan, perangkat, dan sumber lain untuk mendeteksi ancaman dan pelanggaran keamanan, dan untuk menghasilkan peringatan.

otomatisasi respons keamanan

Tindakan yang telah ditentukan dan diprogram yang dirancang untuk secara otomatis merespons atau memulihkan peristiwa keamanan. Otomatisasi ini berfungsi sebagai kontrol keamanan detektif atau responsif yang membantu Anda menerapkan praktik terbaik AWS keamanan. Contoh tindakan respons otomatis termasuk memodifikasi grup keamanan VPC, menambal instans EC2 Amazon, atau memutar kredensil.

enkripsi sisi server

Enkripsi data di tujuannya, oleh Layanan AWS yang menerimanya.

kebijakan kontrol layanan (SCP)

Kebijakan yang menyediakan kontrol terpusat atas izin untuk semua akun di organisasi. AWS Organizations SCPs menentukan pagar pembatas atau menetapkan batasan pada tindakan yang dapat didelegasikan oleh administrator kepada pengguna atau peran. Anda dapat menggunakan SCPs daftar izin atau daftar penolakan, untuk menentukan layanan atau tindakan mana yang diizinkan atau dilarang. Untuk informasi selengkapnya, lihat Kebijakan kontrol layanan dalam AWS Organizations dokumentasi.

titik akhir layanan

URL titik masuk untuk file Layanan AWS. Anda dapat menggunakan endpoint untuk terhubung secara terprogram ke layanan target. Untuk informasi selengkapnya, lihat Layanan AWS titik akhir di Referensi Umum AWS.

perjanjian tingkat layanan (SLA)

Perjanjian yang menjelaskan apa yang dijanjikan tim TI untuk diberikan kepada pelanggan mereka, seperti waktu kerja dan kinerja layanan.

indikator tingkat layanan (SLI)

Pengukuran aspek kinerja layanan, seperti tingkat kesalahan, ketersediaan, atau throughputnya.

tujuan tingkat layanan (SLO)

Metrik target yang mewakili kesehatan layanan, yang diukur dengan indikator tingkat layanan.

model tanggung jawab bersama

Model yang menjelaskan tanggung jawab yang Anda bagikan AWS untuk keamanan dan kepatuhan cloud. AWS bertanggung jawab atas keamanan cloud, sedangkan Anda bertanggung jawab atas keamanan di cloud. Untuk informasi selengkapnya, lihat Model tanggung jawab bersama.

SIEM

Lihat informasi keamanan dan sistem manajemen acara.

titik kegagalan tunggal (SPOF)

Kegagalan dalam satu komponen penting dari aplikasi yang dapat mengganggu sistem.

SLA

Lihat perjanjian tingkat layanan.

SLI

Lihat indikator tingkat layanan.

SLO

Lihat tujuan tingkat layanan.

split-and-seed model

Pola untuk menskalakan dan mempercepat proyek modernisasi. Ketika fitur baru dan rilis produk didefinisikan, tim inti berpisah untuk membuat tim produk baru. Ini membantu meningkatkan kemampuan dan layanan organisasi Anda, meningkatkan produktivitas pengembang, dan

mendukung inovasi yang cepat. Untuk informasi lebih lanjut, lihat Pendekatan bertahap untuk memodernisasi aplikasi di. AWS Cloud

SPOF

Lihat satu titik kegagalan.

skema bintang

Struktur organisasi database yang menggunakan satu tabel fakta besar untuk menyimpan data transaksional atau terukur dan menggunakan satu atau lebih tabel dimensi yang lebih kecil untuk menyimpan atribut data. Struktur ini dirancang untuk digunakan dalam gudang data atau untuk tujuan intelijen bisnis.

pola ara pencekik

Pendekatan untuk memodernisasi sistem monolitik dengan menulis ulang secara bertahap dan mengganti fungsionalitas sistem sampai sistem warisan dapat dinonaktifkan. Pola ini menggunakan analogi pohon ara yang tumbuh menjadi pohon yang sudah mapan dan akhirnya mengatasi dan menggantikan inangnya. Pola ini diperkenalkan oleh Martin Fowler sebagai cara untuk mengelola risiko saat menulis ulang sistem monolitik. Untuk contoh cara menerapkan pola ini, lihat Memodernisasi layanan web Microsoft ASP.NET (ASMX) lama secara bertahap menggunakan container dan Amazon API Gateway.

subnet

Rentang alamat IP dalam VPC Anda. Subnet harus berada di Availability Zone tunggal.

kontrol pengawasan dan akuisisi data (SCADA)

Di bidang manufaktur, sistem yang menggunakan perangkat keras dan perangkat lunak untuk memantau aset fisik dan operasi produksi.

enkripsi simetris

Algoritma enkripsi yang menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi data.

pengujian sintetis

Menguji sistem dengan cara yang mensimulasikan interaksi pengguna untuk mendeteksi potensi masalah atau untuk memantau kinerja. Anda dapat menggunakan Amazon CloudWatch Synthetics untuk membuat tes ini.

sistem prompt

Teknik untuk memberikan konteks, instruksi, atau pedoman ke LLM untuk mengarahkan perilakunya. Permintaan sistem membantu mengatur konteks dan menetapkan aturan untuk interaksi dengan pengguna.

T

tag

Pasangan nilai kunci yang bertindak sebagai metadata untuk mengatur sumber daya Anda. AWS Tag dapat membantu Anda mengelola, mengidentifikasi, mengatur, mencari, dan memfilter sumber daya. Untuk informasi selengkapnya, lihat Menandai sumber daya AWS.

variabel target

Nilai yang Anda coba prediksi dalam ML yang diawasi. Ini juga disebut sebagai variabel hasil. Misalnya, dalam pengaturan manufaktur, variabel target bisa menjadi cacat produk.

daftar tugas

Alat yang digunakan untuk melacak kemajuan melalui runbook. Daftar tugas berisi ikhtisar runbook dan daftar tugas umum yang harus diselesaikan. Untuk setiap tugas umum, itu termasuk perkiraan jumlah waktu yang dibutuhkan, pemilik, dan kemajuan.

lingkungan uji

Lihat lingkungan.

pelatihan

Untuk menyediakan data bagi model ML Anda untuk dipelajari. Data pelatihan harus berisi jawaban yang benar. Algoritma pembelajaran menemukan pola dalam data pelatihan yang memetakan atribut data input ke target (jawaban yang ingin Anda prediksi). Ini menghasilkan model ML yang menangkap pola-pola ini. Anda kemudian dapat menggunakan model ML untuk membuat prediksi pada data baru yang Anda tidak tahu targetnya.

gerbang transit

Hub transit jaringan yang dapat Anda gunakan untuk menghubungkan jaringan Anda VPCs dan lokal. Untuk informasi selengkapnya, lihat Apa itu gateway transit dalam AWS Transit Gateway dokumentasi.

alur kerja berbasis batang

Pendekatan di mana pengembang membangun dan menguji fitur secara lokal di cabang fitur dan kemudian menggabungkan perubahan tersebut ke cabang utama. Cabang utama kemudian dibangun untuk pengembangan, praproduksi, dan lingkungan produksi, secara berurutan.

akses tepercaya

Memberikan izin ke layanan yang Anda tentukan untuk melakukan tugas di organisasi Anda di dalam AWS Organizations dan di akunnya atas nama Anda. Layanan tepercaya menciptakan peran terkait layanan di setiap akun, ketika peran itu diperlukan, untuk melakukan tugas manajemen untuk Anda. Untuk informasi selengkapnya, lihat Menggunakan AWS Organizations dengan AWS layanan lain dalam AWS Organizations dokumentasi.

penyetelan

Untuk mengubah aspek proses pelatihan Anda untuk meningkatkan akurasi model ML. Misalnya, Anda dapat melatih model ML dengan membuat set pelabelan, menambahkan label, dan kemudian mengulangi langkah-langkah ini beberapa kali di bawah pengaturan yang berbeda untuk mengoptimalkan model.

tim dua pizza

Sebuah DevOps tim kecil yang bisa Anda beri makan dengan dua pizza. Ukuran tim dua pizza memastikan peluang terbaik untuk berkolaborasi dalam pengembangan perangkat lunak.

U

waswas

Sebuah konsep yang mengacu pada informasi yang tidak tepat, tidak lengkap, atau tidak diketahui yang dapat merusak keandalan model ML prediktif. Ada dua jenis ketidakpastian: ketidakpastian epistemik disebabkan oleh data yang terbatas dan tidak lengkap, sedangkan ketidakpastian aleatorik disebabkan oleh kebisingan dan keacakan yang melekat dalam data. Untuk informasi lebih lanjut, lihat panduan Mengukur ketidakpastian dalam sistem pembelajaran mendalam.

tugas yang tidak terdiferensiasi

Juga dikenal sebagai angkat berat, pekerjaan yang diperlukan untuk membuat dan mengoperasikan aplikasi tetapi itu tidak memberikan nilai langsung kepada pengguna akhir atau

memberikan keunggulan kompetitif. Contoh tugas yang tidak terdiferensiasi termasuk pengadaan, pemeliharaan, dan perencanaan kapasitas.

lingkungan atas

Lihat lingkungan.

V

menyedot debu

Operasi pemeliharaan database yang melibatkan pembersihan setelah pembaruan tambahan untuk merebut kembali penyimpanan dan meningkatkan kinerja.

kendali versi

Proses dan alat yang melacak perubahan, seperti perubahan kode sumber dalam repositori.

Peering VPC

Koneksi antara dua VPCs yang memungkinkan Anda untuk merutekan lalu lintas dengan menggunakan alamat IP pribadi. Untuk informasi selengkapnya, lihat Apa itu peering VPC di dokumentasi VPC Amazon.

kerentanan

Kelemahan perangkat lunak atau perangkat keras yang membahayakan keamanan sistem.

W

cache hangat

Cache buffer yang berisi data saat ini dan relevan yang sering diakses. Instance database dapat membaca dari cache buffer, yang lebih cepat daripada membaca dari memori utama atau disk.

data hangat

Data yang jarang diakses. Saat menanyakan jenis data ini, kueri yang cukup lambat biasanya dapat diterima.

fungsi jendela

Fungsi SQL yang melakukan perhitungan pada sekelompok baris yang berhubungan dengan catatan saat ini. Fungsi jendela berguna untuk memproses tugas, seperti menghitung rata-rata bergerak atau mengakses nilai baris berdasarkan posisi relatif dari baris saat ini.

beban kerja

Kumpulan sumber daya dan kode yang memberikan nilai bisnis, seperti aplikasi yang dihadapi pelanggan atau proses backend.

aliran kerja

Grup fungsional dalam proyek migrasi yang bertanggung jawab atas serangkaian tugas tertentu. Setiap alur kerja independen tetapi mendukung alur kerja lain dalam proyek. Misalnya, alur kerja portofolio bertanggung jawab untuk memprioritaskan aplikasi, perencanaan gelombang, dan mengumpulkan metadata migrasi. Alur kerja portofolio mengirimkan aset ini ke alur kerja migrasi, yang kemudian memigrasikan server dan aplikasi.

CACING

Lihat menulis sekali, baca banyak.

WQF

Lihat AWS Kerangka Kualifikasi Beban Kerja.

tulis sekali, baca banyak (WORM)

Model penyimpanan yang menulis data satu kali dan mencegah data dihapus atau dimodifikasi. Pengguna yang berwenang dapat membaca data sebanyak yang diperlukan, tetapi mereka tidak dapat mengubahnya. Infrastruktur penyimpanan data ini dianggap tidak dapat diubah.

Z

eksploitasi zero-day

Serangan, biasanya malware, yang memanfaatkan kerentanan zero-day.

kerentanan zero-day

Cacat atau kerentanan yang tak tanggung-tanggung dalam sistem produksi. Aktor ancaman dapat menggunakan jenis kerentanan ini untuk menyerang sistem. Pengembang sering menyadari kerentanan sebagai akibat dari serangan tersebut.

bisikan zero-shot

Memberikan LLM dengan instruksi untuk melakukan tugas tetapi tidak ada contoh (tembakan) yang dapat membantu membimbingnya. LLM harus menggunakan pengetahuan pra-terlatih untuk menangani tugas. Efektivitas bidikan nol tergantung pada kompleksitas tugas dan kualitas prompt. Lihat juga beberapa bidikan yang diminta.

aplikasi zombie

Aplikasi yang memiliki CPU rata-rata dan penggunaan memori di bawah 5 persen. Dalam proyek migrasi, adalah umum untuk menghentikan aplikasi ini.

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