Membangun Pabrik Cetak Biru Perusahaan dengan menggunakan AWS Service Catalog

AWS Bimbingan Preskriptif

AWS Bimbingan Preskriptif: Membangun Pabrik Cetak Biru Perusahaan dengan menggunakan AWS Service Catalog

Table of Contents

Membangun Pabrik Cetak Biru Perusahaan dengan menggunakan AWS Service Catalog

Amazon Web Services (kontributor)

Oktober 2024 (sejarah dokumen)

Ikhtisar bisnis

Banyak perusahaan menghadapi tantangan saat meningkatkan beban kerja mereka di cloud. Tantangan organisasi ini meliputi:

- Membuat templat infrastruktur sebagai kode (IAc) yang dapat digunakan kembali dalam skala besar untuk beberapa Layanan AWS
- Memvalidasi bahwa template IAc mengikuti praktik terbaik keamanan
- Mengurangi tugas yang tidak berdiferensiasi atau berulang yang dapat secara signifikan mengurangi produktivitas pengembang dan memperpanjang waktu ke pasar
- Menetapkan konsistensi untuk template IAc
- Mengurangi pemanfaatan sumber daya, terutama untuk tim keamanan, untuk menghindari tinjauan manual berulang

Membuat template IAC yang mengikuti praktik terbaik keamanan mengharuskan Anda membuat pagar pembatas dan kontrol keamanan. Secara tradisional, tim platform cloud atau tim keamanan akan secara manual meninjau kode di setiap template IAC. Atau, pengembang akan menyebarkan template IAC di lingkungan non-produksi dan mengandalkan kontrol detektif untuk menemukan masalah keamanan apa pun. Kedua pendekatan ini membutuhkan siklus umpan balik berulang, memperlambat proses pengembangan, dan meningkatkan upaya rekayasa manual.

Akibatnya, banyak perusahaan ingin merampingkan pembuatan, validasi, dan rilis template IAc. Mereka juga menginginkan sarana untuk mengelola dan mengatur template tersebut setelah rilis. Mekanisme manajemen dan tata kelola yang tepat membantu Anda memperbarui template dan memastikan bahwa pengembang memiliki akses ke versi terbaru. Mekanisme ini juga membantu Anda mengawasi dan mengaudit penggunaan templat di seluruh organisasi.

Ikhtisar solusi

Panduan ini menjelaskan solusi Enterprise Blueprint Factory, yang membantu Anda merampingkan pembuatan, validasi, penerbitan, distribusi, dan konsumsi templat infrastruktur sebagai kode (IAc) di seluruh organisasi Anda. Template IAC ini juga disebut cetak biru. Solusi ini mendukung file cetak biru yang merupakan AWS CloudFormationtemplat atau konstruksi. AWS Cloud Development Kit (AWS CDK)

Enterprise Blueprint Factory menggunakan pendekatan berbasis konfigurasi untuk mengotomatiskan berbagi, penerbitan, dan distribusi cetak biru. Pengembang menambahkan cetak biru ke repositori produk dan kemudian menambahkan informasi cetak biru ke file konfigurasi. Ini secara otomatis memulai pipeline rilis integrasi berkelanjutan dan pengiriman berkelanjutan (CI/CD). Pipeline ini memvalidasi bahwa cetak biru mengikuti AWS praktik terbaik keamanan. Ini membantu memastikan bahwa cetak biru organisasi Anda aman menurut desain. Keamanan dengan desain adalah pendekatan rekayasa sistem yang memperhitungkan keamanan melalui seluruh proses pengembangan.

Enterprise Blueprint Factory merilis cetak biru sebagai produk di. AWS Service Catalog Dengan menggunakan Service Catalog, pengguna akhir dapat dengan cepat menerapkan cetak biru yang disetujui yang Anda berikan. Service Catalog juga dirancang untuk menyediakan fitur manajemen dan tata kelola sehingga administrator dapat menentukan kontrol akses yang halus dan mengawasi penggunaan cetak biru.

Audiens yang dituju

Bagian arsitektur Enterprise Blueprint Factory membantu arsitek, manajer, dan pemimpin teknis mengevaluasi solusi ini dan menentukan apakah itu cocok untuk organisasi mereka. Bagian ini menjelaskan apa itu cetak biru, bagaimana Anda dapat menggunakan Service Catalog untuk mengelolanya, dan arsitektur Enterprise Blueprint Factory.

Bagian Menyiapkan Pabrik Cetak Biru Perusahaan membantu DevOps para insinyur menyebarkan Pabrik Cetak Biru Perusahaan di lingkungan Anda. AWS Ini termasuk instruksi terperinci untuk mengatur repositori yang diperlukan dan pipa konfigurasi.

Bagian Menggunakan Pabrik Cetak Biru Perusahaan membantu pengembang cetak biru membuat, memperbarui, atau menghapus cetak biru di lingkungan Anda. Ini memberikan instruksi terperinci untuk mengelola cetak biru sepanjang siklus hidupnya. Untuk membuat cetak biru, pengembang

harus memahami cara membuat templat IAC, seperti templat. CloudFormation Panduan ini tidak menyertakan informasi atau instruksi tentang cara mendefinisikan cetak biru ini.

Tujuan

Pabrik Cetak Biru Perusahaan membantu organisasi Anda mencapai manfaat berikut:

- Validasi bahwa cetak biru mengikuti praktik terbaik keamanan AWS
- Mengotomatiskan dan menstandarisasi proses rilis dan validasi untuk cetak biru
- Meningkatkan produktivitas pengembang dengan mengurangi jumlah tugas manual yang harus mereka lakukan
- Gunakan kontrol akses berbutir halus untuk menentukan cetak biru mana yang dapat diakses pengguna akhir
- Gunakan kontrol versi untuk mengelola pembaruan cetak biru dan membagikannya dengan pengguna akhir
- Bantu pengguna akhir melayani diri sendiri penemuan dan peluncuran cetak biru
- Mengawasi dan mengaudit penggunaan cetak biru di seluruh organisasi

Arsitektur Pabrik Cetak Biru Perusahaan

Template Infrastructure as code (IAc), juga disebut cetak biru, adalah file konfigurasi yang membantu Anda menyediakan dan mengelola sumber daya cloud. Cetak biru mungkin menyediakan sumber daya tunggal, atau mungkin menyediakan arsitektur untuk aplikasi multi-tier yang kompleks. IAc dirancang untuk membantu Anda memusatkan manajemen infrastruktur, menstandarisasi sumber daya, dan meningkatkan skala dengan cepat.

Pabrik Cetak Biru Perusahaan membantu Anda merampingkan pembuatan, validasi, penerbitan, distribusi, dan konsumsi cetak biru di seluruh organisasi Anda. Selain memberikan gambaran arsitektur, bagian ini mengulas komponen arsitektur dari solusi dan siklus hidup cetak biru.

Ketika Anda merilis cetak biru melalui Enterprise Blueprint Factory, cetak biru menjadi produk di. AWS Service Catalog Anda mengumpulkan produk ke dalam satu atau beberapa portofolio dan kemudian memberikan izin yang memungkinkan pengguna akhir mengakses produk dalam portofolio tersebut. Anda dapat menggunakan pembagian portofolio untuk mengizinkan administrator Service Catalog bagi orang lain Akun AWS untuk mendistribusikan produk Anda ke pengguna akhir.

Diagram berikut menunjukkan gambaran tingkat tinggi arsitektur Enterprise Blueprint Factory. Alur kerja ini merilis cetak biru sebagai produk di Service Catalog. Ini juga membuat atau memperbarui portofolio dan saham portofolio untuk membuat cetak biru tersedia bagi pengguna akhir target.

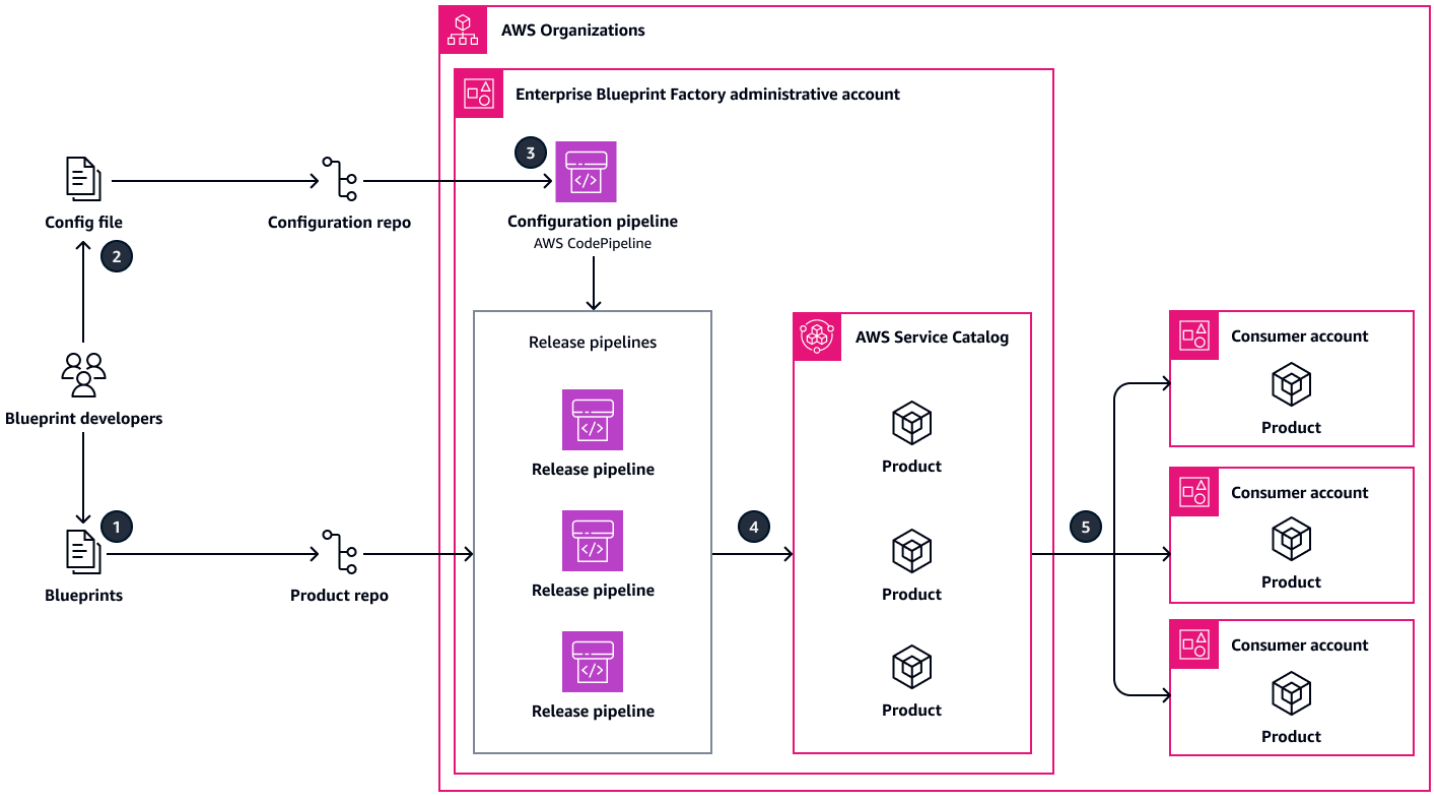


Diagram ini menunjukkan alur kerja berikut:

1. Seorang pengembang membangun cetak biru. Mereka membuat cabang fitur di repositori produk, mendorong cetak biru ke cabang, dan kemudian membuat permintaan tarik. Tim administrasi cetak biru dan tim keamanan meninjau permintaan tarik untuk memastikan bahwa cetak biru memenuhi persyaratan organisasi dan keamanan. Tim-tim ini menyetujui permintaan tarik. Pengembang menggabungkan cabang fitur ke cabang utama. Untuk informasi selengkapnya, lihat Repositori produk dalam panduan ini.
2. Pengembang menambahkan atau memperbarui informasi cetak biru di file konfigurasi yang terletak di repo konfigurasi. Untuk informasi selengkapnya, lihat Repositori konfigurasi dan file Konfigurasi dalam panduan ini.
3. Pembaruan ke file konfigurasi memanggil pipeline konfigurasi. Pipeline ini menggunakan AWS CodePipelinedan AWS CodeBuildmemproyeksikan untuk membuat atau memperbarui portofolio Service Catalog dan pembagian portofolio. Ini juga menciptakan pipa rilis untuk cetak biru. Untuk informasi selengkapnya, lihat Pipa konfigurasi dalam panduan ini.
4. Pipeline rilis melakukan berbagai pemeriksaan keamanan pada cetak biru. Jika cetak biru lolos, pipeline rilis akan menerapkan cetak biru sebagai produk di Service Catalog. Untuk informasi selengkapnya, lihat Rilis pipeline dalam panduan ini.

5. Dengan mengakses produk melalui portofolio dan saham portofolio, pengguna akhir menyebarkan cetak biru di akun konsumen target mereka.

Komponen Pabrik Cetak Biru Perusahaan

Enterprise Blueprint Factory terdiri dari komponen-komponen berikut:

- Repositori produk — Repositori tempat Anda menyimpan cetak biru.
- Repositori konfigurasi — Repositori tempat Anda menyimpan file konfigurasi yang mendefinisikan portofolio dan produk Anda. AWS Service Catalog
- File konfigurasi — File konfigurasi yang menentukan cetak biru apa yang tersedia, siapa yang dapat menggunakannya, dan bagaimana mereka dapat menggunakannya.
- Configuration pipeline — Pipeline DevOps CI/CD yang menyiapkan portofolio Service Catalog dan portofolio share dan membuat pipeline rilis untuk setiap produk.
- Rilis pipeline — Pipeline DevOps CI/CD yang merilis cetak biru sebagai produk Service Catalog.

Tim infrastruktur cloud biasanya mengelola Enterprise Blueprint Factory secara keseluruhan karena mereka harus menyetujui setiap cetak biru. Namun, tim DevOps kode biasanya bertanggung jawab atas pipa konfigurasi dan pipa rilis. Untuk merilis cetak biru baru, pengembang hanya berinteraksi dengan repositori produk, repositori konfigurasi, dan file konfigurasi.

Repositori produk

Repositori produk adalah lokasi terpusat tempat Anda menyimpan cetak biru yang disetujui organisasi Anda. Tim administrasi cetak biru dan tim keamanan meninjau permintaan tarik ke repositori ini untuk memastikan bahwa setiap cetak biru memenuhi persyaratan organisasi dan keamanan. Dalam panduan ini, kami gunakan GitHub untuk repositori, tetapi Anda dapat menggunakan alternatif.

Repositori konfigurasi

Repositori konfigurasi (config repo) adalah lokasi di mana organisasi Anda menyimpan file konfigurasi untuk portofolio Service Catalog dan produk yang dirilis melalui Enterprise Blueprint Factory. Dalam panduan ini, kami gunakan GitHub untuk repositori, tetapi Anda dapat menggunakan alternatif.

File konfigurasi

File konfigurasi Enterprise Blueprint Factory (file konfigurasi) disimpan dalam repositori konfigurasi, yang dimiliki oleh tim administratif cetak biru. Nama file ini adalah bp_config.yml. Saat pengembang memperbarui file ini, tim administratif cetak biru meninjau perubahan tersebut. Menggabungkan perubahan ke cabang utama memulai pipa konfigurasi. File konfigurasi mengatur penerbitan, berbagi, dan distribusi semua cetak biru yang dikelola melalui Enterprise Blueprint Factory.

File konfigurasi adalah file YAMM yang terdiri dari dua objek utama: `portfolios` dan. `products` Berikut ini adalah contoh contoh file konfigurasi:

```
portfolios:
  - portfolio_name: blueprint-portfolio
    owner: Blueprint-team
    provider_name: AWS
    description: "Blueprint portfolio"
    portfolio_access_role:
       - arn:aws:iam::123456789012:role/examplerole
       - arn:aws:iam::123456789012:user/exampleuser
    share_to_ou:
     - org_id: "o-exampleOrgID"
    stack_tags:
      DataClassification: Confidential
      Organization: AWS
products:
  - name: BP-S3-Product
    description: "Blueprint for BP-S3 product"
    product_config_file: 'BP-S3/product_config.json'
    owner: Blueprint-team
    stack_tags:
      DataClassification: Confidential
      Organization: AWS
    portfolio_associations:
      - blueprint-portfolio
    launch_constraint_role: arn:aws:iam::123456789012:role/examplelaunchrole
```

Di `portfolios` objek, Anda menentukan portofolio Service Catalog target Anda. Untuk setiap portofolio, Anda memberikan atribut berikut:

- `portfolio_name`adalah nama portofolio. Atribut ini diperlukan.
- `owner`adalah nama tim yang memiliki portofolio. Atribut ini opsional.

- `provider_name`adalah nama tim atau organisasi yang mengelola portofolio. Nilai default-nya adalah `AWS`. Atribut ini diperlukan.
- `description`adalah deskripsi singkat dari portofolio. Atribut ini opsional.
- `portfolio_access_roles`adalah identitas AWS Identity and Access Management (IAM) (pengguna, peran, atau grup) yang diizinkan untuk mengakses portofolio dan produk terkaitnya. Atribut ini opsional.
- `share_to_ou`adalah unit organisasi (OU) di AWS Organizations mana portofolio dibagi. Pengguna akhir dapat menyebarkan produk portofolio ini Akun AWS yang merupakan anggota OU target. Atribut ini opsional.
- `stack_tags`adalah tag yang diterapkan pada portofolio. Atribut ini opsional.

Dalam `products` objek, Anda menentukan setiap cetak biru yang ingin Anda rilis sebagai produk di Service Catalog. Untuk setiap produk, Anda memberikan atribut berikut:

- `name`adalah nama produk di Service Catalog. Atribut ini diperlukan.
- `description`adalah deskripsi singkat tentang produk. Atribut ini diperlukan.
- `product_config_file`adalah nama file konfigurasi produk cetak biru yang disimpan dalam repositori produk. Atribut ini diperlukan.
- `owner`adalah nama tim yang memiliki produk. Atribut ini diperlukan.
- `stack_tags`adalah tag yang diterapkan pada produk. Atribut ini opsional.
- `portfolio_associations`adalah portofolio target yang berisi produk. Atribut ini opsional.

> **Note**
>
> Kami menyarankan Anda menambahkan produk hanya ke portofolio yang dikelola melalui Enterprise Blueprint Factory. Jika Anda ingin menambahkan produk ke portofolio yang tidak dikelola melalui Pabrik Cetak Biru Perusahaan, kebijakan IAM pengguna harus mengizinkan tindakan tersebut. AssociateProductWithPortfolio Namun, sebagai praktik terbaik keamanan, sebaiknya Anda mengizinkan tindakan ini hanya untuk pipeline konfigurasi Enterprise Blueprint Factory.

- `launch_constraint_role`adalah peran peluncuran yang diasumsikan oleh Service Catalog saat pengguna akhir meluncurkan produk. Atribut ini diperlukan.

Pipa konfigurasi

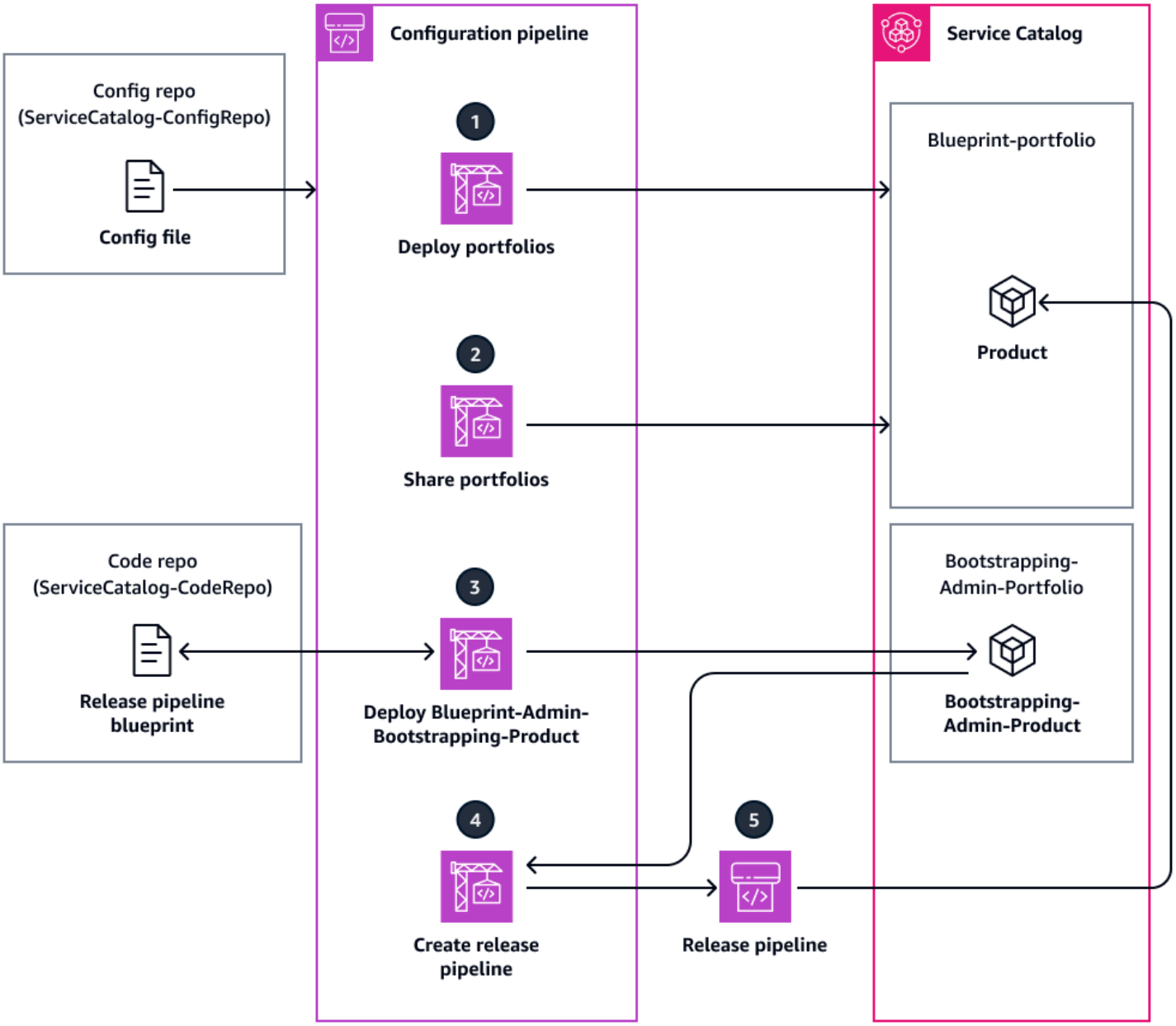
Pipeline konfigurasi (config pipeline) mengotomatiskan konfigurasi portofolio Service Catalog dan pembagian portofolio. Ini juga menciptakan pipa rilis untuk setiap produk. Pipeline ini adalah AWS CodePipelinesumber daya. Pembaruan ke file konfigurasi memanggil pipeline konfigurasi.

Pertama kali Anda menjalankan pipeline konfigurasi, itu membuat dua portofolio tambahan yang tidak ditentukan dalam file konfigurasi Anda:

- `Blueprint-portfolio`— Setiap produk yang Anda gunakan melalui Enterprise Blueprint Factory ditambahkan ke portofolio ini. Portofolio ini tersedia untuk prinsipal IAM dan unit organisasi yang Anda tentukan dalam file konfigurasi.
- `Bootstrapping-Admin-Portfolio`— `Bootstrapping-Admin-Product` Produk dikaitkan dengan portofolio ini. Produk ini adalah CloudFormation template untuk pipa rilis. Izinkan hanya tim administrasi cetak biru untuk mengakses portofolio ini sehingga mereka dapat mengelola produk administrasi.

Tahapan pipa konfigurasi

Gambar berikut menunjukkan tahapan dalam pipeline konfigurasi dan sumber daya yang berinteraksi dengan pipeline. Setiap tahap dalam pipa adalah sebuah AWS CodeBuildproyek.



Berikut ini adalah tahapan dari pipa konfigurasi:

1. Terapkan portofolio — Pipeline konfigurasi menyebarkan portofolio apa pun yang telah ditambahkan ke file konfigurasi atau menghapus portofolio apa pun yang telah dihapus dari file konfigurasi. Jika tidak ada perubahan pada portofolio, maka pipeline melewati tahap ini.
2. Bagikan portofolio — Pipeline konfigurasi berbagi portofolio dengan unit organisasi target (). OUs Jika tidak ada perubahan pada saham portofolio, maka pipa melewati tahap ini.
3. Deploy Blueprint-Admin-Bootstrapping-Product — Pipeline konfigurasi mengambil `bp-pipeline` cetak biru dari `ServiceCatalog-CodeRepo` repo dan menerapkannya ke Service Catalog

sebagai. `Bootstrapping-Admin-Product` Produk ini adalah CloudFormation template yang digunakan untuk membuat pipeline rilis. Menerapkan template ini sebagai produk Service Catalog membantu mempertahankan kontrol versi. Jika tidak ada perubahan pada `bp-pipeline` cetak biru, maka pipa melewati tahap ini.

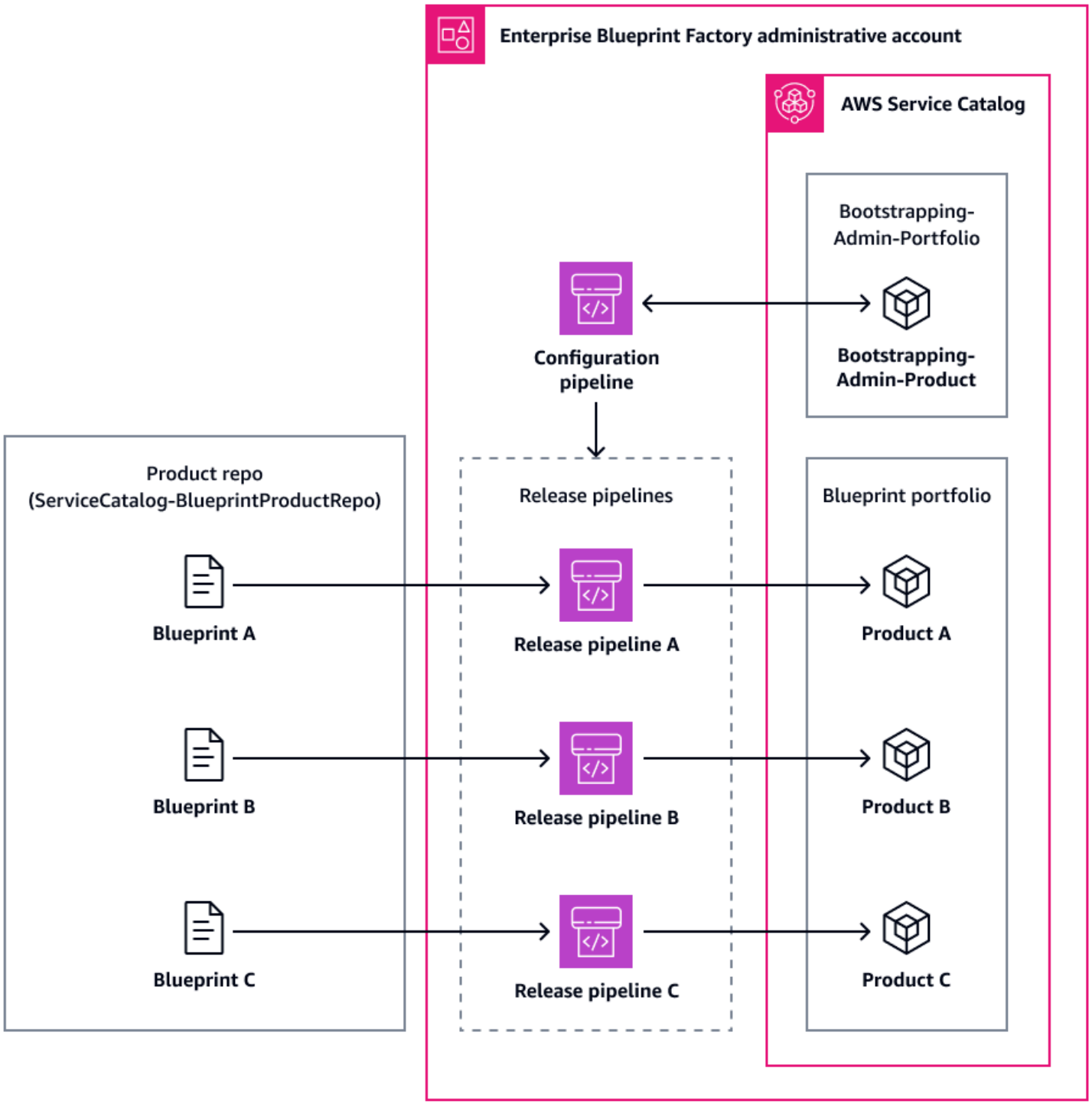
4. Buat pipeline rilis — Berdasarkan atribut produk dalam file konfigurasi, pipeline konfigurasi menyiapkan parameter tumpukan dan meluncurkan CloudFormation tumpukan yang membuat pipeline rilis untuk produk. Untuk informasi selengkapnya, lihat Rilis pipeline dalam panduan ini.
5. Menyebarkan produk — Saluran rilis menyebarkan cetak biru sebagai produk Service Catalog dan mengaitkannya dengan portofolio target. Pengguna akhir sekarang dapat menyebarkan produk Akun AWS yang merupakan anggota OU target.

Rilis pipa

Pipeline rilis mengotomatiskan rilis cetak biru sebagai produk Service Catalog. Pipeline ini adalah AWS CodePipelinesumber daya. Saat organisasi Anda ingin merilis cetak biru baru, pengembang mengunggah template IAC dan file konfigurasi produknya ke repo produk. Menambahkan detail produk ke file konfigurasi memicu pipeline konfigurasi. Pipeline konfigurasi membuat pipeline rilis untuk cetak biru ini. Setiap pembaruan berikutnya pada cetak biru akan memicu pipeline rilis ini untuk memperbarui produk di Service Catalog dengan versi baru.

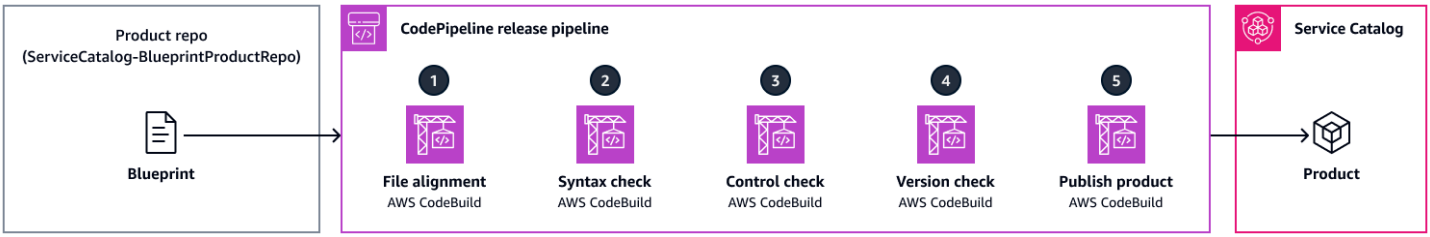
Saluran rilis mencakup kontrol proaktif yang mengotomatiskan pemeriksaan keamanan dan kepatuhan untuk cetak biru Anda. Kontrol proaktif dirancang untuk mencegah penciptaan sumber daya yang tidak sesuai. Kontrol ini dapat mengurangi jumlah peristiwa keamanan yang ditangani oleh jenis kontrol keamanan lainnya, seperti kontrol responsif dan detektif. Karena kontrol proaktif memastikan bahwa sumber daya yang diterapkan sesuai sebelum diterapkan, tidak ada peristiwa deteksi yang memerlukan respons atau remediasi.

Pertama kali Anda memanggil pipeline konfigurasi, itu membuat produk Service Catalog yang diberi nama`Bootstrapping-Admin-Product`. Produk ini adalah CloudFormation template untuk pipa rilis. Seperti yang ditunjukkan pada gambar berikut, pipeline konfigurasi menggunakan `Bootstrapping-Admin-Product` produk untuk membuat pipeline rilis khusus untuk setiap cetak biru baru. Ada one-to-one hubungan antara cetak biru dan pipa rilis.



Tahapan saluran pipa rilis

Gambar berikut menunjukkan tahapan default dalam pipeline rilis dan sumber daya yang berinteraksi dengan pipeline. Setiap tahap dalam pipa adalah sebuah CodeBuild proyek.



Berikut ini adalah tahapan dari pipa rilis:

1. Penyelarasan file — Tahap ini memverifikasi bahwa cetak biru adalah template atau CloudFormation konstruksi. AWS Cloud Development Kit (AWS CDK) Jika cetak biru adalah AWS CDK konstruksi, tahap ini mensintesis konstruksi menjadi templat. AWS CDK CloudFormation Proses ini mengotomatiskan dan menstandarisasi penerapan melalui. CloudFormation Jika ada kesalahan yang ditemukan, pipa gagal.
2. Pemeriksaan sintaks - Kesalahan sintaks adalah penyebab umum kesalahan CloudFormation penerapan. Pada tahap ini, AWS CloudFormation Linter (cfn-lint) memeriksa kesalahan sintaks dengan membandingkan template dengan spesifikasi sumber daya.AWS CloudFormation Ini juga melakukan pemeriksaan lain, seperti memeriksa nilai yang valid untuk properti sumber daya dan kepatuhan terhadap praktik terbaik. Jika ada kesalahan yang ditemukan, pipeline gagal, dan cfn-lint mengembalikan saran.
3. Pemeriksaan kontrol — Pada tahap ini, cfn_nag memeriksa potensi masalah keamanan dengan mencari pola. Misalnya, ia memeriksa grup keamanan dan kebijakan AWS Identity and Access Management (IAM) yang terlalu permisif, enkripsi yang hilang, dan literal kata sandi. Jika ada kesalahan yang ditemukan, pipeline gagal, dan cfn_nag mengembalikan saran.
4. Pemeriksaan versi — Saluran rilis melakukan kontrol versi berdasarkan strategi versi yang ditentukan dalam file konfigurasi produk. Jika versi produk didefinisikan sebagai tidak dapat diubah, Service Catalog menonaktifkan versi produk sebelumnya.
5. Publikasikan produk - Saluran rilis merilis produk di Service Catalog.

> **Note**
>
> Pipa rilis dapat disesuaikan. Misalnya, Anda dapat menghapus tahapan apa pun yang tidak berlaku untuk kasus penggunaan Anda. Anda juga dapat menambahkan lebih banyak tahapan jika Anda ingin menambahkan pemeriksaan kontrol lainnya, validasi tambahan, atau

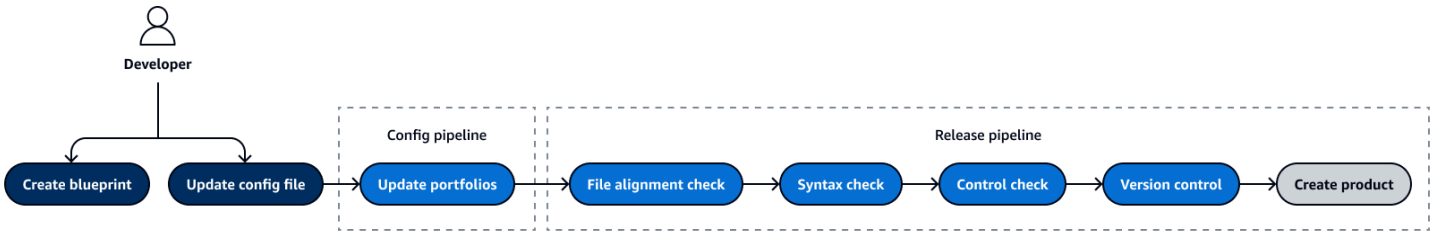
langkah persetujuan manual. Panduan ini tidak menyertakan instruksi untuk memodifikasi pipeline rilis. Untuk informasi lebih lanjut, lihat CodePipelinedan CodeBuilddokumentasi.

Siklus hidup cetak biru di Pabrik Cetak Biru Perusahaan

Siklus hidup cetak biru Enterprise Blueprint Factory terdiri dari tiga tahap khas: pembuatan, pembaruan, dan penghapusan. Tahap siklus hidup memengaruhi tindakan mana yang dilakukan oleh pipeline konfigurasi dan pipeline rilis.

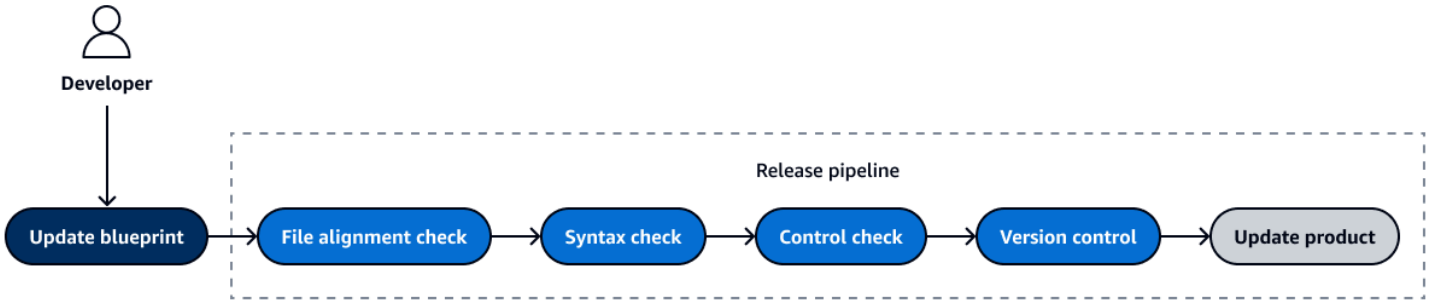
Pembuatan cetak biru

Untuk merilis cetak biru baru sebagai produk di AWS Service Catalog, pengembang menggabungkan cetak biru ke dalam repositori produk, memperbarui portofolio dalam file konfigurasi, dan menambahkan produk baru ke file konfigurasi. Ini memanggil pipa konfigurasi. Pipeline konfigurasi membuat pipeline rilis untuk produk. Dalam pipeline rilis, cetak biru mengalami beberapa pemeriksaan keamanan. Pipeline rilis kemudian menyebarkan cetak biru sebagai produk Service Catalog.

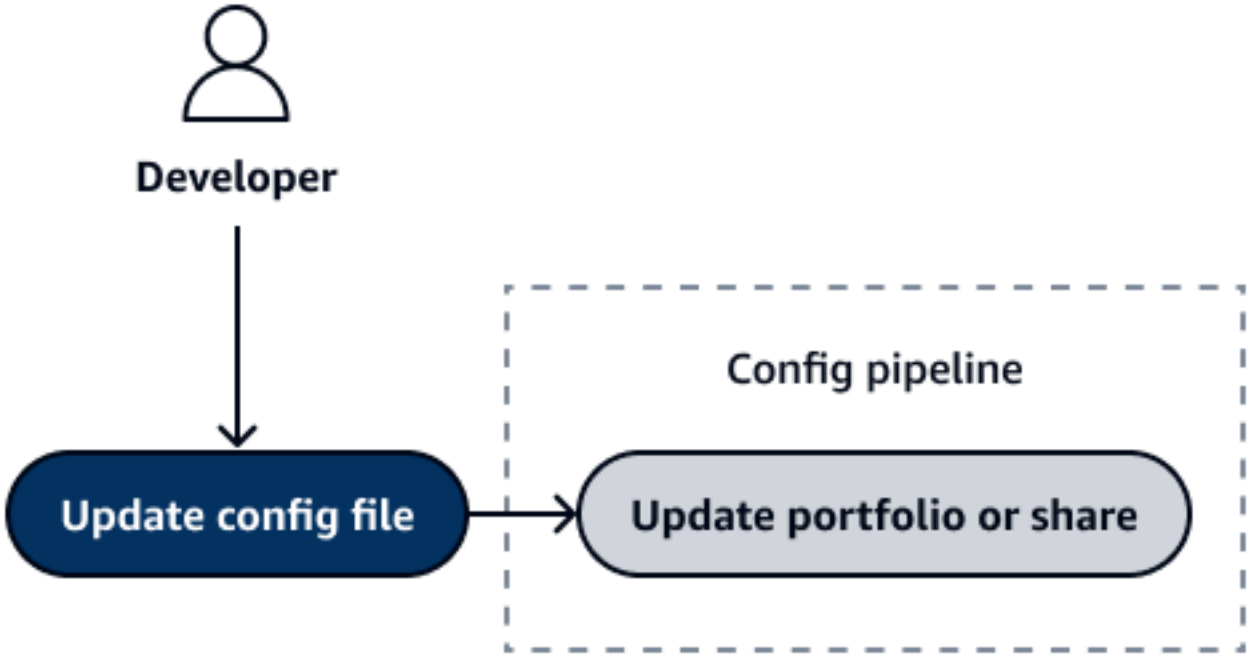


Pembaruan cetak biru

Pengembang dapat memperbarui produk di Service Catalog dengan menggabungkan versi terbaru dari cetak biru ke dalam repositori produk. Pembaruan ini memanggil pipeline rilis untuk produk. Template yang diperbarui menjalani pemeriksaan keamanan di pipeline rilis. Pipeline rilis menyebarkan versi baru dari produk Service Catalog. Untuk informasi selengkapnya tentang cara Service Catalog memperbarui versi produk, lihat Mengelola versi dalam dokumentasi Service Catalog.



Atau, Anda dapat memperbarui portofolio Service Catalog mana yang terkait dengan cetak biru atau Anda dapat mengubah konfigurasi berbagi untuk portofolio tersebut. Dalam hal ini, pengembang memperbarui file konfigurasi di repo konfigurasi. Pipeline konfigurasi memperbarui portofolio atau pembagian portofolio. Dalam hal ini, produk dalam Service Catalog tidak berubah, meskipun sekarang dapat dimasukkan dalam portofolio yang berbeda.



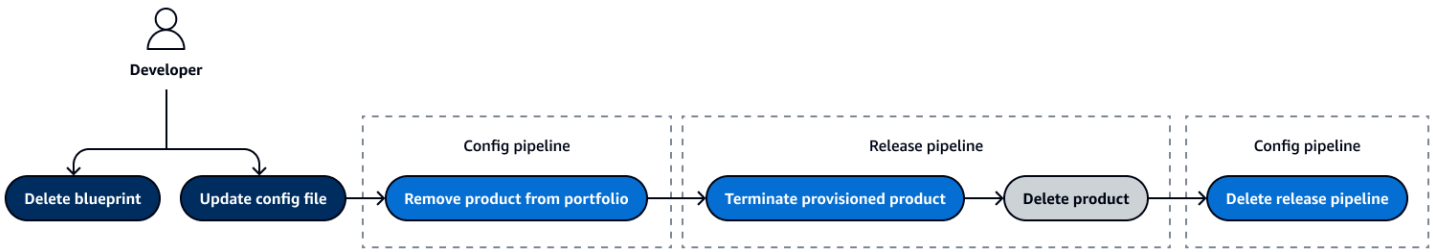
Penghapusan cetak biru

> **Important**
>
> Anda tidak dapat memulihkan produk Service Catalog setelah produk tersebut dihapus. Namun, Anda dapat menerapkan ulang cetak biru sebagai produk baru.

Saat Anda menghapus produk, Service Catalog menghapus semua versi produk dari setiap portofolio yang berisi produk. Untuk informasi selengkapnya, lihat Menghapus produk dalam dokumentasi Service Catalog.

Untuk menghapus cetak biru setelah diterapkan di Service Catalog, pengembang menghapus cetak biru di repo produk. Kemudian mereka menghapus produk dari file konfigurasi. Pipeline konfigurasi memisahkan produk dari portofolio yang mengandungnya dan menghapus semua asosiasi produk. Pipeline rilis mengakhiri produk Service Catalog dan produk yang disediakan. Kemudian, pipeline konfigurasi menghapus pipeline rilis produk.

Jika pipeline konfigurasi tidak dapat memisahkan semua sumber daya produk, maka produk tidak dihapus dan pipeline gagal. Anda harus menyelesaikan pemisahan sumber daya yang gagal dan kemudian memulai ulang pipa. Untuk informasi selengkapnya, lihat Menyelesaikan disasosiasi sumber daya yang gagal saat menghapus produk.



Menyiapkan Pabrik Cetak Biru Perusahaan

Bagian ini membantu Anda mengatur Pabrik Cetak Biru Perusahaan di lingkungan Anda. AWS Ini mencakup instruksi terperinci untuk menyiapkan repositori yang diperlukan dan AWS sumber daya untuk Pabrik Cetak Biru Perusahaan.

Prasyarat

Berikut ini adalah prasyarat untuk menyiapkan Pabrik Cetak Biru Perusahaan di lingkungan Anda: AWS

- Berikut ini Akun AWS:
  - Akun yang digunakan untuk mengelola Enterprise Blueprint Factory dan untuk merilis produk
  - Satu atau lebih akun yang mengkonsumsi produk yang dirilis
- Semua akun adalah:
  - Dikelola sebagai organisasi di AWS Organizations
  - Terletak di unit organisasi yang sama (OU)
  - Organisasi mengikuti account-per-tenant model
- AWS Command Line Interface (AWS CLI), diinstal dan dikonfigurasi
- Izin untuk menyebarkan AWS CloudFormation tumpukan yang membuat sumber daya berikut: AWS
  - Grup CloudWatch log Amazon Logs
  - AWS CodePipeline jaringan pipa
  - AWS CodeBuild proyek
  - Kebijakan dan aturan bus EventBridge acara Amazon
  - AWS Identity and Access Management (IAM) peran dan kebijakan
  - AWS Key Management Service (AWS KMS) kebijakan kunci dan kunci
  - AWS Service Catalog portofolio, produk, dan produk yang disediakan
  - Topik, kebijakan topik, dan langganan Amazon Simple Notification Service (Amazon SNS)
  - Ember Amazon Simple Storage Service (Amazon S3)
  - AWS Systems Manager Parameter Menyimpan parameter

Untuk informasi selengkapnya tentang menyiapkan izin ini, lihat CloudFormation dokumentasi dan Kebijakan implementasi untuk izin hak istimewa paling sedikit. AWS CloudFormation

- Sebuah GitHub akun

Praktik terbaik

Kami menyarankan Anda mengikuti praktik terbaik ini saat menyiapkan Pabrik Cetak Biru Perusahaan di lingkungan Anda: AWS

- Saat mengonfigurasi izin yang diperlukan untuk menyebarkan Pabrik Cetak Biru Perusahaan, ikuti prinsip hak istimewa paling sedikit dan berikan izin minimum yang diperlukan. Untuk informasi selengkapnya, lihat Berikan hak istimewa terkecil dan praktik terbaik Keamanan dalam dokumentasi IAM.
- Saat mengonfigurasi akses ke portofolio Service Catalog, ikuti prinsip hak istimewa paling sedikit dan berikan akses hanya ke peran, pengguna, atau administrator tertentu. Ikuti praktik terbaik keamanan untuk Service Catalog.

Membuat repositori

Bagian ini membantu Anda mengatur repositori konfigurasi dan repositori produk untuk Enterprise Blueprint Factory. Untuk mengatur repositori Anda, Anda melakukan fork pada repositori yang disediakan. GitHub Kemudian, Anda gunakan AWS CodeConnections untuk membuat koneksi ke GitHub repositori Anda. Kemudian, Anda mengkloning GitHub repositori ke mesin lokal Anda.

Untuk melakukan fork GitHub repositori

1. Masuk ke GitHub.
2. Arahkan ke GitHub repositori repo Konfigurasi.
3. Pilih garpu.
4. Pada halaman Buat garpu baru, di kotak nama Repositori, masukkan. `ServiceCatalog-ConfigRepo`
5. (Opsional) Masukkan deskripsi.
6. Pilih Salin cabang utama saja.
7. Pilih Buat garpu.

8. Ulangi langkah-langkah ini untuk melakukan fork pada GitHub repositori repo Kode. Masukkan nama `ServiceCatalog-CodeRepo` untuk repositori ini.
9. Ulangi langkah-langkah ini untuk melakukan fork pada GitHub repositori repo Produk. Masukkan nama `ServiceCatalog-BlueprintProductRepo` untuk repositori ini.

Untuk membuat CodeConnections koneksi

1. Di AWS CLI, masukkan perintah berikut untuk membuat CodeConnections koneksi ke: GitHub

```
aws codeconnections create-connection --provider-type GitHub --connection-name
 <MyConnection>
```

2. Gunakan konsol Alat AWS Pengembang untuk menyelesaikan koneksi. Untuk informasi selengkapnya, lihat Memperbarui sambungan yang tertunda.

Untuk mengkloning repositori bercabang

- Masukkan perintah berikut untuk mengkloning GitHub repositori ke workstation lokal Anda:

```
git clone git@github.com:<user>/aws-enterprise-blueprint-factory-config-repo
 ServiceCatalog-ConfigRepo
git clone git@github.com:<user>/aws-enterprise-blueprint-factory-blueprint-repo
 ServiceCatalog-BlueprintProductRepo
git clone git@github.com:<user>/aws-enterprise-blueprint-factory-code-repo
 ServiceCatalog-CodeRepo
```

Menyiapkan Pabrik Cetak Biru Perusahaan

Petunjuk di bagian ini menjelaskan cara menyiapkan Pabrik Cetak Biru Perusahaan di akun target Anda. Repo produk yang Anda kloning GitHub berisi dua contoh CloudFormation template, `BP-S3` dan. `BP-SNS` Dengan mengikuti petunjuk ini, Anda menerapkan dua contoh cetak biru ini sebagai produk di Service Catalog.

Untuk mengatur peran

1. Di akun Pengembang Blueprint, buat kebijakan kepercayaan berikut, lalu simpan sebagai: `sc-enduserrole-trust-policy.json`

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::123456789012:role/ServiceCatalogEndUserRole"
    },
    "Action": "sts:AssumeRole"
  }
}
```

2. Masukkan perintah berikut untuk membuat peran `ServiceCatalogEndUserRole` IAM:

```
aws iam create-role \
--role-name ServiceCatalogEndUserRole \
--assume-role-policy-document file://sc-enduserrole-trust-policy.json
aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AWSServiceCatalogEndUserFullAccess \
-- role-name ServiceCatalogEndUserRole
```

> **Note**
>
> Pengembang menggunakan `ServiceCatalogEndUserRole` peran tersebut untuk menyediakan produk Service Catalog. Peran ini tidak memerlukan izin untuk membuat sumber daya yang ditentukan dalam cetak biru. Ini mengikuti praktik terbaik dari izin yang paling tidak memiliki hak istimewa dan pemisahan tugas.

3. Buat kebijakan kepercayaan berikut dan kemudian simpan sebagai`sc-launchconstraintrole-trust-policy.json`:

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

```
}
```

4. Masukkan perintah berikut untuk membuat peran `ServiceCataloglogLaunchConstraintRole` IAM:

```
aws iam create-role \
--role-name ServiceCataloglogLaunchConstraintRole \
--assume-role-policy-document file://sc-launchconstraintrole-trust-policy.json
aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AmazonSNSFullAccess \
--role-name ServiceCataloglogLaunchConstraintRole
aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AWSCloudFormationFullAccess \
--role-name ServiceCataloglogLaunchConstraintRole
```

5. Tambahkan kebijakan berikut ke peran `ServiceCataloglogLaunchConstraintRole` IAM. Sertakan izin lain yang diperlukan untuk sumber daya produk, seperti yang dijelaskan dalam Mengonfigurasi Peran Peluncuran dalam dokumentasi Service Catalog:

```
{
          "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetObject"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "s3:ExistingObjectTag/servicecatalog:provisioning":"true"
            }
         }
   ]
}
```

> **Note**
>
> Service Catalog menggunakan peran ini untuk menyebarkan CloudFormation tumpukan sebagai produk di Service Catalog. Kebijakan kepercayaan untuk peran ini memastikan bahwa hanya Service Catalog yang dapat mengasumsikan peran tersebut. Pengguna

atau layanan lain tidak dapat mengambil peran ini. Ini mengikuti praktik terbaik pemisahan tugas.

6. Buat kebijakan kepercayaan berikut, lalu simpan sebagai`sc-codebuild-trust-policy.json`:

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

7. Masukkan perintah berikut untuk membuat peran `codebuild-servicecatalog-admin-role` IAM:

```
aws iam create-role \
--role-name codebuild-servicecatalog-admin-role \
--assume-role-policy-document file://sc-codebuild-trust-policy.json
aws iam attach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AWSCodeBuildAdminAccess \
--role-name codebuild-servicecatalog-admin-role
```

> **Note**
>
> CodeBuild Pekerjaan di pipeline konfigurasi menggunakan peran ini.

Untuk mengatur ember Amazon S3

- Untuk membuat bucket Amazon Simple Storage Service (Amazon S3) yang digunakan untuk menyimpan CodePipeline artefak, ikuti petunjuk dalam Membuat bucket di dokumentasi Amazon S3. Ikuti praktik terbaik Keamanan untuk Amazon S3.

Untuk mengatur AWS Systems Manager parameter

- Ikuti petunjuk dalam Membuat parameter Parameter Store di Systems Manager untuk membuat parameter Systems Manager dalam tabel berikut. Parameter ini digunakan dalam CloudFormation template yang menyebarkan pipeline konfigurasi.

Nama parameter	Tipe	Deskripsi
`/blueprints/resources/vpc_id`	String	Parameter yang menyimpan ID target virtual private cloud (VPC).
`/blueprints/resources/subnets`	StringList	Parameter yang IDs menyimpan subnet target.
`/blueprints/resources/securitygroups`	StringList	Parameter yang IDs menyimpan kelompok keamanan target.
`/blueprints/resources/artifacts-bucket-name`	String	Parameter yang menyimpan nama bucket Amazon S3 yang digunakan untuk CodePipeline artefak.
`/blueprints/resources/BlueprintRepo`	String	Parameter yang menyimpan GitHub repo tempat cetak biru Enterprise Blueprint Factory disimpan. Nilai default-nya adalah `<user>/aws-enterprise-blueprint-factory-blueprint-repo` .

Nama parameter	Tipe	Deskripsi
`/blueprints/resources/CodeRepo`	String	Parameter yang menyimpan GitHub repo tempat kode pipa konfigurasi Enterprise Blueprint Factory dan kode disimpan. `Bootstrapping-Admin-Product` Nilai default-nya adalah `<user>/aws-enterprise-blueprint-factory-code-repo` .
`/blueprints/resources/ConfigRepo`	String	Parameter yang menyimpan GitHub repo tempat file konfigurasi Enterprise Blueprint Factory disimpan. Nilai default-nya adalah `<user>/aws-enterprise-blueprint-factory-config-repo` .

Untuk memperbarui CloudFormation template

1. Di repositori kode (`ServiceCatalog-CodeRepo`), buka file ServiceCatalog-pipeline.yml.
2. Edit nilai default untuk parameter berikut dalam file ini:

   - `ConfigRepositoryName`adalah parameter Systems Manager yang menyimpan GitHub repo tempat file konfigurasi Enterprise Blueprint Factory disimpan. Nilai default-nya adalah `/blueprints/resources/ConfigRepo`.
   - `CodeRepositoryName`adalah parameter Systems Manager yang menyimpan GitHub repo tempat kode pipa konfigurasi Enterprise Blueprint Factory dan kode disimpan. `Bootstrapping-Admin-Product` Nilai default-nya adalah `/blueprints/resources/CodeRepo`.

- `BlueprintRepositoryName`adalah parameter Systems Manager yang menyimpan GitHub repo tempat cetak biru Enterprise Blueprint Factory disimpan. Nilai default-nya adalah `/blueprints/resources/BlueprintRepo`.
- `BranchName`adalah cabang dari repositori konfigurasi tempat file konfigurasi disimpan. Nilai default-nya adalah `main`.
- `VPCID`adalah parameter Systems Manager yang menyimpan ID dari VPC target. Nilai default-nya adalah `/blueprints/resources/vpc_id`.
- `Subnets`adalah parameter Systems Manager yang IDs menyimpan subnet target. Nilai default-nya adalah `/blueprints/resources/subnets`.
- `SecurityGroupIds`adalah parameter Systems Manager IDs yang menyimpan kelompok keamanan target. Nilai default-nya adalah `/blueprints/resources/securitygroups`.
- `IamRoleName`adalah nama peran IAM yang digunakan CodeBuild pekerjaan. Nilai defaultnya adalah`codebuild-servicecatalog-admin-role`.
- `EnvironmentType`adalah lingkungan tempat Anda menerapkan Pabrik Cetak Biru Perusahaan. Nilai default-nya adalah `DEV`.
- `ArtifactBucket`adalah parameter Systems Manager yang menyimpan bucket Amazon S3 tempat CodePipeline menyimpan artefak. Nilai defaultnya adalah`/blueprints/resources/artifacts-bucket-name`.
- `CodeConnectionArn`adalah Nama Sumber Daya Amazon (ARN) dari CodeConnections koneksi ke. GitHub

3. Simpan dan tutup file ServiceCatalog-Pipeline.yml.
4. Masukkan perintah berikut untuk menggabungkan perubahan ke dalam repositori kode:

```
cd ServiceCatalog-CodeRepo
git add ServiceCatalog-Pipeline.yml
git commit -m "<description of change>"
git push origin main
```

5. Di repositori konfigurasi (`ServiceCatalog-ConfigRepo`), buka file bp_config.yml.
6. Perbarui nilai di bagian portofolio sesuai kebutuhan untuk organisasi Anda. Misalnya, perbarui `share_to_ou` atribut `portfolio_access_roles` dan. Untuk informasi selengkapnya, lihat File konfigurasi dalam panduan ini.
7. Simpan dan tutup file bp_config.yml.
8. Masukkan perintah berikut untuk menggabungkan perubahan ke dalam repositori kode:

```
cd ServiceCatalog-ConfigRepo
git add bp_config.yml
git commit -m "<description of change>"
git push origin main
```

Untuk menyebarkan tumpukan CloudFormation

1. Masuk ke akun administratif Enterprise Blueprint Factory.
2. Beralih ke peran IAM yang memiliki izin administratif.
3. Buka konsol CloudFormation.
4. Pada bilah navigasi di bagian atas layar, pilih target Wilayah AWS.
5. Pada halaman Stacks, pilih Buat tumpukan di kanan atas, lalu pilih Dengan sumber daya baru (standar).
6. Untuk Siapkan templat, pilih Templat sudah siap.
7. Di bawah Tentukan templat, pilih Unggah file templat.
8. Pilih Pilih File, navigasikan ke `ServiceCatalog-CodeRepo` folder, lalu pilih ServiceCatalog-Pipeline.yl.
9. Pilih Berikutnya untuk melanjutkan dan memvalidasi template.
10. Untuk nama Stack, masukkan nama untuk tumpukan.
11. Di bagian Parameter, jangan ubah nilai default.
12. Pilih Berikutnya.
13. Pada halaman Configure stack options, jangan ubah nilai default, lalu pilih Next.
14. Pada halaman Tinjau dan buat, verifikasi detail templat dan tumpukan, lalu pilih Kirim.
15. Pantau kemajuan penerapan tumpukan. Lihat informasi yang lebih lengkap dalam dokumentasi CloudFormation.
16. Tunggu statusnya berubah`CREATE_COMPLETE`.

Untuk memvalidasi penerapan

1. Buka konsol AWS Service Catalog.
2. Di panel navigasi, pilih Produk.

3. Konfirmasikan bahwa ServiceCatalog-Pipeline tersedia dalam daftar produk.
4. Buka konsol AWS CodePipeline.
5. Di Nama, pilih pipeline konfigurasi. Secara default, nama pipeline adalah`ServiceCatalog-Pipeline`.
6. Pilih Lihat riwayat.
7. Lihat status pipa dan eksekusi panggung. Untuk informasi selengkapnya tentang status, lihat Melihat status eksekusi di CodePipeline dokumentasi.
8. Tunggu hingga status pipeline konfigurasi`Succeeded`.
9. Buka konsol Service Catalog.
10. Di panel navigasi, pilih Produk.
11. Konfirmasikan bahwa produk BP-S3 dan produk BP-SNS tersedia. Ini menunjukkan bahwa pipa pelepasan produk untuk cetak biru sampel berhasil diselesaikan.
12. Jika Anda ingin menghapus contoh cetak biru yang Anda gunakan saat menyiapkan Pabrik Cetak Biru Perusahaan, ikuti petunjuk di Menghapus cetak biru.

Hapus Pabrik Cetak Biru Perusahaan

Jika Anda tidak menggunakan Pabrik Cetak Biru Perusahaan, Anda dapat menghapusnya untuk menghentikan biaya yang terkait dengan sumber dayanya. AWS

Untuk menghapus sumber daya

1. Masukkan perintah berikut untuk menghapus peran IAM yang digunakan di akun administratif Enterprise Blueprint Factory:

```
aws iam detach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AWSServiceCatalogEndUserFullAccess \
--role-name ServiceCatalogEndUserRole
aws iam delete-role --role-name ServiceCatalogEndUserRole
aws iam detach-role-policy \
--policy-arn arn:aws:iam::aws:policy/AmazonSNSFullAccess \
--role-name ServiceCataloglogLaunchConstraintRole
aws iam delete-role --role-name ServiceCataloglogLaunchConstraintRole
```

2. Hapus CloudFormation tumpukan untuk Enterprise Blueprint Factory. Untuk petunjuk, lihat Menghapus tumpukan dari CloudFormation konsol atau Menghapus tumpukan dari AWS CLI.

3. Hapus bucket Amazon S3 yang digunakan untuk menyimpan artefak. CodePipeline Untuk petunjuknya, lihat Menghapus bucket di dokumentasi Amazon S3.
4. Hapus parameter Systems Manager berikut dari Parameter Store:

   - `/blueprints/resources/vpc_id`
   - `/blueprints/resources/subnets`
   - `/blueprints/resources/securitygroups`
   - `/blueprints/resources/artifacts-bucket-name`
   - `/blueprints/resources/BlueprintRepo`
   - `/blueprints/resources/CodeRepo`
   - `/blueprints/resources/ConfigRepo`

   Untuk petunjuk, lihat Menghapus parameter dari Parameter Store dalam dokumentasi Systems Manager.

Menggunakan Pabrik Cetak Biru Perusahaan

Bagian ini membantu Anda membuat, memperbarui, atau menghapus cetak biru di lingkungan Anda. Ini memberikan instruksi terperinci untuk mengelola cetak biru sepanjang siklus hidupnya.

Untuk membuat atau memperbarui cetak biru khusus, Anda harus memiliki pemahaman tentang cara membuat templat IAC, seperti AWS CloudFormation templat atau konstruksi. AWS Cloud Development Kit (AWS CDK) Panduan ini tidak menyertakan informasi atau instruksi tentang cara menentukan cetak biru yang Anda rilis melalui Pabrik Cetak Biru Perusahaan.

Prasyarat

Berikut ini adalah prasyarat untuk menggunakan Pabrik Cetak Biru Perusahaan di lingkungan Anda: AWS

- AWS Command Line Interface (AWS CLI), diinstal dan dikonfigurasi
- Izin untuk mengambil peran `ServiceCatalogEndUserRole` AWS Identity and Access Management (IAM)
- CloudFormation Template atau AWS CDK konstruksi

Membuat cetak biru

Pipeline Enterprise Blueprint Factory menyebarkan cetak biru yang Anda tentukan dalam file konfigurasi. Pengembang memulai pipeline konfigurasi dengan menggabungkan file konfigurasi ke dalam repositori konfigurasi. Kemudian, Enterprise Blueprint Factory menggunakan `ServiceCatalogLaunchConstraintRole` untuk menyebarkan cetak biru sebagai produk di Service Catalog. Untuk informasi selengkapnya tentang tindakan yang dilakukan pipeline konfigurasi dan pipeline rilis saat Anda membuat cetak biru, lihat Pembuatan cetak biru dalam panduan ini.

Untuk menambahkan cetak biru ke repositori produk

1. Pastikan Anda telah menyiapkan Pabrik Cetak Biru Perusahaan Anda sesuai dengan petunjuk dalam Menyiapkan Pabrik Cetak Biru Perusahaan dalam panduan ini.
2. Konfirmasikan bahwa kebijakan untuk `ServiceCataloglogLaunchConstraintRole` peran tersebut memungkinkan Anda menyediakan sumber daya yang ditentukan dalam cetak biru.

3. Di repositori produk (`ServiceCatalog-BlueprintProductRepo`), buat folder untuk cetak biru baru.
4. Tempelkan template IAC (CloudFormation template atau AWS CDK konstruksi) ke dalam folder yang Anda buat.
5. Buat file bernama product_config.json di folder yang Anda buat.
6. Buka file product_config.json, dan rekatkan yang berikut ini ke dalam file:

```
{
    "SchemaVersion": "1.0",
    "ProductVersionName": "1.0.1",
    "Deprecated_Versions" : [],
    "ProductVersionDescription": "<description>",
    "ProductType": "CLOUD_FORMATION_TEMPLATE",
    "Properties": {
        "TemplateFilePath": "./<folder name>/<file name>"
    }
}
```

Di mana:

- `<description>`adalah deskripsi singkat dari versi cetak biru
- `<folder name>`adalah nama folder yang Anda buat di repositori produk
- `<file name>`adalah nama template IAc

> **Note**
>
> Anda dapat memperbarui versi skema atau nama versi produk agar sesuai dengan kebijakan organisasi Anda.

7. Simpan dan tutup file product_config.json.
8. Masukkan perintah berikut untuk menggabungkan perubahan ke dalam repositori produk:

```
cd ServiceCatalog-BlueprintProductRepo
git add <folder name>/<file name> <folder name>\product_config.json
git commit -m "The first version of <file name> blueprint"
git push origin main
```

Untuk memperbarui file konfigurasi

1. Di repositori konfigurasi (`ServiceCatalog-ConfigRepo`), buka file config.yml.
2. Edit `portfolios` bagian dan `products` bagian sesuai kebutuhan untuk cetak biru baru. Untuk informasi selengkapnya, lihat File konfigurasi dalam panduan ini.
3. Simpan dan tutup file config.yml.
4. Masukkan perintah berikut untuk menggabungkan perubahan ke dalam repositori konfigurasi:

```
cd ServiceCatalog-ConfigRepo
git add config.yml
git commit -m "<description of change>"
git push origin main
```

   Persetujuan permintaan tarik ini memulai pipeline konfigurasi. Pipa konfigurasi membuat pipa rilis untuk produk.

Untuk meninjau log penerapan

1. Masuk ke akun administratif Enterprise Blueprint Factory.
2. Buka konsol AWS CodePipeline.
3. Di Name, pilih pipeline rilis untuk produk. Secara default, nama pipeline adalah`BluePrint_<Product-Name>-<CloudFormation-Stack-Name>`.
4. Pilih Lihat riwayat.
5. Lihat status pipa dan eksekusi panggung. Untuk informasi selengkapnya tentang status, lihat Melihat status eksekusi di CodePipeline dokumentasi.
6. Jika pipa gagal, tinjau penyebab kegagalan. Untuk petunjuk tentang cara mengonfigurasi pemantauan untuk saluran pipa Anda, lihat Memantau saluran pipa dalam dokumentasi. CodePipeline Jika pipeline rilis gagal karena pemeriksaan cfn-lint atau cfn_nag, perbaiki kesalahan dalam templat. Kirim permintaan tarik lain ke repo produk. Ini memulai ulang pipa rilis. Untuk informasi selengkapnya tentang memperbaiki kesalahan templat, lihat bagian Pemecahan Masalah dalam panduan ini.
7. Tunggu hingga status pipeline rilis`Succeeded`.

Untuk memvalidasi penerapan

1. Masuk ke akun konsumen di organisasi.
2. Asumsikan peran `ServiceCatalogEndUserRole` IAM.
3. Buka konsol Service Catalog.
4. Di panel navigasi, pilih Produk.
5. Konfirmasikan bahwa produk baru tersedia dalam daftar produk.

Memperbarui cetak biru

Untuk informasi selengkapnya tentang tindakan yang dilakukan pipeline konfigurasi dan pipeline rilis saat Anda membuat cetak biru, lihat Pembaruan cetak biru dalam panduan ini.

Untuk memperbarui cetak biru

1. Di repositori produk, navigasikan ke folder untuk produk.
2. Tempel template IAc yang diperbarui. Pastikan nama file sama dengan versi sebelumnya.
3. Buka file product_config.json.
4. Untuk`ProductVersionName`, perbarui nomor versi.
5. Jika Anda ingin mencegah versi produk sebelumnya diterapkan di masa mendatang, untuk`Deprecated_Versions`, masukkan nomor versi sebelumnya dalam daftar yang dipisahkan koma.
6. Masukkan perintah berikut untuk menggabungkan perubahan ke dalam repositori produk:

```
cd ServiceCatalog-BlueprintProductRepo
git add <folder name>/<file name> <folder name>\product_config.json
git commit -m "Version <number> of <file name> blueprint"
git push origin main
```

   Persetujuan permintaan tarik ini memulai jalur rilis untuk produk.

Untuk meninjau log penerapan

1. Masuk ke akun administratif Enterprise Blueprint Factory.
2. Buka konsol AWS CodePipeline.

3. Di Nama, pilih pipeline rilis. Secara default, nama pipeline adalah`BluePrint_<Product-Name>-<CloudFormation-Stack-Name>`.
4. Pilih Lihat riwayat.
5. Lihat status pipa dan eksekusi panggung. Untuk informasi selengkapnya tentang status, lihat Melihat status eksekusi di CodePipeline dokumentasi.
6. Jika pipa gagal, tinjau penyebab kegagalan. Untuk petunjuk tentang cara mengonfigurasi pemantauan untuk saluran pipa Anda, lihat Memantau saluran pipa dalam dokumentasi. CodePipeline Jika pipeline rilis gagal karena pemeriksaan cfn-lint atau cfn_nag, perbaiki kesalahan dalam templat. Kirim permintaan tarik lain ke repo produk. Ini memulai ulang pipa rilis. Untuk informasi selengkapnya tentang memperbaiki kesalahan templat, lihat bagian Pemecahan Masalah dalam panduan ini.
7. Tunggu hingga status pipeline rilis`Succeeded`.

Untuk memvalidasi pembaruan

1. Masuk ke akun konsumen di organisasi.
2. Asumsikan peran `ServiceCatalogEndUserRole` IAM.
3. Buka konsol Service Catalog.
4. Di panel navigasi, pilih Produk.
5. Konfirmasikan bahwa versi produk baru tersedia dalam daftar produk.

Menghapus cetak biru

Saat Anda menghapus produk, Service Catalog menghapus semua versi produk dari setiap portofolio yang berisi produk. Untuk informasi selengkapnya, lihat Menghapus produk dalam dokumentasi Service Catalog. Untuk informasi selengkapnya tentang tindakan yang dilakukan pipeline konfigurasi dan pipeline rilis saat Anda membuat cetak biru, lihat Penghapusan cetak biru dalam panduan ini.

Untuk menghapus cetak biru

1. Di repositori konfigurasi, buka file config.yml.
2. Edit bagian produk, hapus atau komentari produk yang ingin Anda hapus.
3. Simpan dan tutup file config.yml.
4. Masukkan perintah berikut untuk menggabungkan perubahan ke dalam repositori konfigurasi:

```
cd ServiceCatalog-ConfigRepo
git add config.yml
git commit -m "<description of change>"
git push origin main
```

Persetujuan permintaan tarik ini memulai pipeline konfigurasi. Pipa konfigurasi menghapus produk dan pipa pelepasannya.

5. Di repositori produk, hapus folder untuk produk, termasuk isinya.
6. Masukkan perintah berikut untuk menggabungkan perubahan ke dalam repositori produk:

```
cd ServiceCatalog-BlueprintProductRepo
git add .
git commit -m "Delete <file name> blueprint"
git push origin main
```

Untuk memvalidasi penghapusan

1. Masuk ke akun konsumen di organisasi.
2. Asumsikan peran `ServiceCatalogEndUserRole` IAM.
3. Buka konsol Service Catalog.
4. Di panel navigasi, pilih Produk.
5. Konfirmasikan bahwa produk yang dihapus tidak lagi tersedia.

Pemecahan Masalah

Saat Anda membuat atau memperbarui cetak biru, alat cfn-lint dan cfn-nag memvalidasi cetak biru. Untuk informasi selengkapnya tentang validasi di pipeline rilis, lihat Rilis pipeline dalam panduan ini. Sintaks atau kesalahan keamanan yang dilaporkan menyebabkan pipeline gagal. Agar berhasil menyebarkan cetak biru melalui pipeline rilis, Anda harus memperbaiki kesalahan dalam cetak biru.

Berikut ini adalah contoh output yang menunjukkan dua kesalahan terkait keamanan, kegagalan dan peringatan.

```
BP-SNS.yml
------------------------------------------------------
```

```
BP-SNS.yml
------------------------------------------------------
| WARN W47
|
| Resource: ["ExampleTopic"]
| Line numbers: [5]
|
| SNS Topic should specify KmsMasterKeyId property
------------------------------------------------------
| FAIL F18
|
| Resource: ["ExampleTopicPolicy"]
| Line numbers: [10]
|
| SNS topic policy should not allow * principal

Failures count: 1
Warnings count: 1
```

Untuk memperbaiki kesalahan ini, dalam file cetak biru, Anda akan mengganti * prinsipal dalam kebijakan topik Amazon Simple Notification Service (Amazon SNS) dan mengaitkan kunci () AWS Key Management Service dengan AWS KMS topik. Contoh kode berikut menunjukkan pembaruan ini.

```
ExampleTopic:
    Type: AWS::SNS::Topic
    Properties:
      TopicName: ExampleTopic
  ExampleTopicPolicy:
    Type: AWS::SNS::TopicPolicy
    Properties:
      KmsMasterKeyId: alias/aws/sns  # Added KMS key
      PolicyDocument:
        Id: Id1
        Version: '2012-10-17'
        Statement:
        - Sid: Sid2
          Effect: Allow
          Principal:
            "Service" : "s3.amazonaws.com"  # Replaced "AWS": '*'
          Action: 'sns:Publish'
          Resource: !Ref ExampleTopic
```

```
      Topics:
        - !Ref ExampleTopic
```

Sumber daya terkait

AWS dokumentasi

- Tutorial: Buat pipeline yang disebarkan ke Service Catalog (AWS CodePipeline dokumentasi)
- AWS CodePipeline dokumentasi
- AWS CodeBuild dokumentasi
- AWS Service Catalog Panduan Administrator
- AWS Service Catalog Panduan Pengguna

AWS posting blog

- Laporkan dan Visualisasikan AWS Service Catalog Estate Anda (posting AWS blog)
- Menerapkan alarm untuk secara otomatis mendeteksi penyimpangan di AWS CloudFormation tumpukan (AWS posting blog)

Kontributor

Individu berikut berkontribusi pada panduan ini.

Mengotorisasi

- Haofei Feng, Arsitek Awan Senior, AWS
- Cam Maxwell, Penasihat Keamanan Utama, AWS
- Joe Guo, Insinyur Dukungan Cloud, AWS
- Shreejesh MV, Arsitek Awan Senior, AWS

Meninjau

- Joseph Dominic, Arsitek Awan, AWS
- Naresh Rajaram, Arsitek Solusi Mitra Konsultan, AWS

Penulisan teknis

- Lilly AbouHarb, Penulis Teknis Senior, AWS

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
Publikasi awal	—	Oktober 10, 2024

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 memproses atau memodifikasi data, seperti menganonimkan, menyunting, atau membuat nama samaran.

Zona Ketersediaan

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 break-glass 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

Dengan 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 atau kelas penyimpanan 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 Region, 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 is commonly described as a pipeline. CI/CDdapat 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 yang ada. 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 pipa CI/CD, 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 of Things (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?

interpretabilitas

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. Akun dapat menjadi anggota dari hanya satu organisasi pada suatu 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 dengan 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 yang dihosting 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). Tipe 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 merujuk 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.

SCADA

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 uptime 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 Tanda dapat membantu Anda mengelola, mengidentifikasi, mengatur, dan memfilter sumber daya. Untuk informasi selengkapnya, lihat Menandai AWS sumber daya Anda.

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.