Migrasi server lokal ke AWS melalui jaringan pribadi dengan menggunakan AWS Application Migration Service

AWS Bimbingan Preskriptif

AWS Bimbingan Preskriptif: Migrasi server lokal ke AWS melalui jaringan pribadi dengan menggunakan AWS Application Migration Service

Table of Contents

Memigrasi server lokal keAWS melalui jaringan pribadi dengan menggunakanAWS Application Migration Service

Mike Kuznetsov dan Dipin Jain, Amazon Web Services (AWS)

Maret 2023 (riwayat dokumen)

Banyak perusahaan bermigrasiAWS ke lingkungan jaringan terisolasi atau semi-terisolasi seperti pusat data lokal atau infrastruktur cloud atau hibrida lainnya. Jaringan terisolasi semacam itu biasanya tidak mengizinkan lalu lintas keluar ke titik akhir eksternal, yang diperlukan untuk migrasi melalui jaringan. Perusahaan lain memang mengizinkan lalu lintas jalan keluar HTTPS dari jaringan internal mereka tetapi tidak mengizinkan komunikasi spesifik pada port jaringan yang diperlukan oleh AWS Application Migration Service, yang merupakan utamaLayanan AWS untuk lift-and-shift migrasi besar. Dalam skenario ketiga, lalu lintas HTTPS diizinkan dari area sumber dan pementasan, tetapi lalu lintas replikasi data diperlukan untuk melewati saluran pribadi karena alasan kepatuhan.

Layanan Migrasi Aplikasi mendukung kasus penggunaan ini dan memungkinkan Anda untuk bermigrasi dari lingkungan terisolasi yang aman dengan hanya menggunakan konektivitas jaringan pribadi/publik pribadi atau hibrida. Panduan ini menjelaskan ketiga skenario ini, mulai dari dua model publik/pribadi hibrida hingga yang sepenuhnya terisolasi, dan berfokus pada langkah-langkah terperinci dan persyaratan infrastruktur untuk opsi khusus pribadi yang paling ketat. Ini dibangun di atas pola PanduanAWS Preskriptif Connect ke data Layanan Migrasi Aplikasi dan bidang kontrol melalui jaringan pribadi dengan menyediakan:

- Detail tambahan tentang konektivitas yang diperlukan di setiap skenario
- PenjelasanAWS sumber daya yang harus dibuat
- Opsi otomatisasi untuk membangun infrastruktur pengujianAWS dan menerapkan infrastruktur selama fase migrasi
- Opsi untuk pemantauan dan pemecahan masalah konektivitas untuk setiap kasus penggunaan

Untuk informasi selengkapnya tentang cara kerja, lihat posting blog berikut:

- Percepat Migrasi Anda denganAWS Application Migration Service
- Cara Menggunakan BaruAWS Application Migration Service untuk Migrasi Angkat-dan-Shift

Skenario

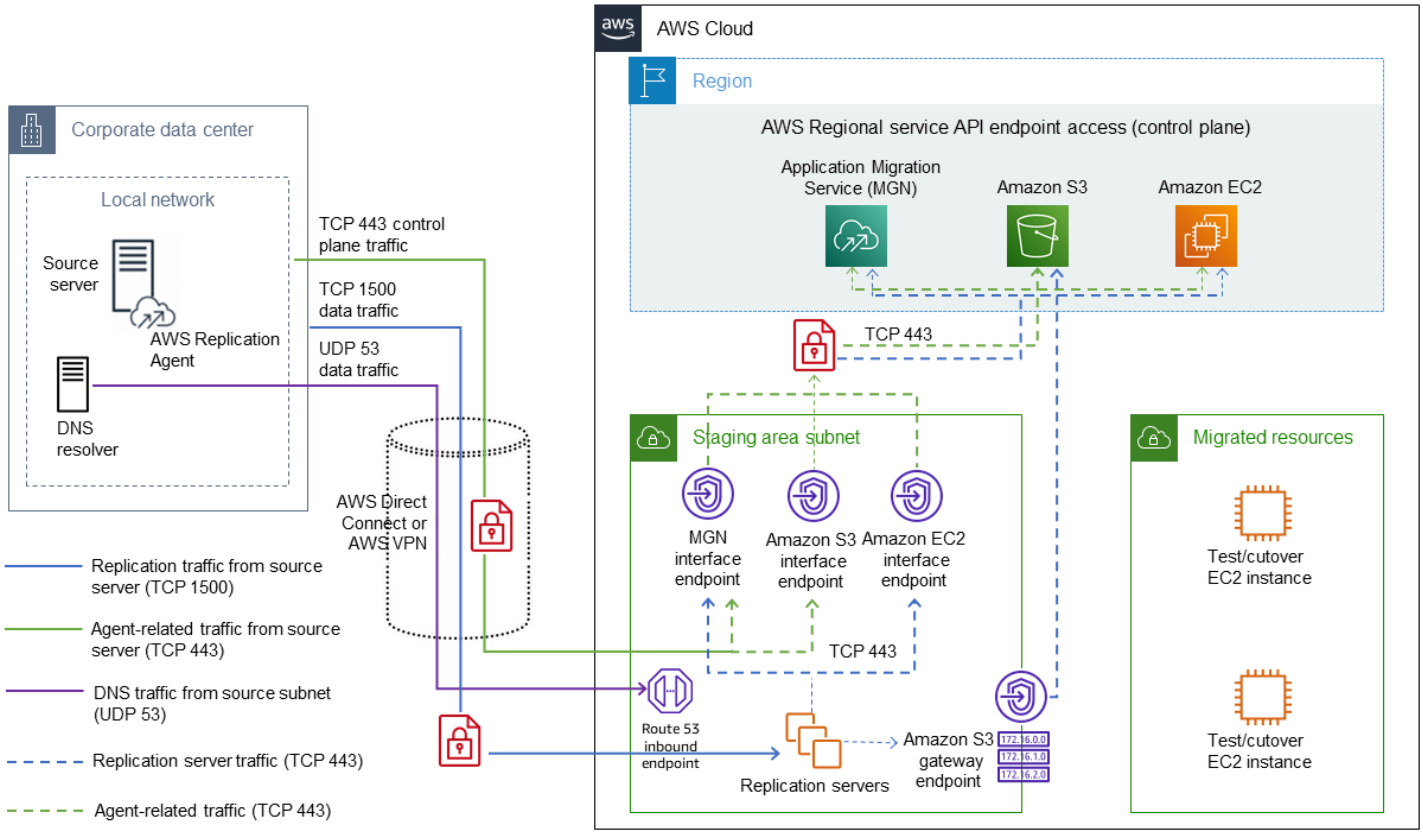
Panduan ini mencakup komponen infrastruktur yang diperlukan untuk dibuat untuk menyelesaikan migrasi untuk skenario berikut:

- Replikasi melalui jaringan pribadi saja, yang merupakan skenario yang paling umum dan membatasi.
- Skenario hibrida di mana komunikasi jalan keluar HTTPS diizinkan tetapi semua lalu lintas lainnya dibatasi. Skenario ini terdiri dari dua opsi:
  - Jalan keluar HTTPS publik di sumber dan sumber daya area pementasan pribadi
  - Jalan keluar HTTPS publik di sumber dan sumber daya area pementasan publik

Untuk setiap skenario, panduan ini menyediakan contoh konfigurasi dan daftar lengkapAWS komponen yang diperlukan.

Replikasi melalui jaringan pribadi saja

Diagram berikut menampilkan arsitektur skenario yang paling ketat, di mana semua lalu lintas melewati saluran pribadi (AWS VPNatauAWS Direct Connect) antara lingkungan sumber danAWS.



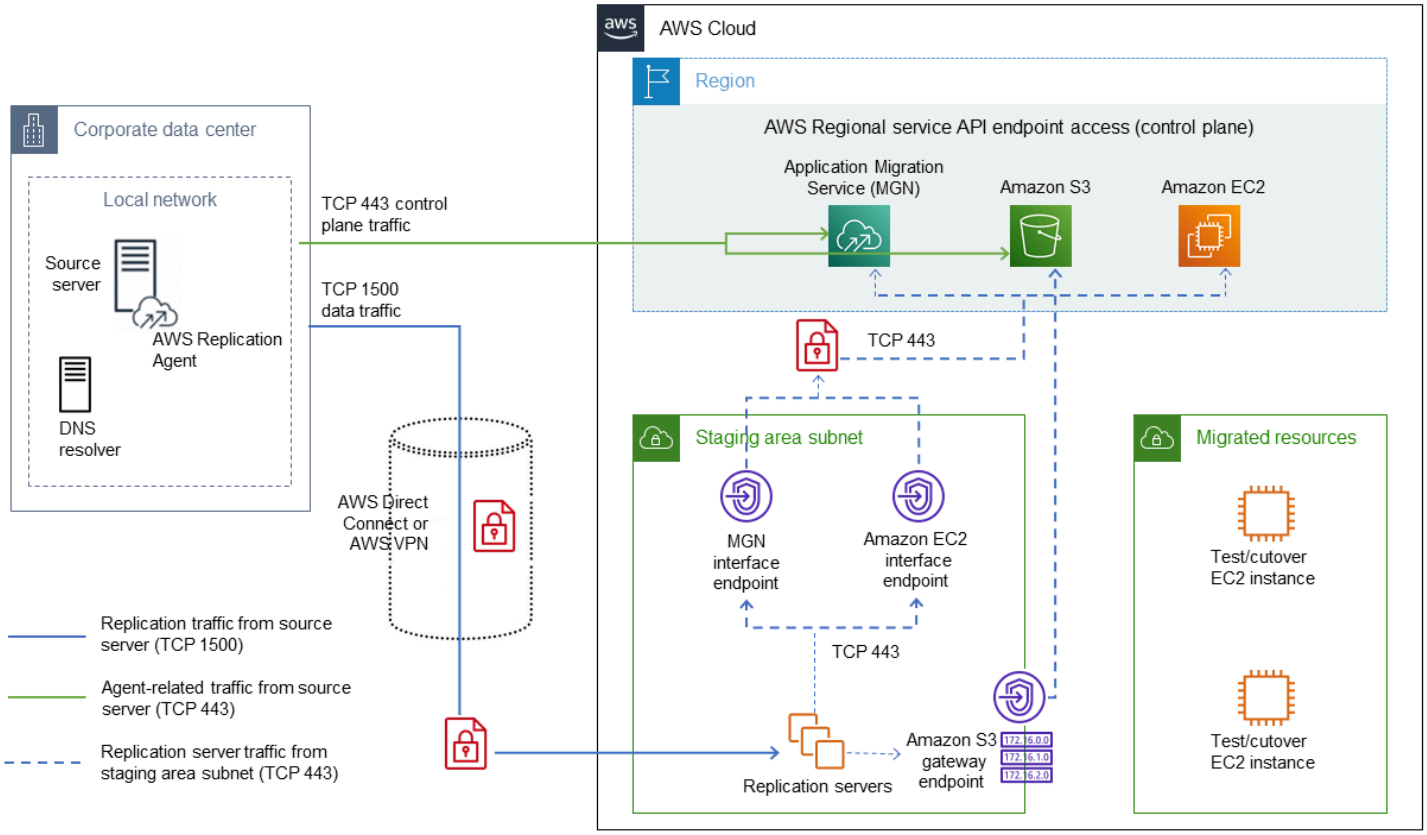
Komponen utama dari arsitektur ini adalah:

- Lingkungan sumber di pusat data perusahaan (di sebelah kiri). Ini adalah lingkungan untuk bermigrasi dari.
- Lingkungan pementasanAWS dengan cloud pribadi virtual pribadi (VPC) dan subnet (di tengah). Ini adalah lingkungan yang akan digunakan Layanan Migrasi Aplikasi untuk membuat sumber daya terkait replikasi. Sumber daya ini mungkin mencakup server replikasi, server konversi, dan volume Elastic Block Store (Amazon EBS) yang terkait dan snapshot Amazon Simple Storage Service (Amazon S3).
- Koneksi VPN dari lingkungan sumber ke pementasan VPC dan subnet (s) untuk menangani tiga jenis lalu lintas:
  - HTTPS/TCP port 443 untuk komunikasi API
  - Port TCP 1500 untuk transfer data
  - Lalu lintas Sistem Nama Domain (DNS) melalui port UDP 53

- Target lingkungan diAWS (di sebelah kanan). Ini bisa menjadi VPC yang sepenuhnya terisolasi atau subnet di lingkungan pementasan. (Catatan: Tidak ada persyaratan konektivitas jaringan dari subnet lingkungan pementasan ke subnet target.)
- Titik akhir antarmuka Amazon VPC untuk Layanan Migrasi Aplikasi, Amazon Elastic Compute Cloud (Amazon EC2), dan Amazon S3 yang dibuat di lingkungan pementasan, dan titik akhir gateway Amazon S3 VPC yang dapat diakses dari subnet pementasan.
- Dan akhirnya, DNS resolver inbound endpoint di subnet pementasan. Ini diperlukan untuk sistem sumber untuk menyelesaikan nama domain yang memenuhi syarat (FQDNs) dari titik akhir VPC ke IP pribadi.

Jalan keluar HTTPS publik di sumber dan sumber daya area pementasan pribadi

Diagram berikut menggambarkan arsitektur dalam skenario hibrida di mana lalu lintas jalan keluar HTTPS diizinkan dari server sumber mana pun dan digunakan untuk berkomunikasi dengan Application Migration Service dan titik akhir Amazon S3, sedangkan data replikasi pada port TCP 1500 melewati saluran pribadi (AWS VPNatauAWS Direct Connect) antara lingkungan sumber danAWS.

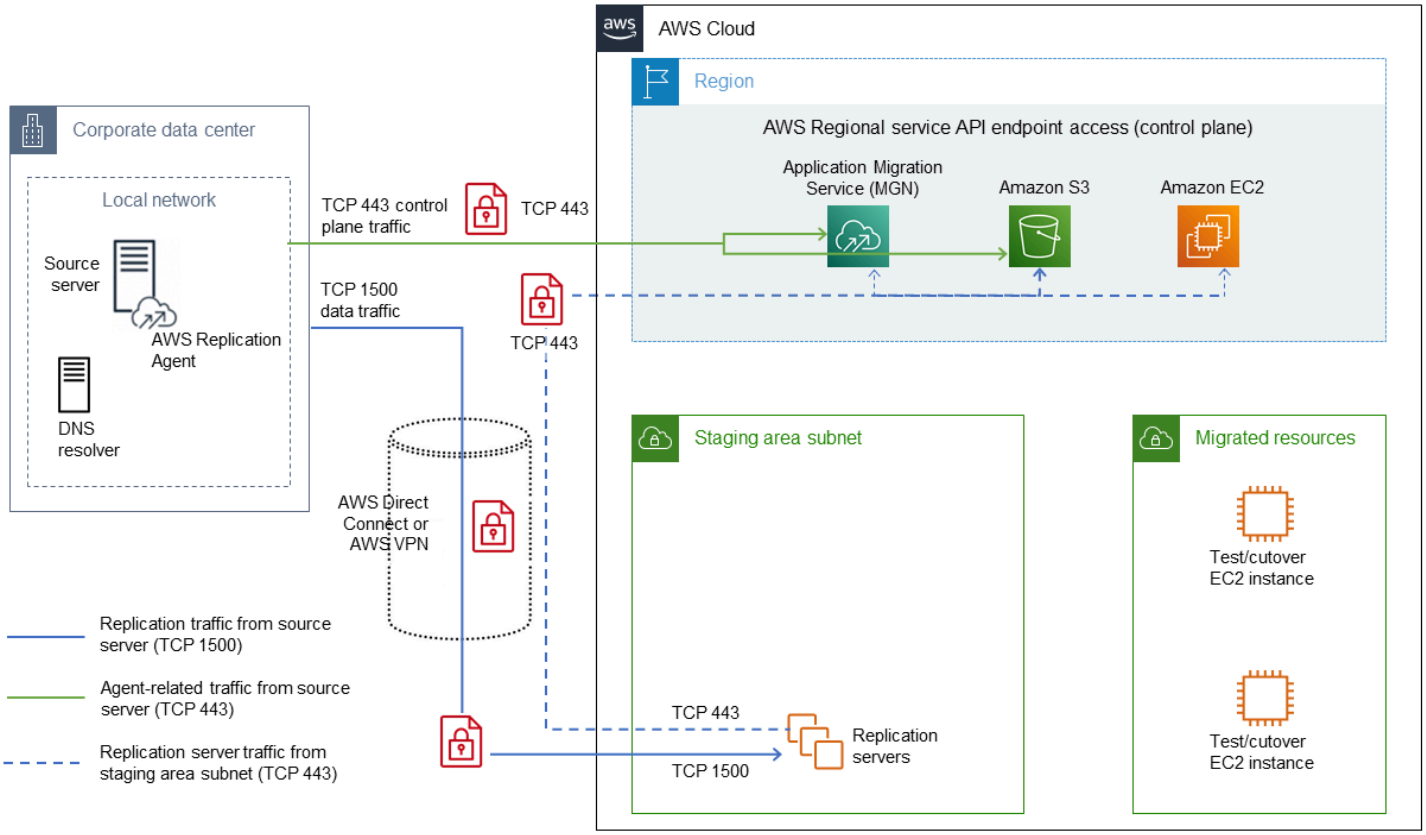


Arsitektur ini menyederhanakan persyaratan untuk subnet area pementasan, karena komunikasi HTTPS dari agen tidak melakukan perjalanan melalui saluran pribadi. Selain itu, tidak perlu membuat endpoint VPC antarmuka Amazon S3 tambahan atau titik akhir resolver masuk Amazon Route 53 untuk lalu lintas DNS, karena server sumber akan menggunakan server DNS tradisional mereka untuk menyelesaikan nama DNS publik standar Layanan Migrasi Aplikasi dan titik akhir Amazon S3.

Namun, dalam skenario ini, sumber daya subnet area pementasan masih berjalan pada jaringan pribadi dan sepenuhnya terisolasi dan tidak memiliki akses publik ke endpoint HTTPS apa pun, sehingga mereka perlu membuat endpoint antarmuka Application Migration Service dan Amazon EC2 serta endpoint gateway Amazon S3.

Jalan keluar HTTPS publik di sumber dan sumber daya area pementasan publik

Dalam kasus di mana sumber daya area pementasan tidak diperlukan untuk berada di subnet sepenuhnya terisolasi, Anda dapat menggunakan alternatif hibrida yang ditunjukkan dalam diagram berikut.



Dalam skenario ini, hanya lalu lintas replikasi data pada port TCP 1500 yang melewati saluran pribadi. Sisa komunikasi, baik dari subnet sumber dan subnet pementasan, terjadi melalui jaringan publik, hingga titik akhir HTTPS publik standar.

Komponen arsitektur dan persyaratan untuk replikasi terbatas

Bagian ini memberikan penjelasan rinci tentang skenario yang paling ketat, di mana semua komunikasi terjadi melalui saluran pribadi saja, dan mencakup penjelasan rinci tentang persyaratan dan komponen yang sesuai yang akan dibangun untuk setiap area.

Penahapan subnet

Subnet pementasan adalah bagian terpenting dari infrastruktur replikasi. Di sinilah semua server replikasi Layanan Migrasi Aplikasi akan diluncurkan, dan berisi alamat IP lalu lintas replikasi akan diarahkan ke. Untuk replikasi data pribadi masuk, konfigurasikan pengaturan server replikasi untuk Layanan Migrasi Aplikasi dengan opsi Gunakan IP pribadi.

Untuk persyaratan keluar, Anda dapat menggunakan opsi Buat IP publik untuk memilih apakah server replikasi akan berkomunikasi denganAWS layanan yang diperlukan (Amazon S3, Application Migration Service, Amazon EC2) melalui IP pribadi atau publik. Opsi standar untuk menyediakan konektivitas internet keluar tercantum dalam dokumentasi Layanan Migrasi Aplikasi: baik alamat IP publik dengan gateway internet atau alamat IP pribadi dengan gateway NAT. Kedua opsi memungkinkan Anda untuk menerapkan skenario hibrida yang disederhanakan di mana lalu lintas replikasi data melewati koneksi pribadi (AWS VPNatauAWS Direct Connect) sementara server replikasi berkomunikasi denganAWS layanan melalui jaringan publik.

Namun, memiliki konektivitas outbound publik biasanya dilarang di lingkungan perusahaan tertutup, dan ini adalah skenario paling ketat yang dibahas di bagian berikutnya. Dalam hal ini, Anda menggunakanAWS PrivateLink dan mengkonfigurasi endpoint VPC berikut dalam subnet pementasan untuk server replikasi:

- Titik akhir gateway VPC untuk berkomunikasi dengan Amazon S3
- Titik akhir antarmuka VPC untuk berkomunikasi dengan Layanan Migrasi Aplikasi dan Amazon EC2

Untuk mempelajari selengkapnya tentang titik akhir VPC, lihat AWS PrivateLinkdokumentasi.

Subnet sumber

Subnet sumber adalah subnet apa pun yang Anda replikasi. Di sinilah server sumber Anda berada dan di mana Anda akan menginstal AgenAWS Replikasi di server ini. Persyaratan jaringan untuk Agen meliputi:

- Berkomunikasi melalui HTTPS/TCP port 443 denganLayanan AWS Amazon S3 dan Application Migration Service
- Berkomunikasi dengan alamat IP server replikasi (pribadi atau publik, berdasarkan pengaturannya)

Agen juga mendukung skenario hybrid di mana komunikasi denganLayanan AWS dapat terjadi melalui jaringan publik (menggunakan lalu lintas HTTPS standar) sementara data replikasi dikirim melalui jaringan pribadi ke IP pribadi dari server replikasi.

Panduan ini berfokus pada skenario yang lebih ketat di mana bahkan lalu lintas HTTPS keLayanan AWS tidak diizinkan dari sistem sumber, jadi titik akhir berikut dikonfigurasi dalam subnet pementasan:

- Titik akhir antarmuka VPC untuk Layanan Migrasi Aplikasi dan Amazon S3 (titik akhir antarmuka regional, bukan titik akhir gateway yang diperlukan untuk server replikasi)
- Endpoint resolver DNS masuk, untuk memungkinkan sumber lokal dan server DNS menyelesaikan alamat IP pribadi untuk titik akhir VPC, yang terletak di subnet pementasan

Subnet target

Subnet target adalah subnet apa pun yang Anda rencanakan untuk meluncurkan server Anda, termasuk instance uji dan langsung. Subnet ini tidak memiliki persyaratan konektivitas jaringan sama sekali, dan dapat ditemukan di VPC lain di Wilayah yang samaAkun AWS dan. Ini karena Application Migration Service menggunakan API Amazon EC2 untuk membuat instans pengujian atau langsung baru (itulah sebabnya server replikasi dalam subnet pementasan memerlukan konektivitas HTTPS keluar ke Amazon EC2), dan mengakses snapshot S3 Regional yang dibuat dari volume EBS yang direplikasi. Tak satu pun dari operasi ini memerlukan akses jaringan langsung ke atau dari subnet target, jadi ini bahkan bisa menjadi subnet pribadi yang sepenuhnya terisolasi.

Namun, Layanan Migrasi Aplikasi juga secara otomatis menginstal beberapa alat seperti EC2Config atauAWS Systems Manager Agen (Agen SSM) pada instans target, dan aktivitas ini memerlukan konektivitas HTTPS/TCP port 443 keluar dari instance target dan subnet.

Praktik terbaik konfigurasi

Bagian ini memberikan penjelasan rinci tentang skenario yang paling ketat, di mana semua komunikasi terjadi melalui saluran pribadi saja, dan mencakup penjelasan rinci tentang persyaratan dan komponen yang sesuai yang akan dibangun untuk setiap area.

Bagian ini menjelaskan konfigurasi untuk skenario yang paling ketat (replikasi hanya melalui jaringan pribadi), seperti yang ditunjukkan pada diagram pertama, berdasarkan pertimbangan yang dibahas sebelumnya. Anda dapat mengonfigurasi kedua skenario hibrida dengan melewatkan bagian dari konfigurasi yang paling ketat:

- Untuk skenario hybrid yang mendukung jalan keluar HTTPS publik di sumber daya area pementasan sumber dan pribadi, titik akhir VPC antarmuka Amazon S3 tidak diperlukan.
- Untuk skenario hybrid yang mendukung jalan keluar HTTPS publik di sumber daya area pementasan sumber dan publik, tidak diperlukan titik akhir VPC di subnet area pementasan.

Bagian berikut mengasumsikan bahwa konfigurasi Layanan Migrasi Aplikasi awal sudah selesai, seperti yang dijelaskan dalam posting blog Mempercepat Migrasi Anda denganAWS Application Migration Service dan Cara Menggunakan BaruAWS Application Migration Service untuk Migrasi Angkat-dan-Shift). Diskusi ini berfokus pada komponen yang spesifik untuk skenario restriktif, dan mengasumsikan subnet pementasan pribadi yang tidak memiliki konektivitas ke internet.

Konfigurasi subnet dan perutean

Untuk skenario yang membatasi, Anda mengonfigurasiAWS sumber daya yang diperlukan di subnet pribadi VPC pementasan. Subnet ini tidak memiliki konektivitas ke internet (tidak ada gateway internet yang melekat pada tabel routing sebagai rute default). Sebaliknya, ia menggunakan gateway virtual yang terkait dengan AWS Site-to-Site VPNgateway (terhubung melalui terowongan IPsec ke gateway lokal), atau terhubung ke gateway transfer atau keAWS Direct Connect layanan untuk menyediakan interkonektivitas pribadi ke pusat data lokal.

Anda akan menggunakan subnet pribadi itu sebagai subnet pementasan untuk sumber daya terkait replikasi yang dikelola oleh Layanan Migrasi Aplikasi, dan Anda akan mengonfigurasi semua akses jaringan yang diperlukan melalui subnet ini dengan menggunakan titik akhir VPC, seperti yang dibahas di bagian berikutnya.

Konfigurasi endpoint VPC

Anda sekarang perlu membuat titik akhir VPC di subnet pementasan untuk menyediakan konektivitas untuk server replikasi dan Agen Layanan Migrasi Aplikasi dari subnet lokal.

Berikut daftar lengkap endpoint VPC yang Anda butuhkan:

- Layanan Migrasi Aplikasi dan titik akhir antarmuka Amazon EC2, yang menyediakan antarmuka jaringan elastis mereka sendiri dengan alamat IP pribadi dan nama DNS pribadi untuk digunakan oleh server replikasi dan Agen. (Agen hanya akan menggunakan endpoint Layanan Migrasi Aplikasi.)
- Titik akhir gateway Amazon S3 yang menyediakan rute tertentu dalam tabel rute subnet (meskipun daftar awalan). Ini akan digunakan oleh server replikasi.
- Titik akhir antarmuka Amazon S3 yang menyediakan elastic network interface tertentu dengan alamat IP pribadi khusus di subnet pribadi. Agen Layanan Migrasi Aplikasi akan menggunakan alamat ini melalui nama DNS tertentu.

Bagian selanjutnya membahas lebih detail tentang cara kerja endpoint VPC. Tabel berikut mencantumkan semua endpoint yang dibuat untuk subnet privat pementasan. (Perhatikan bahwa titik akhir gateway Amazon S3 tidak memiliki antarmuka jaringan yang disediakan tetapi memiliki daftar awalan khusus yang disediakan ke dalam tabel rute subnet, seperti yang akan dijelaskan nanti dalam panduan ini.)

Layanan AWS	VPC endpoint type	Private DNS	Related subnet
Amazon EC2	Antarmuka	Enabled	Reservasi privat pementasan
Layanan Migrasi Aplikasi	Antarmuka	Enabled	Reservasi privat pementasan
Amazon S3	Antarmuka	Tidak tersedia	Reservasi privat pementasan
Amazon S3	Gateway	Tidak tersedia	Connect ke tabel rute subnet pribadi pementasan

Anda dapat membuat endpoint VPC opsional untuk mengaktifkan akses ke instans EC2 pada subnet terisolasi pribadi melaluiAWS Systems Manager, seperti yang dibahas dalam Membuat endpoint VPC dalam dokumentasi Systems Manager.

Layanan AWS	VPC endpoint type	Private DNS	Related subnet
Systems Manager	Antarmuka	Enabled	Reservasi privat pementasan
ssmmessages	Antarmuka	Enabled	Reservasi privat pementasan
ec2messages	Antarmuka	Enabled	Reservasi privat pementasan
AWS Key Management Service (AWS KMS)	Antarmuka	Enabled	Reservasi privat pementasan
Log	Antarmuka	Enabled	Reservasi privat pementasan

VPC endpoint antarmuka

Membuat endpoint antarmuka juga menciptakan elastic network interface khusus untuk setiap subnet yang disediakan oleh endpoint antarmuka yang diberikan. Misalnya, endpoint antarmuka Layanan Migrasi Aplikasi disediakan dalam subnet pribadi di VPC pementasan dengan elastic network interface yang dikaitkan dengan alamat IP di dalam subnet itu, dan juga memiliki tiga nama DNS yang dapat diselesaikan dari subnet ke alamat IP ini:

- Nama DNS pribadi,`mgn.<region>.amazonaws.com`
- Dua nama DNS yang didasarkan pada ID titik akhir (`vpce-xxx`), dengan dan tanpa Region termasuk dalam nama:`vpce-xxx-<region>.<service-name>` dan`vpce-xxx.<service-name>`

Hal ini memungkinkan setiap contoh berjalan di subnet yang menggunakan default Dynamic Host Configuration Protocol (DHCP) pilihan set konfigurasi di VPC, dan memiliki kedua DNS atributenableDnsHostnames danenableDnsSupport diaktifkan, untuk:

- Selesaikan nama DNS dari Application Migration Service (mgn.<region>.amazonaws.com) ke alamat IP pribadi yang ditetapkan ke elastic network interface.
- Connect ke Layanan Migrasi Aplikasi hanya dengan menggunakan jaringan lokal.

Itu memperbaiki konektivitas untuk setiap instans yang berjalan di subnet pementasan (seperti server replikasi Layanan Migrasi Aplikasi atau server konversi) untuk setiapLayanan AWS yang memiliki titik akhir antarmuka yang disediakan di subnet (seperti Amazon EC2, Layanan Migrasi Aplikasi, Systems ManagerAWS KMS, dan sebagainya).

VPC endpoint Gateway

Untuk layanan seperti Amazon S3, tidak ada nama DNS tetap yang dapat disediakan karena setiap bucket memiliki nama DNS sendiri. Untuk skenario ini Anda akan menggunakan titik akhir gateway VPC.

Membuat titik akhir gateway Amazon S3 juga membuat objek daftar awalan tertentu dengan daftar tujuan subnet (dalam notasi CIDR), yang dapat ditambahkan dalam tabel rute subnet. Dengan demikian, nama DNS bucket S3 yang diselesaikan ke alamat IP yang termasuk dalam daftar ini akan dapat diakses melalui konektivitas internal.

Saat Anda menyediakan titik akhir gateway Amazon S3, Anda dapat menentukan subnet dalam tabel rute yang harus menyertakan ID daftar awalan (PL-<id>) tersebut. Tabel rute yang dihasilkan untuk subnet pribadi pementasan harus menyertakan ID daftar awalan, seperti pada tabel rute contoh ini:

Destination	Target
pl-<id>	vpce-<id-of-S3-Gateway-VPC-endpoint>
Rute lain (misalnya, CIDR subnet sumber)	Target apa pun seperti ID gateway virtual
CIDR lokal	"local"

Titik akhir masuk DNS

Konfigurasi yang dijelaskan di bagian sebelumnya cukup untuk instans yang berjalan di dalamAWS subnet, karena sudah dikonfigurasi untuk menggunakan server DNS Amazon Route 53 internal. Namun, server sumber lokal memerlukan langkah tambahan untuk dapat berkomunikasiLayanan AWS secara pribadi. Secara khusus, Agen Layanan Migrasi Aplikasi harus mengunduh penginstal dari Amazon S3 dan kemudian berkomunikasi dengan Layanan Migrasi Aplikasi dengan menggunakan nama DNS yang disediakan dalam dokumentasi. Server lokal menggunakan server DNS default mereka untuk menyelesaikan nama DNS ini, sehingga menghasilkan alamat IP publik. Komunikasi dengan alamat ini melalui HTTPS/TCP port 443 akhirnya diblokir oleh firewall perusahaan.

Untuk mencegah hal ini, Anda perlu mengkonfigurasi server sumber atau server DNS default mereka Amazon Route 53 Resolveruntuk digunakan untuk resolusi nama DNS tertentu atau zona subdomain (yaitu,`*.<region>.amazonaws.com` zona penuh). Ini dapat dikonfigurasi dengan membuat titik akhir masuk Route 53 Resolver, yang, seperti endpoint antarmuka VPC, memiliki elastic network interface khusus yang dibuat di subnet pribadi khusus aktifAWS, dan dengan demikian dapat meneruskan permintaan DNS keAmazon Route 53 Resolver.

Grup keamanan antarmuka jaringan elastis

Setiap elastic network interface memiliki grup keamanan khusus yang terkait dengannya, yang harus mengizinkan lalu lintas yang diharapkan untuk elastic network interface ini dan titik akhir yang sesuai. Dengan demikian, grup keamanan titik akhir DNS resolver harus mengizinkan port UDP masuk 53 (dan terkadang port TCP 53) untuk permintaan DNS, dan grup keamanan titik akhir untuk sebagian besar layanan lainnya (Application Migration Service, Amazon EC2, Systems Manager, dan sebagainya) perlu mengaktifkan port HTTPS/TCP 443 masuk.

Menginstal Agen Layanan Migrasi Aplikasi di server sumber

Untuk menginstal Agen Layanan Migrasi Aplikasi di server sumber, Anda harus menyediakan nama DNS Layanan Migrasi Aplikasi dan titik akhir antarmuka Amazon S3 ke parameter baris perintah Agen (lihat Menginstal Agen di jaringan yang aman dalam dokumentasi Layanan Migrasi Aplikasi).

Untuk endpoint Layanan Migrasi Aplikasi, Anda dapat menggunakan salah satu nama DNS yang terkait dengannya—bidang DNS pribadi (`mgn.<region>.amazonaws.com`) atau nama DNS khusus VPC (`vpce-<VPC-id>-<suffix>.mgn.<region>.vpce.amazonaws.com`)

—dan menyediakan argumen:`--endpoint <FQDN>`. Bahkan, jika Anda melewatkan argumen ini, Agen menggunakan ditentukanWilayah AWS untuk merekonstruksi DNS default FQDN (`mgn.<region>.amazonaws.com`) dan menggunakan FQDN untuk mengakses bidang kontrol Layanan Migrasi Aplikasi. Dalam kebanyakan kasus, perilaku default itu sudah cukup, selama FQDN menyelesaikan dari server sumber dengan benar ke alamat IP pribadi elastic network interface untuk endpoint VPC Layanan Migrasi Aplikasi yang dibuat di subnet pementasan.

Endpoint antarmuka Amazon S3 tidak akan memiliki nama DNS pribadi tunggal (karena setiap bucket S3 akan memiliki sendiri), sehingga opsi tersebut tidak didukung. Namun, endpoint antarmuka Amazon S3 masih memiliki elastic network interface yang terkait dengannya. Ini juga memiliki IP pribadi dan nama DNS wildcard tertentu (dalam format`.vpce-<VPC-ID>-<suffix>.s3.<region>.vpce.amazonaws.com` atau Region-specific. `vpce-<VPC-ID>-<suffix>-<region>.s3.<region>.vpce.amazonaws.com`) yang dapat diselesaikan dengan IP pribadi ini.

Nama DNS wildcard tersebut dapat digunakan untuk`--s3-endpoint` argumen, seperti berikut ini:

```
aws-replication-installer-init.py --region <region> --aws-access-key-id
 <MGN_IAM_ACCESS_KEY>  --aws-secret-access-key <MGN_IAM_SECRET> --no-prompt \
   --endpoint vpce-<VPC-id>-<suffix>.mgn.<region>.vpce.amazonaws.com --s3-endpoint
 vpce-<VPC-ID>-<suffix>-<region>.s3.<region>.vpce.amazonaws.com
```

Bagian selanjutnya memberikan contoh konfigurasi Layanan Migrasi Aplikasi, termasuk semua titik akhir VPC yang diperlukan, dan menerapkan Agen dengan menggunakan titik akhir VPC di server sumber Windows dan Linux. Bagian ini mencakup penerapan manual dan otomatis.

Menyebarkan lingkungan PoC

Banyak pengguna lebih suka menguji secara menyeluruh semua saluran komunikasi dan langkah migrasi terlebih dahulu. Menguji migrasi dari jaringan terisolasi bisa menjadi tantangan. Untuk mengatasi kebutuhan itu,AWS menyediakan dua opsi:

- Sebuah CloudFormation template yang mempersiapkan semua sumber daya yang diperlukan padaAWS. Template membangun lingkungan proof of concept (PoC) yang mengemulasi komponen lingkungan pusat data dan mengaturAWS infrastruktur. Ini termasuk sumber terisolasi dan target VPC, subnet, dan titik akhir VPC.
- Workshop khusus (Migrate the Well-Architected Way) dengan step-by-step petunjuk terperinci untuk membuat lingkungan pengujian Anda (lihat langkah Buat Endpoint VPC).

Atau, Anda dapat menerapkan lingkungan PoC Anda dengan mengikuti langkah-langkah di bagian berikutnya.

Penyebaran manual

Daftar berikut menguraikan langkah-langkah utama untuk penerapan manual di lingkungan Anda. Untuk informasi selengkapnya, lihat pola PanduanAWS Preskriptif Connect ke Data Layanan Migrasi Aplikasi dan bidang kontrol melalui jaringan pribadi.

1. Buat VPC sumber dan area pementasan VPC dengan subnet khusus privat.
2. Buat endpoint VPC berikut di subnet area staging:
    - Layanan Migrasi Aplikasi, dan aktifkan nama DNS pribadi (dibagikan oleh server replikasi dan server sumber).
    - Amazon EC2, dan mengaktifkan nama DNS pribadi (dibagikan oleh server replikasi dan server sumber).
    - Amazon S3 (nama DNS pribadi tidak didukung). Endpoint antarmuka didukung di Direct ConnectAWS VPN,, dan peering VPC. Oleh karena itu, ini diperlukan untuk server sumber saja (dan dapat ditemukan di tempat) untuk terhubung ke bidang kontrol Layanan Migrasi Aplikasi melalui jaringan pribadi.

> **Note**
>
> Titik akhir ssm dan ssmmessages bersifat opsional dan saat ini dibuat untuk menghubungkan server sumber melalui SSM Session Manager.

- Titik akhir gateway Amazon S3 di subnet area staging. Ini diperlukan oleh server replikasi untuk connect ke Amazon S3. Anda harus memperbarui rute untuk subnet area pementasan.

3. Buat titik akhir resolver masuk di area pementasan VPC untuk memungkinkan resolusi catatan DNS pribadi (untuk titik akhir antarmuka VPC) dari sumber VPC.
4. Perbarui opsi DHCP VPC sumber dengan titik akhir resolver masuk dari area pementasan VPC sebagai IP server DNS.
5. Aktifkan peering antara sumber dan pementasan VPC, dan perbarui kedua tabel rute VPC.
6. Buat grup keamanan di sumber dan pementasan VPC untuk mengizinkan port berikut.

Source	Destination	Port	Description
Pusat data sumber	URL layanan Amazon S3	443 (TCP)	Komunikasi melalui port TCP 443
Pusat data sumber	Alamat konsolWilayah AWS khusus Layanan Migrasi Aplikasi	443 (TCP)	Komunikasi antara server sumber dan Layanan Migrasi Aplikasi melalui port TCP 443
Pusat data sumber	Subnet area pementasan	1500 (TCP)	Komunikasi antara server sumber dan subnet area pementasan melalui port TCP 1500
Subnet area pementasan	Alamat konsolWilayah AWS khusus Layanan Migrasi Aplikasi	443 (TCP)	Komunikasi antara subnet area pementasan dan Layanan Migrasi

Source	Destination	Port	Description
			Aplikasi melalui port TCP 443
Subnet area pementasan	URL layanan Amazon S3	443 (TCP)	Komunikasi melalui port TCP 443
Subnet area pementasan	Titik akhir Amazon EC2Wilayah AWS	443 (TCP)	Komunikasi melalui port TCP 443

7. Inisialisasi Srvice Migrasi Aplikasi di area pementasanWilayah AWS dengan memperbarui detail subnet area pementasan dan mengaktifkan komunikasi melalui IP pribadi.
8. Buat peranAWS Identity and Access Management (IAM) untuk menginstal Agen Layanan Migrasi Aplikasi. Lampirkan kebijakan terkelola dan buat kunci akses dan kunci rahasia.
9. Buat profil IAM untuk menghubungkan Amazon EC2 melalui SSM Session Manager.
10. Instal Agen pada mesin sumber.

Mengotomatiskan penyebaran Agen dengan Cloud Migration Factory

Pabrik Migrasi Cloud onAWS mengotomatiskan penerapan Agen Layanan Migrasi Aplikasi untuk skenario jaringan pribadi, dengan parameter baris perintah tambahan. Saat Anda menerapkan solusi ini (lihat opsi untuk penyebaran otomatis), Anda dapat menggunakan skrip ini dan salah satu opsi berikut:

- Jalankan skrip ini secara manual dari baris perintah, seperti yang dijelaskan di bagian Run automations from command prompt pada Panduan Implementasi Pabrik Migrasi Cloud
- Tambahkan skrip ke Pabrik Migrasi dengan mengikuti petunjuk di bagian Manajemen Skrip untuk integrasi penuh dengan Pabrik Migrasi Cloud

Skrip ini mengotomatisasi berikut ini:

- Instalasi Agen Layanan Migrasi Aplikasi di server Windows menggunakan titik akhir pribadi
- Instalasi Agen Layanan Migrasi Aplikasi di server Linux menggunakan titik akhir pribadi

Pemantauan dan pemecahan masalah

Anda dapat memantau Layanan Migrasi Aplikasi dengan menggunakan Amazon CloudWatch, Amazon EventBridge, dan AWS CloudTrail, yang mengumpulkan data mentah dan memprosesnya menjadi near-real-time metrik yang dapat dibaca. Untuk informasi selengkapnya, lihat Memantau Layanan Migrasi Aplikasi dalamAWS dokumentasi.

Jika Anda mengalami masalah dan ingin meluncurkan uji baru atau instans langsung, Anda dapat mengembalikan pengujian atau tindakan langsung. Ini akan mengembalikan status siklus hidup server sumber Anda ke tahap sebelumnya, yang menunjukkan bahwa server ini belum mengalami cutover. Selama pengembalian, Anda juga akan memiliki opsi untuk menghapus pengujian atau instans langsung untuk tujuan penghematan biaya. Untuk informasi selengkapnya, lihat Pemecahan Masalah dalam dokumentasi Layanan Migrasi Aplikasi.

Ketika Agen telah diinstal, server sumber muncul di konsol Layanan Migrasi Aplikasi, dan Anda dapat melihat rincian server untuk memeriksa kemajuan replikasi.

Menguji konektivitas dan resolusi nama dari server sumber

Masuk ke server sumber dengan menggunakan protokol desktop jarak jauh Windows (RDP), Secure Shell (SSH), atauAWS Sessions Manager, dan uji yang berikut ini:

- Konektivitas melalui HTTPS pada port TCP 443 ke endpoint Layanan Migrasi Aplikasi.
  - Pada Windows (dalam PowerShell):

    ```
    Test-NetConnection -ComputerName mgn.<aws_region>.amazonaws.com -Port 443
    ```

  - Di Linux atau Windows (cmd):

    ```
    Telnet mgn.<aws_region>.amazonaws.com 443
    ```

- Konektivitas melalui HTTPS pada port TCP 443 ke titik akhir Amazon S3.
  - Pada Windows (dalam PowerShell):

    ```
    Test-NetConnection -ComputerName <s3_endpoint_name> -Port 443
    ```

  - Di Linux atau Windows (cmd):

```
Telnet <s3_endpoint_name> 443
```

- Konektivitas pada port TCP 1500 ke IP server replikasi:
  - Pada Windows (dalam PowerShell):

```
Test-NetConnection -ComputerName <Replication_Server_Private_IP> -Port 1500
```

  - Di Linux atau Windows (cmd):

```
Telnet <Replication_Server_Private_IP> 1500
```

Selain itu, pastikan titik akhir Amazon EC2 dan Application Migration Service API menyelesaikan IP pribadi dengan menggunakan perintah berikut. (Anda dapat menggunakan perintah yang sama pada Windows dan Linux.)

- `nslookup ec2.<aws_region>.amazonaws.com`
- `nslookup mgn.<aws_region>.amazonaws.com`

Menguji konektivitas dan resolusi nama dari jaringan area pementasan

Untuk menguji konektivitas dari area pementasan, luncurkan instans EC2 sementara di subnet pementasan dan uji yang berikut:

- Konektivitas melalui HTTPS pada port TCP 443 ke endpoint Layanan Migrasi Aplikasi.
  - Pada Windows (dalam PowerShell):

```
Test-NetConnection -ComputerName mgn.<aws_region>.amazonaws.com -Port 443
```

  - Di Linux atau Windows (cmd):

```
Telnet mgn.<aws_region>.amazonaws.com 443
```

- Konektivitas melalui HTTPS pada port TCP 443 ke titik akhir Amazon EC2.
  - Pada Windows (dalam PowerShell):

```
Test-NetConnection -ComputerName ec2.<aws_region>.amazonaws.com -Port 443
```

- Di Linux atau Windows (cmd):

```
Telnet ec2.<aws_region>.amazonaws.com 443
```

Jika inisialisasi replikasi berhenti di langkah “Mengunduh perangkat lunak replikasi” setelah Agen diinstal di server sumber, verifikasi yang berikut.

- resolusi nama:

```
nslookup s3.<aws_region>.amazonaws.com
```

> **Note**
>
> Titik akhir Amazon S3 akan diselesaikan ke IP publik tetapi akan terhubung secara privat melalui titik akhir gateway Amazon S3.

- Konektivitas melalui protokol HTTPS pada port TCP/443.
  - Di Windows:

```
Test-NetConnection -ComputerName s3.<aws_region>.amazonaws.com -Port 443
```

  - Di Linux:

```
Telnet s3.<aws_region>.amazonaws.com 443
```

Kesimpulan

Panduan ini mencakup persyaratan dan memberikan contoh konfigurasi untuk menggunakan Layanan Migrasi Aplikasi untuk lift-and-shift migrasi server dari jaringan lokal yang aman ke konektivitasAWS melalui pribadi (AWS VPNatauAWS Direct Connect). Ini adalah skenario khas untuk banyak migrasi perusahaan. Panduan ini juga memberikan panduan tentang cara untuk menguji dengan menggunakan penyebaran otomatis atau manual, dan memantau dan memecahkan masalah konektivitas jika muncul.

Sumber daya

Posting blog

- Percepat Migrasi Anda denganAWS Application Migration Service
- Cara Menggunakan BaruAWS Application Migration Service untuk Migrasi Angkat-dan-Shift

Panduan dan pola

- Connect ke dataAWS MGN dan kontrol pesawat melalui jaringan pribadi
- AWSstrategi migrasi besar dan praktik terbaik
- Mengotomatiskan migrasi server skala besar dengan Cloud Migration Factory

Solusi

- AWS CloudMengkoordinasikan dan mengotomatiskan migrasi skala besar keAWS solusi Cloud Migration Factory on

Riwayat dokumen

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

Perubahan	Deskripsi	Tanggal
Publikasi awal	—	10 Maret 2021

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 Postgre -Compatible Edition. SQL
- Replatform (angkat dan bentuk ulang) — Pindahkan aplikasi ke cloud, dan perkenalkan beberapa tingkat pengoptimalan untuk memanfaatkan kemampuan cloud. Contoh: Migrasikan database Oracle lokal Anda ke Amazon Relational Database Service (RDSAmazon) 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: Migrasi a Microsoft Hyper-V aplikasi untuk 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.

ACID

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

SQLFungsi 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 AWS di dokumentasi AWS Identity and Access Management (IAM).

sumber data otoritatif

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

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 CAFMengatur panduan ke dalam enam bidang 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 berikan panduan untuk pengembangan, pelatihan, dan komunikasi orang untuk membantu mempersiapkan organisasi untuk adopsi cloud yang sukses. Untuk informasi lebih lanjut, lihat situs AWS CAFweb dan AWS CAFwhitepaper.

AWS Kerangka Kualifikasi Beban Kerja ()AWS WQF

Alat yang mengevaluasi beban kerja migrasi database, merekomendasikan strategi migrasi, dan memberikan perkiraan kerja. AWS WQFdisertakan 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 menyebabkan kerugian bagi 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, API panggilan mencurigakan, dan tindakan serupa. Untuk informasi selengkapnya, lihat Data dalam grafik perilaku di dokumentasi Detektif.

sistem big-endian

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

klasifikasi biner

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

filter mekar

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

deployment biru/hijau

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

bot

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

botnet

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

cabang

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

akses break-glass

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

strategi brownfield

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

cache penyangga

Area memori tempat data yang paling sering diakses disimpan.

kemampuan bisnis

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

perencanaan kelangsungan bisnis () BCP

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

C

CAF

Lihat Kerangka Adopsi AWS Cloud.

penyebaran kenari

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

CCoE

Lihat Cloud Center of Excellence.

CDC

Lihat mengubah pengambilan data.

ubah pengambilan data (CDC)

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

rekayasa kekacauan

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

CI/CD

Lihat integrasi berkelanjutan dan pengiriman berkelanjutan.

klasifikasi

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

Enkripsi sisi klien

Enkripsi data secara lokal, sebelum target Layanan AWS menerimanya.

Pusat Keunggulan Cloud (CCoE)

Tim multi-disiplin yang mendorong upaya adopsi cloud di seluruh organisasi, termasuk mengembangkan praktik terbaik cloud, memobilisasi sumber daya, menetapkan jadwal migrasi, dan memimpin organisasi melalui transformasi skala besar. Untuk informasi selengkapnya, lihat CCoEposting 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, mendefinisikanCCoE, 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. AWS CodeCommit Setiap versi kode disebut cabang. Dalam struktur layanan mikro, setiap repositori

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

cache dingin

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

data dingin

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

visi komputer (CV)

Bidang AI yang menggunakan pembelajaran mesin untuk menganalisis dan mengekstrak informasi dari format visual seperti gambar dan video digital. Misalnya, AWS Panorama menawarkan perangkat yang menambahkan CV ke jaringan kamera lokal, dan Amazon SageMaker menyediakan algoritme pemrosesan gambar untuk CV.

konfigurasi drift

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

database manajemen konfigurasi (CMDB)

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

paket kesesuaian

Kumpulan AWS Config aturan dan tindakan remediasi yang dapat Anda kumpulkan untuk menyesuaikan kepatuhan dan pemeriksaan keamanan Anda. Anda dapat menerapkan paket kesesuaian sebagai entitas tunggal di Akun AWS dan Wilayah, atau di seluruh organisasi, dengan menggunakan templat. YAML 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 umumnya digambarkan sebagai pipa. CI/CD dapat membantu

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

CV

Lihat visi komputer.

D

data saat istirahat

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

klasifikasi data

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

penyimpangan data

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

data dalam transit

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

jala data

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

minimalisasi data

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

perimeter data

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

prapemrosesan data

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

asal data

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

subjek data

Individu yang datanya dikumpulkan dan diproses.

gudang data

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

bahasa definisi database (DDL)

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

bahasa manipulasi basis data (DML)

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. DVSMmemperluas proses pemetaan aliran nilai yang awalnya dirancang untuk praktik manufaktur

lean. 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 ara pencekik, lihat Memodernisasi Microsoft lama. ASP NET(ASMX) layanan web secara bertahap dengan menggunakan kontainer 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.

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.

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 to AWS Identity and Access Management (IAM). Akun atau prinsipal ini dapat terhubung ke layanan endpoint Anda secara pribadi dengan membuat titik akhir antarmuka. VPC Untuk informasi selengkapnya, lihat Membuat layanan titik akhir di dokumentasi Amazon Virtual Private Cloud (AmazonVPC).

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 dapat diakses oleh pengguna akhir. 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 AWS CAF keamanan termasuk 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. EDAdilakukan 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.

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.

G

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.

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 IAM izin. 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.

migrasi database homogen

Memigrasi database sumber Anda ke database target yang berbagi mesin database yang sama (misalnya, Microsoft SQL Server ke Amazon RDS untuk 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 IAM prinsip yang mendefinisikan izin mereka dalam lingkungan. AWS Cloud

aplikasi idle

Aplikasi yang memiliki rata-rata CPU dan penggunaan memori 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, a 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 bertahap

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 selengkapnya, lihat Membangun strategi transformasi digital Internet of Things (IIoT) industri.

inspeksi VPC

Dalam arsitektur AWS multi-akun, terpusat VPC yang mengelola inspeksi lalu lintas jaringan antara VPCs (dalam hal 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. ITILmenyediakan fondasi untukITSM.

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 ITSM alat, 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.

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.

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.

MAP

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. MAPmencakup metodologi migrasi untuk mengeksekusi migrasi lama dengan cara metodis dan seperangkat alat untuk mengotomatiskan 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 terbaik dan pelajaran yang dipetik 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 MPAmemberikan penilaian portofolio terperinci (ukuran kanan server, harga, TCO

perbandingan, analisis biaya migrasi) serta perencanaan migrasi (analisis data aplikasi dan pengumpulan data, pengelompokan aplikasi, prioritas migrasi, dan perencanaan gelombang). MPAAlat ini (memerlukan login) tersedia gratis untuk semua AWS konsultan dan konsultan APN Mitra.

Penilaian Kesiapan Migrasi () MRA

Proses mendapatkan wawasan tentang status kesiapan cloud organisasi, mengidentifikasi kekuatan dan kelemahan, dan membangun rencana aksi untuk menutup kesenjangan yang teridentifikasi, menggunakan. AWS CAF Untuk informasi selengkapnya, lihat panduan kesiapan migrasi. MRAIni 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 oleh 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 AWS Well-Architected.

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. OCMmembantu 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 OCMpanduannya.

kontrol akses asal (OAC)

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

identitas akses asal (OAI)

Di CloudFront, opsi untuk membatasi akses untuk mengamankan konten Amazon S3 Anda. Saat Anda menggunakanOAI, 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, a 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 IAM manajemen yang dilampirkan pada IAM prinsipal untuk menetapkan izin maksimum yang dapat dimiliki pengguna atau peran. Untuk informasi selengkapnya, lihat Batas izin dalam IAM dokumentasi.

Informasi Identifikasi Pribadi () PII

Informasi yang, jika dilihat secara langsung atau dipasangkan dengan data terkait lainnya, dapat digunakan untuk menyimpulkan identitas individu secara wajar. Contohnya 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 kebijakanberbasis sumber daya), atau menentukan izin maksimum untuk semua akun dalam organisasi di (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 pengoptimalan 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, IAM peran, atau pengguna. Untuk informasi selengkapnya, lihat Prinsip dalam istilah dan konsep Peran dalam IAM dokumentasi.

Privasi oleh Desain

Pendekatan dalam rekayasa sistem yang memperhitungkan privasi di seluruh proses rekayasa.

zona yang dihosting pribadi

Container yang menyimpan informasi tentang bagaimana Anda ingin Amazon Route 53 merespons DNS kueri 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.

pseudonimisasi

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

terbitkan/berlangganan (pub/sub)

Pola yang memungkinkan komunikasi asinkron antara layanan mikro untuk meningkatkan skalabilitas dan daya tanggap. Misalnya, dalam layanan mikro berbasis MES, layanan mikro dapat mempublikasikan pesan peristiwa ke saluran yang dapat berlangganan oleh 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 SQL relasional.

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

RACImatriks

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

ransomware

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

RASCImatriks

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 prinsip mana yang diizinkan mengakses, tindakan yang didukung, dan kondisi lain yang harus dipenuhi.

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

Matriks yang mendefinisikan peran dan tanggung jawab untuk semua pihak yang terlibat dalam kegiatan migrasi dan operasi cloud. Nama matriks berasal dari jenis tanggung jawab yang didefinisikan dalam matriks: bertanggung jawab (R), akuntabel (A), dikonsultasikan (C), dan diinformasikan (I). Jenis dukungan (S) adalah opsional. Jika Anda menyertakan dukungan, matriks disebut RASCImatriks, dan jika Anda mengecualikannya, itu disebut RACImatriks.

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.

rotasi

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

kontrol akses baris dan kolom (RCAC)

Penggunaan SQL ekspresi dasar dan fleksibel yang telah menetapkan aturan akses. RCACterdiri 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 (SSO) gabungan, sehingga pengguna dapat masuk ke AWS Management Console atau memanggil AWS API operasi tanpa Anda harus membuat pengguna untuk semua orang di IAM organisasi Anda. Untuk informasi lebih lanjut tentang federasi SAML berbasis 2.0, lihat Tentang federasi SAML berbasis 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.

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.

informasi keamanan dan manajemen acara (SIEM) sistem

Alat dan layanan yang menggabungkan sistem manajemen informasi keamanan (SIM) dan manajemen peristiwa keamanan (SEM). Sebuah SIEM sistem 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 VPC keamanan, menambal EC2 instans 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 SCPsmenentukan 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

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

perjanjian tingkat layanan () SLA

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

indikator tingkat layanan () SLI

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

tujuan tingkat layanan () SLO

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

model tanggung jawab bersama

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

SIEM

Lihat informasi keamanan dan sistem manajemen acara.

satu titik kegagalan (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 Microsoft lama. ASP NET(ASMX) layanan web secara bertahap dengan menggunakan kontainer dan Amazon API Gateway.

subnet

Berbagai alamat IP di AndaVPC. 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.

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

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.

VPCmengintip

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

SQLFungsi 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.

WORM

Lihat menulis sekali, baca banyak.

WQF

Lihat AWSKerangka 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.

aplikasi zombie

Aplikasi yang memiliki rata-rata CPU 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.