Migrasi dari F5 BIG-IP ke F5 BIG-IP VE di Cloud AWS

AWS Bimbingan Preskriptif

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Bimbingan Preskriptif: Migrasi dari F5 BIG-IP ke F5 BIG-IP VE di Cloud AWS

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Merek dagang dan tampilan dagang Amazon tidak boleh digunakan sehubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan di antara pelanggan, atau dengan cara apa pun yang merendahkan atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan hak milik masing-masing pemiliknya, yang mungkin atau tidak terafiliasi, terkait dengan, atau disponsori oleh Amazon.

Table of Contents

Pengantar 1
Hasil bisnis yang ditargetkan 1
Mengevaluasi biaya dan keterampilan migrasi 3
Menilai biaya lisensi dan instans 3
Mengevaluasi AWS dan basis pengetahuan F5 4
Memetakan aplikasi dan merancang arsitektur 6
Memetakan aplikasi 6
Merencanakan arsitektur 11
Merencanakan migrasi 13
Memutuskan apa yang akan dimigrasikan 13
Membersihkan konfigurasi Anda 14
Memilih jenis instans 16
Poin keputusan utama 17
Ikhtisar migrasi tingkat tinggi 18
Migrasi data 21
Migrasi konfigurasi lengkap 21
Memigrasi konfigurasi sebagian 23
Penyebaran kepadatan tinggi tanpa Elastis IPs 24
Menghubungkan Anda VPCs 25
Menghubungkan ke AWS infrastruktur Anda 29
Sumber daya 33
Riwayat dokumen 34
Glosarium 35
..... 35
A 36
B 39
C 41
D 44
E 48
F 50
G 52
H 53
I 54
L 57

M 58
O 62
P 65
Q 68
R 68
D 71
T 75
U 77
V 77
W 78
Z 79
..... lxxx

Migrasi dari F5 BIG-IP ke F5 BIG-IP VE di Cloud AWS

Suresh Veeragoni, Amazon Web Services ()AWS

November 2020 (riwayat dokumen)

Panduan ini memberikan gambaran umum tentang langkah-langkah, arsitektur, alat, dan pertimbangan untuk memigrasikan solusi keamanan dan manajemen lalu lintas F5 BIG-IP ke Amazon Web Services () Cloud.AWSF5 BIG-IP adalah kumpulan produk yang dirancang seputar ketersediaan, kontrol akses, dan solusi keamanan. Mereka berjalan di Sistem Operasi Manajemen Lalu Lintas F5 (TMOS).

Solusi keamanan dan manajemen lalu lintas F5 BIG-IP Anda dimigrasikan ke AWS Cloud dengan menggunakan strategi migrasi rehost dan replatform dari tujuh strategi migrasi umum (7 Rs). Beban kerja F5 akan dimigrasikan dengan menghosting ulang lingkungan yang ada dan menggunakan aspek replatforming, seperti penemuan layanan dan integrasi API.

Panduan ini menguraikan empat langkah utama untuk migrasi Anda.

- Mengevaluasi biaya dan keterampilan migrasi— memahami biaya migrasi dan pengetahuan apa dan produk AWS dan layanan F5 yang diperlukan.
- Memetakan aplikasi dan merancang arsitektur— menilai bagaimana aplikasi Anda cocok bersama dan merancang arsitektur untuk lingkungan masa depan mereka.
- Merencanakan migrasi — gunakan paket tingkat tinggi untuk migrasi Anda dan buat keputusan penting tentang apa yang harus dimigrasikan.
- Migrasi data— terapkan konfigurasi yang tersedia untuk memigrasikan beban kerja F5 BIG-IP ke Cloud dan memigrasikan data Anda. AWS

Untuk gambaran lengkap tentang langkah-langkah migrasi, lihat polanya Memigrasikan beban kerja F5 BIG-IP ke F5 BIG-IP VE di Cloud di situs web Panduan Preskriptif. AWS AWS

Panduan ini ditujukan untuk tim teknik dan arsitektur yang memigrasikan solusi keamanan dan manajemen lalu lintas F5 ke Cloud. AWS

Hasil bisnis yang ditargetkan

Organizations memilih untuk bermigrasi ke AWS Cloud untuk meningkatkan ketangkasan dan ketahanan mereka. Migrasi ini memiliki manfaat yang signifikan tetapi juga memiliki risiko yang harus

dikurangi. Secara khusus, risiko dan kompleksitas adopsi cloud meningkat ketika layanan aplikasi penting, seperti manajemen lalu lintas atau keamanan, dipecah.

Jika Anda memigrasikan beban kerja F5 BIG-IP ke AWS Cloud, Anda dapat fokus pada kelincahan dan mengadopsi model operasional bernilai tinggi di seluruh arsitektur perusahaan Anda. Anda juga akan menciptakan positif bersih untuk adopsi cloud Anda karena lingkungan teknologi Anda dapat digabungkan.

Anda juga dapat menciptakan keuntungan bisnis dengan membatasi vendor atau tool sprawl. Ini mengurangi risiko saat Anda memigrasikan aplikasi karena membatasi atau menghapus perubahan pada jalur data, fitur, alat, dan model operasional dari lingkungan sumber Anda.

Mengevaluasi biaya dan keterampilan migrasi

Sebelum Anda memutuskan untuk memigrasikan solusi keamanan dan manajemen lalu lintas F5 BIG-IP Anda ke AWS Cloud, Anda perlu menilai biaya migrasi dan mengevaluasi keterampilan apa yang diperlukan.

Bagian berikut memberikan ringkasan biaya migrasi potensial, serta ikhtisar pengetahuan tentang produk AWS dan layanan F5 yang dibutuhkan tim Anda.

Topik

- Menilai biaya lisensi dan instans
- Mengevaluasi AWS dan basis pengetahuan F5

Menilai biaya lisensi dan instans

Biaya menjalankan beban kerja F5 BIG-IP di AWS Cloud akan bervariasi berdasarkan biaya lisensi dan instans gabungan Anda. Saat bermigrasi ke AWS Cloud, Anda harus mencocokkan lisensi yang ada dan mengaktifkan fitur dari sistem sumber ke sistem tujuan.

Produk F5 memiliki beberapa model lisensi, tetapi persyaratan bisnis dan teknis Anda biasanya akan bersinggungan dengan model berikut: Bawa Lisensi Anda Sendiri (BYOL), pasar, penawaran pribadi, langganan, dan perjanjian lisensi perusahaan (ELA).

Biaya migrasi juga akan bervariasi tergantung pada apakah Anda menggunakan pay-as-you-go, instans harga tahunan, atau memiliki perjanjian individu dengan. AWS Yang penting, biaya lisensi F5 juga dapat berubah berdasarkan model dan kebutuhan pribadi Anda.

Anda dapat menggunakan Kalkulator AWS Harga untuk memperkirakan potensi biaya operasional Anda. Tiga contoh berikut memberikan wawasan tentang biaya AWS instans dan infrastruktur.

- F5 BIG-IP kecil — 100 Mbps
- F5 BIG-IP menengah — 200 Mbps
- F5 BIG-IP besar — 800 Mbps

Mengevaluasi AWS dan basis pengetahuan F5

Sebelum Anda mulai memigrasikan beban kerja F5 BIG-IP Anda, Anda harus memastikan bahwa tim Anda memiliki pengetahuan tentang produk dan layanan berikut AWS dan F5.

AWS produk dan layanan

- AWS CloudFormationmembantu Anda membuat dan menyediakan penyebaran AWS infrastruktur yang dapat diprediksi dan berulang kali.
- Amazon CloudWatch menyediakan solusi pemantauan yang andal, terukur, dan fleksibel yang dapat Anda mulai gunakan dalam hitungan menit.
- Amazon Elastic Compute Cloud (Amazon EC2) adalah layanan web yang menyediakan kapasitas komputasi yang dapat diubah ukurannya bagi Anda untuk membangun dan meng-host sistem perangkat lunak Anda.
- AWS Identity and Access Management (IAM) adalah layanan web untuk mengontrol akses ke AWS layanan dengan aman.
- AWS Landing Zone adalah solusi yang membantu pelanggan dengan cepat mengatur AWS lingkungan multi-akun yang aman berdasarkan praktik AWS terbaik.
- Amazon Simple Storage Service (Amazon S3) adalah layanan penyimpanan objek berbasis cloud yang membantu Anda menyimpan, melindungi, dan mengambil sejumlah data.
- AWS Security Token Service (AWS STS) membantu Anda meminta kredensil hak istimewa terbatas sementara untuk pengguna.
- AWS Transit Gatewayadalah layanan yang sangat tersedia dan dapat diskalakan untuk mengkonsolidasikan konfigurasi perutean VPC Amazon untuk arsitektur dengan. Wilayah AWS hub-and-spoke
- Amazon Virtual Private Cloud (Amazon VPC) membantu Anda meluncurkan AWS sumber daya ke jaringan virtual yang telah Anda tentukan.

> **Important**
>
> Tim Anda harus memahami berbagai cara untuk menghubungkan satu atau beberapa virtual private cloud (VPCs) ke pusat data yang ada, serta cara membuat sumber daya di AWS infrastruktur Anda. Untuk informasi selengkapnya tentang ini, lihat opsi konektivitas Network-to-Amazon VPC di dokumentasi Amazon VPC.

Produk dan layanan F5

- Traffic Management Operating System (F5 TMOS) adalah fondasi perangkat lunak untuk semua produk jaringan atau lalu lintas F5.
- Local Traffic Manager (F5 LTM) membantu Anda mengontrol lalu lintas jaringan, memilih tujuan yang tepat berdasarkan kinerja server, keamanan, dan ketersediaan.
- Global Traffic Manager (F5 GTM) mendistribusikan permintaan DNS dan aplikasi pengguna berdasarkan kebijakan bisnis, pusat data dan kondisi layanan cloud, lokasi pengguna, dan kinerja aplikasi.
- Access Policy Manager (F5 APM) mengamankan, menyederhanakan, dan memusatkan akses ke aplikasi, dan data APIs, di mana pun pengguna dan aplikasi mereka berada.
- Application Security Manager (F5 ASM) adalah firewall aplikasi web fleksibel yang mengamankan aplikasi web di lingkungan cloud tradisional, virtual, dan pribadi.
- Advanced Firewall Manager (F5 AFM) mengurangi ancaman jaringan sebelum mengganggu sumber daya pusat data penting.
- F5 BIG-IQ menyediakan titik pusat kontrol untuk perangkat fisik dan virtual F5, dan untuk solusi yang berjalan pada mereka.

Memetakan aplikasi dan merancang arsitektur

Bagian berikut membantu Anda memahami bagaimana aplikasi Anda cocok bersama dalam lingkungan yang ada dan bagaimana merancang arsitektur baru mereka.

Topik

- Memetakan aplikasi
- Merencanakan arsitektur

Memetakan aplikasi

Tidak ada pendekatan standar saat Anda memigrasikan aplikasi dan dependensi terkait ke Cloud. AWS Tabel berikut memberikan gambaran umum tentang pertimbangan utama untuk berbagai aplikasi yang biasanya dimigrasikan dengan beban kerja F5 BIG-IP ke Cloud. AWS

Jenis aplikasi	Kasus penggunaan	Tindakan yang disarankan
Aplikasi kustom atau komersial off-the-shelf (COT)	Anda berencana untuk menutup pusat data atau instans colocation setelah memigrasikan aplikasi ke AWS Cloud, atau menjalank an campuran AWS produk atau layanan lokal. Anda tidak berencana untuk memoderni sasi aplikasi ini. Anda mungkin telah mengintegrasikan F5 Applicati on Delivery Controller (ADC) sebagai bagian dari logika aplikasi, dan memerlukannya untuk mem-port logika yang sama ke Cloud. AWS	Tinjau konfigurasi F5 saat ini dan pisahkan ke dalam komponen aplikasi yang perlu dimigrasikan. Pastikan Anda mencocokkan model lisensi yang digunakan , baik melalui modul atau program F5 Good, Better, Best (GBB).

Jenis aplikasi	Kasus penggunaan	Tindakan yang disarankan
	Komponen aplikasi mungkin atau mungkin tidak dimigrasi kan pada saat yang bersamaan.	
Aplikasi dengan kepatuhan tinggi atau persyaratan terkait keamanan	Meskipun aplikasi ini dapat di-host ulang, direplatform, atau direkonstruksi, mereka akan membutuhkan perlindungan lanjutan. Perlindungan lanjutan ini mungkin termasuk perlindun gan perilaku, keamanan aplikasi seluler, deteksi bot tingkat lanjut, kecerdasan IP mendalam, dan penyaringan keluar data respons.	Jika Anda sudah menggunak an F5 ASM, pastikan Anda memigrasikan kebijakan keamanan atau kepatuhan. Jika ini adalah aplikasi baru, maka Anda harus mengevaluasi cara terbaik untuk memanfaatkan F5 ASM atau F5 Web Application Firewall (F5 WAF).
Aplikasi generasi berikutny a atau cloud-native yang dihosting di Amazon Elastic Container Service (Amazon ECS), Amazon Elastic Kubernetes Service (Amazon EKS), atau Amazon hosting K8S EC2	Aplikasi ini memerlukan penyetelan protokol, seperti jenis jaringan seluler atau lossy lainnya, pengoptimalan HTTP, pesawat data yang dapat diprogram (iRULES), atau layanan lanjutan yang menyelaraskan algoritma load-balancing.	Untuk masuknya kontainer , lihat F5 Container Ingress Services dari dokumentasi F5.

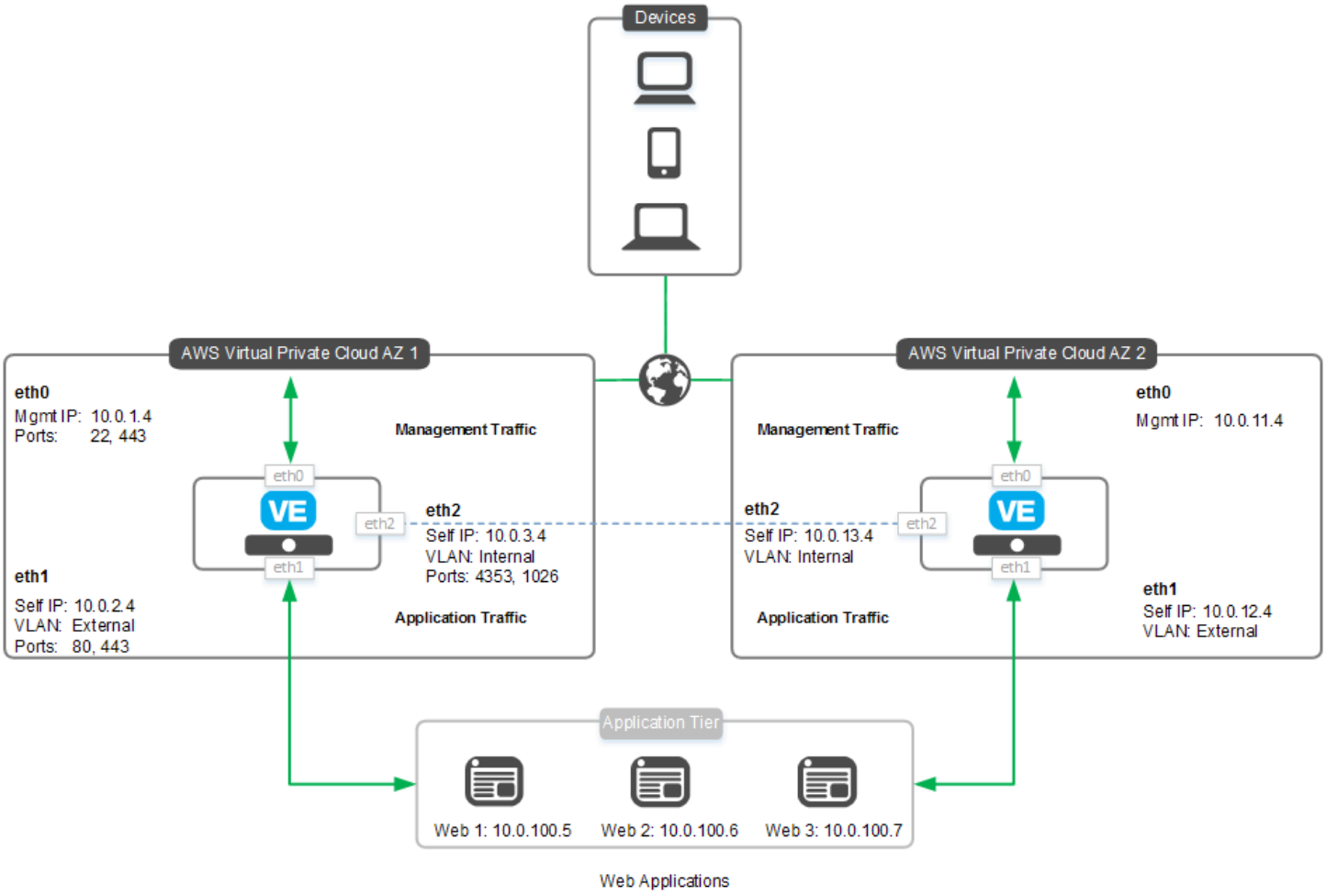
Jenis aplikasi	Kasus penggunaan	Tindakan yang disarankan
Namespace federasi atau aplikasi hybrid	Ini adalah aplikasi di mana pengiriman tingkat presentasi digabungkan di seluruh penyebaran hibrida, atau di mana layanan yang dikonsumsi berada dalam penyebaran hibrida. Misalnya, Anda mungkin menggunakan F5 GTM bersama dengan F5 LTM di tempat, dan telah memanfaatkan fitur-fitur canggih F5 GTM untuk memetakan dependensi kompleks dan logika lanjutan lokasi mana yang akan dikirim pelanggan.	Penyebaran ini harus memiliki minimal dua sistem DNS F5 atau F5 Distributed Cloud DNS. Penyebaran akan membutuhkan pembuatan satu atau lebih VPCs di AWS Cloud. Satu VPC perlu dipetakan ke dalam sistem sebagai pusat data. Ini bisa beberapa VPCs jika Anda menggunakan desain VPC transit.
Aplikasi yang dioptimalkan kinerja	Aplikasi yang mungkin memiliki profil yang sangat disetel pada sesi (L4) dan lapisan aplikasi (L7), aplikasi seluler, atau di mana Anda khawatir dengan peningkatan latensi, pengoptimalan HTTP (SPDY), dan kompresi karena migrasi ke dan dari Cloud. AWS	Ini membutuhkan penyebaran sistem F5 LTM yang menjalankan server virtual tipe standar (proxy TTCP penuh) atau lebih tinggi (proxy aplikasi seperti HTTP), dengan lalu lintas simetris rendah antara server aplikasi dan pelanggan. Lalu lintas dapat diproses oleh Source Network Address Translation (SNAT), atau instance F5 BIG-IP dapat menjadi gateway default untuk tabel instance dan rute.

Jenis aplikasi	Kasus penggunaan	Tindakan yang disarankan
Aplikasi internal di beberapa Availability Zone, ketersediaan tinggi (HA) tetapi tidak ada DNS	Anda perlu menerapkan aplikasi dan ingin mendukung lintas zona untuk meningkatkan ketersediaan, tetapi tidak ingin menggunakan DNS dan tidak dapat mengubah alamat IP.	Anda perlu menggunakan gateway pelanggan di VPC yang diintip ke gateway pribadi virtual untuk mengumumkan ruang alamat alien, serta menggunakan template F5 Advanced HA iApp untuk memanipulasi tabel rute. Sistem F5 dapat menjadi gateway pelanggan di VPC atau solusi pihak ketiga dapat menjadi gateway pelanggan.
Aplikasi WAF atau IDS/IPS	Aplikasi ini memerlukan fitur keamanan canggih seperti tanda tangan SNORT, perlindungan bot, set aturan WAF yang dalam dan kompleks (2900+ tanda tangan), dan integrasi pemindai keamanan.	Pilih topologi AWS CloudFormation template yang memenuhi kebutuhan aplikasi (AWS Auto Scaling, ketersediaan tinggi, mandiri), lalu buat dan validasi kebijakan keamanan yang sesuai.

Jenis aplikasi	Kasus penggunaan	Tindakan yang disarankan
Keamanan dan layanan transit aplikasi VPC	Ini adalah variasi dari VPC transit di mana Anda memusatkan keamanan dan layanan untuk internet atau intranet, dan mengintip ke yang lain. VPCs Topologi ini dapat digunakan bersama dengan jenis aplikasi lain dan daftar kasus penggunaan. Ini digunakan untuk mengurangi permukaan serangan internet dari struktur VPC organisasi, memusatka n kontrol, dan tugas terpisah. Ini juga digunakan untuk memasukkan aplikasi canggih dan layanan keamanan antara VPC tertentu, lainnya VPCs, dan internet.	Menyebarkan VPC transit bersama dengan persyaratan visibilitas alamat IP VPC rekan (aplikasi).
Keamanan DNS, ekspres, dan aplikasi hybrid	Replikasi tabel pencarian DNS yang aman dan konsisten di seluruh AWS Cloud dan pusat data dengan kemampuan untuk menangani volume kueri DNS yang berat; bertahan dari pemadaman koneksi langsung melalui; DNS berbasis kebijakan yang dikelola secara terpusat di seluruh lingkungan AWS Direct Connect; cache DNS dan validasi dan keamanan protokol DNS (DNSSEC).	Gunakan praktik terbaik untuk menyebarkan DNS dan memperlakukan setiap VPC sebagai pusat data virtual.

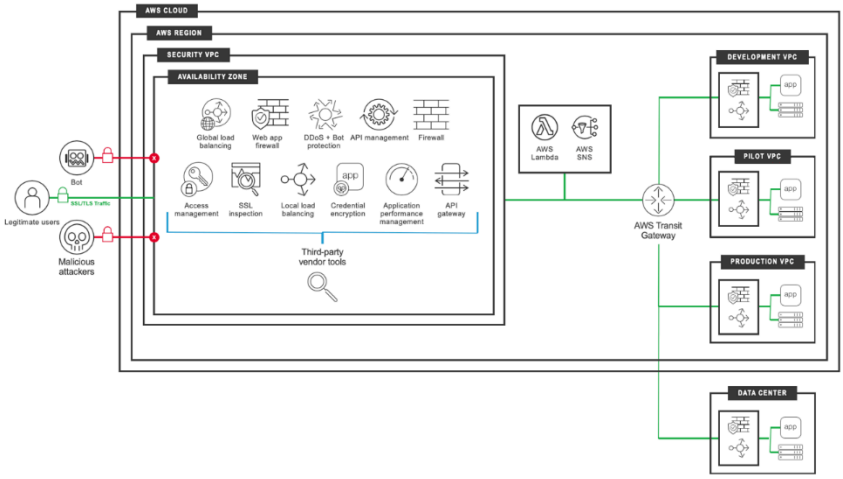
Merencanakan arsitektur

Diagram berikut menunjukkan arsitektur dasar VPC edge dan aplikasi VPCs yang dihubungkan oleh Transit Gateway. AWS VPCs Dapat menjadi bagian dari akun yang sama atau berbeda.



Misalnya, landing zone biasanya menyebarkan akun jaringan yang akan mengontrol tepi VPCs. Arsitektur ini membantu pengguna memanfaatkan kebijakan, proses, dan platform umum di seluruh rangkaian aplikasi.

Diagram berikut menunjukkan dua instance antarmuka jaringan (NIC) dari beban kerja F5 BIG-IP yang digunakan dalam cluster siaga aktif. Anda dapat menambahkan antarmuka jaringan yang lebih elastis ke sistem ini, hingga batas instans. F5 merekomendasikan agar Anda menggunakan pola Multi-AZ untuk penerapan Anda untuk menghindari kegagalan Availability Zone.


AWS CLOUD
AWS REGION
SECURITY VPC
AVAILABILITY ZONE
Global load balancing
Web app firewall
DDoS + Bot protection
API management
Firewall
Access management
SSL inspection
Local load balancing
Credential encryption
Application performance management
API gateway
Third-party vendor tools
Bot
SSL/TLS traffic
Legitimate users
Malicious attackers
AWS Lambda
AWS SNS
AWS Transit Gateway
DEVELOPMENT VPC
PILOT VPC
PRODUCTION VPC
DATA CENTER
app

Merencanakan migrasi

Merencanakan proses migrasi Anda adalah kunci untuk memastikan migrasi yang lancar dan sukses. Bagian berikut menguraikan cara merencanakan migrasi Anda, serta pertimbangan utama untuk itu.

Topik

- Memutuskan apa yang akan dimigrasikan
- Membersihkan konfigurasi Anda
- Memilih jenis instans
- Poin keputusan utama
- Ikhtisar migrasi tingkat tinggi

Memutuskan apa yang akan dimigrasikan

Saat Anda bermigrasi, Anda harus memutuskan beban kerja mana yang penting; beban kerja mana yang “bagus untuk dimiliki” tetapi tidak penting; dan beban kerja mana yang tidak diperlukan dan dapat dihentikan setelah migrasi selesai.

Bagian penting dari proses pengambilan keputusan Anda akan melibatkan persyaratan individu yang Anda miliki untuk otomatisasi, API, perkakas, dan proses lainnya. Anda juga perlu mempertimbangkan persyaratan fungsional dan kinerja organisasi Anda.

Misalnya, Anda mungkin telah menggunakan platform perangkat keras bersama di pusat data yang ada dengan partisi pengguna. Namun, migrasi Anda mungkin mengharuskan layanan berjalan pada sistem yang tidak dibagikan secara luas karena keterbatasan kinerja perpindahan dari solusi yang dipercepat perangkat keras. Misalnya, transaksi Secure Sockets Layer (SSL) per detik (TPS) dapat mengharuskan layanan tertentu tidak berjalan pada sistem bersama.

Setelah Anda mengidentifikasi dan mendokumentasikan aplikasi mana yang akan bermigrasi dan persyaratannya, Anda perlu menyiapkan sistem sumber Anda dengan menggunakan praktik terbaik berikut.

- Jalankan versi F5 TMOS yang sama yang akan Anda jalankan di Cloud. AWS Versi 14.1 atau yang lebih baru direkomendasikan, tetapi versi 13.1 atau yang lebih baru juga dapat digunakan. Meskipun Anda dapat memigrasikan versi 12.1.x, Anda mungkin mengalami masalah keamanan, otomatisasi, dan pemeliharaan.

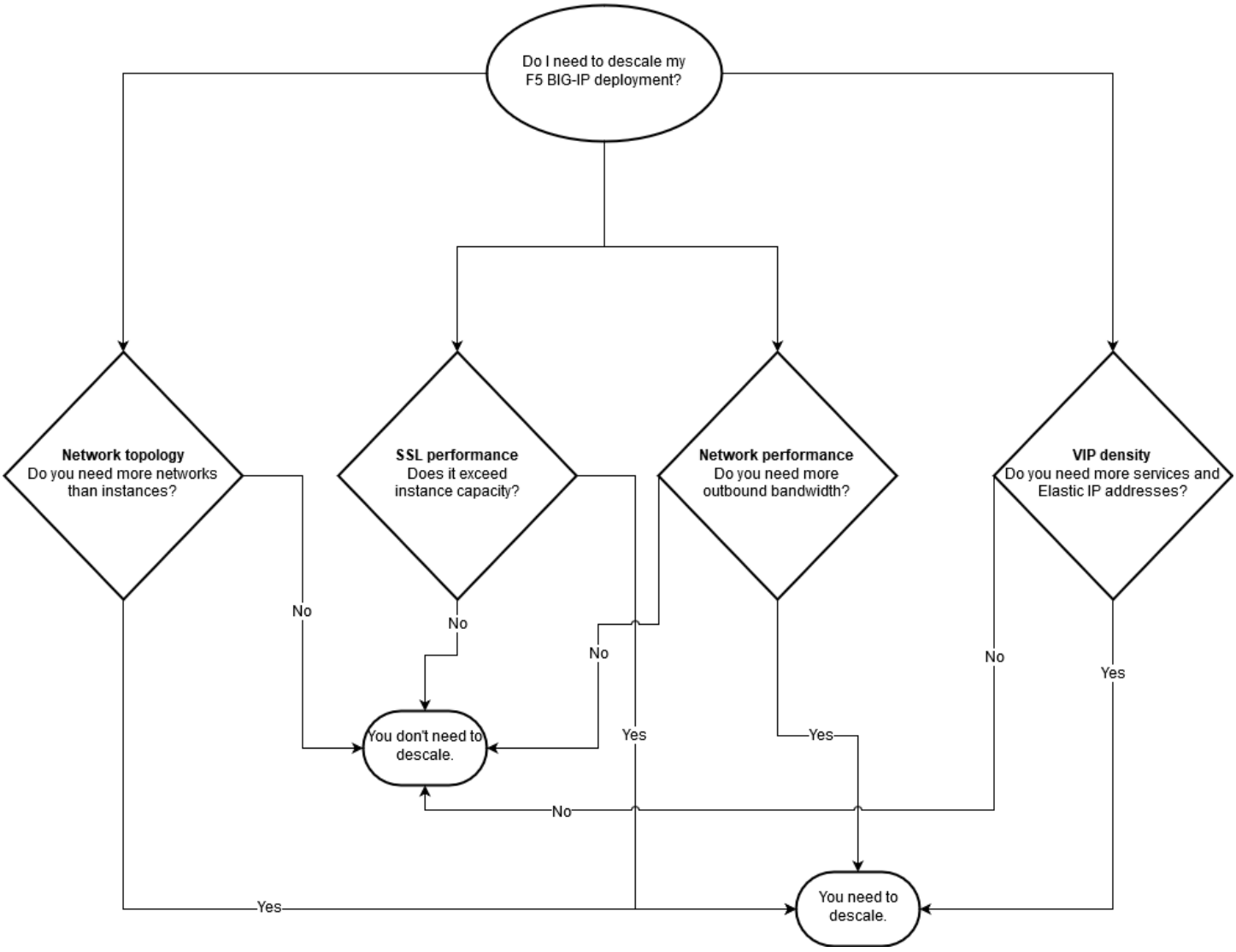
- Memiliki cadangan yang valid dari semua konfigurasi dari setiap perangkat. Karena cadangan Univention Corporate Server (UCS) berisi atribut dan objek yang khusus untuk pusat data (seperti alamat IP, node, atau anggota kumpulan), F5 merekomendasikan agar Anda membuat file perintah shell (SCF) untuk mengedit dan menggabungkan konfigurasi.
- Miliki cadangan semua sertifikat keamanan yang relevan, dan pertimbangkan untuk mengubah dari enkripsi RSA ke ECC untuk kinerja yang lebih baik.
- Memiliki metrik kinerja terperinci di tingkat server virtual untuk penskalaan dan perencanaan kapasitas.
- Miliki solusi F5 Global Server Load Balancing (GSLB) untuk cutover dari pusat data ke Cloud. AWS
- Memahami dampak migrasi dari model perangkat keras ke perangkat lunak dan model virtual dalam hal kinerja, skalabilitas, dan ketersediaan tinggi.
- Memiliki persyaratan yang ditentukan tentang apa yang akan dimigrasikan ke AWS Cloud, dan perhatikan pertimbangan berikut.
  - Ketahuilah bahwa setiap migrasi ke AWS Cloud memerlukan keputusan tentang apakah seluruh atau sebagian konfigurasi akan dimigrasikan. Biasanya, satu gerakan sebagian pada satu waktu lebih efisien.
  - Pahami rute dan alamat IP mana yang akan berubah.
  - Identifikasi kolam SNAT mana yang harus diganti dengan F5 SNAT Automap.

Anda juga harus mempertimbangkan konsultasi AWS Mitra atau tim Layanan Profesional F5. Ini akan membantu memastikan probabilitas tinggi migrasi yang berhasil.

Membersihkan konfigurasi Anda

“Descale” berarti memindahkan konfigurasi F5 BIG-IP ke konfigurasi yang lebih rendah atau lebih hemat biaya, berdasarkan fitur atau metrik yang diperlukan setelah temuan penemuan awal Anda. Anda harus hati-hati mengevaluasi semua opsi ini karena mereka akan mempengaruhi arsitektur dan jumlah contoh yang diperlukan.

Diagram berikut membantu Anda menilai apakah pembersihan kerak sesuai dengan kebutuhan dan persyaratan Anda.



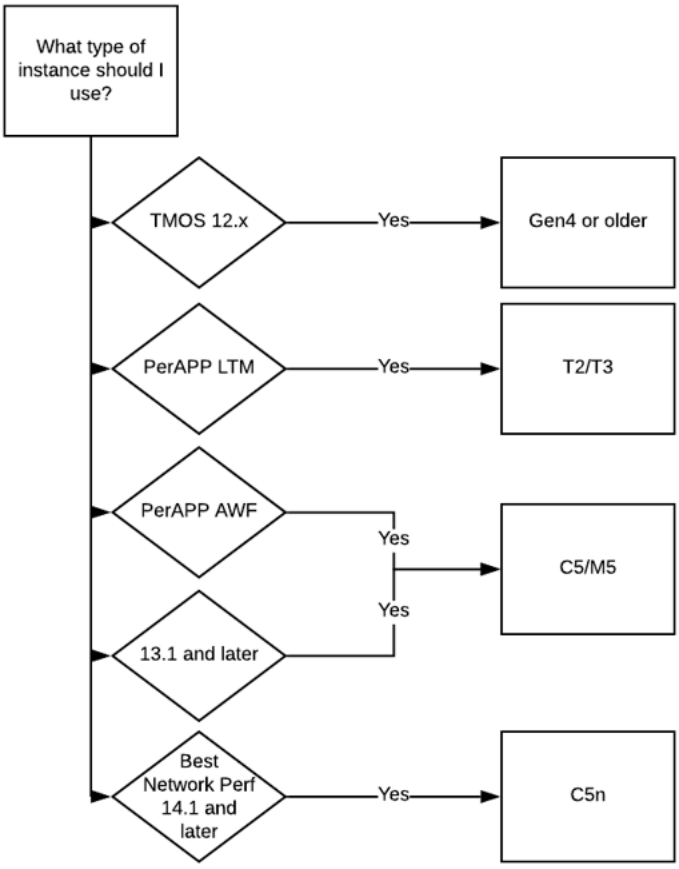
Migrasi juga akan menciptakan pertimbangan baru di bidang-bidang berikut.

- Topologi jaringan — saat ini AWS tidak mendukung `802.1q` tagged VLANs, sehingga jumlah antarmuka instance (minus satu untuk manajemen) menyajikan batas jumlah jaringan yang dapat didukung oleh instance. Jika Anda memerlukan topologi tertentu, Anda perlu mengevaluasinya dibandingkan dengan contoh lain yang didukung F5 di Cloud. AWS
- Kinerja SSL — Peralatan dan sasis F5 memiliki kinerja SSL yang melebihi apa yang dapat dicapai. `x86` Anda harus mengevaluasi persyaratan SSL server agregat dan per-virtual.
- Kinerja jaringan — Anda harus mengevaluasi karakteristik jaringan agregat, keluar, dan internal. AWS tipe instance memiliki karakteristik jaringan yang berbeda (rendah, sedang, tinggi, hingga X, atau khusus) yang harus dipertimbangkan. Ada juga batasan berapa banyak lalu lintas yang dapat dikirim oleh satu instance keluar atau melintasi koneksi langsung.

- Kepadatan VIP — Jika Anda memiliki jumlah alamat IP virtual yang lebih besar (VIPs), Anda harus mempertimbangkan batas instans untuk jumlah VIPs yang dapat dipetakan ke antarmuka jaringan.
- Koneksi bersamaan — Ada batas aliran ke jumlah maksimum koneksi yang dapat didukung oleh instans.
- Status sesi — Aplikasi yang berbeda menggunakan berbagai jenis persistensi. Aplikasi stateful dan stateless akan mengubah metode yang digunakan untuk status bersama, dan ini dapat memengaruhi skala untuk operasi masuk/keluar.

Memilih jenis instans

F5 mendukung beberapa jenis instance dan memilih mana yang akan digunakan dapat menjadi keputusan yang kompleks. Untuk sebagian besar migrasi, `c5n.2xl` dan `c5n.4xl` akan menjadi pilihan contoh yang paling umum karena mereka menawarkan campuran kinerja jaringan, kepadatan CPU, kepadatan antarmuka, dan jumlah IPs yang dapat didukung pada instance. Diagram berikut memberikan contoh contoh mana yang harus dipilih, berdasarkan produk F5 yang Anda gunakan.



Poin keputusan utama

Ada banyak aspek migrasi yang perlu dipertimbangkan, tetapi sebelum memulai migrasi beban kerja F5 BIG-IP Anda, tanyakan pada diri Anda pertanyaan-pertanyaan berikut untuk memperjelas proses migrasi.

Siapa pengguna aplikasi Anda?

Menilai apakah ini adalah pengguna internal (tidak melintasi alamat IP Elastis) atau pengguna eksternal (melintasi alamat IP Elastis). Jika pengguna internal, evaluasi apakah aplikasi dapat menggunakan DNS untuk mengakomodasi kegagalan Availability Zone atau penerapan aktif. Anda juga harus memverifikasi apakah Anda perlu menggunakan pola desain alternatif yang memungkinkan subnet menjangkau beberapa Availability Zone.

Bagian mana dari aplikasi Anda yang akan bermigrasi ke AWS Cloud?

Menilai apakah seluruh aplikasi bergerak atau hanya tingkat presentasi. Anda juga harus mempertimbangkan dependensi tambahan seputar keamanan dan namespace DNS. Evaluasi Anda perlu menentukan apa yang diperlukan dari topologi jaringan. Selain itu, tentukan apa yang diperlukan dari perjanjian tingkat layanan (SLA) jika suatu peristiwa terjadi di tingkat Availability Zone, VPC, atau Region. AWS

Mengapa aplikasi bermigrasi?

Anda mungkin memigrasikan aplikasi Anda karena Anda menutup pusat data atau karena Anda ingin lebih elastisitas. Menilai apakah aplikasi bermigrasi untuk memiliki arsitektur per aplikasi, dibandingkan dengan pola monolitik bersama yang umum di banyak pusat data. Perlu juga mempertimbangkan upaya modernisasi apa yang harus dilakukan bersama dengan migrasi.

Ke mana aplikasi bermigrasi?

Nilai apakah aplikasi perlu pindah ke satu VPC dengan satu Availability Zone atau dua Availability Zone. Tentukan topologi VPC peer atau transit, bersama dengan kebutuhan untuk penyebaran Multi-wilayah. Ini akan berdampak pada desain pola migrasi.

Ikhtisar migrasi tingkat tinggi

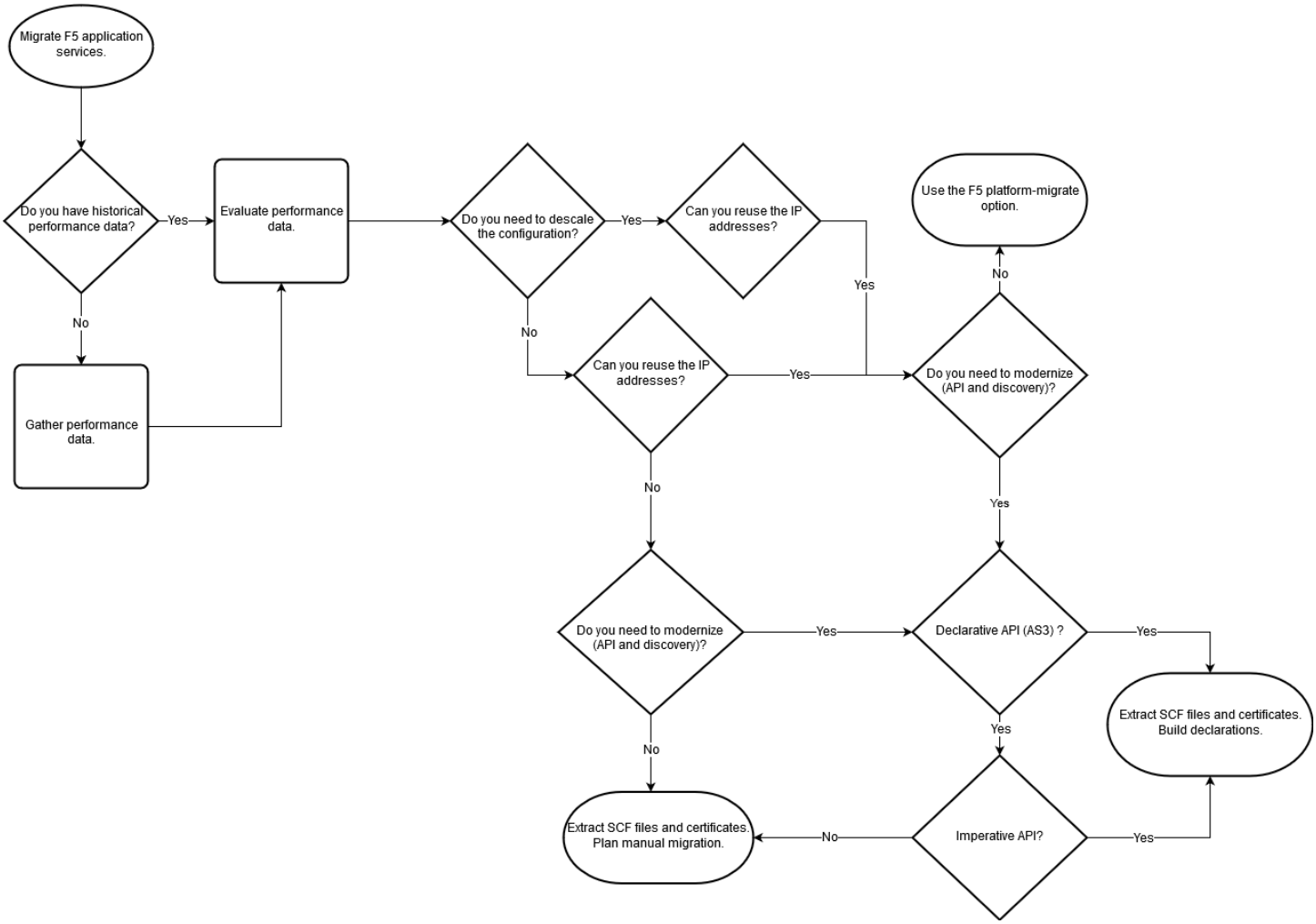
Sebelum Anda memulai migrasi, ada baiknya untuk menjabarkan seluruh proses dari tingkat tinggi. Berikut ini adalah contoh langkah-langkah yang mungkin Anda ambil untuk memigrasikan beban kerja F5 BIG-IP ke Cloud. AWS Langkah-langkah dan proses yang lebih rinci untuk migrasi F5 BIG-IP dapat ditemukan dalam pola Migrasikan beban kerja F5 BIG-IP ke F5 BIG-IP VE di Cloud. AWS

1. Terapkan jumlah yang diperlukan VPCs berdasarkan kebutuhan pribadi Anda. Ini bisa manual atau otomatis melalui alat seperti AWS Landing Zone.
2. Evaluasi lisensi, pemanfaatan, dan konfigurasi F5 saat ini.
3. Mengevaluasi aplikasi publik dan internal.
4. Evaluasi konfigurasi F5 saat ini.
5. Evaluasi ukuran dan persyaratan alamat IP, dan pilih nomor dan jenis F5 dan AWS instance yang diperlukan.
6. Identifikasi strategi migrasi mana yang akan diterapkan. Misalnya, angkat dan geser; angkat, geser dan modernisasi; atau hibrida.
7. Mengevaluasi dan mengidentifikasi desain DNS.

8. Evaluasi bagaimana lalu lintas akan diarahkan ke aplikasi jika ada baik di tempat maupun di AWS Cloud.
9. Lakukan penerapan awal instance F5 dengan menggunakan template. AWS CloudFormation
10. Ubah penerapan untuk memenuhi persyaratan topologi dengan antarmuka jaringan elastis tambahan dan tabel rute.
11. Sejajarkan alamat IP Elastis ke mandiri IPs atau manajemen IPs, dan rencanakan pemetaan IP Elastis ke IP virtual (VIP).
12. Buat alamat sekunder pada antarmuka jaringan elastis untuk VIPs.
13. Terapkan alamat sekunder di AWS Cloud.
14. Petakan alamat IP Elastis ke alamat sekunder untuk VIPs.
15. Tarik konfigurasi dan kompilasi daftar objek untuk dipindahkan.
16. Menyebarkan konfigurasi ke F5 BIG-IP.
17. Petakan alamat sekunder ke VIPs.
18. Uji lalu lintas.
19. Uji failover.
20. Jika Anda membangun hibrida, pastikan Anda memasukkan sistem ke dalam DNS F5.

> **⚠ Important**
>
> Akses ke titik akhir AWS API diperlukan. Alamat IP NAT atau Elastis juga diperlukan untuk ketersediaan tinggi di dalam atau di antara Availability Zones.

Diagram berikut menunjukkan aliran proses tingkat tinggi untuk migrasi F5 BIG-IP.


Migrate F5 application services.
Do you have historical performance data?
Yes
No
Evaluate performance data.
Gather performance data.
Do you need to descale the configuration?
Yes
No
Can you reuse the IP addresses?
Yes
No
Use the F5 platform-migrate option.
Can you reuse the IP addresses?
Yes
No
Do you need to modernize (API and discovery)?
Yes
No
Do you need to modernize (API and discovery)?
Yes
No
Declarative API (AS3) ?
Yes
Yes
Extract SCF files and certificates. Build declarations.
Imperative API?
Yes
No
Extract SCF files and certificates. Plan manual migration.

Migrasi data

Semua migrasi harus diulang pada konfigurasi dan membangun pohon ketergantungan. Saat menggunakan satu file konfigurasi, ini semua dilakukan untuk Anda. Jika Anda menggunakan TMSH API, maka Anda harus mengulangi dan membangun pohon ketergantungan. Bagian berikut akan menguraikan berbagai opsi dan konfigurasi yang tersedia saat memigrasikan beban kerja F5 BIG-IP.

Topik

- Migrasi konfigurasi lengkap
- Memigrasi konfigurasi sebagian
- Penyebaran kepadatan tinggi tanpa Elastis IPs
- Menghubungkan Anda VPCs
- Menghubungkan ke AWS infrastruktur Anda

Migrasi konfigurasi lengkap

Dalam pendekatan ini, Anda mengambil konfigurasi dari sistem yang ada dan memigrasikannya ke sistem baru. Proses ini akan menyalin konfigurasi yang ada, alamat IP, sertifikat, kunci, frasa pass, dan kredenal masuk.

Alasan utama untuk memigrasikan seluruh konfigurasi adalah untuk penggantian like-for-like sistem, seperti upgrade perangkat keras atau RMA. Biasanya, konsep ini tidak berlaku untuk AWS Cloud.

Anda dapat menggunakan file UCS atau SCF untuk memigrasikan konfigurasi lengkap, dan tabel berikut memberikan gambaran umum tentang kelebihan dan kekurangan menggunakannya.

Gunakan file UCS atau qkview

Keuntungan	Kekurangan
Semua file dipindahkan sebagai arsip tunggal.	Kasus penggunaan utama untuk menggunak an file UCS adalah mengganti perangkat yang gagal. Arsip berisi informasi khusus perangkat yang mungkin membuat beban kerja F5 BIG-IP tidak dapat dijangkau.

Keuntungan	Kekurangan
Akun pengguna lokal dipertahankan. Jika mereka terintegrasi dengan direktori aktif Anda, maka konfigurasi dipertahankan.	Jika Anda telah mengonfigurasi integrasi direktori, Anda mungkin memiliki masalah akses. Jika Anda tidak memiliki akses ke kata sandi pengguna, Anda mungkin juga memiliki masalah akses.
Semua konfigurasi server virtual dipertahankan.	Anda mungkin harus mengedit alamat IP perangkat, server virtual, dan anggota pool.
Struktur file dipertahankan.	Anda harus tahu file mana yang akan diedit.
	Proses ini lebih kompleks daripada SCF atau object-by-object bergerak.
	Peningkatan risiko kesalahan, termasuk pemindahan atau potensi konfigurasi gagal dimuat.
	Dirancang untuk seluruh alur kerja penggantian sistem.

Gunakan file SCF

Keuntungan	Kekurangan
Membuat file teks konfigurasi.	Pengeditan akan diperlukan karena akan ada properti khusus perangkat dalam file yang dapat memengaruhi akses jika file hanya dimuat.
Mudah diedit di editor teks Unix atau Linux apa pun.	Anda harus memahami konfigurasi dan struktur file untuk melakukan pengeditan.
File konfigurasi memiliki urutan operasi pemuatan yang benar.	Anda harus tahu bagian mana dari file yang harus dihapus untuk mencegahnya menimpa konfigurasi khusus perangkat.

Keuntungan	Kekurangan
Anda dapat dengan mudah menemukan objek yang akan dimigrasikan.	

Memigrasi konfigurasi sebagian

Ketika Anda memilih untuk memigrasikan konfigurasi parsional, Anda akan menggunakan file TMSH atau SCF sebagai titik awal Anda. Anda juga perlu mencari objek yang ingin Anda pindahkan dan mengompilasinya dalam urutan yang benar. Tabel berikut menguraikan keuntungan dan kerugian dari memigrasi konfigurasi sebagian.

Keuntungan	Kekurangan
Konfigurasi dapat diurai dan koreksi dilakukan saat pekerjaan berlangsung.	Pengetahuan diperlukan dari objek F5 dan struktur file. Anda juga harus bisa membaca iRules.
Perubahan konfigurasi dapat dikelompokkan.	Migrasi membutuhkan waktu.
Lebih mudah untuk memecahkan masalah beban konfigurasi.	Ini bisa memakan waktu untuk mengedit file atau mengekstrak informasi.
Mengurangi risiko terkunci dari perangkat.	
Lebih mudah untuk memindahkan konfigurasi ke topologi yang sesuai.	
Lebih mudah untuk menangani partisi administrator dan domain rute karena ini adalah file datar.	
Struktur file datar memungkinkan penggunaan alat teks Linux jika Anda ingin menemukan dan mengganti alamat IP secara terprogram.	

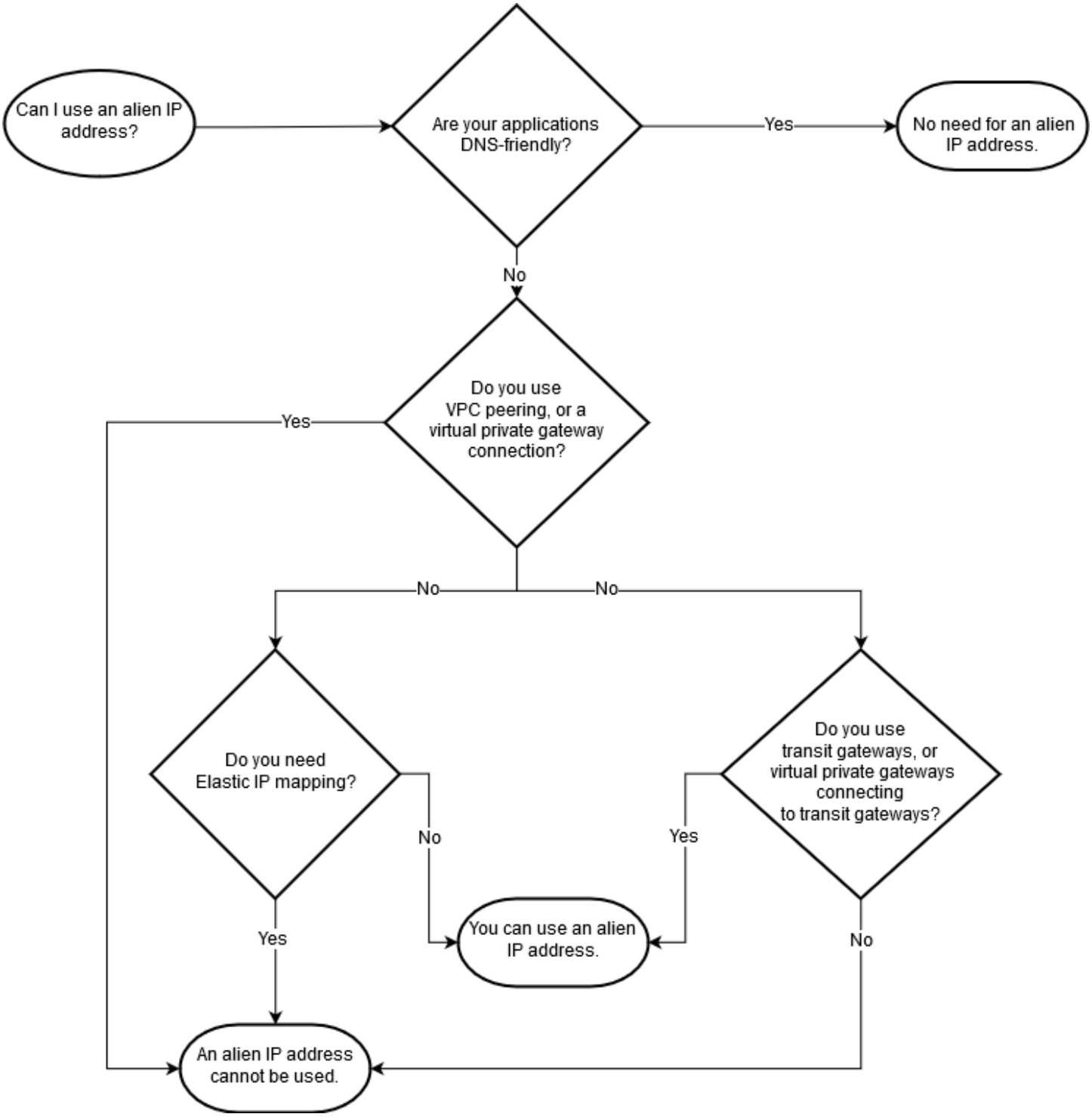
Penyebaran kepadatan tinggi tanpa Elastis IPs

Jika Anda membutuhkan penerapan yang sangat padat, maka Anda dapat beroperasi dalam metrik kinerja dan aplikasi ini tidak memerlukan penggunaan Elastic. IPs Ini disebut sebagai “IP alien.”

IP alien adalah jaringan atau rentang subnet yang berada di luar blok VPC CIDR dan tempat F5 memetakan layanan virtual. Alamat IP alien tidak berfungsi di semua skenario, tetapi dapat digunakan untuk kepadatan server virtual yang tinggi. Sebelum IP alien dapat digunakan, sumber daya berikut diperlukan.

- Satu subnet untuk meng-host aplikasi
- Penerapan F5 BIG-IP dengan Ekstensi Cloud Failover untuk mengelola rute
- Rute dalam tabel AWS rute yang menunjuk ke antarmuka jaringan elastis

Menggunakan alamat IP alien memang memiliki implikasi untuk bagaimana Anda interkoneksi VPCs ke orang lain VPCs, serta bagaimana Anda dapat interkoneksi VPCs ke pusat data Anda. Diagram berikut membantu menentukan apakah alamat IP alien diperlukan.



Menghubungkan Anda VPCs

Tabel berikut menunjukkan pertimbangan utama ketika Anda menghubungkan Anda. VPCs

Keamanan VPC dengan VPC peering		VPC Keamanan dengan AWS Transit Gateway		VPC keamanan dengan interkoneksi VPN	
Keuntungan	Kekurangan	Keuntungan	Kekurangan	Keuntungan	Kekurangan
• Mudah dan cepat untuk mengatur • Perutean sederhana • Redundansi tinggi • Bandwidth tinggi	• Hanya mendukung lalu lintas dari rentang CIDR yang ditetapkan VPC • Tidak dapat memasukkan pemeriksaan keamanan antara VPCs • Kompleks untuk dikelola dalam skala (semuanya point-to-point)	• Mudah diatur • Perutean fleksibel tanpa SNAT • Redundansi tinggi • Bandwidth tinggi • Mudah dikelola dalam skala besar	• Routing lebih kompleks (tabel rute VPC dan tabel rute Transit AWS Gateway) • Topologi kompleks untuk memasukkan inspeksi keamanan antara VPCs	• Perutean fleksibel tanpa SNAT • Penyisipan inspeksi keamanan yang mudah antara VPCs	• Bandwidth rendah • Failover dependen spesifik vendor yang kompleks • Kompleks untuk dikelola dalam skala (semuanya point-to-point)

Klien (mengirim SYN)	AWS Transit Gateway	Peering VPC	VPN antara VPCs	Ikhtisar solusi dan kemungkinan masalah
Internet atau AWS Direct Connect layanan dalam satu VPC dengan subnet publik atau pribadi.	N/A	N/A	N/A	Lalu lintas melintasi gateway internet, atau gateway virtual - tidak perlu melintasi lebih dari batas VPC. VPC bertindak sebagai jaringan rintisan yang dirancang. Lalu lintas masuk dari tempat ke AWS Cloud (AWS Direct Connect, VPN).
Internet atau AWS Direct Connect dalam VPC dengan klien lain VPCs (misalnya , anggota kumpulan di VPC lain), tidak ada SNAT.	Ya	Tidak	Ya	AWS Transit Gateway atau VPNs izinkan lalu lintas untuk melewati filter peering VPC yang hanya CIDRs dapat dilewati oleh VPC yang ditugaskan. Solusi VPN akan dibatasi. Tidak ada perutean multi-jalur biaya yang sama (ECMP) (hanya satu rute) dan tidak ada bandwidth (sekitar 1,2 GB-detik per terowongan, secara umum hanya satu terowongan).
Internet atau AWS Direct Connect ke layanan dalam VPC dengan pelanggan lain VPCs (misalnya , anggota kumpulan di VPC lain), dengan SNAT.	Ya (tapi tidak diperlukan)	Ya	Ya (tapi tidak diperlukan)	Karena interkoneksi antara VPCs melihat lalu lintas dari VPC yang ditugaskan CIDRs, apa pun akan berfungsi. Solusi VPN akan dibatasi. Tidak ada ECMP (hanya satu rute) dan tidak ada bandwidth (sekitar 1,2 GB-detik per terowongan, secara umum hanya satu terowongan).

Klien (mengirim SYN)	AWS Transit Gateway	Peering VPC	VPN antara VPCs	Ikhtisar solusi dan kemungkinan masalah
Di dalam VPC untuk layanan di VPC yang sama.	N/A	N/A	N/A	Semua lalu lintas dibatasi ke satu VPC. Interkoneksi tidak diperlukan.
Di dalam satu VPC ke VPC layanan. Layanan ada di VPC CIDR tujuan.	Ya (tapi tidak diperlukan)	Ya	Ya (tapi tidak diperlukan)	Karena interkoneksi antara VPCs melihat lalu lintas dari VPC yang ditugaskan CIDRs, apa pun akan berfungsi.
Di dalam satu VPC ke VPC layanan. Layanan berada di luar jangkauan VPC CIDR.	Ya	Tidak	Ya	Karena interkoneksi antara VPCs melihat lalu lintas dari VPC yang ditugaskan CIDRs, apa pun akan berfungsi. Solusi VPN akan dibatasi. Tidak ada ECMP (hanya satu rute) dan tidak ada bandwidth (sekitar 1,2 GB-detik per terowongan, secara umum hanya satu terowongan).
Di dalam satu VPC ke layanan internet.	N/A	N/A	N/A	Lalu lintas berasal dari CIDR yang ditugaskan VPC, jika Elastic IP, NAT, atau konstruksi tabel rute inline maka lalu lintas akan mengalir.

Klien (mengirim SYN)	AWS Transit Gateway	Peering VPC	VPN antara VPCs	Ikhtisar solusi dan kemungkinan masalah
Di dalam VPC ke layanan internet, routing keluar melalui VPC keamanan atau inspeksi.	Ya	Tidak	Ya	Karena interkoneksi antara VPCs melihat lalu lintas dari luar rentang CIDR yang ditetapkan VPC, peering VPC tidak dapat digunakan. Solusi VPN akan dibatasi. Tidak ada ECMP (hanya satu rute) dan tidak ada bandwidth (sekitar 1,2 GB-detik per terowongan, secara umum hanya satu terowongan).

Menghubungkan ke AWS infrastruktur Anda

Tabel berikut menunjukkan pertimbangan utama saat Anda terhubung ke AWS infrastruktur baru selama migrasi BIG-IP F5.

Metode konektivitas	Dukungan protokol perutean	Batas bandwidth	Alamat IP titik akhir (publik, pribadi, atau keduanya)	Support untuk ruang alamat alien	Dukungan multi-VPC untuk satu koneksi	Dukungan Multi-Wilayah
Internet	N/A	Anda menautkan ke AWS, 5 GB-detik per instans keluar	Publik	Tidak	Ya	Ya
VPN - VPC	Statis, BGP	IPsec batas (sekitar	Privat	Ya (Anda harus mengatur	Tidak	Tidak

Metode konektivitas	Dukungan protokol perutean	Batas bandwidth	Alamat IP titik akhir (publik, pribadi, atau keduanya)	Support untuk ruang alamat alien	Dukungan multi-VPC untuk satu koneksi	Dukungan Multi-Wilayah
		1,2 GB-detik per terowongan)		IPsec terowongan tambahan dari F5 BIG-IP di VPC ke gateway virtual yang terhubung ke VPC).		
VPN dan AWS Transit Gateway	Statis, BGP	IPsec batas (sekitar 1,2 GB-detik per terowongan)	Privat	Ya	Ya	Tidak (jika gateway transit diperpanjang, itu akan terpengaruh)

Metode konektivitas	Dukungan protokol perutean	Batas bandwidth	Alamat IP titik akhir (publik, pribadi, atau keduanya)	Support untuk ruang alamat alien	Dukungan multi-VPC untuk satu koneksi	Dukungan Multi-Wilayah
AWS Direct Connect - VPC	Statis, BGP	AWS Direct Connect batas (mendukung ikatan), instance individual dibatasi hingga 5 GB-detik	Keduanya	Tidak	Tidak	Tidak
AWS Direct Connect - pintu gerbang	Statis, BGP	AWS Direct Connect batas (mendukung ikatan), instance individual dibatasi hingga 5 GB-detik	Keduanya	Tidak	Ya	Ya

Metode konektivitas	Dukungan protokol perutean	Batas bandwidth	Alamat IP titik akhir (publik, pribadi, atau keduanya)	Support untuk ruang alamat alien	Dukungan multi-VPC untuk satu koneksi	Dukungan Multi-Wilayah
AWS Direct Connect gateway - AWS Transit Gateway (terbatas pada beberapa AWS Wilayah)	Statis, BGP	AWS Direct Connect batas (mendukung ikatan), instance individual dibatasi hingga 5 GB-detik	Konfirmasi verbal dari tim AWS arsitek	Ya	Ya	Terbatas untuk beberapa daerah

Sumber daya

Dokumentasi F5

- Ekstensi Failover Cloud F5
- Streaming Telemetri F5
- Lab Topologi F5
- Layanan Aplikasi F5 di AWS: ikhtisar (video)
- Layanan Aplikasi F5 3 Panduan Pengguna Ekstensi
- F5 devcentral GitHub
- F5 iControl REST wiki
- Ikhtisar F5 dari file konfigurasi tunggal (11.x - 15.x)
- Whitepaper F5
- Ikhtisar opsi “platform-migrate” arsip UCS
- Pusat Pengetahuan Edisi Cloud BIG-IP F5

AWS sumber daya

- F5 di Marketplace AWS
- F5 BIG-IP VE aktif: Mulai Cepat AWS

AWS Mitra

- F5 pada AWS

Panduan dan pola terkait

- Migrasikan beban kerja F5 BIG-IP ke F5 BIG-IP VE di Cloud AWS

Riwayat dokumen

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

Perubahan	Deskripsi	Tanggal
Publikasi awal	—	16 November 2020

AWS Glosarium Panduan Preskriptif

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

Nomor

7 Rs

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

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

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

A

ABAC

Lihat kontrol akses berbasis atribut.

layanan abstrak

Lihat layanan terkelola.

ASAM

Lihat atomisitas, konsistensi, isolasi, daya tahan.

migrasi aktif-aktif

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

migrasi aktif-pasif

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

fungsi agregat

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

AI

Lihat kecerdasan buatan.

AIOps

Lihat operasi kecerdasan buatan.

anonimisasi

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

anti-pola

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

kontrol aplikasi

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

portofolio aplikasi

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

kecerdasan buatan (AI)

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

operasi kecerdasan buatan (AIOps)

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

enkripsi asimetris

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

atomisitas, konsistensi, isolasi, daya tahan (ACID)

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

kontrol akses berbasis atribut (ABAC)

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

sumber data otoritatif

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

Zona Ketersediaan

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

AWS Kerangka Adopsi Cloud (AWS CAF)

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

AWS Kerangka Kualifikasi Beban Kerja (AWS WQF)

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

B

bot buruk

Bot yang dimaksudkan untuk mengganggu atau membahayakan individu atau organisasi.

BCP

Lihat perencanaan kontinuitas bisnis.

grafik perilaku

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

sistem big-endian

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

klasifikasi biner

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

filter mekar

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

deployment biru/hijau

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

bot

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

botnet

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

cabang

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

akses break-glass

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

strategi brownfield

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

cache penyangga

Area memori tempat data yang paling sering diakses disimpan.

kemampuan bisnis

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

perencanaan kelangsungan bisnis (BCP)

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

C

KAFE

Lihat Kerangka Adopsi AWS Cloud.

penyebaran kenari

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

CCoE

Lihat Cloud Center of Excellence.

CDC

Lihat mengubah pengambilan data.

ubah pengambilan data (CDC)

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

rekayasa kekacauan

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

CI/CD

Lihat integrasi berkelanjutan dan pengiriman berkelanjutan.

klasifikasi

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

Enkripsi sisi klien

Enkripsi data secara lokal, sebelum target Layanan AWS menerimanya.

Pusat Keunggulan Cloud (CCoE)

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

komputasi cloud

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

model operasi cloud

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

tahap adopsi cloud

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

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

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

CMDB

Lihat database manajemen konfigurasi.

repositori kode

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

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

cache dingin

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

data dingin

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

visi komputer (CV)

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

konfigurasi drift

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

database manajemen konfigurasi (CMDB)

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

paket kesesuaian

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

integrasi berkelanjutan dan pengiriman berkelanjutan (CI/CD)

Proses mengotomatiskan sumber, membangun, menguji, pementasan, dan tahap produksi dari proses rilis perangkat lunak. CI/CD is commonly described as a pipeline. CI/CDdapat membantu

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

CV

Lihat visi komputer.

D

data saat istirahat

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

klasifikasi data

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

penyimpangan data

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

data dalam transit

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

jala data

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

minimalisasi data

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

perimeter data

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

prapemrosesan data

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

asal data

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

subjek data

Individu yang datanya dikumpulkan dan diproses.

gudang data

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

bahasa definisi database (DDL)

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

bahasa manipulasi basis data (DHTML)

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

DDL

Lihat bahasa definisi database.

ansambel yang dalam

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

pembelajaran mendalam

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

defense-in-depth

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

administrator yang didelegasikan

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

deployment

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

lingkungan pengembangan

Lihat lingkungan.

kontrol detektif

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

pemetaan aliran nilai pengembangan (DVSM)

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

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

kembar digital

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

tabel dimensi

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

musibah

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

pemulihan bencana (DR)

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

DML~

Lihat bahasa manipulasi basis data.

desain berbasis domain

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

DR

Lihat pemulihan bencana.

deteksi drift

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

DVSM

Lihat pemetaan aliran nilai pengembangan.

E

EDA

Lihat analisis data eksplorasi.

EDI

Lihat pertukaran data elektronik.

komputasi tepi

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

pertukaran data elektronik (EDI)

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

enkripsi

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

kunci enkripsi

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

endianness

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

titik akhir

Lihat titik akhir layanan.

layanan endpoint

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

perencanaan sumber daya perusahaan (ERP)

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

enkripsi amplop

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

lingkungan

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

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

epik

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

ERP

Lihat perencanaan sumber daya perusahaan.

analisis data eksplorasi (EDA)

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

F

tabel fakta

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

gagal cepat

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

batas isolasi kesalahan

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

cabang fitur

Lihat cabang.

fitur

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

pentingnya fitur

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

transformasi fitur

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

beberapa tembakan mendorong

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

FGAC

Lihat kontrol akses berbutir halus.

kontrol akses berbutir halus (FGAC)

Penggunaan beberapa kondisi untuk mengizinkan atau menolak permintaan akses.

migrasi flash-cut

Metode migrasi database yang menggunakan replikasi data berkelanjutan melalui pengambilan data perubahan untuk memigrasikan data dalam waktu sesingkat mungkin, alih-alih menggunakan pendekatan bertahap. Tujuannya adalah untuk menjaga downtime seminimal mungkin.

FM

Lihat model pondasi.

model pondasi (FM)

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

G

AI generatif

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

pemblokiran geografis

Lihat pembatasan geografis.

pembatasan geografis (pemblokiran geografis)

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

Alur kerja Gitflow

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

gambar emas

Sebuah snapshot dari sistem atau perangkat lunak yang digunakan sebagai template untuk menyebarkan instance baru dari sistem atau perangkat lunak itu. Misalnya, di bidang manufaktur, gambar emas dapat digunakan untuk menyediakan perangkat lunak pada beberapa perangkat dan membantu meningkatkan kecepatan, skalabilitas, dan produktivitas dalam operasi manufaktur perangkat.

strategi greenfield

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

pagar pembatas

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

H

HA

Lihat ketersediaan tinggi.

migrasi database heterogen

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

ketersediaan tinggi (HA)

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

modernisasi sejarawan

Pendekatan yang digunakan untuk memodernisasi dan meningkatkan sistem teknologi operasional (OT) untuk melayani kebutuhan industri manufaktur dengan lebih baik. Sejarawan

adalah jenis database yang digunakan untuk mengumpulkan dan menyimpan data dari berbagai sumber di pabrik.

data penahanan

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

migrasi database homogen

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

data panas

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

perbaikan terbaru

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

periode hypercare

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

I

IAc

Lihat infrastruktur sebagai kode.

kebijakan berbasis identitas

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

aplikasi idle

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

IIoT

Lihat Internet of Things industri.

infrastruktur yang tidak dapat diubah

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

masuk (masuknya) VPC

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

migrasi inkremental

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

Industri 4.0

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

infrastruktur

Semua sumber daya dan aset yang terkandung dalam lingkungan aplikasi.

infrastruktur sebagai kode (IAc)

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

Internet of Things industri (IIoT)

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

inspeksi VPC

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

Internet of Things (IoT)

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

interpretabilitas

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

IoT

Lihat Internet of Things.

Perpustakaan informasi TI (ITIL)

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

Manajemen layanan TI (ITSM)

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

ITIL

: Lihat perpustakaan informasi TI.

ITSM

: Lihat manajemen layanan TI.

L

kontrol akses berbasis label (LBAC)

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

landing zone

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

model bahasa besar (LLM)

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

migrasi besar

: Migrasi 300 atau lebih server.

LBAC

: Lihat kontrol akses berbasis label.

hak istimewa paling sedikit

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

angkat dan geser

Lihat 7 Rs.

sistem endian kecil

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

LLM

Lihat model bahasa besar.

lingkungan yang lebih rendah

Lihat lingkungan.

M

pembelajaran mesin (ML)

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

cabang utama

Lihat cabang.

malware

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

layanan terkelola

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

sistem eksekusi manufaktur (MES)

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

PETA

Lihat Program Percepatan Migrasi.

mekanisme

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

akun anggota

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

MES

Lihat sistem eksekusi manufaktur.

Transportasi Telemetri Antrian Pesan (MQTT)

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

layanan mikro

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

informasi selengkapnya, lihat Mengintegrasikan layanan mikro dengan menggunakan layanan tanpa AWS server.

arsitektur microservices

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

Program Percepatan Migrasi (MAP)

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

migrasi dalam skala

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

pabrik migrasi

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

metadata migrasi

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

pola migrasi

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

Penilaian Portofolio Migrasi (MPA)

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

Penilaian Kesiapan Migrasi (MRA)

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

strategi migrasi

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

ML

Lihat pembelajaran mesin.

modernisasi

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

penilaian kesiapan modernisasi

Evaluasi yang membantu menentukan kesiapan modernisasi aplikasi organisasi; mengidentifikasi manfaat, risiko, dan dependensi; dan menentukan seberapa baik organisasi dapat mendukung keadaan masa depan aplikasi tersebut. Hasil penilaian adalah cetak biru arsitektur target, peta

jalan yang merinci fase pengembangan dan tonggak untuk proses modernisasi, dan rencana aksi untuk mengatasi kesenjangan yang diidentifikasi. Untuk informasi lebih lanjut, lihat Mengevaluasi kesiapan modernisasi untuk aplikasi di. AWS Cloud

aplikasi monolitik (monolit)

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

MPA

Lihat Penilaian Portofolio Migrasi.

MQTT

Lihat Transportasi Telemetri Antrian Pesan.

klasifikasi multiclass

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

infrastruktur yang bisa berubah

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

O

OAC

Lihat kontrol akses asal.

OAI

Lihat identitas akses asal.

OCM

Lihat manajemen perubahan organisasi.

migrasi offline

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

OI

Lihat integrasi operasi.

OLA

Lihat perjanjian tingkat operasional.

migrasi online

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

OPC-UA

Lihat Komunikasi Proses Terbuka - Arsitektur Terpadu.

Komunikasi Proses Terbuka - Arsitektur Terpadu (OPC-UA)

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

perjanjian tingkat operasional (OLA)

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

Tinjauan Kesiapan Operasional (ORR)

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

teknologi operasional (OT)

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

integrasi operasi (OI)

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

jejak organisasi

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

manajemen perubahan organisasi (OCM)

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

kontrol akses asal (OAC)

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

identitas akses asal (OAI)

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

ORR

Lihat tinjauan kesiapan operasional.

OT

Lihat teknologi operasional.

keluar (jalan keluar) VPC

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

P

batas izin

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

Informasi Identifikasi Pribadi (PII)

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

PII

Lihat informasi yang dapat diidentifikasi secara pribadi.

buku pedoman

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

PLC

Lihat pengontrol logika yang dapat diprogram.

PLM

Lihat manajemen siklus hidup produk.

kebijakan

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

ketekunan poliglot

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

penilaian portofolio

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

predikat

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

predikat pushdown

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

kontrol preventif

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

principal

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

privasi berdasarkan desain

Pendekatan rekayasa sistem yang memperhitungkan privasi melalui seluruh proses pengembangan.

zona yang dihosting pribadi

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

kontrol proaktif

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

manajemen siklus hidup produk (PLM)

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

lingkungan produksi

Lihat lingkungan.

pengontrol logika yang dapat diprogram (PLC)

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

rantai cepat

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

pseudonimisasi

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

publish/subscribe (pub/sub)

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

Q

rencana kueri

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

regresi rencana kueri

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

R

Matriks RACI

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

LAP

Lihat Retrieval Augmented Generation.

ransomware

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

Matriks RASCI

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

RCAC

Lihat kontrol akses baris dan kolom.

replika baca

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

arsitek ulang

Lihat 7 Rs.

tujuan titik pemulihan (RPO)

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

tujuan waktu pemulihan (RTO)

Penundaan maksimum yang dapat diterima antara gangguan layanan dan pemulihan layanan.

refactor

Lihat 7 Rs.

Wilayah

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

regresi

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

rehost

Lihat 7 Rs.

melepaskan

Dalam proses penyebaran, tindakan mempromosikan perubahan pada lingkungan produksi.

memindahkan

Lihat 7 Rs.

memplatform ulang

Lihat 7 Rs.

pembelian kembali

Lihat 7 Rs.

ketahanan

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

kebijakan berbasis sumber daya

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

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

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

kontrol responsif

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

melestarikan

Lihat 7 Rs.

pensiun

Lihat 7 Rs.

Retrieval Augmented Generation (RAG)

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

rotasi

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

kontrol akses baris dan kolom (RCAC)

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

RPO

Lihat tujuan titik pemulihan.

RTO

Lihat tujuan waktu pemulihan.

buku runbook

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

D

SAML 2.0

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

SCADA

Lihat kontrol pengawasan dan akuisisi data.

SCP

Lihat kebijakan kontrol layanan.

Rahasia

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

keamanan dengan desain

Pendekatan rekayasa sistem yang memperhitungkan keamanan melalui seluruh proses pengembangan.

kontrol keamanan

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

pengerasan keamanan

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

sistem informasi keamanan dan manajemen acara (SIEM)

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

otomatisasi respons keamanan

Tindakan yang telah ditentukan dan diprogram yang dirancang untuk secara otomatis merespons atau memulihkan peristiwa keamanan. Otomatisasi ini berfungsi sebagai kontrol keamanan

detektif atau responsif yang membantu Anda menerapkan praktik terbaik AWS keamanan. Contoh tindakan respons otomatis termasuk memodifikasi grup keamanan VPC, menambal instans EC2 Amazon, atau memutar kredensil.

enkripsi sisi server

Enkripsi data di tujuannya, oleh Layanan AWS yang menerimanya.

kebijakan kontrol layanan (SCP)

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

titik akhir layanan

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

perjanjian tingkat layanan (SLA)

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

indikator tingkat layanan (SLI)

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

tujuan tingkat layanan (SLO)

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

model tanggung jawab bersama

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

SIEM

Lihat informasi keamanan dan sistem manajemen acara.

titik kegagalan tunggal (SPOF)

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

SLA

Lihat perjanjian tingkat layanan.

SLI

Lihat indikator tingkat layanan.

SLO

Lihat tujuan tingkat layanan.

split-and-seed model

Pola untuk menskalakan dan mempercepat proyek modernisasi. Ketika fitur baru dan rilis produk didefinisikan, tim inti berpisah untuk membuat tim produk baru. Ini membantu meningkatkan kemampuan dan layanan organisasi Anda, meningkatkan produktivitas pengembang, dan mendukung inovasi yang cepat. Untuk informasi lebih lanjut, lihat Pendekatan bertahap untuk memodernisasi aplikasi di. AWS Cloud

SPOF

Lihat satu titik kegagalan.

skema bintang

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

pola ara pencekik

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

subnet

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

kontrol pengawasan dan akuisisi data (SCADA)

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

enkripsi simetris

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

pengujian sintetis

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

sistem prompt

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

T

tag

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

variabel target

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

daftar tugas

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

lingkungan uji

Lihat lingkungan.

pelatihan

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

gerbang transit

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

alur kerja berbasis batang

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

akses tepercaya

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

penyetelan

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

tim dua pizza

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

U

waswas

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

tugas yang tidak terdiferensiasi

Juga dikenal sebagai angkat berat, pekerjaan yang diperlukan untuk membuat dan mengoperasikan aplikasi tetapi itu tidak memberikan nilai langsung kepada pengguna akhir atau memberikan keunggulan kompetitif. Contoh tugas yang tidak terdiferensiasi termasuk pengadaan, pemeliharaan, dan perencanaan kapasitas.

lingkungan atas

Lihat lingkungan.

V

menyedot debu

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

kendali versi

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

Peering VPC

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

kerentanan

Kelemahan perangkat lunak atau perangkat keras yang membahayakan keamanan sistem.

W

cache hangat

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

data hangat

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

fungsi jendela

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

beban kerja

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

aliran kerja

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

CACING

Lihat menulis sekali, baca banyak.

WQF

Lihat AWS Kerangka Kualifikasi Beban Kerja.

tulis sekali, baca banyak (WORM)

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

Z

eksploitasi zero-day

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

kerentanan zero-day

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

bisikan zero-shot

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

aplikasi zombie

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

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