



AWS Dasar Keamanan Startup

AWS Bimbingan Preskriptif



AWS Bimbingan Preskriptif: AWS Dasar Keamanan Startup

Copyright © 2024 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
Audiens yang dituju	1
Kerangka dasar dan tanggung jawab keamanan	2
Mengamankan akun Anda	3
ACCT.01 Tetapkan kontak tingkat akun	3
ACCT.02 Batasi penggunaan pengguna root	4
ACCT.03 Konfigurasi akses konsol	5
ACCT.04 Tetapkan izin	6
ACCT.05 Membutuhkan MFA	7
ACCT.06 Menerapkan kebijakan kata sandi	8
ACCT.07 Log peristiwa	9
ACCT.08 Mencegah akses publik ke bucket S3 pribadi	10
ACCT.09 Hapus sumber daya yang tidak digunakan	11
ACCT.10 Biaya monitor	11
ACCT.11 Aktifkan GuardDuty	12
ACCT.12 Memantau masalah berisiko tinggi	12
Mengamankan beban kerja Anda	14
WKLD.01 Gunakan IAM peran untuk izin	14
WKLD.02 Gunakan kebijakan berbasis sumber daya	15
WKLD.03 Gunakan rahasia singkat atau layanan manajemen rahasia	16
WKLD.04 Lindungi rahasia aplikasi	17
WKLD.05 Mendeteksi dan memulihkan rahasia yang terungkap	18
WKLD.06 Gunakan Systems Manager alih-alih SSH atau RDP	18
WKLD.07 Log peristiwa data untuk bucket S3 tertentu	19
WKLD.08 Enkripsi volume Amazon EBS	20
WKLD.09 Enkripsi basis data Amazon RDS	21
WKLD.10 Menyebarkan sumber daya pribadi di subnet pribadi	21
WKLD.11 Gunakan grup keamanan untuk membatasi akses	21
WKLD.12 Gunakan VPC titik akhir untuk mengakses layanan	23
WKLD.13 Memerlukan HTTPS semua titik akhir web publik	24
WKLD.14 Gunakan layanan perlindungan tepi untuk titik akhir publik	25
WKLD.15 Gunakan template untuk menerapkan kontrol keamanan	26
Kontributor	27
Riwayat dokumen	28

Glosarium	30
#	30
A	31
B	34
C	36
D	39
E	43
F	45
G	47
H	48
I	49
L	52
M	53
O	57
P	60
Q	63
R	63
D	66
T	70
U	72
V	72
W	73
Z	74
.....	lxxv

AWS Dasar Keamanan Startup

Amazon Web Services ([kontributor](#))

Mei 2023 ([riwayat dokumen](#))

AWS Startup Security Baseline (AWS SSB) adalah seperangkat kontrol yang menciptakan fondasi minimum bagi bisnis untuk membangun dengan aman AWS tanpa mengurangi kelincahan mereka. Kontrol ini membentuk dasar dari postur keamanan Anda dan difokuskan pada pengamanan kredensial, memungkinkan pencatatan dan visibilitas, mengelola informasi kontak, dan menerapkan batasan data dasar.

Kontrol dalam panduan ini dirancang dengan mempertimbangkan startup awal, mengurangi risiko keamanan yang paling umum tanpa memerlukan upaya yang signifikan. Banyak startup memulai perjalanan mereka AWS Cloud dengan satu. Akun AWS Seiring pertumbuhan organisasi, mereka bermigrasi ke arsitektur multi-akun. Panduan dalam panduan ini dirancang untuk arsitektur akun tunggal, tetapi membantu Anda mengatur kontrol keamanan yang mudah dimigrasi atau dimodifikasi saat Anda beralih ke arsitektur multi-akun.

Kontrol di AWS SSB dipisahkan menjadi dua kategori: akun dan beban kerja. Kontrol akun membantu menjaga Akun AWS keamanan Anda. Ini termasuk rekomendasi untuk mengatur akses pengguna, kebijakan, dan izin, dan itu termasuk rekomendasi untuk cara memantau akun Anda untuk aktivitas yang tidak sah atau berpotensi berbahaya. Kontrol beban kerja membantu mengamankan sumber daya dan kode Anda di cloud, seperti aplikasi, proses backend, dan data. Ini termasuk rekomendasi seperti enkripsi dan mengurangi ruang lingkup akses.

Note

Beberapa kontrol yang direkomendasikan dalam panduan ini menggantikan default yang dikonfigurasi selama penyiapan awal, sementara sebagian besar mengonfigurasi pengaturan dan kebijakan baru. Dokumen ini sama sekali tidak boleh dianggap komprehensif dari semua kontrol yang tersedia.

Audiens yang dituju

Panduan ini paling cocok untuk startup yang berada di tahap awal pengembangan, dengan staf dan operasi minimal.

Startup atau bisnis lain yang berada dalam tahap operasi dan pertumbuhan selanjutnya masih dapat memperoleh nilai yang signifikan dari meninjau kontrol ini terhadap praktik mereka saat ini. Jika Anda mengidentifikasi celah, Anda dapat menerapkan kontrol individu dalam panduan ini dan kemudian mengevaluasinya untuk kesesuaian sebagai solusi jangka panjang.

Note

Kontrol yang direkomendasikan dalam panduan ini bersifat mendasar. Startup atau perusahaan lain yang beroperasi pada tahap skala atau kecanggihan selanjutnya harus menambahkan kontrol tambahan sebagaimana berlaku.

Kerangka dasar dan tanggung jawab keamanan

[AWS Well-Architected](#) membantu arsitek cloud membangun infrastruktur yang aman, berkinerja tinggi, tangguh, dan efisien untuk aplikasi dan beban kerja mereka. AWS Startup Security Baseline sejalan dengan [pilar keamanan](#) dari AWS Well-Architected Framework. Pilar keamanan menjelaskan cara memanfaatkan teknologi cloud untuk melindungi data, sistem, dan aset dengan cara yang dapat meningkatkan postur keamanan Anda. Ini membantu Anda memenuhi persyaratan bisnis dan peraturan Anda dengan mengikuti AWS rekomendasi saat ini.

Anda dapat menilai kepatuhan Anda terhadap praktik terbaik Well-Architected dengan menggunakan in Anda. [AWS Well-Architected Tool](#) Akun AWS

Keamanan dan kepatuhan adalah tanggung jawab bersama antara AWS dan pelanggan. [Model tanggung jawab bersama](#) sering dijelaskan dengan mengatakan bahwa AWS bertanggung jawab atas keamanan cloud (yaitu, untuk melindungi infrastruktur yang menjalankan semua layanan yang ditawarkan di AWS Cloud), dan Anda bertanggung jawab atas keamanan di cloud (sebagaimana ditentukan oleh AWS Cloud layanan yang Anda pilih). Dalam model tanggung jawab bersama, menerapkan kontrol keamanan dalam dokumen ini adalah bagian dari tanggung jawab Anda sebagai pelanggan.

Mengamankan akun Anda

Kontrol dan rekomendasi di bagian ini membantu menjaga keamanan AWS akun Anda. Ini menekankan penggunaan AWS Identity and Access Management (IAM) pengguna, kelompok pengguna, dan peran (juga dikenal sebagai prinsipal) untuk akses manusia dan mesin, membatasi penggunaan pengguna root, dan membutuhkan otentikasi multi-faktor. Di bagian ini, Anda mengonfirmasi bahwa AWS memiliki informasi kontak yang diperlukan untuk menghubungi Anda mengenai aktivitas dan status akun Anda. Anda juga menyiapkan layanan pemantauan, seperti, Amazon AWS Trusted Advisor, dan GuardDuty AWS Budgets, sehingga Anda diberi tahu tentang aktivitas di akun Anda dan dapat merespons dengan cepat jika aktivitas tersebut tidak sah atau tidak terduga.

Bagian ini berisi topik berikut:

- [ACCT.01 Setel kontak tingkat akun ke daftar distribusi email yang valid](#)
- [ACCT.02 Batasi penggunaan pengguna root](#)
- [ACCT.03 Konfigurasi akses konsol untuk setiap pengguna](#)
- [ACCT.04 Tetapkan izin](#)
- [ACCT.05 Memerlukan otentikasi multi-faktor untuk masuk](#)
- [ACCT.06 Menerapkan kebijakan kata sandi](#)
- [ACCT.07 Mengirimkan CloudTrail log ke bucket S3 yang dilindungi](#)
- [ACCT.08 Mencegah akses publik ke bucket S3 pribadi](#)
- [ACCT.09 Hapus kelompok yang tidak terpakai VPCs, subnet, dan keamanan](#)
- [ACCT.10 Konfigurasi AWS Budgets untuk memantau pengeluaran Anda](#)
- [ACCT.11 Aktifkan dan tanggapilah notifikasi GuardDuty](#)
- [ACCT.12 Memantau dan menyelesaikan masalah berisiko tinggi dengan menggunakan Trusted Advisor](#)

ACCT.01 Setel kontak tingkat akun ke daftar distribusi email yang valid

Saat menyiapkan kontak utama dan alternatif untuk AWS akun Anda, gunakan daftar distribusi email alih-alih alamat email individu. Menggunakan daftar distribusi email memastikan bahwa kepemilikan

dan jangkauan dipertahankan saat individu di organisasi Anda datang dan pergi. Tetapkan kontak alternatif untuk pemberitahuan penagihan, operasi, dan keamanan, dan gunakan daftar distribusi email yang sesuai. AWS menggunakan alamat email ini untuk menghubungi Anda, jadi penting bagi Anda untuk tetap mengaksesnya.

Untuk mengedit nama akun Anda, kata sandi pengguna akar, dan alamat email pengguna akar

1. Masuk ke halaman Pengaturan Akun di konsol [Billing and Cost Management](#).
2. Pada halaman Pengaturan Akun, di samping Pengaturan Akun, memilih Mengedit.
3. Di samping bidang yang ingin Anda perbarui, pilih Edit.
4. Setelah Anda memasukkan perubahan, memilih Simpan perubahan.
5. Setelah Anda selesai membuat semua perubahan, memilih Selesai.

Untuk mengedit informasi kontak Anda

1. Pada halaman [Pengaturan Akun](#), di bawah Informasi Kontak, pilih Edit.
2. Untuk bidang yang ingin Anda ubah, masukkan informasi terbaru Anda, lalu pilih Perbarui.

Untuk menambahkan, memperbarui, atau menghapus kontak alternatif

1. Pada halaman [Pengaturan Akun](#), di bawah Kontak Alternatif, pilih Edit.
2. Untuk bidang yang ingin Anda ubah, masukkan informasi terbaru Anda, lalu pilih Perbarui.

ACCT.02 Batasi penggunaan pengguna root

Pengguna root dibuat saat Anda mendaftar untuk AWS akun, dan pengguna ini memiliki hak kepemilikan penuh dan izin atas akun yang tidak dapat diubah. Hanya gunakan pengguna root untuk tugas-tugas tertentu yang membutuhkannya. Untuk informasi selengkapnya, lihat [Tugas yang memerlukan kredensi pengguna root](#) (IAM dokumentasi). Lakukan semua tindakan lain di akun Anda dengan menggunakan jenis IAM identitas lain, seperti pengguna gabungan dengan IAM peran. Untuk informasi selengkapnya, lihat [kredensi AWS keamanan](#) (IAM dokumentasi).

Untuk membatasi penggunaan pengguna root

1. Memerlukan otentikasi multi-faktor (MFA) untuk pengguna root seperti yang dijelaskan dalam [ACCT.05 Memerlukan otentikasi multi-faktor untuk masuk](#)

2. Buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Untuk informasi selengkapnya tentang mengonfigurasi akses pengguna, lihat [ACCT.03 Konfigurasi akses konsol untuk setiap pengguna](#).

ACCT.03 Konfigurasi akses konsol untuk setiap pengguna

Sebagai praktik terbaik, AWS merekomendasikan penggunaan kredensial sementara untuk memberikan akses Akun AWS dan sumber daya. Kredensial sementara memiliki masa pakai yang terbatas, jadi Anda tidak perlu memutarinya atau mencabutnya secara eksplisit saat tidak lagi diperlukan. Untuk informasi selengkapnya, lihat [Kredensial keamanan sementara](#) (IAMdokumentasi).

Untuk pengguna manusia, AWS merekomendasikan untuk menggunakan identitas federasi dari penyedia identitas terpusat (iDP), seperti, Okta, Active Directory AWS IAM Identity Center, atau Ping Identity. Pengguna federasi memungkinkan Anda menentukan identitas di satu lokasi terpusat, dan pengguna dapat mengautentikasi dengan aman ke beberapa aplikasi dan situs web, termasuk AWS, hanya dengan menggunakan satu set kredensial. Untuk informasi lebih lanjut, lihat [Federasi identitas di AWS](#) dan [Pusat IAM Identitas](#) (AWS situs web).

Note

Federasi identitas dapat mempersulit transisi dari arsitektur akun tunggal ke arsitektur multi-akun. Adalah umum bagi startup untuk menunda penerapan federasi identitas sampai mereka telah membentuk arsitektur multi-akun yang dikelola. AWS Organizations

Untuk mengatur federasi identitas

1. Jika Anda menggunakan Pusat IAM Identitas, lihat [Memulai](#) (dokumentasi Pusat IAM Identitas).
Jika Anda menggunakan iDP eksternal atau pihak ketiga, lihat [Membuat penyedia IAM identitas](#) (IAMdokumentasi).
2. Pastikan bahwa IDP Anda memberlakukan otentikasi multi-faktor (). MFA
3. Terapkan izin sesuai dengan. [ACCT.04 Tetapkan izin](#)

Untuk startup yang tidak siap untuk mengkonfigurasi federasi identitas, Anda dapat membuat pengguna langsung di IAM. Ini bukan praktik terbaik keamanan yang direkomendasikan karena ini adalah kredensial jangka panjang yang tidak pernah kedaluwarsa. Namun, ini adalah praktik umum

untuk startup dalam operasi awal untuk mencegah kesulitan transisi ke arsitektur multi-akun ketika mereka siap secara operasional.

Sebagai baseline, Anda dapat membuat IAM pengguna untuk setiap orang yang perlu mengakses. AWS Management Console Jika Anda mengonfigurasi IAM pengguna, jangan bagikan kredensial di seluruh pengguna, dan putar kredensi jangka panjang secara teratur.

Warning

IAM pengguna memiliki kredensi jangka panjang, yang menghadirkan risiko keamanan. Untuk membantu mengurangi risiko ini, kami menyarankan agar Anda memberikan pengguna ini hanya izin yang mereka perlukan untuk melakukan tugas dan menghapus pengguna ini ketika mereka tidak lagi diperlukan.

Untuk membuat IAM pengguna

1. [Buat IAM pengguna](#) (IAM dokumentasi).
2. Terapkan izin sesuai dengan [ACCT.04 Tetapkan izin](#)

ACCT.04 Tetapkan izin

Konfigurasi izin pengguna di akun dengan menetapkan kebijakan ke IAM identitas mereka (grup pengguna atau peran). Anda dapat menyesuaikan izin, atau Anda dapat melampirkan [kebijakan AWS terkelola](#), yang merupakan kebijakan mandiri yang dirancang AWS untuk memberikan izin bagi banyak kasus penggunaan umum. Jika Anda menyesuaikan izin, ikuti praktik terbaik keamanan untuk [memberikan hak istimewa paling sedikit](#). Keistimewaan paling sedikit adalah praktik pemberian izin minimum yang dibutuhkan setiap pengguna untuk melakukan tugas mereka.

Jika Anda menggunakan identitas federasi, pengguna mengakses akun dengan mengambil IAM peran melalui penyedia identitas eksternal. IAM Peran menentukan apa yang diizinkan dilakukan oleh pengguna yang diautentikasi oleh IDP organisasi Anda. AWS Anda menerapkan kebijakan khusus atau AWS terkelola ke peran ini untuk mengonfigurasi izin.

Untuk menetapkan izin untuk identitas federasi

- Jika Anda menggunakan Pusat IAM Identitas, lihat [Menggunakan IAM kebijakan dalam kumpulan izin](#) (dokumentasi Pusat IAM Identitas).

Jika Anda menggunakan iDP eksternal atau pihak ketiga, lihat [Menambahkan izin IAM identitas \(IAMdokumentasi\)](#).

Jika Anda menggunakan IAM pengguna, Anda dapat menggunakan grup atau peran pengguna untuk mengelola izin bagi beberapa IAM pengguna. Kami merekomendasikan grup pengguna untuk startup karena mereka lebih mudah dikelola dan tidak terlalu rentan terhadap kesalahan konfigurasi yang dapat menimbulkan risiko keamanan bagi akun Anda. Tetapkan pengguna ke grup pengguna berdasarkan fungsi pekerjaan mereka. Contoh kelompok pengguna termasuk insinyur aplikasi, data, jaringan, dan Operasi Pengembangan (DevOps). Anda juga dapat membagi tipe pengguna menjadi kelompok pengguna yang lebih kecil berdasarkan otoritas pengambilan keputusan, seperti untuk insinyur senior atau non-senior.

Untuk menetapkan izin bagi pengguna IAM

1. [Buat grup IAM pengguna](#) (IAMdokumentasi).
2. [Lampirkan kebijakan AWS terkelola ke grup IAM pengguna](#) (IAMdokumentasi).

ACCT.05 Memerlukan otentikasi multi-faktor untuk masuk

Dengan otentikasi multi-faktor (MFA), pengguna memiliki perangkat yang menghasilkan respons terhadap tantangan otentikasi. Setiap kredensi pengguna dan respons yang dihasilkan perangkat diperlukan untuk menyelesaikan proses masuk. Sebagai praktik terbaik keamanan, aktifkan MFA Akun AWS akses, terutama untuk kredensial jangka panjang seperti pengguna root akun dan IAM pengguna.

Untuk mengatur MFA untuk pengguna root

1. Masuk ke [AWS Management Console](#).
2. Di sisi kanan bilah navigasi, pilih nama akun Anda, lalu pilih Kredensial Keamanan Saya.
3. Jika perlu, pilih Lanjutkan ke Kredensial Keamanan.
4. Perluas bagian Multi-Factor Authentication (MFA).
5. Pilih AktifkanMFA.
6. Ikuti petunjuk panduan untuk mengonfigurasi MFA perangkat Anda sesuai dengan itu. Untuk informasi selengkapnya, lihat [Autentikasi AWS multi-faktor di IAM](#) (IAMdokumentasi).

Untuk mengatur MFA di Pusat IAM Identitas

- [Aktifkan MFA](#) (dokumentasi Pusat IAM Identitas)

Untuk mengatur MFA untuk IAM pengguna Anda sendiri

1. [Dengan menggunakan kredensial masuk Anda, masuk ke konsol. IAM](#)
2. Di bilah navigasi di kanan atas, pilih nama pengguna Anda, dan kemudian pilih Kredensial Keamanan Saya.
3. Pada tab AWS IAMkredensial, di bagian Autentikasi multi-faktor, pilih Kelola perangkat. MFA

Untuk mengatur MFA untuk IAM pengguna lain

1. Masuk ke AWS Management Console dan buka [IAMkonsol](#).
2. Di panel navigasi, pilih Pengguna.
3. Pilih nama pengguna yang ingin Anda aktifkanMFA, lalu pilih tab Security credentials.
4. Di samping MFAPerangkat yang Ditugaskan, pilih Kelola.
5. Ikuti petunjuk panduan untuk mengonfigurasi MFA perangkat Anda sesuai dengan itu. Untuk informasi selengkapnya, lihat [Autentikasi AWS multi-faktor di IAM](#) (IAMdokumentasi).

ACCT.06 Menerapkan kebijakan kata sandi

Pengguna masuk ke AWS Management Console dengan memberikan kredensial masuk, dan MFA direkomendasikan. Mengharuskan kata sandi mematuhi kebijakan kata sandi yang kuat untuk membantu mencegah penemuan melalui kekerasan atau rekayasa sosial.

Untuk informasi selengkapnya tentang rekomendasi terbaru untuk kata sandi yang kuat, lihat [Panduan Kebijakan Kata Sandi](#) di situs web Center for Internet Security (CIS).

Untuk IAM pengguna, Anda dapat mengonfigurasi persyaratan kata sandi dalam kebijakan IAM kata sandi khusus. Untuk informasi selengkapnya, lihat [Menyetel kebijakan kata sandi akun](#) (IAMdokumentasi).

Untuk membuat kebijakan kata sandi khusus

1. Masuk ke AWS Management Console dan buka [IAMkonsol](#).

2. Di panel navigasi, pilih Pengaturan akun.
3. Di bagian Kebijakan kata sandi, pilih Ubah kebijakan kata sandi.
4. Pilih opsi yang ingin Anda terapkan pada kebijakan kata sandi Anda, lalu pilih Simpan perubahan.

ACCT.07 Mengirimkan CloudTrail log ke bucket S3 yang dilindungi

Tindakan yang diambil oleh pengguna, peran, dan layanan di AWS akun Anda dicatat sebagai peristiwa di AWS CloudTrail. CloudTrail diaktifkan secara default, dan di CloudTrail konsol, Anda dapat mengakses 90 hari informasi riwayat acara. Untuk melihat, mencari, mengunduh, mengarsipkan, menganalisis, dan menanggapi aktivitas akun di seluruh AWS infrastruktur Anda, lihat [Melihat peristiwa dengan riwayat CloudTrail Acara](#) (CloudTrail dokumentasi).

Untuk menyimpan CloudTrail riwayat lebih dari 90 hari dengan data tambahan, Anda membuat jejak baru yang mengirimkan file log ke bucket Amazon Simple Storage Service (Amazon S3) untuk semua jenis peristiwa. Saat membuat jejak di CloudTrail konsol, Anda membuat jejak multi-wilayah.

Untuk membuat jejak yang mengirimkan log untuk semua Wilayah AWS ke bucket S3

1. [Buat jejak](#) (CloudTrail dokumentasi). Pada halaman Pilih peristiwa log, lakukan hal berikut:
 - a. Untuk API aktivitas, pilih Baca dan Tulis.
 - b. Untuk lingkungan praproduksi, pilih Kecualikan AWS KMS peristiwa. Ini mengecualikan semua AWS Key Management Service (AWS KMS) peristiwa dari jejak Anda. AWS KMS membaca tindakan seperti Encrypt, Decrypt, dan GenerateDataKey dapat menghasilkan volume besar peristiwa.

Untuk lingkungan produksi, pilih untuk mencatat peristiwa manajemen Tulis, dan kosongkan kotak centang untuk Kecualikan AWS KMS peristiwa. Ini tidak termasuk peristiwa AWS KMS baca volume tinggi tetapi masih mencatat peristiwa penulisan yang relevan, seperti, DisableDelete, dan. ScheduleKey Ini adalah pengaturan AWS KMS pencatatan minimum yang disarankan untuk lingkungan produksi.

2. Jejak baru muncul di halaman Trails. Dalam waktu sekitar 15 menit, CloudTrail menerbitkan file log yang menunjukkan panggilan antarmuka pemrograman AWS aplikasi (API) yang dilakukan di akun Anda. Anda dapat melihat file log di bucket S3 yang Anda tentukan.

Untuk membantu mengamankan bucket S3 tempat Anda menyimpan file log CloudTrail

1. Tinjau [kebijakan bucket Amazon S3](#) (CloudTrail dokumentasi) untuk setiap dan semua bucket tempat Anda menyimpan file log dan sesuaikan sesuai kebutuhan untuk menghapus akses yang tidak perlu.
2. Sebagai praktik keamanan terbaik, pastikan untuk menambahkan kunci `aws:SourceArn` kondisi secara manual ke kebijakan bucket. Untuk informasi selengkapnya, lihat [Membuat atau memperbarui bucket Amazon S3 yang akan digunakan untuk menyimpan file log untuk jejak organisasi](#) (CloudTrail dokumentasi).
3. [Aktifkan MFA Hapus](#) (dokumentasi Amazon S3).

ACCT.08 Mencegah akses publik ke bucket S3 pribadi

Secara default, hanya pengguna root Akun AWS dan IAM prinsipal, jika digunakan, memiliki izin untuk membaca dan menulis ke bucket Amazon S3 yang dibuat oleh prinsipal tersebut. IAMPrinsipal tambahan diberikan akses dengan menggunakan kebijakan berbasis identitas, dan kondisi akses dapat diberlakukan dengan menggunakan kebijakan bucket. Anda dapat membuat kebijakan bucket yang memberikan akses publik umum ke bucket, ember publik.

Bucket yang dibuat pada atau setelah 28 April 2023 mengaktifkan pengaturan Blokir Akses Publik secara default. Untuk bucket yang dibuat sebelum tanggal ini, pengguna mungkin salah mengonfigurasi kebijakan bucket dan secara tidak sengaja memberikan akses ke publik. Anda dapat mencegah kesalahan konfigurasi ini dengan mengaktifkan pengaturan Blokir Akses Publik untuk setiap bucket. Jika Anda tidak memiliki kasus penggunaan saat ini atau masa depan untuk bucket S3 publik, aktifkan pengaturan ini di Akun AWS level tersebut. Setelan ini mencegah kebijakan yang mengizinkan akses publik.

Untuk mencegah akses publik ke bucket S3

- [Konfigurasi blokir setelan akses publik untuk bucket S3 Anda](#) (dokumentasi Amazon S3).

AWS Trusted Advisor menghasilkan temuan kuning untuk bucket S3 yang memungkinkan daftar atau akses baca ke publik dan menghasilkan temuan merah untuk ember yang memungkinkan unggahan atau penghapusan publik. Sebagai garis dasar, ikuti kontrol [ACCT.12 Memantau dan menyelesaikan masalah berisiko tinggi dengan menggunakan Trusted Advisor](#) untuk mengidentifikasi dan memperbaiki bucket yang salah konfigurasi. Bucket S3 yang dapat diakses publik juga ditunjukkan di konsol Amazon S3.

ACCT.09 Hapus kelompok yang tidak terpakai VPCs, subnet, dan keamanan

Untuk mengurangi kemungkinan masalah keamanan, hapus atau matikan sumber daya apa pun yang tidak digunakan. Di AWS akun baru, secara default virtual private cloud (VPC) dibuat secara otomatis di setiap akun Wilayah AWS, yang memungkinkan Anda menetapkan alamat IP publik di subnet publik. Namun, jika ini tidak VPCs diperlukan, ini menimbulkan risiko paparan sumber daya yang tidak diinginkan.

Jika tidak digunakan, hapus default VPCs di semua Wilayah, bukan hanya di Wilayah tempat Anda dapat menerapkan beban kerja. Menghapus VPC juga menghapus komponennya, seperti subnet dan grup keamanan.

Note

Anda dapat melihat semua Wilayah dan VPCs di [konsol Amazon EC2 Global View](#). Untuk informasi selengkapnya, lihat [Daftar dan filter sumber daya di seluruh Wilayah menggunakan Amazon EC2 Global View](#) (EC2 dokumentasi Amazon).

Untuk menghapus default yang tidak digunakan VPCs

1. [Hapus VPC \(VPC dokumentasi Amazon\) Anda](#).
2. Ulangi sesuai kebutuhan VPCs di Wilayah lain.

ACCT.10 Konfigurasi AWS Budgets untuk memantau pengeluaran Anda

AWS Budgets memungkinkan pemantauan biaya bulanan dan penggunaan dengan pemberitahuan ketika biaya diperkirakan melebihi ambang batas target. Pemberitahuan biaya yang diperkirakan dapat memberikan indikasi aktivitas tak terduga, memberikan pertahanan ekstra selain sistem pemantauan lainnya, seperti AWS Trusted Advisor dan Amazon GuardDuty. Memantau dan memahami AWS biaya Anda juga merupakan bagian dari kebersihan operasional yang baik.

Untuk mengatur anggaran di AWS Budgets

- [Buat anggaran biaya](#) (AWS Budgets dokumentasi).

ACCT.11 Aktifkan dan tanggapilah notifikasi GuardDuty

Amazon GuardDuty adalah layanan pendeteksi ancaman yang terus memantau perilaku berbahaya atau tidak sah untuk membantu melindungi AWS akun, beban kerja, dan data Anda. Ketika mendeteksi aktivitas yang tidak terduga dan berpotensi berbahaya, GuardDuty memberikan temuan keamanan terperinci untuk visibilitas dan remediasi. GuardDuty dapat mendeteksi ancaman seperti aktivitas penambangan cryptocurrency, akses dari klien dan relay Tor, perilaku tak terduga, dan kredensi yang dikompromikan IAM. Aktifkan GuardDuty dan tanggapilah temuan untuk menghentikan perilaku yang berpotensi berbahaya atau tidak sah di AWS lingkungan Anda. Untuk informasi selengkapnya tentang temuan di GuardDuty, lihat [Menemukan jenis](#) (GuardDuty dokumentasi).

Anda dapat menggunakan Amazon CloudWatch Events untuk menyiapkan notifikasi otomatis saat GuardDuty membuat temuan atau perubahan temuan. Pertama, Anda menyiapkan topik Amazon Simple Notification Service (Amazon SNS) dan menambahkan titik akhir, atau alamat email, ke topik tersebut. Kemudian, Anda menyiapkan CloudWatch acara untuk GuardDuty temuan, dan aturan acara memberi tahu titik akhir dalam topik Amazon SNS.

Untuk mengaktifkan GuardDuty dan GuardDuty pemberitahuan

1. [Aktifkan Amazon GuardDuty](#) (GuardDuty dokumentasi).
2. [Buat aturan CloudWatch Acara untuk memberi tahu Anda tentang GuardDuty temuan](#) (GuardDuty dokumentasi).

ACCT.12 Memantau dan menyelesaikan masalah berisiko tinggi dengan menggunakan Trusted Advisor

AWS Trusted Advisor memindai AWS infrastruktur Anda secara pasif untuk masalah berisiko tinggi atau berdampak tinggi yang terkait dengan keamanan, kinerja, biaya, dan keandalan. Ini memberikan informasi rinci tentang sumber daya yang terpengaruh dan rekomendasi remediasi. Untuk daftar lengkap cek dan deskripsi, lihat [AWS Trusted Advisor cek referensi](#) (Trusted Advisor dokumentasi).

Meninjau Trusted Advisor temuan secara berulang, dan memulihkan masalah yang diperlukan. Jika Anda memiliki paket AWS Business Support atau Enterprise Support, Anda dapat berlangganan email temuan mingguan. Untuk informasi selengkapnya, lihat [Mengatur preferensi notifikasi](#) (AWS Support dokumentasi).

Untuk melihat masalah di Trusted Advisor

- Tinjau setiap kategori cek sesuai dengan petunjuk di [Lihat kategori cek](#) (AWS Support dokumentasi). Minimal, kami sarankan untuk meninjau tindakan yang direkomendasikan masalah, yang berwarna merah.

Mengamankan beban kerja Anda

Kontrol dan rekomendasi di bagian ini membantu Anda mengamankan beban kerja Anda berjalan AWS, saat Anda sedang membangunnya. Mereka menekankan praktik aman untuk mengelola rahasia aplikasi dan ruang lingkup akses, meminimalkan rute akses ke sumber daya pribadi, dan menggunakan enkripsi untuk melindungi data dalam perjalanan dan saat istirahat.

Bagian ini berisi topik berikut:

- [WKLD.01 Gunakan IAM peran untuk menghitung izin lingkungan](#)
- [WKLD.02 Batasi cakupan penggunaan kredensi dengan izin kebijakan berbasis sumber daya](#)
- [WKLD.03 Gunakan rahasia singkat atau layanan manajemen rahasia](#)
- [WKLD.04 Mencegah rahasia aplikasi agar tidak terungkap](#)
- [WKLD.05 Mendeteksi dan memulihkan rahasia yang terungkap](#)
- [WKLD.06 Gunakan Systems Manager alih-alih SSH atau RDP](#)
- [WKLD.07 Log peristiwa data untuk bucket S3 dengan data sensitif](#)
- [WKLD.08 Enkripsi volume Amazon EBS](#)
- [WKLD.09 Enkripsi basis data Amazon RDS](#)
- [WKLD.10 Menyebarkan sumber daya pribadi ke subnet pribadi](#)
- [WKLD.11 Membatasi akses jaringan dengan menggunakan grup keamanan](#)
- [WKLD.12 Gunakan VPC titik akhir untuk mengakses layanan yang didukung](#)
- [WKLD.13 Memerlukan HTTPS semua titik akhir web publik](#)
- [WKLD.14 Gunakan layanan perlindungan tepi untuk titik akhir publik](#)
- [WKLD.15 Tentukan kontrol keamanan dalam template dan terapkan dengan menggunakan praktik CI/CD](#)

WKLD.01 Gunakan IAM peran untuk menghitung izin lingkungan

Dalam AWS Identity and Access Management (IAM), peran mewakili sekumpulan izin yang dapat diasumsikan oleh seseorang atau layanan untuk jangka waktu yang dapat dikonfigurasi. Menggunakan peran menghilangkan kebutuhan untuk menyimpan atau mengelola kredensial jangka panjang, secara signifikan mengurangi kemungkinan penggunaan yang tidak diinginkan. Tetapkan IAM peran langsung ke instans, AWS Fargate tugas dan layanan Amazon Elastic Compute Cloud EC2 (Amazon), AWS Lambda fungsi, dan layanan AWS komputasi lainnya kapan pun didukung.

Aplikasi yang menggunakan AWS SDK dan berjalan di lingkungan komputasi ini secara otomatis menggunakan kredensial IAM peran untuk otentikasi.

Pendekatan dan instruksi untuk menggunakan IAM peran untuk setiap layanan dapat ditemukan di [AWS Dokumentasi](#) untuk layanan. Misalnya, lihat yang berikut ini:

- [IAMperan untuk Amazon EC2](#) (EC2dokumentasi Amazon)
- [IAMperan untuk tugas](#) (dokumentasi Amazon Elastic Container Service)
- [Peran eksekusi Lambda \(dokumentasi Lambda\)](#)

WKLD.02 Batasi cakupan penggunaan kredensi dengan izin kebijakan berbasis sumber daya

Kebijakan adalah objek yang dapat menentukan izin atau menentukan kondisi akses. Ada dua jenis kebijakan utama:

- Kebijakan berbasis identitas dilampirkan ke kepala sekolah dan menentukan apa izin kepala sekolah di lingkungan. AWS
- Kebijakan berbasis sumber daya dilampirkan ke sumber daya, seperti bucket Amazon Simple Storage Service (Amazon S3), atau titik akhir virtual private cloud (). VPC Kebijakan ini menentukan prinsip mana yang diizinkan mengakses, tindakan yang didukung, dan kondisi lain yang harus dipenuhi.

Agar prinsipal diizinkan mengakses untuk melakukan tindakan terhadap sumber daya, ia harus memiliki izin yang diberikan dalam kebijakan berbasis identitas dan memenuhi persyaratan kebijakan berbasis sumber daya. Untuk informasi selengkapnya, lihat Kebijakan [berbasis identitas dan kebijakan berbasis sumber daya](#) (dokumentasi). IAM

Ketentuan yang disarankan untuk kebijakan berbasis sumber daya meliputi:

- Batasi akses hanya ke prinsipal dalam organisasi tertentu (didefinisikan dalam AWS Organizations) dengan menggunakan kondisi. `aws:PrincipalOrgID`
- Batasi akses ke lalu lintas yang berasal dari titik tertentu VPC atau VPC titik akhir dengan menggunakan `aws:SourceVpc` atau `aws:SourceVpce` kondisi, masing-masing.
- Izinkan atau tolak lalu lintas berdasarkan alamat IP sumber dengan menggunakan suatu `aws:SourceIp` kondisi.

Berikut ini adalah contoh kebijakan berbasis sumber daya yang menggunakan `aws:PrincipalOrgID` kondisi untuk mengizinkan hanya prinsipal di organisasi yang mengakses bucket S3: `<o-xxxxxxxxxxxx> <bucket-name>`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowFromOrganization",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::<bucket-name>/*",
      "Condition": {
        "StringEquals": {"aws:PrincipalOrgID": "<o-xxxxxxxxxxxx>"}
      }
    }
  ]
}
```

WKLD.03 Gunakan rahasia singkat atau layanan manajemen rahasia

Rahasia aplikasi sebagian besar terdiri dari kredensial, seperti pasangan kunci, token akses, sertifikat digital, dan kredensial masuk. Aplikasi ini menggunakan rahasia ini untuk mendapatkan akses ke layanan lain yang bergantung padanya, seperti database. Untuk membantu melindungi rahasia ini, kami menyarankan agar rahasia tersebut bersifat sementara (dihasilkan pada saat permintaan dan berumur pendek, seperti dengan IAM peran) atau diambil dari layanan manajemen rahasia. Ini mencegah paparan yang tidak disengaja melalui mekanisme yang kurang aman, seperti bertahan dalam file konfigurasi statis. Ini juga membuatnya lebih mudah untuk mempromosikan kode aplikasi dari pengembangan ke lingkungan produksi.

Untuk layanan manajemen rahasia, sebaiknya gunakan kombinasi Parameter Store, kemampuan, dan AWS Systems Manager: AWS Secrets Manager

- Gunakan Parameter Store untuk mengelola rahasia dan parameter lain yang merupakan pasangan nilai kunci individual, berbasis string, panjang keseluruhan pendek, dan sering diakses. Anda menggunakan kunci AWS Key Management Service (AWS KMS) untuk mengenkripsi rahasia. Tidak ada biaya untuk menyimpan parameter di tingkat standar Parameter Store. Untuk informasi

selengkapnya tentang tingkatan parameter, lihat [Mengelola tingkatan parameter \(dokumentasi Systems Manager\)](#).

- Gunakan Secrets Manager untuk menyimpan rahasia yang ada dalam bentuk dokumen (seperti beberapa pasangan nilai kunci terkait), berukuran lebih besar dari 4 KB (seperti sertifikat digital), atau akan mendapat manfaat dari rotasi otomatis.

Anda dapat menggunakan Parameter Store APIs untuk mengambil rahasia yang disimpan di Secrets Manager. Ini memungkinkan Anda untuk membakukan kode dalam aplikasi Anda saat menggunakan kombinasi kedua layanan.

Untuk mengelola rahasia di Parameter Store

1. [Buat AWS KMS kunci simetris](#) (AWS KMS dokumentasi).
2. [Buat SecureString parameter](#) (dokumentasi Systems Manager). Rahasia di Parameter Store menggunakan tipe SecureString data.
3. Dalam aplikasi Anda, ambil parameter dari Parameter Store dengan menggunakan AWS SDK untuk bahasa pemrograman Anda. Untuk contoh kode, lihat [GetParameter](#)(AWS SDKCode Library).

Untuk mengelola rahasia di Secrets Manager

1. [Buat rahasia](#) (dokumentasi Secrets Manager).
2. [Ambil rahasia dari AWS Secrets Manager dalam kode](#) (dokumentasi Secrets Manager).

Penting untuk dibaca [Gunakan pustaka caching AWS Secrets Manager sisi klien untuk meningkatkan ketersediaan dan latensi penggunaan rahasia Anda \(posting blog\)](#). AWS Menggunakan sisi klien SDKs, yang sudah menerapkan praktik terbaik, harus mempercepat dan menyederhanakan penggunaan dan integrasi Secrets Manager.

WKLD04 Mencegah rahasia aplikasi agar tidak terungkap

Selama pengembangan lokal, rahasia aplikasi dapat disimpan dalam konfigurasi lokal atau file kode dan secara tidak sengaja diperiksa ke repositori kode sumber. Repositori tidak aman yang dihosting di penyedia layanan publik dapat dikenakan akses tidak sah dan penemuan rahasia ini selanjutnya. Gunakan alat yang tersedia untuk mencegah rahasia diperiksa. Gabungkan pemeriksaan untuk rahasia yang terpapar sebagai bagian dari proses peninjauan kode manual Anda.

Beberapa alat umum yang dapat mencegah rahasia aplikasi diperiksa ke repositori kode sumber adalah:

- [Gitleaks \(repositori\)](#) GitHub
- [Whispers](#) (GitHubrepositori)
- [deteksi-rahasia](#) (repositori) GitHub
- [git-rahasia \(repositori\)](#) GitHub
- [TruffleHog](#)(GitHubrepositori)

WKLD.05 Mendeteksi dan memulihkan rahasia yang terungkap

Di dalam [WKLD.03 Gunakan rahasia singkat atau layanan manajemen rahasia](#) dan [WKLD04 Mencegah rahasia aplikasi agar tidak terungkap](#), Anda menempatkan langkah-langkah di tempat untuk melindungi rahasia. Dalam kontrol ini, Anda menerapkan solusi yang dapat mendeteksi jika rahasia telah melewati langkah-langkah pencegahan ini, dan Anda dapat memperbaikinya.

Amazon CodeGuru Reviewer mendeteksi rahasia aplikasi dalam kode sumber dan menyediakan mekanisme untuk memulihkan dan mempublikasikan rahasia yang terdeteksi di Secrets Manager. Kode aplikasi untuk mengambil rahasia dari Secrets Manager juga disediakan. Lakukan analisis biaya-manfaat untuk menentukan apakah solusi ini tepat untuk bisnis Anda. Sebagai alternatif, beberapa solusi open-source dalam [WKLD04 Mencegah rahasia aplikasi agar tidak terungkap](#) menyediakan kemampuan deteksi untuk rahasia yang ada.

Untuk mengatur integrasi CodeGuru Reviewer dengan Secrets Manager

- [Gunakan CodeGuru Reviewer untuk mengidentifikasi rahasia hardcode dan AWS Secrets Manager mengamankannya](#) (posting AWS blog dan panduan panduan).

WKLD.06 Gunakan Systems Manager alih-alih SSH atau RDP

Subnet publik, yang memiliki rute default yang menunjuk ke gateway internet, secara inheren merupakan risiko keamanan yang lebih besar daripada subnet pribadi, yang tidak memiliki rute ke internet. Anda dapat menjalankan EC2 instance di subnet pribadi dan menggunakan kemampuan Session Manager AWS Systems Manager untuk mengakses instans dari jarak jauh melalui () atau. AWS Command Line Interface AWS CLI AWS Management Console Anda kemudian dapat menggunakan konsol AWS CLI atau untuk memulai sesi yang terhubung ke instance melalui

terowongan aman, mencegah kebutuhan untuk mengelola kredensial tambahan yang digunakan untuk Secure Shell (SSH) atau protokol desktop jarak jauh Windows (RDP).

Gunakan Pengelola Sesi alih-alih menjalankan EC2 instance di subnet publik, menjalankan kotak lompat, atau menjalankan host benteng.

Untuk mengatur Manajer Sesi

1. Pastikan EC2 instans menggunakan sistem operasi terbaru Amazon Machine Images (AMIs), seperti Amazon Linux atau Ubuntu. AWS Systems Manager Agen (SSMAgen) sudah diinstal sebelumnya di. AMI
2. Pastikan instance memiliki konektivitas, baik melalui gateway internet atau melalui VPC titik akhir, ke alamat ini (diganti **<Region>** dengan yang sesuai Wilayah AWS):
 - a. `ec2messages.<Region>.amazonaws.com`
 - b. `ssm.<Region>.amazonaws.com`
 - c. `ssmmessages.<Region>.amazonaws.com`
3. Lampirkan kebijakan AWS terkelola AmazonSSMManagedInstanceCore ke IAM peran yang terkait dengan instans Anda.

Untuk informasi selengkapnya, lihat [Menyiapkan Session Manager](#) (dokumentasi Systems Manager).

Untuk memulai sesi

- [Mulai sesi](#) (dokumentasi Systems Manager).

WKLD.07 Log peristiwa data untuk bucket S3 dengan data sensitif

Secara default, AWS CloudTrail menangkap peristiwa manajemen, peristiwa yang membuat, memodifikasi, atau menghapus sumber daya di akun Anda. Peristiwa manajemen ini tidak menangkap operasi baca atau tulis ke objek individual di bucket Amazon Simple Storage Service. Selama acara keamanan, penting untuk menangkap akses atau penggunaan data yang tidak sah pada catatan individu atau tingkat objek. Gunakan CloudTrail untuk mencatat peristiwa data untuk bucket S3 apa pun yang menyimpan data sensitif atau penting bisnis, untuk tujuan deteksi dan audit.

Note

Biaya tambahan berlaku untuk peristiwa data pencatatan. Untuk informasi selengkapnya, lihat [harga AWS CloudTrail](#).

Untuk mencatat peristiwa data untuk jejak

1. Masuk ke AWS Management Console dan buka [CloudTrailkonsol](#)
2. Di panel navigasi, pilih Jalur, lalu pilih nama jejak.
3. Dalam Rincian umum, pilih Edit untuk mengubah pengaturan berikut. Anda tidak dapat mengubah nama jejak.
 - a. Dalam peristiwa Data, pilih Edit.
 - b. Untuk sumber peristiwa Data, pilih S3.
 - c. Untuk Semua bucket S3 saat ini dan masa depan, hapus Baca dan Tulis.
 - d. Dalam pemilihan bucket Individual, telusuri bucket tempat mencatat peristiwa data. Anda dapat memilih beberapa ember di jendela ini. Pilih Tambahkan bucket untuk mencatat peristiwa data untuk bucket lainnya. Pilih untuk mencatat peristiwa Baca, seperti `GetObject`, Menulis peristiwa, seperti `PutObject`, atau keduanya.
 - e. Pilih Perbarui jejak.

WKLD.08 Enkripsi volume Amazon EBS

Menerapkan enkripsi volume Amazon Elastic Block Store (AmazonEBS) sebagai perilaku default di AWS akun Anda. Volume terenkripsi memiliki kinerja operasi input/output per detik (IOPS) yang sama dengan volume yang tidak terenkripsi dengan efek minimal pada latensi. Ini mencegah pembangunan kembali volume di kemudian hari karena kepatuhan atau alasan lain. Untuk informasi selengkapnya, lihat [Praktik terbaik yang harus diketahui untuk EBS enkripsi Amazon](#) (posting AWS blog).

Untuk mengenkripsi volume Amazon EBS

- [Aktifkan enkripsi secara default](#) (EC2dokumentasi Amazon).

WKLD.09 Enkripsi basis data Amazon RDS

Mirip dengan [WKLD.08 Enkripsi volume Amazon EBS](#), aktifkan enkripsi database Amazon Relational Database Service (RDS Amazon). Enkripsi ini dilakukan pada tingkat volume yang mendasarinya dan memiliki IOPS kinerja yang sama dengan volume yang tidak terenkripsi dengan efek minimal pada latensi. Untuk informasi selengkapnya, lihat [Ikhtisar mengenkripsi RDS sumber daya Amazon](#) (RDS dokumentasi Amazon).

Untuk mengenkripsi instance RDS database

- [Enkripsi instance database](#) (RDS dokumentasi Amazon).

WKLD.10 Menyebarkan sumber daya pribadi ke subnet pribadi

Menyebarkan sumber daya yang tidak memerlukan akses internet langsung, seperti EC2 instance, database, antrian, caching, atau infrastruktur lainnya, ke subnet pribadi. VPC Subnet pribadi tidak memiliki rute yang dinyatakan dalam tabel rute mereka ke gateway internet terlampir dan tidak dapat menerima lalu lintas internet. Lalu lintas yang berasal dari subnet pribadi yang ditujukan untuk internet harus menjalani terjemahan alamat jaringan (NAT) melalui AWS NAT Gateway terkelola atau EC2 instance yang menjalankan NAT proses di subnet publik. Untuk informasi selengkapnya tentang isolasi jaringan, lihat [Keamanan infrastruktur di Amazon VPC](#) (VPC dokumentasi Amazon).

Gunakan praktik berikut saat membuat sumber daya dan subnet pribadi:

- Saat membuat subnet pribadi, nonaktifkan alamat publik penetapan otomatis. IPv4
- Saat membuat EC2 instance pribadi, nonaktifkan Auto-assign IP Publik. Ini mencegah IP publik ditetapkan jika instance secara tidak sengaja disebarkan ke subnet publik melalui kesalahan konfigurasi.

Anda menentukan subnet untuk sumber daya sebagai bagian dari konfigurasinya, bila diperlukan.

WKLD.11 Membatasi akses jaringan dengan menggunakan grup keamanan

Gunakan grup keamanan untuk mengontrol lalu lintas ke EC2 instans, RDS database, dan sumber daya lain yang didukung. Grup keamanan bertindak sebagai firewall virtual yang dapat

diterapkan ke setiap kelompok sumber daya terkait untuk secara konsisten menentukan aturan untuk memungkinkan lalu lintas masuk dan keluar. Selain aturan berdasarkan alamat IP dan port, kelompok keamanan mendukung aturan untuk memungkinkan lalu lintas dari sumber daya yang terkait dengan kelompok keamanan lainnya. Misalnya, grup keamanan database dapat memiliki aturan untuk mengizinkan hanya lalu lintas dari grup keamanan server aplikasi.

Secara default, grup keamanan mengizinkan semua lalu lintas keluar tetapi tidak mengizinkan lalu lintas masuk. Aturan lalu lintas keluar dapat dihapus, atau Anda dapat mengonfigurasi aturan tambahan yang ditambahkan untuk membatasi lalu lintas keluar dan mengizinkan lalu lintas masuk. Jika grup keamanan tidak memiliki aturan keluar, lalu lintas keluar yang berasal dari instans Anda tidak diperbolehkan. Untuk informasi selengkapnya, lihat [Mengontrol lalu lintas ke sumber daya menggunakan grup keamanan](#) (VPCdokumentasi Amazon).

Dalam contoh berikut, ada tiga grup keamanan yang mengontrol lalu lintas dari Application Load Balancer ke EC2 instance yang terhubung ke database Amazon RDS for My. SQL

Grup keamanan	Aturan-aturan ke dalam	Aturan-aturan ke luar
Grup keamanan Application Load Balancer	<p>Deskripsi: Izinkan HTTPS lalu lintas dari mana saja</p> <p>Jenis: HTTPS</p> <p>Sumber: Di mana saja- IPv4 (0.0.0.0/0)</p>	<p>Deskripsi: Izinkan semua lalu lintas ke mana saja</p> <p>Jenis: Semua lalu lintas</p> <p>Tujuan: Di mana saja- IPv4 (0.0.0.0/0)</p>
EC2kelompok keamanan contoh	<p>Deskripsi: Izinkan HTTP lalu lintas dari Application Load Balancer</p> <p>Jenis: HTTP</p> <p>Sumber: Grup keamanan Application Load Balancer</p>	<p>Deskripsi: Izinkan semua lalu lintas ke mana saja</p> <p>Jenis: Semua lalu lintas</p> <p>Tujuan: Di mana saja- IPv4 (0.0.0.0/0)</p>
RDSkelompok keamanan basis data	<p>Deskripsi: Izinkan SQL lalu lintas saya dari EC2 contoh</p> <p>Tipe: Saya SQL</p>	Tidak ada aturan keluar

Grup keamanan	Aturan-aturan ke dalam	Aturan-aturan ke luar
	Sumber: grup keamanan EC2 contoh	

WKLD.12 Gunakan VPC titik akhir untuk mengakses layanan yang didukung

Dalam VPCs, sumber daya yang perlu mengakses AWS atau layanan eksternal lainnya memerlukan rute ke internet ($0.0.0.0/0$) atau ke alamat IP publik dari layanan target. Gunakan VPC titik akhir untuk mengaktifkan rute IP pribadi dari layanan Anda VPC ke layanan yang didukung AWS atau lainnya, mencegah kebutuhan untuk menggunakan gateway internet, NAT perangkat, koneksi jaringan pribadi virtual (VPN), atau AWS Direct Connect koneksi.

VPC endpoint mendukung melampirkan kebijakan dan kelompok keamanan untuk mengontrol akses lebih lanjut ke layanan. Misalnya, Anda dapat menulis kebijakan VPC titik akhir untuk Amazon DynamoDB agar hanya mengizinkan tindakan tingkat item dan mencegah tindakan tingkat tabel untuk semua sumber daya VPC di, terlepas dari kebijakan izinnya sendiri. Anda juga dapat menulis kebijakan bucket S3 untuk mengizinkan hanya permintaan yang berasal dari VPC titik akhir tertentu, sehingga menolak semua akses eksternal lainnya. VPC endpoint juga dapat memiliki aturan grup keamanan yang, misalnya, membatasi akses ke hanya EC2 instance yang terkait dengan grup keamanan khusus aplikasi, seperti tingkat logika bisnis aplikasi web.

Ada berbagai jenis VPC titik akhir. Anda mengakses sebagian besar layanan dengan menggunakan titik akhir VPC antarmuka. DynamoDB diakses menggunakan titik akhir gateway. Amazon S3 mendukung antarmuka dan titik akhir gateway. Titik akhir Gateway direkomendasikan untuk beban kerja yang terdapat dalam satu AWS akun dan Wilayah, dan tidak dikenakan biaya tambahan. Titik akhir antarmuka direkomendasikan jika diperlukan akses yang lebih dapat diperluas, seperti ke bucket S3 dari yang lain VPCs, dari jaringan lokal, atau dari yang lain. Wilayah AWS Titik akhir antarmuka dikenakan biaya uptime per jam dan biaya pemrosesan data per GB, yang keduanya lebih rendah dari biaya masing-masing untuk mengirim data melalui Gateway. $0.0.0.0/0$ AWS NAT

Lihat sumber daya berikut untuk informasi tambahan tentang penggunaan VPC titik akhir:

- Untuk informasi selengkapnya tentang memilih antara titik akhir gateway dan antarmuka untuk Amazon S3, [lihat Memilih Strategi Titik Akhir VPC Anda untuk Amazon S3](#) (posting blog). AWS
- [Akses Layanan AWS menggunakan VPC titik akhir antarmuka](#) (VPC dokumentasi Amazon).

- [Titik akhir Gateway](#) (VPCdokumentasi Amazon).
- Misalnya kebijakan bucket S3 yang membatasi akses ke titik akhir tertentu VPC atau VPC titik akhir, lihat [Membatasi akses ke spesifik \(dokumentasi Amazon VPC S3\)](#).
- Misalnya kebijakan titik akhir DynamoDB yang membatasi tindakan, lihat Kebijakan titik akhir [untuk DynamoDB \(dokumentasi Amazon\)](#). VPC

WKLD.13 Memerlukan HTTPS semua titik akhir web publik

Perlu HTTPS memberikan kredibilitas tambahan ke titik akhir web Anda, izinkan titik akhir Anda menggunakan sertifikat untuk membuktikan identitas mereka, dan mengonfirmasi bahwa semua lalu lintas antara titik akhir Anda dan klien yang terhubung dienkripsi. Untuk situs web publik, ini memberikan manfaat tambahan dari peringkat mesin pencari yang lebih tinggi.

Banyak AWS layanan menyediakan endpoint web publik untuk sumber daya Anda, seperti, Amazon AWS Elastic Beanstalk, Amazon API Gateway CloudFront, Elastic Load Balancing, dan. AWS Amplify Untuk petunjuk tentang bagaimana kebutuhan HTTPS untuk masing-masing layanan ini, lihat berikut ini:

- [Elastic Beanstalk](#) (dokumentasi Elastic Beanstalk)
- [CloudFront](#)(CloudFront dokumentasi)
- [Application Load Balancer](#) (Pusat AWS Pengetahuan)
- [Classic Load Balancer](#) (Pusat AWS Pengetahuan)
- [Amplify](#) (Amplify dokumentasi)

Situs web statis yang dihosting di Amazon S3 tidak mendukung. HTTPS Untuk HTTPS meminta situs web ini, Anda dapat menggunakannya CloudFront. Akses publik ke bucket S3 yang menyajikan konten melalui tidak CloudFront diperlukan.

Untuk digunakan CloudFront untuk melayani situs web statis yang dihosting di Amazon S3

1. [Gunakan CloudFront untuk melayani situs web statis yang dihosting di Amazon S3](#) (Pusat AWS Pengetahuan).
2. Jika Anda mengonfigurasi akses ke bucket S3 publik, [memerlukan HTTPS antara pemirsa dan CloudFront](#) (CloudFrontdokumentasi).

Jika Anda mengonfigurasi akses ke bucket S3 pribadi, [batasi akses ke konten Amazon S3 dengan menggunakan identitas akses asal](#) (dokumentasi). CloudFront

Selain itu, konfigurasi endpoint HTTPS untuk memerlukan protokol dan cipher Transport Layer Security (TLS) modern, kecuali kompatibilitas dengan protokol yang lebih lama diperlukan. Misalnya, gunakan `ELBSecurityPolicy-FS-1-2-Res-2020-10` atau kebijakan terbaru yang tersedia untuk HTTPS pendengar Application Load Balancer, bukan default. `ELBSecurityPolicy-2016-08` Kebijakan terbaru memerlukan minimal TLS 1,2, kerahasiaan maju, dan sandi yang kuat yang kompatibel dengan browser web modern.

Untuk informasi selengkapnya tentang kebijakan keamanan yang tersedia untuk titik akhir HTTPS publik, lihat:

- [Kebijakan SSL keamanan yang telah ditetapkan untuk Classic Load Balancers](#) (dokumentasi Elastic Load Balancing)
- [Kebijakan keamanan untuk Application Load Balancer Anda](#) (dokumentasi Elastic Load Balancing)
- [Protokol dan cipher yang didukung antara pemirsa](#) dan (dokumentasi) CloudFront CloudFront

WKLD.14 Gunakan layanan perlindungan tepi untuk titik akhir publik

Daripada melayani lalu lintas langsung dari layanan komputasi seperti EC2 instance atau kontainer, gunakan layanan perlindungan tepi. Ini memberikan lapisan keamanan tambahan antara lalu lintas masuk dari internet dan sumber daya Anda yang melayani lalu lintas itu. Layanan ini dapat memfilter lalu lintas yang tidak diinginkan, menegakkan enkripsi, dan menerapkan perutean atau aturan lain, seperti load balancing, sebelum lalu lintas mencapai sumber daya internal Anda.

AWS Layanan yang dapat memberikan perlindungan endpoint publik meliputi, Elastic Load Balancing AWS WAF CloudFront, GatewayAPI, dan Amplify Hosting. Jalankan layanan VPC berbasis, seperti Elastic Load Balancing, di subnet publik sebagai proxy ke sumber daya layanan web yang berjalan di subnet pribadi.

CloudFront, API Gateway, dan Amazon Route 53 memberikan perlindungan dari serangan penolakan layanan (DDoS) terdistribusi Layer 3 dan 4 tanpa biaya, dan AWS WAF dapat melindungi terhadap serangan Layer 7.

Petunjuk untuk memulai dengan masing-masing layanan ini dapat ditemukan di sini:

- [Memulai dengan AWS WAF](#) (AWS situs web)
- [Memulai dengan Amazon CloudFront](#) (CloudFront dokumentasi)
- [Memulai Elastic Load Balancing](#) (dokumentasi Elastic Load Balancing)
- [Memulai dengan API Gateway](#) (dokumentasi API Gateway)
- [Memulai dengan Amplify Hosting](#) (Amplify documentation)

WKLD15 Tentukan kontrol keamanan dalam template dan terapkan dengan menggunakan praktik CI/CD

Infrastructure as code (IAC) adalah praktik mendefinisikan semua sumber daya dan konfigurasi AWS layanan Anda dalam templat dan kode yang Anda gunakan dengan menggunakan pipeline continuous integration and continuous delivery (CI/CD), pipeline yang sama yang digunakan untuk menyebarkan aplikasi perangkat lunak. Layanan IAC, seperti AWS CloudFormation, mendukung kebijakan berbasis IAM identitas dan berbasis sumber daya dan mendukung AWS layanan keamanan, seperti Amazon GuardDuty, Amazon WAF, dan Amazon VPC. Tangkap artefak ini sebagai template IAC, komit template ke repositori kode sumber, dan kemudian terapkan dengan menggunakan pipeline CI/CD.

Kecuali diperlukan sebaliknya, komit kebijakan izin aplikasi dengan kode aplikasi di repositori yang sama, dan kelola kebijakan sumber daya umum dan konfigurasi layanan keamanan di repositori kode terpisah dan pipeline penerapan.

Untuk informasi selengkapnya tentang memulai dengan IAC aktif AWS, lihat [AWS Cloud Development Kit \(AWS CDK\) dokumentasi](#).

Kontributor

Kontributor dokumen ini meliputi:

- Jay Michael, Arsitek Solusi Utama (penulis utama)
- Cole Calistra, Arsitek Solusi Utama
- Justin Plock, Arsitek Solusi Utama
- Faisal Farooq, Arsitek Solusi
- Michael Nguyen, Sr. Arsitek Solusi
- Ritik Khatwani, Sr. Arsitek Solusi
- Paul Hawkins, Kepala Sekolah, Kantor Kepala Petugas Keamanan Informasi () CISO

Terima kasih khusus kepada orang-orang berikut yang juga membantu dengan bimbingan dan ulasan:

- Robert Taruh
- Mike Sullivan
- Bob Lee III

Riwayat dokumen

Tabel berikut menjelaskan perubahan signifikan pada panduan ini. Jika Anda ingin diberi tahu tentang pembaruan masa depan, Anda dapat berlangganan [RSSumpnan](#).

Perubahan	Deskripsi	Tanggal
Pengaturan bucket Amazon S3	Kami memperbarui bagian ACCT.08 Mencegah akses publik ke bucket S3 pribadi untuk mencerminkan bahwa bucket Amazon S3 yang dibuat setelah 28 April 2023 mengaktifkan pengaturan Blokir Akses Publik secara default.	18 Mei 2023
IAMpraktik terbaik keamanan	Kami memperbarui panduan ini untuk penyelarasan dengan praktik terbaik AWS Identity and Access Management (IAM) terbaru. Untuk informasi selengkapnya, lihat Praktik terbaik keamanan dalam IAM dokumentasi.	1 Februari 2023
IAMperan	Kami menyediakan tautan tambahan ke Layanan AWS dokumentasi di bagian WKLD.01 Gunakan IAM peran untuk izin lingkungan komputasi .	September 22, 2022
Kebijakan kata sandi	Kami memperbarui rekomendasi untuk kata sandi yang kuat untuk menggunakan panduan	10 Mei 2022

terbaru dari Pusat Keamanan
Internet (CIS).

[Publikasi awal](#)

—

13 April 2022

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. SQL
- 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 (RDS Amazon) untuk Oracle di AWS Cloud
- Pembelian kembali (drop and shop) - Beralih ke produk yang berbeda, biasanya dengan beralih dari lisensi tradisional ke model SaaS. Contoh: Migrasikan sistem manajemen hubungan pelanggan (CRM) Anda ke Salesforce.com.
- Rehost (lift dan shift) — Pindahkan aplikasi ke cloud tanpa membuat perubahan apa pun untuk memanfaatkan kemampuan cloud. Contoh: Migrasikan database Oracle lokal Anda ke Oracle pada instance EC2 di AWS Cloud
- Relokasi (hypervisor-level lift and shift) — Pindahkan infrastruktur ke cloud tanpa membeli perangkat keras baru, menulis ulang aplikasi, atau memodifikasi operasi yang ada. Anda memigrasikan server dari platform lokal ke layanan cloud untuk platform yang sama. Contoh: Migrasi a Microsoft Hyper-V aplikasi untuk AWS.
- Pertahankan (kunjungi kembali) - Simpan aplikasi di lingkungan sumber Anda. Ini mungkin termasuk aplikasi yang memerlukan refactoring besar, dan Anda ingin menunda pekerjaan itu sampai nanti, dan aplikasi lama yang ingin Anda pertahankan, karena tidak ada pembenaran bisnis untuk memigrasikannya.

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

A

ABAC

Lihat [kontrol akses berbasis atribut](#).

layanan abstrak

Lihat [layanan terkelola](#).

ACID

Lihat [atomisitas, konsistensi, isolasi, daya tahan](#).

migrasi aktif-aktif

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

migrasi aktif-pasif

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

fungsi agregat

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

AI

Lihat [kecerdasan buatan](#).

AIOps

Lihat [operasi kecerdasan buatan](#).

anonimisasi

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

anti-pola

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

kontrol aplikasi

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

portofolio aplikasi

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

kecerdasan buatan (AI)

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

operasi kecerdasan buatan (AIOps)

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

enkripsi asimetris

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

atomisitas, konsistensi, isolasi, daya tahan () ACID

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

kontrol akses berbasis atribut () ABAC

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

sumber data otoritatif

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

Zona Ketersediaan

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

AWS Kerangka Adopsi Cloud (AWS CAF)

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

AWS Kerangka Kualifikasi Beban Kerja ()AWS WQF

Alat yang mengevaluasi beban kerja migrasi database, merekomendasikan strategi migrasi, dan memberikan perkiraan kerja. AWS 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 menyebabkan kerugian bagi individu atau organisasi.

BCP

Lihat [perencanaan kontinuitas bisnis](#).

grafik perilaku

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

sistem big-endian

Sistem yang menyimpan byte paling signifikan terlebih dahulu. Lihat juga [endianness](#).

klasifikasi biner

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

filter mekar

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

deployment biru/hijau

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

bot

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

botnet

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

cabang

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

akses break-glass

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

CAF

Lihat [Kerangka Adopsi AWS Cloud](#).

penyebaran kenari

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

CCoE

Lihat [Cloud Center of Excellence](#).

CDC

Lihat [mengubah pengambilan data](#).

ubah pengambilan data (CDC)

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

rekayasa kekacauan

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

CI/CD

Lihat [integrasi berkelanjutan dan pengiriman berkelanjutan](#).

klasifikasi

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

Enkripsi sisi klien

Enkripsi data secara lokal, sebelum target Layanan AWS menerimanya.

Pusat Keunggulan Cloud (CCoE)

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

komputasi cloud

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

model operasi cloud

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

tahap adopsi cloud

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

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

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

CMDB

Lihat [database manajemen konfigurasi](#).

repositori kode

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

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

cache dingin

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

data dingin

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

visi komputer (CV)

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

konfigurasi drift

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

database manajemen konfigurasi (CMDB)

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

paket kesesuaian

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

integrasi berkelanjutan dan pengiriman berkelanjutan (CI/CD)

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

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

CV

Lihat [visi komputer](#).

D

data saat istirahat

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

klasifikasi data

Proses untuk mengidentifikasi dan mengkategorikan data dalam jaringan Anda berdasarkan kekritisannya 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 database (DML)

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

DDL

Lihat [bahasa definisi database](#).

ansambel yang dalam

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

pembelajaran mendalam

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

defense-in-depth

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

administrator yang didelegasikan

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

deployment

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

lingkungan pengembangan

Lihat [lingkungan](#).

kontrol detektif

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

pemetaan aliran nilai pengembangan () DVSM

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

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

kembar digital

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

tabel dimensi

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

musibah

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

pemulihan bencana (DR)

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

DML

Lihat [bahasa manipulasi basis data](#).

desain berbasis domain

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

DR

Lihat [pemulihan bencana](#).

deteksi drift

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

DVSM

Lihat [pemetaan aliran nilai pengembangan](#).

E

EDA

Lihat [analisis data eksplorasi](#).

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

perencanaan sumber daya perusahaan (ERP)

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

enkripsi amplop

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

lingkungan

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

- Development Environment — Sebuah contoh dari aplikasi yang berjalan yang hanya tersedia untuk tim inti yang bertanggung jawab untuk memelihara aplikasi. Lingkungan pengembangan digunakan untuk menguji perubahan sebelum mempromosikannya ke lingkungan atas. Jenis lingkungan ini kadang-kadang disebut sebagai lingkungan pengujian.
- lingkungan yang lebih rendah — Semua lingkungan pengembangan untuk aplikasi, seperti yang digunakan untuk build awal dan pengujian.
- lingkungan produksi — Sebuah contoh dari aplikasi yang berjalan yang 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 AWS CAF keamanan termasuk manajemen identitas dan akses, kontrol detektif, keamanan infrastruktur, perlindungan data, dan respons insiden. Untuk informasi selengkapnya tentang epos dalam strategi AWS migrasi, lihat [panduan implementasi program](#).

ERP

Lihat [perencanaan sumber daya perusahaan](#).

analisis data eksplorasi () EDA

Proses menganalisis dataset untuk memahami karakteristik utamanya. Anda mengumpulkan atau mengumpulkan data dan kemudian melakukan penyelidikan awal untuk menemukan pola, mendeteksi anomali, dan memeriksa asumsi. 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

Memberikan sejumlah kecil contoh yang menunjukkan tugas dan output yang diinginkan sebelum memintanya untuk melakukan tugas serupa. [LLM](#) 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. FM 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 (OU). Pagar pembatas preventif menegakkan kebijakan untuk memastikan keselarasan dengan standar kepatuhan. Mereka diimplementasikan dengan menggunakan kebijakan kontrol layanan dan batas IAM izin. Detective guardrails mendeteksi pelanggaran kebijakan dan masalah kepatuhan, dan menghasilkan peringatan untuk remediasi. Mereka diimplementasikan dengan menggunakan AWS Config, AWS Security Hub, Amazon GuardDuty, AWS Trusted Advisor, Amazon Inspector, dan pemeriksaan khusus AWS Lambda .

H

HA

Lihat [ketersediaan tinggi](#).

migrasi database heterogen

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

ketersediaan tinggi (HA)

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

modernisasi sejarawan

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

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

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 untuk SQL Server). Migrasi homogen biasanya merupakan bagian dari upaya rehosting atau replatforming. Anda dapat menggunakan utilitas database asli untuk memigrasi skema.

data panas

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

perbaikan terbaru

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

periode hypercare

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

|

IAC

Lihat [infrastruktur sebagai kode](#).

kebijakan berbasis identitas

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

|

aplikasi idle

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

IloT

Lihat [Internet of Things industri](#).

infrastruktur yang tidak dapat diubah

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

masuk (masuknya) VPC

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

migrasi 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 selengkapnya, lihat [Membangun strategi transformasi digital Internet of Things \(IIoT\) industri](#).

inspeksi VPC

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

Internet of Things (IoT)

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

interpretabilitas

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

IoT

Lihat [Internet of Things](#).

Perpustakaan informasi TI (ITIL)

Serangkaian praktik terbaik untuk memberikan layanan TI dan menyelaraskan layanan ini dengan persyaratan bisnis. ITIL menyediakan fondasi 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 ITSM alat, lihat [panduan integrasi operasi](#).

ITIL

Lihat [perpustakaan informasi TI](#).

ITSM

Lihat [manajemen layanan TI](#).

L

kontrol akses berbasis label () LBAC

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

landing zone

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

model bahasa besar (LLM)

Model [AI](#) pembelajaran mendalam yang dilatih sebelumnya pada sejumlah besar data. An LLM dapat melakukan banyak 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.

MAP

Lihat [Program Percepatan Migrasi](#).

mekanisme

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

akun anggota

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

MES

Lihat [sistem eksekusi manufaktur](#).

Transportasi Telemetri Antrian Pesan () MQTT

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

layanan mikro

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

informasi selengkapnya, lihat [Mengintegrasikan layanan mikro dengan menggunakan layanan tanpa AWS server](#).

arsitektur microservices

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

Program Percepatan Migrasi (MAP)

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

migrasi dalam skala

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

pabrik migrasi

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

metadata migrasi

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

pola migrasi

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

Penilaian Portofolio Migrasi (MPA)

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

Penilaian Kesiapan Migrasi (MRA)

Proses mendapatkan wawasan tentang status kesiapan cloud organisasi, mengidentifikasi kekuatan dan kelemahan, dan membangun rencana aksi untuk menutup kesenjangan yang teridentifikasi, menggunakan AWS CAF. Untuk informasi selengkapnya, lihat [panduan kesiapan migrasi](#). MRA ini 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 [Mengurai monolit](#) menjadi layanan mikro.

MPA

Lihat [Penilaian Portofolio Migrasi](#).

MQTT

Lihat [Transportasi Telemetri Antrian Pesan](#).

klasifikasi multiclass

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

infrastruktur yang bisa berubah

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

O

OAC

Lihat [kontrol akses asal](#).

OAI

Lihat [identitas akses asal](#).

OCM

Lihat [manajemen perubahan organisasi](#).

migrasi offline

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

OI

Lihat [integrasi operasi](#).

OLA

Lihat [perjanjian tingkat operasional](#).

migrasi online

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

OPC-UA

Lihat [Komunikasi Proses Terbuka - Arsitektur Terpadu](#).

Komunikasi Proses Terbuka - Arsitektur Terpadu (OPC-UA)

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

perjanjian tingkat operasional () OLA

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

tinjauan kesiapan operasional () ORR

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

teknologi operasional (OT)

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

integrasi operasi (OI)

Proses modernisasi operasi di cloud, yang melibatkan perencanaan kesiapan, otomatisasi, dan integrasi. Untuk informasi selengkapnya, lihat [panduan integrasi operasi](#).

jejak organisasi

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

manajemen perubahan organisasi (OCM)

Kerangka kerja untuk mengelola transformasi bisnis utama yang mengganggu dari perspektif orang, budaya, dan kepemimpinan. 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 [OCMpanduannya](#).

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 PUT dan DELETE permintaan ke bucket S3.

identitas akses asal (OAI)

Di CloudFront, opsi untuk membatasi akses untuk mengamankan konten Amazon S3 Anda. Saat Anda 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, a VPC yang menangani koneksi jaringan yang dimulai dari dalam aplikasi. [Arsitektur Referensi AWS Keamanan](#) merekomendasikan pengaturan akun Jaringan Anda dengan inbound, outbound, dan inspeksi VPCs untuk melindungi antarmuka dua arah antara aplikasi Anda dan internet yang lebih luas.

P

batas izin

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

Informasi Identifikasi Pribadi () PII

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

PII

Lihat informasi yang [dapat diidentifikasi secara pribadi](#).

buku pedoman

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

PLC

Lihat [pengontrol logika yang dapat diprogram](#).

PLM

Lihat [manajemen siklus hidup produk](#).

kebijakan

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

ketekunan poliglott

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

penilaian portofolio

Proses menemukan, menganalisis, dan memprioritaskan portofolio aplikasi untuk merencanakan migrasi. Untuk informasi selengkapnya, lihat [Mengevaluasi kesiapan migrasi](#).

predikat

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

predikat pushdown

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

kontrol preventif

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

principal

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

privasi 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 DNS kueri untuk domain dan subdomainnya dalam satu atau lebih VPCs Untuk informasi selengkapnya, lihat [Bekerja dengan zona yang dihosting pribadi](#) di dokumentasi Route 53.

kontrol proaktif

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

manajemen siklus hidup produk () PLM

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

lingkungan produksi

Lihat [lingkungan](#).

pengontrol logika yang dapat diprogram () PLC

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

rantai cepat

Menggunakan output dari satu [LLM](#) prompt 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 pengenalan 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 layanan mikro berbasis [MES](#), layanan mikro dapat mempublikasikan pesan peristiwa ke saluran yang dapat berlangganan oleh layanan mikro lainnya. Sistem dapat menambahkan layanan mikro baru tanpa mengubah layanan penerbitan.

Q

rencana kueri

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

regresi rencana kueri

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

R

RACImatriks

Lihat [bertanggung jawab, akuntabel, dikonsultasikan, diinformasikan \(\) RACI](#).

RAG

Lihat [Retrieval Augmented Generation](#).

ransomware

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

RASCI matriks

Lihat [bertanggung jawab, akuntabel, dikonsultasikan, diinformasikan \(\) RACI](#).

RCAC

Lihat [kontrol akses baris dan kolom](#).

replika baca

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

arsitek ulang

Lihat [7 Rs](#).

tujuan titik pemulihan (RPO)

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

tujuan waktu pemulihan (RTO)

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

refactor

Lihat [7 Rs](#).

Wilayah

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

regresi

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

rehost

Lihat [7 Rs](#).

melepaskan

Dalam proses penyebaran, tindakan mempromosikan perubahan pada lingkungan produksi.

memindahkan

Lihat [7 Rs](#).

memplatform ulang

Lihat [7 Rs](#).

pembelian kembali

Lihat [7 Rs](#).

ketahanan

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

kebijakan berbasis sumber daya

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

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

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

kontrol responsif

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

melestarikan

Lihat [7 Rs](#).

pensiun

Lihat [7 Rs](#).

Pengambilan Generasi Augmented () RAG

Teknologi [AI generatif](#) di mana [LLM](#) referensi sumber data otoritatif yang berada di luar sumber data pelatihannya sebelum menghasilkan respons. Misalnya, RAG model 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 kredensial.

kontrol akses baris dan kolom (RCAC)

Penggunaan SQL ekspresi 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 (SSO) gabungan, sehingga pengguna dapat masuk ke AWS Management Console atau memanggil AWS API operasi tanpa Anda harus membuat pengguna untuk semua orang di IAM organisasi Anda. Untuk informasi lebih lanjut tentang federasi SAML berbasis 2.0, lihat [Tentang federasi SAML berbasis 2.0](#) dalam dokumentasi. IAM

SCADA

Lihat [kontrol pengawasan dan akuisisi data](#).

SCP

Lihat [kebijakan kontrol layanan](#).

Rahasia

Dalam AWS Secrets Manager, informasi rahasia atau terbatas, seperti kata sandi atau kredensial pengguna, yang Anda simpan dalam bentuk terenkripsi. Ini terdiri dari nilai rahasia dan metadatanya. 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.

informasi keamanan dan manajemen acara (SIEM) sistem

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

otomatisasi respons keamanan

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

[detektif](#) atau [responsif](#) yang membantu Anda menerapkan praktik terbaik AWS keamanan. Contoh tindakan respons otomatis termasuk memodifikasi grup VPC keamanan, menambal EC2 instans Amazon, atau memutar kredensial.

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

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

perjanjian tingkat layanan () SLA

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

indikator tingkat layanan () SLI

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

tujuan tingkat layanan () SLO

Metrik target yang mewakili kesehatan layanan, yang diukur dengan indikator [tingkat layanan](#).

model tanggung jawab bersama

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

SIEM

Lihat [informasi keamanan dan sistem manajemen acara](#).

satu titik kegagalan (SPOF)

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

SLA

Lihat [perjanjian tingkat layanan](#).

SLI

Lihat [indikator tingkat layanan](#).

SLO

Lihat [tujuan tingkat layanan](#).

split-and-seed model

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

SPOF

Lihat [satu titik kegagalan](#).

skema bintang

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

pola ara pencekik

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

subnet

Berbagai alamat IP di AndaVPC. Subnet harus berada di Availability Zone tunggal.

kontrol pengawasan dan akuisisi data () SCADA

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

enkripsi simetris

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

pengujian sintetis

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

sistem prompt

Teknik untuk memberikan konteks, instruksi, atau pedoman [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.

VPCmengintip

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

kerentanan

Kelemahan perangkat lunak atau perangkat keras yang membahayakan keamanan sistem.

W

cache hangat

Cache buffer yang berisi data terkini 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

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

beban kerja

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

aliran kerja

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

WORM

Lihat [menulis sekali, baca banyak](#).

WQF

Lihat [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

[LLM](#) Memberikan instruksi untuk melakukan tugas tetapi tidak ada contoh (bidikan) 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 rata-rata CPU dan penggunaan memori di bawah 5 persen. Dalam proyek migrasi, adalah umum untuk menghentikan aplikasi ini.

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