Merancang dan menerapkan pencatatan dan pemantauan dengan Amazon CloudWatch

AWS Bimbingan Preskriptif

AWS Bimbingan Preskriptif: Merancang dan menerapkan pencatatan dan pemantauan dengan Amazon CloudWatch

Table of Contents

Merancang dan menerapkan penebangan dan pemantauan dengan Amazon CloudWatch

Khurram Nizami, Amazon Web Services (AWS)

April 2023 (riwayat dokumen)

Panduan ini membantu Anda merancang dan menerapkan pencatatan dan pemantauan dengan Amazon CloudWatch dan layanan manajemen dan tata kelola Amazon Web Services (AWS) terkait untuk beban kerja yang menggunakan instans Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Container Service (Amazon ECS), Amazon Elastic Kubernetes Service (Amazon EKS) AWS Lambda, dan server lokal. Panduan ini ditujukan untuk tim operasi, DevOps teknisi, dan teknisi aplikasi yang mengelola beban kerja diAWS Cloud.

Pendekatan logging dan monitoring Anda harus didasarkan pada enam pilar dariAWS Well-Architected Framework. Pilar-pilar ini adalah keunggulan operasional, keamanan, keandalan, efisiensi kinerja, dan optimalisasi biaya. Solusi pemantauan dan mengkhawatirkan yang dirancang dengan baik meningkatkan keandalan dan kinerja dengan membantu Anda menganalisis dan menyesuaikan infrastruktur secara proaktif.

Panduan ini tidak secara ekstensif membahas penebangan dan pemantauan untuk keamanan atau pengoptimalan biaya karena ini adalah topik yang memerlukan evaluasi mendalam. Ada banyakAWS layanan yang mendukung pencatatan dan pemantauan keamanan, termasuk AWS CloudTrailAWS Config, Amazon Inspector, Amazon Detective, Amazon Macie, Amazon GuardDuty, dan AWS Security Hub. Anda juga dapat menggunakan AWS Cost Explorer, AWSAnggaran, dan metrikCloudWatch penagihan untuk pengoptimalan biaya.

Tabel berikut menguraikan enam area yang harus ditangani oleh solusi logging dan monitoring Anda.

Menangkap dan menelan file log dan metrik	Identifikasi, konfigurasikan, dan kirim log dan metrik sistem dan aplikasi keAWS layanan dari berbagai sumber.
Mencari dan menganalisis log	Cari dan analisis log untuk manajemen operasi, identifikasi masalah, pemecahan masalah, dan analisis aplikasi.

Memantau metrik dan mengkhawatirkan	Identifikasi dan lakukan pengamatan dan tren dalam beban kerja Anda.
Memantau ketersediaan aplikasi dan layanan	Kurangi waktu henti dan tingkatkan kemampuan Anda untuk memenuhi target tingkat layanan dengan terus memantau ketersediaan layanan.
Melacak aplikasi	Melacak permintaan aplikasi dalam sistem dan dependensi eksternal untuk menyempurnakan kinerja, melakukan analisis akar penyebab, dan memecahkan masalah.
Membuat dasbor dan visualisasi	Buat dasbor yang berfokus pada metrik dan pengamatan yang relevan untuk sistem dan beban kerja Anda, yang membantu peningkat an berkelanjutan dan penemuan masalah secara proaktif.

CloudWatch dapat memenuhi sebagian besar persyaratan penebangan dan pemantauan, dan memberikan solusi yang andal, dapat diskalakan, dan fleksibel. BanyakAWS layanan secara otomatis menyediakan CloudWatch metrik, selain integrasi CloudWatch logging untuk pemantauan dan analisis. CloudWatch juga menyediakan agen dan driver log untuk mendukung berbagai opsi komputasi seperti server (baik di cloud maupun di tempat), kontainer, dan komputasi tanpa server. Panduan ini juga mencakupAWS layanan berikut yang digunakan dengan logging dan monitoring:

- AWS Systems ManagerDistributor, Manajer Negara Systems Manager, dan Otomatisasi Systems Manager untuk mengotomatiskan, mengkonfigurasi, dan memperbarui CloudWatch agen untuk instans EC2 dan server lokal Anda
- Amazon OpenSearch Service untuk agregasi, penelusuran, dan analisis log lanjutan
- Pemeriksaan kesehatan Amazon Route 53 dan CloudWatchSynthetics untuk memantau ketersediaan aplikasi dan layanan
- Amazon Managed Service for Prometheus untuk memantau aplikasi dalam kontainer dalam skala besar
- AWS X-Rayuntuk pelacakan aplikasi dan analisis runtime

- Amazon Managed Grafana untuk memvisualisasikan dan menganalisis data dari berbagai sumber (misalnya CloudWatch, Amazon OpenSearch Service, dan Amazon Timestream)

LayananAWS komputasi yang Anda pilih juga memengaruhi implementasi dan konfigurasi solusi logging dan monitoring Anda. Misalnya, CloudWatch implementasi dan konfigurasi berbeda untuk Amazon EC2, Amazon ECS, Amazon EKS, dan Lambda.

Pemilik aplikasi dan beban kerja seringkali dapat melupakan penebangan dan pemantauan atau mengkonfigurasi dan menerapkannya secara tidak konsisten. Ini berarti bahwa beban kerja memasuki produksi dengan observabilitas terbatas, yang menyebabkan keterlambatan dalam mengidentifikasi masalah dan meningkatkan waktu yang dibutuhkan untuk memecahkan masalah dan menyelesaikannya. Minimal, solusi logging dan monitoring Anda harus mengatasi lapisan sistem untuk log dan metrik tingkat sistem operasi (OS), selain lapisan aplikasi untuk log dan metrik aplikasi. Panduan ini menyediakan pendekatan yang direkomendasikan untuk menangani dua lapisan ini di berbagai jenis komputasi, termasuk tiga jenis komputasi yang diuraikan dalam tabel berikut.

Instans EC2 yang berjalan lama dan tidak dapat diubah	Log dan metrik sistem dan aplikasi di beberapa sistem operasi (OS) di beberapaAWS Wilayah atau akun.
Wadah	Log dan metrik sistem dan aplikasi untuk klaster Amazon ECS dan Amazon EKS Anda, termasuk contoh untuk konfigurasi yang berbeda.
Tanpa server	Log dan metrik sistem dan aplikasi untuk fungsi dan pertimbangan Lambda Anda untuk penyesuaian.

Panduan ini menyediakan solusi logging dan monitoring yang membahas CloudWatch danAWS layanan terkait di bidang-bidang berikut:

- Merencanakan CloudWatch penyebaran Anda- Pertimbangan untuk merencanakan CloudWatch penyebaran dan panduan Anda tentang memusatkan CloudWatch konfigurasi Anda.
- Mengonfigurasi CloudWatch agen untuk instans EC2 dan server lokal— rincian CloudWatch konfigurasi untuk tingkat sistem dan tingkat aplikasi logging dan metrik.

- CloudWatch pendekatan penginstalan agen untuk Amazon EC2 dan server lokal- Pendekatan untuk menginstal CloudWatch agen, termasuk penyebaran otomatis menggunakan Systems Manager di beberapa Wilayah dan akun.
- Pencatatan dan pemantauan di Amazon ECS — Panduan untuk mengonfigurasi CloudWatch pencatatan dan metrik tingkat klaster dan tingkat aplikasi di Amazon ECS.
- Pencatatan dan pemantauan di Amazon EKS — Panduan untuk mengonfigurasi CloudWatch pencatatan dan metrik tingkat klaster dan tingkat aplikasi di Amazon EKS.
- Pemantauan Prometheus di Amazon EKS— Memperkenalkan dan membandingkan Amazon Managed Service untuk Prometheus dengan pemantauan CloudWatch Container Insights untuk Prometheus.
- Pencatatan dan metrik untukAWS Lambda- Panduan untuk mengonfigurasi CloudWatch fungsi Lambda Anda.
- Mencari dan menganalisis log masuk CloudWatch— Metode untuk menganalisis log Anda menggunakan Amazon CloudWatch Application Insights, CloudWatch Logs Insights, dan memperluas analisis log ke Amazon OpenSearch Service.
- Opsi yang mengkhawatirkan dengan CloudWatch- Memperkenalkan CloudWatch Alarm dan Deteksi CloudWatch Anomali dan memberikan panduan tentang pembuatan dan pengaturan alarm.
- Memantau ketersediaan aplikasi dan layanan- Memperkenalkan dan membandingkan pemeriksaan kesehatan CloudWatch Synthetics dan Route 53 untuk pemantauan ketersediaan otomatis.
- Aplikasi penelusuran denganAWS X-Ray— Pendahuluan dan penyiapan pelacakan aplikasi menggunakan X-Ray untuk Amazon EC2, Amazon ECS, Amazon EKS, dan Lambda
- Dasbor dan visualisasi dengan CloudWatch- Pengantar CloudWatch Dasbor untuk meningkatkan observabilitas di seluruhAWS beban kerja.
- Integrasi CloudWatch denganAWSjasa— Menjelaskan bagaimana CloudWatch terintegrasi dengan berbagaiAWS layanan.
- Amazon Managed Grafana untuk dasbor dan visualisasi— Memperkenalkan dan membandingkan Amazon Managed Grafana dengan CloudWatch untuk dashboard dan visualisasi.

Contoh implementasi digunakan di seluruh panduan ini di seluruh area ini dan juga tersedia dari GitHub repositoriAWS Sampel.

Hasil bisnis yang ditargetkan

Membuat solusi logging dan monitoring yang dirancang untukAWSCloud merupakan bagian integral untuk mencapaienam keuntungan dari komputasi awan. Solusi pencatatan dan pemantauan Anda akan membantu organisasi TI Anda mencapai hasil bisnis yang menguntungkan proses bisnis, mitra bisnis, karyawan, dan pelanggan Anda. Anda dapat mengharapkan empat hasil berikut setelah menerapkan solusi logging dan monitoring selaras denganAWSWell-Architected Kerangka:

Mempercepat kesiapan operasional

Mengaktifkan solusi logging dan monitoring merupakan komponen penting dalam mempersiapkan beban kerja untuk dukungan dan penggunaan produksi. Kesiapan operasional dapat dengan cepat menjadi hambatan jika Anda terlalu bergantung pada proses manual dan juga dapat mengurangi waktu ke nilai (TTV) untuk investasi TI Anda. Pendekatan yang tidak efektif juga menghasilkan keterbatasan beban kerja Anda. Hal ini dapat meningkatkan risiko pemadaman berkepanjangan, ketidakpuasan pelanggan, dan proses bisnis yang gagal.

Anda dapat menggunakan pendekatan panduan ini untuk menstandarisasi dan mengotomatisasi pencatatan dan pemantauan Anda padaAWSCloud. Beban kerja baru kemudian memerlukan persiapan dan intervensi manual minimal untuk penebangan dan pemantauan produksi. Hal ini juga membantu mengurangi waktu dan langkah-langkah yang diperlukan untuk membuat standar logging dan monitoring pada skala untuk beban kerja yang berbeda di beberapa akun dan Wilayah.

Meningkatkan keunggulan operasional

Panduan ini menyediakan beberapa praktik terbaik untuk penebangan dan pemantauan yang membantu beragam beban kerja memenuhi tujuan bisnis dankeunggulan operasional. Panduan ini juga menyediakancontoh rinci dan open-source, template dapat digunakan kembaliyang dapat Anda gunakan dengan pendekatan infrastruktur sebagai kode (IAC) untuk menerapkan solusi logging dan monitoring yang dirancang dengan baik menggunakanAWSlayanan. Meningkatkan keunggulan operasional bersifat berulang dan membutuhkan perbaikan yang berkelanjutan. Panduan ini memberikan saran tentang cara untuk terus meningkatkan praktik penebangan dan pemantauan.

Meningkatkan visibilitas operasional

Proses dan aplikasi bisnis Anda mungkin didukung oleh sumber daya TI yang berbeda dan di-host pada jenis komputasi yang berbeda, baik di lokasi maupun diAWSCloud. Visibilitas operasional Anda dapat dibatasi oleh implementasi strategi logging dan pemantauan yang tidak konsisten dan tidak lengkap. Mengadopsi pendekatan logging dan monitoring yang komprehensif membantu Anda dengan cepat mengidentifikasi, mendiagnosis, dan menanggapi masalah di seluruh beban kerja Anda. Panduan ini membantu Anda merancang dan menerapkan pendekatan untuk meningkatkan visibilitas operasional lengkap Anda dan mengurangi waktu rata-rata untuk menyelesaikan (MTTR) kegagalan. Pendekatan logging dan monitoring yang komprehensif juga membantu organisasi Anda meningkatkan kualitas layanan, meningkatkan pengalaman pengguna akhir, dan memenuhi perjanjian tingkat layanan (SLA).

Menskalakan operasi dan mengurangi biaya overhead

Anda dapat menskalakan praktik pencatatan dan pemantauan dari panduan ini untuk mendukung beberapa Wilayah dan akun, sumber daya jangka pendek, dan beberapa lingkungan. Panduan ini menyediakan pendekatan dan contoh untuk mengotomatisasi langkah-langkah manual (misalnya menginstal dan mengkonfigurasi agen, metrik pemantauan, dan memberi tahu atau mengambil tindakan ketika masalah terjadi). Pendekatan ini sangat membantu ketika adopsi cloud Anda matang dan tumbuh dan Anda perlu menskalakan kemampuan operasional tanpa meningkatkan aktivitas atau sumber daya manajemen cloud.

Merencanakan CloudWatch penyebaran Anda

Kompleksitas dan ruang lingkup solusi logging dan monitoring tergantung pada beberapa faktor, termasuk:

- Berapa banyak lingkungan, Wilayah, dan akun yang digunakan dan bagaimana jumlah ini dapat meningkat.
- Variasi dan jenis beban kerja dan arsitektur yang ada.
- Jenis komputasi dan OS yang harus dicatat dan dipantau.
- Apakah ada lokasi dan AWS infrastruktur lokal.
- Persyaratan agregasi dan analitik dari beberapa sistem dan aplikasi.
- Persyaratan keamanan yang mencegah paparan log dan metrik yang tidak sah.
- Produk dan solusi yang harus terintegrasi dengan solusi pencatatan dan pemantauan Anda untuk mendukung proses operasional.

Anda harus secara teratur meninjau dan memperbarui solusi pencatatan dan pemantauan Anda dengan penerapan beban kerja baru atau yang diperbarui. Pembaruan untuk pencatatan, pemantauan, dan pengkhawatiran Anda harus diidentifikasi dan diterapkan saat masalah diamati. Masalah-masalah ini kemudian dapat diidentifikasi dan dicegah secara proaktif di masa depan.

Anda harus memastikan bahwa Anda secara konsisten menginstal dan mengkonfigurasi perangkat lunak dan layanan untuk menangkap dan menelan log dan metrik. Pendekatan pencatatan dan pemantauan yang mapan menggunakan layanan dan solusi vendor perangkat lunak ganda AWS atau independen (ISV) untuk domain yang berbeda (misalnya, keamanan, kinerja, jaringan, atau analitik). Setiap domain memiliki persyaratan penerapan dan konfigurasi sendiri.

Kami merekomendasikan penggunaan CloudWatch untuk menangkap dan menyerap log dan metrik untuk beberapa OS dan jenis komputasi. Banyak AWS layanan digunakan CloudWatch untuk mencatat, memantau, dan menerbitkan log dan metrik, tanpa memerlukan konfigurasi lebih lanjut. CloudWatch menyediakan agen perangkat lunak yang dapat diinstal dan dikonfigurasi untuk OS dan lingkungan yang berbeda. Bagian berikut menguraikan cara menerapkan, menginstal, dan mengonfigurasi CloudWatch agen untuk beberapa akun, Wilayah, dan konfigurasi:

Topik

- Menggunakan CloudWatch akun terpusat atau terdistribusi

- Mengelola file konfigurasi CloudWatch agen

Menggunakan CloudWatch akun terpusat atau terdistribusi

Meskipun CloudWatch dirancang untuk memantau AWS layanan atau sumber daya dalam satu akun dan Wilayah, Anda dapat menggunakan akun pusat untuk menangkap log dan metrik dari beberapa akun dan Wilayah. Jika Anda menggunakan lebih dari satu akun atau Wilayah, Anda harus mengevaluasi apakah akan menggunakan pendekatan akun terpusat atau akun individual untuk menangkap log dan metrik. Biasanya, pendekatan hybrid diperlukan untuk penyebaran multi-akun dan Multi-wilayah untuk mendukung persyaratan keamanan, analitik, operasi, dan pemilik beban kerja.

Tabel berikut memberikan area yang perlu dipertimbangkan ketika memilih untuk menggunakan pendekatan terpusat, terdistribusi, atau hibrida.

Struktur akun	Organisasi Anda mungkin memiliki beberapa akun terpisah (misalnya, akun untuk beban kerja non-produksi dan produksi) atau ribuan akun untuk aplikasi tunggal di lingkungan tertentu. Sebaiknya Anda memelihara log dan metrik aplikasi di akun tempat beban kerja berjalan, yang memberi pemilik beban kerja akses ke log dan metrik. Hal ini memungkinkan mereka untuk memiliki peran aktif dalam logging dan monitoring. Kami juga menyarankan Anda menggunak an akun logging terpisah untuk mengumpulkan semua log beban kerja untuk analisis, agregasi, tren, dan operasi terpusat. Akun logging terpisah juga dapat digunakan untuk keamanan, pengarsip an dan pemantauan, dan analitik.
Persyaratan akses	Anggota tim (misalnya, pemilik beban kerja atau pengembang) memerlukan akses ke log dan metrik untuk memecahkan masalah dan melakukan perbaikan. Log harus disimpan di akun beban kerja untuk mempermudah akses dan pemecahan masalah. Jika log dan metrik dipertahankan di akun terpisah dari beban kerja, pengguna mungkin perlu secara teratur bergantian antar akun. Menggunakan akun terpusat memberikan informasi log kepada pengguna yang berwenang tanpa memberikan akses ke akun

	beban kerja. Ini dapat menyederhanakan persyaratan akses untuk beban kerja analitik di mana agregasi diperlukan dari beban kerja yang berjalan di beberapa akun. Akun logging terpusat juga dapat memiliki opsi pencarian dan agregasi alternatif, seperti kluster OpenSearch Layanan Amazon. Amazon OpenSearch Service menyediakan kontrol akses berbutir halus hingga ke tingkat bidang untuk log Anda. Kontrol akses berbutir halus penting ketika Anda memiliki data sensitif atau rahasia yang memerlukan akses dan izin khusus.
Operasi	Banyak organisasi memiliki tim operasi dan keamanan terpusat atau organisasi eksternal untuk dukungan operasional yang memerluka n akses ke log untuk pemantauan. Pencatatan dan pemantauan terpusat dapat mempermudah identifikasi tren, pencarian, agregat, dan melakukan analitik di semua akun dan beban kerja. Jika organisasi Anda menggunakan pendekatan "Anda membangun nya, Anda menjalankannya" DevOps, maka pemilik beban kerja memerlukan pencatatan dan pemantauan informasi di akun mereka. Pendekatan hybrid mungkin diperlukan untuk memenuhi operasi pusat dan analitik, selain kepemilikan beban kerja terdistribusi.
Lingkungan	Anda dapat memilih untuk meng-host log dan metrik di lokasi pusat untuk akun produksi dan menyimpan log dan metrik untuk lingkunga n lain (misalnya, pengembangan atau pengujian) di akun yang sama atau terpisah, tergantung pada persyaratan keamanan dan arsitektu r akun. Ini membantu mencegah data sensitif yang dibuat selama produksi diakses oleh khalayak yang lebih luas.

CloudWatch menyediakan beberapa opsi untuk memproses log secara real time dengan filter CloudWatch berlangganan. Anda dapat menggunakan filter langganan untuk mengalirkan log secara real time ke AWS layanan untuk pemrosesan kustom, analisis, dan pemuatan ke sistem lain. Ini bisa sangat membantu jika Anda mengambil pendekatan hibrid di mana log dan metrik Anda tersedia di masing-masing akun dan Wilayah, selain akun dan Wilayah terpusat. Daftar berikut memberikan contoh AWS layanan yang dapat digunakan untuk ini:

- Amazon Data Firehose — Firehose menyediakan solusi streaming yang secara otomatis menskalakan dan mengubah ukuran berdasarkan volume data yang dihasilkan. Anda tidak perlu mengelola jumlah pecahan dalam aliran data Amazon Kinesis dan Anda dapat langsung terhubung ke Amazon Simple Storage Service (Amazon S3) OpenSearch , Amazon Service, atau Amazon Redshift tanpa pengkodean tambahan. Firehose adalah solusi efektif jika Anda ingin memusatkan log Anda di layanan tersebut. AWS
- Amazon Kinesis Data Streams — Kinesis Data Streams adalah solusi yang tepat jika Anda perlu mengintegrasikan dengan layanan yang Firehose tidak mendukung dan menerapkan logika pemrosesan tambahan. Anda dapat membuat tujuan CloudWatch Log Amazon di akun dan Wilayah yang menentukan aliran data Kinesis di akun pusat dan AWS Identity and Access Management peran (IAM) yang memberinya izin untuk menempatkan catatan di aliran. Kinesis Data Streams menyediakan landing zone terbuka yang fleksibel untuk data log Anda yang kemudian dapat digunakan oleh berbagai opsi. Anda dapat membaca data log Kinesis Data Streams ke akun Anda, melakukan pra-pemrosesan, dan mengirim data ke tujuan yang Anda pilih.

  Namun, Anda harus mengonfigurasi pecahan untuk aliran sehingga ukurannya sesuai untuk data log yang dihasilkan. Kinesis Data Streams bertindak sebagai perantara sementara atau antrian untuk data log Anda, dan Anda dapat menyimpan data dalam aliran Kinesis selama antara satu hingga 365 hari. Kinesis Data Streams juga mendukung kemampuan replay, yang berarti Anda dapat memutar ulang data yang tidak dikonsumsi.
- OpenSearch Layanan Amazon - CloudWatch Log dapat mengalirkan log dalam grup log ke OpenSearch klaster di akun individu atau terpusat. Saat Anda mengonfigurasi grup log untuk mengalirkan data ke OpenSearch klaster, fungsi Lambda dibuat di akun dan Wilayah yang sama dengan grup log Anda. Fungsi Lambda harus memiliki koneksi jaringan dengan cluster. OpenSearch Anda dapat menyesuaikan fungsi Lambda untuk melakukan preprocessing tambahan, selain menyesuaikan konsumsi ke Amazon Service. OpenSearch Pencatatan terpusat dengan Amazon OpenSearch Service memudahkan analisis, penelusuran, dan pemecahan masalah di beberapa komponen dalam arsitektur cloud Anda.
- Lambda - Jika Anda menggunakan Kinesis Data Streams, Anda perlu menyediakan dan mengelola sumber daya komputasi yang menggunakan data dari aliran Anda. Untuk menghindari hal ini, Anda dapat mengalirkan data log langsung ke Lambda untuk diproses dan mengirimkannya ke tujuan berdasarkan logika Anda. Ini berarti Anda tidak perlu menyediakan dan mengelola sumber daya komputasi untuk memproses data yang masuk. Jika Anda memilih untuk menggunakan Lambda, pastikan solusi Anda kompatibel dengan kuota Lambda.

Anda mungkin perlu memproses atau membagikan data log yang disimpan dalam CloudWatch Log dalam format file. Anda dapat membuat tugas ekspor untuk mengekspor grup log ke Amazon S3 untuk tanggal atau rentang waktu tertentu. Misalnya, Anda dapat memilih untuk mengekspor log setiap hari ke Amazon S3 untuk analitik dan audit. Lambda dapat digunakan untuk mengotomatiskan solusi ini. Anda juga dapat menggabungkan solusi ini dengan replikasi Amazon S3 untuk mengirimkan dan memusatkan log Anda dari beberapa akun dan Wilayah ke satu akun dan Wilayah terpusat.

Konfigurasi CloudWatch agen juga dapat menentukan `credentials` bidang di `agent`bagian tersebut. Ini menentukan peran IAM untuk digunakan saat mengirim metrik dan log ke akun yang berbeda. Jika ditentukan, bidang ini berisi `role_arn` parameter. Bidang ini dapat digunakan ketika Anda hanya memerlukan pencatatan dan pemantauan terpusat di akun dan Wilayah terpusat tertentu.

Anda juga dapat menggunakan AWS SDK untuk menulis aplikasi pemrosesan kustom Anda sendiri dalam bahasa pilihan Anda, membaca log dan metrik dari akun Anda, dan mengirim data ke akun terpusat atau tujuan lain untuk diproses dan dipantau lebih lanjut.

Mengelola file konfigurasi CloudWatch agen

Sebaiknya Anda membuat konfigurasi CloudWatch agen Amazon standar yang menyertakan log sistem dan metrik yang ingin Anda ambil di semua instans Amazon Elastic Compute Cloud (Amazon EC2) dan server lokal. Anda dapat menggunakan wizard file konfigurasi CloudWatch agen untuk membantu Anda membuat file konfigurasi. Anda dapat menjalankan wizard konfigurasi beberapa kali untuk menghasilkan konfigurasi unik untuk sistem dan lingkungan yang berbeda. Anda juga dapat memodifikasi file konfigurasi atau membuat variasi dengan menggunakan skema file konfigurasi. File konfigurasi CloudWatch agen dapat disimpan dalam parameter AWS Systems Manager Parameter Store. Anda dapat membuat parameter Parameter Store terpisah jika Anda memiliki beberapa file konfigurasi CloudWatch agen. Jika Anda menggunakan beberapa akun AWS atau Wilayah AWS, Anda harus mengelola dan memperbarui parameter Parameter Store di setiap akun dan Wilayah. Atau, Anda dapat mengelola CloudWatch konfigurasi secara terpusat sebagai file di Amazon S3 atau alat kontrol versi pilihan Anda.

`amazon-cloudwatch-agent-ctl`Skrip yang disertakan dengan CloudWatch agen memungkinkan Anda menentukan file konfigurasi, parameter Parameter Store, atau konfigurasi default agen. Konfigurasi default sejajar dengan set metrik dasar yang telah ditentukan sebelumnya dan mengonfigurasi agen untuk melaporkan metrik memori dan ruang disk. CloudWatch Namun, itu tidak

termasuk konfigurasi file log apa pun. Konfigurasi default juga diterapkan jika Anda menggunakan Systems Manager Quick Setup untuk CloudWatch agen.

Karena konfigurasi default tidak termasuk logging dan tidak disesuaikan untuk kebutuhan Anda, kami sarankan Anda membuat dan menerapkan CloudWatch konfigurasi Anda sendiri, disesuaikan dengan kebutuhan Anda.

Mengelola CloudWatch konfigurasi

Secara default, CloudWatch konfigurasi dapat disimpan dan diterapkan sebagai parameter Parameter Store atau sebagai file CloudWatch konfigurasi. Pilihan terbaik akan tergantung pada kebutuhan Anda. Pada bagian ini, kami membahas pro dan kontra untuk dua opsi ini. Solusi representatif juga dirinci untuk mengelola file CloudWatch konfigurasi untuk beberapa akun AWS dan Wilayah AWS.

Parameter Systems Manager Menyimpan parameter

Menggunakan parameter Parameter Store untuk mengelola CloudWatch konfigurasi berfungsi dengan baik jika Anda memiliki satu file konfigurasi CloudWatch agen standar yang ingin Anda terapkan dan kelola dalam satu set kecil akun dan Wilayah AWS. Ketika Anda menyimpan CloudWatch konfigurasi Anda sebagai parameter Parameter Store, Anda dapat menggunakan alat konfigurasi CloudWatch agen (`amazon-cloudwatch-agent-ctl`di Linux) untuk membaca dan menerapkan konfigurasi dari Parameter Store tanpa mengharuskan Anda untuk menyalin file konfigurasi ke instance Anda. Anda dapat menggunakan dokumen AmazonCloudWatch-ManageAgent Systems Manager Command untuk memperbarui CloudWatch konfigurasi pada beberapa instans EC2 dalam sekali proses. Karena parameter Parameter Store bersifat regional, Anda harus memperbarui dan mempertahankan CloudWatch parameter Parameter Store Anda di setiap Wilayah AWS dan akun AWS. Jika Anda memiliki beberapa CloudWatch konfigurasi yang ingin Anda terapkan ke setiap instance, Anda harus menyesuaikan dokumen AmazonCloudWatch-ManageAgent Command untuk menyertakan parameter ini.

CloudWatch file konfigurasi

Mengelola CloudWatch konfigurasi Anda sebagai file mungkin berfungsi dengan baik jika Anda memiliki banyak akun AWS dan Wilayah dan Anda mengelola beberapa file CloudWatch konfigurasi. Dengan menggunakan pendekatan ini, Anda dapat menelusuri, mengatur, dan mengelolanya dalam struktur folder. Anda dapat menerapkan aturan keamanan ke folder atau file individual untuk membatasi dan memberikan akses seperti izin pembaruan dan baca. Anda dapat membagikan dan

mentransfernya di luar AWS untuk kolaborasi. Anda dapat mengontrol versi file untuk melacak dan mengelola perubahan. Anda dapat menerapkan CloudWatch konfigurasi secara kolektif dengan menyalin file konfigurasi ke direktori konfigurasi CloudWatch agen tanpa menerapkan setiap file konfigurasi satu per satu. Untuk Linux, direktori CloudWatch konfigurasi ditemukan di`/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d`. Untuk Windows, direktori konfigurasi ditemukan di`C:\ProgramData\Amazon\AmazonCloudWatchAgent\Configs`.

Ketika Anda memulai CloudWatch agen, agen secara otomatis menambahkan setiap file yang ditemukan di direktori ini untuk membuat file konfigurasi CloudWatch komposit. File konfigurasi harus disimpan di lokasi pusat (misalnya, bucket S3) yang dapat diakses oleh akun dan Wilayah yang Anda butuhkan. Contoh solusi menggunakan pendekatan ini disediakan.

Mengatur CloudWatch konfigurasi

Terlepas dari pendekatan yang digunakan untuk mengelola CloudWatch konfigurasi Anda, atur CloudWatch konfigurasi Anda. Anda dapat mengatur konfigurasi Anda ke dalam jalur file atau Parameter Store menggunakan pendekatan seperti berikut ini.

/config/standar/jendela/ec2	Simpan file CloudWatch konfigurasi khusus Windows standar untuk Amazon EC2. Anda dapat mengkategorikan konfigurasi sistem operasi standar (OS) Anda untuk berbagai versi Windows, jenis instans EC2, dan lingkungan di bawah folder ini.
/config/standard/windows/onpremis	Simpan file CloudWatch konfigurasi standar khusus Windows untuk server lokal. Anda juga lebih lanjut mengkategorikan konfigurasi OS standar Anda untuk berbagai versi Windows, jenis server, dan lingkungan di bawah folder ini.
/config/standar/linux/ec2	Simpan file CloudWatch konfigurasi khusus Linux standar Anda untuk Amazon EC2. Anda dapat lebih lanjut mengkategorikan konfigura si OS standar Anda untuk berbagai distribus i Linux, jenis instans EC2, dan lingkungan di bawah folder ini.

/config/standard/linux/onpremis	Simpan file CloudWatch konfigurasi khusus Linux standar Anda untuk server lokal. Anda dapat lebih lanjut mengkategorikan konfigura si OS standar Anda untuk berbagai distribus i Linux, jenis server, dan lingkungan di bawah folder ini.
/config/ecs	Simpan file CloudWatch konfigurasi yang khusus untuk Amazon Elastic Container Service (Amazon ECS) Container Service (Amazon ECS) jika Anda menggunakan instans penampung Amazon ECS. Konfigurasi ini dapat ditambahkan ke konfigurasi Amazon EC2 standar untuk pencatatan dan pemantauan tingkat sistem khusus Amazon ECS.
/config/ <application_name>	Simpan file CloudWatch konfigurasi khusus aplikasi Anda. Anda dapat mengkategorikan aplikasi Anda lebih lanjut dengan folder dan awalan tambahan untuk lingkungan dan versi.

Contoh: Menyimpan file CloudWatch konfigurasi dalam bucket S3

Bagian ini memberikan contoh menggunakan Amazon S3 untuk menyimpan file CloudWatch konfigurasi dan runbook Systems Manager kustom untuk mengambil dan menerapkan file konfigurasi. CloudWatch Pendekatan ini dapat mengatasi beberapa tantangan menggunakan parameter Systems Manager Parameter Store untuk CloudWatch konfigurasi dalam skala besar:

- Jika Anda menggunakan beberapa Wilayah, Anda harus menyinkronkan pembaruan CloudWatch konfigurasi di setiap Area Parameter Store. Parameter Store adalah layanan Regional dan parameter yang sama harus diperbarui di setiap Wilayah yang menggunakan CloudWatch agen.
- Jika Anda memiliki beberapa CloudWatch konfigurasi, Anda harus memulai pengambilan dan penerapan setiap konfigurasi Parameter Store. Anda harus secara individual mengambil setiap CloudWatch konfigurasi dari Parameter Store dan juga memperbarui metode pengambilan setiap kali Anda menambahkan konfigurasi baru. Sebaliknya, CloudWatch menyediakan direktori

konfigurasi untuk menyimpan file konfigurasi dan menerapkan setiap konfigurasi dalam direktori, tanpa mengharuskannya ditentukan secara individual.

- Jika Anda menggunakan beberapa akun, Anda harus memastikan bahwa setiap akun baru memiliki CloudWatch konfigurasi yang diperlukan di Parameter Store-nya. Anda juga perlu memastikan bahwa setiap perubahan konfigurasi diterapkan ke akun ini dan Wilayah mereka di masa mendatang.

Anda dapat menyimpan CloudWatch konfigurasi di bucket S3 yang dapat diakses dari semua akun dan Wilayah Anda. Anda kemudian dapat menyalin konfigurasi ini dari bucket S3 ke direktori CloudWatch konfigurasi dengan menggunakan runbook Systems Manager Automation dan Systems Manager State Manager. Anda dapat menggunakan template CloudFormation AWS cloudwatch-config-s3-bucket.yaml untuk membuat bucket S3 yang dapat diakses dari beberapa akun dalam organisasi di AWS Organizations. Template menyertakan `OrganizationID` parameter yang memberikan akses baca ke semua akun dalam organisasi Anda.

Runbook Systems Manager sampel tambahan, yang disediakan di bagian Pengaturan Manajer Negara dan Distributor untuk penerapan CloudWatch agen dan konfigurasi panduan ini, dikonfigurasi untuk mengambil file menggunakan bucket S3 yang dibuat oleh template AWS 3-bucket.yaml. cloudwatch-config-s CloudFormation

Atau, Anda dapat menggunakan sistem kontrol versi (misalnya, GitHub atau AWS CodeCommit) untuk menyimpan file konfigurasi Anda. Jika Anda ingin secara otomatis mengambil file konfigurasi yang disimpan dalam sistem kontrol versi, Anda harus mengelola atau memusatkan penyimpanan kredensi dan memperbarui runbook Otomasi Systems Manager yang digunakan untuk mengambil kredensil di seluruh akun dan Wilayah Anda.

Mengonfigurasi CloudWatch agen untuk instans EC2 dan server lokal

Banyak organisasi menjalankan beban kerja pada server fisik dan mesin virtual (VM). Beban kerja ini biasanya berjalan pada OS yang berbeda yang masing-masing memiliki persyaratan instalasi dan konfigurasi unik untuk menangkap dan menelan metrik.

Jika Anda memilih untuk menggunakan instans EC2, Anda dapat memiliki tingkat kontrol yang tinggi atas konfigurasi instans dan OS Anda. Namun, tingkat kontrol dan tanggung jawab yang lebih tinggi ini mengharuskan Anda untuk memantau dan menyesuaikan konfigurasi untuk mencapai penggunaan yang lebih efisien. Anda dapat meningkatkan efektivitas operasional Anda dengan menetapkan standar untuk pencatatan dan pemantauan, serta menerapkan pendekatan instalasi dan konfigurasi standar untuk menangkap dan menelan log dan metrik.

Organizations yang memigrasikan atau memperluas investasi TI mereka keAWSCloud dapat memanfaatkan CloudWatch untuk mencapai solusi logging dan monitoring terpadu. CloudWatch harga berarti Anda secara bertahap membayar metrik dan log yang ingin Anda tangkap. Anda juga dapat menangkap log dan metrik untuk server lokal menggunakan yang serupa CloudWatch proses instalasi agen seperti itu untuk Amazon EC2.

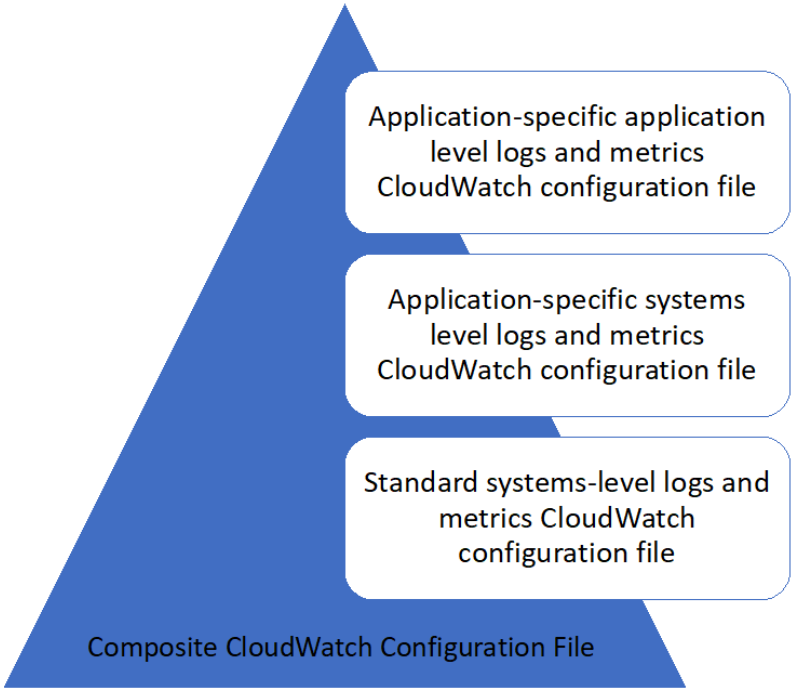
Sebelum Anda mulai menginstal dan menerapkan CloudWatch, pastikan bahwa Anda mengevaluasi konfigurasi logging dan metrik untuk sistem dan aplikasi Anda. Pastikan bahwa Anda menentukan log standar dan metrik yang perlu Anda ambil untuk OS yang ingin Anda gunakan. Log dan metrik sistem adalah dasar dan standar untuk solusi logging dan monitoring karena dihasilkan oleh OS dan berbeda untuk Linux dan Windows. Ada metrik penting dan file log yang tersedia di seluruh distribusi Linux, selain yang spesifik untuk versi Linux atau distribusi. Varians ini juga terjadi antara versi Windows yang berbeda.

Mengonfigurasi CloudWatch agen

CloudWatch menangkap metrik dan log untuk Amazon EC2 dan server lokal menggunakanAgen CloudWatch dan file konfigurasi agenyang spesifik untuk setiap OS. Sebaiknya Anda menentukan konfigurasi metrik standar organisasi dan penangkapan log sebelum Anda mulai menginstal CloudWatch agen berskala di akun Anda.

Anda dapat menggabungkan beberapa CloudWatch konfigurasi agen untuk membentuk komposit CloudWatch konfigurasi agen. Salah satu pendekatan yang disarankan adalah menentukan dan

membagi konfigurasi untuk log dan metrik Anda di tingkat sistem dan aplikasi. Diagram berikut menggambarkan bagaimana beberapa jenis file konfigurasi CloudWatch untuk kebutuhan yang berbeda dapat digabungkan untuk membentuk konfigurasi CloudWatch komposit:



Log dan metrik ini juga dapat diklasifikasikan dan dikonfigurasi lebih lanjut untuk lingkungan atau persyaratan tertentu. Misalnya, Anda dapat menentukan subset log dan metrik yang lebih kecil dengan presisi lebih rendah untuk lingkungan pengembangan yang tidak diatur, dan set yang lebih besar dan lebih lengkap dengan presisi yang lebih tinggi untuk lingkungan produksi yang diatur.

Mengkonfigurasi penangkapan log untuk instans EC2

Secara default, Amazon EC2 tidak memantau atau menangkap file log. Sebagai gantinya, file log ditangkap dan dicerna CloudWatch Log oleh CloudWatch perangkat lunak agen diinstal pada instans EC2 Anda,AWSAPI, atauAWS Command Line Interface(AWS CLI). Sebaiknya gunakan CloudWatch agen untuk menelan file log ke CloudWatch Log untuk Amazon EC2 dan server lokal.

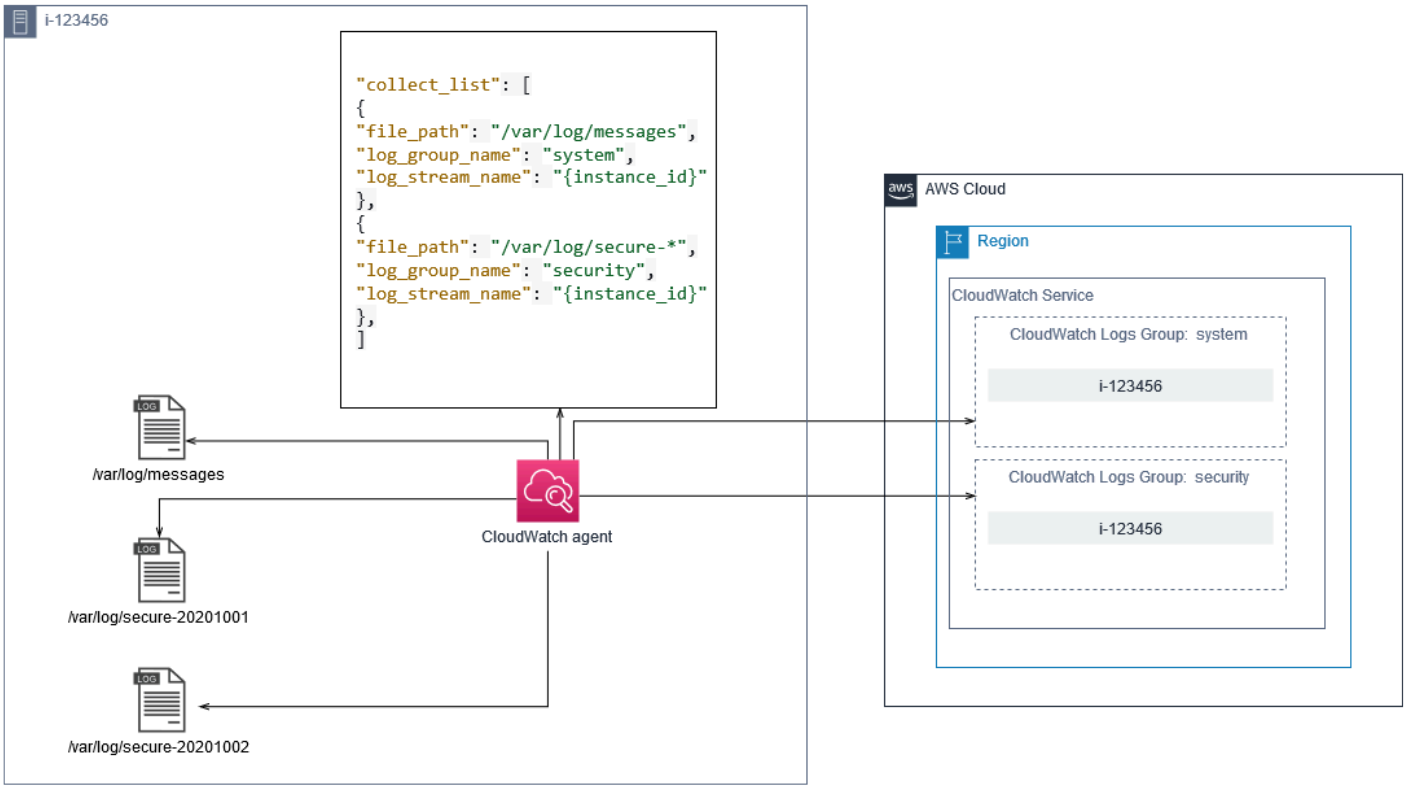
Anda dapat mencari dan memfilter log, serta mengekstrak metrik dan menjalankan otomatisasi berdasarkan patching pola dari file log di CloudWatch. CloudWatch mendukung plaintext, space delimited, dan JSON-diformat filter dan sintaks pola pilihan, dengan JSON-diformat log

memberikan fleksibilitas yang paling. Untuk meningkatkan opsi penyaringan dan analisis, Anda harus menggunakan output log yang diformat bukan teks biasa.

Parameter CloudWatch agen menggunakan file konfigurasi yang mendefinisikan log dan metrik untuk dikirim ke CloudWatch. CloudWatch kemudian menangkap setiap file log sebagaialiran logdan mengelompokkan aliran log ini kegrup log. Ini membantu Anda melakukan operasi di seluruh log dari instans EC2 Anda, seperti mencari string yang cocok.

Nama aliran log default sama dengan ID instans EC2 dan nama grup log default sama dengan path file log. Nama log harus unik dalam CloudWatch grup log. Anda dapat menggunakan`instance_id`,`hostname`,`local_hostname`, atau`ip_address`untuk substitusi dinamis dalam log stream dan log nama grup, yang berarti bahwa Anda dapat menggunakan yang sama CloudWatch File konfigurasi agen di beberapa instans EC2.

Diagram berikut menunjukkan CloudWatch konfigurasi agen untuk menangkap log. Grup log didefinisikan oleh file log yang ditangkap dan berisi aliran log terpisah untuk setiap instans EC2 karena`{instance_id}`variabel digunakan untuk nama log stream dan ID instans EC2 unik.



Grup log menentukan retensi, tag, keamanan, filter metrik, dan cakupan pencarian untuk aliran log yang dikandungnya. Perilaku pengelompokan default berdasarkan nama file log membantu Anda

mencari, membuat metrik, dan alarm pada data yang spesifik untuk file log di instans EC2 di akun dan Wilayah. Anda harus mengevaluasi apakah penyempurnaan grup log lebih lanjut diperlukan. Misalnya, akun Anda mungkin dibagikan oleh beberapa unit bisnis dan memiliki pemilik teknis atau operasi yang berbeda. Ini berarti bahwa Anda harus lebih menyempurnakan nama grup log untuk mencerminkan pemisahan dan kepemilikan. Pendekatan ini memungkinkan Anda untuk memusatkan analisis dan pemecahan masalah pada instans EC2 yang relevan.

Jika beberapa lingkungan menggunakan satu akun, Anda dapat memisahkan pencatatan untuk beban kerja yang berjalan di setiap lingkungan. Tabel berikut menunjukkan konvensi penamaan kelompok log yang mencakup unit bisnis, proyek atau aplikasi, dan lingkungan.

Nama grup log	`/<Business unit>/<Project or application name>/<Environment>/<Log file name>`
Nama pengaliran log	`<EC2 instance ID>`

Anda juga dapat mengelompokkan semua file log untuk instans EC2 ke dalam grup log yang sama. Hal ini membuat lebih mudah untuk mencari dan menganalisis di seluruh satu set file log untuk instans EC2 tunggal. Ini berguna jika sebagian besar instans EC2 Anda melayani satu aplikasi atau beban kerja dan setiap instans EC2 melayani tujuan tertentu. Tabel berikut menunjukkan bagaimana grup log dan log stream penamaan dapat diformat untuk mendukung pendekatan ini.

Nama grup log	`/<Business unit>/<Project or application name>/<Environment>/<EC2 instance ID>`
Nama pengaliran log	`<Log file name>`

Mengkonfigurasi penangkapan metrik untuk instans EC2

Secara default, instans EC2 Anda diaktifkan untuk pemantauan dasar danset standar metrik(misalnya, CPU, jaringan, atau metrik terkait penyimpanan) secara otomatis dikirim ke CloudWatch setiap lima menit. CloudWatch Metrik dapat bervariasi tergantung pada keluarga

instans, misalnya,Instance kinerja yang dapat dilonjakkanmemiliki metrik untuk kredit CPU. Metrik standar Amazon EC2 disertakan dalam harga instans Anda. Jika Anda mengaktifkanpemantauan terperinciuntuk instans EC2 Anda, Anda dapat menerima data dalam waktu satu menit. Frekuensi periode memengaruhi biaya CloudWatch Anda, jadi pastikan Anda mengevaluasi apakah pemantauan terperinci diperlukan untuk semua atau hanya beberapa instans EC2 Anda. Misalnya, Anda dapat mengaktifkan pemantauan terperinci untuk beban kerja produksi tetapi menggunakan pemantauan dasar untuk beban kerja non-produksi.

Server lokal tidak menyertakan metrik default apa pun untuk CloudWatch dan harus menggunakan CloudWatch agen,AWS CLI, atauAWSSDK untuk menangkap metrik. Ini berarti bahwa Anda harus menentukan metrik yang ingin Anda tangkap (misalnya, pemanfaatan CPU) di CloudWatch file konfigurasi. Anda dapat membuat CloudWatch file konfigurasi yang menyertakan metrik instans EC2 standar untuk server lokal Anda dan menerapkannya selain standar Anda CloudWatch konfigurasi.

Metrikdi CloudWatch didefinisikan secara unik dengan nama metrik dan dimensi nol atau lebih, dan dikelompokkan secara unik dalam namespace metrik. Metrik yang disediakan olehAWSlayanan memiliki namespace yang dimulai dengan`AWS`(misalnya,`AWS/EC2`), dan non-AWSmetrik dianggap metrik khusus. Metrik yang Anda konfigurasikan dan tangkap dengan CloudWatch agen semua dianggap metrik kustom. Karena jumlah metrik yang dibuat memengaruhi CloudWatch biaya, Anda harus mengevaluasi apakah setiap metrik diperlukan untuk semua atau hanya beberapa instans EC2 Anda. Misalnya, Anda dapat menentukan serangkaian metrik lengkap untuk beban kerja produksi tetapi menggunakan subset yang lebih kecil dari metrik ini untuk beban kerja non-produksi.

`CWAgent`adalah namespace default untuk metrik yang diterbitkan oleh CloudWatch agen. Mirip dengan grup log, namespace metrik mengatur satu set metrik sehingga mereka dapat ditemukan bersama di satu tempat. Anda harus memodifikasi namespace untuk mencerminkan unit bisnis, proyek atau aplikasi, dan lingkungan (misalnya,`/<Business unit>/<Project or application name>/<Environment>`). Pendekatan ini berguna jika beberapa beban kerja yang tidak terkait menggunakan akun yang sama. Anda juga dapat menghubungkan konvensi penamaan namespace Anda dengan CloudWatch log konvensi penamaan kelompok.

Metrik juga diidentifikasi oleh dimensi mereka, yang membantu Anda menganalisisnya terhadap serangkaian kondisi dan merupakan properti yang dicatat oleh pengamatan. Amazon EC2 termasukmetrik terpisahuntuk instans EC2 dengan`InstanceId`dan`AutoScalingGroupName`dimensi. Anda juga menerima metrik dengan`ImageId`dan`InstanceType`dimensi jika Anda mengaktifkan pemantauan terperinci. Misalnya, Amazon EC2 menyediakan metrik instans EC2 terpisah untuk pemanfaatan CPU dengan`InstanceId`dimensi, selain memisahkan metrik pemanfaatan CPU

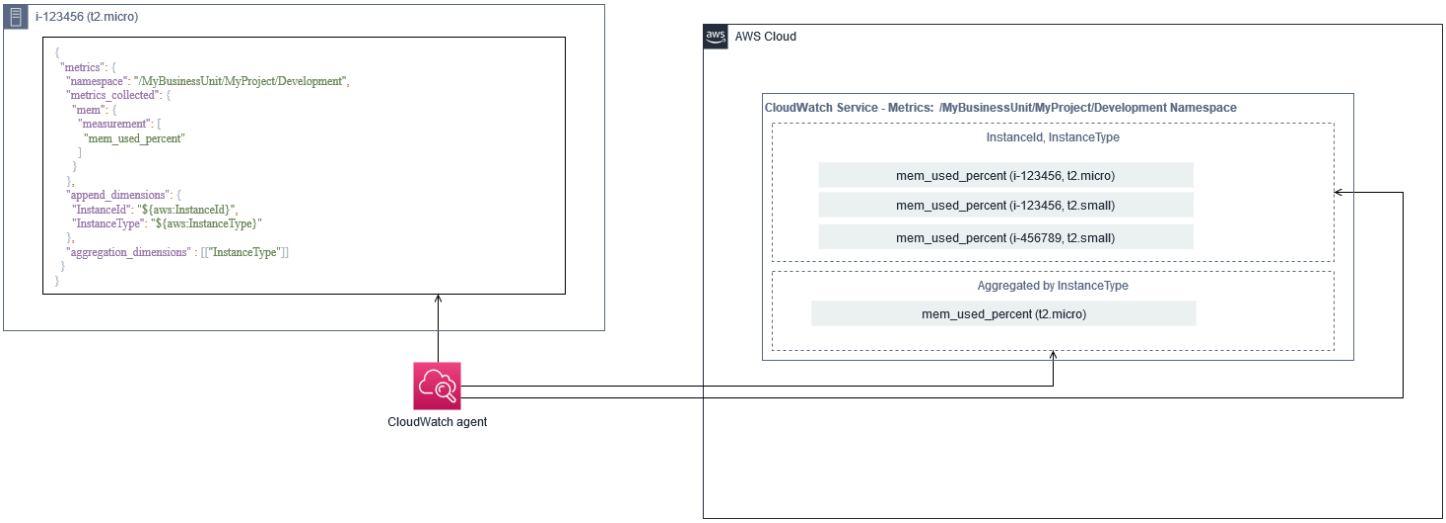
untuk`InstanceType`dimensi. Ini membantu Anda menganalisis pemanfaatan CPU untuk setiap instans EC2 yang unik, di samping semua instans EC2 dari spesifiktipe instans.

Menambahkan lebih banyak dimensi meningkatkan kemampuan analisis Anda tetapi juga meningkatkan biaya keseluruhan Anda, karena setiap kombinasi nilai dimensi metrik dan unik menghasilkan metrik baru. Misalnya, jika Anda membuat metrik untuk persentase pemanfaatan memori terhadap`InstanceId`dimensi, maka ini adalah metrik baru untuk setiap instans EC2. Jika organisasi Anda menjalankan ribuan instans EC2, hal ini menyebabkan ribuan metrik dan menghasilkan biaya yang lebih tinggi. Untuk mengontrol dan memprediksi biaya, pastikan Anda menentukan kardinalitas metrik dan dimensi mana yang menambah nilai terbanyak. Misalnya, Anda dapat menentukan serangkaian dimensi lengkap untuk metrik beban kerja produksi Anda tetapi subset yang lebih kecil dari dimensi ini untuk beban kerja non-produksi.

Anda dapat menggunakan`append_dimensions`properti untuk menambahkan dimensi ke satu atau semua metrik yang ditentukan dalam CloudWatch konfigurasi. Anda juga dapat menambahkan`ImageId`,`InstanceId`,`InstanceType`, dan`AutoScalingGroupName`untuk semua metrik di CloudWatch konfigurasi. Atau, Anda dapat menambahkan nama dimensi sewenang-wenang dan nilai untuk metrik tertentu dengan menggunakan`append_dimensions`properti pada metrik itu. CloudWatch juga dapat agregat statistik pada dimensi metrik yang Anda tetapkan dengan`aggregation_dimensions`properti.

Misalnya, Anda dapat mengumpulkan memori yang digunakan terhadap`InstanceType`dimensi untuk melihat memori rata-rata yang digunakan oleh semua instans EC2 untuk setiap jenis instans. Jika Anda menggunakan`t2.micro`instans yang berjalan di Wilayah, Anda dapat menentukan apakah beban kerja menggunakan`t2.micro`kelas overutilizing atau underutilizing memori yang disediakan. Underutilization mungkin merupakan tanda beban kerja menggunakan kelas EC2 dengan kapasitas memori yang tidak diperlukan. Sebaliknya, kelebihan pemanfaatan mungkin merupakan tanda beban kerja yang menggunakan kelas Amazon EC2 dengan memori yang tidak mencukupi.

Diagram berikut menunjukkan sampel CloudWatch konfigurasi metrik yang menggunakan namespace kustom, dimensi ditambahkan, dan agregasi oleh`InstanceType`.



Tingkat sistem CloudWatch konfigurasi

Metrik dan log tingkat sistem adalah komponen sentral dari solusi pemantauan dan penebangan, dan CloudWatch agen memiliki opsi konfigurasi khusus untuk Windows dan Linux.

Sebaiknya Anda menggunakanWizard berkas konfigurasi CloudWatchatau skema file konfigurasi untuk menentukan CloudWatch file konfigurasi agen untuk setiap OS yang Anda berencana untuk mendukung. Tambahan beban kerja khusus, log tingkat OS dan metrik dapat didefinisikan secara terpisah CloudWatch file konfigurasi dan ditambahkan ke konfigurasi standar. File konfigurasi unik ini harus disimpan secara terpisah dalam bucket S3 di mana file tersebut dapat diambil oleh instans EC2 Anda. Contoh setup bucket S3 untuk tujuan ini dijelaskan dalamMengelola CloudWatch konfigurasibagian dari panduan ini. Anda dapat secara otomatis mengambil dan menerapkan konfigurasi ini menggunakan State Manager dan Distributor.

Konfigurasi log tingkat sistem

Log tingkat sistem sangat penting untuk mendiagnosis dan memecahkan masalah di tempat atau diAWSCloud. Pendekatan pengambilan log Anda harus menyertakan log sistem dan keamanan yang dihasilkan oleh OS. File log yang dihasilkan OS mungkin berbeda tergantung pada versi OS.

Parameter CloudWatch agen mendukung pemantauan Windows peristiwa log dengan memberikan nama log peristiwa. Anda dapat memilih log acara Windows yang ingin Anda pantau (misalnya`System`,`Application`, atau`Security`).

Sistem, aplikasi, dan log keamanan untuk sistem Linux biasanya disimpan dalam`/var/log`direktori. Tabel berikut mendefinisikan file log default umum yang harus Anda pantau, tetapi Anda harus

memeriksa`/etc/rsyslog.conf`atau`/etc/syslog.conf`file untuk menentukan pengaturan spesifik untuk file log sistem Anda.

Distribusi Fedora	`/var/log/boot.log*` — Bootup log
(Amazon Linux, CentOS, Red Hat Enterprise Linux)	`/var/log/dmesg` — Log Kernel
	`/var/log/secure` — Log keamanan dan otentikasi
	`/var/log/messages` — Log sistem umum
	`/var/log/cron*` — Log Cron
	`/var/log/cloud-init-output.log` — Output dari`Userdata`skrip perusahaan rintisan
Debian	`/var/log/syslog` — Bootup log
(Ubuntu)	`/var/log/cloud-init-output.log` — Output dari`Userdata`skrip perusahaan rintisan
	`/var/log/auth.log` — Log keamanan dan otentikasi
	`/var/log/kern.log` — Log Kernel

Organisasi Anda mungkin juga memiliki agen atau komponen sistem lain yang menghasilkan log yang ingin Anda pantau. Anda harus mengevaluasi dan memutuskan file log mana yang dihasilkan oleh agen atau aplikasi ini, dan memasukkannya ke dalam konfigurasi Anda dengan mengidentifikasi lokasi file mereka. Misalnya, Anda harus menyertakan Systems Manager dan CloudWatch log agen dalam konfigurasi Anda. Tabel berikut menyediakan lokasi log agen ini untuk Windows dan Linux.

Windows	Agen CloudWatch	`$Env:ProgramData\Amazon\AmazonCloudWatchAgent\Logs\ama`

		zon-cloudwatch-agent.log
	Agen Systems Manager	%PROGRAMDATA%\Amazon\SSM\Logs\amazon-ssm-agent.log %PROGRAMDATA%\Amazon\SSM\Logs\errors.log %PROGRAMDATA%\Amazon\SSM\Logs\audits\amazon-ssm-agent-audit-YYYY-MM-DD
Linux	Agen CloudWatch	/opt/aws/amazon-cloudwatch-agent/logs/amazon-cloudwatch-agent.log
	Agen Systems Manager	/var/log/amazon/ssm/amazon-ssm-agent.log /var/log/amazon/ssm/errors.log /var/log/amazon/ssm/audits/amazon-ssm-agent-audit-YYYY-MM-DD

CloudWatch mengabaikan file log jika file log didefinisikan dalam CloudWatch konfigurasi agen tetapi tidak ditemukan. Ini berguna ketika Anda ingin mempertahankan konfigurasi log tunggal untuk Linux, bukan konfigurasi terpisah untuk setiap distribusi. Hal ini juga berguna ketika file log tidak ada sampai agen atau aplikasi perangkat lunak mulai berjalan.

Konfigurasi metrik tingkat sistem

Pemanfaatan memori dan ruang disk tidak disertakan dalam metrik standar yang disediakan oleh Amazon EC2. Untuk menyertakan metrik ini, Anda harus menginstal dan mengonfigurasi CloudWatch agen pada instans EC2 Anda. Parameter CloudWatch penyihir konfigurasi agen menciptakan CloudWatch konfigurasi denganmetrik yang telah ditetapkandan Anda dapat menambahkan atau menghapus metrik sesuai kebutuhan. Pastikan bahwa Anda meninjau set metrik yang telah ditetapkan untuk menentukan tingkat yang sesuai yang Anda butuhkan.

Pengguna akhir dan pemilik beban kerja harus mempublikasikan metrik sistem tambahan berdasarkan persyaratan khusus untuk server atau instans EC2. Definisi metrik ini harus disimpan, diversi, dan dipelihara secara terpisah CloudWatch file konfigurasi agen, dan dibagikan di lokasi pusat (misalnya, Amazon S3) untuk digunakan kembali dan otomatisasi.

Metrik standar Amazon EC2 tidak secara otomatis ditangkap di server lokal. Metrik ini harus didefinisikan dalam CloudWatch file konfigurasi agen yang digunakan oleh instans lokal. Anda dapat membuat file konfigurasi metrik terpisah untuk instans lokal dengan metrik seperti pemanfaatan CPU, dan metrik ini ditambahkan ke file konfigurasi metrik standar.

Tingkat aplikasi CloudWatch konfigurasi

Log dan metrik aplikasi dihasilkan dengan menjalankan aplikasi dan aplikasi spesifik. Pastikan bahwa Anda menentukan log dan metrik yang diperlukan untuk memantau aplikasi yang secara teratur digunakan oleh organisasi Anda. Misalnya, organisasi Anda mungkin telah standar di Microsoft Internet Information Server (IIS) untuk aplikasi berbasis web. Anda dapat membuat log standar dan metrik CloudWatch konfigurasi untuk IIS yang juga dapat digunakan di seluruh organisasi Anda. File konfigurasi spesifik aplikasi dapat disimpan di lokasi terpusat (misalnya, bucket S3) dan diakses oleh pemilik beban kerja atau melalui pengambilan otomatis, dan disalin ke CloudWatch direktori konfigurasi. Parameter CloudWatch agen secara otomatis menggabungkan file konfigurasi CloudWatch yang ditemukan di direktori file konfigurasi setiap instans EC2 atau server menjadi komposit CloudWatch konfigurasi. Hasil akhirnya adalah CloudWatch konfigurasi yang mencakup konfigurasi tingkat sistem standar organisasi Anda, serta semua tingkat aplikasi yang relevan CloudWatch konfigurasi.

Pemilik beban kerja harus mengidentifikasi dan mengkonfigurasi file log dan metrik untuk semua aplikasi dan komponen penting.

Mengkonfigurasi log tingkat aplikasi

Aplikasi-tingkat logging bervariasi tergantung pada apakah aplikasi adalah komersial off-the-shelf (COTS) atau aplikasi yang dikembangkan khusus. Aplikasi COTS dan komponennya mungkin menyediakan beberapa opsi untuk konfigurasi log dan output, seperti tingkat detail log, format file log, dan lokasi file log. Namun, sebagian besar aplikasi COTS atau pihak ketiga tidak mengizinkan Anda mengubah logging secara mendasar (misalnya, memperbarui kode aplikasi untuk menyertakan pernyataan log tambahan atau format yang tidak dapat dikonfigurasi). Minimal, Anda harus mengkonfigurasi opsi logging untuk aplikasi COTS atau pihak ketiga untuk mencatat peringatan dan informasi tingkat kesalahan, sebaiknya dalam format JSON.

Anda dapat mengintegrasikan aplikasi yang dikembangkan khusus dengan CloudWatch Log dengan menyertakan file log aplikasi di CloudWatch konfigurasi. Aplikasi khusus memberikan kualitas dan kontrol log yang lebih baik karena Anda dapat menyesuaikan format output log, mengkategorikan dan memisahkan output komponen untuk memisahkan file log, selain menyertakan rincian tambahan yang diperlukan. Pastikan Anda meninjau dan menstandarisasi pada pustaka logging dan data dan pemformatan yang diperlukan untuk organisasi Anda sehingga analitik dan pemrosesan menjadi lebih mudah.

Anda juga dapat menulis ke CloudWatch aliran log dengan CloudWatch Beberapa catatan`PutLogEvents`API panggilan atau dengan menggunakanAWSSDK. Anda dapat menggunakan API atau SDK untuk persyaratan logging kustom, seperti mengkoordinasikan pencatatan ke aliran log tunggal di seperangkat komponen dan server yang terdistribusi. Namun, solusi termudah untuk mempertahankan dan paling banyak berlaku adalah mengkonfigurasi aplikasi Anda untuk menulis ke file log dan kemudian menggunakan CloudWatch agen untuk membaca dan streaming file log ke CloudWatch.

Anda juga harus mempertimbangkan jenis metrik yang ingin Anda ukur dari file log aplikasi Anda. Anda dapat menggunakan filter metrik untuk mengukur, grafik, dan alarm pada data ini dalam CloudWatch grup log. Misalnya, Anda dapat menggunakan filter metrik untuk menghitung upaya masuk yang gagal dengan mengidentifikasi mereka di log Anda.

Anda juga dapat membuat metrik khusus untuk aplikasi yang dikembangkan khusus dengan menggunakanMetrik tertanam CloudWatchformatdalam file log aplikasi Anda.

Konfigurasi metrik tingkat aplikasi

Metrik khusus adalah metrik yang tidak disediakan secara langsung olehAWSlayanan CloudWatch dan mereka diterbitkan dalam namespace kustom di CloudWatch metrik. Semua metrik aplikasi

dianggap kustom CloudWatch metrik. Metrik aplikasi mungkin sejajar dengan instans EC2, komponen aplikasi, panggilan API, atau bahkan fungsi bisnis. Anda juga harus mempertimbangkan pentingnya dan kardinalitas dimensi yang Anda pilih untuk metrik Anda. Dimensi dengan kardinalitas tinggi menghasilkan sejumlah besar metrik kustom dan dapat meningkatkan CloudWatch biaya.

CloudWatch membantu Anda menangkap metrik tingkat aplikasi dengan berbagai cara, termasuk yang berikut ini:

- Tangkap metrik tingkat proses dengan menentukan proses individual yang ingin Anda tangkap dariplugin procstat.
- Aplikasi menerbitkan metrik untuk Windows Performance Monitor dan metrik ini didefinisikan dalam CloudWatch konfigurasi.
- Filter dan pola metrik diterapkan terhadap log aplikasi di CloudWatch.
- Sebuah aplikasi menulis ke CloudWatch log dengan menggunakan CloudWatch Format metrik tertanam.
- Aplikasi mengirimkan metrik ke CloudWatch melalui API atauAWSSDK.
- Aplikasi mengirimkan metrik kecollectdatauStatsDdaemon dengan dikonfigurasi CloudWatch agen.

Anda dapat menggunakan procstat untuk memantau dan mengukur proses aplikasi penting dengan agen CloudWatch. Ini membantu Anda untuk meningkatkan alarm dan mengambil tindakan (misalnya, pemberitahuan atau proses restart) jika proses kritis tidak lagi berjalan untuk aplikasi Anda. Anda juga dapat mengukur karakteristik kinerja proses aplikasi Anda dan meningkatkan alarm jika proses tertentu bertindak tidak normal.

Pemantauan procstat juga berguna jika Anda tidak dapat memperbarui aplikasi COTS Anda dengan metrik khusus tambahan. Misalnya, Anda dapat membuat`my_process`metrik yang mengukur`cpu_time`dan termasuk kebiasaan`application_version`dimensi. Anda juga dapat menggunakan banyak CloudWatch file konfigurasi agen untuk aplikasi jika Anda memiliki dimensi yang berbeda untuk metrik yang berbeda.

Jika aplikasi Anda berjalan pada Windows, Anda harus mengevaluasi apakah sudah menerbitkan metrik untuk Windows Performance Monitor. Banyak aplikasi COTS terintegrasi dengan Windows Performance Monitor, yang membantu Anda dengan mudah memantau metrik aplikasi. CloudWatch juga terintegrasi dengan Windows Performance Monitor dan Anda dapat menangkap metrik yang sudah tersedia di dalamnya.

Pastikan Anda meninjau format logging dan informasi log yang disediakan oleh aplikasi Anda untuk menentukan metrik mana yang dapat diekstraksi dengan filter metrik. Anda dapat meninjau log historis untuk aplikasi untuk menentukan bagaimana pesan kesalahan dan shutdown abnormal diwakili. Anda juga harus meninjau masalah yang dilaporkan sebelumnya untuk menentukan apakah metrik dapat ditangkap untuk mencegah masalah berulang. Anda juga harus meninjau dokumentasi aplikasi dan meminta pengembang aplikasi untuk mengkonfirmasi bagaimana pesan kesalahan dapat diidentifikasi.

Untuk aplikasi yang dikembangkan khusus, bekerja dengan pengembang aplikasi untuk menentukan metrik penting yang dapat diimplementasikan dengan menggunakan CloudWatch Format metrik tertanam,AWSSDK, atauAWSAPI Pendekatan yang disarankan adalah menggunakan format metrik tertanam. Anda dapat menggunakanAWSmenyediakan pustaka format metrik tertanam open-source untuk membantu Anda menulis pernyataan Anda dalam format yang diperlukan. Anda juga perlu memperbaruispesifik aplikasi CloudWatch konfigurasiuntuk memasukkan agen format metrik tertanam. Hal ini menyebabkan agen berjalan pada instans EC2 bertindak sebagai endpoint format metrik tertanam lokal yang mengirimkan metrik format metrik tertanam ke CloudWatch.

Jika aplikasi Anda sudah mendukung metrik penerbitan untuk collectd atau statsd, Anda dapat memanfaatkannya untuk menelan metrik ke CloudWatch.

CloudWatch pendekatan penginstalan agen untuk Amazon EC2 dan server lokal

Mengotomatiskan proses instalasi CloudWatch agen membantu Anda menerapkannya dengan cepat dan konsisten serta menangkap log dan metrik yang diperlukan. Ada beberapa pendekatan untuk mengotomatisasi instalasi CloudWatch agen, termasuk dukungan multi-akun dan Multi-wilayah. Pendekatan instalasi otomatis berikut dibahas:

- Menginstal CloudWatch agen menggunakan Distributor Systems Manager dan Manajer Negara Systems Manager — Sebaiknya gunakan pendekatan ini jika EC2 instans dan server lokal Anda menjalankan agen Systems Manager. Ini memastikan bahwa CloudWatch agen terus diperbarui dan Anda dapat melaporkan dan memulihkan server yang tidak memiliki CloudWatch agen. Pendekatan ini juga menskalakan untuk mendukung beberapa akun dan Wilayah.
- Menyebarkan CloudWatch agen sebagai bagian dari skrip data pengguna selama penyediaan EC2 instans - Amazon EC2 memungkinkan Anda menentukan skrip startup yang dijalankan saat pertama kali boot atau reboot. Anda dapat menentukan skrip untuk mengotomatiskan proses pengunduhan dan instalasi agen. Ini juga dapat dimasukkan dalam AWS CloudFormation skrip dan produk AWS Service Catalog. Pendekatan ini mungkin sesuai dengan kebutuhan jika ada pendekatan instalasi dan konfigurasi agen yang disesuaikan untuk beban kerja tertentu yang menyimpang dari standar Anda.
- Termasuk CloudWatch agen di Amazon Machine Images (AMIs) - Anda dapat menginstal CloudWatch agen di kustom Anda AMIs untuk AmazonEC2. EC2Contoh yang menggunakan agen AMI akan secara otomatis menginstal dan memulai agen. Namun, Anda harus memastikan agen dan konfigurasinya diperbarui secara berkala.

Instalasi CloudWatch agen menggunakan Systems Manager Distributor dan State Manager

Anda dapat menggunakan Systems Manager State Manager dengan Systems Manager Distributor untuk menginstal dan memperbarui CloudWatch agen secara otomatis di server dan EC2 instans. Distributor menyertakan paket `AmazonCloudWatchAgent` AWS terkelola yang menginstal versi CloudWatch agen terbaru.

Pendekatan instalasi ini memiliki prasyarat berikut:

- Agen Systems Manager harus diinstal dan berjalan di server atau EC2 instans Anda. Agen Systems Manager sudah diinstal sebelumnya di Amazon Linux, Amazon Linux 2, dan beberapaAMIs. Agen juga harus diinstal dan dikonfigurasi pada gambar lain atau lokal VMs dan server.

> **Note**
>
> Amazon Linux 2 mendekati akhir dukungan. Untuk informasi selengkapnya, lihat Amazon Linux 2 FAQs.

- IAMPeran atau kredensional yang memiliki izin yang diperlukan CloudWatch dan Systems Manager harus dilampirkan ke EC2 instance atau ditentukan dalam file kredensil untuk server lokal. Misalnya, Anda dapat membuat IAM peran yang menyertakan kebijakan AWS terkelola: `AmazonSSMManagedInstanceCore` untuk Systems Manager dan `CloudWatchAgentServerPolicy` for CloudWatch. Anda dapat menggunakan ssm-cloudwatch-instance-role AWS CloudFormation template.yaml untuk menerapkan IAM peran dan profil instance yang menyertakan kedua kebijakan ini. Template ini juga dapat dimodifikasi untuk menyertakan IAM izin standar lainnya untuk EC2 instance Anda. Untuk server lokal atauVMs, harus mengonfigurasi CloudWatch agen untuk menggunakan peran layanan Systems Manager yang dikonfigurasi untuk server lokal. Untuk informasi selengkapnya tentang hal ini, lihat Bagaimana cara mengonfigurasi server lokal yang menggunakan Agen Systems Manager dan CloudWatch agen terpadu agar hanya menggunakan kredensil sementara? di pusat AWS pengetahuan.

Daftar berikut memberikan beberapa keuntungan untuk menggunakan pendekatan Systems Manager Distributor dan State Manager untuk menginstal dan memelihara CloudWatch agen:

- Instalasi otomatis untuk beberapa OSs - Anda tidak perlu menulis dan memelihara skrip untuk setiap OS untuk mengunduh dan menginstal CloudWatch agen.
- Pemeriksaan pembaruan otomatis — Manajer Negara secara otomatis dan teratur memeriksa apakah setiap EC2 instance memiliki CloudWatch versi terbaru.
- Pelaporan kepatuhan — Dasbor kepatuhan Systems Manager menunjukkan EC2 contoh mana yang gagal menginstal paket Distributor dengan sukses.
- Instalasi otomatis untuk EC2 instans yang baru diluncurkan — EC2 Instans baru yang diluncurkan ke akun Anda secara otomatis menerima agen. CloudWatch

Namun, Anda juga harus mempertimbangkan tiga bidang berikut sebelum Anda memilih pendekatan ini:

- Tabrakan dengan asosiasi yang ada — Jika asosiasi lain sudah menginstal atau mengonfigurasi CloudWatch agen, maka kedua asosiasi tersebut dapat saling mengganggu dan berpotensi menyebabkan masalah. Saat menggunakan pendekatan ini, Anda harus menghapus asosiasi yang ada yang menginstal atau memperbarui CloudWatch agen dan konfigurasi.
- Memperbarui file konfigurasi agen kustom - Distributor melakukan instalasi dengan menggunakan file konfigurasi default. Jika Anda menggunakan file konfigurasi khusus atau beberapa file CloudWatch konfigurasi, Anda harus memperbarui konfigurasi setelah instalasi.
- Pengaturan Multi-Wilayah atau multi-akun - Asosiasi Manajer Negara harus diatur di setiap akun dan Wilayah. Akun baru di lingkungan multi-akun harus diperbarui untuk menyertakan asosiasi Manajer Negara. Anda perlu memusatkan atau menyinkronkan CloudWatch konfigurasi sehingga beberapa akun dan Wilayah dapat mengambil dan menerapkan standar yang Anda perlukan.

Menyiapkan State Manager dan Distributor untuk penyebaran dan konfigurasi CloudWatch agen

Anda dapat menggunakan Systems Manager Quick Setup untuk mengonfigurasi fitur Systems Manager dengan cepat, termasuk menginstal dan memperbarui CloudWatch agen secara otomatis pada EC2 instans Anda. Pengaturan Cepat menyebarkan AWS CloudFormation tumpukan yang menyebarkan dan mengonfigurasi sumber daya Systems Manager berdasarkan pilihan Anda.

Daftar berikut menyediakan dua tindakan penting yang dilakukan oleh Quick Setup untuk instalasi dan pembaruan CloudWatch agen otomatis:

1. Buat dokumen kustom Systems Manager — Quick Setup membuat dokumen Systems Manager berikut untuk digunakan dengan State Manager. Nama dokumen mungkin berbeda tetapi isinya tetap sama:
   - `CreateAndAttachIAMToInstance`— Membuat profil `AmazonSSMRoleForInstancesQuickSetup` peran dan contoh jika tidak ada dan melampirkan `AmazonSSMManagedInstanceCore` kebijakan ke peran tersebut. Ini tidak termasuk `CloudWatchAgentServerPolicy` IAM kebijakan yang diperlukan. Anda harus memperbarui kebijakan ini dan memperbarui dokumen Systems Manager ini untuk menyertakan kebijakan ini seperti yang dijelaskan di bagian berikut.

- `InstallAndManageCloudWatchDocument`— Menginstal CloudWatch agen dengan Distributor dan mengonfigurasi setiap EC2 instance satu kali dengan konfigurasi CloudWatch agen default menggunakan dokumen `AWS-ConfigureAWSPackage` Systems Manager.
- `UpdateCloudWatchDocument`— Memperbarui CloudWatch agen dengan menginstal CloudWatch agen terbaru menggunakan dokumen `AWS-ConfigureAWSPackage` Systems Manager. Memperbarui atau menghapus instalan agen tidak menghapus file CloudWatch konfigurasi yang ada dari EC2 instance.

2. Buat asosiasi State Manager — Asosiasi State Manager dibuat dan dikonfigurasi untuk menggunakan dokumen Systems Manager yang dibuat khusus. Nama asosiasi Manajer Negara mungkin berbeda tetapi konfigurasinya tetap sama:
   - `ManageCloudWatchAgent`— Menjalankan dokumen `InstallAndManageCloudWatchDocument` Systems Manager satu kali untuk setiap EC2 instance.
   - `UpdateCloudWatchAgent`— Menjalankan dokumen `UpdateCloudWatchDocument` Systems Manager setiap 30 hari untuk setiap EC2 instance.
   - Menjalankan dokumen `CreateAndAttachIAMToInstance` Systems Manager satu kali untuk setiap EC2 instance.

Anda harus menambah dan menyesuaikan konfigurasi Quick Setup yang telah selesai untuk menyertakan CloudWatch izin dan mendukung konfigurasi kustom CloudWatch . Secara khusus, `CreateAndAttachIAMToInstance` dan `InstallAndManageCloudWatchDocument` dokumen perlu diperbarui. Anda dapat memperbarui dokumen Systems Manager yang dibuat oleh Quick Setup secara manual. Atau, Anda dapat menggunakan CloudFormation template Anda sendiri untuk menyediakan sumber daya yang sama dengan pembaruan yang diperlukan serta mengkonfigurasi dan menyebarkan sumber daya Systems Manager lainnya dan tidak menggunakan Quick Setup.

> **Important**
>
> Quick Setup membuat AWS CloudFormation tumpukan untuk menyebarkan dan mengonfigurasi sumber daya Systems Manager berdasarkan pilihan Anda. Jika memperbarui pilihan Pengaturan Cepat, Anda mungkin perlu memperbarui ulang dokumen Systems Manager secara manual.

Bagian berikut menjelaskan cara memperbarui sumber daya Systems Manager yang dibuat oleh Quick Setup secara manual, serta menggunakan AWS CloudFormation template Anda sendiri untuk melakukan Quick Setup yang diperbarui. Kami menyarankan Anda menggunakan AWS CloudFormation template Anda sendiri untuk menghindari memperbarui sumber daya secara manual yang dibuat oleh Quick Setup dan AWS CloudFormation.

Gunakan Pengaturan Cepat Systems Manager dan perbarui sumber daya Systems Manager yang dibuat secara manual

Sumber daya Systems Manager yang dibuat oleh pendekatan Quick Setup harus diperbarui untuk menyertakan izin CloudWatch agen yang diperlukan dan mendukung beberapa file CloudWatch konfigurasi. Bagian ini menjelaskan cara memperbarui IAM peran dan dokumen Systems Manager agar menggunakan bucket S3 terpusat yang berisi CloudWatch konfigurasi yang dapat diakses dari beberapa akun. Membuat bucket S3 untuk menyimpan file CloudWatch konfigurasi dibahas di Mengelola CloudWatch konfigurasi bagian panduan ini.

Perbarui dokumen **`CreateAndAttachIAMToInstance`** Systems Manager

Dokumen Systems Manager yang dibuat oleh Quick Setup ini memeriksa apakah sebuah EC2 instance memiliki profil IAM instans yang ada yang melekat padanya. Jika ya, itu melampirkan `AmazonSSMManagedInstanceCore` kebijakan ke peran yang ada. Ini melindungi EC2 instans yang ada dari kehilangan AWS izin yang mungkin ditetapkan melalui profil instans yang ada. Anda perlu menambahkan langkah dalam dokumen ini untuk melampirkan `CloudWatchAgentServerPolicy` IAM kebijakan ke EC2 instance yang sudah memiliki profil instance terlampir. Dokumen Systems Manager juga membuat IAM peran jika tidak ada dan EC2 instance tidak memiliki profil instance yang dilampirkan padanya. Anda harus memperbarui bagian dokumen ini untuk juga menyertakan `CloudWatchAgentServerPolicy` IAM kebijakan.

Tinjau dokumen CreateAndAttachIAMToInstancesampel.yaml yang telah selesai dan bandingkan dengan dokumen yang dibuat oleh Quick Setup. Edit dokumen yang ada untuk menyertakan langkah dan perubahan yang diperlukan. Berdasarkan pilihan Quick Setup, dokumen yang dibuat oleh Quick Setup mungkin berbeda dari dokumen sampel yang disediakan, jadi pastikan Anda melakukan penyesuaian yang diperlukan. Dokumen sampel menyertakan pilihan opsi Quick Setup untuk memindai instance untuk patch yang hilang setiap hari dan oleh karena itu menyertakan kebijakan untuk Systems Manager Patch Manager.

Perbarui dokumen **`InstallAndManageCloudWatchDocument`** Systems Manager

Dokumen Systems Manager yang dibuat oleh Quick Setup ini menginstal CloudWatch agen dan mengonfigurasinya dengan konfigurasi CloudWatch agen default. CloudWatch Konfigurasi default sejajar dengan set metrik dasar yang telah ditentukan sebelumnya. Anda harus mengganti langkah konfigurasi default dan menambahkan langkah-langkah untuk mengunduh file CloudWatch konfigurasi Anda dari bucket S3 CloudWatch konfigurasi Anda.

Tinjau dokumen yang diperbarui InstallAndManageCloudWatchDocument.yaml yang telah selesai dan bandingkan dengan dokumen yang dibuat oleh Quick Setup. Dokumen yang dibuat oleh Quick Setup Anda mungkin berbeda, jadi pastikan Anda telah membuat penyesuaian yang diperlukan. Edit dokumen Anda yang ada untuk menyertakan langkah dan perubahan yang diperlukan.

Gunakan AWS CloudFormation alih-alih Pengaturan Cepat

Alih-alih menggunakan Quick Setup, Anda dapat menggunakan AWS CloudFormation untuk mengkonfigurasi Systems Manager. Pendekatan ini memungkinkan Anda untuk menyesuaikan konfigurasi Systems Manager sesuai dengan kebutuhan spesifik Anda. Pendekatan ini juga menghindari pembaruan manual ke sumber daya Systems Manager yang dikonfigurasi yang dibuat oleh Quick Setup untuk mendukung CloudWatch konfigurasi kustom.

Fitur Quick Setup juga menggunakan AWS CloudFormation dan membuat kumpulan AWS CloudFormation tumpukan untuk menyebarkan dan mengkonfigurasi sumber daya Systems Manager berdasarkan pilihan Anda. Sebelum dapat menggunakan kumpulan AWS CloudFormation tumpukan, Anda harus membuat IAM peran yang digunakan AWS CloudFormation StackSets untuk mendukung penerapan di beberapa akun atau Wilayah. Pengaturan Cepat menciptakan peran yang diperlukan untuk mendukung penerapan Multi-wilayah atau multi-akun. AWS CloudFormation StackSets Anda harus menyelesaikan prasyarat AWS CloudFormation StackSets jika Anda ingin mengonfigurasi dan menerapkan sumber daya Systems Manager di beberapa Wilayah atau beberapa akun dari satu akun dan Wilayah. Untuk informasi selengkapnya tentang ini, lihat Prasyarat untuk operasi set tumpukan dalam dokumentasi. AWS CloudFormation

Tinjau AWS CloudFormation template AWS- QuickSetup - SSMHostMgmt .yaml untuk Pengaturan Cepat yang disesuaikan.

Anda harus meninjau sumber daya dan kemampuan dalam AWS CloudFormation template dan membuat penyesuaian sesuai dengan kebutuhan Anda. Anda harus mengontrol versi AWS CloudFormation template yang Anda gunakan dan secara bertahap menguji perubahan untuk mengonfirmasi hasil yang diperlukan. Selain itu, Anda harus melakukan tinjauan keamanan cloud

untuk menentukan apakah ada penyesuaian kebijakan yang diperlukan berdasarkan persyaratan organisasi Anda.

Anda harus menerapkan AWS CloudFormation tumpukan dalam satu akun pengujian dan Wilayah, dan melakukan kasus pengujian yang diperlukan untuk menyesuaikan dan mengonfirmasi hasil yang diinginkan. Anda kemudian dapat melanjutkan penerapan Anda ke beberapa Wilayah dalam satu akun, lalu ke beberapa akun dan beberapa wilayah.

Pengaturan Cepat yang Disesuaikan dalam satu akun dan Wilayah dengan AWS CloudFormation tumpukan

Jika Anda hanya menggunakan satu akun dan Wilayah, Anda dapat menerapkan contoh lengkap sebagai AWS CloudFormation tumpukan alih-alih kumpulan AWS CloudFormation tumpukan. Namun jika memungkinkan, kami menyarankan Anda menggunakan pendekatan set tumpukan multi-akun, Multi-wilayah meskipun hanya menggunakan satu akun dan Wilayah. Menggunakan AWS CloudFormation StackSets membuatnya lebih mudah untuk memperluas ke akun dan Wilayah tambahan di masa depan.

Gunakan langkah-langkah berikut untuk menerapkan AWS CloudFormation template AWS-QuickSetup - SSMHostMgmt .yaml sebagai AWS CloudFormation tumpukan dalam satu akun dan Wilayah:

1. Unduh template dan periksa ke sistem kontrol versi pilihan Anda (misalnya, AWS CodeCommit).
2. Sesuaikan nilai AWS CloudFormation parameter default berdasarkan persyaratan organisasi Anda.
3. Sesuaikan jadwal asosiasi Manajer Negara.
4. Sesuaikan dokumen Systems Manager dengan ID `InstallAndManageCloudWatchDocument` logis. Konfirmasikan bahwa awalan bucket S3 sejajar dengan awalan untuk bucket S3 yang berisi konfigurasi Anda. CloudWatch
5. Ambil dan rekam Amazon Resource Name (ARN) untuk bucket S3 yang berisi konfigurasi Anda CloudWatch . Untuk informasi lebih lanjut tentang ini, lihat Mengelola CloudWatch konfigurasi bagian panduan ini. Tersedia contoh AWS CloudFormation template cloudwatch-config-s3-bucket.yaml yang menyertakan kebijakan bucket untuk menyediakan akses baca ke akun. AWS Organizations
6. Terapkan AWS CloudFormation template Pengaturan Cepat yang disesuaikan ke akun yang sama dengan bucket S3 Anda:

- Untuk `CloudWatchConfigBucketARN` parameternya, masukkan bucket ARN S3.
- Lakukan penyesuaian pada opsi parameter tergantung pada kemampuan yang ingin Anda aktifkan untuk Systems Manager.

7. Terapkan EC2 instance pengujian dengan dan tanpa IAM peran untuk mengonfirmasi bahwa EC2 instance berfungsi dengannya CloudWatch.

- Terapkan asosiasi Manajer `AttachIAMToInstance` Negara. Ini adalah runbook Systems Manager yang dikonfigurasi untuk berjalan sesuai jadwal. Asosiasi Manajer Negara yang menggunakan runbook tidak diterapkan secara otomatis ke EC2 instance baru dan dapat dikonfigurasi untuk dijalankan secara terjadwal. Untuk informasi selengkapnya, lihat Menjalankan otomatisasi dengan pemicu menggunakan State Manager di dokumentasi Systems Manager.
- Konfirmasikan bahwa EC2 instance memiliki IAM peran yang diperlukan terlampir.
- Konfirmasikan bahwa agen Systems Manager bekerja dengan benar dengan mengonfirmasi bahwa EC2 instance terlihat di Systems Manager.
- Konfirmasikan bahwa CloudWatch agen bekerja dengan benar dengan melihat CloudWatch log dan metrik berdasarkan CloudWatch konfigurasi dari bucket S3 Anda.

Pengaturan Cepat yang Disesuaikan di beberapa Wilayah dan beberapa akun dengan AWS CloudFormation StackSets

Jika Anda menggunakan beberapa akun dan Wilayah, maka Anda dapat menerapkan AWS CloudFormation template AWS- QuickSetup - SSMHostMgmt .yaml sebagai kumpulan tumpukan. Anda harus menyelesaikan AWS CloudFormation StackSetprasyarat sebelum menggunakan set tumpukan. Persyaratan bervariasi tergantung pada apakah Anda menerapkan set tumpukan dengan izin yang dikelola sendiri atau dikelolalayanan.

Kami menyarankan Anda menerapkan set tumpukan dengan izin yang dikelola layanan sehingga akun baru secara otomatis menerima Pengaturan Cepat yang disesuaikan. Anda harus menerapkan kumpulan tumpukan yang dikelola layanan dari akun AWS Organizations manajemen atau akun administrator yang didelegasikan. Anda harus menerapkan kumpulan tumpukan dari akun terpusat yang digunakan untuk otomatisasi yang telah mendelegasikan hak administrator, bukan akun manajemen. AWS Organizations Kami juga menyarankan Anda menguji penerapan set tumpukan Anda dengan menargetkan unit organisasi pengujian (OU) dengan satu atau sedikit akun dalam satu Wilayah.

1. Selesaikan langkah 1 hingga 5 dari Pengaturan Cepat yang Disesuaikan dalam satu akun dan Wilayah dengan AWS CloudFormation tumpukan bagian panduan ini.
2. Masuk ke AWS Management Console, buka AWS CloudFormation consoler dan pilih Buat: StackSet
   - Pilih Template siap dan Upload file template. Unggah AWS CloudFormation template yang Anda sesuaikan dengan kebutuhan Anda.
   - Tentukan detail set tumpukan:
     - Masukkan nama set tumpukan, misalnya,`StackSet-SSM-QuickSetup`.
     - Lakukan penyesuaian pada opsi parameter tergantung pada kemampuan yang ingin Anda aktifkan untuk Systems Manager.
     - Untuk `CloudWatchConfigBucketARN` parameternya, masukkan bucket S3 ARN untuk CloudWatch konfigurasi Anda.
     - Tentukan opsi kumpulan tumpukan, pilih apakah Anda akan menggunakan izin yang dikelola layanan dengan AWS Organizations atau izin yang dikelola sendiri.
       - Jika Anda memilih izin yang dikelola sendiri, masukkan detail AWSCloudFormationStackSetAdministrationRoledan AWSCloudFormationStackSetExecutionRoleIAMperan. Peran administrator harus ada di akun dan peran eksekusi harus ada di setiap akun target
     - Untuk izin yang dikelola layanan dengan AWS Organizations, sebaiknya Anda menerapkan terlebih dahulu ke OU pengujian, bukan seluruh organisasi.
       - Pilih apakah Anda ingin mengaktifkan penerapan otomatis. Kami menyarankan Anda memilih Diaktifkan. Untuk perilaku penghapusan akun, pengaturan yang disarankan adalah Hapus tumpukan.
     - Untuk izin yang dikelola sendiri, masukkan AWS akun IDs untuk akun yang ingin Anda atur. Anda harus mengulangi proses ini untuk setiap akun baru jika Anda menggunakan izin yang dikelola sendiri.
     - Masukkan Wilayah tempat Anda akan menggunakan CloudWatch dan Systems Manager.
     - Konfirmasikan bahwa penerapan berhasil dengan melihat status di tab Instans Operasi dan Tumpukan untuk kumpulan tumpukan.
     - Uji Systems Manager CloudWatch tersebut dan bekerja dengan benar di akun yang digunakan dengan mengikuti langkah 7 dari Pengaturan Cepat yang Disesuaikan dalam satu akun dan Wilayah dengan AWS CloudFormation tumpukan bagian panduan ini.

Pertimbangan untuk mengonfigurasi server lokal

CloudWatch Agen untuk server lokal dan VMs diinstal dan dikonfigurasi dengan menggunakan pendekatan serupa untuk EC2 instance. Namun, tabel berikut memberikan pertimbangan yang harus Anda evaluasi saat menginstal dan mengonfigurasi CloudWatch agen di server lokal dan. VMs

Arahkan CloudWatch agen ke kredenal sementara yang sama yang digunakan untuk Systems Manager.	Saat menyiapkan Systems Manager di lingkungan hibrid yang menyertakan server lokal, Anda dapat mengaktifkan Systems Manager dengan IAM peran. Anda harus menggunakan peran yang dibuat untuk EC2 instans Anda yang mencakup `AmazonSSM ManagedInstanceCore` kebijakan `CloudWatchAgentServerPolicy` dan kebijakan. Hal ini mengakibatkan agen Systems Manager mengambil dan menulis kredensil sementara ke file kredensial lokal. Anda dapat mengarahkan konfigurasi CloudWatch agen Anda ke file yang sama. Anda dapat menggunakan proses dari Konfigurasi server lokal yang menggunakan agen Systems Manager dan CloudWatch agen terpadu untuk hanya menggunakan kredensil sementara di Pusat Pengetahuan. AWS Anda juga dapat mengotomatiskan proses ini dengan mendefinisikan runbook Automation Systems Manager dan asosiasi State Manager terpisah, dan menargetkan instance lokal Anda dengan tag. Saat membuat aktivasi Systems Manager untuk instans lokal, Anda harus menyertakan tag yang mengidentifikasi instance sebagai instance lokal.

Pertimbangkan untuk menggunakan akun dan Wilayah yang memiliki VPN atau AWS Direct Connect mengakses dan AWS PrivateLink.	Anda dapat menggunakan AWS Direct Connect or AWS Virtual Private Network (AWS VPN) untuk membuat koneksi pribadi antara jaringan lokal dan virtual private cloud (VPC). AWS PrivateLinkmembuat koneksi pribadi ke CloudWatch Log dengan titik VPC akhir antarmuka. Pendekatan ini berguna jika Anda memiliki batasan yang mencegah data dikirim melalui internet publik ke titik akhir layanan publik.
Semua metrik harus disertakan dalam file CloudWatch konfigurasi.	Amazon EC2 menyertakan metrik standar (misalnya, CPU pemanfaatan) tetapi metrik ini harus ditentukan untuk instans lokal. Anda dapat menggunakan file konfigurasi platform terpisah untuk menentukan metrik ini untuk server lokal dan kemudian menambahkan konfigurasi ke konfigurasi CloudWatch metrik standar untuk platform.

Pertimbangan untuk contoh fana EC2

EC2instans bersifat sementara, atau sementara, jika disediakan oleh Amazon Auto EC2 Scaling, Amazon, Instans Spot EMR AmazonEC2, atau. AWS Batch EC2Instans fana dapat menyebabkan sejumlah besar CloudWatch aliran di bawah grup log umum tanpa informasi tambahan tentang asal runtime mereka.

Jika Anda menggunakan EC2 instance singkat, pertimbangkan untuk menambahkan informasi kontekstual dinamis tambahan di grup log dan nama aliran log. Misalnya, Anda dapat menyertakan ID permintaan Instans Spot, nama EMR klaster Amazon, atau nama grup Auto Scaling. Informasi ini dapat bervariasi untuk EC2 instance yang baru diluncurkan dan Anda mungkin harus mengambil dan mengonfigurasinya saat runtime. Anda dapat melakukan ini dengan menulis file konfigurasi CloudWatch agen saat boot dan memulai ulang agen untuk menyertakan file konfigurasi yang diperbarui. Hal ini memungkinkan pengiriman log dan metrik untuk CloudWatch menggunakan informasi runtime dinamis.

Anda juga harus memastikan bahwa metrik dan log Anda dikirim oleh CloudWatch agen sebelum EC2 instance fana Anda dihentikan. CloudWatch Agen menyertakan `flush_interval` parameter yang dapat dikonfigurasi untuk menentukan interval waktu pembilasan log dan buffer metrik. Anda dapat menurunkan nilai ini berdasarkan beban kerja Anda dan menghentikan CloudWatch agen dan memaksa buffer untuk flush sebelum EC2 instance dihentikan.

Menggunakan solusi otomatis untuk menyebarkan agen CloudWatch

Jika Anda menggunakan solusi otomatisasi (misalnya, Ansible atau Chef), Anda dapat memanfaatkannya untuk menginstal dan memperbarui CloudWatch agen secara otomatis. Jika Anda menggunakan pendekatan ini, Anda harus mengevaluasi pertimbangan berikut:

- Validasi bahwa otomatisasi mencakup OSs dan versi OS yang Anda dukung. Jika skrip otomatisasi tidak mendukung semua organisasi AndaOSs, Anda harus menentukan solusi alternatif untuk yang tidak didukungOSs.
- Validasi bahwa solusi otomatisasi secara teratur memeriksa pembaruan dan peningkatan CloudWatch agen. Solusi otomatisasi Anda harus secara teratur memeriksa pembaruan CloudWatch agen, atau secara teratur menghapus dan menginstal ulang agen. Anda dapat menggunakan fungsionalitas solusi penjadwal atau otomatisasi untuk memeriksa dan memperbarui agen secara teratur.
- Validasi bahwa Anda dapat mengonfirmasi pemasangan agen dan kepatuhan konfigurasi. Solusi otomatisasi Anda harus memungkinkan Anda untuk menentukan kapan suatu sistem tidak menginstal agen atau kapan agen tidak berfungsi. Anda dapat menerapkan pemberitahuan atau alarm ke dalam solusi otomatisasi Anda sehingga instalasi dan konfigurasi yang gagal dilacak.

Menyebarkan CloudWatch agen selama penyediaan instance dengan skrip data pengguna

Anda dapat menggunakan pendekatan ini jika Anda tidak berencana untuk menggunakan Systems Manager dan ingin menggunakannya secara selektif CloudWatch untuk EC2 instans Anda. Biasanya, pendekatan ini digunakan satu kali atau ketika konfigurasi khusus diperlukan. AWS menyediakan tautan langsung untuk CloudWatch agen yang dapat diunduh di skrip data awal atau pengguna Anda. Paket instalasi agen dapat dijalankan secara diam-diam tanpa interaksi pengguna, yang berarti Anda dapat menggunakannya dalam penerapan otomatis. Jika Anda menggunakan pendekatan ini, Anda harus mengevaluasi pertimbangan berikut:

- Peningkatan risiko bahwa pengguna tidak akan menginstal agen atau mengonfigurasi metrik standar. Pengguna dapat menyediakan instance tanpa menyertakan langkah-langkah yang diperlukan untuk menginstal CloudWatch agen. Mereka juga dapat salah mengkonfigurasi agen, yang dapat menyebabkan ketidakkonsistenan pencatatan dan pemantauan.
- Skrip instalasi harus spesifik OS dan cocok untuk versi OS yang berbeda. Anda memerlukan skrip terpisah jika Anda bermaksud menggunakan Windows dan Linux. Skrip Linux juga harus memiliki langkah-langkah instalasi yang berbeda berdasarkan distribusi.
- Anda harus memperbarui CloudWatch agen secara teratur dengan versi baru jika tersedia. Ini dapat diotomatisasi jika Anda menggunakan Systems Manager dengan State Manager, tetapi Anda juga dapat mengonfigurasi skrip data pengguna untuk dijalankan kembali saat startup instance. CloudWatch Agen kemudian diperbarui dan diinstal ulang pada setiap reboot.
- Anda harus mengotomatiskan pengambilan dan penerapan konfigurasi standar CloudWatch. Ini dapat diotomatisasi jika Anda menggunakan Systems Manager dengan State Manager, tetapi Anda juga dapat mengonfigurasi skrip data pengguna untuk mengambil file konfigurasi saat boot dan memulai ulang CloudWatch agen.

Termasuk CloudWatch agen di AMIs

Keuntungan menggunakan pendekatan ini adalah Anda tidak perlu menunggu CloudWatch agen diinstal dan dikonfigurasi, dan Anda dapat segera mulai masuk dan memantau. Ini membantu Anda memantau langkah penyediaan instans dan startup dengan lebih baik jika instance gagal dimulai. Pendekatan ini juga tepat jika Anda tidak berencana untuk menggunakan agen Systems Manager. Jika Anda menggunakan pendekatan ini, Anda harus mengevaluasi pertimbangan berikut:

- Proses pembaruan harus ada karena AMIs mungkin tidak menyertakan versi CloudWatch agen terbaru. CloudWatch Agen yang dipasang di an AMI hanya saat ini hingga terakhir kali AMI dibuat. Anda harus menyertakan metode tambahan untuk memperbarui agen secara teratur dan ketika EC2 instance disediakan. Jika Anda menggunakan Systems Manager, Anda dapat menggunakan Instalasi CloudWatch agen menggunakan Systems Manager Distributor dan State Manager solusi yang disediakan dalam panduan ini untuk ini. Jika Anda tidak menggunakan Systems Manager, Anda dapat menggunakan skrip data pengguna untuk memperbarui agen saat startup dan reboot instance.
- File konfigurasi CloudWatch agen Anda harus diambil pada saat startup instance. Jika Anda tidak menggunakan Systems Manager, Anda dapat mengonfigurasi skrip data pengguna untuk mengambil file konfigurasi saat boot dan kemudian memulai ulang CloudWatch agen.

- CloudWatch Agen harus dimulai ulang setelah CloudWatch konfigurasi Anda diperbarui.
- AWS kredensil tidak boleh disimpan di. AMI Pastikan tidak ada AWS kredensil lokal yang disimpan di file. AMI Jika Anda menggunakan AmazonEC2, Anda dapat menerapkan IAM peran yang diperlukan ke instans Anda dan menghindari kredensi lokal. Jika Anda menggunakan instance lokal, Anda harus mengotomatiskan atau memperbarui kredenal instans secara manual sebelum memulai agen. CloudWatch

Pencatatan dan pemantauan di Amazon ECS

Amazon Elastic Container Service (Amazon ECS) menyediakan dua tipe peluncuran untuk menjalankan kontainer dan yang menentukan jenis infrastruktur yang menampung tugas dan layanan; jenis peluncuran ini adalah dan AWS Fargate Amazon EC2. Kedua jenis peluncuran terintegrasi dengan CloudWatch tetapi konfigurasi dan dukungan bervariasi.

Bagian berikut membantu Anda memahami cara menggunakan CloudWatch untuk logging dan pemantauan di Amazon ECS.

Topik

Mengkonfigurasi CloudWatch dengan tipe peluncuran EC2

Dengan tipe peluncuran EC2, Anda menyediakan kluster Amazon ECS dari instans EC2 yang menggunakan CloudWatch agen untuk pencatatan dan pemantauan. AMI Amazon ECS yang dioptimalkan telah diinstal sebelumnya dengan agen kontainer Amazon ECS dan menyediakan CloudWatch metrik untuk cluster Amazon ECS.

Metrik default ini termasuk dalam biaya Amazon ECS, tetapi konfigurasi default untuk Amazon ECS tidak memantau file log atau metrik tambahan (misalnya, ruang disk kosong). Anda dapat menggunakan AWS Management Console untuk menyediakan kluster Amazon ECS dengan tipe peluncuran EC2, ini membuat AWS CloudFormation tumpukan yang menyebarkan Amazon EC2 Auto Scaling grup dengan konfigurasi peluncuran. Namun, pendekatan ini berarti Anda tidak dapat memilih AMI khusus atau menyesuaikan konfigurasi peluncuran dengan pengaturan yang berbeda atau skrip boot up tambahan.

Untuk memantau log dan metrik tambahan, Anda harus menginstal CloudWatch agen di instans penampung Amazon ECS Anda. Anda dapat menggunakan pendekatan instalasi untuk instans EC2 dari Instalasi CloudWatch agen menggunakan Systems Manager Distributor dan State Manager bagian panduan ini. Namun, Amazon ECS AMI tidak menyertakan agen Systems Manager yang

diperlukan. Anda harus menggunakan konfigurasi peluncuran kustom dengan skrip data pengguna yang menginstal agen Systems Manager saat membuat klaster Amazon ECS. Hal ini memungkinkan instance container Anda untuk mendaftar dengan Systems Manager dan menerapkan asosiasi State Manager untuk menginstal, mengonfigurasi, dan memperbarui CloudWatch agen. Saat State Manager menjalankan dan memperbarui konfigurasi CloudWatch agen Anda, itu juga menerapkan konfigurasi tingkat sistem standar Anda untuk CloudWatch Amazon EC2. Anda juga dapat menyimpan CloudWatch konfigurasi standar untuk Amazon ECS di bucket S3 untuk CloudWatch konfigurasi Anda dan menerapkannya secara otomatis dengan State Manager.

Anda harus memastikan bahwa peran IAM atau profil instans yang diterapkan ke instans penampung Amazon ECS Anda menyertakan persyaratan dan kebijakan. `CloudWatchAgentServerPolicy` `AmazonSSMManagedInstanceCore` Anda dapat menggunakan template ecs_cluster_with_cloudwatch_linux.yaml untuk menyediakan kluster Amazon ECS berbasis Linux AWS CloudFormation . Template ini membuat cluster Amazon ECS dengan konfigurasi peluncuran khusus yang menginstal Systems Manager dan menerapkan CloudWatch konfigurasi khusus untuk memantau file log khusus untuk Amazon ECS.

Anda harus menangkap log berikut untuk instans penampung Amazon ECS Anda, serta log instans EC2 standar Anda:

- Output startup agen Amazon ECS - `/var/log/ecs/ecs-init.log`
- Output agen Amazon ECS - `/var/log/ecs/ecs-agent.log`
- Penyedia kredensi IAM meminta log - `/var/log/ecs/audit.log`

Untuk informasi selengkapnya tentang tingkat keluaran, pemformatan, dan opsi konfigurasi tambahan, lihat lokasi file log Amazon ECS di dokumentasi Amazon ECS.

> **Important**
>
> Instalasi atau konfigurasi agen tidak diperlukan untuk jenis peluncuran Fargate karena Anda tidak menjalankan atau mengelola instans kontainer EC2.

Instans kontainer Amazon ECS harus menggunakan AMI dan agen kontainer Amazon ECS terbaru yang dioptimalkan. AWS menyimpan parameter Penyimpanan Parameter Systems Manager publik dengan informasi AMI Amazon ECS yang dioptimalkan, termasuk ID AMI. Anda dapat mengambil AMI terbaru yang dioptimalkan dari Parameter Store dengan menggunakan format

parameter Parameter Store untuk AMI yang dioptimalkan Amazon ECS. Anda dapat merujuk ke parameter Parameter Store publik yang mereferensikan AMI terbaru atau rilis AMI tertentu di AWS CloudFormation template Anda.

AWS menyediakan parameter Parameter Store yang sama di setiap Wilayah yang didukung. Ini berarti bahwa AWS CloudFormation template yang mereferensikan parameter ini dapat digunakan kembali di seluruh Wilayah dan akun tanpa AMI diperbarui. Anda dapat mengontrol penyebaran AMI Amazon ECS yang lebih baru ke organisasi Anda dengan merujuk ke rilis tertentu, yang membantu Anda mencegah penggunaan AMI Amazon ECS baru yang dioptimalkan hingga Anda mengujinya.

Log kontainer Amazon ECS untuk jenis peluncuran EC2 dan Fargate

Amazon ECS menggunakan definisi tugas untuk menyebarkan dan mengelola kontainer sebagai tugas dan layanan. Anda mengonfigurasi kontainer yang ingin Anda luncurkan ke cluster Amazon ECS Anda dalam definisi tugas. Logging dikonfigurasi dengan driver log di tingkat kontainer. Beberapa opsi driver log menyediakan kontainer Anda dengan sistem logging yang berbeda (misalnya`awslogs`,`fluentd`,`gelf`,`json-file`,`journald`,`logentries`,`splunk`,`syslog`, atau`awsfirelens`) tergantung pada apakah Anda menggunakan jenis peluncuran EC2 atau Fargate. Jenis peluncuran Fargate menyediakan subset dari opsi driver log berikut:`awslogs`,, `splunk` dan. `awsfirelens` AWS menyediakan driver `awslogs` log untuk menangkap dan mengirimkan output kontainer ke CloudWatch Log. Pengaturan driver log memungkinkan Anda untuk menyesuaikan grup log, Wilayah, dan awalan aliran log bersama dengan banyak opsi lainnya.

Penamaan default untuk grup log dan opsi yang digunakan oleh opsi Konfigurasi Otomatis CloudWatch Log AWS Management Console adalah`/ecs/<task_name>`. Nama log stream yang digunakan oleh Amazon ECS memiliki `<awslogs-stream-prefix>/<container_name>/<task_id>` format. Kami menyarankan Anda menggunakan nama grup yang mengelompokkan log Anda berdasarkan persyaratan organisasi Anda. Dalam tabel berikut, `image_name` dan `image_tag` disertakan dalam nama log stream.

Nama grup log	`/<Business unit>/<Project or application name>/<Environment>/<Cluster name>/<Task name>`
Awalan nama aliran log	`/<image_name>/<image_tag>`

Informasi ini juga tersedia dalam definisi tugas. Namun, tugas diperbarui secara berkala dengan revisi baru, yang berarti bahwa definisi tugas mungkin menggunakan yang berbeda `image_name` dan `image_tag` dari yang digunakan definisi tugas saat ini. Untuk informasi selengkapnya dan saran penamaan, lihat Merencanakan CloudWatch penyebaran Anda bagian panduan ini.

Jika Anda menggunakan pipeline continuous integration dan continuous delivery (CI/CD) atau proses otomatis, Anda dapat membuat revisi definisi tugas baru untuk aplikasi Anda dengan setiap build image Docker yang baru. Misalnya, Anda dapat menyertakan nama gambar Docker, tag gambar, GitHub revisi, atau informasi penting lainnya dalam revisi definisi tugas dan konfigurasi logging Anda sebagai bagian dari proses CI/CD Anda.

Menggunakan perutean log khusus FireLens untuk Amazon ECS

FireLens untuk Amazon ECS membantu Anda merutekan log ke Fluentd atau Fluent Bit sehingga Anda dapat langsung mengirim log kontainer ke AWS layanan dan tujuan Jaringan AWS Mitra (APN) serta mendukung pengiriman log ke Log. CloudWatch

AWS menyediakan image Docker untuk Fluent Bit dengan plugin pra-instal untuk Amazon Kinesis Data Streams, Amazon Data Firehose, dan Log. CloudWatch Anda dapat menggunakan driver FireLens log alih-alih driver `awslogs` log untuk penyesuaian dan kontrol lebih lanjut atas log yang dikirim ke CloudWatch Log.

Misalnya, Anda dapat menggunakan driver FireLens log untuk mengontrol output format log. Ini berarti bahwa CloudWatch log penampung Amazon ECS secara otomatis diformat sebagai objek JSON dan menyertakan properti berformat JSON untuk`ecs_cluster`,,,,, dan. `ecs_task_arn` `ecs_task_definition` `container_id` `container_name` `ec2_instance_id` Host fasih diekspos ke container Anda melalui variabel `FLUENT_HOST` and `FLUENT_PORT` environment saat Anda menentukan `awsfirelens` driver. Ini berarti Anda dapat langsung masuk ke router log dari kode Anda dengan menggunakan pustaka logger yang lancar. Misalnya, aplikasi Anda mungkin menyertakan `fluent-logger-python` library untuk log ke Fluent Bit dengan menggunakan nilai yang tersedia dari variabel lingkungan.

Jika Anda memilih FireLens untuk menggunakan Amazon ECS, Anda dapat mengonfigurasi pengaturan yang sama dengan driver `awslogs` log dan menggunakan pengaturan lain juga. Misalnya, Anda dapat menggunakan definisi ecs-task-nginx-firelensetugas.json Amazon ECS yang meluncurkan server NGINX yang dikonfigurasi untuk digunakan untuk masuk. FireLens CloudWatch Ini juga meluncurkan wadah FireLens Fluent Bit sebagai sespan untuk logging.

Metrik untuk Amazon ECS

Amazon ECS menyediakan CloudWatch metrik standar (misalnya, pemanfaatan CPU dan memori) untuk jenis peluncuran EC2 dan Fargate di tingkat cluster dan layanan dengan agen kontainer Amazon ECS. Anda juga dapat menangkap metrik untuk layanan, tugas, dan kontainer menggunakan Wawasan CloudWatch Kontainer, atau menangkap metrik penampung kustom Anda sendiri dengan menggunakan format metrik yang disematkan.

Container Insights adalah CloudWatch fitur yang menyediakan metrik seperti pemanfaatan CPU, pemanfaatan memori, lalu lintas jaringan, dan penyimpanan di cluster, instance container, layanan, dan tingkat tugas. Container Insights juga membuat dasbor otomatis yang membantu Anda menganalisis layanan dan tugas, dan melihat rata-rata memori atau pemanfaatan CPU di tingkat kontainer. Container Insights menerbitkan metrik kustom ke namespace `ECS/ContainerInsights` kustom yang dapat Anda gunakan untuk membuat grafik, mengkhawatirkan, dan dasbor.

Anda dapat mengaktifkan metrik Container Insight dengan mengaktifkan Container Insights untuk setiap kluster Amazon ECS individual. Jika Anda juga ingin melihat metrik di tingkat instans penampung, Anda dapat meluncurkan CloudWatch agen sebagai wadah daemon di cluster Amazon ECS Anda. Anda dapat menggunakan AWS CloudFormation template cwagent-ecs-instance-metric-cfn.yaml untuk menyebarkan agen CloudWatch sebagai layanan Amazon ECS. Yang penting, contoh ini mengasumsikan bahwa Anda membuat konfigurasi CloudWatch agen kustom yang sesuai dan menyimpannya di Parameter Store dengan kunci`ecs-cwagent-daemon-service`.

CloudWatchAgen yang digunakan sebagai wadah daemon untuk CloudWatch Container Insights mencakup disk tambahan, memori, dan metrik CPU seperti `instance_cpu_reserved_capacity` dan `instance_memory_reserved_capacity` dengan, dimensi. `ClusterName` `ContainerInstanceId` `InstanceId` Metrik pada tingkat instance container diimplementasikan oleh Container Insights dengan menggunakan format metrik yang CloudWatch disematkan. Anda dapat mengonfigurasi metrik tingkat sistem tambahan untuk instans penampung Amazon ECS Anda dengan menggunakan pendekatan dari bagian panduan iniMenyiapkan State Manager dan Distributor untuk penyebaran dan konfigurasi CloudWatch agen.

Membuat metrik aplikasi khusus di Amazon ECS

Anda dapat membuat metrik khusus untuk aplikasi Anda dengan menggunakan format metrik yang CloudWatch disematkan. Driver `awslogs` log dapat menafsirkan pernyataan format metrik yang CloudWatch disematkan.

Variabel `CW_CONFIG_CONTENT` lingkungan dalam contoh berikut diatur ke isi parameter `cwagentconfig` Systems Manager Parameter Store. Anda dapat menjalankan agen dengan konfigurasi dasar ini untuk mengonfigurasinya sebagai titik akhir format metrik tertanam. Namun, itu tidak lagi diperlukan.

```
  {
  "logs": {
    "metrics_collected": {
      "emf": { }
    }
  }
}
```

Jika Anda memiliki penerapan Amazon ECS di beberapa akun dan Wilayah, Anda dapat menggunakan AWS Secrets Manager rahasia untuk menyimpan CloudWatch konfigurasi dan mengonfigurasi kebijakan rahasia untuk membagikannya dengan organisasi Anda. Anda dapat menggunakan opsi rahasia dalam definisi tugas Anda untuk mengatur `CW_CONFIG_CONTENT` variabel.

Anda dapat menggunakan pustaka format metrik tertanam sumber terbuka yang AWS disediakan di aplikasi Anda dan menentukan variabel `AWS_EMF_AGENT_ENDPOINT` lingkungan untuk terhubung ke wadah sespan CloudWatch agen Anda yang bertindak sebagai titik akhir format metrik tertanam. Misalnya, Anda dapat menggunakan contoh aplikasi Python ecs_cw_emf_example untuk mengirim metrik dalam format metrik tertanam ke wadah sespan agen yang dikonfigurasi sebagai titik akhir format metrik tertanam. CloudWatch

Plugin Fluent Bit untuk juga CloudWatch dapat digunakan untuk mengirim pesan format metrik yang disematkan. Anda juga dapat menggunakan contoh aplikasi Python ecs_firelense_emf_example untuk mengirim metrik dalam format metrik tertanam ke wadah sidecar Firelens untuk Amazon ECS.

Jika Anda tidak ingin menggunakan format metrik tertanam, Anda dapat membuat dan memperbarui CloudWatch metrik melalui AWS API atau AWS SDK. Kami tidak merekomendasikan pendekatan ini kecuali Anda memiliki kasus penggunaan tertentu, karena ini menambahkan overhead pemeliharaan dan manajemen ke kode Anda.

Pencatatan dan pemantauan di Amazon EKS

Amazon Elastic Kubernetes Service (Amazon EKS) terintegrasi dengan CloudWatch Log untuk bidang kontrol Kubernetes. Pesawat kontrol disediakan sebagai layanan terkelola oleh Amazon EKS dan Anda bisamengaktifkan logging tanpa menginstal agen CloudWatch. Parameter CloudWatch agen juga dapat digunakan untuk menangkap node Amazon EKS dan log kontainer. Fluent Bit dan Fluentdjuga didukung untuk mengirim log kontainer Anda ke CloudWatch Log.

CloudWatch Container Insights menyediakan solusi pemantauan metrik yang komprehensif untuk Amazon EKS di tingkat klaster, simpul, pod, tugas, dan layanan. Amazon EKS juga mendukung beberapa opsi untuk pengambilan metrik danganPrometheus. Bidang pengendali Amazon EKSmenyediakan endpoint metrikyang mengekspos metrik dalam format Prometheus. Anda dapat menerapkan Prometheus ke dalam klaster Amazon EKS Anda untuk menggunakan metrik ini.

Anda juga dapatmengatur CloudWatch agen untuk mengeruk metrik Prometheusdan menciptakan CloudWatch metrik, selain mengkonsumsi titik akhir Prometheus lainnya. Pemantauan Wawasan Kontainer untuk Prometheusjuga dapat secara otomatis menemukan dan menangkap metrik Prometheus dari beban kerja dan sistem yang didukung dan terisi.

Anda dapat menginstal dan mengonfigurasi CloudWatch agen pada node Amazon EKS Anda, dengan cara yang sama dengan pendekatan yang digunakan untuk Amazon EC2 dengan Distributor dan State Manager, untuk menyelaraskan node Amazon EKS Anda dengan konfigurasi logging dan pemantauan sistem standar Anda.

Pencatatan untuk Amazon EKS

Kubernetes logging dapat dibagi menjadi control plane logging, node logging, dan application logging. ParameterBidang kendali Kubernetesadalah seperangkat komponen yang mengelola klaster Kubernetes dan menghasilkan log yang digunakan untuk tujuan audit dan diagnostik. Dengan Amazon EKS, Anda bisamenyalakan log untuk komponen pesawat kontrol yang berbedadan mengirim mereka ke CloudWatch.

Kubernetes juga menjalankan komponen sistem sepertikubeletdankube-proxypada setiap node Kubernetes yang menjalankan Pod Anda. Komponen-komponen ini menulis log dalam setiap node dan Anda dapat mengkonfigurasi CloudWatch dan Wawasan Kontainer untuk menangkap log ini untuk setiap node Amazon EKS.

Kontainer dikelompokkan sebagaipolongdalam klaster Kubernetes dan dijadwalkan berjalan pada node Kubernetes Anda. Sebagian besar aplikasi kontainer menulis ke output standar dan kesalahan standar, dan mesin kontainer mengalihkan output ke driver logging. Di Kubernetes, log kontainer ditemukan di`/var/log/pods`direktori pada node. Anda dapat mengonfigurasi CloudWatch dan Wawasan Kontainer untuk menangkap log ini untuk setiap pod Amazon EKS Anda.

Pencatatan bidang kendali Amazon EKS

Kluster Amazon EKS terdiri dari pesawat kontrol penyewa tunggal dengan ketersediaan tinggi untuk klaster Kubernetes Anda dan node Amazon EKS yang menjalankan kontainer Anda. Node pesawat kontrol berjalan di akun yang dikelola olehAWS. Node pesawat kontrol klaster Amazon EKS terintegrasi dengan CloudWatch dan Anda dapat mengaktifkan penebangan untuk komponen pesawat kontrol tertentu.

Log disediakan untuk setiap instance komponen pesawat kontrol Kubernetes.AWSmengelola kesehatan node pesawat kontrol Anda dan menyediakanservice level agreement (SLA) untuk endpoint Kubernetes.

Pencatatan simpul Amazon EKS

Sebaiknya Anda menggunakanWawasan Kontainer CloudWatchuntuk menangkap log dan metrik untuk Amazon EKS. Wawasan Kontainer mengimplementasikan metrik klaster, node, dan pod-level dengan CloudWatch agen, dan Fluent Bit atau Fluentd untuk menangkap log ke CloudWatch. Wawasan Kontainer juga menyediakan dasbor otomatis dengan tampilan berlapis dari yang Anda tangkap CloudWatch metrik. Wawasan Kontainer digunakan sebagai CloudWatch DaemonSet dan Fluent Bit DaemonSet yang berjalan pada setiap node Amazon EKS. Node Fargate tidak didukung oleh Container Insights karena node dikelola olehAWSdan tidak mendukung DaemonSets. Penebangan Fargate untuk Amazon EKS dicakup secara terpisah dalam panduan ini.

Tabel berikut menunjukkan CloudWatch log kelompok dan log ditangkap olehKonfigurasi penangkapan log Fluentd atau Fluent Bituntuk Amazon EKS.

`/aws/containerinsights/Cluster_Name/application`	Semua file log`/var/log/containers`. Direktori ini menyediakan tautan simbolik ke semua log kontainer Kubernetes di`/var/log/pods` struktur direktori. Ini menangkap log kontainer aplikasi Anda menulis

	kestdoutataustderr. Ini juga mencakup log untuk kontainer sistem Kubernetes sepertiaws-vpc-cni-init,kube-proxy , dancoreDNS.
/aws/containerinsights/Cluster_Name/host	Log dari/var/log/dmesg ,/var/log/secure , dan/var/log/messages .
/aws/containerinsights/Cluster_Name/dataplane	Login /var/log/journal untuk kubelet.service , kubeproxy .service , dan docker.service .

Jika Anda tidak ingin menggunakan Wawasan Kontainer dengan Fluent Bit atau Fluentd untuk logging, Anda dapat menangkap log node dan kontainer dengan CloudWatch agen diinstal pada simpul Amazon EKS. Node Amazon EKS adalah instans EC2, yang berarti Anda harus memasukkannya ke dalam pendekatan logging tingkat sistem standar untuk Amazon EC2. Jika Anda menginstal CloudWatch agen menggunakan Distributor dan State Manager, maka node Amazon EKS juga disertakan dalam CloudWatch instalasi agen, konfigurasi, dan update.

Tabel berikut menunjukkan log yang spesifik untuk Kubernetes dan Anda harus menangkap jika Anda tidak menggunakan Container Insights dengan Fluent Bit atau Fluentd untuk logging.

/var/log/containers	Direktori ini menyediakan tautan simbolik ke semua log kontainer Kubernetes di bawah/var/log/pods struktur direktori. Ini secara efektif menangkap log kontainer aplikasi Anda menulis kestdoutataustderr. Ini termasuk log untuk kontainer sistem Kubernete s sepertiaws-vpc-cni-init ,kube-proxy , dancoreDNS. Penting: Ini tidak diperlukan jika Anda menggunakan Wawasan Kontainer.
var/log/aws-routed-eni/ipamd.log /var/log/aws-routed-eni/plugin.log	Log untuk daemon L-IPAM dapat ditemukan di sini

Anda harus memastikan bahwa node Amazon EKS menginstal dan mengonfigurasi CloudWatch agen untuk mengirim log tingkat sistem yang sesuai dan metrik. Namun, AMI yang dioptimalkan Amazon EKS tidak termasuk agen Systems Manager. Dengan menggunakantemplat peluncuran, Anda dapat mengotomatisasi instalasi agen Systems Manager dan default CloudWatch konfigurasi yang menangkap log spesifik Amazon EKS penting dengan skrip startup yang diimplementasikan melalui bagian data pengguna. Node Amazon EKS digunakan menggunakan grup Auto Scaling sebagaigrup simpul terkelolaatau sebagaiSimpul yang dikelola sendiri.

Dengan kelompok-kelompok node terkelola, Anda menyediakanTemplat peluncuranyang mencakup bagian data pengguna untuk mengotomatisasi instalasi agen Systems Manager dan CloudWatch konfigurasi. Anda dapat menyesuaikan dan menggunakanamazon_eks_managed_node_group_launch_config.yaml AWS CloudFormationtemplate untuk membuat template peluncuran yang menginstal agen Systems Manager, CloudWatch agen, dan juga menambahkan konfigurasi logging spesifik Amazon EKS ke CloudWatch Direktori konfigurasi. Template ini dapat digunakan untuk memperbarui templat peluncuran grup node terkelola Amazon EKS Anda dengan infrastructure-as-code Pendekatan (IAC). Setiap pembaruan keAWS CloudFormationKetentuan template versi baru dari templat peluncuran. Anda kemudian dapat memperbarui grup node untuk menggunakan versi template baru dan memilikiproses siklus aktif terkelolamemperbarui node Anda tanpa downtime. Pastikan bahwa profil peran dan instans IAM yang diterapkan pada grup node terkelola Anda mencakup`CloudWatchAgentServerPolicy`dan`AmazonSSMManagedInstanceCore` AWSkebijakan terkelola.

Dengan node yang dikelola sendiri, Anda secara langsung menyediakan dan mengelola strategi siklus hidup dan pembaruan untuk node Amazon EKS Anda. Node yang dikelola sendiri memungkinkan Anda menjalankan node Windows di klaster Amazon EKS danBottlerocket, bersama denganopsi lainnya. Anda dapat menggunakanAWS CloudFormationuntuk menerapkan node yang dikelola sendiri ke dalam klaster Amazon EKS Anda, yang berarti Anda dapat menggunakan IAC dan pendekatan perubahan terkelola untuk klaster Amazon EKS Anda.AWSmenyediakanamazon-eks-nodegroup.yaml AWS CloudFormationtemplate yang dapat Anda gunakan apa adanya atau menyesuaikan. Template menyediakan semua sumber daya yang diperlukan untuk node Amazon EKS dalam klaster (misalnya, peran IAM terpisah, grup keamanan, grup Auto Scaling Amazon EC2, dan templat peluncuran). Parameteramazon-eks-nodegroup.yaml AWS CloudFormationtemplate adalah versi terbaru yang menginstal agen Systems Manager yang diperlukan, CloudWatch agen, dan juga menambahkan konfigurasi logging spesifik Amazon EKS ke CloudWatch Direktori konfigurasi.

Logging untuk Amazon EKS di Fargate

Dengan Amazon EKS di Fargate, Anda dapat menerapkan Pod tanpa mengalokasikan atau mengelola node Kubernetes Anda. Ini menghilangkan kebutuhan untuk menangkap log tingkat sistem untuk node Kubernetes Anda. Untuk menangkap log dari Pod Fargate Anda, Anda dapat menggunakan Fluent Bit untuk meneruskan log langsung ke CloudWatch. Hal ini memungkinkan Anda untuk secara otomatis merutekan log CloudWatch tanpa konfigurasi lebih lanjut atau kontainer sidecar untuk pod Amazon EKS Anda di Fargate. Untuk informasi selengkapnya tentang hal ini, lihatPencatatan log Fargatedalam dokumentasi Amazon EKS danBit Fasih untuk Amazon EKSpadaAWSBlog. Solusi ini menangkap`STDOUT`dan`STDERR`input/output (I/O) mengalir dari wadah Anda dan mengirimkannya ke CloudWatch melalui Fluent Bit, berdasarkan konfigurasi Fluent Bit yang ditetapkan untuk klaster Amazon EKS di Fargate.

Metrik untuk Amazon EKS dan Kubernetes

Kubernetes menyediakan API metrik yang memungkinkan Anda mengakses metrik penggunaan sumber daya (misalnya, penggunaan CPU dan memori untuk node dan Pod), tetapi API hanya menyediakan informasi point-in-time dan bukan metrik historis. ParameterServer metrik Kubernetesbiasanya digunakan untuk penerapan Amazon EKS dan Kubernetes untuk menggabungkan metrik, memberikan informasi historis jangka pendek tentang metrik, dan fitur dukungan sepertiPenskala Otomatis Pod Horizontal.

Amazon EKS mengekspos metrik pesawat kontrol melalui server API Kubernetesdalam format Prometheusdan CloudWatch dapat menangkap dan menelan metrik ini. CloudWatch dan Wawasan Kontainer juga dapat dikonfigurasi untuk menyediakan penangkapan, analisis, dan pengkhawatirannya metrik komprehensif untuk node dan Pod Amazon EKS Anda.

Metrik bidang kendali Kubernetes

Kubernetes mengekspos metrik control plane dalam format Prometheus dengan menggunakan`/metrics`Titik akhir HTTP API. Anda harus menginstalPrometheusdi klaster Kubernetes Anda untuk membuat grafik dan melihat metrik ini dengan browser web. Anda juga dapatmenelan metrik yang terpaparoleh server API Kubernetes ke CloudWatch.

Node dan metrik sistem untuk Kubernetes

Kubernetes menyediakan Prometheusserver metrikpod yang Anda bisamenyebarkan dan menjalankanpada klaster Kubernetes Anda untuk klaster, node, dan pod-level CPU dan statistik

memori. Metrik ini digunakan dengan Penskala Otomatis Pod Horizontal dan Vertical Pod Autoscaler. CloudWatch juga dapat memberikan metrik ini.

Anda harus menginstal Kubernetes Metrics Server jika menggunakan Dasbor Kubernetes atau autoscalers pod horizontal dan vertikal. Dasbor Kubernetes membantu Anda menelusuri dan mengonfigurasi klaster, node, pod, dan konfigurasi terkait Kubernetes, serta melihat metrik CPU dan memori dari Kubernetes Metrics Server. Anda dapat menerapkan solusi ini untuk setiap cluster dengan mengikuti langkah-langkah dari Menerapkan Dasbor Kubernetes dalam dokumentasi Amazon EKS.

Metrik yang disediakan oleh Kubernetes Metrics Server tidak dapat digunakan untuk tujuan penskalaan non-otomatis (misalnya pemantauan). Metrik dimaksudkan untuk point-in-time analisis dan bukan analisis historis. Dasbor Kubernetes menyebarkan `dashboard-metrics-scraper` untuk menyimpan metrik dari Kubernetes Metrics Server dalam waktu singkat.

Wawasan Kontainer menggunakan versi kontainer CloudWatch agen yang berjalan di Kubernetes DaemonSet untuk menemukan semua kontainer yang berjalan dalam kluster dan memberikan metrik tingkat noda. Mengumpulkan data kinerja di setiap lapisan tumpukan kinerja. Anda dapat menggunakan Quick Start dari AWS Mulai Cepat atau konfigurasikan Wawasan Kontainer secara terpisah. Quick Start mengatur pemantauan metrik dengan CloudWatch agen dan penebangan dengan Fluent Bit sehingga Anda hanya perlu menyebarkan sekali untuk logging dan monitoring.

Karena node Amazon EKS adalah instans EC2, Anda harus menangkap metrik tingkat sistem, selain metrik yang ditangkap oleh Container Insights, dengan menggunakan standar yang Anda tetapkan untuk Amazon EC2. Anda dapat menggunakan pendekatan yang sama dari Menyiapkan State Manager dan Distributor untuk penyebaran dan konfigurasi CloudWatch agen bagian panduan ini untuk menginstal dan mengonfigurasi CloudWatch agen untuk klaster Amazon EKS Anda. Anda dapat memperbarui file konfigurasi CloudWatch khusus Amazon EKS untuk menyertakan metrik serta konfigurasi log spesifik Amazon EKS Anda.

Parameter CloudWatch agen dengan dukungan Prometheus dapat secara otomatis menemukan dan mengikis metrik Prometheus dari beban kerja dan sistem yang didukung dan terisi. Ini menelan mereka sebagai CloudWatch log dalam format metrik tertanam untuk analisis dengan CloudWatch Log Wawasan dan secara otomatis membuat metrik CloudWatch.

> **Important**
>
> Anda harus menyebarkan versi khusus dari CloudWatch agen untuk mengumpulkan metrik Prometheus. Ini adalah agen terpisah dari CloudWatch agen dikerahkan untuk Wawasan

Wadah. Anda dapat menggunakanprometheus_jmxcontoh aplikasi Java, yang mencakup penyebaran dan konfigurasi file untuk CloudWatch penyebaran pod agen dan Amazon EKS untuk mendemonstrasikan penemuan metrik Prometheus. Untuk informasi selengkapnya, lihatSiapkan contoh beban kerja Java/JMX di Amazon EKS dan Kubernetesdalam dokumentasi CloudWatch. Anda juga dapat mengonfigurasi CloudWatch agen untuk menangkap metrik dari target Prometheus lain yang berjalan di klaster Amazon EKS Anda.

Metrik aplikasi

Anda dapat membuat metrik khusus Anda sendiri danganFormat metrik tertanam CloudWatch. Untuk menelan pernyataan format metrik tertanam, Anda perlu mengirim entri format metrik tertanam ke titik akhir format metrik tertanam. Parameter CloudWatch agen dapat dikonfigurasi sebagaikontainer sidecar di pod Amazon EKS Anda. Parameter CloudWatch konfigurasi agen disimpan sebagai Kubernetes ConfigMap dan membaca oleh Anda CloudWatch agen sidecar kontainer untuk memulai metrik format endpoint tertanam.

Anda juga dapat mengatur aplikasi sebagai target Prometheus dan mengonfigurasi agen CloudWatch, dengan dukungan Prometheus, untuk menemukan, mengikis, dan menelan metrik Anda ke CloudWatch. Misalnya, Anda dapat menggunakaneksportir JMX open-sourcedengan aplikasi Java Anda untuk mengekspos JMX Beans untuk konsumsi Prometheus oleh CloudWatch agen.

Jika Anda tidak ingin menggunakan format metrik tertanam, Anda juga dapat membuat dan memperbarui metrik CloudWatch menggunakanAWSAPIatauAWS SDK. Namun, kami tidak merekomendasikan pendekatan ini karena mencampur pemantauan dan logika aplikasi.

Metrik untuk Amazon EKS di Fargate

Fargate secara otomatis menyediakan node Amazon EKS untuk menjalankan Pod Kubernetes sehingga Anda tidak perlu memantau dan mengumpulkan metrik level node-level. Namun, Anda harus memantau metrik untuk Pod yang berjalan pada node Amazon EKS Anda di Fargate. Wawasan Kontainer saat ini tidak tersedia untuk Amazon EKS di Fargate karena memerlukan kemampuan berikut yang saat ini tidak didukung:

- DaemonSets saat ini tidak didukung. Wawasan Kontainer dikerahkan dengan menjalankan CloudWatch agen sebagai DaemonSet pada setiap node cluster.
- Volume persisten HostPath tidak didukung. Parameter CloudWatch wadah agen menggunakan volume persisten HostPath sebagai prasyarat untuk mengumpulkan data metrik kontainer.

- Fargate mencegah kontainer istimewa dan akses ke host informasi.

Anda dapat menggunakanbuilt-in log router untuk Fargateuntuk mengirim pernyataan format metrik tertanam ke CloudWatch. Router log menggunakan Fluent Bit, yang memiliki CloudWatch plugin yang dapat dikonfigurasi untuk mendukung pernyataan format metrik tertanam.

Anda dapat mengambil dan menangkap metrik tingkat pod untuk node Fargate Anda dengan menerapkan server Prometheus di klaster Amazon EKS Anda untuk mengumpulkan metrik dari node Fargate Anda. Karena Prometheus memerlukan penyimpanan persisten, Anda dapat menggunakan Prometheus di Fargate jika menggunakan Amazon Elastic File System (Amazon EFS) untuk penyimpanan persisten. Anda juga dapat menerapkan Prometheus pada node yang didukung Amazon EC2. Untuk informasi selengkapnya, lihatMemantau Amazon EKSAWS Fargatemenggunakan Prometheus dan GrafanapadaAWSBlog.

Pemantauan Prometheus di Amazon EKS

Layanan Terkelola Amazon untuk Prometheusmenyediakan scalable, aman,AWSlayanan terkelola untuk Prometheus open-source. Anda dapat menggunakan bahasa kueri Prometheus (ProMQL) untuk memantau kinerja beban kerja kontainer tanpa mengelola infrastruktur dasar untuk menelan, menyimpan, dan melakukan kueri metrik operasional. Anda dapat mengumpulkan metrik Prometheus dari Amazon EKS dan Amazon ECS dengan menggunakanAWSDistro untuk OpenTelemetry (ADOT)atau Prometheus server sebagai agen koleksi.

Pemantauan Wawasan Kontainer CloudWatch untuk Prometheusmemungkinkan Anda untuk mengkonfigurasi dan menggunakan CloudWatch agen untuk menemukan metrik Prometheus dari beban kerja Amazon ECS, Amazon EKS, dan Kubernetes, dan menelannya sebagai metrik CloudWatch. Solusi ini sesuai jika CloudWatch adalah solusi pengamatan dan pemantauan utama Anda. Namun, daftar berikut menguraikan kasus penggunaan di mana Amazon Managed Service for Prometheus memberikan lebih banyak fleksibilitas untuk menelan, menyimpan, dan kueri metrik Prometheus:

- Amazon Managed Service for Prometheus memungkinkan Anda untuk menggunakan server Prometheus yang ada yang digunakan di Amazon EKS atau Kubernetes yang dikelola sendiri dan mengonfigurasinya untuk menulis ke Amazon Managed Service for Prometheus alih-alih menyimpan data yang dikonfigurasi secara lokal. Ini menghilangkan pengangkatan berat yang tidak berdiferensiasi dalam mengelola penyimpanan data yang sangat tersedia untuk server Prometheus Anda dan infrastrukturnya. Amazon Managed Service for Prometheus adalah pilihan yang tepat ketika Anda memiliki penyebaran Prometheus dewasa yang ingin Anda manfaatkan diAWSCloud.
- Grafana secara langsung mendukung Prometheus sebagai sumber data untuk visualisasi. Jika Anda ingin menggunakan Grafana dengan Prometheus bukan CloudWatch Dasbor untuk pemantauan kontainer Anda, maka Amazon Managed Service for Prometheus dapat memenuhi kebutuhan Anda. Amazon Managed Service for Prometheus terintegrasi dengan Amazon Managed Grafana untuk menyediakan solusi pemantauan dan visualisasi sumber terbuka yang dikelola.
- Prometheus memungkinkan Anda untuk melakukan analisis pada metrik operasional Anda dengan menggunakan kueri ProMQL. Sebaliknya,sang CloudWatch agen menelan metrik Prometheus dalam format metrik tersematke CloudWatch Log yang menghasilkan CloudWatch metrik. Anda dapat query log format metrik tersemat menggunakan CloudWatch Logs Insights.
- Jika Anda tidak berencana untuk menggunakan CloudWatch untuk pemantauan dan pengambilan metrik, maka Anda harus menggunakan Amazon Managed Service untuk Prometheus dengan

server Prometheus dan solusi visualisasi seperti Grafana. Anda perlu mengkonfigurasi server Prometheus Anda untuk mengikis metrik dari target Prometheus Anda dan mengkonfigurasi servermenulis jarak jauh ke Amazon Managed Service untuk ruang kerja Prometheus. Jika Anda menggunakan Amazon Managed Grafana, maka Anda dapatlangsung mengintegrasikan Amazon Managed Grafana dengan Amazon Managed Service untuk sumber data Prometheus Anda dengan menggunakan plugin yang disertakan. Karena data metrik disimpan di Amazon Managed Service untuk Prometheus, tidak ada dependensi untuk menyebarkan CloudWatch agen atau persyaratan untuk menelan data ke CloudWatch. Parameter CloudWatch agen diperlukan untuk pemantauan Wawasan Wawasan untuk Prometheus.

Anda juga dapat menggunakan Kolektor ADOT untuk mengikis dari aplikasi yang diinstrumentasi Prometheus dan mengirim metrik ke Amazon Managed Service untuk Prometheus. Untuk informasi selengkapnya tentang Kolektor ADOT, lihatAWSDistro untuk OpenTelemetrydokumentasi.

Pencatatan dan metrik untukAWS Lambda

Lambdamenghilangkan kebutuhan untuk mengelola dan memantau server untuk beban kerja Anda dan secara otomatis bekerja dengan CloudWatchMetrik dan CloudWatch Log tanpa konfigurasi atau instrumentasi lebih lanjut dari kode aplikasi Anda. Bagian ini membantu Anda memahami karakteristik kinerja sistem yang digunakan oleh Lambda dan bagaimana pilihan konfigurasi Anda memengaruhi kinerja. Ini juga membantu Anda mencatat dan memantau fungsi Lambda Anda untuk pengoptimalan kinerja dan mendiagnosis masalah tingkat aplikasi.

Pencatatan fungsi Lambda

Lambda secara otomatis mengalirkan output standar dan pesan kesalahan standar dari fungsi Lambda ke CloudWatch Log, tanpa memerlukan driver logging. Lambda juga secara otomatis menyediakan kontainer yang menjalankan fungsi Lambda Anda dan mengonfigurasinya untuk menampilkan pesan log dalam aliran log terpisah.

Pemanggilan berikutnya dari fungsi Lambda Anda dapat menggunakan kembali wadah dan output yang sama ke aliran log yang sama. Lambda juga dapat menyediakan wadah baru dan menampilkan pemanggilan ke aliran log baru.

Lambda secara otomatis membuat grup log saat fungsi Lambda Anda pertama kali dipanggil. Fungsi Lambda dapat memiliki beberapa versi dan Anda dapat memilih versi yang ingin Anda jalankan. Semua log untuk pemanggilan fungsi Lambda disimpan dalam grup log yang sama. Nama tidak dapat diubah dan ada di`/aws/lambda/<YourLambdaFunctionName>`format. Aliran log terpisah dibuat di grup log untuk setiap instance fungsi Lambda. Lambda memiliki konvensi penamaan standar untuk aliran log yang menggunakan`YYYY/MM/DD/[<FunctionVersion>]<InstanceId>`format. The`InstanceId`dihasilkan olehAWSuntuk mengidentifikasi instance fungsi Lambda.

Kami menyarankan Anda memformat pesan log Anda dalam format JSON karena Anda dapat menanyakannya dengan lebih mudah CloudWatch Wawasan Log. Mereka juga dapat lebih mudah disaring dan diekspor. Anda dapat menggunakan pustaka logging untuk menyederhanakan proses ini atau menulis fungsi penanganan log Anda sendiri. Sebaiknya gunakan pustaka logging untuk membantu memformat dan mengklasifikasikan pesan log. Misalnya, jika fungsi Lambda Anda ditulis dengan Python, Anda dapat menggunakanModul logging Pythonuntuk mencatat pesan dan mengontrol format output. Lambda secara asli menggunakan pustaka logging Python untuk fungsi

Lambda yang ditulis dengan Python, dan Anda dapat mengambil dan menyesuaikan logger dalam fungsi Lambda Anda.AWS Labs telah menciptakanAWSLambda Powertools untuk Pythontoolkit pengembang untuk mempermudah memperkaya pesan log dengan data kunci seperti cold start. Toolkit ini tersedia untuk Python, Java, TypeScript, dan .NET.

Praktik terbaik lainnya adalah mengatur tingkat keluaran log dengan menggunakan variabel dan menyesuaikannya berdasarkan lingkungan dan kebutuhan Anda. Kode fungsi Lambda Anda, selain pustaka yang digunakan, dapat menampilkan sejumlah besar data log tergantung pada tingkat keluaran log. Ini dapat memengaruhi biaya pencatatan Anda dan memengaruhi kinerja.

Lambda memungkinkan Anda untuk mengatur variabel lingkungan untuk lingkungan runtime fungsi Lambda Anda tanpa memperbarui kode Anda. Misalnya, Anda dapat membuat`LAMBDA_LOG_LEVEL`variabel lingkungan yang mendefinisikan tingkat keluaran log yang dapat Anda ambil dari kode Anda. Contoh berikut mencoba untuk mengambil`LAMBDA_LOG_LEVEL`variabel lingkungan dan menggunakan nilai untuk menentukan output logging. Jika variabel lingkungan tidak disetel, defaultnya`INFO`tingkat.

```
import logging
from os import getenv

logger = logging.getLogger()
log_level = getenv("LAMBDA_LOG_LEVEL", "INFO")
level = logging.getLevelName(log_level)
logger.setLevel(level)
```

Mengirim log ke tujuan lain dari CloudWatch

Anda dapat mengirim log ke tujuan lain (misalnya, Amazon OpenSearch Layanan atau fungsi Lambda) dengan menggunakan filter berlangganan. Jika Anda tidak menggunakan Amazon OpenSearch Layanan, Anda dapat menggunakan fungsi Lambda untuk memproses log dan mengirimkannya keAWSLayanan pilihan Anda menggunakanAWSSDK.

Anda juga dapat menggunakan SDK untuk tujuan log di luarAWSCloud di fungsi Lambda Anda untuk langsung mengirim pernyataan log ke tujuan pilihan Anda. Jika Anda memilih opsi ini, kami sarankan Anda mempertimbangkan dampak latensi, waktu pemrosesan tambahan, penanganan kesalahan dan coba lagi, dan penggabungan logika operasional ke fungsi Lambda Anda.

Metrik fungsi Lambda

Lambda memungkinkan Anda menjalankan kode Anda tanpa mengelola atau menskalakan server dan ini hampir menghilangkan beban audit dan diagnostik tingkat sistem. Namun, tetap penting untuk memahami metrik kinerja dan pemanggilan di tingkat sistem untuk fungsi Lambda Anda. Ini membantu Anda mengoptimalkan konfigurasi sumber daya dan meningkatkan kinerja kode. Memantau dan mengukur kinerja secara efektif dapat meningkatkan pengalaman pengguna dan menurunkan biaya Anda dengan mengukur fungsi Lambda Anda dengan tepat. Biasanya, beban kerja yang berjalan sebagai fungsi Lambda juga memiliki metrik tingkat aplikasi yang perlu ditangkap dan dianalisis. Lambda secara langsung mendukung format metrik yang disematkan untuk menangkap tingkat aplikasi CloudWatch metrik lebih mudah.

Metrik tingkat sistem

Lambda secara otomatis terintegrasi dengan CloudWatch Metrik dan menyediakan satu setmetrik standar untuk fungsi Lambda Anda. Lambda juga menyediakan dasbor pemantauan terpisah untuk setiap fungsi Lambda dengan metrik ini. Dua metrik penting yang perlu Anda pantau adalah kesalahan dan kesalahan pemanggilan. Memahami perbedaan antara kesalahan pemanggilan dan jenis kesalahan lainnya membantu Anda mendiagnosis dan mendukung penerapan Lambda.

Kesalahan pemanggilanmencegah fungsi Lambda Anda berjalan. Kesalahan ini terjadi sebelum kode Anda dijalankan sehingga Anda tidak dapat menerapkan penanganan kesalahan dalam kode Anda untuk mengidentifikasi mereka. Sebagai gantinya, Anda harus mengonfigurasi alarm untuk fungsi Lambda Anda yang mendeteksi kesalahan ini dan memberi tahu pemilik operasi dan beban kerja. Kesalahan ini sering terkait dengan kesalahan konfigurasi atau izin dan dapat terjadi karena perubahan konfigurasi atau izin Anda. Kesalahan pemanggilan mungkin memulai percobaan ulang, yang menyebabkan beberapa pemanggilan fungsi Anda.

Fungsi Lambda yang berhasil dipanggil mengembalikan respons HTTP 200 bahkan jika pengecualian dilemparkan oleh fungsi tersebut. Fungsi Lambda Anda harus menerapkan penyerahan kesalahan dan memunculkan pengecualian sehingga`Errors`metrik menangkap dan mengidentifikasi fungsi Lambda Anda yang gagal. Anda harus mengembalikan respons yang diformat dari pemanggilan fungsi Lambda yang menyertakan informasi untuk menentukan apakah proses gagal sepenuhnya, sebagian, atau berhasil.

CloudWatch memberiCloudWatch Wawasan Lambdayang dapat Anda aktifkan untuk fungsi Lambda individual. Lambda Insights mengumpulkan, mengumpulkan, dan merangkum metrik tingkat

sistem (misalnya, waktu CPU, memori, disk, dan penggunaan jaringan). Lambda Insights juga mengumpulkan, mengumpulkan, dan merangkum informasi diagnostik (misalnya, start dingin dan penutupan pekerja Lambda) untuk membantu Anda mengisolasi dan menyelesaikan masalah dengan cepat.

Lambda Insights menggunakan format metrik yang disematkan untuk secara otomatis memancarkan informasi kinerja ke`/aws/lambda-insights/`grup log dengan awalan nama aliran log berdasarkan nama fungsi Lambda Anda. Peristiwa log kinerja ini dibuat CloudWatch metrik yang menjadi dasar untuk otomatis CloudWatch dasbor. Kami menyarankan Anda mengaktifkan Lambda Insights untuk pengujian kinerja dan lingkungan produksi. Metrik tambahan yang dibuat oleh Lambda Insights meliputi`memory_utilization`yang membantu mengukur fungsi Lambda dengan benar sehingga Anda menghindari pembayaran untuk kapasitas yang tidak diperlukan.

Metrik aplikasi

Anda juga dapat membuat dan menangkap metrik aplikasi Anda sendiri di CloudWatch menggunakan format metrik tertanam. Anda dapat memanfaatkanAWS menyediakan pustaka untuk format metrik yang disematkanuntuk membuat dan memancarkan pernyataan format metrik yang disematkan ke CloudWatch. Lambda terintegrasi CloudWatch fasilitas logging dikonfigurasi untuk memproses dan mengekstrak pernyataan format metrik tertanam yang diformat dengan tepat.

Mencari dan menganalisis log masuk CloudWatch

Setelah log dan metrik ditangkap ke dalam format dan lokasi yang konsisten, Anda dapat mencari dan menganalisisnya untuk membantu meningkatkan efisiensi operasional, selain mengidentifikasi dan memecahkan masalah. Kami menyarankan Anda menangkap log Anda dalam format yang terbentuk dengan baik (misalnya, JSON) untuk membuatnya lebih mudah untuk mencari dan menganalisis log Anda. Sebagian besar beban kerja menggunakan kumpulanAWS sumber daya seperti jaringan, komputasi, penyimpanan, dan database. Jika memungkinkan, Anda harus secara kolektif menganalisis metrik dan log dari sumber daya ini dan menghubungkannya agar dapat memantau dan mengelola semuaAWS beban kerja Anda secara efektif.

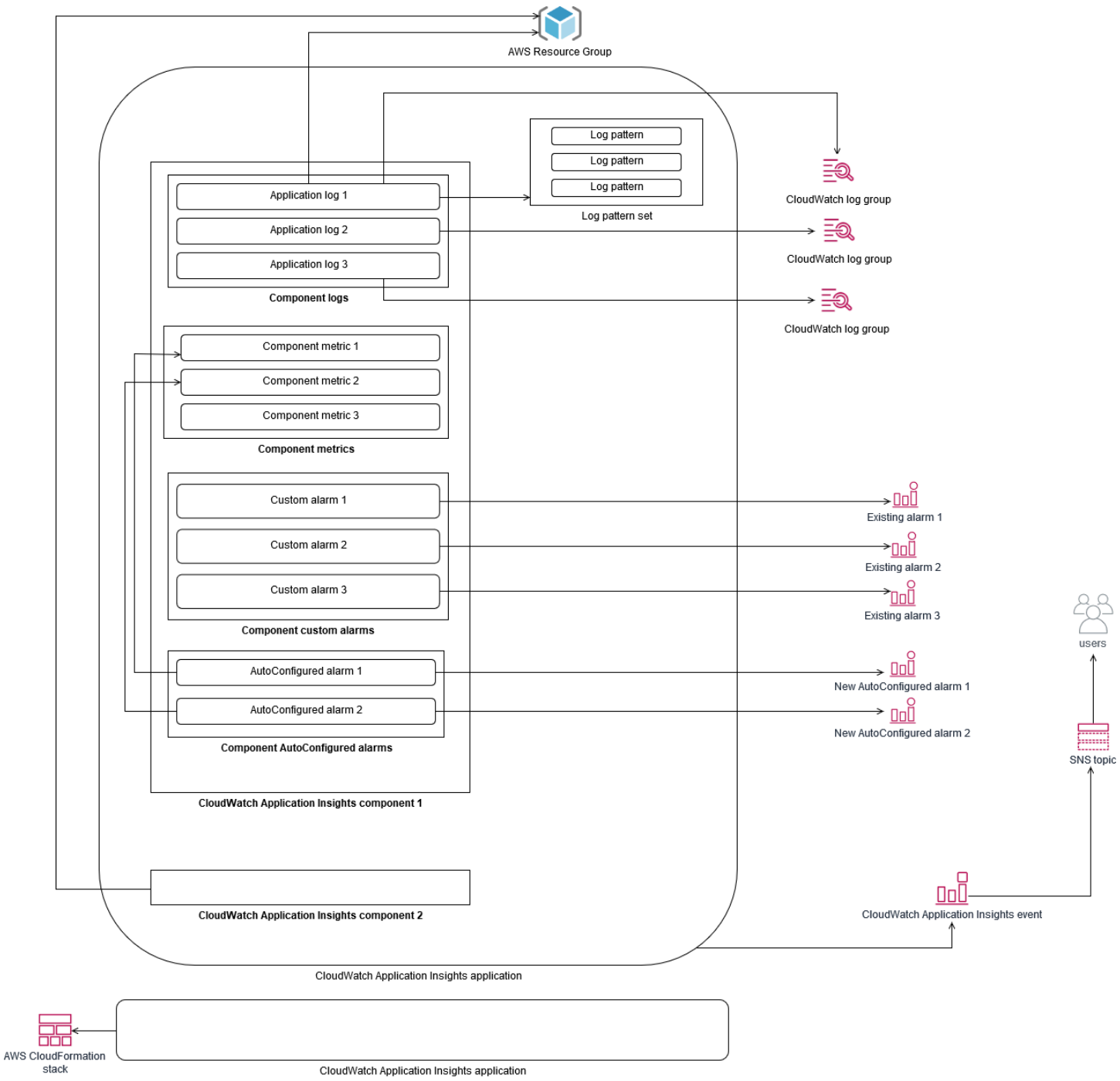
CloudWatch menyediakan beberapa fitur untuk membantu menganalisis log dan metrik, seperti CloudWatch Application Insights untuk secara kolektif menentukan dan memantau metrik dan log untuk aplikasi di berbagaiAWS sumber daya, DeteksiCloudWatch Anomali untuk menampilkan anomali untuk Anda metrik, dan CloudWatch Logs Insights untuk secara interaktif mencari dan menganalisis data log Anda di CloudWatch Logs.

Secara kolektif memantau dan menganalisis aplikasi dengan CloudWatch Application Insights

Pemilik aplikasi dapat menggunakan Amazon CloudWatch Application Insights untuk menyiapkan pemantauan dan analisis otomatis untuk beban kerja. Ini dapat dikonfigurasi selain pemantauan tingkat sistem standar yang dikonfigurasi untuk semua beban kerja di akun. Menyiapkan pemantauan melalui CloudWatch Application Insights juga dapat membantu tim aplikasi secara proaktif menyelaraskan operasi dan mengurangi mean time to recovery (MTTR). CloudWatch Wawasan Aplikasi dapat membantu mengurangi upaya yang diperlukan untuk menetapkan penebangan dan pemantauan tingkat aplikasi. Ini juga menyediakan kerangka kerja berbasis komponen yang membantu tim dalam membagi tanggung jawab penebangan dan pemantauan.

CloudWatch Application Insights menggunakan grup sumber daya untuk mengidentifikasi sumber daya yang harus dipantau secara kolektif sebagai aplikasi. Sumber daya yang didukung dalam grup sumber daya menjadi komponen CloudWatch aplikasi Application Insights yang ditentukan secara individual. Setiap komponen CloudWatch aplikasi Application Insights Anda memiliki log, metrik, dan alarmnya sendiri.

Untuk log, Anda menentukan kumpulan pola log yang harus digunakan untuk komponen dan dalam CloudWatch aplikasi Application Insights Anda. Kumpulan pola log adalah kumpulan pola log untuk dicari berdasarkan ekspresi reguler, bersama dengan tingkat keparahan rendah, sedang, atau tinggi saat pola terdeteksi. Untuk metrik, Anda memilih metrik untuk memantau setiap komponen dari daftar metrik khusus layanan dan didukung. Untuk alarm, CloudWatch Application Insights secara otomatis membuat dan mengonfigurasi alarm deteksi standar atau anomali untuk metrik yang sedang dipantau. CloudWatch Application Insights memiliki konfigurasi otomatis untuk metrik dan pengambilan log untuk teknologi yang diuraikan dalam Log dan metrik yang didukung oleh CloudWatch Application Insights dalam CloudWatch dokumentasi. Diagram berikut menunjukkan hubungan antara komponen CloudWatch Application Insights dan konfigurasi logging dan monitoring mereka. Setiap komponen telah menentukan log dan metriknya sendiri untuk dipantau menggunakan CloudWatch log dan metrik.



Instans EC2 yang dipantau oleh CloudWatch Application Insights memerlukan Systems Manager dan CloudWatch agen serta izin. Untuk informasi selengkapnya tentang ini, lihat Prasyarat untuk mengonfigurasi aplikasi dengan CloudWatch Application Insights dalam CloudWatch dokumentasi. CloudWatch Application Insights menggunakan Systems Manager untuk menginstal dan memperbarui CloudWatch agen. Metrik dan log yang dikonfigurasi di CloudWatch Application Insights membuat file konfigurasi CloudWatch agen yang disimpan dalam parameter Systems

Manager dengan`AmazonCloudWatch-ApplicationInsights-SSMParameter` awalan untuk setiap komponen CloudWatch Application Insights. Ini menghasilkan file konfigurasi CloudWatch agen terpisah yang ditambahkan ke direktori konfigurasi CloudWatch agen pada instans EC2. Perintah Systems Manager dijalankan untuk menambahkan konfigurasi ini ke konfigurasi aktif pada instans EC2. Menggunakan CloudWatch Application Insights tidak memengaruhi pengaturan konfigurasi CloudWatch agen yang ada. Anda dapat menggunakan CloudWatch Application Insights selain konfigurasi CloudWatch agen tingkat aplikasi dan sistem Anda sendiri. Namun, Anda harus memastikan bahwa konfigurasinya tidak tumpang tindih.

Melakukan analisis CloudWatch log dengan Wawasan Log

CloudWatch Wawasan Log memudahkan pencarian beberapa grup log dengan menggunakan bahasa kueri sederhana. Jika log aplikasi Anda terstruktur dalam format JSON, Wawasan CloudWatch Log secara otomatis menemukan bidang JSON di seluruh aliran log Anda dalam beberapa grup log. Anda dapat menggunakan Wawasan CloudWatch Log untuk menganalisis log aplikasi dan sistem Anda, yang menyimpan kueri Anda untuk penggunaan di future. Sintaks kueri untuk Wawasan CloudWatch Log mendukung fungsi seperti agregasi dengan fungsi, misalnya, sum (), avg (), count (), min (), dan max (), yang dapat membantu mengatasi masalah aplikasi atau analisis kinerja Anda.

Jika Anda menggunakan format metrik tersemat untuk membuat CloudWatch metrik, Anda dapat mengkueri log format metrik tersemat untuk menghasilkan metrik satu kali dengan menggunakan fungsi agregasi yang didukung. Ini membantu mengurangi biaya CloudWatch pemantauan Anda dengan menangkap titik data yang diperlukan untuk menghasilkan metrik tertentu sesuai kebutuhan, alih-alih secara aktif menangkapnya sebagai metrik khusus. Ini sangat efektif untuk dimensi dengan kardinalitas tinggi yang akan menghasilkan sejumlah besar metrik. CloudWatch Container Insights juga mengambil pendekatan ini dan menangkap data kinerja terperinci tetapi hanya menghasilkan CloudWatch metrik untuk subset data ini.

Misalnya, entri metrik tertanam berikut ini hanya menghasilkan sekumpulan CloudWatch metrik terbatas dari data metrik yang diambil dalam pernyataan format metrik tertanam:

```
{
 "AutoScalingGroupName": "eks-e0bab7f4-fa6c-64ba-dbd9-094aee6cf9ba",
 "CloudWatchMetrics": [
 {
 "Metrics": [
 {
```

```
"Unit": "Count",
"Name": "pod_number_of_container_restarts"
}
],
"Dimensions": [
[
"PodName",
"Namespace",
"ClusterName"
]
],
"Namespace": "ContainerInsights"
}
],
"ClusterName": "eksdemo",
"InstanceId": "i-03b21a16b854aa4ca",
"InstanceType": "t3.medium",
"Namespace": "amazon-cloudwatch",
"NodeName": "ip-172-31-10-211.ec2.internal",
"PodName": "cloudwatch-agent",
"Sources": [
"cadvisor",
"pod",
"calculated"
],
"Timestamp": "1605111338968",
"Type": "Pod",
"Version": "0",
"pod_cpu_limit": 200,
"pod_cpu_request": 200,
"pod_cpu_reserved_capacity": 10,
"pod_cpu_usage_system": 3.268605094109382,
"pod_cpu_usage_total": 8.899539221131045,
"pod_cpu_usage_user": 4.160042847048305,
"pod_cpu_utilization": 0.44497696105655227,
"pod_cpu_utilization_over_pod_limit": 4.4497696105655224,
"pod_memory_cache": 4096,
"pod_memory_failcnt": 0,
"pod_memory_hierarchical_pgfault": 0,
"pod_memory_hierarchical_pgmajfault": 0,
"pod_memory_limit": 209715200,
"pod_memory_mapped_file": 0,
"pod_memory_max_usage": 43024384,
```

```
 "pod_memory_pgfault": 0,
 "pod_memory_pgmajfault": 0,
 "pod_memory_request": 209715200,
 "pod_memory_reserved_capacity": 5.148439982463127,
 "pod_memory_rss": 38481920,
 "pod_memory_swap": 0,
 "pod_memory_usage": 42803200,
 "pod_memory_utilization": 0.6172094650851303,
 "pod_memory_utilization_over_pod_limit": 11.98828125,
 "pod_memory_working_set": 25141248,
 "pod_network_rx_bytes": 3566.4174629544723,
 "pod_network_rx_dropped": 0,
 "pod_network_rx_errors": 0,
 "pod_network_rx_packets": 3.3495665260575094,
 "pod_network_total_bytes": 4283.442421354973,
 "pod_network_tx_bytes": 717.0249584005006,
 "pod_network_tx_dropped": 0,
 "pod_network_tx_errors": 0,
 "pod_network_tx_packets": 2.6964010534762948,
 "pod_number_of_container_restarts": 0,
 "pod_number_of_containers": 1,
 "pod_number_of_running_containers": 1,
 "pod_status": "Running"
}
```

Namun, Anda dapat menanyakan metrik yang diambil untuk mendapatkan wawasan lebih lanjut. Sebagai contoh, Anda dapat menjalankan kueri berikut untuk melihat 20 Pod terbaru dengan kesalahan halaman memori:

```
fields @timestamp, @message
| filter (pod_memory_pgfault > 0)
| sort @timestamp desc
| limit 20
```

Melakukan analisis log dengan Amazon OpenSearch Service

CloudWatch terintegrasi dengan Amazon OpenSearch Service dengan memungkinkan Anda melakukan streaming data log dari grup CloudWatch log ke klaster OpenSearch Layanan Amazon pilihan Anda dengan filter langganan. Anda dapat menggunakan CloudWatch untuk pengambilan dan analisis log dan metrik primer, lalu menambahkannya dengan Amazon OpenSearch Service untuk kasus penggunaan berikut:

- Kontrol akses data berbutir halus — Amazon OpenSearch Service memungkinkan Anda membatasi akses ke data hingga ke tingkat bidang dan membantu menganonimkan data di bidang berdasarkan izin pengguna. Ini berguna jika Anda ingin mendukung pemecahan masalah tanpa mengekspos data sensitif.
- Agregat dan log pencarian di beberapa akun, Wilayah, dan infrastruktur — Anda dapat melakukan streaming log dari beberapa akun dan Wilayah ke dalam klaster OpenSearch Layanan Amazon yang umum. Tim operasi terpusat Anda dapat menganalisis tren, masalah, dan melakukan analitik di seluruh akun dan Wilayah. Streaming CloudWatch log ke Amazon OpenSearch Service juga membantu Anda mencari dan menganalisis aplikasi Multi-wilayah di lokasi pusat.
- Kirim dan perkaya log langsung ke Amazon OpenSearch Service dengan menggunakan ElasticSearch agen — Komponen tumpukan aplikasi dan teknologi Anda dapat menggunakan OS yang tidak didukung oleh CloudWatch agen. Anda mungkin juga ingin memperkaya dan mengubah data log sebelum dikirim ke solusi logging Anda. Amazon OpenSearch Service mendukung klien Elasticsearch standar seperti pengirim data keluarga Elastic Beats dan Logstash yang mendukung pengayaan dan transformasi log sebelum mengirim data log ke Amazon OpenSearch Service.
- Solusi manajemen operasi yang ada menggunakan Tumpukan ElasticSearch, Logstash, Kibana (ELK) untuk pencatatan dan pemantauan - Anda mungkin sudah memiliki investasi yang signifikan di Amazon OpenSearch Service atau Elasticsearch sumber terbuka dengan banyak beban kerja yang sudah dikonfigurasi. Anda mungkin juga memiliki dasbor operasional yang telah dibuat di Kibana yang ingin Anda gunakan.

Jika Anda tidak berencana untuk menggunakan CloudWatch log, Anda dapat menggunakan agen, driver log, dan pustaka yang didukung Amazon OpenSearch Service (misalnya, Fluent Bit, Fluentd, logstash, dan Open Distro for ElasticSearch API) untuk mengirimkan log Anda langsung ke Amazon OpenSearch Service dan bypass CloudWatch. Namun, Anda juga harus menerapkan solusi untuk menangkap log yang dihasilkan olehAWS layanan. CloudWatch Log adalah solusi penangkapan log utama untuk banyakAWS layanan dan beberapa layanan secara otomatis membuat grup log baru CloudWatch. Misalnya, Lambda membuat grup log baru untuk setiap fungsi Lambda. Anda dapat menyiapkan filter langganan untuk grup log untuk melakukan streaming lognya ke Amazon OpenSearch Service. Anda dapat mengonfigurasi filter langganan secara manual untuk setiap grup log individual yang ingin Anda streaming ke Amazon OpenSearch Service. Atau, Anda dapat menerapkan solusi yang secara otomatis berlangganan grup log baru ke ElasticSearch klaster. Anda dapat melakukan streaming log ke ElasticSearch klaster di akun yang sama atau akun terpusat. Streaming log ke ElasticSearch klaster di akun yang sama membantu pemilik beban kerja untuk menganalisis dan mendukung beban kerja mereka dengan lebih baik.

Anda harus mempertimbangkan untuk menyiapkan ElasticSearch klaster di akun terpusat atau bersama untuk menggabungkan log di seluruh akun, Wilayah, dan aplikasi Anda. Misalnya,AWS Control Tower menyiapkan akun Arsip Log yang digunakan untuk pencatatan terpusat. Saat akun baru dibuatAWS Control Tower,AWS CloudTrail danAWS Config lognya dikirimkan ke bucket S3 di akun terpusat ini. Pencatatan yang diinstrumentasi olehAWS Control Tower adalah untuk konfigurasi, perubahan, dan pencatatan audit.

Untuk membuat solusi analisis log aplikasi terpusat dengan Amazon OpenSearch Service, Anda dapat menerapkan satu atau lebih klaster Amazon OpenSearch Service terpusat ke akun logging terpusat dan mengonfigurasi grup log di akun Anda yang lain untuk melakukan streaming log ke Amazon OpenSearch Service terpusat cluster.

Anda dapat membuat klaster Amazon OpenSearch Service terpisah untuk menangani berbagai aplikasi atau lapisan arsitektur cloud Anda yang mungkin didistribusikan ke seluruh akun Anda. Menggunakan klaster Amazon OpenSearch Service yang terpisah membantu Anda mengurangi risiko keamanan dan ketersediaan dan memiliki klaster Amazon OpenSearch Service yang umum dapat mempermudah pencarian dan menghubungkan data dalam klaster yang sama.

Opsi yang mengkhawatirkan dengan CloudWatch

Melakukan analisis satu kali dan otomatis terhadap metrik penting membantu Anda mendeteksi dan menyelesaikan masalah sebelum memengaruhi beban kerja Anda. CloudWatch memudahkan grafik dan membandingkan beberapa metrik dengan menggunakan beberapa statistik selama periode waktu tertentu. Anda dapat menggunakan CloudWatch untuk mencari di semua metrik dengan nilai dimensi yang diperlukan untuk menemukan metrik yang Anda butuhkan untuk analisis Anda.

Sebaiknya Anda memulai pendekatan penangkapan metrik dengan menyertakan serangkaian metrik dan dimensi awal untuk digunakan sebagai dasar untuk memantau beban kerja. Seiring waktu, beban kerja jatuh tempo dan Anda dapat menambahkan metrik dan dimensi tambahan untuk membantu Anda menganalisis dan mendukungnya lebih lanjut. Aplikasi atau beban kerja Anda mungkin menggunakan beberapaAWSsumber daya dan memiliki metrik kustom mereka sendiri, Anda harus mengelompokkan sumber daya ini di bawah namespace untuk membuatnya lebih mudah untuk mengidentifikasi.

Anda juga harus mempertimbangkan bagaimana data pencatatan dan pemantauan berkorelasi sehingga Anda dapat dengan cepat mengidentifikasi data pencatatan dan pemantauan yang relevan untuk mendiagnosis masalah tertentu. Anda dapat menggunakanServiceLensuntuk mengkorelasikan jejak, metrik, log, dan alarm untuk mendiagnosis masalah. Anda juga harus mempertimbangkan menyertakan dimensi tambahan dalam metrik dan pengidentifikasi dalam log untuk beban kerja Anda untuk membantu Anda mencari dan mengidentifikasi masalah di seluruh sistem dan layanan dengan cepat.

Menggunakan CloudWatch alarm untuk memantau dan alarm

Anda dapat menggunakanAlarm CloudWatchuntuk mengurangi pemantauan manual dalam beban kerja atau aplikasi Anda. Anda harus mulai dengan meninjau metrik yang Anda tangkap untuk setiap komponen beban kerja dan menentukan ambang batas yang sesuai untuk setiap metrik. Pastikan bahwa Anda mengidentifikasi anggota tim mana yang harus diberi tahu ketika ambang batas dilanggar. Anda harus menetapkan dan menargetkan kelompok distribusi, bukan anggota tim individual.

Alarm CloudWatch dapat berintegrasi dengan solusi manajemen layanan Anda untuk secara otomatis membuat tiket baru dan menjalankan alur kerja operasional. Misalnya,AWSmenyediakanAWSKonektor Manajemen untukServiceNowdanMeja Layanan Jirauntuk

membantu Anda dengan cepat mengatur integrasi. Pendekatan ini sangat penting untuk memastikan bahwa alarm yang diangkat diakui dan selaras dengan alur kerja operasi yang ada yang mungkin sudah didefinisikan dalam produk ini.

Anda juga dapat membuat beberapa alarm untuk metrik yang sama yang memiliki ambang batas dan periode evaluasi yang berbeda, yang membantu membangun proses eskalasi. Misalnya, jika Anda memiliki`OrderQueueDepth`metrik yang melacak pesanan pelanggan, Anda mungkin menentukan ambang batas yang lebih rendah selama periode rata-rata satu menit singkat yang memberitahukan anggota tim aplikasi melalui email atauKendur. Anda juga dapat menentukan alarm lain untuk metrik yang sama selama periode 15 menit yang lebih lama pada ambang yang sama dan halaman, email, dan memberi tahu tim aplikasi dan tim aplikasi memimpin. Akhirnya, Anda dapat menentukan alarm ketiga untuk ambang batas rata-rata keras selama periode 30 menit yang memberitahukan manajemen atas dan memberi tahu semua anggota tim yang sebelumnya diberi tahu. Membuat beberapa alarm membantu Anda mengambil tindakan yang berbeda untuk kondisi yang berbeda. Anda dapat mulai dengan proses notifikasi sederhana dan kemudian menyesuaikan dan memperbaikinya sesuai kebutuhan.

Menggunakan CloudWatch deteksi anomali untuk memantau dan alarm

Anda dapat menggunakanDeteksi anomali CloudWatchjika Anda tidak yakin tentang ambang batas untuk mengajukan metrik tertentu atau jika Anda ingin alarm menyesuaikan nilai ambang batas secara otomatis berdasarkan nilai historis yang diamati. CloudWatch Deteksi anomali sangat berguna untuk metrik yang mungkin memiliki perubahan aktivitas yang teratur dan dapat diprediksi, misalnya, pesanan pembelian harian untuk pengiriman hari yang sama meningkat sebelum waktu cutoff. Deteksi anomali memungkinkan ambang batas yang menyesuaikan secara otomatis dan dapat membantu mengurangi alarm palsu. Anda dapat mengaktifkan deteksi anomali untuk setiap metrik dan statistik, dan mengkonfigurasi CloudWatch alarm berdasarkan outlier.

Misalnya, Anda dapat mengaktifkan deteksi anomali untuk`CPUUtilization`metrik dan`AVG`statistik pada instans EC2. Deteksi anomali kemudian menggunakan data historis hingga 14 hari untuk membuat model machine learning (ML). Anda dapat membuat beberapa alarm dengan band deteksi anomali yang berbeda untuk membuat proses eskalasi alarm, mirip dengan membuat beberapa alarm standar dengan ambang batas yang berbeda.

Untuk informasi selengkapnya tentang bagian ini, lihatMembuat alarm CloudWatch berdasarkan pada deteksi anomalidi CloudWatch dokumentasi.

Mengkhawatirkan di beberapa Wilayah dan akun

Pemilik aplikasi dan beban kerja harus membuat alarm tingkat aplikasi untuk beban kerja yang mencakup beberapa Wilayah. Sebaiknya buat alarm terpisah di setiap akun dan Wilayah yang digunakan beban kerja Anda. Anda dapat menyederhanakan dan mengotomatisasi proses ini dengan menggunakan akun dan Wilayah agnostikAWS CloudFormation StackSets dan template untuk menyebarkan sumber daya aplikasi dengan alarm yang diperlukan. templateAnda dapat mengkonfigurasi tindakan alarm untuk menargetkan topik Amazon Simple Notification Service (Amazon SNS) umum, yang berarti tindakan pemberitahuan atau remediasi yang sama digunakan terlepas dari akun atau Wilayah.

Di lingkungan multi-akun dan Multi-wilayah, kami menyarankan agar Anda membuat alarm gabungan untuk akun dan Wilayah Anda untuk memantau masalah akun dan Regional dengan menggunakanAWS CloudFormation StackSets dan metrik agregat, seperti rata-rata`CPUUtilization`di semua instans EC2.

Anda juga harus mempertimbangkan untuk membuat alarm standar untuk setiap beban kerja yang dikonfigurasi untuk standar CloudWatch metrik dan log yang Anda tangkap. Misalnya, Anda dapat membuat alarm terpisah untuk setiap instans EC2 yang memonitor metrik pemanfaatan CPU dan memberi tahu tim operasi pusat ketika pemanfaatan CPU rata-rata lebih dari 80% setiap hari. Anda juga dapat membuat alarm standar yang memonitor pemanfaatan CPU rata-rata di bawah 10% setiap hari. Alarm ini membantu tim operasi pusat untuk bekerja dengan pemilik beban kerja tertentu untuk mengubah ukuran instans EC2 bila diperlukan.

Mengotomatisasi pembuatan alarm dengan tag instans EC2

Membuat seperangkat alarm standar untuk instans EC2 Anda dapat memakan waktu, tidak konsisten, dan rawan kesalahan. Anda dapat mempercepat proses pembuatan alarm dengan menggunakanamazon-cloudwatch-auto-alarmsolusi untuk secara otomatis membuat satu set standar alarm CloudWatch untuk instans EC2 Anda dan membuat alarm kustom berdasarkan tag instans EC2. Solusi ini menghilangkan kebutuhan untuk membuat alarm standar secara manual dan dapat berguna selama migrasi skala besar instans EC2 yang menggunakan alat seperti CloudEndure. Anda juga dapat menerapkan solusi ini denganAWS CloudFormation StackSets untuk mendukung beberapa Wilayah dan akun. Untuk informasi selengkapnya, lihatMenggunakan tag untuk membuat dan memelihara Amazon CloudWatch alarm untuk instans Amazon EC2padaAWSBlog.

Memantau ketersediaan aplikasi dan layanan

CloudWatch membantu Anda memantau dan menganalisis aspek kinerja dan runtime aplikasi dan beban kerja Anda. Anda juga harus memantau aspek ketersediaan dan jangkauan aplikasi dan beban kerja Anda. Anda dapat mencapai hal ini dengan menggunakan pendekatan pemantauan aktif denganPemeriksaan kondisi Amazon Route 53danCloudWatch Synthetics.

Anda dapat menggunakan pemeriksaan kesehatan Route 53 ketika Anda ingin memantau konektivitas ke halaman web melalui HTTP atau HTTPS, atau konektivitas jaringan melalui TCP ke nama Domain Name System (DNS) publik atau alamat IP. Rute 53 pemeriksaan kesehatan memulai koneksi dari Daerah yang Anda tentukan pada interval sepuluh detik atau 30 detik. Anda dapat memilih beberapa Wilayah untuk pemeriksaan kesehatan untuk dijalankan, setiap pemeriksaan kesehatan berjalan secara independen, dan Anda harus memilih setidaknya tiga Wilayah. Anda dapat mencari badan respons permintaan HTTP atau HTTPS untuk substring tertentu jika muncul dalam 5,120 byte data pertama yang dikembalikan untuk evaluasi pemeriksaan kesehatan. Permintaan HTTP atau HTTPS dianggap sehat jika mengembalikan respons 2xx atau 3xx. Rute 53 pemeriksaan kesehatan dapat digunakan untuk membuat pemeriksaan kesehatan komposit dengan memeriksa kesehatan pemeriksaan kesehatan lainnya. Anda dapat melakukan ini jika Anda memiliki beberapa titik akhir layanan dan Anda ingin melakukan pemberitahuan yang sama ketika salah satu dari mereka menjadi tidak sehat. Jika Anda menggunakan Route 53 untuk DNS, Anda dapat mengkonfigurasi Route 53 kegagal ke entri DNS lainjika pemeriksaan kesehatan menjadi tidak sehat. Untuk setiap beban kerja penting, Anda harus mempertimbangkan pengaturan pemeriksaan kesehatan Route 53 untuk titik akhir eksternal yang sangat penting untuk operasi normal. Rute 53 pemeriksaan kesehatan dapat membantu Anda menghindari menulis logika failover ke dalam aplikasi Anda.

Sintetis CloudWatch memungkinkan Anda mendefinisikan kenari sebagai skrip untuk mengevaluasi kesehatan dan ketersediaan beban kerja Anda. Canary adalah skrip yang ditulis dalam Node.js atau Python dan bekerja melalui protokol HTTP atau HTTPS. Mereka membuat fungsi Lambda di akun Anda yang menggunakan Node.js atau Python sebagai kerangka kerja. Setiap kenari yang Anda tetapkan dapat melakukan beberapa panggilan HTTP atau HTTPS ke titik akhir yang berbeda. Ini berarti Anda dapat memantau kesehatan serangkaian langkah, seperti kasus penggunaan atau titik akhir dengan dependensi hilir. Canary membuat CloudWatch metrik yang mencakup setiap langkah yang dijalankan sehingga Anda dapat alarm dan mengukur langkah yang berbeda secara independen. Meskipun burung kenari memerlukan lebih banyak perencanaan dan upaya untuk mengembangkan daripada pemeriksaan kesehatan Route 53, mereka memberi Anda pendekatan

pemantauan dan evaluasi yang sangat dapat disesuaikan. Canaries juga mendukung sumber daya pribadi yang berjalan dalam virtual private cloud (VPC) Anda, yang membuatnya ideal untuk pemantauan ketersediaan ketika Anda tidak memiliki alamat IP publik untuk titik akhir. Anda juga dapat menggunakan kenari untuk memantau beban kerja lokal selama Anda memiliki konektivitas dari dalam VPC ke titik akhir. Hal ini sangat penting ketika Anda memiliki beban kerja yang mencakup titik akhir yang ada di tempat.

Aplikasi penelusuran denganAWS X-Ray

Permintaan melalui aplikasi Anda mungkin terdiri dari panggilan ke database, aplikasi, dan layanan web yang berjalan di server lokal, Amazon EC2, kontainer, atau Lambda. Dengan menerapkan pelacakan aplikasi, Anda dapat dengan cepat mengidentifikasi akar penyebab masalah dalam aplikasi Anda yang menggunakan komponen dan layanan terdistribusi. Anda dapat menggunakanAWS X-Rayuntuk melacak permintaan aplikasi Anda di beberapa komponen. Sampel X-Ray dan memvisualisasikan permintaan padagrafik layananketika mereka mengalir melalui komponen aplikasi Anda dan setiap komponen direpresentasikan sebagai segmen. X-Ray menghasilkan pengidentifikasi jejak sehingga Anda dapat mengkorelasikan permintaan saat mengalir melalui beberapa komponen, yang membantu Anda melihat permintaan dari ujung ke ujung. Anda dapat lebih meningkatkan ini dengan menyertakan anotasi dan metadata untuk membantu secara unik mencari dan mengidentifikasi karakteristik permintaan.

Sebaiknya konfigurasikan dan instrumen setiap server atau titik akhir dalam aplikasi Anda dengan X-Ray. X-Ray diimplementasikan dalam kode aplikasi Anda dengan melakukan panggilan ke layanan X-Ray. X-Ray juga menyediakanAWSSDK untuk berbagai bahasa, termasuk klien berinstrumen yang secara otomatis mengirim data ke X-Ray. X-Ray SDK menyediakan patch ke pustaka umum yang digunakan untuk melakukan panggilan ke layanan lain (misalnya, HTTP, MySQL, PostgreSQL, atau MongoDB).

X-Ray menyediakan daemon X-Ray yang dapat Anda instal dan jalankan di Amazon EC2 dan Amazon ECS untuk menyampaikan data ke X-Ray. X-Ray membuat jejak untuk aplikasi Anda yang menangkap data kinerja dari server dan kontainer yang menjalankan daemon X-Ray yang melayani permintaan. X-Ray secara otomatis menginstruksikan panggilan AndaAWSlayanan, seperti Amazon DynamoDB, sebagai subsegment melalui menambalAWSSDK. X-Ray juga dapat secara otomatis berintegrasi dengan fungsi Lambda.

Jika komponen aplikasi Anda melakukan panggilan ke layanan eksternal yang tidak dapat mengkonfigurasi dan menginstal daemon X-Ray atau instrumen kode, Anda dapat membuatsubsegment untuk membungkus panggilan ke layanan eksternal. X-Ray berkorelasi CloudWatch log dan metrik dengan jejak aplikasi Anda jika Anda menggunakanAWS X-Ray SDK for Java, yang berarti Anda dapat dengan cepat menganalisis metrik dan log terkait untuk permintaan.

Menyebarkan daemon X-Ray untuk melacak aplikasi dan layanan di Amazon EC2

Anda perlu menginstal dan menjalankan daemon X-Ray pada instans EC2 yang dijalankan oleh komponen aplikasi atau layanan mikro Anda. Anda dapat menggunakanskrip data penggunauntuk menyebarkan daemon X-Ray saat instans EC2 disediakan atau Anda dapat memasukkannya ke dalam proses pembuatan AMI jika Anda membuat AMI sendiri. Hal ini dapat sangat berguna ketika instans EC2 bersifat sementara.

Anda harus menggunakan State Manager untuk memastikan daemon X-Ray diinstal secara konsisten di instans EC2 Anda. Untuk Amazon EC2Windowscontoh, Anda dapat menggunakan Systems ManagerAWSDokumen -RunPowerShellScriptmenjalankanSkrip jendelayang mengunduh dan menginstal agen X-Ray. Untuk instans EC2 di Linux, Anda dapat menggunakanAWS-RunShellScript dokumen untuk menjalankan script Linux yangdownload dan menginstal agen sebagai layanan.

Anda dapat menggunakan Systems ManagerAWSDokumen -RunRemoteScriptuntuk menjalankan script dalam lingkungan multi-akun. Anda harus membuat bucket S3 yang dapat diakses dari semua akun Anda dan kami sarankanmembuat bucket S3 dengan kebijakan bucket berbasis organisasijika Anda menggunakanAWS Organizations. Anda kemudian mengunggah skrip ke bucket S3 tetapi pastikan bahwa peran IAM untuk instans EC2 Anda memiliki izin untuk mengakses bucket dan skrip.

Anda juga dapat mengonfigurasi State Manager untuk mengaitkan skrip ke instans EC2 yang menginstal agen X-Ray. Karena semua instans EC2 Anda mungkin tidak memerlukan atau menggunakan X-Ray, Anda dapat menargetkan asosiasi dengan tag instans. Misalnya, Anda dapat membuat asosiasi Manajer Negara berdasarkan kehadiran`InstallAWSXRayDaemonWindows`atau`InstallAWSXRayDaemonLinux`tag.

Menyebarkan daemon X-Ray untuk melacak aplikasi dan layanan di Amazon ECS atau Amazon EKS

Anda dapat menyebarkanX-Ray daemonsebagai wadah sidecar untuk beban kerja berbasis kontainer seperti Amazon ECS atau Amazon EKS. Kontainer aplikasi Anda kemudian dapat terhubung ke wadah sidecar Anda dengan penautan kontainer jika Anda menggunakan Amazon ECS, atau kontainer dapat langsung terhubung ke kontainer sidecar di localhost jika Anda menggunakanMode jaringan awsvpc.

Untuk Amazon EKS, Anda dapat menentukan daemon X-Ray dalam definisi pod aplikasi Anda dan kemudian aplikasi Anda dapat terhubung ke daemon melalui localhost pada port kontainer yang Anda tentukan.

Mengkonfigurasi Lambda untuk melacak permintaan ke X-Ray

Aplikasi Anda mungkin menyertakan panggilan ke fungsi Lambda. Anda tidak perlu menginstal daemon X-Ray untuk Lambda karena proses daemon dikelola penuh oleh Lambda dan tidak dapat dikonfigurasi oleh pengguna. Anda dapat mengaktifkannya untuk fungsi Lambda Anda dengan menggunakanAWS Management Consoledan memeriksaPelacakan Aktifdi konsol X-Ray.

Untuk instrumentasi lebih lanjut, Anda dapat menggabungkan X-Ray SDK dengan fungsi Lambda Anda untuk merekam panggilan keluar dan menambahkan anotasi atau metadata.

Menginstrumentasi aplikasi Anda untuk X-Ray

Anda harus mengevaluasi X-Ray SDK yang selaras dengan bahasa pemrograman aplikasi Anda dan mengklasifikasikan semua panggilan yang dibuat aplikasi Anda ke sistem lain. Tinjau klien yang disediakan oleh perpustakaan yang Anda pilih dan lihat apakah SDK dapat secara otomatis melakukan pelacakan instrumen untuk permintaan atau respons aplikasi Anda. Tentukan apakah klien yang disediakan oleh SDK dapat digunakan untuk sistem hilir lainnya. Untuk sistem eksternal yang panggilan aplikasi Anda dan yang tidak dapat Anda instrumen dengan X-Ray, Anda harus membuat subsegmen kustom untuk menangkap dan mengidentifikasi mereka dalam informasi jejak Anda.

Ketika Anda instrumen aplikasi Anda, pastikan bahwa Anda membuat anotasi untuk membantu Anda mengidentifikasi dan mencari permintaan. Misalnya, aplikasi Anda mungkin menggunakan pengenal untuk pelanggan, seperti`customer id`, atau segmen pengguna yang berbeda berdasarkan peran mereka dalam aplikasi.

Anda dapat membuat maksimum 50 anotasi untuk setiap pelacakan tetapi Anda dapat membuat objek metadata yang berisi satu atau lebih bidang selama dokumen segmen tidak melebihi 64 kilobyte. Anda harus secara selektif menggunakan anotasi untuk menemukan informasi dan menggunakan objek metadata untuk memberikan lebih banyak konteks yang membantu memecahkan masalah permintaan setelah berada.

Mengonfigurasi aturan pengambilan sampel X-Ray

olehmenyesuaikan aturan pengambilan sampel, Anda dapat mengontrol jumlah data yang Anda catat dan mengubah perilaku pengambilan sampel tanpa mengubah atau men-deploy ulang kode Anda. Aturan pengambilan sampel memberi tahu SDK X-Ray jumlah permintaan yang harus dicatat untuk satu set kriteria. Secara default, catatan X-Ray SDKpermintaan pertama setiap detik dan lima persen dari setiap permintaan tambahan. Satu permintaan per detik adalah reservoir. Tindakan ini memastikan bahwa setidaknya satu pelacakan dicatat setiap detik selama layanan melayani permintaan. Lima persen adalah tingkat di mana permintaan tambahan diambil sampel di luar ukuran reservoir.

Anda harus meninjau dan memperbarui konfigurasi default untuk menentukan nilai yang sesuai untuk akun Anda. Persyaratan Anda mungkin berbeda dalam pengembangan, pengujian, uji kinerja, dan lingkungan produksi. Anda mungkin memiliki aplikasi yang memerlukan aturan pengambilan sampel mereka sendiri berdasarkan jumlah lalu lintas yang mereka terima atau tingkat kekritisan mereka. Anda harus mulai dengan garis dasar dan secara teratur mengevaluasi ulang apakah baseline memenuhi kebutuhan Anda.

Dasbor dan visualisasi dengan CloudWatch

Dasbor membantu Anda dengan cepat fokus pada bidang perhatian untuk aplikasi dan beban kerja. CloudWatch menyediakan dasbor otomatis dan Anda juga dapat dengan mudah membuat dasbor yang menggunakan CloudWatch metrik. CloudWatch dasbor memberikan wawasan lebih daripada melihat metrik dalam isolasi karena mereka membantu Anda menghubungkan beberapa metrik dan mengidentifikasi tren. Misalnya, dasbor yang mencakup pesanan yang diterima, memori, pemanfaatan CPU, dan koneksi database dapat membantu Anda mengkorelasikan perubahan dalam metrik beban kerja di beberapaAWSsumber daya sementara jumlah pesanan Anda meningkat atau menurun.

Anda harus membuat dasbor di akun dan tingkat aplikasi untuk memantau beban kerja dan aplikasi. Anda dapat memulai dengan menggunakan CloudWatch dashboard otomatis, yangAWSDasbor tingkat layanan yang telah dikonfigurasikan dengan metrik khusus layanan. Dasbor layanan otomatis menampilkan semua standar CloudWatch metrik untuk layanan. Dasbor otomatis grafik semua sumber daya yang digunakan untuk setiap metrik layanan dan membantu Anda dengan cepat mengidentifikasi sumber daya outlier di seluruh akun Anda. Ini dapat membantu Anda mengidentifikasi sumber daya dengan pemanfaatan tinggi dan rendah, yang dapat membantu Anda mengoptimalkan biaya Anda.

Membuat dasbor lintas layanan

Anda dapat membuat dashboard lintas layanan dengan melihat dashboard tingkat layanan otomatis untukAWSlayanan dan menggunakanTambahkan ke dasborpilihan dariTindakanmenu. Anda kemudian dapat menambahkan metrik dari dasbor otomatis lainnya ke dasbor baru Anda dan menghapus metrik untuk mempersempit fokus dasbor. Anda juga harus menambahkan metrik kustom Anda sendiri untuk melacak pengamatan kunci (misalnya, pesanan yang diterima atau transaksi per detik). Membuat dasbor lintas layanan kustom Anda sendiri membantu Anda fokus pada metrik yang paling relevan untuk beban kerja Anda. Sebaiknya Anda membuat dasbor lintas layanan tingkat akun yang mencakup metrik kunci dan menampilkan semua beban kerja di akun.

Jika Anda memiliki ruang kantor pusat atau area umum untuk tim operasi cloud, Anda dapat menampilkan CloudWatch dashboard pada monitor TV besar dalam mode layar penuh dengan refresh otomatis.

Membuat dasbor khusus aplikasi atau beban kerja

Sebaiknya Anda membuat dasbor khusus aplikasi dan beban kerja yang berfokus pada metrik dan sumber daya utama untuk setiap aplikasi penting atau beban kerja di lingkungan produksi Anda. Dasbor khusus aplikasi dan beban kerja berfokus pada metrik aplikasi atau beban kerja khusus Anda dan pentingAWSmetrik sumber daya yang mempengaruhi kinerja mereka.

Anda harus secara teratur mengevaluasi dan menyesuaikan CloudWatch dasbor aplikasi atau beban kerja untuk melacak metrik kunci setelah insiden terjadi. Anda juga harus memperbarui dasbor khusus aplikasi atau beban kerja saat fitur diperkenalkan atau pensiun. Pembaruan beban kerja dan dasbor khusus aplikasi harus menjadi aktivitas yang diperlukan untuk peningkatan kualitas secara berkelanjutan, selain pencatatan dan pemantauan.

Dasbor lintas akun atau lintas akun lintas Wilayah

AWSsumber daya terutama Regional dan metrik, alarm, dan dasbor khusus untuk Wilayah yang digunakan sumber daya. Hal ini dapat mengharuskan Anda mengubah Wilayah untuk melihat metrik, dasbor, dan alarm untuk beban kerja dan aplikasi lintas wilayah. Jika Anda memisahkan aplikasi dan beban kerja Anda ke beberapa akun, Anda mungkin juga diminta untuk mengautentikasi ulang dan masuk ke setiap akun. Namun, CloudWatch mendukung tampilan data lintas akun dan lintas wilayah dari satu akun, yang berarti Anda dapat melihat metrik, alarm, dasbor, dan widget log dalam satu akun dan Wilayah. Ini sangat berguna jika Anda memiliki akun logging dan monitoring terpusat.

Pemilik akun dan pemilik tim aplikasi harus membuat dasbor untuk aplikasi lintas wilayah khusus akun untuk memantau metrik kunci secara efektif di lokasi terpusat. Dasbor CloudWatch secara otomatis mendukung widget lintas wilayah, yang berarti Anda dapat membuat dasbor yang mencakup metrik dari beberapa Wilayah tanpa konfigurasi lebih lanjut.

Pengecualian penting adalah CloudWatch Log Wawasan widget karena data log hanya dapat ditampilkan untuk akun dan Wilayah yang saat ini Anda login ke. Anda dapat membuat metrik khusus wilayah dari log Anda dengan menggunakan filter metrik dan metrik ini dapat ditampilkan pada dasbor lintas wilayah. Anda kemudian dapat beralih ke Wilayah tertentu ketika Anda perlu menganalisis lebih lanjut log tersebut.

Tim operasi harus membuat dasbor terpusat yang memantau metrik lintas akun dan lintas Wilayah. Misalnya, Anda dapat membuat dasbor lintas akun yang mencakup pemanfaatan CPU agregat di setiap akun dan Wilayah. Anda juga dapat menggunakanmatematika metrikuntuk menggabungkan dan data dasbor di beberapa akun dan Wilayah.

Menggunakan metrik matematika untuk menyempurnakan pengamatan dan mengkhawatirkan

Anda dapat menggunakan metrik matematika untuk membantu menghitung metrik dalam format dan ekspresi yang relevan untuk beban kerja Anda. Metrik yang dihitung dapat disimpan dan dilihat di dasbor untuk tujuan pelacakan. Misalnya, metrik volume Amazon EBS standar menyediakan jumlah bacaan (`VolumeReadOps`) dan menulis (`VolumeWriteOps`) operasi dilakukan selama periode tertentu.

Namun,AWSmemberikan pedoman tentang kinerja volume Amazon EBS di IOPS. Anda dapat membuat grafik dan menghitung IOPS untuk volume Amazon EBS Anda dalam matematika metrik dengan menambahkan`VolumeReadOps`dan`VolumeWriteOps`dan kemudian membagi dengan periode yang dipilih untuk metrik ini.

Dalam contoh ini, kita meringkas IOPS dalam periode dan kemudian membagi dengan panjang periode untuk mendapatkan IOPS. Anda kemudian dapat mengatur alarm terhadap ekspresi matematika metrik ini untuk mengingatkan Anda ketika IOPS volume mendekati kapasitas maksimum untuk jenis volumenya. Untuk informasi selengkapnya dan contoh tentang penggunaan matematika metrik untuk memantau sistem file Amazon Elastic File System (Amazon EFS) CloudWatch metrik, lihatAmazon CloudWatch metrik matematika menyederhanakan pemantauan hampir real-time dari sistem file Amazon EFS Anda dan banyak lagipadaAWSBlog.

Menggunakan dasbor otomatis untuk Amazon ECS, Amazon EKS, dan Lambda dengan CloudWatchContainer Wawasan dan CloudWatch Wawasan Lambda

Wawasan Kontainer CloudWatch menciptakan dasbor otomatis dinamis untuk beban kerja kontainer yang berjalan di Amazon ECS dan Amazon EKS. Anda harus mengaktifkan Container Insights untuk memiliki observabilitas CPU, memori, disk, jaringan, dan informasi diagnostik seperti kegagalan restart kontainer. Wawasan Kontainer menghasilkan dasbor dinamis yang dapat Anda filter dengan cepat di klaster, instance container atau node, service, task, pod, dan level container individual. Wawasan Wadahdikonfigurasi pada tingkat cluster dan node atau kontainer instancetergantung padaAWSlayanan.

Mirip dengan Container Insights, CloudWatch Lambda Insights menciptakan dasbor otomatis dinamis untuk fungsi Lambda Anda. Solusi ini mengumpulkan, menggabungkan, dan merangkum metrik

tingkat sistem, termasuk waktu CPU, memori, cakram, dan jaringan. Aplikasi ini juga mengumpulkan, menggabungkan, dan merangkum informasi diagnostik seperti proses mulai yang dingin dan penonaktifan pekerja Lambda untuk membantu Anda mengisolasi dan segera menyelesaikan masalah dengan fungsi Lambda Anda. Lambda diaktifkan pada tingkat fungsi dan tidak memerlukan agen apa pun.

Wawasan Kontainer dan Lambda Insights juga membantu Anda dengan cepat beralih ke log aplikasi atau kinerja, pelacakan X-Ray, dan peta layanan untuk memvisualisasikan beban kerja kontainer Anda. Mereka berdua menggunakan CloudWatch format metrik tertanam untuk menangkap CloudWatch metrik dan log kinerja.

Anda dapat membuat bersama CloudWatch dasbor untuk beban kerja Anda yang menggunakan metrik yang ditangkap oleh Container Insights dan Lambda Insights. Anda bisa melakukan ini dengan memfilter dan melihat dasbor otomatis CloudWatch Wawasan Kontainer dan kemudian memilihTambahkan ke Dasborpilihan yang memungkinkan Anda untuk menambahkan metrik yang ditampilkan ke dasbor CloudWatch standar. Anda kemudian dapat menghapus atau menyesuaikan metrik dan menambahkan metrik lain untuk mewakili beban kerja Anda dengan benar.

Integrasi CloudWatch denganAWSjasa

AWSmenyediakan banyak layanan yang mencakup opsi konfigurasi tambahan untuk logging dan metrik. Layanan ini sering memungkinkan Anda untuk mengkonfigurasi CloudWatch Log untuk output log dan CloudWatch metrik untuk output metrik. Infrastruktur dasar yang digunakan untuk menyediakan layanan ini dikelola olehAWSdantidak dapat diakses, tetapi Anda dapat menggunakan opsi logging dan metrik untuk layanan yang disediakan untuk mendapatkan wawasan lebih lanjut dan memecahkan masalah. Misalnya, Anda dapat mempublikasikanLog alur VPC ke CloudWatch, atau Anda juga bisakonfigurasikan instans Amazon Relational Database Service (Amazon RDS) untuk mempublikasikan log ke CloudWatch.

KebanyakanAWSlog API panggilan denganintegrasi keAWS CloudTrail. CloudTrail pulamendukung integrasi dengan CloudWatch Beberapa catatandan ini berarti Anda dapat mencari dan menganalisis aktivitas diAWSlayanan. Anda juga dapat menggunakan Amazon CloudWatch Peristiwa atau Amazon EventBridge untuk membuat dan mengkonfigurasi otomatisasi dan pemberitahuan dengan CloudWatch Acara aturan acara untuk tindakan tertentu yang dilakukan diAWSlayanan. Layanan tertentuIntegrasi secara langsungbersama CloudWatch Kejadian dan EventBridge. Anda juga dapatmembuat acara yang disampaikan melalui CloudTrail.

Amazon Managed Grafana untuk dasbor dan visualisasi

Amazon Managed Grafanadapat digunakan untuk mengamati dan memvisualisasikanAWSbeban kerja. Amazon Managed Grafana membantu Anda memvisualisasikan dan menganalisis data operasional Anda dalam skala besar. Grafanaadalah platform analitik sumber terbuka yang membantu Anda melakukan kueri, memvisualisasikan, memperingatkan, dan memahami metrik Anda di mana pun mereka disimpan. Amazon Managed Grafana sangat berguna jika organisasi Anda sudah menggunakan Grafana untuk visualisasi beban kerja yang ada dan Anda ingin memperluas cakupanAWSbeban kerja. Anda dapat menggunakan Amazon Managed Grafana dengan CloudWatch olehmenambahkannya sebagai sumber data, yang berarti bahwa Anda dapat membuat visualisasi menggunakan CloudWatchmetrik. Dukungan Grafana Terkelola AmazonAWS Organizationsdan Anda dapat memusatkan dasbor menggunakan CloudWatch metrik dari beberapa akun dan Wilayah.

Tabel berikut memberikan keuntungan dan pertimbangan untuk menggunakan Amazon Managed Grafana alih-alih CloudWatch untuk dashboard. Pendekatan hibrida mungkin cocok berdasarkan kebutuhan pengguna akhir, beban kerja, dan aplikasi Anda yang berbeda.

Membuat visualisasi dan dasbor yang terintegrasi dengan sumber data yang didukung oleh Amazon Managed Grafana dan Grafana open-source	Amazon Managed Grafana membantu Anda membuat visualisasi dan dasbor dari berbagai sumber data, termasuk CloudWatch metrik. Amazon Managed Grafana menyertakan sejumlah sumber data bawaan yang menjangkauAWSlayanan, perangkat lunak sumber terbuka, dan perangkat lunak COTS. Untuk informasi selengkapnya tentang ini, lihatSumber data bawaandalam dokumentasi Amazon Managed Grafana. Anda juga dapat menambahkan dukungan untuk lebih banyak sumber data dengan meningkatkan ruang kerja AndaGrafana Enterprise. Grafana juga mendukungplugin sumber datayang memungkinkan Anda untuk berkomunikasi dengan sistem eksternal yang berbeda. CloudWatchdasbor membutuhkan CloudWatc

	h metrik atau CloudWatch Kueri Wawasan Log untuk data yang akan ditampilkan di CloudWatc h Dasbor.
Kelola akses ke solusi dasbor Anda secara terpisah dariAWSakses akun	Amazon Managed Grafana memerlukan penggunaanAWS IAM Identity Center(IAM Identity Center) danAWS Organizationsuntuk otentikasi dan otorisasi. Hal ini memungkin kan Anda untuk mengautentikasi pengguna ke Grafana dengan menggunakan federasi identitas yang mungkin sudah Anda gunakan dengan IAM Identity Center atauAWS Organizations. Namun, jika Anda tidak menggunakan IAM Identity Center atauAWS Organizations, kemudian diatur sebagai bagian dari proses penyiapan Amazon Managed Grafana. Ini mungkin menjadi masalah jika organisasi Anda telah membatasi penggunaan IAM Identity Center atauAWS Organizations.
Menelan dan mengakses data melintasi beberapa akun dan Wilayah denganAWS Organizationsintegrasi	Amazon Managed Grafana terintegrasi denganAWS Organizationsuntuk memungkin kan Anda membaca data dariAWSsumber seperti CloudWatch dan Amazon OpenSearc h Layanan di semua akun Anda. Hal ini memungkinkan untuk membuat dasbor yang menampilkan visualisasi menggunakan data di seluruh akun Anda. Untuk mengaktifkan akses data secara otomatisAWS Organizations, Anda perlu menyiapkan ruang kerja Amazon Managed Grafana Anda diAWS Organizat ionsakun manajemen. Hal ini tidak dianjurka n berdasarkanAWS Organizationspraktik terbaik untuk akun manajemen. Sebaliknya, CloudWatch pulamendukung dasbor lintas-ak un, lintas-Wilayah untuk CloudWatch metrik.

Gunakan widget visualisasi lanjutan dan definisi Grafana yang tersedia di komunitas open-sour ce	Grafana menyediakan banyak koleksi visualisa si yang dapat Anda gunakan saat membuat dasbor Anda. Ada juga perpustakaan besar dasbor yang dikontribusikan komunitas yang dapat Anda edit dan gunakan kembali sesuai dengan kebutuhan Anda.
Gunakan dasbor dengan penerapan Grafana baru dan yang sudah ada	Jika Anda sudah menggunakan Grafana, Anda dapat mengimpor dan mengekspor dasbor dari penerapan Grafana Anda dan menyesuaikannya untuk digunakan di Amazon Managed Grafana. Amazon Managed Grafana memungkinkan Anda untuk menstandarisasi Grafana sebagai solusi dashboard Anda.
Penyiapan dan konfigurasi lanjutan untuk ruang kerja, izin, dan sumber data	Amazon Managed Grafana memungkin kan Anda membuat beberapa ruang kerja Grafana yang memiliki kumpulan sumber data, pengguna, dan kebijakan yang dikonfigu rasi sendiri. Ini dapat membantu Anda memenuhi persyaratan kasus penggunaan yang lebih canggih, serta konfigurasi keamanan tingkat lanjut. Kemampuan canggih mungkin mengharuskan tim Anda untuk mengemban gkan pengalaman mereka dengan Grafana jika mereka belum memiliki keterampilan ini.

Merancang dan menerapkan penebangan dan pemantauan dengan CloudWatch FAQ

Bagian ini memberikan jawaban atas pertanyaan yang sering diajukan tentang merancang dan menerapkan solusi logging dan monitoring dengan CloudWatch.

Dimana saya menyimpan CloudWatch File konfigurasi?

Parameter CloudWatch agen untuk Amazon EC2 dapat menerapkan beberapa file konfigurasi yang disimpan dalam CloudWatch direktori konfigurasi. Idealnya, Anda harus menyimpan konfigurasi CloudWatch sebagai satu set file karena Anda dapat mengontrol versi dan menggunakannya lagi di beberapa akun dan lingkungan. Untuk informasi selengkapnya tentang ini, lihatMengelola CloudWatch konfigurasibagian dari panduan ini. Atau, Anda dapat menyimpan file konfigurasi Anda di repositori di GitHub dan mengotomatisasi pengambilan file konfigurasi ketika instans EC2 baru disediakan.

Bagaimana cara membuat tiket di solusi manajemen layanan saya saat alarm dinaikkan?

Anda mengintegrasikan sistem manajemen layanan dengan topik Amazon Simple Notification Service (Amazon SNS) dan mengonfigurasi CloudWatch alarm untuk memberitahukan topik SNS saat alarm dinaikkan. Sistem terintegrasi Anda menerima pesan SNS dan dapat membuat tiket menggunakan API atau SDK sistem manajemen layanan Anda.

Bagaimana cara menggunakan CloudWatch untuk menangkap file log di kontainer saya?

Tugas Amazon ECS dan Pod Amazon EKS dapat dikonfigurasi agar secara otomatis mengirim output STDOUT dan STDERR ke CloudWatch. Pendekatan yang direkomendasikan untuk penebangan aplikasi kontainer adalah memiliki kontainer mengirim output mereka ke STDOUT dan STDERR. Hal ini juga tercakup dalamTwelve-Factor Aplikasi Manifesto.

Namun, jika Anda ingin mengirim file log tertentu CloudWatch maka Anda dapat me-mount volume di pod Amazon EKS atau definisi tugas Amazon ECS ke tempat aplikasi Anda akan menulis banyak file

dan menggunakan wadah sidecar untuk Fluentd atau Fluent Bit untuk mengirim log ke CloudWatch. Anda harus mempertimbangkan simbolik menautkan file log tertentu di kontainer Anda`/dev/stdout`dan`/dev/stderr`. Untuk informasi selengkapnya tentang ini, lihatLihat log untuk kontainer atau layanandalam dokumentasi Docker.

Bagaimana cara memantau masalah kesehatanAWSlayanan?

Anda dapat menggunakanAWS Health Dashboarduntuk memantauAWSperistiwa kondisi. Anda juga dapat merujuk keaws-kesehatan-alat GitHub repositori untuk solusi otomatisasi sampel yang terkait denganAWSperistiwa kondisi.

Bagaimana saya dapat membuat kustom CloudWatch metrik ketika tidak ada dukungan agen?

Anda dapat menggunakan format metrik tersemat untuk menelan metrik ke CloudWatch. Anda juga dapat menggunakanAWSSDK (misalnya,put_metric_data),AWS CLI(misalnya,put-metric-data), atauAWSAPI (misalnya,PutMetricData) untuk membuat metrik kustom. Anda harus mempertimbangkan bagaimana logika kustom akan dipertahankan jangka panjang. Salah satu pendekatan adalah menggunakan Lambda dengan dukungan format metrik tertanam terintegrasi untuk membuat metrik Anda, bersama dengan CloudWatch Peristiwa peristiwaaturan jadwaluntuk menetapkan periode untuk metrik.

Bagaimana cara mengintegrasikan alat pencatatan dan pemantauan yang ada denganAWS?

Anda harus merujuk pada panduan yang disediakan oleh vendor perangkat lunak atau layanan untuk mengintegrasikanAWS. Anda mungkin dapat menggunakan perangkat lunak agen, SDK, atau API yang disediakan untuk mengirim log dan metrik ke solusinya. Anda mungkin juga dapat menggunakan solusi open-source, seperti Fluentd atau Fluent Bit, dikonfigurasi sesuai spesifikasi vendor. Anda juga dapat menggunakanAWSSDK dan CloudWatch Log filter berlangganan dengan Lambda dan Kinesis Data Streams untuk membuat prosesor log kustom dan pengirim. Akhirnya, Anda juga harus mempertimbangkan bagaimana Anda akan mengintegrasikan perangkat lunak jika Anda menggunakan beberapa akun dan Wilayah.

Sumber daya

Pengantar

- AWSWell-Architected

Hasil bisnis yang ditargetkan

- logging-monitoring-apg-guide-contoh
- Enam keuntungan komputasi awan

Merencanakan CloudWatch penyebaran Anda

- AWS OrganizationsTerminologi dan konsep
- AWS Systems ManagerPengaturan Cepat
- Mengumpulkan metrik dan log dari instans Amazon EC2 dan server lokal dengan CloudWatch agen
- cloudwatch-config-s3-ember.yaml
- Buat file konfigurasi CloudWatch agen dengan wizard
- Enterprise DevOps: Mengapa Anda harus menjalankan apa yang Anda bangun
- Mengekspor data log ke Amazon S3
- Kontrol akses detail di Amazon OpenSearch Service
- Kuota Lambda
- Membuat atau mengedit file konfigurasi CloudWatch agen secara manual
- Pemrosesan data log secara real-time dengan langganan
- Alat untuk membangunAWS

Mengonfigurasi CloudWatch agen untuk instans EC2 dan server lokal

- Dimensi metrik Amazon EC2

- Instans Performa yang Dapat Dilonjakkan
- CloudWatch agen set metrik yang telah ditetapkan
- Kumpulkan metrik proses dengan plugin procstat
- Mengkonfigurasi CloudWatch agen untuk procstat
- Aktifkan atau nonaktifkan pemantauan terperinci untuk instans Anda
- Menelan log kardinalitas tinggi dan menghasilkan metrik dengan format metrik CloudWatch tertanam
- Bekerja dengan grup log dan aliran log
- Buat daftar CloudWatch metrik yang tersedia untuk instans Anda
- PutLogEvents
- Ambil metrik kustom dengan collectd
- Mengambil metrik kustom dengan StatsD

CloudWatch pendekatan instalasi agen untuk Amazon EC2 dan server lokal

- Membuat peran layanan IAM untuk lingkungan hibrid
- Membuat aktivasi instans-terkelola untuk lingkungan hibrid
- Buat peran IAM dan pengguna untuk digunakan dengan CloudWatch agen
- Unduh dan konfigurasikan CloudWatch agen menggunakan baris perintah
- Bagaimana cara mengonfigurasi server lokal yang menggunakan agen Systems Manager dan CloudWatch agen terpadu untuk hanya menggunakan kredensyal sementara?
- Prasyarat untuk operasi set tumpukan
- Menggunakan instans spot

Pencatatan log dan pemantauan di Amazon ECS

- amazon-cloudwatch-logs-for-lancar-bit
- CloudWatch Metrik Amazon ECS
- Metrik Wawasan Kontainer Amazon ECS
- Agen kontainer Amazon ECS

- Jenis peluncuran ECS Amazon
- Menerapkan CloudWatch agen untuk mengumpulkan metrik tingkat instans EC2 di Amazon ECS
- ecs_cluster_with_cloudwatch_linux.yaml
- ecs_cw_emf_example
- ecs_firelense_emf_example
- ecs-task-nginx-firelense.json
- Mengambil metadata AMI yang dioptimalkan Amazon ECS
- Menggunakan driver log awslogs
- Menggunakan pustaka klien untuk menghasilkan log format metrik tersemat

Pencatatan log dan pemantauan di Amazon EKS

- Pencatatan bidang kendali Amazon EKS
- amazon_eks_managed_node_group_launch_config.yaml
- Simpul Amazon EKS
- amazon-eks-nodegroup.yaml
- Perjanjian Tingkat Layanan Amazon EKS
- Pemantauan metrik Prometheus Wawasan Kontainer
- Bidang kontrol metrik dengan Prometheus
- Men-deploy Dasbor Kubernetes (UI web)
- Fargate penebangan
- Bit Fasih untuk Amazon EKS di Fargate
- Cara menangkap log aplikasi saat menggunakan Amazon EKS di Fargate
- Menginstal CloudWatch agen untuk mengumpulkan metrik Prometheus
- Menginstal Server Metrik Kubernetes
- kubernetes/dasbor
- Penskala Otomatis Pod Horizontal Kubernetes
- Komponen Control Plane Kubernetes
- Polong Kubernetes
- Luncurkan dukungan templat

- Grup simpul terkelola
- Perilaku pembaruan simpul terkelola
- metrik-server
- Memantau Amazon EKS di Fargate menggunakan Prometheus dan Grafana
- prometheus_jmx
- prometheus/jmx_exporter
- Mengikis sumber Prometheus tambahan dan mengimpor metrik tersebut
- Simpul yang dikelola sendiri
- Kirim log ke CloudWatch Log
- Menyiapkan FluentD sebagai DaemonSet untuk mengirim log ke CloudWatch Logs
- Menyiapkan contoh beban kerja Java/JMX di Amazon EKS dan Kubernetes
- Tutorial untuk menambahkan target pengikisan Prometheus baru: metrik Server API Prometheus
- Vertical Pod Autoscaler

Pencatatan dan metrik untukAWS Lambda

- Kesalahan doa Lambda
- logging — Logging fasilitas untuk Python
- Menggunakan pustaka klien untuk menghasilkan log format metrik tersemat
- Bekerja dengan metrik fungsi Lambda

Mencari dan menganalisis log CloudWatch

- Keluarga Beats
- Logstash elastis
- Tumpukan Elastis
- Streaming CloudWatch Log data ke Amazon OpenSearch Service

Opsi yang mengkhawatirkan dengan CloudWatch

- amazon-cloudwatch-auto-alarms

- AWSKonektor Manajemen Layanan untuk Jira Service Management
- AWSKonektor Manajemen Layanan untuk ServiceNow

Memantau ketersediaan aplikasi dan layanan

- Mengonfigurasi failover DNS

Menelusuri aplikasi denganAWS X-Ray

- Jaringan tugas Amazon ECS
- Mengonfigurasi aturan pengambilan sampel di konsol X-Ray
- Jalankan PowerShell perintah atau skrip Windows
- Menjalankan daemon X-Ray di Amazon EC2
- Mengirim data jejak ke X-Ray
- Grafik layanan di X-Ray

Dasbor dan visualisasi dengan CloudWatch

- Amazon CloudWatch Metric Math menyederhanakan pemantauan hampir waktu nyata sistem file Amazon EFS Anda
- Menyiapkan CloudWatch Wawasan Kontainer
- Menggunakan matematika metrik

CloudWatch integrasi denganAWS layanan

- AWS CloudTrailLayanan yang didukung dan integrasi
- CloudWatch Acara contoh acara dari layanan yang didukung
- Acara disampaikan melalui CloudTrail
- Memantau file CloudTrail log dengan CloudWatch Log
- Menerbitkan log mesin basis data ke CloudWatch Logs
- Menerbitkan log aliran ke CloudWatch Log

Amazon Managed Grafana untuk dasbor dan visualisasi

- Praktik terbaik untuk akun manajemen diAWS Organizations
- Sumber data bawaan untuk Amazon Managed Grafana
- Dasbor lintas akun dan lintas Wilayah di CloudWatch
- Plugin Grafana

Riwayat dokumen

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

Perubahan	Deskripsi	Tanggal
Informasi logging yang diperbarui	Memperbarui bagian tentang penebangan untukAWS Lambda.	17 April
Informasi konfigurasi yang diperbarui	Memperbarui dan mengganti nama bagian tentang membuat dan menyimpan CloudWatch konfigurasi.	9 Februari
Informasi metrik yang diperbarui	Memperbarui informasi metrik aplikasi khusus di bagian Metrik untuk Amazon ECS.	31 Januari
Pemberitahuan pratinjau yang dihapus	Grafana yang dikelola umumnya tersedia.	25 Mei
Bagian yang dihapus	CloudWatch Metrik SDK tidak lagi didukung.	7 Januari
Publikasi awal	—	30 April 2021

AWS Glosarium Panduan Preskriptif

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

Nomor

7 Rs

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

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

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

A

ABAC

Lihat kontrol akses berbasis atribut.

layanan abstrak

Lihat layanan terkelola.

ASAM

Lihat atomisitas, konsistensi, isolasi, daya tahan.

migrasi aktif-aktif

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

migrasi aktif-pasif

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

fungsi agregat

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

AI

Lihat kecerdasan buatan.

AIOps

Lihat operasi kecerdasan buatan.

anonimisasi

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

anti-pola

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

kontrol aplikasi

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

portofolio aplikasi

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

kecerdasan buatan (AI)

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

operasi kecerdasan buatan (AIOps)

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

enkripsi asimetris

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

atomisitas, konsistensi, isolasi, daya tahan (ACID)

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

kontrol akses berbasis atribut (ABAC)

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

sumber data otoritatif

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

Zona Ketersediaan

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

AWS Kerangka Adopsi Cloud (AWS CAF)

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

AWS Kerangka Kualifikasi Beban Kerja (AWS WQF)

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

B

bot buruk

Bot yang dimaksudkan untuk mengganggu atau 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, panggilan API yang mencurigakan, dan tindakan serupa. Untuk informasi selengkapnya, lihat Data dalam grafik perilaku di dokumentasi Detektif.

sistem big-endian

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

klasifikasi biner

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

filter mekar

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

deployment biru/hijau

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

bot

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

botnet

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

cabang

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

akses break-glass

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

strategi brownfield

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

cache penyangga

Area memori tempat data yang paling sering diakses disimpan.

kemampuan bisnis

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

perencanaan kelangsungan bisnis (BCP)

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

C

KAFE

Lihat Kerangka Adopsi AWS Cloud.

penyebaran kenari

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

CCoE

Lihat Cloud Center of Excellence.

CDC

Lihat mengubah pengambilan data.

ubah pengambilan data (CDC)

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

rekayasa kekacauan

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 AWS layanan menerimanya.

Cloud Center of Excellence (CCoE)

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

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

cache dingin

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

data dingin

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

visi komputer (CV)

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

konfigurasi drift

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

database manajemen konfigurasi (CMDB)

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

paket kesesuaian

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

integrasi berkelanjutan dan pengiriman berkelanjutan (CI/CD)

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

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

CV

Lihat visi komputer.

D

data saat istirahat

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

klasifikasi data

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

penyimpangan data

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

data dalam transit

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

jala data

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

minimalisasi data

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

perimeter data

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

prapemrosesan data

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

asal data

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

subjek data

Individu yang datanya dikumpulkan dan diproses.

gudang data

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

bahasa definisi database (DDL)

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

bahasa manipulasi basis data (DHTML)

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

DDL

Lihat bahasa definisi database.

ansambel yang dalam

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

pembelajaran mendalam

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

defense-in-depth

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

administrator yang didelegasikan

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

deployment

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

lingkungan pengembangan

Lihat lingkungan.

kontrol detektif

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

pemetaan aliran nilai pengembangan (DVSM)

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

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

kembar digital

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

tabel dimensi

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

musibah

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

pemulihan bencana (DR)

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

DML~

Lihat bahasa manipulasi database.

desain berbasis domain

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

DR

Lihat pemulihan bencana.

deteksi drift

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

DVSM

Lihat pemetaan aliran nilai pengembangan.

E

EDA

Lihat analisis data eksplorasi.

komputasi tepi

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

enkripsi

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

kunci enkripsi

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

endianness

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

titik akhir

Lihat titik akhir layanan.

layanan endpoint

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

perencanaan sumber daya perusahaan (ERP)

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

enkripsi amplop

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

lingkungan

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

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

epik

Dalam metodologi tangkas, kategori fungsional yang membantu mengatur dan memprioritaskan pekerjaan Anda. Epik memberikan deskripsi tingkat tinggi tentang persyaratan dan tugas

implementasi. Misalnya, epos keamanan AWS CAF mencakup manajemen identitas dan akses, kontrol detektif, keamanan infrastruktur, perlindungan data, dan respons insiden. Untuk informasi selengkapnya tentang epos dalam strategi AWS migrasi, lihat panduan implementasi program.

ERP

Lihat perencanaan sumber daya perusahaan.

analisis data eksplorasi (EDA)

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

F

tabel fakta

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

gagal cepat

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

batas isolasi kesalahan

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

cabang fitur

Lihat cabang.

fitur

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

pentingnya fitur

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

transformasi fitur

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

FGAC

Lihat kontrol akses berbutir halus.

kontrol akses berbutir halus (FGAC)

Penggunaan beberapa kondisi untuk mengizinkan atau menolak permintaan akses.

migrasi flash-cut

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

G

pemblokiran geografis

Lihat pembatasan geografis.

pembatasan geografis (pemblokiran geografis)

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

Alur kerja Gitflow

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

strategi greenfield

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

pagar pembatas

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

H

HA

Lihat ketersediaan tinggi.

migrasi database heterogen

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

ketersediaan tinggi (HA)

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

modernisasi sejarawan

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

migrasi database homogen

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

data panas

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

perbaikan terbaru

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

periode hypercare

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

I

IAc

Lihat infrastruktur sebagai kode.

kebijakan berbasis identitas

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

aplikasi idle

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

IIoT

Lihat Internet of Things industri.

infrastruktur yang tidak dapat diubah

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

masuk (masuknya) VPC

Dalam arsitektur AWS multi-akun, VPC yang menerima, memeriksa, dan merutekan koneksi jaringan dari luar aplikasi. Arsitektur Referensi AWS Keamanan merekomendasikan pengaturan akun Jaringan Anda dengan VPC masuk, keluar, dan inspeksi 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, VPC terpusat yang mengelola inspeksi lalu lintas jaringan antara VPC (dalam hal yang sama atau berbeda Wilayah AWS), internet, dan jaringan lokal. Arsitektur Referensi AWS Keamanan merekomendasikan pengaturan akun Jaringan Anda dengan VPC masuk, keluar, dan inspeksi 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 selengkapnya, lihat Interpretabilitas model pembelajaran mesin dengan AWS.

IoT

Lihat Internet of Things.

Perpustakaan informasi TI (ITIL)

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

Manajemen layanan TI (ITSM)

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

ITIL

Lihat perpustakaan informasi TI.

ITSM

Lihat manajemen layanan TI.

L

kontrol akses berbasis label (LBAC)

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

landing zone

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

migrasi besar

Migrasi 300 atau lebih server.

LBAC

Lihat kontrol akses berbasis label.

hak istimewa paling sedikit

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

angkat dan geser

Lihat 7 Rs.

sistem endian kecil

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

lingkungan yang lebih rendah

Lihat lingkungan.

M

pembelajaran mesin (ML)

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

cabang utama

Lihat cabang.

malware

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

layanan terkelola

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

sistem eksekusi manufaktur (MES)

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

PETA

Lihat Program Percepatan Migrasi.

mekanisme

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

akun anggota

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

MES

Lihat sistem eksekusi manufaktur.

Transportasi Telemetri Antrian Pesan (MQTT)

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

layanan mikro

Layanan kecil dan independen yang berkomunikasi melalui API yang terdefinisi dengan baik 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 API ringan. Setiap layanan mikro dalam arsitektur ini dapat diperbarui, digunakan, dan diskalakan untuk memenuhi permintaan fungsi tertentu dari suatu aplikasi. Untuk informasi selengkapnya, lihat Menerapkan layanan mikro di AWS.

Program Percepatan Migrasi (MAP)

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

migrasi dalam skala

Proses memindahkan sebagian besar portofolio aplikasi ke cloud dalam gelombang, dengan lebih banyak aplikasi bergerak pada tingkat yang lebih cepat di setiap gelombang. Fase ini menggunakan praktik 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 AWS dengan Layanan Migrasi Aplikasi.

Penilaian Portofolio Migrasi (MPA)

Alat online yang menyediakan informasi untuk memvalidasi kasus bisnis untuk bermigrasi ke. AWS Cloud MPA menyediakan penilaian portofolio terperinci (ukuran kanan server, harga,

perbandingan TCO, analisis biaya migrasi) serta perencanaan migrasi (analisis data aplikasi dan pengumpulan data, pengelompokan aplikasi, prioritas migrasi, dan perencanaan gelombang). Alat MPA (memerlukan login) tersedia gratis untuk semua AWS konsultan dan konsultan APN Partner.

Penilaian Kesiapan Migrasi (MRA)

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

strategi migrasi

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

ML

Lihat pembelajaran mesin.

modernisasi

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

penilaian kesiapan modernisasi

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

aplikasi monolitik (monolit)

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

Anda dapat menggunakan arsitektur microservices. Untuk informasi lebih lanjut, lihat 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 kelompok TI fungsional untuk diberikan satu sama lain, untuk mendukung perjanjian tingkat layanan (SLA).

Tinjauan Kesiapan Operasional (ORR)

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

teknologi operasional (OT)

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

integrasi operasi (OI)

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

jejak organisasi

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

manajemen perubahan organisasi (OCM)

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

kontrol akses asal (OAC)

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

identitas akses asal (OAI)

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

ORR

Lihat tinjauan kesiapan operasional.

OT

Lihat teknologi operasional.

keluar (jalan keluar) VPC

Dalam arsitektur AWS multi-akun, VPC yang menangani koneksi jaringan yang dimulai dari dalam aplikasi. Arsitektur Referensi AWS Keamanan merekomendasikan pengaturan akun Jaringan

Anda dengan VPC masuk, keluar, dan inspeksi untuk melindungi antarmuka dua arah antara aplikasi Anda dan internet yang lebih luas.

P

batas izin

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

Informasi Identifikasi Pribadi (PII)

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

PII

Lihat informasi yang dapat diidentifikasi secara pribadi.

buku pedoman

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

PLC

Lihat pengontrol logika yang dapat diprogram.

PLM

Lihat manajemen siklus hidup produk.

kebijakan

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

persistensi poliglot

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

penilaian portofolio

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

predikat

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

predikat pushdown

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

kontrol preventif

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

principal

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

Privasi oleh Desain

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

zona host pribadi

Container yang menyimpan informasi tentang bagaimana Anda ingin Amazon Route 53 merespons kueri DNS untuk domain dan subdomainnya dalam satu atau beberapa VPC. Untuk

informasi selengkapnya, lihat Bekerja dengan zona yang dihosting pribadi di dokumentasi Route 53.

kontrol proaktif

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

manajemen siklus hidup produk (PLM)

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

lingkungan produksi

Lihat lingkungan.

pengontrol logika yang dapat diprogram (PLC)

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

pseudonimisasi

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

terbitkan/berlangganan (pub/sub)

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

Q

rencana kueri

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

regresi rencana kueri

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

R

Matriks RACI

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

ransomware

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

Matriks RASCI

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

RCAC

Lihat kontrol akses baris dan kolom.

replika baca

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

arsitek ulang

Lihat 7 Rs.

tujuan titik pemulihan (RPO)

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

tujuan waktu pemulihan (RTO)

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

refactor

Lihat 7 Rs.

Wilayah

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

regresi

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

rehost

Lihat 7 Rs.

melepaskan

Dalam proses penyebaran, tindakan mempromosikan perubahan pada lingkungan produksi.

memindahkan

Lihat 7 Rs.

memplatform ulang

Lihat 7 Rs.

pembelian kembali

Lihat 7 Rs.

ketahanan

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

kebijakan berbasis sumber daya

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

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

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

kontrol responsif

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

melestarikan

Lihat 7 Rs.

pensiun

Lihat 7 Rs.

rotasi

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

kontrol akses baris dan kolom (RCAC)

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

RPO

Lihat tujuan titik pemulihan.

RTO

Lihat tujuan waktu pemulihan.

buku runbook

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

D

SAML 2.0

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

PENIPUAN

Lihat kontrol pengawasan dan akuisisi data.

SCP

Lihat kebijakan kontrol layanan.

Rahasia

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

kontrol keamanan

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

pengerasan keamanan

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

sistem informasi keamanan dan manajemen acara (SIEM)

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

otomatisasi respons keamanan

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

enkripsi sisi server

Enkripsi data di tujuannya, oleh AWS layanan yang menerimanya.

kebijakan kontrol layanan (SCP)

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

titik akhir layanan

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

perjanjian tingkat layanan (SLA)

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

indikator tingkat layanan (SLI)

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

tujuan tingkat layanan (SLO)

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

model tanggung jawab bersama

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

SIEM

Lihat informasi keamanan dan sistem manajemen acara.

titik kegagalan tunggal (SPOF)

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

SLA

Lihat perjanjian tingkat layanan.

SLI

Lihat indikator tingkat layanan.

SLO

Lihat tujuan tingkat layanan.

split-and-seed model

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

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

SPOF

Lihat satu titik kegagalan.

skema bintang

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

pola ara pencekik

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

subnet

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

kontrol pengawasan dan akuisisi data (SCADA)

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

enkripsi simetris

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

pengujian sintetis

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

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 VPC dan jaringan lokal Anda. Untuk informasi selengkapnya, lihat Apa itu gateway transit dalam AWS Transit Gateway dokumentasi.

alur kerja berbasis batang

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

akses tepercaya

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

penyetelan

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

tim dua pizza

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

U

waswas

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

tugas yang tidak terdiferensiasi

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

lingkungan atas

Lihat lingkungan.

V

menyedot debu

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

kendali versi

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

Peering VPC

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

kerentanan

Kelemahan perangkat lunak atau perangkat keras yang membahayakan keamanan sistem.

W

cache hangat

Cache buffer yang berisi data 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

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

beban kerja

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

aliran kerja

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

CACING

Lihat menulis sekali, baca banyak.

WQF

Lihat Kerangka Kualifikasi Beban Kerja AWS.

tulis sekali, baca banyak (WORM)

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

Z

eksploitasi zero-day

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

kerentanan zero-day

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

aplikasi zombie

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

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