AWS Panduan keputusan

AWS CloudTrail atau Amazon CloudWatch?

AWS CloudTrail atau Amazon CloudWatch?: AWS Panduan keputusan

Table of Contents

AWS CloudTrail atau Amazon CloudWatch?

Pahami perbedaannya dan pilih yang tepat untuk Anda

Tujuan	Untuk membantu Anda menentukan AWS CloudTrail apakah Amazon CloudWatch adalah pilihan yang tepat untuk menjaga visibilitas, keamanan, dan efisiensi operasional lingkunga n cloud Anda.
Terakhir diperbarui	September 20, 2024
Layanan yang tercakup	• AWS CloudTrail • Amazon CloudWatch

Pengantar

Saat menerapkan beban kerja bisnis penting ke perusahaan AWS Cloud, penting untuk menjaga visibilitas, keamanan, dan efisiensi operasional di lingkungan cloud Anda. Ada sejumlah area utama yang harus ditangani:

- Transparansi operasional — Melacak siapa yang melakukan apa yang ada di lingkungan cloud Anda dan memantau kinerja sumber daya Anda.
- Jaminan keamanan — Mendeteksi panggilan API yang tidak biasa atau pemanfaatan sumber daya yang mungkin mengindikasikan ancaman keamanan.
- Kepatuhan terhadap peraturan — Mempertahankan catatan rinci aktivitas pengguna dan perubahan infrastruktur untuk tujuan audit.
- Manajemen kinerja - Memantau pemanfaatan sumber daya dan metrik kinerja aplikasi.
- Respons insiden — data dan peringatan untuk mengidentifikasi dan menanggapi masalah operasional dengan cepat.
- Pengendalian biaya — wawasan tentang penggunaan sumber daya untuk membantu mengelola pengeluaran cloud.
- Otomatisasi — respons otomatis terhadap peristiwa tertentu atau ambang kinerja.

AWS menawarkan dua layanan utama untuk membantu mengatasi masalah ini:

- AWS CloudTrailterutama difokuskan pada tata kelola, kepatuhan, dan audit operasional. Ini mencatat semua panggilan API yang dibuat dalam AWS lingkungan Anda. Fitur kunci:
  - Melacak semua Akun AWS aktivitas, termasuk panggilan API, tindakan yang diambil di Konsol Manajemen AWS, AWS SDKs, alat baris perintah, dan AWS layanan lainnya.
  - Menyediakan log terperinci dari setiap tindakan, termasuk siapa yang melakukan panggilan, layanan yang digunakan, dan sumber daya apa yang terpengaruh.
  - Berguna untuk audit keamanan, melacak aktivitas pengguna, dan mengidentifikasi tindakan yang berpotensi berbahaya.
- Amazon CloudWatch adalah layanan pemantauan dan observabilitas yang menyediakan data dan wawasan yang dapat ditindaklanjuti untuk aplikasi dan AWS infrastruktur lokal, serta hybrid. Fitur utama meliputi:
  - Memantau AWS sumber daya dan aplikasi yang berjalan AWS secara real-time, termasuk metrik, log, dan alarm.
  - Memberikan wawasan terperinci tentang kinerja sistem, tingkat kesalahan, pemanfaatan sumber daya, dan banyak lagi.
  - Memungkinkan pengaturan alarm untuk memicu tindakan (misalnya, penskalaan sumber daya) berdasarkan kondisi tertentu.

Meskipun kedua layanan sangat penting untuk lingkungan cloud yang kuat dan aman, keduanya berbeda dalam kasus penggunaannya, dan kemampuan yang mereka tawarkan.

Berikut adalah pandangan tingkat tinggi tentang perbedaan utama antara layanan ini untuk membantu Anda memulai.

Kategori	CloudTrail	CloudWatch
Tujuan utama	Pelacakan dan audit aktivitas API	Pemantauan waktu nyata dan manajemen kinerja
Data yang dikumpulkan	Log panggilan API, termasuk siapa yang melakukan panggilan, kapan, dan sumber daya apa yang terpengaruh	Metrik, log, dan peristiwa yang terkait dengan kinerja sumber daya dan perilaku aplikasi

Kategori	CloudTrail	CloudWatch
Kasus penggunaan	Audit keamanan, kepatuhan , dan pelacakan perubahan lingkungan	Memantau pemanfaatan sumber daya, pengaturan alarm, dan manajemen kinerja
Keamanan dan kepatuhan	Membantu memenuhi persyaratan keamanan dan kepatuhan dengan menyediak an log aktivitas terperinci	Memantau kinerja sistem untuk anomali keamanan dan membantu menjaga integritas operasional
Retensi log	90 hari terakhir dari sejarah peristiwa. Dapat membuat jejak dan penyimpanan data acara (menggunakan CloudTrail Danau) untuk menyimpan catatan aktivitas selama lebih dari 90 hari.	Retensi data jangka pendek untuk pemantauan dan pemecahan masalah waktu nyata
Alarm dan notifikasi	Tidak terutama digunakan untuk alarm, tetapi dapat memicu tindakan berdasarkan aktivitas API	Mengaktifkan pengaturan alarm untuk metrik tertentu atau peristiwa log, dengan respons otomatis
Integrasi	Sering digunakan dengan layanan keamanan seperti AWS Config dan IAM untuk meningkatkan manajemen keamanan	Terintegrasi dengan berbagai AWS layanan untuk pemantauan dan otomatisasi yang komprehensif
Pertimbangan Biaya	Biaya berdasarkan volume log yang dihasilkan dan disimpan	Biaya berdasarkan jumlah metrik, log, dan alarm yang dipantau
Granularitas data	Menyediakan log terperinc i dari setiap panggilan API dengan informasi terperinci	Menyediakan metrik agregat dan data log untuk pemantaua n waktu nyata

Kategori	CloudTrail	CloudWatch
Kontrol akses	Memungkinkan Anda melacak pola akses dan perubahan izin pengguna	Membantu Anda memantau dan mengoptimalkan akses ke sumber daya berdasarkan metrik kinerja
Cakupan sumber daya	Akun AWS-lebar	AWS Sumber daya individu
Pelacakan waktu nyata	Dekat waktu nyata (dalam 5 menit)	Real-time atau mendekati real-time
Visualisasi	Terbatas; sering digunakan dengan alat lain	Dasbor dan grafik bawaan

Perbedaan antara CloudTrail dan CloudWatch

Jelajahi perbedaan antara CloudTrail dan CloudWatch di sejumlah bidang utama.

Primary purpose

AWS CloudTrail

- Menyediakan jejak audit komprehensif dari semua aktivitas API dalam file Akun AWS. Berfokus pada merekam siapa yang melakukan apa, kapan, dan dari mana. Ini termasuk tindakan yang diambil melalui Konsol Manajemen AWS, AWS SDKs, alat baris perintah, dan AWS layanan lainnya. CloudTrail menjawab pertanyaan seperti “Siapa yang menghentikan EC2 contoh ini?” atau “Perubahan apa yang dilakukan pada kebijakan IAM ini?”

Amazon CloudWatch

- Memantau kesehatan operasional dan kinerja sumber AWS daya dan aplikasi. CloudWatch mengumpulkan dan melacak metrik, mengumpulkan dan memantau file log, dan menyetel alarm. Ini membantu Anda memahami kinerja aplikasi Anda dan merespons perubahan kinerja di seluruh sistem. CloudWatch menjawab pertanyaan seperti “Apakah pemanfaatan CPU EC2 instans Amazon saya terlalu tinggi?” atau “Berapa banyak kesalahan yang dihasilkan oleh fungsi Lambda saya?”

Ringkasan

CloudTrail membantu Anda melacak dan mengaudit aktivitas pengguna untuk keamanan dan kepatuhan, sementara CloudWatch itu tentang memantau dan mengoptimalkan kinerja sistem dan kesehatan operasional. Kedua alat melayani peran yang berbeda, namun saling melengkapi, dalam mengelola lingkungan cloud.

Data collected

AWS CloudTrail

- Berfokus pada pengambilan log terperinci dari semua aktivitas API di AWS lingkungan Anda. Ini termasuk informasi tentang siapa yang membuat panggilan API, kapan dibuat, tindakan yang diambil, dan sumber daya yang terlibat. CloudTrailLog menyediakan jejak audit yang komprehensif, penting untuk melacak perubahan, memastikan kepatuhan, dan menyelidiki insiden keamanan.

Amazon CloudWatch

- Mengumpulkan data kinerja dan operasional dari AWS sumber daya dan aplikasi Anda. Ini termasuk metrik seperti penggunaan CPU, pemanfaatan memori, lalu lintas jaringan, dan log aplikasi, serta metrik khusus yang dapat Anda tentukan. Data yang dikumpulkan CloudWatch digunakan untuk pemantauan waktu nyata, pengoptimalan kinerja, dan pengaturan alarm untuk memicu tindakan otomatis berdasarkan kondisi tertentu.

Ringkasan

CloudTrail mengumpulkan data yang terkait dengan aktivitas pengguna dan penggunaan API untuk tujuan audit dan keamanan, sambil CloudWatch mengumpulkan metrik dan log untuk memantau, mengelola, dan mengoptimalkan kinerja sistem dan kesehatan operasional. Keduanya memberikan wawasan kritis tetapi melayani berbagai aspek manajemen cloud.

Use cases

AWS CloudTrail

- Terutama digunakan untuk audit keamanan, kepatuhan, dan audit operasional. CloudTrailmenyediakan catatan terperinci tentang panggilan API dan aktivitas pengguna di AWS lingkungan Anda, sehingga penting untuk melacak perubahan, menyelidiki insiden keamanan, dan memastikan bahwa organisasi Anda memenuhi persyaratan peraturan.

Misalnya, CloudTrail berguna dalam skenario di mana Anda perlu memantau siapa yang mengakses sumber daya tertentu, melacak perubahan yang dibuat pada konfigurasi, atau mengaudit aktivitas di beberapa Akun AWS.

Amazon CloudWatch

- Dirancang untuk pemantauan real-time, manajemen kinerja, dan efisiensi operasional. CloudWatch digunakan untuk memantau kesehatan AWS sumber daya dan aplikasi Anda dengan mengumpulkan dan melacak metrik, log, dan peristiwa. CloudWatch memungkinkan Anda menyetel alarm yang memicu tindakan otomatis, seperti penskalaan sumber daya atau mengirim pemberitahuan saat ambang batas tertentu terpenuhi. Kasus penggunaan CloudWatch termasuk memantau kinerja aplikasi, mengelola pemanfaatan sumber daya, mendeteksi anomali, dan memastikan sistem Anda berjalan secara optimal untuk mencegah downtime.

Security and compliance

AWS CloudTrail

- Penting untuk menjaga keamanan dan kepatuhan di AWS lingkungan. CloudTrail menyediakan jejak audit komprehensif dari semua panggilan API, termasuk siapa yang melakukan panggilan, kapan dibuat, dan tindakan yang diambil. Pencatatan terperinci ini penting untuk memenuhi standar kepatuhan, melakukan audit keamanan, dan menyelidiki insiden. Dengan melacak aktivitas pengguna dan perubahan sumber daya, CloudTrail membantu memastikan akuntabilitas dan transparansi, yang merupakan persyaratan utama untuk banyak kerangka peraturan.

Amazon CloudWatch

- Berperan dalam keamanan dengan memungkinkan deteksi anomali operasional. Misalnya, Anda dapat menggunakan CloudWatch untuk memantau metrik yang menunjukkan potensi masalah keamanan, seperti lonjakan yang tidak biasa dalam lalu lintas jaringan atau penggunaan CPU. Selain itu, CloudWatch dapat memicu alarm dan respons otomatis ketika ambang batas tertentu terpenuhi, memungkinkan manajemen insiden proaktif. Log yang ditangkap juga CloudWatch dapat digunakan untuk melacak peristiwa operasional, yang sangat penting untuk memahami konteks insiden keamanan.

Ringkasan

Bersama-sama, CloudTrail menyediakan log audit yang diperlukan untuk kepatuhan, sambil CloudWatch menawarkan pemantauan waktu nyata yang membantu mendeteksi dan merespons ancaman keamanan, berkontribusi pada lingkungan cloud yang aman dan sesuai.

Log retention

AWS CloudTrail

- Secara default, riwayat CloudTrail acara mencatat 90 hari terakhir peristiwa manajemen untuk akun Anda.
- Pengguna dapat membuat jejak untuk menyimpan log tanpa batas dalam bucket S3.
- Tidak ada penghapusan otomatis log yang disimpan di Amazon S3, memungkinkan retensi jangka panjang.
- Pengguna dapat menerapkan kebijakan siklus hidup pada bucket S3 untuk mengelola biaya penyimpanan jangka panjang.
- CloudTrail dapat dikonfigurasi untuk mengirim log ke CloudWatch Log untuk opsi retensi yang lebih fleksibel.

Amazon CloudWatch

- Retensi CloudWatch log di Log lebih fleksibel dan dapat dikonfigurasi.
- Periode retensi default bervariasi menurut grup log, biasanya disetel ke “Tidak Pernah Kedaluwarsa”.
- Pengguna dapat mengatur periode retensi kustom mulai dari satu hari hingga 10 tahun, atau memilih retensi yang tidak terbatas.
- Grup log yang berbeda dapat memiliki periode retensi yang berbeda.
- Setelah periode retensi, log dihapus secara otomatis untuk mengelola biaya penyimpanan.
- CloudWatch Log dapat diekspor ke Amazon S3 untuk penyimpanan jangka panjang jika diperlukan.

Alarms and notifications

AWS CloudTrail

- Terutama berfokus pada aktivitas API logging dan tidak memiliki kemampuan alarm atau notifikasi bawaan. Namun, Anda dapat berintegrasi dengan CloudWatch Log dan CloudWatch alarm untuk mengonfigurasi alarm untuk CloudTrail acara. Pengaturan ini biasanya digunakan untuk mengingatkan Anda tentang peristiwa terkait keamanan, seperti upaya akses yang tidak sah atau perubahan pada sumber daya penting.

Amazon CloudWatch

- Dirancang khusus untuk pemantauan waktu nyata dan mencakup fitur alarm dan notifikasi yang kuat. CloudWatch memungkinkan Anda menyetel alarm berdasarkan metrik, data log, atau ambang batas yang ditentukan khusus. Ketika ambang batas ini dilanggar, CloudWatch dapat mengirim pemberitahuan melalui Amazon SNS (Amazon Simple Notification Service), memicu tindakan otomatis seperti penskalaan instance, atau melakukan langkah-langkah perbaikan khusus menggunakan. AWS Lambda Ini membuat alat CloudWatch penting untuk manajemen sistem proaktif, mengingatkan Anda tentang masalah kinerja atau anomali operasional saat terjadi.

Integration

CloudTrail dan CloudWatch menawarkan opsi integrasi yang luas dengan AWS layanan lain dan alat eksternal, meningkatkan fungsionalitas dan utilitas mereka.

CloudTrail integrasi

- Amazon S3: Simpan log jangka panjang untuk arsip dan analisis
- CloudWatch Log: Aktifkan analisis log waktu nyata dan peringatan
- Amazon EventBridge: Memicu tindakan otomatis berdasarkan peristiwa API
- AWS Config: Berikan masukan untuk pelacakan konfigurasi dan kepatuhan
- AWS Security Hub CSPM: Berkontribusi pada manajemen postur keamanan terpusat
- AWS Lake Formation: Aktifkan tata kelola data lake dari log CloudTrail
- Amazon Athena: Lakukan kueri SQL pada CloudTrail log yang disimpan di Amazon S3

CloudWatch integrasi

- Amazon SNS: Kirim pemberitahuan untuk alarm dan acara
- AWS Lambda: Memicu fungsi tanpa server berdasarkan metrik atau log

- EC2 Auto Scaling Amazon: Sesuaikan kapasitas berdasarkan metrik kinerja
- AWS Systems Manager: Mengotomatiskan tugas operasional berdasarkan data CloudWatch
- AWS X-Ray: Gabungkan dengan data jejak untuk wawasan aplikasi yang mendalam
- Layanan kontainer (Amazon ECS, Amazon EKS): Pantau aplikasi kontainer
- Alat pihak ketiga: Ekspor metrik dan log ke platform pemantauan eksternal

Cost considerations

AWS CloudTrail

- CloudTrail dihargai terutama pada jumlah peristiwa yang dicatat dan disimpan. Secara default, riwayat CloudTrail acara mencatat dan menyimpan, tanpa biaya, 90 hari terakhir acara manajemen untuk akun Anda. Namun, jika Anda mengaktifkan peristiwa data (seperti tindakan tingkat objek S3) atau membuat beberapa jejak, Anda dikenakan biaya berdasarkan volume peristiwa dan penyimpanan yang diperlukan di Amazon S3. Biaya tambahan mungkin timbul jika Anda menggunakan fitur-fitur canggih seperti CloudTrail Insights, yang memberikan analisis lebih dalam tentang aktivitas API yang tidak biasa.

Amazon CloudWatch

- CloudWatch memiliki struktur penetapan harga yang lebih kompleks berdasarkan beberapa faktor, termasuk jumlah metrik khusus yang Anda pantau, jumlah peristiwa log yang dicerna dan disimpan, serta penggunaan alarm dan dasbor. Pemantauan dasar untuk AWS layanan tidak dikenakan biaya, tetapi pemantauan terperinci dan metrik khusus dikenakan biaya. Penyimpanan log diberi harga berdasarkan volume data yang dicerna dan disimpan, dengan biaya tambahan untuk menyiapkan dan memelihara alarm atau menggunakan Wawasan Log untuk analisis CloudWatch log lanjutan.

Data granularity

AWS CloudTrail

- CloudTrail memberikan perincian tinggi dengan mencatat setiap panggilan API individu yang dibuat di lingkungan Anda AWS . Setiap entri log mencakup informasi terperinci seperti siapa yang membuat permintaan, tindakan yang dilakukan, sumber daya yang terpengaruh, dan waktu tindakan. Tingkat detail ini sangat penting untuk audit, pemantauan keamanan, dan

kepatuhan, karena memungkinkan Anda melacak tindakan dan perubahan pengguna tertentu hingga panggilan API yang tepat.

Amazon CloudWatch

- CloudWatch berfokus pada data agregat untuk pemantauan dan manajemen kinerja. Ini mengumpulkan metrik secara berkala (biasanya setiap menit atau lima menit) dan mencatat data operasional dari AWS sumber daya. Meskipun CloudWatch memberikan wawasan terperinci tentang kinerja sistem dan perilaku aplikasi, datanya lebih teragregasi dibandingkan dengan. CloudTrail Misalnya, Anda dapat memantau penggunaan CPU rata-rata dari waktu ke waktu daripada permintaan atau tindakan individual. CloudWatch Log, bagaimanapun, dapat memberikan lebih banyak data terperinci yang mirip dengan CloudTrail tetapi sering digunakan untuk menganalisis log operasional daripada melacak panggilan API.

Real-time tracking

AWS CloudTrail

- CloudTrail tidak secara inheren dirancang untuk pelacakan waktu nyata tetapi dapat dikonfigurasi untuk memberikan near-real-time peringatan. Secara default, CloudTrail merekam aktivitas API, tetapi ada sedikit penundaan dalam pengiriman log. Untuk pelacakan lebih cepat, Anda dapat berintegrasi CloudTrail dengan Amazon CloudWatch Events atau AWS Lambda memicu tindakan berdasarkan panggilan atau aktivitas API tertentu segera setelah dicatat. Pengaturan ini memungkinkan near-real-time pemantauan peristiwa keamanan penting atau perubahan konfigurasi.

Amazon CloudWatch

- CloudWatch, di sisi lain, dibangun untuk pelacakan real-time kinerja sistem dan aplikasi. Ini terus memantau metrik dari AWS sumber daya dan dapat langsung memicu alarm atau pemberitahuan ketika ambang batas yang telah ditentukan terlampaui. CloudWatch juga mengumpulkan dan menganalisis data log secara real-time, memungkinkan Anda untuk memantau log aplikasi, mendeteksi anomali, dan menanggapi masalah operasional saat terjadi. Ini membuat alat CloudWatch penting untuk menjaga kesehatan dan kinerja AWS lingkungan Anda secara real time.

Gunakan

Sekarang setelah Anda membaca tentang kriteria untuk memilih antara AWS CloudTrail dan Amazon CloudWatch, Anda dapat memilih layanan yang memenuhi kebutuhan Anda, dan menggunakan informasi berikut untuk membantu Anda mulai menggunakan masing-masing.

AWS CloudTrail

- Memulai dengan AWS CloudTrail

  AWS CloudTrail adalah AWS layanan yang membantu Anda mengaktifkan audit operasional dan risiko, tata kelola, dan kepatuhan Anda. Akun AWS Inilah cara memulainya.

  Jelajahi panduan

- Meninjau Akun AWS aktivitas

  Pelajari cara meninjau aktivitas AWS API terbaru di fitur CloudTrail riwayat peristiwa Akun AWS penggunaan Anda.

  Gunakan tutorialnya

- Buat jejak

  Pelajari cara membuat jejak untuk mencatat aktivitas AWS API di semua Wilayah termasuk data dan peristiwa Wawasan.

  Gunakan tutorialnya

- Praktik terbaik keamanan di AWS CloudTrail

  Panduan ini memberikan praktik terbaik keamanan detektif dan preventif untuk digunakan AWS CloudTrail di organisasi Anda.

  Jelajahi panduan

Amazon CloudWatch

- Memulai dengan Amazon CloudWatch

  Pantau AWS sumber daya Anda dan aplikasi yang Anda jalankan AWS secara real time menggunakan Amazon CloudWatch. Anda dapat menggunakan CloudWatch untuk

mengumpulkan dan melacak metrik, yang merupakan variabel yang dapat Anda ukur untuk sumber daya dan aplikasi Anda.

Jelajahi panduan

- Memulai dengan Amazon CloudWatch Metrics

  Panduan ini membahas pemantauan dasar dan pemantauan terperinci, cara membuat grafik metrik, dan cara menggunakan deteksi CloudWatch anomali.

  Jelajahi panduan

- Siapkan Wawasan Kontainer di Amazon EKS dan Kubernetes

  Siapkan add-on Amazon CloudWatch Observability ESK dan ADTO di klaster EKS Anda untuk mengirim metrik. CloudWatch Anda juga akan belajar cara mengatur Fluent Bit atau Fluentd untuk mengirim log ke Log. CloudWatch

  Jelajahi panduan

- Memulai dengan Amazon CloudWatch Application Insights

  Pelajari cara menggunakan konsol untuk mengaktifkan CloudWatch Application Insights mengelola aplikasi Anda untuk pemantauan.

  Jelajahi panduan

- Menggunakan Container Insights

  Pelajari cara CloudWatch Container Insights mengumpulkan, menggabungkan, dan merangkum metrik dan log dari aplikasi container dan layanan mikro Anda.

  Jelajahi panduan

- Menyiapkan Wawasan Kontainer di Amazon ECS

  Pelajari cara mengonfigurasi metrik tingkat kluster dan layanan, menerapkan ADOT untuk mengumpulkan metrik tingkat EC2 instans, dan menyiapkan FireLens untuk mengirim log ke Log. CloudWatch

  Jelajahi panduan

Riwayat dokumen untuk AWS CloudTrail atau Amazon CloudWatch?

Tabel berikut menjelaskan perubahan penting pada panduan keputusan ini. Untuk pemberitahuan tentang pembaruan panduan ini, Anda dapat berlangganan umpan RSS.

Perubahan	Deskripsi	Tanggal
Rilis awal	Rilis awal panduan keputusan.	September 20, 2024

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