aws

Panduan Pengguna

Menandai AWS Sumber Daya dan Editor Tag

Versi 1.0

Menandai AWS Sumber Daya dan Editor Tag: Panduan Pengguna

Table of Contents

Apa itu Tag Editor? 1
Metode penandaan 2
Pelajari selengkapnya 3
Praktik dan strategi terbaik 3
Praktik terbaik 3
Tag penamaan praktik terbaik 4
Strategi penandaan umum 6
Kategori penandaan 8
Memulai 10
Prasyarat 11
Mendaftar untuk Akun AWS 11
Buat pengguna dengan akses administratif 11
Buat sumber daya 13
Menyiapkan izin 13
Izin untuk layanan individual 13
Izin yang diperlukan untuk menggunakan konsol Editor Tag 14
Memberikan izin untuk menggunakan Editor Tag 16
Otorisasi dan kontrol akses berdasarkan tag 18
Menemukan sumber daya untuk diberi tag 19
Melihat dan mengedit tag yang ada untuk sumber daya yang dipilih 21
Ekspor hasil ke file.csv 22
Mengelola tag 23
Tambahkan tag ke sumber daya yang dipilih 24
Edit tag sumber daya yang dipilih 25
Hapus tag dari sumber daya yang dipilih 26
Menggunakan tag dalam IAM kebijakan 28
Tag dan kontrol akses berbasis atribut 28
Kunci kondisi terkait tag 28
Contoh IAM kebijakan yang menggunakan tag 29
AWS Organizations kebijakan tag 32
Prasyarat dan izin 32
Prasyarat untuk mengevaluasi kepatuhan terhadap kebijakan tag 32
Izin untuk mengevaluasi kepatuhan untuk akun 33
Izin untuk mengevaluasi kepatuhan seluruh organisasi 34

Kebijakan bucket Amazon S3 untuk penyimpanan laporan 36
Mengevaluasi kepatuhan untuk akun 37
Mengevaluasi kepatuhan seluruh organisasi 39
Memantau perubahan tag 43
Perubahan tag menghasilkan EventBridge acara 43
Lambda dan tanpa server 45
Tutorial pemantauan 45
Langkah 1. Buat fungsi Lambda 47
Langkah 2. Siapkan IAM izin yang diperlukan 50
Langkah 3. Lakukan tes pendahuluan fungsi Lambda Anda 52
Langkah 4. Buat EventBridge aturan yang meluncurkan fungsi 54
Langkah 5. Uji solusi lengkapnya 55
Ringkasan tutorial 57
Pemecahan masalah perubahan tag 59
Coba lagi perubahan tag yang gagal 60
Keamanan 61
Perlindungan data 61
Enkripsi data 63
Privasi lalu lintas antar jaringan 63
Pengelolaan identitas dan akses 63
Audiens 64
Mengautentikasi dengan identitas 64
Mengelola akses menggunakan kebijakan 68
Bagaimana Tag Editor bekerja dengan IAM 70
Contoh kebijakan berbasis identitas 74
Memecahkan masalah 78
Pencatatan dan pemantauan 80
CloudTrail Integrasi 80
Validasi kepatuhan 83
Ketangguhan 84
Keamanan infrastruktur 85
Kuota layanan Editor Tag 86
Riwayat dokumen 88
..... xcii

Apa itu Tag Editor?

Tag Editor memungkinkan Anda mengelola tag secara efektif. Tag adalah pasangan kunci dan nilai yang bertindak sebagai metadata untuk mengatur sumber daya Anda AWS . Dengan sebagian besar AWS sumber daya, Anda memiliki opsi untuk menambahkan tag saat Anda membuat sumber daya. Contoh sumber daya termasuk instans Amazon Elastic Compute Cloud (AmazonEC2), bucket Amazon Simple Storage Service (Amazon S3), atau bucket rahasia. AWS Secrets Manager

> **Important**
>
> Jangan menyimpan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Kami menggunakan tag untuk memberi Anda layanan penagihan dan administrasi. Tag tidak dimaksudkan untuk digunakan dalam data sensitif atau privat.

Tag membantu Anda mengelola, mengidentifikasi, mengatur, dan memfilter sumber daya. Anda dapat membuat tag untuk mengategorikan sumber daya berdasarkan tujuan, pemilik, lingkungan, atau kriteria lainnya.

Setiap tag memiliki dua bagian:

- Sebuah kunci tag (misalnya, `CostCenter`, `Environment`, atau `Project`). Kunci tag peka huruf besar dan kecil.
- Nilai tag (misalnya, `111122223333` atau`Production`). Seperti kunci tag, nilai tag peka huruf besar dan kecil.

> **Note**
>
> Meskipun kunci tag sensitif huruf besar/kecil, IAM memiliki validasi tambahan untuk IAM sumber daya untuk mencegah penerapan kunci tag yang hanya berbeda dalam casing. Kami merekomendasikan untuk tidak menggunakan kunci yang hanya berbeda dalam casing. Sebagai gantinya, Anda dapat menggunakan Kebijakan Kontrol Layanan (SCPs), yang memberikan kontrol pusat atas izin maksimum yang tersedia untuk IAM pengguna dan IAM peran di organisasi Anda.

Metode penandaan sumber daya

Ada tiga cara untuk menambahkan tag ke AWS sumber daya Anda:

- Layanan AWS APIoperasi — API Operasi penandaan didukung secara langsung. Layanan AWS Untuk mengetahui fungsionalitas penandaan yang Layanan AWS disediakan masing-masing, lihat dokumentasi layanan di indeks AWS dokumentasi.
- Konsol Editor Tag - Beberapa layanan mendukung penandaan dengan konsol Editor Tag.
- Resource Groups Tagging API — Sebagian besar layanan juga mendukung penandaan menggunakan. AWS Resource Groups Tagging API

> **Note**
>
> Anda juga dapat menggunakan AWS Service Catalog TagOptions Library untuk mengelola tag pada produk yang disediakan dengan mudah. A TagOptionadalah pasangan nilai kunci yang dikelola di Service Catalog. Ini bukan AWS tag, tetapi berfungsi sebagai template untuk membuat AWS tag berdasarkan TagOption.

Anda dapat menandai sumber daya untuk semua layanan yang menghasilkan biaya di. AWS Untuk layanan berikut, AWS rekomendasikan alternatif yang lebih baru Layanan AWS yang mendukung penandaan untuk memenuhi kasus penggunaan pelanggan dengan lebih baik.

Direktori Cloud Amazon	Amazon CloudSearch	Amazon Cognito Sync
AWS Data Pipeline	Amazon Elastic Transcoder	Amazon Machine Learning
AWS OpsWorks Stacks	Amazon S3 Glacier Langsung	Amazon SimpleDB
Manajer WorkSpaces Aplikasi Amazon	AWS DeepLens	

Pelajari selengkapnya

Halaman ini memberikan informasi umum tentang AWS sumber daya penandaan. Untuk informasi selengkapnya tentang menandai sumber daya dalam AWS layanan tertentu, lihat dokumentasinya. Berikut ini juga merupakan sumber informasi yang baik tentang penandaan:

- Untuk selengkapnya AWS Resource Groups Tagging API, lihat Panduan API Referensi Penandaan Resource Groups.
- Untuk informasi tentang fungsionalitas penandaan yang Layanan AWS disediakan masing-masing, lihat dokumentasi layanan dalam indeks AWS dokumentasi.
- Untuk informasi tentang penggunaan tag dalam IAM kebijakan untuk membantu mengontrol siapa yang dapat melihat dan berinteraksi dengan AWS sumber daya Anda, lihat Mengontrol akses ke dan untuk IAM pengguna serta peran yang menggunakan tag di Panduan IAM Pengguna.

Praktik dan strategi terbaik

Bagian ini memberikan informasi tentang praktik dan strategi terbaik saat menandai AWS sumber daya Anda dan menggunakan Editor Tag.

Menandai praktik terbaik

Saat Anda membuat strategi penandaan untuk AWS sumber daya, ikuti praktik terbaik:

- Jangan menambahkan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Tag dapat diakses oleh banyak AWS layanan, termasuk penagihan. Tag tidak dimaksudkan untuk digunakan dalam data sensitif atau privat.
- Gunakan format tag terstandardisasi yang peka huruf besar dan kecil serta terapkan secara konsisten di semua jenis sumber daya.
- Pertimbangkan pedoman tag yang mendukung berbagai tujuan, seperti mengelola kontrol akses sumber daya, pelacakan biaya, otomatisasi, dan organisasi.
- Gunakan alat otomatis untuk membantu mengelola tag sumber daya. Tag Editor dan Resource Groups Tagging API memungkinkan kontrol terprogram tag, membuatnya lebih mudah untuk mengelola, mencari, dan memfilter tag dan sumber daya secara otomatis.
- Gunakan terlalu banyak tag daripada terlalu sedikit tag.
- Ingatlah bahwa mudah mengubah tag untuk mengakomodasi perubahan persyaratan bisnis, tetapi pertimbangkan konsekuensi dari perubahan di masa mendatang. Misalnya, mengubah tag kontrol

akses berarti Anda juga harus memperbarui kebijakan yang mereferensikan tag tersebut dan mengontrol akses ke sumber daya Anda.

- Anda dapat secara otomatis menerapkan standar penandaan yang dipilih organisasi Anda untuk diadopsi dengan membuat dan menerapkan kebijakan tag menggunakan. AWS Organizations Kebijakan tag memungkinkan Anda menentukan aturan penandaan yang menentukan nama kunci yang valid dan nilai yang valid untuk setiap kunci. Anda dapat memilih untuk hanya memantau, memberi Anda kesempatan untuk mengevaluasi dan membersihkan tag yang ada. Setelah tag Anda sesuai dengan standar yang Anda pilih, Anda kemudian dapat mengaktifkan penegakan dalam kebijakan tag untuk mencegah tag yang tidak sesuai dibuat. Untuk informasi selengkapnya, lihat Kebijakan tag di Panduan AWS Organizations Pengguna.

Tag penamaan praktik terbaik

Ini adalah beberapa praktik terbaik dan konvensi penamaan yang kami sarankan agar Anda gunakan dengan tag Anda.

Nama kunci untuk AWS tag peka huruf besar/kecil jadi pastikan bahwa mereka digunakan secara konsisten. Misalnya, kunci tag `CostCenter` dan `costcenter` berbeda. Satu kunci tag mungkin dikonfigurasi sebagai tag alokasi biaya untuk analisis dan pelaporan keuangan, dan kunci tag lainnya mungkin tidak dikonfigurasi untuk penggunaan yang sama.

Sejumlah tag telah ditentukan sebelumnya oleh AWS atau dibuat secara otomatis oleh berbagai Layanan AWS tag. Banyak tag yang AWS dihasilkan menggunakan nama kunci yang semuanya huruf kecil, dengan tanda hubung yang memisahkan kata dalam nama, dan awalan diikuti oleh titik dua untuk mengidentifikasi layanan sumber untuk tag tersebut. Misalnya, lihat yang berikut ini:

- `aws:ec2spot:fleet-request-id`adalah tag yang mengidentifikasi Permintaan Instans EC2 Spot Amazon yang meluncurkan instance.
- `aws:cloudformation:stack-name`adalah tag yang mengidentifikasi AWS CloudFormation tumpukan yang menciptakan sumber daya.
- `elasticbeanstalk:environment-name`adalah tag yang mengidentifikasi aplikasi yang menciptakan sumber daya.

Pertimbangkan untuk memberi nama tag Anda menggunakan aturan berikut:

- Gunakan semua huruf kecil untuk kata-kata.
- Gunakan tanda hubung untuk memisahkan kata-kata.

- Gunakan awalan diikuti dengan titik dua untuk mengidentifikasi nama organisasi atau nama yang disingkat.

Misalnya, untuk perusahaan fiktif bernama AnyCompany, Anda dapat menentukan tag seperti:

- `anycompany:cost-center`untuk mengidentifikasi kode Pusat Biaya internal.
- `anycompany:environment-type`untuk mengidentifikasi apakah lingkungan adalah pengembangan, pengujian, atau produksi.
- `anycompany:application-id`untuk mengidentifikasi aplikasi tempat sumber daya dibuat.

Awalan memastikan bahwa tag dapat dikenali dengan jelas sebagaimana didefinisikan oleh organisasi Anda dan bukan oleh AWS atau alat pihak ketiga yang mungkin Anda gunakan. Menggunakan semua huruf kecil dengan tanda hubung untuk pemisah menghindari kebingungan tentang cara menggunakan huruf besar pada nama tag. Misalnya, `anycompany:project-id` lebih mudah diingat daripada`ANYCOMPANY:ProjectID`,`anycompany:projectID`, atau`Anycompany:ProjectId`.

Batas dan persyaratan penamaan tag

Persyaratan penggunaan dan penamaan dasar berikut berlaku untuk tag:

- Setiap sumber daya dapat memiliki maksimum 50 tag yang dibuat pengguna.
- Tag yang dibuat sistem yang dimulai dengan `aws:` dicadangkan untuk penggunaan AWS dan tidak diperhitungkan dalam batas ini. Anda tidak dapat mengedit atau menghapus tag yang dimulai dengan prefiks `aws:`.
- Untuk setiap sumber daya, setiap kunci tag harus unik, dan setiap kunci tag hanya dapat memiliki satu nilai.
- Kunci tag harus minimal 1 dan maksimal 128 karakter Unicode di UTF -8.
- Nilai tag harus minimal 0 dan maksimal 256 karakter Unicode di UTF -8.
- Karakter yang diizinkan dapat bervariasi menurut AWS layanan. Untuk informasi tentang karakter apa yang dapat Anda gunakan untuk menandai sumber daya di AWS layanan tertentu, lihat dokumentasinya. Secara umum, karakter yang diizinkan adalah huruf, angka, spasi yang dapat direpresentasikan dalam UTF -8, dan karakter berikut: _.:/= + - @.
- Kunci dan nilai tanda peka huruf besar-kecil. Sebagai praktik terbaik, putuskan strategi untuk memanfaatkan tag dan terapkan strategi tersebut secara konsisten di semua jenis sumber daya.

Misalnya, putuskan apakah akan menggunakan `Costcenter`, `costcenter`, atau `CostCenter` dan menggunakan kesepakatan yang sama untuk semua tag. Hindari penggunaan tag yang serupa dengan perlakuan kasus yang tidak konsisten.

Strategi penandaan umum

Gunakan strategi penandaan berikut untuk membantu mengidentifikasi dan mengelola AWS sumber daya.

Daftar Isi

- Tag untuk organisasi sumber daya
- Tag untuk alokasi biaya
- Tag untuk otomatisasi
- Tag untuk kontrol akses
- Tata kelola penandaan

Tag untuk organisasi sumber daya

Tag adalah cara yang baik untuk mengatur AWS sumber daya di AWS Management Console. Anda dapat mengonfigurasi tag yang akan ditampilkan dengan sumber daya dan dapat mencari serta memfilter berdasarkan tag. Dengan AWS Resource Groups layanan ini, Anda dapat membuat grup AWS sumber daya berdasarkan satu atau beberapa tag atau bagian tag. Anda juga dapat membuat grup berdasarkan kemunculannya dalam AWS CloudFormation tumpukan. Dengan menggunakan Resource Groups dan Tag Editor, Anda dapat menggabungkan dan melihat data untuk aplikasi yang terdiri dari beberapa layanan, sumber daya, dan Wilayah di satu tempat.

Tag untuk alokasi biaya

AWS Cost Explorer dan laporan penagihan terperinci memungkinkan Anda memecah AWS biaya berdasarkan tag. Biasanya, Anda menggunakan tag bisnis seperti pusat biaya/unit bisnis, pelanggan, atau proyek untuk mengaitkan AWS biaya dengan dimensi alokasi biaya tradisional. Tetapi, laporan alokasi biaya dapat menyertakan tag apa pun. Hal ini memungkinkan Anda mengaitkan biaya dengan dimensi teknis atau keamanan, seperti aplikasi, lingkungan, atau program kepatuhan tertentu.

Untuk beberapa layanan, Anda dapat menggunakan `createdBy` tag AWS yang dihasilkan untuk tujuan alokasi biaya, untuk membantu memperhitungkan sumber daya yang mungkin

tidak dikategorikan. Tag `createdBy` hanya tersedia untuk sumber daya dan layanan AWS yang didukung. Nilainya berisi data yang terkait dengan peristiwa tertentu API atau konsol. Untuk informasi selengkapnya, lihat Tag Alokasi Biaya yang Dihasilkan AWS dalam Panduan Pengguna AWS Billing and Cost Management .

Tag untuk otomatisasi

Tag sumber daya atau khusus layanan sering digunakan untuk memfilter sumber daya selama aktivitas otomatisasi. Tag otomatisasi digunakan untuk ikut serta atau keluar dari tugas otomatis atau untuk mengidentifikasi versi sumber daya tertentu untuk diarsipkan, diperbarui, atau dihapus. Misalnya, Anda dapat menjalankan skrip `start` atau `stop` otomatis yang menonaktifkan lingkungan pengembangan selama jam nonbisnis untuk mengurangi biaya. Dalam skenario ini, tag instans Amazon Elastic Compute Cloud (AmazonEC2) adalah cara sederhana untuk mengidentifikasi instance untuk memilih keluar dari tindakan ini. Untuk skrip yang menemukan dan menghapus EBS snapshot Amazon yang basi out-of-date, atau bergulir, tag snapshot dapat menambahkan dimensi tambahan kriteria penelusuran.

Tag untuk kontrol akses

IAMkebijakan mendukung kondisi berbasis tag, memungkinkan Anda membatasi IAM izin berdasarkan tag atau nilai tag tertentu. Misalnya, izin IAM pengguna atau peran dapat menyertakan kondisi untuk membatasi EC2 API panggilan ke lingkungan tertentu (seperti pengembangan, pengujian, atau produksi) berdasarkan tag mereka. Strategi yang sama dapat digunakan untuk membatasi API panggilan ke jaringan Amazon Virtual Private Cloud (AmazonVPC) tertentu. Support untuk izin tingkat sumber daya berbasis tag adalah layanan khususIAM. Saat Anda menggunakan syarat berbasis tag untuk kontrol akses, pastikan untuk menentukan dan membatasi siapa yang dapat mengubah tag. Untuk informasi selengkapnya tentang penggunaan tag untuk mengontrol API akses ke AWS sumber daya, lihat AWS layanan yang berfungsi IAM di Panduan IAM Pengguna.

Tata kelola penandaan

Strategi penandaan yang efektif menggunakan tag standar dan menerapkannya secara konsisten dan terprogram di seluruh sumber daya. AWS Anda dapat menggunakan pendekatan reaktif dan proaktif untuk mengatur tag di lingkungan Anda. AWS

- Tata kelola reaktif adalah untuk menemukan sumber daya yang tidak ditandai dengan benar menggunakan alat seperti Resource Groups TaggingAPI, Aturan AWS Config, dan skrip kustom. Untuk menemukan sumber daya secara manual, Anda dapat menggunakan Tag Editor dan laporan penagihan mendetail.

- Tata kelola proaktif menggunakan alat seperti AWS CloudFormation, Service Catalog, kebijakan tag di AWS Organizations, atau izin IAM tingkat sumber daya untuk memastikan tag standar diterapkan secara konsisten pada pembuatan sumber daya.

  Misalnya, Anda dapat menggunakan AWS CloudFormation `Resource Tags` properti untuk menerapkan tag ke jenis sumber daya. Di Service Catalog, Anda dapat menambahkan portofolio dan tag produk yang digabungkan dan diterapkan ke produk secara otomatis saat diluncurkan. Bentuk tata kelola proaktif yang lebih ketat mencakup tugas otomatis. Misalnya, Anda dapat menggunakan Penandaan Resource Groups API untuk mencari tag AWS lingkungan, atau menjalankan skrip untuk mengkarantina atau menghapus sumber daya yang ditandai dengan tidak benar.

Kategori penandaan

Perusahaan yang paling efektif dalam penggunaan tag biasanya membuat grup tag yang relevan dengan bisnis untuk mengatur sumber daya mereka di sepanjang dimensi teknis, bisnis, dan keamanan. Perusahaan yang menggunakan proses otomatis untuk mengelola infrastruktur mereka juga menyertakan tag khusus otomatisasi tambahan.

Tag teknis	Tag untuk otomatisasi	Tag bisnis	Tag keamanan
• Nama – Mengidentifikasi sumber daya individu • ID Aplikasi – Mengidentifikasi sumber daya yang terkait dengan aplikasi tertentu • Peran Aplikasi – Menjelaskan fungsi dari sumber daya tertentu (seperti server web, broker pesan, basis data)	• Tanggal/Waktu – Mengidentifikasi tanggal atau waktu sumber daya harus diluncurkan, dihentikan, dihapus, atau diputar • Ikut serta/keluar – Menunjukkan apakah sumber daya harus disertakan dalam aktivitas otomatis seperti meluncurkan, menghentikan,	• Proyek – Mengidentifikasi proyek yang didukung sumber daya • Pemilik – Mengidentifikasi siapa yang bertanggung jawab atas sumber daya • Pusat Biaya/Unit Bisnis – Mengidentifikasi pusat biaya atau unit bisnis yang terkait dengan sumber daya, biasanya	• Kerahasiaan – Pengidentifikasi untuk tingkat kerahasiaan data tertentu yang didukung sumber daya • Kepatuhan – Pengidentifikasi untuk beban kerja yang harus mematuhi persyaratan kepatuhan tertentu

Tag teknis	Tag untuk otomatisasi	Tag bisnis	Tag keamanan
• Klaster – Mengidentifikasi kumpulan sumber daya yang berbagi konfigurasi umum dan menjalankan fungsi tertentu untuk aplikasi • Lingkungan – Membedakan antara pengembangan, pengujian, dan sumber daya produksi • Versin – Membantu membedakan antara versi sumber daya atau aplikasi	atau mengubah ukuran instans • Keamanan - Menentukan persyaratan, seperti enkripsi atau mengaktifkan log VPC aliran Amazon; mengidentifikasi tabel rute atau grup keamanan yang memerlukan pengawasan ekstra	untuk alokasi dan pelacakan biaya • Pelanggan – Mengidentifikasi klien tertentu yang dilayani oleh grup sumber daya tertentu	

Memulai dengan Tag Editor

> **Important**
>
> Jangan menyimpan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Kami menggunakan tag untuk memberi Anda layanan penagihan dan administrasi. Tag tidak dimaksudkan untuk digunakan dalam data sensitif atau privat.

Untuk menambahkan tag ke—atau mengedit atau menghapus tag—beberapa sumber daya sekaligus, gunakan Editor Tag. Degan Tag Editor, Anda dapat mencari sumber daya yang ingin Anda beri tag, lalu mengelola tag untuk sumber daya tersebut dalam hasil pencarian Anda.

Untuk memulai Editor Tag

1. Masuk ke AWS Management Console.
2. Lakukan salah satu dari langkah-langkah berikut:
   - Pilih Layanan. Kemudian, di bawah Manajemen & Tata Kelola, pilih Resource Groups & Tag Editor. Di panel navigasi di sebelah kiri, pilih Editor Tag.
   - Gunakan tautan langsung: AWS Konsol Editor Tag.

Tidak semua sumber daya dapat menerapkan tag. Untuk informasi tentang sumber daya yang didukung Editor Tag, lihat kolom tag Editor Tag di Jenis sumber daya yang didukung di AWS Resource Groups Panduan Pengguna. Jika jenis sumber daya yang ingin Anda tag tidak didukung, biarkan AWS tahu dengan memilih Umpan balik di sudut kiri bawah jendela konsol.

Untuk informasi tentang izin dan peran yang diperlukan untuk menandai sumber daya, lihatMenyiapkan izin.

Topik

- Prasyarat untuk bekerja dengan Editor Tag
- Menyiapkan izin

Prasyarat untuk bekerja dengan Editor Tag

Sebelum Anda mulai bekerja untuk menandai sumber daya Anda, pastikan Anda telah aktif Akun AWS dengan sumber daya yang ada dan hak yang sesuai untuk menandai sumber daya dan membuat grup.

Topik

- Mendaftar untuk Akun AWS
- Buat pengguna dengan akses administratif
- Buat sumber daya

Mendaftar untuk Akun AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar untuk Akun AWS

1. Buka https://portal.aws.amazon.com/billing/pendaftaran.
2. Ikuti petunjuk online.

   Bagian dari prosedur pendaftaran melibatkan tindakan menerima panggilan telepon dan memasukkan kode verifikasi di keypad telepon.

   Ketika Anda mendaftar untuk Akun AWS, sebuah Pengguna root akun AWSdiciptakan. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya di akun. Sebagai praktik keamanan terbaik, tetapkan akses administratif ke pengguna, dan gunakan hanya pengguna root untuk melakukan tugas yang memerlukan akses pengguna root.

AWS mengirimi Anda email konfirmasi setelah proses pendaftaran selesai. Kapan saja, Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan masuk https://aws.amazon.comke/ dan memilih Akun Saya.

Buat pengguna dengan akses administratif

Setelah Anda mendaftar untuk Akun AWS, amankan Anda Pengguna root akun AWS, aktifkan AWS IAM Identity Center, dan buat pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Amankan Anda Pengguna root akun AWS

1. Masuk ke AWS Management Consolesebagai pemilik akun dengan memilih pengguna Root dan memasukkan Akun AWS alamat email. Di laman berikutnya, masukkan kata sandi.

   Untuk bantuan masuk menggunakan pengguna root, lihat Masuk sebagai pengguna root di AWS Sign-In Panduan Pengguna.
2. Aktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

   Untuk petunjuknya, lihat Mengaktifkan MFA perangkat virtual untuk Akun AWS root user (konsol) di Panduan IAM Pengguna.

Buat pengguna dengan akses administratif

1. Aktifkan Pusat IAM Identitas.

   Untuk petunjuk, lihat Mengaktifkan AWS IAM Identity Centerdi AWS IAM Identity Center Panduan Pengguna.
2. Di Pusat IAM Identitas, berikan akses administratif ke pengguna.

   Untuk tutorial tentang menggunakan Direktori Pusat Identitas IAM sebagai sumber identitas Anda, lihat Mengkonfigurasi akses pengguna dengan default Direktori Pusat Identitas IAMdi AWS IAM Identity Center Panduan Pengguna.

Masuk sebagai pengguna dengan akses administratif

- Untuk masuk dengan pengguna Pusat IAM Identitas, gunakan login URL yang dikirim ke alamat email saat Anda membuat pengguna Pusat IAM Identitas.

  Untuk bantuan masuk menggunakan pengguna Pusat IAM Identitas, lihat Masuk ke AWS akses portal di AWS Sign-In Panduan Pengguna.

Tetapkan akses ke pengguna tambahan

1. Di Pusat IAM Identitas, buat set izin yang mengikuti praktik terbaik menerapkan izin hak istimewa paling sedikit.

   Untuk petunjuknya, lihat Membuat set izin di AWS IAM Identity Center Panduan Pengguna.

2. Tetapkan pengguna ke grup, lalu tetapkan akses masuk tunggal ke grup.

   Untuk petunjuk, lihat Menambahkan grup di AWS IAM Identity Center Panduan Pengguna.

Buat sumber daya

Anda harus memiliki sumber daya di Akun AWS untuk tag. Untuk informasi selengkapnya tentang jenis sumber daya yang didukung, lihat kolom Tag Editor Tagging di bawah Jenis sumber daya yang didukung di AWS Resource Groups Panduan Pengguna.

Menyiapkan izin

Untuk memanfaatkan sepenuhnya Editor Tag, Anda mungkin memerlukan izin tambahan untuk menandai sumber daya atau untuk melihat kunci dan nilai tag sumber daya. Izin ini ada dalam kategori berikut:

- Izin untuk layanan individual sehingga Anda dapat menandai sumber daya dari layanan tersebut dan memasukkannya ke dalam grup sumber daya.
- Izin yang diperlukan untuk menggunakan konsol Editor Tag.

Jika Anda seorang administrator, Anda dapat memberikan izin untuk pengguna Anda dengan membuat kebijakan melalui AWS Identity and Access Management (IAM) layanan. Pertama-tama Anda membuat IAM peran, pengguna, atau grup, lalu menerapkan kebijakan dengan izin yang mereka butuhkan. Untuk informasi tentang membuat dan melampirkan IAM kebijakan, lihat Bekerja dengan kebijakan.

Izin untuk layanan individual

> **Important**
>
> Bagian ini menjelaskan izin yang diperlukan jika Anda ingin menandai sumber daya dari yang lain AWS konsol layanan dan APIs.

Untuk menambahkan tag ke sumber daya, Anda memerlukan izin yang diperlukan untuk layanan yang menjadi sumber daya tersebut. Misalnya, untuk menandai EC2 instans Amazon, Anda

harus memiliki izin untuk operasi penandaan di layanan tersebutAPI, seperti Amazon EC2 CreateTagsoperasi.

Izin yang diperlukan untuk menggunakan konsol Editor Tag

Untuk menggunakan konsol Editor Tag untuk mencantumkan dan menandai sumber daya, izin berikut harus ditambahkan ke pernyataan kebijakan pengguna diIAM. Anda juga dapat menambahkan AWS kebijakan terkelola yang dipertahankan dan tetap up to date AWS, atau Anda dapat membuat dan memelihara kebijakan kustom Anda sendiri.

Penggunaan AWS kebijakan terkelola untuk izin Editor Tag

Tag Editor mendukung hal berikut AWS kebijakan terkelola yang dapat Anda gunakan untuk memberikan seperangkat izin yang telah ditentukan sebelumnya kepada pengguna Anda. Anda dapat melampirkan kebijakan terkelola ini ke peran, pengguna, atau grup apa pun seperti kebijakan lain yang Anda buat.

ResourceGroupsandTagEditorReadOnlyAccess

Kebijakan ini memberikan IAM peran terlampir atau izin pengguna untuk memanggil operasi hanya-baca untuk keduanya AWS Resource Groups dan tag editor. Untuk membaca tag sumber daya, Anda juga harus memiliki izin untuk sumber daya tersebut melalui kebijakan terpisah. Pelajari lebih lanjut di berikut Catatan penting.

ResourceGroupsandTagEditorFullAccess

Kebijakan ini memberikan IAM peran terlampir atau izin pengguna untuk memanggil operasi Resource Groups dan operasi tag baca dan tulis di Editor Tag. Untuk membaca atau menulis tag sumber daya, Anda juga harus memiliki izin untuk sumber daya tersebut melalui kebijakan terpisah. Pelajari lebih lanjut di berikut Catatan penting.

Important

Dua kebijakan sebelumnya memberikan izin untuk memanggil operasi Editor Tag dan menggunakan konsol Editor Tag. Namun, Anda juga harus memiliki izin tidak hanya untuk menjalankan operasi, tetapi juga izin yang sesuai untuk sumber daya tertentu yang tagnya Anda coba akses. Untuk memberikan akses ke tag tersebut, Anda juga harus melampirkan salah satu kebijakan berikut:

- Bagian AWS kebijakan terkelola ReadOnlyAccessmemberikan izin untuk operasi hanya-baca untuk setiap sumber daya layanan. AWS secara otomatis menjaga kebijakan ini tetap up to date dengan yang baru Layanan AWS saat mereka tersedia.
- Banyak layanan menyediakan read-only khusus layanan AWS kebijakan terkelola yang dapat Anda gunakan untuk membatasi akses hanya ke sumber daya yang disediakan oleh layanan tersebut. Misalnya, Amazon EC2 menyediakan AmazonEC2ReadOnlyAccess.
- Anda dapat membuat kebijakan sendiri yang hanya memberikan akses ke operasi hanya-baca khusus untuk beberapa layanan dan sumber daya yang ingin diakses pengguna. Kebijakan ini menggunakan strategi allowlist atau strategi denylist.

  Strategi allowlist memanfaatkan fakta bahwa akses ditolak secara default sampai Anda secara eksplisit mengizinkannya dalam kebijakan. Jadi, Anda dapat menggunakan kebijakan seperti contoh berikut.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [ "tag:*" ],
            "Resource": "<ARNs of resources to allow tagging>"
        }
    ]
}
```

  Atau, Anda dapat menggunakan strategi denylist yang memungkinkan akses ke semua sumber daya kecuali yang Anda blokir secara eksplisit. Ini memerlukan kebijakan terpisah yang berlaku untuk pengguna yang relevan yang memungkinkan akses. Kebijakan contoh berikut kemudian menolak akses ke sumber daya tertentu yang terdaftar oleh Amazon Resource Name (ARN).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
             "Action": [ "tag:*" ],
            "Resource": "<ARNs of resources to disallow tagging>"
        }
```

```
    ]
}
```

Menambahkan izin Editor Tag secara manual

- `tag:*`(Izin ini memungkinkan semua tindakan Editor Tag. Jika Anda ingin membatasi tindakan yang tersedia bagi pengguna, Anda dapat mengganti tanda bintang dengan tindakan tertentu, atau dengan daftar tindakan yang dipisahkan koma.)
- `tag:GetResources`
- `tag:TagResources`
- `tag:UntagResources`
- `tag:getTagKeys`
- `tag:getTagValues`
- `resource-explorer:*`
- `resource-groups:SearchResources`
- `resource-groups:ListResourceTypes`

> **Note**
>
> `resource-groups:SearchResources`Izin ini memungkinkan Editor Tag untuk mencantumkan sumber daya saat Anda memfilter pencarian menggunakan kunci tag atau nilai.
> `resource-explorer:ListResources`Izin ini memungkinkan Editor Tag untuk mencantumkan sumber daya saat Anda mencari sumber daya tanpa menentukan tag penelusuran.

Memberikan izin untuk menggunakan Editor Tag

Untuk menambahkan kebijakan untuk menggunakan AWS Resource Groups dan Tag Editor untuk peran, lakukan hal berikut.

1. Buka IAMkonsol ke halaman Peran.

2. Temukan peran yang ingin Anda berikan izin Editor Tag. Pilih nama peran untuk membuka halaman Ringkasan peran.
3. Di Izin pilih, pilih Tambahkan izin.
4. Pilih Lampirkan kebijakan yang ada secara langsung.
5. Pilih Buat kebijakan.
6. Pada JSONtab, tempel pernyataan kebijakan berikut.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "tag:GetResources",
        "tag:TagResources",
        "tag:UntagResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "resource-explorer:*",
        "resource-groups:SearchResources",
        "resource-groups:ListResourceTypes"
      ],
      "Resource": "*"
    }
  ]
}
```

> **Note**
>
> Contoh pernyataan kebijakan ini memberikan izin untuk hanya melakukan tindakan Editor Tag.

7. Pilih Berikutnya: Tanda dan kemudian pilih Berikutnya: Tinjau.
8. Masukkan nama dan deskripsi untuk kebijakan baru. Misalnya, **`AWSTaggingAccess`**.
9. Pilih Buat kebijakan.

Setelah kebijakan disimpanIAM, Anda dapat melampirkannya ke prinsipal lain, seperti peran, grup, atau pengguna. Untuk informasi selengkapnya tentang cara menambahkan kebijakan ke prinsipal, lihat Menambahkan dan menghapus izin IAM identitas di Panduan IAM Pengguna.

Otorisasi dan kontrol akses berdasarkan tag

Layanan AWS mendukung yang berikut ini:

- Kebijakan berbasis tindakan — Misalnya, Anda dapat membuat kebijakan yang memungkinkan pengguna untuk melakukan `GetTagKeys` atau `GetTagValues` beroperasi, tetapi tidak ada yang lain.
- Izin tingkat sumber daya dalam kebijakan — Banyak layanan mendukung penggunaan ARNsuntuk menentukan sumber daya individual dalam kebijakan.
- Otorisasi berdasarkan tag — Banyak layanan mendukung penggunaan tag sumber daya dalam kondisi kebijakan. Misalnya, Anda dapat membuat kebijakan yang memungkinkan pengguna mengakses penuh ke grup yang memiliki tag yang sama dengan pengguna. Untuk informasi selengkapnya, lihat ABAC Untuk apa AWS? di AWS Identity and Access Management Panduan Pengguna.
- Kredensial sementara — Pengguna dapat mengambil peran dengan kebijakan yang memungkinkan operasi Editor Tag.

Editor Tag tidak menggunakan peran terkait layanan apa pun.

Untuk informasi lebih lanjut tentang bagaimana Tag Editor terintegrasi dengan AWS Identity and Access Management (IAM), lihat topik-topik berikut di AWS Identity and Access Management Panduan Pengguna:

- AWS layanan yang bekerja dengan IAM
- Tindakan, sumber daya, dan kunci kondisi untuk Editor Tag
- Mengontrol akses ke AWS sumber daya menggunakan kebijakan

Menemukan sumber daya untuk diberi tag

Dengan Editor Tag, Anda membuat kueri untuk menemukan sumber daya dalam satu atau lebih Wilayah AWS yang tersedia untuk penandaan. Anda dapat memilih hingga 20 jenis sumber daya individual, atau membuat kueri di Semua jenis sumber daya. Kueri Anda dapat menyertakan sumber daya yang sudah memiliki tag, atau sumber daya yang tidak memiliki tag. Untuk informasi selengkapnya, lihat kolom Tag Editor Tagging di Jenis sumber daya yang didukung di Panduan AWS Resource Groups Pengguna.

Setelah menemukan sumber daya untuk diberi tag, Anda dapat menggunakan Editor Tag untuk menambahkan tag, atau melihat, mengedit, atau menghapus tag.

Untuk menemukan sumber daya untuk diberi tag

1. Buka konsol Editor Tag.
2. (Opsional) Pilih Wilayah AWS tempat untuk mencari sumber daya yang akan diberi tag. Secara default, Wilayah Anda saat ini digunakan. Untuk prosedur ini, pilih us-east-1 dan us-west-2.
3. Pilih setidaknya satu jenis sumber daya dari daftar dropdown Jenis sumber daya. Anda dapat menambahkan atau mengedit tag hingga 20 jenis sumber daya individu sekaligus, atau memilih Semua jenis sumber daya. Untuk prosedur ini, pilih AWS::: :Instance danEC2: :S3 AWS: :Bucket.
4. (Opsional) Di bidang Tag, masukkan kunci tag, atau kunci tag dan pasangan nilai, untuk membatasi sumber daya saat ini Wilayah AWS hanya yang ditandai dengan nilai yang Anda tentukan. Saat Anda memasukkan kunci tag, kunci tag yang cocok di Wilayah saat ini muncul dalam daftar. Anda dapat memilih kunci tag dari daftar. Editor Tag secara otomatis melengkapi kunci tag untuk Anda saat Anda mengetik karakter yang cukup untuk mencocokkan kunci yang ada. Pilih Tambah atau tekan Enter setelah Anda selesai tag. Dalam contoh ini, filter untuk sumber daya yang memiliki kunci tag Stage. Nilai tag adalah opsional tetapi mempersempit hasil kueri lebih lanjut. Untuk menambahkan lebih banyak tag, pilih Tambah. Kueri menetapkan `AND` operator ke tag, jadi hanya sumber daya yang cocok dengan jenis sumber daya yang ditentukan dan semua tag tertentu yang dikembalikan oleh kueri.

> **Note**
>
> Konsol Editor Tag saat ini tidak mendukung wildcard.

Untuk menemukan sumber daya dengan beberapa nilai untuk kunci tag, tambahkan tag lain dengan kunci yang sama ke kueri, tetapi tentukan nilai yang berbeda. Hasilnya mencakup semua sumber daya yang ditandai dengan kunci tag yang sama dan yang memiliki salah satu nilai yang dipilih. Pencarian ini peka huruf besar/kecil.

Biarkan kotak Tag kosong untuk menemukan semua sumber daya dari jenis yang ditentukan dalam yang dipilih Wilayah AWS. Kueri ini mengembalikan sumber daya yang memiliki tag apa pun, dan menyertakan yang tidak memiliki tag. Untuk menghapus tag dari kueri Anda, pilih X pada label tag.

Untuk menemukan sumber daya yang memiliki tag, tetapi dengan nilai kosong, pilih (nilai kosong).

> **Note**
>
> Sebelum Anda dapat menemukan sumber daya dengan tag yang ditentukan, mereka harus telah diterapkan ke setidaknya satu sumber daya dari jenis yang ditentukan saat ini Wilayah AWS.

5. Saat kueri sudah siap, pilih Sumber daya pencarian. Hasil ditampilkan sebagai tabel di area hasil pencarian Sumber Daya.

   Untuk memfilter sejumlah besar sumber daya, masukkan teks filter apa pun, seperti bagian dari nama sumber daya, di Filter sumber daya.

   > **Note**
   >
   > Anda dapat menggunakan substring untuk memfilter hasil Anda.

6. (Opsional) Untuk mengonfigurasi kolom yang ditampilkan Editor Tag di hasil pencarian sumber daya Anda, pilih ikon roda gigi Preferensi di hasil pencarian sumber daya.

   Pada halaman Preferensi, pilih jumlah baris yang ingin ditampilkan di hasil penelusuran. Jika Anda ingin melihat semua teks dalam tabel, pilih kotak centang Garis Bungkus.

   Aktifkan kolom yang ingin ditampilkan Editor Tag di hasil Anda. Anda dapat menampilkan kolom untuk setiap tag yang muncul di hasil penelusuran atau subset hasil pencarian yang dipilih. Anda

dapat melakukan ini kapan saja setelah Anda menemukan sumber daya untuk ditandai. Untuk mengaktifkan kolom, pilih ikon sakelar di sebelah tag dan ubah dari mati ke aktif.

Setelah selesai mengonfigurasi kolom yang terlihat dan jumlah baris yang ditampilkan, pilih Konfirmasi.

Melihat dan mengedit tag yang ada untuk sumber daya yang dipilih

Editor Tag menunjukkan tag yang ada pada sumber daya yang dipilih yang ada di hasil pencarian sumber daya Temukan untuk menandai kueri.

Jika Anda mengaktifkan kolom Tag apa pun seperti yang dijelaskan di bagian sebelumnya, Anda dapat melihat nilai tag saat ini untuk setiap sumber daya di hasil penelusuran.

> **Note**
>
> Topik ini menjelaskan cara mengedit tag untuk sumber daya individual. Anda juga dapat mengedit tag massal untuk beberapa sumber daya yang dipilih secara bersamaan. Untuk informasi selengkapnya, lihat Mengelola tag dengan Editor Tag.

Untuk mengedit tag inline di tabel hasil pencarian

1. Pilih nilai untuk tag pada sumber daya yang ingin Anda edit.

   > **Note**
   >
   > - Jika sumber daya yang dipilih saat ini tidak memiliki tag dengan kunci yang dipilih, nilai akan ditampilkan sebagai (tidak ditandai).
   > - Jika sumber daya yang dipilih memang memiliki tag dengan kunci yang dipilih tetapi tanpa nilai, nilai akan ditampilkan sebagai '—'.

2. Anda dapat memasukkan nilai baru atau memilih dari salah satu nilai yang sudah ada pada sumber daya lain dengan tag ini. Anda juga dapat menghapus tag dari sumber daya yang satu ini dengan memilih Hapus tag.

Untuk melihat semua tag untuk sumber daya individu

1. Dalam hasil kueri Temukan sumber daya untuk menandai, pilih nomor di kolom Tag untuk sumber daya apa pun yang ingin Anda lihat tag yang ada. Sumber daya dengan tanda hubung di kolom Tag tidak memiliki tag yang ada.
2. Lihat tag yang ada di tag Sumber Daya. Anda juga dapat membuka jendela ini dengan memilih Kelola tag sumber daya yang dipilih, saat Anda mengubah atau menghapus tag dari halaman Kelola tag.

> **Note**
>
> Jika Anda tidak melihat tag yang baru-baru ini Anda terapkan ke sumber daya, coba segarkan jendela browser Anda.

Ekspor hasil ke file.csv

Anda dapat mengekspor hasil pencarian sumber daya untuk menandai kueri ke file nilai yang dipisahkan koma (.csv). File.csv mencakup nama sumber daya, layanan, Wilayah, sumber dayaIDs, jumlah total tag, dan kolom untuk setiap kunci tag unik dalam koleksi. File.csv dapat membantu Anda mengembangkan strategi penandaan untuk sumber daya di organisasi Anda, atau menentukan di mana ada tumpang tindih atau ketidakkonsistenan dalam penandaan di seluruh sumber daya.

1. Dalam hasil kueri Temukan sumber daya untuk menandai, pilih Ekspor sumber daya ke CSV.
2. Ketika Anda diminta oleh browser Anda, pilih untuk membuka file.csv, atau menyimpannya ke lokasi yang nyaman.

Mengelola tag dengan Editor Tag

Setelah Anda menemukan sumber daya yang ingin Anda tag, Anda dapat menambahkan, menghapus, dan mengedit tag untuk beberapa atau semua hasil pencarian Anda. Editor Tag menunjukkan tag apa pun yang dilampirkan ke sumber daya. Ini juga menunjukkan kepada Anda apakah tag tersebut ditambahkan di Editor Tag, oleh konsol layanan sumber daya, atau dengan menggunakanAPI.

Important

Jangan menyimpan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Kami menggunakan tag untuk memberi Anda layanan penagihan dan administrasi. Tag tidak dimaksudkan untuk digunakan dalam data sensitif atau privat.

Cara lain untuk mengelola tag Anda

Topik ini membahas sumber daya penandaan dengan menggunakan Editor Tag di AWS Management Console. Namun, Anda juga dapat mengelola tag di AWS sumber daya dengan menggunakan alat-alat berikut:

- Anda dapat mengetik atau skrip perintah di shell prompt Anda dengan menggunakan `resourcegroupstaggingapi`perintah di AWS Command Line Interface (AWS CLI).
- Anda dapat membuat dan menjalankan PowerShell skrip dengan menggunakan AWS Resource Groups Menandai API di AWS Tools for PowerShell Core.
- Anda dapat membuat dan menjalankan program dengan salah satu yang tersedia AWS SDKsdengan menggunakan penandaan grup Resource APIs, seperti penandaan untuk APIs Python atau penandaan untuk Java. APIs

Saat menambahkan, menghapus, atau mengedit tag yang ada, Anda hanya mengubah tag pada sumber daya yang Anda pilih di hasil Cari sumber daya untuk menandai kueri. Anda dapat memilih hingga 500 sumber daya untuk mengelola tag.

Tambahkan tag ke sumber daya yang dipilih

Anda dapat menggunakan Editor Tag untuk menambahkan tag ke sumber daya yang dipilih yang ada di hasil Cari sumber daya untuk menandai kueri.

> **Note**
>
> Topik ini menjelaskan cara mengedit tag secara massal untuk beberapa sumber daya. Anda juga dapat mengedit nilai tag untuk sumber daya individual. Untuk informasi selengkapnya, lihat Melihat dan mengedit tag yang ada untuk sumber daya yang dipilih.

1. Buka konsol Editor Tag, dan kirimkan kueri yang mengembalikan beberapa sumber daya yang ingin Anda tag.
2. Di tabel hasil kueri Temukan sumber daya untuk menandai, pilih kotak centang di sebelah sumber daya yang ingin Anda tambahkan tag. Masukkan string teks di Filter sumber daya di bagian atas tabel untuk memfilter bagian dari nama sumber daya, ID, kunci tag, atau nilai tag. Di kolom Tag, perhatikan bahwa sumber daya dalam hasil sudah memiliki tag yang diterapkan padanya.
3. Pilih kotak centang untuk satu atau beberapa sumber daya, lalu pilih Kelola tag sumber daya yang dipilih.
4. Pada halaman Kelola tag, lihat tag pada sumber daya yang Anda pilih. Meskipun kueri asli Anda mengembalikan lebih banyak sumber daya, Anda hanya menambahkan tag ke sumber daya yang Anda pilih di langkah 1. Pilih Tambahkan tanda.
5. Masukkan kunci tag dan nilai tag opsional. Untuk prosedur ini, Anda akan menambahkan kunci tag **`Team`** dan nilai tag**`Development`**.

   > **Note**
   >
   > Sumber daya dapat memiliki maksimal 50 tag yang diterapkan pengguna. Anda mungkin tidak dapat menambahkan tag baru ke sumber daya jika mendekati 50 tag yang diterapkan pengguna. AWS tag yang dihasilkan tidak berlaku untuk batas 50 tag. Kunci tag juga harus unik dalam sumber daya yang Anda pilih. Anda tidak dapat menambahkan tag baru dengan kunci yang cocok dengan kunci tag yang sudah ada di sumber daya yang dipilih.

6. Setelah selesai menambahkan tag, pilih Tinjau dan terapkan perubahan.

7. Jika Anda menerima perubahan, pilih Terapkan perubahan ke semua yang dipilih.
8. Bergantung pada jumlah sumber daya yang Anda pilih, menerapkan tag baru dapat memakan waktu beberapa menit. Jangan meninggalkan halaman atau membuka halaman lain di tab browser yang sama. Jika perubahan berhasil, spanduk sukses hijau ditampilkan di bagian atas halaman. Tunggu spanduk sukses atau gagal muncul di halaman sebelum Anda melanjutkan.

   Jika perubahan tag pada beberapa atau semua sumber daya tidak berhasil, lihat Mengatasi masalah perubahan tag. Setelah menyelesaikan perubahan tag yang gagal (seperti izin yang tidak memadai), Anda dapat mencoba lagi perubahan tag pada sumber daya yang gagal mengubah tag. Untuk informasi selengkapnya, lihat the section called “Coba lagi perubahan tag yang gagal”.

Edit tag sumber daya yang dipilih

Anda dapat menggunakan Editor Tag untuk mengubah nilai tag yang ada pada sumber daya yang dipilih yang ada di hasil Cari sumber daya untuk menandai kueri. Mengedit tag mengubah nilai tag pada semua sumber daya yang dipilih yang memiliki kunci tag yang sama. Anda tidak dapat mengganti nama kunci tag, tetapi Anda dapat menghapus tag dan membuat tag dengan nama baru untuk menggantikan kunci tag asli. Ini menghapus semua tag dengan kunci itu pada sumber daya yang dipilih.

> **Important**
>
> Jangan menyimpan informasi identitas pribadi (PII) atau informasi rahasia atau sensitif lainnya dalam tag. Kami menggunakan tag untuk memberi Anda layanan penagihan dan administrasi. Tag tidak dimaksudkan untuk digunakan dalam data sensitif atau privat.

1. Dalam hasil kueri Temukan sumber daya untuk menandai, pilih kotak centang di sebelah sumber daya yang ingin Anda ubah tag yang ada. Masukkan string teks di Filter sumber daya untuk memfilter bagian dari nama atau ID sumber daya. Di kolom Tag, perhatikan bahwa sumber daya dalam hasil sudah memiliki tag yang diterapkan padanya.
2. Pilih Kelola tag sumber daya yang dipilih.
3. Pada halaman Kelola tag, di Edit tag sumber daya yang dipilih, lihat tag pada sumber daya yang Anda pilih. Meskipun kueri asli Anda mungkin telah mengembalikan lebih banyak sumber daya, Anda mengubah tag hanya untuk sumber daya yang Anda pilih di langkah 1.

4. Mengubah, menambah, atau menghapus nilai tag. Tag yang ada harus memiliki kunci tag, tetapi nilai tag bersifat opsional.

   Dalam prosedur ini, kami mengubah nilai **`Team`** tag menjadi**`QA`**.

   Jika sumber daya dalam pilihan Anda memiliki nilai yang berbeda untuk kunci yang sama, Sumber daya yang dipilih memiliki nilai tag yang berbeda ditampilkan di bidang Nilai tag. Dalam hal ini, menempatkan kursor Anda di kotak akan membuka daftar tarik-turun dari semua nilai yang tersedia untuk kunci tag ini di sumber daya yang Anda pilih.

   Jika sumber daya dalam pilihan Anda memiliki nilai tag yang Anda inginkan, nilai tag disorot saat Anda mengetiknya. Misalnya, jika sumber daya dalam pilihan Anda sudah memiliki nilai tag**`QA`**, nilainya disorot saat Anda mengetik**`Q`**. Nilai dalam daftar tarik-turun membantu menjaga nilai tag tetap konsisten di seluruh sumber daya. Nilai tag diubah pada semua sumber daya yang dipilih. Dalam contoh ini, nilai tag diubah menjadi **`QA`** untuk semua sumber daya yang dipilih yang memiliki kunci **`Team`** tag. Untuk sumber daya terpilih yang tidak memiliki **`Team`** tag, **`Team`** tag dengan nilai **`QA`** ditambahkan.
5. Setelah selesai mengubah tag, pilih Tinjau dan terapkan perubahan.
6. Jika Anda menerima perubahan, pilih Terapkan perubahan ke semua yang dipilih.
7. Bergantung pada jumlah sumber daya yang Anda pilih, pengeditan tag dapat memakan waktu beberapa menit. Jangan meninggalkan halaman atau membuka halaman lain di tab browser yang sama. Jika perubahan berhasil, spanduk sukses hijau ditampilkan di bagian atas halaman. Tunggu spanduk sukses atau gagal muncul di halaman sebelum Anda melanjutkan.

   Jika perubahan tag pada beberapa atau semua sumber daya tidak berhasil, lihat Mengatasi masalah perubahan tag. Setelah menyelesaikan akar penyebab perubahan tag yang gagal (seperti izin yang tidak mencukupi), Anda dapat mencoba lagi perubahan tag pada sumber daya yang gagal mengubah tag. Untuk informasi selengkapnya, lihat the section called “Coba lagi perubahan tag yang gagal”.

Hapus tag dari sumber daya yang dipilih

Anda dapat menggunakan Editor Tag untuk menghapus tag dari sumber daya yang dipilih yang ada di hasil Cari sumber daya untuk menandai kueri. Menghapus tag akan menghapus tag dari semua sumber daya yang dipilih yang memiliki tag. Karena Anda tidak dapat mengedit kunci tag, Anda dapat menghapus tag dan menggantinya dengan tag baru jika Anda perlu mengedit kunci tag. Ini menghapus semua tag dengan kunci itu pada sumber daya yang dipilih.

1. Dalam hasil pencarian Cari sumber daya untuk menandai kueri, pilih kotak centang di sebelah sumber daya yang ingin Anda hapus tag. Masukkan string teks di Filter sumber daya untuk memfilter bagian dari nama atau ID sumber daya.
2. Pilih Kelola tag sumber daya yang dipilih.
3. Pada halaman Kelola tag, di Edit tag sumber daya yang dipilih, lihat tag pada sumber daya yang Anda pilih. Meskipun kueri asli Anda mungkin telah mengembalikan lebih banyak sumber daya, Anda mengubah tag hanya untuk sumber daya yang Anda pilih di langkah 1.
4. Pilih Hapus tag di samping tag apa pun yang ingin Anda hapus. Dalam prosedur ini, kami menghapus **`Team`** tag.

   > **Note**
   >
   > Memilih Hapus tag menghapus tag dari semua sumber daya yang dipilih yang memiliki tag.

5. Pilih Tinjau dan terapkan perubahan.
6. Pada halaman konfirmasi, pilih Terapkan perubahan ke semua yang dipilih.
7. Bergantung pada jumlah sumber daya yang Anda pilih, menghapus tag dapat memakan waktu beberapa menit. Jangan meninggalkan halaman atau membuka halaman lain di tab browser yang sama. Jika perubahan berhasil, spanduk sukses hijau ditampilkan di bagian atas halaman. Tunggu spanduk sukses atau gagal muncul di halaman sebelum Anda melanjutkan.

   Jika perubahan tag pada beberapa atau semua sumber daya tidak berhasil, lihat Memecahkan Masalah Perubahan Tag. Setelah menyelesaikan akar penyebab perubahan tag yang gagal (seperti izin yang tidak mencukupi), Anda dapat mencoba lagi perubahan tag pada sumber daya yang gagal mengubah tag. Untuk informasi selengkapnya, lihat the section called “Coba lagi perubahan tag yang gagal”.

Menggunakan tag dalam kebijakan IAM izin

AWS Identity and Access Management (IAM) adalah Layanan AWS yang Anda gunakan untuk membuat dan mengelola kebijakan izin yang menentukan siapa yang dapat mengakses AWS sumber daya Anda. Setiap upaya untuk mengakses AWS layanan atau membaca atau menulis AWS sumber daya adalah akses yang dikendalikan oleh IAM kebijakan.

Kebijakan ini memungkinkan Anda memberikan akses terperinci ke sumber daya Anda. Salah satu fitur yang dapat Anda gunakan untuk menyempurnakan akses ini adalah `Condition`elemen kebijakan. Elemen ini memungkinkan Anda menentukan kondisi yang harus sesuai dengan permintaan untuk menentukan apakah permintaan dapat dilanjutkan. Di antara hal-hal yang dapat Anda periksa dengan `Condition` elemen adalah sebagai berikut:

- Tag yang dilampirkan ke pengguna atau peran membuat permintaan.
- Tag yang dilampirkan ke sumber daya yang merupakan objek permintaan.

Tag dan kontrol akses berbasis atribut

Tag dapat menjadi bagian penting dari strategi kontrol AWS akses Anda. Untuk informasi tentang penggunaan tag sebagai atribut dalam strategi kontrol akses (ABAC) berbasis atribut, lihat Mengontrol akses ke AWS sumber daya menggunakan tag dan Mengontrol akses ke dan untuk IAM pengguna dan peran yang menggunakan tag, baik dalam IAMPanduan Pengguna.

Ada tutorial komprehensif yang menunjukkan cara memberikan akses ke berbagai proyek dan grup menggunakan tag di IAMtutorial: Tentukan izin untuk mengakses AWS sumber daya berdasarkan tag di Panduan AWS Identity and Access Management Pengguna.

Jika Anda menggunakan penyedia identitas SAML berbasis (iDP) untuk login tunggal, Anda dapat melampirkan tag ke peran yang diasumsikan yang menyediakan akses ke pengguna Anda. Untuk informasi selengkapnya, lihat IAMtutorial: Gunakan tag SAML sesi untuk ABAC di Panduan AWS Identity and Access Management Pengguna.

Kunci kondisi terkait tag

Tabel berikut menjelaskan kunci kondisi yang dapat Anda gunakan dalam kebijakan IAM izin untuk mengontrol akses berdasarkan tag. Kunci kondisi ini memungkinkan Anda melakukan hal berikut:

- Bandingkan tag pada prinsipal yang memanggil operasi.
- Bandingkan tag yang disediakan untuk operasi sebagai parameter.
- Bandingkan tag yang dilampirkan ke sumber daya yang akan diakses oleh operasi.

Untuk detail lengkap tentang kunci kondisi dan cara menggunakannya, lihat halaman yang ditautkan di kolom Nama kunci kondisi.

Nama kunci kondisi	Deskripsi
aws:PrincipalTag	Membandingkan tag yang dilampirkan pada prinsipal (IAMperan atau pengguna) yang membuat permintaan dengan tag yang Anda tentukan dalam kebijakan.
aws:RequestTag	Membandingkan pasangan nilai kunci tag yang diteruskan ke permintaan sebagai parameter dengan pasangan nilai kunci tag yang Anda tentukan dalam kebijakan.
aws:ResourceTag	Membandingkan pasangan kunci-nilai yang dilampirkan ke sumber daya dengan pasangan nilai kunci tag yang Anda tentukan dalam kebijakan.
aws:TagKeys	Membandingkan hanya kunci tag dalam permintaan dengan kunci yang Anda tentukan dalam kebijakan.

Contoh IAM kebijakan yang menggunakan tag

Example Contoh 1: Memaksa pengguna untuk melampirkan tag tertentu saat mereka membuat sumber daya

Contoh kebijakan IAM izin berikut menunjukkan cara memaksa pengguna yang membuat atau memodifikasi tag IAM kebijakan untuk menyertakan tag dengan kunci. `Owner` Selain itu, kebijakan mengharuskan nilai tag disetel ke nilai yang sama dengan `Owner` tag yang saat ini dilampirkan ke prinsipal pemanggil. Agar strategi ini berfungsi, semua prinsipal harus memiliki `Owner` tag yang terpasang, dan pengguna harus dicegah untuk memodifikasi tag itu. Jika upaya untuk membuat atau memodifikasi kebijakan terjadi tanpa menyertakan `Owner` tag, kebijakan tidak cocok dan operasi tidak diizinkan.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "TagCustomerManagedPolicies",
            "Effect": "Allow",
            "Action": [
                "iam:CreatePolicy",
                "iam:TagPolicy"
            ],
            "Resource": "arn:aws:iam::123456789012:policy/*",
            "Condition": {
                "StringEquals": {"aws:RequestTag/Owner": "${aws:PrincipalTag/Owner}"}
            }
        }
    ]
}
```

Example Contoh 2: Gunakan tag untuk membatasi akses ke sumber daya ke “pemiliknya”

Contoh kebijakan IAM izin berikut memungkinkan pengguna menghentikan EC2 instance Amazon yang sedang berjalan hanya jika prinsipal panggilan diberi tag dengan nilai `project` tag yang sama dengan instance.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor1",
      "Effect": "Allow",
      "Action": [
        "ec2:StopInstances"
      ],
      "Resource": [
        "arn:aws:iam::123456789012:instance/*"
      ],
      "Condition": {
        "StringEquals": {"aws:ResourceTag/project": "${aws:PrincipalTag/project}"}
      }
    }
  ]
}
```

Contoh ini adalah contoh dari kontrol akses berbasis atribut () ABAC. Untuk informasi selengkapnya dan contoh tambahan penggunaan IAM kebijakan guna menerapkan strategi kontrol akses berbasis tag, lihat topik berikut di Panduan AWS Identity and Access Management Pengguna:

- Mengontrol akses ke AWS sumber daya menggunakan tag
- Mengontrol akses ke dan untuk IAM pengguna dan peran menggunakan tag
- IAMtutorial: Tentukan izin untuk mengakses AWS sumber daya berdasarkan tag - Menunjukkan cara memberikan akses ke berbagai proyek dan grup menggunakan beberapa tag.

AWS Organizations kebijakan tag

Kebijakan tag adalah jenis kebijakan yang Anda buat AWS Organizations. Anda dapat menggunakan kebijakan tag untuk membantu menstandarisasi tag di seluruh sumber daya di akun organisasi Anda. Untuk menggunakan kebijakan tag, sebaiknya ikuti alur kerja yang dijelaskan di Memulai kebijakan tag di AWS Organizations Panduan Pengguna. Seperti yang disebutkan di halaman itu, alur kerja yang disarankan termasuk menemukan dan mengoreksi tag yang tidak sesuai. Untuk menyelesaikan tugas-tugas ini, Anda menggunakan konsol Editor Tag.

Prasyarat dan izin

Sebelum Anda dapat mengevaluasi kepatuhan terhadap kebijakan tag di Editor Tag, Anda harus memenuhi persyaratan dan menetapkan izin yang diperlukan.

Topik

- Prasyarat untuk mengevaluasi kepatuhan terhadap kebijakan tag
- Izin untuk mengevaluasi kepatuhan untuk akun
- Izin untuk mengevaluasi kepatuhan seluruh organisasi
- Kebijakan bucket Amazon S3 untuk penyimpanan laporan

Prasyarat untuk mengevaluasi kepatuhan terhadap kebijakan tag

Mengevaluasi kepatuhan terhadap kebijakan tag memerlukan hal-hal berikut:

- Anda harus terlebih dahulu mengaktifkan fitur di AWS Organizations, dan membuat dan melampirkan kebijakan tag. Untuk informasi selengkapnya, lihat halaman berikut di AWS Organizations Panduan Pengguna:
  - Prasyarat dan izin untuk mengelola kebijakan tag
  - Mengaktifkan kebijakan tag
  - Memulai dengan kebijakan tag
- Untuk menemukan tag yang tidak sesuai pada sumber daya akun, Anda memerlukan kredensi masuk untuk akun tersebut dan izin yang tercantum di dalamnya. Izin untuk mengevaluasi kepatuhan untuk akun
- Untuk mengevaluasi kepatuhan di seluruh organisasi, Anda memerlukan kredensi masuk untuk akun manajemen organisasi dan izin yang tercantum di dalamnya. Izin untuk mengevaluasi

kepatuhan seluruh organisasi Anda dapat meminta laporan kepatuhan hanya dari Wilayah AWS AS Timur (Virginia N.).

Izin untuk mengevaluasi kepatuhan untuk akun

Menemukan tag yang tidak sesuai pada sumber daya akun memerlukan izin berikut:

- `organizations:DescribeEffectivePolicy`— Untuk mendapatkan isi dari kebijakan tag efektif untuk akun.
- `tag:GetResources`— Untuk mendapatkan daftar sumber daya yang tidak sesuai dengan kebijakan tag terlampir.
- `tag:TagResources`— Untuk menambah atau memperbarui tag. Anda juga memerlukan izin khusus layanan untuk membuat tag. Misalnya, untuk menandai sumber daya di Amazon Elastic Compute Cloud (AmazonEC2), Anda memerlukan izin untuk. `ec2:CreateTags`
- `tag:UnTagResources`— Untuk menghapus tag. Anda juga memerlukan izin khusus layanan untuk menghapus tag. Misalnya, untuk menghapus tag sumber daya di AmazonEC2, Anda memerlukan izin untuk. `ec2:DeleteTags`

Contoh berikut AWS Identity and Access Management (IAM) kebijakan memberikan izin untuk mengevaluasi kepatuhan tag untuk akun.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EvaluateAccountCompliance",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeEffectivePolicy",
                "tag:GetResources",
                "tag:TagResources",
                "tag:UnTagResources"
            ],
            "Resource": "*"
        }
    ]
}
```

Untuk informasi selengkapnya tentang IAM kebijakan dan izin, lihat Panduan IAM Pengguna.

Izin untuk mengevaluasi kepatuhan seluruh organisasi

Mengevaluasi kepatuhan seluruh organisasi terhadap kebijakan tag memerlukan izin berikut:

- `organizations:DescribeEffectivePolicy`— Untuk mendapatkan konten kebijakan tag yang dilampirkan ke organisasi, unit organisasi (OU), atau akun.
- `tag:GetComplianceSummary`— Untuk mendapatkan ringkasan sumber daya yang tidak sesuai di semua akun di organisasi.
- `tag:StartReportCreation`— Untuk mengekspor hasil evaluasi kepatuhan terbaru ke file. Kepatuhan seluruh organisasi dievaluasi setiap 48 jam.
- `tag:DescribeReportCreation`— Untuk memeriksa status pembuatan laporan.
- `s3:ListAllMyBuckets`— Untuk membantu mengakses laporan kepatuhan di seluruh organisasi.
- `s3:GetBucketAcl`— Untuk memeriksa Daftar Kontrol Akses (ACL) bucket Amazon S3 yang menerima laporan kepatuhan.
- `s3:GetObject`— Untuk mengambil laporan kepatuhan dari bucket Amazon S3 milik layanan.
- `s3:PutObject`— Untuk menempatkan laporan kepatuhan di bucket Amazon S3 yang ditentukan.

Contoh IAM kebijakan berikut memberikan izin untuk mengevaluasi kepatuhan seluruh organisasi. Ganti masing-masing *`placeholder`* dengan informasi Anda sendiri:

- *`bucket_name`* — Nama ember Amazon S3 Anda
- *`organisasi_id`* — ID organisasi Anda

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EvaluateAccountCompliance",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeEffectivePolicy",
                "tag:StartReportCreation",
                "tag:DescribeReportCreation",
                "tag:GetComplianceSummary",
                "s3:ListAllMyBuckets"
```

```
            ],
            "Resource": "*"
        },
        {
            "Sid": "GetBucketAclForReportDelivery",
            "Effect": "Allow",
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::bucket_name",
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaLast": "tagpolicies.tag.amazonaws.com"
                }
            }
        },
        {
            "Sid": "GetObjectForReportDelivery",
            "Effect": "Allow",
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::*/tag-policy-compliance-reports/*",
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaLast": "tagpolicies.tag.amazonaws.com"
                }
            }
        },
        {
            "Sid": "PutObjectForReportDelivery",
            "Effect": "Allow",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::bucket_name/AwsTagPolicies/organization_id/*",
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaLast": "tagpolicies.tag.amazonaws.com"
                },
                "StringLike": {
                    "s3:x-amz-copy-source": "*/tag-policy-compliance-reports/*"
                }
            }
        }
    ]
}
```

Untuk informasi selengkapnya tentang IAM kebijakan dan izin, lihat Panduan IAM Pengguna.

Kebijakan bucket Amazon S3 untuk penyimpanan laporan

Untuk membuat laporan kepatuhan di seluruh organisasi, identitas yang Anda gunakan untuk menelepon `StartReportCreation` API harus memiliki akses ke bucket Amazon Simple Storage Service (Amazon S3) di Wilayah AS Timur (Virginia N.) untuk menyimpan laporan. Kebijakan Tag menggunakan kredensional identitas panggilan untuk mengirimkan laporan kepatuhan ke bucket yang ditentukan.

Jika bucket dan identitas yang digunakan untuk memanggil `StartReportCreation` API milik akun yang sama, kebijakan bucket Amazon S3 tambahan tidak diperlukan untuk kasus penggunaan ini.

Jika akun yang terkait dengan identitas yang digunakan untuk menelepon berbeda dari akun yang memiliki bucket Amazon S3, kebijakan bucket berikut harus dilampirkan ke bucket. `StartReportCreation` API Ganti masing-masing *`placeholder`* dengan informasi Anda sendiri:

- *`bucket_name`* — Nama ember Amazon S3 Anda
- *`organisasi_id`* — ID organisasi Anda
- *`identitas_ ARN`* — ARN IAM Identitas yang digunakan untuk memanggil `StartReportCreation` API

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CrossAccountTagPolicyACL",
            "Effect": "Allow",
            "Principal": {
                "AWS": "identity_ARN"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::bucket_name"
         },
         {
            "Sid": "CrossAccountTagPolicyBucketDelivery",
            "Effect": "Allow",
            "Principal": {
                "AWS": "identity_ARN"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::bucket_name/AwsTagPolicies/organization_id/*"
```

```
            }
        ]
}
```

Mengevaluasi kepatuhan untuk akun

Anda dapat mengevaluasi kepatuhan akun di organisasi Anda dengan kebijakan tag yang efektif.

> **Important**
>
> Sumber daya yang tidak diberi tag tidak akan muncul sebagai tag tidak patuh dalam hasil. Untuk menemukan sumber daya yang tidak ditandai di akun Anda, gunakan Penjelajah Sumber Daya AWS dengan kueri yang menggunakan. **`tag:none`** Untuk informasi selengkapnya, lihat Mencari sumber daya yang tidak ditandai di Penjelajah Sumber Daya AWS Panduan Pengguna.

Kebijakan tag efektif menentukan aturan penandaan yang berlaku untuk akun. Kebijakan tag yang efektif adalah agregasi kebijakan tag apa pun yang diwarisi akun, ditambah kebijakan tag apa pun yang langsung dilampirkan ke akun. Bila Anda melampirkan kebijakan tag ke root organisasi, maka kebijakan tag tersebut akan berlaku untuk semua akun di organisasi Anda. Ketika Anda melampirkan kebijakan tag ke unit organisasi (OU), itu berlaku untuk semua akun dan OUs yang menjadi milik OU.

> **Note**
>
> Jika Anda belum membuat kebijakan tag, lihat Memulai kebijakan tag di Panduan AWS Organizations Pengguna.

Untuk menemukan tag yang tidak sesuai, Anda harus memiliki izin berikut:

- `organizations:DescribeEffectivePolicy`
- `tag:GetResources`
- `tag:TagResources`
- `tag:UntagResources`

Untuk mengevaluasi kepatuhan akun dengan kebijakan tag efektifnya (konsol)

1. Saat masuk ke akun yang kepatuhannya ingin Anda periksa, buka konsol Kebijakan Tag.
2. Bagian Kebijakan tag efektif menunjukkan kapan kebijakan terakhir diperbarui dan kunci tag yang ditentukan. Anda dapat memperluas kunci tag untuk melihat informasi tentang nilainya, perlakuan kasus, dan apakah nilai diberlakukan untuk jenis sumber daya tertentu.

   > **Note**
   >
   > Jika Anda masuk ke akun manajemen, Anda harus memilih akun untuk melihat kebijakan efektifnya dan melihat informasi kepatuhan.

3. Di bagian Sumber daya dengan tag yang tidak sesuai, tentukan tag mana yang akan dicari Wilayah AWS untuk tag yang tidak sesuai. Secara opsional, Anda juga dapat mencari berdasarkan jenis sumber daya. Kemudian pilih Cari sumber daya.

   Hasil real-time ditampilkan di bagian Hasil pencarian. Untuk mengubah jumlah hasil yang dikembalikan per halaman atau kolom yang akan ditampilkan, pilih ikon pengaturan.
4. Dalam hasil pencarian, pilih sumber daya dengan tag yang tidak sesuai.
5. Di kotak dialog yang mencantumkan tag sumber daya, pilih hyperlink untuk membuka Layanan AWS tempat sumber daya dibuat. Dari konsol itu, perbaiki tag yang tidak sesuai.

   > **Tip**
   >
   > Jika Anda tidak yakin tag mana yang tidak sesuai, buka bagian Kebijakan tag efektif untuk akun di konsol Kebijakan Tag. Anda dapat memperluas kunci tag untuk melihat aturan penandaannya.

6. Ulangi proses menemukan dan mengoreksi tag hingga sumber daya akun yang Anda pedulikan sesuai di setiap Wilayah.

Untuk menemukan tag yang tidak sesuai (AWS CLI,) AWS API

Gunakan perintah dan operasi berikut untuk menemukan tag yang tidak sesuai:

- AWS Command Line Interface (AWS CLI):
  - aws resourcegroupstaggingapi get-resources
  - aws resourcegroupstaggingapi tag-resources

- aws resourcegroupstaggingapi untag-resources

  Untuk prosedur lengkap penggunaan kebijakan tag di AWS CLI, lihat Menggunakan kebijakan tag AWS CLI di Panduan AWS Organizations Pengguna.

- AWS Resource Groups Tagging API:
  - GetResources
  - TagResources
  - UntagResources

Langkah selanjutnya

Kami menyarankan Anda mengulangi proses menemukan dan memperbaiki masalah kepatuhan. Lanjutkan hingga sumber daya akun yang Anda pedulikan sesuai dengan kebijakan tag efektif di setiap Wilayah.

Menemukan dan mengoreksi tag yang tidak sesuai adalah proses berulang karena berbagai alasan, termasuk yang berikut:

- Penggunaan kebijakan tag organisasi Anda dapat berkembang dari waktu ke waktu.
- Butuh waktu untuk mempengaruhi perubahan dalam organisasi Anda saat membuat sumber daya.
- Kepatuhan dapat berubah kapan saja sumber daya baru dibuat atau ketika tag baru ditetapkan ke sumber daya.
- Kebijakan tag efektif akun diperbarui setiap kali kebijakan tag dilampirkan atau terlepas darinya. Kebijakan tag efektif juga diperbarui setiap kali terjadi perubahan untuk menandai kebijakan yang diwarisi akun.

Jika Anda masuk sebagai akun manajemen di organisasi, Anda juga dapat membuat laporan. Laporan ini menampilkan informasi tentang semua sumber daya yang ditandai di akun organisasi Anda. Untuk informasi selengkapnya, lihat Mengevaluasi kepatuhan seluruh organisasi.

Mengevaluasi kepatuhan seluruh organisasi

Anda dapat mengevaluasi kepatuhan organisasi Anda dengan kebijakan tag yang efektif. Anda dapat membuat laporan yang mencantumkan semua sumber daya yang ditandai di akun di seluruh organisasi Anda dan apakah setiap sumber daya sesuai dengan kebijakan tag yang efektif.

> **Important**
>
> Sumber daya yang tidak diberi tag tidak akan muncul sebagai tag tidak patuh dalam hasil. Untuk menemukan sumber daya yang tidak ditandai di akun Anda, gunakan Penjelajah Sumber Daya AWS dengan query yang menggunakan**`tag:none`**. Untuk informasi selengkapnya, lihat Mencari sumber daya yang tidak ditandai di Penjelajah Sumber Daya AWS Panduan Pengguna.

Anda dapat membuat laporan dari akun manajemen organisasi Anda di `us-east-1` Wilayah AWS hanya. Akun yang menghasilkan laporan harus memiliki akses ke ember Amazon S3 di Wilayah AS Timur (Virginia N.). Bucket harus memiliki kebijakan bucket terlampir seperti yang ditunjukkan dalam kebijakan bucket Amazon S3 untuk menyimpan laporan.

Untuk membuat laporan kepatuhan di seluruh organisasi, Anda harus memiliki izin berikut:

- `organizations:DescribeEffectivePolicy`
- `tag:GetComplianceSummary`
- `tag:StartReportCreation`
- `tag:DescribeReportCreation`
- `s3:ListAllMyBuckets`
- `s3:GetBucketAcl`
- `s3:GetObject`
- `s3:PutObject`

Untuk contoh IAM kebijakan yang menampilkan izin ini, tinjau Izin untuk mengevaluasi kepatuhan di seluruh organisasi.

Untuk menghasilkan laporan kepatuhan di seluruh organisasi (konsol)

1. Buka konsol Kebijakan Tag.
2. Pilih tab Root organisasi ini, dan di dekat bagian bawah halaman, pilih Buat laporan.
3. Di layar Hasilkan laporan, tentukan tempat menyimpan laporan.
4. Pilih Mulai mengekspor.

Setelah laporan selesai, Anda dapat mengunduhnya dari bagian Laporan ketidakpatuhan di tab root Organisasi.

> **Catatan**
>
> Kepatuhan seluruh organisasi dievaluasi setiap 48 jam. Ini menghasilkan yang berikut:
>
> - Diperlukan waktu hingga 48 jam agar perubahan pada kebijakan tag atau sumber daya ditampilkan dalam laporan kepatuhan di seluruh organisasi. Sebagai contoh, anggaplah bahwa Anda memiliki kebijakan tag yang mendefinisikan tag standar baru untuk jenis sumber daya. Sumber daya jenis yang tidak memiliki tag ini dapat ditampilkan sebagai sesuai dalam laporan hingga 48 jam.
> - Meskipun Anda dapat membuat laporan kapan saja, hasil laporan tidak diperbarui hingga evaluasi berikutnya selesai.
> - NoncompliantKeysKolom mencantumkan kunci tag pada sumber daya yang tidak sesuai dengan kebijakan tag efektif.
> - KeysWithNonCompliantValuesKolom mencantumkan kunci yang ditentukan dalam kebijakan efektif yang ada di sumber daya dengan perlakuan kasus yang salah atau nilai yang tidak sesuai.
> - Jika Anda menutup sebuah Akun AWS yang merupakan anggota organisasi, dapat terus muncul dalam laporan kepatuhan tag hingga 90 hari.

Untuk menghasilkan laporan kepatuhan di seluruh organisasi (AWS CLI, AWS API)

Gunakan perintah dan operasi berikut untuk membuat laporan kepatuhan di seluruh organisasi, memeriksa statusnya, dan melihat laporan:

- AWS Command Line Interface AWS CLI):
  - aws resourcegroupstaggingapi start-report-creation
  - aws resourcegroupstaggingapi describe-report-creation
  - aws resourcegroupstaggingapi get-compliance-summary

  Untuk prosedur lengkap untuk menggunakan kebijakan tag di AWS CLI, lihat Menggunakan kebijakan tag di AWS CLIdi AWS Organizations Panduan Pengguna.
- AWS API:
  - StartReportCreation

- DescribeReportCreation
- GetComplianceSummary

Pantau perubahan tag dengan alur kerja tanpa server dan Amazon EventBridge

Amazon EventBridge mendukung perubahan tag pada AWS sumber daya. Menggunakan EventBridge jenis ini, Anda dapat membuat EventBridge aturan untuk mencocokkan perubahan tag dan merutekan peristiwa ke satu atau beberapa target. Misalnya, target mungkin merupakan AWS Lambda fungsi untuk memanggil alur kerja otomatis. Topik ini menyediakan tutorial untuk menggunakan Lambda untuk membangun solusi tanpa server yang hemat biaya untuk memproses perubahan tag pada sumber daya Anda dengan aman. AWS

Perubahan tag menghasilkan EventBridge acara

EventBridge memberikan aliran peristiwa sistem yang mendekati real-time yang menggambarkan perubahan AWS sumber daya. Banyak AWS sumber daya mendukung tag, yang merupakan atribut khusus yang ditentukan pengguna untuk mengatur dan mengkategorikan AWS sumber daya dengan mudah. Kasus penggunaan umum untuk tag adalah kategorisasi alokasi biaya, keamanan kontrol akses, dan otomatisasi.

Dengan EventBridge, Anda dapat memantau perubahan tag dan melacak status tag pada AWS sumber daya. Sebelumnya, untuk mencapai fungsionalitas serupa, Anda mungkin terus melakukan polling APIs dan mengatur beberapa panggilan. Sekarang, setiap perubahan pada tag termasuk layanan individualAPIs, Editor Tag, dan Tagging API akan memulai perubahan tag pada acara sumber daya. Contoh berikut menunjukkan EventBridge peristiwa khas yang diminta oleh perubahan tag. Ini menunjukkan kunci tag baru, diperbarui, atau dihapus, dan nilai yang terkait.

```
{
  "version": "0",
  "id": "bddcf1d6-0251-35a1-aab0-adc1fb47c11c",
  "detail-type": "Tag Change on Resource",
  "source": "aws.tag",
  "account": "123456789012",
  "time": "2018-09-18T20:41:38Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa"
  ],
  "detail": {
    "changed-tag-keys": [
```

```
      "a-new-key",
      "an-updated-key",
      "a-deleted-key"
    ],
    "tags": {
      "a-new-key": "tag-value-on-new-key-just-added",
      "an-updated-key": "tag-value-was-just-changed",
      "an-unchanged-key": "tag-value-still-the-same"
    },
    "service": "ec2",
    "resource-type": "instance",
    "version": 3,
  }
}
```

Semua EventBridge acara memiliki bidang tingkat atas yang sama:

- versi - Secara default, nilai ini diatur ke `0` (nol) di semua acara.
- id - Nilai unik dihasilkan untuk setiap acara. Ini dapat membantu dalam melacak peristiwa saat mereka bergerak melalui aturan ke target dan diproses.
- detail-type - Mengidentifikasi, dalam kombinasi dengan `source` bidang, bidang dan nilai yang muncul di bidang detail.
- sumber - Mengidentifikasi layanan yang merupakan sumber acara. Sumber untuk perubahan tag adalah`aws.tag`.
- waktu — Stempel waktu acara.
- wilayah — Mengidentifikasi dari Wilayah AWS mana peristiwa itu berasal.
- resource — JSON Array ini berisi Amazon Resource Names (ARNs) yang mengidentifikasi sumber daya yang terlibat dalam acara tersebut. Ini adalah sumber di mana tag telah berubah.
- detail — Sebuah JSON objek, yang isinya berbeda tergantung pada jenis acara. Untuk perubahan tag pada sumber daya, bidang rinci berikut disertakan:
  - changed-tag-keys— Tombol tag yang diubah oleh acara ini.
  - layanan — Layanan yang dimiliki sumber daya. Dalam contoh ini, layanannya adalah`ec2`, yaitu AmazonEC2.
  - jenis sumber daya — Jenis sumber daya layanan. Dalam contoh ini, ini adalah EC2 contoh Amazon.
  - versi - Versi set tag. Versi dimulai pada 1 dan bertambah ketika tag diubah. Anda dapat menggunakan versi untuk memverifikasi urutan peristiwa perubahan tag.

- tag — Tag yang dilampirkan ke sumber daya setelah perubahan.

Untuk informasi selengkapnya, lihat pola EventBridge acara Amazon di Panduan EventBridge Pengguna Amazon.

Dengan menggunakan EventBridge, Anda dapat membuat aturan yang cocok dengan pola peristiwa tertentu berdasarkan bidang yang berbeda. Kami menunjukkan bagaimana melakukan ini dalam tutorial. Selain itu, kami menunjukkan bagaimana EC2 instance Amazon dapat dihentikan secara otomatis jika tag tertentu tidak dilampirkan ke instance. Kami menggunakan EventBridge bidang untuk membuat pola agar sesuai dengan peristiwa tag untuk instance yang meluncurkan fungsi Lambda.

Lambda dan tanpa server

AWS Lambda mengikuti paradigma tanpa server untuk menjalankan kode di cloud. Anda menjalankan kode hanya ketika diperlukan, tanpa memikirkan server. Anda hanya membayar untuk waktu komputasi yang tepat yang Anda gunakan. Meskipun disebut tanpa server, itu tidak berarti bahwa tidak ada server. Tanpa server dalam konteks ini berarti Anda tidak perlu menyediakan, mengonfigurasi, atau mengelola server yang digunakan untuk menjalankan kode Anda. AWS melakukan semua itu untuk Anda, sehingga Anda dapat fokus pada kode Anda. Untuk informasi selengkapnya tentang Lambda, lihat Ikhtisar AWS Lambda Produk.

Tutorial: Secara otomatis menghentikan EC2 instans Amazon yang tidak memiliki tag yang diperlukan

Sebagai kolam Anda AWS sumber daya dan Akun AWS yang Anda kelola tumbuh, Anda dapat menggunakan tag untuk membuatnya lebih mudah untuk mengkategorikan sumber daya Anda. Tag biasanya digunakan untuk kasus penggunaan kritis seperti alokasi biaya dan keamanan. Untuk mengelola secara efektif AWS sumber daya, sumber daya Anda perlu ditandai secara konsisten. Seringkali, ketika sumber daya disediakan, ia mendapatkan semua tag yang sesuai. Namun, proses selanjutnya dapat menghasilkan perubahan tag yang menghasilkan penyimpangan dari kebijakan tag perusahaan. Dengan memantau perubahan pada tag Anda, Anda dapat melihat penyimpangan tag dan segera merespons. Ini memberi Anda lebih percaya diri bahwa proses yang bergantung pada sumber daya Anda yang dikategorikan dengan benar akan menghasilkan hasil yang diinginkan.

Contoh berikut menunjukkan cara memantau perubahan tag pada EC2 instans Amazon untuk memverifikasi bahwa instance tertentu terus memiliki tag yang diperlukan. Jika tag instance berubah

dan instance tidak lagi memiliki tag yang diperlukan, fungsi Lambda dipanggil untuk mematikan instance secara otomatis. Mengapa Anda ingin melakukan ini? Ini memastikan bahwa semua sumber daya ditandai sesuai dengan kebijakan tag perusahaan Anda, untuk alokasi biaya yang efektif, atau untuk dapat mempercayai keamanan berdasarkan kontrol akses berbasis atribut (). ABAC

> **Important**
>
> Kami sangat menyarankan agar Anda melakukan tutorial ini di akun non-produksi di mana Anda tidak dapat secara tidak sengaja mematikan instance penting.
> Kode contoh dalam tutorial ini sengaja membatasi dampak skenario ini hanya pada instance pada daftar instance. IDs Anda harus memperbarui daftar dengan contoh IDs bahwa Anda bersedia untuk menutup untuk tes. Ini membantu memastikan bahwa Anda tidak dapat secara tidak sengaja mematikan setiap instance di Wilayah di Akun AWS.
> Setelah pengujian, pastikan semua instans Anda ditandai sesuai dengan strategi penandaan perusahaan Anda. Kemudian, Anda dapat menghapus kode yang membatasi fungsi hanya pada instance IDs pada daftar.

Contoh ini menggunakan JavaScript dan versi 16.x dari Node.js. Contoh menggunakan contoh Akun AWS ID 123456789012 dan Wilayah AWS AS Timur (Virginia N.) (`us-east-1`). Ganti ini dengan ID dan Wilayah akun pengujian Anda sendiri.

> **Note**
>
> Jika konsol Anda menggunakan Wilayah yang berbeda untuk defaultnya, pastikan Anda mengganti Wilayah yang Anda gunakan dalam tutorial ini setiap kali Anda mengubah konsol. Penyebab umum kegagalan tutorial ini adalah memiliki instance dan fungsi di dua Wilayah yang berbeda.

Jika Anda menggunakan Wilayah yang berbeda dari`us-east-1`, pastikan bahwa Anda mengubah semua referensi dalam contoh kode berikut ke Wilayah pilihan Anda.

Topik

- Langkah 1. Buat fungsi Lambda
- Langkah 2. Siapkan IAM izin yang diperlukan
- Langkah 3. Lakukan tes pendahuluan fungsi Lambda Anda

- Langkah 4. Buat EventBridge aturan yang meluncurkan fungsi
- Langkah 5. Uji solusi lengkapnya
- Ringkasan tutorial

Langkah 1. Buat fungsi Lambda

Untuk membuat fungsi Lambda

1. Buka AWS Lambda konsol manajemen.
2. Pilih Buat fungsi dan kemudian Tulis dari awal.
3. Untuk Nama fungsi, ketik **`AutoEC2Termination`**.
4. Untuk Runtime, pilih Node.js 16.x.
5. Simpan semua bidang lain pada nilai defaultnya, dan pilih Buat fungsi.
6. Pada tab Kode pada halaman `AutoEC2Termination` detail, buka file index.js untuk melihat kodenya.

   - Jika tab dengan index.js terbuka, Anda dapat memilih kotak edit di tab itu untuk mengedit kodenya.
   - Jika tab dengan index.js tidak terbuka, klik sekunder file index.js di bawah EC2Terminator folder Auto di panel navigasi. Kemudian pilih Buka.
7. Di tab index.js, tempel kode berikut di kotak editor, ganti apa pun yang sudah ada.

   Ganti nilainya `RegionToMonitor` dengan Region tempat Anda ingin menjalankan fungsi ini.

```
// Set the following line to specify which Region's instances you want to monitor
// Only instances in this Region are succesfully stopped on a match

const RegionToMonitor = "us-east-1"

// Specify the instance ARNs to check.
// This limits the function for safety to avoid the tutorial shutting down all
 instances in account
// The first ARN is a "dummy" that matches the test event you create in Step 3.
// Replace the second ARN with one that matches a real instance that you want to
 monitor and that you can
// safely stop

const InstanceList = [
```

```
    "i-0000000aaaaaaaaaa",
    "i-05db4466d02744f07"
];

// The tag key name and value that marks a "valid" instance. Instances in the
 previous list that
// do NOT have the following tag key and value are stopped by this function

const ValidKeyName = "valid-key";
const ValidKeyValue = "valid-value";

// Load and configure the AWS SDK
const AWS = require('aws-sdk');
// Set the AWS Region
AWS.config.update({region: RegionToMonitor});
// Create EC2 service object.
const ec2 = new AWS.EC2({apiVersion: '2016-11-15'});

exports.handler = (event, context, callback) => {

  // Retrieve the details of the reported event.
  var detail = event.detail;
  var tags = detail["tags"];
  var service = detail["service"];
  var resourceType = detail["resource-type"];
  var resource = event.resources[0];
  var resourceSplit = resource.split("/");
  var instanceId = resourceSplit[resourceSplit.length - 1];

  // If this event is not for an EC2 resource, then do nothing.
  if (!(service === "ec2")) {
    console.log("Event not for correct service -- no action (", service, ")" );
    return;
  }

  // If this event is not about an instance, then do nothing.
  if (!(resourceType === "instance")) {
    console.log("Event not for correct resource type -- no action (", resourceType,
 ")" );
    return;
  }

  // CAUTION - Removing the following 'if' statement causes the function to run
 against
```

```
 //           every EC2 instance in the specified Region in the calling Akun AWS.
 //           If you do this and an instance is not tagged with the approved tag
key
 //           and value, this function stops that instance.

 // If this event is not for the ARN of an instance in our include list, then do
nothing.
 if (InstanceList.indexOf(instanceId)<0) {
   console.log("Event not for one of the monitored instances -- no action (",
resource, ")");
   return;
 }

 console.log("Tags changed on monitored EC2 instance (",instanceId,")");

 // Check attached tags for expected tag key and value pair
 if ( tags.hasOwnProperty(ValidKeyName) && tags[ValidKeyName] == "valid-value"){
   // Required tags ARE present
   console.log("The instance has the required tag key and value -- no action");
   callback(null, "no action");
   return;
 }

 // Required tags NOT present
 console.log("This instance is missing the required tag key or value -- attempting
to stop the instance");

 var params = {
   InstanceIds: [instanceId],
   DryRun: true
 };

 // call EC2 to stop the selected instances
 ec2.stopInstances(params, function(err, data) {
   if (err && err.code === 'DryRunOperation') {
     // dryrun succeeded, so proceed with "real" stop operation
     params.DryRun = false;
     ec2.stopInstances(params, function(err, data) {
       if (err) {
         console.log("Failed to stop instance");
         callback(err, "fail");
       } else if (data) {
         console.log("Successfully stopped instance", data.StoppingInstances);
         callback(null, "Success");
```

```
        }
      });
    } else {
      console.log("Dryrun attempt failed");
      callback(err);
    }
  });
};
```

8. Pilih Deploy untuk menyimpan perubahan Anda dan membuat versi baru fungsi aktif.

Fungsi Lambda ini memeriksa tag EC2 instance Amazon, seperti yang dilaporkan oleh peristiwa perubahan tag di. EventBridge Dalam contoh ini, jika instance dalam acara tersebut kehilangan kunci tag yang diperlukan `valid-key` atau jika tag tersebut tidak memiliki nilai`valid-value`, maka fungsi tersebut mencoba menghentikan instance. Anda dapat mengubah pemeriksaan logis ini atau persyaratan tag untuk kasus penggunaan spesifik Anda sendiri.

Biarkan jendela konsol Lambda tetap terbuka di browser Anda.

Langkah 2. Siapkan IAM izin yang diperlukan

Sebelum fungsi berhasil dijalankan, Anda harus memberikan fungsi izin untuk menghentikan sebuah EC2 instance. Bagian AWS peran yang diberikan lambda_basic_executiontidak memiliki izin itu. Dalam tutorial ini, Anda memodifikasi kebijakan IAM izin default yang dilampirkan ke peran eksekusi fungsi bernama`AutoEC2Termination-role-`*`uniqueid`*. Izin tambahan minimum yang diperlukan untuk tutorial ini adalah`ec2:StopInstances`.

Untuk informasi selengkapnya tentang membuat IAM kebijakan EC2 khusus Amazon, lihat AmazonEC2: Mengizinkan memulai atau menghentikan EC2 Instans dan memodifikasi grup keamanan, secara terprogram dan di konsol di Panduan Pengguna. IAM

Untuk membuat kebijakan IAM izin dan melampirkannya ke peran eksekusi fungsi Lambda

1. Di tab atau jendela browser yang berbeda, buka halaman Peran IAM konsol.
2. Mulai mengetik nama peran**`AutoEC2Termination`**, dan ketika muncul dalam daftar, pilih nama peran.
3. Pada halaman Ringkasan peran, pilih tab Izin dan pilih nama satu kebijakan yang sudah dilampirkan.
4. Pada halaman Ringkasan kebijakan, pilih Edit kebijakan.

5. Pada tab Editor Visual, pilih Tambahkan izin tambahan.
6. Untuk Layanan, pilih EC2.
7. Untuk Tindakan, pilih StopInstances. Anda dapat mengetik **`Stop`** di bilah pencarian, dan kemudian memilih `StopInstances` kapan muncul.
8. Untuk Sumber Daya, pilih Semua sumber daya, pilih Kebijakan tinjauan, lalu pilih Simpan perubahan.

   Ini secara otomatis membuat versi baru kebijakan dan menetapkan versi tersebut sebagai default.

   Kebijakan akhir Anda akan terlihat mirip dengan contoh berikut.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "ec2:StopInstances",
            "Resource": "*"
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": "logs:CreateLogGroup",
            "Resource": "arn:aws:logs:us-east-1:123456789012:*"
        },
        {
            "Sid": "VisualEditor2",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:us-east-1:123456789012:log-group:/aws/lambda/
AutoEC2Termination:*"
        }
    ]
}
```

Langkah 3. Lakukan tes pendahuluan fungsi Lambda Anda

Pada langkah ini, Anda mengirimkan acara pengujian ke fungsi Anda. Fungsionalitas pengujian Lambda bekerja dengan mengirimkan peristiwa pengujian yang disediakan secara manual. Fungsi memproses peristiwa uji seperti jika acara itu berasal EventBridge. Anda dapat menentukan beberapa peristiwa pengujian dengan nilai yang berbeda untuk menjalankan semua bagian yang berbeda dari kode Anda. Pada langkah ini, Anda mengirimkan peristiwa pengujian yang menunjukkan bahwa tag EC2 instans Amazon berubah, dan tag baru tidak menyertakan kunci dan nilai tag yang diperlukan.

Untuk menguji fungsi Lambda Anda

1. Kembali ke jendela atau tab dengan konsol Lambda dan buka tab Uji untuk fungsi Otomatis EC2Termination Anda.
2. Pilih Buat acara baru.
3. Untuk Nama peristiwa, masukkan **`SampleBadTagChangeEvent`**.
4. Dalam Acara JSON, ganti teks dengan contoh peristiwa yang ditunjukkan dalam contoh teks berikut. Anda tidak perlu mengubah akun, Wilayah, atau ID instans agar peristiwa pengujian ini berfungsi dengan benar.

```
{
  "version": "0",
  "id": "bddcf1d6-0251-35a1-aab0-adc1fb47c11c",
  "detail-type": "Tag Change on Resource",
  "source": "aws.tag",
  "account": "123456789012",
  "time": "2018-09-18T20:41:38Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:ec2:us-east-1:123456789012:instance/i-0000000aaaaaaaaaa"
  ],
  "detail": {
    "changed-tag-keys": [
      "valid-key"
    ],
    "tags": {
      "valid-key": "NOT-valid-value"
    },
    "service": "ec2",
    "resource-type": "instance",
```

```
    "version": 3
  }
}
```

5. Pilih Simpan, lalu pilih Uji.

   Tes tampaknya gagal, tapi tidak apa-apa.

   Anda akan melihat kesalahan berikut di tab Hasil eksekusi di bawah Respons.

```
{
  "errorType": "InvalidInstanceID.NotFound",
  "errorMessage": "The instance ID 'i-0000000aaaaaaaaaa' does not exist",
  ...
}
```

   Kesalahan terjadi karena instance yang ditentukan dalam acara pengujian tidak ada.

   Informasi pada tab Hasil eksekusi, di bagian Log Fungsi, menunjukkan bahwa fungsi Lambda Anda berhasil mencoba menghentikan sebuah instance. EC2 Namun, gagal karena kode awalnya mencoba DryRunoperasi untuk menghentikan instance, yang menunjukkan bahwa ID instance tidak valid.

```
START RequestId: 390c1f8d-0d9b-4b44-b087-8de64479ab44 Version: $LATEST
2022-11-30T20:17:30.427Z    390c1f8d-0d9b-4b44-b087-8de64479ab44    INFO    Tags
 changed on monitored EC2 instance ( i-0000000aaaaaaaaaa )
2022-11-30T20:17:30.427Z    390c1f8d-0d9b-4b44-b087-8de64479ab44    INFO    This
 instance is missing the required tag key or value -- attempting to stop the
 instance
2022-11-30T20:17:31.206Z    390c1f8d-0d9b-4b44-b087-8de64479ab44    INFO    Dryrun
 attempt failed
2022-11-30T20:17:31.207Z    390c1f8d-0d9b-4b44-b087-8de64479ab44    ERROR   Invoke
 Error     {"errorType":"InvalidInstanceID.NotFound","errorMessage":"The instance
 ID 'i-0000000aaaaaaaaaa' does not
 exist","code":"InvalidInstanceID.NotFound","message":"The instance ID
 'i-0000000aaaaaaaaaa' does not
 exist","time":"2022-11-30T20:17:31.205Z","requestId":"a5192c3b-142d-4cec-
bdbc-685a9b7c7abf","statusCode":400,"retryable":false,"retryDelay":36.87870631147607,"stack
["InvalidInstanceID.NotFound: The instance ID 'i-0000000aaaaaaaaaa' does
 not exist","    at Request.extractError (/var/runtime/node_modules/aws-sdk/
lib/services/ec2.js:50:35)","    at Request.callListeners (/var/runtime/
node_modules/aws-sdk/lib/sequential_executor.js:106:20)","    at Request.emit
```

```
 (/var/runtime/node_modules/aws-sdk/lib/sequential_executor.js:78:10)","    at
 Request.emit (/var/runtime/node_modules/aws-sdk/lib/request.js:686:14)","    at
 Request.transition (/var/runtime/node_modules/aws-sdk/lib/request.js:22:10)","
    at AcceptorStateMachine.runTo (/var/runtime/node_modules/aws-sdk/lib/
state_machine.js:14:12)","    at /var/runtime/node_modules/aws-sdk/lib/
state_machine.js:26:10","    at Request.<anonymous> (/var/runtime/node_modules/aws-
sdk/lib/request.js:38:9)","    at Request.<anonymous> (/var/runtime/node_modules/
aws-sdk/lib/request.js:688:12)","    at Request.callListeners (/var/runtime/
node_modules/aws-sdk/lib/sequential_executor.js:116:18)"]}
END RequestId: 390c1f8d-0d9b-4b44-b087-8de64479ab44
```

6. Untuk membuktikan bahwa kode tidak mencoba menghentikan instance ketika tag yang benar digunakan, Anda dapat membuat dan mengirimkan peristiwa pengujian lain.

   Pilih tab Uji di atas Sumber kode. Konsol menampilkan acara SampleBadTagChangeEventpengujian yang ada.

7. Pilih Buat acara baru.
8. Untuk nama Acara, ketik**`SampleGoodTagChangeEvent`**.
9. Pada baris 17, hapus **`NOT-`** untuk mengubah nilainya menjadi**`valid-value`**.
10. Di bagian atas jendela Test event, pilih Save, lalu pilih Test.

    Output menampilkan berikut ini, yang menunjukkan bahwa fungsi mengenali tag yang valid dan tidak mencoba untuk mematikan instance.

```
START RequestId: 53631a49-2b54-42fe-bf61-85b9e91e86c4 Version: $LATEST
2022-12-01T23:24:12.244Z    53631a49-2b54-42fe-bf61-85b9e91e86c4    INFO    Tags
 changed on monitored EC2 instance ( i-0000000aaaaaaaaaa )
2022-12-01T23:24:12.244Z    53631a49-2b54-42fe-bf61-85b9e91e86c4    INFO    The
 instance has the required tag key and value -- no action
END RequestId: 53631a49-2b54-42fe-bf61-85b9e91e86c4
```

    Biarkan konsol Lambda tetap terbuka di browser Anda.

Langkah 4. Buat EventBridge aturan yang meluncurkan fungsi

Sekarang Anda dapat membuat EventBridge aturan yang cocok dengan acara dan menunjuk ke fungsi Lambda Anda.

Untuk membuat EventBridge aturan

1. Di tab atau jendela browser yang berbeda, buka EventBridge konsol ke halaman Create Rule.
2. Untuk Nama, masukkan**`ec2-instance-rule`**, lalu pilih Berikutnya.
3. Gulir ke bawah ke metode Creation dan pilih Custom pattern (JSONeditor).
4. Di kotak pengeditan, tempel teks pola berikut, lalu pilih Berikutnya.

```
{
  "source": [
    "aws.tag"
  ],
  "detail-type": [
    "Tag Change on Resource"
  ],
  "detail": {
    "service": [
      "ec2"
    ],
    "resource-type": [
      "instance"
    ]
  }
}
```

   Aturan ini cocok dengan `Tag Change on Resource` peristiwa untuk EC2 instans Amazon dan memanggil apa pun yang Anda tentukan sebagai Target di langkah berikutnya.
5. Selanjutnya, tambahkan fungsi Lambda Anda sebagai target. Dalam kotak Target 1, di bawah Pilih target, pilih fungsi Lambda.
6. Di bawah Fungsi, pilih EC2Termination fungsi Otomatis yang Anda buat sebelumnya, lalu pilih Berikutnya.
7. Pada halaman Konfigurasi tag, pilih Berikutnya. Kemudian pada halaman Tinjau dan buat, pilih Buat aturan. Ini juga secara otomatis memberikan izin EventBridge untuk menjalankan fungsi Lambda yang ditentukan.

Langkah 5. Uji solusi lengkapnya

Anda dapat menguji hasil akhir Anda dengan membuat EC2 instance dan melihat apa yang terjadi ketika Anda mengubah tagnya.

Untuk menguji solusi pemantauan dengan instance nyata

1. Buka EC2konsol Amazon ke halaman Instans.
2. Buat EC2 instance Amazon. Sebelum Anda meluncurkannya, lampirkan tag dengan kunci `valid-key` dan nilainya`valid-value`. Untuk informasi tentang cara membuat dan meluncurkan instance, lihat Langkah 1: Meluncurkan instance di Panduan EC2 Pengguna Amazon. Dalam prosedur Untuk meluncurkan instance, pada langkah 3, di mana Anda memasukkan tag Nama, juga pilih Tambahkan tag tambahan, pilih Tambah tag, lalu masukkan Kunci **`valid-key`** dan Nilai dari**`valid-value`**. Anda dapat Melanjutkan tanpa key pair jika instance ini semata-mata untuk keperluan tutorial ini dan Anda berencana untuk menghapus instance ini setelah Anda menyelesaikannya. Kembali ke tutorial ini ketika Anda mencapai akhir Langkah 1; Anda tidak perlu melakukan Langkah 2: Connect to your instance.
3. Salin InstanceIddari konsol.
4. Beralih dari EC2 konsol Amazon ke konsol Lambda. Pilih EC2Termination fungsi Otomatis Anda, pilih tab Kode, lalu pilih tab index.js untuk mengedit kode Anda.
5. Ubah entri kedua di `InstanceList` dengan menempelkan nilai yang Anda salin dari konsol AmazonEC2. Pastikan `RegionToMonitor` nilainya cocok dengan Wilayah yang berisi instance yang Anda tempelkan.
6. Pilih Deploy untuk membuat perubahan Anda aktif. Fungsi ini sekarang siap untuk diaktifkan oleh perubahan tag ke instance itu di Wilayah tertentu.
7. Beralih dari konsol Lambda ke konsol AmazonEC2.
8. Ubah Tag yang dilampirkan ke instance dengan menghapus tag valid-key atau dengan mengubah nilai kunci itu.

   > **Note**
   >
   > Untuk informasi tentang cara mengubah tag pada EC2 instance Amazon yang sedang berjalan, lihat Menambahkan dan menghapus tag pada sumber daya individual di Panduan EC2 Pengguna Amazon.

9. Tunggu beberapa detik, lalu segarkan konsol. Instance harus mengubah status Instance menjadi Stopping dan kemudian ke Stopped.
10. Beralih dari EC2 konsol Amazon ke konsol Lambda dengan fungsi Anda, dan pilih tab Monitor.
11. Pilih tab Log, dan dalam tabel Pemanggilan terbaru, pilih entri terbaru di LogStreamkolom.

CloudWatch Konsol Amazon terbuka ke halaman peristiwa Log untuk pemanggilan terakhir fungsi Lambda Anda. Entri terakhir akan terlihat mirip dengan contoh berikut.

```
2022-11-30T12:03:57.544-08:00    START RequestId: b5befd18-2c41-43c8-
a320-3a4b2317cdac Version: $LATEST
2022-11-30T12:03:57.548-08:00    2022-11-30T20:03:57.548Z b5befd18-2c41-43c8-
a320-3a4b2317cdac INFO Tags changed on monitored EC2 instance ( arn:aws:ec2:us-
west-2:123456789012:instance/i-1234567890abcdef0 )
2022-11-30T12:03:57.548-08:00    2022-11-30T20:03:57.548Z b5befd18-2c41-43c8-
a320-3a4b2317cdac INFO This instance is missing the required tag key or value --
 attempting to stop the instance
2022-11-30T12:03:58.488-08:00    2022-11-30T20:03:58.488Z b5befd18-2c41-43c8-
a320-3a4b2317cdac INFO Successfully stopped instance [ { CurrentState: { Code: 64,
 Name: 'stopping' }, InstanceId: 'i-1234567890abcdef0', PreviousState: { Code: 16,
 Name: 'running' } } ]
2022-11-30T12:03:58.546-08:00    END RequestId: b5befd18-2c41-43c8-
a320-3a4b2317cdac
```

Ringkasan tutorial

Tutorial ini menunjukkan cara membuat EventBridge aturan agar sesuai dengan perubahan tag pada peristiwa sumber daya untuk EC2 instance Amazon. Aturan menunjuk ke fungsi Lambda yang secara otomatis mematikan instance jika tidak memiliki tag yang diperlukan.

EventBridge Dukungan Amazon untuk perubahan tag AWS sumber daya membuka kemungkinan untuk membangun otomatisasi berbasis peristiwa di banyak Layanan AWS. Menggabungkan kemampuan ini dengan AWS Lambda memberi Anda alat untuk membangun solusi tanpa server yang mengakses AWS sumber daya dengan aman, skala sesuai permintaan, dan hemat biaya.

Kasus penggunaan lain yang mungkin untuk tag-change-on-resource EventBridge acara tersebut meliputi:

- Luncurkan peringatan jika seseorang mengakses sumber daya Anda dari alamat IP yang tidak biasa — Gunakan tag untuk menyimpan alamat IP sumber setiap pengunjung yang mengakses sumber daya Anda. Perubahan pada tag menghasilkan CloudWatch peristiwa. Anda dapat menggunakan peristiwa itu untuk membandingkan alamat IP sumber dengan daftar alamat IP yang valid dan mengaktifkan email peringatan jika alamat IP sumber tidak valid.
- Pantau jika ada perubahan pada kontrol akses berbasis tag untuk sumber daya — Jika Anda telah menyiapkan akses ke sumber daya menggunakan kontrol akses berbasis atribut (tagABAC), Anda

dapat menggunakan EventBridge peristiwa yang dihasilkan oleh perubahan apa pun pada tag untuk meminta audit oleh tim keamanan Anda.

Pemecahan masalah perubahan tag

Daftar periksa berikut mungkin berguna jika terjadi kesalahan saat Anda mencoba menerapkan atau mengubah tag pada sumber daya yang dipilih di Temukan sumber daya untuk menandai hasil kueri.

- Sumber daya mungkin sudah memiliki jumlah tag maksimum. Umumnya, sumber daya dapat memiliki maksimal 50 tag yang ditentukan pengguna. AWS tag yang dihasilkan tidak dihitung menuju maksimum 50 tag. Pengguna lain mungkin juga menambahkan tag ke sumber daya yang sama pada saat yang sama, yang dapat meningkatkan tag sumber daya secara maksimal.
- Beberapa layanan memungkinkan set karakter yang berbeda (atau membatasi set karakter yang diizinkan) untuk membuat tag. Jika Anda menambahkan atau mengubah tag menggunakan karakter khusus, tinjau persyaratan tag dalam dokumentasi layanan sumber daya untuk memverifikasi bahwa karakter tersebut diizinkan oleh layanan.
- Anda mungkin tidak memiliki izin untuk mengubah tag untuk sumber daya. Jika Anda tidak memiliki izin untuk melihat tag yang ada di sumber daya, Anda tidak dapat membuat perubahan pada tag sumber daya.
- Anda mungkin tidak memiliki izin untuk mengubah sumber daya. Perubahan pada metadata sumber daya mungkin dibatasi oleh administrator lain.
- Sumber daya mungkin telah diedit atau dihapus oleh pengguna atau proses lain. Misalnya, asumsikan bahwa sumber daya diluncurkan sebagai bagian dari pembuatan AWS CloudFormation tumpukan. Jika tumpukan dihapus atau tidak lagi dalam keadaan aktif, sumber daya mungkin tidak lagi tersedia.
- Perubahan tag mungkin tidak dimungkinkan jika sumber daya offline atau dihentikan, atau jika pembaruan lain (seperti peningkatan perangkat lunak) ke sumber daya sedang berlangsung.
- Perubahan tag dapat gagal jika Anda menutup tab browser atau mengubah halaman sebelum perubahan tag selesai. Biarkan perubahan tag selesai, dan tunggu banner sukses atau gagal muncul di halaman, sebelum Anda meninggalkan halaman.
- Meskipun ada batas tarif untuk layanan tersebut AWS Resource Groups Tagging API, layanan yang Anda beri tag mungkin memberlakukan batas terpisah yang mungkin Anda tekan sebelum batas Penandaan API Resource Groups.

Coba lagi perubahan tag yang gagal

Jika perubahan tag gagal pada setidaknya satu sumber daya yang Anda pilih, Editor Tag menampilkan spanduk merah di bagian bawah halaman. Spanduk menunjukkan pesan kesalahan untuk setiap jenis kegagalan yang terjadi. Untuk setiap kesalahan, spanduk mengidentifikasi sumber daya tertentu di mana Editor Tag tidak dapat membuat perubahan tag. Setelah Anda meninjau dan memecahkan masalah kesalahan, pilih Coba lagi perubahan tag yang gagal pada sumber daya untuk mencoba lagi perubahan hanya pada sumber daya yang gagal mengubah tag.

Keamanan di Editor Tag

Keamanan cloud di AWS merupakan prioritas tertinggi. Sebagai pelanggan AWS, Anda mendapatkan manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara AWS dan Anda. Model tanggung jawab bersama menjelaskan hal ini sebagai keamanan dari cloud dan keamanan di cloud:

- Keamanan cloud – AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan Layanan AWS dalam AWS Cloud. AWS juga memberi Anda layanan yang dapat digunakan dengan aman. Auditor pihak ketiga secara berkala menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari AWS program kepatuhan. Untuk informasi selengkapnya tentang program kepatuhan yang berlaku untuk Editor Tag, lihat AWSLayanan dalam Lingkup menurut Program Kepatuhan.
- Keamanan dalam cloud – Tanggung jawab Anda ditentukan oleh Layanan AWS yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan Editor Tag. Topik berikut menunjukkan cara mengonfigurasi Editor Tag untuk memenuhi tujuan keamanan dan kepatuhan Anda.

Topik

- Perlindungan data di Editor Tag
- Manajemen identitas dan akses untuk Editor Tag
- Pencatatan dan pemantauan di Editor Tag
- Validasi kepatuhan untuk Editor Tag
- Ketahanan dalam Editor Tag
- Keamanan infrastruktur di Editor Tag

Perlindungan data di Editor Tag

Bagian AWS model tanggung jawab bersama model berlaku untuk perlindungan data di Editor Tag. Seperti yang dijelaskan dalam model ini, AWS bertanggung jawab untuk melindungi infrastruktur

global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk menjaga kontrol atas konten Anda yang di-host di infrastruktur ini. Anda juga bertanggung jawab atas konfigurasi keamanan dan tugas manajemen untuk Layanan AWS yang Anda gunakan. Untuk informasi selengkapnya tentang privasi data, lihat Privasi Data FAQ. Untuk informasi tentang perlindungan data di Eropa, lihat AWS Model Tanggung Jawab Bersama dan posting GDPR blog di AWS Blog Keamanan.

Untuk tujuan perlindungan data, kami menyarankan Anda untuk melindungi Akun AWS kredensi dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan otentikasi multi-faktor (MFA) dengan setiap akun.
- GunakanSSL/TLSuntuk berkomunikasi dengan AWS sumber daya. Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail. Untuk informasi tentang menggunakan CloudTrail jalur untuk menangkap AWS kegiatan, lihat Bekerja dengan CloudTrail jalan setapak di AWS CloudTrail Panduan Pengguna.
- Gunakan AWS solusi enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan FIPS 140-3 modul kriptografi yang divalidasi saat mengakses AWS melalui antarmuka baris perintah atauAPI, gunakan FIPS titik akhir. Untuk informasi selengkapnya tentang FIPS titik akhir yang tersedia, lihat Federal Information Processing Standard (FIPS) 140-3.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk ketika Anda bekerja dengan Editor Tag atau lainnya Layanan AWS menggunakan konsol,API, AWS CLI, atau AWS SDKs. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Jika Anda memberikan URL ke server eksternal, kami sangat menyarankan agar Anda tidak menyertakan informasi kredensil dalam URL untuk memvalidasi permintaan Anda ke server tersebut.

Enkripsi data

Informasi penandaan tidak dienkripsi. Meskipun tidak dienkripsi, tag dapat berisi informasi yang digunakan sebagai bagian dari strategi keamanan Anda, jadi penting untuk mengontrol siapa yang dapat mengakses tag pada sumber daya. Sangat penting bagi Anda untuk mengontrol siapa yang dapat memodifikasi tag karena akses tersebut dapat digunakan untuk meningkatkan izin seseorang.

Enkripsi diam

Tidak ada cara tambahan untuk mengisolasi layanan atau lalu lintas jaringan yang khusus untuk Editor Tag. Jika berlaku, gunakan AWS isolasi khusus. Anda dapat menggunakan Editor Tag API dan konsol di cloud pribadi virtual (VPC) untuk membantu memaksimalkan privasi dan keamanan infrastruktur.

Enkripsi bergerak

Data Editor Tag dienkripsi saat transit ke database internal layanan untuk cadangan. Ini tidak dapat dikonfigurasi pengguna.

Manajemen kunci

Tag Editor saat ini tidak terintegrasi dengan AWS Key Management Service dan tidak mendukung AWS KMS keys.

Privasi lalu lintas antar jaringan

Tag Editor digunakan HTTPS untuk semua transmisi antara pengguna Tag Editor dan AWS. Tag Editor menggunakan transport layer security (TLS) 1.3, tetapi juga mendukung TLS 1.2.

Manajemen identitas dan akses untuk Editor Tag

AWS Identity and Access Management (IAM) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. IAMadministrator mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya Editor Tag. IAMadalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

- Audiens

- Mengautentikasi dengan identitas
- Mengelola akses menggunakan kebijakan
- Bagaimana Tag Editor bekerja dengan IAM
- Contoh kebijakan berbasis identitas Editor Tag
- Pemecahan Masalah identitas dan akses Editor Tag

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan di Editor Tag.

Pengguna layanan — Jika Anda menggunakan layanan Editor Tag untuk melakukan pekerjaan Anda, administrator Anda memberi Anda kredensi dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak fitur Editor Tag untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara akses dikelola dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di Editor Tag, lihatPemecahan Masalah identitas dan akses Editor Tag.

Administrator layanan - Jika Anda bertanggung jawab atas sumber daya Editor Tag di perusahaan Anda, Anda mungkin memiliki akses penuh ke Editor Tag. Tugas Anda adalah menentukan fitur dan sumber daya Editor Tag mana yang harus diakses pengguna layanan Anda. Anda kemudian harus mengirimkan permintaan ke IAM administrator Anda untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep dasarIAM. Untuk mempelajari selengkapnya tentang bagaimana perusahaan Anda dapat menggunakan IAM Editor Tag, lihatBagaimana Tag Editor bekerja dengan IAM.

IAMadministrator - Jika Anda seorang IAM administrator, Anda mungkin ingin mempelajari detail tentang cara menulis kebijakan untuk mengelola akses ke Editor Tag. Untuk melihat contoh kebijakan berbasis identitas Editor Tag yang dapat Anda gunakan, lihat. IAM Contoh kebijakan berbasis identitas Editor Tag

Mengautentikasi dengan identitas

Otentikasi adalah cara Anda masuk AWS menggunakan kredensi identitas Anda. Anda harus diautentikasi (masuk ke AWS) sebagai Pengguna root akun AWS, sebagai IAM pengguna, atau dengan mengambil peranIAM.

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensi yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (Pusat IAM Identitas), autentikasi masuk tunggal perusahaan Anda, dan kredensi Google atau Facebook Anda adalah contoh identitas federasi. Saat Anda masuk sebagai identitas federasi, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan IAM peran. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

Bergantung pada jenis pengguna Anda, Anda dapat masuk ke AWS Management Console atau portal AWS akses. Untuk informasi selengkapnya tentang masuk AWS, lihat Cara masuk ke Panduan AWS Sign-In Pengguna Anda Akun AWS.

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensil Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Untuk informasi selengkapnya tentang menggunakan metode yang disarankan untuk menandatangani permintaan sendiri, lihat Menandatangani AWS API permintaan di Panduan IAM Pengguna.

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari lebih lanjut, lihat Autentikasi multi-faktor di Panduan AWS IAM Identity Center Pengguna dan Menggunakan otentikasi multi-faktor (MFA) AWS di Panduan Pengguna. IAM

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya di akun. Identitas ini disebut pengguna Akun AWS root dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas yang mengharuskan Anda masuk sebagai pengguna root, lihat Tugas yang memerlukan kredensi pengguna root di IAMPanduan Pengguna.

Pengguna dan Grup

IAMPengguna adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, sebaiknya mengandalkan kredensi sementara daripada

membuat IAM pengguna yang memiliki kredensi jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan khusus yang memerlukan kredensil jangka panjang dengan IAM pengguna, kami sarankan Anda memutar kunci akses. Untuk informasi selengkapnya, lihat Memutar kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensi jangka panjang di IAMPanduan Pengguna.

IAMGrup adalah identitas yang menentukan kumpulan IAM pengguna. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat memiliki grup bernama IAMAdminsdan memberikan izin grup tersebut untuk mengelola sumber dayaIAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari lebih lanjut, lihat Kapan membuat IAM pengguna (bukan peran) di Panduan IAM Pengguna.

Peran

IAMPeran adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Ini mirip dengan IAM pengguna, tetapi tidak terkait dengan orang tertentu. Anda dapat mengambil IAM peran sementara AWS Management Console dengan beralih peran. Anda dapat mengambil peran dengan memanggil AWS CLI atau AWS API operasi atau dengan menggunakan kustomURL. Untuk informasi selengkapnya tentang metode penggunaan peran, lihat Metode untuk mengambil peran dalam Panduan IAM Pengguna.

IAMperan dengan kredensi sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat Membuat peran untuk Penyedia Identitas pihak ketiga di Panduan IAM Pengguna. Jika Anda menggunakan Pusat IAM Identitas, Anda mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah diautentikasi, Pusat IAM Identitas menghubungkan izin yang disetel ke peran. IAM Untuk informasi tentang set izin, lihat Set izin dalam Panduan Pengguna AWS IAM Identity Center .
- Izin IAM pengguna sementara — IAM Pengguna atau peran dapat mengambil IAM peran untuk sementara mengambil izin yang berbeda untuk tugas tertentu.

- Akses lintas akun — Anda dapat menggunakan IAM peran untuk memungkinkan seseorang (prinsipal tepercaya) di akun lain mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM Panduan Pengguna. IAM
- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Misalnya, saat Anda melakukan panggilan dalam suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.
  - Sesi akses teruskan (FAS) — Saat Anda menggunakan IAM pengguna atau peran untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FASmenggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. FASPermintaan hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan saat membuat FAS permintaan, lihat Meneruskan sesi akses.
  - Peran layanan — Peran layanan adalah IAMperan yang diasumsikan layanan untuk melakukan tindakan atas nama Anda. IAMAdministrator dapat membuat, memodifikasi, dan menghapus peran layanan dari dalamIAM. Untuk informasi selengkapnya, lihat Membuat peran untuk mendelegasikan izin ke Layanan AWS dalam IAMPanduan Pengguna.
  - Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke peran layanan. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. IAMAdministrator dapat melihat, tetapi tidak mengedit izin untuk peran terkait layanan.
- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan IAM peran untuk mengelola kredenal sementara untuk aplikasi yang berjalan pada EC2 instance dan membuat AWS CLI atau AWS API meminta. Ini lebih baik untuk menyimpan kunci akses dalam EC2 instance. Untuk menetapkan AWS peran ke EC2 instance dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instance berisi peran dan memungkinkan program yang berjalan pada EC2 instance untuk mendapatkan kredensi

sementara. Untuk informasi selengkapnya, lihat Menggunakan IAM peran untuk memberikan izin ke aplikasi yang berjalan di EC2 instans Amazon di IAMPanduan Pengguna.

Untuk mempelajari apakah akan menggunakan IAM peran atau IAM pengguna, lihat Kapan membuat IAM peran (bukan pengguna) di Panduan IAM Pengguna.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izinnya. AWS mengevaluasi kebijakan ini ketika prinsipal (pengguna, pengguna root, atau sesi peran) membuat permintaan. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai JSON dokumen. Untuk informasi selengkapnya tentang struktur dan isi dokumen JSON kebijakan, lihat Ringkasan JSON kebijakan di Panduan IAM Pengguna.

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Secara default, pengguna dan peran tidak memiliki izin. Untuk memberikan izin kepada pengguna untuk melakukan tindakan pada sumber daya yang mereka butuhkan, IAM administrator dapat membuat IAM kebijakan. Administrator kemudian dapat menambahkan IAM kebijakan ke peran, dan pengguna dapat mengambil peran.

IAMkebijakan menentukan izin untuk tindakan terlepas dari metode yang Anda gunakan untuk melakukan operasi. Misalnya, anggaplah Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan itu bisa mendapatkan informasi peran dari AWS Management Console, AWS CLI, atau AWS API.

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan JSON izin yang dapat dilampirkan ke identitas, seperti pengguna, grup IAM pengguna, atau peran. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Membuat IAM kebijakan di Panduan Pengguna. IAM

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan yang dikelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran dalam. Akun AWS Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan terkelola atau kebijakan sebaris, lihat Memilih antara kebijakan terkelola dan kebijakan sebaris di IAMPanduan Pengguna.

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen JSON kebijakan yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan kepercayaan IAM peran dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

Kebijakan berbasis sumber daya merupakan kebijakan inline yang terletak di layanan tersebut. Anda tidak dapat menggunakan kebijakan AWS terkelola IAM dalam kebijakan berbasis sumber daya.

Daftar kontrol akses (ACLs)

Access control lists (ACLs) mengontrol prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACLsmirip dengan kebijakan berbasis sumber daya, meskipun mereka tidak menggunakan format dokumen kebijakan. JSON

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung. ACLs Untuk mempelajari selengkapnyaACLs, lihat Ikhtisar daftar kontrol akses (ACL) di Panduan Pengembang Layanan Penyimpanan Sederhana Amazon.

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang kurang umum. Jenis-jenis kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda oleh jenis kebijakan yang lebih umum.

- Batas izin — Batas izin adalah fitur lanjutan tempat Anda menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas (pengguna atau peran). IAM IAM Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan

berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batas izin, lihat Batas izin untuk IAM entitas di IAMPanduan Pengguna.

- Kebijakan kontrol layanan (SCPs) — SCPs adalah JSON kebijakan yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di AWS Organizations. AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur dalam organisasi, Anda dapat menerapkan kebijakan kontrol layanan (SCPs) ke salah satu atau semua akun Anda. SCPMembatasi izin untuk entitas di akun anggota, termasuk masing-masing Pengguna root akun AWS. Untuk informasi selengkapnya tentang Organizations danSCPs, lihat Kebijakan kontrol layanan di Panduan AWS Organizations Pengguna.
- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan secara tegas dalam salah satu kebijakan ini membatalkan izin. Untuk informasi selengkapnya, lihat Kebijakan sesi di Panduan IAM Pengguna.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat Logika evaluasi kebijakan di Panduan IAM Pengguna.

Bagaimana Tag Editor bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke Editor Tag, Anda harus memahami IAM fitur apa yang tersedia untuk digunakan dengan Editor Tag. Untuk mendapatkan tampilan tingkat tinggi tentang cara Layanan AWS kerja Editor Tag dan lainnyaIAM, lihat Layanan AWS yang berfungsi IAM di Panduan IAM Pengguna.

Topik

- Kebijakan berbasis identitas Editor Tag
- Kebijakan berbasis sumber daya
- Otorisasi berdasarkan tanda

- IAMPeran Editor Tag

Kebijakan berbasis identitas Editor Tag

Dengan kebijakan IAM berbasis identitas, Anda dapat menentukan tindakan dan sumber daya yang diizinkan atau ditolak selain kondisi di mana tindakan diizinkan atau ditolak. Editor Tag mendukung tindakan, sumber daya, dan kunci kondisi tertentu. Untuk mempelajari semua elemen yang Anda gunakan dalam JSON kebijakan, lihat referensi elemen IAM JSON kebijakan di Panduan IAM Pengguna.

Tindakan

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

`Action`Elemen JSON kebijakan menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam kebijakan. Tindakan kebijakan biasanya memiliki nama yang sama dengan AWS API operasi terkait. Ada beberapa pengecualian, seperti tindakan khusus izin yang tidak memiliki operasi yang cocok. API Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

Menyertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Tindakan kebijakan di Editor Tag menggunakan awalan berikut sebelum tindakan:`tag:`. Tindakan Editor Tag dilakukan sepenuhnya di konsol, tetapi memiliki awalan `tag` di entri log.

Misalnya, untuk memberikan izin kepada seseorang untuk menandai sumber daya dengan `tag:TagResources` API operasi, Anda menyertakan `tag:TagResources` tindakan tersebut dalam kebijakan mereka. Pernyataan kebijakan harus memuat elemen `Action` atau `NotAction`. Tag Editor mendefinisikan serangkaian tindakannya sendiri yang menjelaskan tugas yang dapat Anda lakukan dengan layanan ini.

Untuk menentukan beberapa tindakan penandaan dalam satu pernyataan, pisahkan dengan koma sebagai berikut.

```
"Action": [
      "tag:action1",
      "tag:action2",
```

```
      "tag:action3"
```

Anda juga dapat menentukan beberapa tindakan menggunakan wildcard (*). Misalnya, untuk menentukan semua tindakan yang dimulai dengan kata `Get`, sertakan tindakan berikut.

```
"Action": "tag:Get*"
```

Untuk melihat daftar tindakan Editor Tag, lihat Tindakan, sumber daya, dan kunci kondisi untuk Editor Tag di Referensi Otorisasi Layanan.

Sumber daya

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, principal dapat melakukan tindakan pada suatu sumber daya, dan dalam suatu syarat.

Elemen `Resource` JSON kebijakan menentukan objek atau objek yang tindakan tersebut berlaku. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Sebagai praktik terbaik, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, misalnya operasi pencantuman, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

```
"Resource": "*"
```

Tag Editor tidak memiliki sumber daya sendiri. Sebaliknya, ia memanipulasi metadata (tag) yang melekat pada sumber daya yang dibuat oleh orang lain. Layanan AWS

Kunci syarat

Administrator dapat menggunakan AWS JSON kebijakan untuk menentukan siapa yang memiliki akses ke apa. Yaitu, di mana utama dapat melakukan tindakan pada sumber daya, dan dalam kondisi apa.

Elemen `Condition` (atau blok `Condition`) akan memungkinkan Anda menentukan kondisi yang menjadi dasar suatu pernyataan berlaku. Elemen `Condition` bersifat opsional. Anda dapat

membuat ekspresi bersyarat yang menggunakan operator kondisi, misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta.

Jika Anda menentukan beberapa elemen `Condition` dalam sebuah pernyataan, atau beberapa kunci dalam elemen `Condition` tunggal, maka AWS akan mengevaluasinya menggunakan operasi `AND` logis. Jika Anda menentukan beberapa nilai untuk satu kunci kondisi, AWS mengevaluasi kondisi menggunakan `OR` operasi logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Misalnya, Anda dapat memberikan izin IAM pengguna untuk mengakses sumber daya hanya jika ditandai dengan nama IAM pengguna mereka. Untuk informasi selengkapnya, lihat elemen IAM kebijakan: variabel dan tag di Panduan IAM Pengguna.

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. Untuk melihat semua kunci kondisi AWS global, lihat kunci konteks kondisi AWS global di Panduan IAM Pengguna.

Editor Tag tidak mendefinisikan kunci kondisi khusus layanan apa pun.

Contoh

Untuk melihat contoh kebijakan berbasis identitas Editor Tag, lihat. Contoh kebijakan berbasis identitas Editor Tag

Kebijakan berbasis sumber daya

Editor Tag tidak mendukung kebijakan berbasis sumber daya karena tidak menentukan sumber dayanya sendiri.

Otorisasi berdasarkan tanda

Otorisasi berdasarkan tag adalah bagian dari strategi keamanan yang disebut atribut-based access control (). ABAC

Untuk mengontrol akses ke sumber daya berdasarkan tagnya, Anda memberikan informasi tag dalam elemen kondisi kebijakan menggunakan`aws:ResourceTag/`*`key-name`*`,aws:RequestTag/`*`key-name`*, atau kunci `aws:TagKeys` kondisi. Anda dapat menerapkan tag ke sumber daya saat Anda membuat atau memperbarui sumber daya.

Untuk melihat contoh kebijakan berbasis identitas untuk membatasi akses ke sumber daya berdasarkan tag pada sumber daya tersebut, lihat Melihat grup berdasarkan tag. Untuk informasi

selengkapnya tentang kontrol akses berbasis atribut (ABAC), lihat Untuk apa? ABAC AWS dalam IAMUser Guide.

IAMPeran Editor Tag

IAMPeran adalah entitas di dalam Anda Akun AWS yang memiliki izin khusus. Editor Tag tidak memiliki atau menggunakan peran layanan.

Menggunakan kredensi sementara dengan Tag Editor

Di Editor Tag, Anda dapat menggunakan kredenal sementara untuk masuk dengan federasi, mengambil IAM peran, atau untuk mengambil peran lintas akun. Anda memperoleh kredensi keamanan sementara dengan memanggil AWS STS API operasi seperti AssumeRoleatau. GetFederationToken

Peran terkait layanan

Peran terkait layanan memungkinkan Layanan AWS untuk mengakses sumber daya di layanan lain untuk menyelesaikan tindakan atas nama Anda.

Editor Tag tidak memiliki atau menggunakan peran terkait layanan.

Peran layanan

Fitur ini memungkinkan layanan untuk menerima peran layanan atas nama Anda.

Editor Tag tidak memiliki atau menggunakan peran layanan.

Contoh kebijakan berbasis identitas Editor Tag

Secara default, prinsipal IAM, seperti peran dan pengguna, tidak memiliki izin untuk membuat atau memodifikasi tag. Mereka juga tidak dapat melakukan tugas menggunakanAWS Management Console, AWS Command Line Interface (AWS CLI), atau AWS API. Administrator IAM harus membuat kebijakan IAM yang memberikan izin kepada prinsipal untuk melakukan operasi API tertentu pada sumber daya tertentu yang mereka butuhkan. Administrator kemudian harus melampirkan kebijakan tersebut ke kepala sekolah yang memerlukan izin tersebut.

Untuk petunjuk cara membuat kebijakan berbasis identitas IAM menggunakan contoh dokumen kebijakan JSON ini, lihat Membuat Kebijakan di Tab JSON di Panduan Pengguna IAM.

Topik

- Praktik terbaik kebijakan
- Menggunakan konsol Tag Editor dan Resource Groups Tagging API
- Izinkan pengguna melihat izin mereka sendiri
- Melihat grup berdasarkan tag

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya Editor Tag di akun Anda. Tindakan ini dikenai biaya untuk Akun AWS Anda. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulai menggunakan kebijakan yang dikelola AWS dan beralih ke izin dengan hak akses paling rendah – Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan yang dikelola AWS yang memberikan izin untuk banyak kasus penggunaan umum. Kebijakan ini ada di Akun AWS Anda. Sebaiknya Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola pelanggan AWS yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat kebijakan yang dikelola AWS atau kebijakan yang dikelola AWS untuk fungsi pekerjaan di Panduan Pengguna IAM.
- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukan ini dengan menentukan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, juga dikenal sebagai izin hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk menerapkan izin, lihat Kebijakan dan izin di IAM di Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Misalnya, Anda dapat menulis syarat kebijakan untuk menentukan bahwa semua pengajuan harus dikirim menggunakan SSL. Anda juga dapat menggunakan kondisi untuk memberi akses ke tindakan layanan jika digunakan melalui Layanan AWS yang spesifk, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Syarat di Panduan Pengguna IAM.
- Menggunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda guna memastikan izin yang aman dan berfungsi – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang

dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat validasi kebijakan Analizer Akses IAM di Panduan Pengguna IAM.

- Wajibkan autentikasi multi-faktor (MFA) – Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Akun AWS Anda, aktifkan MFA untuk keamanan tambahan. Untuk mewajibkan MFA saat operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Mengonfigurasi akses API yang dilindungi MFA di Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat Praktik terbaik keamanan di IAM di Panduan Pengguna IAM.

Menggunakan konsol Tag Editor dan Resource Groups Tagging API

Untuk mengakses konsol Editor Tag dan Resource Groups Tagging API, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang tag yang dilampirkan ke sumber daya di AndaAkun AWS. Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, perintah konsol dan API tidak akan berfungsi sebagaimana dimaksudkan untuk prinsipal IAM dengan kebijakan tersebut.

Untuk memastikan bahwa prinsipal tersebut masih dapat menggunakan Editor Tag, lampirkan kebijakan berikut (atau kebijakan yang berisi izin yang tercantum dalam kebijakan berikut) ke entitas. Untuk informasi selengkapnya, lihat Menambahkan izin ke pengguna dalam Panduan Pengguna IAM:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "tag:GetResources",
        "tag:TagResources",
        "tag:UntagResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "resource-explorer:List*"
      ],
      "Resource": "*"
    }
  ]
}
```

Untuk informasi selengkapnya tentang pemberian akses ke Editor Tag dan Resource Groups Tagging API, lihat. Memberikan izin untuk menggunakan Editor Tag

Izinkan pengguna melihat izin mereka sendiri

Contoh ini menunjukkan cara membuat kebijakan yang mengizinkan para pengguna IAM melihat kebijakan inline dan terkelola yang dilampirkan ke identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan pada konsol atau menggunakan AWS CLI atau AWS API secara terprogram.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Melihat grup berdasarkan tag

Anda dapat menggunakan kondisi dalam kebijakan berbasis identitas untuk mengontrol akses ke sumber daya Editor Tag berdasarkan tag. Contoh ini menunjukkan cara Anda membuat kebijakan yang memungkinkan melihat sumber daya, dalam contoh ini, grup sumber daya. Namun, izin diberikan hanya jika tag grup `project` memiliki nilai yang sama dengan `project` tag yang dilampirkan pada prinsipal panggilan.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "resource-groups:ListGroups",
            "Resource": "arn:aws:resource-groups::region:account_ID:group/group_name"
        },
        {
            "Effect": "Allow",
            "Action": "resource-groups:ListGroups",
            "Resource": "arn:aws:resource-groups::region:account_ID:group/group_name",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/project": "${aws:PrincipalTag/
project}"}
            }
        }
    ]
}
```

Anda dapat melampirkan kebijakan ini ke pengguna di akun Anda. Jika pengguna dengan kunci tag `project` dan nilai tag `alpha` mencoba untuk melihat grup sumber daya, grup juga harus diberi tag`project=alpha`. Jika tidak, pengguna ditolak aksesnya. Kunci tanda syarat `project` sama dengan kedua `Project` dan `project` karena nama kunci syarat tidak terpengaruh huruf besar/kecil. Untuk informasi selengkapnya, lihat Elemen kebijakan IAM JSON: Syarat dalam Panduan Pengguna IAM.

Pemecahan Masalah identitas dan akses Editor Tag

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan Editor Tag dan IAM.

Topik

- Saya tidak berwenang untuk melakukan tindakan di Editor Tag
- Saya tidak berwenang untuk melakukan iam: PassRole

Saya tidak berwenang untuk melakukan tindakan di Editor Tag

Jika AWS Management Console memberi tahu bahwa Anda tidak diberi otorisasi untuk melakukan tindakan, Anda harus menghubungi administrator untuk mendapatkan bantuan. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Contoh kesalahan berikut terjadi ketika pengguna `mateojackson` mencoba menggunakan konsol untuk melihat tag pada sumber daya tetapi tidak memiliki `tag:GetTagKeys` izin.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 tag:GetTagKeys on resource: arn:aws:resource-groups::us-west-2:123456789012:resource-
type/my-test-resource
```

Dalam hal ini, Mateo meminta administratornya untuk memperbarui kebijakannya untuk mengizinkan dia mengakses sumber daya `my-test-resource` menggunakan tindakan `tag:GetTagKeys`.

Saya tidak berwenang untuk melakukan iam: PassRole

Jika Anda menerima kesalahan yang tidak diizinkan untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran ke Editor Tag.

Sebagian Layanan AWS mengizinkan Anda untuk memberikan peran yang sudah ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait-layanan. Untuk melakukan tindakan tersebut, Anda harus memiliki izin untuk memberikan peran pada layanan tersebut.

Contoh kesalahan berikut terjadi ketika pengguna IAM bernama `marymajor` mencoba menggunakan konsol untuk melakukan tindakan di Editor Tag. Namun, tindakan tersebut memerlukan layanan untuk mendapatkan izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut pada layanan.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dalam kasus ini, kebijakan Mary harus diperbarui agar dia mendapatkan izin untuk melakukan tindakan `iam:PassRole` tersebut.

Jika Anda membutuhkan bantuan, hubungi administrator AWS Anda. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

Pencatatan dan pemantauan di Editor Tag

Semua tindakan Editor Tag masukAWS CloudTrail.

Logging Panggilan API Editor Tag dengan CloudTrail

Tag Editor terintegrasi denganAWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau Layanan AWS dalam Editor Tag. CloudTrail menangkap semua panggilan API untuk Tag Editor sebagai peristiwa, termasuk panggilan dari konsol Editor Tag dan dari panggilan kode ke Resource Groups Tagging API. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara terus menerus ke bucket Amazon S3, termasuk peristiwa untuk Editor Tag. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuat untuk Editor Tag, alamat IP dari mana permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Untuk informasi selengkapnya CloudTrail, lihat Panduan AWS CloudTrail Pengguna.

Informasi Editor Tag di CloudTrail

CloudTrail diaktifkan pada Akun AWS saat Anda membuat akun. Saat aktivitas terjadi di Editor Tag, atau di konsol Editor Tag, aktivitas tersebut direkam dalam suatu CloudTrail peristiwa bersama dengan Layanan AWS peristiwa lain dalam riwayat Peristiwa. Anda dapat melihat, mencari, dan mengunduh peristiwa terbaru di Akun AWS Anda. Untuk informasi selengkapnya, lihat Melihat peristiwa dengan Riwayat CloudTrail acara.

Untuk catatan acara yang sedang berlangsung di AndaAkun AWS, termasuk acara untuk Editor Tag, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di konsol, jejak tersebut berlaku untuk semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di partisi AWS dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi lainnya Layanan AWS untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat sumber daya berikut:

- Membuat jejak untuk Akun AWS Anda

- CloudTraillayanan dan integrasi yang didukung
- Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail
- Menerima file CloudTrail log dari beberapa Wilayah dan Menerima file CloudTrail log dari beberapa akun

Semua tindakan Editor Tag dicatat oleh CloudTrail dan didokumentasikan dalam Referensi API Editor Tag. Tindakan Editor Tag di konsol dicatat oleh CloudTrail, dan ditampilkan sebagai peristiwa dengan `tagging.amazonaws.com` a`eventSource`.

Setiap peristiwa atau entri log berisi informasi tentang siapa yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan berikut:

- Apakah permintaan dibuat dengan kredensial akar atau pengguna IAM.
- Apakah permintaan dibuat dengan kredensial keamanan sementara untuk suatu peran atau pengguna gabungan.
- Apakah permintaan tersebut dibuat oleh Layanan AWS lain.

Untuk informasi selengkapnya, lihat elemen CloudTrail `userIdentity`.

Memahami entri file log Editor Tag

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Sebuah peristiwa mewakili satu permintaan dari sumber apa pun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, sehingga file tersebut tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan tindakan`TagResources`.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-1661372702",
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-1661372702",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
```

```
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/cli-role",
                "accountId": "123456789012",
                "userName": "cli-role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-24T20:25:03Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-08-24T20:27:14Z",
    "eventSource": "tagging.amazonaws.com",
    "eventName": "TagResources",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "72.21.198.65",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resourcegroupstaggingapi.tag-resources",
    "requestParameters": {
        "resourceARNList": [
            "arn:aws:events:us-east-1:123456789012:rule/SecretsManagerMonitorRule"
        ],
        "tags": {
            "owner": "alice"
        }
    },
    "responseElements": {
        "failedResourcesMap": {}
    },
    "requestID": "8f9ea891-4125-460c-802f-26c11EXAMPLE",
    "eventID": "b2c9322a-aad7-424b-8f0b-423daEXAMPLE",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "tagging.us-east-1.amazonaws.com"
```

```
    }
}
```

Validasi kepatuhan untuk Editor Tag

Untuk mempelajari apakah an Layanan AWS berada dalam lingkup program kepatuhan tertentu, lihat Layanan AWS di Lingkup oleh Program Kepatuhan Layanan AWS dan pilih program kepatuhan yang Anda minati. Untuk informasi umum, lihat Program AWS Kepatuhan Program AWS .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Mengunduh Laporan di AWS Artifact .

Tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- Panduan Memulai Cepat Keamanan dan Kepatuhan — Panduan penerapan ini membahas pertimbangan arsitektur dan memberikan langkah-langkah untuk menerapkan lingkungan dasar AWS yang berfokus pada keamanan dan kepatuhan.
- Arsitektur untuk HIPAA Keamanan dan Kepatuhan di Amazon Web Services — Whitepaper ini menjelaskan bagaimana perusahaan dapat menggunakan AWS untuk membuat HIPAA aplikasi yang memenuhi syarat.

  > **Note**
  >
  > Tidak semua Layanan AWS HIPAA memenuhi syarat. Untuk informasi selengkapnya, lihat Referensi Layanan yang HIPAA Memenuhi Syarat.

- AWS Sumber Daya AWS — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- AWS Panduan Kepatuhan Pelanggan - Memahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan Layanan AWS dan memetakan panduan untuk kontrol keamanan di berbagai kerangka kerja (termasuk Institut Standar dan Teknologi Nasional (NIST), Dewan Standar Keamanan Industri Kartu Pembayaran (PCI), dan Organisasi Internasional untuk Standardisasi ()). ISO
- Mengevaluasi Sumber Daya dengan Aturan dalam Panduan AWS Config Pengembang — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.

- AWS Security Hub— Ini Layanan AWS memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS. Security Hub menggunakan kontrol keamanan untuk sumber daya AWS Anda serta untuk memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat Referensi kontrol Security Hub.
- Amazon GuardDuty — Ini Layanan AWS mendeteksi potensi ancaman terhadap beban kerja Akun AWS, kontainer, dan data Anda dengan memantau lingkungan Anda untuk aktivitas yang mencurigakan dan berbahaya. GuardDuty dapat membantu Anda mengatasi berbagai persyaratan kepatuhan, seperti PCIDSS, dengan memenuhi persyaratan deteksi intrusi yang diamanatkan oleh kerangka kerja kepatuhan tertentu.
- AWS Audit ManagerIni Layanan AWS membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

Ketahanan dalam Editor Tag

Editor Tag melakukan pencadangan otomatis ke sumber daya layanan internal. Cadangan ini tidak dapat dikonfigurasi pengguna. Cadangan dienkripsi, baik saat istirahat maupun dalam perjalanan. Tag Editor menyimpan data pelanggan di Amazon DynamoDB.

Infrastruktur global AWS dibangun di sekitar Wilayah AWS dan Availability Zone. Wilayah AWS menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi yang terhubung dengan jaringan latensi rendah, throughput tinggi, dan jaringan yang sangat berlebihan. Dengan Availability Zone, Anda dapat merancang dan mengoperasikan aplikasi dan basis data yang secara otomatis melakukan failover di antara Availability Zone tanpa gangguan. Zona Ketersediaan lebih sangat tersedia, lebih toleran kesalahan, dan lebih dapat diskalakan daripadai infrastruktur pusat data tunggal atau multi tradisional.

Jika Anda menghapus tag secara tidak sengaja, hubungi AWS SupportPusat.

Untuk informasi selengkapnya tentang Wilayah AWS dan Availability Zone, lihat Infrastruktur Global AWS.

Keamanan infrastruktur di Editor Tag

Tag Editor tidak menyediakan cara tambahan untuk mengisolasi layanan atau lalu lintas jaringan. Jika berlaku, gunakan isolasi AWS khusus. Anda dapat menggunakan Tag Editor API dan konsol di virtual private cloud (VPC) untuk membantu memaksimalkan privasi dan keamanan infrastruktur.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses Editor Tag melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Pengangkutan (TLS). Kami membutuhkan TSL 1.2 dan merekomendasikan TSL 1.3.
- Sandi cocok dengan sistem kerahasiaan maju sempurna (perfect forward secrecy, PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani menggunakan access key ID dan secret access key yang terkait dengan prinsipal AWS Identity and Access Management (IAM). Atau, Anda dapat menggunakan AWS Security Token Service(AWS STS) untuk menghasilkan kredenal keamanan sementara untuk menandatangani permintaan.

Editor Tag tidak mendukung kebijakan berbasis sumber daya.

Anda dapat memanggil operasi API Editor Tag dari lokasi jaringan mana pun, tetapi Editor Tag mendukung kebijakan akses berbasis sumber daya, yang dapat mencakup pembatasan berdasarkan alamat IP sumber. Anda juga dapat menggunakan kebijakan Editor Tag untuk mengontrol akses dari titik akhir Amazon Virtual Private Cloud (Amazon VPC) tertentu atau VPC tertentu. Secara efektif, pendekatan ini mengisolasi akses jaringan ke sumber daya tertentu hanya dari VPC tertentu dalam AWS jaringan.

Kuota layanan

Tabel berikut memberikan informasi tentang kuota layanan untuk Tag Editor.

Kuota ini saat ini tidak dapat disesuaikan menggunakan konsol Service Quotas. Hubungi AWS Support.

Nama	Default
Tag terlampir per sumber daya	50 tag yang ditentukan pengguna (tag AWS yang dihasilkan tidak dihitung terhadap batas ini.)
Tag nama kunci	Minimal 1, maksimum 128 karakter Unicode di UTF -8. Karakter yang diizinkan termasuk huruf, angka, spasi, dan karakter berikut: `_ . : / = + - @` Nama kunci tidak dapat dimulai `aws:` karena awalan itu dicadangkan untuk AWS digunakan. **Note** Beberapa Layanan AWS memiliki beberapa karakter tambahan atau batasan panjang. Untuk detailnya, lihat

Nama	Default
	dokumentasi untuk layanan tertentu.
Nilai tag	Minimal 0, maksimal 256 karakter Unicode di UTF -8. Karakter yang diizinkan termasuk huruf, angka, spasi, dan karakter berikut: `_ . : / = + - @` **Note** Beberapa Layanan AWS memiliki beberapa karakter tambahan atau batasan panjang. Untuk detailnya, lihat dokumentasi untuk layanan tertentu.
Tingkat panggilan GetResourcesAPIoperasi	Maksimal 15 panggilan per detik
Tingkat panggilan API operasi berikut: • TagResources • UntagResources • GetTagKeys • GetTagValues	Maksimal 5 panggilan per detik

Sejarah dokumen Editor Tag

Perubahan	Deskripsi	Tanggal
Izin yang diperbarui untuk mengevaluasi kepatuhan seluruh organisasi	Memperbarui Izin untuk mengevaluasi kepatuhan di seluruh organisasi untuk menyertakan izin yang membantu mengakses laporan kepatuhan.	Agustus 28, 2024
Konten yang diperbarui	Judul topik yang diperbaru i dan konten yang direorgan isasi untuk meningkatkan keterbacaan dan kemampuan ditemukan.	Juli 25, 2024
Menandai konten dari Referensi Umum AWS pindah ke panduan ini	Topik tentang menandai Anda AWS Sumber daya dipindahk an dari Referensi Umum AWS untuk panduan ini.	24 Maret 2023
IAMpembaruan praktik terbaik	Panduan yang diperbarui untuk menyelaraskan dengan praktik IAM terbaik. Untuk informasi selengkapnya, lihat Praktik terbaik keamanan di IAM.	Januari 3, 2023
Memindahkan dokumentasi Editor Tag ke panduannya sendiri	Dokumentasi Editor Tag sekarang disediakan dalam panduan penggunanya sendiri alih-alih menjadi bagian dari AWS Resource Groups Panduan Pengguna.	13 Desember 2022

Periksa kepatuhan dengan kebijakan tag	Setelah Anda membuat dan melampirkan kebijakan tag ke akun menggunakan AWS Organizations, Anda dapat menemukan tag yang tidak sesuai pada sumber daya di akun organisasi Anda.	26 November 2019
Editor Tag sekarang mendukung pencarian sumber daya yang tidak ditandai	Anda sekarang dapat mencari sumber daya di Editor Tag yang tidak memiliki nilai tag yang diterapkan untuk kunci tag tertentu.	Selasa, 18 Juni 2019
Konsol Editor Tag bergerak keluar dari AWS Systems Manager konsol	Konsol Tag Editor sekarang independen dari konsol Systems Manager. Meskipun Anda masih dapat menemukan pointer ke konsol Tag Editor di bilah navigasi kiri Systems Manager, Anda dapat membuka konsol Editor Tag langsung dari menu drop-down di kiri atas AWS Management Console.	5 Juni 2019
Alat Editor Tag lama dan lama tidak lagi tersedia	Penyebutan Editor Tag yang lebih lama, klasik, atau lama telah dihapus; alat ini tidak lagi tersedia di AWS. Gunakan Editor Tag sebagai gantinya.	14 Mei 2019

Editor Tag sekarang mendukung sumber daya penandaan di berbagai wilayah	Editor Tag sekarang memungkinkan Anda mencari dan mengelola tag sumber daya di beberapa wilayah, dengan wilayah Anda saat ini ditambahkan ke kueri sumber daya secara default.	2 Mei 2019
Editor Tag sekarang mendukung mengekspor hasil kueri ke CSV	Anda dapat mengekspor hasil kueri pada halaman Temukan Sumber Daya untuk menandai ke file yang CSV diformat. Kolom Region baru ditampilk an dalam hasil query Editor Tag. Tag Editor sekarang memungkinkan Anda mencari sumber daya yang memiliki nilai kosong untuk kunci tag tertentu. Tandai nilai kunci pelengkapan otomatis saat Anda mengetik nilai unik di antara kunci yang ada.	2 April 2019

Tag Editor sekarang mendukung penambahan semua jenis sumber daya ke kueri	Anda dapat menerapkan tag hingga 20 jenis sumber daya individual dalam satu operasi, atau Anda dapat memilih Semua jenis sumber daya untuk menanyakan semua jenis sumber daya di suatu wilayah. Pelengkapan otomatis telah ditambahkan ke bidang kunci Tag kueri untuk membantu mengaktifkan kunci tag yang konsisten di antara sumber daya. Jika perubahan tag gagal pada beberapa sumber daya, Anda dapat mencoba lagi perubahan tag hanya pada sumber daya yang perubahan tag gagal.	19 Maret 2019
Tag Editor sekarang mendukung beberapa jenis sumber daya dalam pencarian	Anda dapat menerapkan tag hingga 20 jenis sumber daya dalam satu operasi. Anda juga dapat memilih kolom yang ditampilkan kepada Anda di hasil penelusuran, termasuk kolom untuk setiap kunci tag unik yang ditemukan di hasil penelusuran atau sumber daya yang dipilih dari hasil.	26 Februari 2019

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