aws

Panduan Administrasi

Amazon Detective

Amazon Detective: Panduan Administrasi

Table of Contents

Apa itu Amazon Detective?

Amazon Detective membantu Anda menganalisis, menyelidiki, dan mengidentifikasi akar masalah temuan keamanan atau aktivitas yang mencurigakan. Detective secara otomatis mengumpulkan data log dariAWS sumber daya Anda. Kemudian menggunakan pembelajaran mesin, analisis statistik, dan teori grafik untuk menghasilkan visualisasi yang membantu Anda melakukan investigasi keamanan yang lebih cepat dan lebih efisien. Agregasi, ringkasan, dan konteks Detective membantu Anda menganalisis dan menentukan sifat dan tingkat kemungkinan masalah keamanan.

Dengan Detective, Anda dapat mengakses hingga satu tahun data peristiwa historis. Data ini tersedia melalui sekumpulan visualisasi yang menunjukkan perubahan jenis dan volume aktivitas pada jendela waktu yang dipilih. Detective menghubungkan perubahan ini dengan GuardDuty temuan. Untuk informasi lebih lanjut tentang data sumber di Detective, lihatSumber data yang digunakan dalam grafik perilaku.

Bagaimana cara kerja Detective?

Detective secara otomatis mengekstrak peristiwa berbasis waktu seperti upaya masuk, panggilan API, dan lalu lintas jaringan dariAWS CloudTrail dan log aliran Amazon VPC. Hal ini juga menelan temuan terdeteksi oleh GuardDuty.

Dari peristiwa tersebut, Detective menggunakan pembelajaran mesin dan visualisasi untuk membuat tampilan interaktif yang terpadu tentang perilaku sumber daya Anda dan interaksi di antara keduanya dari waktu ke waktu. Anda dapat menjelajahi grafik perilaku ini untuk memeriksa tindakan berbeda seperti upaya masuk yang gagal atau panggilan API yang mencurigakan. Anda juga dapat melihat bagaimana tindakan ini memengaruhi sumber daya sepertiAWS akun dan instans Amazon EC2. Anda dapat menyesuaikan cakupan dan garis waktu grafik perilaku untuk berbagai tugas:

- Dengan cepat menyelidiki aktivitas apa pun yang berada di luar norma.
- Identifikasi pola yang mungkin mengindikasikan masalah keamanan.
- Memahami semua sumber daya yang dipengaruhi oleh temuan.

Visualisasi khusus Detective memberikan dasar untuk dan meringkas informasi akun. Temuan ini dapat membantu menjawab pertanyaan seperti “Apakah ini panggilan API yang tidak biasa untuk peran ini?” Atau “Apakah lonjakan lalu lintas dari contoh ini diharapkan?”

Dengan Detective, Anda tidak perlu mengatur data apa pun atau mengembangkan, mengkonfigurasi, atau menyesuaikan kueri dan algoritme Anda sendiri. Tidak ada biaya di muka dan Anda hanya membayar untuk acara yang dianalisis, tanpa perangkat lunak tambahan untuk digunakan atau umpan lain untuk berlangganan.

Siapa yang menggunakan Detective?

Ketika akun mengaktifkan Detective, itu menjadi akun administrator untuk grafik perilaku. Grafik perilaku adalah sekumpulan data yang diekstrak dan dianalisis terkait dari satu atau lebihAWS akun. Akun administrator mengundang akun anggota untuk menyumbangkan data mereka ke grafik perilaku akun administrator.

Detective juga terintegrasi denganAWS Organizations. Akun manajemen organisasi Anda menunjuk akun administrator Detective untuk organisasi. Akun administrator Detective memungkinkan akun organisasi sebagai akun anggota dalam grafik perilaku organisasi.

Untuk informasi tentang cara Detective menggunakan data sumber dari akun grafik perilaku, lihatSumber data yang digunakan dalam grafik perilaku.

Untuk informasi tentang cara akun administrator mengelola grafik perilaku, lihatMengelola akun. Untuk informasi tentang cara akun anggota mengelola undangan grafik perilaku dan keanggotaan, lihatthe section called “Untuk akun anggota: Mengelola undangan dan keanggotaan”.

Akun administrator menggunakan analitik dan visualisasi yang dihasilkan dari grafik perilaku untuk menyelidikiAWS sumber daya dan GuardDuty temuan. Menggunakan integrasi Detective dengan GuardDuty danAWS Security Hub, Anda dapat berputar dari GuardDuty temuan di layanan ini langsung ke konsol Detective.

Investigasi Detective berfokus pada aktivitas yang terhubung keAWS sumber daya yang terlibat. Untuk ikhtisar proses investigasi di Detective, lihat Cara Amazon Detective digunakan untuk penyelidikan dalam Panduan Pengguna Detective.

Istilah dan konsep Detektif Amazon

Istilah dan konsep berikut penting untuk memahami Amazon Detective dan cara kerjanya.

Akun Administrator

Akun AWSYang memiliki grafik perilaku dan yang menggunakan grafik perilaku untuk penyelidikan.

Akun administrator mengundang akun anggota untuk menyumbangkan data mereka ke grafik perilaku. Untuk informasi selengkapnya, lihat the section called “Mengundang akun anggota ke grafik perilaku”.

Untuk grafik perilaku organisasi, akun administrator adalah akun administrator Detektif yang ditunjuk oleh akun manajemen organisasi. Untuk informasi selengkapnya, lihat the section called “Menunjuk akun administrator Detektif”. Akun administrator Detektif dapat mengaktifkan akun organisasi apa pun sebagai akun anggota dalam grafik perilaku organisasi. Untuk informasi selengkapnya, lihat the section called “Mengelola akun anggota organisasi”.

Akun administrator juga dapat melihat penggunaan data untuk grafik perilaku, dan menghapus akun anggota dari grafik perilaku.

Organisasi Sistem Otonomi (ASO)

Organisasi berjudul yang ditugaskan sistem otonom. Sistem otonom ini adalah jaringan heterogen atau seperangkat jaringan yang menggunakan logika dan kebijakan perutean yang serupa.

Grafik perilaku

Kumpulan data terkait yang dihasilkan dari data sumber masuk yang terkait dengan satu atau lebihAkun AWS.

Setiap grafik perilaku menggunakan struktur temuan, entitas, dan hubungan yang sama.

Akun administrator yang didelegasikan () AWS Organizations

Dalam Organisasi, akun administrator yang didelegasikan untuk suatu layanan dapat mengelola penggunaan layanan untuk organisasi.

Di Detektif, akun administrator Detektif juga merupakan akun administrator yang didelegasikan, kecuali akun administrator Detektif adalah akun manajemen organisasi. Akun manajemen organisasi tidak dapat berupa akun administrator yang didelegasikan.

Di Detektif, delegasi diri diperbolehkan. Akun manajemen organisasi dapat mendelegasikan akun mereka sendiri untuk menjadi administrator delegasi Detektif tetapi ini akan terdaftar atau diingat hanya dalam lingkup Detektif dan bukan organisasi.

Akun administrator detektif

Akun yang ditunjuk oleh akun manajemen organisasi menjadi akun administrator untuk grafik perilaku organisasi di Wilayah. Untuk informasi selengkapnya, lihat the section called “Menunjuk akun administrator Detektif”.

Detektif merekomendasikan bahwa akun manajemen organisasi memilih akun selain akun mereka.

Jika akun bukan akun manajemen organisasi, maka akun administrator Detektif juga merupakan akun administrator yang didelegasikan untuk Detektif dalam Organisasi.

Data sumber detektif

Versi informasi yang diproses dan terstruktur dari jenis umpan berikut:

- Log dari AWS layanan, seperti AWS CloudTrail log dan Amazon VPC Flow Logs
- Temuan GuardDuty

Detektif menggunakan data sumber Detektif untuk mengisi grafik perilaku. Detektif juga menyimpan salinan data sumber Detektif untuk mendukung analitiknya.

Entitas

Item yang diekstrak dari data yang dicerna.

Setiap entitas memiliki tipe, yang mengidentifikasi jenis objek yang diwakilinya. Contoh jenis entitas termasuk alamat IP, instans Amazon EC2, dan AWS pengguna.

Entitas dapat berupa AWS sumber daya yang Anda kelola, atau alamat IP eksternal yang telah berinteraksi dengan sumber daya Anda.

Untuk setiap entitas, data sumber juga digunakan untuk mengisi properti entitas. Nilai properti dapat diekstraksi langsung dari catatan sumber atau digabungkan di beberapa catatan.

Menemukan

Masalah keamanan yang terdeteksi oleh AmazonGuardDuty.

Menemukan kelompok

Kumpulan temuan, entitas, dan bukti terkait yang mungkin terkait dengan peristiwa atau masalah keamanan yang sama. Detektif menghasilkan kelompok temuan berdasarkan model pembelajaran mesin bawaan.

Bukti detektif

Detektif mengidentifikasi bukti tambahan yang terkait dengan kelompok temuan berdasarkan data dalam grafik perilaku Anda yang dikumpulkan dalam 45 hari terakhir. Bukti ini disajikan sebagai temuan dengan nilai keparahan Informasi. Bukti menyediakan informasi pendukung yang menyoroti aktivitas yang tidak biasa atau perilaku yang tidak diketahui yang berpotensi mencurigakan bila dilihat dalam kelompok temuan. Contoh dari ini mungkin geolokasi baru diamati atau panggilan API diamati dalam waktu lingkup temuan. Pada saat ini, temuan ini hanya dapat dilihat di Detektif dan tidak dikirim ke Security Hub.

Menemukan ikhtisar

Satu halaman yang menyediakan ringkasan informasi tentang temuan.

Ikhtisar temuan berisi daftar entitas yang terlibat untuk temuan. Dari daftar, Anda dapat berputar ke profil untuk entitas.

Ikhtisar temuan juga berisi panel detail yang berisi atribut temuan.

Entitas volume tinggi

Entitas yang memiliki koneksi ke atau dari sejumlah besar entitas lain selama interval waktu. Misalnya, instans EC2 mungkin memiliki koneksi dari jutaan alamat IP. Jumlah koneksi melebihi ambang batas yang dapat diakomodasi oleh Detektif.

Ketika waktu lingkup saat ini berisi interval waktu volume tinggi, Detektif memberi tahu pengguna.

Untuk informasi selengkapnya, lihat Melihat detail untuk entitas volume tinggi di Panduan Pengguna Amazon Detective.

Investigasi

Proses triaging aktivitas mencurigakan atau menarik, menentukan ruang lingkup, sampai ke sumber atau penyebab yang mendasarinya, dan kemudian menentukan bagaimana untuk melanjutkan.

Akun Anggota

Akun administrator Akun AWS yang diundang untuk menyumbangkan data ke grafik perilaku. Dalam grafik perilaku organisasi, akun anggota dapat berupa akun organisasi yang diaktifkan akun administrator Detektif sebagai akun anggota.

Akun anggota yang diundang dapat menanggapi undangan grafik perilaku dan menghapus akun mereka dari grafik perilaku. Untuk informasi selengkapnya, lihat the section called “Untuk akun anggota: Mengelola undangan dan keanggotaan”.

Akun organisasi tidak dapat mengubah keanggotaannya dalam grafik perilaku organisasi.

Semua akun anggota juga dapat melihat informasi penggunaan untuk akun mereka di seluruh grafik perilaku tempat mereka menyumbangkan data.

Mereka tidak memiliki akses lain ke grafik perilaku.

Grafik perilaku organisasi

Grafik perilaku yang dimiliki oleh akun administrator Detektif. Akun manajemen organisasi menunjuk akun administrator Detektif. Untuk informasi selengkapnya, lihat the section called “Menunjuk akun administrator Detektif”.

Dalam grafik perilaku organisasi, akun administrator Detektif mengontrol apakah akun organisasi adalah akun anggota. Akun organisasi tidak dapat menghapus dirinya sendiri dari grafik perilaku organisasi.

Akun administrator Detektif juga dapat mengundang akun lain ke grafik perilaku organisasi.

Profil

Satu halaman yang menyediakan kumpulan visualisasi data yang terkait dengan aktivitas untuk entitas.

Untuk temuan, profil membantu analis untuk menentukan apakah temuan tersebut menjadi perhatian tulus atau positif palsu.

Profil memberikan informasi untuk mendukung penyelidikan terhadap temuan atau untuk perburuan umum untuk aktivitas yang mencurigakan.

Panel profil

Sebuah visualisasi tunggal pada profil. Setiap panel profil dimaksudkan untuk membantu menjawab pertanyaan atau pertanyaan tertentu untuk membantu analis dalam penyelidikan.

Panel profil dapat berisi pasangan nilai kunci, tabel, garis waktu, diagram batang, atau bagan geolokasi.

Hubungan

Aktivitas yang terjadi antara entitas individu. Hubungan juga diekstraksi dari data sumber yang masuk.

Mirip dengan entitas, hubungan memiliki tipe, yang mengidentifikasi jenis entitas yang terlibat dan arah koneksi. Contoh jenis relasi adalah alamat IP yang terhubung ke instans Amazon EC2.

Waktu lingkup

Jendela waktu yang digunakan untuk lingkup data yang ditampilkan pada profil.

Waktu lingkup default untuk temuan mencerminkan kali pertama dan terakhir ketika aktivitas mencurigakan diamati.

Waktu lingkup default untuk profil entitas adalah 24 jam sebelumnya.

Wilayah dan kuota Amazon Detective

Ketika menggunakan Amazon Detective, menyadari kuota ini.

Wilayah Detective dan titik akhir

Untuk melihat daftarWilayah AWS tempat Detective tersedia, lihat endpoint layanan Detective.

kuota Detective

Detective memiliki kuota berikut, yang tidak dapat dikonfigurasi.

Resource	Kuota	Comments
Jumlah akun anggota	1.200	Jumlah akun anggota yang dapat ditambahkan akun administrator ke grafik perilaku.
Volume data grafik perilaku — peringatan volume	9 TB per hari	Jika volume data grafik perilaku lebih besar dari 9 TB per hari, maka Detective menampilkan peringatan bahwa grafik perilaku mendekati volume maksimum yang diizinkan.
Volume data grafik perilaku — tidak ada akun baru	10 TB per hari	Jika volume data grafik perilaku lebih besar dari 10 TB per hari, maka Anda tidak dapat menambahkan akun anggota baru ke grafik perilaku.
Volume data grafik perilaku - hentikan penyerapan data ke dalam grafik perilaku	15 TB per hari	Jika volume data grafik perilaku lebih besar dari 15 TB per hari, maka Detective berhenti menelan data ke dalam grafik perilaku. 15 TB per hari mencerminkan volume data normal dan lonjakan volume data.

Resource	Kuota	Comments
		Untuk mengaktifkan kembali penyerapan data, Anda harus menghubungiAWS Support.

Internet Explorer 11 tidak didukung

Anda tidak dapat menggunakan Detective dengan Internet Explorer 11.

Menyiapkan Detektif Amazon

Saat Anda mengaktifkan Detektif Amazon, Detektif membuat grafik perilaku khusus Wilayah yang memiliki akun Anda sebagai akun administratornya. Ini awalnya satu-satunya akun dalam grafik perilaku. Akun administrator kemudian dapat mengundang AWS akun lain untuk menyumbangkan data mereka ke grafik perilaku. Lihat Mengelola akun.

Mengaktifkan Detective in a Region untuk pertama kalinya juga memulai uji coba gratis 30 hari untuk grafik perilaku. Jika akun menonaktifkan Detective dan kemudian mengaktifkannya lagi, tidak ada uji coba gratis yang tersedia. Lihat Tentang uji coba gratis untuk grafik perilaku.

Setelah uji coba gratis, setiap akun dalam grafik perilaku ditagih untuk data yang mereka kontribusikan. Akun administrator dapat melacak penggunaan dan melihat total biaya yang diproyeksikan untuk periode 30 hari tipikal untuk seluruh grafik perilaku mereka. Untuk informasi selengkapnya, lihat the section called “Penggunaan dan biaya akun administrator”. Akun anggota dapat melacak penggunaan dan biaya yang diproyeksikan untuk grafik perilaku yang mereka miliki. Untuk informasi selengkapnya, lihat the section called “Pelan”.

Daftar Isi

Prasyarat dan rekomendasi Detektif Amazon

Sebelum Anda dapat mengaktifkan Amazon Detective, Anda harus memiliki file. Akun AWS

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/signup.
2. Ikuti petunjuk secara online.

   Anda akan diminta untuk menerima panggilan telepon dan memasukkan kode verifikasi pada keypad telepon sebagai bagian dari prosedur pendaftaran.

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

AWS mengirimi Anda email konfirmasi setelah proses pendaftaran selesai. Anda dapat melihat aktivitas akun saat ini dan mengelola akun dengan mengunjungi https://aws.amazon.com/ dan memilih Akun Saya.

Membuat pengguna administratif

Setelah Anda mendaftar Akun AWS, amankan 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 alamat Akun AWS email Anda. Di halaman berikutnya, masukkan kata sandi Anda.

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

   Untuk petunjuk, lihat Mengaktifkan perangkat MFA virtual untuk pengguna Akun AWS root (konsol) Anda di Panduan Pengguna IAM.

Membuat pengguna administratif

1. Aktifkan Pusat Identitas IAM.

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

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

Masuk sebagai pengguna administratif

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

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

Anda juga perlu mengetahui persyaratan dan rekomendasi berikut.

AWS Command Line Interface Versi yang didukung

Untuk menggunakan AWS CLI to melakukan tugas Detective, versi minimum yang diperlukan adalah 1.16.303.

Direkomendasikan penyelarasan dengan GuardDuty dan AWS Security Hub

Jika Anda terdaftar GuardDuty dan AWS Security Hub, kami menyarankan agar akun Anda menjadi akun administrator untuk layanan tersebut. Jika akun administrator sama untuk ketiga layanan, maka poin integrasi berikut bekerja dengan mulus.

- Di GuardDuty atau Security Hub, saat melihat detail untuk GuardDuty temuan, Anda dapat beralih dari detail temuan ke profil pencarian Detektif.
- Di Detektif, saat menyelidiki GuardDuty temuan, Anda dapat memilih opsi untuk mengarsipkan temuan itu.

Jika Anda memiliki akun administrator GuardDuty dan Security Hub yang berbeda, sebaiknya Anda menyelaraskan akun administrator berdasarkan layanan yang lebih sering Anda gunakan.

- Jika Anda menggunakan GuardDuty lebih sering, maka aktifkan Detective menggunakan akun GuardDuty administrator.

  Jika Anda menggunakan AWS Organizations untuk mengelola akun, tetapkan akun GuardDuty administrator sebagai akun administrator Detektif untuk organisasi.
- Jika Anda lebih sering menggunakan Security Hub, aktifkan Detective menggunakan akun administrator Security Hub.

Jika Anda menggunakan Organizations untuk mengelola akun, tetapkan akun administrator Security Hub sebagai akun administrator Detektif untuk organisasi.

Jika Anda tidak dapat menggunakan akun administrator yang sama di semua layanan, maka setelah mengaktifkan Detective, Anda dapat membuat peran lintas akun secara opsional. Peran ini memberikan akses akun administrator ke akun lain.

Untuk informasi tentang cara IAM mendukung jenis peran ini, lihat Menyediakan akses ke pengguna IAM di AWS akun lain yang Anda miliki di Panduan Pengguna IAM.

Memberikan izin Detektif yang diperlukan

Sebelum Anda dapat mengaktifkan Detektif, Anda harus memastikan bahwa kepala IAM Anda memiliki izin Detektif yang diperlukan. Prinsipal dapat berupa pengguna atau peran yang sudah Anda gunakan, atau Anda dapat membuat pengguna atau peran baru yang akan digunakan untuk Detektif.

Saat Anda mendaftar ke Amazon Web Services (AWS), akun Anda secara otomatis mendaftar untuk semua Layanan AWS, termasuk Amazon Detective. Namun, untuk mengaktifkan dan menggunakan Detektif, pertama-tama Anda harus menyiapkan izin yang memungkinkan Anda mengakses konsol Detektif Amazon dan operasi API. Anda atau administrator Anda dapat melakukan ini dengan menggunakan AWS Identity and Access Management (IAM) untuk melampirkan kebijakan `AmazonDetectiveFullAccess` terkelola ke kepala IAM Anda, yang memberikan akses ke semua tindakan Detektif.

Pembaruan yang disarankan untuk frekuensi GuardDuty CloudWatch notifikasi

Di GuardDuty, detektor dikonfigurasi dengan frekuensi CloudWatch notifikasi Amazon untuk melaporkan kejadian temuan berikutnya. Ini termasuk mengirim notifikasi ke Detektif.

Secara default, frekuensinya enam jam. Ini berarti bahwa bahkan jika temuan berulang kali, kejadian baru tidak tercermin dalam Detektif sampai enam jam kemudian.

Untuk mengurangi jumlah waktu yang dibutuhkan Detektif untuk menerima pembaruan ini, kami menyarankan agar akun GuardDuty administrator mengubah pengaturan pada detektor mereka menjadi 15 menit. Perhatikan bahwa mengubah konfigurasi tidak berpengaruh pada biaya penggunaan GuardDuty.

Untuk informasi tentang menyetel frekuensi notifikasi, lihat Memantau GuardDuty Temuan dengan CloudWatch Acara Amazon di Panduan GuardDuty Pengguna Amazon.

Mengaktifkan Detektif Amazon

Ketika Anda mengaktifkan Detektif, Anda menunjuk akun administrator Detektif dan mengundang akun lain untuk menjadi akun anggota. Hubungan administrator-anggota terbentuk ketika akun calon anggota menerima undangan. Untuk detail selengkapnya, lihat Mengelola akun.

Dalam grafik perilaku organisasi, akun administrator Detektif mengelola keanggotaan grafik perilaku untuk semua akun organisasi. Untuk informasi selengkapnya tentang cara mengelola akun administrator Detektif, lihat Menunjuk akun administrator Detektif untuk organisasi.

Anda dapat mengaktifkan Detective dari konsol Detective, Detective API, atau. AWS Command Line Interface

Anda hanya dapat mengaktifkan Detektif sekali di setiap Wilayah. Jika Anda sudah menjadi akun administrator untuk grafik perilaku di Wilayah, maka Anda tidak dapat mengaktifkan Detektif lagi di Wilayah tersebut.

Mengaktifkan Detektif (Konsol)

Anda dapat mengaktifkan Amazon Detective dari file. AWS Management Console

Untuk mengaktifkan Detective (konsol)

1. Masuk ke AWS Management Console. Kemudian buka konsol Detective di https://console.aws.amazon.com/detective/.
2. Pilih Mulai.
3. Pada halaman Aktifkan Detektif Amazon, Align akun administrator (disarankan) menjelaskan rekomendasi untuk menyelaraskan akun administrator antara Detektif dan Amazon dan. GuardDuty AWS Security Hub Lihat the section called “Direkomendasikan penyelarasan dengan GuardDuty dan AWS Security Hub”.
4. Tombol Lampirkan kebijakan IAM membawa Anda langsung ke konsol IAM dan membuka kebijakan yang disarankan, Anda memiliki opsi untuk melampirkan kebijakan yang disarankan ke kepala sekolah yang Anda gunakan untuk Detektif. Jika Anda tidak memiliki izin untuk beroperasi di konsol IAM, dalam izin yang diperlukan, Anda dapat menyalin kebijakan Nama Sumber

Daya Amazon (ARN) untuk memberikannya kepada administrator IAM Anda. Mereka dapat melampirkan kebijakan atas nama Anda.

Konfirmasikan bahwa kebijakan IAM yang diperlukan sudah ada.

5. Bagian Tambahkan tag memungkinkan Anda menambahkan tag ke grafik perilaku.

   Untuk menambahkan tanda, lakukan hal berikut:

   a. Pilih Tambahkan tanda baru.
   b. Untuk Kunci, masukkan nama tag.
   c. Untuk Nilai, masukkan nilai tag.

   Untuk menghapus tag, pilih opsi Hapus untuk tag itu.

6. Pilih Aktifkan Detektif Amazon.
7. Setelah mengaktifkan Detektif, Anda dapat mengundang akun anggota ke grafik perilaku Anda.

   Untuk menavigasi ke halaman Manajemen akun, pilih Tambahkan anggota sekarang. Untuk informasi tentang mengundang akun anggota, lihatthe section called “Mengundang akun anggota ke grafik perilaku”.

Mengaktifkan Detektif (Detective API,) AWS CLI

Anda dapat mengaktifkan Amazon Detective dari Detective API atau file. AWS Command Line Interface

Untuk mengaktifkan Detective (Detective API,) AWS CLI

- Detective API: Gunakan operasi. `CreateGraph`
- AWS CLI: Pada baris perintah, jalankan `create-graph`perintah.

```
aws detective create-graph --tags '{"tagName": "tagValue"}'
```

Perintah berikut memungkinkan Detektif dan menetapkan nilai `Department` tag ke. `Security`

```
aws detective create-graph --tags '{"Department": "Security"}'
```

Mengaktifkan Detektif di Seluruh Wilayah (skrip Python aktif) GitHub

Detective menyediakan skrip open-source GitHub yang melakukan hal berikut:

- Mengaktifkan Detektif untuk akun administrator dalam daftar Wilayah yang ditentukan
- Menambahkan daftar akun anggota yang disediakan ke setiap grafik perilaku yang dihasilkan
- Mengirim email undangan ke akun anggota
- Secara otomatis menerima undangan untuk akun anggota

Untuk informasi tentang cara mengkonfigurasi dan menggunakan GitHub skrip, lihatMenggunakan skrip Amazon Detective Python.

Memeriksa bahwa data sedang diekstraksi

Setelah Anda mengaktifkan Detective, Detective mulai menyerap dan mengekstrak data dari AWS akun Anda ke dalam grafik perilaku Anda.

Untuk ekstraksi awal, data biasanya tersedia dalam grafik perilaku dalam waktu 2 jam.

Salah satu cara untuk memeriksa bahwa Detective mengekstraksi data adalah dengan mencari contoh nilai pada halaman Detective Search.

Untuk memeriksa nilai contoh pada halaman Pencarian

1. Buka konsol Amazon Detective di. https://console.aws.amazon.com/detective/
2. Di panel navigasi, pilih Cari.
3. Dari menu Pilih jenis, pilih jenis item.

   Contoh dari data Anda berisi kumpulan sampel pengidentifikasi tipe yang dipilih yang ada dalam data grafik perilaku Anda.

   Jika Anda dapat melihat nilai contoh, maka Anda tahu bahwa data sedang dicerna dan diekstraksi ke dalam grafik perilaku Anda.

Tentang uji coba gratis untuk grafik perilaku

Amazon Detective menyediakan uji coba gratis 30 hari untuk setiap akun di setiap Wilayah. Uji coba gratis untuk akun dimulai saat pertama kali salah satu tindakan berikut terjadi.

- Akun memungkinkan Detektif secara manual dan menjadi akun administrator untuk grafik perilaku.
- Akun ditetapkan sebagai akun administrator Detektif untuk organisasiAWS Organizations, dan mengaktifkan Detektif untuk pertama kalinya.
- Jika akun administrator Detektif sudah mengaktifkan Detektif sebelum mereka ditunjuk, maka akun tersebut tidak memulai uji coba gratis 30 hari baru.
- Akun menerima undangan untuk menjadi akun anggota dalam grafik perilaku dan diaktifkan sebagai akun anggota.
- Akun organisasi diaktifkan sebagai akun anggota oleh akun administrator Detektif.

Uji coba gratis berlangsung selama 30 hari sejak saat itu. Akun tidak ditagih untuk data apa pun yang diproses selama periode tersebut. Ketika masa percobaan berakhir, Detektif mulai menagih akun untuk data yang dikontribusikannya pada grafik perilaku. Untuk informasi lebih lanjut tentang bagaimana Anda dapat melacak aktivitas Detektif Anda, memantau penggunaan dan melihat proyeksi biaya lihat. Melacak tindakan dan penggunaan di Amazon Detective Untuk informasi lebih lanjut tentang harga, lihat Harga Detektif

Periode 30 hari yang sama digunakan untuk semua grafik perilaku di Wilayah. Misalnya, akun diaktifkan sebagai akun anggota untuk grafik perilaku. Ini memulai uji coba gratis 30 hari. Setelah 10 hari, akun diaktifkan untuk grafik perilaku kedua di Wilayah yang sama. Untuk grafik perilaku kedua, akun menerima 20 hari data gratis.

Uji coba gratis memberikan banyak manfaat:

- Akun administrator dapat menjelajahi fitur dan fungsionalitas Detektif untuk memverifikasi nilainya.
- Administrator dan akun anggota dapat memantau jumlah data dan perkiraan biaya sebelum Detektif mulai menagihnya untuk itu. Lihat the section called “Penggunaan dan biaya akun administrator” dan the section called “Pelan”.

Uji coba gratis untuk sumber data opsional

Detektif juga menyediakan uji coba 30 hari gratis untuk sumber data opsional. Uji coba gratis ini terpisah dari uji coba gratis yang disediakan untuk sumber data Detektif inti saat Detektif pertama kali diaktifkan.

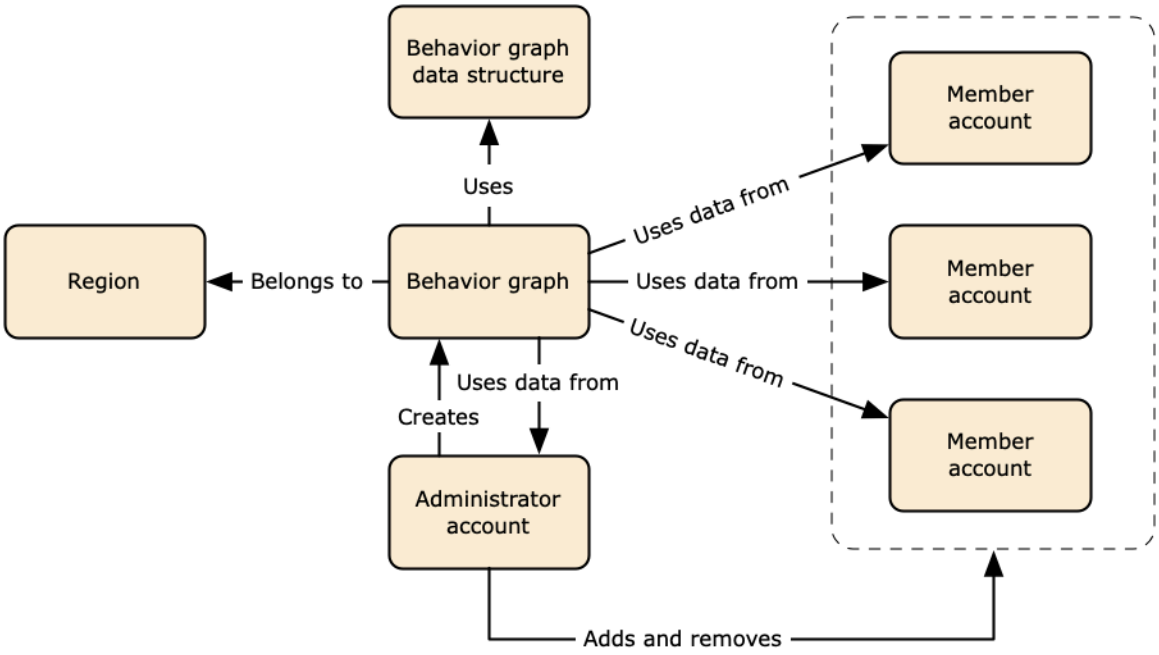
> **Note**
>
> Jika pelanggan menonaktifkan paket sumber data opsional dalam waktu 7 hari setelah mengaktifkannya, Detektif melakukan reset otomatis satu kali uji coba gratis untuk paket sumber data tersebut jika diaktifkan lagi.

Untuk mengaktifkan atau menonaktifkan sumber data opsional lihatJenis sumber data opsional di Detective.

Sumber data yang digunakan dalam grafik perilaku

Untuk mengisi grafik perilaku, Amazon Detective menggunakan data sumber dari akun administrator grafik perilaku dan akun anggota.

Dengan Detective, Anda dapat mengakses hingga satu tahun data peristiwa historis. Data ini tersedia melalui sekumpulan visualisasi yang menunjukkan perubahan jenis dan volume aktivitas pada jendela waktu yang dipilih. Detective menghubungkan perubahan ini dengan GuardDuty temuan.



Untuk detail tentang struktur data grafik perilaku, lihat Ikhtisar struktur data grafik perilaku di Panduan Pengguna Detective.

Jenis sumber data inti di Detective

Detective menelan data dari jenis log ini: AWS

- Log AWS CloudTrail
- Amazon Virtual Private Cloud VirPC VirPC
- Untuk akun yang terdaftarGuardDuty, Detective juga menelan GuardDuty temuan.

Detective mengkonsumsi CloudTrail dan peristiwa log aliran VPC menggunakan aliran independen dan duplikat dan log aliran VPC. CloudTrail Proses ini tidak memengaruhi atau menggunakan

konfigurasi log aliran VPC yang ada CloudTrail dan Anda. Mereka juga tidak mempengaruhi kinerja atau meningkatkan biaya Anda untuk layanan ini.

Jenis sumber data opsional di Detective

Detective menawarkan paket sumber opsional selain tiga sumber data yang ditawarkan dalam paket inti Detective (paket inti termasuk AWS CloudTrail log, log Aliran VPC, dan GuardDuty temuan). Paket sumber data opsional dapat dimulai atau dihentikan untuk grafik perilaku kapan saja.

Detective menyediakan uji coba gratis 30 hari untuk semua paket sumber inti dan opsional per Wilayah.

> **Note**
>
> Detective menyimpan semua data yang diterima dari setiap paket sumber data hingga 1 tahun.

Saat ini paket sumber opsional berikut tersedia:

- Log audit EKS

  Paket sumber data opsional ini memungkinkan Detective untuk menyerap informasi terperinci tentang klaster EKS di lingkungan Anda dan menambahkan data tersebut ke grafik perilaku Anda. Lihat Log audit Amazon EKS untuk Detective untuk detail.
- AWStemuan keamanan

  Paket sumber data opsional ini memungkinkan Detective untuk menyerap data dari Security Hub dan menambahkan data tersebut ke grafik perilaku Anda. Lihat AWStemuan keamanan untuk detail.

Memulai atau menghentikan sumber data opsional:

1. Buka konsol Detective di https://console.aws.amazon.com/detective/.
2. Dari panel navigasi di bawah Pengaturan, pilih Umum.
3. Di bawah Paket sumber opsional, pilih Perbarui. Kemudian pilih sumber data yang ingin Anda aktifkan atau batalkan pilihan kotak untuk sumber data yang sudah diaktifkan dan pilih Perbarui untuk mengubah paket sumber data mana yang diaktifkan.

> **Note**
>
> Jika Anda berhenti dan kemudian me-restart sumber data opsional Anda akan melihat celah dalam data yang ditampilkan pada beberapa profil entitas. Kesenjangan ini akan dicatat di tampilan konsol dan mewakili periode waktu ketika sumber data dihentikan. Ketika sumber data dimulai ulang Detective tidak surut menelan data.

Log audit Amazon EKS untuk Detective

Log audit Amazon EKS adalah paket sumber data opsional yang dapat ditambahkan ke grafik perilaku Detective Anda. Anda dapat melihat paket sumber opsional yang tersedia, dan statusnya di akun Anda, dari halaman Pengaturan di konsol atau melalui Detective API.

Uji coba gratis 30 hari disediakan untuk sumber data ini. Untuk mempelajari lebih lanjut lihatUji coba gratis untuk sumber data opsional.

Mengaktifkan log audit Amazon EKS memungkinkan Detective menambahkan informasi mendalam tentang sumber daya yang dibuat dengan Amazon EKS ke grafik perilaku Anda. Sumber data ini meningkatkan informasi yang diberikan tentang tipe entitas berikut: Klaster EKS, Kubernetes Pod, Container Image dan subjek Kubernetes.

Selain itu, Jika Anda telah mengaktifkan log audit EKS sebagai sumber data di Amazon, GuardDuty Anda akan dapat melihat detail untuk temuan Kubernetes. GuardDuty Untuk info lebih lanjut tentang mengaktifkan sumber data ini di GuardDuty lihat perlindungan Kubernetes di Amazon. GuardDuty

> **Note**
>
> Sumber data ini diaktifkan secara default untuk grafik perilaku baru yang dibuat setelah 26 Juli 2022. Untuk grafik perilaku yang dibuat sebelum 26 Juli 2022, grafik tersebut harus diaktifkan secara manual.

Menambahkan atau menghapus log audit Amazon EKS sebagai sumber data opsional:

1. Buka konsol Detective di https://console.aws.amazon.com/detective/.
2. Dari panel navigasi di bawah Pengaturan, pilih Umum.
3. Di bawah Paket sumber, pilih log audit EKS untuk mengaktifkan sumber data ini. Jika sudah diaktifkan, pilih lagi untuk berhenti menelan log audit EKS ke dalam grafik perilaku Anda.

AWStemuan keamanan

AWStemuan keamanan adalah paket sumber data opsional yang dapat ditambahkan ke grafik perilaku Detective Anda.

Anda dapat melihat paket sumber opsional yang tersedia, dan statusnya di akun Anda, dari halaman Pengaturan di konsol atau melalui Detective API.

Uji coba gratis 30 hari disediakan untuk sumber data ini. Untuk mempelajari lebih lanjut lihatUji coba gratis untuk sumber data opsional.

Mengaktifkan temuan AWS keamanan memungkinkan Detective menggunakan temuan dari Security Hub yang dikumpulkan oleh Security Hub dari layanan hulu dalam format temuan standar yang disebut AWS Security Format (ASFF), yang menghilangkan kebutuhan akan upaya konversi data yang memakan waktu. Kemudian mengkorelasikan temuan yang tertelan di seluruh produk untuk memprioritaskan yang paling penting.

Menambahkan atau menghapus temuan AWS keamanan sebagai sumber data opsional:

> **Note**
>
> Sumber data temuan AWS keamanan diaktifkan secara default untuk grafik perilaku baru yang dibuat setelah 16 Mei 2023. Untuk grafik perilaku yang dibuat sebelum 16 Mei 2023, grafik tersebut harus diaktifkan secara manual.

1. Buka konsol Detective di https://console.aws.amazon.com/detective/.
2. Dari panel navigasi di bawah Pengaturan, pilih Umum.
3. Di bawah Paket sumber, pilih temuan AWS keamanan untuk mengaktifkan sumber data ini. Jika sudah diaktifkan, pilih lagi untuk berhenti menelan temuan AWS Security Finding Format (ASFF) ke dalam grafik perilaku Anda.

Temuan yang didukung saat ini

Detective menelan semua temuan ASFF di Security Hub dari layanan yang dimiliki oleh Amazon atau. AWS

- Untuk melihat daftar integrasi layanan yang didukung, lihat Integrasi layanan AWS yang Tersedia di AWS Security Hub Panduan Pengguna.

- Untuk daftar sumber daya yang didukung, lihat Sumber daya di Panduan AWS Security Hub Pengguna.
- AWSTemuan Layanan dengan status Kepatuhan tidak diatur ke `FAILED` dan temuan agregat lintas wilayah tidak tertelan.

Bagaimana Detective menelan dan menyimpan data sumber

Saat Detective diaktifkan, Detective mulai menelan data sumber dari akun administrator grafik perilaku. Karena akun anggota ditambahkan ke grafik perilaku, Detective juga mulai menggunakan data dari akun anggota tersebut.

Data sumber Detective terdiri dari versi terstruktur dan diproses dari feed asli. Untuk mendukung analitik Detective, Detective menyimpan salinan data sumber Detective.

Proses penyimpanan data ke Amazon Simple Storage Service (Amazon S3) di penyimpanan data sumber Detective. Saat data sumber baru tiba, komponen Detective lainnya mengambil data dan memulai proses ekstraksi dan analitik. Untuk informasi selengkapnya, lihat Cara Detective menggunakan data sumber untuk mengisi grafik perilaku di Panduan Pengguna Detective.

Bagaimana Detective memberlakukan kuota volume data untuk grafik perilaku

Detective memiliki kuota yang ketat pada volume data yang memungkinkan dalam setiap grafik perilaku. Volume data adalah jumlah data per hari yang mengalir ke grafik perilaku Detective.

Detective memberlakukan kuota ini ketika akun administrator memungkinkan Detective, dan ketika akun anggota menerima undangan untuk berkontribusi pada grafik perilaku.

- Jika volume data untuk akun administrator melebihi 10 TB per hari, maka akun administrator tidak dapat mengaktifkan Detective.
- Jika volume data yang ditambahkan dari akun anggota akan menyebabkan grafik perilaku melebihi 10 TB per hari, akun anggota tidak dapat diaktifkan.

Volume data untuk grafik perilaku juga dapat tumbuh secara alami dari waktu ke waktu. Detective memeriksa volume data grafik perilaku setiap hari untuk memastikan bahwa itu tidak melebihi kuota.

Jika volume data grafik perilaku mendekati kuota, Detective menampilkan pesan peringatan di konsol. Untuk menghindari melebihi kuota, Anda dapat menghapus akun anggota.

Jika volume data grafik perilaku melebihi 10 TB per hari, maka Anda tidak dapat menambahkan akun anggota baru ke grafik perilaku.

Jika volume data grafik perilaku melebihi 15 TB per hari, maka Detective berhenti menelan data ke dalam grafik perilaku. Kuota 15 TB per hari mencerminkan volume data normal dan lonjakan volume data. Saat kuota ini tercapai, tidak ada data baru yang dicerna ke dalam grafik perilaku, tetapi data yang ada tidak dihapus. Anda masih dapat menggunakan data historis itu untuk penyelidikan. Konsol menampilkan pesan untuk menunjukkan bahwa penyerapan data ditangguhkan untuk grafik perilaku.

Jika penyerapan data ditangguhkan, Anda harus bekerja sama AWS Support untuk mengaktifkannya kembali. Jika memungkinkan, sebelum Anda menghubungiAWS Support, coba hapus akun anggota untuk mendapatkan volume data di bawah kuota. Ini membuatnya lebih mudah untuk mengaktifkan kembali penyerapan data untuk grafik perilaku.

Mengelola akun

Setiap grafik perilaku berisi data dari satu atau beberapa akun. Ketika sebuah akun mengaktifkan Detektif, akun tersebut menjadi akun administrator untuk grafik perilaku, dan akun anggota akan memilih akun anggota untuk grafik perilaku. Grafik perilaku dapat memiliki hingga 1.200 akun anggota.

Jika Anda terintegrasi dengan AWS Organizations, maka akun manajemen organisasi menunjuk akun administrator Detektif untuk organisasi. Akun administrator Detektif itu kemudian menjadi akun administrator untuk grafik perilaku organisasi. Akun administrator Detektif dapat mengaktifkan akun organisasi apa pun sebagai akun anggota dalam grafik perilaku organisasi. Akun organisasi tidak dapat menghapus dirinya sendiri dari grafik perilaku organisasi.

Akun administrator juga dapat mengundang akun untuk bergabung dengan grafik perilaku. Ketika akun menerima undangan, Detektif mengaktifkan akun sebagai akun anggota. Akun anggota yang ditambahkan melalui undangan dapat menghapus dirinya sendiri dari grafik perilaku.

Ketika akun diaktifkan sebagai akun anggota, Detektif mulai menelan dan mengekstrak data akun anggota ke dalam grafik perilaku tersebut.

Detective membebankan biaya setiap akun untuk data yang dikontribusikannya pada setiap grafik perilaku. Untuk informasi tentang melacak volume data untuk setiap akun dalam grafik perilaku, lihatthe section called “Penggunaan dan biaya akun administrator”.

Konten

Pembatasan akun dan rekomendasi di Detective

Bila mengelola akun di Amazon Detective, perhatikan pembatasan dan rekomendasi berikut.

Jumlah maksimum akun anggota

Detective memungkinkan hingga 1.200 akun anggota di setiap grafik perilaku.

Akun dan Wilayah

Jika Anda menggunakanAWS Organizations untuk mengelola akun, akun manajemen organisasi menunjuk akun administrator Detective untuk organisasi. Detective untuk perilaku perilaku.

Akun administrator Detective harus sama di semua Wilayah. Akun manajemen organisasi menunjuk akun administrator Detective secara terpisah di setiap Wilayah. Akun administrator Detective juga mengelola grafik perilaku organisasi dan akun anggota secara terpisah di setiap Wilayah.

Untuk akun anggota yang dibuat berdasarkan undangan, asosiasi administrator-anggota hanya dibuat di Wilayah tempat undangan dikirim. Akun administrator harus mengaktifkan Detective di setiap Wilayah, dan memiliki grafik perilaku terpisah di setiap Wilayah. Akun administrator kemudian mengundang setiap akun untuk diasosiasikan sebagai akun anggota di Wilayah tersebut.

Akun dapat berupa akun anggota dari beberapa grafik perilaku di Wilayah yang sama. Akun hanya dapat berupa akun administrator dari satu grafik perilaku per Wilayah. Akun dapat berupa akun administrator di berbagai Wilayah.

Penyelarasan akun administrator dengan Security Hub dan GuardDuty

Untuk memastikan bahwa integrasi denganAWS Security Hub dan Amazon GuardDuty bekerja dengan lancar, kami menyarankan agar akun yang sama adalah akun administrator di semua layanan ini.

Lihat the section called “Direkomendasikan penyelarasan dengan GuardDuty dan AWS Security Hub”.

Memberikan izin yang diperlukan untuk akun administrator

Untuk memastikan bahwa akun administrator memiliki izin yang diperlukan untuk mengelola grafik perilakunya, lampirkan kebijakan`AmazonDetectiveFullAccess` terkelola ke pokok IAM.

Mencerminkan pembaruan organisasi di Detective

Perubahan pada organisasi tidak segera tercermin dalam Detective.

Untuk sebagian besar perubahan, seperti akun organisasi baru dan dihapus, diperlukan waktu hingga satu jam bagi Detective untuk diberi tahu.

Perubahan pada akun administrator Detective yang ditunjuk di Organizations membutuhkan lebih sedikit waktu untuk menyebar.

Melakukan transisi untuk menggunakan Organizations untuk mengelola akun grafik perilaku

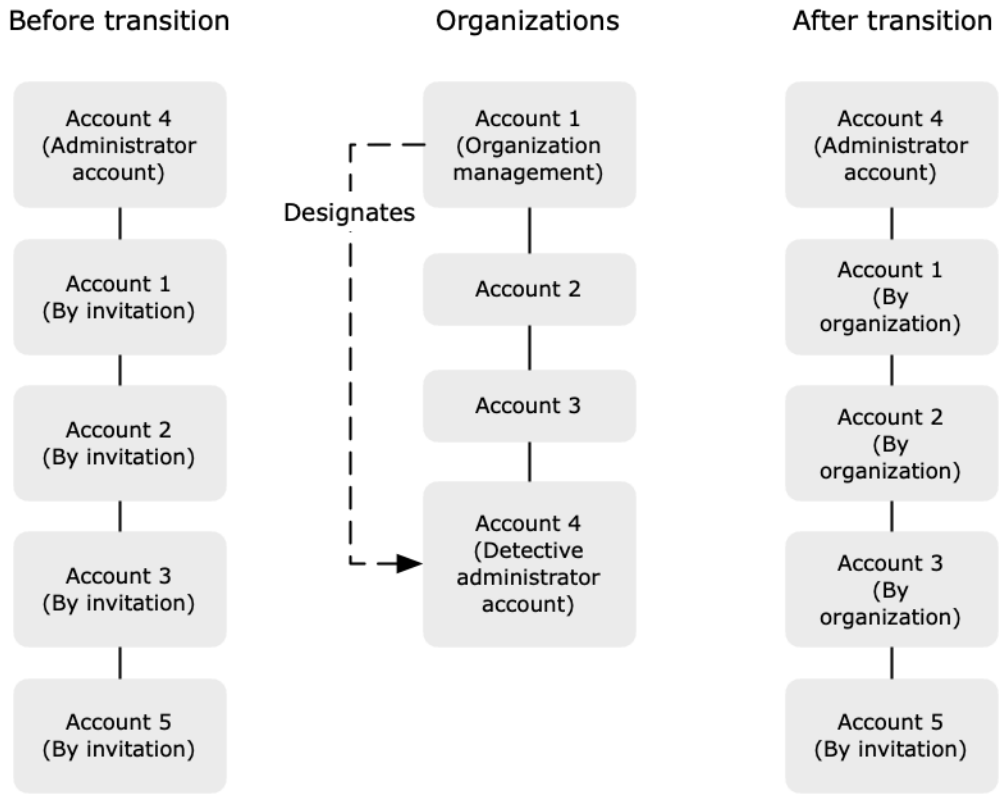
Anda mungkin memiliki grafik perilaku yang ada dengan akun anggota yang menerima undangan manual. Jika Anda terdaftarAWS Organizations, gunakan langkah-langkah berikut untuk menggunakan Organizations untuk mengaktifkan dan mengelola akun anggota alih-alih menggunakan proses undangan manual:

1. Tentukan akun administrator Detective untuk organisasi Anda. Ini menciptakan grafik perilaku organisasi.

   Jika akun administrator Detective sudah memiliki grafik perilaku, maka grafik perilaku tersebut menjadi grafik perilaku organisasi.
2. Aktifkan akun organisasi sebagai akun anggota dalam grafik perilaku organisasi.

   Jika grafik perilaku organisasi memiliki akun anggota yang ada yaitu akun organisasi, akun tersebut akan diaktifkan secara otomatis.

Diagram berikut menunjukkan ikhtisar struktur grafik perilaku sebelum transisi, konfigurasi dalam Organizations, dan struktur akun grafik perilaku setelah transisi.



Menetapkan akun administrator Detective untuk organisasi Anda

Akun manajemen organisasi Anda menunjuk akun administrator Detective dari organisasi Anda. Lihat the section called “Menunjuk akun administrator Detektif”.

Untuk mempermudah transisi, Detective merekomendasikan agar Anda memilih akun administrator saat ini sebagai akun administrator Detective untuk organisasi.

Jika ada akun administrator yang didelegasikan untuk Detective dalam Organizations, maka Anda harus menggunakan akun tersebut atau akun manajemen organisasi sebagai akun administrator Detective.

Jika tidak, saat pertama kali Anda menunjuk akun administrator Detective yang bukan akun manajemen Organizations, Detective memanggil Organisasi untuk menjadikan akun tersebut sebagai akun administrator yang didelegasikan untuk Detective.

Mengaktifkan akun organisasi sebagai akun anggota

Akun administrator Detective adalah akun administrator untuk grafik perilaku organisasi. Akun administrator Detective memilih akun organisasi untuk diaktifkan sebagai akun anggota dalam grafik perilaku organisasi. Lihat the section called “Mengelola akun anggota organisasi”.

Pada halaman akun, akun administrator Detective melihat semua akun dalam organisasi.

Jika akun administrator Detective sudah menjadi akun administrator untuk grafik perilaku, maka grafik perilaku tersebut menjadi grafik perilaku organisasi. Akun organisasi yang sudah menjadi akun anggota dalam grafik perilaku tersebut diaktifkan sebagai akun anggota secara otomatis. Akun organisasi lain memiliki status Bukan anggota.

Akun organisasi memiliki jenis Oleh organisasi, bahkan jika mereka sebelumnya adalah akun anggota berdasarkan undangan.

Akun anggota yang bukan milik organisasi memiliki tipe Dengan undangan.

Halaman Manajemen akun juga menyediakan opsi, Secara otomatis mengaktifkan akun organisasi baru, untuk secara otomatis mengaktifkan akun baru saat ditambahkan ke organisasi. Lihat the section called “Mengaktifkan akun organisasi baru secara otomatis”. Opsi awalnya dimatikan.

Saat akun administrator Detective pertama kali menampilkan halaman Manajemen akun, akun tersebut akan menampilkan pesan yang berisi tombol Aktifkan semua akun organisasi. Bila Anda memilih Aktifkan semua akun organisasi, Detective melakukan tindakan berikut:

- Mengaktifkan semua akun organisasi saat ini sebagai akun anggota.
- Mengaktifkan opsi untuk mengaktifkan akun organisasi baru secara otomatis.

Ada juga opsi Aktifkan semua akun organisasi pada daftar akun anggota.

Tindakan yang tersedia untuk akun

Akun administrator dan anggota memiliki akses ke tindakan Detective berikut. Dalam tabel, nilai-nilai memiliki arti berikut:

- Apa saja — Akun dapat melakukan tindakan untuk semua akun di bawah akun administrator Detective yang sama.
- Diri - Akun hanya dapat melakukan tindakan di akun mereka sendiri.
- Dash (—) — Akun tidak dapat melakukan tindakan.

Tabel berikut memberikan izin default untuk akun administrator dan anggota. Anda dapat menggunakan kebijakan IAM khusus untuk membatasi akses lebih lanjut ke fitur dan fungsi Detective.

Action	Akun Administrator (Organisasi)	Akun Administrator (Undangan)	Anggota (Organisasi)	Anggota (Undangan)
Lihat akun	Setiap	Setiap	Mandiri (Lihat akun administrator)	Mandiri (Lihat akun administrator)
akun anggota	Setiap Akun yang diundang dihapus Akun organisasi dipisahkan	Setiap	–	Mandiri
Menambah atau menghapus paket sumber data opsional	Apa saja (Pengaturan berlaku untuk semua akun anggota)	Apa saja (Pengaturan berlaku untuk semua akun anggota)	–	–
Nonaktifkan Detective	Mandiri	Mandiri	–	–
Melihat data grafik perilaku	Setiap	Setiap	–	–
Mengaktifkan atau menonaktifkan paket sumber data opsional	Semua	Semua	–	–

Menunjuk akun administrator Detektif untuk suatu organisasi

Dalam grafik perilaku organisasi, akun administrator Detektif mengelola keanggotaan grafik perilaku untuk semua akun organisasi.

Bagaimana akun administrator Detektif dikelola

Akun manajemen organisasi menunjuk akun administrator Detektif untuk organisasi di masing-masingWilayah AWS.

Tidak perlu menetapkan akun administrator yang didelegasikan.

Akun administrator Detektif juga menjadi akun administrator yang didelegasikan untuk Detektif diAWS Organizations. Pengecualiannya adalah jika akun manajemen organisasi menunjuk dirinya sebagai akun administrator Detektif. Akun manajemen organisasi tidak dapat menjadi administrator yang didelegasikan di Organizations.

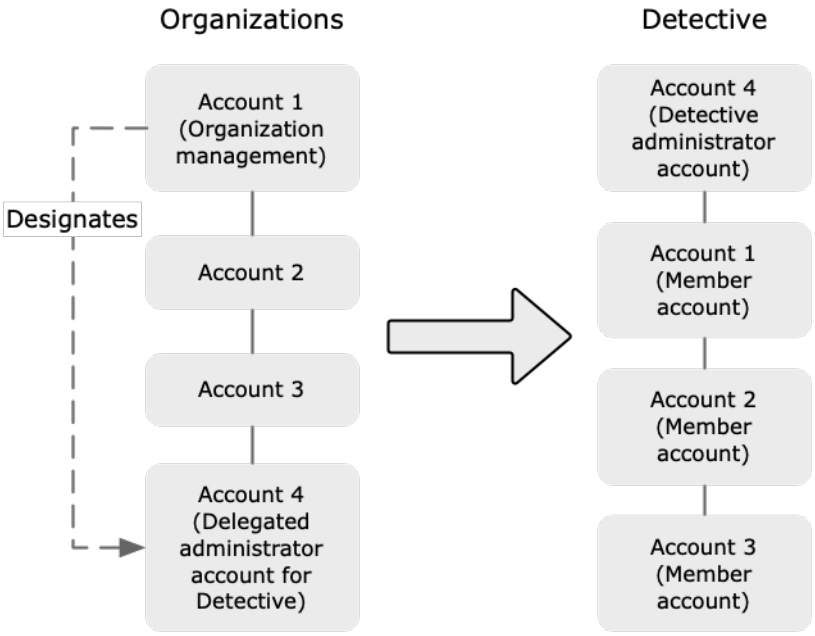
Setelah akun administrator yang didelegasikan diatur dalam Organizations, akun manajemen organisasi hanya dapat memilih akun administrator yang didelegasikan atau akun mereka sendiri sebagai akun administrator Detektif. Kami menyarankan Anda untuk memilih akun administrator yang didelegasikan.

Membuat dan mengelola grafik perilaku organisasi

Saat akun manajemen organisasi memilih akun administrator Detektif, Detektif membuat grafik perilaku baru untuk akun tersebut. Grafik perilaku itu adalah grafik perilaku organisasi.

Jika akun administrator Detektif adalah akun administrator untuk grafik perilaku yang ada, maka grafik perilaku tersebut menjadi grafik perilaku organisasi.

Akun administrator Detektif memilih akun organisasi untuk diaktifkan sebagai akun anggota dalam grafik perilaku organisasi.



Akun administrator Detektif juga dapat mengirim undangan ke akun yang bukan milik organisasi. Untuk informasi selengkapnya, lihat the section called “Mengelola akun anggota organisasi” dan the section called “Mengelola akun yang diundang”.

Menghapus akun administrator Detektif

Akun manajemen organisasi dapat menghapus akun administrator Detektif saat ini di Wilayah. Saat Anda menghapus akun administrator Detektif, Detektif hanya menghapusnya dari Wilayah saat ini. Itu tidak mengubah akun administrator yang didelegasikan di Organizations.

Saat akun manajemen organisasi menghapus akun administrator Detektif di Wilayah, Detektif akan menghapus grafik perilaku organisasi. Detektif dinonaktifkan untuk akun administrator Detektif yang dihapus.

Untuk menghapus akun administrator yang didelegasikan saat ini untuk Detective, Anda menggunakan Organizations API. Saat Anda menghapus akun administrator yang didelegasikan untuk Detective in Organizations, Detective menghapus semua grafik perilaku organisasi di mana akun administrator yang didelegasikan adalah akun administrator Detektif. Grafik perilaku organisasi yang memiliki akun manajemen organisasi sebagai akun administrator Detektif tidak terpengaruh.

Izin yang diperlukan untuk mengonfigurasi akun administrator Detektif

Untuk memastikan bahwa akun manajemen organisasi dapat mengonfigurasi akun administrator Detektif, Anda dapat melampirkan`AmazonDetectiveOrganizationsAccess`kebijakan yang dikelolauntuk AndaAWS Identity and Access Management(IAM) entitas.

Menunjuk akun administrator Detektif (konsol)

Akun manajemen organisasi dapat menggunakan konsol Detektif untuk menunjuk akun administrator Detektif.

Anda tidak perlu mengaktifkan Detektif untuk mengelola akun administrator Detektif. Anda dapat mengelola akun administrator Detektif dariAktifkan Detektifhalaman.

Untuk menetapkan akun administrator detektif administrator detektif (Aktifkan Detektifhalaman)

1. Buka konsol Detektif Amazon Detective dihttps://console.aws.amazon.com/detective/.
2. Pilih Mulai.
3. DiIzin yang diperlukan untuk akun administratorpanel, berikan izin yang diperlukan ke akun yang Anda pilih sehingga mereka dapat beroperasi sebagai administrator Detektif dengan akses penuh ke semua tindakan di Detektif. Untuk beroperasi sebagai administrator, Kami merekomendasikan melampirkan`AmazonDetectiveFullAccess`kebijakan untuk kepala sekolah.
4. PilihLampirkan kebijakan dari IAMuntuk melihat kebijakan yang disarankan secara langsung di konsol IAM.
5. Bergantung pada apakah Anda memiliki izin di konsol IAM, lanjutkan sebagai berikut:
   - Jika Anda memiliki izin untuk beroperasi di konsol IAM, lampirkan kebijakan yang disarankan ke prinsipal yang Anda gunakan untuk Detektif.
   - Jika Anda tidak memiliki izin untuk beroperasi di konsol IAM, salin Amazon Resource Name (ARN) dari kebijakan tersebut dan berikan ke administrator IAM Anda. Mereka kemudian dapat melampirkan kebijakan atas nama Anda.
6. Di bawahadministrator yang didelegasikan, pilih akun administrator Detektif.

   Opsi yang tersedia tergantung pada apakah Anda memiliki akun administrator yang didelegasikan untuk Detective in Organizations.

- Jika Anda tidak memiliki akun administrator yang didelegasikan untuk Detective in Organizations, maka masukkan pengenal akun akun untuk menunjuknya sebagai akun administrator Detektif.

  Anda mungkin memiliki akun administrator dan grafik perilaku yang ada dari proses undangan manual. Jika demikian, kami sarankan Anda menetapkan akun itu sebagai akun administrator Detektif.

  Jika Anda memiliki akun administrator yang didelegasikan di Organizations for Amazon GuardDuty,AWS Security Hub, atau Amazon Macie, lalu Detective meminta Anda untuk memilih salah satu akun tersebut. Anda juga dapat memasukkan akun yang berbeda.
- Jika Anda memiliki akun administrator yang didelegasikan untuk Detective in Organizations, maka Anda diminta untuk memilih akun tersebut atau akun Anda. Kami menyarankan Anda untuk memilih akun administrator yang didelegasikan.

7. Pilih Delegasikan.

Jika Detektif diaktifkan, atau merupakan akun anggota dalam grafik perilaku yang ada, maka Anda dapat menunjuk akun administrator Detektif dariUmumhalaman.

Untuk menetapkan akun administrator detektif administrator detektif (Umumhalaman)

1. Buka konsol Detektif Amazon Detective dihttps://console.aws.amazon.com/detective/.
2. Di panel navigasi Detektif, di bawahPengaturan, pilihUmum.
3. DiKebijakan yang dikelolapanel, Anda dapat mempelajari lebih lanjut tentang semua kebijakan terkelola yang didukung Detektif. Anda dapat memberikan izin yang diperlukan ke akun tergantung pada tindakan yang Anda ingin pengguna lakukan di Detective. Untuk beroperasi sebagai administrator, Kami merekomendasikan melampirkan`AmazonDetectiveFullAccess`kebijakan untuk kepala sekolah.
4. Bergantung pada apakah Anda memiliki izin di konsol IAM, lanjutkan sebagai berikut:

   - Jika Anda memiliki izin untuk beroperasi di konsol IAM, lampirkan kebijakan yang disarankan ke prinsipal yang Anda gunakan untuk Detektif.
   - Jika Anda tidak memiliki izin untuk beroperasi di konsol IAM, salin Amazon Resource Name (ARN) dari kebijakan tersebut dan berikan ke administrator IAM Anda. Mereka kemudian dapat melampirkan kebijakan atas nama Anda.

Opsi yang tersedia tergantung pada apakah Anda memiliki akun administrator yang didelegasikan untuk Detective in Organizations.

- Jika Anda tidak memiliki akun administrator yang didelegasikan untuk Detective in Organizations, maka masukkan pengenal akun akun untuk menunjuknya sebagai akun administrator Detektif.

  Anda mungkin memiliki akun administrator dan grafik perilaku yang ada dari proses undangan manual. Jika demikian, maka kami sarankan Anda menunjuk akun itu sebagai akun administrator Detektif.

  Jika Anda memiliki akun administrator yang didelegasikan di Organizations for Amazon GuardDuty,AWS Security Hub, atau Amazon Macie, lalu Detective meminta Anda untuk memilih salah satu akun tersebut. Anda juga dapat memasukkan akun yang berbeda.
- Jika Anda memiliki akun administrator yang didelegasikan untuk Detective in Organizations, maka Anda diminta untuk memilih akun tersebut atau akun Anda. Kami menyarankan Anda untuk memilih akun administrator yang didelegasikan.

5. Pilih Delegasikan.

Menunjuk akun administrator Detektif (Detective API, AWS CLI)

Untuk menunjuk akun administrator Detektif, Anda dapat menggunakan panggilan API atauAWS Command Line Interface. Anda harus menggunakan kredensil akun manajemen organisasi.

Jika Anda sudah memiliki akun administrator yang didelegasikan untuk Detektif dalam organisasi, maka Anda harus memilih akun itu atau akun Anda, kami sarankan Anda memilih akun administrator yang didelegasikan.

Untuk menunjuk akun administrator Detektif (Detective API,AWS CLI)

- Detective API:Gunakan`EnableOrganizationAdminAccount`operasi. Anda harus memberikanAWSpengenal akun akun administrator Detektif. Untuk mendapatkan pengenal akun, gunakan`ListOrganizationAdminAccounts`operasi.
- AWS CLI:Pada baris perintah, jalankan`enable-organization-admin-account`perintah.

```
aws detective enable-organization-admin-account --account-id <admin account ID>
```

Contoh

```
aws detective enable-organization-admin-account --account-id 777788889999
```

Menghapus akun administrator Detektif (konsol)

Dari konsol Detektif, Anda dapat menghapus akun administrator Detektif.

Saat Anda menghapus akun administrator Detektif, Detektif dinonaktifkan untuk akun tersebut, dan grafik perilaku organisasi akan dihapus. Akun administrator detektif hanya dihapus di wilayah yang didelegasikan.

> **Important**
>
> Menghapus akun administrator Detective tidak memengaruhi akun administrator yang didelegasikan di Organizations.

Untuk menghapus akun administrator Detektif (Aktifkan Detektifhalaman)

1. Buka konsol Detektif Amazon Detective dihttps://console.aws.amazon.com/detective/.
2. Pilih Mulai.
3. Di bawahAdministrator yang didelegasikan, pilihNonasikan Detektif Amazon.
4. Pada kotak dialog konfirmasi, masukkan**`disable`**, lalu pilihNonasikan Detektif Amazon.

Untuk menghapus akun administrator Detektif (Umumhalaman)

1. Buka konsol Detektif Amazon Detective dihttps://console.aws.amazon.com/detective/.
2. Di panel navigasi Detektif, di bawahPengaturan, pilihUmum.
3. Di bawahAdministrator yang didelegasikan, pilihNonasikan Detektif Amazon.
4. Pada kotak dialog konfirmasi, masukkan**`disable`**, lalu pilihNonasikan Detektif Amazon.

Menghapus akun administrator Detective (Detective API,AWS CLI)

Untuk menghapus akun administrator Detektif, Anda dapat menggunakan panggilan API atauAWS CLI. Anda harus menggunakan kredensil akun manajemen organisasi.

Saat Anda menghapus akun administrator Detektif, Detektif dinonaktifkan untuk akun tersebut, dan grafik perilaku organisasi akan dihapus.

> **Important**
>
> Menghapus akun administrator Detective tidak memengaruhi akun administrator yang didelegasikan di Organizations.

Untuk menghapus akun administrator Detective (Detective API,AWS CLI)

- Detective API:Gunakan`DisableOrganizationAdminAccount`operasi.

  Saat Anda menggunakan API Detektif untuk menghapus akun administrator Detektif, akun tersebut hanya akan dihapus di Wilayah tempat panggilan atau perintah API dikeluarkan.
- AWS CLI:Pada baris perintah, jalankan`disable-organization-admin-account`perintah.

```
aws detective disable-organization-admin-account
```

Tidak perlu untuk menghapus akun administrator yang didelegasikan.AWS CLI)

Menghapus akun administrator Detective tidak secara otomatis menghapus akun administrator yang didelegasikan di Organizations. Untuk menghapus akun administrator yang didelegasikan untuk Detective, Anda dapat menggunakan Organizations API.

Saat Anda menghapus akun administrator yang didelegasikan, ini akan menghapus semua grafik perilaku organisasi di mana akun administrator yang didelegasikan adalah akun administrator Detektif. Ini juga menonaktifkan Detektif untuk akun di Wilayah tersebut.

Untuk menghapus akun administrator yang didelegasikan (Organizations API,AWS CLI)

- API organisasi:GunakanDeregisterDelegatedAdministratoroperasi. Anda harus memberikan pengenal akun dari akun administrator Detektif, dan kepala layanan untuk Detektif, yaitudetective.amazonaws.com.
- AWS CLI:Pada baris perintah, jalankanderegister-delegated-administratorperintah.

```
aws organizations deregister-delegated-administrator --account-id <Detective
 administrator account ID> --service-principal <Detective service principal>
```

Contoh

```
aws organizations deregister-delegated-administrator --account-id 777788889999 --
service-principal detective.amazonaws.com
```

Melihat daftar akun

Akun administrator dapat menggunakan konsol Detektif atau API untuk melihat daftar akun. Daftar ini dapat mencakup:

- Akun yang diundang oleh akun administrator untuk bergabung dengan grafik perilaku. Akun ini memiliki jenis Undangan.
- Untuk grafik perilaku organisasi, semua akun dalam organisasi. Akun ini memiliki jenis Berdasarkan organisasi.

Hasilnya tidak termasuk akun anggota yang diundang yang menolak undangan atau akun administrator dihapus dari grafik perilaku. Ini hanya mencakup akun dengan status berikut.

Verifikasi sedang berlangsung

Untuk akun yang diundang, Detektif memverifikasi alamat email akun sebelum mengirim undangan.

Untuk akun organisasi, Detective memverifikasi bahwa akun tersebut milik organisasi. Detective juga memverifikasi bahwa itu adalah akun administrator Detective yang mengaktifkan akun tersebut.

Verifikasi gagal

Verifikasi gagal. Undangan tidak dikirim, atau akun organisasi tidak diaktifkan sebagai anggota.

Diundang

Untuk akun yang diundang. Undangan telah dikirim, tetapi akun anggota belum merespons.

Bukan anggota

Untuk akun organisasi dalam grafik perilaku organisasi. Akun organisasi saat ini bukan akun anggota. Itu tidak menyumbangkan data ke grafik perilaku organisasi.

Aktif

Untuk akun yang diundang, akun anggota menerima undangan dan menyumbangkan data ke grafik perilaku.

Untuk akun organisasi dalam grafik perilaku organisasi, akun administrator Detektif mengaktifkan akun sebagai akun anggota. Akun menyumbangkan data ke grafik perilaku organisasi.

Tidak diaktifkan

Untuk akun yang diundang, akun anggota menerima undangan, tetapi tidak dapat diaktifkan.

Untuk akun organisasi dalam grafik perilaku organisasi, akun administrator Detektif mencoba mengaktifkan akun, tetapi akun tidak dapat diaktifkan.

Untuk akun yang diundang, Detektif memeriksa jumlah akun anggota. Jumlah maksimum akun anggota untuk grafik perilaku adalah 1.200. Jika grafik perilaku sudah berisi 1.200 akun anggota, maka akun baru tidak dapat diaktifkan.

Detektif memeriksa apakah volume data Anda berada dalam kuota Detektif. Volume data yang mengalir ke grafik perilaku harus kurang dari maksimum yang diizinkan oleh Detective. Jika volume saat ini yang dicerna di atas batas 10 TB per hari untuk volume data grafik Perilaku, maka Detective tidak akan mengizinkan Anda untuk menambahkan akun anggota tambahan.

Daftar akun (Konsol)

Anda dapat menggunakan AWS Management Console untuk melihat dan memfilter daftar akun Anda.

Untuk menampilkan daftar akun (konsol)

1. Masuk ke AWS Management Console. Kemudian buka konsol Detective di https://console.aws.amazon.com/detective/.
2. Di panel navigasi Detektif, pilih Manajemen akun.

   Daftar akun anggota berisi akun berikut:

   - Akun Anda
   - Akun yang Anda undang untuk menyumbangkan data ke grafik perilaku
   - Dalam grafik perilaku organisasi, semua akun organisasi

   Untuk setiap akun, daftar menampilkan informasi berikut:

   - Pengidentifikasi AWS akun.
   - Untuk akun organisasi, nama akun.
   - Jenis akun (Dengan undangan atau Berdasarkan organisasi).
   - Untuk akun yang diundang, alamat email pengguna root akun.
   - Status akun.
   - Volume data harian untuk akun. Detektif tidak dapat mengambil volume data untuk akun yang tidak diaktifkan sebagai akun anggota.
   - Tanggal ketika status akun terakhir diperbarui.

Anda dapat menggunakan tab di bagian atas tabel untuk memfilter daftar berdasarkan status akun anggota. Setiap tab menunjukkan jumlah akun anggota yang cocok.

- Pilih Semua untuk melihat semua akun anggota.
- Pilih Diaktifkan untuk melihat akun yang berstatus Diaktifkan.
- Pilih Tidak diaktifkan untuk melihat akun yang memiliki status selain Diaktifkan.

Anda juga dapat menambahkan filter lain ke daftar akun anggota.

Untuk menambahkan filter ke daftar akun dalam grafik perilaku (konsol)

1. Pilih kotak filter.

2. Pilih kolom yang ingin Anda gunakan untuk memfilter daftar.
3. Untuk kolom yang ditentukan, pilih nilai yang akan digunakan untuk filter.
4. Untuk menghapus filter, pilih ikon x di kanan atas.
5. Untuk memperbarui daftar dengan informasi status terbaru, pilih ikon penyegaran di kanan atas.

Daftar akun anggota Anda (Detective API,) AWS CLI

Anda dapat menggunakan panggilan API atau AWS Command Line Interface untuk melihat daftar akun anggota dalam grafik perilaku Anda.

Untuk mendapatkan ARN dari grafik perilaku Anda untuk digunakan dalam permintaan, gunakan operasi. `ListGraphs`

Untuk mengambil daftar akun anggota (Detective API,) AWS CLI

- Detective API: Gunakan operasi. `ListMembers` Untuk mengidentifikasi grafik perilaku yang dimaksud, tentukan grafik perilaku ARN.

  Perhatikan bahwa untuk grafik perilaku organisasi, `ListMembers`tidak menampilkan akun organisasi yang tidak Anda aktifkan sebagai akun anggota atau yang Anda lepaskan dari grafik perilaku.
- AWS CLI: Pada baris perintah, jalankan `list-members`perintah.

  ```
  aws detective list-members --graph-arn <behavior graph ARN>
  ```

  Contoh:

  ```
  aws detective list-members --graph-arn arn:aws:detective:us-
  east-1:111122223333:graph:123412341234
  ```

Untuk mengambil detail tentang akun anggota tertentu dalam grafik perilaku Anda (Detective API,) AWS CLI

- Detective API: Gunakan operasi. `GetMembers` Tentukan grafik perilaku ARN dan daftar pengidentifikasi akun untuk akun anggota.
- AWS CLI: Pada baris perintah, jalankan `get-members`perintah.

```
aws detective get-members --account-ids <member account IDs> --graph-arn <behavior
 graph ARN>
```

Contoh:

```
aws detective get-members --account-ids 444455556666 123456789012 --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Mengelola akun organisasi sebagai akun anggota

Dalam grafik perilaku organisasi, akun administrator Detektif menentukan akun organisasi mana yang akan diaktifkan sebagai akun anggota.

Mereka dapat mengonfigurasi Detektif untuk mengaktifkan akun organisasi baru sebagai akun anggota secara otomatis, atau mereka dapat mengaktifkan akun organisasi secara manual.

Akun administrator Detektif juga dapat memisahkan akun organisasi dari grafik perilaku organisasi.

Daftar Isi

Mengaktifkan akun organisasi baru sebagai akun anggota secara otomatis

Akun administrator Detektif dapat mengonfigurasi Detektif untuk mengaktifkan akun organisasi baru secara otomatis sebagai akun anggota dalam grafik perilaku organisasi.

Ketika akun baru ditambahkan ke organisasi Anda, akun tersebut ditambahkan ke daftar di halaman Manajemen akun. Untuk akun organisasi, Type is By Organization.

Secara default, akun organisasi baru tidak diaktifkan sebagai akun anggota. Status mereka bukan anggota.

Ketika Anda memilih untuk mengaktifkan akun organisasi secara otomatis, Detektif mulai mengaktifkan akun baru sebagai akun anggota saat ditambahkan ke organisasi. Detective tidak mengaktifkan akun organisasi yang ada yang belum diaktifkan.

Detektif dapat mengaktifkan akun organisasi sebagai akun anggota hanya jika jumlah maksimum akun anggota untuk grafik perilaku adalah 1.200. Jika grafik perilaku Anda sudah berisi 1.200 akun anggota, maka akun baru tidak dapat diaktifkan.

Detektif memeriksa apakah volume data Anda berada dalam kuota Detektif. Volume data yang mengalir ke grafik perilaku harus kurang dari maksimum yang diizinkan oleh Detective. Jika volume saat ini yang dicerna di atas batas 10 TB per hari, Anda tidak dapat menambahkan lebih banyak akun dan Detective akan menonaktifkan konsumsi data lebih lanjut.

Mengaktifkan akun organisasi baru secara otomatis (konsol)

Pada halaman Manajemen akun, pengaturan Aktifkan akun organisasi baru secara otomatis menentukan apakah akan mengaktifkan akun secara otomatis saat ditambahkan ke organisasi.

Untuk secara otomatis mengaktifkan akun organisasi baru sebagai akun anggota

1. Buka konsol Amazon Detective di. https://console.aws.amazon.com/detective/
2. Di panel navigasi Detektif, pilih Manajemen akun.
3. Alihkan Aktifkan akun organisasi baru secara otomatis ke posisi aktif.

Mengaktifkan akun organisasi baru secara otomatis (Detective API,) AWS CLI

Untuk menentukan apakah akan mengaktifkan akun organisasi baru secara otomatis sebagai akun anggota, akun administrator dapat menggunakan Detective API atau file. AWS Command Line Interface

Untuk melihat dan mengelola konfigurasi, Anda harus memberikan grafik perilaku ARN. Untuk mendapatkan ARN, gunakan operasi. `ListGraphs`

Untuk melihat konfigurasi saat ini untuk mengaktifkan akun organisasi secara otomatis

- Detective API: Gunakan operasi. `DescribeOrganizationConfiguration`

  Sebagai tanggapan, jika akun organisasi baru diaktifkan secara otomatis, maka `AutoEnable` adalah`true`.
- AWS CLI: Pada baris perintah, jalankan `describe-organization-configuration`perintah.

```
aws detective describe-organization-configuration --graph-arn <behavior graph ARN>
```

Contoh

```
aws detective describe-organization-configuration --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

Untuk mengaktifkan akun organisasi baru secara otomatis

- Detective API: Gunakan operasi. `UpdateOrganizationConfiguration` Untuk mengaktifkan akun organisasi baru secara otomatis, setel `AutoEnable` ke`true`.
- AWS CLI: Pada baris perintah, jalankan `update-organization-configuration`perintah.

```
aws detective update-organization-configuration --graph-arn <behavior graph ARN> --
auto-enable | --no-auto-enable
```

Contoh

```
aws detective update-organization-configuration --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234 --auto-enable
```

Mengaktifkan akun organisasi sebagai akun anggota

Jika Anda tidak secara otomatis mengaktifkan akun organisasi baru, maka Anda dapat mengaktifkan akun tersebut secara manual. Anda juga harus mengaktifkan akun yang Anda putuskan secara manual.

Menentukan apakah akun dapat diaktifkan

Anda tidak dapat mengaktifkan akun organisasi sebagai akun anggota jika grafik perilaku organisasi sudah memiliki maksimum 1.200 akun yang diaktifkan. Dalam hal ini, status akun organisasi tetap Bukan anggota. Akun tidak menyumbangkan data ke grafik perilaku.

Segera setelah akun anggota dapat diaktifkan, Detektif secara otomatis mengubah status akun anggota menjadi Diaktifkan. Misalnya, status akun anggota berubah menjadi Diaktifkan jika akun administrator menghapus akun anggota lain untuk memberi ruang bagi akun.

Mengaktifkan akun organisasi sebagai akun anggota (konsol)

Dari halaman Manajemen akun, Anda dapat mengaktifkan akun organisasi sebagai akun anggota.

Untuk mengaktifkan akun organisasi sebagai akun anggota

1. Buka konsol Amazon Detective di. https://console.aws.amazon.com/detective/
2. Di panel navigasi Detektif, pilih Manajemen akun.
3. Untuk melihat daftar akun yang saat ini tidak diaktifkan, pilih Tidak diaktifkan.
4. Anda dapat memilih akun organisasi tertentu, atau mengaktifkan semua akun organisasi.

   Untuk mengaktifkan akun organisasi yang dipilih:

   a. Pilih setiap akun organisasi yang ingin Anda aktifkan.
   b. Pilih Aktifkan akun.

   Untuk mengaktifkan semua akun organisasi, pilih Aktifkan semua akun organisasi.

Mengaktifkan akun organisasi sebagai akun anggota (Detective API,) AWS CLI

Anda dapat menggunakan Detective API atau AWS Command Line Interface untuk mengaktifkan akun organisasi sebagai akun anggota dalam grafik perilaku organisasi. Untuk mendapatkan ARN grafik perilaku Anda untuk digunakan dalam permintaan, gunakan operasi. `ListGraphs`

Untuk mengaktifkan akun organisasi sebagai akun anggota (Detective API,) AWS CLI

- Detective API: Gunakan operasi. `CreateMembers` Anda harus memberikan grafik ARN.

  Untuk setiap akun, tentukan pengenal akun. Akun organisasi dalam grafik perilaku organisasi tidak menerima undangan. Anda tidak perlu memberikan alamat email atau informasi undangan lainnya.
- AWS CLI: Pada baris perintah, jalankan `create-members`perintah.

```
aws detective create-members --accounts AccountId=<AWS account ID> --graph-
arn <behavior graph ARN>
```

Contoh

```
aws detective create-members --accounts AccountId=444455556666 AccountId=123456789012
 --graph-arn arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Memutuskan akun organisasi sebagai akun anggota

Untuk menghentikan pengambilan data dari akun organisasi dalam grafik perilaku organisasi, Anda dapat memisahkan akun. Data yang ada untuk akun itu tetap ada dalam grafik perilaku.

Saat Anda memisahkan akun organisasi, status berubah menjadi Bukan anggota. Detektif berhenti menelan data dari akun itu, tetapi akun tetap dalam daftar.

Memutuskan akun organisasi (konsol)

Dari halaman Manajemen akun, Anda dapat memisahkan akun organisasi sebagai akun anggota.

1. Buka konsol Amazon Detective di. https://console.aws.amazon.com/detective/
2. Di panel navigasi Detektif, pilih Manajemen akun.
3. Untuk menampilkan daftar akun yang diaktifkan, pilih Diaktifkan.
4. Pilih kotak centang untuk setiap akun untuk dipisahkan.
5. Pilih Tindakan. Kemudian pilih Nonaktifkan akun.

   Status akun untuk akun yang terputus berubah menjadi Bukan anggota.

Memutuskan akun organisasi (Detective API,) AWS CLI

Anda dapat menggunakan Detective API atau AWS Command Line Interface untuk memisahkan akun organisasi sebagai akun anggota dalam grafik perilaku Anda.

Untuk mendapatkan ARN grafik perilaku Anda untuk digunakan dalam permintaan, gunakan operasi. `ListGraphs`

Untuk memisahkan akun organisasi dari grafik perilaku organisasi (Detective API,) AWS CLI

- Detective API: Gunakan operasi. `DeleteMembers` Tentukan grafik ARN dan daftar pengidentifikasi akun untuk memisahkan akun anggota.
- AWS CLI: Pada baris perintah, jalankan `delete-members`perintah.

```
aws detective delete-members --account-ids <account ID list> --graph-arn <behavior
 graph ARN>
```

Contoh

```
aws detective delete-members --account-ids 444455556666 123456789012 --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Mengelola akun anggota yang diundang

Akun administrator dapat mengundang akun untuk menjadi akun anggota dalam grafik perilaku. Ketika akun anggota menerima undangan dan diaktifkan, Detektif Amazon mulai menyerap dan mengekstrak data akun anggota ke dalam grafik perilaku tersebut.

Untuk grafik perilaku selain grafik perilaku organisasi, semua akun anggota adalah akun yang diundang.

Akun administrator Detektif juga dapat mengundang akun yang bukan akun organisasi ke grafik perilaku organisasi.

Akun administrator dapat menghapus akun anggota yang diundang dari grafik perilaku.

Daftar Isi

Mengundang akun anggota ke grafik perilaku

Akun administrator dapat mengundang akun untuk berkontribusi pada grafik perilaku. Grafik perilaku dapat berisi hingga 1.200 akun anggota.

Pada tingkat tinggi, proses mengundang akun untuk berkontribusi pada grafik perilaku adalah sebagai berikut.

1. Untuk setiap akun anggota untuk ditambahkan, akun administrator menyediakan pengenal AWS akun dan alamat email pengguna root.

2. Detektif memvalidasi bahwa alamat email adalah alamat email pengguna root untuk akun tersebut. Jika informasi akun valid, Detektif mengirimkan undangan ke akun anggota.

   Detektif tidak melakukan validasi ini atau mengirim undangan email ke akun anggota di Wilayah ini:

   - AWS GovCloud Wilayah (AS-Timur)
   - AWS GovCloud Wilayah (AS-Barat)

   Untuk Wilayah lain, Anda dapat `DisableEmailNotification` menggunakan CreateMembersoperasi Detective API. Jika `DisableEmailNotification` disetel ke true, maka Detective tidak akan mengirim undangan ke akun anggota. Ini adalah pengaturan yang berguna untuk akun yang dikelola secara terpusat.
3. Akun anggota menerima atau menolak undangan.

   Bahkan jika akun administrator tidak mengirim email undangan, akun anggota tetap harus menanggapi undangan.
4. Setelah akun anggota menerima undangan, Detektif mulai menyerap data dari akun anggota ke dalam grafik perilaku.
5. Segera setelah akun anggota memenuhi syarat untuk diaktifkan, Detektif secara otomatis mengubah status akun anggota menjadi Diaktifkan.

   Misalnya, status akun anggota berubah menjadi Diaktifkan jika akun administrator menghapus akun anggota lain untuk memberi ruang bagi akun.

   Jika lebih dari satu akun tidak diaktifkan, maka Detektif mengaktifkan akun dalam urutan di mana mereka diundang. Proses untuk memeriksa apakah akan mengaktifkan akun Not enabled berjalan setiap jam.

   Akun administrator juga dapat mengaktifkan akun secara manual, alih-alih menunggu proses otomatis. Misalnya, akun administrator mungkin ingin memilih akun yang akan diaktifkan. Lihat the section called “Mengaktifkan akun anggota yang tidak diaktifkan”.

   Perhatikan bahwa Detektif mulai secara otomatis mengaktifkan akun yang Tidak diaktifkan pada 12 Mei 2021. Akun yang tidak diaktifkan sebelumnya tidak diaktifkan secara otomatis. Akun administrator harus mengaktifkannya secara manual.

Mengundang akun individual ke grafik perilaku (Konsol)

Anda dapat secara manual menentukan akun anggota yang akan diundang untuk menyumbangkan data mereka ke grafik perilaku.

Untuk secara manual memilih akun anggota yang akan diundang (konsol)

1. Buka konsol Amazon Detective di. https://console.aws.amazon.com/detective/
2. Di panel navigasi Detektif, pilih Manajemen akun.
3. Pilih Tindakan. Kemudian pilih Undang akun.
4. Di bawah Tambah akun, pilih Tambahkan akun individual.
5. Untuk menambahkan akun anggota ke daftar undangan, lakukan langkah-langkah berikut.

   a. Pilih Tambah akun.

   b. Untuk ID AWS Akun, masukkan ID AWS akun.

   c. Untuk alamat Email, masukkan alamat email pengguna root untuk akun tersebut.
6. Untuk menghapus akun dari daftar, pilih Hapus untuk akun itu.
7. Di bawah Personalisasi email undangan, tambahkan konten yang disesuaikan untuk disertakan dalam email undangan.

   Misalnya, Anda dapat menggunakan area ini untuk memberikan informasi kontak. Atau gunakan untuk mengingatkan akun anggota bahwa mereka perlu melampirkan kebijakan IAM yang diperlukan kepada pengguna atau peran mereka sebelum mereka dapat menerima undangan.
8. Kebijakan IAM akun anggota berisi teks kebijakan IAM yang diperlukan untuk akun anggota. Undangan email mencakup teks kebijakan ini. Untuk menyalin teks kebijakan, pilih Salin.
9. Pilih Undang.

Mengundang daftar akun anggota ke grafik perilaku (Konsol)

Dari konsol Detektif, Anda dapat menyediakan `.csv` file yang berisi daftar akun anggota untuk diundang ke grafik perilaku Anda.

Baris pertama dalam file adalah baris header. Setiap akun kemudian terdaftar pada baris terpisah. Setiap entri akun anggota berisi ID AWS akun dan alamat email pengguna root akun.

Contoh:

```
Account ID,Email address
111122223333,srodriguez@example.com
444455556666,rroe@example.com
```

Ketika Detective memproses file, ia mengabaikan akun yang sudah diundang, kecuali status akun Verifikasi gagal. Status tersebut menunjukkan bahwa alamat email yang diberikan untuk akun tidak cocok dengan alamat email pengguna root akun. Dalam hal ini, Detective menghapus undangan asli dan mencoba lagi untuk memverifikasi alamat email dan mengirim undangan.

Opsi ini juga menyediakan template yang dapat Anda gunakan untuk membuat daftar akun.

Untuk mengundang akun anggota dari daftar.csv (konsol)

1. Buka konsol Amazon Detective di. https://console.aws.amazon.com/detective/
2. Di panel navigasi Detektif, pilih Manajemen akun.
3. Pilih Tindakan. Kemudian pilih Undang akun.
4. Di bawah Tambah akun, pilih Tambah dari.csv.
5. Untuk mengunduh file templat agar berfungsi, pilih Unduh template.csv.
6. Untuk memilih file yang berisi daftar akun, pilih Pilih file.csv.
7. Di bawah Tinjau akun anggota, verifikasi daftar akun anggota yang ditemukan Detektif dalam file.
8. Di bawah Personalisasi email undangan, tambahkan konten yang disesuaikan untuk disertakan dalam email undangan.

   Misalnya, Anda dapat memberikan informasi kontak, atau mengingatkan akun anggota tentang kebijakan IAM yang diperlukan.
9. Kebijakan IAM akun anggota berisi teks kebijakan IAM yang diperlukan untuk akun anggota. Undangan email mencakup teks kebijakan ini. Untuk menyalin teks kebijakan, pilih Salin.
10. Pilih Undang.

Mengundang akun anggota ke grafik perilaku (Detective API,) AWS CLI

Anda dapat menggunakan Detective API atau akun AWS Command Line Interface untuk mengundang anggota untuk menyumbangkan data mereka ke grafik perilaku. Untuk mendapatkan ARN dari grafik perilaku Anda untuk digunakan dalam permintaan, gunakan operasi. `ListGraphs`

Untuk mengundang akun anggota ke grafik perilaku (Detective API,) AWS CLI

- Detective API: Gunakan operasi. `CreateMembers` Anda harus memberikan grafik ARN. Untuk setiap akun, tentukan pengenal akun dan alamat email pengguna root.

  Untuk tidak mengirim email undangan ke akun anggota, atur `DisableEmailNotification` ke true. Secara default, `DisableEmailNotification` adalah false.

  Jika Anda mengirim email undangan, Anda dapat secara opsional memberikan teks khusus untuk ditambahkan ke email undangan.
- AWS CLI: Pada baris perintah, jalankan `create-members` perintah.

```
aws detective create-members --accounts AccountId=<AWS account ID>,EmailAddress=<root
 user email address> --graph-arn <behavior graph ARN> --message "<Custom message
 text>"
```

  Contoh

```
aws detective create-members --accounts
 AccountId=444455556666,EmailAddress=mmajor@example.com
 AccountId=123456789012,EmailAddress=jstiles@example.com --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234 --message "This is Paul
 Santos. I need to add your account to the data we use for security investigation in
 Amazon Detective. If you have any questions, contact me at psantos@example.com."
```

  Untuk menunjukkan tidak mengirim email undangan ke akun anggota, sertakan`--disable-email-notification`.

```
aws detective create-members --accounts AccountId=<AWS account ID>,EmailAddress=<root
 user email address> --graph-arn <behavior graph ARN> --disable-email-notification
```

  Contoh

```
aws detective create-members --accounts
 AccountId=444455556666,EmailAddress=mmajor@example.com
 AccountId=123456789012,EmailAddress=jstiles@example.com --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234 --disable-email-
notification
```

Menambahkan daftar akun anggota di seluruh Wilayah (skrip Python aktif) GitHub

Detective menyediakan skrip open-source GitHub yang memungkinkan Anda melakukan hal berikut:

- Tambahkan daftar akun anggota tertentu ke grafik perilaku akun administrator di seluruh daftar Wilayah yang ditentukan.
- Jika akun administrator tidak memiliki grafik perilaku di Wilayah, maka skrip juga mengaktifkan Detektif dan membuat grafik perilaku di Wilayah tersebut.
- Kirim email undangan ke akun anggota.
- Secara otomatis menerima undangan untuk akun anggota.

Untuk informasi tentang cara mengkonfigurasi dan menggunakan GitHub skrip, lihatMenggunakan skrip Amazon Detective Python.

Mengaktifkan akun anggota yang tidak diaktifkan

Setelah akun anggota menerima undangan, Amazon Detective memeriksa jumlah akun anggota. Jumlah maksimum akun anggota untuk grafik perilaku adalah 1.200. Jika grafik perilaku Anda sudah berisi 1.200 akun anggota, maka akun baru tidak dapat diaktifkan. Jika Detektif tidak dapat mengaktifkan akun anggota, maka ia menetapkan status akun anggota ke Tidak diaktifkan.

Akun anggota yang Tidak diaktifkan tidak menyumbangkan data ke grafik perilaku.

Detective secara otomatis mengaktifkan akun karena grafik perilaku dapat mengakomodasi mereka.

Anda juga dapat mencoba mengaktifkan akun anggota secara manual yang tidak diaktifkan akun anggota. Misalnya, Anda dapat menghapus akun anggota yang ada untuk mengurangi volume data. Alih-alih menunggu proses otomatis untuk mengaktifkan akun, Anda dapat mencoba mengaktifkan Akun anggota yang tidak diaktifkan.

Mengaktifkan akun anggota yang Tidak diaktifkan (Konsol)

Daftar akun anggota mencakup opsi untuk mengaktifkan akun anggota terpilih yang Tidak diaktifkan.

Untuk mengaktifkan akun anggota yang tidak diaktifkan

1. Buka konsol Amazon Detective di. https://console.aws.amazon.com/detective/
2. Di panel navigasi Detektif, pilih Manajemen akun.

3. Di bawah Akun anggota saya, pilih kotak centang untuk mengaktifkan setiap akun anggota.

   Anda hanya dapat mengaktifkan akun anggota yang memiliki status Tidak diaktifkan.

4. Pilih Aktifkan akun.

Detektif menentukan apakah akun anggota dapat diaktifkan. Jika akun anggota dapat diaktifkan, status akan berubah menjadi Diaktifkan.

Mengaktifkan akun anggota yang Tidak diaktifkan (Detective API,) AWS CLI

Anda dapat menggunakan panggilan API atau AWS Command Line Interface untuk mengaktifkan satu akun anggota yang tidak diaktifkan. Untuk mendapatkan ARN dari grafik perilaku Anda untuk digunakan dalam permintaan, gunakan operasi. `ListGraphs`

Untuk mengaktifkan akun anggota yang tidak diaktifkan

- Detective API: Gunakan operasi `StartMonitoringMember`API. Anda harus memberikan grafik perilaku ARN. Untuk mengidentifikasi akun anggota, gunakan pengenal AWS akun.
- AWS CLI: Pada baris perintah, jalankan `start-monitoring-member`perintah:

```
start-monitoring-member --graph-arn <behavior graph ARN> --account-id <AWS account
 ID>
```

Sebagai contoh:

```
start-monitoring-member --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234 --account-id 444455556666
```

Menghapus akun anggota yang diundang dari grafik perilaku

Akun administrator dapat menghapus akun anggota dari grafik perilaku kapan saja.

Detektif secara otomatis menghapus akun anggota yang dihentikan di AWS, kecuali di Wilayah AWS GovCloud (AS-Timur) dan AWS GovCloud (AS-Barat).

Ketika akun anggota yang diundang dihapus dari grafik perilaku, hal berikut akan terjadi.

- Akun anggota dihapus dari akun anggota Saya.

- Amazon Detective berhenti menelan data dari akun yang dihapus.

Detective tidak menghapus data yang ada dari grafik perilaku, yang mengumpulkan data di seluruh akun anggota.

Menghapus akun anggota yang diundang dari grafik perilaku (konsol)

Anda dapat menggunakan AWS Management Console untuk menghapus akun anggota yang diundang dari grafik perilaku Anda.

Untuk menghapus akun anggota (konsol)

1. Buka konsol Amazon Detective di. https://console.aws.amazon.com/detective/
2. Di panel navigasi Detektif, pilih Manajemen akun.
3. Dalam daftar akun, pilih kotak centang untuk menghapus setiap akun anggota.

   Anda tidak dapat menghapus akun Anda sendiri dari daftar.
4. Pilih Tindakan. Kemudian pilih Nonaktifkan akun.

Menghapus akun anggota yang diundang dari grafik perilaku (Detective API,) AWS CLI

Anda dapat menggunakan Detective API atau AWS Command Line Interface untuk menghapus akun anggota yang diundang dari grafik perilaku Anda. Untuk mendapatkan ARN dari grafik perilaku Anda untuk digunakan dalam permintaan, gunakan operasi. `ListGraphs`

Untuk menghapus akun anggota yang diundang dari grafik perilaku Anda (Detective API,) AWS CLI

- Detective API: Gunakan operasi. `DeleteMembers` Tentukan grafik ARN dan daftar pengidentifikasi akun untuk dihapus akun anggota.
- AWS CLI: Pada baris perintah, jalankan `delete-members`perintah.

```
aws detective delete-members --account-ids <account ID list> --graph-arn <behavior
 graph ARN>
```

Contoh:

```
aws detective delete-members --account-ids 444455556666 123456789012 --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Menghapus daftar akun anggota yang diundang di seluruh Wilayah (skrip Python aktif) GitHub

Detective menyediakan skrip sumber terbuka di. GitHub Anda dapat menggunakan skrip ini untuk menghapus daftar akun anggota tertentu dari grafik perilaku akun administrator di seluruh daftar Wilayah yang ditentukan.

Untuk informasi tentang cara mengkonfigurasi dan menggunakan GitHub skrip, lihatMenggunakan skrip Amazon Detective Python.

Untuk akun anggota: Mengelola undangan grafik perilaku dan keanggotaan

Amazon Detective menagih setiap akun anggota untuk data yang dicerna untuk setiap grafik perilaku yang dikontribusikannya.

Halaman Manajemen akun memungkinkan akun anggota untuk melihat akun administrator untuk grafik perilaku yang menjadi anggotanya.

Akun anggota yang diundang ke grafik perilaku dapat melihat dan menanggapi undangan mereka. Mereka juga dapat menghapus akun mereka dari grafik perilaku.

Untuk grafik perilaku organisasi, akun organisasi tidak mengontrol apakah akun mereka adalah akun anggota. Akun administrator Detektif memilih akun organisasi untuk mengaktifkan atau menonaktifkan sebagai akun anggota.

Daftar Isi

Kebijakan IAM yang diperlukan untuk akun anggota

Sebelum akun anggota dapat melihat dan mengelola undangan, kebijakan IAM yang diperlukan harus dilampirkan pada prinsipal mereka. Prinsipal dapat berupa pengguna atau peran yang sudah ada, atau Anda dapat membuat pengguna atau peran baru yang akan digunakan untuk Detektif.

Idealnya, akun administrator meminta administrator IAM mereka melampirkan kebijakan yang diperlukan.

Kebijakan IAM akun anggota memberikan akses ke tindakan akun anggota di Amazon Detective. Undangan email untuk berkontribusi pada grafik perilaku mencakup teks kebijakan IAM tersebut.

Untuk menggunakan kebijakan ini, ganti *<behavior graph ARN>* dengan grafik ARN.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:AcceptInvitation",
        "detective:DisassociateMembership",
        "detective:RejectInvitation"
      ],
      "Resource": "<behavior graph ARN>"
    },
   {
    "Effect":"Allow",
    "Action":[
        "detective:BatchGetMembershipDatasources",
        "detective:GetFreeTrialEligibility",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListInvitations"
    ],
    "Resource":"*"
   }
 ]
}
```

Perhatikan bahwa akun organisasi dalam grafik perilaku organisasi tidak menerima undangan dan tidak dapat memisahkan akun mereka dari grafik perilaku organisasi. Jika mereka tidak termasuk dalam grafik perilaku lain, maka mereka hanya memerlukan `ListInvitations` izin. `ListInvitations`memungkinkan mereka untuk melihat akun administrator untuk grafik perilaku. Izin untuk mengelola undangan dan memisahkan keanggotaan hanya berlaku untuk keanggotaan berdasarkan undangan.

Melihat daftar undangan grafik perilaku

Dari konsol Amazon Detective, Detective API, atau AWS Command Line Interface, akun anggota dapat melihat undangan grafik perilaku mereka.

Melihat undangan grafik perilaku (konsol)

Anda dapat melihat undangan grafik perilaku dari. AWS Management Console

Untuk melihat undangan grafik perilaku (konsol)

1. Masuk ke AWS Management Console. Kemudian buka konsol Detective di https://console.aws.amazon.com/detective/.
2. Di panel navigasi Detektif, pilih Manajemen akun.

Pada halaman Pengelolaan akun, Akun administrator saya berisi undangan grafik perilaku terbuka dan diterima di Wilayah saat ini. Untuk akun organisasi, Akun administrator saya juga berisi grafik perilaku organisasi.

Jika akun Anda saat ini dalam masa uji coba gratis, halaman tersebut juga menampilkan jumlah hari yang tersisa dalam uji coba gratis Anda.

Daftar tidak berisi undangan yang Anda tolak, keanggotaan yang Anda pasrahkan, atau keanggotaan yang dihapus oleh akun administrator.

Setiap undangan menunjukkan nomor akun administrator, tanggal undangan diterima, dan status undangan saat ini.

- Untuk undangan yang belum Anda tanggapi, statusnya adalah Diundang.
- Untuk undangan yang Anda terima, status Diaktifkan atau Tidak diaktifkan.

  Jika status Diaktifkan, akun Anda akan menyumbangkan data ke grafik perilaku.

  Jika status tidak diaktifkan, akun Anda tidak akan menyumbangkan data ke grafik perilaku.

  Jika akun Anda tidak menyebabkan grafik perilaku melebihi kuota Detektif, Detektif memperbarui status akun Anda ke Aktif. Jika tidak, statusnya tetap Tidak diaktifkan.

  Ketika grafik perilaku dapat mengakomodasi volume data untuk akun Anda, Detective secara otomatis memperbaruinya ke Diaktifkan. Misalnya, akun administrator mungkin menghapus akun

anggota lain sehingga akun Anda dapat diaktifkan. Akun administrator juga dapat mengaktifkan akun Anda secara manual.

Melihat undangan grafik perilaku (Detective API,) AWS CLI

Anda dapat mencantumkan undangan grafik perilaku dari Detective API atau file. AWS Command Line Interface

Untuk mengambil daftar undangan yang terbuka dan diterima ke grafik perilaku (Detective API,) AWS CLI

- Detective API: Gunakan operasi. `ListInvitations`
- AWS CLI: Pada baris perintah, jalankan `list-invitations`perintah.

```
aws detective list-invitations
```

Menanggapi undangan grafik perilaku

Setelah Anda menerima undangan, Detektif memeriksa jumlah akun anggota. Jumlah maksimum akun anggota untuk grafik perilaku adalah 1.200. Jika grafik perilaku Anda sudah berisi 1.200 akun anggota, maka akun baru tidak dapat diaktifkan.

Setelah Anda menerima undangan, Detektif diaktifkan di akun Anda. Detektif memeriksa apakah volume data Anda berada dalam kuota Detektif. Volume data yang mengalir ke grafik perilaku harus kurang dari maksimum yang diizinkan oleh Detective. Jika volume saat ini yang dicerna di atas batas 10 TB per hari, Anda tidak dapat menambahkan lebih banyak akun dan Detective akan menonaktifkan konsumsi data lebih lanjut. Konsol Detective menampilkan notifikasi untuk menunjukkan bahwa volume data terlalu besar dan statusnya tetap Tidak diaktifkan.

Jika Anda menolak undangan, maka itu dihapus dari daftar undangan Anda, dan Detektif tidak menggunakan data akun Anda dalam grafik perilaku.

Menanggapi undangan grafik perilaku (konsol)

Anda dapat menggunakan AWS Management Console untuk menanggapi undangan email, yang mencakup tautan ke konsol Detektif. Anda hanya dapat menanggapi undangan yang berstatus Diundang.

Untuk menanggapi undangan grafik perilaku (konsol)

1. Buka konsol Amazon Detective di. https://console.aws.amazon.com/detective/
2. Di panel navigasi Detektif, pilih Manajemen akun.
3. Di bawah Akun administrator saya, untuk menerima undangan dan mulai menyumbangkan data ke grafik perilaku, pilih Terima undangan.

   Untuk menolak undangan dan menghapusnya dari daftar, pilih Tolak.

Menanggapi undangan grafik perilaku (Detective API,) AWS CLI

Anda dapat menanggapi undangan grafik perilaku dari Detective API atau file. AWS Command Line Interface

Untuk menerima undangan grafik perilaku (Detective API,) AWS CLI

- Detective API: Gunakan operasi. `AcceptInvitation` Anda harus menentukan grafik ARN.
- AWS CLI: Pada baris perintah, jalankan `accept-invitation`perintah.

```
aws detective accept-invitation --graph-arn <behavior graph ARN>
```

Contoh:

```
aws detective accept-invitation --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

Untuk menolak undangan grafik perilaku (Detective API,) AWS CLI

- Detective API: Gunakan operasi. `RejectInvitation` Anda harus menentukan grafik ARN.
- AWS CLI: Pada baris perintah, jalankan `reject-invitation`perintah.

```
aws detective reject-invitation --graph-arn <behavior graph ARN>
```

Contoh:

```
aws detective reject-invitation --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

Menghapus akun Anda dari grafik perilaku

Setelah menerima undangan, Anda dapat menghapus akun dari grafik perilaku kapan saja. Saat Anda menghapus akun dari grafik perilaku, Detektif Amazon berhenti memasukkan data dari akun Anda ke dalam grafik perilaku. Data yang ada tetap dalam grafik perilaku.

Hanya akun yang diundang yang dapat menghapus akun mereka dari grafik perilaku. Akun organisasi tidak dapat menghapus akun mereka dari grafik perilaku organisasi.

Menghapus akun Anda dari grafik perilaku (Konsol)

Anda dapat menggunakan AWS Management Console untuk menghapus akun Anda dari grafik perilaku.

Untuk menghapus akun Anda dari grafik perilaku (konsol)

1. Buka konsol Amazon Detective di. https://console.aws.amazon.com/detective/
2. Di panel navigasi Detektif, pilih Manajemen akun.
3. Di bawah Akun administrator saya, untuk grafik perilaku tempat Anda ingin mengundurkan diri, pilih Mengundurkan diri.

Menghapus akun Anda dari grafik perilaku (Detective API,) AWS CLI

Anda dapat menggunakan Detective API atau AWS Command Line Interface untuk menghapus akun Anda dari grafik perilaku.

Untuk menghapus akun Anda dari grafik perilaku (Detective API,) AWS CLI

- Detective API: Gunakan operasi. `DisassociateMembership` Anda harus menentukan grafik ARN.
- AWS CLI: Pada baris perintah, jalankan `disassociate-membership`perintah.

```
aws detective disassociate-membership --graph-arn <behavior graph ARN>
```

Contoh:

```
aws detective disassociate-membership --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

Pengaruh tindakan akun pada grafik perilaku

Tindakan ini memiliki efek berikut pada data dan akses Amazon Detective.

Detective dinonaktifkan

Ketika akun administrator menonaktifkan Detective, berikut ini terjadi:

- Grafik perilaku dihapus.
- Detective berhenti menelan data dari akun administrator dan akun anggota untuk grafik perilaku tersebut.

Akun anggota dihapus dari grafik perilaku

Ketika akun anggota dihapus dari grafik perilaku, Detective berhenti menelan data dari akun tersebut.

Data yang ada dalam grafik perilaku tidak terpengaruh.

Untuk akun yang diundang, akun dihapus dari daftar Akun anggota saya.

Untuk akun organisasi dalam grafik perilaku organisasi, status akun berubah menjadi Bukan anggota.

Akun anggota meninggalkan organisasi

Ketika akun anggota meninggalkan sebuah organisasi, berikut ini terjadi:

- Akun dihapus dari daftar Akun anggota saya untuk grafik perilaku organisasi.
- Detective berhenti menelan data dari akun itu.

Data yang ada dalam grafik perilaku tidak terpengaruh.

AWSakun ditangguhkan

Ketika akun administrator ditangguhkanAWS, akun kehilangan izin untuk melihat grafik perilaku di Detective. Detective berhenti menelan data ke dalam grafik perilaku.

Ketika akun anggota ditangguhkanAWS, Detective berhenti menelan data untuk akun tersebut.

Setelah 90 hari, akun dihentikan atau diaktifkan kembali. Ketika akun administrator diaktifkan kembali, izin Detektifnya dipulihkan. Detective melanjutkan menelan data dari akun. Ketika akun anggota diaktifkan kembali, Detective melanjutkan penyerapan data dari akun.

AWSakun ditutup

KetikaAWS akun ditutup, Detective menanggapi penutupan sebagai berikut.

- Untuk akun administrator, Detective menghapus grafik perilaku.
- Untuk akun anggota, Detective menghapus akun dari grafik perilaku.

AWS mempertahankan data kebijakan untuk akun selama 90 hari sejak tanggal efektif penutupan akun administrator. Di akhir periode 90 hari, AWS menghapus semua data kebijakan untuk akun secara permanen.

- Untuk mempertahankan temuan selama lebih dari 90 hari, Anda dapat mengarsipkan kebijakan. Anda juga dapat menggunakan tindakan kustom dengan EventBridge aturan untuk menyimpan temuan dalam bucket S3.
- Selama AWS mempertahankan data kebijakan, saat Anda membuka kembali akun yang tertutup, AWS menetapkan ulang akun sebagai administrator layanan dan memulihkan data kebijakan layanan untuk akun.
- Untuk informasi selengkapnya, lihat Menutup akun.

> **Important**
>
> Untuk pelanggan di Wilayah AWS GovCloud (US):
>
> - Sebelum menutup akun Anda, cadangkan, lalu hapus sumber daya akun. Anda tidak akan lagi memiliki akses ke mereka setelah Anda menutup akun.

Melacak tindakan dan penggunaan di Amazon Detective

Untuk membantu Anda melacak aktivitas Detective Anda, halaman Penggunaan menunjukkan jumlah data yang tertelan dan biaya yang diproyeksikan.

- Untuk akun administrator, halaman Penggunaan menampilkan volume data dan biaya yang diproyeksikan di seluruh grafik perilaku.
- Untuk akun anggota, halaman Penggunaan menampilkan volume data dan proyeksi biaya untuk akun mereka di seluruh grafik perilaku yang mereka kontribusikan.

Detective juga mendukungAWS CloudTrail penebangan.

Konten

Memantau penggunaan dan biaya untuk grafik perilaku (akun administrator)

Amazon Detective menagih setiap akun untuk data yang digunakan dalam setiap grafik perilaku yang dimiliki akun tersebut. Detective mengenakan tarif tetap berjenjang per GB untuk semua data terlepas dari sumbernya.

Untuk akun administrator, halaman Penggunaan konsol Detective memungkinkan Anda untuk melihat volume data yang dicerna Berdasarkan sumber data atau Dengan akun selama 30 hari sebelumnya. Akun administrator juga melihat biaya yang diproyeksikan untuk periode 30 hari tipikal untuk akun mereka dan untuk keseluruhan grafik perilaku.

Untuk melihat informasi penggunaan Detective

1. Masuk ke AWS Management Console. Kemudian buka konsol Detective di https://console.aws.amazon.com/detective/.
2. Di panel navigasi Detective, di bawah Pengaturan, pilih Penggunaan.

3. Pilih tab untuk memilih antara melihat penggunaan Berdasarkan sumber data atau Menurut akun.

Volume data yang dicerna untuk setiap akun

Volume yang tertelan oleh akun anggota mencantumkan akun aktif dalam grafik perilaku. Itu tidak mencantumkan akun anggota yang telah dihapus.

Untuk setiap akun, daftar volume yang dicerna menyediakan informasi berikut.

- Alamat email pengguna root dan pengenalAWS akun.
- Tanggal ketika akun mulai menyumbangkan data ke grafik perilaku.

  Untuk akun administrator, ini adalah tanggal ketika akun diaktifkan Detective.

  Untuk akun anggota, ini adalah tanggal ketika akun diaktifkan sebagai akun anggota setelah menerima undangan.
- Volume data yang dicerna dari akun selama 30 hari sebelumnya. Total mencakup semua jenis sumber.
- Apakah akun tersebut saat ini dalam periode uji coba gratis. Untuk akun yang saat ini dalam masa uji coba gratis, daftar tersebut menampilkan jumlah hari yang tersisa.

  Jika tidak ada akun yang berada dalam periode uji coba gratis, maka kolom status uji coba gratis tidak ditampilkan.

Biaya yang diproyeksikan untuk grafik perilaku

Biaya proyeksi akun ini menunjukkan biaya yang diproyeksikan selama 30 hari data untuk akun administrator. Biaya yang diproyeksikan didasarkan pada volume rata-rata harian untuk akun administrator.

> **Important**
>
> Jumlah ini hanya biaya yang diproyeksikan. Ini memproyeksikan total biaya untuk data akun administrator untuk jangka waktu 30 hari yang khas. Hal ini didasarkan pada penggunaan dari 30 hari sebelumnya. Lihat the section called “Bagaimana Detective menghitung biaya yang diproyeksikan”.

Biaya yang diproyeksikan untuk grafik perilaku

Biaya proyeksi semua akun menunjukkan total biaya yang diproyeksikan selama 30 hari data untuk keseluruhan grafik perilaku. Biaya yang diproyeksikan didasarkan pada volume rata-rata harian untuk setiap akun.

> **Important**
>
> Jumlah ini hanya biaya yang diproyeksikan. Ini memproyeksikan total biaya untuk data grafik perilaku untuk jangka waktu 30 hari yang khas. Hal ini didasarkan pada penggunaan dari 30 hari sebelumnya. Biaya yang diproyeksikan tidak termasuk akun anggota yang dihapus dari grafik perilaku. Lihat the section called “Bagaimana Detective menghitung biaya yang diproyeksikan”.

Volume data yang dicerna oleh paket sumber

Pilih Berdasarkan paket sumber untuk melihat volume data yang dicantumkan oleh paket sumber berbeda yang diaktifkan dalam grafik perilaku Anda.

Semua akun dapat melihat data ini untuk akun mereka sendiri. Akun administrator dapat melihat panel tambahan yang mencantumkan penggunaan berdasarkan paket sumber untuk setiap anggota. Itu tidak mencantumkan akun anggota yang telah dihapus.

Inti Detective

Panel inti Detective menunjukkan volume data yang dicerna dari sumber inti Detective (CloudTrail log, log Aliran VPC, dan GuardDuty temuan) selama 30 hari terakhir.

Log audit EKS

Panel log audit EKS menunjukkan volume data yang dicerna dari sumber log audit EKS selama 30 hari terakhir. Panel untuk paket sumber ini hanya tersedia jika log audit EKS diaktifkan untuk grafik perilaku Anda.

Memantau penggunaan dan biaya di seluruh grafik perilaku (akun anggota)

Amazon Detective menagih setiap akun untuk data yang digunakan dalam setiap grafik perilaku yang dimiliki akun tersebut. Detective mengenakan tarif tetap berjenjang per GB untuk semua data terlepas dari sumbernya.

Untuk akun anggota, halaman Penggunaan menampilkan volume data dan proyeksi biaya 30 hari untuk akun tersebut saja.

Untuk melihat informasi penggunaan Detective

1. Masuk ke AWS Management Console. Kemudian buka konsol Detective di https://console.aws.amazon.com/detective/.
2. Di panel navigasi Detective, di bawah Pengaturan, pilih Penggunaan.

Volume yang tertelan untuk setiap grafik perilaku

Volume tertelan akun ini mencantumkan grafik perilaku yang berkontribusi pada akun anggota. Ini tidak termasuk keanggotaan yang Anda mengundurkan diri, atau keanggotaan yang dihapus akun administrator.

Untuk setiap grafik perilaku, daftar menyertakan informasi berikut.

- Nomor akun akun administrator
- Volume data yang dicerna dari akun anggota selama 30 hari sebelumnya. Total mencakup semua jenis sumber.
- Tanggal akun yang diaktifkan untuk grafik perilaku.

Biaya yang diproyeksikan di seluruh grafik perilaku

Biaya proyeksi akun ini menunjukkan biaya yang diproyeksikan selama 30 hari data untuk akun anggota di semua grafik perilaku yang dikontribusikan. Biaya yang diproyeksikan didasarkan pada volume rata-rata harian untuk akun anggota.

> **Important**
>
> Jumlah ini hanya biaya yang diproyeksikan. Ini memproyeksikan total biaya untuk data akun administrator untuk jangka waktu 30 hari yang khas. Hal ini didasarkan pada penggunaan dari 30 hari sebelumnya. Lihat the section called “Bagaimana Detective menghitung biaya yang diproyeksikan”.

Bagaimana Amazon Detective menghitung biaya yang diproyeksikan

Untuk menghitung nilai biaya yang diproyeksikan yang ditampilkan pada halaman Penggunaan, Detective melakukan hal berikut.

1. Untuk mendapatkan biaya yang diproyeksikan untuk akun individu dalam grafik perilaku, Detective melakukan hal berikut.
   a. Menghitung volume rata-rata per hari. Ini menambahkan volume data di semua hari aktif dan kemudian membaginya dengan jumlah hari akun telah aktif.

      Jika akun diaktifkan lebih dari 30 hari yang lalu, maka jumlah hari adalah 30. Jika akun diaktifkan kurang dari 30 hari yang lalu, maka itu adalah jumlah hari sejak tanggal penerimaan.

      Misalnya, jika akun diaktifkan 12 hari yang lalu, maka Detective menambahkan volume yang dicerna selama 12 hari itu dan kemudian membaginya dengan 12.
   b. Mengalikan rata-rata harian akun dengan 30. Ini adalah proyeksi penggunaan 30 hari untuk akun.
   c. Menggunakan model harga untuk menghitung biaya 30 hari yang diproyeksikan untuk penggunaan 30 hari yang diproyeksikan.
2. Untuk mendapatkan total biaya yang diproyeksikan untuk grafik perilaku, Detective melakukan hal berikut:
   a. Menggabungkan proyeksi penggunaan 30 hari dari semua akun dalam grafik perilaku.
   b. Menggunakan model harga untuk menghitung biaya 30 hari yang diproyeksikan untuk total proyeksi penggunaan 30 hari.
3. Untuk mendapatkan total biaya yang diproyeksikan untuk akun anggota di seluruh grafik perilaku, Detective melakukan hal berikut:

a. Menggabungkan proyeksi penggunaan 30 hari di semua grafik perilaku.

b. Menggunakan model harga untuk menghitung proyeksi biaya 30 hari untuk total proyeksi penggunaan 30 hari.

4. Jika Anda menggunakan VPC Amazon bersama, Detektif menghitung biaya yang diproyeksikan berdasarkan aktivitas pemantauan. Kami menyarankan Anda meninjau biaya yang diproyeksikan untuk investigasi khusus untuk lingkungan Anda.

   a. Jika akun anggota Detektif memiliki VPC Amazon bersama dan ada akun Non-Detektif lainnya yang menggunakan VPC bersama, Detektif akan memantau semua lalu lintas dari VPC tersebut. Penggunaan dan biaya akan meningkat dan Detective akan memberikan visualisasi pada semua arus lalu lintas dalam VPC.

   b. Jika Anda memiliki instans EC2 di dalam VPC Amazon bersama dan pemilik bersama bukan anggota Detektif, Detektif tidak akan memantau lalu lintas apa pun dari VPC, dan penggunaan serta biaya akan berkurang. Jika Anda ingin melihat arus lalu lintas dalam VPC, Anda harus menambahkan pemilik Amazon VPC sebagai anggota grafik Detektif Anda.

Mencatat log panggilan API Amazon Detective denganAWS CloudTrail

Detective terintegrasi denganAWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atauAWS layanan di Detective. CloudTrail menangkap semua panggilan API untuk Detective sebagai peristiwa. Panggilan yang direkam mencakup panggilan dari konsol Detective dan panggilan kode ke operasi API Detective.

- Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman berkelanjutan dari CloudTrail peristiwa ke bucket Amazon S3, termasuk peristiwa untuk Detective.
- Jika Anda tidak membuat konfigurasi jejak, Anda masih dapat melihat kejadian terbaru dalam konsol CloudTrail di Riwayat peristiwa.

Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan hal berikut:

- Permintaan yang dibuat untuk Detective
- Alamat IP dari mana permintaan itu dibuat
- Siapa yang membuat permintaan

- Ketika itu dibuat
- Detail tambahan tentang permintaan

Untuk mempelajari lebih lanjut CloudTrail, lihat PanduanAWS CloudTrail Pengguna.

Informasi Detective di CloudTrail

CloudTrail diaktifkan diAWS akun Anda saat Anda membuat akun. Ketika aktivitas terjadi di Detective, aktivitas tersebut dicatat dalam CloudTrail peristiwa, bersama peristiwaAWS layanan lainnya, di Riwayat. Anda dapat melihat, mencari, dan mengunduh peristiwa terbaru di akun AWS Anda. Untuk informasi selengkapnya, lihat Melihat Kejadian dengan Riwayat CloudTrail Kejadian.

Untuk catatan berkelanjutan tentang peristiwa diAWS akun Anda, termasuk peristiwa untuk Detective, buat jejak. Jejak memungkinkan CloudTrail untuk mengirim berkas log ke bucket Amazon S3.

Secara default, saat Anda membuat jejak di dalam konsol tersebut, jejak diterapkan ke semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di partisi AWS dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Anda juga dapat mengonfigurasiAWS layanan lainnya untuk menganalisis lebih lanjut dan bertindak berdasarkan data peristiwa yang dikumpulkan di CloudTrail log.

Untuk informasi selengkapnya, lihat yang berikut:

- Ikhtisar untuk Membuat Jejak
- CloudTrail Layanan dan Integrasi yang Didukung
- Mengonfigurasi Notifikasi Amazon SNS untuk CloudTrail
- Menerima Berkas CloudTrail Log dari Beberapa Wilayah dan Menerima Berkas CloudTrail Log dari Beberapa Akun

CloudTrail mencatat semua operasi Detective, yang didokumentasikan dalam Detective API Reference.

Misalnya, panggilan ke`CreateMembers`,`AcceptInvitation`, dan`DeleteMembers` operasi menghasilkan entri dalam file CloudTrail log.

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

- Jika permintaan tersebut dibuat dengan kredensial pengguna root atau AWS Identity and Access Management (IAM)
- Jika permintaan tersebut dibuat dengan kredensi keamanan sementara atau tidak untuk peran atau pengguna gabungan
- Jika permintaan tersebut dibuat oleh layanan AWS lainnya

Untuk informasi lain, lihat Elemen userIdentity CloudTrail .

Memahami entri berkas log Detective

Jejak adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai berkas log ke bucket Amazon S3 yang Anda tentukan. CloudTrail berkas log berisi satu atau beberapa entri log.

Peristiwa menunjukkan satu permintaan dari sumber mana pun. Peristiwa mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail berkas log bukan jejak API publik, sehingga entri tersebut tidak muncul dalam urutan tertentu.

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


```
      {
            "EventId": "f2545ee3-170f-4340-8af4-a983c669ce37",
            "Username": "JaneRoe",
            "EventTime": 1571956406.0,
            "CloudTrailEvent": "{\"eventVersion\":\"1.05\",\"userIdentity\":
{\"type\":\"AssumedRole\",\"principalId\":\"AROAJZARKEP6WKJ5JHSUS:JaneRoe\",\"arn
\":\"arn:aws:sts::111122223333:assumed-role/1A4R5SKSPGG9V/JaneRoe\",\"accountId
\":\"111122223333\",\"accessKeyId\":\"AKIAIOSFODNN7EXAMPLE\",\"sessionContext\":
{\"attributes\":{\"mfaAuthenticated\":\"false\",\"creationDate\":\"2019-10-24T21:54:56Z
\"},\"sessionIssuer\":{\"type\":\"Role\",\"principalId\":\"AROAJZARKEP6WKJ5JHSUS
\",\"arn\":\"arn:aws:iam::111122223333:role/1A4R5SKSPGG9V\",\"accountId\":
\"111122223333\",\"userName\":\"JaneRoe\"}}},\"eventTime\":\"2019-10-24T22:33:26Z
\",\"eventSource\":\"detective.amazonaws.com\",\"eventName\":\"AcceptInvitation
\",\"awsRegion\":\"us-east-2\",\"sourceIPAddress\":\"192.0.2.123\",\"userAgent
\":\"aws /3 aws-sdk-java/1.11.648 Linux/4.14.133-97.112.amzn2.x86_64 OpenJDK_64-
Bit_Server_VM/25.201-b09 java/1.8.0_201 vendor/Oracle_Corporation exec-env/
AWS_Lambda_java8\",\"errorCode\":\"ValidationException\",\"requestParameters\":
{\"masterAccount\":\"111111111111\"},\"responseElements\":{\"message\":\"Invalid
 request body\"},\"requestID\":\"8437ff99-5ec4-4b1a-8353-173be984301f\",\"eventID\":
```

\"f2545ee3-170f-4340-8af4-a983c669ce37\",\"readOnly\":false,\"eventType\":\"AwsApiCall
\",\"recipientAccountId\":\"111122223333\"}",
            "EventName": "AcceptInvitation",
            "EventSource": "detective.amazonaws.com",
            "Resources": []
        },

Mengelola tag untuk grafik perilaku

Anda dapat menetapkan tag ke grafik perilaku. Anda kemudian dapat menggunakan nilai tag dalam kebijakan IAM untuk mengelola akses ke fungsi grafik perilaku di Detective. Lihat the section called “Otorisasi berdasarkan tag grafik perilaku Detektif”.

Anda juga dapat menggunakan tag sebagai alat untuk pelaporan biaya. Misalnya, untuk melacak biaya yang terkait dengan keamanan, Anda dapat menetapkan tag yang sama ke grafik perilaku Detective, sumber dayaAWS Security Hub hub, dan GuardDuty detektor Amazon. DiAWS Cost Explorer, Anda kemudian dapat mencari tag itu untuk melihat tampilan konsolidasi biaya di seluruh sumber daya tersebut.

Melihat tag untuk grafik perilaku (Console)

Anda mengelola tag untuk grafik perilaku Anda dari halaman Umum.

Untuk melihat daftar tag yang ditetapkan ke grafik perilaku

1. Buka konsol Detective Amazon dihttps://console.aws.amazon.com/detective/.
2. Di panel navigasi, pada Pengaturan, pilih Umum.

Mencantumkan tag untuk grafik perilaku (Detective API,AWS CLI)

Anda dapat menggunakan Detective API atauAWS Command Line Interface untuk mendapatkan daftar tag untuk grafik perilaku Anda.

Untuk mendapatkan daftar tag untuk grafik perilaku (Detective API,AWS CLI)

- Detective API: Gunakan `ListTagsForResource`operasi. Anda harus memberikan ARN grafik perilaku Anda.
- AWS CLI: Pada baris perintah, jalankan`list-tags-for-resource` perintah.

```
aws detective list-tags-for-resource --resource-arn <behavior graph ARN>
```

Contoh

```
aws detective list-tags-for-resource --resource-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

Penambahan tag ke grafik

Dari daftar tag pada halaman Umum, Anda dapat menambahkan nilai tag ke grafik perilaku.

Menambahkan tag ke grafik perilaku

1. Pilih Add new tag (Tambahkan tanda baru).
2. Untuk Kunci, masukkan nama tag.
3. Untuk Nilai, masukkan nilai tag.

Menambahkan tag ke grafik perilaku (Detective API,AWS CLI)

Anda dapat menggunakan Detective API atauAWS CLI untuk menambahkan nilai tag ke grafik perilaku Anda.

Untuk menambahkan tag ke grafik perilaku (Detective API,AWS CLI)

- Detective API: Gunakan `TagResource`operasi. Anda memberikan grafik perilaku ARN dan nilai tag untuk ditambahkan.
- AWS CLI: Pada baris perintah, jalankan`tag-resource` perintah.

```
aws-detective tag-resource --aws detective tag-resource --resource-arn <behavior
 graph ARN> --tags '{"TagName":"TagValue"}'
```

Contoh

```
aws detective tag-resource --resource-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234 --tags '{"Department":"Finance"}'
```

Removing tags from a behavior graph (Console)

Untuk menghapus tag dari daftar di halaman Umum, pilih opsi Hapus untuk tag tersebut.

Menghapus tag dari grafik perilaku (Detective API,AWS CLI)

Anda dapat menggunakan Detective API atauAWS CLI untuk menghapus nilai tag dari grafik perilaku Anda.

Untuk menghapus tag dari grafik perilaku (Detective API,AWS CLI)

- Detective API: Gunakan `UntagResource`operasi. Anda memberikan grafik perilaku ARN, dan nama-nama tag yang akan dihapus.
- AWS CLI: Pada baris perintah, jalankan`untag-resource` perintah.

```
aws detective untag-resource --resource-arn <behavior graph ARN> --tag-keys "TagName"
```

Contoh

```
aws detective untag-resource --resource-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234 --tag-keys "Department"
```

Keamanan di Amazon Detective

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

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

- Keamanan cloud – AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan layanan AWS di dalam AWS Cloud. AWS juga memberi layanan yang dapat Anda gunakan dengan aman.

  Auditor pihak ketiga menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari program kepatuhan AWS.

  Untuk mempelajari tentang program kepatuhan yang berlaku untuk Detektif Amazon, lihat AWSLayanan dalam Lingkup berdasarkan Program Kepatuhan.
- Keamanan di cloud – Tanggung jawab Anda ditentukan menurut layanan AWS yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain termasuk sensitivitas data Anda, persyaratan perusahaan Anda, serta hukum dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan Detective. Topik berikut menunjukkan cara mengonfigurasi Detektif untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga belajar cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan sumber daya Detektif Anda.

Konten

- Keamanan infrastruktur di Amazon Detective
- Praktik praktik Praktik Praktik Praktik Praktik Praktik Praktik Detective

Perlindungan data di Amazon Detective

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di Amazon Detective. Sebagaimana diuraikan dalam model ini, AWS bertanggung jawab untuk memberikan perlindungan terhadap infrastruktur global yang menjalankan semua AWS Cloud. Anda harus bertanggung jawab untuk memelihara kendali terhadap konten yang di-hosting pada infrastruktur ini. Anda juga bertanggung jawab atas tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Untuk informasi selengkapnya tentang privasi data, lihat FAQ Privasi Data. Untuk informasi tentang perlindungan data di Eropa, silakan lihat postingan blog Model Tanggung Jawab Bersama AWS dan GDPR di Blog Keamanan AWS.

Untuk tujuan perlindungan data, sebaiknya Anda melindungi kredensial Akun AWS dan menyiapkan AWS IAM Identity Center atau AWS Identity and Access Management (IAM) untuk pengguna individu. Dengan cara seperti itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugas mereka. Kami juga merekomendasikan agar Anda mengamankan data Anda dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk melakukan komunikasi dengan sumber daya AWS. Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Siapkan API dan log aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi enkripsi AWS, bersama dengan semua kontrol keamanan default dalam Layanan AWS.
- Gunakan layanan keamanan terkelola lanjutan seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 ketika mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Untuk informasi selengkapnya tentang titik akhir FIPS yang tersedia, silakan lihat Standar Pemrosesan Informasi Federal (FIPS) 140-2.

Sebaiknya Anda tidak memasukkan informasi rahasia atau sensitif, seperti alamat email pelanggan, ke dalam tanda atau bidang teks bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan Detective atau lainnya Layanan AWS menggunakan konsol, APIAWS CLI, atau AWS SDK. Data apa

pun yang Anda masukkan ke dalam tanda atau bidang teks bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau diagnostik. Saat Anda memberikan URL ke server eksternal, sebaiknya Anda tidak menyertakan informasi kredensial di URL untuk memvalidasi permintaan Anda ke server tersebut.

Detective mengenkripsi semua data yang diproses dan disimpan saat istirahat dan dalam perjalanan.

Konten

Manajemen kunci untuk Amazon Detective

Karena Detective tidak menyimpan data pelanggan yang dapat diidentifikasi secara pribadi, ia menggunakanKunci yang dikelola AWS.

Jenis kunci KMS ini dapat digunakan di beberapa akun. LihatdeskripsiAWSkunci yang dimiliki diAWS Key Management ServicePanduan Developer Developer.

Jenis tombol KMS ini berputar secara otomatis setiap satu tahun (sekitar 365 hari). Lihatdeskripsi rotasi kunci diAWS Key Management ServicePanduan Developer Developer.

Manajemen identitas dan akses untuk Amazon Detective

(IAM) AWS Identity and Access Management adalah Layanan AWS yang membantu seorang administrator dalam mengendalikan akses ke sumber daya AWS secara aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya Detektif. IAM adalah sebuah layanan Layanan AWS yang dapat Anda gunakan tanpa dikenakan biaya tambahan.

Daftar Isi

Audiens

Bagaimana Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan di Detective.

Pengguna layanan — Jika Anda menggunakan layanan Detektif untuk melakukan pekerjaan Anda, maka administrator Anda memberi Anda kredensi dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak fitur Detektif 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 Detective, lihat. Memecahkan masalah identitas dan akses Detektif Amazon

Administrator layanan — Jika Anda bertanggung jawab atas sumber daya Detektif di perusahaan Anda, Anda mungkin memiliki akses penuh ke Detektif. Tugas Anda adalah menentukan fitur dan sumber daya Detektif mana yang harus diakses pengguna layanan Anda. Kemudian, Anda harus mengirimkan permintaan kepada administrator IAM Anda untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep dasar IAM. Untuk mempelajari lebih lanjut tentang bagaimana perusahaan Anda dapat menggunakan IAM dengan Detective, lihat. Bagaimana Amazon Detective bekerja dengan IAM

Administrator IAM — Jika Anda seorang administrator IAM, Anda mungkin ingin mempelajari detail tentang cara menulis kebijakan untuk mengelola akses ke Detektif. Untuk melihat contoh kebijakan berbasis identitas Detektif yang dapat Anda gunakan di IAM, lihat. Contoh kebijakan berbasis identitas Detektif Amazon

Mengautentikasi Menggunakan Identitas

Autentikasi merupakan cara Anda untuk masuk ke AWS dengan menggunakan kredensial identitas Anda. Anda harus terautentikasi (masuk keAWS) sebagai Pengguna root akun AWS, sebagai pengguna IAM, atau dengan mengambil peran IAM.

Anda dapat masuk ke AWS sebagai identitas terfederasi dengan menggunakan kredensial yang disediakan melalui sumber identitas. AWS IAM Identity Center Para pengguna (Pusat Identitas IAM), otentikasi sign-on tunggal perusahaan Anda, dan kredensial Google atau Facebook Anda merupakan contoh identitas terfederasi. Saat Anda masuk sebagai identitas terfederasi, administrator Anda sebelumnya menyiapkan federasi identitas dengan menggunakan peran IAM. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil suatu peran.

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

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 kredensial Anda. Jika Anda tidak menggunakan peralatan AWS, maka Anda harus menandatangani sendiri permintaan tersebut. Untuk informasi selengkapnya tentang penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, silakan lihat Menandatangani permintaan API AWS di Panduan Pengguna IAM.

Terlepas dari metode autentikasi yang Anda gunakan, Anda mungkin juga diminta untuk menyediakan informasi keamanan tambahan. Sebagai contoh, AWS menyarankan supaya Anda menggunakan autentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari selengkapnya, silakan lihat Autentikasi multi-faktor di Panduan Pengguna AWS IAM Identity Center dan Menggunakan autentikasi multi-faktor (MFA) di AWS di Panduan Pengguna IAM.

Pengguna root Akun AWS

Ketika Anda membuat Akun AWS, Anda memulai dengan satu identitas masuk yang memiliki akses ke semua Layanan AWS dan sumber daya di akun tersebut. Identitas ini disebut pengguna root Akun AWS dan diakses dengan cara masuk ke alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan 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, silakan lihat Tugas yang memerlukan kredensial pengguna root di Panduan Pengguna IAM.

Pengguna dan Grup IAM

Pengguna IAM adalah identitas dalam Akun AWS Anda yang memiliki izin khusus untuk satu orang atau aplikasi. Apabila memungkinkan, kami menyarankan untuk mengandalkan pada kredensial temporer alih-alih membuat pengguna IAM yang memiliki kredensyal jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan khusus yang memerlukan kredensial jangka panjang dengan pengguna IAM, kami menyarankan Anda memutar kunci akses. Untuk informasi selengkapnya, silakan lihat Memutar kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang di Panduan Pengguna IAM.

Grup IAM adalah identitas yang menerangkan secara spesifik kumpulan pengguna IAM. Anda tidak dapat masuk sebagai kelompok. Anda dapat menggunakan grup untuk menerangkan secara spesifik izin untuk beberapa pengguna sekaligus. Grup membuat izin lebih mudah dikelola untuk sekelompok besar pengguna. Sebagai contoh, Anda dapat memiliki grup yang diberi nama AdminIAM dan memberikan izin kepada grup tersebut untuk mengelola sumber daya IAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran tersebut dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial temporer. Untuk mempelajari selengkapnya, silakan lihat Kapan harus membuat pengguna IAM (alih-alih peran) di Panduan Pengguna IAM.

IAM Role

Peran IAM merupakan identitas dalam Akun AWS Anda yang memiliki izin khusus. Peran ini mirip dengan pengguna IAM, tetapi tidak terkait dengan orang tertentu. Anda dapat menggunakan peran IAM untuk sementara dalam AWS Management Console dengan berganti peran. Anda dapat mengambil peran dengan cara memanggil operasi API AWS CLI atau AWS atau menggunakan URL kustom. Untuk informasi selengkapnya tentang cara menggunakan peran, silakan lihat menggunakan peran IAM di Panduan Pengguna IAM.

IAM role dengan kredensial temporer berguna dalam situasi berikut:

- Akses pengguna gabungan – Untuk menetapkan izin ke sebuah identitas terfederasi, Anda harus membuat sebuah peran dan menentukan izin untuk peran tersebut. Ketika identitas gabungan terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberikan izin yang ditentukan oleh peran. Untuk informasi tentang peran-peran untuk federasi, silakan lihat Membuat sebuah peran untuk Penyedia Identitas pihak ketiga di Panduan Pengguna IAM. Jika Anda menggunakan Pusat Identitas IAM, Anda mengonfigurasi serangkain izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas tersebut diautentikasi, Pusat Identitas IAM mengkorelasikan izin yang diatur ke peran dalam IAM. Untuk informasi tentang rangkaian izin, silakan lihat Rangkaian izin di Panduan Pengguna AWS IAM Identity Center.
- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM untuk sementara mengambil izin berbeda untuk tugas tertentu.
- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (pengguna utama tepercaya) di akun berbeda untuk mengakses sumber daya yang ada di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, pada beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih

menggunakan suatu peran sebagai proksi). Untuk mempelajari perbedaan antara kebijakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, silakan lihat Bagaimana peran IAM role berbeda dari kebijakan berbasis sumber daya dalam Panduan Pengguna IAM.

- Akses lintas layanan – Sebagian Layanan AWS menggunakan fitur di Layanan AWS lainnya. Sebagai contoh, ketika Anda melakukan panggilan dalam suatu layanan, lazim pada layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Suatu layanan mungkin melakukan hal tersebut menggunakan izin pengguna utama panggilan, menggunakan peran layanan, atau peran tertaut layanan.
  - Sesi akses maju (FAS) – Ketika Anda menggunakan pengguna IAM atau peran IAM untuk melakukan tindakan-tindakan di AWS, Anda akan dianggap sebagai seorang pengguna utama. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian dilanjutkan oleh tindakan lain pada layanan yang berbeda. FAS menggunakan izin dari pengguna utama untuk memanggil Layanan AWS, yang dikombinasikan dengan Layanan AWS yang diminta untuk membuat pengajuan ke layanan hilir. Permintaan FAS hanya diajukan ketika sebuah layanan menerima pengajuan yang memerlukan interaksi dengan Layanan AWS lain atau sumber daya lain untuk diselesaikan. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, silakan lihat Meneruskan sesi akses.
  - Peran layanan – Sebuah peran layanan adalah sebuah peran IAM yang dijalankan oleh suatu layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, memodifikasi, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, silakan lihat Membuat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.
  - Peran tertaut layanan – Peran tertaut layanan adalah tipe peran layanan yang tertaut dengan Layanan AWS. Layanan tersebut dapat menjalankan peran untuk melakukan sebuah tindakan atas nama Anda. Peran tertaut layanan akan muncul di Akun AWS Anda dan dimiliki oleh layanan tersebut. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran tertaut layanan.
- Aplikasi yang berjalan di Amazon EC2 – Anda dapat menggunakan peran IAM untuk mengelola kredensial temporer untuk aplikasi yang berjalan di instans EC2 dan mengajukan permintaan AWS CLI atau API AWS. Cara ini lebih baik daripada menyimpan kunci akses dalam instans EC2. Untuk menugaskan sebuah peran AWS ke instans EC2 dan membuatnya tersedia untuk semua aplikasinya, Anda dapat membuat sebuah profil instans yang dilampirkan ke instans. Profil instans berisi peran dan memungkinkan program yang berjalan di instans EC2 untuk mendapatkan

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

Untuk mempelajari apakah kita harus menggunakan peran IAM atau pengguna IAM, silakan lihat Kapan harus membuat peran IAM (alih-alih pengguna) di Panduan Pengguna IAM.

Mengelola Akses Menggunakan Kebijakan

Anda mengendalikan akses di AWS dengan membuat kebijakan dan melampirkannya ke identitas atau sumber daya AWS. Kebijakan adalah objek di AWS yang, ketika terkait dengan identitas atau sumber daya, akan menentukan izinnya. AWS mengevaluasi kebijakan-kebijakan tersebut ketika seorang pengguna utama (pengguna, root user, atau sesi peran) mengajukan permintaan. Izin dalam kebijakan menentukan apakah permintaan diberikan atau ditolak. Sebagian besar kebijakan disimpan di AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang struktur dan isi dokumen kebijakan JSON, silakan lihat Gambaran Umum kebijakan JSON di Panduan Pengguna IAM.

Administrator dapat menggunakan kebijakan JSON AWS untuk menentukan secara spesifik siapa yang memiliki akses pada apa. Yaitu, pengguna utama manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan syarat apa.

Secara bawaan, para pengguna dan peran tidak memiliki izin. Untuk mengabulkan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian akan dapat menambahkan kebijakan IAM ke peran, dan para pengguna dapat mengambil peran.

Kebijakan IAM mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk pengoperasiannya. Sebagai contoh, anggap saja Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole` . Pengguna dengan kebijakan tersebut dapat memperoleh informasi peran dari AWS Management Console, AWS CLI, atau APIAWS.

Kebijakan Berbasis Identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, misalnya pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol apa yang pengguna tindakan dan peran dapat kerjakan, pada sumber daya mana, dan dalam keadaan apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, silakan lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan terkelola. Kebijakan inline ditanam secara langsung ke pengguna tunggal, grup, atau peran. Kebijakan terkelola adalah kebijakan yang berdiri sendiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran di Akun AWS Anda. Kebijakan terkelola mencakup kebijakan terkelola AWS dan kebijakan terkelola pelanggan. Untuk mempelajari cara memilih antara kebijakan terkelola atau kebijakan inline, silakan lihat Memilih antara kebijakan terkelola dan kebijakan inline diPanduan Pengguna IAM.

Kebijakan Berbasis Sumber Daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan-kebijakan berbasis sumber daya adalah kebijakan terpercaya peran IAM 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 yang dilampiri kebijakan, kebijakan tersebut menentkan tindakan apa yang dapat dilakukan oleh pengguna utama yang ditentukan di sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan pengguna utama dalam kebijakan berbasis sumber daya. Pengguna utama dapat mencakup akun, pengguna, peran, pengguna gabungan, atau Layanan AWS.

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

Daftar Kontrol Akses (ACL)

Daftar kontrol akses (ACL) mengendalikan pengguna utama mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis sumber daya, meskipun kebijakan-kebijakan tersebut tidak menggunakan format dokumen kebijakan JSON.

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh-contoh layanan yang mendukung ACL. Untuk mempelajari ACL selengkapnya, silakan lihat Gambaran umum daftar kontrol akses (ACL) di Panduan Pengembang Layanan Penyimpanan Ringkas Amazon.

Tipe Kebijakan Lainnya

AWS mendukung tipe kebijakan tambahan, yang kurang umum. Tipe-tipe kebijakan ini dapat mengatur izin maksimum yang diberikan kepada Anda oleh tipe kebijakan yang lebih umum.

- Batasan izin – Batasan izin adalah fitur lanjutan tempat Anda mengatur izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas IAM (pengguna IAM atau peran IAM).

Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batas 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 menindihi izin. Untuk informasi selengkapnya tentang batasan izin, silakan lihat Batasan izin untuk entitas IAM di Panduan Pengguna IAM.

- Kebijakan kontrol layanan (SCP) – SCP adalah kebijakan JSON yang menentukan izin maksimum untuk sebuah organisasi atau unit organisasi (OU) di AWS Organizations. AWS Organizations adalah layanan untuk mengelompokkan dan secara terpusat mengelola beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur di suatu organisasi, maka Anda dapat menerapkan kebijakan kontrol layanan (SCP) ke salah satu atau ke semua akun Anda. SCP membatasi izin untuk entitas dalam akun anggota, termasuk setiap Pengguna root akun AWS. Untuk informasi selengkapnya tentang Organisasi dan SCP, silakan lihat Cara kerja SCP di Panduan Pengguna AWS Organizations.
- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara terprogram untuk peran atau pengguna gabungan. Izin sesi yang dihasilkan adalah perpotongan kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga dapat berasal dari kebijakan berbasis sumber daya. Penolakan eksplisit dalam salah satu kebijakan ini menindihi izin. Untuk informasi selengkapnya, silakan lihat Kebijakan sesi di Panduan Pengguna IAM.

Berbagai Tipe Kebijakan

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

Bagaimana Amazon Detective bekerja dengan IAM

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya Detektif Amazon. Mereka juga tidak dapat melakukan tugas menggunakan API AWS Management Console, AWS CLI, or AWS. Administrator Detektif harus memiliki kebijakan AWS Identity and Access Management (IAM) yang memberikan izin kepada pengguna dan peran IAM 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.

Detective menggunakan kebijakan berbasis identitas IAM untuk memberikan izin untuk jenis pengguna dan tindakan berikut:

- Akun administrator — Akun administrator adalah pemilik grafik perilaku, yang menggunakan data dari akun mereka. Akun administrator dapat mengundang akun anggota untuk menyumbangkan data mereka ke grafik perilaku. Mereka juga menggunakan grafik perilaku untuk triase dan penyelidikan temuan dan sumber daya yang terkait dengan akun tersebut.

  Anda dapat menyiapkan kebijakan agar pengguna selain akun administrator dapat melakukan berbagai jenis tugas. Misalnya, pengguna dari akun administrator mungkin hanya memiliki izin untuk mengelola akun anggota. Pengguna lain mungkin hanya memiliki izin untuk menggunakan grafik perilaku untuk penyelidikan.
- Akun anggota — Akun anggota adalah akun yang diundang untuk menyumbangkan data ke grafik perilaku. Akun anggota menanggapi undangan. Setelah menerima undangan, akun anggota dapat menghapus akun mereka dari grafik perilaku.

Untuk mendapatkan tampilan tingkat tinggi tentang cara kerja Detektif dan Layanan AWS lainnya dengan IAM, lihat Membuat kebijakan pada tab JSON di Panduan Pengguna IAM.

Kebijakan berbasis identitas Detektif

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan tindakan dan sumber daya yang diizinkan atau ditolak, serta kondisi di mana tindakan diizinkan atau ditolak. Detective mendukung tindakan, sumber daya, dan kunci kondisi tertentu.

Untuk mempelajari semua elemen yang Anda gunakan dalam kebijakan JSON, lihat Referensi Elemen Kebijakan JSON IAM dalam Panduan Pengguna IAM.

Tindakan

Administrator dapat menggunakan kebijakan JSON AWS untuk menentukan secara spesifik siapa yang memiliki akses pada apa. Yaitu, pengguna utama manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan syarat apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan-tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Tindakan-tindakan kebijakan biasanya memiliki nama yang sama sebagaimana operasi API AWS yang dikaitkan padanya. Ada beberapa pengecualian, misalnya tindakan yang memiliki izin saja yang tidak memiliki operasi

API yang cocok. Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam sebuah kebijakan. Tindakan-tindakan tambahan ini disebut tindakan dependen.

Menyertakan tindakan dalam suatu kebijakan untuk memberikan izin guna melakukan operasi yang terkait.

Pernyataan kebijakan harus mencakup `Action` elemen atau `NotAction` elemen. `Action`Elemen mencantumkan tindakan yang diizinkan oleh kebijakan. `NotAction`Elemen mencantumkan tindakan yang tidak diizinkan.

Tindakan yang didefinisikan untuk Detective mencerminkan tugas yang dapat Anda lakukan menggunakan Detective. Tindakan kebijakan di Detektif memiliki awalan berikut:. `detective:`

Misalnya, untuk memberikan izin menggunakan operasi `CreateMembers` API guna mengundang akun anggota ke grafik perilaku, Anda menyertakan `detective:CreateMembers` tindakan tersebut dalam kebijakan mereka.

Untuk menetapkan secara spesifik beberapa tindakan dalam satu pernyataan, pisahkan tindakan-tindakan tersebut dengan koma. Misalnya, untuk akun anggota, kebijakan mencakup serangkaian tindakan yang terkait dengan pengelolaan undangan:

```
"Action": [
      "detective:ListInvitations",
      "detective:AcceptInvitation",
      "detective:RejectInvitation",
      "detective:DisassociateMembership
]
```

Anda juga dapat menggunakan wildcard (*) untuk menentukan beberapa tindakan. Misalnya, untuk mengelola data yang digunakan dalam grafik perilaku mereka, akun administrator di Detective harus dapat melakukan tugas-tugas berikut:

- Lihat daftar akun anggota mereka (`ListMembers`).
- Dapatkan informasi tentang akun anggota yang dipilih (`GetMembers`).
- Undang akun anggota ke grafik perilaku mereka (`CreateMembers`).
- Hapus anggota dari grafik perilaku mereka (`DeleteMembers`).

Alih-alih mencantumkan tindakan ini secara terpisah, Anda dapat memberikan akses ke semua tindakan yang diakhiri dengan kata`Members`. Kebijakan untuk itu dapat mencakup tindakan berikut:

```
"Action": "detective:*Members"
```

Untuk melihat daftar tindakan Detektif, lihat Tindakan yang ditentukan oleh Detektif Amazon di Referensi Otorisasi Layanan.

Sumber daya

Administrator dapat menggunakan kebijakan JSON AWS untuk menentukan secara spesifik siapa yang memiliki akses pada apa. Yaitu, pengguna utama manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan syarat apa.

Elemen kebijakan JSON `Resource` menentukan objek atau objek-objek yang menjadi target penerapan tindakan. Pernyataan harus menyertakan entah elemen `Resource` atau `NotResource`. Praktik terbaiknya, tentukan sumber daya menggunakan Amazon Resource Name (ARN). Anda dapat melakukan ini untuk tindakan-tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin tingkat sumber daya, seperti operasi daftar, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan berlaku untuk semua sumber daya.

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

Untuk informasi selengkapnya tentang format ARN, lihat Amazon Resource Names (ARN) dan Namespace Layanan AWS.

Untuk Detective, satu-satunya jenis sumber daya adalah grafik perilaku. Sumber daya grafik perilaku di Detective memiliki ARN berikut:

```
arn:aws:detective:${Region}:${AccountId}:graph:${GraphId}
```

Misalnya, grafik perilaku memiliki nilai-nilai berikut:

- Wilayah untuk grafik perilaku adalah`us-east-1`.
- ID akun untuk ID akun administrator adalah`111122223333`.
- ID grafik dari grafik perilaku adalah`027c7c4610ea4aacaf0b883093cab899`.

Untuk mengidentifikasi grafik perilaku ini dalam sebuah `Resource` pernyataan, Anda akan menggunakan ARN berikut:

```
"Resource": "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
```

Untuk menentukan beberapa sumber daya dalam `Resource` pernyataan, gunakan koma untuk memisahkannya.

```
"Resource": [
      "resource1",
      "resource2"
]
```

Misalnya, AWS akun yang sama dapat diundang untuk menjadi akun anggota di lebih dari satu grafik perilaku. Dalam kebijakan untuk akun anggota tersebut, `Resource` pernyataan tersebut akan mencantumkan grafik perilaku yang mereka undang.

```
"Resource": [
      "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899",
      "arn:aws:detective:us-east-1:444455556666:graph:056d2a9521xi2bbluw1d164680eby416"
]
```

Beberapa tindakan Detektif, seperti membuat grafik perilaku, mencantumkan grafik perilaku, dan daftar undangan grafik perilaku, tidak dilakukan pada grafik perilaku tertentu. Untuk tindakan tersebut, `Resource` pernyataan harus menggunakan wildcard (*).

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

Untuk tindakan akun administrator, Detektif selalu memverifikasi bahwa pengguna yang membuat permintaan milik akun administrator untuk grafik perilaku yang terpengaruh. Untuk tindakan akun anggota, Detektif selalu memverifikasi bahwa pengguna yang membuat permintaan milik akun anggota. Bahkan jika kebijakan IAM memberikan akses ke grafik perilaku, jika pengguna bukan milik akun yang benar, pengguna tidak dapat melakukan tindakan tersebut.

Untuk semua tindakan yang dilakukan pada grafik perilaku tertentu, kebijakan IAM harus menyertakan grafik ARN. Grafik ARN dapat ditambahkan nanti. Misalnya, ketika akun pertama kali mengaktifkan Detektif, kebijakan IAM awal menyediakan akses ke semua tindakan Detektif, menggunakan wildcard untuk grafik ARN. Hal ini memungkinkan pengguna untuk segera mulai mengelola akun anggota dan melakukan investigasi dalam grafik perilaku mereka. Setelah grafik perilaku dibuat, Anda dapat memperbarui kebijakan untuk menambahkan grafik ARN.

Kunci syarat

Administrator dapat menggunakan kebijakan JSON AWS untuk menentukan siapa yang memiliki akses ke hal apa. Yaitu, pengguna utama manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan syarat apa.

Elemen `Condition` (atau blok `Condition`) akan memungkinkan Anda menentukan syarat yang menjadi dasar suatu pernyataan berlaku. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi bersyarat yang menggunakan operator syarat, misalnya sama dengan atau kurang dari, untuk mencocokkan syarat 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 dengan menggunakan operasi `AND` yang logis. Jika Anda menentukan beberapa niilai untuk satu kunci persyaratan, maka AWS akan mengevaluasi syarat tersebut menggunakan operasi `OR` yang logis. Semua persyaratan harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan syarat. Sebagai contoh, Anda dapat memberikan izin kepada pengguna IAM untuk mengakses sumber daya hanya jika izin tersebut mempunyai tag yang sesuai dengan nama pengguna IAM mereka. Untuk informasi selengkapnya, silakan lihat Elemen kebijakan IAM: variabel dan tag di Panduan Pengguna IAM.

AWS mendukung kunci-kunci syarat global dan kunci-kunci syarat spesifik layanan. Untuk melihat semua kunci persyaratan global AWS, silakan lihat kunci konteks syarat global AWS di Panduan Pengguna IAM.

Detective tidak mendefinisikan set sendiri dari kunci kondisi. Itu mendukung penggunaan kunci kondisi global. Untuk melihat semua kunci syarat global AWS, lihat Kunci Konteks Syarat Global AWS dalam Panduan Pengguna IAM.

Untuk mempelajari tindakan dan sumber daya yang memungkinkan Anda menggunakan kunci kondisi, lihat Tindakan yang ditentukan oleh Detektif Amazon.

Contoh

Untuk melihat contoh kebijakan berbasis identitas Detektif, lihat. Contoh kebijakan berbasis identitas Detektif Amazon

Kebijakan berbasis sumber daya Detektif (Tidak didukung)

Detective tidak mendukung kebijakan berbasis sumber daya.

Otorisasi berdasarkan tag grafik perilaku Detektif

Setiap grafik perilaku dapat diberi nilai tag. Anda dapat menggunakan nilai tag tersebut dalam pernyataan kondisi untuk mengelola akses ke grafik perilaku.

Pernyataan kondisi untuk nilai tag menggunakan format berikut.

```
{"StringEquals"{"aws:ResourceTag/<tagName>": "<tagValue>"}}
```

Misalnya, gunakan kode berikut untuk mengizinkan atau menolak tindakan ketika nilai `Department` tag tersebut`Finance`.

```
{"StringEquals"{"aws:ResourceTag/Department": "Finance"}}
```

Untuk contoh kebijakan yang menggunakan nilai tag sumber daya, lihatthe section called “Akun administrator: Membatasi akses berdasarkan nilai tag”.

Peran Detektif IAM

IAM role adalah entitas di dalam akun AWS Anda yang memiliki izin tertentu.

Menggunakan kredensil sementara dengan Detective

Anda dapat menggunakan kredensial sementara untuk masuk dengan gabungan, menjalankan IAM role, atau menjalankan peran lintas akun. Anda memperoleh kredensil keamanan sementara dengan memanggil operasi AWS STS API seperti AssumeRoleatau. GetFederationToken

Detective mendukung menggunakan kredensil sementara.

Peran terkait layanan

Peran terkait layanan mengizinkan layanan AWS untuk mengakses sumber daya di layanan lain untuk menyelesaikan tindakan atas nama Anda. Peran terkait layanan muncul di akun IAM Anda dan dimiliki oleh layanan tersebut. Administrator IAM dapat melihat tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Untuk detail tentang membuat atau mengelola peran terkait layanan Detektif, lihat. the section called “Menggunakan peran terkait layanan”

Peran layanan (Tidak didukung)

Fitur ini memungkinkan layanan untuk menerima peran layanan atas nama Anda. Peran ini mengizinkan layanan untuk mengakses sumber daya di layanan lain untuk menyelesaikan tindakan atas nama Anda. Peran layanan muncul di akun IAM Anda dan dimiliki oleh akun tersebut. Ini berarti administrator IAM dapat mengubah izin untuk peran ini. Namun, melakukan hal itu dapat merusak fungsionalitas layanan.

Detektif tidak mendukung peran layanan.

Contoh kebijakan berbasis identitas Detektif Amazon

Secara default, pengguna dan peran IAM tidak memiliki izin untuk membuat atau memodifikasi sumber daya Detektif. Mereka juga tidak dapat melakukan tugas menggunakan API AWS Management Console, AWS CLI, or AWS.

Administrator IAM harus membuat kebijakan IAM yang memberikan izin kepada pengguna dan peran untuk melakukan operasi API tertentu pada sumber daya yang diperlukan. Administrator kemudian melampirkan kebijakan tersebut ke pengguna IAM atau grup yang memerlukan izin tersebut.

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

Topik

- Praktik terbaik kebijakan
- Menggunakan konsol Detective
- Memungkinkan pengguna untuk melihat izin mereka sendiri
- Akun administrator: Mengelola akun anggota dalam grafik perilaku
- Akun administrator: Menggunakan grafik perilaku untuk penyelidikan
- Akun anggota: Mengelola undangan grafik perilaku dan keanggotaan
- Akun administrator: Membatasi akses berdasarkan nilai tag

Praktik terbaik kebijakan

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

- Mulailah dengan kebijakan terkelola AWS dan beralih ke izin dengan hak akses paling rendah – Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan terkelola AWS yang memberikan izin untuk banyak kasus penggunaan umum. Kebijakan tedapat di Akun AWS Anda. Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola pelanggan AWS yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, silakan lihat kebijakan-kebijakan terkelola AWS atau kebijakan-kebijakan terkelola AWS untuk fungsi tugas 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 mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan pengguna IAM untuk mengajukan izin, silakan lihat Kebijakan dan izin di IAM di Panduan Pengguna IAM.
- Gunakan syarat dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu syarat ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis syarat kebijakan untuk menentukan bahwa semua pengajuan harus dikirim menggunakan SSL. Anda juga dapat menggunakan syarat untuk memberi akses ke tindakan layanan jika digunakan melalui Layanan AWS yang spesifk, sepertiAWS CloudFormation. Untuk informasi selengkapnya, silakan lihat Elemen kebijakan JSON IAM: Syarat di Panduan Pengguna IAM.
- Gunakan Analizer Akses IAM untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – Analizer Akses IAM memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. Analizer Akses IAM menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, silakan lihat validasi kebijakan Analizer Akses IAM di Panduan Pengguna IAM.
- Memerlukan 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 meminta MFA ketika operasi API dipanggil, tambahkan syarat MFA pada kebijakan Anda. Untuk informasi selengkapnya, silakan lihat Mengonfigurasi akses API yang diproteksi MFA di Panduan Pengguna IAM.

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

Menggunakan konsol Detective

Untuk menggunakan konsol Detektif Amazon, pengguna atau peran harus memiliki akses ke tindakan yang relevan, yang cocok dengan tindakan terkait di API.

Untuk mengaktifkan Detektif dan menjadi akun administrator untuk grafik perilaku, pengguna atau peran harus diberikan izin untuk tindakan tersebut`CreateGraph`.

Untuk menggunakan konsol Detektif untuk melakukan tindakan akun administrator, pengguna atau peran harus diberikan izin untuk tindakan tersebut`ListGraphs`. Ini memberikan izin untuk mengambil grafik perilaku akun mereka sebagai akun administrator. Mereka juga harus diberikan izin untuk melakukan tindakan akun administrator tertentu.

Tindakan akun administrator yang paling dasar adalah melihat daftar akun anggota dalam grafik perilaku, dan menggunakan grafik perilaku untuk penyelidikan.

- Untuk melihat daftar akun anggota dalam grafik perilaku, kepala sekolah harus diberikan izin untuk `ListMembers` tindakan tersebut.
- Untuk melakukan investigasi dalam grafik perilaku, kepala sekolah harus diberikan izin untuk `SearchGraph` tindakan tersebut.

Untuk menggunakan konsol Detektif untuk melakukan tindakan akun anggota, pengguna atau peran harus diberikan izin untuk tindakan tersebut`ListInvitations`. Ini memberikan izin untuk melihat undangan grafik perilaku. Mereka kemudian dapat diberikan izin untuk tindakan akun anggota tertentu.

Memungkinkan pengguna untuk melihat izin mereka sendiri

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

```
{
    "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": "*"
        }
    ]
}
```

Akun administrator: Mengelola akun anggota dalam grafik perilaku

Kebijakan contoh ini ditujukan untuk pengguna akun administrator yang hanya bertanggung jawab untuk mengelola akun anggota yang digunakan dalam grafik perilaku. Kebijakan ini juga memungkinkan pengguna untuk melihat informasi penggunaan dan menonaktifkan Detektif. Kebijakan tidak memberikan izin untuk menggunakan grafik perilaku untuk penyelidikan.

```
{"Version":"2012-10-17",
  "Statement":[
   {
    "Effect":"Allow",
    "Action":
["detective:ListMembers","detective:CreateMembers","detective:DeleteMembers","detective:DeleteG
    "Resource":"arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
  },
  {
```

```
    "Effect":"Allow",
    "Action":["detective:CreateGraph","detective:ListGraphs"],
    "Resource":"*"
  }
 ]
}
```

Akun administrator: Menggunakan grafik perilaku untuk penyelidikan

Kebijakan contoh ini ditujukan untuk pengguna akun administrator yang menggunakan grafik perilaku hanya untuk penyelidikan. Mereka tidak dapat melihat atau mengedit daftar akun anggota dalam grafik perilaku.

```
{"Version":"2012-10-17",
  "Statement":[
   {
    "Effect":"Allow",
    "Action":["detective:SearchGraph"],
    "Resource":"arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
   },
   {
    "Effect":"Allow",
    "Action":["detective:ListGraphs"],
    "Resource":"*"
  }
 ]
}
```

Akun anggota: Mengelola undangan grafik perilaku dan keanggotaan

Kebijakan contoh ini ditujukan untuk pengguna yang termasuk dalam akun anggota. Dalam contoh, akun anggota termasuk dalam dua grafik perilaku. Kebijakan memberikan izin untuk menanggapi undangan dan menghapus akun anggota dari grafik perilaku.

```
{"Version":"2012-10-17",
  "Statement":[
   {
    "Effect":"Allow",
   "Action":
["detective:AcceptInvitation","detective:RejectInvitation","detective:DisassociateMembership"],
   "Resource":[
```

```
       "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899",
       "arn:aws:detective:us-
east-1:444455556666:graph:056d2a9521xi2bbluw1d164680eby416"
    ]
  },
  {
    "Effect":"Allow",
    "Action":["detective:ListInvitations"],
    "Resource":"*"
  }
 ]
}
```

Akun administrator: Membatasi akses berdasarkan nilai tag

Kebijakan berikut memungkinkan pengguna menggunakan grafik perilaku untuk penyelidikan jika `SecurityDomain` tag grafik perilaku cocok dengan `SecurityDomain` tag pengguna.

```
{
    "Version":"2012-10-17",
    "Statement":[ {
        "Effect":"Allow",
        "Action":["detective:SearchGraph"],
        "Resource":"arn:aws:detective:*:*:graph:*",
        "Condition": {
            "StringEquals"{
                "aws:ResourceTag/SecurityDomain": "aws:PrincipalTag/SecurityDomain"
            }
        }
    },
    {
        "Effect":"Allow",
        "Action":["detective:ListGraphs"],
        "Resource":"*"
    } ]
}
```

Kebijakan berikut mencegah pengguna menggunakan grafik perilaku untuk penyelidikan jika nilai `SecurityDomain` tag untuk grafik perilaku adalah`Finance`.

```
{
```

```
    "Version":"2012-10-17",
    "Statement":[ {
        "Effect":"Deny",
        "Action":["detective:SearchGraph"],
        "Resource":"arn:aws:detective:*:*:graph:*",
        "Condition": {
            "StringEquals": {"aws:ResourceTag/SecurityDomain": "Finance"}
        }
    } ]
}
```

Memecahkan masalah identitas dan akses Detektif Amazon

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan Detective dan IAM. Jika Anda mengalami masalah yang ditolak akses atau kesulitan serupa saat bekerja dengan AWS Identity and Access Management (IAM), lihat topik Pemecahan Masalah IAM di Panduan Pengguna IAM.

Aku tidak berwenang untuk melakukan tindakan di Detective

Jika AWS Management Console memberi tahu bahwa Anda tidak diotorisasi untuk melakukan tindakan, Anda harus menghubungi administrator untuk mendapatkan bantuan. Administrator adalah orang yang memberikan nama pengguna dan kata sandi Anda untuk Anda.

Contoh kesalahan berikut terjadi ketika pengguna `mateojackson` IAM mencoba menggunakan konsol untuk menerima undangan untuk menjadi akun anggota untuk grafik perilaku, tetapi tidak memiliki `detective:AcceptInvitation` izin.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to
 perform: detective:AcceptInvitation on resource: arn:aws:detective:us-
east-1:444455556666:graph:567856785678
```

Dalam hal ini, Mateo meminta administratornya untuk memperbarui kebijakannya untuk memungkinkannya mengakses sumber daya `arn:aws:detective:us-east-1:444455556666:graph:567856785678` dengan menggunakan tindakan `detective:AcceptInvitation`.

Saya tidak berwenang untuk melakukan iam: PassRole

Jika Anda menerima kesalahan bahwa Anda tidak berwenang untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran ke Detektif.

Sebagian Layanan AWS mengizinkan Anda untuk memberikan peran yang sudah ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran tertaut-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 Detective. 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 memberikan kredensial masuk Anda.

Saya ingin mengizinkan orang-orang di luar AWS akun saya untuk mengakses sumber daya Detektif saya

Anda dapat membuat peran yang dapat digunakan para pengguna di akun lain atau orang-orang di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa yang dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACL), Anda dapat menggunakan kebijakan tersebut untuk memberi akses kepada orang ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa hal berikut:

- Untuk mengetahui apakah Detective mendukung fitur-fitur ini, lihat. Bagaimana Amazon Detective bekerja dengan IAM
- Untuk mempelajari cara memberikan akses ke sumber daya di seluruh Akun AWS yang Anda miliki, silakan lihat Menyediakan akses ke pengguna IAM di Akun AWS lainnya yang Anda miliki di Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses ke sumber daya Anda ke pihak ketiga Akun AWS, silakan lihat Menyediakan akses ke akun Akun AWS yang dimiliki oleh pihak ketiga dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, silakan lihat Menyediakan akses ke pengguna terautentikasi eksternal (gabungan identitas) di Panduan Pengguna IAM .

- Untuk mempelajari perbedaan antara penggunaan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Perbedaan IAM role dan kebijakan berbasis sumber daya di Panduan Pengguna IAM.

Menggunakan peran tertaut layanan untuk Detective

Amazon Detective menggunakan peran terkait layananAWS Identity and Access Management (IAM). Peran tertaut layanan adalah jenis IAM role unik yang tertaut langsung ke Detective. Peran terkait layanan ditentukan sebelumnya oleh Detective dan mencakup semua izin yang diperlukan layanan untuk menghubungiAWS layanan lainnya atas nama Anda.

Peran terkait layanan memudahkan pengaturan Detective menjadi lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. Detective menentukan izin peran tertaut layanan, kecuali jika ditentukan berbeda, hanya Detective yang dapat mengasumsikan perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, serta bahwa kebijakan izin tidak dapat dilampirkan ke entitas IAM lainnya.

Anda dapat menghapus peran tertaut layanan hanya setelah menghapus sumber daya terkait terlebih dahulu. Ini melindungi sumber daya Detective karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya.

Untuk informasi tentang layanan lain yang support peran yang terkait dengan layanan, lihat Layanan AWS yang Bekerja dengan IAM dan mencari layanan yang memiliki Ya dalam kolom Peran Tertaut Layanan. Pilih Ya dengan tautan untuk melihat dokumentasi peran tertaut layanan untuk layanan tersebut.

Izin peran tertaut layanan untuk Detective

Detective menggunakan peran tertaut layanan bernama AWSServiceRoleForDetective—Memungkinkan Detective untuk mengaksesAWS Organizations informasi atas nama Anda.

Peran AWSServiceRoleForDetective terkait layanan memercayakan layanan berikut untuk menjalankan peran tersebut:

- `detective.amazonaws.com`

Peran AWSServiceRoleForDetective terkait layanan menggunakan kebijakan terkelola `AmazonDetectiveServiceLinkedRolePolicy`.

Anda harus mengonfigurasi izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat Izin peran tertaut layanan dalam Panduan Pengguna IAM.

Membuat peran tertaut layanan untuk Detective

Anda tidak perlu membuat peran tertaut layanan secara manual. Ketika Anda menetapkan akun administrator Detective untuk organisasi diAWS Management Console,AWS CLI, atauAWS API, Detective menciptakan peran terkait layanan untuk Anda.

Jika Anda menghapus peran tertaut layanan ini, dan ingin membuatnya lagi, Anda dapat mengulangi proses yang sama untuk membuat kembali peran tersebut di akun Anda. Saat Anda menentukan administrator Detective untuk organisasi, Detective membuatkan peran tertaut layanan untuk Anda.

Menyunting peran tertaut layanan untuk Detective

Detective tidak mengizinkan Anda mengedit peran AWSServiceRoleForDetective tertaut layanan. Setelah Anda membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan peran tersebut. Namun, Anda dapat mengedit penjelasan peran menggunakan IAM. Untuk informasi selengkapnya, lihat Mengedit peran yang terkait dengan layanan dalam Panduan Pengguna IAM.

Menghapus peran tertaut layanan untuk Detective

Jika Anda tidak perlu lagi menggunakan fitur atau layanan yang memerlukan peran terkait layanan, kami merekomendasikan Anda menghapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan yang tidak dipantau atau dipelihara secara aktif. Tetapi, Anda harus membersihkan sumber daya peran yang terhubung dengan layanan sebelum menghapusnya secara manual.

> **Note**
>
> Jika layanan Detective menggunakan peran tersebut ketika Anda mencoba menghapus sumber daya, penghapusan mungkin gagal. Jika hal tersebut terjadi, tunggu beberapa menit dan coba operasi lagi.

Untuk menghapus sumber daya Detective yang digunakan oleh AWSServiceRoleForDetective

1. Hapus administrator Detective. Lihat the section called “Menunjuk akun administrator Detektif”.

2. Ulangi proses di setiap Wilayah tempat Anda menunjuk akun administrator Detective.

Untuk menghapus peran tertaut layanan secara manual gunakan IAM

Gunakan konsol IAM, AWS CLI, atau AWS API untuk menghapus peran terkait layanan AWSServiceRoleForDetective. Untuk informasi lebih lanjut, lihat Menghapus Peran Tertaut Layanan di Panduan Pengguna IAM.

Wilayah yang Didukung untuk peran tertaut layanan

Detective memberikan dukungan dengan peran tertaut layanan di semua Wilayah tempat layanan tersedia. Untuk informasi lebih lanjut, lihat Wilayah dan Titik Akhir AWS.

AWSkebijakan terkelola untuk Amazon Detective

Kebijakan terkelola AWS adalah kebijakan mandiri yang dibuat dan oleh dilakukan AWS. Kebijakan terkelola AWS dirancang untuk memberikan izin bagi banyak kasus penggunaan umum sehingga Anda dapat mulai menetapkan izin kepada pengguna, grup, dan peran.

Perlu diingat bahwa kebijakan terkelola AWS mungkin tidak memberikan izin hak akses paling rendah untuk kasus penggunaan khusus Anda karena tersedia untuk digunakan semua pelanggan AWS. Kami menyarankan Anda untuk mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola pelanggan yang khusus untuk kasus penggunaan Anda.

Anda tidak dapat mengubah izin yang ada dalam kebijakan-kebijakan terkelola AWS. Jika AWS memperbarui izin yang ditentukan dalam sebuah kebijakan terkelola AWS, maka pembaruan itu akan mempengaruhi semua identitas pengguna utama (pengguna, grup, dan peran) yang terkait dengan kebijakan tersebut. AWS kemungkinan besar akan memperbarui kebijakan terkelola AWS saat sebuah Layanan AWS baru diluncurkan atau operasi API baru tersedia untuk layanan yang sudah ada.

Untuk informasi selengkapnya, silakan lihat kebijakan terkelola AWS di Panduan Pengguna IAM.

Kebijakan terkelola AWS: AmazonDetectiveFullAccess

Anda dapat melampirkan kebijakan `AmazonDetectiveFullAccess` ke identitas-identitas IAM Anda.

Kebijakan ini memberikan izin administratif yang memungkinkan akses penuh utama ke semua tindakan Detektif Amazon. Anda dapat melampirkan kebijakan ini ke kepala sekolah sebelum mereka mengaktifkan Detektif untuk akun mereka. Itu juga harus dilampirkan pada peran yang digunakan untuk menjalankan skrip Detective Python untuk membuat dan mengelola grafik perilaku.

Prinsipal dengan izin ini dapat mengelola akun anggota, menambahkan tag ke grafik perilaku mereka, dan menggunakan Detektif untuk penyelidikan. Mereka juga dapat mengarsipkan GuardDuty temuan. Kebijakan ini memberikan izin yang dibutuhkan konsol Detektif untuk menampilkan nama akun untuk akun yang ada di dalamnya. AWS Organizations

Detail izin

Kebijakan ini mencakup izin berikut:

- `detective`— Memungkinkan kepala sekolah akses penuh ke semua tindakan Detektif.
- `organizations`— Memungkinkan kepala sekolah untuk mengambil dari AWS Organizations informasi tentang akun dalam suatu organisasi. Jika akun milik organisasi, izin ini memungkinkan konsol Detektif menampilkan nama akun selain nomor akun.
- `guardduty`— Memungkinkan kepala sekolah untuk mendapatkan dan mengarsipkan GuardDuty temuan dari dalam Detektif.
- `securityhub`— Memungkinkan kepala sekolah untuk mendapatkan temuan Security Hub dari dalam Detektif.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "detective:*",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:ArchiveFindings"
```

```
            ],
            "Resource": "arn:aws:guardduty:*:*:detector/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:GetFindings",
                "guardduty:ListDetectors"

            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                 "securityHub:GetFindings"
            ],
            "Resource": "*"
         }
    ]
}
```

Kebijakan terkelola AWS: AmazonDetectiveMemberAccess

Anda dapat melampirkan `AmazonDetectiveMemberAccess` kebijakan ke entitas IAM Anda.

Kebijakan ini menyediakan akses anggota ke Detektif Amazon dan akses cakupan ke konsol.

Dengan kebijakan ini, Anda dapat:

- Lihat undangan ke keanggotaan grafik Detektif dan terima atau tolak undangan tersebut.
- Lihat bagaimana aktivitas Anda di Detective berkontribusi terhadap biaya penggunaan layanan ini di halaman Penggunaan.
- Mengundurkan diri dari keanggotaan Anda dalam grafik.

Kebijakan ini memberikan izin hanya-baca yang memungkinkan akses cakupan ke Detektif konsol.

Detail izin

Kebijakan ini mencakup izin berikut:

- `detective`— Memungkinkan akses anggota ke Detektif.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:AcceptInvitation",
        "detective:BatchGetMembershipDatasources",
        "detective:DisassociateMembership",
        "detective:GetFreeTrialEligibility",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListInvitations",
        "detective:RejectInvitation"
      ],
      "Resource": "*"
    }
  ]
}
```

Kebijakan terkelola AWS: AmazonDetectiveInvestigatorAccess

Anda dapat melampirkan `AmazonDetectiveInvestigatorAccess` kebijakan ke entitas IAM Anda.

Kebijakan ini menyediakan akses penyidik ke layanan Detektif dan akses cakupan ke dependensi UI konsol Detektif. Kebijakan ini memberikan izin untuk mengaktifkan investigasi Detektif di Detektif untuk pengguna IAM dan peran IAM. Anda dapat menyelidiki untuk mengidentifikasi indikator kompromi seperti temuan menggunakan laporan investigasi, yang memberikan analisis dan wawasan tentang indikator keamanan. Laporan ini diberi peringkat berdasarkan tingkat keparahan, yang ditentukan menggunakan analisis perilaku Detektif dan pembelajaran mesin. Anda dapat menggunakan laporan untuk memprioritaskan remediasi sumber daya.

Detail izin

Kebijakan ini mencakup izin berikut:

- `detective`— Memungkinkan penyidik kepala sekolah mengakses tindakan Detektif, untuk mengaktifkan investigasi Detektif, dan untuk memungkinkan menemukan ringkasan kelompok.
- `guardduty`— Memungkinkan kepala sekolah untuk mendapatkan dan mengarsipkan GuardDuty temuan dari dalam Detektif.
- `securityhub`— Memungkinkan kepala sekolah untuk mendapatkan temuan Security Hub dari dalam Detektif.
- `organizations`— Memungkinkan kepala sekolah untuk mengambil informasi tentang akun dalam suatu organisasi dari. AWS Organizations Jika akun milik organisasi, maka izin ini memungkinkan konsol Detektif untuk menampilkan nama akun selain nomor akun.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DetectivePermissions",
      "Effect": "Allow",
      "Action": [
        "detective:BatchGetGraphMemberDatasources",
        "detective:BatchGetMembershipDatasources",
        "detective:DescribeOrganizationConfiguration",
        "detective:GetFreeTrialEligibility",
        "detective:GetGraphIngestState",
        "detective:GetMembers",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListDatasourcePackages",
        "detective:ListGraphs",
        "detective:ListHighDegreeEntities",
        "detective:ListInvitations",
        "detective:ListMembers",
        "detective:ListOrganizationAdminAccount",
        "detective:ListTagsForResource",
        "detective:SearchGraph",
        "detective:StartInvestigation",
```

```
        "detective:GetInvestigation",
        "detective:ListInvestigations",
        "detective:UpdateInvestigationState",
        "detective:ListIndicators",
        "detective:InvokeAssistant"
      ],
      "Resource": "*"
    },
    {
      "Sid": "OrganizationsPermissions",
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource": "*"
    },
    {
      "Sid": "GuardDutyPermissions",
      "Effect": "Allow",
      "Action": [
        "guardduty:ArchiveFindings",
        "guardduty:GetFindings",
        "guardduty:ListDetectors"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SecurityHubPermissions",
      "Effect": "Allow",
      "Action": [
        "securityHub:GetFindings"
      ],
      "Resource": "*"
    }
  ]
}
```

AWSkebijakan terkelola: AmazonDetectiveOrganizationsAccess

Anda dapat melampirkan `AmazonDetectiveOrganizationsAccess` kebijakan ke entitas IAM Anda.

Kebijakan ini memberikan izin untuk mengaktifkan dan mengelola Detektif Amazon dalam suatu organisasi. Anda dapat mengaktifkan Detektif di seluruh organisasi dan menentukan akun administrator yang didelegasikan untuk Detektif.

Detail izin

Kebijakan ini mencakup izin berikut:

- `detective`— Memungkinkan kepala sekolah mengakses tindakan Detektif.
- `iam`— Menentukan bahwa peran layanan terkait dibuat ketika `EnableOrganizationAdminAccount` Detective memanggil.
- `organizations`— Memungkinkan kepala sekolah untuk mengambil informasi tentang akun dalam suatu organisasi dari. AWS Organizations Jika akun milik organisasi, maka izin ini memungkinkan konsol Detektif untuk menampilkan nama akun selain nomor akun. Mengaktifkan integrasi AWS layanan, memungkinkan register dan deregister akun anggota yang ditentukan sebagai administrator Delegasi, dan memungkinkan prinsipal untuk mengambil akun administrator Delegasi di layanan keamanan lain seperti Amazon Detective, Amazon, Amazon Macie, dan. GuardDuty AWS Security Hub

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:DisableOrganizationAdminAccount",
        "detective:EnableOrganizationAdminAccount",
        "detective:ListOrganizationAdminAccount"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "*",
      "Condition": {
```

```
        "StringEquals": {
          "iam:AWSServiceName": "detective.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "organizations:ServicePrincipal": [
            "detective.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "organizations:ServicePrincipal": [
            "detective.amazonaws.com",
            "guardduty.amazonaws.com",
            "macie.amazonaws.com",
            "securityhub.amazonaws.com"
          ]
```

```
        }
      }
    }
  ]
}
```

Kebijakan terkelola AWS: AmazonDetectiveServiceLinkedRole

Anda tidak dapat melampirkan `AmazonDetectiveServiceLinkedRole` kebijakan ke entitas IAM Anda. Kebijakan ini dilampirkan pada peran terkait layanan yang memungkinkan Detektif melakukan tindakan atas nama Anda. Untuk informasi selengkapnya, lihat the section called “Menggunakan peran terkait layanan”.

Kebijakan ini memberikan izin administratif yang memungkinkan peran terkait layanan untuk mengambil informasi akun untuk organisasi.

Detail izin

Kebijakan ini mencakup izin berikut:

- `organizations`— Mengambil informasi akun untuk suatu organisasi.

```
{
  "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
              "organizations:DescribeAccount",
              "organizations:ListAccounts"
            ],
            "Resource": "*"
        }
    ]
}
```

Detective update ke AWS kebijakan terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk Detektif sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman Riwayat dokumen.

Perubahan	Deskripsi	Tanggal
AmazonDetectiveInvestigatorAccess— Pembaruan kebijakan yang ada	Menambahkan investigasi Detektif dan menemukan tindakan ringkasan kelompok ke kebijakan. `AmazonDetectiveInvestigatorAccess` Tindakan ini memungkinkan memulai, mengambil, dan memperbarui investigasi Detektif; dan mendapatkan ringkasan menemukan kelompok dari dalam Detektif.	26 November 2023
AmazonDetectiveFullAccessdan AmazonDetectiveInvestigatorAccess— Pembaruan kebijakan yang ada	Detective menambahkan `GetFindings` tindakan Security Hub ke `AmazonDetectiveFullAccess` dan `AmazonDetectiveInvestigatorAccess` kebijakan. Tindakan ini memungkinkan mendapatkan temuan Security Hub dari dalam Detektif.	16 Mei 2023
AmazonDetectiveOrganizationsAccess – Kebijakan baru	Detektif menambahkan `AmazonDetectiveOrganizationsAccess` kebijakan.	Maret 02, 2023

Perubahan	Deskripsi	Tanggal
	Kebijakan ini memberikan izin untuk mengaktifkan dan mengelola Detektif dalam suatu organisasi	
AmazonDetectiveMemberAccess – Kebijakan baru	Detektif menambahkan kebijakan . `AmazonDetectiveMemberAccess` Kebijakan ini memberikan akses anggota ke Detektif dan akses cakupan ke dependensi UI konsol.	Januari 17, 2023
AmazonDetectiveFullAccess— Pembaruan untuk kebijakan yang ada	Detektif menambahkan GuardDuty `GetFindings` tindakan ke kebijakan. `AmazonDetectiveFullAccess` Tindakan ini memungkinkan mendapatkan GuardDuty temuan dari dalam Detektif.	Januari 17, 2023
AmazonDetectiveInvestigatorAccess – Kebijakan baru	Detektif menambahkan kebijakan . `AmazonDetectiveInvestigatorAccess` Kebijakan ini memungkinkan kepala sekolah untuk melakukan investigasi di Detektif.	Januari 17, 2023
AmazonDetectiveServiceLinkedRole – Kebijakan baru	Detective menambahkan kebijakan baru untuk peran terkait layanannya. Kebijakan ini memungkinkan peran terkait layanan untuk mengambil informasi tentang akun dalam organisasi.	Desember 16, 2021

Perubahan	Deskripsi	Tanggal
Detektif mulai melacak perubahan	Detective mulai melacak perubahan untuk kebijakan yang AWS dikelola.	10 Mei 2021

Pencatatan dan pemantauan di Amazon Detective

Amazon Detective terintegrasiAWS CloudTrail. CloudTrail merekam semua panggilan API Detective kejadian.

Untuk detail tentang penggunaan CloudTrail logging untuk Detective, lihatthe section called “Mencatat log panggilan API Detective dengan CloudTrail”.

Validasi kepatuhan untuk Amazon Detective

Amazon Detective adalah dalam Lingkup programAWS jaminan. Untuk informasi lebih lanjut, lihat Health Information Trust Alliance Common Security Framework (HITRUST) CSF .

Untuk daftar layanan AWS dalam cakupan program kepatuhan tertentu, lihat Layanan AWS dalam Cakupan Program Kepatuhan. Untuk informasi umum, lihat Program Kepatuhan AWS.

Anda bisa mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Pengunduhan Laporan dalam AWS Artifact.

AWSmenyediakan sumber daya berikut untuk membantu kepatuhan:

- Panduan Quick Start Keamanan dan Kepatuhan – Panduan deployment ini membahas pertimbangan arsitektur dan menyediakan langkah untuk deployment lingkungan dasar yang fokus pada keamanan dan kepatuhan di AWS.
- Mengevaluasi sumber daya dengan aturan dalam AWS Config Panduan Developer – Layanan AWS Config akan menilai seberapa patuh konfigurasi sumber daya Anda terhadap praktik internal, panduan industri, dan aturan.
- AWS Security Hub – Layanan AWS ini memberikan pandangan komprehensif tentang status keamanan Anda dalam AWS yang membantu Anda memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik.

Ketahanan di Amazon Detective

Infrastruktur global AWS dibangun di sekitar Wilayah AWS dan Availability Zone. AWS Wilayah menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan jaringan berlatensi rendah, throughput yang tinggi, dan sangat redundan. Dengan Availability Zone, Anda dapat mendesain dan mengoperasikan aplikasi dan basis data yang secara otomatis mengalami kegagalan di antara zona tanpa gangguan. Availability Zone lebih tersedia, memiliki toleransi kesalahan, dan dapat diskalakan dibandingkan dengan satu atau beberapa infrastruktur pusat data tradisional.

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

Selain infrastrukturAWS global, Detective memanfaatkan ketahanan yang dibangun ke Amazon DynamoDB dan Amazon Simple Storage Service (Amazon S3).

Arsitektur Detective juga tahan terhadap kegagalan Availability Zone tunggal. Ketahanan ini dibangun ke dalam Detective, dan tidak memerlukan konfigurasi apa pun.

Keamanan infrastruktur di Amazon Detective

Sebagai layanan terkelola, Amazon Detective; dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat Keamanan AWS Cloud. Untuk merancang AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan Infrastruktur dalam Kerangka Kerja Pilar Keamanan yang AWS Diarsiteksikan dengan Baik.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses Detektif; melalui jaringan. Klien harus mendukung hal berikut:

- Transport Layer Security (TLS). Kami membutuhkan TLS 1.2 dan merekomendasikan TLS 1.3.
- Suite cipher dengan kerahasiaan maju sempurna (PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan sistem yang lebih baru mendukung mode ini.

Selain itu, permintaan harus ditandatangani menggunakan access key ID dan secret access key yang terkait dengan principal IAM. Atau Anda bisa menggunakan AWS Security Token Service (AWS STS) untuk membuat kredensial keamanan sementara guna menandatangani permintaan.

Praktik praktik Praktik Praktik Praktik Praktik Praktik Praktik Detective

Detective menyediakan sejumlah fitur keamanan yang dapat dipertimbangkan ketika Anda mengembangkan dan menerapkan kebijakan keamanan Anda sendiri. Praktik terbaik berikut adalah pedoman umum dan tidak mewakili solusi keamanan yang lengkap. Karena praktik terbaik ini mungkin tidak sesuai atau cukup untuk lingkungan Anda, anggap praktik terbaik tersebut sebagai pertimbangan yang membantu dan bukan sebagai rekomendasi.

Untuk Detective, praktik terbaik keamanan dikaitkan dengan pengelolaan akun dalam grafik perilaku.

Praktik Praktik Praktik Praktik Praktik Praktik Prak

Saat mengundang akun anggota ke grafik perilaku Anda, hanya undang akun yang Anda awasi.

Batasi akses ke grafik perilaku. Ketika pengguna memiliki akses ke grafik perilaku, mereka dapat melihat semua temuan untuk akun anggota. Temuan semacam itu mungkin mengekspos informasi keamanan yang sensitif.

Praktik terbaik untuk akun anggota

Saat Anda menerima undangan ke grafik perilaku, pastikan untuk memvalidasi sumber undangan.

Periksa pengidentifikasiAWS akun akun administrator yang mengirim undangan. Verifikasi bahwa Anda tahu siapa akun itu milik, dan bahwa akun undangan memiliki alasan yang sah untuk memantau data keamanan Anda.

Nonaktifkan Amazon Detective

Akun administrator untuk grafik perilaku dapat menonaktifkan Amazon Detective dari konsol Detective, Detective API, atauAWS Command Line Interface. Saat Anda menonaktifkan Detective, grafik perilaku dan data Detective yang terkait akan dihapus.

Setelah grafik perilaku dihapus, itu tidak dapat dipulihkan.

Daftar Isi

Menonaktifkan Detective (Konsol)

Anda dapat menonaktifkan Amazon Detective dariAWS Management Console.

Untuk menonaktifkan Detective (konsol)

1. Buka konsol Detective Amazon dihttps://console.aws.amazon.com/detective/.
2. Di panel navigasi Detective, di bawah Pengaturan, pilih Umum.
3. Pada halaman Umum, di bawah Nonaktifkan Detective, pilih Nonaktifkan Detective.
4. Saat diminta untuk mengonfirmasi, ketik**`disable`**.
5. Pilih Nonaktifkan Detective.

Menonaktifkan Detective (Detective API,AWS CLI)

Anda dapat menonaktifkan Amazon Detective dari Detective API atauAWS Command Line Interface. Untuk mendapatkan ARN grafik perilaku Anda untuk digunakan dalam permintaan, gunakan `ListGraphs`operasi.

Untuk menonaktifkan Detective (Detective API,AWS CLI)

- Detective API: Gunakan `DeleteGraph`operasi. Anda harus memberikan grafik ARN.
- AWS CLI: Di baris perintah, jalankan `delete-graph`perintah.

```
aws detective delete-graph --graph-arn <graph ARN>
```

Contoh:

```
aws detective delete-graph --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

Menonaktifkan Detective lintas Wilayah (skrip Python aktif GitHub)

Detective menyediakan skrip open-source GitHub yang memungkinkan Anda menonaktifkan Detective untuk akun administrator di daftar Regions yang ditentukan.

Untuk informasi tentang cara mengkonfigurasi dan menggunakan GitHub skrip, lihatMenggunakan skrip Amazon Detective Python.

Menggunakan skrip Amazon Detective Python

Amazon Detective menyediakan satu set skrip Python sumber terbuka dalam GitHub repositori amazon-detective-multiaccount-scripts. Lakukan seperti pada skrip dengan Python 3.

Anda dapat menggunakan ini untuk melakukan tugas-tugas berikut:

- Aktifkan Detective untuk akun administrator di seluruh Wilayah.

  Ketika Anda mengaktifkan Detective, Anda dapat menetapkan nilai tag ke grafik perilaku.
- Tambahkan akun anggota ke grafik perilaku akun administrator di seluruh Wilayah.
- Opsional mengirim email undangan ke akun anggota. Anda juga dapat mengkonfigurasi permintaan untuk tidak mengirim email undangan.
- Hapus akun anggota dari grafik perilaku akun administrator di seluruh Wilayah.
- Nonaktifkan Detective untuk akun administrator di seluruh Wilayah. Bila akun administrator menonaktifkan Detective, grafik perilaku akun administrator di setiap Wilayah dinonaktifkan.

Ikhtisar`enableDetective.py` naskah

Lakukan seperti pada`enableDetective.py` skrip berikut ini:

1. Memungkinkan Detective untuk akun administrator di setiap Wilayah yang ditentukan, jika akun administrator belum mengaktifkan Detective di Wilayah tersebut.

   Ketika Anda menggunakan skrip untuk mengaktifkan Detective, Anda dapat menetapkan nilai tag ke grafik perilaku.
2. Secara opsional mengirim undangan dari akun administrator ke akun anggota yang ditentukan untuk setiap grafik perilaku.

   Pesan email undangan menggunakan konten pesan default dan tidak dapat disesuaikan.

   Anda juga dapat mengkonfigurasi permintaan untuk tidak mengirim email undangan.
3. Secara otomatis menerima undangan untuk akun anggota.

   Karena skrip secara otomatis menerima undangan, akun anggota dapat mengabaikan pesan ini.

Sebaiknya hubungi langsung ke akun anggota untuk memberi tahu mereka bahwa undangan diterima secara otomatis.

Ikhtisar`disableDetective.py` naskah

`disableDetective.py`Skrip menghapus akun anggota yang ditentukan dari grafik perilaku akun administrator di seluruh Wilayah yang ditentukan.

Ini juga menyediakan opsi untuk menonaktifkan Detective untuk akun administrator di seluruh Wilayah yang ditentukan.

Izin yang diperlukan untuk skrip

Skrip memerlukanAWS peran yang sudah ada sebelumnya di akun administrator dan di semua akun anggota yang Anda tambahkan atau hapus.

> **Note**
>
> Nama peran harus sama di semua akun.

Praktik terbaik yang direkomendasikan oleh kebijakan IAM adalah menggunakan peran yang paling tidak memiliki cakupan. Untuk menjalankan alur kerja skrip untuk membuat grafik, membuat anggota, dan menambahkan anggota ke grafik, izin yang diperlukan adalah:

- detektif:CreateGraph
- detektif:CreateMembers
- detektif:DeleteGraph
- detektif:DeleteMembers
- detektif:ListGraphs
- detektif:ListMembers
- detektif:AcceptInvitation

Hubungan kepercayaan peran

Hubungan kepercayaan peran harus memungkinkan instans atau kredenial lokal Anda untuk mengambil peran tersebut.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<ACCOUNTID>:user/<USERNAME>"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Jika Anda tidak memiliki peran umum yang mencakup izin yang diperlukan, Anda harus membuat peran dengan setidaknya izin tersebut di setiap akun anggota. Anda juga harus membuat peran di akun administrator.

Ketika Anda membuat peran, pastikan Anda melakukan hal berikut:

- Gunakan nama peran yang sama di setiap akun.
- Tambahkan izin yang diperlukan di atas (disarankan) atau pilih kebijakan AmazonDetectiveFullAccessterkelola.
- Tambahkan blok relasi kepercayaan peran seperti yang dibahas di atas.

Untuk mengotomatiskan proses ini, Anda dapat menggunakan`EnableDetective.yaml`AWS CloudFormation template. Karena template hanya menciptakan sumber daya global, template dapat dijalankan di Wilayah mana pun.

Menyiapkan lingkungan run untuk skrip Python

Anda dapat menjalankan skrip baik dari instans EC2 atau dari mesin lokal.

Meluncurkan dan mengonfigurasi instans EC2

Salah satu opsi untuk menjalankan skrip adalah menjalankannya dari instance EC2.

Untuk meluncurkan dan mengonfigurasi instans EC2

1. Luncurkan instans EC2 di akun administrator Anda. Untuk detail tentang cara meluncurkan instans EC2, lihat Memulai dengan Instans Linux Amazon EC2 dalam Panduan Pengguna Amazon EC2 untuk Instans Linux.
2. Lampirkan ke instance peran IAM yang memiliki izin untuk memungkinkan instance memanggil`AssumeRole` dalam akun administrator.

   Jika Anda menggunakan`EnableDetective.yaml`AWS CloudFormation template, maka peran instance dengan profil bernama`EnableDetective` dibuat.

   Jika tidak, untuk informasi tentang membuat peran instans, lihat posting blog Mudah Mengganti atau Melampirkan Peran IAM ke Instans EC2 yang Ada dengan Menggunakan Konsol EC2.
3. Pasang perangkat lunak yang diperlukan:
   - APT:`sudo apt-get -y install python3-pip python3 git`
   - RPM:`sudo yum -y install python3-pip python3 git`
   - Boto (versi minimum 1.15):`sudo pip install boto3`
4. Mengkloning ke instans EC2.

   ```
   git clone https://github.com/aws-samples/amazon-detective-multiaccount-scripts.git
   ```

Mengkonfigurasi mesin lokal untuk menjalankan skrip

Anda juga dapat menjalankan skrip dari mesin lokal Anda.

Untuk mengkonfigurasi mesin lokal untuk menjalankan skrip

1. Pastikan Anda telah menyiapkan kredensi mesin lokal untuk akun administrator yang memiliki izin untuk meneleponAssumeRole.
2. Pasang perangkat lunak yang diperlukan:
   - Python 3
   - Boto (versi minimum 1.15)
   - GitHub skrip

Platform	Petunjuk Penyiapan
Windows	1. Instal Python 3 (https://www.python.org/downloads/windows/). 2. Buka prompt perintah. 3. Untuk menginstal Boto, jalankan:`pip install boto3` 4. Unduh kode sumber skrip dari GitHub (https://github.com/aws-samples/amazon-detective-multiaccount-scripts).
Mac	1. Instal Python 3 (https://www.python.org/downloads/mac-osx/). 2. Buka prompt perintah. 3. Untuk menginstal Boto, jalankan:`pip install boto3` 4. Unduh kode sumber skrip dari GitHub (https://github.com/aws-samples/amazon-detective-multiaccount-scripts).
Linux	1. Untuk menginstal Python 3, jalankan salah satu dari berikut ini: • `sudo apt-get -y install install python3-pip python3 git` • `sudo yum install git python` 2. Untuk menginstal Boto, jalankan:`sudo pip install boto3` 3. Kloning kode sumber skrip dari https://github.com/aws-samples/amazon-detective-multiaccount-scripts.

Membuat `.csv` daftar akun anggota untuk ditambahkan atau dihapus

Untuk mengidentifikasi akun anggota yang akan ditambahkan atau dihapus dari grafik perilaku, Anda menyediakan `.csv` file yang berisi daftar akun.

Cantumkan setiap akun pada baris terpisah. Setiap entri akun anggota berisi IDAWS akun dan alamat email pengguna root akun.

Lihat contoh berikut ini:

```
111122223333,srodriguez@example.com
444455556666,rroe@example.com
```

Menjalankan**enableDetective.py**

Anda dapat menjalankan`enableDetective.py` skrip dari instans EC2 atau mesin lokal Anda.

Untuk menjalankan**enableDetective.py**

1. Salin`.csv` file ke`amazon-detective-multiaccount-scripts` direktori pada instans EC2 atau mesin lokal Anda.
2. Ubah ke direktori `amazon-detective-multiaccount-scripts`.
3. Jalankan`enableDetective.py` skrip.

   ```
   enableDetective.py --master_account administratorAccountID --assume_role roleName
    --input_file inputFileName --tags tagValueList --enabled_regions regionList  --
   disable_email
   ```

Ketika Anda menjalankan skrip, ganti nilai berikut:

`administratorAccountID`

IDAWS akun untuk akun administrator.

`roleName`

NamaAWS peran yang harus diasumsikan di akun administrator dan setiap akun anggota.

`inputFileName`

Nama`.csv` file yang berisi daftar akun anggota untuk ditambahkan ke grafik perilaku akun administrator.

`tagValueList`

(Opsional) Daftar nilai tag yang dipisahkan dengan koma untuk menetapkan ke grafik perilaku baru.

Untuk setiap nilai tag, formatnya adalah*key*=*value*. Misalnya:

```
--tags Department=Finance,Geo=Americas
```

regionList

(Opsional) Daftar Wilayah yang dipisahkan dengan koma untuk menambahkan akun anggota ke grafik perilaku akun anggota ke grafik perilaku akun administrator. Misalnya:

```
--enabled_regions us-east-1,us-east-2,us-west-2
```

Akun administrator mungkin belum mengaktifkan Detective di Wilayah. Dalam hal ini, skrip memungkinkan Detective dan membuat grafik perilaku baru untuk akun administrator.

Jika Anda tidak memberikan daftar Wilayah, maka skrip bertindak di semua Wilayah yang didukung Detective.

`--disable_email`

(Opsional) Jika disertakan, Detective tidak mengirim email undangan ke akun anggota.

Menjalankan**disableDetective.py**

Anda dapat menjalankan`disableDetective.py` skrip dari instans EC2 atau mesin lokal Anda.

Untuk menjalankan**disableDetective.py**

1. Salin`.csv` file ke`amazon-detective-multiaccount-scripts` direktori.
2. Untuk menggunakan`.csv` file untuk menghapus akun anggota yang terdaftar dari grafik perilaku akun administrator di daftar Wilayah yang ditentukan, jalankan`disableDetective.py` skrip sebagai berikut:

   ```
   disabledetective.py --master_account administratorAccountID --assume_role roleName
    --input_file inputFileName --disabled_regions regionList
   ```
3. Untuk menonaktifkan Detective untuk akun administrator di semua Wilayah, jalankan`disableDetective.py` skrip dengan`--delete-master` bendera.

   ```
   disabledetective.py --master_account administratorAccountID --assume_role roleName
    --input_file inputFileName --disabled_regions regionList --delete_master
   ```

Ketika Anda menjalankan skrip, ganti nilai berikut:

administratorAccountID

IDAWS akun untuk akun administrator.

roleName

NamaAWS peran yang harus diasumsikan di akun administrator dan setiap akun anggota.

inputFileName

Nama `.csv` file yang berisi daftar akun anggota yang akan dihapus dari grafik perilaku akun administrator.

Anda harus menyediakan `.csv` file bahkan jika Anda menonaktifkan Detective.

regionList

(Opsional) Daftar Wilayah yang dipisahkan dengan koma untuk melakukan hal berikut:

- Hapus akun anggota dari grafik perilaku akun administrator.
- Jika `--delete-master` bendera disertakan, nonaktifkan Detective.

Misalnya:

```
--disabled_regions us-east-1,us-east-2,us-west-2
```

Jika Anda tidak memberikan daftar Wilayah, maka skrip bertindak di semua Wilayah yang didukung Detective.

Riwayat dokumen untuk Panduan Administrasi Detektif

Tabel berikut menjelaskan perubahan penting pada dokumentasi sejak rilis terakhir Detective. Untuk notifikasi tentang pembaruan dokumentasi ini, Anda dapat berlangganan ke umpan RSS.

- Pembaruan dokumentasi terbaru: 02 Februari 2024

Perubahan	Deskripsi	Tanggal
Menghapus persyaratan GuardDuty keanggotaan Amazon	Anda tidak lagi diharuskan menjadi GuardDuty pelanggan untuk mengaktifkan Amazon Detective. Persyaratan untuk GuardDuty mengaktifkan akun Anda selama 48 jam sebelum mengaktifkan Detektif telah dihapus.	Februari 2, 2024
Perubahan cara Detektif membaca lalu lintas arus untuk VPC bersama	Jika Anda menggunakan VPC Amazon bersama, Anda mungkin melihat perubahan lalu lintas yang dipantau oleh Detektif. Kami menyarankan Anda meninjau perubahan dalam detail Aktivitas untuk volume aliran VPC secara keseluruhan guna memahami dampak potensial pada cakupan Anda, dan meninjau cara Detektif menghitung biaya yang diproyeksikan untuk memahami bagaimana hal itu dapat memengaruhi biaya layanan Anda.	Desember 20, 2023

Menambahkan informasi kebijakan terkelola ke bagian keamanan	Menambahkan investigasi Detektif dan menemukan tindakan ringkasan kelompok ke kebijakan. `AmazonDetectiveInvestigatorAccess`	26 November 2023
Titik akhir dan kuota Detektif Amazon	Detektif sekarang tersedia di Wilayah Israel (Tel Aviv).	Agustus 25, 2023
Menambahkan temuan AWS keamanan sebagai paket sumber data opsional baru.	Detective sekarang menyediakan temuan AWS keamanan sebagai paket sumber data opsional. Paket sumber data opsional ini memungkinkan Detective untuk menyerap data dari Security Hub dan menambahkan data tersebut ke grafik perilaku Anda.	16 Mei 2023
Menambahkan panel konsol baru di konsol Detektif untuk membantu pengguna memilih kebijakan AWS terkelola yang sesuai untuk kasus penggunaan spesifik mereka.	Detective menawarkan kebijakan terkelola untuk aman pilih izin yang Anda butuhkan.	3 April 2023

Menambahkan informasi kebijakan terkelola ke bagian keamanan	Detektif sekarang mendukung tindakan GuardDuty mendapatkan temuan melalui kebijakan. AmazonDetectiveFullAccess Bab keamanan sekarang memberikan rincian tentang kebijakan terkelola baru berikut untuk Detektif: AmazonDetectiveMemberAccess dan. AmazonDetectiveInvestigatorAccess	Januari 17, 2023
Menambahkan retensi data	Dengan Detective, Anda dapat mengakses data peristiwa historis hingga satu tahun.	Desember 20, 2022
Menambahkan istilah yang terkait dengan menemukan grup	Detective sekarang mendukung pencarian grup yang menghubungkan temuan terkait bersama-sama dalam satu tampilan untuk membantu Anda menyelidiki potensi aktivitas berbahaya di lingkungan Anda. Dari profil grup pencarian, Anda dapat beralih ke profil entitas dan menemukan ikhtisar yang terkait dengan grup tersebut.	3 Agustus 2022

Menambahkan sumber data opsional baru	Detective sekarang mendukung log audit EKS sebagai paket sumber data opsional. Akun administrator dapat mengaktifkan sumber data baru ini untuk grafik perilaku yang ada. Grafik yang dibuat setelah tanggal ini akan mengaktifkan sumber data ini secara default. Administrator dapat menonaktifkan sumber data ini secara manual kapan saja.	26 Juli 2022
Peran terkait layanan baru dan kebijakan terkelola untuk Detektif	Detektif sekarang memiliki peran terkait layanan,. `AWSServiceRoleForDetective` Peran terkait layanan digunakan untuk mengakses data Organizations atas nama Anda. Peran tersebut menggunakan kebijakan `AmazonDetectiveServiceLinkedRolePolicy` terkelola baru.	Desember 16, 2021

Integrasi ditambahkan dengan AWS Organizations	Detective sekarang terintegrasi dengan Organizations. Akun manajemen organisasi menunjuk akun administrator Detektif untuk organisasi. Akun administrator Detektif dapat melihat semua akun di organisasi, dan mengaktifkan akun tersebut sebagai akun anggota dalam grafik perilaku organisasi.	Desember 16, 2021
Nilai yang diperbarui untuk kuota volume data grafik perilaku	Meningkatkan kuota volume data untuk grafik perilaku. Pada 3,24 TB per hari, Detektif mengeluarkan peringatan. Dengan 3,6 TB per hari, tidak ada akun baru yang dapat ditambahkan. Pada 4,5 TB per hari, Detective berhenti menelan data ke dalam grafik perilaku.	10 Juni 2021
Menambahkan nilai tag ke opsi skrip Python	Saat Anda menggunakan skrip Detective Python untuk `enableDetective.py` mengaktifkan Detective, Anda sekarang dapat menetapkan nilai tag ke grafik perilaku.	19 Mei 2021

Menambahkan pengaktifan otomatis akun anggota yang lolos pemeriksaan volume data	Ketika akun anggota menerima undangan, statusnya Diterima (Tidak diaktifkan) sampai Detektif memverifikasi bahwa data mereka tidak akan menyebabkan volume data grafik perilaku melebihi kuota. Jika volume data tidak menjadi masalah, Detektif secara otomatis mengubah status menjadi Diterima (Diaktifkan). Perhatikan bahwa akun anggota yang ada yang saat ini Diterima (Tidak diaktifkan) tidak dapat diaktifkan secara otomatis.	12 Mei 2021
Menambahkan informasi kebijakan terkelola ke bagian keamanan	Bagian baru di bagian keamanan memberikan rincian tentang kebijakan terkelola untuk Detektif. Detective saat ini menyediakan kebijakan terkelola tunggal,. `AmazonDetectiveFullAccess`	10 Mei 2021
Mengubah nilai volume data dalam daftar akun anggota	Pada halaman manajemen akun, daftar akun anggota sekarang menampilkan volume data harian untuk setiap akun anggota. Sebelumnya daftar menampilkan volume sebagai persentase dari total volume yang diizinkan.	29 April 2021

Opsi yang direvisi untuk mengelola akun anggota	Mengganti menu Kelola akun dengan menu Tindakan. Menggabungkan opsi untuk menambahkan akun individual dan menambahkan akun dari file.csv. Memindahkan Aktifkan akun dari Kelola akun ke opsi terpisah di samping Tindakan.	5 April 2021
Menambahkan tag grafik perilaku dan otorisasi berdasarkan tag	Saat mengaktifkan Detektif, Anda dapat menambahkan tag ke grafik perilaku. Anda dapat mengelola tag untuk grafik perilaku dari halaman Umum. Detective juga mendukung otorisasi berdasarkan nilai tag.	31 Maret 2021
Perbedaan tambahan untuk AWS GovCloud (US) Wilayah	Detektif sekarang tersedia di Wilayah. AWS GovCloud (US) Di AWS GovCloud (AS-Timur) dan AWS GovCloud (AS-Barat), Detektif tidak mengirim email undangan ke akun anggota. Detektif juga tidak secara otomatis menghapus akun anggota yang dimatikan. AWS	24 Maret 2021
Menambahkan tab untuk memfilter daftar akun anggota berdasarkan status akun anggota	Daftar akun anggota sekarang menampilkan tab yang dapat Anda gunakan untuk memfilter daftar berdasarkan status akun anggota. Anda dapat melihat semua akun anggota, yang memiliki status Diterima (Diaktifkan), atau yang memiliki status selain Diterima (Diaktifkan).	16 Maret 2021

Menambahkan opsi ke skrip Python untuk menekan email undangan	`enableDetective.py` Skrip Detektif sekarang menyediakan opsi. `--disable_email` Ketika Anda menyertakan opsi itu, Detektif tidak mengirim email undangan ke akun anggota.	26 Februari 2021
Mengubah “akun master” menjadi “akun administrator”	Istilah "akun utama" diubah menjadi "akun administrator." Istilah ini juga diubah di konsol Detective dan API.	25 Februari 2021
Menambahkan opsi API untuk tidak mengirim email undangan ke akun anggota	Saat menggunakan Detective API untuk menambahkan akun anggota, akun administrator dapat memilih untuk tidak mengirim email undangan ke akun anggota.	25 Februari 2021
Kuota akun member meningkat menjadi 1.200	Akun master sekarang dapat mengundang hingga 1.200 akun anggota ke grafik perilaku mereka. Sebelumnya kuota adalah 1.000.	11 Desember 2020
Menambahkan nilai untuk kuota volume data grafik perilaku	Memperbarui informasi tentang kuota volume data grafik perilaku untuk menambahkan nilai kuota tertentu.	11 Desember 2020

Akun anggota sekarang dapat melihat penggunaan dan biaya yang diproyeksikan	Akun anggota sekarang dapat melihat informasi penggunaan mereka sendiri. Untuk akun anggota, halaman Penggunaan menunjukkan jumlah data yang dicerna ke dalam setiap grafik perilaku yang mereka kontribusikan. Akun anggota juga dapat melihat proyeksi biaya 30 hari mereka.	26 Mei 2020
Uji coba gratis sekarang per akun, bukan per grafik perilaku	Setiap akun Amazon Detective sekarang menerima uji coba gratis terpisah di setiap Wilayah. Uji coba gratis dimulai baik ketika akun mengaktifkan Detektif, atau pertama kali akun diaktifkan sebagai akun anggota.	26 Mei 2020
Skrip Python open source baru di GitHub	amazon-detective-multiaccount-scriptsRepositori baru di GitHub menyediakan skrip Python open source yang dapat Anda gunakan untuk mengelola grafik perilaku di seluruh Wilayah. Anda dapat mengaktifkan Detektif, menambahkan akun anggota, menghapus akun anggota, dan menonaktifkan Detektif.	21 Januari 2020

Memperkenalkan Detektif Amazon	Detective menggunakan pembelajaran mesin dan visualisasi yang dibuat khusus untuk membantu Anda menganalisis dan menyelidiki masalah keamanan di seluruh beban kerja Amazon Web Services (). AWS	2 Desember 2019

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