Hub Armada untuk Manajemen PerangkatAWS IoT

Armada untukAWS IoTPanduan Manajemen Perangkat

Hub Armada untuk Manajemen PerangkatAWS IoT: Armada untukAWS IoTPanduan Manajemen Perangkat

Table of Contents

Armada Hub untukAWS IoTManajemen Perangkat?

Hub Armada untukAWS IoTManajemen Perangkat (Fleet Hub), Anda dapat membangun aplikasi web mandiri untuk memantau kesehatan armada perangkat Anda. Anda dapat membuat aplikasi ini tersedia bagi pengguna di organisasi Anda, bahkan jika mereka tidak memilikiAWSakun. Gunakan Fleet Hub untuk mengelola tugas umum di seluruh armada seperti menyelidiki dan memperbaiki masalah operasional dan keamanan.

Fleet Hub menyediakan kemampuan berikut.

- Armada Perangkat dalam hampir waktu nyata.
- Atur peringatan untuk memberi tahu teknisi Anda tentang perilaku yang tidak biasa.
- Menjalankan pekerjaan.

> Note
>
> Untuk Fleet Hub untuk mengindeks data status konektivitas, Hal Anda harus terhubungAWS IoT Coredengan ID klien sama dengan nama Thing.

Hub ArmadaAWS IoTManajemen Perangkat

Administrator dapat menggunakan Armada Hub untukAWS IoTManajemen Perangkat untuk membuat aplikasi web yang aman dalam beberapa menit tanpa menyediakan sumber daya atau menulis kode apa pun. Aplikasi web yang Anda buat dengan menggunakan Fleet Hub terintegrasi dengan sistem identitas yang ada, seperti Active Directory. Hal ini memungkinkan administrator Anda untuk menerapkan model otentikasi dan otorisasi mereka sendiri.

Aplikasi web Fleet Hub terintegrasi denganAWS IoT Corepengindeksan armada dan pemantauan perangkat. Integrasi ini memberikan kemampuan untuk memantau data kesehatan perangkat dan membuat alarm saat perangkat di armada Anda mencapai keadaan tertentu.

Aplikasi Fleet Hub menggunakan`AWSIoTFleetHubFederationAccess`kebijakan terkelola. Untuk informasi selengkapnya, lihat ??? (p. 41).

Kasus penggunaan:

- Visualisasikan masalah konektivitas perangkat - Anda dapat melihat jumlah perangkat yang terputus di armada, status koneksi terakhir untuk perangkat, dan alasan atau alasan mengapa perangkat terputus.
- Atur alarm - Anda dapat mengatur ambang batas yang memicu alarm saat sejumlah perangkat tertentu terputus. Alarm juga dapat memberi tahu Anda saat perangkat atau perangkat memutuskan sambungan karena alasan tertentu. Anda kemudian dapat melihat data perangkat terperinci untuk menyelidiki dan memecahkan masalah.
- Jalankan pekerjaan - Anda dapat menjalankan operasi jarak jauh (seperti pembaruan firmware) pada satu perangkat lagi.

Cara kerja pengindeksan data Fleet Hub

Anda dapat menggunakan konsol Fleet Hub untuk mengaktifkan pengindeksan armada untuk armada perangkat Anda. Ketika Anda mengaktifkan pengindeksan armada di Fleet Hub, Anda mengaktifkannya untuk seluruh armada dan membuatnya tersedia untuk semua aplikasi Fleet Hub.

Ketika diaktifkan, indeks armada mengindeks semuaAWS IoT Core-managed bidang secara otomatis. Anda juga dapat menggunakan pengindeksan armada untuk menambahkan data kustom yang dapat Anda gunakan untuk query dan agregat data dalam aplikasi Fleet Hub.

Cara kerja alarm Fleet Hub

Aplikasi web Fleet Hub menyediakan antarmuka yang memungkinkan pengguna membuat alarm. Langkah-langkah berikut menunjukkan cara pengguna membuat alarm di Fleet Hub.

1. Buat kueri ke data agregat - Tentukan kueri yang menggabungkan perangkat yang ingin ditargetkan pengguna Anda dengan menggunakan bidang yang dapat dicari.
2. Konfigurasi ambang batas - Mengatur ambang batas yang memicu alarm ketika kondisi dalam data diindeks (seperti status konektivitas selama interval tertentu) tercapai.
3. Konfigurasi pemberitahuan - Tentukan sekelompok penerima yang diberi tahu Fleet Hub saat perangkat yang ditentukan berada dalam alarm.

Cara kerja Fleet Hub

Anda dapat menggunakan konsol Fleet Hub untuk menjalankan operasi jarak jauh pada perangkat.

Ketika template pekerjaan diaktifkan, Anda dapat membuat pekerjaan tertentu dari template dalam aplikasi Fleet Hub Anda.

Armada Hub untukAWS IoTManajemen Perangkat untuk administrator

Bagian ini berisi panduan untuk administrator tentang cara membuat dan mengelola Fleet Hub untukAWS IoTAplikasi web Manajemen Perangkat.

Topik

Mulai

Bagian ini menjelaskan cara membuat dan mengatur Fleet Hub untukAWS IoTAplikasi web Manajemen Perangkat.

Topik

Buat aplikasi Armada Hub pertama Anda

Prasyarat

Daftar berikut berisi sumber daya yang Anda butuhkan untuk membuat aplikasi web Fleet Hub.

- Akun AWS.
- AWSSistem Masuk Tunggaldiaktifkan untuk akun Anda. (Jika belum mengaktifkan layanan ini,AWS IoT Corekonsol (https://console.aws.amazon.com/iot/) meminta Anda untuk melakukannya.)

Buat aplikasi web Fleet Hub pertama Anda

Langkah-langkah berikut menjelaskan cara membuat Fleet Hub untukAWS IoTAplikasi web Manajemen Perangkat.

1. Arahkan keAWS IoT Corekonsol (https://console.aws.amazon.com/iot/), dan di panel kiri, memilihArmada Hub, dan kemudianAplikasi.

2. Pada halaman aplikasi, pilihMembuat aplikasi.
3. PadaMengonfigurasi Sistem Masuk Tunggallaman, jika Anda belum mengaktifkanAWS IAM Identity Center (successor to AWS Single Sign-On)(IAM Identity Center), ikuti langkah-langkah untuk mengaktifkannya.AWS Organizations mengirimi Anda email. Pilih tautan di email untuk menyelesaikan aktivasiIAM Identity Center.

   Note

   Anda dapat menghubungkan penyedia identitas Anda sendiriIAM Identity Center. Untuk informasi selengkapnya, lihatApaAWSSistem Masuk Tunggal?danConnect ke penyedia identitas eksternal Anda.

   Halaman tersebut memberi tahu Anda jika Anda sudah mengaktifkannyaIAM Identity Center.

   Pilih Selanjutnya.
4. PadaIndeksAWS IoTdata, meninjau informasi diBagaimana aliran data bekerja dariAWS IoTke Armada Hubbagian. Halaman ini menghubungkan Anda ke halaman diAWS IoT Corekonsol tempat Anda dapat mengaktifkan dan mengelolaAWS IoT Corepengindeksan armada. Anda dapat menggunakan layanan ini untuk mengindeks, mencari, dan menggabungkan data registri, data bayangan, data konektivitas perangkat (peristiwa siklus hidup perangkat), dan data pelanggaran perangkat. Anda juga dapat membuat bidang khusus selain bidang terkelola yangAWS IoT Coreindeks pengindeksan armada secara default.

   - Jika Anda telah mengaktifkan pengindeksan armada, halaman ini menampilkan pengaturan pengindeksan armada dan bidang khusus Anda.

   - Jika Anda belum mengaktifkan pengindeksan dan konektivitas benda, Anda harus melakukannya untuk menggunakan Fleet Hub.

   Setelah selesai mengelola dan meninjau pengaturan pengindeksan armada, pilihSelanjutnya.

   Untuk informasi selengkapnya tentang cara mengaktifkan pengindeksan armada untuk aplikasi Fleet Hub, lihatMengelola pengindeksan armada untuk aplikasi Fleet Hub (p. 5).
5. PadaMengonfigurasi aplikasihalaman, diPeran aplikasibagian, buat peran layanan baru atau pilih peran layanan yang ada. Aplikasi web Fleet Hub Anda mengasumsikan peran ini ketika menggunakan sumber daya Fleet Hub. Pengguna federasi memiliki izin yang sama dengan peran saat mereka menggunakan aplikasi web.

   - Jika Anda membuat peran baru, nama peran harus dimulai dengan string berikut:`AWSIotFleetHub_`*`random_string`*.

   - Jika Anda memilih peran yang ada, pastikan peran tersebut memiliki izin yang ada di dokumen kebijakan. Untuk melihat izin yang dibutuhkan aplikasi web Fleet Hub Anda, pilihMeninjau detail peran. Jendela terbuka yang menunjukkan dokumen kebijakan yang diterapkan layanan untuk peran baru apa pun yang Anda buat dari halaman ini.
6. PadaMengonfigurasi aplikasihalaman, diProperti aplikasibagian, masukkan nama untuk aplikasi Anda. Secara opsional, Anda juga dapat memasukkan deskripsi aplikasi.

   Pilih Create application (Buat aplikasi).
7. PadaAplikasihalaman, pilih aplikasi yang Anda buat dan pilihMeninjau detail. Tinjau detail aplikasi.

   Note

   Untuk informasi selengkapnya tentang kemungkinan solusi untuk menyelesaikan masalah sebagai administrator Fleet Hub, lihatPemecahan Masalah (p. 7).

Mengelola pengindeksan armada untuk aplikasi Fleet Hub

Anda dapat menggunakanAWS IoT Corekonsol atauAWS CLIuntuk mengaktifkan pengindeksan armada dan mengkonfigurasi sumber data berikut untuk diindeks:AWS IoTregistrasidataAWS IoT Device Shadowdata[AWS IoTkonektivitas](#)data, dan[AWS IoT Device Defenderpelanggaran](#)data. Langkah-langkah berikut menjelaskan cara mengaktifkan pengindeksan armada untuk Armada HubAWS IoTManajemen Perangkat diAWS IoT Corekonsol. Untuk melihat langkah-langkah menggunakanAWS CLI, lihat[Mengelola hal pengindeksan](#).

> **Important**
>
> 20 Juli 2022 adalah rilis Ketersediaan UmumAWS IoTIntegrasi pengindeksan armada Manajemen Perangkat denganAWS IoT Corebernama bayangan danAWS IoT Device Defendermendeteksi pelanggaran. Dengan rilis GA ini, Anda dapat mengindeks bayangan bernama tertentu dengan menentukan nama bayangan. Jika Anda menambahkan bayangan bernama untuk pengindeksan selama periode pratinjau publik fitur ini dari 30 November 2021 hingga 19 Juli 2022, kami menyarankan Anda untuk mengkonfigurasi ulang pengaturan pengindeksan armada Anda dan memilih nama bayangan tertentu untuk mengurangi biaya pengindeksan dan mengoptimalkan kinerja. Untuk informasi selengkapnya tentang cara mengkonfigurasi ulang pengaturan pengindeksan armada, lihat[Mengelola pengindeksan armada](#).

1. Arahkan keAWS IoT Corekonsol (https://console.aws.amazon.com/iot/), dan di panel kiri, memilihPengaturan.
2. PadaPengaturanhalaman, arahkan kePengindeksan armadabagian, lalu pilihMengelola pengindeksan.
3. PadaMengelola pengindeksan armadahalaman, diKonfigurasibagian, pilihHal pengindeksandan sumber data yang Anda inginkanAWS IoTuntuk indeks. Anda harus mengaktifkan hal pengindeksan dan konektivitas hal untuk menggunakan Fleet Hub.
4. (Opsional) PadaMengelola pengindeksan armadahalaman, diBidang khusus untuk agregasi-opsionalbagian, buat bidang khusus selain bidang terkelola yang indeks pengindeksan armada secara default.

   Setelah selesai mengelola dan meninjau pengaturan pengindeksan armada, pilihSelanjutnya.

   Diperlukan beberapa saat bagi pengindeksan armada untuk memperbarui pengaturan. Untuk informasi lebih lanjut tentang cara mengelola pengindeksan armada, lihat[Mengelola pengindeksan armada](#).

Menambahkan pengguna ke aplikasi Fleet Hub

Armada Hub untukAWS IoTAplikasi web Manajemen Perangkat tidak berisi pengguna saat baru dibuat. Anda harus menambahkan pengguna sebelum Anda dan anggota organisasi Anda dapat menggunakan aplikasi. Langkah-langkah dalam topik ini menjelaskan cara menambahkan pengguna ke aplikasi Anda.

Anda menambahkan pengguna dari sistem identitas Anda yang ada dengan mengaturAWS IAM Identity Center (successor to AWS Single Sign-On)(IAM Identity Center) untuk akun Anda. Anda dapat menghubungkan penyedia identitas Anda sendiriIAM Identity Center. Untuk informasi selengkapnya, lihat[ApaAWSSistem Masuk Tunggal?](#).

1. PadaAplikasihalaman, pilih aplikasi web Anda dariAplikasi Armada HubDaftar. Pilih View details (Lihat detail).
2. Di halaman detail aplikasi, pilihMenambahkan pengguna.
3. DiTambahkan pengguna Fleet Hubjendela, pilih pengguna dari organisasi Anda bahwa Anda ingin memiliki akses ke aplikasi. MemiilihTambahkan pengguna yang dipilih.
4. Di halaman detail aplikasi, verifikasi bahwa Anda melihat pengguna yang Anda pilih diPengguna Armada HubDaftar.

AWSdanAWS IoT CoreLayanan yang berinteraksi Armada Hub untukAWS IoTManajemen Perangkat

Topik ini menjelaskan bagaimana fitur di Fleet Hub untukAWS IoTManajemen Perangkat berinteraksi dengan lainnyaAWSlayanan untuk memberikan kemampuan dalam aplikasi web Fleet Hub Anda.

Tabel berikut menunjukkan apaAWSHub Armada untukAWS IoTManajemen Perangkat menggunakan untuk mengimplementasikan setiap fitur.

Kemampuan	AWS layanan	Deskripsi
Mengintegrasikan sistem identitas yang ada, seperti Active Directory.	AWS IAM Identity Center (successor to AWS Single Sign-On) (IAM Identity Center)	Anda menambahkan pengguna dari sistem identitas Anda yang ada dengan menyiapkanAWS IAM Identity Center (successor to AWS Single Sign-On)(IAM Identity Center) untuk akun Anda. Anda dapat menghubungkan penyedia identitas Anda sendiriIAM Identity Center. Untuk informasi selengkapnya, lihatApaAWSSistem Masuk Tunggal?
Membuat kueri dengan menggunakanAWS-dikelola dan bidang kustom.	AWS IoTPengindeksan armada	Gunakan layanan pengindeksan armada untuk mengindeks, mencari, dan menggabungkan data registri, data bayangan, dan data konektivitas perangkat (peristiwa siklus hidup perangkat). Anda juga dapat membuat bidang khusus selain bidang terkelola yangAWS IoT Coreindeks pengindeksan armada secara default. Untuk informasi lebih lanjut tentang pengindeksan armada, lihatPengindeksan Armada.
Buat alarm untuk satu set perangkat yang ditentukan oleh kueri.	Amazon CloudWatch (CloudWatch)	Dasbor Fleet Hub mengekspos metrik CloudWatch yang dapat Anda gunakan dalam kombinasi dengan bidang yang dapat dicari untuk membuat ambang batas yang mengkhawatirkan. Selain itu, Anda dapat membuat alarm CloudWatch yang menghasilkan notifikasi Amazon Simple Notification Service (Amazon SNS) kapan pun jumlah perangkat yang terhubung berada di bawah kuantitas yang ditentukan.

Kemampuan	AWS layanan	Deskripsi
		Untuk informasi tentang CloudWatch, lihatApa yang Dimaksud dengan Amazon CloudWatch? Untuk informasi tentang bagaimanaAWS IoT Corebekerja dengan CloudWatch untuk membuat metrik dan alarm, lihatPemantauanAWS IoTalarm dan metrik menggunakan CloudWatch.

Pemecahan Masalah

Bagian ini menyediakan informasi pemecahan masalah dan solusi yang mungkin untuk membantu menyelesaikan masalah sebagai administrator Armada Hub.

Gejala	Solusi
Tautan aplikasi web saya tidak berfungsi.	Mungkin diperlukan waktu beberapa jam setelah Anda membuat aplikasi agar tautan berfungsi.
Saya tidak bisa masuk ke aplikasi web saya.	Pastikan Anda telah menambahkan setidaknya satu pengguna ke aplikasi Anda. Pastikan peran Anda memiliki hubungan kepercayaan yang sesuai seperti berikut ini: `{"Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "Service": "iotfleethub.amazonaws.com" }, "Action": "sts:AssumeRole" } ] }` Untuk informasi selengkapnya tentang cara mengedit hubungan kepercayaan IAM, lihatMengedit hubungan kepercayaan untuk peran yang ada.
Saya tidak dapat membuat aplikasi web.	Pastikan Anda belum mencapai batas total aplikasi web.
Saya tidak melihat bidang khusus yang saya harapkan.	Periksa untuk memastikan bahwa Anda telah mengatur pengindeksan armada dengan benar. Untuk informasi lebih lanjut tentang pengindeksan armada, lihatPengindeksan armada.

Armada HubAWS IoTManajemen Perangkat untuk pengguna

Bagian ini berisi informasi untuk pengguna Fleet Hub untukAWS IoTAplikasi web Manajemen Perangkat. Untuk informasi tentang membuat aplikasi Fleet Hub dan menambahkan pengguna ke aplikasi tersebut, lihatArmada Hub untukAWS IoTManajemen Perangkat untuk administrator (p. 3).

Topik

Mulai

Bagian ini berisi informasi tentang memulai dengan menggunakan fitur Fleet Hub untukAWS IoTAplikasi web Manajemen Perangkat.

Topik

Buat kueri pertama Anda

Topik ini akan memandu Anda melalui langkah-langkah untuk membuat Fleet Hub sederhana untukAWS IoTKueri Manajemen Perangkat. Query ditentukan menggunakan sintaks permintaan pencarian.

Prasyarat

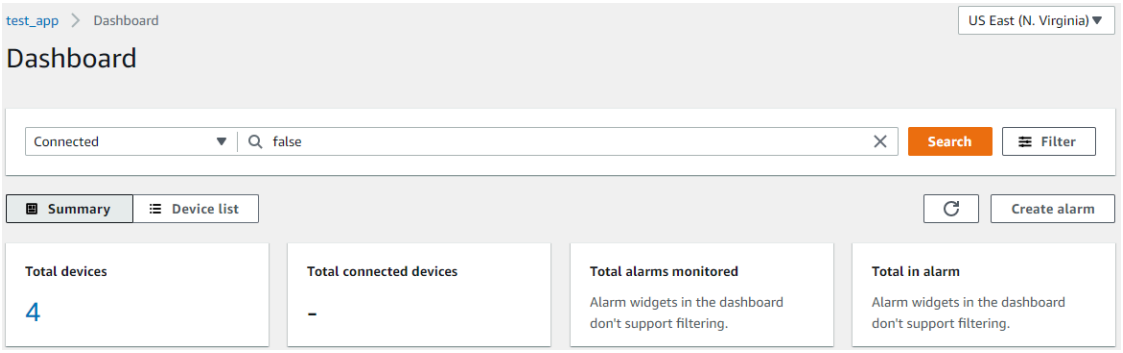
- Aplikasi Fleet Hub yang terkait denganAWS IoT Coreakun yang berisi perangkat (hal-hal).
- Akun di organisasi Anda yang memiliki izin untuk menggunakan aplikasi Fleet Hub.

Buat kueri Fleet Hub pertama Anda

Buat kueri Fleet Hub pertama Anda

1. Arahkan ke aplikasi Fleet Hub Anda.

   Tampilan dasbor default menampilkan daftar semua perangkat yang berisi atribut terkelola dan kustom. Atribut yang berisiatributawalan adalah atribut kustom.
2. Pada menu di bagian atas halaman, pilihMENGHUBUNGdariSemua bidang. ENTER**`false`**di kotak teks di samping menu dropdown.



3. Untuk melakukan pencarian, pilihCari. Anda melihat daftar semua perangkat yang tidak terhubungAWS IoT Core.

Untuk informasi selengkapnya tentang sintaks kueri dan kueri contoh kueri, lihatSintaksis Kueri,Kueri hal sampel, danContoh pertanyaan kelompok hal.

Buat alarm pertama Anda

Topik ini akan memandu Anda melalui langkah-langkah untuk membuat Fleet Hub sederhana untukAWS IoTAlarm Manajemen Perangkat.

Prasyarat

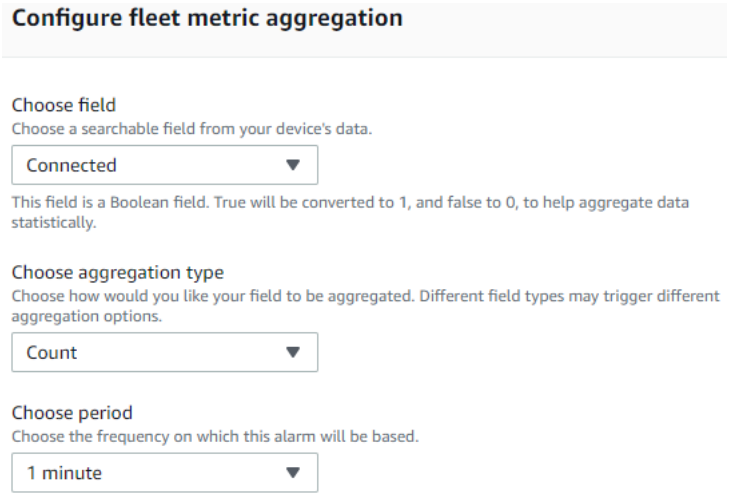
- Aplikasi Fleet Hub yang terkait denganAWS IoT Coreakun yang berisi perangkat (hal-hal).
- Akun di organisasi Anda yang memiliki izin untuk menggunakan aplikasi Fleet Hub.

Membuat alarm pertama Anda

Buat alarm Fleet Hub pertama Anda

1. Arahkan ke aplikasi Fleet Hub Anda.
2. Jika Anda ingin menargetkan serangkaian perangkat tertentu, buat kueri. Untuk instruksi tentang cara membuat kueri sederhana, lihatthe section called “Buat kueri pertama Anda” (p. 8). Jika Anda tidak membuat kueri, alarm Anda akan berlaku untuk semua perangkat di armada Anda.
3. Pada halaman dasbor default, pilihBuat alarm.
4. PadaBangun metrik agregasihalaman, verifikasi bahwa kueri Anda muncul di bawahKueri target. DiMengkonfigurasi agregasi metrik armadabagian, padaPilih bidangmenu, pilihMENGHUBUNG. IniAWS-managed field menunjukkan apakah perangkat tersambung keAWS IoT Core. ParameterPilih bidangmenuAWSbidang yang dikelola dan bidang khusus yang telah dibuat oleh administrator AndaAWS IoTpengindeksan armada
5. UntukPilih jenis agregasi, memilih salah satu opsi berikut.
   - Maksimum- Konfigurasikan ambang batas maksimum.
   - Jumlah- Konfigurasikan hitungan tertentu sebagai ambang batas.
   - Jumlah- Konfigurasikan jumlah sebagai ambang batas.
   - Minimum- Konfigurasikan ambang batas minimum.
   - Rata-rata- Konfigurasikan ambang rata-rata.
6. UntukPilih Periode, pilih durasi kondisi yang ditentukan dalam menu sebelumnya yang akan memicu alarm.

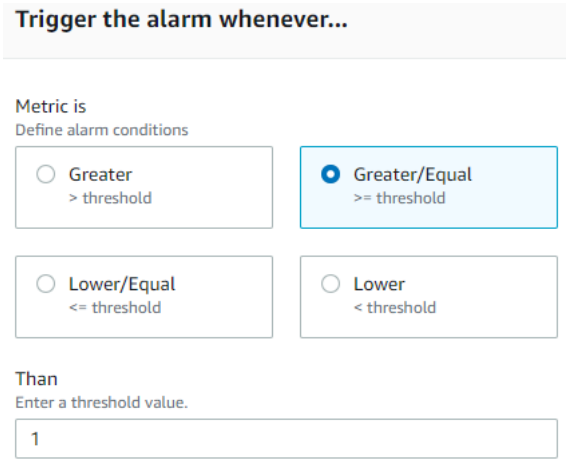
Contoh pengaturan untukMengkonfigurasi agregasi metrik armadadapat terlihat seperti berikut ini:



Pilih Selanjutnya.

7. PadaMengatur Ambanghalaman, diMemicu alarm setiap kali...bagian, memilih salah satu opsi berikut.
   - Lebih besar- Alarm ketika metrik dan tipe agregasi melebihi nilai yang ditentukan.
   - Besar/Sama- Alarm ketika metrik dan tipe agregasi sama atau melebihi nilai yang ditentukan.
   - LEBIH RENDAH- Alarm ketika metrik dan jenis agregasi jatuh di bawah nilai yang ditentukan.
   - LEBIH RENDAH/Sama- Alarm ketika metrik dan tipe agregasi sama atau turun di bawah nilai yang ditentukan.
8. DiDarikotak teks, tentukan nilai yang akan digunakan sebagai ambang batas untuk alarm.

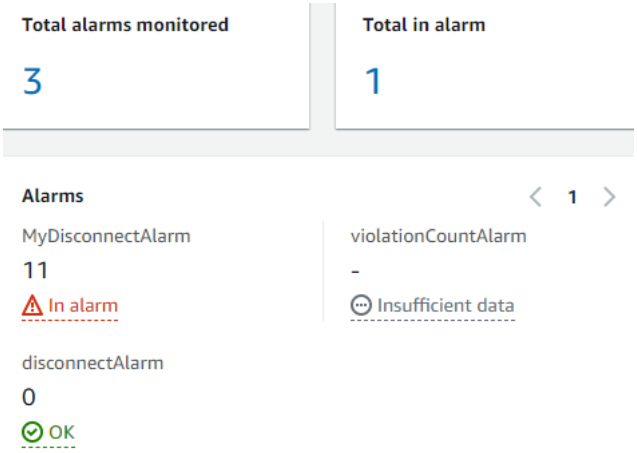
   Contoh pengaturan untukMengatur Ambangdapat terlihat seperti berikut ini:



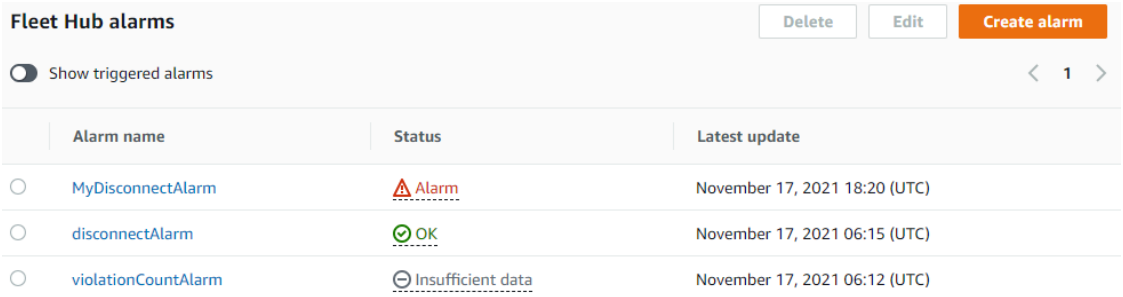
   Pilih Selanjutnya.

9. PadaBeri tahu penggunahalaman, diBeri tahu - opsional, masukkan nama untuk daftar email yang berisi pengguna di organisasi Anda yang menerima pemberitahuan saat alarm aktif. Masukkan daftar alamat email yang dipisahkan koma untuk mengisi daftar ini.
10. DiRincianbagian, masukkan nama untuk alarm Anda, dan opsional masukkan deskripsi untuk alarm Anda. Pilih Selanjutnya.
11. PadaUlasanhalaman, memverifikasi informasi yang Anda masukkan pada halaman sebelumnya. Pilih Submit (Kirim). Anda kembali ke dasbor default.

12. Di dasbor default, widget alarm menampilkan informasi dari semua alarm yang Anda buat.



Untuk melihat detail alarm yang Anda buat, di panel navigasi kiri, pilihAlarm Armada Hub.



Meninjau detail perangkat

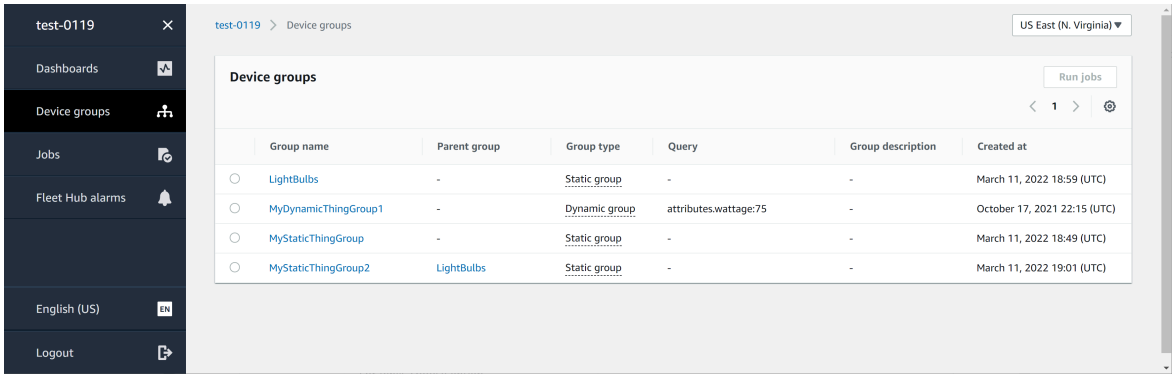
Topik ini akan memandu Anda melalui langkah-langkah untuk melihat detail tentang grup perangkat Anda dan perangkat Anda.

Prasyarat

- Aplikasi Fleet Hub yang terkait denganAWS IoT Coreakun yang berisi perangkat (hal-hal).
- Akun di organisasi Anda yang memiliki izin untuk menggunakan aplikasi Fleet Hub.

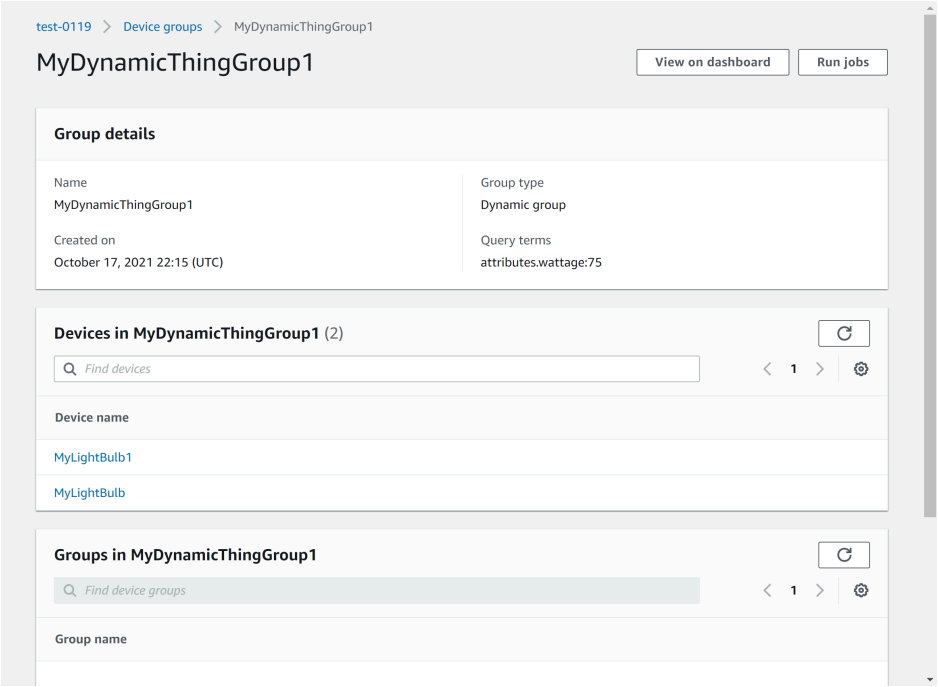
Grup perangkat

Ketika Anda masuk ke aplikasi web Fleet Hub Anda, Anda melihatGrup perangkatpada panel navigasi kiri. ParameterGrup perangkathalaman daftar semua kelompok perangkat dalam aplikasi web Fleet Hub Anda. Untuk melihat detail grup perangkat, pilih grup perangkat tertentu dariNama kelompokkolom.



Perincian grup perangkat

ParameterPerincian grup perangkathalaman berisi informasi tentang grup perangkat yang Anda pilih. Untuk melihat detail perangkat, pilih perangkat tertentu dariNama perangkatkolomPerangkat di***XXX***bagian.



Perincian Perangkat

ParameterPerincian Perangkathalaman berisi informasi tentang perangkat yang Anda pilih.

Detail

ParameterRincianbagian berisi informasi berikut tentang perangkat Anda:

- Nama perangkat— Nama sumber daya hal yang mewakili perangkat Anda. Untuk informasi selengkapnya, lihatBagaimana mengelola hal-hal dengan registri.

- Tipe Hal- Jenis hal yang terkait dengan perangkat Anda. Anda dapat menggunakan tipe hal untuk menyimpan informasi yang umum untuk semua hal dengan tipe hal yang sama. Untuk informasi selengkapnya, lihatTipe Hal.

- Timestamp koneksi terakhir- Stempel waktu untuk saat perangkat Anda terakhir terhubungAWS IoT.
- Tautan perangkat yang dapat dibagikan- Tautan yang dapat dibagikan yang menunjuk kePerincian Perangkathalaman perangkat yang dipilih.
- Status koneksi terakhir- Status koneksi perangkat Anda keAWS IoT. Jika perangkat Anda tersambung, nilainya adalah`true`. Jika tidak terhubung, nilainya adalah`false`.
- Memutus alasan— Alasan mengapa perangkat Anda terputus.

Data yang dilaporkan

ParameterData yang dilaporkanbagian berisi informasi tentang data registri perangkat Anda, data bayangan perangkat, dan grup hal.

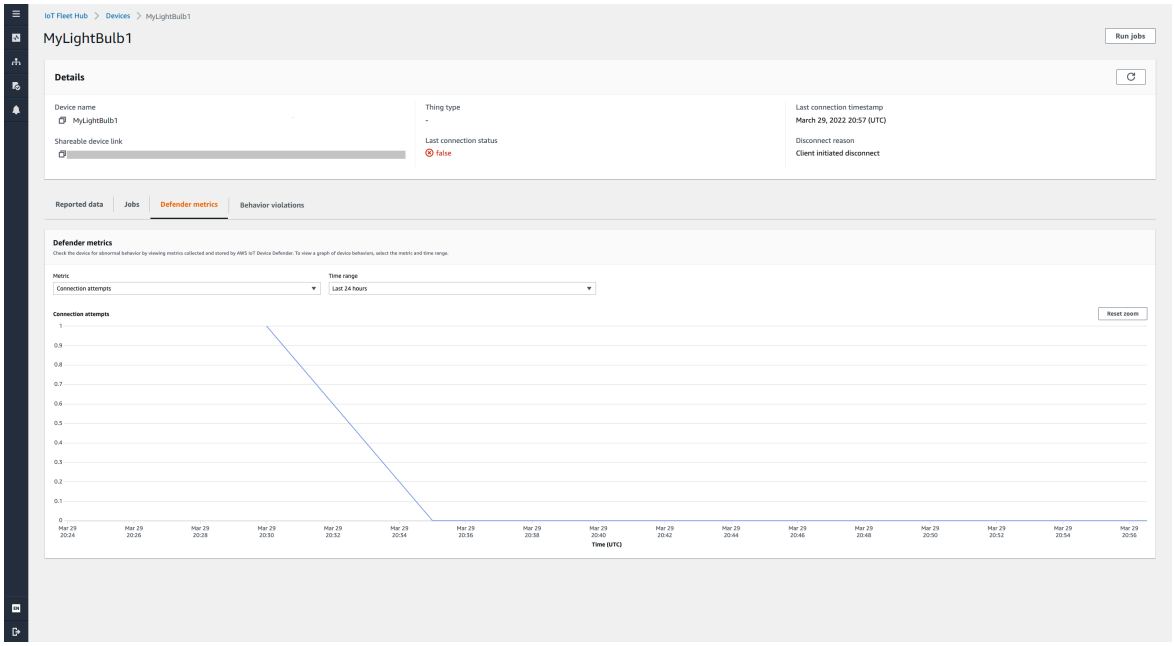
- Bidang Perangkat- Bidang yang diindeks perangkat Anda diAWS IoTpengindeksan armada Untuk informasi selengkapnya, lihatMengelola pengindeksan armada.
- Bayangan Perangkat- Bayangan yang terkait dengan perangkat Anda. Bayangan perangkat dapat mencakup bayangan klasik yang tidak disebutkan namanya dan bayangan bernama. Untuk informasi selengkapnya, lihatAWS IoTBayangan perangkat.
- Grup perangkat— Grup perangkat yang terkait dengan perangkat Anda. Grup perangkat dapat menyertakan grup benda statis dan grup benda dinamis. Untuk informasi selengkapnya, lihatKelompok hal statisdanKelompok hal yang dinamis.

Tugas

ParameterTugasbagian menampilkan semua pekerjaan yang berjalan pada perangkat. Setiap pekerjaan memiliki halaman detail yang menampilkan informasi ringkasan tentang pekerjaan, termasuk informasi target dan waktu proses. Untuk informasi selengkapnya, lihatBekerja dengan pekerjaan dan template pekerjaan di Fleet Hub untukAWS IoTManajemen Perangkat, danTugas.

Metrik bek

ParameterMetrik bekbagianAWS IoT Device Defendermetrik yang terkait dengan perangkat yang Anda pilih saat ini. Anda dapat menggunakan data metrik yang ditampilkan untuk memvisualisasikan operasi perangkat Anda dalam jangka waktu yang Anda pilih. Untuk melihat data metrik bek dari aplikasi Fleet Hub Anda, administrator Fleet Hub Anda harus terlebih dahulu menyiapkanAWS IoT Device Defendermetrik yang terkait dengan perangkat yang dipilih. Untuk informasi selengkapnya tentang cara membuat dan menyiapkanAWS IoT Device Defendermetrik untuk perangkat Anda, lihatMetrik khusus,Metrik sisi perangkat, danMetrik sisi cloud.



Pelanggaran perilaku

ParameterPelanggaran perilakubagian menampilkan diindeksAWS IoT Device Defendermendeteksi data pelanggaran yang terkait dengan perangkat yang Anda pilih saat ini. Data pelanggaran perilaku dapat mencakup jumlah pelanggaran, waktu pelanggaran terakhir, dan nilai metrik pelanggaran terakhir. Untuk melihat data pelanggaran perilaku dari aplikasi Fleet Hub, administrator Fleet Hub Anda harus menyiapkanAWS IoT Device Defenderpelanggaran perilaku dalam profil keamanan dan konfigurasiAWS IoT Device Defenderpelanggaran dipengindeksan armada. Untuk informasi selengkapnya tentang cara menyiapkan pelanggaran perilaku diAWS IoT Device Defenderprofil keamanan, lihatAWS IoT Device DefenderMendeteksi. Untuk informasi selengkapnya tentang cara mengonfigurasiAWS IoT Device Defenderpelanggaran, lihatMengelola pengindeksan armada untuk aplikasi Fleet HubdanMengelola Hal Pengindeksan.

Kueri dan filter

Anda dapat menggunakan Armada Hub untukAWS IoTKueri Manajemen Perangkat untuk membuat dan melihat daftar hal di armada perangkat Anda. SemuaAWSkolom -managed tersedia untuk Anda sebagai filter kueri. Anda juga dapat membuat bidang kustom dengan menggunakanAWS IoTpengindeksan armada. Untuk informasi selengkapnya tentang pengindeksan armada, lihatPengindeksan armada.

Topik

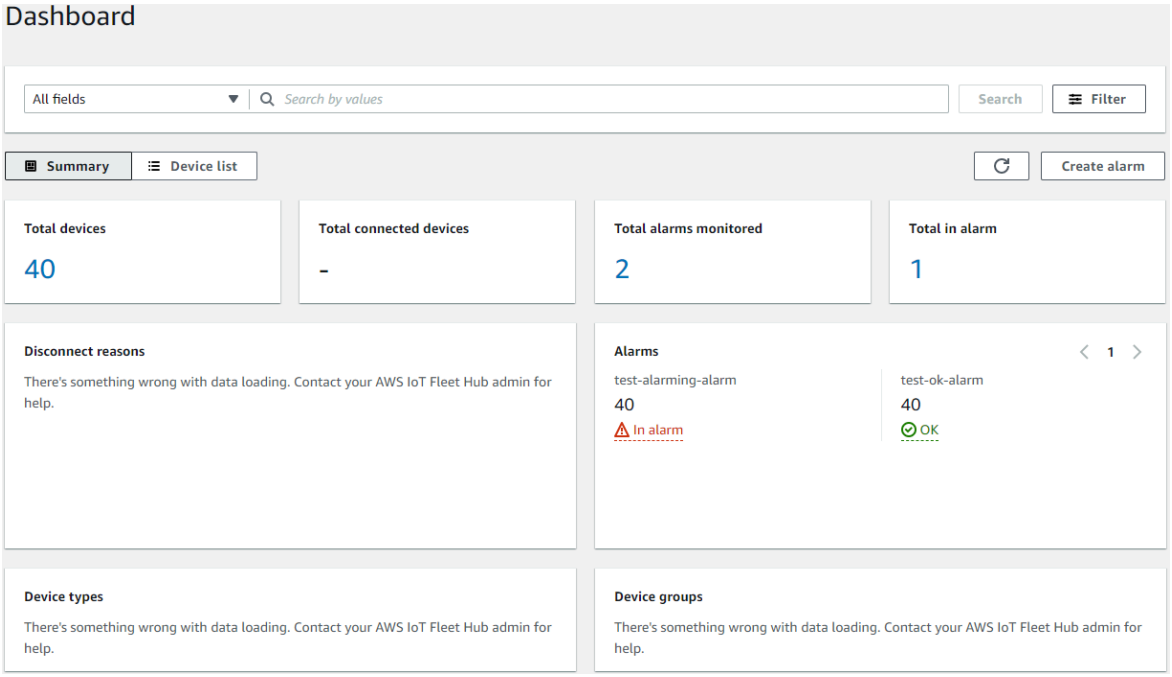
Lihat dasbor

Saat pertama kali masuk ke Fleet HubAWS IoTAplikasi web Manajemen Perangkat, Anda melihat dashboard yang menyajikan dua tampilan data tentang perangkat dalam armada Anda.

Ringkasan

Parameterringkasantampilan menampilkan tampilan data yang digulung tentang semua perangkat di armada Anda. Ini memberikan informasi berikut.

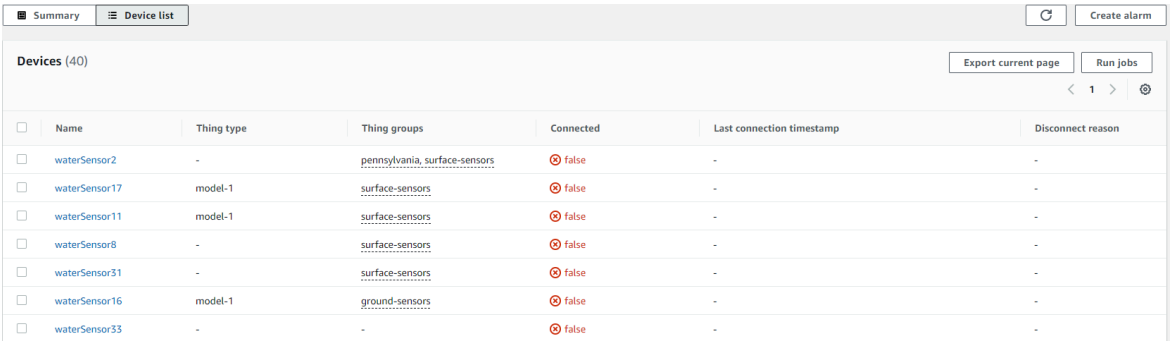
- Jumlah total perangkat
- Jumlah perangkat yang terhubung
- Daftar alasan mengapa perangkat terputus
- Jenis hal yang telah Anda buat untuk armada Anda dan jumlah perangkat untuk setiap jenis
- Kelompok hal yang telah Anda buat untuk armada Anda dan jumlah perangkat di setiap grup



Daftar perangkat

ParameterDaftar perangkattampilan menampilkan tabel yang mencantumkan perangkat di armada Anda. Tabel tersebut memberikan informasi berikut untuk setiap perangkat dalam daftar.

- Nama perangkat
- Status koneksi perangkat
- Cap waktu untuk koneksi terakhir perangkat
- Untuk perangkat yang tidak terhubung, alasan mengapa perangkat tersebut terputus
- Jenis benda perangkat
- Kelompok hal perangkat
- Bidang kustom yang telah Anda buat di layanan pengindeksan armada



Pada daftar perangkat, Anda dapat memilihEkspor halaman saat iniuntuk mendownload file CSV yang berisi perangkat yang ditampilkan pada halaman (tetapi tidak pada halaman berikutnya, jika daftar dipaginasi).

Anda dapat menggunakan kueri dan filter untuk mempersempit jumlah perangkat yang menghasilkan data ringkasan dalam tampilan pertama dan yang muncul dalam daftar perangkat. Untuk informasi selengkapnya tentang menggunakan kueri dan filter untuk mendapatkan informasi lebih spesifik tentang perangkat di armada Anda, lihatthe section called “Membuat kueri” (p. 16).

Membuat kueri dengan filter

Topik ini menjelaskan bagaimana Fleet Hub untukAWS IoTKueri Manajemen Perangkat bekerja dan memandu Anda melalui langkah-langkah yang diperlukan untuk membuat kueri dengan filter.

Anda dapat mengontrol jumlah dan jenis perangkat yang ditampilkan di ringkasan dasbor dan tampilan daftar dengan menggunakan kueri. Anda memfilter kueri dengan menggunakanAWS-managed dan custom fields dariAWS IoTpengindeksan armada. Jika Anda ingin bidang, termasuk bidang bayangan perangkat, muncul di dasbor Anda, administrator harus membuatnya sebagai bidang agregasi di layanan pengindeksan armada. Untuk informasi selengkapnya tentang pengindeksan armada, lihatPengindeksan armada.

Anda juga dapat menambahkan kata kunci ke pertanyaan Anda. Kata kunci berlaku di semua bidang yang dapat dicari. Mereka juga menghitung terhadap batas tiga filter yang dapat Anda terapkan dalam satu kueri.

Bagian berikut menjelaskan langkah-langkah yang diperlukan untuk membuat kueri yang khas.

Membuat kueri

Langkah-langkah berikut menjelaskan cara membuat kueri yang khas.

Prasyarat

- Sebuah aplikasi Fleet Hub terkait denganAWS IoT Coreakun yang berisi beberapa perangkat (hal)
- Akun yang memiliki izin untuk menggunakan aplikasi Fleet Hub

Buat kueri Fleet Hub pertama Anda dengan filter di konsol

1. Arahkan ke aplikasi Fleet Hub Anda.
2. Pada dasbor default, verifikasi bahwa Anda dapat melihatDaftar perangkattab dan jumlah total perangkat (hal) di asosiasiAWS IoT Coreakun.

   Dasbor default berisi tab navigasi, termasuk satu untuk daftar perangkat. Ini menampilkan jumlah total perangkat di terkaitAWS IoT Coreakun dan jumlah total perangkat yang terhubung.

3. Pada dasbor default, pilihDaftar perangkattab. Pastikan bahwa Anda melihat daftar semua perangkat yang berisi atribut terkelola dan kustom. Atribut kustom berisiatributawalan.

   Secara default, dasbor daftar perangkat menampilkan atribut khusus dan terkelola untuk semua perangkat yang terkaitAWS IoT Coreakun.
4. Di bagian atas halaman, masukkan kata kunci yang ingin Anda sertakan dalam kueri Anda. Kueri kata kunci berlaku untuk semua bidang.
5. Di bagian atas halaman, pilihFilter.
6. DiFiltermodal, di bawahBidang, pilih bidang yang ingin Anda gunakan sebagai filter. Di bawahOperator, pilih satu opsi. Akhirnya, untukNilai, pilih nilai field yang akan digunakan dalam filter Anda.

   Anda dapat menambahkan hingga tiga filter. Kueri kata kunci dihitung terhadap nomor ini.
7. Untuk melakukan kueri Anda, pilihMenerapkan filter. Hasilnya menunjukkan semua perangkat yang sesuai dengan kueri Anda.

Bekerja dengan pekerjaan dan template pekerjaan di Fleet Hub untukAWS IoTManajemen Perangkat

Note

Fitur templat dalam pratinjau dan dapat berubah sewaktu-waktu.

Pekerjaan adalah operasi jarak jauh yang dikirim dan dijalankan pada satu atau lebih perangkat yang terhubungAWS IoT. Misalnya, Anda dapat menentukan pekerjaan yang menginstruksikan satu set perangkat untuk mengunduh dan menginstal pembaruan aplikasi atau firmware, reboot, memutar sertifikat, atau melakukan operasi pemecahan masalah jarak jauh. Anda dapat menjalankan pekerjaan yang telah dikonfigurasi sebelumnya dari Fleet Hub untukAWS IoTAplikasi web Manajemen Perangkat. Administrator organisasi Anda membuat template pekerjaan diAWS IoTkonsol dan lampirkan kebijakan yang membuat template tersedia untuk pengguna Fleet Hub. Dalam aplikasi Fleet Hub, Anda menentukan perangkat atau grup perangkat tempat pekerjaan berjalan.

Administrator juga membuat grup perangkat yang dapat Anda lihat di aplikasi Anda. Untuk melihat grup ini, pilihGrup perangkatdi panel navigasi. Bila Anda menentukan grup perangkat sebagai target, Anda dapat menentukan salah satu dari dua jenis opsi berikut untuk cara kerja berjalan.

- snapshot: Pekerjaan berjalan sekali.
- berkelanjutan: Setelah menjalankan awal, pekerjaan berjalan pada perangkat apa pun yang ditambahkan ke grup.

Untuk informasi selengkapnya tentang cara membuat dan mengelola templat tugas, lihatJob. Untuk informasi selengkapnya tentang cara kerja, lihatTugas.

Lowongan kerja Running

Anda dapat menjalankan pekerjaan dari beberapa lokasi dalam aplikasi Fleet Hub, tetapi langkah-langkah berikut selalu sama.

1. Pilih grup atau satu atau beberapa perangkat sebagai target.
2. Pilih Jalankan tugas.
3. Di bawahPemilihan target Job, pilih salah satuberkesinambunganatauRekam Jepret.
4. Pilih template pekerjaan. Verifikasi bahwa teks di bawahRingkasan Jobmenjelaskan jenis tugas yang ingin Anda jalankan.

5. Secara opsional, masukkan nama untuk tugas tersebut.
6. Memilih Jalankan.

Anda dapat memilih target dan mengikuti langkah-langkah berikut dari lokasi berikut di aplikasi Fleet Hub Anda.

- Tab daftar perangkat di dasbor.
- Halaman rincian perangkat tertentu.
- Halaman grup perangkat.
- Halaman rincian grup perangkat tertentu.

Melihat dan Mengelola Tugas

Anda dapat melihat pekerjaan yang berjalan di armada Anda di lokasi berikut.

- Halaman daftar pekerjaan - Halaman ini menampilkan semua pekerjaan yang berjalan di armada Anda. Untuk melihat halaman ini, pilihTugasdi panel navigasi.
- Halaman rincian untuk perangkat tertentu - Halaman ini menampilkan semua pekerjaan yang berjalan pada perangkat.

Setiap pekerjaan memiliki halaman rincian yang menampilkan informasi ringkasan tentang pekerjaan, termasuk target dan informasi runtime. Halaman ini menampilkan status runtime tugas di setiap perangkat. Ini juga menampilkan total berikut.

- Jumlah berjalan.
- Jumlah dibatalkan berjalan.
- Jumlah berjalan sukses.
- Jumlah berjalan yang gagal.
- Jumlah berjalan ditolak.
- Jumlah antrian berjalan.
- Jumlah berlangsung berjalan.
- Jumlah berjalan dihapus.
- Jumlah habis habis berjalan.

Untuk membatalkan pekerjaan, pilih pekerjaan dan pilihMembatalkan.

Alarm

Bagian ini menjelaskan cara Fleet HubAWS IoTAlarm Manajemen Perangkat bekerja dan memandu Anda melalui langkah-langkah yang diperlukan untuk membuat alarm.

Saat Anda membuat alarm Fleet Hub, alarm ini berlaku untuk semua perangkat yang saat ini ditampilkan di dasbor Anda. Jika Anda tidak menerapkan kueri, alarm berlaku untuk semua perangkat di armada Anda. Untuk informasi tentang menggunakan dasbor Anda dan membuat kueri, lihatthe section called “Kueri dan filter” (p. 14).

Alarm menggunakan metrik Amazon CloudWatch (CloudWatch) yang dikombinasikan dengan bidang yang dapat dicari dariAWS IoTLayanan pengindeksan armada untuk membuat alarm CloudWatch. Selain itu,

Anda dapat membuat alarm yang menghasilkan pesan Amazon Simple Notification Service (Amazon SNS) setiap kali tingkat baterai rata-rata perangkat dalam armada Anda turun di bawah 50%.

Armada Hub alarm menggunakanGetStatisticsdanGetPercentileskemampuan layanan pengindeksan armada untuk query data agregat. Misalnya, saat membuat alarm yang melacak bidang numerik khusus, Anda dapat membuat ambang batas yang mengkhawatirkan yang berlaku pada nilai berikut dari atribut yang ditentukan.

- Maksimum
- Count
- Jumlah
- Minimum
- Rata-rata
- Nilai dalam persentil ke-10, 50, 90, 95, atau 99

Untuk informasi selengkapnya tentang kueri data agregat dalam layanan pengindeksan armada, lihatMenanyakan data agregat.

Tabel berikut berisi beberapa contoh tipe agregasi yang tersedia untukAWS-dikelola dan bidang kustom.

Bidang	Tipe agregasi
Tipe hal(AWSbidang string -managed)	Count
Grup hal(AWSbidang string -managed)	Count
Terhubung(AWS-dikelola bidang Boolean) Nilai dari`true`adalah 1. Nilai dari`false`adalah 0.	• Maksimum • Count • Jumlah • Minimum • Rata-rata
shadow.reported.batterylevel(bidang agregasi numerik dibuat dalam layanan pengindeksan armada)	• Maksimum • Count • Jumlah • Minimum • Rata-rata • p10 (persentil ke-10) • p50 (persentil ke-50) • p90 (persentil ke-90) • p95 (persentil ke-95) • p99 (persentil 99)

Selain menentukan bidang agregasi dan jenis, Anda juga menentukan nilai berikut.

- Durasi waktu (1 menit atau 5 menit) diperlukan untuk ambang batas yang mengkhawatirkan yang ditentukan untuk memicu alarm.
- Salah satu operator perbandingan berikut untuk diterapkan ke bidang agregasi tertentu dan jenis.
  - Lebih besar
  - Lebih Besar/Sama
  - Lebih rendah

  - Rendah/Sama
- Nilai yang akan digunakan dengan operator perbandingan yang Anda tentukan.
- Daftar alamat email orang di organisasi Anda yang menerima pesan Amazon SNS setiap kali alarm Anda dipicu.
- Nama alarm.

Untuk membuat alarm Fleet Hub, lihatthe section called “Membuat alarm” (p. 20).

Membuat alarm

Topik ini memandu Anda melalui langkah-langkah yang diperlukan untuk membuat Fleet HubAWS IoTAlarm Manajemen Perangkat. Ini mengasumsikan bahwa administrator Anda telah membuat bidang agregasi dari bidang bayangan perangkat bernamashadow.reported.batterylevel. Bidang kustom ini menunjukkan tingkat baterai perangkat. Anda perlu meminta administrator untuk membuat bidang kustom yang dapat dicari diAWS IoTlayanan pengindeksan armada.

Alarm yang Anda buat mengirimkan pesan Amazon Simple Notification Service (Amazon SNS) ke daftar orang di organisasi Anda setiap kali tingkat baterai rata-rata perangkat dalam armada Anda turun di bawah 50% selama periode 1 menit.

Membuat kueri Fleet Hub

1. Arahkan ke aplikasi Fleet Hub Anda.
2. Jika Anda ingin menargetkan serangkaian perangkat tertentu, buat kueri. Untuk instruksi tentang cara membuat kueri sederhana, lihatthe section called “Membuat kueri dengan filter” (p. 16). Jika Anda tidak membuat kueri, alarm akan berlaku untuk semua perangkat di armada Anda.
3. Pada halaman dasbor default, pilihMembuat alarm.
4. PadaMembangun metrik agregasihalaman, verifikasi bahwa kueri Anda muncul di bawahKueri target. DiMengkonfigurasi agregasi metrik armadabagian, untukPilih bidang, pilihshadow.reported.batterylevel. Menu ini berisiAWSbidang -managed dan bidang kustom yang administrator Anda telah dibuat diAWS IoTlayanan pengindeksan armada.
5. UntukPilih tipe agregasi, pilihRata-rata. Pilihan ini mendasarkan alarm pada nilai tingkat baterai rata-rata di armada perangkat Anda.
6. UntukPilih periode, pilih1 menit. Ini memicu alarm saat armada perangkat Anda tetap dalam keadaan mengkhawatirkan yang ditentukan selama satu menit.

   Pilih Selanjutnya.
7. PadaAmbang batas sethalaman, diMemicu alarm kapanpun...bagian, pilihRendah/Sama. Ini memicu alarm ketika nilai tingkat baterai rata-rata turun di bawah nilai yang Anda tentukan.
8. DiDarikotak teks, masukkan 50.

   Pilih Selanjutnya.
9. PadaBeri tahu penggunahalaman, diBeri tahu - opsionalbagian, masukkan nama untuk daftar email yang berisi pengguna di organisasi Anda yang menerima pemberitahuan saat alarm aktif. Masukkan daftar alamat email yang dipisahkan koma untuk mengisi daftar ini.
10. DiRincian alarmBagian, masukkan nama untuk alarm Anda, dan masukkan deskripsi untuk alarm Anda. Pilih Selanjutnya.
11. PadaTinjauhalaman, verifikasi informasi yang Anda masukkan pada halaman sebelumnya. Pilih Submit (Kirim). Anda kembali ke dasbor default.
12. Pada dasbor default, di panel navigasi kiri, pilihAlarm Armada Hub. Pastikan bahwa Anda melihat alarm yang Anda buat.

Pemecahan Masalah

Bagian ini menyediakan informasi pemecahan masalah dan solusi yang mungkin untuk membantu menyelesaikan masalah sebagai pengguna Fleet Hub.

Gejala	Solusi
Saya tidak dapat menambahkan lebih banyak filter atau istilah ke kueri saya.	Pastikan Anda belum mencapai batas empat istilah dan filter kueri.
Saya tidak dapat menemukan metrik kustom.	Minta administrator Anda untuk membuat metrik di layanan pengindeksan armada.
Alarm saya tidak menunjukkan data apapun.	Data alarm membutuhkan waktu beberapa menit.
Aku perlu mengubah perangkat yang ditargetkan alarm saya.	Buka dasbor Anda dan ubah kueri.
Saya melihat kesalahan ketika saya mengubah Wilayah di dasbor saya.	Minta administrator Anda untuk memastikan bahwa pengindeksan armada diaktifkan di Wilayah yang Anda pilih.

Hub Armada untukAWS IoTManajemen Perangkat

Pemantauan adalah bagian penting dari pemeliharaan keandalan, ketersediaan, dan performa Hub Armada dan lainnyaAWSsolusi.AWSmenyediakan alat pemantauan berikut untuk mengawasi Armada Hub, melaporkan saat terjadi kesalahan, dan mengambil tindakan otomatis jika diperlukan.

- AWS CloudTrail merekam panggilan API dan peristiwa terkait yang dilakukan oleh atau atas nama akun AWS Anda dan mengirimkan berkas log ke bucket Amazon S3 yang Anda tentukan. Anda dapat mengidentifikasi pengguna dan akun mana yang memanggil AWS, alamat IP sumber yang melakukan panggilan, dan kapan panggilan tersebut terjadi. Untuk mengetahui informasi selengkapnya, lihat Panduan Pengguna AWS CloudTrail.

Topik

Hub Armada untukAWS IoTManajemen Perangkat API denganAWS CloudTrail

Hub Armada untukAWS IoTManajemen Perangkat terintegrasi denganAWS CloudTrail. Layanan CloudTrail menyediakan catatan tindakan yang dimiliki pengguna, peran, atauAWSlayanan mengambil di Fleet Hub. CloudTrail merekam semua panggilan API untuk Armada Hub sebagai peristiwa. Panggilan yang direkam mencakup konsol Armada Hub dan panggilan kode ke operasi API Armada.

Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman berkelanjutan peristiwa CloudTrail ke bucket Amazon S3, termasuk peristiwa untuk Armada Hub. Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru dalam konsol CloudTrail di Riwayat peristiwa.

Dengan informasi yang dikumpulkan CloudTrail, Anda dapat menentukan permintaan yang dibuat ke Hub Armada, alamat IP asal permintaan tersebut dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail lainnya.

Untuk mempelajari selengkapnya tentang CloudTrail, lihat Panduan Pengguna AWS CloudTrail.

Informasi Armada Hub di CloudTrail

AWS CloudTrail diaktifkan pada akun AWS Anda saat Anda membuat akun tersebut. Saat aktivitas terjadi di Hub Armada, aktivitas tersebut direkam di peristiwa CloudTrail bersama lainnyaAWSperistiwa layanan diRiwayat peristiwa. Anda dapat melihat, mencari, dan mengunduh peristiwa terbaru di akun AWS Anda. Untuk informasi selengkapnya, lihat Melihat peristiwa dengan riwayat peristiwa CloudTrail.

Untuk catatan berkelanjutan tentang peristiwa diAWSakun, termasuk peristiwa untuk Armada Hub, buat jejak. Jejak memungkinkan CloudTrail untuk mengirim berkas log ke bucket Amazon Simple Storage Service (Amazon S3). Secara default, saat Anda membuat jejak di dalam konsol tersebut, jejak diterapkan ke semua Wilayah AWS. Jejak mencatat kejadian dari semua Wilayah di partisi AWS dan mengirimkan berkas log ke bucket Amazon S3 yang Anda tentukan.

Anda dapat mengonfigurasi layanan AWS lainnya untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan di log CloudTrail. Untuk mengetahui informasi selengkapnya, lihat hal berikut:

- Gambaran umum untuk membuat jejak
- Layanan dan integrasi yang didukung CloudTrail
- Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail
- Menerima berkas log CloudTrail dari beberapa Wilayah
- Menerima berkas log CloudTrail dari beberapa akun

CloudTrail mencatat semua tindakan Armada Hub. Tindakan tersebut didokumentasikan dalam Referensi API AWS IoT. Misalnya, panggilan ke tindakan `CreateApplication` dan `UpdateApplication` menghasilkan entri di berkas log CloudTrail.

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 kredensial keamanan sementara untuk peran atau pengguna gabungan
- Jika permintaan tersebut dibuat oleh layanan AWS lainnya

Untuk informasi selengkapnya, lihat elemen userIdentity CloudTrail.

Hub Armada untukAWS IoTEntri berkas log Manajemen Perangkat

Jejak adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai berkas log ke bucket Amazon S3 yang telah Anda tentukan.

File log CloudTrail berisi satu atau beberapa entri log. Peristuwa mewakili satu permintaan dari sumber apa pun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya.

Berkas log CloudTrail bukan jejak tumpukan terurut dari panggilan API publik, sehingga berkas tersebut tidak muncul dalam urutan tertentu.

Example

Entri log CloudTrail berikut menampilkan informasi tentang tindakan `CreateApplication`.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "principal-id",
        "arn": "arn:aws:sts::123456789012:assumed-role/Admin/test-user-name",
        "accountId": "123456789012",
        "accessKeyId": "access-key",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "principal-id",
                "arn": "arn:aws:iam::123456789012:role/Admin",
```

```
                    "accountId": "123456789012",
                    "userName": "Admin"
                },
                "webIdFederationData": {},
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2020-12-04T19:59:53Z"
                }
            }
        },
        "eventTime": "2020-12-04T20:02:38Z",
        "eventSource": "iotfleethub.amazonaws.com",
        "eventName": "CreateApplication",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "72.22.186.61",
        "userAgent": "console.amazonaws.com",
        "requestParameters": {
            "applicationDescription": "Test application description",
            "applicationName": "Test application name",
            "clientToken": "c9bc7f45-3737-4ee9-9b0f-5de1aab169b2"
        },
        "responseElements": {
            "applicationUrl": "https://application-id.app.iotfleethub.aws",
            "applicationArn": "arn:aws:iotfleethub:us-
east-1:123456789012:application/application-id",
            "applicationId": "application-id"
        },
        "requestID": "5456304e-31c5-4336-9bbe-a375e3728eee",
        "eventID": "9ffb5d72-9267-4f4e-88e6-d26051133c8c",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "recipientAccountId": "123456789012"
    }
```

Security untuk Armada untukAWS IoTManajemen Perangkat

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

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

- Keamanan cloud – AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan layanan-layanan AWS di dalam AWS Cloud. AWS juga memberikan Anda layanan yang dapat digunakan dengan aman. Auditor pihak ketiga melakukan pengujian dan verifikasi secara berkala terhadap efektivitas keamanan kami sebagai bagian dari Program Kepatuhan AWS. Untuk mempelajari program kepatuhan yang berlaku di Fleet Hub, lihatAWSLayanan dalam Lingkup oleh Program Kepatuhan.
- Keamanan dalam cloud – Tanggung jawab Anda ditentukan oleh 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 akan membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan Fleet Hub untukAWS IoTManajemen Perangkat. Topik berikut menunjukkan kepada Anda cara mengonfigurasi Fleet Hub untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga akan belajar bagaimana menggunakanAWSlayanan yang membantu Anda memantau dan mengamankan sumber daya Armada Anda.

Topik

Perlindungan data di Armada untuk

ParameterAWS Model tanggung jawab bersamaberlaku untuk perlindungan data di Fleet Hub untukAWS IoTManajemen Perangkat. 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. Konten ini meliputi konfigurasi keamanan dan tugas-tugas pengelolaan untuk berbagai layanan Layanan AWS yang Anda gunakan. Untuk informasi lebih lanjut tentang privasi data, lihat FAQ tentang Privasi Data. Untuk informasi tentang perlindungan data di Eropa, 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 akun pengguna individu dengan AWS Identity and Access Management (IAM). 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 ini:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk melakukan komunikasi dengan sumber daya AWS. Kami merekomendasikan TLS 1.2 atau versi yang lebih baru.
- 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 pribadi yang disimpan di Amazon Simple Storage Service (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 lebih lanjut tentang titik akhir FIPS yang tersedia, lihat Standar Pemrosesan Informasi Federal (FIPS) 140-2.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan Fleet Hub atau lainnyaAWSlayanan menggunakan konsol, API,AWS CLI, atauAWSSDK. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menyarankan jangan menyertakan informasi kredensial di URL untuk memvalidasi permintaan Anda ke server tersebut.

Enkripsi saat Istirahat

Armada melindungi data at rest melalui enkripsi sisi server. Untuk informasi lebih lanjut, lihat Enkripsi data di AWS IoT di Panduan Developer AWS IoT.

Enkripsi dalam transit

Dalam deployment cloud alur, Fleet Hub melindungi data dalam transit dengan menggunakan protokol Keamanan Lapisan Pengangkutan (TLS). Untuk informasi selengkapnya, lihat Keamanan transportasi di AWS IoT di Panduan Developer AWS IoT.

Identity and Access Management untuk Fleet Hub for AWS IoT Device Management

AWS Identity and Access Management(IAM) adalahLayanan AWSyang membantu administrator dalam mengendalikan akses keAWSsumber daya. Administrator IAM mengontrol siapa yang bisamengonfirmasi(masuk) danresmi(memiliki izin) untuk menggunakan sumber daya Fleet Hub. IAM adalahLayanan AWSyang dapat Anda gunakan tanpa biaya tambahan.

Topik

Penonton

Bagaimana Anda menggunakanAWS Identity and Access Management(IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan di Fleet Hub.

Pengguna layanan— Jika Anda menggunakan layanan Fleet Hub untuk melakukan tugas Anda, administrator Anda akan memberikan kredensyal dan izin yang dibutuhkan. Saat Anda menggunakan lebih banyak fitur Fleet Hub untuk melakukan pekerjaan, Anda mungkin memerlukan izin tambahan. Memahami cara akses dikelola dapat membantu Anda untuk meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di Fleet Hub, lihatPemecahan masalah identitas dan akses Fleet Hub for AWS IoT Device Management (p. 38).

Administrator layanan— Jika Anda bertanggung jawab atas sumber daya Fleet Hub di perusahaan Anda, Anda mungkin memiliki akses penuh ke Fleet Hub. Tugas Anda adalah menentukan fitur dan sumber daya Fleet Hub mana yang dapat diakses karyawan Anda. Anda kemudian harus mengirimkan permintaan ke administrator IAM Anda untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep dasar IAM. Untuk mempelajari selengkapnya tentang cara perusahaan Anda dapat menggunakan IAM dengan Fleet Hub, lihatCara kerja Fleet Hub for AWS IoT Device Management dengan IAM (p. 31).

Administrator IAM— Jika Anda adalah administrator IAM, Anda perlu mempelajari dengan mendetail cara menulis kebijakan untuk mengelola akses ke Fleet Hub. Untuk melihat contoh kebijakan berbasis identitas Fleet yang dapat Anda gunakan di IAM, lihatContoh kebijakan berbasis identitas untuk Fleet Hub for AWS IoT Device Management (p. 36).

Mengautentikasi dengan identitas

Autentikasi adalah cara Anda untuk masuk ke AWS menggunakan kredensial identitas Anda. Untuk informasi selengkapnya tentang cara masuk menggunakan AWS Management Console, lihat Masuk ke AWS Management Console sebagai pengguna IAM atau pengguna root dalam Panduan Pengguna IAM.

Anda harus terautentikasi (masuk ke AWS) sebagai pengguna root Akun AWS, pengguna IAM, atau dengan menggunakan IAM role. Anda juga dapat menggunakan autentikasi single sign-on milik perusahaan Anda, atau bahkan masuk menggunakan Google atau Facebook. Dalam kasus ini, administrator Anda sebelumnya telah menyiapkan federasi identitas menggunakan IAM role. Saat Anda mengakses AWS menggunakan kredensial dari perusahaan lain, secara tidak langsung Anda mengambil sebuah peran.

Untuk masuk secara langsung ke AWS Management Console, gunakan kata sandi Anda dengan alamat email pengguna asal atau nama pengguna IAM Anda. Anda dapat mengakses AWS secara terprogram menggunakan kunci akses pengguna asal atau pengguna IAM Anda. AWS menyediakan SDK dan alat baris perintah untuk menandatangani permintaan Anda secara kriptografis menggunakan kredensial Anda. Jika Anda tidak menggunakan peralatan AWS, Anda harus menandatangani sendiri permintaan tersebut. Lakukan ini menggunakan Versi Tanda Tangan 4, sebuah protokol untuk mengautentikasi permintaan API masuk. Untuk informasi selengkapnya tentang autentikasi permintaan, lihat proses penandatanganan Versi Tanda Tangan 4 dalam Referensi Umum AWS.

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

Pengguna root Akun AWS

Ketika Anda pertama kali membuatAkun AWSAnda mulai dengan identitas masuk tunggal yang memiliki akses penuh ke semuaLayanan AWSdan sumber daya di akun. Identitas ini disebut pengguna root Akun AWS dan diakses dengan cara masuk menggunakan alamat email dan kata sandi yang Anda gunakan saat membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas

sehari-hari, bahkan tugas administratif. Sebagai gantinya, patuhi praktik terbaik dalam menggunakan pengguna root saja untuk membuat pengguna IAM pertama Anda. Kemudian, kunci kredensial pengguna root dengan aman dan gunakan kredensial itu untuk melakukan beberapa tugas manajemen akun dan layanan saja.

Pengguna dan grup IAM

Pengguna IAM adalah identitas dalam akun Akun AWS Anda yang memiliki izin khusus untuk satu orang atau aplikasi. Pengguna IAM dapat memiliki kredensial jangka panjang, seperti nama pengguna dan kata sandi atau satu set access key. Untuk mempelajari cara membuat kunci akses, lihat Mengelola access key untuk pengguna IAM dalam Panduan Pengguna IAM. Saat Anda membuat access key untuk pengguna IAM, pastikan bahwa Anda melihat pasangan kunci dan menyimpannya dengan aman. Anda tidak dapat memulihkan secret access key di masa mendatang. Sebaliknya, Anda harus membuat pasangan access key baru.

Grup IAM adalah identitas yang menentukan kumpulan dari para pengguna IAM. Anda tidak dapat masuk sebagai kelompok. Anda dapat menggunakan grup untuk menentukan izin untuk beberapa pengguna sekaligus. Grup membuat izin lebih mudah dikelola untuk set besar pengguna. Misalnya, Anda dapat memiliki grup yang diberi nama IAMAdmins dan memberikan izin kepada grup tersebut untuk mengelola sumber daya IAM.

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

IAM role

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

IAM role dengan kredensial sementara berguna dalam situasi berikut:

- Izin pengguna IAM sementara – Pengguna IAM dapat menggunakan IAM role untuk sementara dan mendapatkan izin yang berbeda untuk tugas tertentu.
- Akses pengguna gabungan – Alih-alih membuat pengguna IAM, Anda dapat menggunakan identitas yang sudah ada dari AWS Directory Service, direktori pengguna korporasi Anda, atau penyedia identitas web. Ini dikenal sebagai pengguna gabungan. AWS menugaskan peran kepada pengguna gabungan saat akses diminta melalui penyedia identitas. Untuk informasi selengkapnya tentang pengguna gabungan, lihat Pengguna dan peran gabungan dalam Panduan Pengguna IAM.
- Akses lintas akun – Anda dapat menggunakan IAM role agar seseorang (principal tepercaya) di akun lain diizinkan untuk mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapaLayanan AWSAnda dapat melampirkan kebijakan langsung ke sumber daya (alih-alih menggunakan peran sebagai proksi). Untuk mempelajari perbedaan antara kebijakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Perbedaan antara IAM role dan kebijakan berbasis sumber daya dalam Panduan Pengguna IAM.
- Akses lintas layanan- BeberapaLayanan AWSmenggunakan fitur diLayanan AWS. Sebagai conoth, ketika Anda melakukan panggilan dalam suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Layanan mungkin melakukan ini menggunakan izin panggilan principal, menggunakan peran layanan, atau peran tertaut layanan.
  - Izin prinsipal – Saat Anda menggunakan pengguna IAM atau IAM role untuk melakukan tindakan di AWS, Anda dianggap sebagai principal. Kebijakan memberikan izin kepada principal. Saat Anda

menggunakan beberapa layanan, Anda mungkin melakukan tindakan yang kemudian memicu tindakan lain di layanan yang berbeda. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk mengetahui apakah suatu tindakan memerlukan tindakan dependen tambahan dalam suatu kebijakan, lihat Tindakan, sumber daya, dan kunci syarat untuk Fleet Hub for AWS IoT Device Management di Referensi Otorisasi Layanan.

- Peran layanan – Peran layanan adalah IAM role yang diambil oleh layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, memodifikasi, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihatMembuat peran untuk mendelegasikan izin keLayanan AWSdi dalamPanduan Pengguna IAM.
- Peran yang terhubung dengan layananPeran yang terhubung dengan layanan adalah jenis peran layanan yang tertaut denganLayanan AWS. Layanan dapat menggunakan peran untuk melakukan tindakan atas nama Anda. Peran tertaut layanan muncul di akun IAM Anda dan dimiliki oleh layanan tersebut. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

- Aplikasi yang berjalan di Amazon EC2 – Anda dapat menggunakan IAM role untuk mengelola kredensial sementara untuk aplikasi yang berjalan pada instans EC2, dan membuat permintaan API AWS CLI atau AWS. Menyimpan access key di dalam instans EC2 lebih disarankan. 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, lihat Menggunakan IAM role untuk memberikan izin ke aplikasi yang berjalan di instans Amazon EC2 dalam Panduan Pengguna IAM.

Untuk mempelajari kapan waktunya menggunakan IAM role atau pengguna IAM, lihat Kapan harus membuat IAM role (bukan pengguna) dalam Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengendalikan akses di AWS dengan membuat kebijakan dan melampirkannya ke identitas IAM atau sumber daya AWS. Kebijakan adalah objek di AWS, yang saat terkait dengan identitas atau sumber daya, akan menentukan izinnya. Anda dapat masuk sebagai pengguna root atau pengguna IAM, atau Anda dapat menggunakan IAM role. Ketika Anda kemudian membuat permintaan, AWS mengevaluasi kebijakan berbasis identitas atau kebijakan berbasis sumber daya yang terkait. Izin dalam kebijakan dapat menentukan permintaan yang diizinkan atau ditolak. Sebagian besar kebijakan disimpan di AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang struktur dan isi dokumen kebijakan JSON, lihat Gambaran Umum kebijakan JSON dalam Panduan Pengguna IAM.

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

Setiap entitas IAM (pengguna atau peran) dimulai tanpa izin. Dengan kata lain, secara default, pengguna tidak dapat melakukan apa pun, termasuk mengubah kata sandi mereka sendiri. Untuk memberikan izin kepada pengguna untuk melakukan sesuatu, administrator harus melampirkan kebijakan izin kepada pengguna. Atau administrator dapat menambahkan pengguna ke grup yang memiliki izin yang dimaksudkan. Ketika administrator memberikan izin untuk grup, semua pengguna dalam grup tersebut diberikan izin tersebut.

Kebijakan IAM mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk pengoperasiannya. Misalnya, Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan tersebut dapat memperoleh informasi peran dari API AWS Management Console, the AWS CLI, or the AWS.

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke identitas, seperti pengguna IAM, grup pengguna, atau peran. Kebijakan ini mengontrol tipe tindakan yang dapat

dilakukan oleh pengguna dan peran, di sumber daya mana, dan dalam syarat. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

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

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan tepercaya IAM role 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 tersebut, kebijakan menetapkan tindakan apa yang dapat dilakukan oleh principal tertentu di sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan principal dalam kebijakan berbasis sumber daya. Principal dapat mencakup akun, pengguna, peran, pengguna, peran, pengguna, atauLayanan AWS.

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

Daftar kontrol akses (ACL)

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

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung ACL. Untuk mempelajari ACL selengkapnya, lihat Gambaran umum daftar kontrol akses (ACL) dalam Panduan Developer Amazon Simple Storage Service.

Tipe kebijakan lainnya

AWS mendukung tipe kebijakan tambahan, yang kurang umum. 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 atau IAM role). Anda dapat menetapkan batas izin untuk suatu entitas. Izin yang dihasilkan adalah persimpangan 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 dapat membatalkan izin. Untuk informasi selengkapnya tentang batasan izin, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.
- Kebijakan Kontrol Layanan (SCPs) – 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 mengelola beberapa akun Akun AWS secara terpusat yang dimiliki oleh bisnis Anda. Jika Anda mengaktifkan semua fitur di sebuah 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 Organizations dan SCP, lihat Cara kerja SCP dalam Panduan Pengguna AWS Organizations.
- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter saat Anda membuat sesi sementara secara terprogram bagi peran atau pengguna gabungan. Izin sesi yang dihasilkan adalah persimpangan 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 membatalkan izin. Untuk informasi selengkapnya, lihat Kebijakan sesi dalam Panduan Pengguna IAM.

Berbagai tipe kebijakan

Ketika beberapa tipe kebijakan berlaku untuk sebuah permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan untuk mengizinkan permintaan ketika beberapa tipe kebijakan dilibatkan, lihat Logika evaluasi kebijakan dalam Panduan Pengguna IAM.

Cara kerja Fleet Hub for AWS IoT Device Management dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke Fleet Hub, Anda harus memahami berbagai fitur IAM yang mendukung Fleet Hub.

Fitur IAM yang dapat Anda gunakan dengan Fleet Hub for AWS IoT Device Management

Fitur IAM	Armada untuk
Kebijakan berbasis identitas (p. 31)	Ya
Kebijakan berbasis sumber daya (p. 32)	Tidak
Tindakan kebijakan (p. 32)	Ya
Sumber daya kebijakan (p. 33)	Ya
Kunci syarat kebijakan (p. 34)	Ya
ACLs (p. 34)	Tidak
ABAC (tanda dalam kebijakan) (p. 34)	Ya
Kredensial sementara (p. 35)	Ya
Izin pelaku utama (p. 35)	Ya
Peran layanan (p. 35)	Ya
Peran terkait layanan (p. 36)	Tidak

Untuk mendapatkan tampilan tingkat tinggi tentang bagaimana Armada dan lainnyaAWSlayanan bekerja dengan sebagian besar fitur IAM, lihatAWSlayanan yang bekerja dengan IAMdi dalamPanduan Pengguna IAM.

Kebijakan berbasis identitas untuk Armada

Hanya mendukung kebijakan berbasis identitas	Ya

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke identitas, seperti pengguna IAM, grup pengguna, atau peran. Kebijakan ini mengontrol tipe tindakan yang dapat

dilakukan oleh pengguna dan peran, di sumber daya mana, dan dalam syarat. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Membuat kebijakan IAM dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan tindakan dan sumber daya yang diizinkan atau ditolak, serta kondisi di mana tindakan tersebut diperbolehkan atau ditolak. Anda tidak dapat menentukan pelaku utama dalam kebijakan berbasis identitas karena itu berlaku untuk pengguna atau peran yang dilampiri kebijakan. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan IAM JSON dalam Panduan Pengguna IAM.

Contoh kebijakan berbasis identitas untuk Armada

Untuk melihat contoh kebijakan berbasis identitas Fleet Hub, lihatContoh kebijakan berbasis identitas untuk Fleet Hub for AWS IoT Device Management (p. 36).

Kebijakan berbasis sumber daya dalam Fleet Hub

Mendukung kebijakan berbasis sumber daya	Tidak

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contoh kebijakan berbasis sumber daya adalah kebijakan tepercaya IAM role 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 tersebut, kebijakan menetapkan tindakan apa yang dapat dilakukan oleh principal tertentu di sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan principal dalam kebijakan berbasis sumber daya. Principal dapat mencakup akun, pengguna, peran, pengguna, peran, pengguna, atauLayanan AWS.

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan seluruh akun atau entitas IAM di akun lain sebagai prinsipal di kebijakan berbasis sumber daya. Menambahkan prinsipal lintas akun ke kebijakan berbasis sumber daya hanya setengah dari membangun hubungan kepercayaan. Ketika pelaku utama dan sumber daya berada di Akun AWS yang berbeda, Administrator IAM di akun tepercaya juga harus memberikan izin kepada entitas pelaku utama (pengguna atau peran) untuk mengakses sumber daya. Izin diberikan dengan melampirkan kebijakan berbasis identitas ke entitas. Namun, jika kebijakan berbasis sumber daya memberikan akses ke prinsipal dalam akun yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi lebih lanjut, lihat Perbedaan IAM role dengan kebijakan berbasis sumber daya dalam Panduan Pengguna IAM.

Tindakan kebijakan untuk Armada untuk

> **Note**
>
> Aplikasi Fleet Hub menggunakan`AWSIoTFleetHubFederationAccess`kebijakan terkelola. Untuk informasi selengkapnya, lihat ??? (p. 41).

Mendukung tindakan kebijakan	Ya

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

Elemen `Action` dari kebijakan JSON menjelaskan tindakan-tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Tindakan kebijakan biasanya memiliki nama

yang sama sebagai operasi API AWS terkait. Ada beberapa pengecualian, misalnya tindakan hanya dengan izin yang tidak memiliki operasi API yang cocok. Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam kebijakan. Tindakan tambahan ini disebut tindakan dependen.

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

Untuk melihat daftar tindakan Fleet Hub, lihatTindakan yang ditentukan olehFleet Hub for AWS IoT Device Managementdi dalamReferensi Otorisasi Layanan.

Tindakan kebijakan di Fleet Hub menggunakan prefiks berikut sebelum tindakan:

```
iotfleethub
```

Untuk menetapkan beberapa tindakan dalam satu pernyataan, pisahkan dengan koma.

```
"Action": [
      "iotfleethub:action1",
      "iotfleethub:action2"
         ]
```

Untuk melihat contoh kebijakan berbasis identitas Fleet Hub, lihatContoh kebijakan berbasis identitas untuk Fleet Hub for AWS IoT Device Management (p. 36).

Sumber daya kebijakan untuk Fleet Hub

Mendukung sumber daya kebijakan	Ya

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

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

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

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

Untuk melihat daftar jenis sumber daya Fleet dan ARN-nya, lihatSumber daya ditentukan olehFleet Hub for AWS IoT Device Managementdi dalamReferensi Otorisasi Layanan. Untuk mempelajari tindakan yang dapat menentukan ARN setiap sumber daya, lihat Tindakan yang ditentukan Fleet Hub for AWS IoT Device Management.

Untuk melihat contoh kebijakan berbasis identitas Fleet Hub, lihatContoh kebijakan berbasis identitas untuk Fleet Hub for AWS IoT Device Management (p. 36).

Kunci syarat kebijakan untuk Armada untuk Armada untuk

Mendukung kunci kondisi kebijakan khusus layanan	Ya

Administrator dapat menggunakan kebijakan JSON AWS untuk menentukan siapa yang memiliki akses ke hal apa. Yaitu, prinsipal mana yang dapat melakukan tindakan pada sumber daya apa, dan menurut persyaratan apa.

Elemen `Condition` (atau `Condition` blok) memungkinkan Anda menentukan syarat di mana suatu pernyataan berlaku. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi bersyarat yang menggunakan operator syarat, seperti sama dengan atau kurang dari, untuk mencocokkan syarat dalam kebijakan dengan nilai dalam permintaan.

Jika Anda menentukan beberapa elemen `Condition` dalam pernyataan, atau beberapa kunci dalam satu elemen `Condition`, AWS akan mengevaluasinya denga menggunakan operasi logika `AND`. Jika Anda menetapkan beberapa nilai untuk kunci syarat tunggal, AWS akan mengevaluasi syarat tersebut dengan menggunakan operasi logika `OR`. Semua persyaratan harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan syarat. Sebagai contoh, Anda dapat memberikan izin pengguna IAM untuk mengakses sumber daya hanya jika ditandai dengan nama pengguna IAM mereka. Untuk informasi lebih lanjut, lihat Elemen kebijakan IAM: variabel dan tag dalam Panduan Pengguna IAM.

AWS mendukung kunci syarat global dan kunci syarat khusus layanan. Untuk melihat semua kunci syarat global AWS, lihat Kunci konteks syarat global AWS dalam Panduan Pengguna IAM.

Untuk melihat daftar kunci kondisi Armada, lihatKunci syarat untukFleet Hub for AWS IoT Device Managementdi dalamReferensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan dengan kunci syarat tertentu, lihat Tindakan yang ditentukan Fleet Hub for AWS IoT Device Management.

Untuk melihat contoh kebijakan berbasis identitas Fleet Hub, lihatContoh kebijakan berbasis identitas untuk Fleet Hub for AWS IoT Device Management (p. 36).

Daftar kontrol akses (ACL) di Fleet Hub

Mendukung ACL	Tidak

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

Kontrol akses berbasis atribut (ABAC) dengan Armada

Mendukung ABAC (tanda dalam kebijakan)	Ya

Kontrol akses berbasis atribut (ABAC) adalah strategi otorisasi yang mendefinisikan izin berdasarkan atribut. Di AWS, atribut ini disebut tanda. Anda dapat melampirkan tanda ke entitas IAM (pengguna atau peran) dan ke banyak sumber daya AWS. Penandaan entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian Anda merancang kebijakan ABAC untuk mengizinkan operasi ketika tanda pelaku utama cocok dengan tanda di sumber daya yang ingin diakses.

ABAC sangat membantu di lingkungan yang berkembang dengan cepat dan membantu dalam situasi ketika manajemen kebijakan menjadi rumit.

Untuk mengontrol akses berdasarkan tandanya, Anda memberikan informasi tanda di elemen syarat kebijakan dengan menggunakan kunci syarat `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, atau `aws:TagKeys`.

Untuk informasi lebih lanjut tentang ABAC, lihat Apa itu ABAC? dalam Panduan Pengguna IAM. Untuk melihat tutorial dengan langkah-langkah untuk menyiapkan ABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) dalam Panduan Pengguna IAM.

Menggunakan kredensyal Sementara dengan Fleet Hub

Mendukung penggunaan kredensial sementara	Ya

BeberapaLayanan AWStidak berfungsi saat Anda masuk menggunakan kredensyal sementara. Untuk informasi tambahan, termasukLayanan AWSbekerja dengan mandat sementara, lihatLayanan AWSyang bekerja dengan IAMdi dalamPanduan Pengguna IAM.

Anda menggunakan kredensial sementara jika Anda masuk ke AWS Management Console menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, saat Anda mengakses AWS dengan menggunakan tautan masuk tunggal (SSO) perusahaan Anda, proses tersebut akan membuat kredensial sementara secara otomatis. Anda juga secara otomatis membuat kredensial sementara ketika Anda masuk ke konsol sebagai pengguna dan kemudian beralih peran. Untuk informasi selengkapnya tentang beralih peran, lihat Beralih ke peran (konsol) dalam Panduan Pengguna IAM.

Anda dapat secara manual membuat kredensial sementara menggunakan AWS CLI atau API AWS. Anda kemudian dapat menggunakan kredensial sementara tersebut untuk mengakses AWS. AWS menyarankan agar Anda membuat kredensial sementara secara dinamis alih-alih menggunakan access key jangka panjang. Untuk informasi lebih lanjut, lihat Kredensial keamanan sementara di IAM.

Izin prinsipal lintas layanan untuk Armada

Mendukung izin pelaku utama	Ya

Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan di AWS, Anda dianggap sebagai pelaku utama. Kebijakan memberikan izin kepada prinsipal. Saat Anda menggunakan beberapa layanan, Anda mungkin melakukan tindakan yang kemudian memicu tindakan lain di layanan yang berbeda. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk mengetahui apakah suatu tindakan memerlukan tindakan dependen tambahan dalam suatu kebijakan, lihat Tindakan, sumber daya, dan kunci syarat untuk Fleet Hub for AWS IoT Device Management di Referensi Otorisasi Layanan.

Peran layanan untuk Fleet Hub

Mendukung peran layanan	Ya

Peran layanan adalah IAM role yang diambil oleh layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, memodifikasi, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihatMembuat peran untuk mendelegasikan izin keLayanan AWSdi dalamPanduan Pengguna IAM.

Warning

Mengubah izin untuk peran layanan dapat merusak fungsionalitas Fleet. Edit peran layanan hanya jika Fleet Hub memberikan panduan untuk melakukannya.

Peran terkait layanan untuk Armada untuk Armada untuk

Mendukung peran yang tertaut dengan layanan	Tidak

Peran yang terhubung dengan layanan adalah jenis peran layanan yang tertaut denganLayanan AWS. Layanan dapat menggunakan peran untuk melakukan tindakan atas nama Anda. Peran tertaut 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 pembuatan atau pengelolaan peran yang terhubung dengan layanan, lihat Layanan AWS yang bekerja dengan IAM. Cari layanan dalam tabel yang memiliki `Yes` di kolom Service-linked role (Peran yang terhubung dengan layanan). Pilih tautan Ya untuk melihat dokumentasi peran yang terhubung dengan layanan untuk layanan tersebut.

Contoh kebijakan berbasis identitas untuk Fleet Hub for AWS IoT Device Management

Secara default, pengguna IAM dan IAM role tidak memiliki izin untuk membuat atau memodifikasi sumber daya Fleet Hub. Mereka juga tidak dapat melakukan tugas menggunakan AWS Management Console, AWS CLI, atau API AWS. Administrator IAM harus membuat kebijakan IAM yang memberikan izin kepada para pengguna dan peran untuk melakukan tindakan di sumber daya yang mereka perlukan. Administrator kemudian harus melampirkan kebijakan tersebut ke pengguna IAM atau grup yang memerlukan izin tersebut.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM dengan menggunakan contoh dokumen kebijakan JSON ini, lihatMembuat kebijakan IAMdi dalamPanduan Pengguna IAM.

Topik

Praktik terbaik kebijakan

Kebijakan berbasis identitas adalah pilihan yang sangat tepat. Kebijakan ini menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya Fleet Hub di akun Anda. Tindakan ini membuat Akun AWS Anda terkena biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Memulai menggunakanAWSkebijakan yang dikelola- Untuk mulai menggunakan Fleet Hub dengan cepat, gunakanAWSkebijakan yang dikelola untuk memberi karyawan Anda izin yang mereka perlukan. Kebijakan ini sudah tersedia di akun Anda dan dikelola, serta diperbarui oleh AWS. Untuk informasi selengkapnya, lihat Memulai menggunakan izin dengan kebijakan yang dikelola AWS dalam Panduan Pengguna IAM.
- Pemberian hak istimewa terendah – Ketika Anda membuat kebijakan kustom, berikan izin yang diperlukan saja untuk melakukan tugas. Mulai dengan satu set izin minimum dan berikan izin tambahan sesuai kebutuhan. Melakukan hal tersebut lebih aman daripada memulai dengan izin yang terlalu

fleksibel, lalu mencoba memperketatnya nanti. Untuk informasi selengkapnya, lihat Pemberian hak istimewa terendah dalam Panduan Pengguna IAM.

- Aktifkan autentikasi multifaktor (MFA) untuk operasi sensitif – Untuk keamanan ekstra, mintalah pengguna IAM untuk menggunakan autentikasi multifaktor (MFA) guna mengakses sumber daya atau operasi API yang sensitif. Untuk informasi selengkapnya, lihat Menggunakan autentikasi multifaktor (MFA) dalam AWS dalam Panduan Pengguna IAM.
- Gunakan syarat kebijakan untuk keamanan tambahan – Selama bisa dilakukan, tentukan persyaratan agar kebijakan berbasis identitas Anda mengizinkan akses ke sumber daya. Misalnya, Anda dapat menulis persyaratan untuk menentukan jangkauan alamat IP yang diizinkan untuk mengajukan permintaan. Anda juga dapat menulis ketentuan untuk mengizinkan permintaan hanya dalam rentang tanggal atau waktu tertentu, atau untuk mengharuskan penggunaan SSL atau MFA. Untuk informasi lebih lanjut, lihat Elemen kebijakan IAM JSON: Ketentuan dalam Panduan Pengguna IAM.

Menggunakan konsol Fleet Hub

Untuk mengakses konsol Fleet Hub for AWS IoT Device Management tersebut, Anda harus memiliki rangkaian izin minimum. Izin ini harus memperbolehkan Anda untuk membuat daftar dan melihat detail tentang sumber daya Fleet Hub di AndaAkun AWS. Jika Anda membuat kebijakan berbasis identitas yang lebih ketat dari izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana dimaksudkan untuk entitas (pengguna atau peran IAM) dengan kebijakan tersebut.

Anda tidak perlu mengizinkan konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau API AWS. Alih-alih, izinkan akses hanya ke tindakan yang sesuai dengan operasi API yang Anda coba lakukan.

Untuk memastikan bahwa pengguna dan peran masih dapat menggunakan konsol Fleet Hub, lampirkan juga Fleet Hub`ConsoleAccess`atau`ReadOnly` AWSkebijakan terkelola untuk entitas. Untuk informasi selengkapnya, lihat Menambahkan izin ke pengguna dalam Panduan Pengguna IAM.

Perbolehkan 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 ini pada konsol atau secara terprogram menggunakan AWS CLI atau API 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": "*"
        }
    ]
}
```

Pemecahan masalah identitas dan akses Fleet Hub for AWS IoT Device Management

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin dialami saat bekerja dengan Fleet Hub dan IAM.

Topik

- Saya tidak diotorisasi untuk melakukan tindakan di Armada (p. 38)
- Saya tidak memiliki izin untuk melakukan:PassRole (p. 38)
- Saya ingin melihat access key saya (p. 39)
- Saya seorang administrator dan ingin mengizinkan orang lain mengakses Armada (p. 39)
- Saya ingin mengizinkan orang di luar sayaAWSakun untuk mengakses sumber daya Fleet Hub saya (p. 39)

Saya tidak diotorisasi untuk melakukan tindakan di Armada

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

> Note
>
> Aplikasi Fleet Hub menggunakan`AWSIoTFleetHubFederationAccess`kebijakan terkelola. Untuk informasi selengkapnya, lihat ??? (p. 41).

Contoh kesalahan berikut terjadi ketika pengguna IAM `mateojackson` mencoba menggunakan konsol untuk melihat detail tentang suatu sumber daya fiktif *`my-example-widget`*, tetapi tidak memiliki izin fiktif `iotfleethub:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 iotfleethub:GetWidget on resource: my-example-widget
```

Dalam hal ini, Mateo meminta administratornya untuk memperbarui kebijakannya agar dia dapat mengakses *`my-example-widget`* menggunakan `iotfleethub:`*`GetWidget`* tindakan.

Saya tidak memiliki izin untuk melakukan:PassRole

Jika Anda menerima kesalahan bahwa Anda tidak terotorisasi untuk melakukan tindakan `iam:PassRole`, Anda harus menghubungi administrator untuk mendapatkan bantuan. Administrator Anda adalah orang yang memberikan Anda nama pengguna dan kata sandi Anda. Minta orang tersebut untuk memperbarui kebijakan Anda agar Anda dapat memberikan peran ke Fleet Hub.

BeberapaLayanan AWSmengizinkan Anda untuk meneruskan peran yang sudah ada ke layanan tersebut, alih-alih membuat peran layanan atau peran tertaut layanan baru. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh galat berikut terjadi ketika pengguna IAM bernama`marymajor`mencoba menggunakan konsol untuk melakukan tindakan di Fleet Hub. Namun, tindakan tersebut mengharuskan layanan untuk memiliki izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut ke layanan.

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

Dalam kasus ini, Mary meminta administrator untuk memperbarui kebijakannya agar mengizinkannya untuk melakukan tindakan `iam:PassRole`.

Saya ingin melihat access key saya

Setelah membuat access key pengguna IAM, Anda dapat melihat access key ID Anda setiap saat. Namun, Anda tidak dapat melihat secret access key Anda lagi. Jika Anda kehilangan secret key, Anda harus membuat pasangan access key baru.

Access key terdiri dari dua bagian: access key ID (misalnya, `AKIAIOSFODNN7EXAMPLE`) dan secret access key (misalnya, `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`). Seperti nama pengguna dan kata sandi, Anda harus menggunakan access key ID dan secret access key sekaligus untuk mengautentikasi permintaan Anda. Kelola access key Anda seaman nama pengguna dan kata sandi Anda.

> Important
>
> Jangan memberikan access key Anda kepada pihak ke tiga, bahkan untuk membantu menemukan ID pengguna kanonis Anda. Anda mungkin memberi seseorang akses permanen ke akun Anda, dengan melakukan ini.

Saat Anda membuat pasangan access key, Anda diminta menyimpan access key ID dan secret access key di lokasi yang aman. secret access key hanya tersedia saat Anda membuatnya. Jika Anda kehilangan secret access key Anda, Anda harus menambahkan access key baru ke pengguna IAM Anda. Anda dapat memiliki maksimum dua access key. Jika Anda sudah memiliki dua, Anda harus menghapus satu pasangan kunci sebelum membuat pasangan baru. Untuk melihat instruksi, lihat Mengelola access keys di Panduan Pengguna IAM.

Saya seorang administrator dan ingin mengizinkan orang lain mengakses Armada

Untuk mengizinkan orang lain mengakses Fleet Hub, Anda harus membuat entitas IAM (pengguna atau peran) untuk orang atau aplikasi yang memerlukan akses. Mereka akan menggunakan kredensial untuk entitas tersebut untuk mengakses AWS. Anda kemudian harus melampirkan kebijakan untuk entitas tersebut agar memperoleh izin yang tepat di Fleet Hub.

Untuk segera mulai, lihat Membuat pengguna dan grup khusus IAM pertama Anda di Panduan Pengguna IAM.

Saya ingin mengizinkan orang di luar sayaAWSakun untuk mengakses sumber daya Fleet Hub 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 pada orang ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa hal berikut:

- Untuk mempelajari apakah Armada mendukung fitur ini atau tidak, lihatCara kerja Fleet Hub for AWS IoT Device Management dengan IAM (p. 31).
- Untuk mempelajari cara memberikan akses ke sumber daya di seluruh Akun AWS yang Anda miliki, lihat Menyediakan akses ke pengguna IAM di akun Akun AWS lain yang Anda miliki dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses ke sumber daya Anda ke Akun AWS pihak ketiga, lihat Menyediakan akses ke akun Akun AWS yang dimiliki oleh pihak ketiga dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat Menyediakan akses ke pengguna terautentikasi eksternal (gabungan identitas) dalam 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.

Validasi Kepatuhan untuk Armada untukAWS IoTManajemen Perangkat

Auditor pihak ketiga menilai keamanan dan kepatuhan Armada sebagai bagian dari beberapaAWSprogram kepatuhan. Program ini mencakup SOC, PCI, FedRAMP, HIPAA, dan lainnya.

Untuk mempelajari apakah atau lainnyaLayanan AWSberada dalam lingkup program kepatuhan tertentu, lihatAWSLayanan dalam Lingkup oleh Program Kepatuhan. Untuk informasi umum, lihat Program Kepatuhan AWS.

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

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

- Panduan Quick Start Keamanan dan Kepatuhan – Panduan deployment ini membahas pertimbangan arsitektur dan menyediakan langkah-langkah untuk melakukan deployment terhadap lingkungan dasar di AWS yang menjadi fokus keamanan dan kepatuhan.
- Merancang untuk Keamanan dan Kepatuhan HIPAA pada Amazon Web Services- Whitepaper ini menjelaskan bagaimana perusahaan dapat menggunakanAWSuntuk membuat aplikasi yang memenuhi syarat HIPAA.

  Note

  Tidak semua Layanan AWS memenuhi syarat HIPAA. Untuk informasi selengkapnya, lihat Referensi Layanan yang Memenuhi Syarat HIPAA.
- Sumber Daya Kepatuhan AWS – Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- Mengevaluasi Sumber Daya dengan Aturan di Panduan Developer AWS Config – Layanan AWS Config menilai seberapa baik konfigurasi sumber daya Anda dalam mematuhi praktik-praktik internal, pedoman industri, dan regulasi internal.
- AWS Security Hub – Layanan AWS ini menyediakan pandangan yang komprehensif tentang status keamanan Anda dalam AWS yang membantu Anda memeriksa kepatuhan Anda terhadap standar industri dan praktik terbaik untuk keamanan.

- AWS Audit Manager – Layanan AWS ini akan membantu Anda untuk terus-menerus mengaudit penggunaan AWS untuk menyederhanakan bagaimana Anda mengelola risiko dan kepatuhan terhadap regulasi dan standar industri.

Ketahanan di Armada untukAWS IoTManajemen Perangkat

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.

AWSkebijakan terkelola untuk Armada untukAWS IoTManajemen Perangkat

Untuk menambahkan izin ke para pengguna, grup, dan peran, akan lebih mudah menggunakan kebijakan terkelola AWS dibandingkan dengan menulis kebijakan sendiri. Dibutuhkan waktu dan keahlian untuk membuat kebijakan terkelola pelanggan IAM yang hanya menyediakan izin sesuai kebutuhan tim Anda. Untuk mulai dengan cepat, Anda dapat menggunakan kebijakan-kebijakan terkelola AWS kami. Kebijakan-kebijakan ini mencakup kasus penggunaan umum dan tersedia di akun AWS Anda. Untuk informasi lebih lanjut tentang kebijakan-kebijakan terkelola AWS, lihat kebijakan terkelola AWS di Panduan Pengguna IAM.

Layanan AWS mempertahankan dan memperbarui kebijakan-kebijakan terkelola AWS. Anda tidak dapat mengubah izin yang ada dalam kebijakan-kebijakan yang dikelola AWS. Layanan terkadang menambahkan izin tambahan ke kebijakan yang dikelola AWS untuk mendukung fitur-fitur baru. Jenis pembaruan ini akan memengaruhi semua identitas (pengguna, grup, dan peran) di mana kebijakan tersebut dilampirkan. Layanan kemungkinan besar akan memperbarui kebijakan yang dikelola AWS saat ada fitur baru yang diluncurkan atau saat ada operasi baru yang tersedia. Layanan tidak menghapus izin yang ada di kebijakan yang dikelola AWS, sehingga pembaruan-pembaruan yang terjadi pada kebijakan tidak akan membuat izin yang ada rusak.

Selain itu, AWS mendukung kebijakan-kebijakan terkelola untuk fungsi tugas yang mencakup beberapa layanan. Misalnya,ReadOnlyAccess AWSkebijakan terkelola menyediakan akses hanya baca ke semuaAWSlayanan dan sumber daya. Saat layanan meluncurkan fitur baru, AWS menambahkan izin hanya-baca untuk operasi dan sumber daya yang baru. Untuk melihat daftar dan deskripsi dari kebijakan-kebijakan fungsi tugas, lihat kebijakan terkelola AWS untuk fungsi tugas di Panduan Pengguna IAM.

AWSkebijakan terkelola: AWSIoTFleetHubFederationAccess

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

Kebijakan ini memberikan Armada untukAWS IoTManajemen Perangkat mengfederasikan izin yang diperlukan untuk mengambil tindakan kepada penggunaAWS IoTdan lainnyaAWSlayanan dari aplikasi web Fleet Hub.

Untuk informasi selengkapnya tentang menambahkan pengguna ke aplikasi web Fleet Hub, lihat??? (p. 5).

Lihat kebijakan ini di[AWSkonsol](#).

Detail Izin

Kebijakan ini mencakup izin berikut:

- `iot`- MengambilAWS IoTdata perangkat dan melakukan tindakan tingkat armada.
- `iotfleethub`- Ambil metadata aplikasi Fleet Hub.
- `cloudwatch`- Mengambil CloudWatch alarm dan data metrik. Juga memungkinkan membuat dan menghapus tindakan scoped ke alarm Fleet Hub.
- `sns`- Jalankan operasi buat, baca, hapus, berlangganan, dan berhenti berlangganan. Operasi ini scoped untuk topik Fleet Hub SNS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iot:DescribeIndex",
                "iot:DescribeThingGroup",
                "iot:GetBucketsAggregation",
                "iot:GetCardinality",
                "iot:GetIndexingConfiguration",
                "iot:GetPercentiles",
                "iot:GetStatistics",
                "iot:SearchIndex",
                "iot:CreateFleetMetric",
                "iot:ListFleetMetrics",
                "iot:DeleteFleetMetric",
                "iot:DescribeFleetMetric",
                "iot:UpdateFleetMetric",
                "iot:DescribeCustomMetric",
                "iot:ListCustomMetrics",
                "iot:ListDimensions",
                "iot:ListMetricValues",
                "iot:ListThingGroups",
                "iot:ListThingsInThingGroup",
                "iot:ListJobTemplates",
                "iot:DescribeJobTemplate",
                "iot:ListJobs",
                "iot:CreateJob",
                "iot:CancelJob",
                "iot:DescribeJob",
                "iot:ListJobExecutionsForJob",
                "iot:ListJobExecutionsForThing",
                "iot:DescribeJobExecution",
                "iot:ListSecurityProfiles",
                "iot:DescribeSecurityProfile",
                "iot:ListActiveViolations",
                "iot:GetThingShadow",
                "iot:ListNamedShadowsForThing",
```

```
                "iot:CancelJobExecution",
                "iot:DescribeEndpoint",
                "iotfleethub:DescribeApplication",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:GetMetricData",
                "cloudwatch:ListMetrics",
                "sns:ListTopics"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "sns:CreateTopic",
                "sns:DeleteTopic",
                "sns:ListSubscriptionsByTopic",
                "sns:Subscribe",
                "sns:Unsubscribe"
            ],
            "Resource": "arn:aws:sns:*:*:iotfleethub*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricAlarm",
                "cloudwatch:DeleteAlarms",
                "cloudwatch:DescribeAlarmHistory"
            ],
            "Resource": "arn:aws:cloudwatch:*:*:iotfleethub*"
        }
    ]
}
```

Pembaruan Fleet HubAWSkebijakan yang dikelola

Melihat detail tentang pembaruanAWSkebijakan yang dikelola untuk Fleet Hub karena layanan ini mulai melacak perubahan ini. Untuk informasi lebih lanjut, lihat ArmadaRiwayat dokumentasi (p. 46)halaman.

Perubahan	Deskripsi	Tanggal
AWSIoTFleetHubFederationAccess (p. 41) — Permbaruan ke kebijakan yang sudah ada	Fleet Hub menambahkan izin baru untuk memungkinkan pengguna aplikasi mengambilAWS IoT Device Defenderdata metrik di aplikasi Fleet Hub.	4 April 2022
AWSIoTFleetHubFederationAccess (p. 41) — Permbaruan ke kebijakan yang sudah ada	Fleet Hub menambahkan izin baru untuk memungkinkan pengguna aplikasi mengambil sumber data tambahan untuk pengindeksan. Izin juga ditambahkan untuk memungkinkan pengguna aplikasi membatalkanAWS IoTeksekusi pekerjaan dalam aplikasi.	15 November 2021

Perubahan	Deskripsi	Tanggal
AWSIoTFleetHubFederationAccess (p. 41) — Permbaruan ke kebijakan yang sudah ada	Fleet Hub menambahkan izin baru bagi pengguna aplikasi untuk mengambil data Thing Group dan melakukan operasi CRUDAWS IoTpekerjaan.	24 Mei 2021
AWSIoTFleetHubFederationAccess (p. 41) — Permbaruan ke kebijakan yang sudah ada	Fleet Hub menghapus izin untuk API dasbor Fleet Hub yang tidak didukung.	12 April 2021
AWSIoTFleetHubFederationAccess (p. 41) – Kebijakan baru	Fleet Hub menambahkan kebijakan baru yang memberikan izin yang diperlukan bagi pengguna aplikasi Fleet Hub untuk mengambil data perangkat dan melakukanAWS IoTtindakan.	12 April 2021
Armada untuk melacak perubahan	Armada mulai melacak perubahan untukAWSkebijakan terkelola.	12 April 2021

Keamanan infrastruktur di Armada untukAWS IoTManajemen Perangkat

Sebagai layanan terkelola, Fleet Hub untukAWS IoTManajemen Perangkat dilindungi olehAWSprosedur keamanan jaringan global yang dijelaskan dalamAmazon Web Services: Whitepaper Ikhtisar Proses Keamanan.

Anda menggunakanAWSpanggilan API yang dipublikasikan untuk mengakses Fleet Hub melalui jaringan. Klien harus mendukung Keamanan Lapisan Pengangkutan (TLS) 1.0 atau versi yang lebih baru. Kami merekomendasikan TLS 1.2 atau versi yang lebih baru. Klien juga harus mendukung suite cipher dengan perfect forward secrecy (PFS) seperti Ephemeral Diffie-Hellman (DHE) atau Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). 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.

Pencegahan wakil bingung lintas layanan

Masalah wakil yang membingungkan adalah masalah keamanan di mana entitas yang tidak memiliki izin untuk melakukan tindakan dapat memaksa entitas yang lebih istimewa untuk melakukan tindakan. MasukAWS, peniruan lintas layanan dapat mengakibatkan masalah wakil bingung. Peniruan lintas layanan dapat terjadi ketika satu layanan (layanan panggilan) memanggil layanan lain (disebut layanan). Layanan panggilan dapat dimanipulasi untuk menggunakan izinnya untuk bertindak pada sumber daya pelanggan lain dengan cara yang seharusnya tidak memiliki izin untuk mengakses. Untuk mencegah hal ini,AWSmenyediakan alat yang membantu Anda melindungi data Anda untuk semua layanan dengan prinsip-prinsip layanan yang telah diberikan akses ke sumber daya di akun Anda.

Untuk membatasi izin yang diberikan Fleet Hub layanan lain ke sumber daya, kami sarankan untuk menggunakan`aws:SourceArn`dan`aws:SourceAccount`kunci konteks kondisi global dalam kebijakan

sumber daya. Jika Anda menggunakan kedua kunci konteks kondisi global,`aws:SourceAccount`nilai dan akun di`aws:SourceArn`nilai harus menggunakan ID akun yang sama ketika digunakan dalam pernyataan kebijakan yang sama.

Cara paling efektif untuk melindungi terhadap masalah wakil yang bingung adalah dengan menggunakan`aws:SourceArn`kunci konteks kondisi global dengan Amazon Resource Name (ARN) dari sumber daya. Untuk Fleet Hub,`aws:SourceArn`harus sesuai dengan format: `arn:aws:iot:`*`region`*`:`*`account-id`*`:*`. Pastikan bahwa*daerah*cocok dengan Wilayah Hub Armada Anda dan*ID akun*cocok ID akun pelanggan Anda.

Contoh berikut menunjukkan cara mencegah masalah wakil bingung dengan menggunakan`aws:SourceArn`dan`aws:SourceAccount`kunci konteks kondisi global dalam kebijakan kepercayaan peran Fleet Hub. Untuk menemukan peran ARN Armada Hub Anda, buka bagian Fleet Hub diAWS IoTkonsol dan pilih aplikasi Fleet Hub Anda untuk melihat halaman detail aplikasi.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "iotfleethub.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:iot:us-east-1:123456789012:*"
        }
      }
    }
  ]
}
```

Riwayat dokumentasi

Tabel berikut menjelaskan pembaruan pada dokumentasi Armada Hub. Untuk perubahan padaAWSkebijakan terkelola untuk Fleet Hub, lihatAWSkebijakan terkelola untuk Armada Hub untukAWS IoTManajemen Perangkat (p. 41).

Perubahan	Deskripsi	Tanggal
Hub Armada untukAWS IoTRilis ketersediaan umum Manajemen Perangkat	Konten yang diperbarui untuk mencerminkan perbaikan yang dilakukan pada Fleet Hub untukAWS IoTManajemen Perangkat selama periode pratinjau.	25 Mei 2021.
Rilis Armada Hub untukAWS IoTManajemen Perangkat	Diterbitkan versi rilis pratinjauHub Armada untukAWS IoTManajemen Perangkat Panduan Pengguna.	16 Desember 2020.

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