Hub Armada untuk Panduan Manajemen AWS IoT Perangkat

Fleet Hub untuk Manajemen AWS IoT Perangkat

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Fleet Hub untuk Manajemen AWS IoT Perangkat: Hub Armada untuk Panduan Manajemen AWS IoT Perangkat

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Merek dagang dan tampilan dagang Amazon tidak boleh digunakan sehubungan dengan produk atau layanan apa pun yang bukan milik Amazon, dengan cara apa pun yang dapat menyebabkan kebingungan di antara pelanggan, atau dengan cara apa pun yang merendahkan atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan hak milik masing-masing pemiliknya, yang mungkin atau tidak terafiliasi, terkait dengan, atau disponsori oleh Amazon.

Table of Contents

... v
Untuk apa Armada HubAWS IoTManajemen Perangkat? ... 1
Bagaimana Armada HubAWS IoTManajemen Perangkat bekerja ... 1
Cara kerja pengindeksan data Fleet Hub ... 2
Cara kerja alarm Fleet Hub ... 2
Cara kerja Fleet Hub ... 2
Fleet Hub untuk Manajemen AWS IoT Perangkat untuk administrator ... 4
Memulai ... 4
Buat aplikasi Fleet Hub pertama Anda ... 4
Kelola pengindeksan armada untuk aplikasi Fleet Hub ... 6
Tambahkan pengguna ke aplikasi Fleet Hub ... 8
AWSdan AWS IoT Core layanan yang berinteraksi dengan Fleet Hub untuk Manajemen AWS IoT Perangkat ... 8
Pemecahan Masalah ... 10
Hub Armada untuk Manajemen AWS IoT Perangkat untuk pengguna ... 13
Mulai ... 13
Buat kueri pertama Anda ... 13
Buat alarm pertama Anda ... 14
Melihat detail perangkat ... 17
Kueri dan filter ... 22
Lihat dasbor ... 22
Buat kueri dengan filter ... 24
Bekerja dengan pekerjaan dan template pekerjaan di Fleet Hub untukAWS IoTManajemen Perangkat ... 25
Lowongan kerja Running ... 26
Melihat dan Mengelola Tugas ... 27
Alarm ... 27
Membuat alarm ... 30
Pemecahan Masalah ... 31
Hub untuk ManajemenAWS IoT Perangkat ... 32
Logging Fleet Hub untuk panggilan API ManajemenAWS IoT Perangkat denganAWS CloudTrail ... 32
Informasi Fleet Hub di CloudTrail ... 32
Memahami Fleet Hub untuk entri file log ManajemenAWS IoT Perangkat ... 34

Keamanan ... 36
Perlindungan data ... 37
Enkripsi saat Istirahat ... 38
Enkripsi bergerak ... 38
Identity and Access Management ... 38
Audiens ... 38
Mengautentikasi dengan identitas ... 39
Mengelola akses menggunakan kebijakan ... 43
Bagaimana Fleet Hub for AWS IoT Device Management bekerja dengan IAM ... 46
Contoh kebijakan berbasis identitas ... 53
Pemecahan Masalah ... 56
Validasi kepatuhan ... 58
Ketahanan ... 59
AWS kebijakan terkelola ... 60
AWSIoTFleetHubFederationAccess ... 60
Pembaruan kebijakan ... 63
Keamanan infrastruktur ... 64
Pencegahan "confused deputy" lintas layanan ... 65
Hub Armada end-of-life (EOL) FAQs ... 67
Kapan Fleet Hub pergi end-of-life? ... 67
Apa yang terjadi pada aplikasi Fleet Hub saya pada end-of-life tanggal tersebut? ... 68
Apa yang terjadi pada AWS sumber daya dasar saya pada dan setelah end-of-life tanggal? ... 68
Bagaimana cara menghapus aplikasi Fleet Hub sebelum end-of-life tanggal? ... 68
Akankah menghapus aplikasi Fleet Hub secara otomatis menghapus sumber daya yang mendasarinya? ... 70
Bagaimana cara menghapus AWS sumber daya dasar saya? ... 70
Bagaimana cara menghapus pekerjaan? ... 70
Bagaimana cara menghapus alarm Fleet Hub? ... 71
Bagaimana cara menghapus pengguna Pusat IAM Identitas yang dibuat dari Fleet Hub? ... 72
APIsMana yang tidak lagi berfungsi pada dan setelah end-of-life tanggal? ... 72
Apa saja fungsi Fleet Hub yang ada dan bagaimana cara mengaksesnya di konsol? ... 73
Riwayat dokumentasi ... 75

AWS akan menghentikan fitur AWS IoT Device Management Fleet Hub pada 18 Oktober 2025 dan tidak lagi menerima pelanggan baru. Pelanggan AWS IoT Device Management Fleet Hub yang ada akan dapat menggunakan Fleet Hub hingga 17 Oktober 2025. Untuk informasi selengkapnya, lihat Fleet Hub end-of-life (EOL) FAQs.

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

Untuk apa Armada HubAWS IoTManajemen Perangkat?

Dengan Fleet Hub untukAWS IoTManajemen Perangkat (Fleet Hub), Anda dapat membangun aplikasi web mandiri untuk memantau kesehatan armada perangkat Anda. Anda dapat membuat aplikasi ini tersedia untuk 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.

- Pantau armada perangkat dalam waktu hampir nyata.
- Tetapkan peringatan untuk memberi tahu teknisi Anda tentang perilaku yang tidak biasa.
- Menjalankan pekerjaan.

> **Note**
>
> Agar Fleet Hub dapat mengindeks data status konektivitas, Hal-hal Anda harus terhubungAWS IoT Coredengan ID klien sama dengan nama Thing.

Bagaimana Armada HubAWS IoTManajemen Perangkat bekerja

Administrator dapat menggunakan Fleet Hub untukAWS IoTManajemen Perangkat untuk membuat aplikasi web yang aman dalam beberapa menit tanpa menyediakan sumber daya apa pun 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 dalam armada Anda mencapai keadaan tertentu.

Aplikasi Fleet Hub menggunakan`AWSIoTFleetHubFederationAccess`kebijakan yang dikelola. Untuk informasi selengkapnya, lihat ???.

Contoh kasus penggunaan:

- Visualisasikan masalah konektivitas perangkat - Anda dapat melihat jumlah perangkat yang terputus di armada Anda, status koneksi terakhir untuk perangkat, dan alasan atau alasan mengapa perangkat terputus.
- Setel alarm - Anda dapat mengatur ambang batas yang memicu alarm saat sejumlah perangkat tertentu terputus. Alarm juga dapat memberi tahu Anda saat perangkat atau perangkat terputus 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 atau lebih perangkat.

Cara kerja pengindeksan data Fleet Hub

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

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

Cara kerja alarm Fleet Hub

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

1. Buat kueri untuk mengumpulkan data - Tentukan kueri yang menggabungkan perangkat yang ingin ditargetkan pengguna Anda dengan menggunakan bidang yang dapat dicari.
2. Konfigurasi ambang batas - Tetapkan ambang batas yang memicu alarm saat kondisi dalam data yang diindeks (seperti status konektivitas selama interval tertentu) tercapai.
3. Konfigurasikan notifikasi - Tentukan grup penerima yang diberitahukan oleh Fleet Hub saat perangkat yang ditentukan berada dalam alarm.

Cara kerja Fleet Hub

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

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

Fleet Hub untuk Manajemen AWS IoT Perangkat untuk administrator

Bagian ini berisi panduan bagi administrator tentang cara membuat dan mengelola Fleet Hub untuk aplikasi web Manajemen AWS IoT Perangkat.

Topik

- Memulai
- AWSdan AWS IoT Core layanan yang berinteraksi dengan Fleet Hub untuk Manajemen AWS IoT Perangkat
- Pemecahan Masalah

Memulai

Bagian ini menjelaskan cara membuat dan mengatur Fleet Hub untuk aplikasi web Manajemen AWS IoT Perangkat.

Topik

- Buat aplikasi Fleet Hub pertama Anda
- Kelola pengindeksan armada untuk aplikasi Fleet Hub
- Tambahkan pengguna ke aplikasi Fleet Hub

Buat aplikasi Fleet Hub pertama Anda

Prasyarat

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

- Akun AWS.
- AWS IAM Identity Centerdiaktifkan untuk akun Anda. (Jika Anda belum mengaktifkan layanan ini, AWS IoT Core console (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 untuk aplikasi web Manajemen AWS IoT Perangkat.

1. Arahkan ke AWS IoT Core console (https://console.aws.amazon.com/iot/), dan di panel kiri, pilih Fleet Hub, lalu Applications.
2. Pada halaman aplikasi, pilih Buat aplikasi.
3. Pada halaman Siapkan Pusat Identitas IAM, jika Anda belum mengaktifkan AWS IAM Identity Center (Pusat Identitas IAM), ikuti langkah-langkah untuk mengaktifkannya. AWS Organizations mengirimi Anda email. Pilih tautan di email untuk menyelesaikan pengaktifan IAM Identity Center.

   > **Note**
   >
   > Anda dapat menghubungkan penyedia identitas Anda sendiri ke IAM Identity Center. Untuk informasi lebih lanjut, lihat Apa itu AWS IAM Identity Center? dan Connect ke penyedia identitas eksternal Anda.
   > Saat membuat aplikasi Fleet Hub, Anda harus membuat instance organisasi IAM Identity Center jika Anda belum memilikinya. Aplikasi Fleet Hub yang Anda buat juga harus sama dengan Wilayah AWS instance organisasi IAM Identity Center. Untuk informasi selengkapnya lihat Mengaktifkan Pusat Identitas IAM dan instans Organisasi Pusat Identitas IAM.

   Halaman ini memberi tahu Anda jika Anda telah mengaktifkan IAM Identity Center.

   Pilih Berikutnya.
4. Pada halaman AWS IoT Data indeks, tinjau informasi di bagian Cara kerja aliran data dari AWS IoT ke Fleet Hub. Halaman ini menautkan Anda ke halaman di AWS IoT Core konsol tempat Anda dapat mengaktifkan dan mengelola pengindeksan AWS IoT Core 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 kustom selain bidang terkelola yang mengindeks indeks AWS IoT Core armada secara default.

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

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

Setelah selesai mengelola dan meninjau pengaturan pengindeksan armada, pilih Berikutnya.

Untuk informasi selengkapnya tentang cara mengaktifkan pengindeksan armada untuk aplikasi Fleet Hub, lihat Mengelola pengindeksan armada untuk aplikasi Fleet Hub.

5. Pada halaman Konfigurasi aplikasi, di bagian Peran aplikasi, buat peran layanan baru atau pilih peran layanan yang ada. Aplikasi web Fleet Hub Anda mengambil peran ini saat menggunakan sumber daya Fleet Hub. Pengguna federasi memiliki izin yang sama dengan peran ketika 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, pilih Lihat detail peran. Jendela terbuka yang menunjukkan kepada Anda dokumen kebijakan yang diterapkan layanan untuk peran baru apa pun yang Anda buat dari halaman ini.

6. Pada halaman Konfigurasi aplikasi, di bagian Properti aplikasi, masukkan nama untuk aplikasi Anda. Secara opsional, Anda juga dapat memasukkan deskripsi aplikasi.

   Pilih Create application (Buat aplikasi).

7. Pada halaman Aplikasi, pilih aplikasi yang Anda buat dan pilih Lihat detail. Tinjau detail aplikasi.

> **Note**
>
> Untuk informasi selengkapnya tentang kemungkinan solusi untuk menyelesaikan masalah sebagai administrator Fleet Hub, lihat Pemecahan Masalah.

Kelola pengindeksan armada untuk aplikasi Fleet Hub

Anda dapat menggunakan AWS IoT Core konsol atau AWS CLI untuk mengaktifkan pengindeksan armada dan mengonfigurasi sumber data berikut untuk diindeks: data AWS IoT registri, data AWS

IoT Device Shadow, data AWS IoT konektivitas, dan data AWS IoT Device Defender pelanggaran. Langkah-langkah berikut menjelaskan cara mengaktifkan pengindeksan armada untuk aplikasi Fleet Hub for AWS IoT Device Management di AWS IoT Core konsol. Untuk melihat langkah-langkah yang digunakan AWS CLI, lihat Mengelola pengindeksan hal.

> **Important**
>
> 20 Juli 2022 adalah rilis Ketersediaan Umum integrasi pengindeksan armada Manajemen AWS IoT Perangkat dengan bayangan AWS IoT Core bernama dan AWS IoT Device Defender mendeteksi 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 mendorong Anda untuk mengonfigurasi ulang pengaturan pengindeksan armada Anda dan memilih nama bayangan tertentu untuk mengurangi biaya pengindeksan dan mengoptimalkan kinerja. Untuk informasi selengkapnya tentang cara mengonfigurasi ulang setelan pengindeksan armada, lihat Mengelola pengindeksan armada.

1. Arahkan ke AWS IoT Core konsol (https://console.aws.amazon.com/iot/), dan di panel kiri, pilih Pengaturan.
2. Pada halaman Pengaturan, navigasikan ke bagian Pengindeksan Armada, lalu pilih Kelola pengindeksan.
3. Pada halaman Kelola pengindeksan armada, di bagian Konfigurasi, pilih Pengindeksan hal dan sumber data yang AWS IoT ingin Anda indeks. Anda harus mengaktifkan pengindeksan benda dan konektivitas benda untuk menggunakan Fleet Hub.
4. (Opsional) Pada halaman Kelola pengindeksan armada, di bagian Bidang kustom untuk agregasi-opsional, buat bidang kustom selain bidang terkelola yang mengindeks pengindeksan armada secara default.

   Setelah selesai mengelola dan meninjau pengaturan pengindeksan armada, pilih Berikutnya.

   Diperlukan waktu beberapa saat untuk pengindeksan armada untuk memperbarui pengaturan. Untuk informasi selengkapnya tentang cara mengelola pengindeksan armada, lihat Mengelola pengindeksan armada.

Tambahkan pengguna ke aplikasi Fleet Hub

Aplikasi web Fleet Hub for AWS IoT Device Management Anda tidak berisi pengguna apa pun 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 yang ada dengan menyiapkan AWS IAM Identity Center (IAM Identity Center) untuk akun Anda. Anda dapat menghubungkan penyedia identitas Anda sendiri ke IAM Identity Center. Untuk informasi lebih lanjut, lihat Apa itu Pusat Identitas IAM? .

1. Pada halaman Aplikasi, pilih aplikasi web Anda dari daftar aplikasi Fleet Hub. Pilih Lihat detail.
2. Pada halaman detail aplikasi, pilih Tambah pengguna.
3. Di jendela Add Fleet Hub users, pilih pengguna dari organisasi yang ingin Anda akses ke aplikasi. Pilih Tambahkan pengguna yang dipilih.
4. Pada halaman detail aplikasi, verifikasi bahwa Anda melihat pengguna yang Anda pilih dalam daftar pengguna Fleet Hub.

AWSdan AWS IoT Core layanan yang berinteraksi dengan Fleet Hub untuk Manajemen AWS IoT Perangkat

Topik ini menjelaskan bagaimana fitur di Fleet Hub for AWS IoT Device Management berinteraksi dengan AWS layanan lain untuk menghadirkan kemampuan dalam aplikasi web Fleet Hub Anda.

Tabel berikut menunjukkan AWS layanan apa yang digunakan Fleet Hub for AWS IoT Device Management untuk mengimplementasikan setiap fitur.

Kemampuan	AWS layanan	Deskripsi
Integrasikan sistem identitas yang ada, seperti Active Directory.	AWS IAM Identity Center(Pusat Identitas IAM)	Anda menambahkan pengguna dari sistem identitas yang ada dengan menyiapkan AWS IAM Identity Center (IAM Identity Center) untuk akun Anda. Anda dapat menghubungkan penyedia identitas Anda sendiri ke IAM Identity Center.

Kemampuan	AWS layanan	Deskripsi
		Untuk informasi lebih lanjut, lihat Apa ituAWS IAM Identity Center? dan identitas Tenaga Kerja.
Buat kueri dengan menggunakan bidang AWS yang dikelola, bidang khusus, dan atribut apa pun di sumber data terindeks Anda.	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 untuk agregasi selain bidang terkelola yang indeks pengindeksan AWS IoT armada secara default. Untuk informasi lebih lanjut tentang pengindeksan armada, lihat Pengindeksan armada.

Kemampuan	AWS layanan	Deskripsi
Buat alarm untuk satu set perangkat yang ditentukan oleh kueri.	Amazon CloudWatch (CloudWatch)	Dasbor Fleet Hub mengekspos CloudWatch metrik yang dapat Anda gunakan dalam kombinasi dengan bidang yang dapat dicari untuk membuat ambang batas yang mengkhawatirkan. Misalnya, Anda dapat membuat CloudWatch alarm yang menghasilkan notifikasi Amazon Simple Notification Service (Amazon SNS) setiap kali jumlah perangkat yang terhubung berada di bawah jumlah yang ditentukan. Untuk informasi tentangCloudWatch, lihat Apa itu AmazonCloudWatch? Untuk informasi tentang cara AWS IoT Core bekerja dengan CloudWatch membuat metrik dan alarm, lihat Memantau AWS IoT alarm dan metrik menggunakan. CloudWatch

Pemecahan Masalah

Bagian ini menyediakan informasi pemecahan masalah dan kemungkinan solusi untuk membantu menyelesaikan masalah sebagai administrator Fleet Hub.

Gejala	Solusi
Tautan aplikasi web saya tidak berfungsi.	Mungkin perlu 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: JSON `{"Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "Service": "iotfleethub.amazonaws.com" }, "Action": "sts:AssumeRole" } ] }` Untuk informasi selengkapnya tentang cara mengedit hubungan kepercayaan IAM, lihat Mengedit hubungan kepercayaan untuk peran yang ada.
Saya tidak bisa membuat aplikasi web.	Pastikan Anda belum mencapai batas jumlah total aplikasi web.
Saya tidak melihat bidang khusus yang saya harapkan.	Periksa untuk memastikan bahwa Anda telah mengatur pengindeksan armada dengan benar.

Gejala	Solusi
	Untuk informasi selengkapnya tentang pengindeksan armada, lihat Pengindeksan armada.

Hub Armada untuk Manajemen AWS IoT Perangkat untuk pengguna

Bagian ini berisi informasi untuk pengguna aplikasi web Fleet Hub for AWS IoT Device Management. Untuk informasi tentang membuat aplikasi Fleet Hub dan menambahkan pengguna ke dalamnya, lihatFleet Hub untuk Manajemen AWS IoT Perangkat untuk administrator.

Topik

- Mulai
- Kueri dan filter
- Bekerja dengan pekerjaan dan template pekerjaan di Fleet Hub untukAWS IoTManajemen Perangkat
- Alarm
- Pemecahan Masalah

Mulai

Bagian ini berisi informasi tentang memulai dengan menggunakan fitur Fleet Hub untuk aplikasi web Manajemen AWS IoT Perangkat.

Topik

- Buat kueri pertama Anda
- Buat alarm pertama Anda
- Melihat detail perangkat

Buat kueri pertama Anda

Topik ini memandu Anda melalui langkah-langkah untuk membuat kueri Fleet Hub untuk Manajemen AWS IoT Perangkat. Query ditentukan menggunakan sintaks permintaan pencarian.

Prasyarat

- Aplikasi Fleet Hub yang terkait dengan AWS IoT Core akun yang berisi perangkat (hal-hal).

- Akun di organisasi Anda yang memiliki izin untuk menggunakan aplikasi Fleet Hub.

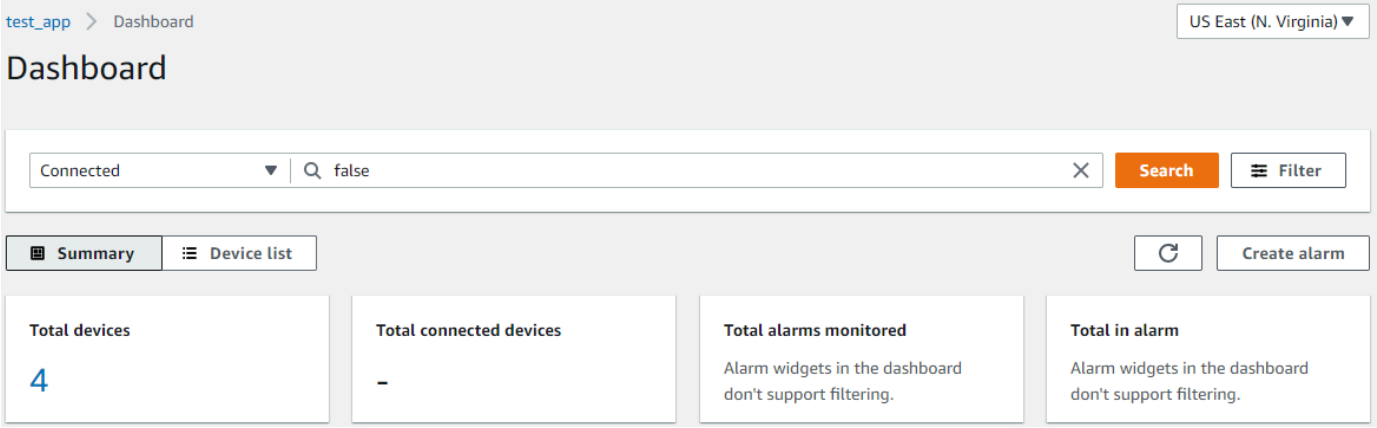
Buat kueri Fleet Hub pertama Anda

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 berisi awalan atribut adalah atribut khusus.

2. Pada menu di bagian atas halaman, pilih Terhubung dari Semua bidang. Masukkan **`false`** di kotak teks di sebelah menu dropdown.



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

Untuk informasi lebih lanjut tentang sintaks query dan contoh query, lihat sintaks Query, Contoh hal query, dan Contoh hal query kelompok.

Buat alarm pertama Anda

Topik ini memandu Anda melalui langkah-langkah untuk membuat alarm Fleet Hub untuk Manajemen AWS IoT Perangkat sederhana.

Prasyarat

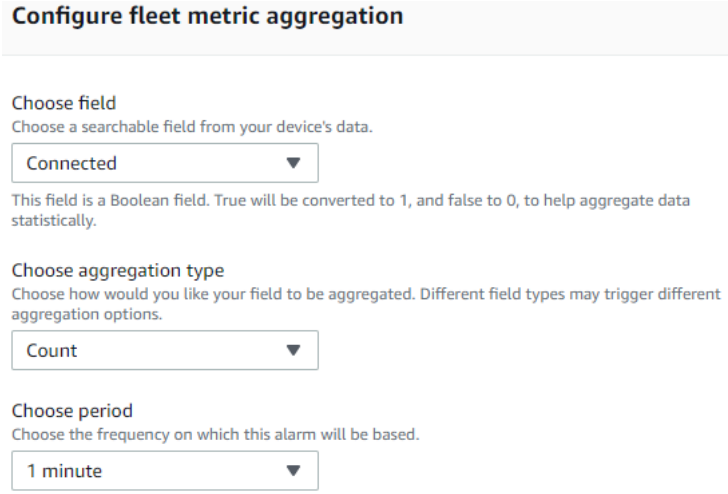
- Aplikasi Fleet Hub yang terkait dengan AWS IoT Core akun yang berisi perangkat (hal-hal).
- Akun di organisasi Anda yang memiliki izin untuk menggunakan aplikasi Fleet Hub.

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”. Jika Anda tidak membuat kueri, alarm Anda akan berlaku untuk semua perangkat di armada Anda.
3. Pada halaman dasbor default, pilih Buat alarm.
4. Pada halaman Metrik agregasi build, verifikasi bahwa kueri Anda muncul di bawah Kueri target. Di bagian Konfigurasi agregasi metrik armada, pada menu Pilih bidang, pilih Terhubung. Bidang AWS -managed ini menunjukkan apakah perangkat terhubung keAWS IoT Core. Menu kolom Pilih berisi bidang AWS -managed dan bidang khusus yang telah dibuat administrator Anda dalam pengindeksan AWS IoT armada.
5. Untuk Pilih tipe agregasi, pilih salah satu opsi berikut.
   - Maksimum -- Konfigurasikan ambang batas maksimum.
   - Hitung -- Konfigurasikan hitungan tertentu sebagai ambang batas.
   - Jumlah -- Konfigurasikan jumlah sebagai ambang batas.
   - Minimum -- Konfigurasikan ambang batas minimum.
   - Rata-rata -- Konfigurasikan ambang batas rata-rata.
6. Untuk Pilih periode, pilih durasi kondisi yang ditentukan dalam menu sebelumnya yang akan memicu alarm.

   Contoh pengaturan untuk Mengonfigurasi agregasi metrik armada dapat terlihat seperti berikut:



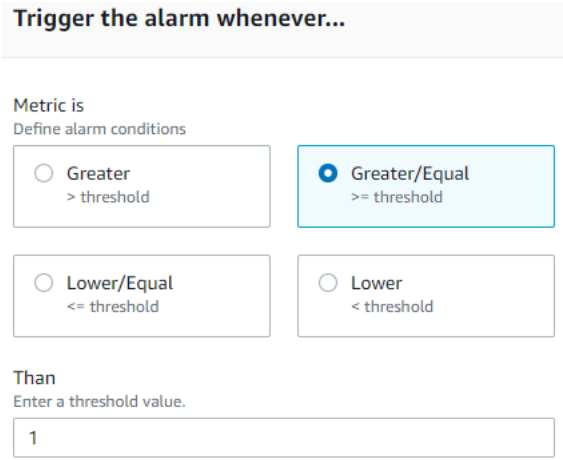
Pilih Selanjutnya.

7. Pada halaman Set threshold, di Trigger alarm setiap kali... bagian, memilih salah satu opsi berikut.

   - Lebih besar -- Alarm ketika metrik agregasi dan jenis melebihi nilai yang ditentukan.
   - Lebih besar/Sama -- Alarm ketika metrik agregasi dan jenis sama atau melebihi nilai yang ditentukan.
   - Lebih rendah -- Alarm ketika metrik agregasi dan jenis jatuh di bawah nilai yang ditentukan.
   - Lower/Equal -- Alarm ketika metrik agregasi dan jenis sama atau jatuh di bawah nilai yang ditentukan.

8. Dalam Dari kotak teks, tentukan nilai yang akan digunakan sebagai ambang batas alarm.

   Pengaturan contoh untuk Ambang Batas Atur dapat terlihat seperti berikut:



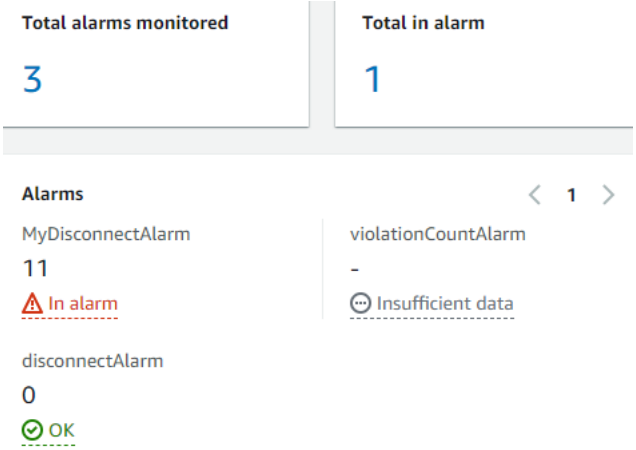
   Pilih Selanjutnya.

9. Pada halaman Beri tahu pengguna, di bagian Notify -- 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.

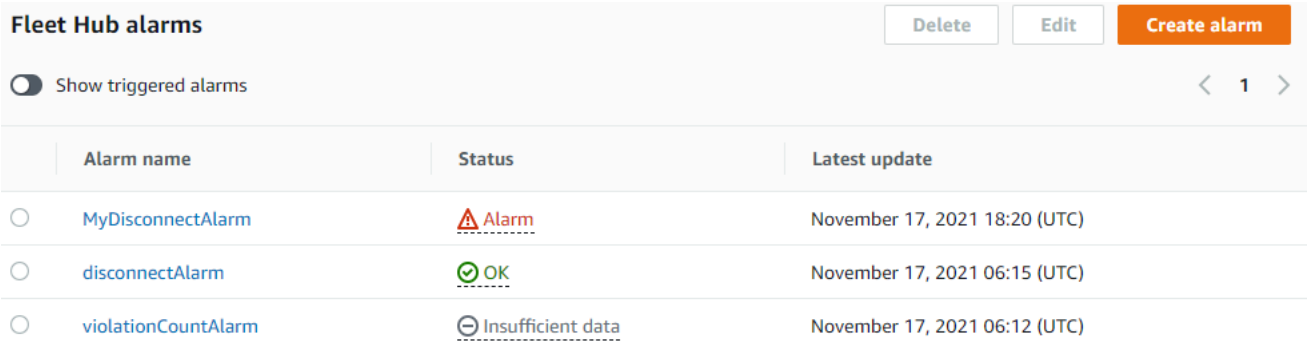
10. Di bagian Alarm, masukkan nama untuk alarm Anda, dan masukkan deskripsi untuk alarm Anda secara opsional. Pilih Selanjutnya.

11. Di halaman Tinjau, verifikasi informasi yang Anda masukkan di 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, pilih alarm Fleet Hub.



Melihat detail perangkat

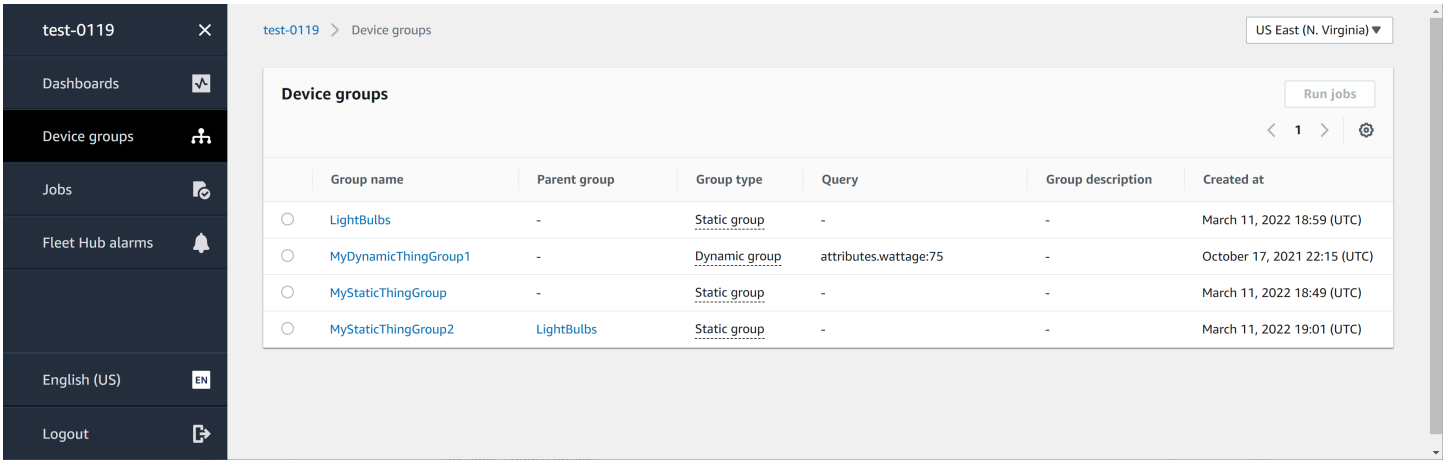
Topik ini memandu Anda melalui langkah-langkah untuk melihat detail tentang grup perangkat dan perangkat Anda.

Prasyarat

- Aplikasi Fleet Hub yang terkait dengan AWS IoT Core akun yang berisi perangkat (hal-hal).
- Akun di organisasi Anda yang memiliki izin untuk menggunakan aplikasi Fleet Hub.

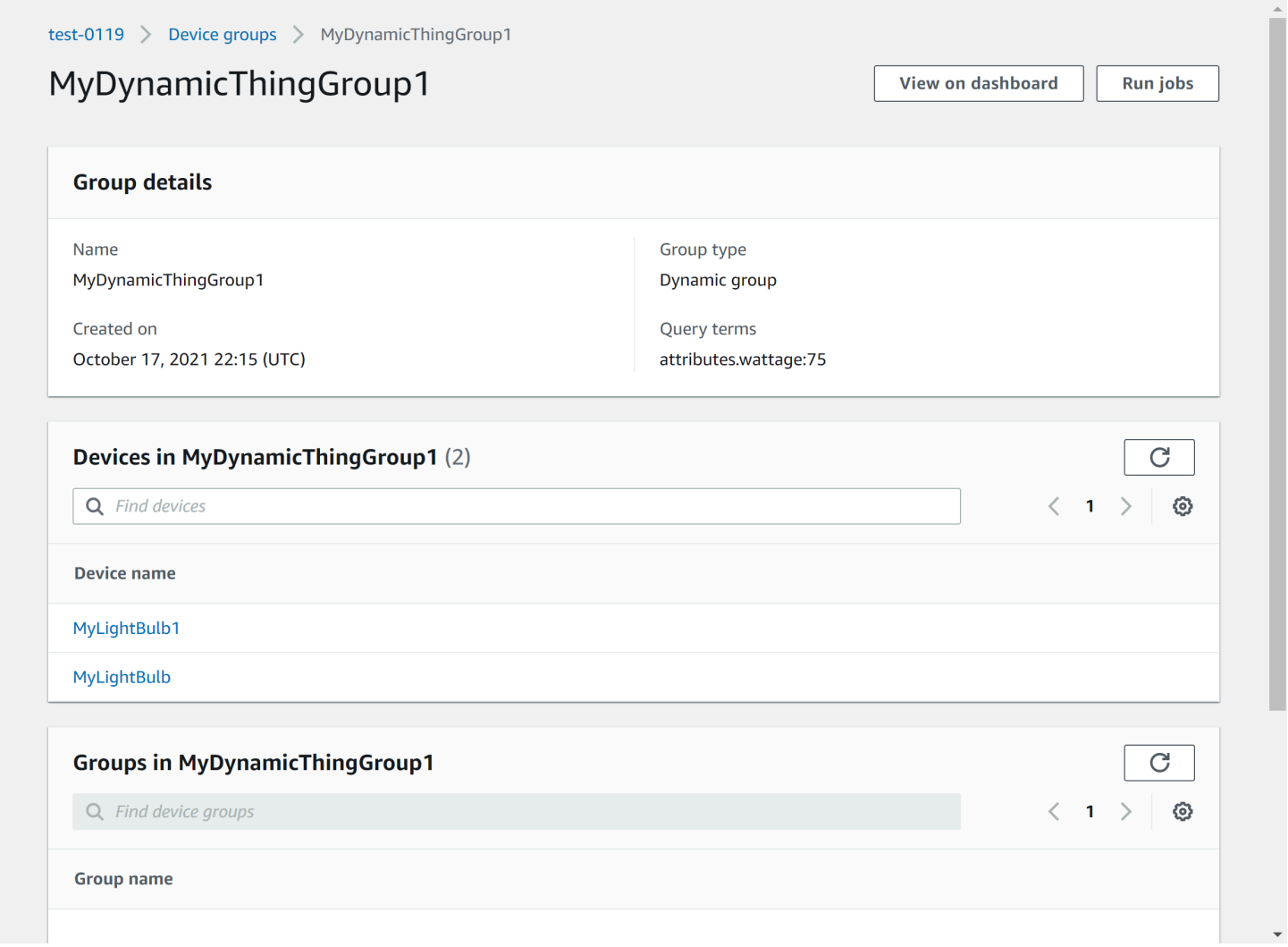
Grup perangkat

Saat masuk ke aplikasi web Fleet Hub, Anda melihat Grup perangkat di panel navigasi kiri. Halaman Grup Perangkat mencantumkan semua grup perangkat di aplikasi web Fleet Hub Anda. Untuk melihat detail grup perangkat, pilih grup perangkat tertentu dari kolom Nama grup.



Perincian grup perangkat perangkat

Halaman detail grup perangkat berisi informasi tentang grup perangkat yang Anda pilih. Untuk melihat detail perangkat, pilih perangkat tertentu dari kolom Nama perangkat di bagian Perangkat di ***XXX***.



Detail perangkat

Halaman Detail perangkat berisi informasi tentang perangkat yang Anda pilih.

> **Note**
>
> Jika klien Anda menggunakan ID klien yang berbeda dari Thing Name saat terhubungAWS IoT, status konektivitas “benda” Anda tidak akan diindeks oleh Fleet Indexing.

Detail

Bagian Detail berisi informasi berikut tentang perangkat Anda:

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

- Jenis benda - 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, lihat Jenis benda.

- Stempel waktu sambungan terakhir - Stempel waktu untuk saat perangkat Anda terakhir terhubung. AWS IoT

- Tautan perangkat yang dapat dibagikan — Tautan yang dapat dibagikan yang mengarah ke halaman detail Perangkat pada perangkat yang dipilih.

- Status koneksi terakhir — Status koneksi perangkat Anda keAWS IoT. Jika perangkat Anda terhubung, nilainya adalah`true`. Jika tidak terhubung, nilainya adalah`false`.

- Lepaskan alasan — Alasan mengapa perangkat Anda terputus.

Data yang dilaporkan

Bagian Data yang dilaporkan berisi informasi tentang data registri perangkat Anda, data bayangan perangkat, dan grup benda.

- Bidang perangkat - Bidang yang diindeks perangkat Anda dalam pengindeksan AWS IoT armada. Untuk informasi selengkapnya, lihat Mengelola 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, lihat bayangan AWS IoT perangkat.

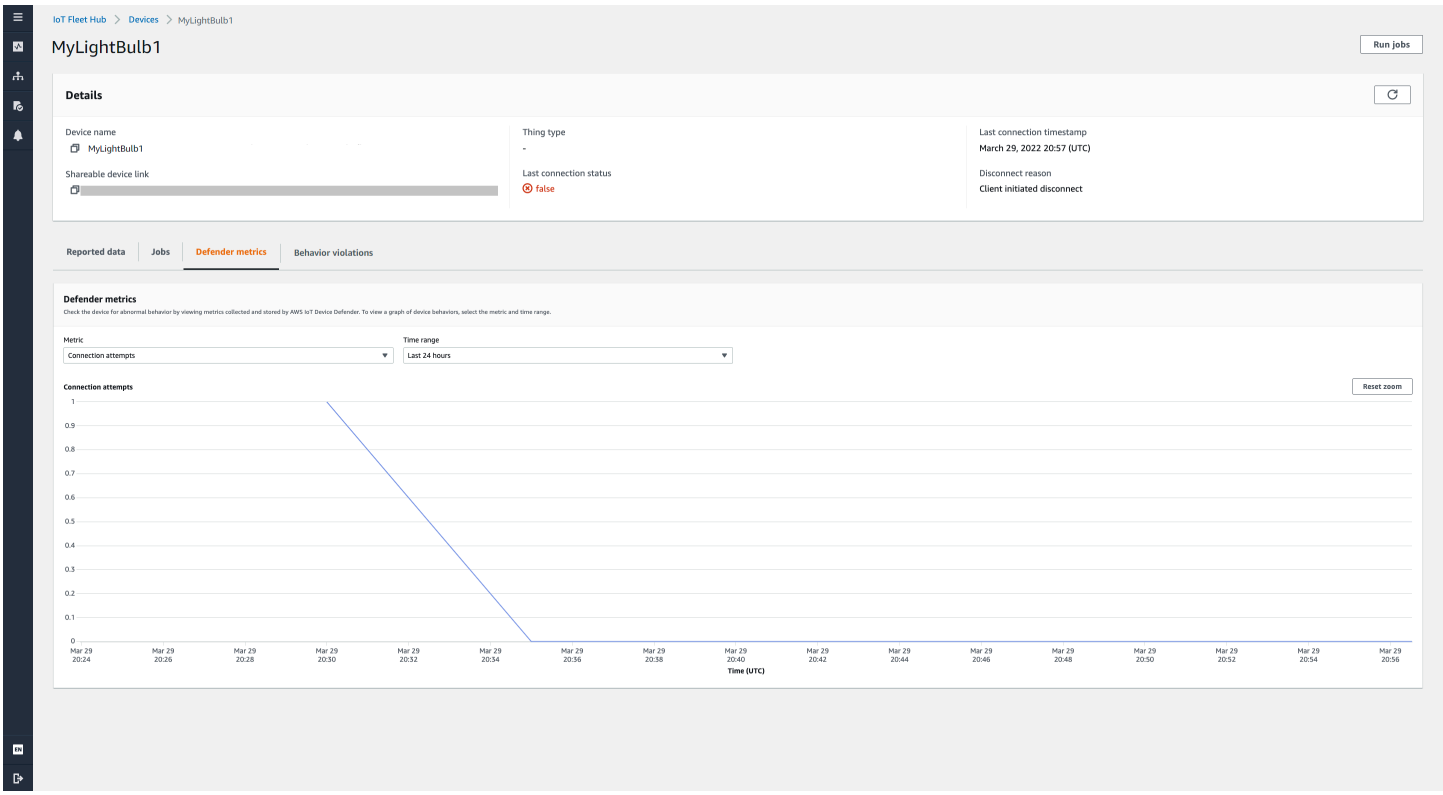
- Grup perangkat — Grup perangkat yang terkait dengan perangkat Anda. Grup perangkat dapat menyertakan grup benda statis dan grup benda dinamis. Untuk informasi lebih lanjut, lihat Static thing groups dan Dynamic thing groups.

Tugas

Bagian Pekerjaan menampilkan semua pekerjaan yang berjalan di perangkat. Setiap pekerjaan memiliki halaman detail yang menampilkan informasi ringkasan tentang pekerjaan, termasuk informasi target dan waktu proses. Untuk informasi selengkapnya, lihat Bekerja dengan pekerjaan dan template pekerjaan di Hub Armada untuk Manajemen AWS IoT Perangkat, dan Pekerjaan.

Metrik Pertahanan Pertahanan

Bagian metrik Defender menampilkan AWS IoT Device Defender metrik 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 pembela dari aplikasi Fleet Hub, administrator Fleet Hub Anda harus terlebih dahulu menyiapkan AWS IoT Device Defender metrik yang terkait dengan perangkat yang dipilih. Untuk informasi selengkapnya tentang cara membuat dan menyiapkan AWS IoT Device Defender metrik untuk perangkat Anda, lihat Metrik khusus, metrik sisi perangkat, dan metrik sisi Cloud.



Pelanggaran perilaku

Bagian Pelanggaran perilaku menampilkan data pelanggaran AWS IoT Device Defender deteksi terindeks 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 menyiapkan pelanggaran AWS IoT Device Defender perilaku di profil keamanan dan mengonfigurasi AWS IoT Device Defender pelanggaran dalam pengindeksan armada. Untuk informasi selengkapnya tentang cara mengatur pelanggaran perilaku di profil AWS IoT Device Defender keamanan, lihat AWS IoT Device DefenderMendeteksi. Untuk informasi selengkapnya tentang cara mengonfigurasi AWS IoT Device Defender pelanggaran, lihat Mengelola pengindeksan armada untuk aplikasi Fleet Hub dan Mengelola pengindeksan.

Kueri dan filter

Anda dapat menggunakan kueri Fleet Hub for AWS IoT Device Management untuk membuat dan melihat daftar hal-hal di armada perangkat Anda. Semua bidang yang AWS dikelola, bidang khusus, dan atribut apa pun dalam sumber data yang diindeks tersedia untuk Anda sebagai filter kueri. Anda juga dapat membuat bidang khusus untuk mengaktifkan agregasi the section called “Alarm” dengan menggunakan pengindeksan AWS IoT armada. Untuk informasi selengkapnya tentang pengindeksan armada, lihat Pengindeksan armada.

Topik

- Lihat dasbor
- Buat kueri dengan filter

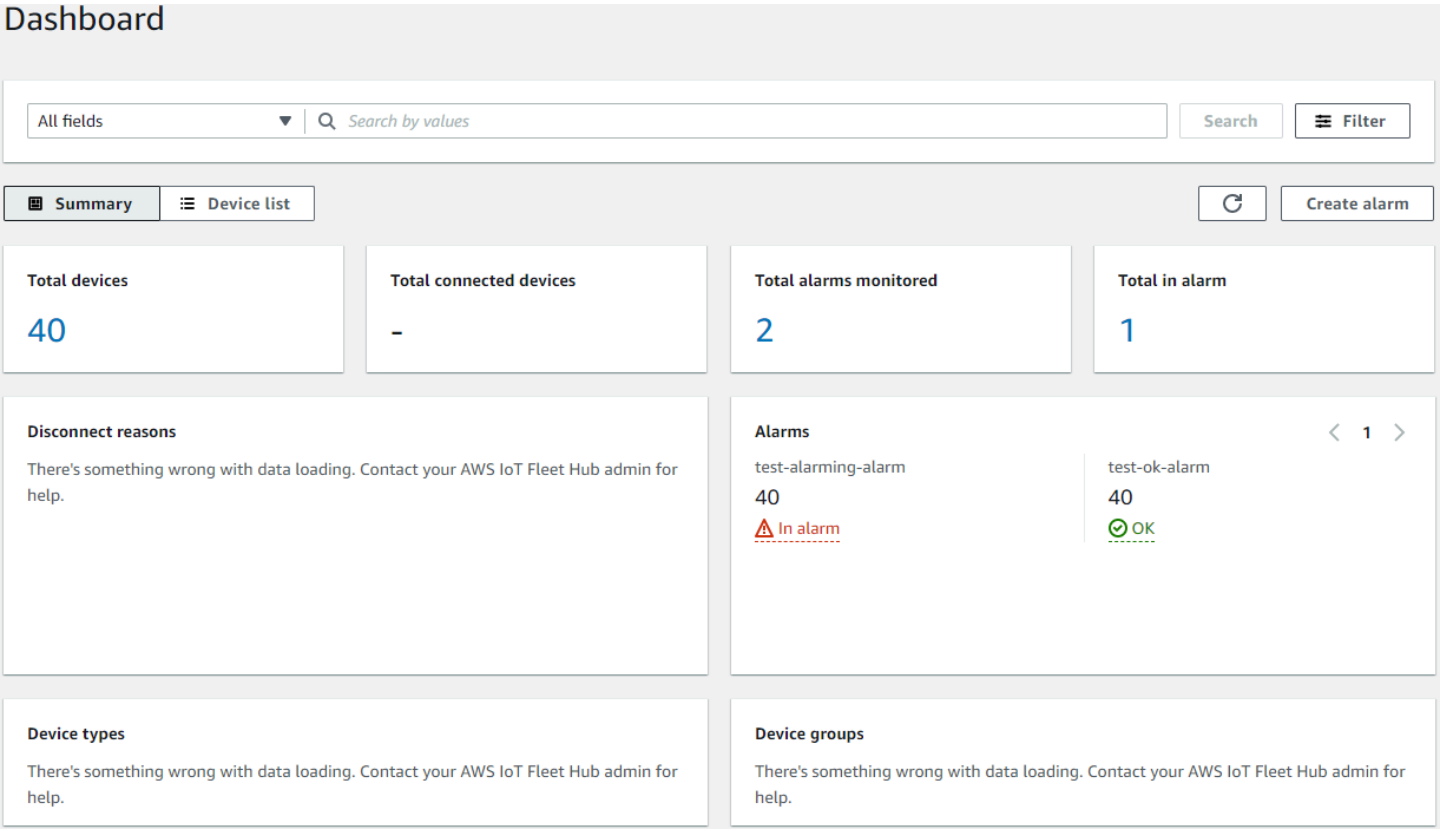
Lihat dasbor

Saat Anda masuk ke aplikasi web Fleet Hub for AWS IoT Device Management, Anda akan melihat dasbor yang menyajikan dua tampilan data tentang perangkat di armada Anda.

Ringkasan

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

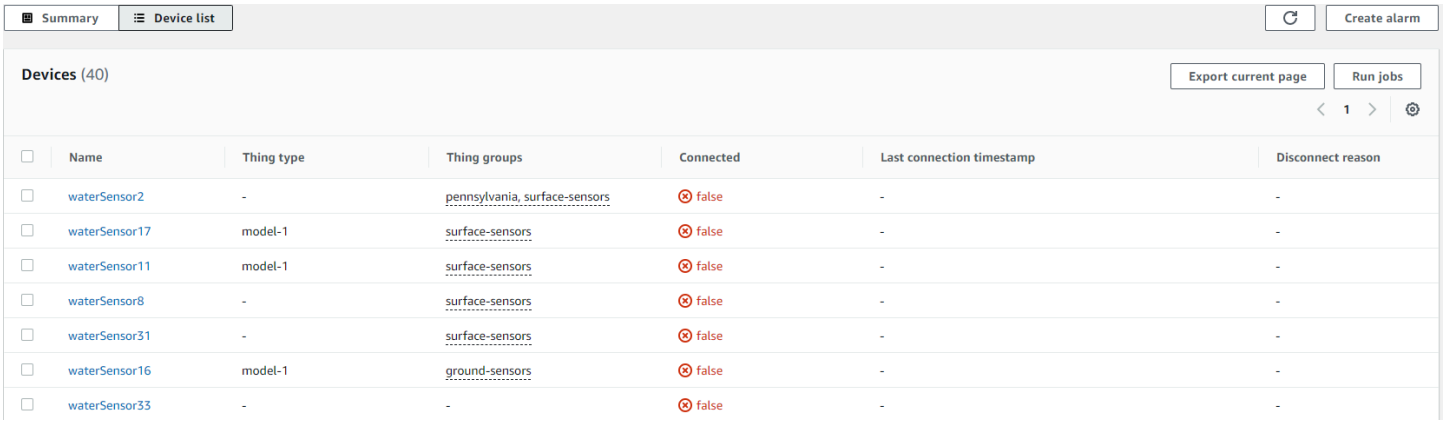
- Jumlah total perangkat
- Jumlah perangkat yang terhubung
- Daftar alasan mengapa perangkat terputus
- Jenis benda yang telah Anda buat untuk armada Anda dan jumlah perangkat untuk setiap jenis
- Grup benda yang telah Anda buat untuk armada Anda dan jumlah perangkat di setiap grup



Daftar perangkat

Tampilan daftar Perangkat menampilkan tabel yang mencantumkan perangkat di armada Anda. Tabel memberikan informasi berikut untuk setiap perangkat dalam daftar.

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



Untuk mengunduh CSV file yang berisi perangkat yang ditampilkan di halaman, pada daftar perangkat, pilih Ekspor halaman saat ini. Perhatikan bahwa jika daftar diberi paginasi, ini hanya mengunduh data yang ditampilkan di halaman saat ini, bukan pada halaman berikutnya.

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

Buat kueri dengan filter

Topik ini menjelaskan cara kerja kueri Fleet Hub for AWS IoT Device Management dan memandu Anda melalui langkah-langkah yang diperlukan untuk membuat kueri dengan filter.

Anda dapat mengontrol jumlah dan jenis perangkat yang ditampilkan pada ringkasan dasbor dan tampilan daftar dengan menggunakan kueri. Anda memfilter kueri dengan menggunakan bidang yang AWS dikelola, bidang khusus, dan atribut apa pun dari sumber data yang diindeks dari pengindeksan armada. AWS IoT Untuk informasi lebih lanjut tentang pengindeksan armada, lihat Pengindeksan armada.

Anda juga dapat menambahkan kata kunci ke kueri 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 tipikal.

Membuat kueri

Langkah-langkah berikut menjelaskan cara membuat kueri khas.

Prasyarat

- Aplikasi Fleet Hub yang terkait dengan AWS IoT Core akun 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. Di dasbor default, verifikasi bahwa Anda dapat melihat tab Daftar perangkat dan jumlah total perangkat (benda) di AWS IoT Core akun asosiasi.
3. Di dasbor default, pilih tab Daftar perangkat. Pastikan Anda melihat daftar semua perangkat yang berisi atribut terkelola dan kustom. Atribut kustom berisi awalan atribut.
4. Di bagian atas halaman, masukkan kata kunci apa pun yang ingin Anda sertakan dalam kueri Anda. Kueri kata kunci berlaku untuk semua bidang.
5. Di bagian atas halaman, pilih Filter.
6. Dalam modal Filter, di bawah Bidang, pilih bidang yang ingin Anda gunakan sebagai filter. Di bawah Operator, pilih opsi. Terakhir, untuk Nilai, pilih nilai bidang yang akan digunakan dalam filter Anda.

   Anda dapat menambahkan hingga tiga filter. Kueri kata kunci dihitung terhadap nomor ini.
7. Untuk melakukan kueri, pilih Terapkan filter. Hasilnya menunjukkan semua perangkat yang cocok 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”.

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 menggunakanGetStatisticsdanGetPercentilieskemampuan 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

Bidang	Tipe agregasi
	• 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”.

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 “Buat kueri dengan filter”. 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 khusus.	Minta administrator Anda untuk membuat metrik di layanan pengindeksan armada.
Alarm saya tidak menunjukkan data apapun.	Alarm membutuhkan waktu beberapa menit.
Aku perlu mengubah perangkat yang menargetkan allarm saya.	Buka dasbor Anda dan ubah kueri.
Saya melihat kesalahan ketika saya mengubah Wilayah di dasbor saya.	Minta administrator Anda untuk memastika n bahwa pengindeksan armada diaktifkan di Wilayah yang Anda pilih.
Status konektivitas “hal” saya tidak diindeks oleh Fleeting Indexing.	Pastikan klien Anda menggunakan ID klien yang sama dengan Thing Name saat menghubungkanAWS IoT. Jika klien Anda menggunakan ID yang berbeda dari Thing Name saat terhubungAWS IoT, status konektivi tas “benda” Anda tidak akan diindeks oleh Fleet Indexing.

Hub untuk ManajemenAWS IoT Perangkat

Pemantauan adalah bagian penting dari pemeliharaan keandalan, ketersediaan, dan performa Hub danAWS solusi Anda. AWSmenyediakan alat pemantauan berikut untuk mengawasi 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

- Logging Fleet Hub untuk panggilan API ManajemenAWS IoT Perangkat denganAWS CloudTrail

Logging Fleet Hub untuk panggilan API ManajemenAWS IoT Perangkat denganAWS CloudTrail

Fleet Hub untuk ManajemenAWS IoT Perangkat terintegrasi denganAWS CloudTrail. CloudTrail Layanan ini menyediakan catatan tindakan yang dilakukan oleh pengguna, peran, atauAWS layanan di Hub. CloudTrail merekam semua panggilan API untuk Hub sebagai peristiwa. Panggilan yang direkam mencakup panggilan dari konsol Hub dan panggilan kode ke operasi API Hub.

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

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

Untuk mempelajari lebih lanjut CloudTrail, lihat PanduanAWS CloudTrail Pengguna.

Informasi Fleet Hub di CloudTrail

AWS CloudTrail diaktifkan pada akun AWS Anda saat Anda membuat akun tersebut. Ketika aktivitas terjadi di Hub, aktivitas tersebut dicatat dalam CloudTrail peristiwa bersama peristiwaAWS layanan

lainnya di Riwayat kejadian. Anda dapat melihat, mencari, dan mengunduh peristiwa terbaru di akun AWS Anda. Untuk informasi selengkapnya, lihat Melihat peristiwa dengan riwayat CloudTrail peristiwa.

Untuk catatan berkelanjutan tentang peristiwa diAWS akun Anda, termasuk peristiwa untuk Hub, buatlah 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 peristiwa dari semua Wilayah di partisi AWS dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan.

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

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

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

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

- Jika permintaan tersebut dibuat dengan kredensi root atauAWS Identity and Access Management pengguna
- 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 .

Memahami Fleet Hub untuk entri file log ManajemenAWS IoT Perangkat

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

CloudTrail berkas log 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.

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

Example

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

```
{
    "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"
    }
```

Keamanan di Fleet Hub untuk Manajemen AWS IoT Perangkat

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

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

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari Program AWS Kepatuhan Program AWS Kepatuhan . Untuk mempelajari tentang program kepatuhan yang berlaku untuk Fleet Hub, lihat AWS Layanan dalam Lingkup berdasarkan AWS Layanan Program Kepatuhan .
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain termasuk sensitivitas data Anda, persyaratan perusahaan Anda, serta hukum dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan Fleet Hub for AWS IoT Device Management. Topik berikut menunjukkan cara mengonfigurasi Fleet Hub untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga akan belajar cara menggunakan AWS layanan lain yang membantu Anda memantau dan mengamankan sumber daya Fleet Hub Anda.

Topik

- Perlindungan data di Fleet Hub
- Identity and Access Management untuk Fleet Hub for AWS IoT Device Management
- Validasi kepatuhan untuk Fleet Hub untuk Manajemen AWS IoT Perangkat
- Ketahanan di Hub Armada untuk Manajemen Perangkat AWS IoT
- AWS kebijakan terkelola untuk Fleet Hub untuk Manajemen AWS IoT Perangkat
- Keamanan infrastruktur di Fleet Hub untuk Manajemen AWS IoT Perangkat
- Pencegahan "confused deputy" lintas layanan

Perlindungan data di Fleet Hub

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di Fleet Hub untuk Manajemen AWS IoT Perangkat. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Lihat informasi yang lebih lengkap tentang privasi data dalam Pertanyaan Umum Privasi Data. Lihat informasi tentang perlindungan data di Eropa di pos blog Model Tanggung Jawab Bersama dan GDPR AWS di Blog Keamanan AWS .

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

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan AWS sumber daya. Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail. Untuk informasi tentang penggunaan CloudTrail jejak untuk menangkap AWS aktivitas, lihat Bekerja dengan CloudTrail jejak di AWS CloudTrail Panduan Pengguna.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola tingkat lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-3 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi selengkapnya tentang titik akhir FIPS yang tersedia di Standar Pemrosesan Informasi Federal (FIPS) 140-3.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan Fleet Hub atau lainnya Layanan AWS menggunakan konsol, API AWS CLI, atau AWS SDKs. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan

atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

Enkripsi saat Istirahat

Fleet Hub melindungi data saat istirahat melalui enkripsi sisi server. Untuk informasi lebih lanjut, lihat Enkripsi data di AWS IoT di Panduan Developer AWS IoT .

Enkripsi bergerak

Dalam penyebaran arus cloud, Fleet Hub melindungi data dalam perjalanan dengan menggunakan protokol Transport Layer Security (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) adalah Layanan AWS yang membantu administrator mengontrol akses ke AWS sumber daya dengan aman. Administrator IAM mengontrol siapa yang dapat diautentikasi (masuk) dan diberi wewenang (memiliki izin) untuk menggunakan sumber daya Fleet Hub. IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

- Audiens
- Mengautentikasi dengan identitas
- Mengelola akses menggunakan kebijakan
- Bagaimana Fleet Hub for AWS IoT Device Management bekerja dengan IAM
- Contoh kebijakan berbasis identitas untuk Fleet Hub for AWS IoT Device Management
- Memecahkan masalah Fleet Hub for AWS IoT Device Management identitas dan akses

Audiens

Cara Anda menggunakan AWS 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 pekerjaan Anda, administrator Anda memberi Anda kredensi dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak fitur Fleet Hub untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara akses dikelola dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di Fleet Hub, lihatMemecahkan masalah Fleet Hub for AWS IoT Device Management identitas dan akses.

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 harus diakses pengguna layanan Anda. Kemudian, Anda harus mengirimkan permintaan kepada administrator IAM untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep dasar IAM. Untuk mempelajari lebih lanjut tentang bagaimana perusahaan Anda dapat menggunakan IAM dengan Fleet Hub, lihatBagaimana Fleet Hub for AWS IoT Device Management bekerja dengan IAM.

Administrator IAM - Jika Anda seorang administrator IAM, Anda mungkin ingin mempelajari detail tentang cara menulis kebijakan untuk mengelola akses ke Fleet Hub. Untuk melihat contoh kebijakan berbasis identitas Fleet Hub yang dapat Anda gunakan di IAM, lihat. Contoh kebijakan berbasis identitas untuk Fleet Hub for AWS IoT Device Management

Mengautentikasi dengan identitas

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

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

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

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara

kriptografis dengan menggunakan kredensil Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Guna mengetahui informasi selengkapnya tentang penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, lihat AWS Signature Version 4 untuk permintaan API dalam Panduan Pengguna IAM.

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

Akun AWS pengguna root

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

Identitas gabungan

Sebagai praktik terbaik, mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS dengan menggunakan kredensi sementara.

Identitas federasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, direktori Pusat Identitas AWS Directory Service, atau pengguna mana pun yang mengakses Layanan AWS dengan menggunakan kredensil yang disediakan melalui sumber identitas. Ketika identitas federasi mengakses Akun AWS, mereka mengambil peran, dan peran memberikan kredensyal sementara.

Untuk manajemen akses terpusat, kami sarankan Anda menggunakan AWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat Identitas IAM, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua aplikasi Akun AWS dan aplikasi Anda. Untuk informasi tentang Pusat Identitas IAM, lihat Apakah itu Pusat Identitas IAM? dalam Panduan Pengguna AWS IAM Identity Center .

Pengguna dan grup IAM

Pengguna IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, kami merekomendasikan untuk mengandalkan kredensial sementara, bukan membuat pengguna IAM yang memiliki kredensial jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan tertentu yang memerlukan kredensial jangka panjang dengan pengguna IAM, kami merekomendasikan Anda merotasi kunci akses. Untuk informasi selengkapnya, lihat Merotasi kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang dalam Panduan Pengguna IAM.

Grup IAM adalah identitas yang menentukan sekumpulan pengguna IAM. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat meminta kelompok untuk menyebutkan IAMAdmins dan memberikan izin kepada grup tersebut untuk mengelola sumber daya IAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari selengkapnya, lihat Kasus penggunaan untuk pengguna IAM dalam Panduan Pengguna IAM.

Peran IAM

Peran IAM adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Peran ini mirip dengan pengguna IAM, tetapi tidak terkait dengan orang tertentu. Untuk mengambil peran IAM sementara AWS Management Console, Anda dapat beralih dari pengguna ke peran IAM (konsol). Anda dapat mengambil peran dengan memanggil operasi AWS CLI atau AWS API atau dengan menggunakan URL kustom. Untuk informasi selengkapnya tentang cara menggunakan peran, lihat Metode untuk mengambil peran dalam Panduan Pengguna IAM.

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat Buat peran untuk penyedia identitas pihak ketiga dalam Panduan Pengguna IAM. Jika menggunakan Pusat Identitas IAM, Anda harus mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas

tersebut diautentikasi, Pusat Identitas IAM akan mengorelasikan set izin ke peran dalam IAM. Untuk informasi tentang set izin, lihat Set izin dalam Panduan Pengguna AWS IAM Identity Center .

- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM guna mendapatkan berbagai izin secara sementara untuk tugas tertentu.
- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (prinsipal tepercaya) di akun lain untuk mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM dalam Panduan Pengguna IAM.
- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Misalnya, saat Anda melakukan panggilan dalam suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.
  - Sesi akses teruskan (FAS) — Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses maju.
  - Peran layanan – Peran layanan adalah peran IAM yang dijalankan oleh layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Buat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.
  - Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke peran layanan. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.
- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan peran IAM untuk mengelola kredensi sementara untuk aplikasi yang berjalan pada EC2 instance dan membuat AWS CLI atau

AWS permintaan API. Ini lebih baik untuk menyimpan kunci akses dalam EC2 instance. Untuk menetapkan AWS peran ke EC2 instance dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instance berisi peran dan memungkinkan program yang berjalan pada EC2 instance untuk mendapatkan kredensyal sementara. Untuk informasi selengkapnya, lihat Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan di EC2 instans Amazon di Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izinnya. AWS mengevaluasi kebijakan ini ketika prinsipal (pengguna, pengguna root, atau sesi peran) membuat permintaan. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai 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 AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

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

Kebijakan IAM mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk melakukan operasinya. Misalnya, anggaplah Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan tersebut bisa mendapatkan informasi peran dari AWS Management Console, API AWS CLI, atau AWS API.

Kebijakan berbasis identitas

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

lihat Tentukan izin IAM kustom dengan kebijakan terkelola pelanggan dalam Panduan Pengguna IAM.

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan yang dikelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat Anda lampirkan ke beberapa pengguna, grup, dan peran dalam. Akun AWS Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan yang dikelola atau kebijakan inline, lihat Pilih antara kebijakan yang dikelola 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 kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Untuk sumber daya tempat kebijakan dilampirkan, kebijakan menentukan tindakan apa yang dapat dilakukan oleh prinsipal tertentu pada sumber daya tersebut dan dalam kondisi apa. Anda harus menentukan prinsipal dalam kebijakan berbasis sumber daya. Prinsipal dapat mencakup akun, pengguna, peran, pengguna federasi, atau. Layanan AWS

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

Daftar kontrol akses (ACLs)

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

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

Jenis-jenis kebijakan lain

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

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

dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batasan izin, lihat Batasan izin untuk entitas IAM dalam Panduan Pengguna IAM.

- Kebijakan kontrol layanan (SCPs) — SCPs adalah kebijakan JSON yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di. AWS Organizations AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur dalam suatu organisasi, maka Anda dapat menerapkan kebijakan kontrol layanan (SCPs) ke salah satu atau semua akun Anda. SCP membatasi izin untuk entitas di akun anggota, termasuk masing-masing. Pengguna root akun AWS Untuk informasi selengkapnya tentang Organizations dan SCPs, lihat Kebijakan kontrol layanan di Panduan AWS Organizations Pengguna.
- Kebijakan kontrol sumber daya (RCPs) — RCPs adalah kebijakan JSON yang dapat Anda gunakan untuk menetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda tanpa memperbarui kebijakan IAM yang dilampirkan ke setiap sumber daya yang Anda miliki. RCP membatasi izin untuk sumber daya di akun anggota dan dapat memengaruhi izin efektif untuk identitas, termasuk Pengguna root akun AWS, terlepas dari apakah itu milik organisasi Anda. Untuk informasi selengkapnya tentang Organizations dan RCPs, termasuk daftar dukungan Layanan AWS tersebut RCPs, lihat Kebijakan kontrol sumber daya (RCPs) di Panduan AWS Organizations Pengguna.
- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya, lihat Kebijakan sesi dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

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

Bagaimana Fleet Hub for AWS IoT Device Management bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke Fleet Hub, pelajari fitur IAM apa yang tersedia untuk digunakan dengan Fleet Hub.

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

Fitur IAM	Dukungan Fleet Hub
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
Kunci kondisi kebijakan	Ya
ACLs	Tidak
ABAC (tanda dalam kebijakan)	Ya
Kredensial sementara	Ya
Izin principal	Ya
Peran layanan	Ya
Peran terkait layanan	Tidak

Untuk mendapatkan tampilan tingkat tinggi tentang cara kerja Fleet Hub dan AWS layanan lainnya dengan sebagian besar fitur IAM, lihat AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM.

Kebijakan berbasis identitas untuk Fleet Hub

Mendukung kebijakan berbasis identitas: Ya

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang dapat Anda lampirkan ke sebuah identitas, seperti pengguna IAM, grup pengguna IAM, atau peran IAM. Kebijakan ini mengontrol jenis tindakan yang dapat dilakukan oleh pengguna dan peran, di sumber daya mana, dan berdasarkan kondisi seperti apa. Untuk mempelajari cara membuat kebijakan berbasis identitas, lihat Tentukan izin IAM kustom dengan kebijakan terkelola pelanggan dalam Panduan Pengguna IAM.

Dengan kebijakan berbasis identitas IAM, Anda dapat menentukan secara spesifik apakah tindakan dan sumber daya diizinkan atau ditolak, serta kondisi yang menjadi dasar dikabulkan atau ditolaknya tindakan tersebut. Anda tidak dapat menentukan secara spesifik prinsipal dalam sebuah kebijakan berbasis identitas karena prinsipal berlaku bagi pengguna atau peran yang melekat kepadanya. Untuk mempelajari semua elemen yang dapat Anda gunakan dalam kebijakan JSON, lihat Referensi elemen kebijakan JSON IAM dalam Panduan Pengguna IAM.

Contoh kebijakan berbasis identitas untuk Fleet Hub

Untuk melihat contoh kebijakan berbasis identitas Fleet Hub, lihat. Contoh kebijakan berbasis identitas untuk Fleet Hub for AWS IoT Device Management

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

Untuk mengaktifkan akses lintas akun, Anda dapat menentukan secara spesifik seluruh akun atau entitas IAM di akun lain sebagai prinsipal dalam kebijakan berbasis sumber daya. Menambahkan prinsipal akun silang ke kebijakan berbasis sumber daya hanya setengah dari membangun hubungan kepercayaan. Ketika prinsipal dan sumber daya berbeda Akun AWS, administrator IAM di akun tepercaya juga harus memberikan izin entitas utama (pengguna atau peran) untuk mengakses sumber daya. Mereka memberikan izin dengan melampirkan kebijakan berbasis identitas kepada

entitas. Namun, jika kebijakan berbasis sumber daya memberikan akses ke principal dalam akun yang sama, tidak diperlukan kebijakan berbasis identitas tambahan. Untuk informasi selengkapnya, lihat Akses sumber daya lintas akun di IAM dalam Panduan Pengguna IAM.

Tindakan kebijakan untuk Fleet Hub

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

Mendukung tindakan kebijakan: Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

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

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

Untuk melihat daftar tindakan Fleet Hub, lihat Tindakan yang ditentukan oleh Fleet Hub for AWS IoT Device Management dalam Referensi Otorisasi Layanan.

Tindakan kebijakan di Fleet Hub menggunakan awalan berikut sebelum tindakan:

```
iotfleethub
```

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

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

```
        ]
```

Untuk melihat contoh kebijakan berbasis identitas Fleet Hub, lihat. Contoh kebijakan berbasis identitas untuk Fleet Hub for AWS IoT Device Management

Sumber daya kebijakan untuk Fleet Hub

Mendukung sumber daya kebijakan: Ya

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

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

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

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

Untuk melihat daftar jenis sumber daya Fleet Hub dan jenisnya ARNs, lihat Sumber daya yang ditentukan oleh Fleet Hub for AWS IoT Device Management dalam Referensi Otorisasi Layanan. Untuk mempelajari tindakan yang dapat menentukan ARN setiap sumber daya, lihat Tindakan yang ditentukan oleh Fleet Hub for AWS IoT Device Management.

Untuk melihat contoh kebijakan berbasis identitas Fleet Hub, lihat. Contoh kebijakan berbasis identitas untuk Fleet Hub for AWS IoT Device Management

Kunci kondisi kebijakan untuk Fleet Hub

Mendukung kunci kondisi kebijakan khusus layanan: Yes

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen `Condition` (atau blok `Condition`) akan memungkinkan Anda menentukan kondisi yang menjadi dasar suatu pernyataan berlaku. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi bersyarat yang menggunakan operator kondisi, misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta.

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

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

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

Untuk melihat daftar kunci kondisi Fleet Hub, lihat Kunci kondisi untuk Fleet Hub for AWS IoT Device Management Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat Tindakan yang ditentukan oleh Fleet Hub for AWS IoT Device Management.

Untuk melihat contoh kebijakan berbasis identitas Fleet Hub, lihat. Contoh kebijakan berbasis identitas untuk Fleet Hub for AWS IoT Device Management

Daftar kontrol akses (ACLs) di Fleet Hub

Mendukung ACLs: Tidak

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

Kontrol akses berbasis atribut (ABAC) dengan Fleet Hub

Mendukung ABAC (tanda dalam kebijakan): Ya

Kontrol akses berbasis atribut (ABAC) adalah strategi otorisasi yang menentukan izin berdasarkan atribut. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke banyak AWS sumber daya. Penandaan ke entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian rancanglah kebijakan ABAC untuk mengizinkan operasi ketika tanda milik prinsipal cocok dengan tanda yang ada di sumber daya yang ingin diakses.

ABAC sangat berguna di lingkungan yang berkembang dengan cepat dan berguna di situasi saat manajemen kebijakan menjadi rumit.

Untuk mengendalikan akses berdasarkan tanda, berikan informasi tentang tanda di elemen kondisi dari kebijakan menggunakan kunci kondisi `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi untuk hanya beberapa jenis sumber daya, nilainya adalah Parsial.

Untuk informasi selengkapnya tentang ABAC, lihat Tentukan izin dengan otorisasi ABAC dalam Panduan Pengguna IAM. Untuk melihat tutorial yang menguraikan langkah-langkah pengaturan ABAC, lihat Menggunakan kontrol akses berbasis atribut (ABAC) dalam Panduan Pengguna IAM.

Menggunakan kredensyal Sementara dengan Fleet Hub

Mendukung kredensial sementara: Ya

Beberapa Layanan AWS tidak berfungsi saat Anda masuk menggunakan kredensi sementara. Untuk informasi tambahan, termasuk yang Layanan AWS bekerja dengan kredensi sementara, lihat Layanan AWS yang bekerja dengan IAM di Panduan Pengguna IAM.

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

Anda dapat membuat kredenal sementara secara manual menggunakan API AWS CLI atau AWS . Anda kemudian dapat menggunakan kredensyal sementara tersebut untuk mengakses. AWS AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensyal sementara alih-

alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat Kredensial keamanan sementara di IAM.

Izin utama lintas layanan untuk Fleet Hub

Mendukung sesi akses maju (FAS): Ya

Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat Sesi akses maju.

Peran layanan untuk Fleet Hub

Mendukung peran layanan: Ya

Peran layanan adalah peran IAM yang diambil oleh sebuah layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat Buat sebuah peran untuk mendelegasikan izin ke Layanan AWS dalam Panduan pengguna IAM.

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

Peran terkait layanan untuk Fleet Hub

Mendukung peran terkait layanan: Tidak

Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.

Untuk detail tentang pembuatan atau manajemen peran terkait layanan, lihat Layanan AWS yang berfungsi dengan IAM. Cari layanan dalam tabel yang memiliki `Yes` di kolom Peran terkait layanan. Pilih tautan Ya untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

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

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya Fleet Hub. Mereka juga tidak dapat melakukan tugas dengan menggunakan AWS Management Console, AWS Command Line Interface (AWS CLI), atau AWS API. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM dengan menggunakan contoh dokumen kebijakan JSON ini, lihat Membuat kebijakan IAM (konsol) di Panduan Pengguna IAM.

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh Fleet Hub, termasuk format ARNs untuk setiap jenis sumber daya, lihat Kunci tindakan, sumber daya, dan kondisi Fleet Hub for AWS IoT Device Management di Referensi Otorisasi Layanan.

Topik

- Praktik terbaik kebijakan
- Menggunakan konsol Fleet Hub
- Mengizinkan pengguna melihat izin mereka sendiri

Praktik terbaik kebijakan

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

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi

selengkapnya, lihat Kebijakan yang dikelola AWS atau Kebijakan yang dikelola AWS untuk fungsi tugas dalam Panduan Pengguna IAM.

- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat Kebijakan dan izin dalam IAM dalam Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat Elemen kebijakan JSON IAM: Kondisi dalam Panduan Pengguna IAM.
- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat Validasi kebijakan dengan IAM Access Analyzer dalam Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Anda, Akun AWS aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat Amankan akses API dengan MFA dalam Panduan Pengguna IAM.

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

Menggunakan konsol Fleet Hub

Untuk mengakses Fleet Hub for AWS IoT Device Management konsol, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang sumber daya Fleet Hub di tempat Anda Akun AWS. Jika Anda membuat kebijakan berbasis identitas

yang lebih ketat daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna atau peran) dengan kebijakan tersebut.

Anda tidak perlu mengizinkan izin konsol minimum untuk pengguna yang melakukan panggilan hanya ke AWS CLI atau AWS API. Sebagai gantinya, izinkan akses hanya ke tindakan yang sesuai dengan operasi API yang coba mereka lakukan.

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

Mengizinkan pengguna melihat izin mereka sendiri

Contoh ini menunjukkan cara membuat kebijakan yang mengizinkan pengguna IAM melihat kebijakan inline dan terkelola yang dilampirkan ke identitas pengguna mereka. Kebijakan ini mencakup izin untuk menyelesaikan tindakan ini di konsol atau menggunakan API atau secara terprogram. AWS CLI 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": "*"
        }
    ]
}
```

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

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

Topik

- Saya tidak berwenang untuk melakukan tindakan di Fleet Hub
- Saya tidak berwenang untuk melakukan iam: PassRole
- Saya ingin mengizinkan orang di luar AWS akun saya untuk mengakses sumber daya Fleet Hub saya

Saya tidak berwenang untuk melakukan tindakan di Fleet Hub

Jika AWS Management Console memberitahu Anda bahwa Anda tidak berwenang untuk melakukan suatu tindakan, maka Anda harus menghubungi administrator Anda untuk bantuan. Administrator Anda adalah orang yang memberi Anda kredensial masuk.

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

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 berwenang untuk melakukan iam: PassRole

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

Beberapa Layanan AWS memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

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

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

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

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

Saya ingin mengizinkan orang di luar AWS akun saya untuk mengakses sumber daya Fleet Hub saya

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

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mengetahui apakah Fleet Hub mendukung fitur ini, lihatBagaimana Fleet Hub for AWS IoT Device Management bekerja dengan IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh sumber daya Akun AWS yang Anda miliki, lihat Menyediakan akses ke pengguna IAM di pengguna lain Akun AWS yang Anda miliki di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda kepada pihak ketiga Akun AWS, lihat Menyediakan akses yang Akun AWS dimiliki oleh pihak ketiga dalam Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat Menyediakan akses ke pengguna terautentikasi eksternal (federasi identitas) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara menggunakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Akses sumber daya lintas akun di IAM di Panduan Pengguna IAM.

Validasi kepatuhan untuk Fleet Hub untuk Manajemen AWS IoT Perangkat

Auditor pihak ketiga menilai keamanan dan kepatuhan Fleet Hub sebagai bagian dari beberapa program AWS kepatuhan. Program ini mencakup SOC, PCI, FedRAMP, HIPAA, dan lainnya.

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

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

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

- Kepatuhan dan Tata Kelola Keamanan – Panduan implementasi solusi ini membahas pertimbangan arsitektur serta memberikan langkah-langkah untuk menerapkan fitur keamanan dan kepatuhan.
- Referensi Layanan yang Memenuhi Syarat HIPAA — Daftar layanan yang memenuhi syarat HIPAA. Tidak semua memenuhi Layanan AWS syarat HIPAA.

- AWS Sumber Daya AWS — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- AWS Panduan Kepatuhan Pelanggan - Memahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan Layanan AWS dan memetakan panduan untuk kontrol keamanan di berbagai kerangka kerja (termasuk Institut Standar dan Teknologi Nasional (NIST), Dewan Standar Keamanan Industri Kartu Pembayaran (PCI), dan Organisasi Internasional untuk Standardisasi (ISO)).
- Mengevaluasi Sumber Daya dengan Aturan dalam Panduan AWS Config Pengembang — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub— Ini Layanan AWS memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS. Security Hub menggunakan kontrol keamanan untuk sumber daya AWS Anda serta untuk memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat Referensi kontrol Security Hub.
- Amazon GuardDuty — Ini Layanan AWS mendeteksi potensi ancaman terhadap beban kerja Akun AWS, kontainer, dan data Anda dengan memantau lingkungan Anda untuk aktivitas mencurigakan dan berbahaya. GuardDuty dapat membantu Anda mengatasi berbagai persyaratan kepatuhan, seperti PCI DSS, dengan memenuhi persyaratan deteksi intrusi yang diamanatkan oleh kerangka kerja kepatuhan tertentu.
- AWS Audit ManagerIni Layanan AWS membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

Ketahanan di Hub Armada untuk Manajemen Perangkat AWS IoT

Infrastruktur AWS global dibangun di sekitar AWS Wilayah dan Zona Ketersediaan. AWS Wilayah menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang serta mengoperasikan aplikasi dan basis data yang secara otomatis melakukan fail over di antara zona tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur pusat data tunggal atau multi tradisional.

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

AWS kebijakan terkelola untuk Fleet Hub untuk Manajemen AWS IoT Perangkat

Untuk menambahkan izin ke pengguna, grup, dan peran, lebih mudah menggunakan kebijakan AWS terkelola daripada menulis kebijakan sendiri. Dibutuhkan waktu dan keahlian untuk membuat kebijakan yang dikelola pelanggan IAM yang hanya memberi tim Anda izin yang mereka butuhkan. Untuk memulai dengan cepat, Anda dapat menggunakan kebijakan AWS terkelola kami. Kebijakan ini mencakup kasus penggunaan umum dan tersedia di AWS akun Anda. Untuk informasi selengkapnya tentang kebijakan AWS AWS terkelola, lihat kebijakan terkelola di Panduan Pengguna IAM.

AWS layanan memelihara dan memperbarui kebijakan AWS terkelola. Anda tidak dapat mengubah izin dalam kebijakan AWS terkelola. 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 dari kebijakan AWS terkelola, sehingga pembaruan kebijakan tidak akan merusak izin yang ada.

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

AWS kebijakan terkelola: AWSIo TFleet HubFederationAccess

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

Kebijakan ini memberikan izin kepada pengguna federasi Fleet Hub for AWS IoT Device Management yang mereka perlukan untuk mengambil tindakan AWS IoT dan AWS layanan lainnya dari aplikasi web Fleet Hub.

Untuk informasi selengkapnya tentang menambahkan pengguna ke aplikasi web Fleet Hub, lihat???.

Lihat kebijakan ini di AWS konsol.

Detail izin

Kebijakan ini mencakup izin berikut:

- `iot`- Ambil data AWS IoT perangkat dan lakukan tindakan tingkat armada.
- `iotfleethub`- Ambil metadata aplikasi Fleet Hub.
- `cloudwatch`- Ambil CloudWatch alarm dan data metrik. Juga memungkinkan membuat dan menghapus tindakan yang tercakup ke alarm Fleet Hub.
- `sns`- Lakukan operasi membuat, membaca, menghapus, berlangganan, dan berhenti berlangganan. Operasi ini mencakup topik SNS Fleet Hub.

JSON

```
{
    "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 Hub ke kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk Fleet Hub sejak layanan ini mulai melacak perubahan ini. Untuk informasi selengkapnya, lihat halaman riwayat Dokumentasi Fleet Hub.

Perubahan	Deskripsi	Tanggal
AWSIoTFleetHubFederationAccess — Permbaruan ke kebijakan yang sudah ada	Fleet Hub menambahkan izin baru untuk memungkinkan pengguna aplikasi mengambil data AWS IoT Device Defender metrik di aplikasi Fleet Hub.	4 April 2022
AWSIoTFleetHubFederationAccess – Pembaruan ke kebijakan yang ada	Fleet Hub menambahkan izin baru untuk memungkinkan pengguna aplikasi mengambil sumber data tambahan untuk pengindeksan. Izin juga ditambahkan untuk memungkinkan pengguna aplikasi membatalkan eksekusi AWS IoT pekerjaan di dalam aplikasi.	15 November 2021
AWSIoTFleetHubFederationAccess – Pembaruan ke kebijakan yang ada	Fleet Hub menambahkan izin baru bagi pengguna aplikasi untuk mengambil data Thing Group dan melakukan operasi CRUD pada pekerjaan. AWS IoT	24 Mei 2021

Perubahan	Deskripsi	Tanggal
AWSIoTFleetHubFederationAccess – Pembaruan ke kebijakan yang ada	Fleet Hub menghapus izin untuk dasbor Fleet Hub yang tidak didukung. APIs	12 April 2021
AWSIoTFleetHubFederationAccess – Kebijakan baru	Fleet Hub menambahkan kebijakan baru yang memberikan izin yang diperlukan bagi pengguna aplikasi Fleet Hub untuk mengambil data perangkat dan melakukan tindakan. AWS IoT	12 April 2021
Fleet Hub mulai melacak perubahan	Fleet Hub mulai melacak perubahan untuk kebijakan yang AWS dikelola.	12 April 2021

Keamanan infrastruktur di Fleet Hub untuk Manajemen AWS IoT Perangkat

Sebagai layanan terkelola, Fleet Hub for AWS IoT Device Management dilindungi oleh prosedur keamanan jaringan AWS global yang dijelaskan dalam whitepaper Amazon Web Services: Overview of Security Processes.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses Fleet Hub melalui jaringan. Klien harus mendukung Keamanan Lapisan Pengangkutan (TLS) 1.2 atau versi yang lebih baru. Kami merekomendasikan menggunakan TLS 1.3. Klien juga harus mendukung cipher suite 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 ID kunci akses dan kunci akses rahasia yang terkait dengan prinsipal IAM. Atau Anda dapat menggunakan AWS Security Token Service (AWS STS) untuk menghasilkan kredensial keamanan sementara untuk menandatangani permintaan.

Pencegahan "confused deputy" lintas layanan

Masalah "confused deputy" adalah masalah keamanan saat entitas yang tidak memiliki izin untuk melakukan suatu tindakan dapat memaksa entitas yang memilik hak akses lebih tinggi untuk melakukan tindakan tersebut. Pada tahun AWS, peniruan lintas layanan dapat mengakibatkan masalah wakil yang membingungkan. Peniruan identitas lintas layanan dapat terjadi ketika satu layanan (layanan yang dipanggil) memanggil layanan lain (layanan yang dipanggil). Layanan panggilan dapat dimanipulasi untuk menggunakan izinnya untuk bertindak atas sumber daya pelanggan lain dengan cara yang seharusnya tidak memiliki izin untuk mengakses. Untuk mencegah hal ini, AWS menyediakan alat yang membantu Anda melindungi data untuk semua layanan dengan principal layanan yang telah diberi akses ke sumber daya di akun Anda.

Untuk membatasi izin yang diberikan Fleet Hub layanan lain ke sumber daya, sebaiknya gunakan kunci konteks kondisi `aws:SourceAccount`global `aws:SourceArn`dan global dalam kebijakan sumber daya. Jika Anda menggunakan kedua kunci konteks kondisi global, `aws:SourceAccount` nilai dan akun dalam `aws:SourceArn` nilai harus menggunakan ID akun yang sama saat digunakan dalam pernyataan kebijakan yang sama.

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

Contoh berikut menunjukkan cara mencegah masalah deputi yang membingungkan dengan menggunakan kunci konteks kondisi `aws:SourceArn` dan `aws:SourceAccount` global dalam kebijakan kepercayaan peran Fleet Hub. Untuk menemukan ARN peran Fleet Hub Anda, buka bagian Fleet Hub di AWS IoT konsol dan pilih aplikasi Fleet Hub Anda untuk melihat halaman detail aplikasi.

JSON

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

Hub Armada end-of-life (EOL) FAQs

Hub Armada end-of-life FAQs

- Kapan Fleet Hub pergi end-of-life?
- Apa yang terjadi pada aplikasi Fleet Hub saya pada end-of-life tanggal tersebut?
- Apa yang terjadi pada AWS sumber daya dasar saya pada dan setelah end-of-life tanggal?
- Bagaimana cara menghapus aplikasi Fleet Hub sebelum end-of-life tanggal?
- Akankah menghapus aplikasi Fleet Hub secara otomatis menghapus sumber daya yang mendasarinya?
- Bagaimana cara menghapus AWS sumber daya dasar saya?
- APIsMana yang tidak lagi berfungsi pada dan setelah end-of-life tanggal?
- Apa saja fungsi Fleet Hub yang ada dan bagaimana cara mengaksesnya di konsol?

Kapan Fleet Hub pergi end-of-life?

AWS akan menghentikan Fleet Hub for AWS IoT Device Management pada 18 Oktober 2025. Fleet Hub akan bertransisi ke EOL dalamnya secara bertahap. Fungsionalitas yang tersedia dari Fleet Hub juga tersedia di dalam AWS IoT Device Management konsol untuk terus mendukung kebutuhan bisnis Anda.

1. Pada 17 Oktober 2024, AWS akan menghentikan orientasi pelanggan baru ke Fleet Hub. Jika Anda tidak memiliki aplikasi Fleet Hub sebelum 17 Oktober 2024, Anda diidentifikasi sebagai pelanggan Fleet Hub baru. Jika tidak, Anda diidentifikasi sebagai pelanggan Fleet Hub yang ada.
2. Pelanggan Fleet Hub yang ada dapat terus menggunakan aplikasi Fleet Hub hingga 17 Oktober 2025. Dari 17 Oktober 2024 hingga 17 Oktober 2025, tidak akan ada pembaruan fitur baru untuk Fleet Hub dan AWS akan mendukung perbaikan bug kritis.
3. Pada 18 Oktober 2025, AWS akan menghentikan dukungan untuk Fleet Hub for AWS IoT Device Management. Pada tanggal ini, Fleet Hub akan mencapainya end-of-life dan Anda tidak akan lagi dapat menggunakan Fleet Hub. Penghentian Fleet Hub tidak memengaruhi kemampuan lainnya AWS IoT Device Management . Anda dapat terus menggunakan fungsionalitas yang ada yang disediakan oleh AWS IoT Device Management. Untuk informasi selengkapnya, lihat ???.

Apa yang terjadi pada aplikasi Fleet Hub saya pada end-of-life tanggal tersebut?

Pada EOL tanggal 18 Oktober 2025, aplikasi Fleet Hub Anda akan dihapus dan Anda tidak lagi dapat mengakses Fleet Hub. AWS Sumber daya Anda yang terkait dengan Fleet Hub tidak akan dihapus secara otomatis. Sumber daya ini mencakup AWS IoT Device Management pekerjaan, komponen alarm Fleet Hub seperti metrik AWS IoT Device Management armada, CloudWatch alarm, dan topik AmazonSNS. Anda dapat terus mengakses sumber daya ini secara independen dari AWS Management Console, AWS CLI, atau AWS SDK untuk kebutuhan pemantauan Anda. Untuk menghapus AWS sumber daya dasar Anda, lihat???.

Apa yang terjadi pada AWS sumber daya dasar saya pada dan setelah end-of-life tanggal?

Anda dapat terus mengakses AWS sumber daya dasar yang terkait dengan Fleet Hub secara independen dari AWS Management Console kebutuhan pemantauan Anda. Sumber daya ini mencakup AWS IoT Device Management pekerjaan, komponen alarm Fleet Hub seperti metrik AWS IoT Device Management armada, CloudWatch alarm, dan topik AmazonSNS. Pengguna aplikasi Fleet Hub ditugaskan sendiri dari kumpulan pengguna Pusat IAM Identitas Anda. Jika pengguna Pusat IAM Identitas Anda dibuat semata-mata untuk mengakses aplikasi Fleet Hub dan Anda tidak menggunakannya untuk AWS layanan lain, Anda dapat menghapusnya dari tab pengguna dan aplikasi di Pusat IAM Identitas dalam konsol. Untuk informasi selengkapnya, lihat ???.

Bagaimana cara menghapus aplikasi Fleet Hub sebelum end-of-life tanggal?

Untuk menghapus aplikasi Fleet Hub sebelum EOL tanggal, gunakan AWS IoT konsol atau `--delete-application` AWS CLI perintah.

> **Note**
>
> Menghapus aplikasi Fleet Hub tidak akan menghapus AWS sumber daya dasar yang terkait dengan Fleet Hub. Untuk menghapus sumber daya ini, lihat the section called “Bagaimana cara menghapus AWS sumber daya dasar saya?”

Untuk menghapus aplikasi Fleet Hub menggunakan AWS IoT konsol, ikuti langkah-langkahnya.

1. Buka AWS IoT konsol, dari navigasi kiri, pilih Fleet Hub, lalu pilih Aplikasi.
2. Pada halaman Aplikasi, pilih aplikasi Fleet Hub yang ingin Anda hapus. Pilih Hapus. Anda akan melihat jendela prompt yang meminta konfirmasi Anda untuk menghapus aplikasi. Masukkan “hapus” untuk mengonfirmasi penghapusan, lalu pilih hapus.

Untuk menghapus aplikasi Fleet Hub menggunakan AWS CLI, ikuti langkah-langkahnya.

1. Untuk menghapus aplikasi Fleet Hub Anda menggunakan AWS CLI, Anda perlu mengetahui ID aplikasi. Jalankan `--list-applications`CLIperintah terlebih dahulu untuk mencantumkan semua aplikasi Fleet Hub Anda dan aplikasinyaIDs.

   Untuk membuat daftar aplikasi Fleet Hub Anda dengan aplikasi merekaIDs, jalankan perintah berikut.

   ```
   aws iotfleethub --list-applications --region us-west-2
   ```

   Output dari perintah dapat terlihat seperti berikut.

   ```
   {
    "applicationSummaries": [
     {
      "applicationId": "68d0603a-66c9-43bf-b93f-a90e7ee5cf76",
      "applicationName": "test_app1",
      "applicationUrl": "https://12ad0603a-66c9-43bf-b93f-
   a90e7ee5cf76.app.iotfleethub.aws",
      "applicationCreationDate": 1698174116,
      "applicationLastUpdateDate": 1698174117,
      "applicationState": "ACTIVE"
     },
     {
      "applicationId": "b6198497-cd5b-400c-9b82-1c82b69cb66c",
      "applicationName": "test_app2",
      "applicationUrl": "https://c6198490-
   cd5a-400c-9b82-1c82b69cb66c.app.iotfleethub.aws",
      "applicationCreationDate": 1684355213,
      "applicationLastUpdateDate": 1684355214,
      "applicationState": "ACTIVE"
     }
   ```

```
 ]
}
```

2. Untuk menghapus aplikasi Fleet Hub Anda, jalankan AWS CLI perintah berikut.

```
aws iotfleethub --delete-application --application-id b6198497-
cd5b-400c-9b82-1c82b69cb66c --region us-west-2
```

Perintah tidak menghasilkan output. Anda dapat menjalankan `--list-applications` CLI perintah untuk memeriksa apakah aplikasi yang ditentukan telah dihapus atau tidak.

Akankah menghapus aplikasi Fleet Hub secara otomatis menghapus sumber daya yang mendasarinya?

Tidak. Menghapus aplikasi Fleet Hub tidak akan secara otomatis menghapus sumber daya yang mendasarinya. Untuk menghapus AWS sumber daya yang terkait dengan Fleet Hub, lihat???.

Bagaimana cara menghapus AWS sumber daya dasar saya?

Fleet Hub memungkinkan pelanggan untuk membuat AWS sumber daya seperti AWS IoT Device Management pekerjaan dan alarm Fleet Hub. Menghapus aplikasi Fleet Hub tidak menghapus sumber daya ini, dan Anda dapat terus mengaksesnya untuk mendukung kebutuhan bisnis Anda seperti yang dijelaskan dalam???. Untuk menghapus sumber daya dasar ini, ikuti langkah-langkah di bawah ini.

Bagaimana cara menghapus pekerjaan?

Untuk menghapus pekerjaan, Anda harus membatalkan pekerjaan terlebih dahulu. Anda dapat membatalkan pekerjaan langsung dari Fleet Hub sebelum EOL tanggal. Anda juga dapat menggunakan AWS IoT konsol untuk membatalkan dan menghapus pekerjaan kapan pun Anda mau.

Untuk membatalkan pekerjaan dari aplikasi Fleet Hub Anda

1. Buka aplikasi Fleet Hub Anda, pilih tab Pekerjaan.
2. Pilih pekerjaan yang ingin Anda batalkan.
3. Pilih Batalkan pekerjaan.

Untuk membatalkan dan menghapus pekerjaan dari AWS IoT konsol

1. Pergi ke Tindakan jarak jauh, pilih tab Pekerjaan.
2. Pilih pekerjaan yang ingin Anda batalkan.
3. Pilih Batalkan.
4. Pada tab Jobs yang sama, pilih pekerjaan yang ingin Anda hapus.
5. Pilih Hapus.

Bagaimana cara menghapus alarm Fleet Hub?

Anda dapat menghapus alarm Fleet Hub langsung di dalam aplikasi Fleet Hub. Ini akan secara otomatis menghapus semua komponen yang mendasarinya seperti metrik armada, CloudWatch alarm, dan topik AmazonSNS. Di aplikasi Fleet Hub Anda, navigasikan ke tab alarm Fleet Hub, pilih alarm yang ingin Anda hapus dan pilih Hapus. Atau, Anda dapat menghapus alarm Fleet Hub menggunakan AWS Management Console. Anda mungkin ingin mengikuti langkah-langkah ini untuk menghapus beberapa aplikasi di seluruh AWS wilayah.

Untuk menghapus alarm Fleet Hub dari aplikasi Fleet Hub

1. Di aplikasi Fleet Hub, navigasikan ke tab alarm Fleet Hub.
2. Pilih alarm yang ingin Anda hapus dan pilih Hapus. Tindakan ini akan menghapus semua komponen yang mendasarinya.

Untuk menghapus metrik armada dari konsol AWS IoT

1. Pergi ke Kelola dari navigasi kiri dari AWS IoT konsol. Dari Semua perangkat, pilih Metrik Armada.
2. Pilih semua metrik armada yang namanya diawali dengan “iotfleethub”.
3. Pilih Hapus.

Untuk menghapus CloudWatch alarm dari konsol CloudWatch

1. Buka tab Semua alarm di dalam CloudWatch konsol.
2. Pilih semua metrik yang namanya diawali dengan “iotfleethub”.
3. Buka Tindakan dan pilih Hapus.

Untuk menghapus SNS topik Amazon yang menerima alarm yang dibuat dari konsol Amazon SNS

1. Buka tab Topik dalam SNS konsol Amazon.
2. Pilih semua topik yang namanya diawali dengan “iotfleethub”.
3. Pilih Hapus.

Bagaimana cara menghapus pengguna Pusat IAM Identitas yang dibuat dari Fleet Hub?

Jika pengguna Pusat IAM Identitas Anda dibuat semata-mata untuk mengakses aplikasi Fleet Hub dan Anda tidak menggunakannya untuk AWS layanan lain, Anda dapat menghapusnya dari tab pengguna dan aplikasi di Pusat IAM Identitas dalam konsol.

APIsMana yang tidak lagi berfungsi pada dan setelah end-of-life tanggal?

Kami akan menghentikan semua yang APIs terkait dengan manajemen siklus hidup aplikasi Fleet Hub pada 18 Oktober 2025. Perhatikan bahwa APIs ini hanya terkait dengan Fleet Hub dan tidak memengaruhi AWS IoT Device Management fungsi lainnya. Pelanggan Fleet Hub yang ada dapat terus menggunakan ini APIs hingga 17 Oktober 2025.

- CreateApplication
- DeleteApplication
- DescribeApplication
- ListApplication
- ListTagsForResource
- TagResource
- UntagResource
- UpdateApplication

Apa saja fungsi Fleet Hub yang ada dan bagaimana cara mengaksesnya di konsol?

Fleet Hub menawarkan fungsionalitas pemantauan dan manajemen utama berikut yang dibangun menggunakan AWS IoT Device Management fitur. Semua kemampuan ini tersedia di luar aplikasi Fleet Hub. Mereka langsung berada di dalam AWS IoT Device Management konsol yang dapat terus Anda akses untuk mendukung kebutuhan bisnis Anda.

Ringkasan status konektivitas armada

Dasbor Fleet Hub merangkum status konektivitas armada IoT Anda dengan detail konektivitas. Ini menunjukkan jumlah perangkat yang terhubung, terputus dan distribusi perangkat yang terputus dengan alasan pemutusan. Dasbor pemantauan status konektivitas yang setara tersedia di AWS IoT konsol di bawah tab Monitor. Anda dapat mengaktifkan widget untuk memantau jumlah perangkat yang terhubung, tingkat pemutusan dan alasan pemutusan di sana. Untuk informasi selengkapnya, lihat AWS IoT Device Management menambahkan dasbor pemantauan metrik konektivitas terpadu.

Alarm Hub Armada

Alarm Fleet Hub memungkinkan Anda membuat dan memantau alarm berbasis ambang batas. Alarm Fleet Hub memanfaatkan metrik armada yang disediakan oleh pengindeksan AWS IoT Device Management armada dan alarm Amazon. CloudWatch Anda dapat langsung memantau metrik armada ini di CloudWatch konsol Amazon dan mengkonfigurasi ulang mereka di AWS IoT konsol. Metrik armada dan CloudWatch alarm yang namanya diawali dengan 'iotfleethub' dikaitkan dengan Fleet Hub. Anda dapat terus mengaksesnya dari konsol. Anda dapat menggunakan Amazon CloudWatch untuk memantau metrik ini dari waktu ke waktu dan melihat tren. Anda juga dapat membuat metrik armada tambahan dari AWS IoT konsol lalu memantaunya dan mengatur alarm di Amazon. CloudWatch Untuk informasi selengkapnya, lihat Melihat metrik armada di CloudWatch.

Pencarian perangkat

Fleet Hub memungkinkan Anda menerapkan beberapa filter menggunakan kriteria dari sumber data yang diindeks untuk menyempurnakan pencarian perangkat Anda. Fitur ini memanfaatkan fungsi pencarian pengindeksan armada. Pencarian perangkat tersedia untuk digunakan langsung melalui AWS IoT Device Management konsol, dari halaman pencarian hal lanjutan. Untuk menemukan halaman pencarian Advanced thing, pilih Things from Manage, lalu pilih All devices. Pilih Pencarian lanjutan di sudut kanan atas halaman Things.

Eksekusi Job

Anda dapat menjalankan pekerjaan langsung dari Fleet Hub dengan memilih sesuatu atau grup sebagai target. Anda juga dapat menjalankan pekerjaan dari halaman Pekerjaan di AWS IoT Device Management Konsol, di mana Anda dapat menentukan sesuatu, grup statis, atau grup dinamis sebagai target pelaksanaan pekerjaan.

Tampilan detail perangkat

Fleet Hub menyediakan tampilan detail tingkat perangkat (benda) dari halaman Semua Perangkat. Tampilan detail tingkat perangkat serupa tersedia langsung dari tab Things di dalam AWS IoT Device Management Konsol, atau dengan mengklik hal tertentu yang ditampilkan melalui hasil kueri penelusuran pengindeksan armada.

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.

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 pratinjau Hub Armada untukAWS IoTManajemen Perangkat Panduan Pengguna.	16 Desember 2020.