Guide de gestion de Fleet Hub pour les AWS IoT appareils

Fleet Hub pour la gestion des AWS IoT appareils

Fleet Hub pour la gestion des AWS IoT appareils: Guide de gestion de Fleet Hub pour les AWS IoT appareils

Table of Contents

AWS supprimera la fonctionnalité AWS IoT Device Management Fleet Hub le 18 octobre 2025 et n'accepte plus de nouveaux clients. Les clients existants de AWS IoT Device Management Fleet Hub pourront utiliser Fleet Hub jusqu'au 17 octobre 2025. Pour plus d'informations, consultez Fleet Hub end-of-life (EOL). FAQs

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.

Qu'est-ce que Fleet Hub pour la gestion des AWS IoT appareils ?

Avec Fleet Hub pour la gestion des AWS IoT appareils (Fleet Hub), vous pouvez créer des applications Web autonomes pour surveiller l'état de santé de vos flottes d'appareils. Vous pouvez mettre ces applications à la disposition des utilisateurs de votre organisation, même s'ils n'ont pas de AWS compte. Utilisez le Hub de Flotte pour gérer les tâches courantes à l'échelle de la flotte, telles que l'investigation et la résolution des problèmes opérationnels et de sécurité.

le Hub de Flotte fournit les fonctionnalités suivantes.

- Surveillez les flottes d'appareils en temps quasi-réel.
- Définissez des alertes pour informer vos techniciens en cas de comportement inhabituel.
- Exécution de tâches

> **Note**
>
> Pour que Fleet Hub puisse indexer les données d'état de connectivité, vos objets doivent se connecter AWS IoT Core avec un identifiant client égal au nom de l'objet.

Comment fonctionne Fleet Hub pour la gestion des AWS IoT appareils

Les administrateurs peuvent utiliser Fleet Hub pour la gestion des AWS IoT appareils afin de créer des applications Web sécurisées en quelques minutes sans fournir de ressources ni écrire de code. Les applications Web que vous créez à l'aide de le Hub de Flotte s'intègrent à vos systèmes d'identité existants, tels qu'Active Directory. Cela permet à vos administrateurs d'appliquer leurs propres modèles d'authentification et d'autorisation.

Les applications Web Fleet Hub s'intègrent à l'indexation des AWS IoT Core flottes et à la surveillance des appareils. Ces intégrations permettent de surveiller les données de santé des appareils et de créer des alarmes lorsque les appareils de votre parc atteignent un état spécifié.

Les applications le Hub de Flotte utilisent la politique `AWSIoTFleetHubFederationAccess` gérée. Pour de plus amples informations, veuillez consulter ???.

Exemples de cas d'utilisation :

- Visualisez les problèmes de connectivité des appareils : vous pouvez voir le nombre d'appareils déconnectés de votre parc, l'état de la dernière connexion d'un appareil et la ou les raisons pour lesquelles les appareils se sont déconnectés.
- Définissez des alarmes : vous pouvez définir des seuils qui déclenchent des alarmes lorsqu'un certain nombre d'appareils se déconnectent. Les alarmes peuvent également vous avertir lorsqu'un ou plusieurs appareils se déconnectent pour une raison particulière. Vous pouvez ensuite consulter les données détaillées de l'appareil pour étudier et résoudre les problèmes.
- Exécuter des tâches : vous pouvez exécuter des opérations à distance (telles que des mises à jour du microprogramme) sur un ou plusieurs appareils.

Comment fonctionne l'indexation des données de le Hub de Flotte

Vous pouvez utiliser la console le Hub de Flotte pour activer l'indexation du parc de votre parc d'appareils. Lorsque vous activez l'indexation de flotte dans le Hub de Flotte, vous l'activez pour l'ensemble de la flotte et vous la rendez disponible pour toutes les applications le Hub de Flotte.

Lorsqu'elle est activée, l'indexation du parc indexe automatiquement tous les champs AWS IoT Core gérés. Vous pouvez également utiliser l'indexation de flotte pour ajouter des données personnalisées que vous pouvez utiliser pour interroger et agréger des données dans les applications le Hub de Flotte.

Comment fonctionnent les alarmes le Hub de Flotte

Les applications Web le Hub de Flotte fournissent une interface qui permet à vos utilisateurs de créer des alarmes. Les étapes suivantes montrent comment les utilisateurs créent des alarmes dans le Hub de Flotte.

1. Créez une requête pour agréger les données : spécifiez une requête qui regroupe les appareils que vos utilisateurs souhaitent cibler à l'aide de champs consultables.
2. Configurer le seuil - Définissez un seuil qui déclenche les alarmes lorsqu'une condition des données indexées (telle que l'état de connectivité sur un intervalle spécifié) est atteinte.
3. Configurer la notification - Spécifiez un groupe de destinataires que le Hub de Flotte avertit lorsque les appareils spécifiés sont en état d'alarme.

Comment fonctionnent les jobs de le Hub de Flotte

Vous pouvez utiliser la console le Hub de Flotte pour exécuter des opérations à distance sur des appareils.

Lorsque les modèles de tâches sont activés, vous pouvez créer des tâches spécifiques à partir des modèles de vos applications le Hub de Flotte.

Fleet Hub pour la gestion des AWS IoT appareils pour les administrateurs

Cette section contient des instructions destinées aux administrateurs sur la façon de créer et de gérer les applications Web Fleet Hub pour la gestion des AWS IoT appareils.

Rubriques

Premiers pas

Cette section explique comment créer et configurer Fleet Hub pour les applications Web de gestion des AWS IoT appareils.

Rubriques

Création de votre première application Fleet Hub

Prérequis

La liste suivante contient les ressources dont vous avez besoin pour créer une application Web Fleet Hub.

- Un compte AWS.
- AWS IAM Identity Centeractivé pour votre compte. (Si vous n'avez pas encore activé ce service, la AWS IoT Core console (https://console.aws.amazon.com/iot/) vous invite à le faire.)

Créez votre première application Web Fleet Hub

Les étapes suivantes décrivent comment créer des applications Web Fleet Hub pour la gestion des AWS IoT appareils.

1. Accédez à la AWS IoT Core console (https://console.aws.amazon.com/iot/), puis dans le panneau de gauche, choisissez Fleet Hub, puis Applications.
2. Dans la page Applications, choisissez Create application.(Créer une application).
3. Sur la page Configurer le centre d'identité IAM, si vous n'avez pas activé AWS IAM Identity Center (IAM Identity Center), suivez les étapes pour l'activer. AWS Organizations vous envoie un e-mail. Cliquez sur le lien contenu dans l'e-mail pour terminer l'activation d'IAM Identity Center.

   > **Note**
   >
   > Vous pouvez connecter votre propre fournisseur d'identité à IAM Identity Center. Pour plus d'informations, voir Qu'est-ce que c'est AWS IAM Identity Center ? et connectez-vous à votre fournisseur d'identité externe.
   > Lorsque vous créez une application Fleet Hub, vous devez créer une instance d'organisation d'IAM Identity Center si vous n'en avez pas déjà une. L'application Fleet Hub que vous créez doit également se trouver dans la même instance Région AWS d'organisation qu'IAM Identity Center. Pour plus d'informations, voir Activation des instances d'IAM Identity Center et d'organisation d'IAM Identity Center.

   La page vous indique si vous avez déjà activé IAM Identity Center.

   Choisissez Suivant.
4. Sur la page AWS IoT des données de l'index, consultez les informations de la section Comment fonctionne le flux de données depuis et AWS IoT vers Fleet Hub. Cette page vous renvoie aux pages de la AWS IoT Core console où vous pouvez activer et gérer l'indexation du AWS IoT Core parc de véhicules. Vous pouvez utiliser ce service pour indexer, rechercher et agréger vos données de registre, vos données d'ombre, vos données de connectivité des appareils (événements du cycle de vie des appareils) et vos données de violations des appareils. Vous pouvez également créer des champs personnalisés en plus des champs gérés que l'indexation des AWS IoT Core flottes indexe par défaut.

- Si vous avez activé l'indexation de flotte, cette page affiche les paramètres d'indexation de votre flotte et les champs personnalisés.

- Si vous n'avez pas activé l'indexation des objets et la connectivité des objets, vous devez le faire pour utiliser Fleet Hub.

Lorsque vous avez terminé de gérer et de revoir les paramètres d'indexation de votre flotte, choisissez Next.

Pour plus d'informations sur la façon d'activer l'indexation de flotte pour les applications Fleet Hub, voir Gestion de l'indexation de flotte pour les applications Fleet Hub.

5. Sur la page Configurer l'application, dans la section Rôle de l'application, créez un nouveau rôle de service ou sélectionnez un rôle de service existant. Votre application Web Fleet Hub assume ce rôle lorsqu'elle utilise les ressources de Fleet Hub. Les utilisateurs fédérés disposent des mêmes autorisations que le rôle lorsqu'ils utilisent l'application Web.

   - Si vous créez un nouveau rôle, le nom du rôle doit commencer par la chaîne suivante : `AWSIotFleetHub_`*`random_string`*.

   - Si vous sélectionnez un rôle existant, assurez-vous qu'il dispose des autorisations indiquées dans le document de stratégie. Pour voir les autorisations dont votre application Web Fleet Hub a besoin, choisissez Afficher les détails du rôle. Une fenêtre s'ouvre et indique le document de politique que le service applique à tout nouveau rôle que vous créez à partir de cette page.

6. Sur la page Configurer l'application, dans la section Propriétés de l'application, entrez le nom de votre application. En option, vous pouvez également saisir une description.

   Choisissez Créer une application.

7. Sous l'onglet Applications choisissez l'application que vous avez créée dans , puis choisissez Afficher les détails.. Vérifiez les détails de la demande.

> **Note**
>
> Pour plus d'informations sur les solutions possibles pour résoudre les problèmes en tant qu'administrateur de Fleet Hub, consultez la section Résolution des problèmes.

Gérez l'indexation du parc pour les applications Fleet Hub

Vous pouvez utiliser la AWS IoT Core console ou le AWS CLI pour activer l'indexation du parc et configurer les sources de données suivantes à indexer : données de AWS IoT registre, données AWS IoT Device Shadow, données de AWS IoT connectivité et données de AWS IoT Device Defender violations. Les étapes suivantes décrivent comment activer l'indexation de flotte pour Fleet Hub pour les applications de gestion des AWS IoT appareils dans AWS IoT Core la console. Pour consulter les étapes d'utilisation AWS CLI, reportez-vous à la section Gestion de l'indexation des objets.

> **Important**
>
> Le 20 juillet 2022 est la version de disponibilité générale de l'intégration de l'indexation du parc de AWS IoT dispositifs de gestion des appareils avec des ombres AWS IoT Core nommées et de la AWS IoT Device Defender détection des violations. Avec cette version GA, vous pouvez indexer des shadows nommées spécifiques en spécifiant les noms des shadows. Si vous avez ajouté vos shadows nommées pour l'indexation pendant la période de préversion publique de cette fonctionnalité, du 30 novembre 2021 au 19 juillet 2022, nous vous encourageons à reconfigurer les paramètres d'indexation de votre flotte et à choisir des noms shadows spécifiques pour réduire les coûts d'indexation et optimiser les performances. Pour plus d'informations sur la façon de reconfigurer les paramètres d'indexation de votre flotte, consultez la section Gestion de l'indexation de la flotte.

1. Accédez à la AWS IoT Core console (https://console.aws.amazon.com/iot/), puis dans le panneau de gauche, sélectionnez Paramètres.
2. Sur la page Paramètres, accédez à la section Indexation de la flotte, puis choisissez Gérer l'indexation.
3. Sur la page Gérer l'indexation du parc, dans la section Configuration, choisissez l'indexation des objets et les sources de données que vous souhaitez AWS IoT indexer. Vous devez activer l'indexation et la connectivité des objets pour utiliser Fleet Hub.

4. (Facultatif) Sur la page Gérer l'indexation de la flotte, dans la section Champs personnalisés pour l'agrégation-facultatif, créez des champs personnalisés en plus des champs gérés que l'indexation du parc indexe par défaut.

   Lorsque vous avez terminé de gérer et de revoir les paramètres d'indexation de votre flotte, choisissez Next.

   L'indexation de la flotte peut prendre un certain temps pour mettre à jour les paramètres. Pour plus d'informations sur la gestion de l'indexation de la flotte, consultez la section Gestion de l'indexation de la flotte.

Ajouter des utilisateurs aux applications Fleet Hub

Votre application Web Fleet Hub for AWS IoT Device Management ne contient aucun utilisateur lorsqu'elle vient d'être créée. Vous devez ajouter des utilisateurs avant que vous et les membres de votre organisation puissiez utiliser l'application. Les étapes décrites dans cette rubrique décrivent comment ajouter des utilisateurs à votre application.

Vous pouvez ajouter des utilisateurs à partir de votre système d'identité existant en configurant AWS IAM Identity Center (IAM Identity Center) pour votre compte. Vous pouvez connecter votre propre fournisseur d'identité à IAM Identity Center. Pour plus d'informations, consultez What Is IAM Identity Center?.

1. Sur la page Applications, choisissez votre application Web dans la liste des applications Fleet Hub. Sélectionnez Afficher les détails.
2. Sur la page Application details, choisissez .
3. Dans la fenêtre Ajouter des utilisateurs de Fleet Hub, sélectionnez les utilisateurs de votre organisation auxquels vous souhaitez avoir accès à l'application. Choisissez Ajouter les utilisateurs sélectionnés.
4. Sur la page des détails de l'application, vérifiez que les utilisateurs que vous avez sélectionnés figurent dans la liste des utilisateurs de Fleet Hub.

AWS et AWS IoT Core des services qui interagissent avec Fleet Hub pour la gestion des AWS IoT appareils

Cette rubrique explique comment les fonctionnalités de Fleet Hub pour la gestion des AWS IoT appareils interagissent avec d'autres AWS services afin de fournir les fonctionnalités de vos applications Web Fleet Hub.

Le tableau suivant indique les AWS services utilisés par Fleet Hub for AWS IoT Device Management pour implémenter chaque fonctionnalité.

Capacité	AWS service	Description
Intégrez les systèmes d'identité existants, tels qu'Active Directory.	AWS IAM Identity Center (Centre d'identité IAM)	Vous pouvez ajouter des utilisateurs à partir de votre système d'identité existant en configurant AWS IAM Identity Center (IAM Identity Center) pour votre compte. Vous pouvez connecter votre propre fournisseur d'identité à IAM Identity Center. Pour plus d'informations, consultez Qu'est-ce que AWS IAM Identity Center? et les identités du personnel.
Créez des requêtes en utilisant des champs AWS gérés, des champs personnalisés et tous les attributs de vos sources de données indexées.	AWS IoT indexation de la flotte	Utilisez le service d'indexation de la flotte pour indexer, rechercher et agréger vos données de registre, vos données d'ombre et vos données de connectivité des appareils (événements du cycle de vie des appareils). Vous pouvez également créer des champs personnalisés

Capacité	AWS service	Description
		pour l'agrégation en plus des champs gérés que l'indexation des AWS IoT flottes indexe par défaut. Pour plus d'informations sur l'indexation des flottes, consultez la section Indexation de la flotte.

Capacité	AWS service	Description
Créez des alarmes pour un ensemble d'appareils spécifiés par une requête.	Amazon CloudWatch (CloudWatch)	Les tableaux de bord de Fleet Hub CloudWatch présentent des indicateurs que vous pouvez utiliser en combinaison avec des champs consultables pour créer des seuils alarmants. Par exemple, vous pouvez créer une CloudWatch alarme qui génère une notification Amazon Simple Notification Service (Amazon SNS) chaque fois que le nombre d'appareils connectés est inférieur à une quantité spécifiée. Pour plus d'informations CloudWatch, consultez Qu'est-ce qu'Amazon CloudWatch ? Pour plus d'informations sur la façon dont AWS IoT Core fonctionne la création CloudWatch de métriques et d'alarmes, voir Surveiller les AWS IoT alarmes et les métriques à l'aide de CloudWatch.

Résolution des problèmes

Cette section fournit des informations de dépannage et des solutions possibles pour aider à résoudre les problèmes en tant qu'administrateur du Fleet Hub.

Symptôme	Solution
Le lien vers mon application Web ne fonctionne pas.	Après la création de votre application, quelques heures peuvent s'écouler avant que le lien ne s'affiche.
Je n'arrive pas à me connecter à mon application Web.	Vérifiez que vous avez ajouté au moins un utilisateur à votre application. Assurez-vous que votre rôle repose sur la relation de confiance appropriée, telle que la suivante : JSON `{"Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "Service": "iotfleethub.amazonaws.com" }, "Action": "sts:AssumeRole" } ] }` Pour plus d'informations sur la modification de la relation de confiance IAM, consultez Modification de la relation d'approbation pour un rôle existant.
Je ne parviens pas à créer une application Web.	Assurez-vous que vous n'avez pas atteint la limite du nombre total d'applications Web.
Je ne vois pas le champ personnalisé auquel je m'attendais.	Vérifiez que vous avez correctement configuré l'indexation du parc.

Symptôme	Solution
	Pour plus d'informations sur l'indexation des flottes, consultez la section Indexation des flottes.

Fleet Hub pour la gestion des AWS IoT appareils pour les utilisateurs

Cette section contient des informations destinées aux utilisateurs des applications Web de gestion des AWS IoT appareils Fleet Hub. Pour plus d'informations sur la création d'applications Hub de flotte et sur l'ajout d'utilisateurs, consultez Fleet Hub pour la gestion des AWS IoT appareils pour les administrateurs.

Rubriques

Premiers pas

Cette section contient des informations sur la manière de commencer à utiliser les fonctionnalités de Fleet Hub pour les applications Web de gestion des AWS IoT appareils.

Rubriques

Création de votre premier rôle

Cette rubrique explique les étapes à suivre pour créer une requête Fleet Hub simple pour la gestion des AWS IoT appareils. Les requêtes sont spécifiées à l'aide d'une syntaxe de requête.

Prérequis

- Une application Fleet Hub associée à un AWS IoT Core compte contenant des appareils (objets).

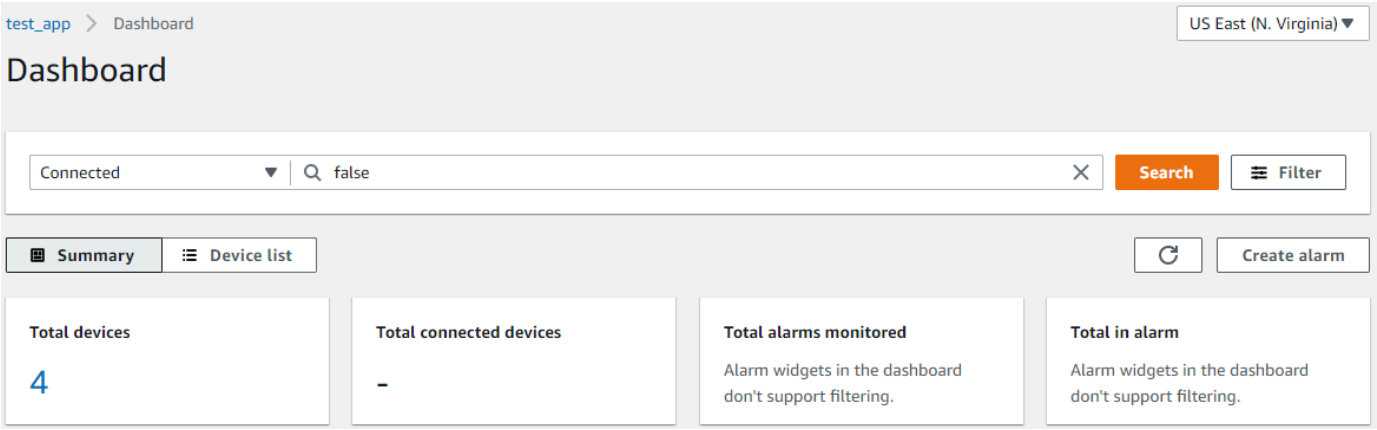
- Un compte de votre organisation autorisé à utiliser l'application Fleet Hub.

Création de votre première requête sur Fleet Hub

Création de votre première requête sur Fleet Hub

1. Accédez à votre application Fleet Hub.

   La vue du tableau de bord par défaut affiche une liste de tous les appareils contenant les attributs gérés et personnalisés. Les attributs contenant le préfixe d'attributs sont des attributs personnalisés.
2. Dans le menu en haut de la page, choisissez Connected depuis All fields. Entrez **`false`** dans la zone de texte à côté du menu déroulant.



3. Pour effectuer la recherche, choisissez Rechercher. La liste de tous les appareils auxquels vous n'êtes pas connectés s'affiche AWS IoT Core.

Pour plus d'informations sur la syntaxe des requêtes et des exemples de requêtes, consultez les rubriques Syntaxe des requêtes, Exemples de requêtes d'objets et Exemples de requêtes de groupes d'objets.

Création de votre premier alarme

Cette rubrique explique les étapes à suivre pour créer une alarme Fleet Hub pour la gestion des AWS IoT appareils simple.

Prérequis

- Une application Fleet Hub associée à un AWS IoT Core compte contenant des appareils (objets).

- Un compte de votre organisation autorisé à utiliser l'application Fleet Hub.

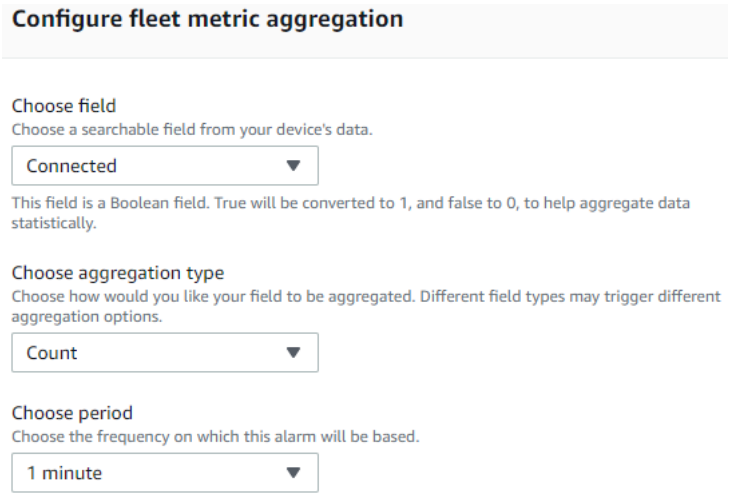
Création de votre première alarme

Création de votre première alarme Fleet Hub

1. Accédez à votre application Fleet Hub.
2. Si vous souhaitez cibler un ensemble spécifique d'appareils, créez une requête. Pour obtenir des instructions sur la création d'une rubrique, consultez the section called “Création de votre premier rôle”. Si vous ne créez pas de requête, votre alarme s'appliquera à tous les appareils de votre parc.
3. Sur la page du tableau de bord par défaut, choisissez Créer une alarme.
4. Sur la page Créer une métrique d'agrégation, vérifiez que votre requête apparaît sous Requête cible. Dans la section Configurer l'agrégation des métriques du parc, dans le menu Choisir un champ, choisissez Connecté. Ce champ AWS géré indique si un appareil est connecté à AWS IoT Core. Le menu Choisir un champ contient les champs AWS gérés et les champs personnalisés que votre administrateur a créés dans le cadre de l'indexation de la AWS IoT flotte.
5. Pour Choisir le type d'agrégation, choisissez l'une des options suivantes.

   - Maximum -- Configurez un seuil maximum.
   - Nombre -- Configurez un nombre spécifique comme seuil.
   - Somme -- configurez une somme comme seuil.
   - Minimum -- configurez un seuil minimum.
   - Moyenne -- Configurez un seuil moyen.
6. Pour Choisir une période, choisissez la durée de la condition spécifiée dans les menus précédents qui déclenchera l'alarme.

   Voici un exemple de paramètre pour Configurer l'agrégation des métriques de flotte :



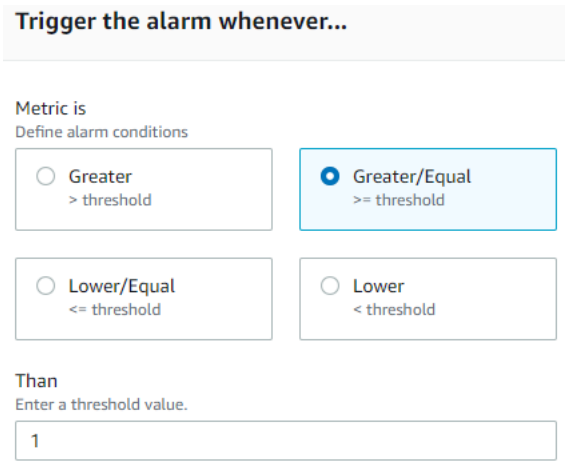
Choisissez Suivant.

7. Sur la page Définir le seuil, dans la section Déclencher l'alarme chaque fois que... section, choisissez l'une des options suivantes.

   - Plus grand -- alarmes lorsque la métrique et le type d'agrégation dépassent la valeur spécifiée.
   - Supérieur/Égal -- alarmes lorsque la métrique et le type d'agrégation sont égaux ou supérieurs à la valeur spécifiée.
   - Plus faible -- alarmes lorsque la métrique et le type d'agrégation tombent en dessous de la valeur spécifiée.
   - Inférieur/égal -- alarme lorsque la métrique et le type d'agrégation sont égaux ou inférieurs à la valeur spécifiée.

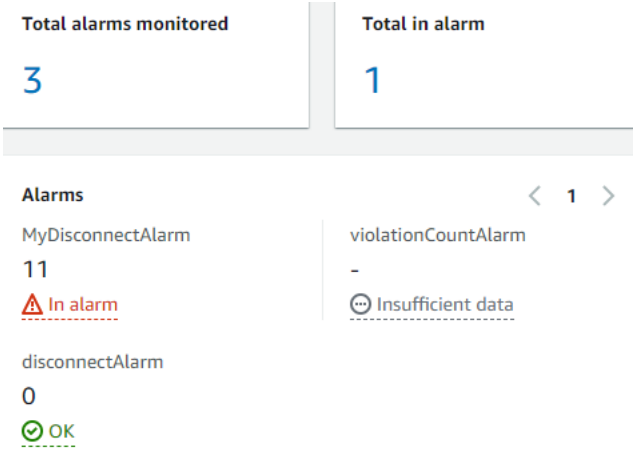
8. Dans la zone de texte Than, spécifiez la valeur à utiliser comme seuil pour l'alarme.

   Par exemple, le paramètre Set threshold peut ressembler à ce qui suit :

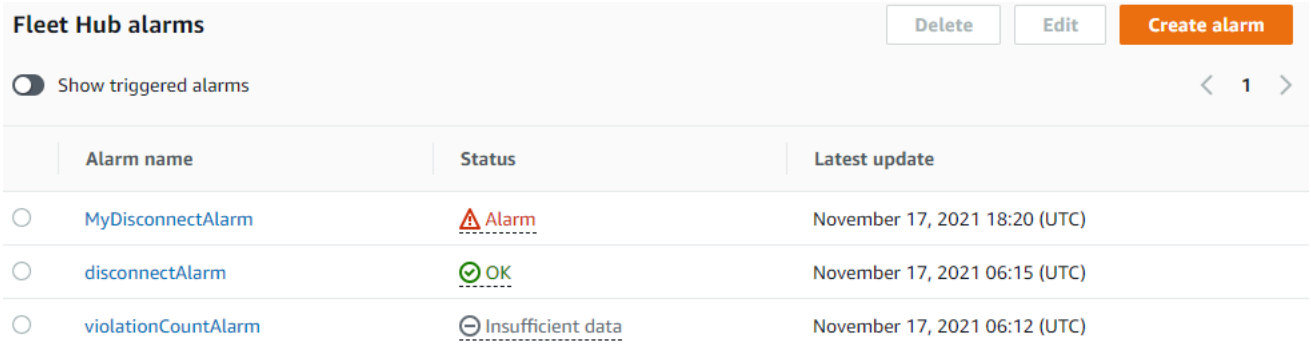


Choisissez Suivant.

9. Sur la page Notifier l'utilisateur, dans la section Notifier -- facultatif, entrez le nom de la liste d'e-mails contenant les utilisateurs de votre organisation qui reçoivent des notifications lorsque l'alarme est active. Entrez une liste d'adresses e-mail séparées par des virgules pour remplir cette liste.
10. Dans la section Détails de l'alarme, entrez le nom de votre alarme, et entrez éventuellement une description de votre alarme. Choisissez Suivant.
11. Sur la page Reviser, passez en revue les informations que vous avez saisies ou sélectionnées sur les pages précédentes. Sélectionnez Envoyer. Vous revenez au tableau de bord par défaut.
12. Sur le tableau de bord par défaut, les widgets d'alarmes affichent les informations de toutes les alarmes que vous avez créées.



Pour voir le détail des alarmes que vous avez créées, dans le panneau de navigation de gauche, sélectionnez les alarmes Fleet Hub.



Afficher les détails des appareils

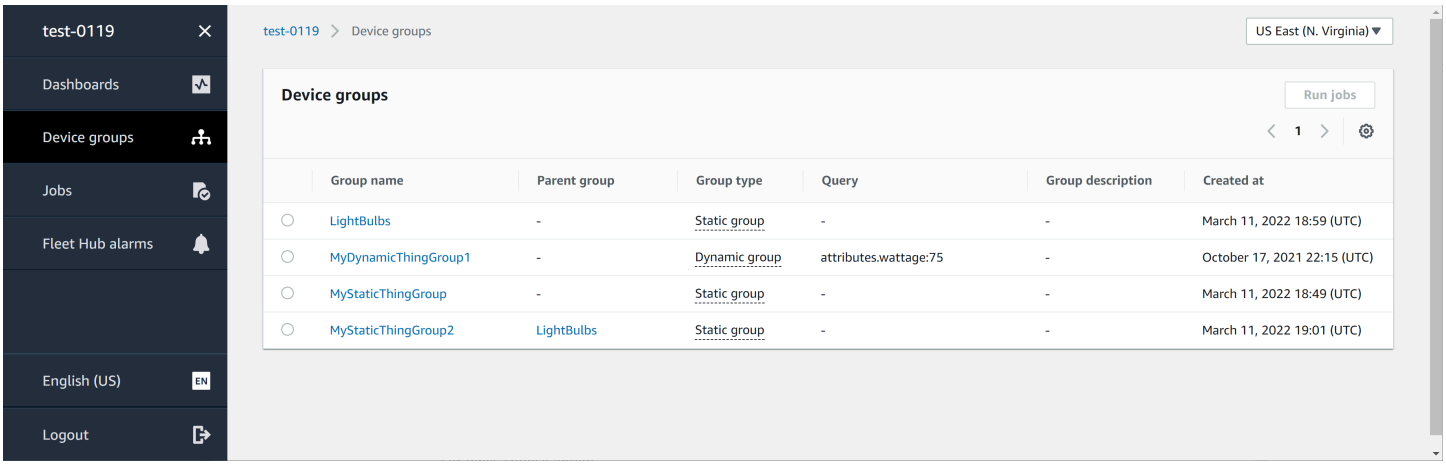
Cette rubrique explique les étapes à suivre pour afficher les informations relatives à vos groupes d'appareils et à vos appareils.

Prérequis

- Une application Fleet Hub associée à un AWS IoT Core compte contenant des appareils (objets).
- Un compte de votre organisation autorisé à utiliser l'application Fleet Hub.

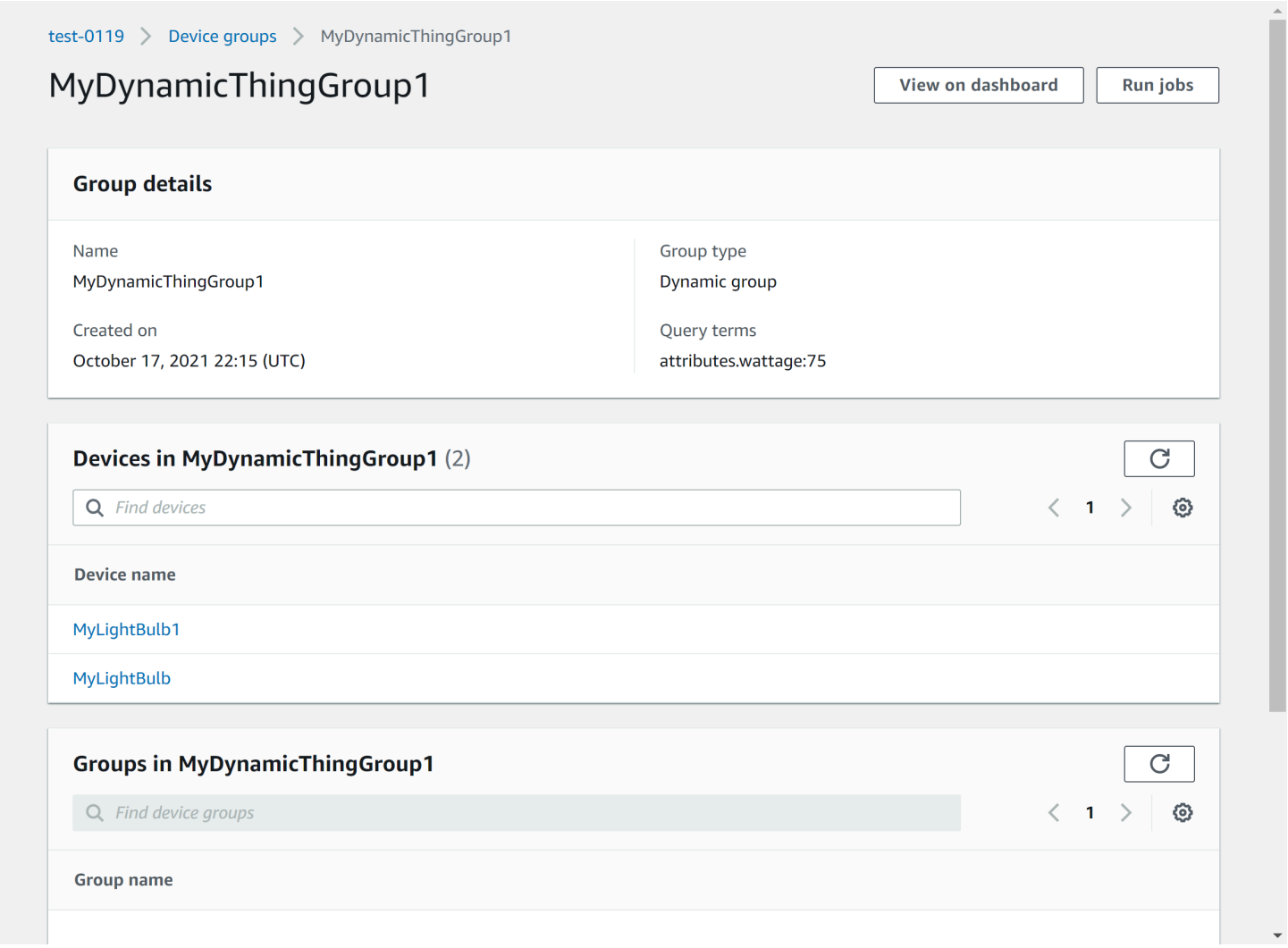
Groupes d'appareils

Lorsque vous vous connectez à votre application Web Fleet Hub, des Groupes d'appareils s'affichent dans le panneau de navigation de gauche. La page Groupes d'appareils répertorie tous les groupes d'appareils de votre application Web Fleet Hub. Pour afficher les détails d'un groupe d'appareils, choisissez un groupe d'appareils spécifique dans la colonne Nom du groupe.



Détails du groupe d'appareils

La page de détails du groupe d'appareils contient des informations sur le groupe d'appareils que vous avez sélectionné. Pour afficher les détails d'un appareil, choisissez-en un spécifique dans la colonne Nom de l'appareil de la ***XXX*** section Appareils.



Détails de l'appareil

La page Détails de l'appareil contient des informations sur l'appareil sélectionné.

> **Note**
>
> Si votre client utilise un identifiant client différent de celui de Thing Name lorsqu'il se connecte AWS IoT, l'état de connectivité de votre « objet » ne sera pas indexé par Fleet Indexing.

Détails

La section Détails contient les informations suivantes concernant votre appareil :

- Nom de l'appareil – le nom de la ressource de objet qui représente votre appareil. Pour plus d'informations, consultez Comment gérer les éléments avec le registre.

- Type d'objet – type d'objet associé à votre appareil. Vous pouvez utiliser le type d'objet pour stocker des informations communes à tous les objets du même type. Pour plus d'informations, consultez la section Types d'objet.

- Horodatage de la dernière connexion : date à laquelle votre appareil s'est connecté pour la dernière fois à. AWS IoT

- Lien vers un appareil partageable – un lien partageable qui pointe vers la page de détails de l'appareil sélectionné.

- État de la dernière connexion : état de connexion de votre appareil à AWS IoT. Si votre appareil est connecté, la valeur est `true`. S'il n'est pas connecté, la valeur est `false`.

- Motif de la déconnexion – La raison pour laquelle votre appareil est déconnecté.

Données déclarées

La section Données signalées contient des informations sur les données de registre, les données d'ombre de l'appareil et les groupes d'objets.

- Champs de l'appareil : champs indexés de votre appareil dans l'indexation du AWS IoT parc. Pour de plus amples informations, veuillez consulter Managing fleet indexing (Gestion de l'indexation de la flotte.

- Ombres de l'appareil – ombres associées à votre appareil. Les ombres de l'appareil peuvent inclure à la fois des ombres classiques anonymes et des ombres nommées. Pour plus d'informations, consultez AWS IoT Device Shadows.

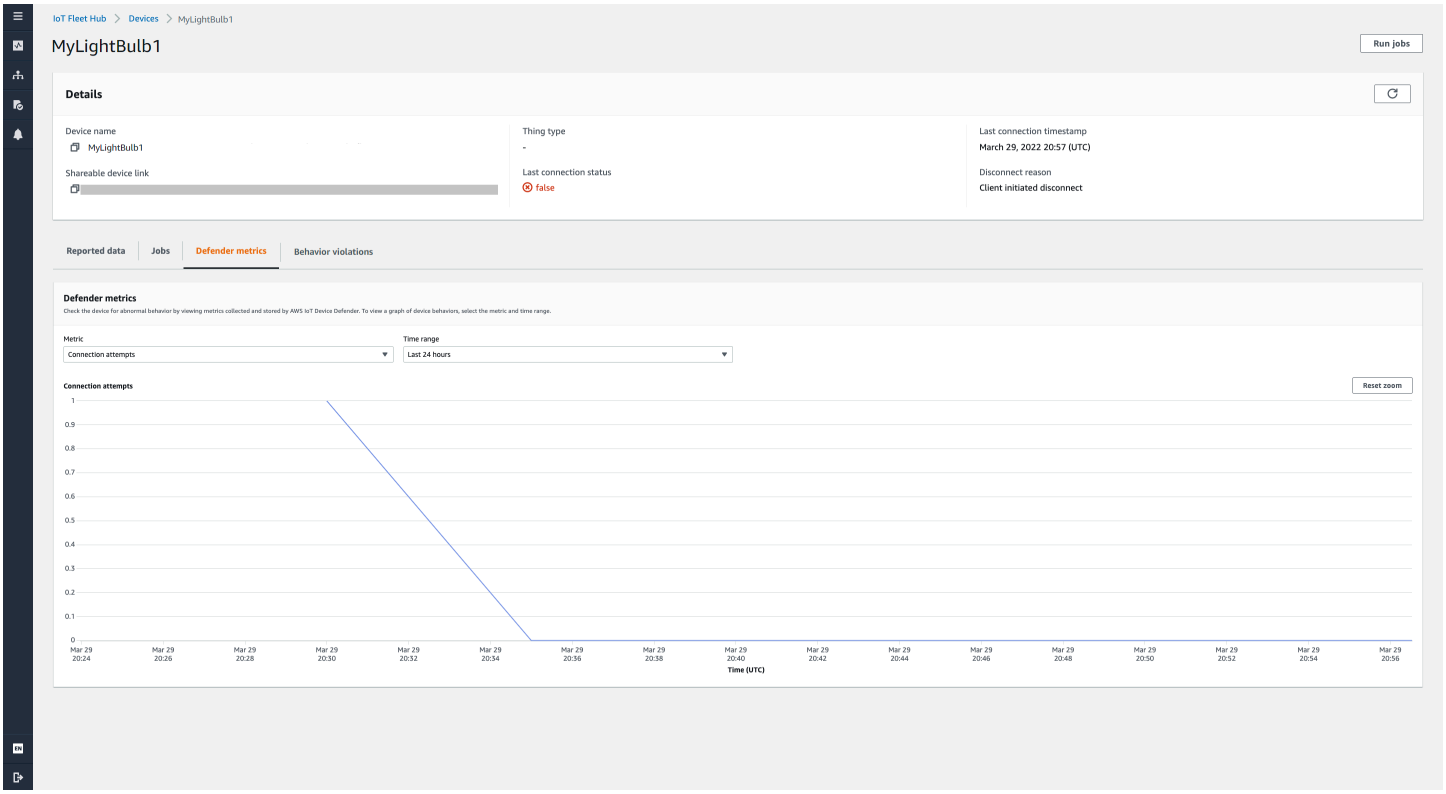
- Groupes d'appareils – Le groupes d'appareils associés à votre appareil. Les groupes d'appareils peuvent inclure à la fois des groupes d'objets statiques et des groupes d'objets dynamiques. Pour de plus amples informations sur les groupes d'objets, veuillez consulter Groupes d'objets statiques dans le .

Tâches

La section Tâches affiche toutes les tâches exécutées sur l'appareil. Chaque tâche possède une page de détails qui affiche des informations récapitulatives sur la tâche, y compris les informations relatives à la cible et à l'exécution. Pour plus d'informations, voir Utilisation des tâches et des modèles de tâches dans Fleet Hub pour la gestion des AWS IoT appareils, et Tâches.

Métriques du défenseur

La section des statistiques de Defender affiche les AWS IoT Device Defender statistiques associées à l'appareil actuellement sélectionné. Vous pouvez utiliser les données de mesure affichées pour visualiser le fonctionnement de votre appareil sur une période de votre choix. Pour consulter les données des métriques du défenseur depuis votre application Fleet Hub, votre administrateur Fleet Hub doit d'abord configurer les AWS IoT Device Defender métriques associées à l'appareil sélectionné. Pour plus d'informations sur la façon de créer et de configurer AWS IoT Device Defender des métriques pour vos appareils, consultez les rubriques Mesures personnalisées, Mesures côté appareil et Mesures côté cloud.



Violations de comportement

La section Violations comportementales affiche les données indexées de AWS IoT Device Defender détection des violations associées à l'appareil actuellement sélectionné. Les données relatives aux

violations de comportement peuvent inclure le nombre de violations, l'heure de la dernière violation et la valeur métrique de la dernière violation. Pour consulter les données relatives aux violations de comportement depuis votre application Fleet Hub, votre administrateur Fleet Hub doit configurer les violations de AWS IoT Device Defender comportement dans un profil de sécurité et configurer les AWS IoT Device Defender violations dans l'indexation de flotte. Pour plus d'informations sur la configuration des violations de comportement dans un profil AWS IoT Device Defender de sécurité, consultez la section AWS IoT Device Defender Détecter. Pour plus d'informations sur la configuration des AWS IoT Device Defender violations, consultez Gérer l'indexation de flotte pour les applications Fleet Hub et Gestion de l'indexation des objets.

Requêtes et filtres

Vous pouvez utiliser Fleet Hub pour les requêtes de gestion des AWS IoT appareils afin de créer et de consulter des listes d'éléments de votre parc d'appareils. Tous les champs AWS gérés, les champs personnalisés et tous les attributs de vos sources de données indexées sont disponibles sous forme de filtres de requête. Vous pouvez également créer des champs personnalisés pour activer l'agrégation à l'aide the section called “Alertes” de l'indexation de AWS IoT flotte. Pour plus d'informations sur l'indexation des flottes, consultez la section Indexation des flottes.

Rubriques

- Affichez le tableau de bord
- Création de requêtes à l'aide de filtres

Affichez le tableau de bord

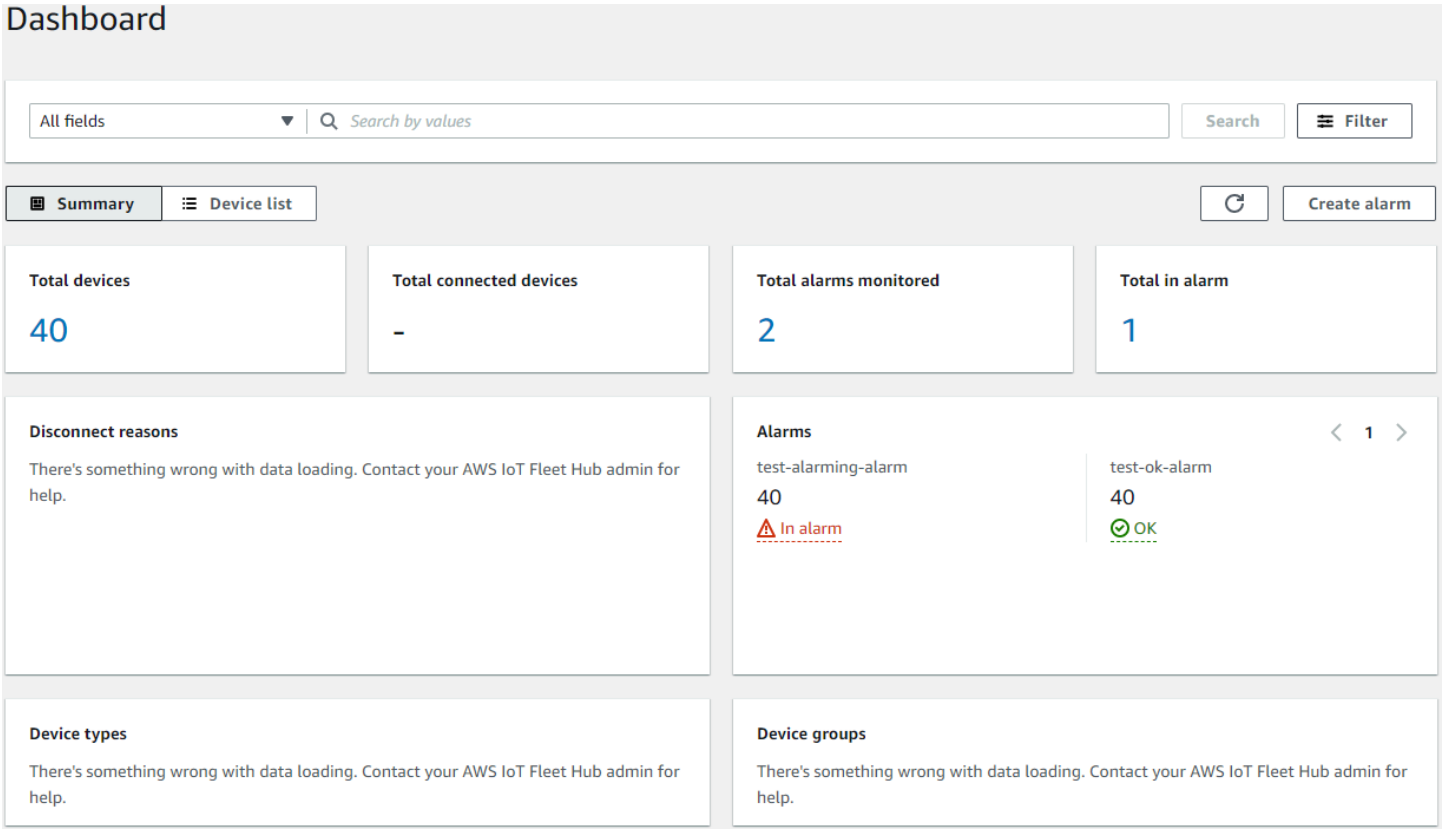
Lorsque vous vous connectez à votre application Web Fleet Hub pour la gestion des AWS IoT appareils, vous voyez un tableau de bord qui présente deux vues des données relatives aux appareils de votre flotte.

Récapitulatif

La vue récapitulative affiche une vue cumulée des données relatives à tous les appareils de votre parc. Il fournit les informations suivantes.

- Nombre total d’appareil
- Nombre d'appareils connectés

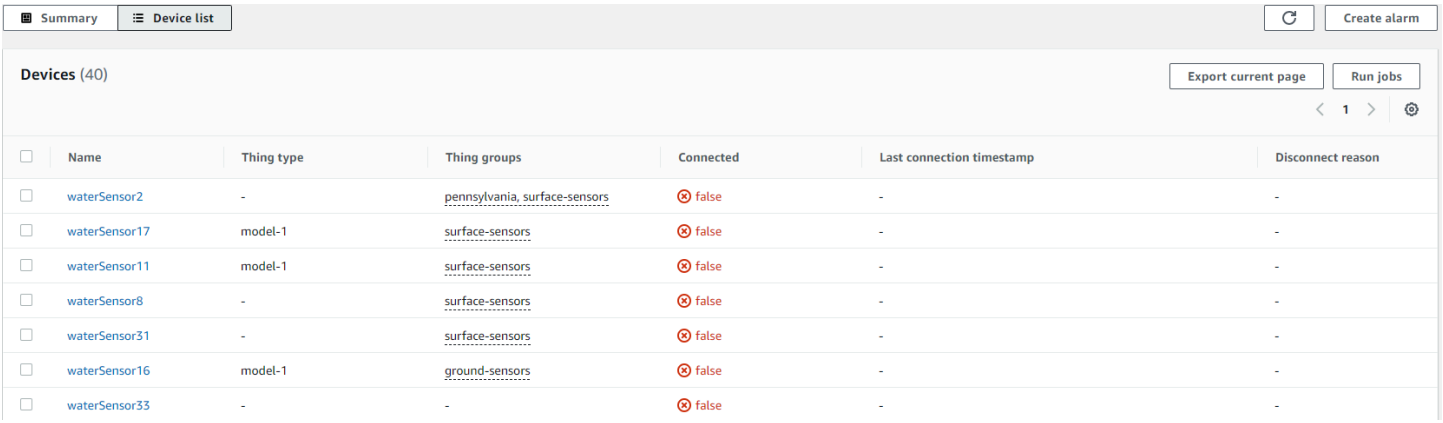
- Liste des raisons pour lesquelles les appareils se sont déconnectés
- Les types d'objets que vous avez créés pour votre flotte et le nombre d'appareils pour chaque type
- Les groupes d'objets que vous avez créés pour votre flotte et le nombre d'appareils dans chaque groupe



Liste des périphériques

L'affichage de la liste des appareils affiche un tableau répertoriant les appareils de votre parc. Le tableau fournit les informations suivantes pour chaque appareil de la liste.

- Nom du dispositif
- État de connexion de l'appareil
- Horodatage de la dernière connexion de l'appareil
- Pour un appareil qui n'est pas connecté, la raison pour laquelle il s'est déconnecté
- Le type d'objet de l'appareil
- Le groupe d'objets de l'appareil
- Les champs personnalisés que vous avez créés dans le service d'indexation de flotte



Pour télécharger un fichier CSV contenant les appareils affichés sur la page, dans la liste des appareils, choisissez Exporter la page actuelle. Notez que si la liste est paginée, cela télécharge uniquement les données affichées sur la page en cours, et non sur les pages suivantes.

Vous pouvez utiliser des requêtes et des filtres pour réduire le nombre d'appareils qui génèrent les données récapitulatives dans la première vue et qui apparaissent dans la liste des appareils. Pour plus d'informations sur l'utilisation des requêtes et des filtres afin d'obtenir des informations plus spécifiques sur les appareils de votre parc, consultezthe section called “Création de requêtes”.

Création de requêtes à l'aide de filtres

Cette rubrique explique le fonctionnement des requêtes Fleet Hub for AWS IoT Device Management et vous explique les étapes nécessaires à la création d'une requête avec des filtres.

Vous pouvez contrôler le nombre et les types d'appareils qui s'affichent dans le résumé de votre tableau de bord et dans les vues de liste à l'aide de requêtes. Vous filtrez les requêtes à l'aide de champs AWS gérés, de champs personnalisés et de tous les attributs issus de vos sources de données indexées issues de l'indexation de AWS IoT flotte. Pour plus d'informations sur l'indexation de la flotte, consultez la section Indexation de la flotte.

Vous pouvez également ajouter des mots clés à vos requêtes. Les mots clés s'appliquent à tous les champs consultables. Ils sont également pris en compte dans la limite de trois filtres que vous pouvez appliquer à une seule requête.

La section suivante décrit les étapes à suivre pour créer une requête type.

Création de requêtes

Les étapes suivantes décrivent comment créer une requête type.

Prérequis

- Une application Fleet Hub associée à un AWS IoT Core compte contenant plusieurs appareils (objets)
- Un compte autorisé à utiliser l'application Fleet Hub

Créez votre première requête Fleet Hub à l'aide d'un filtre dans la console

1. Accédez à votre application Fleet Hub.
2. Sur le tableau de bord par défaut, vérifiez que vous pouvez voir l'onglet Liste des appareils et le nombre total d'appareils (objets) dans le AWS IoT Core compte associé.
3. Sur le tableau de bord par défaut, choisissez l'onglet Liste des appareils. Vérifiez que la liste de tous les appareils contenant les attributs gérés et personnalisés s'affiche. Les attributs personnalisés contiennent le préfixe des attributs.
4. En haut de la page, entrez les mots clés que vous voulez inclure dans votre requête. Les requêtes par mots clés s'appliquent à tous les champs.
5. Dans le haut de la page, cliquez sur Filtre.
6. Dans le mode Filtre, sous Champ, choisissez le champ que vous souhaitez utiliser comme filtre. Sous Opérateur, choisissez une option. Enfin, pour Valeur, choisissez la valeur du champ à utiliser dans votre filtre.

   Vous pouvez ajouter jusqu'à trois filtres. Une requête par mot clé est prise en compte dans ce nombre.
7. Pour exécuter votre requête, choisissez Appliquer les filtres. Les résultats montrent tous les appareils qui correspondent à votre requête.

Utilisation des tâches et des modèles de tâches dans Fleet Hub pour la gestion des AWS IoT appareils

> **Note**
>
> La fonction Modèles de tâche est en version préliminaire et sujette à modifications.

Une tâche est une opération distante qui est envoyée vers un ou plusieurs appareils connectés à AWS IoT. Par exemple, vous pouvez définir une tâche qui ordonne à un ensemble d'appareils de télécharger et d'installer les mises à jour d'une application ou d'un microprogramme, de redémarrer, de procéder à une rotation des certificats ou d'exécuter des opérations de dépannage à distance. Vous pouvez exécuter des tâches préconfigurées depuis Fleet Hub pour les applications Web de gestion des AWS IoT appareils. Les administrateurs de votre organisation créent des modèles de tâches dans la AWS IoT console et y joignent des politiques qui mettent les modèles à la disposition des utilisateurs de Fleet Hub. Dans votre application Fleet Hub, vous spécifiez les appareils ou le groupe d'appareils sur lesquels la tâche s'exécute.

Les administrateurs créent également des groupes d'appareils que vous pouvez consulter dans votre application. Pour afficher les événements , choisissez Groupes d’appareils dans le panneau de navigation. Lorsque vous spécifiez un groupe d'appareils comme cible, vous pouvez définir l'un des deux types d'options suivants pour le mode d'exécution de la tâche.

- instantané : la tâche ne s'exécute qu'une seule fois.
- continu : après son exécution initiale, le job s'exécute sur tous les appareils ajoutés au groupe.

Pour plus d'informations sur la création et la gestion des modèles de tâche, consultez Modèles de tâche. Pour plus d'informations sur le fonctionnement des tâches, consultez Jobs..

Exécution de tâches

Vous pouvez exécuter une tâche à partir de plusieurs emplacements dans une application Fleet Hub, mais les étapes suivantes sont toujours les mêmes.

1. Sélectionnez un groupe ou un ou plusieurs appareils comme cible.
2. Choisissez Exécuter la tâche.
3. Sous Sélection de la cible de tâche, sélectionnez Continu ou Instantané.
4. Sélectionnez un modèle de tâche. Vérifiez que le texte sous Résumé du job décrit le type de job que vous souhaitez exécuter.
5. En option, vous pouvez saisir un nom pour la tâche.
6. Cliquez sur Exécuter.

Vous pouvez sélectionner des cibles et suivre ces étapes depuis les emplacements suivants dans votre application Fleet Hub.

- L'onglet de liste des appareils sur le tableau de bord.
- Page détaillée d'un appareil spécifique.
- Page des groupes d'appareils.
- La page de détails d'un groupe d'appareils spécifique.

Affichage et gestion des journaux

Vous pouvez voir les tâches en cours dans votre parc aux emplacements suivants.

- La page de liste des tâches : cette page affiche toutes les tâches en cours dans votre parc. Pour afficher cette page, choisissez Jobs dans le volet de navigation.
- La page de détails d'un appareil spécifique : cette page affiche toutes les tâches exécutées sur l'appareil.

Chaque tâche possède une page de détails qui affiche des informations récapitulatives sur la tâche, y compris les informations relatives à la cible et à l'exécution. Cette page indique l'état d'exécution de la tâche sur chaque appareil. Il affiche également les totaux suivants.

- Nombre d’executions.
- Nombre de courses annulées.
- Nombre de courses réussies.
- Nombre de courses infructueuses.
- Nombre de courses rejetées.
- Nombre de courses en file d'attente.
- Nombre de courses en cours.
- Nombre de courses supprimées.
- Nombre de courses dont le temps imparti a expiré.

Pour annuler une tâche, sélectionnez-la, puis cliquez sur Annuler.

Alertes

Cette section explique le fonctionnement des alarmes Fleet Hub for AWS IoT Device Management et vous explique les étapes nécessaires à la création d'une alarme.

Lorsque vous créez une alarme Fleet Hub, elle s'applique à tous les appareils actuellement affichés sur votre tableau de bord. Si vous n'appliquez aucune requête, l'alarme s'applique à tous les appareils de votre parc. Pour plus d'informations sur l'utilisation de votre tableau de bord et la création de requêtes, consultezthe section called “Requêtes et filtres”.

Les alarmes utilisent les métriques Amazon CloudWatch (CloudWatch) associées aux champs consultables du service d'indexation de AWS IoT flotte pour créer CloudWatch des alarmes. Par exemple, vous pouvez créer une alarme qui génère un message Amazon Simple Notification Service (Amazon SNS) chaque fois que le niveau de batterie moyen des appareils de votre flotte tombe en dessous de 50 %.

Les alarmes Fleet Hub utilisent les GetPercentilesfonctionnalités GetStatisticset les fonctionnalités du service d'indexation de flotte pour interroger des données agrégées. Par exemple, lorsque vous créez une alarme qui suit un champ numérique personnalisé, vous pouvez créer des seuils d'alarme qui s'appliquent aux valeurs suivantes de l'attribut spécifié.

- Maximum
- Nombre
- Somme
- Minimum
- Moyenne
- Valeurs comprises dans le 10e, 50e, 90e, 95e ou 99e percentile

Pour plus d'informations sur l'interrogation de données agrégées dans le service d'indexation de flotte, consultez la section Interrogation de données agrégées.

Le tableau suivant répertorie quelques exemples des types d'agrégation disponibles pour les champs AWS gérés et personnalisés.

Champ	Type d'agrégation
Type d'objet (AWS-champ de chaîne géré)	Nombre
Groupe d'objets (AWS-champ de chaîne géré)	Nombre
Connecté (AWS-champ booléen géré)	• Maximum • Nombre

Champ	Type d'agrégation
La valeur de `true` .est 1. La valeur `false` .est 0.	• Somme • Minimum • Moyenne
shadow.reported .batterylevel (champ d'agrégation numérique créé dans le service d'indexation de flotte)	• Maximum • Nombre • Somme • Minimum • Moyenne • p10 (10e percentile) • p50 (50e percentile) • p90 (90e percentile) • p95 (95e percentile) • p99 (99e percentile)

Outre la spécification des champs et des types d'agrégation, vous spécifiez également les valeurs suivantes.

- Durée (1 minute ou 5 minutes) nécessaire pour que le seuil d'alarme que vous avez spécifié déclenche l'alarme.
- L'un des opérateurs de comparaison suivants à appliquer au champ et au type d'agrégation que vous avez spécifiés.
  - Plus grand
  - Plus grand/égal
  - Inférieur
  - Inférieur/égal
- La valeur à utiliser avec l'opérateur de comparaison que vous avez spécifié.
- Liste des adresses e-mail des membres de votre organisation qui reçoivent des messages Amazon SNS chaque fois que votre alarme est déclenchée.
- Le nom d'une alarme.

Pour créer une alarme Fleet Hub, voir the section called “Création d’alarmes”.

Création d’alarmes

Cette rubrique décrit les étapes nécessaires à la création d'une alarme Fleet Hub for AWS IoT Device Management. Cela suppose que votre administrateur a créé un champ d'agrégation à partir d'un champ parallèle de l'appareil nommé shadow.repord.batterylevel. Ce champ personnalisé indique le niveau de batterie d'un appareil. Vous devez demander à votre administrateur de créer des champs personnalisés consultables dans le service d'indexation de AWS IoT flotte.

L'alarme que vous créez envoie un message Amazon Simple Notification Service (Amazon SNS) à une liste de personnes de votre organisation chaque fois que le niveau de batterie moyen des appareils de votre flotte tombe en dessous de 50 % pendant une période d'une minute.

Création d'une requête Fleet Hub

1. Accédez à votre application Fleet Hub.
2. Si vous souhaitez cibler un ensemble spécifique d'appareils, créez une requête. Pour savoir comment créer une requête simple, consultez the section called “Création de requêtes à l'aide de filtres”. Si vous ne créez pas de requête, votre alarme s'applique à tous les appareils de votre parc.
3. Sur la page du tableau de bord par défaut, choisissez Créer une alarme.
4. Sur la page Créer une métrique d'agrégation, vérifiez que votre requête apparaît sous Requête cible. Dans la section Configurer l'agrégation des métriques du parc, dans le Choisir champ , sélectionnez shadow.reported d.batterylevel. Ce menu contient les champs AWS gérés et les champs personnalisés que votre administrateur a créés dans le service d'indexation de AWS IoT flotte.
5. Pour Choisir le type d'agrégation, sélectionnez Moyenne. Ce choix base l'alarme sur le niveau moyen de la batterie de votre parc d'appareils.
6. Pour Période, choisissez 1 minute. Cela déclenche l'alarme lorsque votre parc d'appareils reste dans l'état d'alarme spécifié pendant une minute.

   Choisissez Suivant.
7. Sur la page Définir le seuil, dans la section Déclencher l'alarme chaque fois que... section, choisissez Lower/Equal. Cela déclenche l'alarme lorsque le niveau moyen de la batterie tombe en dessous d'une valeur que vous spécifiez.
8. Saisissez 50 dans la zone de texte Than.

Choisissez Suivant.

9. Sur la page Notifier l'utilisateur, dans la section Notifier -- facultatif, entrez le nom de la liste d'e-mails contenant les utilisateurs de votre organisation qui reçoivent des notifications lorsque l'alarme est active. Entrez une liste d'adresses e-mail séparées par des virgules pour remplir cette liste.
10. Dans la section Détails de l'alarme, entrez le nom de votre alarme, et entrez éventuellement une description de votre alarme. Choisissez Suivant.
11. Sur la page Reviser, passez en revue les informations que vous avez saisies ou sélectionnées sur les pages précédentes. Sélectionnez Envoyer. Vous revenez au tableau de bord par défaut.
12. Sur le tableau de bord par défaut, dans le panneau de navigation de gauche, choisissez les alarmes Fleet Hub. Vérifiez que l'alarme que vous avez créée s'affiche.

Résolution des problèmes

Cette section fournit des informations de dépannage et des solutions possibles pour vous aider à résoudre les problèmes liés au Hub de la flotte .

Symptôme	Solution
Je ne parviens pas à ajouter d'autres filtres ou termes à ma requête.	Assurez-vous que vous n'avez pas atteint la limite de quatre termes de requête et filtres.
Je ne trouve pas de métrique personnalisée.	Demandez à votre administrateur de créer la métrique dans le service d'indexation de flotte.
Mon alarme n'affiche aucune donnée.	Quelques minutes sont nécessaires au chargement des données d'alarme.
Je dois changer les appareils ciblés par mon alarme.	Accédez à votre tableau de bord et modifiez la requête.
Une erreur s'affiche lorsque je change de région dans mon tableau de bord.	Demandez à votre administrateur de s'assurer que l'indexation de la flotte est activée dans la région que vous avez sélectionnée.

Symptôme	Solution
L'état de connectivité de mon « objet » n'est pas indexé par Fleeting Indexing.	Assurez-vous que votre client utilise le même identifiant client que Thing Name lorsqu'il se connecte à AWS IoT. Si votre client utilise un identifiant différent de celui de Thing Name lorsqu'il se connecte AWS IoT, l'état de connectivité de votre « objet » ne sera pas indexé par Fleet Indexing.

Surveillance de Fleet Hub pour la gestion des AWS IoT appareils

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances de Fleet Hub et de vos autres AWS solutions. AWS fournit les outils de surveillance suivants pour surveiller Fleet Hub, signaler tout problème et prendre des mesures automatiques le cas échéant.

- AWS CloudTrailcapture les appels d'API et les événements associés effectués par ou pour le compte de votre AWS compte et envoie les fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. Pour plus d'informations, consultez le Guide de l'utilisateur AWS CloudTrail.

Rubriques

Enregistrement des appels d'API Fleet Hub pour la gestion des AWS IoT appareils avec AWS CloudTrail

Fleet Hub pour la gestion des AWS IoT appareils est intégré à AWS CloudTrail. Le CloudTrail service fournit un enregistrement des actions effectuées par un utilisateur, un rôle ou un AWS service dans Fleet Hub. CloudTrail capture tous les appels d'API pour Fleet Hub sous forme d'événements. LLes appels capturés comprennent ceux de la console Fleet Hub et les appels de code aux opérations de l'API Fleet Hub.

Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour Fleet Hub. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements.

À l'aide des informations CloudTrail collectées, vous pouvez déterminer la demande qui a été faite à Fleet Hub, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande et quand, et plus de détails.

Pour en savoir plus CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

Informations sur le Fleet Hub dans CloudTrail

AWS CloudTrail est activé sur votre AWS compte lorsque vous le créez. Lorsqu'une activité se produit dans Fleet Hub, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez afficher, rechercher et télécharger les événements récents dans votre compte AWS . Pour plus d'informations, consultez la section Affichage des événements avec l'historique des CloudTrail événements.

Pour un enregistrement continu des événements de votre AWS compte, y compris des événements pour Fleet Hub, créez un parcours. Un suivi permet CloudTrail de transférer des fichiers journaux vers un compartiment Amazon Simple Storage Service (Amazon S3). Par défaut, lorsque vous créez un journal de suivi dans la console, il s'applique à toutes les régions AWS . Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez.

Vous pouvez également configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

- Présentation de la création d'un journal de suivi
- CloudTrail services et intégrations pris en charge
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers CloudTrail journaux provenant de plusieurs régions
- Réception des fichiers journaux CloudTrail de plusieurs comptes

CloudTrail enregistre toutes les actions de Fleet Hub. Ils sont documentés dans la référence de AWS IoT l'API. Par exemple, les appels aux `UpdateApplication` actions `CreateApplication` et génèrent des entrées dans les fichiers CloudTrail journaux.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été faite avec les informations AWS Identity and Access Management d'identification root ou utilisateur
- Si la demande a été effectuée avec des informations d'identification de sécurité temporaires pour un rôle ou un utilisateur fédéré

- Si la demande a été faite par un autre AWS service

Pour de plus amples informations, veuillez consulter l'élément userIdentity CloudTrail .

Comprendre les entrées du fichier journal de Fleet Hub pour la gestion des AWS IoT appareils

Un journal de suivi est une configuration qui permet d'envoyer des événements sous forme de fichiers journaux à un compartiment Amazon S3 de votre choix.

CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et comprend des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc.

CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

Example

L'entrée de CloudTrail journal suivante contient des informations sur l'`CreateApplication`action.

```
{
    "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"
    }
```

Sécurité dans Fleet Hub pour la gestion des AWS IoT appareils

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cela comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de AWS conformité Programmes de de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à Fleet Hub, voir AWS Services concernés par programme de conformitéAWS .
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise,et de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation de Fleet Hub pour la gestion des AWS IoT appareils. Les rubriques suivantes expliquent comment configurer pour répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser les ressources de votre Fleet Hub.

Rubriques

Protection des données dans Fleet Hub

Le modèle de responsabilité AWS partagée Le modèle s'applique à la protection des données dans Fleet Hub pour la gestion des AWS IoT appareils. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- SSL/TLS À utiliser pour communiquer avec AWS les ressources. Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour capturer AWS des activités, consultez la section Utilisation des CloudTrail sentiers dans le guide de AWS CloudTrail l'utilisateur.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-3 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS disponibles, consultez Norme FIPS (Federal Information Processing Standard) 140-3.

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Nom. Cela inclut lorsque vous travaillez avec Fleet Hub ou autre Services AWS à l'aide de

la console, de l'API ou AWS SDKs. AWS CLI Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Chiffrement au repos

Fleet Hub protège les données au repos grâce au cryptage côté serveur. Pour plus d'informations, veuillez consulter la rubrique Chiffrement au repos AWS IoT dans le AWS IoT Guide du développeur .

Chiffrement en transit

Dans les déploiements cloud des flux, le Hub de la flotte protège les données en transit à l'aide du protocole TLS (Transport Layer Security). Pour de plus amples informations, veuillez consulter Sécurité du transport AWS IoT dans le AWS IoT Manuel du développeur.

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

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Des administrateurs IAM contrôlent les personnes qui peuvent être authentifiées (connectées) et autorisées (dotées d'autorisations) à utiliser des ressources Fleet Hub. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans Fleet Hub.

Utilisateur du service – si vous utilisez le service ACM pour effectuer votre tâche, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Plus vous utiliserez de fonctions pour effectuer votre travail, plus vous pourriez avoir besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une fonctionnalité dans Fleet Hub, consultez Résolution des problèmes Fleet Hub for AWS IoT Device Management d'identité et d'accès.

Administrateur du service – Si vous êtes le responsable des ressources Fleet Hub de votre entreprise, vous bénéficiez probablement d'un accès total à Fleet Hub . Votre responsabilité est de déterminer les fonctionnalités Fleet Hub ainsi que les ressources auxquelles les utilisateurs de votre service doivent accéder. Vous devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM. Pour en savoir plus sur la façon dont votre entreprise peut utiliser IAM avec ACM, veuillez consulter Comment Fleet Hub for AWS IoT Device Management fonctionne avec IAM.

Administrateur IAM – si vous êtes un administrateur IAM, vous souhaiterez peut-être en savoir plus sur la façon d'écrire des stratégies pour gérer l'accès à la Fleet Hub. Pour voir des exemples de politiques basées sur l'identité que vous pouvez utiliser dans IAM, veuillez consulter Exemples de politiques basées sur l'identité pour Fleet Hub for AWS IoT Device Management.

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAM Identity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec

des rôles IAM. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez Comment vous connecter à votre compte Compte AWS dans le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer des demandes vous-même, consultez AWS Signature Version 4 pour les demandes d'API dans le Guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour plus d'informations, consultez Authentification multifactorielle dans le Guide de l'utilisateur AWS IAM Identity Center et Authentification multifactorielle AWS dans IAM dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur racine, consultez Tâches nécessitant des informations d'identification d'utilisateur racine dans le Guide de l'utilisateur IAM.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide Services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies Services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour obtenir des informations sur IAM Identity Center, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme telles que des mots de passe et des clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons d'effectuer une rotation des clés d'accès. Pour plus d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez nommer un groupe IAMAdminset lui donner les autorisations nécessaires pour administrer les ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour plus d'informations, consultez Cas d'utilisation pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité au sein de vous Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Pour assumer temporairement un rôle IAM dans le AWS Management Console, vous pouvez passer d'un rôle d'utilisateur à un rôle IAM (console). Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Méthodes pour endosser un rôle dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré : pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .
- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour en savoir plus sur la différence entre les rôles et les politiques basées sur les ressources pour l'accès intercompte, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.
- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
  - Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains

services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.

- Rôle de service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.
- Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une EC2 instance et qui envoient des demandes AWS CLI d' AWS API. Cela est préférable au stockage des clés d'accès dans l' EC2 instance. Pour attribuer un AWS rôle à une EC2 instance et le rendre disponible pour toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes exécutés sur l' EC2 instance d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utiliser un rôle IAM pour accorder des autorisations aux applications exécutées sur des EC2 instances Amazon dans le guide de l'utilisateur IAM.

Gestion des accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

Politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette

ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Listes de contrôle d'accès (ACLs)

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLs sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et AWS WAF Amazon VPC sont des exemples de services compatibles. ACLs Pour en savoir plus ACLs, consultez la présentation de la liste de contrôle d'accès (ACL) dans le guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d’autorisations qui vous sont accordées par des types de politiques plus courants.

- Limite d’autorisations : une limite d’autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d’autorisations qu’une politique basée sur l’identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d’autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l’identité d’une entité et de ses limites d’autorisation. Les politiques basées sur les ressources qui spécifient l’utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d’autorisations. Un refus explicite dans l’une de ces politiques annule l’autorisation. Pour plus d’informations sur les limites d’autorisations, consultez Limites d’autorisations pour des entités IAM dans le Guide de l’utilisateur IAM.
- Politiques de contrôle des services (SCPs) : SCPs politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans AWS Organizations. AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer des politiques de contrôle des services (SCPs) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités

figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les Organizations SCPs, voir Politiques de contrôle des services dans le Guide de AWS Organizations l'utilisateur.

- Politiques de contrôle des ressources (RCPs) : RCPs politiques JSON que vous pouvez utiliser pour définir le maximum d'autorisations disponibles pour les ressources de vos comptes sans mettre à jour les politiques IAM associées à chaque ressource que vous possédez. Le RCP limite les autorisations pour les ressources des comptes membres et peut avoir un impact sur les autorisations effectives pour les identités, y compris Utilisateur racine d'un compte AWS, qu'elles appartiennent ou non à votre organisation. Pour plus d'informations sur les Organizations RCPs, y compris une liste de ces Services AWS supports RCPs, consultez la section Resource control policies (RCPs) dans le guide de AWS Organizations l'utilisateur.
- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez Politiques de session dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Comment Fleet Hub for AWS IoT Device Management fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès au Fleet Hub, découvrez les fonctions IAM que vous pouvez utiliser avec Fleet Hub.

Fonctionnalités IAM que vous pouvez utiliser avec Fleet Hub for AWS IoT Device Management

Fonctionnalité IAM	Assistance Fleet Hub
Politiques basées sur l'identité	Oui

Fonctionnalité IAM	Assistance Fleet Hub
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique	Oui
ACLs	Non
ABAC (étiquettes dans les politiques)	Oui
Informations d'identification temporaires	Oui
Autorisations de principal	Oui
Rôles de service	Oui
Rôles liés à un service	Non

Pour obtenir une vue d'ensemble de la façon dont Fleet Hub et les autres AWS services fonctionnent avec la plupart des fonctionnalités IAM, consultez la section AWS Services compatibles avec IAM dans le Guide de l'utilisateur IAM.

Politiques basées sur l'identité pour Fleet Hub

Prend en charge les politiques basées sur l'identité : oui

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité,

car celle-ci s’applique à l’utilisateur ou au rôle auquel elle est attachée. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l’utilisateur IAM.

Exemples de stratégies basées sur l'identité pour Fleet Hub

Pour voir des exemples de politiques Fleet Hub basées sur l'identité, consultez Exemples de politiques basées sur l'identité pour Fleet Hub for AWS IoT Device Management.

Politiques basées sur une ressource dans Fleet Hub

Prend en charge les politiques basées sur les ressources : non

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l’accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d’actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. L’ajout d’un principal intercompte à une politique basée sur les ressources ne représente qu’une partie de l’instauration de la relation d’approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un administrateur IAM du compte sécurisé doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l’entité. Toutefois, si une politique basée sur des ressources accorde l’accès à un principal dans le même compte, aucune autre politique basée sur l’identité n’est requise. Pour plus d’informations, consultez Accès intercompte aux ressources dans IAM dans le Guide de l’utilisateur IAM.

Actions politiques pour Fleet Hub

> **Note**
>
> Les applications Fleet Hub utilisent la politique `AWSIoTFleetHubFederationAccess` gérée. Pour de plus amples informations, veuillez consulter ???.

Prend en charge les actions de politique : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour afficher la liste des actions Fleet Hub, consultez Actions définies par Fleet Hub for AWS IoT Device Management dans la Référence de l'autorisation de service.

Les actions de politique dans Fleet Hub utilisent le préfixe suivant avant l'action :

```
iotfleethub
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

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

Pour voir des exemples de politiques Fleet Hub basées sur l'identité, consultez Exemples de politiques basées sur l'identité pour Fleet Hub for AWS IoT Device Management.

Ressources relatives aux politiques pour Fleet Hub

Prend en charge les ressources de politique : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

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

Pour consulter la liste des types de ressources Fleet Hub et leurs caractéristiques ARNs, consultez la section Ressources définies par Fleet Hub for AWS IoT Device Management dans la référence d'autorisation de service. Pour savoir grâce à quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez Actions définies par Fleet Hub for AWS IoT Device Management.

Pour voir des exemples de politiques Fleet Hub basées sur l'identité, consultez Exemples de politiques basées sur l'identité pour Fleet Hub for AWS IoT Device Management.

Clés de condition de Fleet Hub

Prend en charge les clés de condition de politique spécifiques au service : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une `OR` opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez Éléments d'une politique IAM : variables et identifications dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Pour afficher la liste des clés de condition Fleet Hub, consultez Clés de condition pour Fleet Hub for AWS IoT Device Management dans la Référence de l'autorisation de service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez la section Actions définies par Fleet Hub for AWS IoT Device Management.

Pour voir des exemples de politiques Fleet Hub basées sur l'identité, consultez Exemples de politiques basées sur l'identité pour Fleet Hub for AWS IoT Device Management.

Listes de contrôle d'accès (ACLs) dans Fleet Hub

Supports ACLs : Non

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLs sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Contrôle d'accès basé sur les attributs (ABAC) avec Fleet Hub

Prise en charge d'ABAC (balises dans les politiques) : Oui

Le contrôle d'accès par attributs (ABAC) est une stratégie d'autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L'étiquetage des entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l'identification du principal correspond à celle de la ressource à laquelle il tente d'accéder.

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques devient fastidieuse.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informations sur ABAC, consultez Définition d'autorisations avec l'autorisation ABAC dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez Utilisation du contrôle d'accès par attributs (ABAC) dans le Guide de l'utilisateur IAM.

Utilisation des informations d'identification temporaires avec Fleet Hub

Prend en charge les informations d'identification temporaires : oui

Certains Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services AWS fonctionnent avec des informations d'identification temporaires, consultez Services AWS la section relative à l'utilisation d'IAM dans le guide de l'utilisateur d'IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez Passage d'un rôle utilisateur à un rôle IAM (console) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM.

Autorisations principales entre services pour Fleet Hub

Prend en charge les sessions d'accès direct (FAS) : oui

Lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.

Rôles de service pour Fleet Hub

Prend en charge les rôles de service : oui

Un rôle de service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

> **Warning**
>
> La modification des autorisations d'un rôle de service peut interrompre la fonctionnalité de Fleet Hub. Ne modifiez des fonctions du service que quand ACM vous le conseille.

Rôle lié à un service pour Fleet Hub

Prend en charge les rôles liés à un service : non

Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Pour plus d'informations sur la création ou la gestion des rôles liés à un service, consultez Services AWS qui fonctionnent avec IAM. Recherchez un service dans le tableau qui inclut un `Yes` dans la colonne Rôle lié à un service. Choisissez le lien Oui pour consulter la documentation du rôle lié à ce service.

Exemples de politiques basées sur l'identité pour Fleet Hub for AWS IoT Device Management

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou modifier les ressources Fleet Hub. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l'API AWS Management Console, AWS Command Line Interface (AWS CLI) ou de AWS l'API. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques IAM (console) dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par Fleet Hub, y compris le ARNs format de chaque type de ressource, voir Actions, ressources et clés de condition Fleet Hub for AWS IoT Device Management dans la référence d'autorisation de service.

Rubriques

- Bonnes pratiques en matière de politiques
- Utilisation de la console Fleet Hub
- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Bonnes pratiques en matière de politiques

Les stratégies basées sur l'identité déterminent si une personne peut créer, consulter ou supprimer des ressources Fleet Hub dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accordez les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation d'IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utilisez des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez l'Analyseur d'accès IAM pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : l'Analyseur d'accès IAM valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politiques avec IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger la MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Sécurisation de l'accès aux API avec MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Utilisation de la console Fleet Hub

Pour accéder à la Fleet Hub for AWS IoT Device Management console, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et de consulter les détails des ressources Fleet Hub de votre Compte AWS. Si vous créez une politique basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette politique.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API qu'ils tentent d'effectuer.

Pour garantir que les utilisateurs et les rôles peuvent toujours utiliser la console Fleet Hub, associez également le Fleet Hub `ConsoleAccess` ou la politique `ReadOnly` AWS gérée aux entités. Pour plus d'informations, consultez Ajout d'autorisations à un utilisateur dans le Guide de l'utilisateur IAM.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or 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": "*"
        }
    ]
}
```

Résolution des problèmes Fleet Hub for AWS IoT Device Management d'identité et d'accès

Utilisez les informations suivantes pour identifier et résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec Fleet Hub et IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans Fleet Hub
- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite autoriser des personnes extérieures à mon AWS compte à accéder à mes ressources Fleet Hub

Je ne suis pas autorisé à effectuer une action dans Fleet Hub

S'il vous AWS Management Console indique que vous n'êtes pas autorisé à effectuer une action, vous devez contacter votre administrateur pour obtenir de l'aide. Votre administrateur est la personne qui vous a fourni vos informations de connexion.

> **Note**
>
> Les applications Fleet Hub utilisent la politique `AWSIoTFleetHubFederationAccess` gérée. Pour de plus amples informations, veuillez consulter ???.

L'exemple d'erreur suivant se produit quand l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées sur une ressource *`my-example-widget`* fictive, mais ne dispose pas des autorisations `iotfleethub:`*`GetWidget`* fictives.

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

Dans ce cas, Mateo demande à son administrateur de mettre à jour ses politiques pour lui permettre d'accéder à la ressource *`my-example-widget`* à l'aide de l'action `iotfleethub:`*`GetWidget`*.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez une erreur selon laquelle vous n'êtes pas autorisé à exécuter `iam:PassRole` l'action, vos stratégies doivent être mises à jour afin de vous permettre de transmettre un rôle à Fleet Hub.

Certains vous Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour exécuter une action dans ACM. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

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

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite autoriser des personnes extérieures à mon AWS compte à accéder à mes ressources Fleet Hub

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques

basées sur les ressources ou les listes de contrôle d'accès (ACLs), vous pouvez utiliser ces politiques pour autoriser les utilisateurs à accéder à vos ressources.

Pour plus d'informations, consultez les éléments suivants :

- Pour savoir si la flotte prend en charge ces fonctionnalités, consultez Comment Fleet Hub for AWS IoT Device Management fonctionne avec IAM.
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès aux ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour en savoir plus sur la différence entre l'utilisation des rôles et des politiques basées sur les ressources pour l'accès intercompte, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Validation de conformité pour Fleet Hub pour la gestion des AWS IoT appareils

Des auditeurs tiers évaluent la sécurité et la conformité de Fleet Hub dans le cadre de multiples programmes de AWS conformité. Il s'agit notamment des certifications SOC, PCI, FedRAMP, HIPAA et d'autres.

Pour savoir si un programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez Services AWS la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de AWS conformité Programmes AWS de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et

réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Conformité et gouvernance de la sécurité : ces guides de mise en œuvre de solutions traitent des considérations architecturales et fournissent les étapes à suivre afin de déployer des fonctionnalités de sécurité et de conformité.
- Référence des services éligibles HIPAA : liste les services éligibles HIPAA. Tous ne Services AWS sont pas éligibles à la loi HIPAA.
- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation Services AWS et décrivent les directives relatives aux contrôles de sécurité dans de nombreux cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).
- Évaluation des ressources à l'aide des règles du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- Amazon GuardDuty — Cela Service AWS détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité, telles que la norme PCI DSS, en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.
- AWS Audit Manager— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Résilience dans Fleet Hub pour la gestion des AWS IoT appareils

L'infrastructure AWS mondiale est construite autour des AWS régions et des zones de disponibilité. AWS Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur AWS les régions et les zones de disponibilité, consultez la section Infrastructure AWS mondiale.

AWS politiques gérées pour Fleet Hub pour la gestion des AWS IoT appareils

Pour ajouter des autorisations aux utilisateurs, aux groupes et aux rôles, il est plus facile d'utiliser des politiques AWS gérées que de les rédiger vous-même. Il faut du temps et de l'expertise pour créer des politiques gérées par le client IAM qui ne fournissent à votre équipe que les autorisations dont elle a besoin. Pour démarrer rapidement, vous pouvez utiliser nos politiques AWS gérées. Ces politiques couvrent les cas d'utilisation courants et sont disponibles dans votre AWS compte. Pour plus d'informations sur les politiques AWS gérées, voir les politiques AWS gérées dans le guide de l'utilisateur IAM.

AWS les services maintiennent et mettent à jour les politiques AWS gérées. Vous ne pouvez pas modifier les autorisations dans les politiques AWS gérées. Les services ajoutent occasionnellement des autorisations à une politique gérée par AWS pour prendre en charge de nouvelles fonctionnalités. Ce type de mise à jour affecte toutes les identités (utilisateurs, groupes et rôles) auxquelles la politique est attachée. Les services sont très susceptibles de mettre à jour une politique gérée par AWS quand une nouvelle fonctionnalité est lancée ou quand de nouvelles opérations sont disponibles. Les services ne suppriment pas les autorisations d'une politique AWS gérée. Les mises à jour des politiques n'endommageront donc pas vos autorisations existantes.

En outre, AWS prend en charge les politiques gérées pour les fonctions professionnelles qui couvrent plusieurs services. Par exemple, la politique ReadOnlyAccess AWS gérée fournit un accès en lecture seule à tous les AWS services et ressources. Lorsqu'un service lance une nouvelle fonctionnalité,

il AWS ajoute des autorisations en lecture seule pour les nouvelles opérations et ressources. Pour obtenir la liste des politiques de fonctions professionnelles et leurs descriptions, consultez la page politiques gérées par AWS pour les fonctions de tâche dans le Guide de l'utilisateur IAM.

AWS politique gérée : AWSIo TFleet HubFederationAccess

Vous pouvez associer la politique `AWSIoTFleetHubFederationAccess` à vos identités IAM.

Cette politique accorde aux utilisateurs fédérés de Fleet Hub for AWS IoT Device Management les autorisations dont ils ont besoin pour effectuer des actions dans les applications Web de AWS IoT Fleet Hub et dans d'autres AWS services à partir de celles-ci.

Pour plus d'informations sur l'ajout d'utilisateurs aux applications Web Fleet Hub, veuillez consulter ???.

Vous pouvez afficher cette stratégie dans AWS console.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes :

- `iot`- Récupérez les données des AWS IoT appareils et effectuez des actions au niveau de la flotte.
- `iotfleethub` - Récupérez les métadonnées de l'application Fleet Hub.
- `cloudwatch`- Récupérez les données CloudWatch d'alarme et de métrique. Permet également de créer et de supprimer des actions limitées aux alarmes Fleet Hub.
- `sns` - Effectuez des opérations de création, de lecture, de suppression, d'abonnement et de désinscription. Ces opérations sont limitées aux sujets SNS de 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*"
        }
    ]
}
```

Mises à jour des politiques AWS gérées par Fleet Hub

Consultez les détails des mises à jour des politiques AWS gérées pour Fleet Hub depuis que ce service a commencé à suivre ces modifications. Pour plus d'informations, consultez la page d'historique de la documentation de Fleet Hub.

Modification	Description	Date
AWSIoTFleetHubFederationAccess – Mise à jour d’une stratégie existante	Fleet Hub a ajouté de nouvelles autorisations pour permettre aux utilisateurs de l'application de récupérer des données AWS IoT Device	4 avril 2022

Modification	Description	Date
	Defender métriques dans les applications Fleet Hub.	
AWSIoTFleetHubFederationAccess – Mise à jour d'une politique existante	Fleet Hub a ajouté de nouvelles autorisations pour permettre aux utilisateurs de l'application de récupérer des sources de données supplémentaires à des fins d'indexation. Une autorisation est également ajoutée pour permettre aux utilisateurs de l'application d'annuler l'exécution AWS IoT d'une tâche dans l'application.	15 novembre 2021
AWSIoTFleetHubFederationAccess – Mise à jour d'une politique existante	Fleet Hub a ajouté de nouvelles autorisations permettant aux utilisateurs de l'application de récupérer les données de Thing Group et d'effectuer des opérations CRUD sur des AWS IoT tâches.	24 mai 2021
AWSIoTFleetHubFederationAccess – Mise à jour d'une politique existante	Fleet Hub a supprimé les autorisations pour le tableau de bord APIs Fleet Hub non pris en charge.	12 avril 2021

Modification	Description	Date
AWSIoTFleetHubFederationAccess : nouvelle politique	Fleet Hub a ajouté une nouvelle politique qui accorde les autorisations nécessaires aux utilisateurs de l'application Fleet Hub pour récupérer les données des appareils et effectuer des AWS IoT actions.	12 avril 2021
Fleet Hub a commencé à suivre les modifications	Fleet Hub a commencé à suivre les modifications apportées AWS à ses politiques gérées.	12 avril 2021

Sécurité de l'infrastructure dans Fleet Hub pour la gestion des AWS IoT appareils

En tant que service géré, Fleet Hub for AWS IoT Device Management est protégé par les procédures de sécurité du réseau AWS mondial décrites dans le livre blanc Amazon Web Services : présentation des processus de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder à Fleet Hub via le réseau. Les clients doivent prendre en charge le protocole TLS (Transport Layer Security) 1.2 ou version ultérieure. Nous recommandons TLS 1.3. Les clients doivent aussi prendre en charge les suites de chiffrement PFS (Perfect Forward Secrecy) comme Ephemeral Diffie-Hellman (DHE) ou Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l’aide d’un ID de clé d’accès et d’une clé d’accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d’identification de sécurité temporaires et signer les demandes.

Prévention du cas de figure de l'adjoint désorienté entre services

Le problème de député confus est un problème de sécurité dans lequel une entité qui n'est pas autorisée à effectuer une action peut contraindre une entité plus privilégiée à le faire. En AWS, l'usurpation d'identité interservices peut entraîner la confusion des adjoints. L'usurpation d'identité entre services peut se produire lorsqu'un service (le service appelant) appelle un autre service (le service appelé). Le service appelant peut être manipulé pour utiliser ses autorisations afin d'agir sur les ressources d'un autre client de sorte qu'il n'y aurait pas accès autrement. Pour éviter cela, AWS fournit des outils qui vous aident à protéger vos données pour tous les services avec des principaux de service qui ont eu accès aux ressources de votre compte.

Nous vous recommandons d'utiliser les clés de contexte de condition globale `aws:SourceArn` et `aws:SourceAccount` dans les clés de contexte des conditions globales dans les politiques de ressources. Si vous utilisez les deux clés de contexte de condition globale, la valeur `aws:SourceAccount` et le compte de la valeur `aws:SourceArn` doit utiliser le même ID de compte lorsqu'il est utilisé dans la même déclaration de stratégie.

Le moyen le plus efficace de se protéger contre le problème de l'adjoint confus est d'utiliser la clé de `aws:SourceArn` contexte de condition globale avec le nom de ressource Amazon (ARN) complet de la ressource. Pour Fleet Hub, vous `aws:SourceArn` devez respecter le format :`arn:aws:iot:`*`region`*`:`*`account-id`*`:*`. Assurez-vous que cela *`region`* correspond à la région de votre Fleet Hub et *`account-id`* à votre numéro de compte client.

L'exemple suivant utilise les clés de contexte de condition globale `aws:SourceArn` et `aws:SourceAccount` dans une politique d'approbation afin d'empêcher le problème d'adjoint confus. Pour trouver l'ARN de votre rôle Fleet Hub, rendez-vous dans la section Fleet Hub de la AWS IoT console et sélectionnez votre application Fleet Hub pour afficher la page détaillée de l'application.

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:*"
        }
      }
    }
  ]
}
```

Fleet Hub end-of-life (EOL) FAQs

Fleet Hub end-of-life FAQs

Quand va Fleet Hub end-of-life ?

AWS mettra fin à Fleet Hub pour la gestion des AWS IoT appareils le 18 octobre 2025. Fleet Hub passera progressivement à son EOL. Les fonctionnalités mises à disposition par Fleet Hub sont également disponibles dans la AWS IoT Device Management console pour continuer à répondre aux besoins de votre entreprise.

1. Le 17 octobre 2024, AWS nous cesserons d'intégrer de nouveaux clients à Fleet Hub. Si vous n'avez aucune application Fleet Hub avant le 17 octobre 2024, vous êtes identifié comme un nouveau client de Fleet Hub. Dans le cas contraire, vous êtes identifié comme un client existant de Fleet Hub.
2. Les clients existants de Fleet Hub peuvent continuer à utiliser les applications Fleet Hub jusqu'au 17 octobre 2025. Du 17 octobre 2024 au 17 octobre 2025, il n'y aura aucune nouvelle mise à jour des fonctionnalités de Fleet Hub et AWS prendra en charge les corrections de bogues critiques.
3. Le 18 octobre 2025, le support de Fleet Hub pour la gestion des AWS IoT appareils AWS cessera. À cette date, Fleet Hub atteindra son niveau end-of-life et vous ne pourrez plus utiliser Fleet Hub. L'arrêt de Fleet Hub n'a aucune incidence sur les autres AWS IoT Device Management fonctionnalités. Vous pouvez continuer à utiliser les fonctionnalités existantes fournies par AWS IoT Device Management. Pour de plus amples informations, veuillez consulter ???.

Qu'adviendra-t-il de mes applications Fleet Hub à end-of-life cette date ?

À la date d'expiration du 18 octobre 2025, vos applications Fleet Hub seront supprimées et vous ne pourrez plus accéder à Fleet Hub. Vos AWS ressources associées à Fleet Hub ne seront pas automatiquement supprimées. Ces ressources incluent les AWS IoT Device Management tâches, les composants d'alarme de Fleet Hub tels que les indicateurs de AWS IoT Device Management flotte, les CloudWatch alarmes et les rubriques Amazon SNS. Vous pouvez continuer à accéder à ces ressources indépendamment du AWS Management Console AWS SDK ou du SDK pour vos besoins de surveillance. AWS CLI Pour supprimer vos AWS ressources sous-jacentes, consultez???.

Qu'advient-il de mes AWS ressources sous-jacentes à cette date et après end-of-life cette date ?

Vous pouvez continuer à accéder à vos AWS ressources sous-jacentes associées à Fleet Hub indépendamment AWS Management Console de vos besoins de surveillance. Ces ressources incluent les AWS IoT Device Management tâches, les composants d'alarme de Fleet Hub tels que les indicateurs de AWS IoT Device Management flotte, les CloudWatch alarmes et les rubriques Amazon SNS. Les utilisateurs de l'application Fleet Hub sont assignés par vous-même à partir de votre groupe d'utilisateurs IAM Identity Center. Si les utilisateurs de votre IAM Identity Center ont été créés uniquement pour accéder aux applications Fleet Hub et que vous ne les utilisez pas pour d'autres AWS services, vous pouvez les supprimer des onglets utilisateurs et applications d'IAM Identity Center depuis la console. Pour de plus amples informations, veuillez consulter ???.

Comment supprimer les applications Fleet Hub avant end-of-life cette date ?

Pour supprimer vos applications Fleet Hub avant la date de fin de vie, utilisez la AWS IoT console ou la `--delete-application` AWS CLI commande.

> **Note**
>
> La suppression des applications Fleet Hub ne supprimera pas les AWS ressources sous-jacentes associées à Fleet Hub. Pour supprimer ces ressources, voir the section called “Comment supprimer mes AWS ressources sous-jacentes ?”

Pour supprimer des applications Fleet Hub à l'aide de AWS IoT la console, suivez les étapes indiquées.

1. Accédez à AWS IoT la console, dans le menu de navigation de gauche, choisissez Fleet Hub, puis Applications.
2. Sur la page Applications, choisissez l'application Fleet Hub que vous souhaitez supprimer. Sélectionnez Delete (Supprimer). Vous verrez une fenêtre vous demandant de confirmer la suppression de l'application. Entrez « Supprimer » pour confirmer la suppression, puis choisissez Supprimer.

Pour supprimer des applications Fleet Hub à l'aide de AWS CLI, suivez les étapes indiquées.

1. Pour supprimer votre application Fleet Hub à l'aide de AWS CLI, vous devez connaître l'ID de l'application. Exécutez d'abord la commande `--list-applications`CLI pour répertorier toutes vos applications Fleet Hub et leurs applications IDs.

   Pour répertorier vos applications Fleet Hub avec leurs IDs informations, exécutez la commande suivante.

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

   Le résultat de la commande peut ressembler à ce qui suit.

   ```
   {
    "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. Pour supprimer votre application Fleet Hub, exécutez la AWS CLI commande suivante.

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

La commande ne produit pas de sortie. Vous pouvez exécuter la commande `--list-applications` CLI pour vérifier si l'application spécifiée a été supprimée ou non.

La suppression des applications Fleet Hub supprimera-t-elle automatiquement les ressources sous-jacentes ?

Non La suppression des applications Fleet Hub ne supprimera pas automatiquement les ressources sous-jacentes. Pour supprimer les AWS ressources associées à Fleet Hub, consultez???.

Comment supprimer mes AWS ressources sous-jacentes ?

Fleet Hub permet aux clients de créer des AWS ressources telles que des AWS IoT Device Management emplois et des alarmes Fleet Hub. La suppression des applications Fleet Hub ne supprime pas ces ressources, et vous pouvez continuer à y accéder pour répondre aux besoins de votre entreprise, comme décrit dans???. Pour supprimer ces ressources sous-jacentes, suivez les étapes ci-dessous.

Comment supprimer des offres d'emploi ?

Pour supprimer une tâche, vous devez d'abord l'annuler. Vous pouvez annuler des tâches directement depuis Fleet Hub avant la date de fin de vie. Vous pouvez également utiliser la AWS IoT console pour annuler et supprimer des tâches quand vous le souhaitez.

Pour annuler des tâches depuis votre application Fleet Hub

1. Accédez à votre application Fleet Hub, puis sélectionnez l'onglet Jobs.
2. Choisissez le travail que vous souhaitez annuler.

3. Choisissez Annuler le travail.

Pour annuler et supprimer des tâches depuis AWS IoT la console

1. Accédez à Actions à distance, choisissez l'onglet Tâches.
2. Sélectionnez le travail que vous souhaitez annuler.
3. Choisissez Cancel (Annuler).
4. Dans le même onglet Tâches, choisissez la tâche que vous souhaitez supprimer.
5. Sélectionnez Delete (Supprimer).

Comment supprimer les alarmes Fleet Hub ?

Vous pouvez supprimer les alarmes Fleet Hub directement dans l'application Fleet Hub. Cela supprimera automatiquement tous les composants sous-jacents tels que les indicateurs de flotte, les CloudWatch alarmes et les rubriques Amazon SNS. Dans votre application Fleet Hub, accédez à l'onglet des alarmes Fleet Hub, sélectionnez les alarmes que vous souhaitez supprimer et choisissez Supprimer. Vous pouvez également supprimer les alarmes Fleet Hub à l'aide de AWS Management Console. Vous pouvez suivre ces étapes pour supprimer plusieurs applications dans différentes AWS régions.

Pour supprimer les alarmes Fleet Hub de l'application Fleet Hub

1. Dans l'application Fleet Hub, accédez à l'onglet des alarmes Fleet Hub.
2. Sélectionnez les alarmes que vous souhaitez supprimer, puis cliquez sur Supprimer. Cette action supprimera tous les composants sous-jacents.

Pour supprimer les indicateurs de flotte de AWS IoT la console

1. Accédez à Gérer dans le menu de navigation de gauche de AWS IoT la console. Dans Tous les appareils, sélectionnez Fleet Metrics.
2. Sélectionnez toutes les métriques de flotte dont le nom est préfixé par « iotfleethub ».
3. Sélectionnez Delete (Supprimer).

Pour supprimer des CloudWatch alarmes de CloudWatch la console

1. Accédez à l'onglet Toutes les alarmes de CloudWatch la console.

2. Sélectionnez toutes les métriques dont le nom est préfixé par « iotfleethub ».
3. Accédez à Actions, puis choisissez Supprimer.

Pour supprimer les rubriques Amazon SNS recevant des alarmes créées depuis la console Amazon SNS

1. Accédez à l'onglet Rubriques de la console Amazon SNS.
2. Sélectionnez tous les sujets dont le nom est préfixé par « iotfleethub ».
3. Sélectionnez Delete (Supprimer).

Comment supprimer des utilisateurs IAM Identity Center créés depuis Fleet Hub ?

Si les utilisateurs de votre IAM Identity Center ont été créés uniquement pour accéder aux applications Fleet Hub et que vous ne les utilisez pas pour d'autres AWS services, vous pouvez les supprimer des onglets utilisateurs et applications d'IAM Identity Center depuis la console.

Lequel ne APIs fonctionnera plus à end-of-life compter de cette date ?

Nous mettrons fin à toutes les activités APIs associées à la gestion du cycle de vie des applications Fleet Hub le 18 octobre 2025. Notez que celles-ci ne APIs sont associées qu'à Fleet Hub et n'affectent aucune autre AWS IoT Device Management fonctionnalité. Les clients existants de Fleet Hub peuvent continuer à les utiliser APIs jusqu'au 17 octobre 2025.

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

Quelles sont les fonctionnalités existantes de Fleet Hub et comment y accéder depuis la console ?

Fleet Hub propose les fonctionnalités clés de surveillance et de gestion suivantes conçues à l'aide de AWS IoT Device Management fonctionnalités. Ces fonctionnalités sont toutes disponibles en dehors des applications Fleet Hub. Ils se trouvent directement dans la AWS IoT Device Management console à laquelle vous pouvez continuer d'accéder pour répondre aux besoins de votre entreprise.

Résumé de l'état de connectivité de la flotte

Le tableau de bord Fleet Hub résume l'état de connectivité de votre flotte IoT avec des informations détaillées sur la connectivité. Il indique le nombre d'appareils connectés et déconnectés et la répartition des appareils déconnectés par raison de déconnexion. Un tableau de bord de surveillance de l'état de connectivité équivalent est disponible dans la AWS IoT console sous l'onglet Moniteur. Vous pouvez activer des widgets pour surveiller le nombre d'appareils connectés, le taux de déconnexions et les raisons de ces déconnexions. Pour plus d'informations, consultez la section AWS IoT Device Management ajoute un tableau de bord unifié de surveillance des métriques de connectivité.

Alarmes Fleet Hub

Les alarmes Fleet Hub vous permettent de créer et de surveiller des alarmes basées sur des seuils. Les alarmes Fleet Hub exploitent les indicateurs de flotte fournis par l'indexation des AWS IoT Device Management flottes et les CloudWatch alarmes Amazon. Vous pouvez directement surveiller ces statistiques de flotte dans la CloudWatch console Amazon et les reconfigurer dans la AWS IoT console. Les métriques et CloudWatch alarmes de flotte dont les noms sont préfixés par « iotfleethub » sont associées à Fleet Hub. Vous pouvez continuer à y accéder depuis la console. Vous pouvez utiliser Amazon CloudWatch pour suivre ces statistiques au fil du temps et suivre les tendances. Vous pouvez également créer des statistiques de flotte supplémentaires à partir de la AWS IoT console, puis les surveiller et configurer des alarmes sur Amazon CloudWatch. Pour plus d'informations, voir Afficher les statistiques du parc dans CloudWatch.

Recherche d'appareils

Fleet Hub vous permet d'appliquer plusieurs filtres à l'aide de critères issus de sources de données indexées afin d'affiner la recherche sur votre appareil. Cette fonctionnalité utilise la fonctionnalité de recherche de l'indexation des flottes. La recherche par appareil peut être utilisée directement via la AWS IoT Device Management console, depuis la page de recherche avancée

d'objets. Pour accéder à la page de recherche avancée d'objets, choisissez Objets dans Gérer, puis sélectionnez Tous les appareils. Choisissez Recherche avancée dans le coin supérieur droit de la page Objets.

Exécution d’une tâche

Vous pouvez exécuter des tâches directement depuis Fleet Hub en sélectionnant un objet ou un groupe comme cible. Vous pouvez également exécuter des tâches depuis la page Tâches de la AWS IoT Device Management console, où vous pouvez définir un objet, un groupe statique ou un groupe dynamique comme cible pour l'exécution des tâches.

Affichage des détails de l'appareil

Fleet Hub fournit une vue détaillée au niveau de l'appareil (objet) depuis la page Tous les appareils. Une vue détaillée similaire au niveau de l'appareil est disponible directement depuis l'onglet Objets de la AWS IoT Device Management console, ou en cliquant sur un objet spécifique renvoyé via les résultats des requêtes de recherche d'indexation du parc.

Historique de la documentation

Le tableau suivant décrit les mises à jour de la documentation relative à Fleet Hub. Pour les modifications apportées aux politiques AWS gérées pour Fleet Hub, consultez les politiques AWS gérées pour Fleet Hub pour la gestion des AWS IoT appareils.

Modification	Description	Date
Version de disponibilité générale de Fleet Hub for AWS IoT Device Management	Contenu mis à jour pour refléter les améliorations apportées à Fleet Hub pour la gestion des AWS IoT appareils pendant la période de prévisualisation.	25 mai 2021
Version préliminaire de Fleet Hub pour la gestion des AWS IoT appareils	Publication de la version préliminaire du guide de l'utilisateur de Fleet Hub for AWS IoT Device Managemen t.	le 16 décembre 2020