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

À quoi sert Fleet HubAWS IoTGestion des appareils ?

Avec Fleet Hub pourAWS IoTGestion des appareils (Fleet Hub), vous pouvez créer des applications Web autonomes pour surveiller l'état de santé de votre parc d'appareils. Vous pouvez mettre ces applications à la disposition des utilisateurs de votre organisation, même s'ils n'en ont pasAWScomptes. Utilisez Fleet Hub pour gérer les tâches courantes à l'échelle de la flotte, telles que l'investigation et la résolution des problèmes opérationnels et de sécurité.

Fleet Hub 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.
- Tâches en cours.

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

Comment Fleet Hub pourAWS IoTLa gestion des appareils fonctionne

Les administrateurs peuvent utiliser Fleet Hub pourAWS IoTGestion des appareils pour créer des applications Web sécurisées en quelques minutes sans provisionner de ressources ni écrire de code. Les applications Web que vous créez à l'aide de Fleet Hub 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 de Fleet Hub s'intègrent àAWS IoT Coreindexation de la flotte et 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 Fleet Hub utilisent`AWSIoTFleetHubFederationAccess`politique gérée. Pour plus d'informations, veuillez consulter ???.

Exemples de cas d'utilisation :

- Visualisez les problèmes de connectivité des appareils : vous pouvez voir le nombre d'appareils déconnectés dans votre parc, l'état de la dernière connexion d'un appareil et la ou les raisons pour lesquelles les appareils se sont déconnectés.
- Définir 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 Fleet Hub

Vous pouvez utiliser la console Fleet Hub pour activer l'indexation du parc de votre parc d'appareils. Lorsque vous activez l'indexation de la flotte dans Fleet Hub, vous l'activez pour l'ensemble de la flotte et vous la mettez à la disposition de toutes les applications de Fleet Hub.

Lorsqu'elle est activée, l'indexation du parc indexe toutAWS IoT Core-champs gérés automatiquement. Vous pouvez également utiliser l'indexation du parc pour ajouter des données personnalisées que vous pouvez utiliser pour interroger et agréger des données dans les applications Fleet Hub.

Comment fonctionnent les alarmes Fleet Hub

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

1. Créez une requête pour agréger des données : spécifiez une requête qui regroupe les appareils que vos utilisateurs souhaitent cibler à l'aide de champs de recherche.
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 Fleet Hub avertit lorsque les appareils spécifiés sont en alarme.

Comment fonctionnent les offres d'emploi chez Fleet Hub

Vous pouvez utiliser la console Fleet Hub 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 Fleet Hub.

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.

AWSet 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 pour fournir les fonctionnalités de vos applications Web Fleet Hub.

Le tableau suivant indique les AWS services que Fleet Hub for AWS IoT Device Management utilise 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 ajoutez 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, voir Qu'est-ce que c'est AWS IAM Identity Center ? et les identités des collaborateurs.
Créez des requêtes à l'aide de champs AWS gérés, de champs personnalisés et de tous les attributs de vos sources de données indexées.	AWS IoTindexation de la flotte	Utilisez le service d'indexation du parc pour indexer, rechercher et agréger vos données de registre, vos données parallèles et les 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 de la AWS IoT flotte indexe par défaut. Pour plus d'informations sur l'indexation du parc, consultez la section Indexation du parc.

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 de recherche 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 tombe en dessous d'une quantité spécifiée. Pour en savoir plusCloudWatch, consultez Qu'est-ce qu'Amazon CloudWatch ? Pour plus d'informations sur la façon AWS IoT Core de CloudWatch créer des métriques et des alarmes, voir Surveiller les AWS IoT alarmes et les métriques à l'aide deCloudWatch.

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 : `{"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 Fleet Hub for AWS IoT Device Management. Pour plus d'informations sur la création d'applications Fleet Hub et l'ajout d'utilisateurs à celles-ci, consultezFleet Hub pour la gestion des AWS IoT appareils pour les administrateurs.

Rubriques

Démarrer

Cette section contient des informations sur la prise en main des fonctionnalités des applications Web Fleet Hub pour la gestion des AWS IoT appareils.

Rubriques

Création de votre première requête requête requête requête

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

Prérequis

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

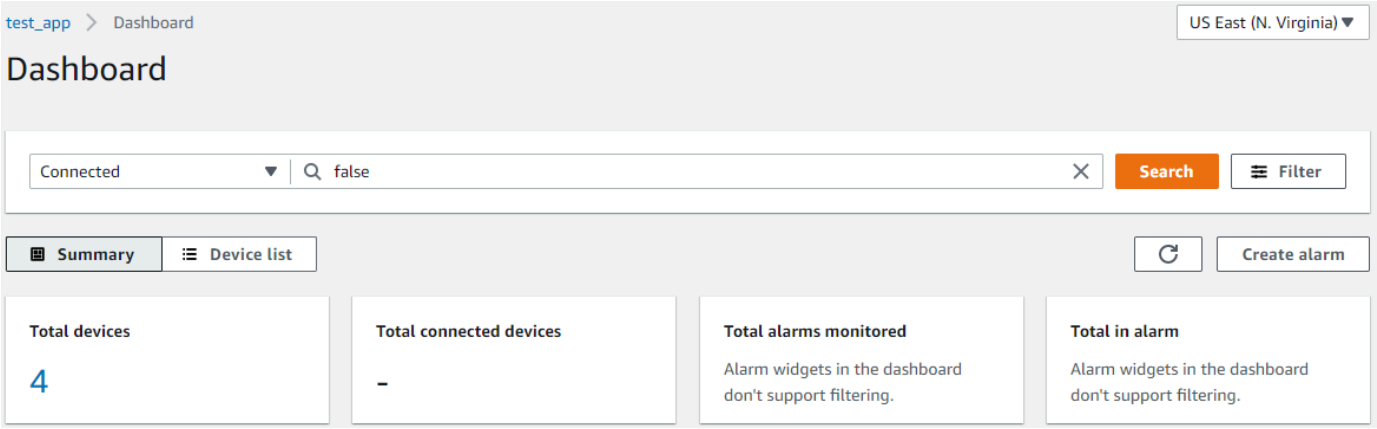
Création de votre première requête Fleet Hub

Création de votre première requête Fleet Hub

1. Accédez à votre application Fleet Hub.

   La vue du tableau de bord par défaut affiche la liste de tous les appareils contenant les attributs gérés et personnalisés. Les attributs qui contiennent le préfixe d'attributs sont des attributs personnalisés.

2. Dans le menu en haut de la page, choisissez Connecté dans tous les champs. Entrez **`false`** dans la zone de texte à côté du menu déroulant.



3. Pour effectuer la recherche, choisissez Rechercher. Vous voyez une liste de tous les appareils qui ne sont pas connectésAWS IoT Core.

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

Création de votre première alarme alarme Alarme

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

Prérequis

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

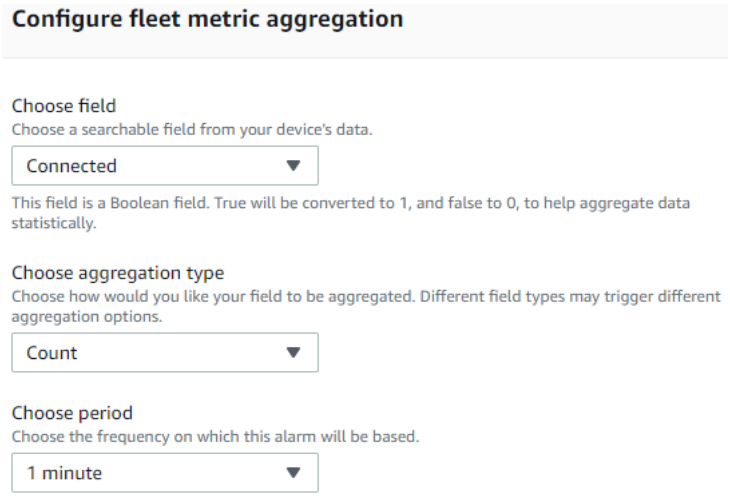
Création de votre première alarme alarme Alarme

Création de votre première alarme Fleet Hub d'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 requête simple, veuillez consulterthe section called “Création de votre première requête requête requête requête”. 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 le champ, choisissez Connecté. Ce AWS champ géré indique si un appareil est connecté àAWS IoT Core. Le menu Choisir un champ contient les AWS champs gérés et les champs personnalisés que votre administrateur a créés lors de l'indexation du AWS IoT parc.
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.

   Un exemple de paramètre pour Configurer l'agrégation des métriques du parc peut ressembler à ce qui suit :



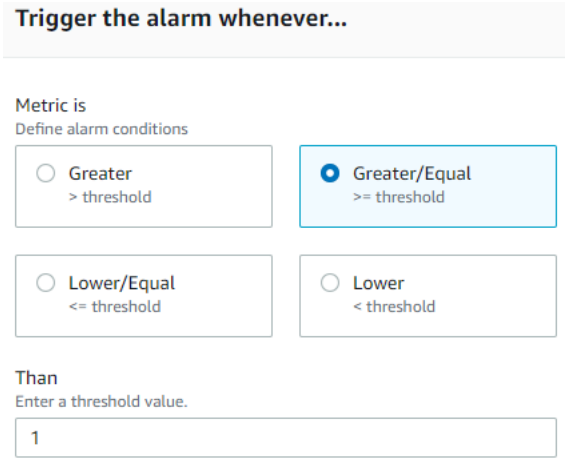
Choisissez Suivant.

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

   - Supérieur : alarmes lorsque la métrique et le type d'agrégation dépassent la valeur spécifiée.
   - Supérieur/Equal : alarme lorsque la métrique et le type d'agrégation sont égaux ou supérieurs à la valeur spécifiée.
   - Faible : alarmes lorsque la métrique et le type d'agrégation tombent en dessous de la valeur spécifiée.
   - Faible/Equal : alarme lorsque la métrique et le type d'agrégation sont égaux ou inférieurs à la valeur spécifiée.

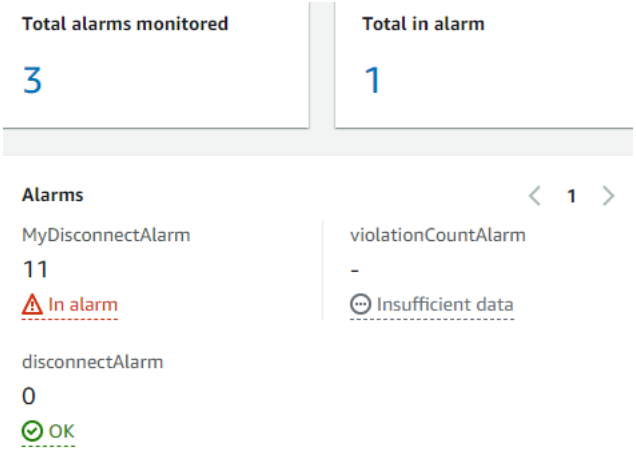
8. Dans la zone de texte Than, spécifiez la valeur à utiliser comme seuil pour l'alarme.

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

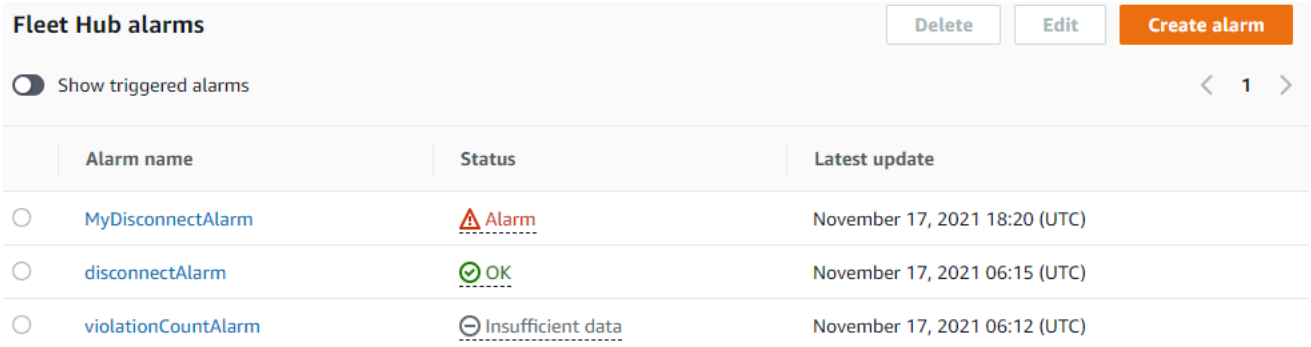


Choisissez Suivant.

9. Sur la page Notifier l'utilisateur, dans la section Notifier -- facultatif, entrez le nom de la liste d'e-mails qui contient les utilisateurs de votre organisation qui reçoivent des notifications lorsque l'alarme est active. Création d'une liste d'adresses e-mail séparées par des virgules pour remplir cette liste.
10. Dans la section Détails de l'alarme, entrez un nom pour votre alarme et, si vous le souhaitez, entrez une description pour votre alarme. Choisissez Suivant.
11. Sur la page Révision, vérifiez les informations que vous avez saisies sur les pages précédentes. Sélectionnez Submit (Envoyer). Vous revenez au tableau de bord par défaut.
12. Sur le tableau de bord par défaut, les widgets d'alarmes affichent des informations sur toutes les alarmes que vous avez créées.



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



Afficher les détails de l'appareil

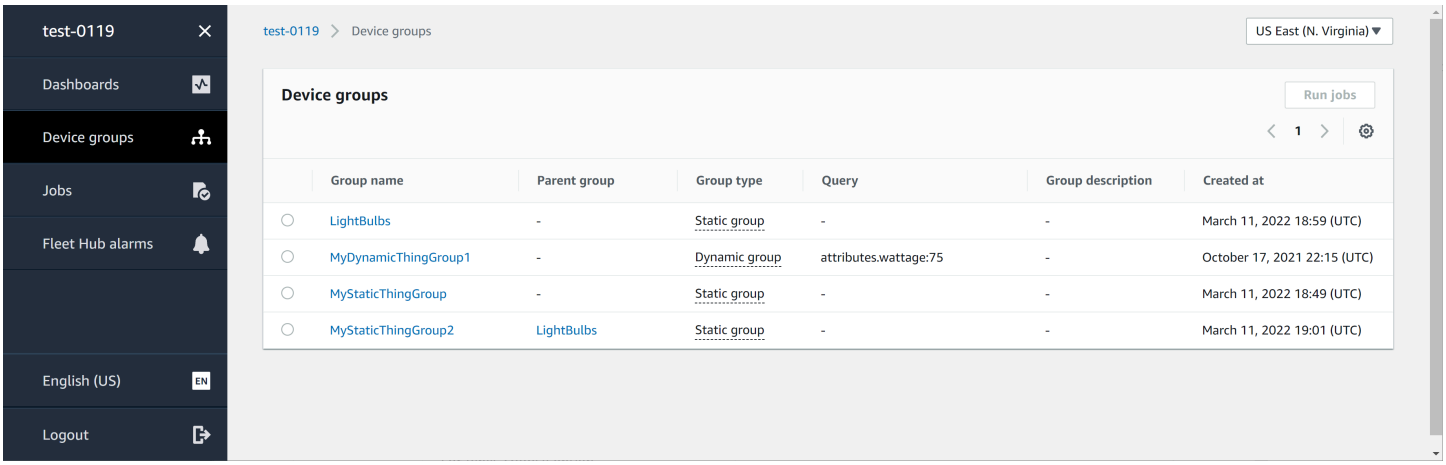
Cette rubrique explique les étapes à suivre pour afficher les détails relatifs à vos groupes d'appareils et à vos appareils.

Prérequis

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

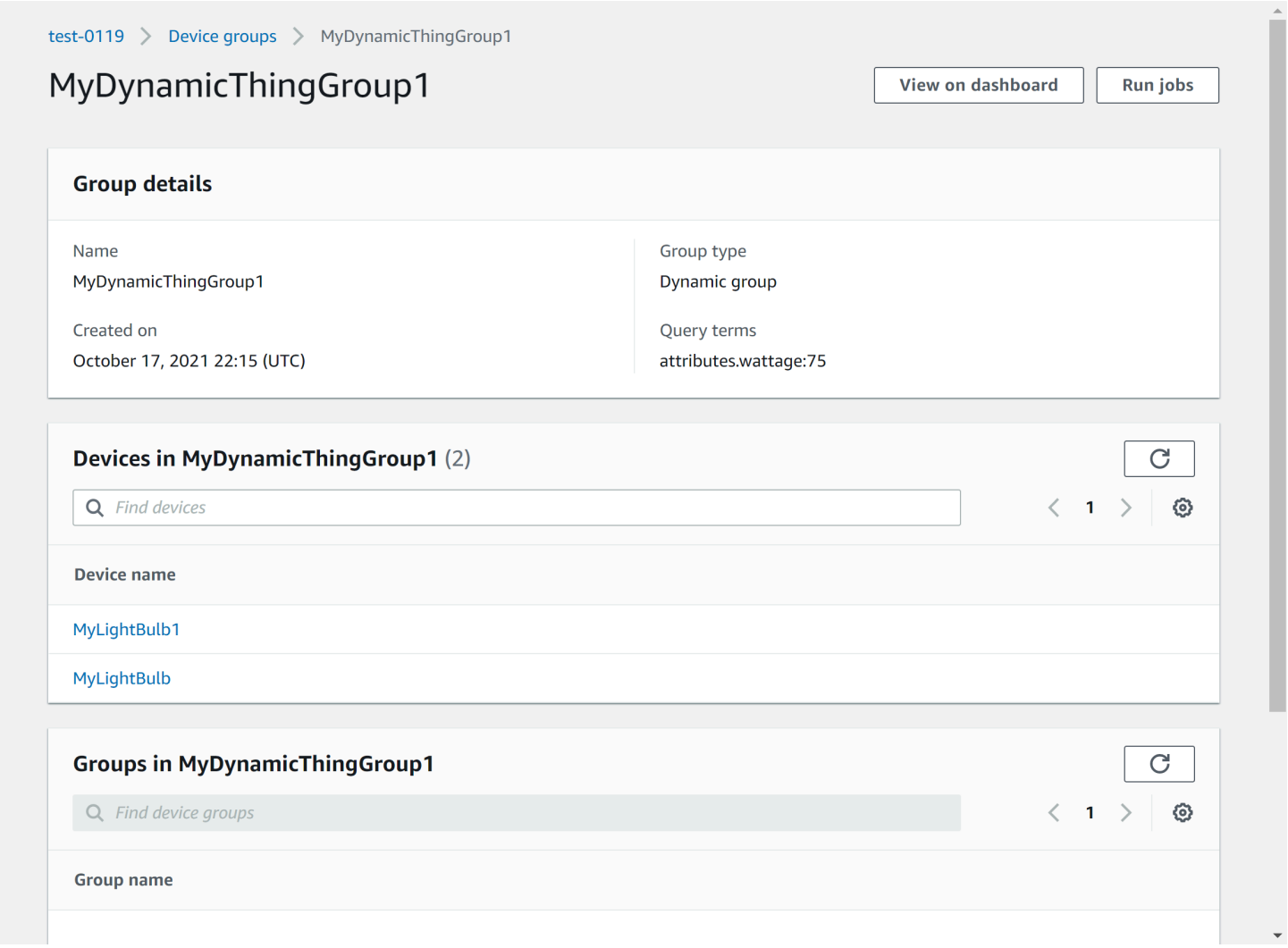
Groupes d'appareils

Lorsque vous vous connectez à votre application Web Fleet Hub, les 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 un appareil spécifique dans la colonne Nom de l'appareil de la section Appareils en ***XXX***.



Détails de l'appareil

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

> **Note**
>
> Si votre client utilise un identifiant client différent de celui de Thing Name lorsqu'il se connecte àAWS 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 : nom de la ressource objet qui représente votre appareil. Pour plus d'informations, voir Comment gérer les choses 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 d'objet. Pour de plus amples informations, veuillez consulter Types d'objet.

- Horodatage de la dernière connexion : horodatage de la dernière connexion de votre appareil. AWS IoT

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

- État de la dernière connexion — État de connexion de votre appareil àAWS IoT. Si votre appareil est connecté, la valeur est`true`. S'il n'est pas connecté, la valeur est`false`.

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

Données déclarées

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

- Champs de l'appareil : les champs indexés de votre appareil dans l'indexation du AWS IoT parc. Pour de plus amples informations, veuillez consulter 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 anonymes classiques et des ombres nommées. Pour de plus amples informations, veuillez consulter AWS IoTDevice Shadow.

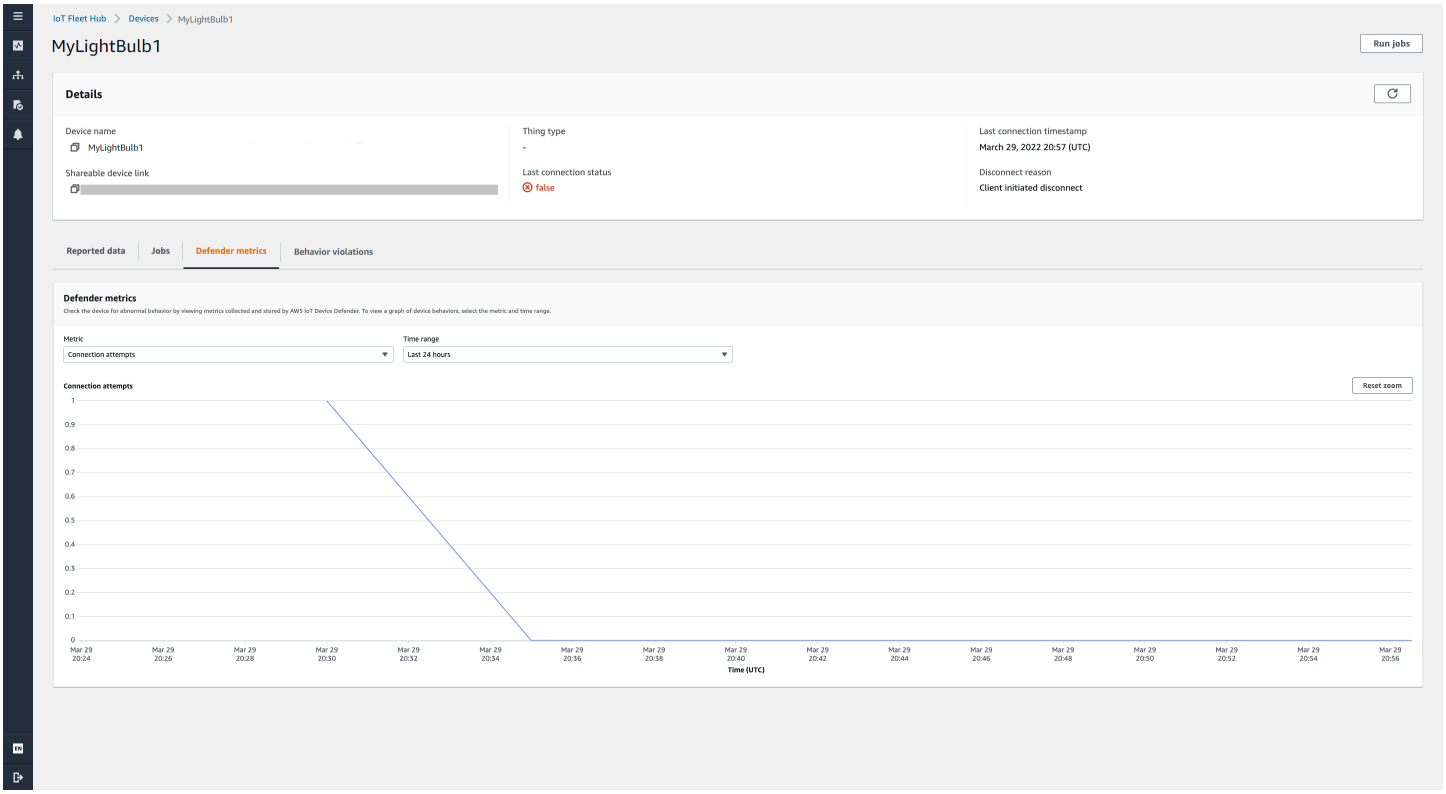
- Groupes d'appareils : groupes d'appareils associés à votre appareil. Les groupes d'appareils peuvent inclure à la fois des groupes d'objets statiques et des groupes d'objets dynamiques. Pour plus d'informations, voir Groupes d'objets statiques et Groupes d'objets dynamiques.

Tâches

La section Tâches affiche toutes les tâches en cours d'exécution sur l'appareil. Chaque tâche comporte une page de détails qui affiche des informations récapitulatives sur la tâche, notamment des informations sur la cible et l'exécution. Pour plus d'informations, consultez la section Utilisation des tâches et des modèles de tâches dans Fleet Hub pour la gestion des AWS IoT appareils et les tâches.

Statistiques de Defender

La section des statistiques de Defender affiche les AWS IoT Device Defender mesures associées à l'appareil actuellement sélectionné. Vous pouvez utiliser les données de mesures affichées pour visualiser le fonctionnement de votre appareil sur une période de votre choix. Pour consulter les données de Defender Metrics depuis votre application Fleet Hub, votre administrateur de 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 mesures pour vos appareils, consultez les sections Mesures personnalisées, Mesures côté appareil et Mesures côté cloud.



Violations du 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 de 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 la flotte. Pour de plus amples informations sur la configuration des violations de comportement dans un profil AWS IoT Device Defender de sécurité, veuillez consulter AWS IoT Device DefenderDétecter. Pour plus d'informations sur la façon de configurer les AWS IoT Device Defender violations, voir Gérer l'indexation du parc pour les applications Fleet Hub et Gérer 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 d'afficher 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 de the section called “Alarmes” l'indexation du AWS IoT parc. Pour plus d'informations sur l'indexation du parc, voir Indexation du parc.

Rubriques

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

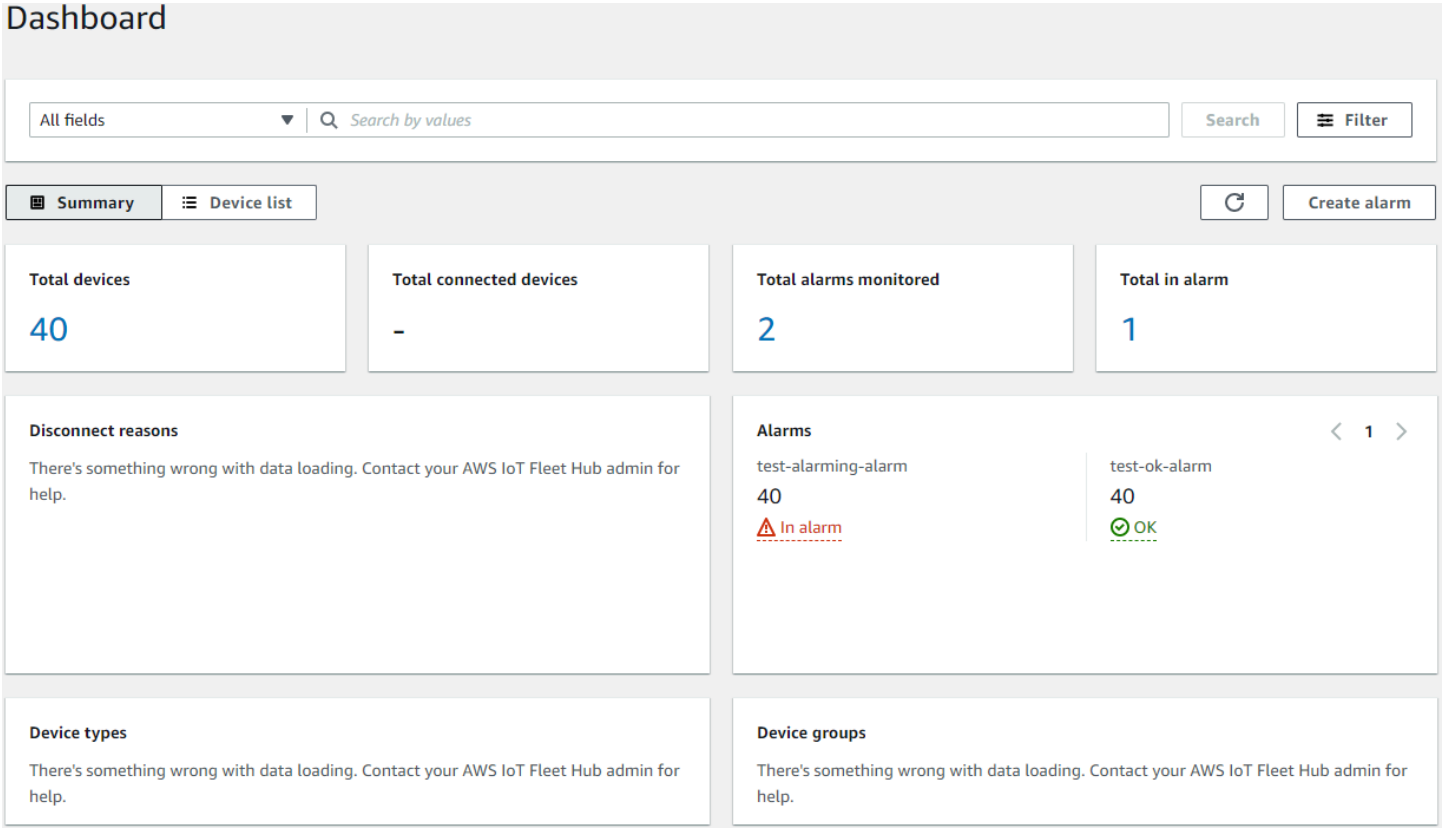
Afficher le tableau de bord

Lorsque vous vous connectez à votre application Web Fleet Hub for AWS IoT Device Management, vous voyez un tableau de bord qui présente deux vues des données relatives aux appareils de votre parc.

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

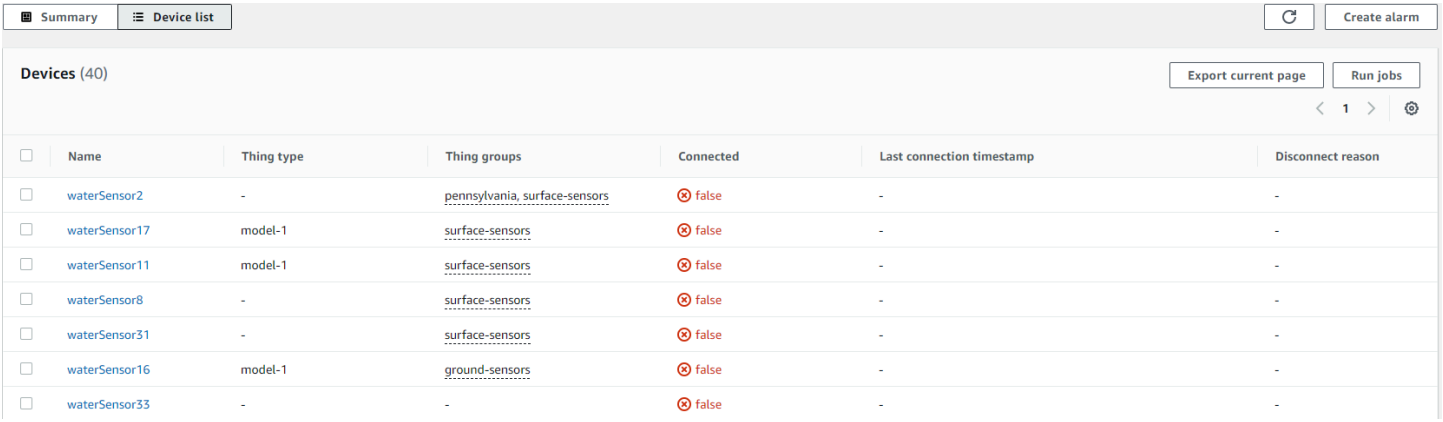


Liste des appareils

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
- L'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 ne télécharge que les données affichées sur la page en cours, pas 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 de Fleet Hub for AWS IoT Device Management et 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 sur les vues récapitulatives et de liste de votre tableau de bord à l'aide de requêtes. Vous filtrez les requêtes à l'aide de champs AWS gérés, de champs personnalisés et de tous les attributs de vos sources de données indexées issues de l'indexation du AWS IoT parc. Pour plus d'informations sur l'indexation du parc, voir Indexation du parc.

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

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

Création de requêtes

Les étapes suivantes décrivent comment créer une requête type.

Prérequis

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

Créez votre première requête Fleet Hub avec 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.

   Le tableau de bord par défaut contient des onglets de navigation, dont un pour la liste des appareils. Il affiche le nombre total d'appareils du AWS IoT Core compte associé et le nombre total d'appareils connectés.
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.

   Par défaut, le tableau de bord de la liste des appareils affiche les attributs personnalisés et gérés pour tous les appareils du AWS IoT Core compte associé.
4. En haut de la page, saisissez le mot clé que vous souhaitez inclure dans votre requête. Les requêtes par mot clé s'appliquent à tous les champs.
5. En haut de la page, choisissez Filtrer.
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 effectuer votre recherche, choisissez Appliquer les filtres. Les résultats indiquent tous les appareils qui correspondent à votre requête.

Utilisation des tâches et des modèles de tâches dans Fleet Hub pourAWS IoTGestion des appareils

> **Note**
>
> La fonction des modèles de tâche est en version préliminaire et susceptible d'être modifiée.

Une tâche est une opération distante qui est envoyée vers un ou plusieurs appareils connectés à et exécutée par celui-ci.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 à partir de Fleet Hub pourAWS IoTApplications Web Device Management. Les administrateurs de votre organisation créent des modèles de travail dans leAWS IoTconsoles et attaches qui rendent les modèles disponibles pour les utilisateurs de Fleet Hub. Dans votre application Fleet Hub, vous spécifiez les appareils ou un groupe d'appareils sur lesquels la tâche s'exécute.

Les administrateurs créent également des groupes d'appareils que vous pouvez afficher dans votre application. Pour voir ces groupes, choisissezGroupes d'appareilsdans le volet de navigation. Lorsque vous spécifiez un groupe d'appareils en tant que cible, vous pouvez spécifier l'un des deux types d'options suivants pour l'exécution de la tâche.

- instantané : Le travail est exécuté une fois.
- continu : Après son exécution initiale, la tâche s'exécute sur n'importe quel appareil ajouté au groupe.

Pour de plus amples informations sur la création et la gestion de modèles de tâche, veuillez consulterModèles de tâche. Pour de plus amples informations sur le fonctionnement des tâches, veuillez consulterTâches.

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. UNDERSélection de cibles Job, choisissez oucontinuouinstantané.
4. Sélectionnez un modèle de tâche. Vérifiez que le texte sousRésumé des Job d'décrit le type de tâche que vous souhaitez exécuter.
5. Le cas échéant, entrez un nom pour la tâche.
6. Cliquez sur Run (Exécuter).

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

- L'onglet Liste des appareils sur le tableau de bord.
- Page de détails d'un appareil spécifique.
- Page Groupes d'appareils.
- Page de détails d'un groupe d'appareils spécifique.

Affichage et gestion de tâches d'

Vous pouvez voir les tâches exécutées dans votre flotte aux emplacements suivants.

- La page Liste des tâches — Cette page affiche toutes les tâches exécutées dans votre flotte. Pour afficher cette page, choisissezTâchesdans le volet de navigation.
- Page de détails d'un appareil spécifique : cette page affiche toutes les tâches exécutées sur l'appareil.

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

- Nombre de pistes.
- Nombre de pistes annulées.
- Nombre de courses réussies.
- Nombre de exécutions ayant échoué.
- Nombre d'essais rejetés.
- Nombre d'essais en file d'attente.

- Nombre d'essais en cours.
- Nombre de pistes supprimées.
- Nombre de points d'attente.

Pour annuler une tâche, sélectionnez la tâche et choisissezAnnuler.

Alarmes

Cette section explique comment Fleet Hub pourAWS IoTLes alarmes Device Management fonctionnent et vous guide à travers les étapes nécessaires pour créer une alarme.

Lorsque vous créez une alarme Fleet Hub, elle s'applique à tous les appareils actuellement affichés dans votre tableau de bord. Si vous n'appliquez aucune requête, l'alarme s'applique à tous les appareils de votre flotte. 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 des mesures Amazon CloudWatch (CloudWatch) en combinaison avec des champs interrogeables de laAWS IoTService d'indexation de flotte pour créer des alarmes CloudWatch. Par exemple, vous pouvez créer une alarme qui génère un message Amazon Simple Notification Service (Amazon SNS) chaque fois que le niveau moyen de batterie des appareils de votre flotte tombe en dessous de 50 %.

Les alarmes Fleet Hub utilisent leGetStatisticsetGetPercentilescapacités 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 alarmants qui s'appliquent aux valeurs suivantes de l'attribut spécifié.

- Maximum
- Nombre
- Somme
- Minimum
- Moyenne
- Valeurs du 10e, 50e, 90e, 95e ou 99e centile

Pour plus d'informations sur l'interrogation des données agrégées dans le service d'indexation de la flotte, consultezInterrogation des données agrégées.

Le tableau suivant répertorie quelques exemples des types d'agrégation disponibles pourAWS-champs 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
Connected(AWSchamp booléen géré) Pour`true`est 1. Pour`false`est 0.	• Maximum • Nombre • Somme • Minimum • Moyenne
niveau de batterie shadow.reported.(champ d'agrégation numérique créé dans le service d'indexation de flotte)	• Maximum • Nombre • Somme • Minimum • Moyenne • p10 (10e centile) • p50 (50e centile) • p90 (90e centile) • p95 (95e centile) • p99 (99e centile)

En plus de spécifier des champs et des types d'agrégation, vous spécifiez également les valeurs suivantes.

- Durée (1 minute ou 5 minutes) nécessaire au seuil d'alarme spécifié pour déclencher l'alarme.
- L'un des opérateurs de comparaison suivants à appliquer à votre champ et à votre type d'agrégation spécifiés.
  - Plus grand
  - Plus grand, égal

  - LOWER
  - Lower/Egal
- La valeur à utiliser avec l'opérateur de comparaison spécifié.
- Liste des adresses e-mail des personnes de votre organisation qui reçoivent des messages Amazon SNS chaque fois que votre alarme est déclenchée.
- Nom d'alarme.

Pour créer une alarme Fleet Hub, consultezthe section called “Création d'alarmes”.

Création d'alarmes

Cette rubrique présente les étapes nécessaires pour créer un hub de flotte pourAWS IoTAlarme de gestion des appareils. Il suppose que votre administrateur a créé un champ d'agrégation à partir d'un champ d'ombre de périphérique nomméniveau de batterie shadow.reported.. Ce champ personnalisé indique le niveau de batterie d'un appareil. Vous devez demander à votre administrateur de créer des champs personnalisés interrogeables dans leAWS IoTService d'indexation de flotte.

L'alarme que vous créez envoie un message Amazon Simple Notification Service (Amazon SNS) à une liste de personnes de votre organisation lorsque le niveau moyen de batterie 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 obtenir des instructions sur la création d'une requête simple, veuillez consulterthe 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 flotte.
3. Sur la page du tableau de bord par défaut, choisissezCréer une alarme.
4. Dans la pageConstruire une métrique d'agrégation, vérifiez que votre requête apparaît sousRequête cible. DansConfigurer l'agrégation des métriques deSection, pourChoisir un champ, choisissezniveau de batterie shadow.reported.. Ce menu contient le menuAWS-les champs gérés et les champs personnalisés que votre administrateur a créés dans leAWS IoTService d'indexation de flotte.
5. PourChoisir un type d'agrégation, choisissezMoyenne. Ce choix fonde l'alarme sur la valeur moyenne de la batterie de votre parc d'appareils.

6. PourChoisir une période, choisissez1 minute. Cela déclenche l'alarme lorsque votre parc d'appareils reste dans l'état alarmant spécifié pendant une minute.

   Choisissez Next (Suivant).
7. Dans la pageDéfinir le seuil, dans laDéclenchez l'alarme dès que...Section, choisissezLower/Egal. Cela déclenche l'alarme lorsque la valeur moyenne de la batterie tombe en dessous de la valeur spécifiée.
8. DansTHANzone de texte, entrez 50.

   Choisissez Next (Suivant).
9. Dans la pageNotifier l'utilisateur, dans laNotify — facultatif, entrez un nom pour la liste de diffusion 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. DansDétails de l'alarme, entrez un nom pour votre alarme et, éventuellement, entrez une description pour votre alarme. Choisissez Next (Suivant).
11. Dans la pageVérification, vérifiez les informations que vous avez saisies sur les pages précédentes. Choisissez Submit (Envoyer). Vous revenez au tableau de bord par défaut.
12. Sur le tableau de bord par défaut, dans le volet gauche de navigation, choisissezAlarmes 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 aider à résoudre les problèmes en tant qu'utilisateur de Fleet Hub.

Symptôme	Solution
Je n'arrive pas à ajouter d'autres filtres ou termes à ma requête.	Assurez-vous de ne pas avoir atteint la limite de quatre termes de requête et de 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.	Le chargement des données d'alarme prend quelques minutes.

Symptôme	Solution
Je dois changer les appareils que mon alarme cible.	Accédez à votre tableau de bord et modifiez la requête.
Un message d'erreur s'affiche lorsque je modifie la 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.
L'état de connectivité de mon « objet » n'est pas indexé par Fleeting Indexing.	Assurez-vous que votre client utilise le même ID client que Thing Name lorsqu'il se connecte àAWS IoT. Si votre client utilise un identifiant différent de celui de Thing Name lorsqu'il se connecte àAWS IoT, l'état de connectivité de votre « objet » ne sera pas indexé par Fleet Indexing.

Gestion des périphériques. Gestion desAWS IoT périphériques

La surveillance constitue une part importante de la gestion de la fiabilité, de la disponibilité et des performances de Fleet et Hub et de vos autresAWS solutions. AWSfournit les outils de flotte suivants.

- AWS CloudTrail capture les appels d'API et les événements associés créés par ou au nom de votre compte AWS et envoie les fichiers journaux à un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes qui ont appelé AWS, l'adresse IP source à partir de laquelle les appels ont été émis, ainsi que le moment où les appels ont eu lieu. Pour de plus amples informations, veuillez consulter le Guide de l'utilisateur AWS CloudTrail.

Rubriques

Enregistrement des appels d'API de Fleet Hub pour la gestion desAWS IoT appareils avecAWS CloudTrail

Fleet Hub pour la gestion desAWS IoT appareils est intégré àAWS CloudTrail. Le CloudTrail service enregistre les actions effectuées par un utilisateur, un rôle ou unAWS service dans Fleet et Hub. CloudTrail capture les appels d'API vers Fleet et Hub en tant qu'événements. Les appels capturés incluent les appels provenant de la console Fleet et Hub et les appels de code vers les opérations API Fleet et Hub.

Si vous créez un journal d'activité, vous pouvez activer la livraison continue d' CloudTrail événements dans un compartiment Amazon S3, y compris des événements Fleet et Hub. Si vous ne configurez pas de journal de suivi, vous pouvez toujours afficher les événements les plus récents dans la CloudTrail console dans Event.

À l'aide des informations CloudTrail collectées, vous pouvez déterminer la demande qui a été envoyée à Fleet et et Hub, l'adresse IP à partir de laquelle la demande a été effectuée, l'auteur et la date de la demande, ainsi que d'autres informations.

Pour en savoir plus CloudTrail, consultez le Guide deAWS CloudTrail l'utilisateur.

Informations sur Fleet Hub dans CloudTrail

AWS CloudTrail est activé sur votre compte AWS lorsque vous créez le compte. Lorsqu'une CloudTrail activité a lieu dans GestionAWS des événements. Vous pouvez afficher, rechercher et télécharger les événements récents dans votre AWS compte. Pour de plus amples informations, veuillez consulter Affichage des CloudTrail événements.

Pour un enregistrement continu des événements dans votreAWS compte, y compris les événements Fleet et Hub, créez un journal de suivi. Un journal d'activité CloudTrail permet de livrer des fichiers journaux à un compartiment Amazon Simple Storage Service (Amazon S3). Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions AWS. Le journal d'activité consigne les événements de toutes les Régions dans la partition AWS et livre les fichiers journaux dans le compartiment Amazon S3 de votre choix.

Vous pouvez également configurer d'autresAWS services afin d'analyser plus en profondeur les données d'événement collectées dans CloudTrail les journaux. Pour en savoir plus, consultez les ressources suivantes :

- Présentation de la création d'un journal d'activité
- CloudTrail services et intégrations pris en charge
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers CloudTrail journaux 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 deAWS IoT l'API. Par exemple, les appels adressés 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 :

- Si la demande a été effectuée avec les informations d'identification utilisateur racine ou AWS Identity and Access Management
- 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 effectuée par un autre service AWS

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

Comprendre les entrées du fichier journal de Fleet Hub forAWS IoT Device Management

Un journal d'activité est une configuration qui permet d'envoyer des événements sous forme de fichiers journaux à un compartiment Simple Storage Service (Amazon S3) que vous spécifiez.

CloudTrail les fichiers journaux peuvent contenir une ou plusieurs entrées. 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 requête, etc.

CloudTrail les fichiers journaux ne constituent pas une trace de pile ordonnée retraçant les appels d'API publics. Ils ne suivent aucun ordre précis.

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.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- 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 140-2 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 (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l'information fédérale).

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 Name (Nom). Cela inclut lorsque vous travaillez avec Fleet Hub ou un autre utilisateur Services AWS à l'aide de la console, de l'API ou AWS des SDK. 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
- Authentification par des identités
- Gestion des accès à l'aide de politiques
- Comment Fleet Hub for AWS IoT Device Management fonctionne avec IAM
- Exemples de politiques basées sur l'identité pour Fleet Hub for AWS IoT Device Management
- Résolution des problèmes Fleet Hub for AWS IoT Device Management d'identité et d'accès

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 la section 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 vous-même les demandes, consultez la section Signature des demandes AWS 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 en savoir plus, consultez Authentification multifactorielle dans le Guide de l’utilisateur AWS IAM Identity Center et Utilisation de l’authentification multifactorielle (MFA) dans l’interface AWS 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 root, consultez Tâches nécessitant des informations d’identification d’utilisateur root 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 une seule 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 tels que les 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 de faire pivoter les 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 avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des 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 en savoir plus, consultez Quand créer un utilisateur IAM (au lieu d'un rôle) 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. Vous pouvez assumer temporairement un rôle IAM dans le en AWS Management Console changeant de rôle. 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 Utilisation de rôles IAM 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 la rubrique 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 connaître la différence entre les rôles et les politiques basées sur les ressources pour l'accès entre comptes, consultez la section Accès aux ressources entre comptes 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 la politique relative à la transmission de demandes FAS, consultez Sessions de transmission 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 une fonction du 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 instance EC2 et qui envoient des demandes d'API. AWS CLI AWS Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un AWS rôle à une instance EC2 et le mettre à la disposition de 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 qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le Guide de l'utilisateur IAM.

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, consultez Quand créer un rôle IAM (au lieu d'un utilisateur) 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 Création de politiques IAM 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. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. 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 (ACL)

Les listes de contrôle d'accès (ACL) vérifie quels principals (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et Amazon VPC sont des exemples de services qui prennent en charge les ACL. AWS WAF Pour en savoir plus sur les listes de contrôle d'accès, consultez Vue d'ensemble des listes 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 remplace 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 (SCP) — Les SCP sont des 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 les politiques de contrôle des services (SCP) 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 organisations et les SCP, consultez Fonctionnement des SCP dans le Guide de l'utilisateur AWS Organizations .

- 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 séance 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

Fonction IAM	Assistance Fleet Hub
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition d'une politique	Oui

Fonction IAM	Assistance Fleet Hub
ACL	Non
ABAC (étiquettes dans les politiques)	Oui
Informations d’identification temporaires	Oui
Autorisations de principal	Oui
Fonctions 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 Création de politiques IAM 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. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. 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 entre comptes 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 la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur d'IAM.

Actions politiques pour Fleet Hub

> **Note**
>
> Les applications Fleet Hub utilisent la politique `AWSIoTFleetHubFederationAccess` gérée. Pour plus d'informations, consultez ???.

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 stratégie 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 afficher la liste des types de ressources Fleet Hub et leurs ARN, consultez Ressources définies par Fleet Hub for AWS IoT Device Management dans la Référence de l'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 (ACL) dans Fleet Hub

Prend en charge les listes ACL	Non

Les listes de contrôle d'accès (ACL) vérifient quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès 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

Prend en charge ABAC (étiquettes 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 l'ABAC, consultez Qu'est-ce que le contrôle d'accès basé sur les attributs (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 Changement de rôle (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 les politiques relatives à l'envoi de demandes FAS, consultez la section Sessions d'accès transmises.

Rôles de service pour Fleet Hub

Prend en charge les fonctions du service	Oui

Une fonction 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 une fonction du 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 dans l'onglet JSON 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 format des ARN pour chacun des types de ressources, veuillez consulter la rubrique Actions,

ressources et clés de condition pour Fleet Hub for AWS IoT Device Management dans la Référence de l'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.
- Accorder 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 de IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utiliser 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 IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : IAM Access Analyzer 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 politique 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 le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Configuration de l'accès aux API protégé par 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 stratégie 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 stratégie.

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 plus d'informations, consultez ???.

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 (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour en savoir plus, 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 à des 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 connaître la différence entre l'utilisation de rôles et de politiques basées sur les ressources pour l'accès entre comptes, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur d'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 :

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- Architecture axée sur la sécurité et la conformité HIPAA sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes à la loi HIPAA.

  > **Note**
  >
  > Tous ne Services AWS sont pas éligibles à la loi HIPAA. Pour plus d'informations, consultez le HIPAA Eligible Services Reference.

- 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 plusieurs 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 ReadOnlyd'accès AWS géré 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 : AWSIoTFleetHubFederationAccess

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 les données métriques. 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.

```
{
    "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 Defender métriques dans les applications Fleet Hub.	4 avril 2022
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 opération	24 mai 2021

Modification	Description	Date
	s CRUD sur des AWS IoT tâches.	
AWSIoTFleetHubFederationAccess – Mise à jour d'une politique existante	Fleet Hub a supprimé les autorisations pour les API de tableau de bord Fleet Hub non prises en charge.	12 avril 2021
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 un problème de confusion chez les 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 la *`région`* correspond à votre région Fleet Hub et que l'*`identifiant de compte correspond`* 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.

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

Historique de la documentation

Le tableau suivant décrit les mises à jour apportées à la documentation de Fleet Hub. Pour des modifications dansAWSstratégies gérées pour Fleet Hub, voirAWSstratégies gérées pour Fleet Hub pourAWS IoTGestion des appareils.

Modification	Description	Date
Fleet Hub pourAWS IoTDisponibilité générale de Device Management	Contenu mis à jour pour refléter les améliorations apportées à Fleet Hub pourAWS IoTGestion des périphériques au cours de la période de version prélimina ire.	25 mai 2021.
Version préliminaire de Fleet Hub pourAWS IoTGestion des appareils	Publication de la version préliminaire duFleet Hub pourAWS IoTGuide de l'utilisa teur de Device Management.	16 décembre 2020.

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.