Utiliser l'API Umbrella Reporting via Postman

Table des matières

Introduction

Ce document décrit comment utiliser l'API Cisco Umbrella Reporting dans Postman.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur Cisco Umbrella.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Aperçu

L'API Umbrella a été publiée en septembre 2022, offrant une plate-forme conviviale et sécurisée qui permet aux utilisateurs de s'appuyer sur Umbrella, de l'étendre et de l'intégrer.

Les terminaux de l'API Umbrella sont hébergés sur api.umbrella.com, avec des chemins regroupés par exemple d'utilisation. Les clés d'API peuvent être gérées à la fois dans le tableau de bord Umbrella, sous Admin > clés d'API, et par programme avec l'API KeyAdmin. Chaque clé peut être configurée de manière granulaire avec plusieurs étendues regroupées en cinq cas d'utilisation principaux :

- Les terminaux API d'administration vous permettent de provisionner et de gérer les clés et

les utilisateurs de l'API Umbrella, d'afficher les rôles et de gérer les clients pour les fournisseurs et les fournisseurs gérés.
- Les terminaux API d'authentification vous permettent d'autoriser les intégrations d'autres services à la plate-forme Umbrella.
- Les déploiements de terminaux API vous permettent de provisionner, surveiller et gérer des réseaux et d'autres entités, et de les sécuriser en les configurant dans vos politiques Umbrella existantes.
- Les stratégies et les points de terminaison API vous permettent de provisionner et de gérer les listes de destinations et les destinations par liste.
- Les points de terminaison API de rapports vous permettent de lire et d'auditer les informations de sécurité en temps réel relatives à vos déploiements. L'API de découverte des applications Umbrella fournit des informations sur vos applications basées sur le cloud.

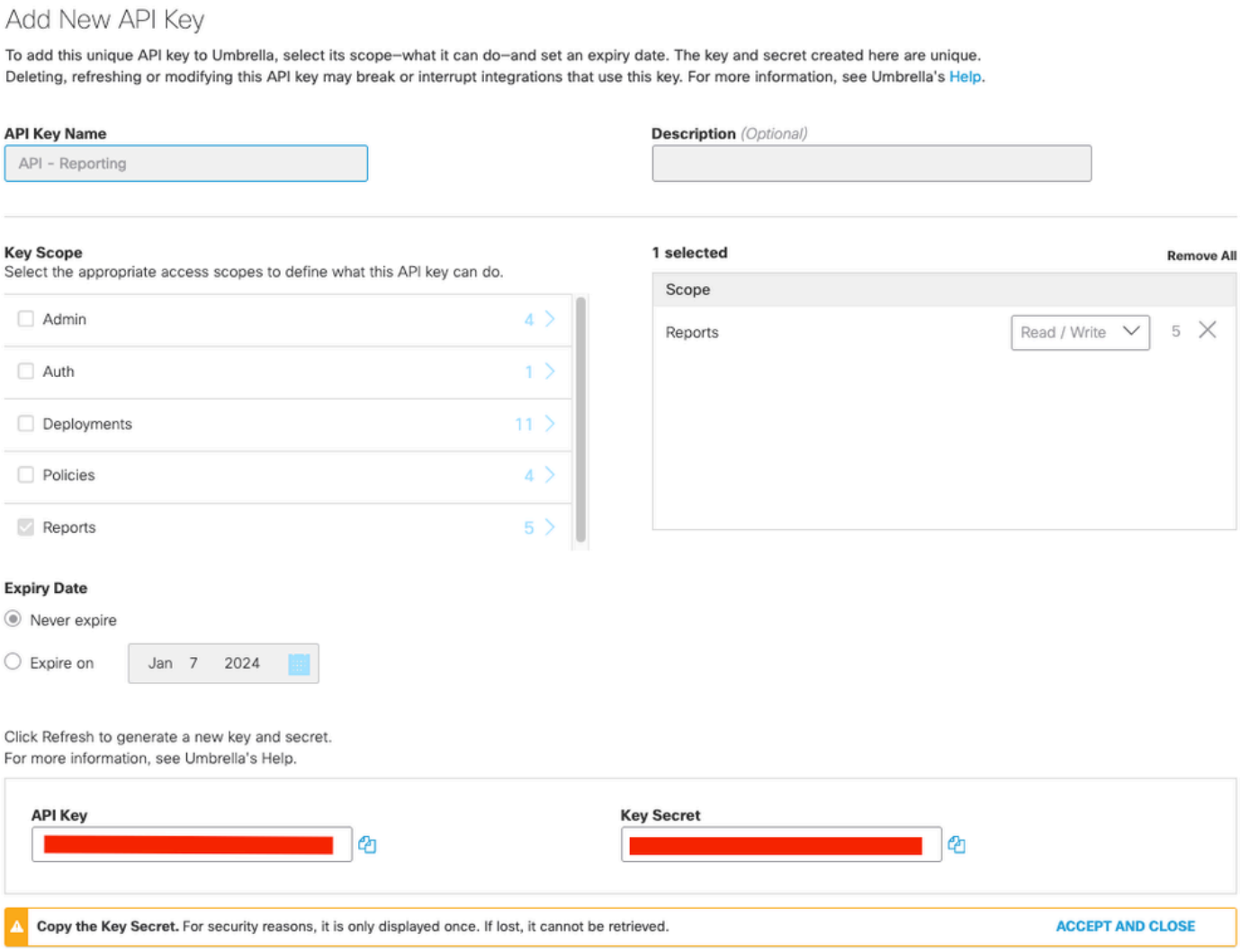
Cet article explique comment collecter des rapports de recherche d'activité via l'API.

Procédure-Cadre

1. Dans le tableau de bord Umbrella, accédez à Admin > API Keys.

2. Sélectionnez API Keys > Add.

3. Sous Portée de la clé, sélectionnez Rapports, puis Créer une clé.



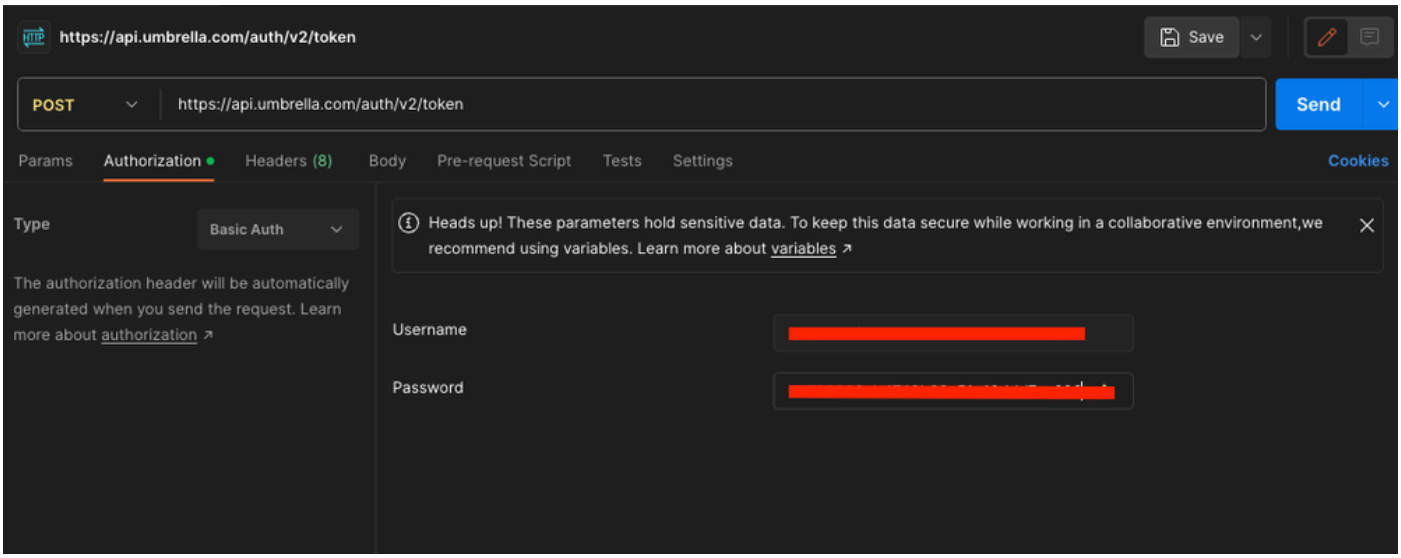
21495050167956

Les administrateurs peuvent ajuster le niveau d'accès par étendue entre Lecture/Écriture et Lecture seule, en fonction de l'utilisation prévue de chaque clé API, tandis que les clés API peuvent être configurées pour expirer à une date prédéfinie. Vous devez collecter la clé/le secret API à cette étape, car ils sont actuellement visibles et ne peuvent pas s'afficher par la suite.

Les informations d'identification API génèrent des jetons d'accès API valides pendant 60 minutes. Cette procédure prend en charge le flux d'informations d'identification du client OAuth 2.0. Dans les environnements Umbrella multiorganisations ou fournisseurs de services, les informations d'identification de l'API de l'organisation parent peuvent être utilisées pour générer des jetons d'accès avec les mêmes étendues pour une organisation enfant spécifiée au cours du processus d'autorisation.

Procédure Postman

Au début, vous devez créer un jeton d'accès OAuth 2.0. Les chemins d'authentification de l'API Umbrella commencent par https://api.umbrella.com/auth/v2. Lors de la soumission d'une requête POST et d'une clé d'API utilisateur en tant que nom d'utilisateur et mot de passe d'API en tant que mot de passe, un jeton d'accès est généré.

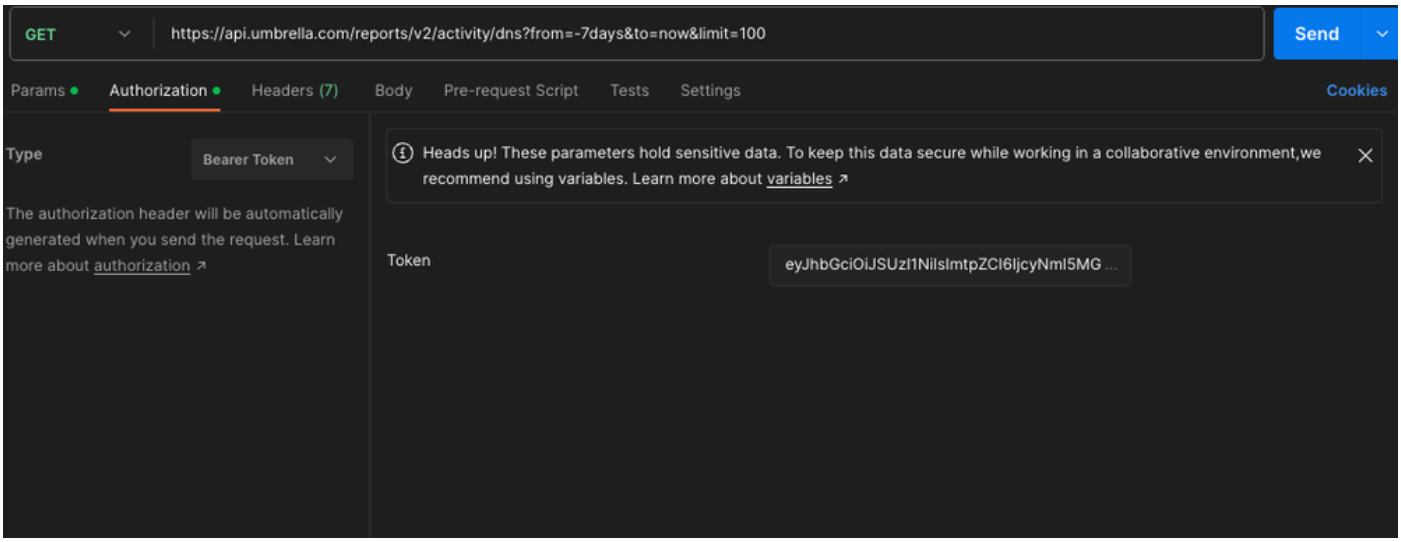


21606708808468

21607051456276

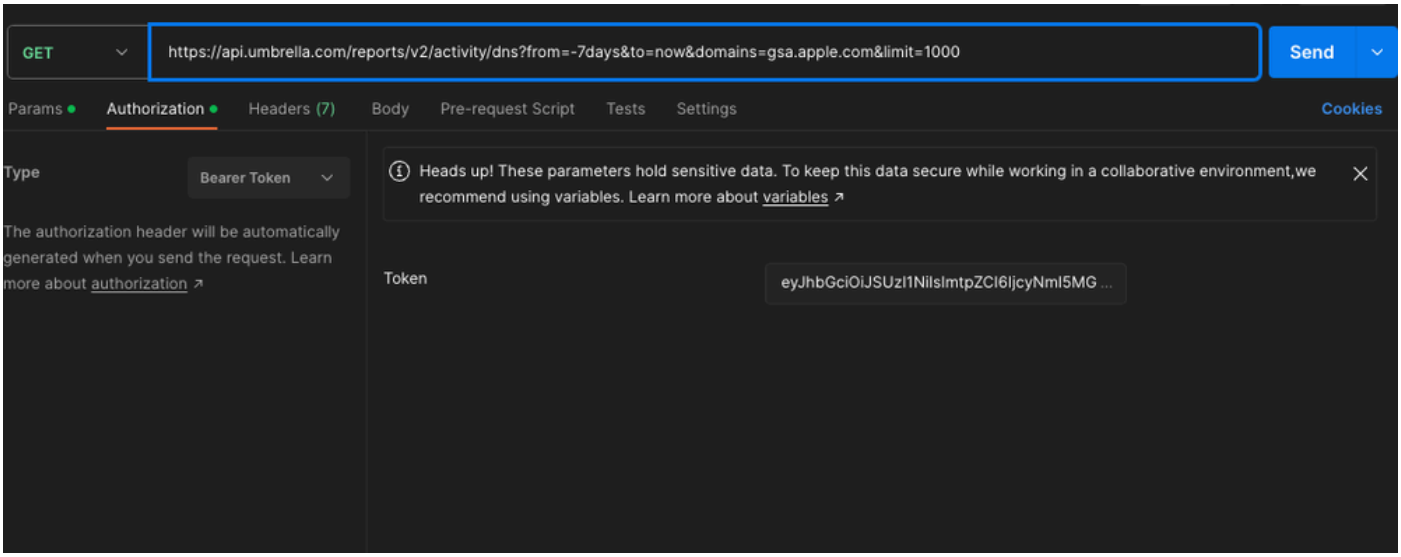
À cette étape, vous devez collecter le jeton d'accès. Vous pouvez désormais récupérer des informations à l'aide du jeton d'accès.

Vous devez sélectionner la méthode GET et entrer à la fois le chemin d'accès de votre API (y compris le paramètre requis) et le jeton d'accès. Dans cet exemple, vous pouvez récupérer 100 rapports de la recherche d'activité exclusivement pour le trafic DNS des 7 derniers jours.



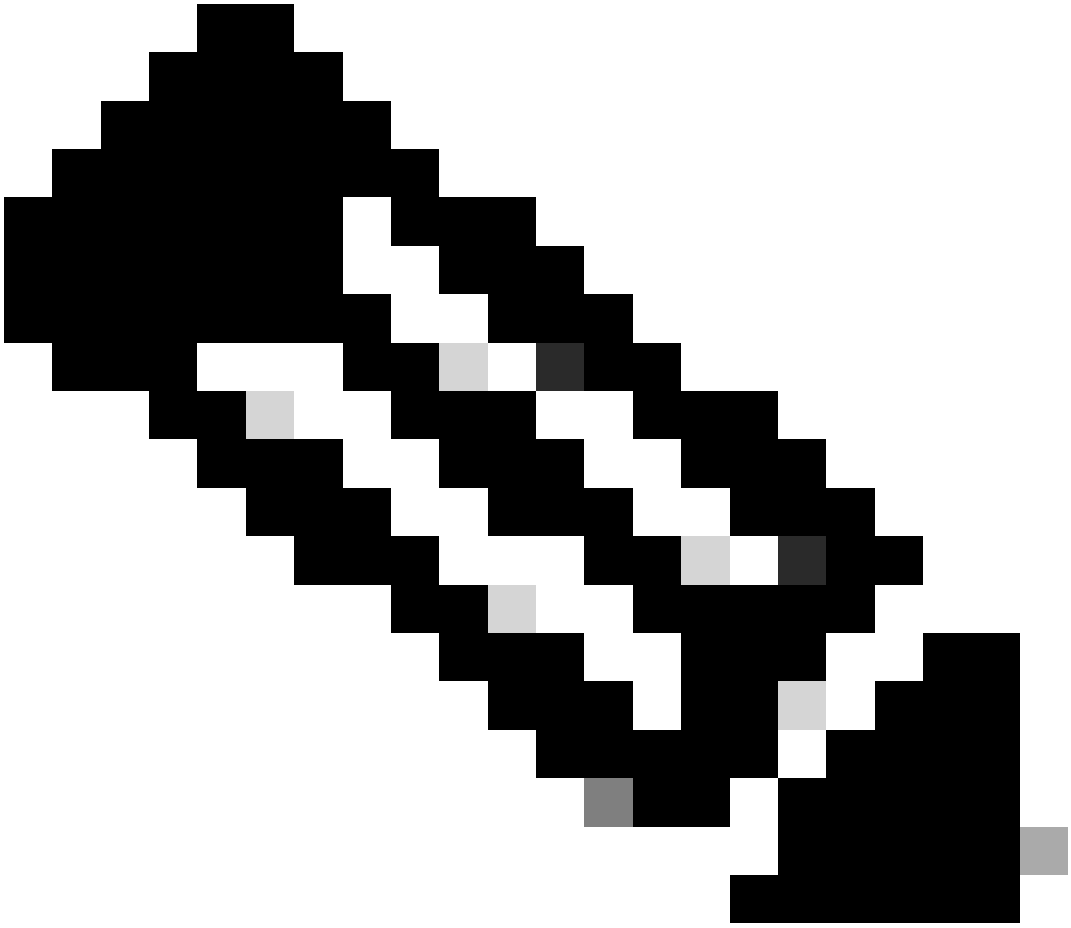
21607952074772

Dans un autre exemple, vous pouvez tenter d'extraire 1 000 rapports de la recherche d'activité, exclusivement pour le trafic DNS des 7 derniers jours, en particulier pour le domaine « gsa.apple.com ».



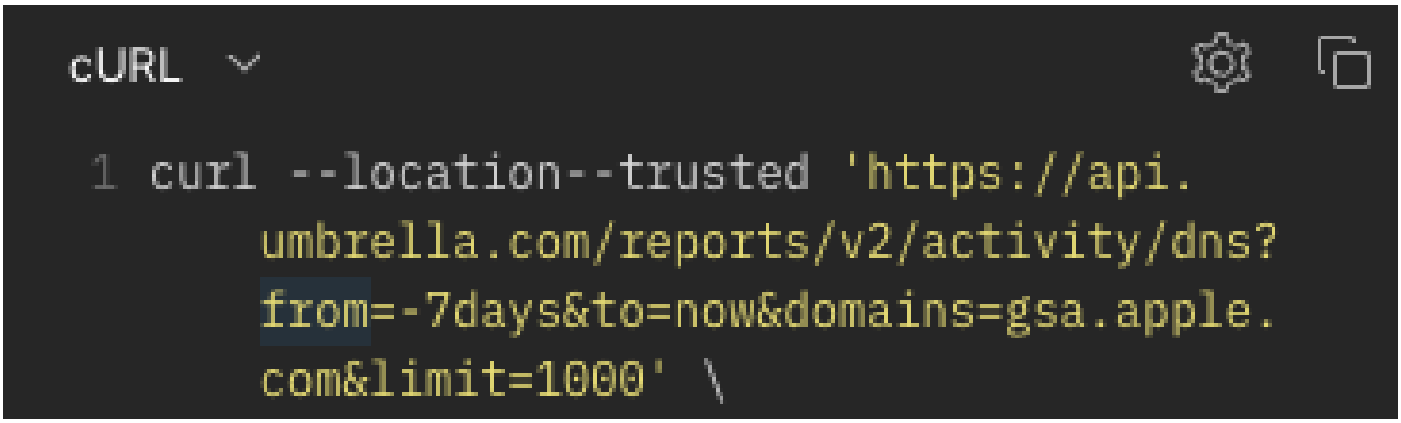
21607927544468

Vous pouvez consulter Request Query Parameters pour découvrir des paramètres supplémentaires que vous pouvez utiliser dans votre requête API.



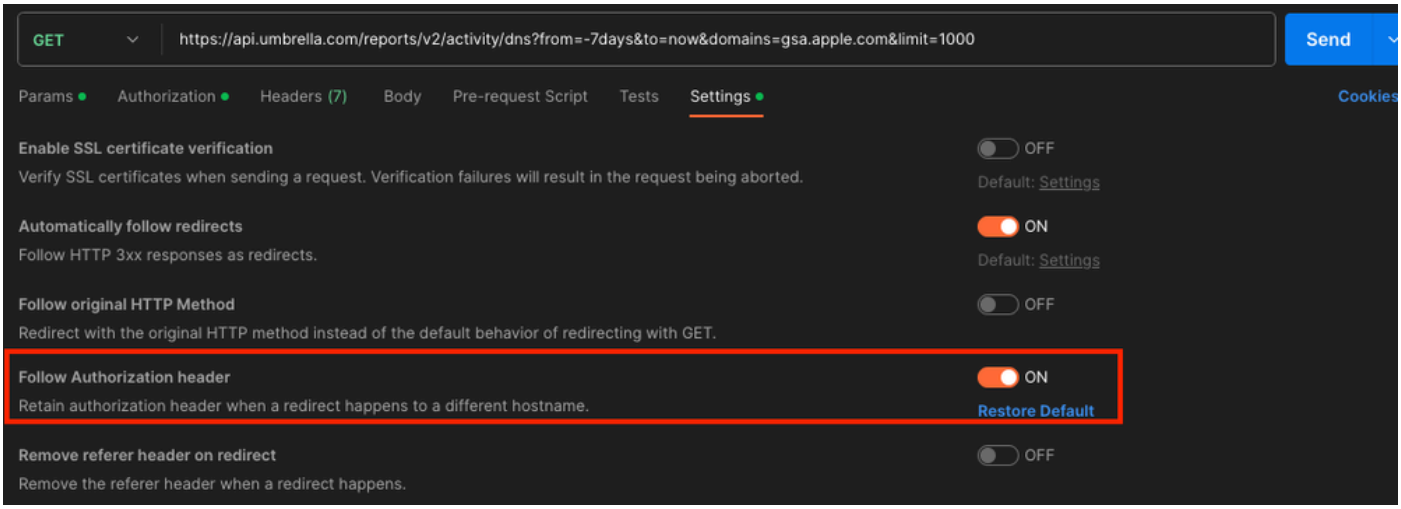
Remarque : Si une demande de client HTTP ne provient pas du même continent que l'emplacement de l'entrepôt de données Umbrella, le serveur Umbrella répond par 302 Found. Pour rediriger automatiquement les requêtes HTTP et conserver l'en-tête d'autorisation HTTP, vous pouvez définir des indicateurs supplémentaires ou activer un paramètre de redirection.

bouclage : Vous devez passer les indicateurs -L ou —location et —location-trusted pour rediriger la requête HTTP curl et conserver l'en-tête d'autorisation.



21608126036628

POSTMAN: Dans l'environnement Postman, accédez à une API et sélectionnez une méthode GET. Accédez à Paramètres > Activer le suivi de l'en-tête d'autorisation pour conserver l'en-tête d'autorisation pour les demandes de redirection.



21608126042388

Réponses

Après avoir envoyé l'action GET à l'URL, vous pouvez recevoir divers codes d'état :

- État : 200 : La demande a obtenu les informations que vous avez demandées.
- État : 400 : demande non valide. Il peut être associé à l'URL que vous avez envoyée pour la requête. Un ou plusieurs paramètres ne sont pas corrects.
- État : 401 : Non autorisé. L'en-tête d'autorisation est manquant ou le jeton est non autorisé.
- État : 403 : Interdit. Le jeton est incorrect.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.