

Dépannage du code d'erreur d'échec du module dans l'intégration XDR d'accès sécurisé

Table des matières

Problème

L'intégration de Cisco Secure Access avec XDR échoue avec une erreur HTTP 431 « Request Header Fields Too Large » au cours de la phase de vérification de l'intégrité. L'intégration avait précédemment fonctionné correctement, mais a soudainement commencé à échouer avec cette erreur lors de la tentative d'établissement de la connexion à l'aide des clés API générées à partir du tableau de bord Cisco Secure Access.

Le message d'erreur spécifique apparaît comme suit :

<#root>

Health check of Module failed: - [v2 Reporting API] There was a client error in the Cisco Secure Access

Cette erreur empêche l'ingestion de données Secure Access dans XDR, ce qui a un impact sur la visibilité de la sécurité et les fonctionnalités de surveillance.

Environnement

- Licence Cisco Secure Access avec Advantage
- Abonnement Cisco XDR
- Locataire Cisco Secure Access
- Intégration API à l'aide des clés générées par le tableau de bord Cisco Secure Access
- Étendues API requises : Examiner > Lecture seule, Rapports > Lecture seule, Déploiements

Résolution

Le problème a été résolu en régénérant la clé et le secret de l'API dans Cisco Secure Access.

Procédez comme suit pour résoudre l'erreur 431 :

Étape 1: Générer de nouvelles clés API

Accédez au tableau de bord Cisco Secure Access et créez de nouvelles clés API avec les étendues requises :

- Étudier : Lecture seule
- Rapports : Lecture seule
- Déploiements : Lecture seule
- Politiques : Lecture/écriture

Étape 2: Application de nouvelles clés à l'intégration XDR

Remplacez les clés d'API existantes dans la configuration d'intégration d'accès sécurisé XDR par les clés nouvellement générées.

Étape 3: Vérification de l'intégration

Testez l'intégration pour confirmer la réussite de la connexion. Les appels API doivent maintenant renvoyer des réponses HTTP 200 au lieu de l'erreur 431.

Détection et prévention proactives

Pour identifier et prévenir des erreurs 431 similaires à l'avenir :

1.- Lors du débogage via des outils comme Postman ou la console du navigateur, vérifiez la colonne de taille pour les en-têtes de requête. Si les en-têtes de requête approchent ou dépassent 8 Ko (8 192 octets), une erreur 431 est générée sur les passerelles API. Des outils externes tels que jwt.io peuvent être utilisés pour vérifier la taille du jeton OAuth.

2.- Analyser les modèles d'erreur :

- Si l'erreur 431 se produit instantanément lors de la connexion initiale d'un contrôle d'intégrité, cela indique que les informations d'identification statiques posent problème
- Si l'erreur 431 ne se produit qu'après l'exécution de l'intégration pendant plusieurs minutes, elle indique une accumulation de cookies au cours des tentatives suivantes

Meilleures pratiques

Désactivez la persistance des cookies ou des sessions dans le client/navigateur d'intégration pour empêcher l'accumulation de taille d'en-tête.

Motif

L'erreur HTTP 431 a été provoquée par la paire clé API et secret spécifique générant un en-tête d'autorisation anormalement volumineux ou mal formé lorsque Base64 a été codé pour l'en-tête d'autorisation HTTP standard.

Les chaînes cryptographiques de la clé API initiale contenaient une séquence de caractères qui, lorsqu'elles étaient codées, se développaient en une taille d'en-tête qui dépassait les limites de la passerelle API, ce qui entraînait le rejet des champs d'en-tête de requête trop volumineux.

Lorsque la clé API a été régénérée, la nouvelle chaîne cryptographique a produit un en-tête d'autorisation correctement dimensionné. Le processus de révocation et de génération d'une nouvelle clé a également effacé le contexte de demande mis en cache du côté du gestionnaire

d'intégration, normalisant ainsi la taille de l'en-tête.

Autres informations utiles

- [Authentification de l'API Cisco Secure Access](#)
- [Intégration de Cisco Secure Access dans XDR](#)
- [Collecter les journaux HAR depuis la console XDR](#)
- [Assistance technique de Cisco et téléchargements](#)

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.