

Risoluzione dei problemi del codice di errore del controllo di integrità del modulo non riuscito nell'integrazione XDR Secure Access

Sommario

Problema

L'integrazione di Cisco Secure Access con XDR ha esito negativo con un errore HTTP 431 "Campi intestazione richiesta troppo grandi" durante la fase di controllo dello stato. L'integrazione aveva funzionato in precedenza, ma improvvisamente ha iniziato a non riuscire con questo errore durante il tentativo di stabilire la connessione utilizzando le chiavi API generate dal dashboard Cisco Secure Access.

Il messaggio di errore specifico viene visualizzato come segue:

<#root>

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

Questo errore impedisce l'acquisizione dei dati di Secure Access in XDR e influisce sulla visibilità della protezione e sulle funzionalità di monitoraggio.

Ambiente

- Cisco Secure Access con licenza Advantage
- Abbonamento a Cisco XDR
- Cisco Secure Access Tenant
- Integrazione API tramite chiavi generate dal dashboard di Cisco Secure Access

- Ambiti API richiesti: Esamina > Sola lettura, Report > Sola lettura, Distribuzioni > Sola lettura, Criteri > Lettura/scrittura

Risoluzione

Il problema è stato risolto rigenerando la chiave e il segreto API in Cisco Secure Access.

Per risolvere l'errore 431, attenersi alla procedura seguente:

Passaggio 1: Genera nuove chiavi API

Passare al dashboard di Cisco Secure Access e creare nuove chiavi API con gli ambiti richiesti:

- Analizza: Read-Only
- Report: Read-Only
- Distribuzioni: Read-Only
- Criteri: Lettura/scrittura

Passaggio 2: Applicazione di nuove chiavi all'integrazione XDR

Sostituire le chiavi API esistenti nella configurazione dell'integrazione di XDR Secure Access con le chiavi appena generate.

Passaggio 3: Verifica integrazione

Eseguire il test dell'integrazione per confermare la connessione. Le chiamate API devono ora restituire risposte HTTP 200 anziché l'errore 431.

Rilevamento e prevenzione proattivi

Per individuare e prevenire errori simili 431 in futuro:

1.- Quando si esegue il debug tramite strumenti come Postman o console del browser, controllare la colonna delle dimensioni per le intestazioni delle richieste. Se le intestazioni delle richieste si avvicinano o superano gli 8 KB (8192 byte), viene generato un errore 431 sui gateway API. È possibile utilizzare strumenti esterni come jwt.io per verificare le dimensioni del token OAuth.

2.- Analizzare i modelli di errore:

- Se l'errore 431 si verifica immediatamente durante l'handshake iniziale di un controllo di integrità, indica che il problema è rappresentato dalle credenziali statiche
- Se l'errore 431 si verifica solo dopo che l'integrazione è stata eseguita per alcuni minuti, indica un accumulo di cookie nei tentativi successivi

Procedure ottimali

Disabilitare la persistenza dei cookie o delle sessioni nel client/browser di integrazione per impedire l'accumulo delle dimensioni dell'intestazione.

Causa

L'errore HTTP 431 è stato causato dalla coppia di chiavi e segreti API specifica che ha generato un'intestazione di autorizzazione insolitamente grande o in formato non valido quando Base64 è codificato per l'intestazione di autorizzazione HTTP standard.

Le stringhe crittografiche nella chiave API iniziale contenevano una sequenza di caratteri che, se codificati, si espandevano fino a raggiungere una dimensione dell'intestazione che superava i limiti del gateway API, causando il rifiuto dei campi intestazione della richiesta troppo grandi.

Quando la chiave API è stata rigenerata, la nuova stringa di crittografia ha prodotto un'intestazione di autorizzazione di dimensioni appropriate. Il processo di revoca e generazione di una nuova chiave ha inoltre cancellato il contesto di richiesta memorizzato nella cache dal lato di Integration

Manager, normalizzando le dimensioni dell'intestazione.

Contenuto correlato

- [Autenticazione API Cisco Secure Access](#)
- [Integrazione di Cisco Secure Access in XDR](#)
- [Raccogli registri HAR da console XDR](#)
- [Supporto tecnico Cisco e download](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).