

Resolución de problemas de comprobación de estado del código de error de módulo fallido en integración XDR de acceso seguro

Contenido

Problema

La integración de Cisco Secure Access con XDR falla con un error HTTP 431 "Solicitar campos de encabezado demasiado grandes" durante la fase de comprobación de estado. Anteriormente, la integración había funcionado correctamente, pero de repente comenzó a fallar con este error al intentar establecer la conexión mediante claves de API generadas desde el panel de acceso seguro de Cisco.

El mensaje de error específico aparece como:

<#root>

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

Este error evita que los datos de Secure Access se ingieran en XDR, lo que afecta a la visibilidad de la seguridad y a las capacidades de supervisión.

Entorno

- Cisco Secure Access con licencia Advantage
- Suscripción a Cisco XDR
- Arrendatario de Cisco Secure Access
- Integración de API mediante claves generadas en el panel de Cisco Secure Access

- Ámbitos de API requeridos: Investigar > Sólo lectura, Informes > Sólo lectura, Implementaciones > Sólo lectura, Políticas > Lectura/escritura

Resolución

El problema se resolvió regenerando la clave API y el secreto en Cisco Secure Access.

Siga estos pasos para resolver el error 431:

Paso 1: Generar nuevas claves de API

Navegue hasta el panel de Cisco Secure Access y cree nuevas claves de API con los ámbitos requeridos:

- Investigar: Sólo-Lectura
- Informes: Sólo-Lectura
- Implementaciones: Sólo-Lectura
- Políticas: Lectura/escritura

Paso 2: Aplicación de nuevas claves a la integración XDR

Reemplace las claves API existentes en la configuración de integración de XDR Secure Access por las claves recién generadas.

Paso 3: Verificar integración

Pruebe la integración para confirmar la conexión correcta. Las llamadas API ahora deben devolver respuestas HTTP 200 en lugar del error 431.

Detección y prevención proactivas

Para identificar y evitar errores 431 similares en el futuro:

1.- Al depurar a través de herramientas como Postman o la consola del navegador, verifique la columna de tamaño para los encabezados de solicitud. Si los encabezados de solicitud se acercan o exceden los 8 KB (8192 bytes), esto genera un error 431 en los gateways de API. Las herramientas externas como jwt.io se pueden utilizar para verificar el tamaño del token de OAuth.

2.- Analizar patrones de error:

- Si el error 431 ocurre instantáneamente durante el intercambio inicial de señales de una comprobación de estado, indica que el problema son las credenciales estáticas
- Si el error 431 ocurre solamente después de que la integración se ejecuta durante varios minutos, apunta a la acumulación de cookies en los reintentos subsiguientes

Mejores medidas

Inhabilite la persistencia de sesión o cookie en el cliente/navegador de integración para evitar la acumulación del tamaño del encabezado.

Causa

El error HTTP 431 fue causado por la clave API específica y el par secreto que genera un encabezado de autorización inusualmente grande o mal formado cuando Base64 se codificó para el encabezado de autorización HTTP estándar.

Las cadenas criptográficas de la clave API inicial contenían una secuencia de caracteres que, al codificarse, se expandían a un tamaño de encabezado que superaba los límites de la puerta de enlace de la API, lo que provocaba el rechazo "Solicitar campos de encabezado demasiado grandes".

Cuando se regeneró la clave de la API, la nueva cadena criptográfica produjo un encabezado de autorización con el tamaño adecuado. El proceso de revocación y generación de una nueva clave

también borró el contexto de solicitud en caché en el lado del administrador de integración, normalizando el tamaño del encabezado.

Contenido relacionado

- [Autenticación API de Cisco Secure Access](#)
- [Integración de Cisco Secure Access en XDR](#)
- [Recopilar registros HAR de la consola XDR](#)
- [Soporte técnico y descargas de Cisco](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).