

La búsqueda de eventos de FMC Unified falla con los nombres de objetos de red en Firepower 7.7

Problema

Al utilizar Cisco Secure Firewall Management Center (FMC) versión 7.7.10.1, los objetos de red y los grupos de objetos no se pueden utilizar como criterios de búsqueda en la página Eventos unificados. Al intentar buscar eventos utilizando nombres de objeto o grupo específicos en IP de origen en la búsqueda de eventos unificada, el FMC no devuelve resultados o muestra un mensaje de error:

The query contains an invalid constraint on the provided field: "Source IP" with value "\${000_ALL-USER_

Los objetos están visibles y se pueden utilizar en Gestión de objetos, y las búsquedas por dirección IP sin procesar funcionan según lo esperado. Este comportamiento afecta tanto a los objetos de red existentes como a los recién creados, lo que dificulta la búsqueda de eventos mediante nombres de objeto o nombres de grupo en la interfaz de Unified Events.

Entorno

- Cisco Secure Firewall Management Center para VMware (FMCv)
- Versión del software: 7.7.10.1
- Tecnología: Cisco Secure Firewall Firepower: 7,7
- Subtecnología: Cisco Secure Firewall: supervisión/eventos/registro - 7.7
- Implementación: Configuración FMC independiente
- FMC contiene más de 1000 objetos de red
- El entorno incluye el historial de migración de FMC in situ a cdFMC y de vuelta a in situ

Resolución

Este problema se debe a un defecto de software conocido y no se puede resolver completamente mediante cambios de configuración en la versión de software actual. Se recomienda aplicar este enfoque de resolución.

Solución alternativa inmediata

Utilice los campos de dirección IP en las búsquedas de Unified Event en lugar de los nombres o grupos de objetos como solución temporal. Al investigar eventos relacionados con objetos o grupos afectados:

1. Vaya a Análisis > Eventos unificados.
2. En los criterios de búsqueda, utilice las direcciones IP reales en lugar de los nombres de objeto.
3. Introduzca la dirección IP o el intervalo IP específicos en los campos IP de origen o IP de destino.
4. Ejecute la búsqueda para recuperar los eventos deseados.

Solución a largo plazo

La corrección permanente requiere la actualización a una futura versión de software de FMC que incluya la resolución para el ID de bug de Cisco CSCws52418. Siga estos pasos:

1. Suscríbase a las notificaciones defectuosas de CSCws52418 para recibir alertas cuando estén disponibles las versiones fijas de FMC.
2. Supervise el estado de los errores para ver si hay actualizaciones sobre la disponibilidad de la solución, programada provisionalmente para mayo de 2026.
3. Planifique una ventana de mantenimiento para actualizar FMC y los dispositivos administrados a una versión que incluya la corrección para CSCws52418 una vez que se publique.

Prevención y recomendaciones

Hasta que se complete la actualización de software:

- Utilice criterios de búsqueda basados en IP en Unified Events (IP de origen/destino) al investigar eventos relacionados con los objetos o grupos afectados.
- Al crear nuevos flujos de trabajo operativos, evite depender únicamente de las búsquedas de nombre de objeto en Unified Events para los procesos operativos o de auditoría en esta versión.
- Documentar los nombres de objetos afectados y sus direcciones IP correspondientes para referencia durante la resolución de problemas.

Causa

El comportamiento es causado por el ID de bug de Cisco CSCws52418, donde el manejo interno de las búsquedas de objetos para las búsquedas de eventos está restringido por un límite interno de aproximadamente 1000 entradas de objeto. Los objetos fuera de este límite no se indizan correctamente o no se devuelven en las búsquedas de eventos unificados por nombre, lo que produce resultados que faltan o errores de "restricción no válida". La reconstrucción de la base de datos de eventos monetdb no resuelve este comportamiento, ya que es una limitación de software codificada en lugar de un problema de corrupción de la base de datos.

Contenido relacionado

- ID de bug de Cisco CSCws52418 - Algunos objetos no están disponibles para la selección en los filtros de búsqueda de eventos
- Id. de error de Cisco CSCwt05296: no se puede utilizar el objeto IPv4-Private-All-RFC1918 recién creado o definido por el sistema como filtro en eventos
- [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).