Información sobre eventos de actualización en terminales seguros para eliminaciones de grupos

Contenido

[Introducción](#)

[Problema](#)

[Solución](#)

Introducción

Este documento describe cómo los registros de auditoría de Secure Endpoint registraron eventos de actualización y eliminación cuando se eliminaron grupos vacíos.

Problema

Los eventos de actualización de esta imagen muestran un nuevo ID de grupo para equipos o estaciones de trabajo, aunque estas estaciones de trabajo no estén visibles en la página del equipo de la consola de AMP. Estos eventos de actualización están asociados con el correo electrónico del usuario de la persona que inició sesión para realizar la eliminación, lo que podría provocar confusión en el cliente sobre lo que ocurrió. En algunos casos, se pueden generar entre 30 y 40 eventos de actualización después de eliminar un grupo vacío.

Solución

Esto es una conducta esperada. Los nombres de host de equipo o equipo que se ven en los eventos de actualización del registro de auditoría durante la eliminación de grupos vacíos pertenecen a dispositivos que antes formaban parte de esos grupos pero que ahora están inactivos. Estas máquinas se eliminaron automáticamente de la consola tras 90 días de

inactividad, pero siguieron formando parte del grupo en el back-end.

Cuando se elimina el grupo, estas máquinas inactivas se mueven al grupo predeterminado, que desencadena los eventos de actualización. Desafortunadamente, dado que estos equipos están inactivos, no aparecen en la consola, por lo que no se pueden encontrar al realizar búsquedas en equipos.

Para obtener una lista completa de las máquinas inactivas que aún están asignadas a un grupo, debe ponerse en contacto con el TAC, ya que esta información no se puede recuperar a través del portal de terminales seguros.

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).