Comprendre les événements de mise à jour dans Secure Endpoint pour les suppressions de groupe

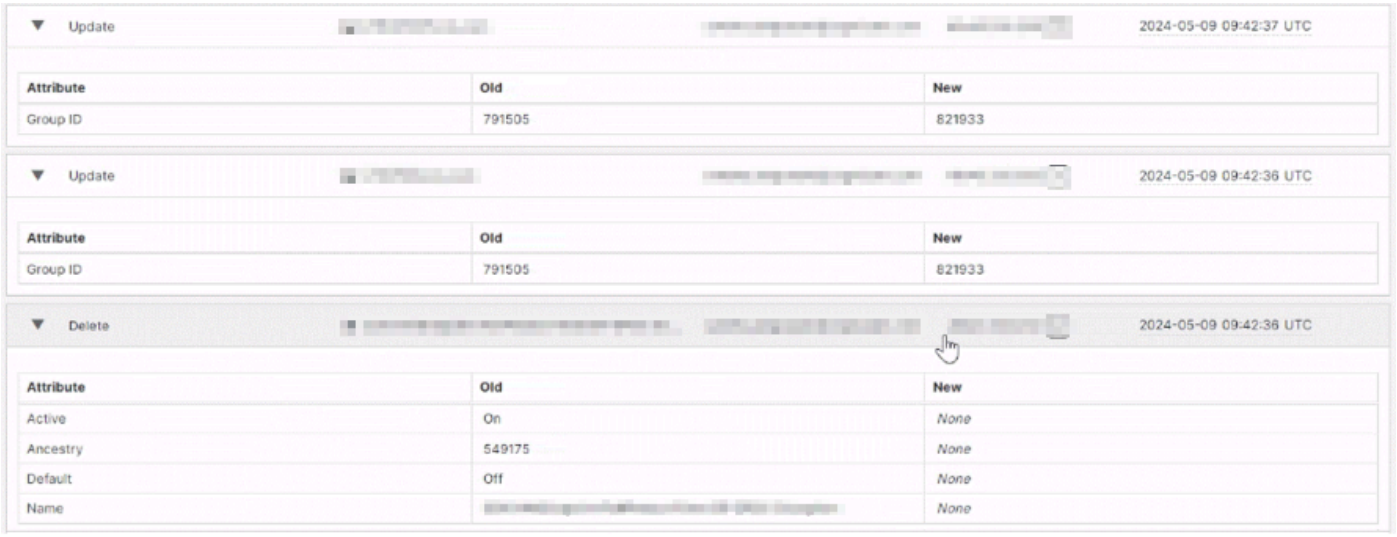
Table des matières

Introduction

Ce document décrit comment les journaux d'audit Secure Endpoint ont enregistré les événements de mise à jour et de suppression lorsque des groupes vides ont été supprimés.

Problème

Les événements de mise à jour de cette image affichent un nouvel ID de groupe pour les ordinateurs ou les stations de travail, même si ces stations de travail ne sont pas visibles sur la page de l'ordinateur de la console AMP. Ces événements de mise à jour sont associés à l'e-mail de l'utilisateur qui s'est connecté pour effectuer la suppression, ce qui peut entraîner une confusion du client quant à ce qui s'est passé. Dans certains cas, 30 à 40 événements de mise à jour peuvent être générés après la suppression d'un groupe vide.



Solution

C'est un comportement prévu. Les noms d'hôtes d'ordinateurs ou d'ordinateurs apparaissant dans les événements de mise à jour du journal d'audit lors de la suppression de groupes vides

appartiennent à des périphériques qui faisaient autrefois partie de ces groupes mais qui sont maintenant inactifs. Ces machines ont été automatiquement retirées de la console après 90 jours d'inactivité, mais elles ont continué à faire partie du groupe dans le back-end.

Lorsque le groupe est supprimé, ces ordinateurs inactifs sont déplacés vers le groupe par défaut, ce qui déclenche les événements de mise à jour. Malheureusement, comme ces ordinateurs sont inactifs, ils n'apparaissent pas dans la console, c'est pourquoi ils sont introuvables lors d'une recherche sous les ordinateurs.

Pour obtenir une liste complète des machines inactives qui sont encore affectées à un groupe, vous devez contacter le TAC, car ces informations ne peuvent pas être récupérées via le portail Secure Endpoint.

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.