Entender os eventos de atualização no endpoint seguro para exclusões de grupo

Contents

[Introdução](#)

[Problema](#)

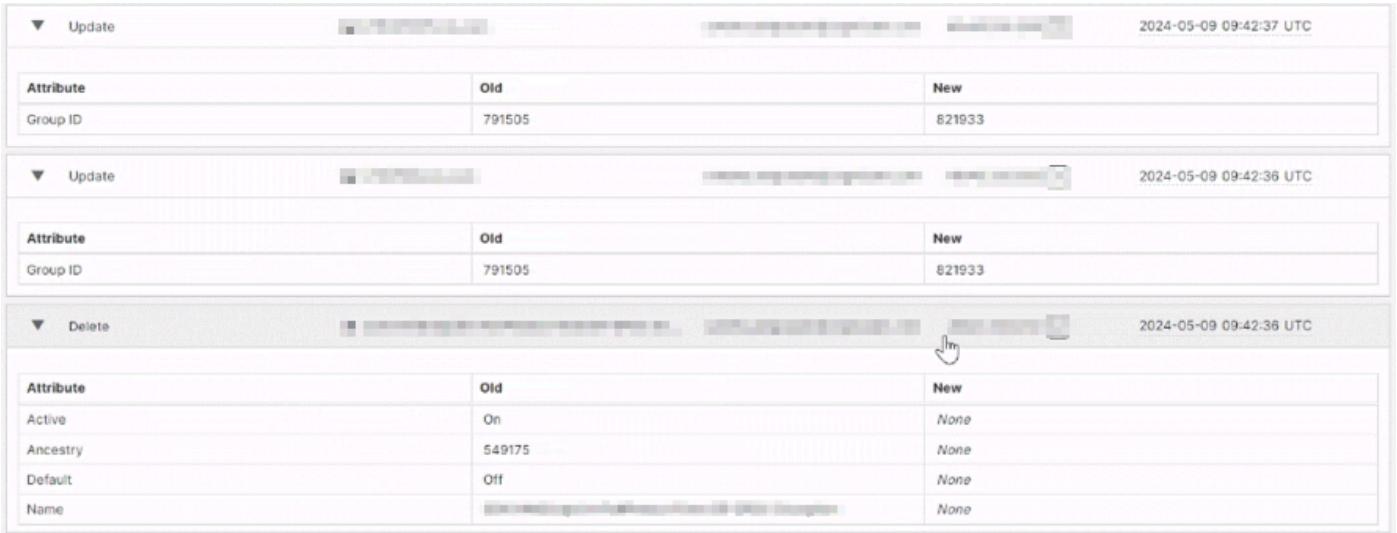
[Solução](#)

Introdução

Este documento descreve como os logs de auditoria do Secure Endpoint registraram eventos de atualização e exclusão quando grupos vazios foram excluídos.

Problema

Os eventos de atualização nessa imagem exibem uma nova ID de grupo para máquinas ou estações de trabalho, mesmo que essas estações de trabalho não estejam visíveis na página do computador do console AMP. Esses eventos de atualização estão associados ao email do usuário da pessoa que fez login para executar a exclusão, o que pode levar à confusão do cliente sobre o que ocorreu. Em alguns casos, 30 a 40 eventos de atualização podem ser gerados após a exclusão de um grupo vazio.



Solução

Este é um comportamento esperado. Os nomes de host da máquina ou do computador vistos nos eventos de atualização do log de auditoria durante a exclusão de grupos vazios pertencem a dispositivos que antes faziam parte desses grupos, mas agora estão inativos. Essas máquinas foram automaticamente removidas do console após 90 dias de inatividade, mas permaneceram

parte do grupo no back-end.

Quando o grupo é excluído, essas máquinas inativas são movidas para o grupo padrão, o que aciona os eventos de atualização. Infelizmente, como esses computadores estão inativos, eles não aparecem no console, e é por isso que não podem ser encontrados ao pesquisar em computadores.

Para obter uma lista completa de computadores inativos que ainda estão atribuídos a um grupo, você precisa entrar em contato com o TAC, pois essas informações não podem ser recuperadas através do portal Secure Endpoint.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.