了解安全终端中的更新事件以进行组删除

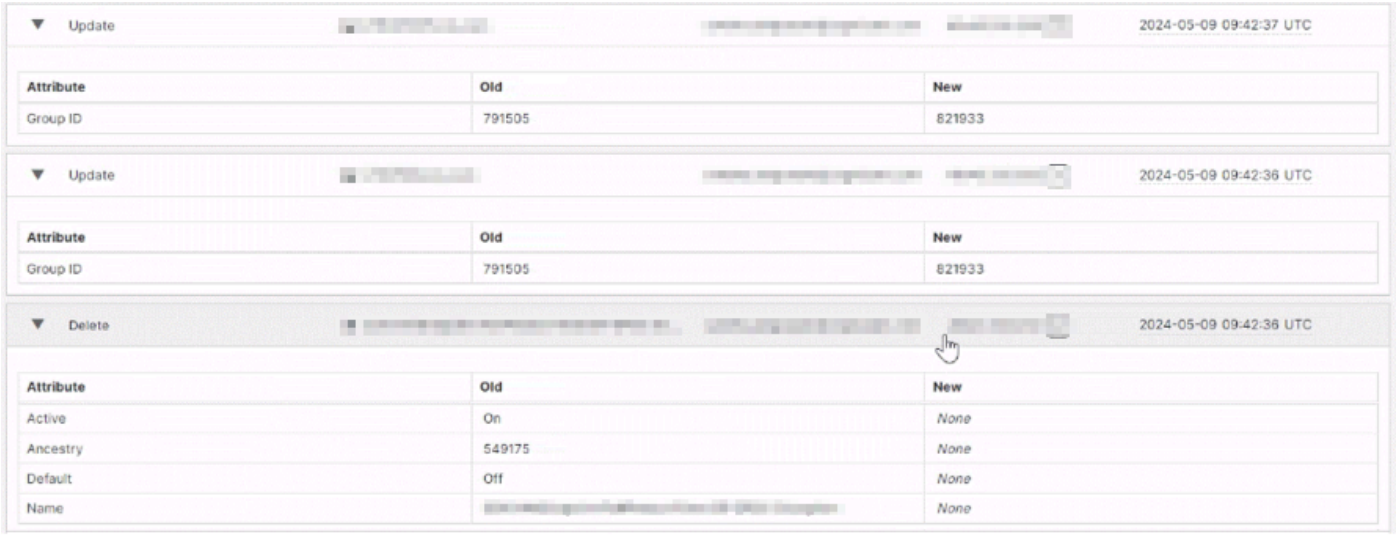
目录

简介

本文档介绍在删除空组时，安全终端审核日志如何记录更新和删除事件。

问题

此图像中的更新事件显示计算机或工作站的新组ID，即使这些工作站在AMP控制台计算机页面上不可见。这些更新事件与登录者执行删除的用户邮件相关联，这可能导致客户端混淆所发生的情况。在某些情况下，删除空组后可生成30-40个更新事件。



解决方案

这是预料之中的行为。在删除空组期间，在审核日志更新事件中看到的计算机或计算机主机名属于曾经属于这些组但现在处于非活动状态的设备。这些计算机在处于非活动状态90天后自动从控制台删除，但它们仍属于后端组。

删除组时，这些非活动计算机将移至默认组，从而触发更新事件。遗憾的是，由于这些计算机处于非活动状态，因此它们不会显示在控制台中，这就是在计算机下搜索时找不到它们的原因。

要获取仍分配到组的非活动计算机的完整列表，您需要联系TAC，因为无法通过安全终端门户检索此信息。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。