

グループの削除用のセキュアエンドポイントの更新イベントについて

内容

[はじめに](#)

[問題](#)

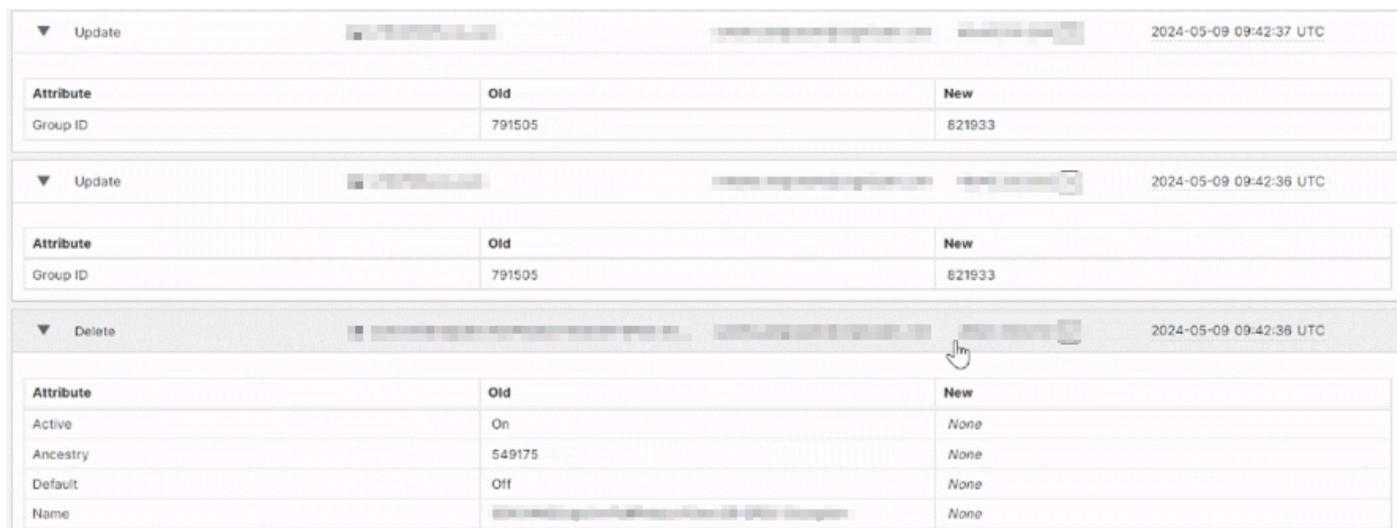
[解決方法](#)

はじめに

このドキュメントでは、空のグループが削除されたときに、セキュアエンドポイント監査ログが更新イベントと削除イベントの両方を記録する方法について説明します。

問題

マシンまたはワークステーションのアップデートイベントは、AMPコンソールコンピュータページには表示されませんが、この図では新しいグループIDが表示されます。これらの更新イベントは、削除を実行するためにログインしたユーザの電子メールに関連付けられます。これにより、発生した問題についてクライアントが混乱する可能性があります。場合によっては、空のグループを削除した後に30 ~ 40の更新イベントを生成できます。



The screenshot displays three log entries from the AMP console, each showing a table of attribute changes. The first two entries are 'Update' events, and the third is a 'Delete' event.

Update		
2024-05-09 09:42:37 UTC		
Attribute	Old	New
Group ID	791505	821933

Update		
2024-05-09 09:42:36 UTC		
Attribute	Old	New
Group ID	791505	821933

Delete		
2024-05-09 09:42:36 UTC		
Attribute	Old	New
Active	On	None
Ancestry	549175	None
Default	Off	None
Name		None

解決方法

これは予期された動作です。空のグループの削除中に監査ログ更新イベントで確認されたマシンまたはコンピュータのホスト名は、以前はこれらのグループに属していたが、現在は非アクティブなデバイスに属しています。これらのマシンは、90日間の非アクティブ状態後にコンソールから自動的に削除されましたが、バックエンドのグループの一部に残っていました。

グループが削除されると、これらの非アクティブなマシンはデフォルトグループに移動され、更新イベントがトリガーされます。残念ながら、これらのコンピュータは非アクティブであるため、コンソールには表示されません。そのため、コンピュータの下で検索しても見つかりません。

グループにまだ割り当てられている非アクティブなマシンの完全なリストを取得するには、TACに連絡する必要があります。これは、この情報をセキュアエンドポイントポータル経由で取得できないためです。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。