恢复已删除的默认主机组

目录

简介

环境

问题

分辨率

- 方法 1：从现有备份导入（如果存在备份，则建议导入）
- 方法 2：导出和导入特定默认主机组或子树
- 方法 3：联系思科TAC

原因

参考资料:

简介

本文档介绍如何通过恢复Cisco安全网络分析中的正确主机组ID来恢复已删除的默认主机组。

环境

- 适用于使用默认主机组和主机分类器应用的思科安全网络分析部署。

问题

当删除默认主机组并使用相同名称创建新主机组以“替换”已删除的原始主机组时，新主机组使用自定义ID而不是默认ID。

需要特定默认主机组才能正常工作的功能（如主机分类器应用）无法检测“替换”主机组。

默认主机组使用两位数ID，例如28或30，用户创建的主机组被视为自定义主机组并使用五位数ID，例如50081。

如果删除了默认主机组，然后将其重新创建为自定义主机组，则重新创建的组会收到五位数ID。

某些功能可能会因此而失败，为了更正此问题，主机组ID必须与默认值匹配。

分辨率

方法 1：从现有备份导入（如果存在备份，则建议导入）

如果在删除之前备份了host_groups.xml文件，则可以通过通过Secure Network Analytics Manager界面导入备份文件来恢复已删除的默认主机组。

1. 登录安全网络分析管理器Web界面。
2. 导航到Configure > System > Host Group Management。
3. 选择Import选项，然后选择Import All。
4. 从本地系统中上传备份host_groups.xml文件。
5. 确认导入，以通过API查询恢复所有主机组。
6. 如有必要，请重新安装主机分类器应用程序以确保正确检测。

方法 2：导出和导入特定默认主机组或子树

如果要仅恢复特定默认主机组或子树，而不覆盖其他自定义主机组，请完成以下详细步骤：

1. 创建临时域
    - 登录安全网络分析(SNA)管理器UI。
    - 导航到配置>系统>域。
    - 点击Add Domain，输入临时域名，然后选择Default。
    - 保存新的临时域。
2. 导出特定默认主机组或子树
    - 切换到刚创建的临时域。
    - 导航到配置>检测>主机组管理。
    - 找到要导出的特定默认主机组或子树。
    - 使用“导出”选项仅将所选主机组或子树导出到本地保存的XML文件。
3. 删除临时域
    - 导航到配置>系统>域。
    - 选择临时域并将其删除以避免混淆。
4. 将导出的主机组或子树导入正确的树/子树
    - 切换到已删除默认主机组的受影响域。
    - 导航到配置>检测>主机组管理。
    - 使用“导入”功能导入以前导出的XML文件。

- 导入时，请确保选择与删除原始默认主机组的位置对应的正确树或子树位置。这可以防止覆盖其他主机组。

5. 确认导入的主机组使用默认的两位ID

   - 使用API查询收集所需信息。您可以在此处找到文档 — 配置管理API。
   - 在响应中查找导入的主机组，并验证其id字段是否与两位数的默认ID匹配。
   - 有关API用法，请参阅安全网络分析API文档以了解身份验证和请求详细信息。

6. 验证主机分类器应用检测

   - 如果未检测到更新的主机组，请重新安装主机分类器应用程序。

方法 3：联系思科TAC

如果上述方法都无法解决问题，或者您有任何疑问，请联系思科TAC以获得进一步帮助。

原因

手动重新创建已删除的默认主机组会导致系统分配五位数的自定义ID。Host Classifier应用程序需要原始的两位数ID;当匹配失败时，应用程序无法检测主机组或对其分类。

参考资料:

配置指南

API Cisco DevNet
开立 TAC 案例

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）。