Récupérer les groupes hôtes par défaut supprimés

Table des matières

Introduction

Environnement

Problème

Résolution

- Méthode 1 : Importer à partir d'une sauvegarde existante (recommandé si une sauvegarde existe)
- Méthode 2 : Exporter et importer un groupe hôte ou une sous-arborescence par défaut spécifique
- Méthode 3 : Contactez le centre d'assistance technique Cisco TAC

Motif

Références:

Introduction

Ce document décrit comment récupérer un groupe d'hôtes par défaut supprimé en restaurant l'ID de groupe d'hôtes correct dans Cisco Secure Network Analytics.

Environnement

- Applicable aux déploiements Cisco Secure Network Analytics qui utilisent des groupes d'hôtes par défaut et l'application Host Classifier.

Problème

Lorsque le groupe d'hôtes par défaut est supprimé et qu'un nouveau groupe d'hôtes est créé avec le même nom pour « remplacer » l'original supprimé, le nouveau groupe d'hôtes utilise un ID personnalisé au lieu de l'ID par défaut.

Les fonctionnalités qui nécessitent le fonctionnement de groupes d'hôtes par défaut spécifiques, telles que l'application Host Classifier, ne parviennent pas à détecter le groupe d'hôtes de « remplacement ».

Les groupes hôtes par défaut utilisent des ID à deux chiffres, par exemple 28 ou 30, et les groupes hôtes créés par l'utilisateur sont considérés comme personnalisés et utilisent des ID à cinq chiffres, par exemple 50081.

Si un groupe hôte par défaut est supprimé, puis recréé en tant que groupe hôte personnalisé, le groupe recréé reçoit un ID à cinq chiffres.

Certaines fonctionnalités peuvent échouer à cause de cela et pour corriger le problème, l'ID du groupe d'hôtes doit correspondre à la valeur par défaut.

Résolution

Méthode 1 : Importer à partir d'une sauvegarde existante (recommandé si une sauvegarde existe)

Si vous disposez d'une sauvegarde du fichier host_groups.xml avant la suppression, vous pouvez restaurer le groupe hôte par défaut supprimé en important le fichier de sauvegarde via l'interface Secure Network Analytics Manager.

1. Connectez-vous à l'interface Web Secure Network Analytics Manager.
2. Accédez à Configure > System > Host Group Management.
3. Sélectionnez l'option Importer et choisissez Importer tout.
4. Téléchargez le fichier de sauvegarde host_groups.xml depuis votre système local.
5. Confirmez l'importation pour restaurer tous les groupes d'hôtes via une requête API.
6. Si nécessaire, réinstallez l'application Host Classifier pour garantir une détection correcte.

Méthode 2 : Exporter et importer un groupe hôte ou une sous-arborescence par défaut spécifique

Si vous souhaitez restaurer uniquement un groupe d'hôtes par défaut ou une sous-arborescence spécifique sans remplacer d'autres groupes d'hôtes personnalisés, procédez comme suit :

1. Créer un domaine temporaire

    - Connectez-vous à l'interface utilisateur du gestionnaire Secure Network Analytics (SNA).
    - Accédez à Configure > System > Domains.
    - Cliquez sur Ajouter un domaine, entrez un nom de domaine temporaire, puis sélectionnez Par défaut.

- Enregistrez le nouveau domaine temporaire.

2. Exporter le groupe d'hôtes ou la sous-arborescence par défaut spécifique

   - Passez au domaine temporaire que vous venez de créer.
   - Naviguez jusqu'à Configure > Detection > Host Group Management.
   - Localisez le groupe d'hôtes ou la sous-arborescence par défaut que vous souhaitez exporter.
   - Utilisez l'option Exporter pour exporter uniquement le groupe d'hôtes ou la sous-arborescence sélectionnés vers un fichier XML enregistré localement.

3. Supprimer le domaine temporaire

   - Accédez à Configure > System > Domains.
   - Sélectionnez le domaine temporaire et supprimez-le pour éviter toute confusion.

4. Importer le groupe d'hôtes ou la sous-arborescence exportés dans l'arborescence/sous-arborescence appropriée

   - Basculez vers le domaine affecté où le groupe d'hôtes par défaut a été supprimé.
   - Naviguez jusqu'à Configure > Detection > Host Group Management.
   - Utilisez la fonction Import pour importer le fichier XML précédemment exporté.
   - Lors de l'importation, veillez à sélectionner l'arborescence ou l'emplacement de sous-arborescence correct correspondant à l'emplacement où le groupe hôte par défaut d'origine a été supprimé. Cela évite d'écraser d'autres groupes hôtes.

5. Confirmez que le groupe d'hôtes importé utilise un ID à deux chiffres par défaut

   - Utilisez la requête API pour collecter les informations nécessaires. La documentation est disponible ici : Configuration Management API.
   - Localisez le groupe d'hôtes importé dans la réponse et vérifiez que son champ d'ID correspond à l'ID par défaut à deux chiffres.
   - Pour l'utilisation de l'API, référez-vous à la documentation de l'API Secure Network Analytics pour l'authentification et les détails des demandes.

6. Vérification de la détection des applications Host Classifier

   - S'il ne détecte pas les groupes d'hôtes mis à jour, réinstallez l'application Host Classifier.

Méthode 3 : Contactez le centre d'assistance technique Cisco TAC

Si aucun de ces éléments ne résout le problème ou si vous avez des questions, contactez le TAC Cisco pour obtenir de l'aide.

Motif

La recréation manuelle d'un groupe d'hôtes par défaut supprimé entraîne l'attribution d'un ID personnalisé à cinq chiffres par le système. L'application Host Classifier attend l'ID à deux chiffres d'origine ; lorsqu'il ne correspond pas, l'application ne peut pas détecter ou classer le groupe d'hôtes.

Références:

Guides de configuration

API Cisco DevNet
Ouvrir un dossier TAC

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.