Recover Deleted Default Host Groups

Contents

Introduction

Environment

Issue

Resolution

- Method 1: Import from Existing Backup (Recommended if Backup Exists)
- Method 2: Export and Import Specific Default Host Group or Subtree
- Method 3: Contact Cisco TAC

Cause

References:

Introduction

This document describes how to recover a deleted default host group by restoring the correct host-group ID in Cisco Secure Network Analytics.

Environment

- Applicable to Cisco Secure Network Analytics deployments that use default host groups and the Host Classifier application.

Issue

When default host group is deleted and a new host group created using the same name to 'replace' the deleted original, the new host group uses a custom ID instead of the default ID.

Features that require specific default host groups to function, such as the Host Classifier application, fail to detect the 'replacement' host group.

Default host groups use two-digit IDs, for example 28 or 30 and user created host groups are considered to be custom and use five-digit IDs, for example 50081.

If a default host group is deleted and then recreated as a custom host group, the recreated group receives a five-digit ID.

Some features can fail because of this and to correct the problem, the host-group ID must match the default value.

Resolution

Method 1: Import from Existing Backup (Recommended if Backup Exists)

If you have a backup of the host_groups.xml file from before the deletion, you can restore the deleted default host group by importing the backup file through the Secure Network Analytics Manager interface.

1. Log in to the Secure Network Analytics Manager web interface.
2. Navigate to **Configure > System > Host Group Management**.
3. Select the Import option and choose Import All.
4. Upload the backup host_groups.xml file from your local system.
5. Confirm the import to restore all host groups via API query.
6. If necessary, reinstall the Host Classifier application to ensure proper detection.

Method 2: Export and Import Specific Default Host Group or Subtree

If you want to restore only a specific default host group or a subtree without overwriting other custom host groups, complete these detailed steps:

1. Create a Temporary Domain
    - Log in to the Secure Network Analytics (SNA) Manager UI.
    - Navigate to **Configure > System > Domains**.
    - Click Add Domain, enter a temporary domain name, and select Default.
    - Save the new temporary domain.
2. Export the Specific Default Host Group or Subtree
    - Switch to the temporary domain you just created.
    - Navigate to **Configure > Detection > Host Group Management**.
    - Locate the specific default host group or subtree you want to export.
    - Use the Export option to export only the selected host group or subtree to an XML file saved locally.
3. Delete the Temporary Domain
    - Navigate to **Configure > System > Domains**.
    - Select the temporary domain and delete it to avoid confusion.
4. Import the Exported Host Group or Subtree into the Correct Tree/Subtree
    - Switch to the affected domain where the default host group was deleted.
    - Navigate to **Configure > Detection > Host Group Management**.

- Use the Import function to import the previously exported XML file.
- When importing, ensure you select the correct tree or subtree location corresponding to where the original default host group was deleted. This prevents overwriting other host groups.

5. Confirm the Imported Host Group Uses the a Default Two-Digit ID

   - Use API query to gather the information needed. Documentation can be found here - Configuration Management API.
   - Locate the imported host group in the response and verify its id field matches the a two-digit default ID.
   - For API usage, refer to the Secure Network Analytics API documentation for authentication and request details.

6. Verify Host Classifier Application Detection

   - If it does not detect the updated host groups, reinstall the Host Classifier application.

Method 3: Contact Cisco TAC

If none of these resolve the issue, or if you have questions, please contact Cisco TAC for further assistance.

Cause

Recreating a deleted default host group manually results in the system assigning a five-digit custom ID. The Host Classifier application expects the original two-digit ID; when it fails to match, the application cannot detect or classify the host group.

References:

Configuration Guides

API Cisco DevNet
Open a TAC Case