Manage Falcon Log Collector Groups

Last updated: May 22, 2025

Overview

Create groups within fleet management to manage the configurations of multiple instances of the Falcon Log Collector. You can create groups using a simplified version of CrowdStrike Query Language (CQL). Using CQL enables you to create dynamic groups. In a dynamic group, new collectors that meet the filter criteria are automatically added when you enroll them in the fleet. For more info about CQL, see Get Started with CrowdStrike Query Language [/documentation/category/nbbb7a91/event-investigation/get-started-with-crowdstrike-query-language].

When you create a group, you merge multiple config snippets. The combined file is validated during the procedure and applied to all the Falcon Log Collector instances in the group.

Combine configuration snippets

You can assign multiple configs to a group to create a complete configuration file, without duplicating configurations.

For example, to manage the configuration of 200 instances, where instances collect data from different sources:

- 115 instances collect data from services and have this combined configuration:

```
sources:
   service:
     type: file
     include: /var/service/*
     sink: logscale


  sinks:
    logscale:
      type: humio
      token: <ingest-token>
      url: <data-connector-url> // example - https://cloud.community.humio.com
```

Note: To avoid integration issues, the URL should not end with `/services/collector`.

- 85 instances collect data from var_log and have a combination of the previous and another configuration:

```
sources:
  var_log:
    type: file
    include: /var/log/*
    sink: logscale
   service:
     type: file
     include: /var/service/*
     sink: logscale

  json_log:
    type: unifiedlog
    format: json
    include:
      - process: securityd
       predicate: eventMessage CONTAINS 'Session ' && subsystem == 'com.apple.securityd'
    parser: "apple/unifiedlog:unifiedlog-json"
    sink: logscale

  sinks:
    logscale:
      type: humio
      token: <ingest-token>
url: <logscale-base-url> // example - https://cloud.community.humio.com
```

In the example case, you would create 3 snippet configurations.

- Create 1 snippet configuration containing the sinks section:

```
sinks:
    logscale:
      type: humio
      token: <ingest-token>
url: <logscale-base-url> // example - https://cloud.community.humio.com
```

- Create 2 snippet configurations containing the different sources sections:

```
sources:
  var_log:
    type: file
    include: /var/log/*
    sink: logscale
```

```
sources:
```

```
service:
  type: file
  include: /var/service/*
  sink: logscale
```

Create a group

Groups allow you to manage the configuration of multiple instances of the Falcon Log Collector. You can also combine configuration snippets to create a configuration that can be applied to all the instances in the group.

You can create groups that contain a static list of instances, using, for example, the ID of specific machines or dynamic filters based on a subset of the CrowdStrike Query Language. For more info about the query language, see Get Started with CrowdStrike Query Language [/documentation/category/nbbb7a91/event-investigation/get-started-with-crowdstrike-query-language].

1. Go to **Next-Gen SIEM > Log management > Data onboarding [/data-connectors]** and click **Fleet Management**.
2. Click **Groups**.
3. Click **New group**.
4. Enter a name for the group.
5. Search for the configuration or configuration snippets you want to apply to the group. The files are combined to create a single valid configuration file.
6. When the resulting configuration meets your requirements, click **Next**. For more info on snippets, see Combine configuration snippets [/documentation/page/pa9df507/manage-falcon-log-collector-groups#meb49ae0].
7. Use the filter to query the instances to add to the group. You can use a subset of the CrowdStrike Query Language to create a list of instances. For example, `version=1.*` filters for any instances running a version which starts with 1.
   The instances in the group automatically update with any new instances that meet the filter criteria.
8. Click **Create group**.

Bulk manage Falcon Log Collector versions

You can remotely update or roll back instance versions by group in the Falcon console.

This feature can only be used for instances that have been installed using the full installation method. For more info about installation methods, see Step 1: Download install the Falcon Log Collector [/documentation/page/q81f4f3a/get-started-with-fleet-management#x7b0acd3]. You can also update specific instances from the **Fleet overview** tab.

1. Go to **Next-Gen SIEM > Log management > Data onboarding [/data-connectors]** and click **Fleet management**.
2. Click **Groups**.
3. Click **Options** ⋮ for the group you want to edit and select **Manage versions**.
4. Select the version to update or downgrade to, and click **Set target version**.

Edit a group

You can edit groups to change the name of the group, the assigned configuration, or the instance included in the group (the filter).

1. Go to **Next-Gen SIEM > Log management > Data onboarding [/data-connectors]** and click **Fleet management**.
2. Click **Groups**.
3. Click **Options** ⋮ for the group you want to edit and select **Edit group**.
4. Edit the name and configuration, as needed. For more info on the configuration or combined configuration for your group, see Create a group [/documentation/page/pa9df507/manage-falcon-log-collector-groups#p5268291].
5. Click **Next**.
6. Edit the CrowdStrike Query Language filters that are applied to create a group of instances. When you edit the query filters of a previously created group, you can preview how the changes affect the number of instances in the group.
7. Click **Update group**.

Delete a group

1. Go to **Next-Gen SIEM > Log management > Data onboarding [/data-connectors]** and click **Fleet management**.
2. Click **Groups**.
3. Click **Options** ⋮ for the group you want to edit and select **Delete group**.
4. Review how many instances are affected by deleting the group.
5. Click **Delete group**.

< **Manage Falcon Log Collector Instance Enrollment[/documentation/page/w55f2d06/manage-falcon-log-collector-instance-enrollment]**