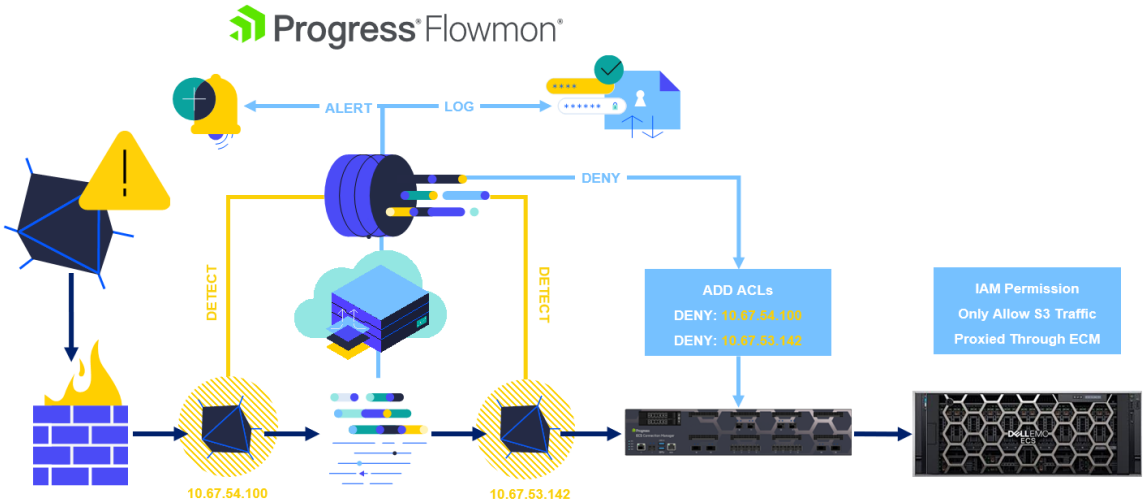
Progress

Flowmon ADS integration with ECS Connection Manager

Description of steps required to implement integration between Flowmon ADS and Progress ECS Connection Manager.

Introduction



Integrating network anomaly detection with intelligent storage application delivery control can help with early warning, detection, and remediation of various security events. Flowmon Anomaly Detection System (ADS) provides real-time detection of threat actors, and through this integration, can automatically configure ECS Connection Manager access control lists to protect Dell ECS storage from being accessed by potentially infected devices.

Document Purpose

This document provides recommended settings used when integrating Progress Flowmon Anomaly Detection System (ADS) and Progress ECS Connection Manager to block a potentially harmful IP(s) from accessing Dell ECS Object storage.

Intended Audience

Administrators responsible for Flowmon ADS and Dell ECS configuration.

Configure Dell ECS

When leveraging ECS Connection Manager to load balance access to Dell ECS storage, we recommend configuring firewall rules to ensure applications cannot access Dell ECS nodes directly.

If the network firewall cannot be configured to ensure applications are not permitted to access Dell ECS nodes directly, Dell ECS IAM permission policies can be configured to ensure only S3 and/or IAM access proxied through the Progress ECS Connection Manager is permitted.

When an IP address is defined as allowed within a Dell ECS IAM permission, Dell ECS leverages the X-Forwarded-For header to validate the client IP. To ensure every request proxied through the ECS Connection Manager contains the allowed ECS Connection Manager IP address, a content switching rule to add the X-Forward-For header value is required. To configure this on the ECS Connection Manager navigate to **Rules & Checking > Content Rules > Create New** and define a rule as shown below:

(Ensure the “Value of Header Field to be replaced” is defined as the ECS Connection Manager virtual service or interface IP address.)

Apply the rule to its respective virtual service by navigating to **Virtual Services > View/Modify Services > Modify > Advanced Properties > HTTP Header Modification > Add Rule** as a request rule.

Configure Progress Flowmon Anomaly Detection System (ADS)

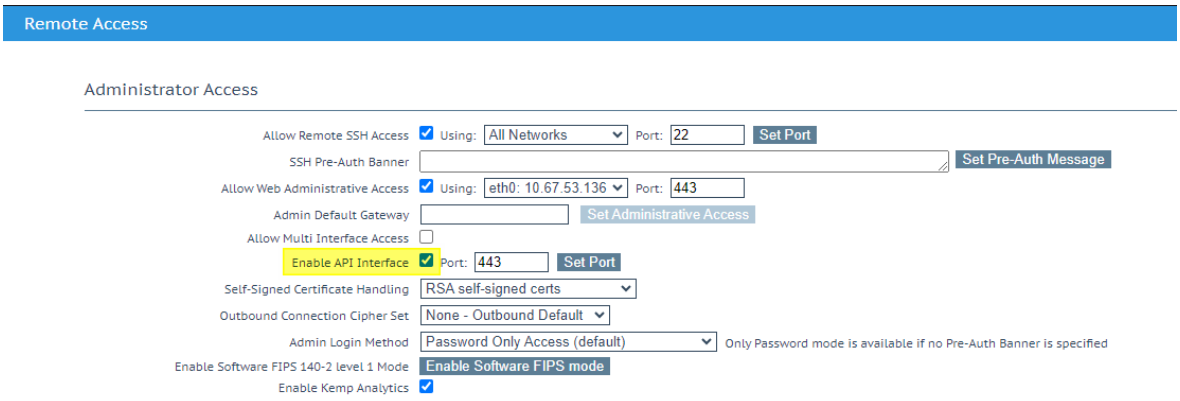
This guide assumes that you have Flowmon ADS configured with active Data Feeds and basic tuning completed. More details about configuration of the Flowmon system are in the User guide, which is included in every Flowmon appliance, or alternatively at the following location: https://docs.progress.com/.

This guide assumes you have ECS Connection Manager deployed and configured to load balance traffic across your Dell ECS cluster.

Enable ECS Connection Manager API Access

Flowmon will access ECS Connection Manager securely using a generated REST API key. Before a REST API key can be generated, REST API access must be enabled within the ECS Connection Manager's UI.

1. Log in to your ECS Connection Manager UI and navigate to **Certificates & Security > Remote Access**
2. Check the **Enable API Interface** box.



3. Generate a ECS Connection Manager API key via the following REST API curl request:

```
curl --location
'https://InsertECSConnectionManagerIPAddress/accessv2' \
--data '{
    "cmd": "addapikey",
    "apiuser": "bal",
    "apipass": "InsertPassword"
}'
```

4. Copy the generated API key to be used in a later step.

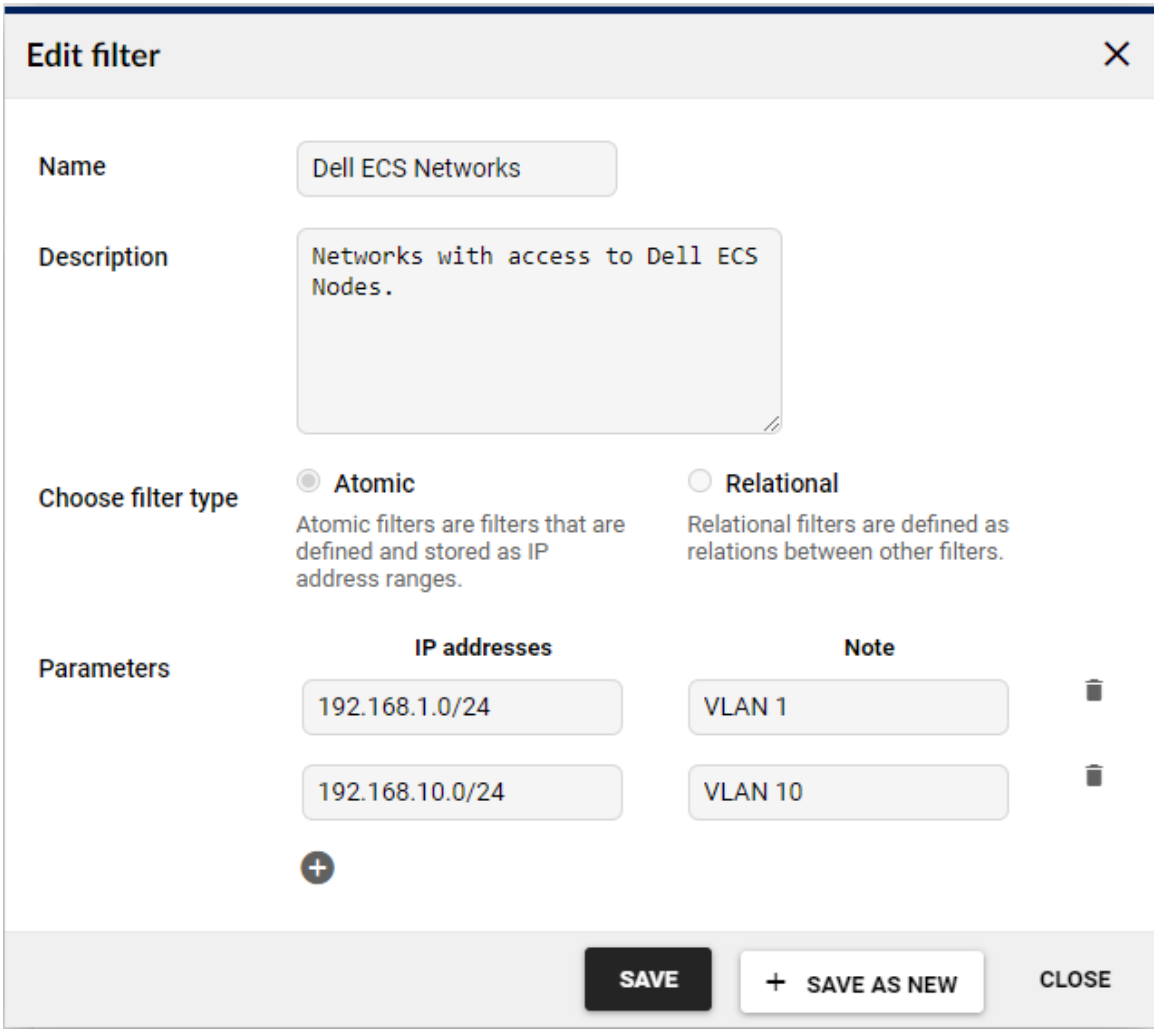
For more information on how to create and use ECS Connection Manager REST API keys, please refer to the following linked document: Interface Description RESTful API

Create a Flowmon ADS Filter

A filter will be used to define a Perspective that limits anomaly detection to the hosts/networks which have access to ECS storage networks.

1. Within the ADS Module, go to **Settings > Processing > Filters**.

2. Click **+ NEW FILTER**.



EXAMPLE ONLY

a) Provide a **Name**.

b) Select **Atomic**.

c) Under **Parameters,** add the networks that have access to PowerScale storage nodes.

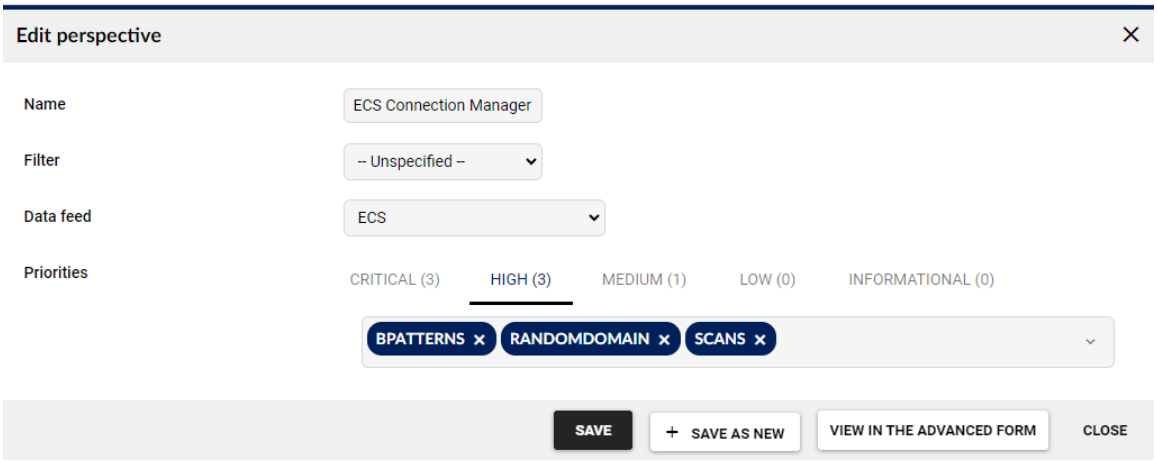
d) Click **SAVE**.

Create Perspective(s)

Create one or more Perspectives to categorize anomalies on the network.

This guide provides an example only. In production, you must identify what traffic your organization would like to enable alerts and triggers on.

1. Within the ADS module, go to **Settings** > **Processing** > **Perspectives**.
2. Click **+ NEW PERSPECTIVE**.



EXAMPLE ONLY

a) Provide a **Name**.

b) Select the relevant **Filter**.

c) Select the relevant **Data feed**.

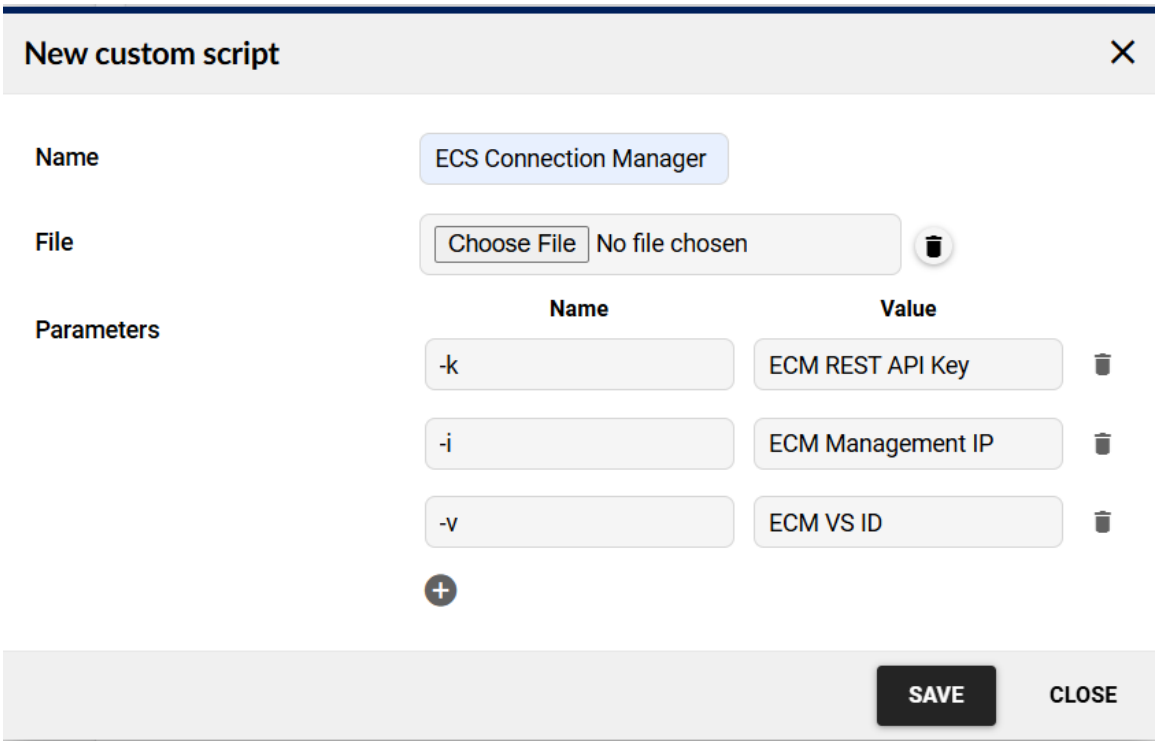
d) Select the priority (Critical, High, Medium, Low, and Informational) and add the relevant detection methods to each priority.

e) Click **SAVE**.

Create a Custom Script (API trigger)

In Flowmon ADS, custom scripts are used to automate actions when anomalous events are detected according to the configured Perspective. Each custom script must be bound to exactly one Perspective. A script can be in the active or inactive state.

1. Within the ADS Module, go to **Settings > System Settings > Custom scripts**.
2. Click **+ NEW CUSTOM SCRIPT**.
3. Provide a **Name** for the script.
4. Under **File**, click **Choose file** and select the custom script to trigger ECS Connection Manager actions.

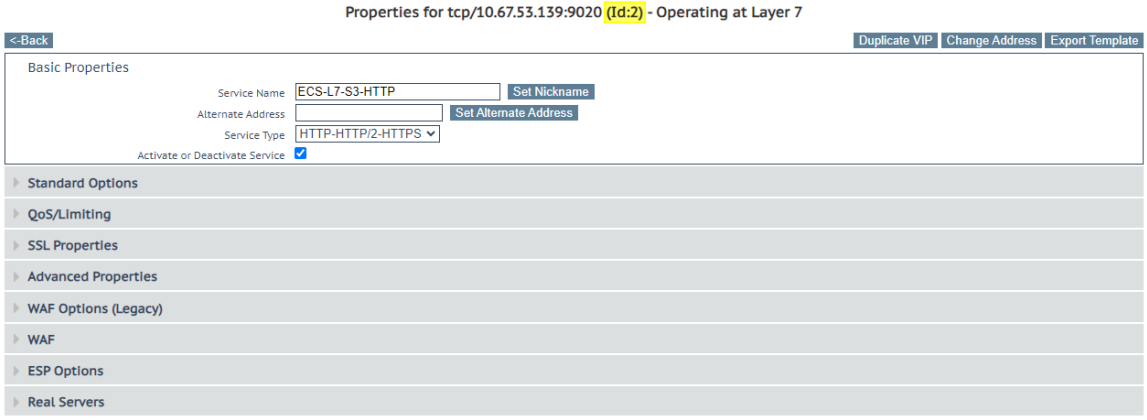


-k = ECS Connection Manager REST API Key.

-i = ECS Connection Manager management IP address.

-v = ECS Connection Manager virtual service ID.

(To gather a virtual service's ID within your ECS Connection Manager UI, Navigate to **Virtual Services > View/Modify Services > Modify.**)

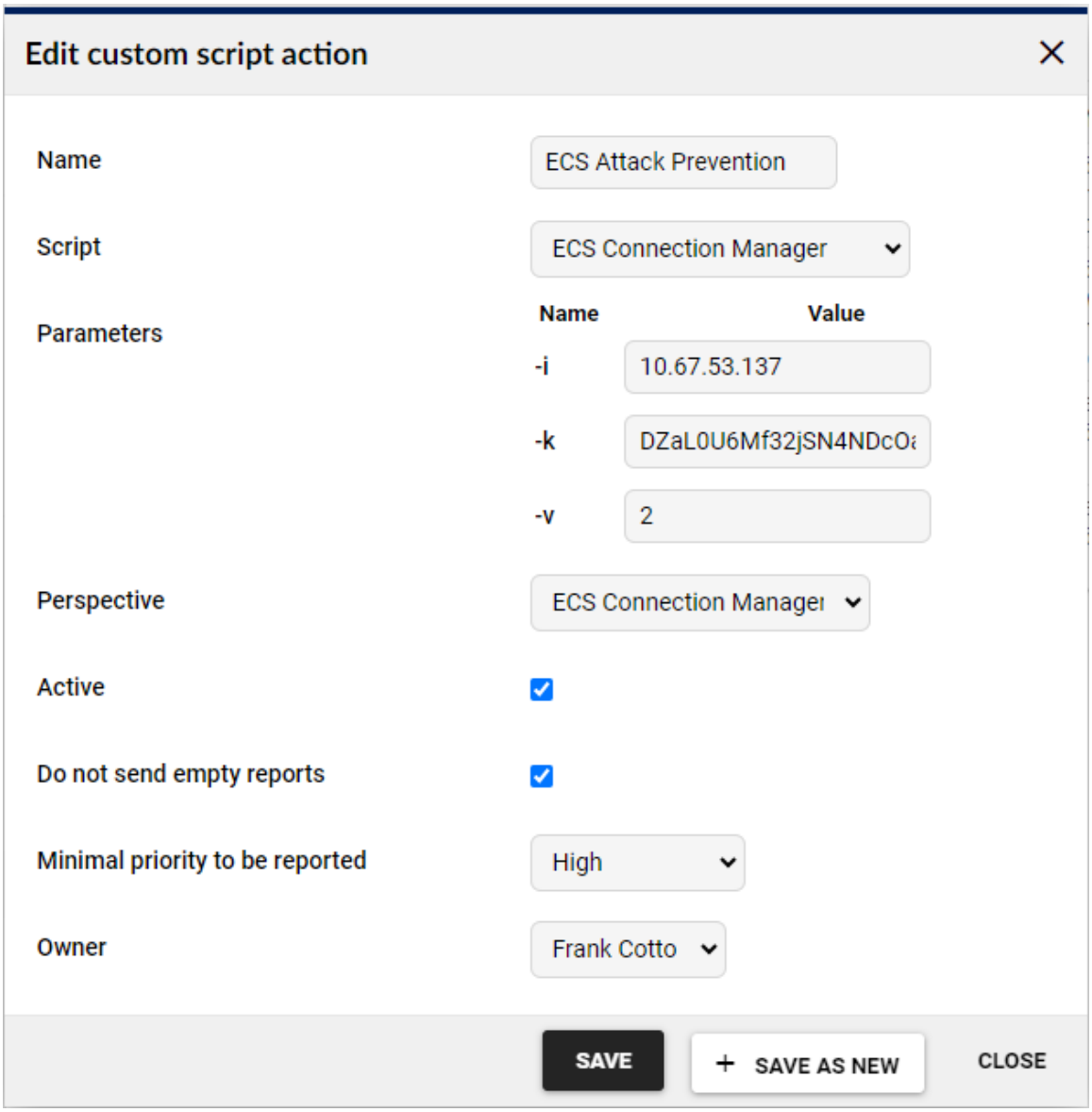


5. Click **SAVE**.
6. Within the ADS Module, go to **Settings > Processing > Custom scripts**.
7. Click **+ NEW CUSTOM SCRIPT ACTION**.
8. Provide a **Name** for the action.

   Select the **Perspective**.
9. Tick the box to make the action **Active**.

10. Set the **Minimum priority to be reported**.

11. Click **SAVE**.



Note: Following investigation and remediation of the Flowmon ADS events which generated ECS Connection Manager ACLs, ACL's can be deleted manually via the Progress ECS Connection Manager UI (**Virtual Services > View/Modify Services > Modify > Advanced Properties > Service Specific Access Control**) or via API.

Perspective Methods

Methods outlined within the perspectives shown are recommendations and should be adjusted as relevant to your network access details. Progress Flowmon engineers are available to assist with determining which methods should be leveraged and we recommend the testing of triggers to ensure all is working as expected before enabling the actions taken by this script in production.

As a good starting point leveraging the methods: SCANS, RANDOMDOMAIN, BPATTERNS, DICTATTACK, SSHDICT, RDPDICT, and BLACKLIST (BotnetActivities, MalwareDomains and BotnetDomains) will provide detection of hosts that are carrying out anomalous actions.