Flowmon ADS integration with PowerScale

Descriptions of steps required to implement integration between Flowmon ADS and Dell PowerScale.

Introduction

Integrating network anomaly detection with file storage can help with early warning, detection, and remediation of various security events. Flowmon Anomaly Detection System (ADS) provides real-time detection of threat actor exploits, and through this integration, can automatically configure PowerScale firewall rules to protect PowerScale 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 Dell PowerScale file storage to block a potentially harmful IP(s) on access to PowerScale by utilizing firewall rules.

Intended Audience

Anyone interested in configuring Progress Flowmon ADS and Dell PowerScale.

Configure Dell PowerScale

The following script can be used with OneFS version 9.5.0.0 or newer as it requires access to PowerScale’s firewall feature-set, which has been introduced in this version.

Ensure that “Firewall policies on the cluster” are enabled within your OneFS Firewall configuration settings.

The OneFS HTTP service should be enabled, and authentication settings should allow “Integrated authentication” and secure HTTP connections within the OneFS HTTP protocol settings. This setting supports the ability to access and authenticate to PowerScale via its API.

PowerScale users should duplicate the “default_pools_policy” Firewall configuration policy and apply the duplicated policy to the desired external network OneFS pools.

Take note of the duplicated policy name, as it will be outlined as a custom script parameter when configuring Flowmon at a later point.

This is the policy that Flowmon will automatically write new rules to, whenever it identifies anomalies within the network surrounding PowerScale.

Note: Following investigation and remediation of the Flowmon ADS events which generated PowerScale firewall rules, rules can be deleted manually via the PowerScale UI or via the PowerScale API.

Configure Progress Flowmon Anomaly Detection System (ADS)

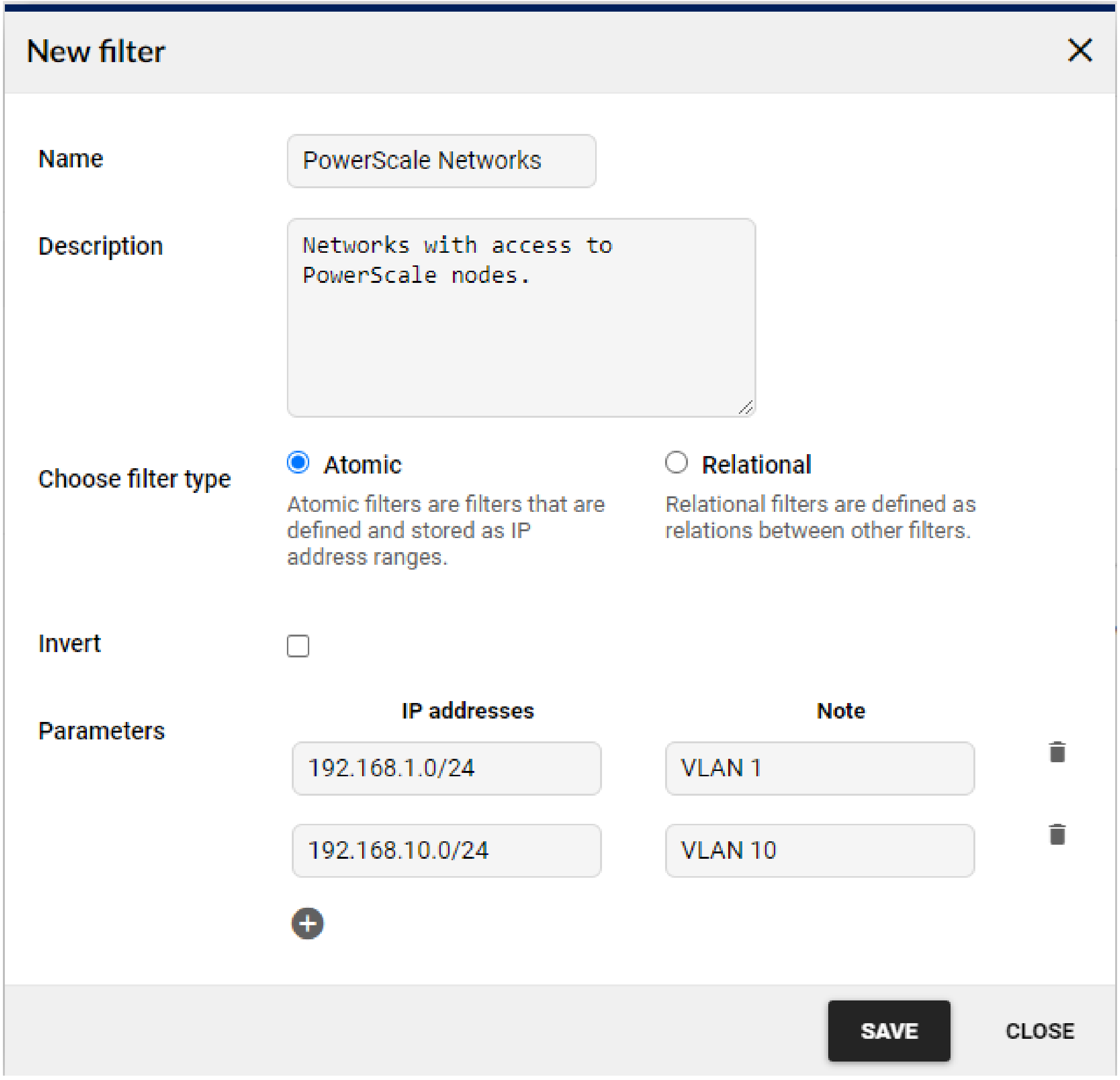
This guide assumes that you have Flowmon ADS configured with active Data Feeds and basic tuning completed. More details about configuration of the Flowmon system are in the User guide, which is included in every Flowmon appliance, or alternatively at the following location: https://docs.progress.com/.

Create a Filter

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

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

2. Click **+ NEW FILTER**.



New filter

Name	PowerScale Networks
Description	Networks with access to PowerScale nodes.
Choose filter type	● Atomic Atomic filters are filters that are defined and stored as IP address ranges. ○ Relational Relational filters are defined as relations between other filters.
Invert	□

Parameters

IP addresses	Note
192.168.1.0/24	VLAN 1
192.168.10.0/24	VLAN 10

EXAMPLE ONLY

a) Provide a **Name**.

b) Select **Atomic**.

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

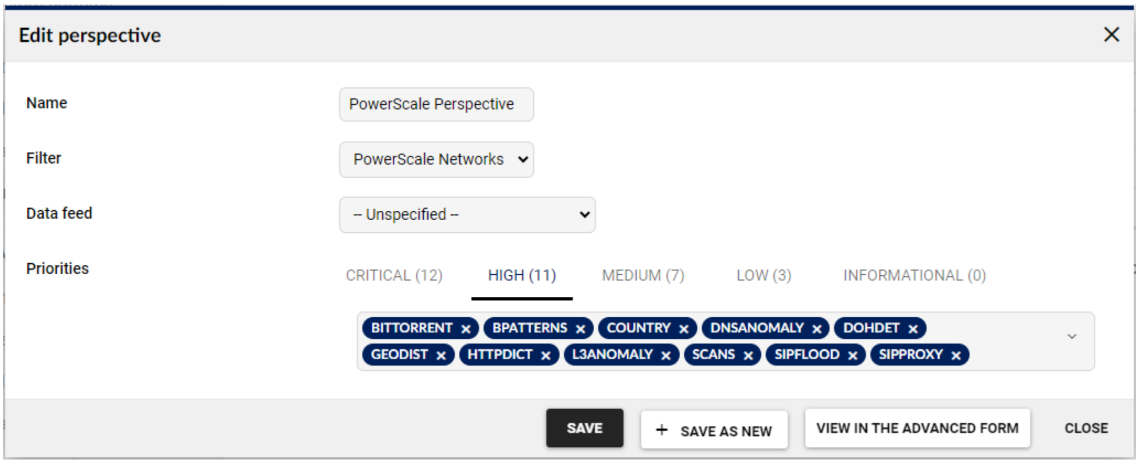
d) Click **SAVE**.

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**.



Edit perspective

Name: PowerScale Perspective

Filter: PowerScale Networks

Data feed: -- Unspecified --

Priorities: HIGH (11)

BITTORRENT, BPATTERNS, COUNTRY, DNSANOMALY, DOHDET, GEODIST, HTTPDICT, L3ANOMALY, SCANS, SIPFLOOD, SIPPROXY

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.

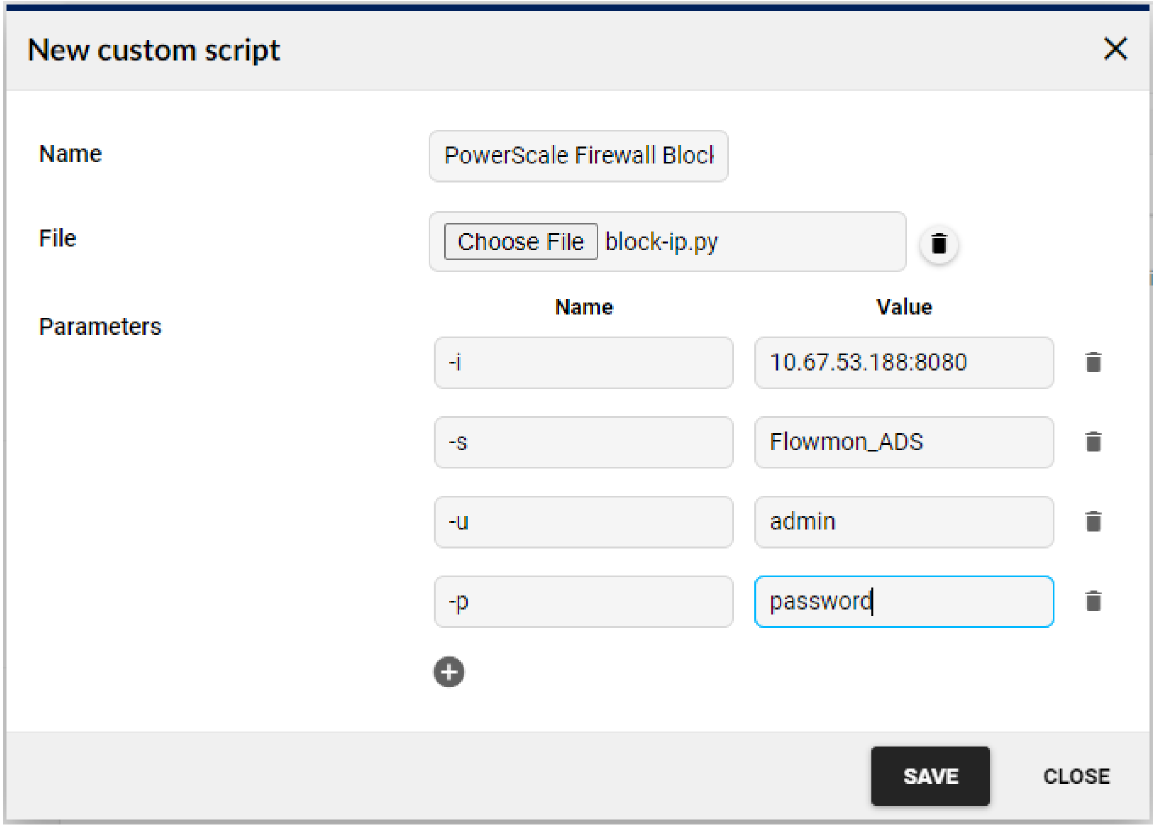
e) Click **SAVE**.

Create a Custom Script (API trigger)

In Flowmon ADS, custom scripts are used to automate actions when activities are needed based on the configured Perspective. Each custom script must be bound to exactly one Perspective. A script can be in the active or inactive state.

You can use the script provided by us which accepts the parameters for IP addresses/hostname and port if needed of Dell PowerScale, username and password for authentication. There is one mandatory parameter and that is name of

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 Veeam Backup & Replication actions.



New custom script

Name: PowerScale Firewall Block

File: Choose File block-ip.py

Parameters

Name	Value
-i	10.67.53.188:8080
-s	Flowmon_ADS
-u	admin
-p	password

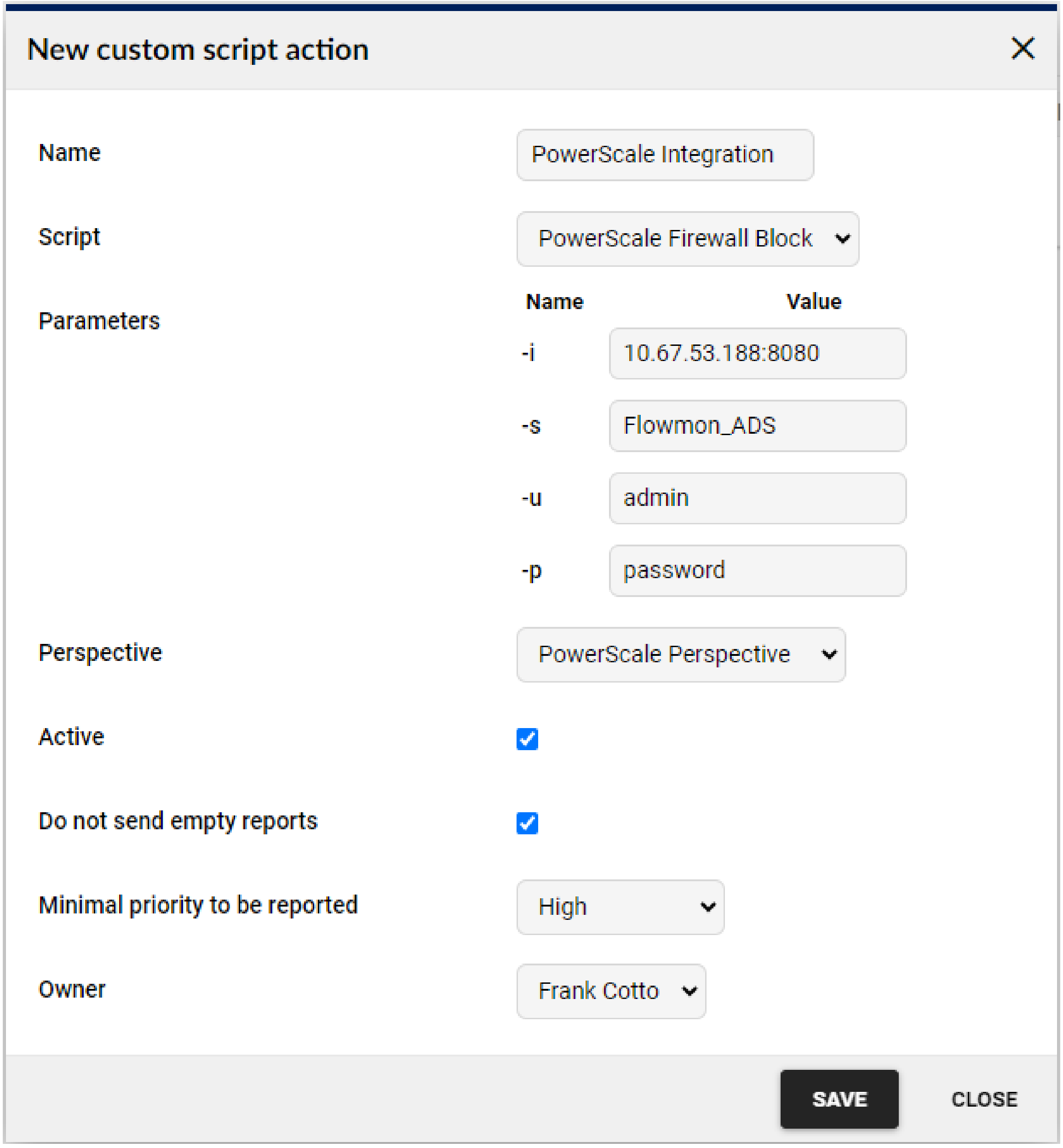
-i = PowerScale IP address which Flowmon will connect to via its API.

-s = PowerScale firewall policy name created to automated rule creation from Flowmon.

-u = PowerScale username used by Flowmon for API authentication to PowerScale API.

-**p** = PowerScale password used by Flowmon for API authentication to PowerScale API.

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.
9. Select the **Perspective**.
10. Tick the box to make the action **Active**.
11. Set the **Minimum priority to be reported**.
12. Click **SAVE**.



New custom script action

Name	PowerScale Integration	
Script	PowerScale Firewall Block	
Parameters	**Name**	**Value**
	-i	10.67.53.188:8080
	-s	Flowmon_ADS
	-u	admin
	-p	password
Perspective	PowerScale Perspective	
Active	☑	
Do not send empty reports	☑	
Minimal priority to be reported	High	
Owner	Frank Cotto	

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, ICMPANOM. and BLACKLIST (BotnetActivities, MalwareDomains and BotnetDomains) will provide detection of hosts that are carrying out anomalous actions.