Progress®

Flowmon ADS integration with Veeam Backup & Replication

Description of steps required to integrate Flowmon Anomaly Detection System (ADS) with Veeam Backup & Replication to identify and report threat actor movements on your network.

Introduction

Integrating Flowmon's network anomaly detection capabilities with Veeam's Backup & Replication solution can promote early warning, detection, and remediation of various security issues.

Document Purpose

This document provides recommended settings used when integrating Flowmon (Anomaly Detection System) ADS and Veeam Backup & Replication.

Intended Audience

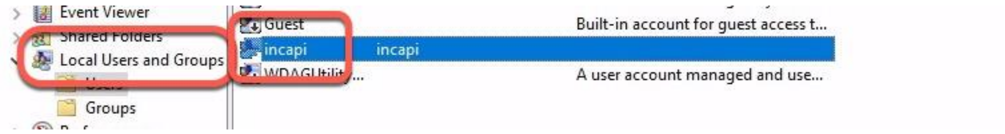
Anyone interested in leveraging Flowmon ADS to alert Veeam administrators to malicious activity sourced from devices that Veeam is deployed to protect and preserve.

Configure Veeam Backup & Replication

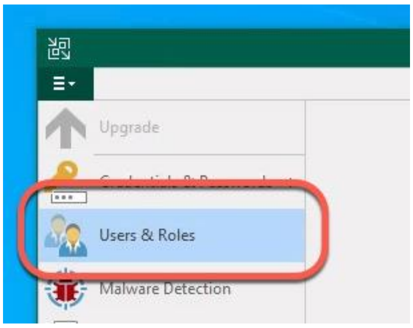
In the version of Veeam Backup & Replication (VBR) 12.2 was added a new feature allowing you to create an Incident API user only and this is recommended to be used with this script.

How to create this user and Role on the VBR Instance:

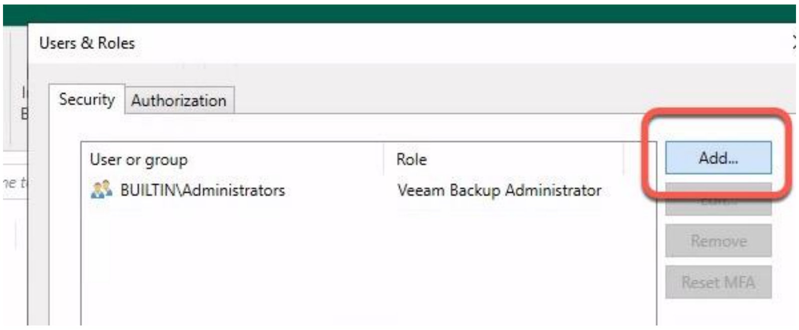
Create a Windows user (this will be the user and password You need within the Script):



Go to Users & Roles within VBR:

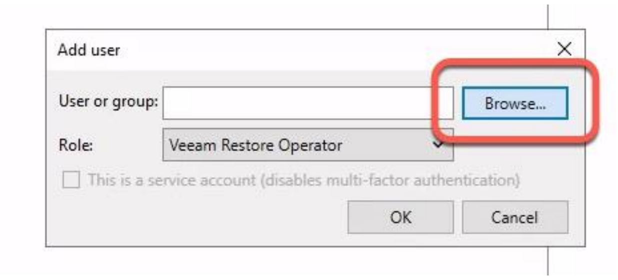


Click Add:



User or group	Role
BUILTIN\Administrators	Veeam Backup Administrator

Browse and add the prior created user:

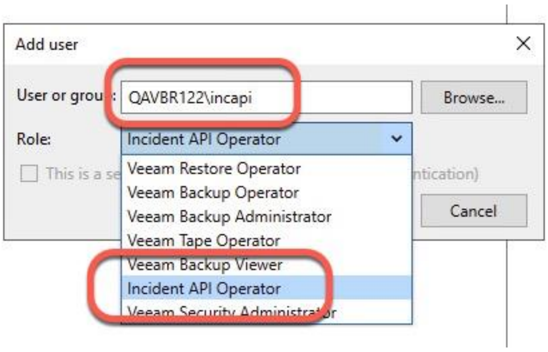


User or group:

Role: Veeam Restore Operator

□ This is a service account (disables multi-factor authentication)

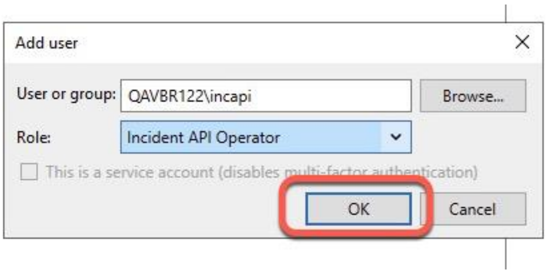
Change the Role to **Incident API Operator**:



User or group: QAVBR122\incapi

Role: Incident API Operator

Click OK twice:



User or group: QAVBR122\incapi

Role: Incident API Operator

□ This is a service account (disables multi-factor authentication)

Configure Progress Flowmon Anomaly Detection System (ADS)

We assume that you have deployed Flowmon ADS and have configured data feeds to filter analyzed network traffic. For more details around Flowmon ADS deployment and configuration please visit the follow documentation page: Progress Flowmon Anomaly Detection System

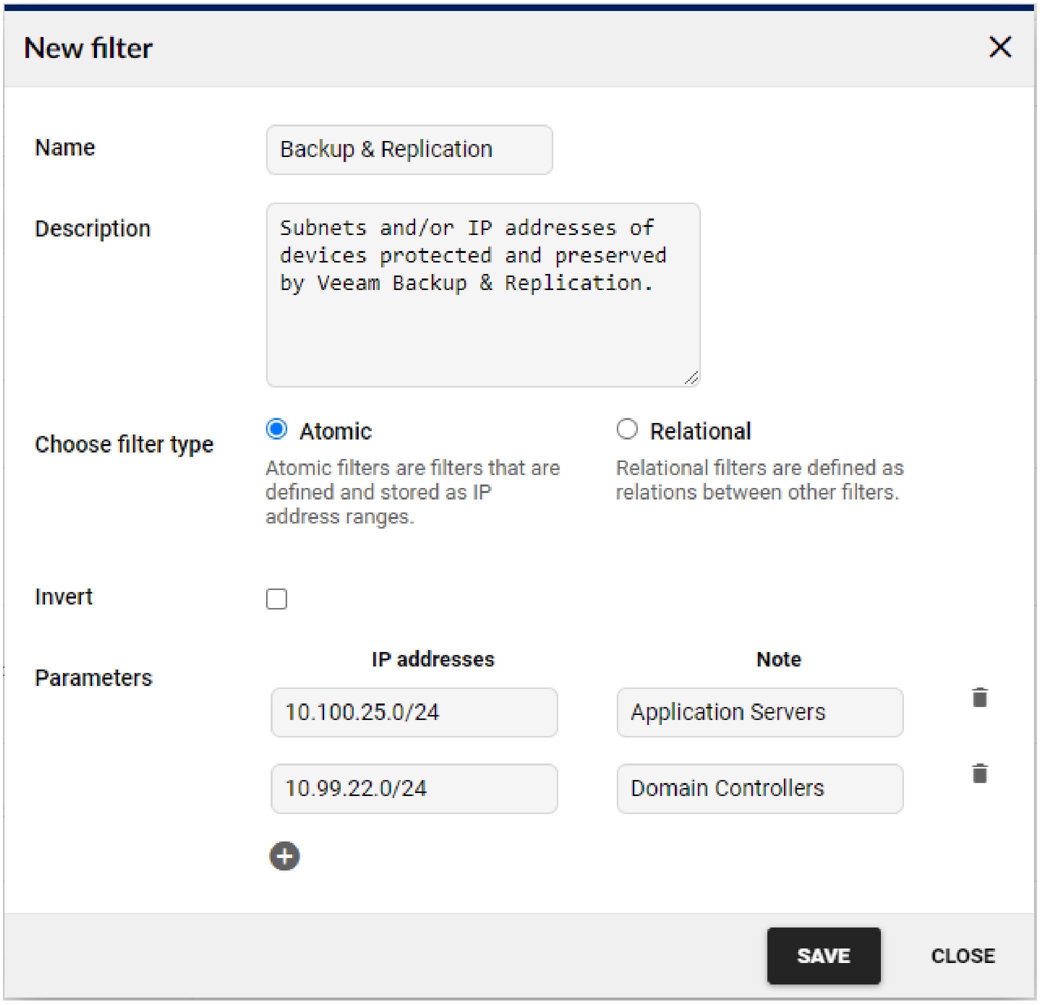
In order to have the script working properly you need a **reverse DNS records** configured for a segment where this script will be used as Veeam Backup & Replication requires to use two identifiers for the notification to be accepted.

Create a Filter

We would use a filter for Perspective as we want to limit detections only to the hosts where the backup is running.

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

2. Click **+ NEW FILTER**.

3. 

New filter

Name: Backup & Replication

Description: Subnets and/or IP addresses of devices protected and preserved by Veeam Backup & Replication.

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
10.100.25.0/24	Application Servers
10.99.22.0/24	Domain Controllers

EXAMPLE ONLY

a) Provide a **Name**.

b) Select **Atomic**.

c) Under **Parameters** add the networks that should be monitored for anomalies.

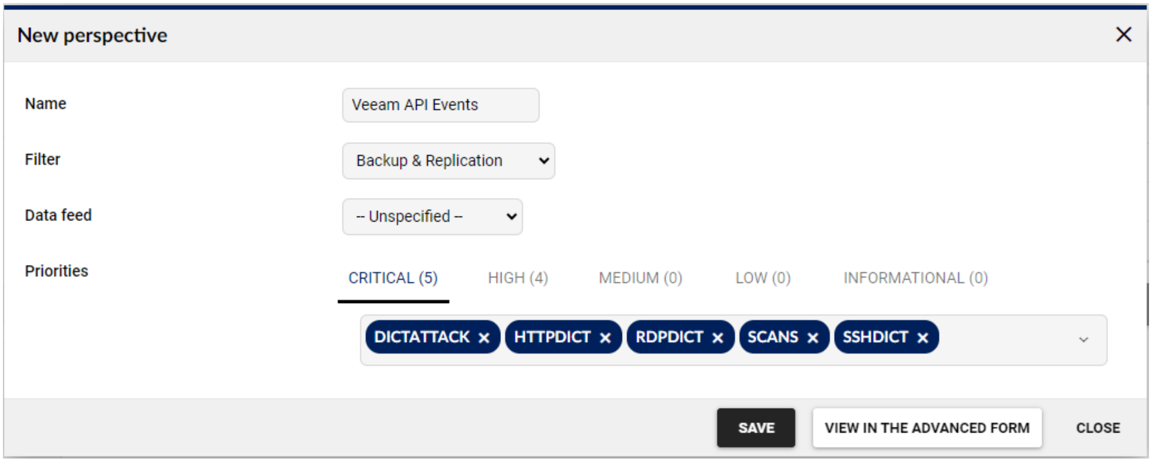
d) Click **SAVE**.

Create Perspective(s)

You can create one or more Perspectives to categorize anomalies on the network.

This document 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.



New perspective

Name: Veeam API Events

Filter: Backup & Replication

Data feed: -- Unspecified --

Priorities: CRITICAL (5) — DICTATTACK, HTTPDICT, RDPDICT, SCANS, SSHDICT

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.

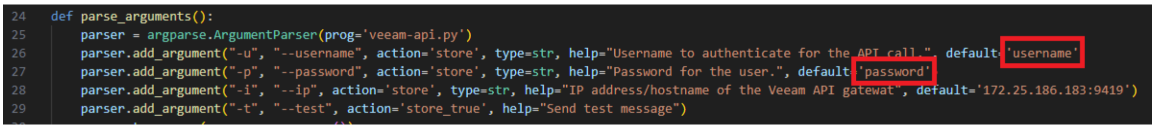
e) Click SAVE.

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.

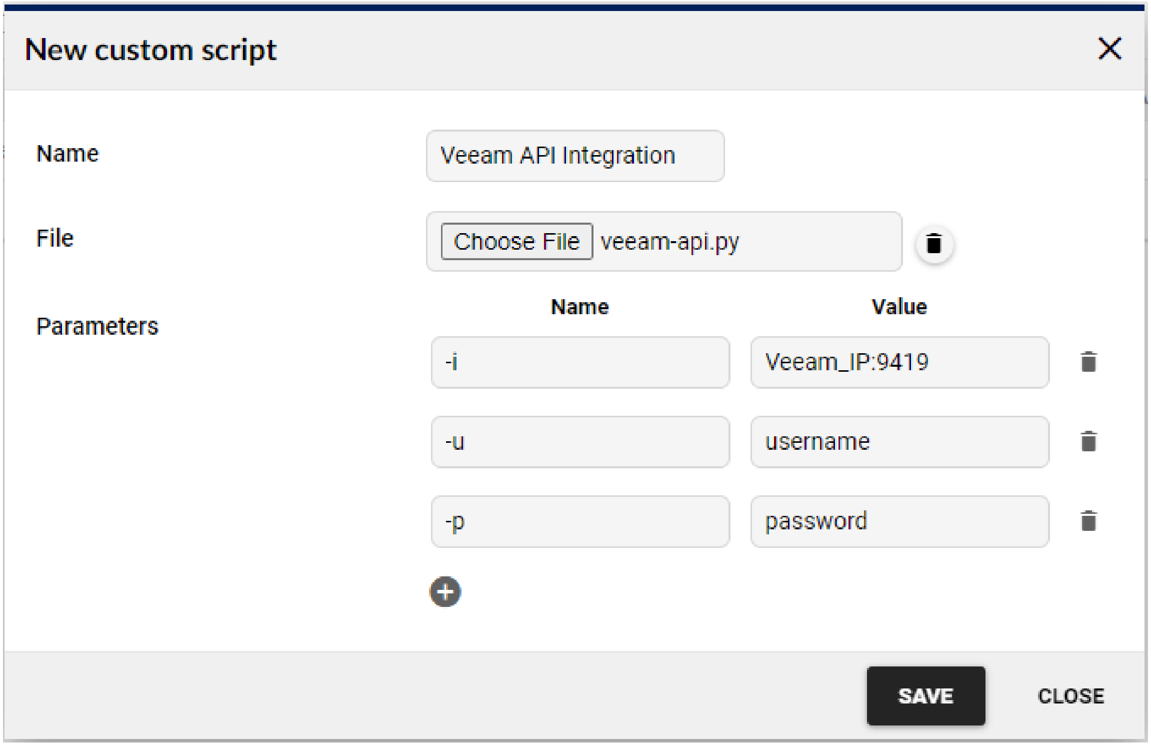
You can use the script provided by us which accepts the parameters for IP addresses/hostname and port if needed of Veeam Backup & Replication, username and password for authentication.

In case you don't want to have your password present in a clear form in Flowmon ADS user interface do not use the Parameters -u and -p and modify the code of the script lines 26 and 27 where is a default value with the correct values. That way it would be used what is in the script as a default value.



```
24  def parse_arguments():
25      parser = argparse.ArgumentParser(prog='veeam-api.py')
26      parser.add_argument("-u", "--username", action='store', type=str, help="Username to authenticate for the API call.", default='username')
27      parser.add_argument("-p", "--password", action='store', type=str, help="Password for the user.", default='password')
28      parser.add_argument("-i", "--ip", action='store', type=str, help="IP address/hostname of the Veeam API gatewat", default='172.25.186.183:9419')
29      parser.add_argument("-t", "--test", action='store_true', help="Send test message")
```

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: Veeam API Integration

File: Choose File veeam-api.py

Parameters

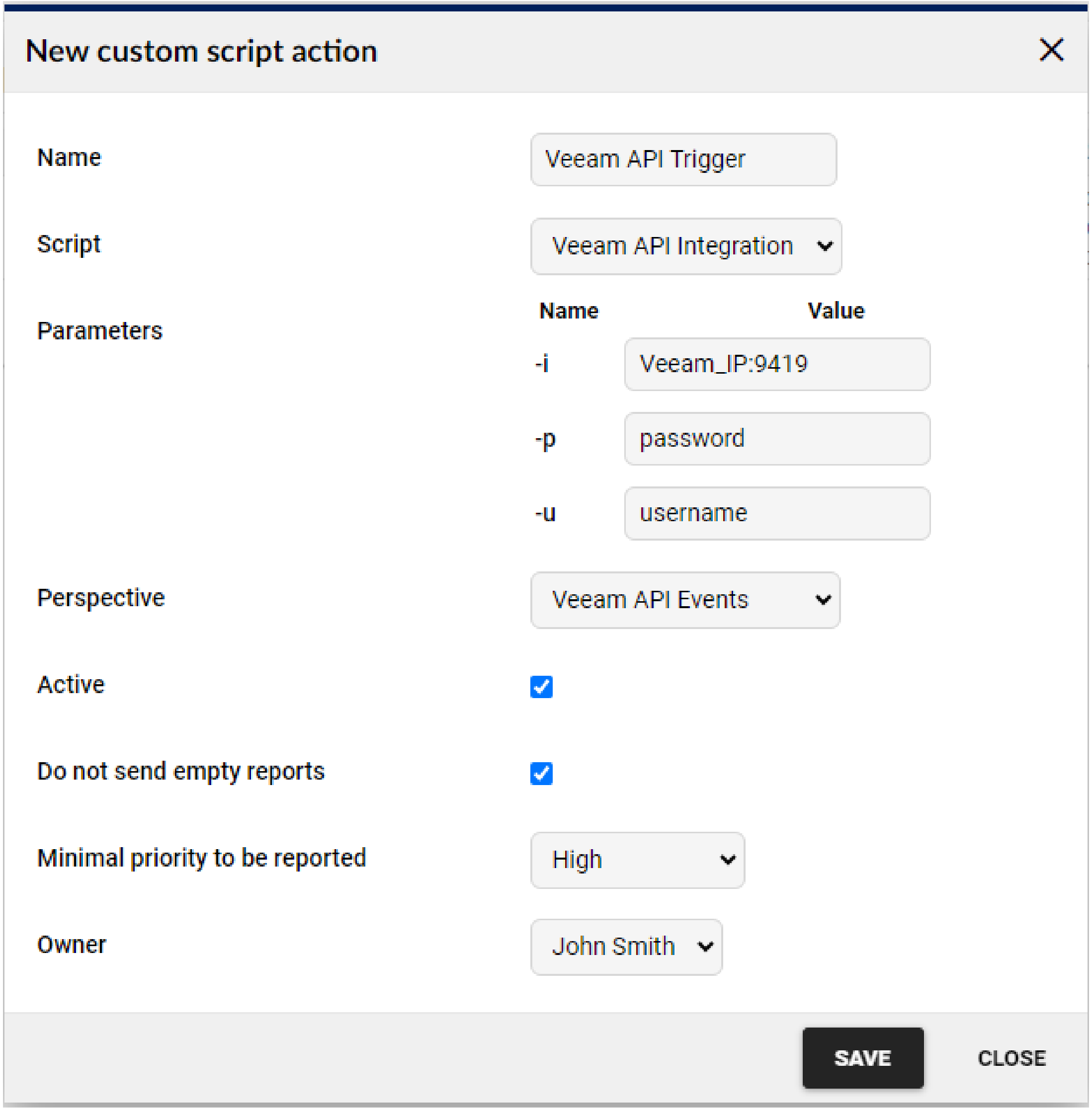
Name	Value
-i	Veeam_IP:9419
-u	username
-p	password

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	Veeam API Trigger
Script	Veeam API Integration
Parameters	

Name	Value
-i	Veeam_IP:9419
-p	password
-u	username

Perspective	Veeam API Events
Active	☑
Do not send empty reports	☑
Minimal priority to be reported	High
Owner	John Smith

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.