Netsurion®
Powering Secure and Agile Networks

How-To Guide

Configuring Amazon VPC Flow to Forward Logs to EventTracker

Publication Date:
September 22, 2021

Abstract

This guide provides instructions to configure Amazon VPC flow logs to EventTracker by means of syslog.

Scope

The configurations detailed in this guide are consistent with **EventTracker version 8.X and later**, and **Amazon VPC Flow.**

Audience

Amazon AWS users, who wish to forward its VPC flow to EventTracker Manager and monitor them using EventTracker.

Table of Contents

Table of Contents 3

1. Overview 4

2. Prerequisites 4

3. Publishing Amazon VPC Flow logs to CloudWatch 4

3.1 IAM roles for publishing flow logs to CloudWatch Logs 4

3.1.1 To create an IAM role for flow logs 5

3.2 To create a flow log for a VPC or a subnet using the console 5

4. Forwarding Flow Logs from CloudWatch to EventTracker 6

4.1 Implementing EventTracker Lambda function 6

4.2 Creating Subscription filters for CloudWatch 7

5. System Extraction 8

About Netsurion 9

Contact Us 10

1. Overview

VPC Flow logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow logs can help you with several tasks, such as:

- Monitoring the traffic that is reaching your instance.
- Determining the direction of the traffic to and from the network interfaces.

EventTracker AWS Lambda function can help you to integrate AWS instance for forwarding VPC Flow logs to EventTracker manager. After integrating the VPC flow, we can visualize traffic flowing through the AWS environment. This traffic details can also be exported using flex report feature which contains information about the identity of source, destination and EC2 instance details generated in this flow.

2. Prerequisites

- **EventTracker v9.3 and later** should be installed.
- **Admin access of AWS Account** should be available during integration.
- EventTracker syslog VCP port **should be publicly NAT**. So that AWS can send logs to EventTracker Manager.
- **EventTrackerAWSAgent v1.0.10 and later** should be configured.

3. Publishing Amazon VPC Flow logs to CloudWatch

3.1 IAM roles for publishing flow logs to CloudWatch Logs

The IAM role that's associated with your flow log much have sufficient permissions to publish flow logs to the specified log group in CloudWatch Logs. The IAM role must belong to your AWS account.

The IAM policy that's attached to you IAM role must include at least the following permissions.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Also ensure that your role has a trust relationship that allows the flow logs service to assume the role.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "vpc-flow-logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

You can update an existing role or use the following procedure to create a new role for use with flow logs.

3.1.1 To create an IAM role for flow logs

1. Open the IAM console at https://console.aws.amazon.com/iam/
2. In the navigation pane, choose **Roles, Create role**.
3. For **Select type of trusted entity**, choose **AWS service**. For **Use case**, choose **EC2**. Choose **Next: Permissions**.
4. On the **Attach permissions policies** page, choose **Next: Tags** and optionally add tags. Choose **Next: Review**.
5. Enter a name for your role and optionally provide a description. Choose **Create role**.
6. Select the name of your role. For **Permissions**, choose **Add inline policy, JSON**.
7. Copy the first policy from IAM roles for publishing flow logs to CloudWatch Logs and paste it in the window. Choose **Review policy**.
8. Enter a name for your policy and choose **Create policy**.
9. Select the name of your role. For **Trust relationships**, choose **Edit trust relationship**. In the existing policy document, change the service from ec2.amazonaws.com to vpc-flow-logs.amazonaws.com. Choose **Update Trust Policy**.
10. On the **Summary** page, note the ARN for your role. You need this ARN when you create your flow log.

3.2 To create a flow log for a VPC or a subnet using the console

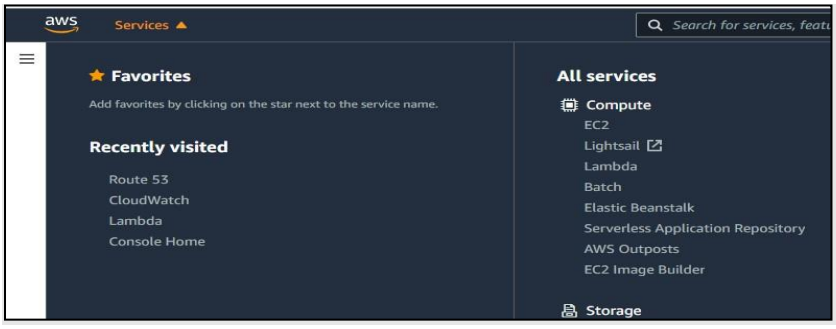
1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Your VPCs** or choose **Subnets**.
3. Select the checkbox for one or more VPCs or subnets and then choose **Actions**, **Create flow log**.
4. For **Filter**, specify the type of traffic to log. Choose **All** to log accepted and rejected traffic.

5. For **Maximum aggregation interval**, choose the maximum period during which a flow is captured and aggregated into one flow log record.
6. For **Destination**, choose **Send to CloudWatch Logs**.
7. For **Destination log group**, choose the name of the destination log group that you have created.
8. For **IAM role**, specify the name of the role that has permissions to publish logs to CloudWatch Logs.
9. For **Log record format** choose **Custom format** and then select all fields from **Log format**.
10. (Optional) Choose **Add new tag** to apply tags to the flow log.
11. Choose **Create flow log**.

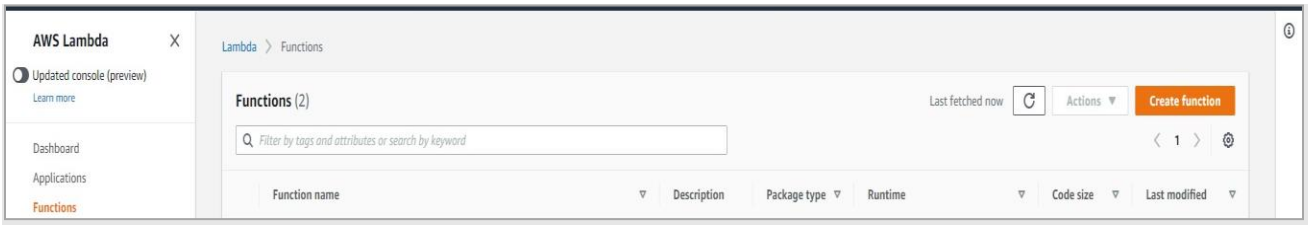
4. Forwarding Flow Logs from CloudWatch to EventTracker

4.1 Implementing EventTracker Lambda function

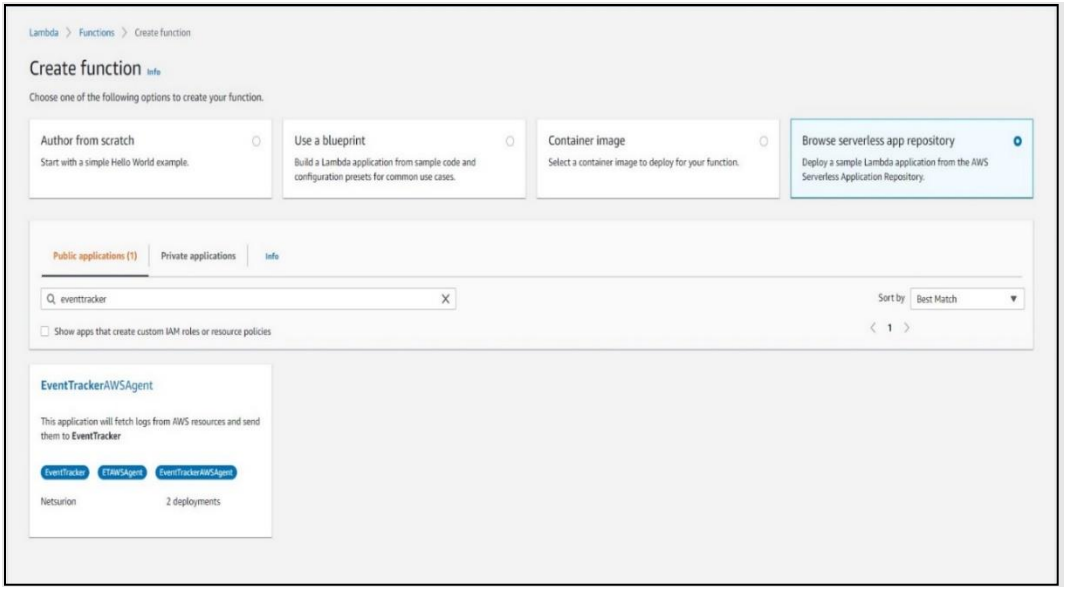
1. Click on **services** and select **lambda.**



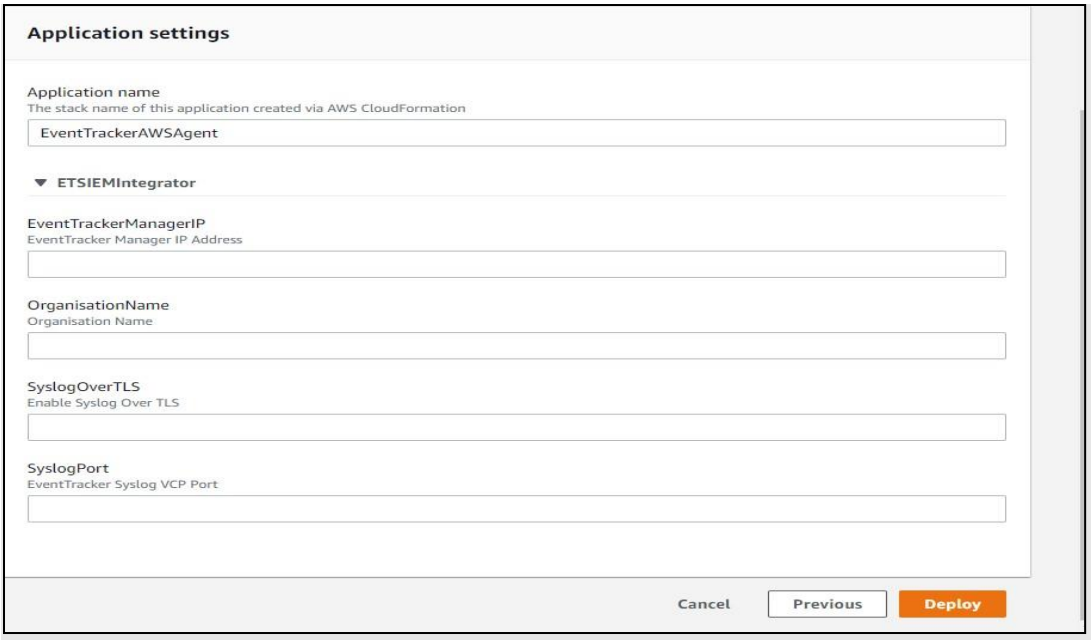
2. In the navigation pane choose **Functions**, then click on **Create function**.



3. Select **Browse serverless app repository.**
4. Search **EventTracker** in public applications. You will get the **EventtrackerAWSAgent** in results.



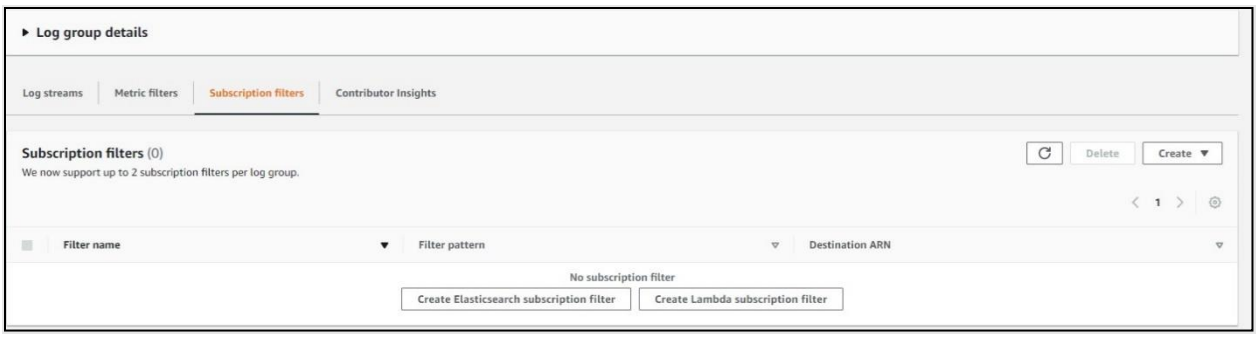
5. Fill in the details and click **Deploy**.



6. Enter the EventTracker Public Manager IP.
7. Enable syslog over TLS as **True** or **False.**
8. Enter the syslog port.
9. After you click **Deploy**, a function is created.

4.2 Creating Subscription filters for CloudWatch

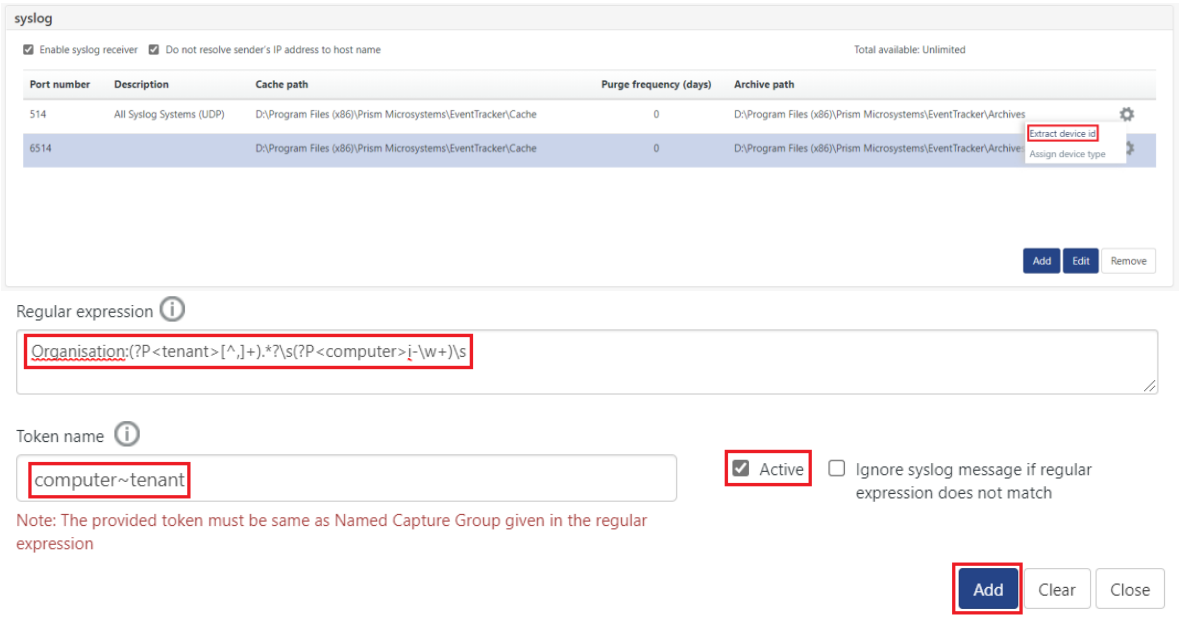
1. Click on **services** and select **CloudWatch.**
2. In the navigation pane, choose **log group**.
3. Click on the **log group** provided while enabling VPC Flow.
4. Go to **subscription filter**.



5. Click on **Create Lambda subscription filter**.
6. Under lambda function, select the lambda function (created after deploying the application) created from the dropdown.
7. Enter subscription filter name, i.e., **VPCFlow**.
8. Click on **start streaming**.

5. System Extraction

1. Login to EventTracker Manager.
2. Navigate to **Admin** > **Manager** > **syslog/Virtual Collection Point.**
3. Hover over on gear icon for getting Extract Id option. Please click on it for extracting system name using below regex:
4. Fill the following details:
   Regular expression: Organisation:(?P<tenant>[^,]+).*?\s(?P<computer>i-\w+)\s
   Token Name: computer~tenant



5. Click on **Add** button for saving the extraction logic.

About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's cybersecurity platforms enable companies to deliver on both. Netsurion's approach of combining purpose-built technology and an ISO-certified security operations center gives customers the ultimate flexibility to adapt and grow, all while maintaining a secure environment.

Netsurion's EventTracker cyber threat protection platform provides SIEM, endpoint protection, vulnerability scanning, intrusion detection and more; all delivered as a managed or co-managed service. Netsurion's BranchSDO delivers purpose-built technology with optional levels of managed services to multi-location businesses that optimize network security, agility, resilience, and compliance for branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit netsurion.com or follow us on Twitter or LinkedIn. Netsurion is #19 among MSSP Alert's 2020 Top 250 MSSPs.

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

EventTracker Enterprise SOC: 877-333-1433 (Option 2)
EventTracker Enterprise for MSP's SOC: 877-333-1433 (Option 3)
EventTracker Essentials SOC: 877-333-1433 (Option 4)
EventTracker Software Support: 877-333-1433 (Option 5)
https://www.netsurion.com/eventtracker-support