Network Monitoring System and eBPF Metrics Interpretation

# Overview

This document provides an interpretation of system and eBPF metrics, and how to use this data for network monitoring and analysis.   
The metrics are collected from both system-level resources (CPU, memory, disk usage) and network performance metrics gathered via   
an eBPF-based monitoring system.  
  
The provided sample data consists of two key sections:  
1. \*\*System Metrics\*\* – Information about the system's resources like CPU usage, memory usage, and disk space.  
2. \*\*eBPF Metrics\*\* – Network performance data collected using eBPF maps, including bandwidth usage, jitter, latency, and outbound traffic per IP address.

# Sample Data

## System Metrics

{  
 "System Metrics": {  
 "CPU Usage": [  
 2.0100502512565113,  
 1.0050251256282556  
 ],  
 "Free Disk": 54.425323486328125,  
 "Free Memory": 0.4799346923828125,  
 "Total Disk": 97.86907196044922,  
 "Total Memory": 3.7775192260742188,  
 "Used Disk": 38.42827224731445,  
 "Used Memory": 1.6742362976074219  
 }  
}

## eBPF Metrics

{  
 "eBPF Metrics": {  
 "Bandwidth Usage": {  
 "25864384": 160,  
 "426857100": 140,  
 "985562553": 90  
 },  
 "DNS Queries": {},  
 "Firewall Rules": {},  
 "HTTP Requests": {},  
 "Jitter": {  
 "426857100": 604169  
 },  
 "Latency": {  
 "426857100": 604169  
 },  
 "Outbound Traffic": {  
 "25864384": 1,  
 "426857100": 2,  
 "985562553": 1  
 }  
 }  
}

# Interpretation of System Metrics

## CPU Usage

"CPU Usage": [  
 2.0100502512565113,  
 1.0050251256282556  
]  
  
\*\*Interpretation\*\*:  
- \*\*CPU Usage\*\* is represented as a percentage (or ratio) of CPU usage over time. The two values in the array could represent the CPU usage over two sampling intervals.  
 - The first value `2.0100502512565113` indicates that the CPU usage at the first interval is approximately \*\*2.01%\*\*.  
 - The second value `1.0050251256282556` indicates that the CPU usage at the second interval is approximately \*\*1.01%\*\*.  
  
\*\*Dashboard Representation\*\*:  
- This data could be represented using a \*\*line chart\*\* or \*\*bar chart\*\* that tracks CPU usage over time.  
  
\*\*Insights\*\*:  
- Low CPU usage like \*\*2%\*\* suggests that the system is under light load.  
- Monitoring these values helps ensure that the CPU is not under-provisioned or overly taxed.

## Memory Metrics

"Free Memory": 0.4799346923828125,  
"Used Memory": 1.6742362976074219,  
"Total Memory": 3.7775192260742188  
  
\*\*Interpretation\*\*:  
- \*\*Free Memory\*\*: The amount of free RAM available in the system, approximately \*\*0.48 GB\*\*.  
- \*\*Used Memory\*\*: The amount of RAM being utilized, approximately \*\*1.67 GB\*\*.  
- \*\*Total Memory\*\*: The total available RAM, approximately \*\*3.78 GB\*\*.  
  
\*\*Dashboard Representation\*\*:  
- \*\*Pie Chart\*\*: To show the ratio of \*\*Used Memory\*\* to \*\*Free Memory\*\*.  
- \*\*Bar Chart\*\*: To track \*\*Used Memory\*\* and \*\*Free Memory\*\* separately over time.  
  
\*\*Insights\*\*:  
- Memory usage of around \*\*1.67 GB\*\* indicates a moderate load on the system, with \*\*approximately 0.48 GB free\*\*.  
- Keeping an eye on memory usage over time can help identify if the system is running out of memory.

## Disk Metrics

"Free Disk": 54.425323486328125,  
"Used Disk": 38.42827224731445,  
"Total Disk": 97.86907196044922  
  
\*\*Interpretation\*\*:  
- \*\*Free Disk\*\*: The amount of available disk space, approximately \*\*54.43 GB\*\*.  
- \*\*Used Disk\*\*: The amount of disk space that has been consumed, approximately \*\*38.43 GB\*\*.  
- \*\*Total Disk\*\*: The total disk space, approximately \*\*97.87 GB\*\*.  
  
\*\*Dashboard Representation\*\*:  
- \*\*Pie Chart\*\* showing the \*\*used\*\* vs \*\*free disk space\*\*.  
- \*\*Bar Chart\*\* for tracking \*\*Used Disk\*\* and \*\*Free Disk\*\* over time.  
  
\*\*Insights\*\*:  
- \*\*54.43 GB free\*\* suggests that there is ample disk space left.  
- It's important to monitor disk usage to avoid running out of space, especially in data-intensive applications.

# Interpretation of eBPF Metrics

## Bandwidth Usage

"Bandwidth Usage": {  
 "25864384": 160,  
 "426857100": 140,  
 "985562553": 90  
}  
  
\*\*Interpretation\*\*:  
- The keys represent \*\*IP addresses\*\* and the values represent the \*\*bandwidth usage\*\* for that IP address in \*\*Mbps\*\*.  
 - \*\*IP 25864384\*\* is using \*\*160 Mbps\*\*.  
 - \*\*IP 426857100\*\* is using \*\*140 Mbps\*\*.  
 - \*\*IP 985562553\*\* is using \*\*90 Mbps\*\*.  
  
\*\*Dashboard Representation\*\*:  
- \*\*Bar Chart\*\*: Show the bandwidth usage for each IP.  
 - X-axis: IP addresses (`25864384`, `426857100`, `985562553`)  
 - Y-axis: Bandwidth (Mbps)  
  
\*\*Insights\*\*:  
- \*\*IP 25864384\*\* is using the highest bandwidth, potentially requiring further investigation for unusual traffic.  
- Alerts can be configured for IP addresses that exceed a certain bandwidth threshold, e.g., \*\*100 Mbps\*\*.

## Jitter

"Jitter": {  
 "426857100": 604169  
}  
  
\*\*Interpretation\*\*:  
- \*\*IP 426857100\*\* has a \*\*jitter value\*\* of \*\*604169 milliseconds\*\*, which translates to \*\*604 seconds\*\*.  
- Jitter measures the variation in packet arrival times, and a high value indicates network instability.  
  
\*\*Dashboard Representation\*\*:  
- \*\*Line Graph\*\*: Track jitter over time for each IP.  
  
\*\*Insights\*\*:  
- \*\*604 seconds of jitter\*\* is extremely high, indicating that the network connection is unstable.  
- \*\*Alerts\*\* can be set for any jitter value above a specific threshold (e.g., \*\*100 ms\*\*), as high jitter can affect real-time services.

## Latency

"Latency": {  
 "426857100": 604169  
}  
  
\*\*Interpretation\*\*:  
- \*\*IP 426857100\*\* has a \*\*latency value\*\* of \*\*604169 milliseconds\*\* (or \*\*604 seconds\*\*).  
- Latency represents the delay in network communication.  
  
\*\*Dashboard Representation\*\*:  
- \*\*Line Graph\*\*: Track latency over time for each IP address.  
  
\*\*Insights\*\*:  
- \*\*604 seconds of latency\*\* is extraordinarily high and indicates a significant network delay.  
- \*\*Alerts\*\* should be configured if latency exceeds a threshold (e.g., \*\*100 ms\*\*), as it can severely impact user experience and application performance.

## Outbound Traffic

"Outbound Traffic": {  
 "25864384": 1,  
 "426857100": 2,  
 "985562553": 1  
}  
  
\*\*Interpretation\*\*:  
- \*\*Outbound Traffic\*\* is represented by IP addresses and their corresponding traffic units.  
 - \*\*IP 25864384\*\* sent \*\*1 unit\*\* of outbound traffic.  
 - \*\*IP 426857100\*\* sent \*\*2 units\*\* of outbound traffic.  
 - \*\*IP 985562553\*\* sent \*\*1 unit\*\* of outbound traffic.  
  
\*\*Dashboard Representation\*\*:  
- \*\*Bar Chart\*\*: Show outbound traffic for each IP.  
 - X-axis: IP addresses  
 - Y-axis: Outbound traffic units  
  
\*\*Insights\*\*:  
- \*\*Outbound traffic\*\* indicates the amount of data being sent from each IP, and unusually high outbound traffic could indicate a potential data exfiltration or misconfigured system.  
- Alerts can be set to trigger when any IP exceeds a certain threshold of outbound traffic, e.g., \*\*100 units\*\*.

# Conclusion and Dashboard Design

### Overall Insights:  
- \*\*System Metrics\*\* provide important information about the state of system resources (CPU, memory, disk). It’s important to monitor these metrics to ensure that the system is not under excessive load or running out of resources.  
- \*\*eBPF Metrics\*\* give insight into the health of the network, focusing on bandwidth usage, jitter, latency, and outbound traffic. These metrics are key to identifying network issues or unusual behavior from specific IP addresses.  
  
### Dashboard Layout:  
1. \*\*System Metrics Panel\*\*:  
 - \*\*CPU Usage\*\*: Line or bar chart  
 - \*\*Memory Usage\*\*: Pie chart showing used vs. free memory  
 - \*\*Disk Usage\*\*: Pie chart showing used vs. free disk space  
  
2. \*\*Network Health Panel\*\* (eBPF Metrics):  
 - \*\*Bandwidth Usage\*\*: Bar chart for each IP  
 - \*\*Jitter\*\*: Line graph showing jitter for each IP  
 - \*\*Latency\*\*: Line graph showing latency for each IP  
 - \*\*Outbound Traffic\*\*: Bar chart showing outbound traffic for each IP  
  
3. \*\*Alerts Panel\*\*:  
 - Alerts based on thresholds for \*\*CPU Usage\*\*, \*\*Memory Usage\*\*, \*\*Bandwidth\*\*, \*\*Jitter\*\*, \*\*Latency\*\*, and \*\*Outbound Traffic\*\*.