GUIDE
SAR Performance Monitoring on Ubuntu

v1.0.1

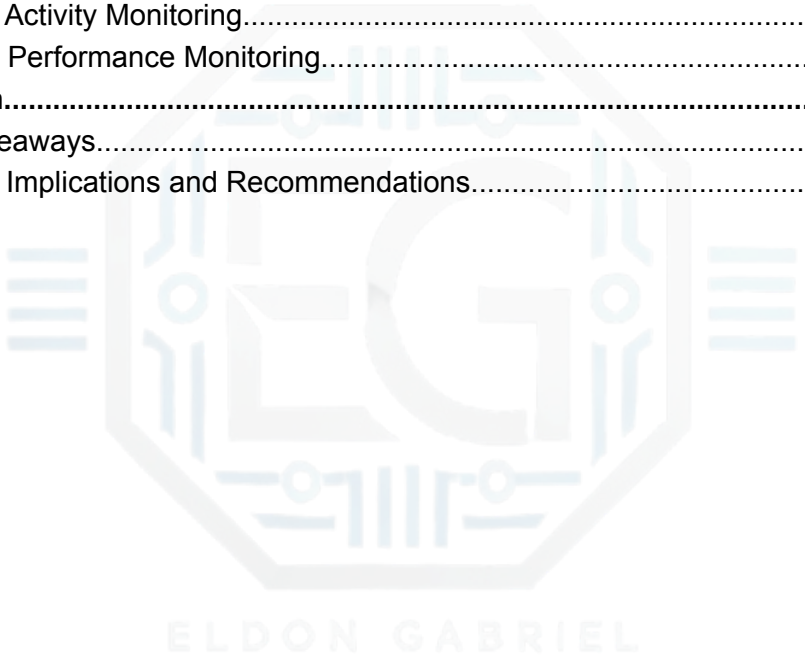
Author:

Eldon Gabriel

March 16, 2026

Security Systems Specialist

Table Of Contents



Disclaimer: This report documents the author's personal work in completing an MCSI lab exercise. It reflects the author's independent understanding and use of the System Activity Reporter (SAR) tool on Ubuntu 24.04.3 LTS in a controlled Linux environment. No MCSI video content, lab materials, or proprietary instructions were shared or distributed. All the information presented complies with the MCSI disclosure requirements and academic integrity policies.

Revision History

Version	Date	Author	Description of Changes
v1.0.0	01/28/2026	Eldon G.	Initial draft.
v1.0.1	03/16/2026	Eldon G.	Title update.

1.0 SAR Performance Monitoring

1.1 Project Description

This document explains the purpose of the SAR and the main commands used to check system performance on Ubuntu 24.04.3 LTS. SAR is part of the `sysstat` tools package. It provides visibility into Linux system performance across the CPU, memory, disk, and network resources.

1.2 SAR Installation and Configuration Overview

On Ubuntu 24.04.3 LTS, SAR is provided by the `sysstat` package and is not enabled by default. Installation was performed using the system package manager.

The `sysstat` package provides SAR and related system monitoring utilities. After installation, data collection must be explicitly enabled to allow SAR to record system activity over time.

When the `sysstat` service is turned on, it operates in the background. It regularly collects performance data that can be checked using SAR commands.

1.2.1 Enabling System Activity Data Collector

To enable historical performance data collection (SAR) on Ubuntu distributions, which is disabled by default, you need to set `ENABLED="true"` in `/etc/default/sysstat`. Once configured, the system activity data collector (sadc) can store the system activity logs in `/var/log/sysstat/`.

1.3 CPU Performance Monitoring

1.3.1 Overall CPU Usage

SAR can be used to view the average CPU usage across all processors in the system. This provides an overview of the CPU utilization, including the time spent on user processes, system processes, I/O waiting, and idle time. This view is useful for determining whether the system is under a heavy CPU load or operating within normal parameters.

1.3.2 Per-Core CPU Usage

SAR also supports per-core CPU usage monitoring. Administrators can observe how workloads are distributed across CPU cores. Per-core statistics help identify uneven loads, bottlenecks, and abnormal CPU behaviors that affect the cores.

1.4 Memory Usage Monitoring

SAR can collect memory utilization statistics to display free and used memory as usage percentages. This information helps to determine system memory availability and potential performance impact. Monitoring memory usage helps identify resource pressure, memory leaks, and potential performance degradation.

1.5 Disk I/O Activity Monitoring

SAR provides visibility for disk input and output activities, including read/write operations and transfer rates. Disk I/O monitoring helps identify whether performance issues are caused by storage bottlenecks rather than CPU or memory limitations.

1.6 Network Performance Monitoring

Network statistics can be collected using SAR to display the traffic data for each network interface. This includes transmitted and received packets, data volume, and error counts. Monitoring network activity helps identify abnormal traffic patterns, such as unexpected spikes in outbound data, which may indicate data exfiltration or misconfigured services.

2.0 Conclusion

2.1 Key Takeaways

- SAR is a core Linux performance monitoring tool provided by `sysstat` utilities.
- On Ubuntu 24.04.3 LTS, `sysstat` must be installed and enabled to collect performance data.
- SAR supports the monitoring of the CPU, memory, disk I/O, and network activity using consistent command-line interfaces.
- This tool provides system-wide and resource-specific performance visibility.

2.2 Security Implications and Recommendations

- System performance monitoring contributes to the early detection of abnormal behavior and potential security incidents.
- Unexpected spikes in CPU, memory, disk, or network usage may indicate misconfiguration or malicious activity.
- SAR should be used in conjunction with logging and security monitoring tools to improve system visibility.
- Without a performance baseline, it is difficult to distinguish between normal system behavior and early signs of failure or compromise.