2025

Research And Explain The Purpose Of SAR Logs

MOSSÉ CYBERSECURITY INSTITUTE

AARON AMRAN BIN AMIRUDDIN

Student ID: nxCLnZGLgyOUMpnDw16rtDvYuTF2

Table of Contents

Importance of Generating and Retaining SAR Logs

Generating and retaining SAR (System Activity Reporter) logs is essential for maintaining, diagnosing, and optimizing a Linux system's performance. Here are some key reasons with explanations:

Historical Performance Data
SAR logs offer a detailed historical record of system activities. By retaining these logs, administrators can analyze performance trends over days, weeks, or months. This historical context is invaluable when troubleshooting issues that might not be immediately apparent or when correlating events with system slowdowns or outages.

Troubleshooting and Root Cause Analysis
When issues arise, having access to past performance metrics can help pinpoint the moment when performance degraded. By comparing historical data with the current state, administrators can identify patterns or anomalies—such as spikes in CPU or memory usage—that lead to the root cause of a problem. This makes diagnosing and resolving issues much more efficient.

Capacity Planning and Resource Optimization
SAR logs provide insight into how system resources (CPU, memory, disk I/O, network activity, etc.) are being utilized over time. This detailed monitoring enables administrators to determine whether existing hardware meets current demands or if additional resources are needed. Effective capacity planning helps in avoiding unexpected bottlenecks and ensures that the system scales appropriately as workloads increase.

Performance Benchmarking
With a consistent log of system activity, administrators can establish performance benchmarks under normal operating conditions. These benchmarks can be used to detect deviations or gradual performance declines, prompting timely interventions before issues escalate into critical failures.

Security and Compliance Auditing
Retaining SAR logs contributes to security monitoring by providing a record of system behavior. Sudden or unexplained changes in system activity might indicate security breaches or unauthorized access. Additionally, maintaining such logs can be important for compliance purposes, where audit trails are required to demonstrate that system performance and security are being actively managed.

Proactive Maintenance
Continuous monitoring with SAR logs enables a proactive approach to system management. Administrators can detect early signs of hardware failure or software misconfigurations—such as abnormal spikes in interrupts or context switches—and take preventive actions before these issues develop into larger problems.

8 Statistics that SAR Logs Can Log

CPU Utilization
SAR logs provide detailed information about CPU usage, including percentages of time spent in user mode, system mode, idle, and I/O wait. Monitoring these metrics helps identify whether the processor is overburdened, if there are inefficient processes consuming excessive CPU time, or if an application is causing spikes in I/O wait. This data is crucial for troubleshooting performance issues and for capacity planning to ensure that the CPU resources meet the workload demands.

Memory Utilization
Memory statistics such as total memory, used memory, free memory, and buffer/cache usage are captured by SAR. These metrics help administrators identify memory leaks, understand how much memory is actively used versus cached, and determine if the system is experiencing memory pressure. Effective monitoring of memory usage is essential to ensure smooth application performance and to prevent out-of-memory errors that can lead to system instability.

Disk I/O Statistics
SAR logs disk-related data including the number of read/write operations, data transfer rates, and average service times. This information is critical for detecting bottlenecks in disk performance. For example, a high number of read/write operations with increasing wait times may indicate that a disk is becoming a performance-limiting factor. Monitoring these metrics allows for proactive measures such as upgrading disk hardware or tuning application I/O patterns.

Network Activity
SAR captures network interface statistics such as packets transmitted/received, errors, collisions, and throughput rates. This data is important for monitoring the health of the network, detecting issues like packet loss or network congestion, and ensuring that bandwidth is sufficient for the system’s needs. It can also help in identifying potential security issues by flagging abnormal traffic patterns.

Paging and Swapping
Paging statistics provide insight into how often the system resorts to using disk space to compensate for inadequate physical memory (i.e., swapping). Frequent paging or swapping is a sign of memory pressure and can severely degrade system performance. By monitoring these metrics, administrators can decide whether it’s necessary to add more physical memory or optimize application memory usage to reduce reliance on swap space.

Context Switches
SAR logs the number of context switches, which occur when the CPU switches from one process or thread to another. A high rate of context switching can indicate that the system is handling many processes concurrently, potentially leading to inefficiencies if the overhead becomes too high. Monitoring this metric helps in understanding process behavior and can guide optimizations to reduce unnecessary multitasking overhead.

Interrupts
The logs include data on hardware interrupts, which are signals from devices indicating that they need attention from the CPU. Monitoring the frequency and nature of interrupts helps in diagnosing

hardware issues or abnormal conditions. An unusually high number of interrupts might point to misbehaving hardware or driver issues that could affect overall system stability and performance.

Load Average

Load average metrics, typically over 1, 5, and 15 minute intervals, reflect the average number of processes waiting for CPU time. This statistic provides a snapshot of the system's demand relative to its processing capacity. High load averages can indicate that the system is overloaded, prompting a review of resource allocation or workload distribution to ensure that system performance remains within acceptable limits.

References

LaCroix, J. '. (2022, August 10). *How to Use Sar (System Activity Reporter)*. Retrieved from linuxjournal.com: https://www.linuxjournal.com/content/how-use-sar-system-activity-reporter

SAR command in Linux to monitor system performance. (2025, March 19). Retrieved from geeksforgeeks.org: https://www.geeksforgeeks.org/sar-command-linux-monitor-system-performance/

Stocker, S. H. (2021, June 17). *Checking Linux system performance with sar*. Retrieved from networkworld.com: https://www.networkworld.com/article/969982/checking-linux-system-performance-with-sar.html