Log Management And security

1.What are some of the reasons you would need to look at the Windows System Log

The main reasons to be looking into Window System is for Security reasons. Logs can reveal unauthorized access attempts, security breaches, or suspicious activities by capturing failed login attempts, privilege escalations, or system changes. Here in my system I have seen This error - " Windows cannot load the extensible counter DLL "C:\Program Files (x86)\VMware\VMware Workstation\vmPerfmon.dll" (Win32 error code The specified module could not be found.)."
This means that the file was unable to be retrieved or open because it was uninstalled.
They can help track system performance over time and identify performance bottlenecks by recording system errors, warnings, and informational messages.

2. Briefly describe how you might manage the growth in the size of system log files
Why would you need to keep copies of log files

Ans Compression and log rotation can be implemented to manage the growth in the size of system log files. We can configure the log system to capture only the necessary errors and setting retention policies, the volume of logs generated can be managed effectively.
Logs can be moved to external storage devices or centralized log management systems.
We would need to keep copies of log files for the investigation and forensic analysis in case of cyber attack. It can also be useful to determine compliance and determine the security posture of a company in cause of an audit.

3. How long do you think system logs should be retained

Every organization would be having its own policy on log retention. For critical systems, logs may need to be retained for **6 months to 1 year** or longer to meet compliance requirements such as PCI DSS, HIPAA, or GDPR.
Non-essential logs can be kept for shorter periods, such as **30-90 days**. In general, logs should be retained long enough to ensure they are available for investigation or auditing purposes, but should also be regularly purged or archived to optimize system performance.