Key Metrics and Logs to Monitor in DevOps

**1. System Metrics**  
 - CPU Usage: Monitor the percentage of CPU being utilized by your applications and services. High CPU usage can indicate a need for optimization or scaling.  
 - Memory Usage: Keep track of how much memory your applications consume. Memory leaks or excessive usage can lead to system instability.  
 - Disk I/O: Monitor the rate of data being read from or written to disk. High disk I/O can be a bottleneck for application performance.  
 - Network I/O: Track the amount of data being sent and received over the network. Network congestion or high latency can impact application performance.  
  
 **2. Application Metrics**  
 - Response Time: Measure the time it takes for your application to respond to user requests. High response times can lead to poor user experience.  
 - Throughput: Monitor the number of requests your application handles over a period of time. This helps in understanding the load and scalability of your system.  
 - Error Rates: Track the frequency of errors occurring in your application. High error rates can indicate issues that need immediate attention.  
 - User Sessions: Monitor the number of active user sessions. This helps in understanding user behavior and system usage patterns.  
  
 **3. Custom Metrics**  
 - Business-Specific KPIs: Track key performance indicators that are specific to your business, such as conversion rates, revenue per user, or customer satisfaction scores.  
 - SLA Adherence: Monitor metrics that help you ensure adherence to Service Level Agreements (SLAs), such as uptime, availability, and response times.  
  
 **4. Log Types**  
 - Application Logs: Capture detailed logs from your application, including errors, warnings, and informational messages. These logs are crucial for diagnosing issues and debugging.  
 - System Logs: Monitor logs from the operating system, including boot messages, kernel logs, and system events. These logs help in identifying issues at the OS level.  
 - Access Logs: Track who accessed your systems and applications, including IP addresses, timestamps, and requested resources. Access logs are essential for security auditing.  
 - Security Logs: Monitor logs related to security events, such as failed login attempts, firewall actions, and security policy violations. These logs help in identifying and mitigating security threats.