| **Term** | **Definition** |
| --- | --- |
| Access logs | Record information about who accessed the application, when they accessed it, and what actions they performed. They can help with auditing and monitoring user activity |
| AIOps | Coined by Gartner, AIOps (artificial intelligence for IT operations) is the application of artificial intelligence (AI) capabilities, such as natural language processing and machine learning models, to automate and streamline operational workflows |
| Alert manager | A flexible metrics collection and alerting tool that can be combined with Prometheus |
| Alerting | Responsive component of a monitoring system that performs actions based on changes in metric values. It helps developers quickly spot issues and pinpoint areas for improvement in their applications |
| API | An application programming interface or API is a set of outlined rules that help various applications communicate with each other. APIs aid in simplifying the process of software development and innovation by allowing applications to exchange data and functionality in a simple and secure manner |
| Application log | Contains information about events that have occurred within a software application |
| Application metrics | Focus on units of processing or work that depend on resources like services or applications |
| Application monitoring | Process developers use to ensure their software performs as intended |
| Application monitoring tools | Application monitoring tools, or application performance monitoring (APM) tools, systematically collect and analyze data to provide real-time insights into the behavior of your application |
| Application Performance Monitoring (APM) | Aggregates and analyzes inbound network data to evaluate the state of the IT environment and identify the root cause of the problem when apps perform sub-optimally |
| Atatus | A distributed tracing tool that provides detailed insights into how requests flow through a distributed system. It offers real-time data visualization and analytics, enabling developers to resolve issues that could impact user experience quickly |
| Availability monitoring | Checks the uptime and downtime of your application by periodically sending requests to verify its responsiveness |
| AWS CloudWatch | A monitoring service provided by Amazon Web Services (AWS) that provides metrics on resources and applications running on AWS |
| Bosun | An open-source alerting tool that has regular features capable of displaying simple graphs and creating alerts using a powerful expression language for alert rules and conditions |
| Business Activity Monitoring (BAM) | These tools take key business performance metrics and track them over time |
| Cabot | It does not collect any data but uses another method to access data by hooking into the APIs of the alerting tools and a pull (rather than a push) model for the data it requires to make alerting decisions |
| Checkpoint | Computers that regularly attempt to interact with a web or network entity |
| CI/CD | CI/CD stands for continuous integration and continuous delivery. CI/CD establishes a quicker and more accurate way of combining the work of multiple people into a single cohesive product |
| Cloud native observability | The practice of monitoring and understanding the behavior of cloud-native applications running in dynamic and distributed environments. Organizations leverage cloud native observability tools to redress application performance issues with business context and take insight-driven actions |
| Cloud native observability tools | An effective cloud native observability tool focuses on comprehensive visibility and empowers technologists to ensure a seamless user experience |
| Cloud-native | The Cloud Native Computing Foundation (or CNCF) describes cloud-native computing as the process of creating and deploying scalable applications on cloud computing platforms using open source software as well as technologies like containers, microservices, and service mesh |
| CNCF | Cloud Native Computing Foundation |
| Container orchestrator | Automates the provisioning, deployment, networking, scaling, availability, and lifecycle management of containers |
| Container-based applications | Applications that run in isolated runtime environments called containers |
| Context propagation | How information about a trace is passed between different services and systems |
| Custom parsing | Implemented when users are required to enter values in a form that the current parse operations do not accept or if some other processing needs to be completed on values before submitting to the application server |
| Datadog | A comprehensive monitoring and analytics platform offering real-time metrics, logs, and traces for cloud-based applications |
| Debugging | A process that includes finding a problem, then its source, and then resolution or identifying a way to work around it |
| Debugging logs | Contain detailed information about variables, method calls, and other debugging data and is used by developers during the development process to trace program flow and identify bugs |
| Dependency monitoring | Allows watching your applications and identify any issues with their performance to give your users the best experience with your application |
| Destinations | Represent where you want your logs to be sent; for example, to console output or a file |
| Distributed logging | A technique used in computing systems to collect and store log data from multiple sources across different nodes or servers |
| Distributed tracing | A technique used to track and observe application requests as they move through distributed systems or microservice environments |
| DNS | Domain Name System or DNS is a distributed database system for managing host names and their associated Internet Protocol (IP) addresses |
| Dynatrace | An end-to-end observability platform that provides an entire observability toolkit from log management, infrastructure monitoring, and application performance monitoring (APM) |
| Error logs | Record error messages generated by the application or system. They contain information about exceptions, stack traces, and error codes that can help developers diagnose and fix problems |
| Error monitoring | Captures stack traces and provides detailed information about the root cause of errors, enabling efficient debugging |
| Error telemetry | Provides information about errors that occur within the application, including stack traces and error messages |
| Errors | An error could mean a failed request or when a request is completed but with the wrong information |
| Evaluations | Assess whether a solution meets the goals identified at the design stage or when the solution was implemented |
| Event logs | Record application events and user actions, such as login attempts and data modifications, and help troubleshoot issues and detect security breaches |
| Error logs | Record error messages generated by the application or system. They contain information about exceptions, stack traces, and error codes that can help developers diagnose and fix problems |
| Error monitoring | Captures stack traces and provides detailed information about the root cause of errors, enabling efficient debugging |
| Error telemetry | Provides information about errors that occur within the application, including stack traces and error messages |
| Errors | An error could mean a failed request or when a request is completed but with the wrong information |
| Evaluations | Assess whether a solution meets the goals identified at the design stage or when the solution was implemented |
| Event logs | Record application events and user actions, such as login attempts and data modifications, and help troubleshoot issues and detect security breaches |
| FluentD | A logging system designed to be decoupled from the backend system. It solves the incompatibility problem by unifying logging formats and routines through its unified logging layer |
| Golden Signals | The four most important metrics for measuring the health of your service or systems: Latency, traffic, errors, and saturation. They identify and resolve an issue, provide a focused view into the health of all services, and enable actionable monitoring. |
| Google Cloud Monitoring | A monitoring service by Google Cloud Platform, or GCP, that provides visibility into infrastructure and application performance across GCP services |
| Grafana | A professional cross-platform, open-source data visualization and metrics analysis tool that provides time-series analytics, which can help you study, analyze and monitor data metrics over time |
| Horizontally scaled infrastructure | Adding additional nodes or machines to your infrastructure to manage new demands |
| Host-based metrics | It comprises the usage or performance of the operating system or hardware |
| HTTP | Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems |
| HTTPS | HTTPS stands for Secure Hypertext Transfer Protocol and is HTTP with a security feature |
| Hybrid-cloud | Hybrid cloud integrates public cloud services, private cloud services, and on-premises infrastructure and provides orchestration, management, and application portability across all three |
| I&O teams | Infrastructure and operations or I&O teams are generally responsible for the administration and management of technology, information, and data |
| Ideal monitoring systems | Have an independent infrastructure, easy-to-use and reliable systems, maintained historical data, and effective correlation of data from different sources |
| Indicators | Anything involved in evaluating the health and performance of an individual machine, disregarding for the moment its application stacks and services |
| Ingestion | The process where log data is formatted and uploaded from external sources such as applications, hosts, and cloud-based logging services |
| Instana | An application performance monitoring (APM) tool that provides real-time visibility into the performance of cloud-native applications |
| Integration monitoring | Integration monitoring identifies the availability and uptime performance of third-party integrations |
| Jaeger | A project under CNCF that aims to address the challenges of developing distributed systems by providing tracing capabilities |
| JSON | JavaScript Object Notation or JSON is the de facto standard for structured logging, but consider using key-value pairs, XML, or another format for your application logs |
| Kibana | An open-source web application that's often used in conjunction with Elasticsearch, a powerful, highly scalable open-source search and analytics engine that allows storing, searching, and analyzing large volumes of data |
| Kubernetes | An open-source container orchestration platform that automates deployment, management, and scaling of containerized applications |
| Latency | Measures the time between when a request is sent and when a request is completed |
| Log alerts | Use log analytics queries to evaluate resource logs at predefined intervals to see how your applications or services are and have been performing |
| Log monitoring | Analyzes logs generated by your application, allowing you to gain insights into its behavior, detect patterns, trace specific events or transactions, and troubleshoot issues effectively |
| Log monitoring software | Perform essential event log monitoring tasks consistently and accurately |
| Log parsing | Converts log files into a readable format for your log management system, enabling data reading, indexing, and storage |
| Logging | A series of messages from an application that provide a recorded log of the application's activities |
| Logs | Records of events, typically in textual or human-readable form |
| Metric alerts | These are based on raw data collected by your monitoring system and provide information about the availability of resources on systems, applications, databases, and web servers |
| Metrics | A kind of real-time operating data accessed through an API using a pull or polling strategy or as an event or telemetry generated, such as a push or notification |
| Mezmo | Formerly known as LogDNA, Mezmo helps developers and IT teams monitor and analyze the performance of their applications and infrastructure |
| Mezmo CLI | The Mezmo Command Line Interface (CLI) client helps in tailing the servers with terminal commands |
| Microservices | Microservices are a way to manage complexity once applications have gotten too large and unwieldy to be updated and maintained easily |
| Monitoring | Allows developers to collect data, measure, and visualize any issues or unexpected events that may occur while an application is running |
| New Relic | A full-stack, all-in-one, cloud-based observability platform that provides insights into application performance, infrastructure health, and user experience |
| Observability | A term used in engineering and computer science to describe the ability to understand the internal state of a system using its external outputs |
| Observable system | Provides sufficient information about its internal workings to allow operators and developers to diagnose issues and understand how it behaves under different circumstances |
| Operational insight | Gives DevOps staff a deeper understanding of IT infrastructure and business systems |
| Parent/Child relationship | One span calls another span as part of its operation, the calling span becomes the parent, and the called span becomes the child |
| Performance logs | Track the application's performance metrics, such as response times, CPU usage, memory consumption, and network traffic. They help identify bottlenecks and optimize performance |
| Performance monitoring | Involves tracking metrics like response time, throughput, error rates, and resource utilization to ensure optimal performance |
| Performance telemetry | Provides information about how the application is performing in terms of response time, throughput, and resource utilization |
| Prometheus | An open-source monitoring and alerting solution built by a company called SoundCloud to monitor servers, virtual machines (or VMs), and databases |
| PromQL | Prometheus provides a functional query language called PromQL (Prometheus Query Language), allowing users to select and aggregate time series data in real-time |
| Random sampling | Selects log records based on specific events, such as errors or warnings |
| Real-user monitoring (RUM) | A passive monitoring technique relying on real users to collect performance data on user paths or transactions |
| RED | Response, Error, and Duration |
| SaaS | SaaS, or software-as-a-service, is application software hosted on the cloud and used over an internet connection via a web browser, mobile app, or thin client |
| Sampling | Logging is collecting only a subset of log events for analysis or storage |
| Sampling strategies | Refer to the techniques for selecting a subset of log records for analysis and storage |
| Saturation | Measures the percentage of use of a system, like how much memory or CPU resources your system utilizes |
| Scripting | The ability to specify the precise actions of a test with synthetic monitoring enables you to walk through important application flows, such as a checkout flow or a sign-up flow, to evaluate the functionality and performance of the system |
| Security monitoring | Tracks anomalies and ensures that potential threats are stopped妯re they are a problem |
| Security telemetry | Provides information about security events, such as failed login attempts or unauthorized access attempts |
| Server pool | A collection of two or more servers that are put up to offer end users a uniform set of services and applications |
| Size-based sampling | Selects log records based on their size, such as selecting only records that exceed a certain threshold |
| SLAs | Service Level Agreements document the commitments that you plan to fulfill for customers |
| Smart Alerts | Smart Alerts provide automatically generated alerting configurations to receive alerts based on out-of-the-box blueprints such as website slowness, JavaScript errors, and HTTP status codes |
| Software-based agent | A computer program that carries out a wide range of tasks on a continuous and self-directed basis on behalf of a person or organization |
| Spans | Represent a particular step in the request's journey and is encoded with crucial data, such as tags, queries, intricate stack traces, logs, and context-giving events |
| Spike protection features | Help to set dynamic thresholds and alerts when data volume limits are being hit |
| Splunk | A software platform that is a proprietary solution used to monitor, search, analyze, and visualize big data |
| SRE | Site reliability engineering (SRE) uses software engineering to automate IT operations tasks - e.g., production system management, change management, incident response, and even emergency response - that would otherwise be performed manually by systems administrators (sysadmins) |
| SRE golden signals | Latency, traffic, errors, and saturation or utilization of the system |
| StatsAgg | It is an alerting and metrics aggregation platform that can act as a proxy for other systems |
| Synthetic monitoring | Tracks anomalies and ensures that potential threats are stopped before they are a problem |
| Synthetic monitoring tools | Solutions offered to verify the performance, availability, reachability, and reliability of a website or application at any time |
| Synthetic traffic | Lightweight, non-intrusive, and secure traffic that emulates user behavior on the network |
| Syslog monitoring software | A tool designed to compare real-time metrics with historical metrics to offer a comprehensive understanding of a network's performance over time |
| System monitoring | System monitoring is designed to provide developers with information about the availability of their software. It provides information about system uptime and the performance of applications |
| Telemetry | System data that is automatically gathered and recorded for monitoring |
| Thanos | Enables unlimited storage capacity for Prometheus deployments, allowing organizations that are utilizing multiple Prometheus servers and clusters access to global metrics views |
| Three Pillars of Observability | Logs, metrics, and traces |
| Time-based sampling | Selects log records at fixed time intervals, such as every minute or every hour |
| Trace | A collection of spans representing a single logical request or workflow. Traces are records of the information pathways or workflows created to follow a work item, like a transaction, through the steps that application logic instructs it to take |
| Trace ID | Unique identifier for an entire trace |
| Tracing | For container-based applications, it involves capturing and analyzing the flow of requests between different application components |
| Traffic | In application monitoring, traffic referes to how in demand your service is |
| TSDB | A time series database or TSDB is a software system optimized for storing and serving time series about related time-value pairs |
| Usage telemetry | Provides information about how users are interacting with the application, such as which features are being used most frequently and which ones are ignored꼠User experience monitoring |
| Visual elements | Charts, graphs, timelines, and other illustrations |
| Visualization | Graphical representation of information of data collected from the business infrastructure that helps you understand and maintain your application's performance |
| Web performance monitoring | Designed to monitor the availability of a web server or service |
| Web transaction | An interaction between a client, commonly a web browser, and one or more databases as the backend of multi-tier engineering |
| Weighted sampling | Assigns weights to log records based on their importance or relevance and then samples accordingly |
| Zipkin | A distributed tracing tool that gathers information on how microservices interact in distributed systems. Instead of logging every single event or piece of data, a subset is selected randomly or by some other criteria for recording |