# Understanding Signals in Azure Monitor

Azure Monitor provides various types of signals to help you monitor and maintain your applications, services, and infrastructure. This document explains three key types of signals: Log Search, Metrics, and Activity Logs, and their roles in a monitoring strategy.

## 1. Log Search Signals

Log Search Signals allow the use of Kusto Query Language (KQL) to search and analyze log data in Azure Monitor Logs. They are valuable for:

- \*\*Detailed Analysis\*\*: Enables searching for specific patterns, issues, or trends within log data, such as failed requests, exceptions, or slow performance.

- \*\*Custom Monitoring\*\*: Allows creating custom alerts based on any condition defined in KQL queries, such as response times exceeding a threshold or error counts surpassing a specific value.

- \*\*Incident Investigation\*\*: Useful for investigating and understanding the root causes of issues by analyzing historical and detailed event data.

## 2. Metrics Signals

Metrics Signals involve monitoring real-time metrics collected from Azure services and resources. These signals are crucial for:

- \*\*Performance Monitoring\*\*: Tracking metrics such as CPU usage, memory usage, and network traffic helps in monitoring the performance and resource usage of your infrastructure.

- \*\*Real-Time Alerts\*\*: Providing near real-time alerts when metrics exceed defined thresholds, allowing for quick response to potential issues.

- \*\*Resource Optimization\*\*: Assists in managing and optimizing resource usage, ensuring efficient resource allocation and avoiding wastage.

## 3. Activity Log Signals

Activity Log Signals track and record administrative actions and configuration changes across Azure resources. They are important for:

- \*\*Security and Compliance\*\*: Monitoring changes within the Azure environment, including resource creation, modification, or deletion, is crucial for security and regulatory compliance.

- \*\*Administrative Monitoring\*\*: Helps detect unusual or unauthorized administrative activities, such as role changes, permission grants, or system configuration adjustments.

- \*\*Incident Analysis\*\*: Provides a detailed history of activities, facilitating incident investigation and understanding configuration changes.

## Conclusion

By leveraging these signals—Log Search, Metrics, and Activity Logs—Azure Monitor enables comprehensive monitoring of your systems. Combining these signals allows for timely alerts and detailed insights, helping you maintain availability, security, and performance.