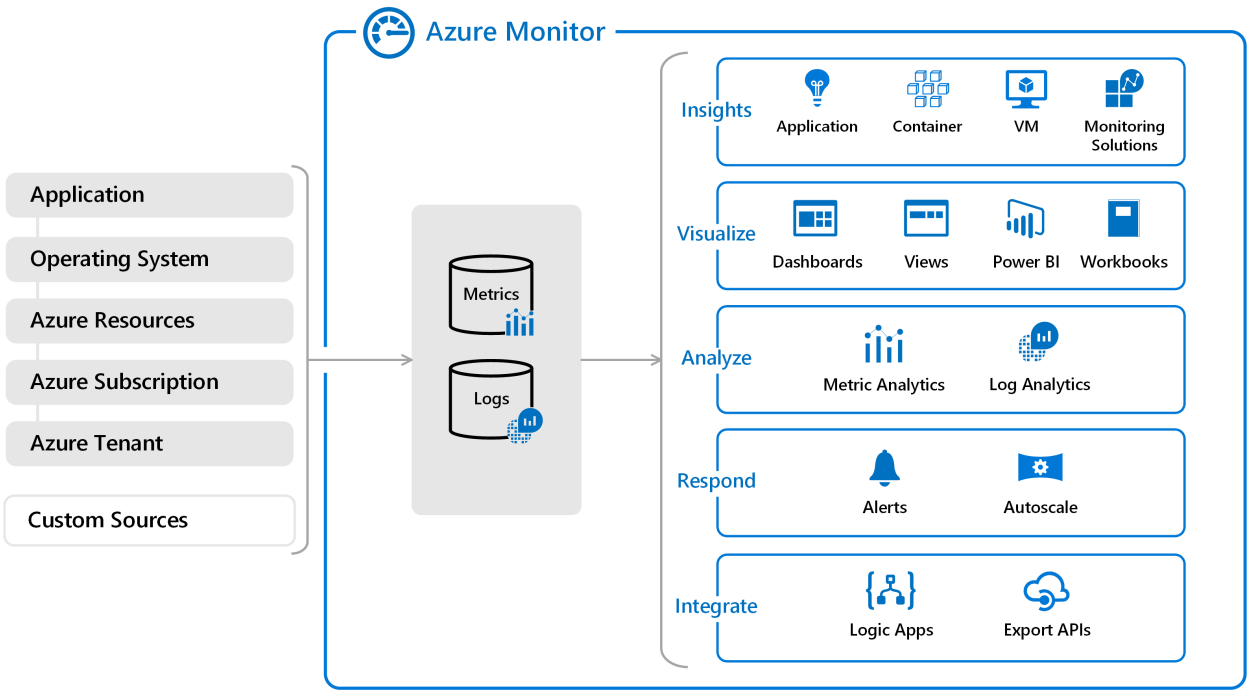
Azure Monitor data platform

03/26/2019 • 6 minutes to read •

In this article

Enabling observability across today's complex computing environments running distributed applications that rely on both cloud and on-premises services, requires collection of operational data from every layer and every component of the distributed system. You need to be able to perform deep insights on this data and consolidate it into a single pane of glass with different perspectives to support the multitude of stakeholders in your organization.

Azure Monitor collects and aggregates data from a variety of sources into a common data platform where it can be used for analysis, visualization, and alerting. It provides a consistent experience on top of data from multiple sources, which gives you deep insights across all your monitored resources and even with data from other services that store their data in Azure Monitor.



Observability data in Azure Monitor

Metrics, logs, and distributed traces are commonly referred to as the three pillars of observability. These are the different kinds of data that a monitoring tool must collect and analyze to provide sufficient observability of a monitored system. Observability can be achieved by correlating data from multiple pillars and aggregating data across the entire set of resources being monitored. Because Azure Monitor stores data from multiple sources together, the data can be correlated and analyzed using a common set of tools. It also correlates data across multiple Azure subscriptions and tenants, in addition to hosting data for other services.

Azure resources generate a significant amount of monitoring data. Azure Monitor consolidates this data along with monitoring data from other sources into either a Metrics or Logs platform. Each is optimized for particular monitoring scenarios, and each supports different features in Azure Monitor. Features such as data analysis, visualizations, or alerting require you to understand the differences so that you can implement your required scenario in the most efficient and cost effective manner. Insights in Azure Monitor such as Application Insights or Azure Monitor for VMs have analysis tools that allow you to focus on the particular monitoring scenario without having to understand the differences between the two types of data.

Metrics

Metrics are numerical values that describe some aspect of a system at a particular point in time. They are collected at regular intervals and are identified with a timestamp, a name, a value, and one or more defining labels. Metrics can be aggregated using a variety of algorithms, compared to other metrics, and analyzed for trends over time.

Metrics in Azure Monitor are stored in a time-series database which is optimized for analyzing time-stamped data. This makes metrics particularly suited for alerting and fast detection of issues. They can tell you how your system is performing but typically need to be combined with logs to identify the root cause of issues.

Metrics are available for interactive analysis in the Azure portal with Azure Metrics Explorer. They can be added to an Azure dashboard for visualization in combination with other data and used for near-real time alerting.

Read more about Azure Monitor Metrics including their sources of data in Metrics in Azure Monitor.

Logs

Logs are events that occurred within the system. They can contain different kinds of data and may be structured or free form text with a timestamp. They may be created

sporadically as events in the environment generate log entries, and a system under heavy load will typically generate more log volume.

Logs in Azure Monitor are stored in a Log Analytics workspace that's based on Azure Data Explorer which provides a powerful analysis engine and rich query language. Logs typically provide enough information to provide complete context of the issue being identified and are valuable for identifying root case of issues.

> **Note**
>
> It's important to distinguish between Azure Monitor Logs and sources of log data in Azure. For example, subscription level events in Azure are written to an **activity log** that you can view from the Azure Monitor menu. Most resources will write operational information to a **resource log** that you can forward to different locations. Azure Monitor Logs is a log data platform that collects activity logs and resource logs along with other monitoring data to provide deep analysis across your entire set of resources.

You can work with log queries interactively with Log Analytics in the Azure portal or add the results to an Azure dashboard for visualization in combination with other data. You can also create log alerts which will trigger an alert based on the results of a schedule query.

Read more about Azure Monitor Logs including their sources of data in Logs in Azure Monitor.

Distributed traces

Traces are series of related events that follow a user request through a distributed system. They can be used to determine behavior of application code and the performance of different transactions. While logs will often be created by individual components of a distributed system, a trace measures the operation and performance of your application across the entire set of components.

Distributed tracing in Azure Monitor is enabled with the Application Insights SDK, and trace data is stored with other application log data collected by Application Insights. This makes it available to the same analysis tools as other log data including log queries, dashboards, and alerts.

Read more about distributed tracing at What is Distributed Tracing?.

Compare Azure Monitor Metrics and Logs

The following table compares Metrics and Logs in Azure Monitor.

Attribute	Metrics	Logs
Benefits	Lightweight and capable of near-real time scenarios such as alerting. Ideal for fast detection of issues.	Analyzed with rich query language. Ideal for deep analysis and identifying root cause.
Data	Numerical values only	Text or numeric data
Structure	Standard set of properties including sample time, resource being monitored, a numeric value. Some metrics include multiple dimensions for further definition.	Unique set of properties depending on the log type.
Collection	Collected at regular intervals.	May be collected sporadically as events trigger a record to be created.
View in Azure portal	Metrics Explorer	Log Analytics
Data sources include	Platform metrics collected from Azure resources. Applications monitored by Application Insights. Custom defined by application or API.	Application and resource logs. Monitoring solutions. Agents and VM extensions. Application requests and exceptions. Azure Security Center. Data Collector API.

Collect monitoring data

Different sources of data for Azure Monitor will write to either a Log Analytics workspace (Logs) or the Azure Monitor metrics database (Metrics) or both. Some sources will write directly to these data stores, while others may write to another location such as Azure storage and require some configuration to populate logs or metrics.

See Metrics in Azure Monitor and Logs in Azure Monitor for a listing of different data sources that populate each type.

Stream data to external systems

In addition to using the tools in Azure to analyze monitoring data, you may have a requirement to forward it to an external tool such as a security information and event management (SIEM) product. This forwarding is typically done directly from monitored resources through Azure Event Hubs. Some sources can be configured to send data directly to an event hub while you can use another process such as a Logic App to retrieve the required data. See Stream Azure monitoring data to an event hub for consumption by an external tool for details.

Next steps

- Read more about Metrics in Azure Monitor.
- Read more about Logs in Azure Monitor.
- Learn about the monitoring data available for different resources in Azure.