Azure Monitor

What is Azure Monitor?

- ✓ Azure Monitor is a full stack monitoring service in Azure that provides a complete set of features to monitor your Azure resources in addition to resources in other clouds and on-premises.

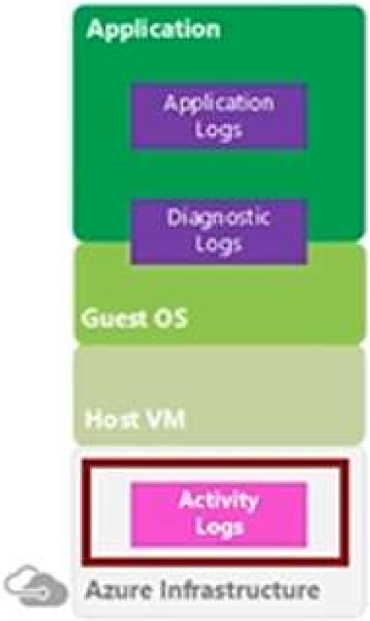
- ✓ As soon as you create an Azure resource, Azure Monitor is enabled and starts collecting metrics and activity logs which you can view and analyze in the Azure portal.

- ✓ With some configuration, you can gather additional monitoring data and enable additional features.

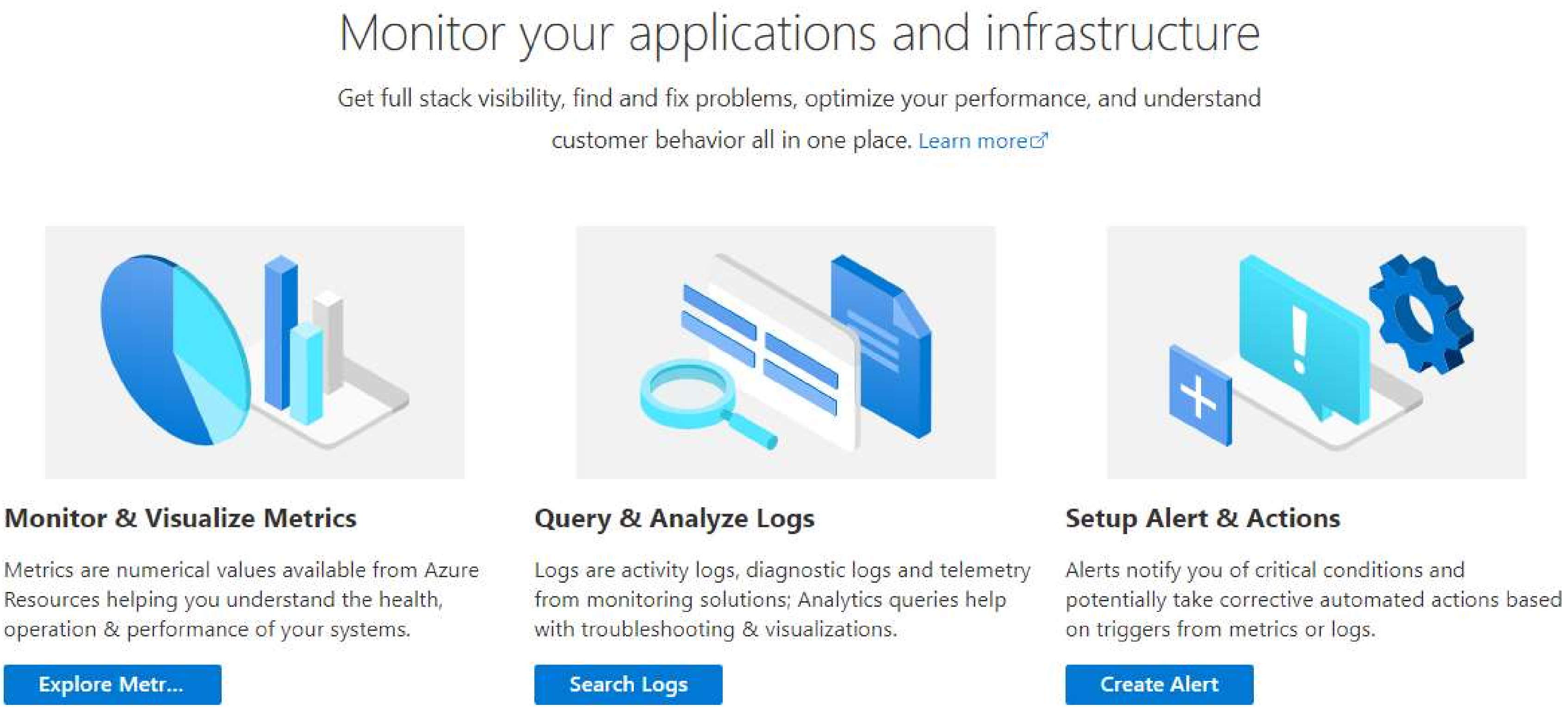
•Platform metrics - Numerical values that are automatically collected
•at regular intervals and describe some aspect of a resource at a particular time.

•Resource logs - Provide insight into operations that were performed within an Azure resource (the data plane), for example getting a secret from a Key Vault or making a request to a database. The content and structure of resource logs varies by the Azure service and resource type.

•Activity log - Provides insight into the operations on each Azure resource in the subscription from the outside (the management plane), for example creating a new resource or starting a virtual machine.



Compute resources only



Monitor your applications and infrastructure

Get full stack visibility, find and fix problems, optimize your performance, and understand customer behavior all in one place. Learn more

Monitor & Visualize Metrics

Metrics are numerical values available from Azure Resources helping you understand the health, operation & performance of your systems.

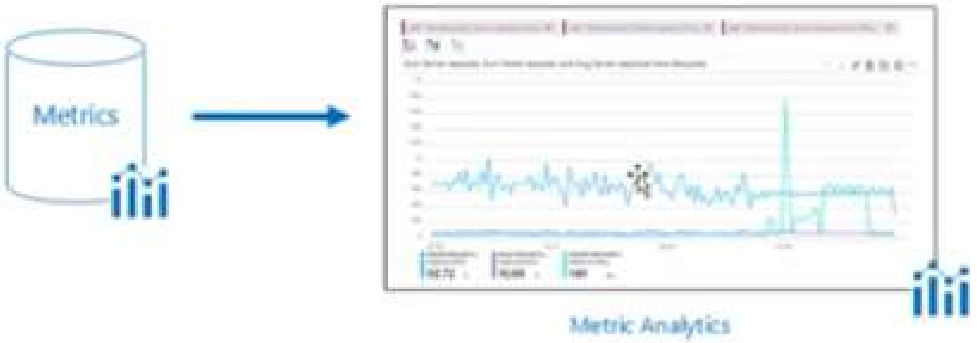
Query & Analyze Logs

Logs are activity logs, diagnostic logs and telemetry from monitoring solutions; Analytics queries help with troubleshooting & visualizations.

Setup Alert & Actions

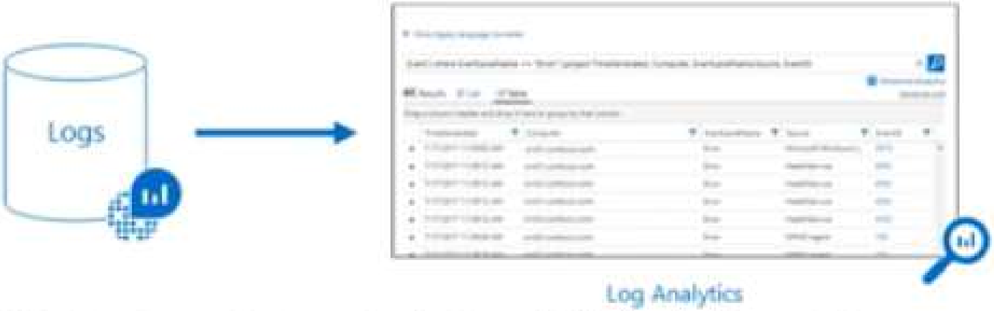
Alerts notify you of critical conditions and potentially take corrective automated actions based on triggers from metrics or logs.

Monitoring Data Platform



- **Metrics** are numerical values that describe some aspect of a system at a point in time. They are lightweight and capable of supporting near real-time scenarios.
- **Logs** contain different kinds of data organized into records with different sets of properties for each type. Telemetry such as events and traces are stored as logs in addition to performance data so that it can all be combined for analysis.

Log Data



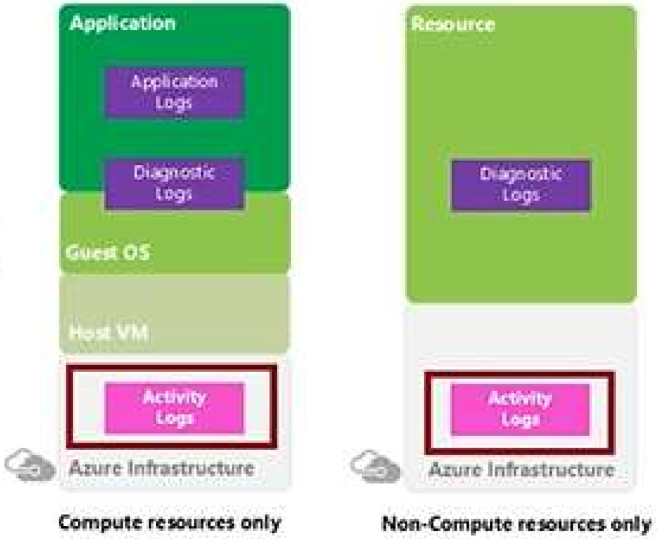
- Log data is stored in Log Analytics which includes a rich query language to quickly retrieve, consolidate, and analyze collected data
- The Data Explorer query language that is suitable for simple log queries but also includes advanced functionality such as aggregations, joins, and smart analytics

Data Types

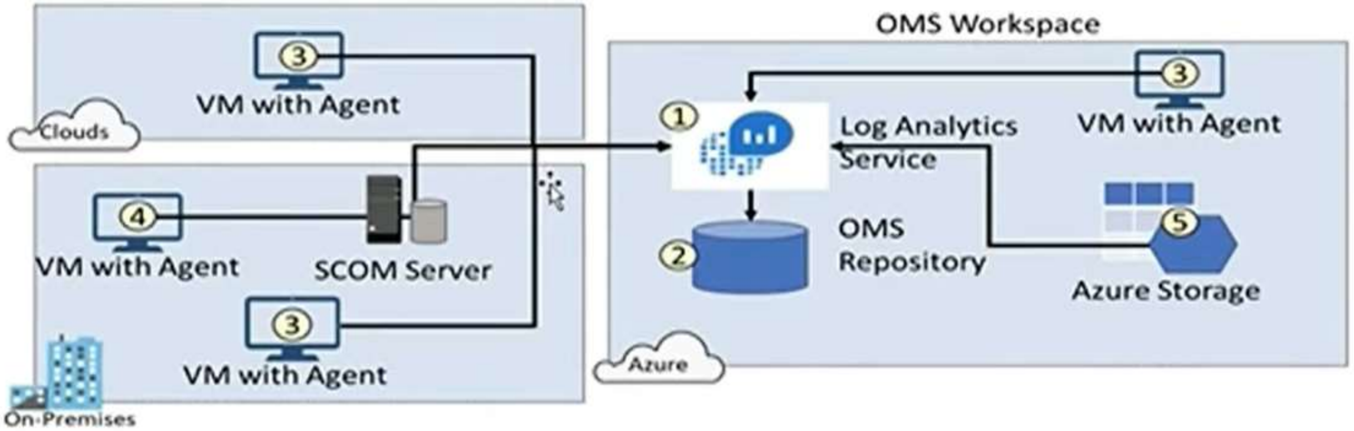
- **Application monitoring data** - Performance and functionality of the code you have written, regardless of its platform
- **Guest OS monitoring** - Azure, another cloud, or on-premises
- **Azure resource monitoring**
- **Azure subscription monitoring** - Operation and management of an Azure subscription, as well as data about the health and operation of Azure itself
- **Azure tenant monitoring** – Operation of tenant-level Azure services, such as Azure Active Directory

Activity Log

- Send data to Log Analytics for advanced search and alerts
- Query or manage events in the Portal, PowerShell, CLI, and REST API
- Stream information to Event Hub
- Archive data to a storage account
- Analyze data with Power BI



Connected Sources



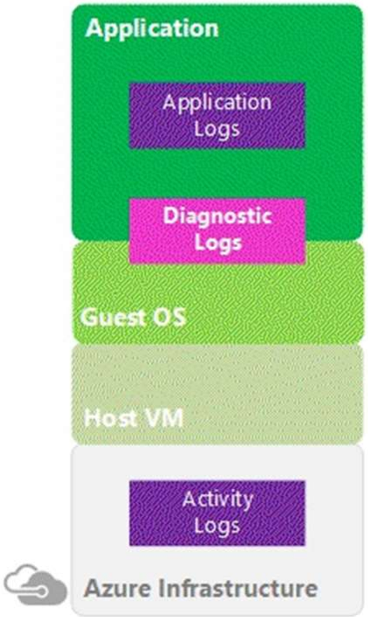
- Connected Sources generate data
- Data can be collected from Windows, Linux, SCOM and Azure Storage

- ✓ Azure Log Analytics Workspace is a cloud-based service provided by Microsoft Azure that enables you to collect, store, and analyze log and performance data from various sources across your infrastructure and applications.

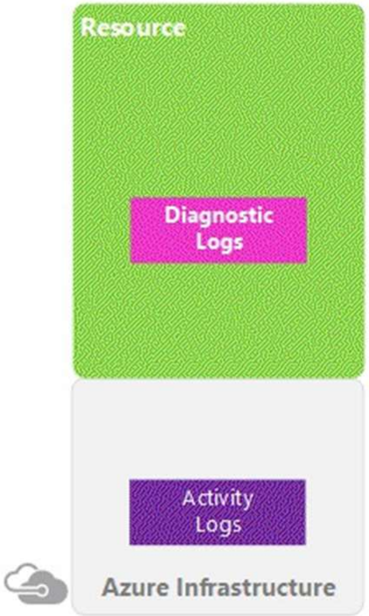
- ✓ It's a part of Azure Monitor, which is Microsoft's comprehensive monitoring solution for Azure resources and applications.

- ✓ Log Analytics can ingest data from various sources, such as virtual machines, containers, applications, and other cloud services.

- ✓ All collected data is stored centrally within the Log Analytics Workspace, providing a unified repository for querying and analyzing logs.



Compute resources only



Non-Compute resources only

Azure Diagnostics Extension can be used only with Azure virtual machines. The Log Analytics agent can be used with virtual machines in Azure, other clouds, and on-premises.