IntelliPaat

Designing and Implementing an Azure Data Solution

DP 203

Monitoring & Security

Agenda

01 What is Azure Monitor?

02 What data does Azure Monitor collect?

03 What can we monitor?

04 Alerts in Azure

05 Azure Security Logging & Auditing

What is Azure Monitor?

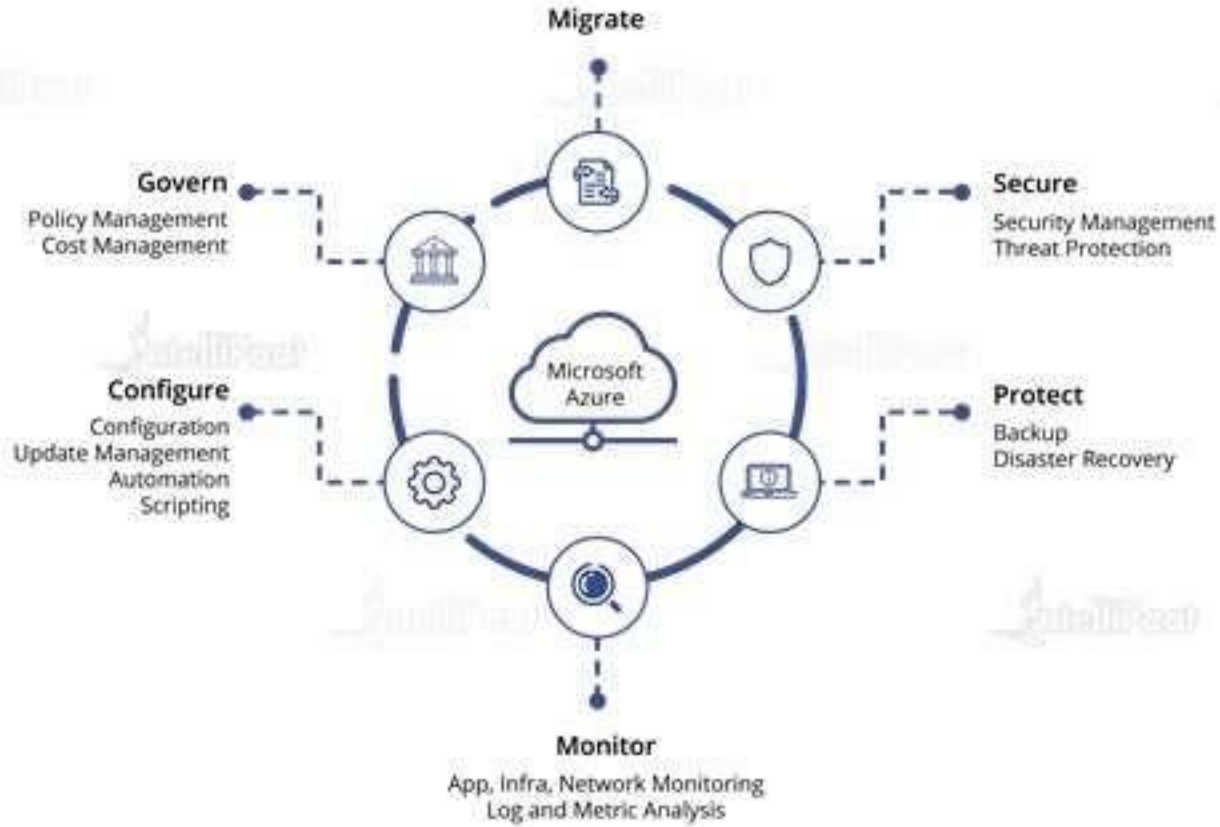
Azure Monitor

Monitoring in Azure is one of the aspects of Azure Management

Management refers to the tasks and processes required to maintain our business applications and resources that support them

Azure Monitor

The below image illustrates the different areas of management that are required to maintain any application or resource



Azure Monitor

It maximizes the availability and performance of our applications and services by delivering a comprehensive solution for collecting, analyzing, and acting on telemetry from our cloud and on-premises environments

It helps us understand how our applications are performing and proactively identifies the issues affecting the applications and the resources they depend on

Azure Monitor

Examples where we can use Azure Monitor

To create visualizations with Azure **dashboards** and **workbooks**

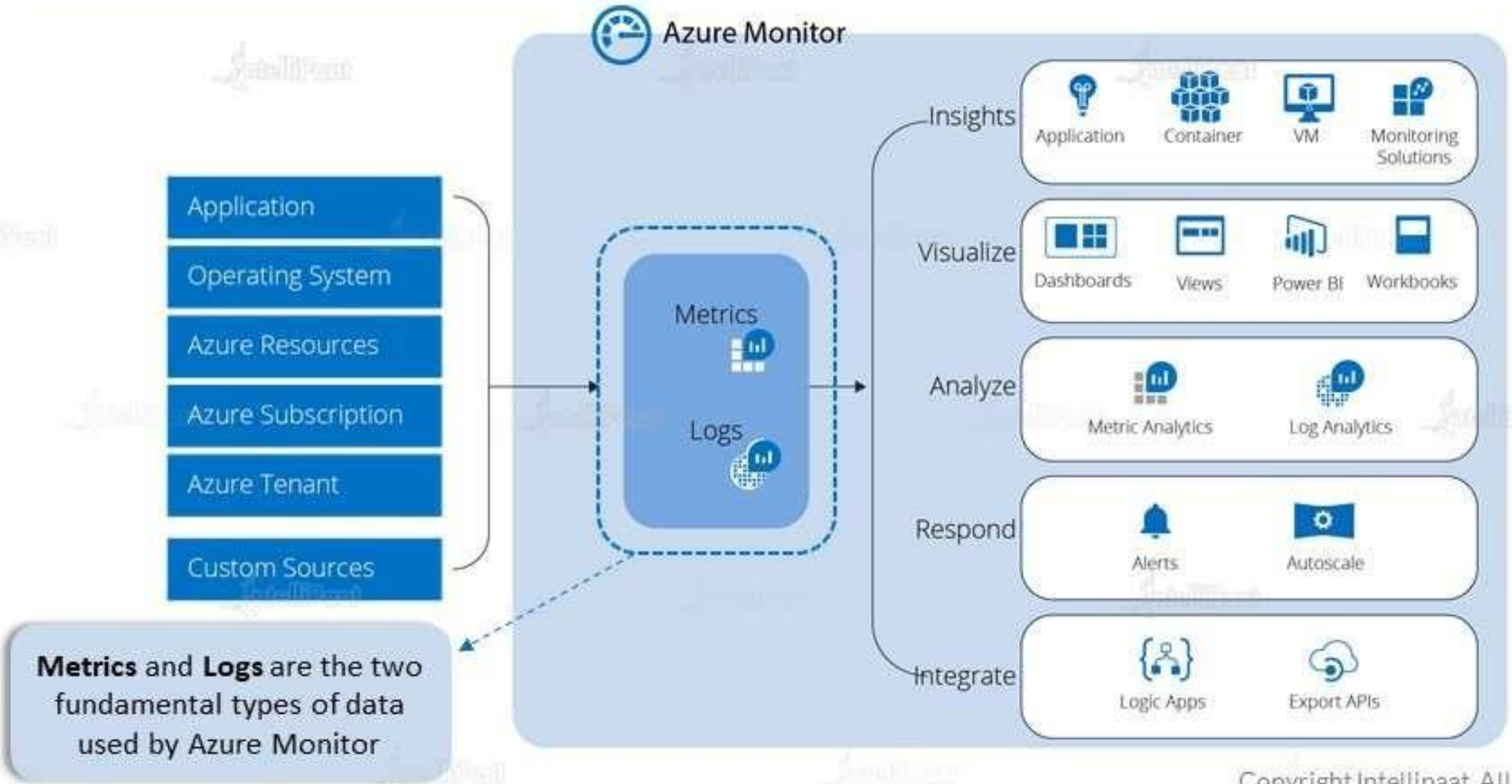
To support operations at scale with **smart alerts** and **automated actions**

To drill down into our monitoring data with **Log Analytics** for troubleshooting and deep diagnostics

To detect issues across applications and their dependencies with **Application Insights**

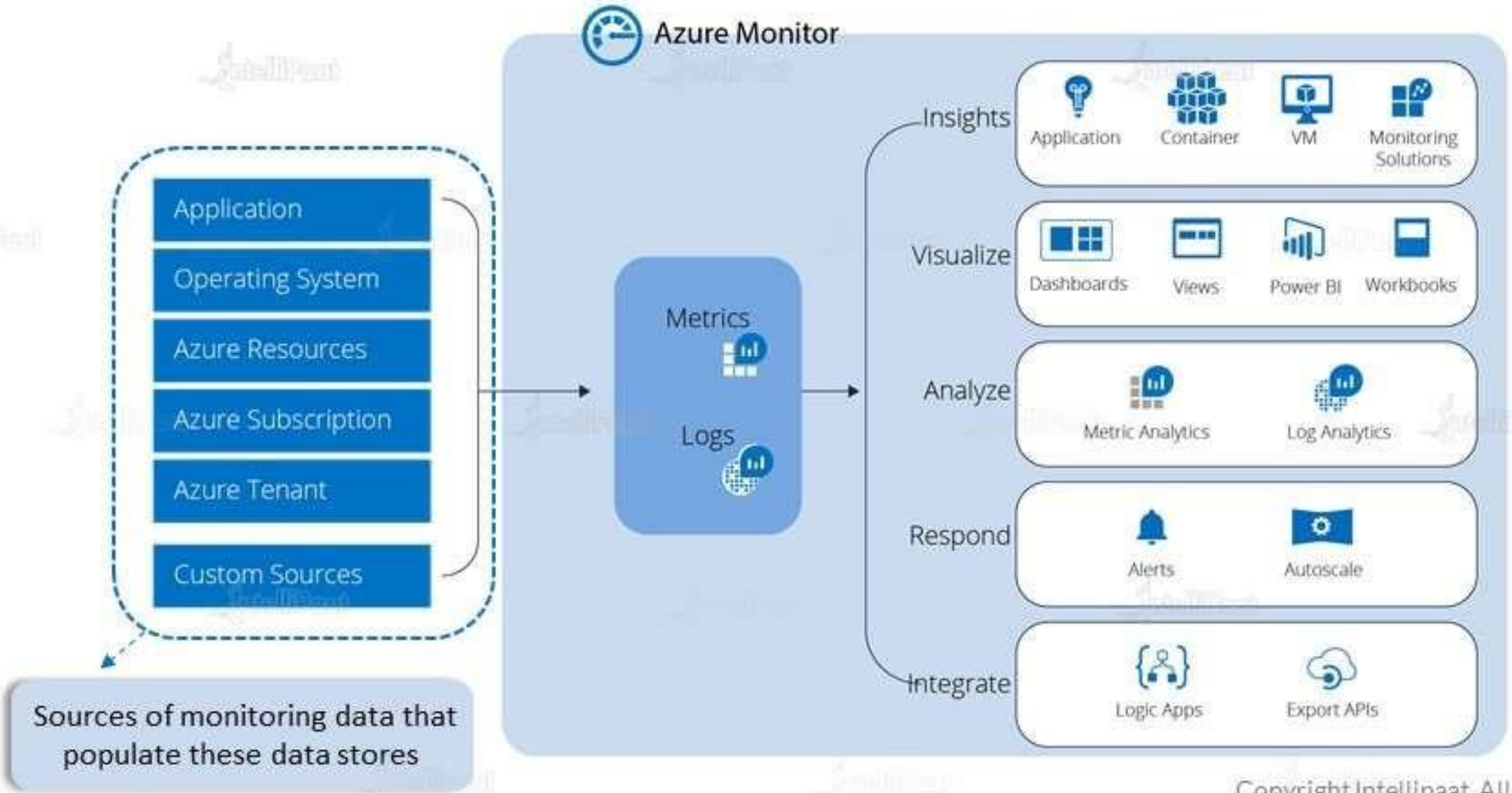
To correlate infrastructure issues with **Azure Monitor for VMs** and **Azure Monitor for Containers**

Azure Monitor

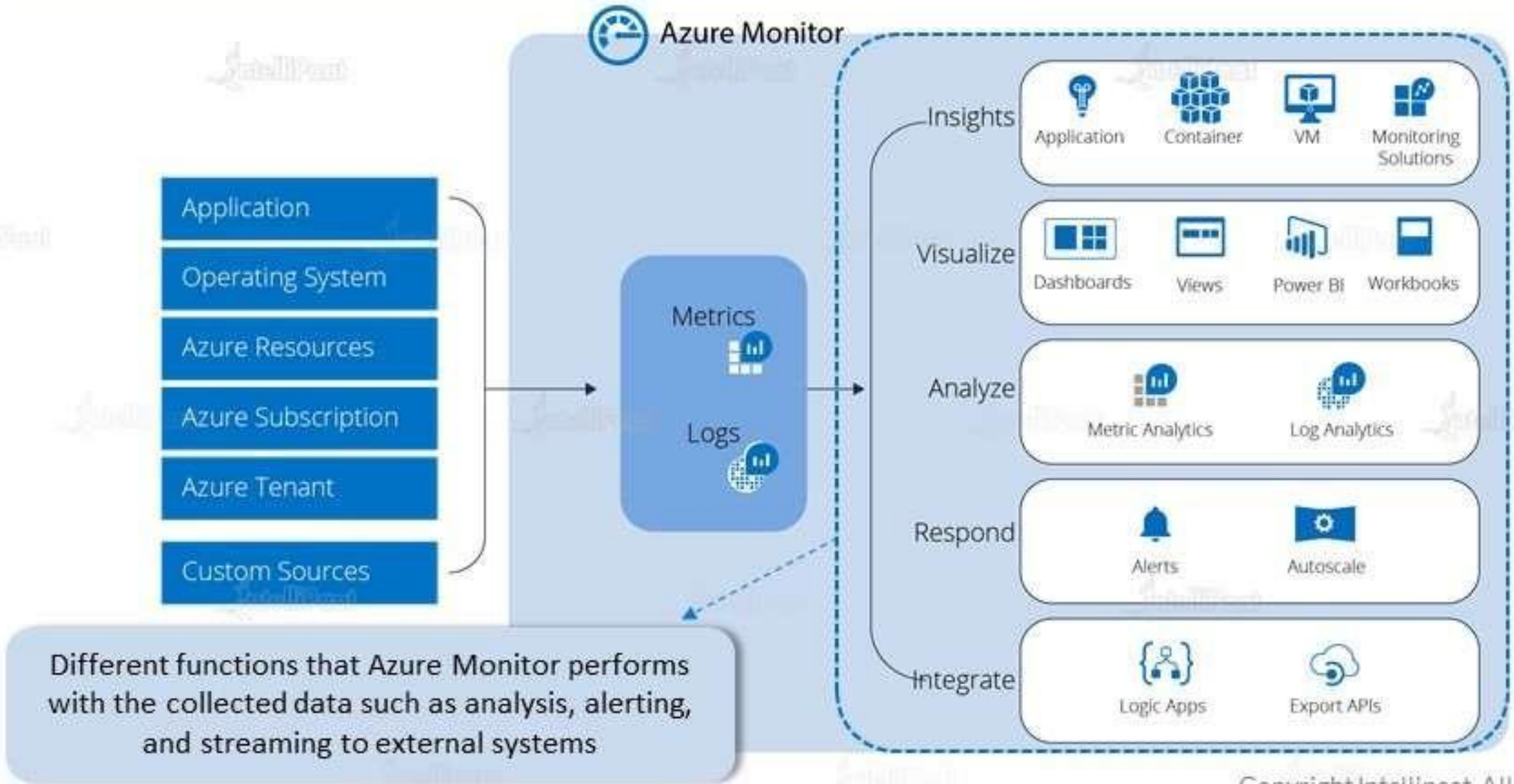


Metrics and **Logs** are the two fundamental types of data used by Azure Monitor

Azure Monitor



Azure Monitor



Different functions that Azure Monitor performs with the collected data such as analysis, alerting, and streaming to external systems

Metrics

Metrics are numerical values that describe some aspect of a system at a particular point in time

Metrics in Azure Monitor are stored in a time series database, optimized for analyzing time-stamped data

They are collected at regular intervals and are identified with a timestamp, a name, a value, and one or more defining labels

Logs

Logs in Azure Monitor are events that occurs within the system

Logs are stored in a Log Analytics workspace, which is based on Azure Data Explorer that provides a powerful analysis engine and rich query language

They can contain different kinds of data and may be structured or free form text with a timestamp.

Metrics vs Logs

Metrics

Lightweight and capable of near-real time scenarios such as alerting and ideal for fast detection of issues

Benefits

01

Logs

Analyzed with rich query language and ideal for deep analysis and identifying the root cause

02

Metrics

Numerical values only

Data

Logs

Text or numeric data

Metrics vs Logs

Metrics

Standard set of properties including sample time, resource being monitored, and a numeric value; some Metrics include multiple dimensions for further definition

Structure

03

Logs

Unique set of properties depending on the log type

Collected at regular intervals

Metrics

04

Collection

May be collected sporadically as events trigger a record to be created

Logs

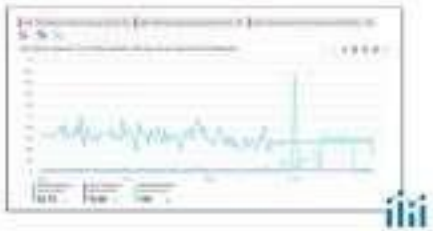
Metrics vs Logs

View in Azure Portal

05

Metrics

Metrics Explorer



Logs

Log Analytics

Platform metrics collected from Azure resources; applications are monitored by Application Insights; and Custom defined by application or API

Metrics

06

Data Sources

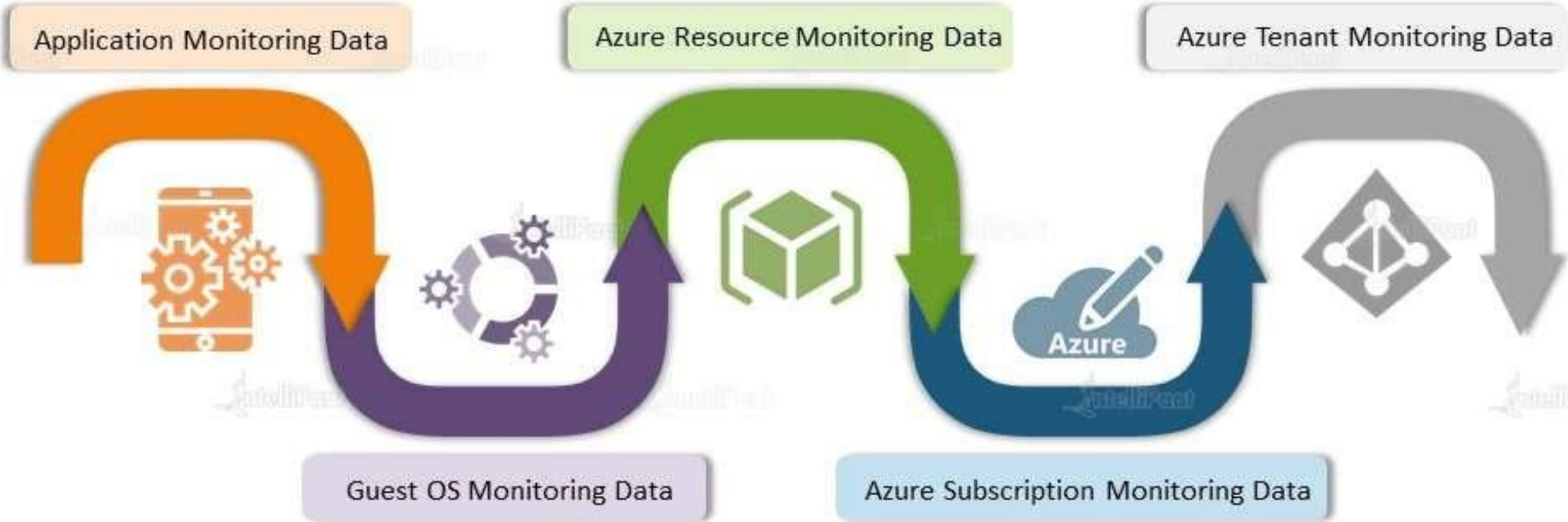
Application and resource logs, Monitoring solutions, Agents and VM extensions, application requests and exceptions, Azure Security Center, and Data Collector API

Logs

What data does Azure Monitor collect?

What data does Azure Monitor collect?

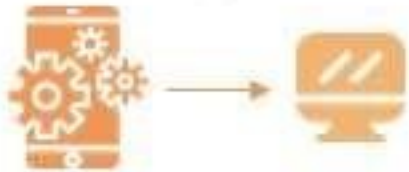
Azure Monitor collects data from each of the following tiers:



What data does Azure Monitor collect?

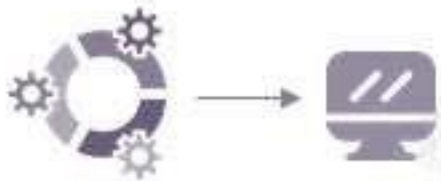
Data about the performance and functionality of the code we have written, regardless of its platform

Application Monitoring Data



Data about the OS on which our application is running. This could be running in Azure, another cloud, or on-premises

Guest OS Monitoring Data



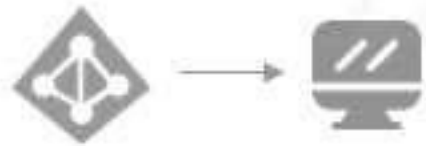
Data about the operation of an Azure resource

Azure Resource Monitoring Data

What data does Azure Monitor collect?

Data about the operation of the tenant-level Azure services, such as Azure Active Directory

Azure Tenant Monitoring Data



Data about the operation and management of an Azure subscription, as well as data about the health and operation of Azure itself

Azure Subscription Monitoring Data

What can we monitor?

Insights and Core Solutions

Insights provide a customized monitoring experience for particular applications and services. They collect and analyze both logs and metrics

Azure Monitor for VMs

Application Insights

Azure Monitor for Storage

Azure Monitor for Containers

Azure Monitor for Resource Groups

Azure Monitor for Cosmos DB

Azure Monitor for Networks

Insights and Core Solutions

Monitors the performance of container workloads deployed to either Azure Container Instances or managed Kubernetes clusters hosted on **Azure Kubernetes Service (AKS)**

Provides a comprehensive view of the health and metrics for all our network resources

An extensible **Application Performance Management (APM)** service to monitor our live web application on any platform

Provides a view of the overall performance, failures, capacity, and operational health of all our Azure Cosmos DB resources in a unified interactive experience

Insights and Core Solutions

Provides a comprehensive monitoring of our Azure Storage accounts by delivering a unified view of our Azure Storage services' performance, capacity, and availability

5

AM for Resource Groups

Triages and diagnoses any problem that our individual resources encounter, while offering the context as to the health and performance of the resource group as a whole

AM for Storage

6

7

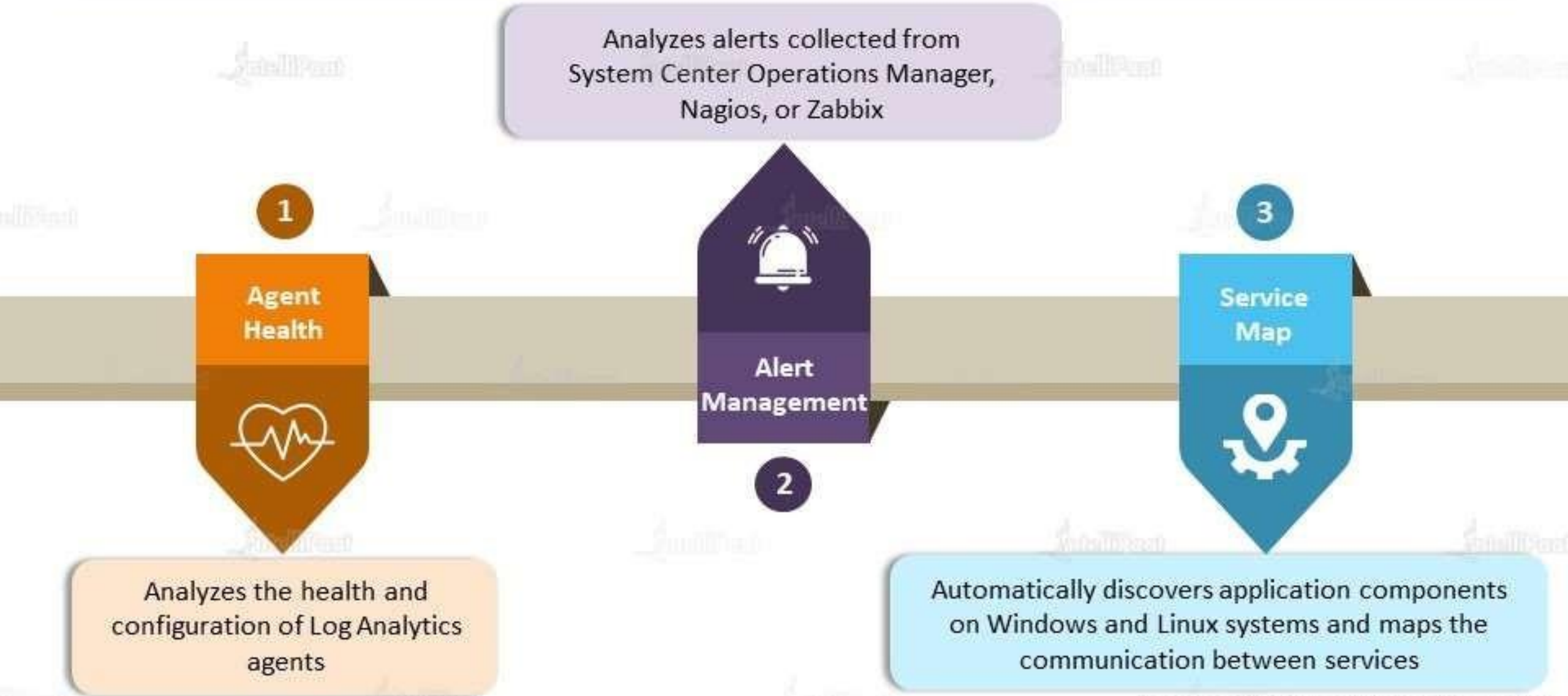
AM for VMs

Monitors our Azure virtual machines (VMs) and virtual machine scale sets at scale. It analyzes the performance and health of our Windows and Linux VMs

Insights and Core Solutions

Core Solutions are based on the log queries and views customized for a particular application or service. They collect and analyze logs only and are being deprecated over time in favor of Insights

Insights and Core Solutions

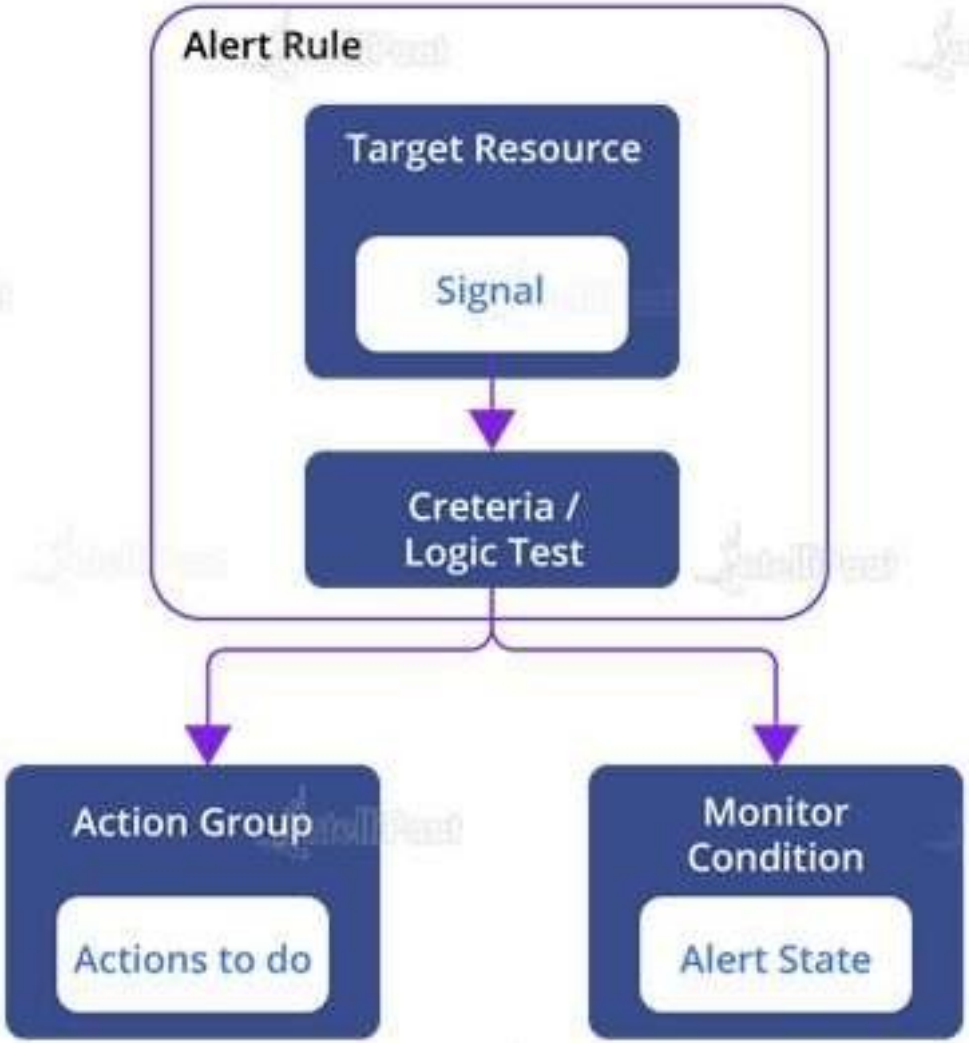


Alerts in Azure

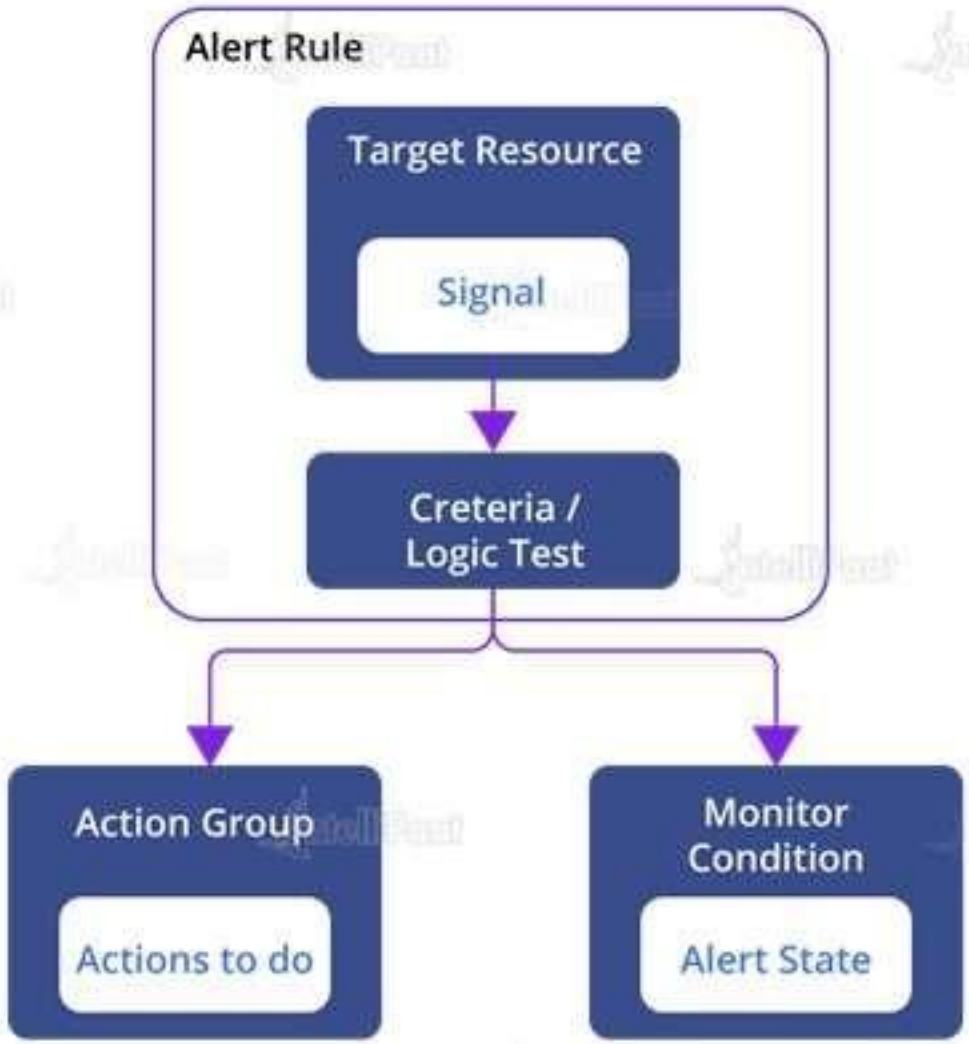
Alerts in Azure

- Alerts proactively notify us when important conditions are found in our monitoring data
- They allow us to identify and address issues before the users of our system notice them
- In the past, Azure Monitor, Application Insights, Log Analytics, and Service Health had separate alerting capabilities
- The previous alert experience and alert types are called Classic alerts

Flow of Alerts



Flow of Alerts



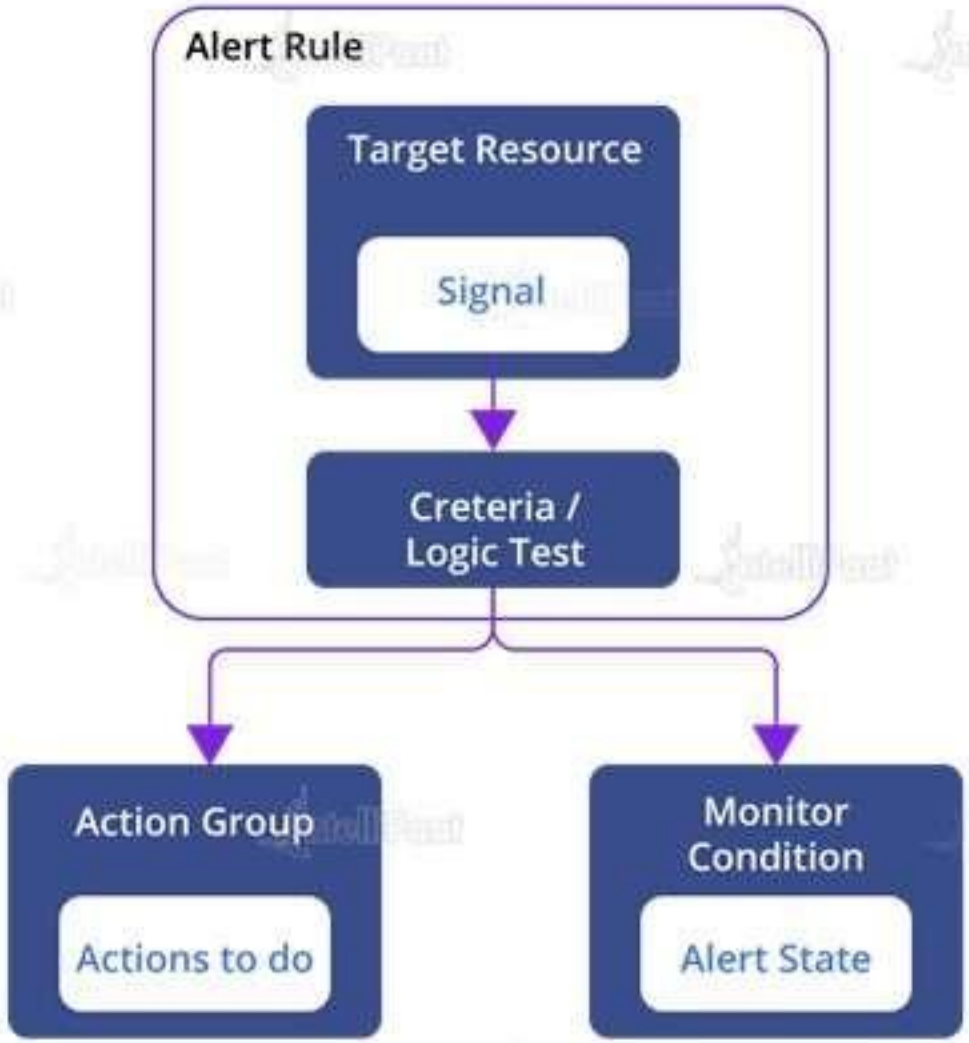
Target Resource

- Defines the scope and signals available for alerting
- Can be any Azure resource

Examples

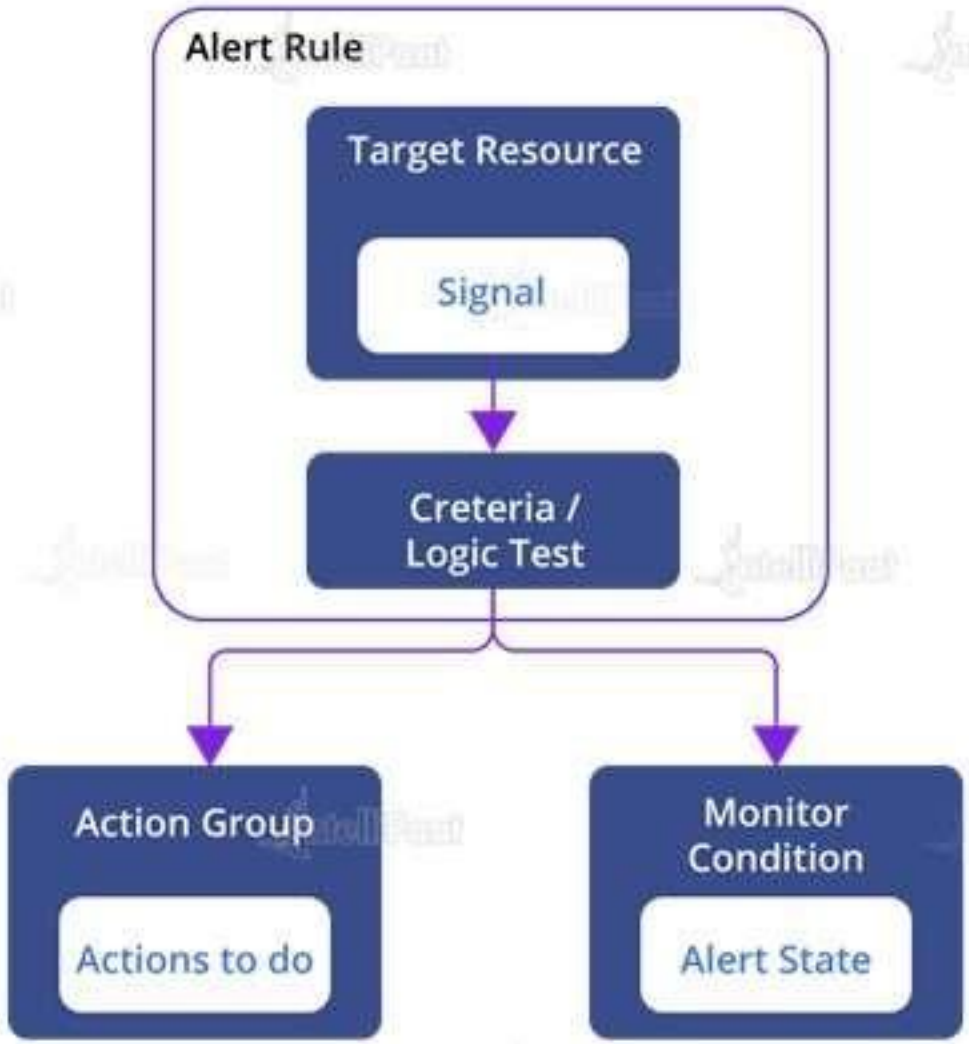
Virtual machines, storage accounts, virtual machine scale sets, Log Analytics workspace, or Application Insights resource

Flow of Alerts



For certain resources (like virtual machines), we can specify multiple resources as the target of an alert rule

Key Attributes of an Alert Rule



Signal

Emitted by the target resource, signals can be of the following types: metric, activity log, Application Insights, and log

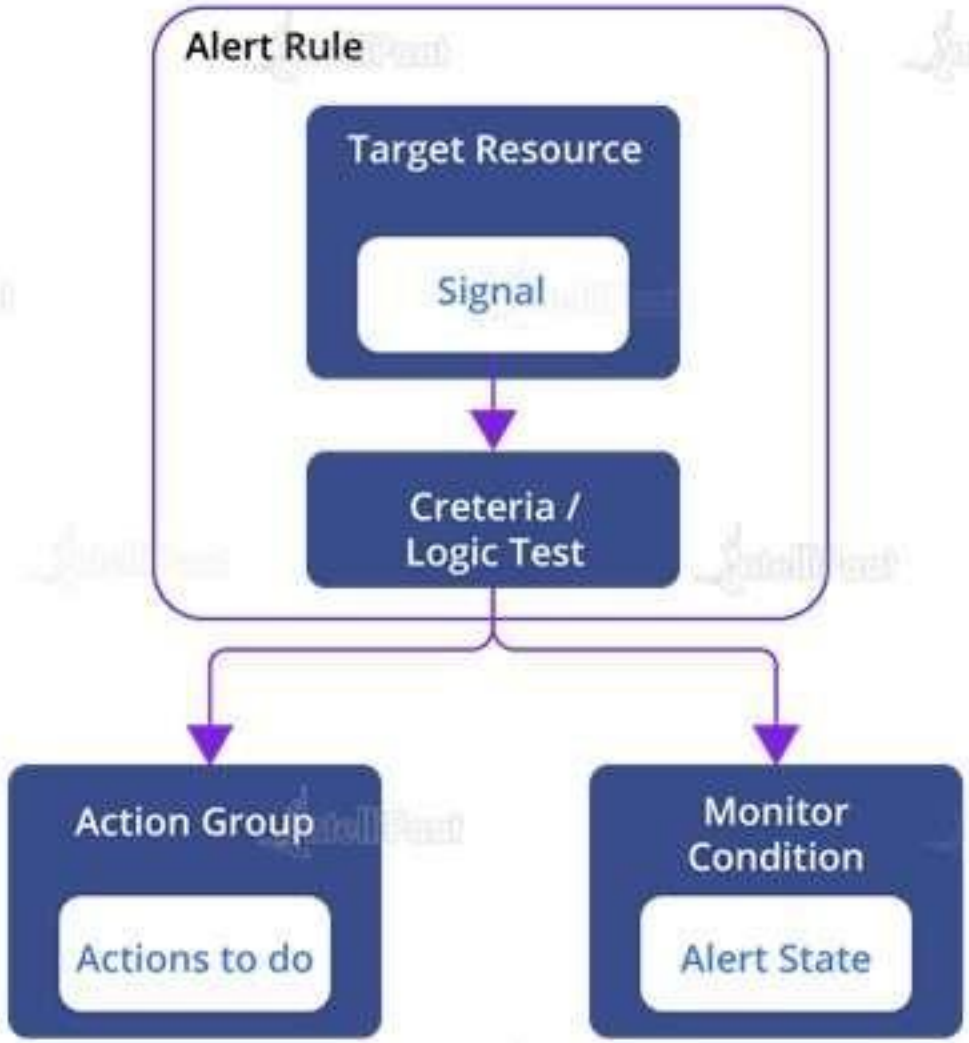
Criteria

A combination of signal and logic applied on a target resource

Examples:

- Percentage CPU > 70%
- Server Response Time > 4 ms
- Result count of a log query > 100

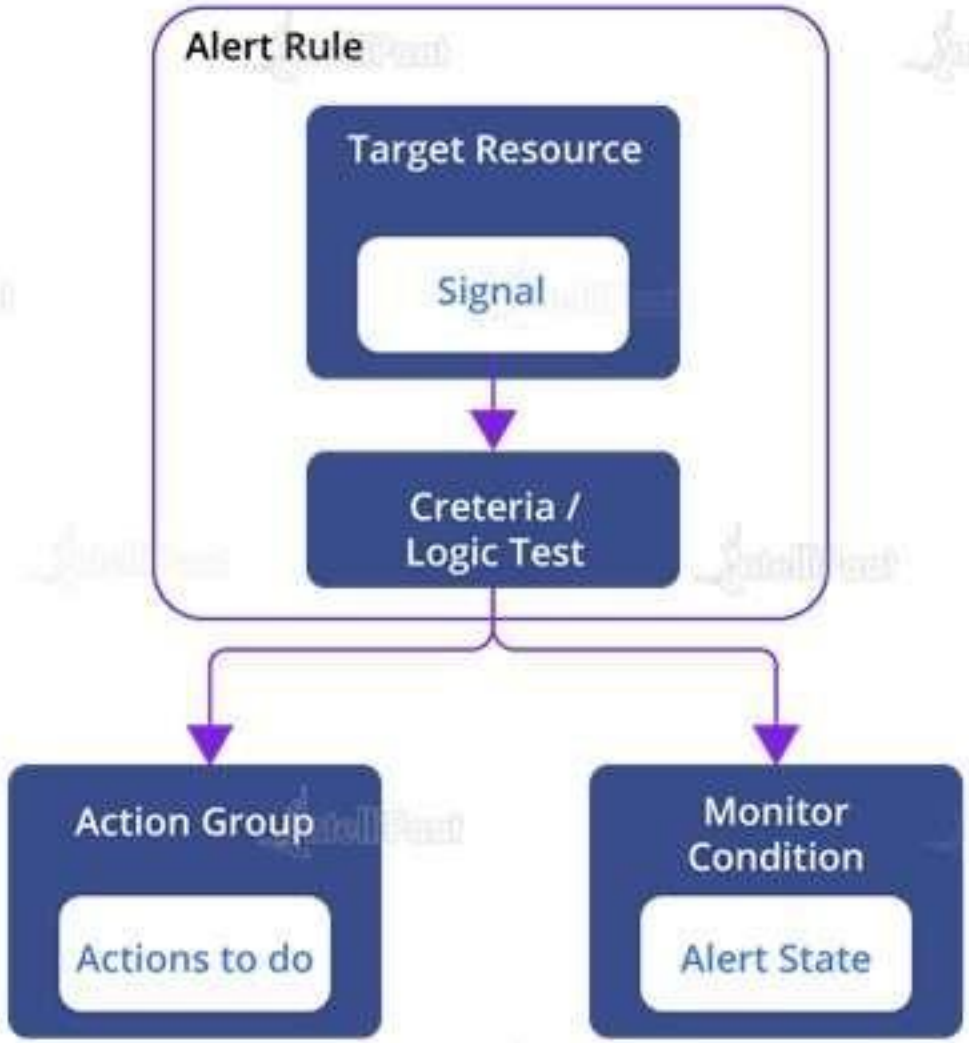
Key Attributes of an Alert Rule



Alert Name: A specific name for the alert rule configured by a user

Alert Description: A description for the alert rule configured by the user

Key Attributes of an Alert Rule



Severity: The severity of an alert after the criteria specified in the alert rule is met. Severity can range from 0 to 4

Sev 0 = Critical
Sev 1 = Error
Sev 2 = Warning
Sev 3 = Informational
Sev 4 = Verbose

Action: The specific action taken when an alert is fired

What can we set an alert on?

We can set an alert on metrics and logs

Metrics

Logs

Important ones among many

Metric values

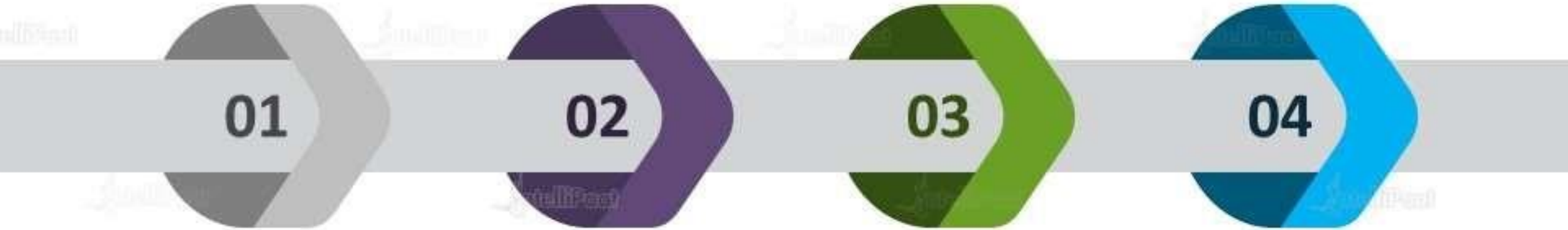
Log search queries

Activity log events

Health of the underlying Azure platform

Tests for website availability

Managing Alerts



We can set the state of an alert to specify where it is in the resolution process

When the criteria specified in the alert rule is met, an alert is created or fired, and it has a status 'New'

We can change the status when we acknowledge an alert and when we close it

All state changes applied to an alert are stored in the history of the alert

Alert States

An alert state is different and independent of the monitor condition. It is set by the user; whereas, the monitor condition is set by the system

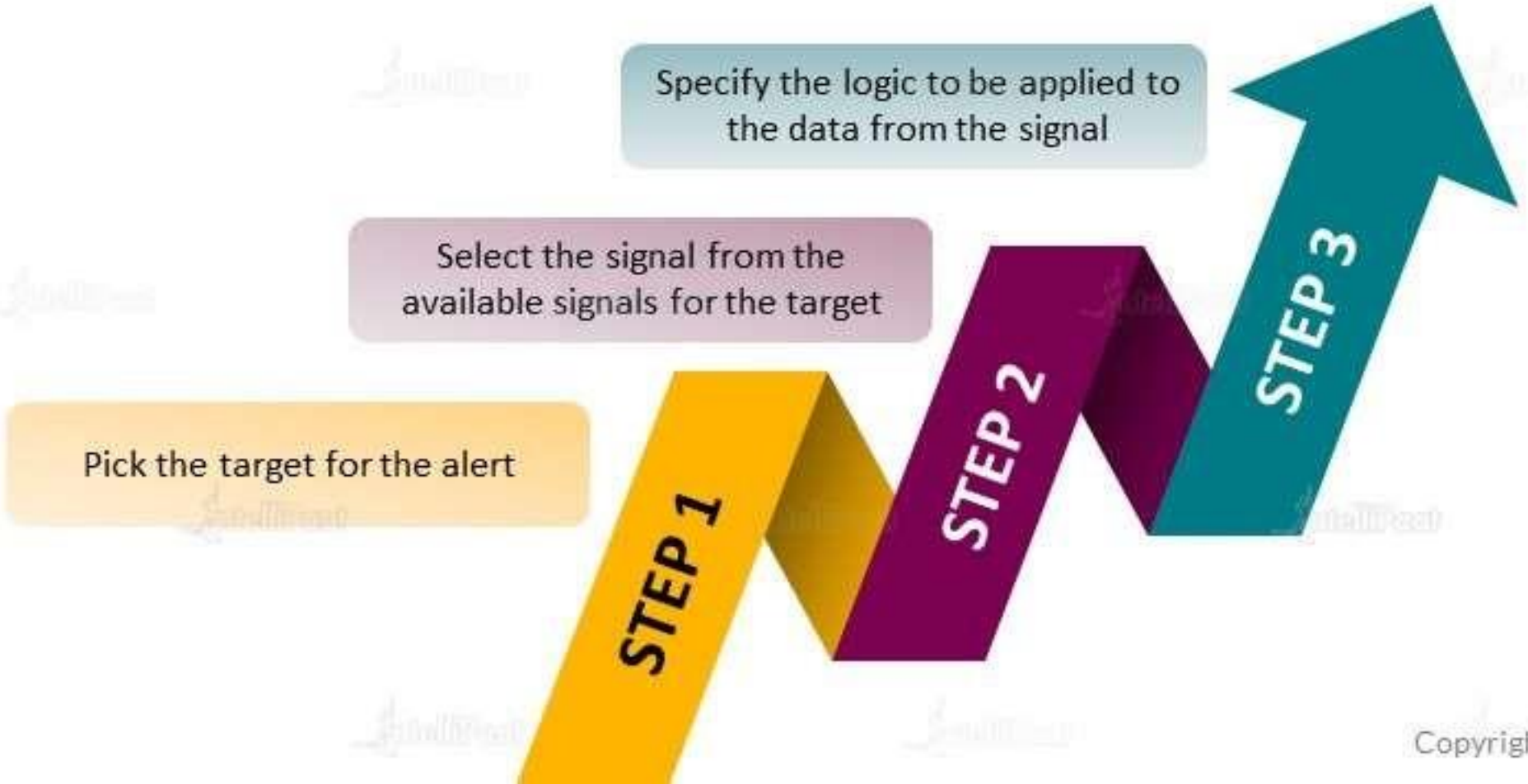
New: The issue has just been detected and hasn't yet been reviewed

Closed: The issue has been resolved. Even after an alert is closed, we can reopen it by changing it into another state

Acknowledged: An administrator has reviewed the alert and has started working on it

How to create an Alert?

We can author alerts in a consistent manner, regardless of the monitoring service or signal type. All fired alerts and related details will be available in a single page



Hands-on: Creating, Viewing, & Managing Metric Alerts Using Azure Monitor

Hands-on: Monitoring Azure Data Factory Pipelines Proactively with Alerts

Azure Security Logging & Auditing

Azure Security Logging & Auditing

Azure provides a wide array of configurable security auditing and logging options to help us identify the gaps in our security policies and mechanisms

The logging data can provide insights into our application and help us:

- Troubleshoot past problems and prevent potential ones
- Improve application performance or maintainability
- Automate actions that would otherwise require manual intervention

Types of Logs in Azure

- **Control/Management Logs**: Provide information about Azure Resource Manager CREATE, UPDATE, and DELETE operations
- **Data Plane Logs**: Provide information about events raised as part of the Azure Resource usage. **Examples:** Windows event system, security, and application logs in a VM and the diagnostics logs configured through Azure Monitor
- **Processed Events**: Provide information about the analyzed events/alerts that have been processed on our behalf. **Examples**: Azure Security Center alerts where Azure Security Center has processed and analyzed our subscription and has provided concise security alerts

Azure SQL Database Auditing

Auditing for Azure SQL Database and SQL Data Warehouse tracks database events and writes them into an audit log in our Azure Storage account, Log Analytics workspace or Event Hubs

We can use SQL Database Auditing to:

Retain an audit trail of the select events. We can define the categories of database actions to be audited

Report on the database activity. We can use pre-configured reports and a dashboard to get started quickly with activity and event reporting

Analyze reports. We can find suspicious events, unusual activities, and trends

Server-level vs Database-level Auditing Policies

An auditing policy can be defined for a specific database or as a default server policy

- A server policy applies to all existing and newly created databases on the server
- If server blob auditing is enabled, it always applies to the database. The database will be audited, regardless of the database auditing settings
- Enabling blob auditing on the database or data warehouse, in addition to enabling it on the server, does not override or change any of the settings of the server blob auditing. Both audits will exist side by side

Hands-on: Azure SQL Database Auditing

IntelliPaat

India: +91-7847955955

US: 1-800-216-8930 (TOLL FREE)

sales@intellipaat.com

24/7 Chat with Our Course Advisor