

Cloud Computing

Caltech

**Center for Technology &
Management Education**

Designing Infrastructure Solutions on Azure



Design a Solution for Logging and Monitoring

Learning Objectives

By the end of this lesson, you will be able to:

- 🕒 Implement appropriate monitoring tools for a solution
- 🕒 Analyze Azure Monitor health and availability monitoring
- 🕒 Initiate automated responses using action groups
- 🕒 Configure and manage alerts



A Day in the Life of an Azure Architect

You are working for an organization as a Cloud Architect. The organization uses multiple Azure subscriptions and has a wide portfolio of products deployed across all subscriptions.

- You need to design a solution to generate a monthly report on all the resource deployments on a per subscription basis.
- Based on the monthly consumption, you also need to set up a budget and alerts so that stakeholders can be notified about the costs incurred so far and even the forecasted pricing.

Additionally, the organization is looking for a solution that can help collect and analyze data such as updates or changes made in any Azure resource.

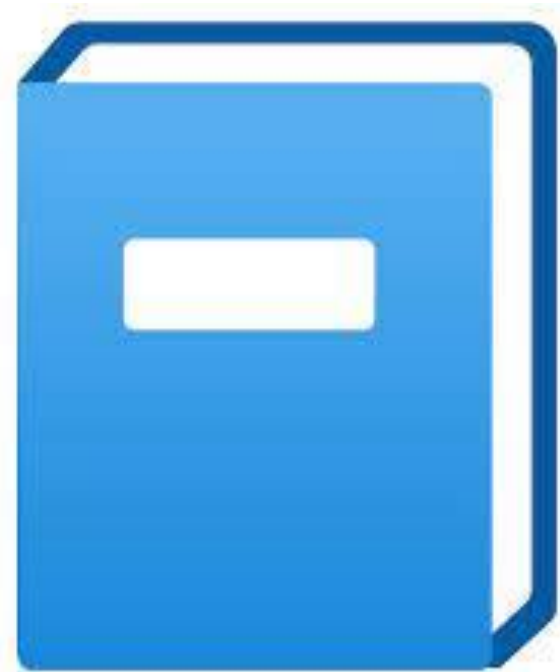
To achieve all the above, along with some additional features, we would be learning a few concepts in this lesson that will help you find a solution for the above scenario.



Design for Azure Workbooks and Azure Insights

Azure Workbooks

Azure workbooks provide a dynamic platform for the processing of data and the development of effective visual reports.



It also allows users to access data from various Azure datasets and merge them to create a seamless interactive experience.

Application Insights

Application Insights is a feature of Azure Monitor. It is a developer and DevOps-focused application performance management service.



Azure Monitor VM

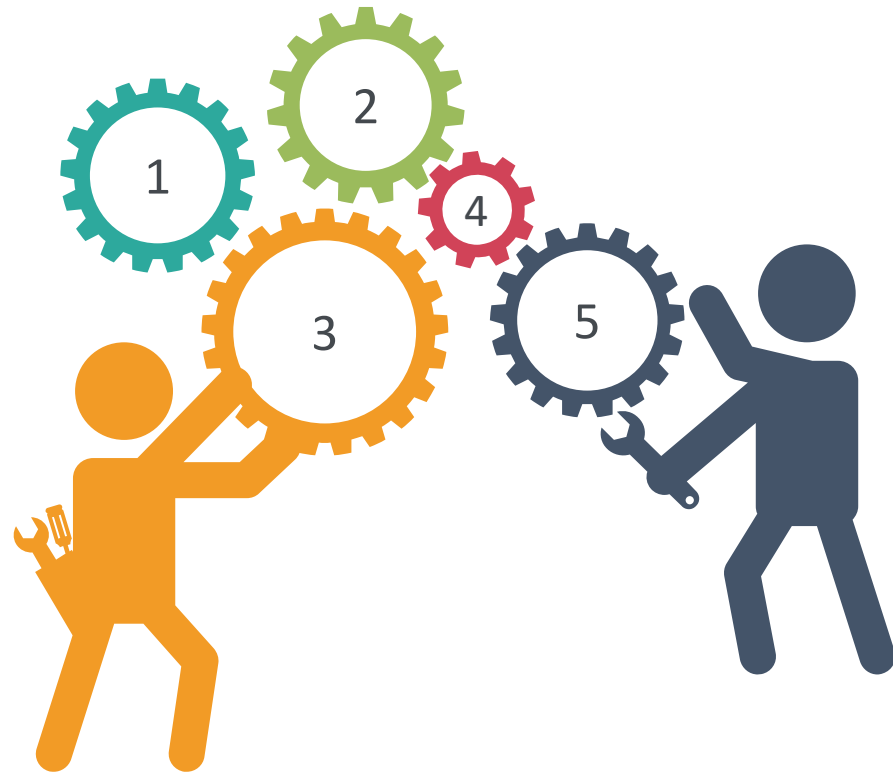
Azure Monitor is a full-featured monitoring service that lets the user keep track of all the Azure resources.



Azure Monitor's functions are linked to the Azure site for the Azure services it monitors. Users do not need to interact with it directly to do a range of monitoring tasks.

Container Insights

Container insights is a feature that allows the user to track the effectiveness of container workloads on the following platforms:



Managed Kubernetes clusters hosted on
Azure Kubernetes Service (AKS)

Self-managed Kubernetes clusters hosted on
Azure using AKS Engine

Container Instances in Azure

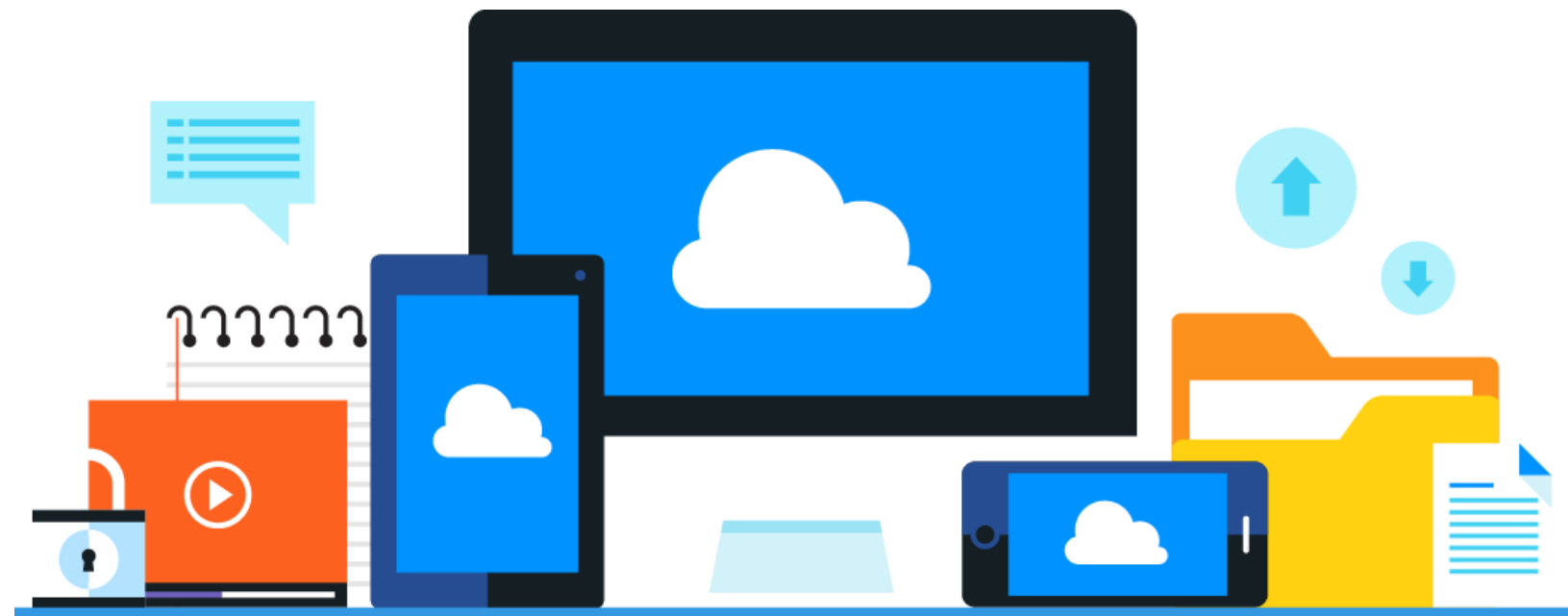
Self-managed Kubernetes clusters hosted on
Azure Stack

Azure Arc-enabled Kubernetes

Recommend Appropriate Monitoring Tools for a Solution

Azure Monitoring

Azure Monitoring collects and analyzes data to assess the application's performance, health, availability, and the resources that it depends on.



Azure Infrastructure Monitoring

These are the different ways of how Azure monitors:

Configuration and change management

Vulnerability management

Vulnerability scanning

Protective monitoring

Incident management



Azure reviews and updates configuration settings and baseline configurations of hardware, software, and network devices annually.

Azure Infrastructure Monitoring

Configuration and change management

Vulnerability management

Vulnerability scanning

Protective monitoring

Incident management



Security update management helps protect systems from known vulnerabilities.

Azure Infrastructure Monitoring

Configuration and change management

Vulnerability management

Vulnerability scanning

Protective monitoring

Incident management



It is performed on server operating systems, databases, and network devices.

Azure Infrastructure Monitoring

Configuration and change management

Vulnerability management

Vulnerability scanning

Protective monitoring

Incident management



Monitoring tools like Microsoft Monitoring Agent (MMA) and System Center Operations Manager are used for active monitoring.

Azure Infrastructure Monitoring

Configuration and change management

Vulnerability management

Vulnerability scanning

Protective monitoring

Incident management



Microsoft implements a security incident management process to facilitate a coordinated response to incidents.

Azure Infrastructure Monitoring

Configuration and change management

Vulnerability management

Vulnerability scanning

Protective monitoring

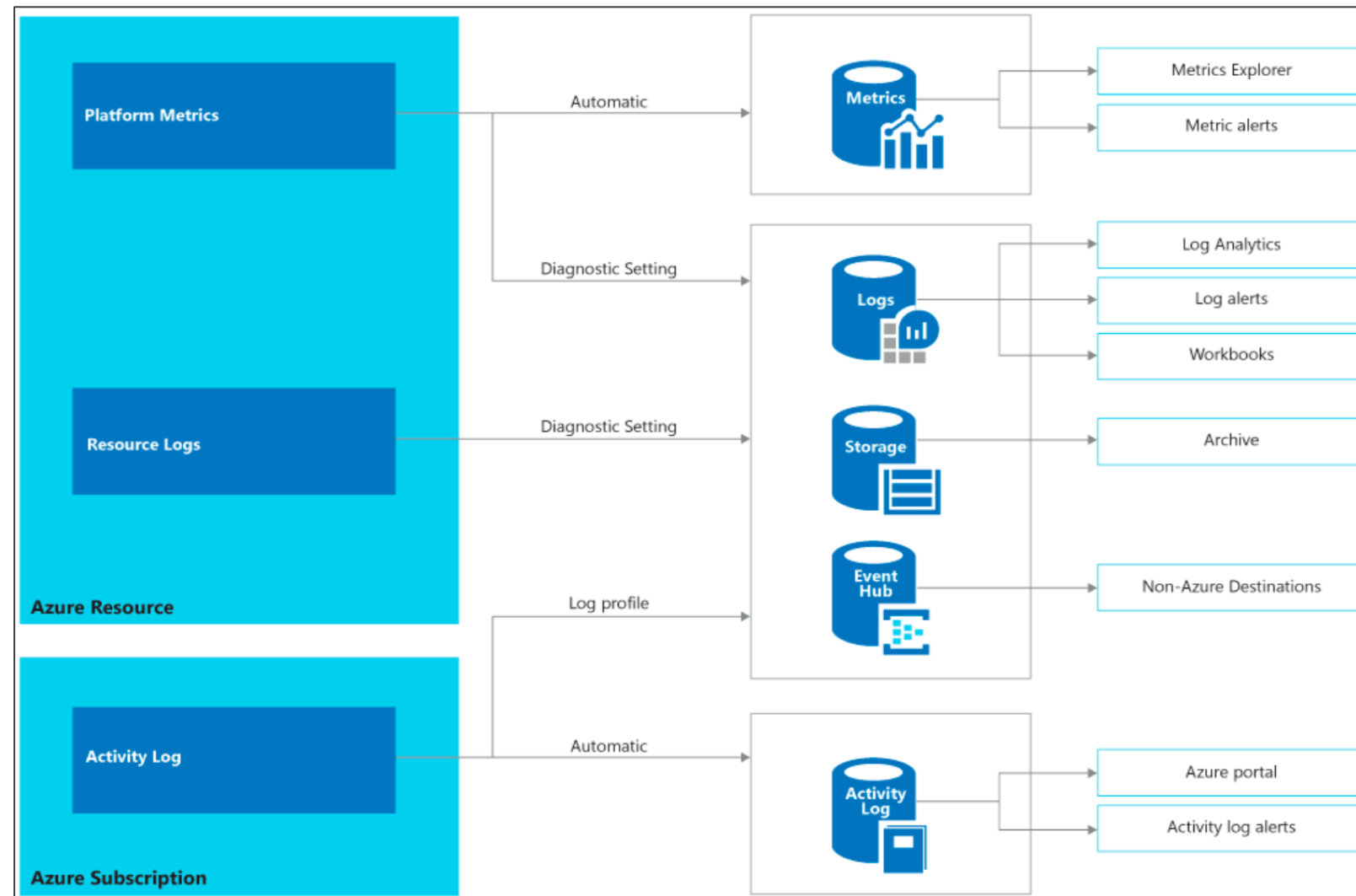
Incident management



Microsoft implements a security incident management process to facilitate a coordinated response to incidents.

Monitoring Data

These are the types of monitoring data:

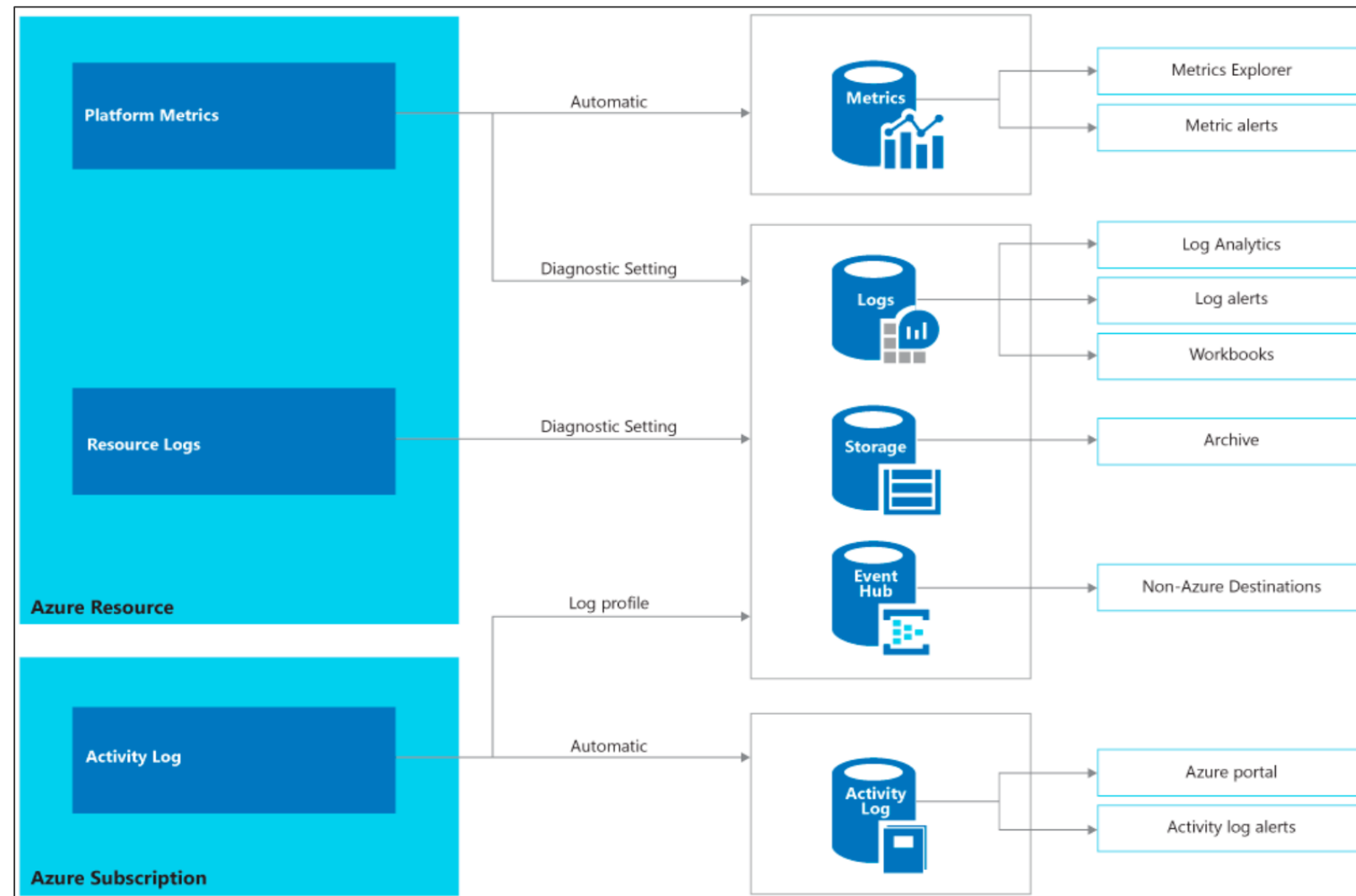


Platform metrics

Numerical values that are automatically collected at regular intervals, which describe some aspects of a resource at a time

Monitoring Data

These are the types of monitoring data:

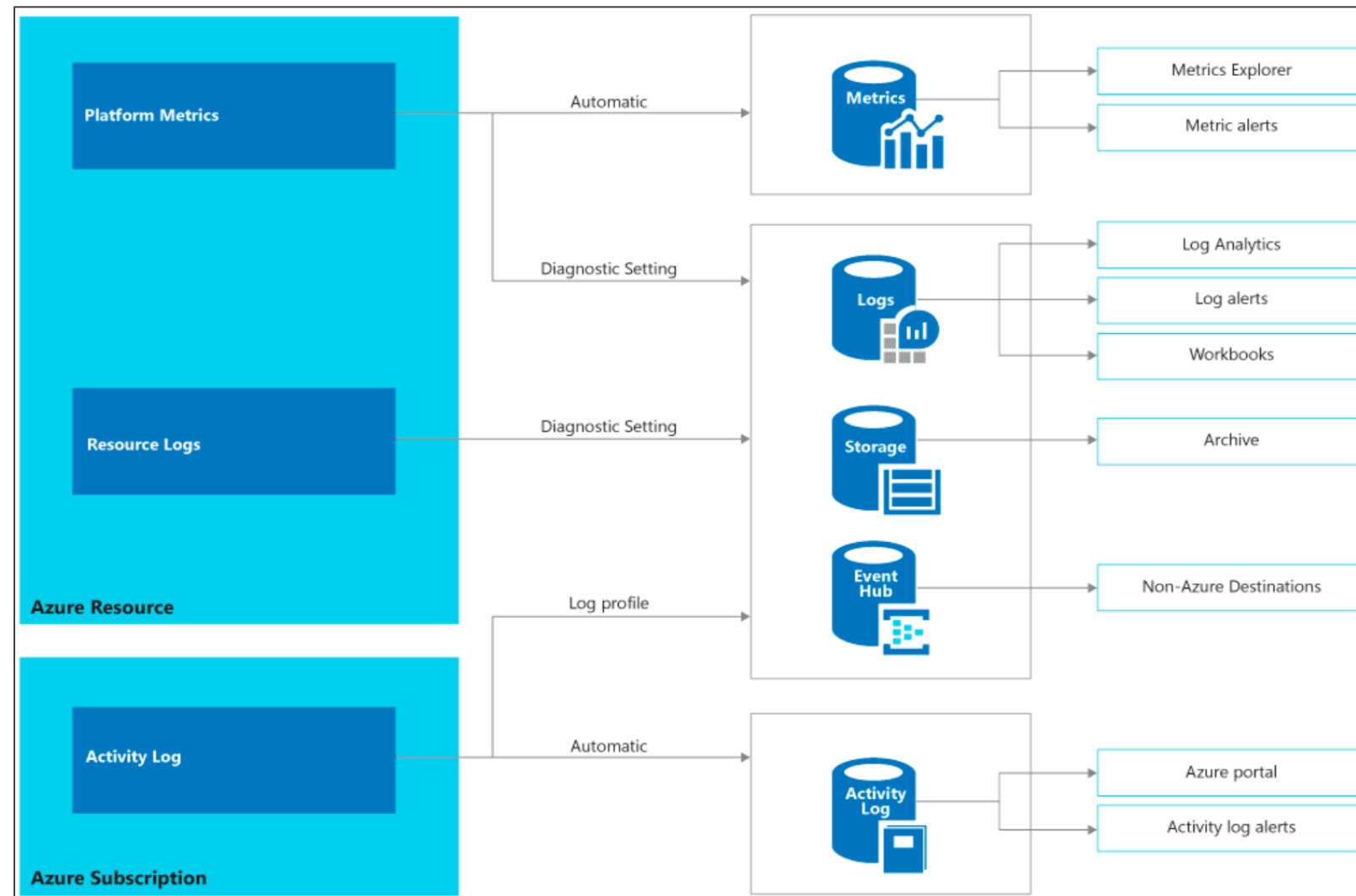


Resource logs

Provide insight into operations that were performed within an Azure resource (the data plane)

Monitoring Data

These are the types of monitoring data:

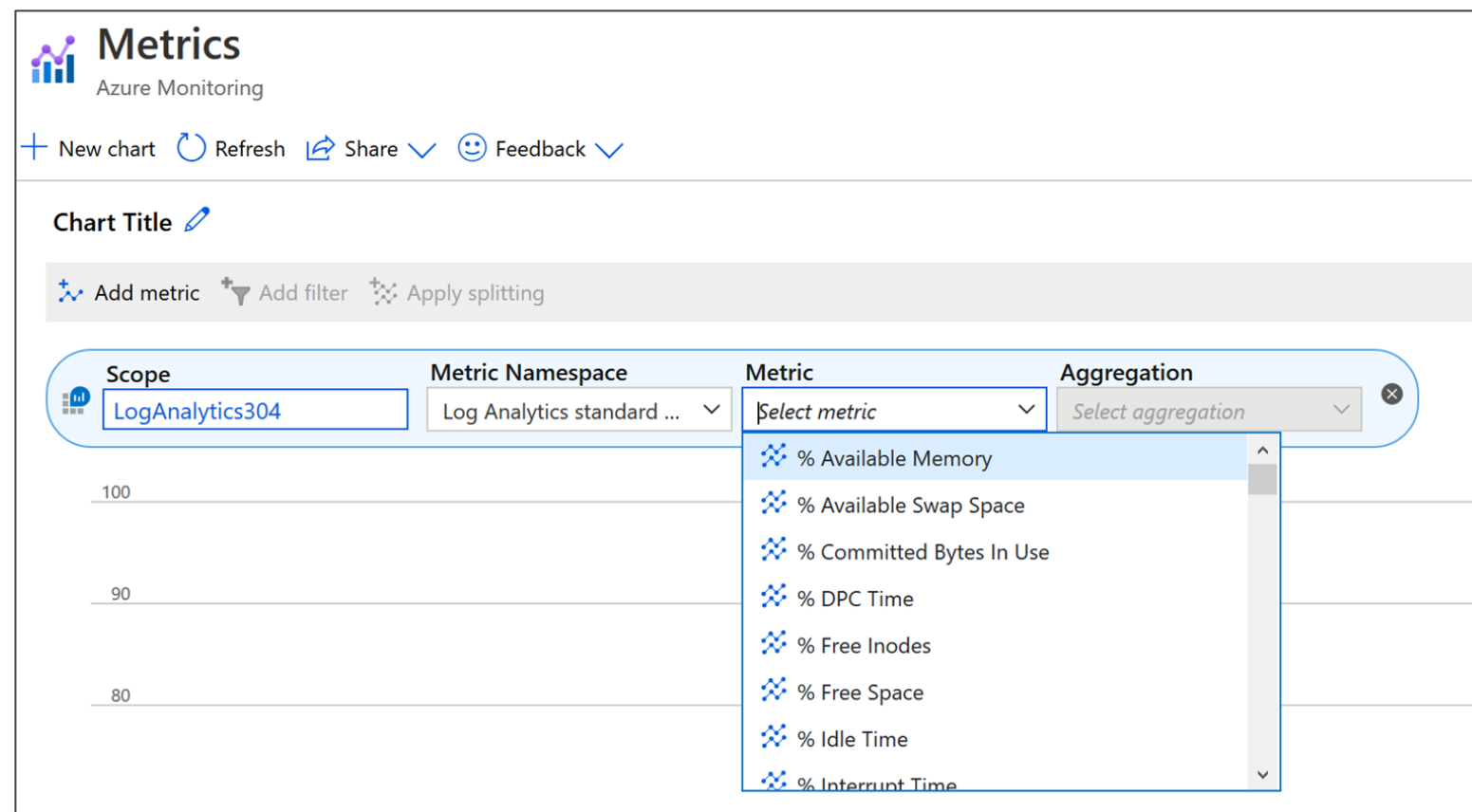


Activity log

Provides insight into the operations on each Azure resource in the subscription from the outside (the management plane)

Configure Monitoring

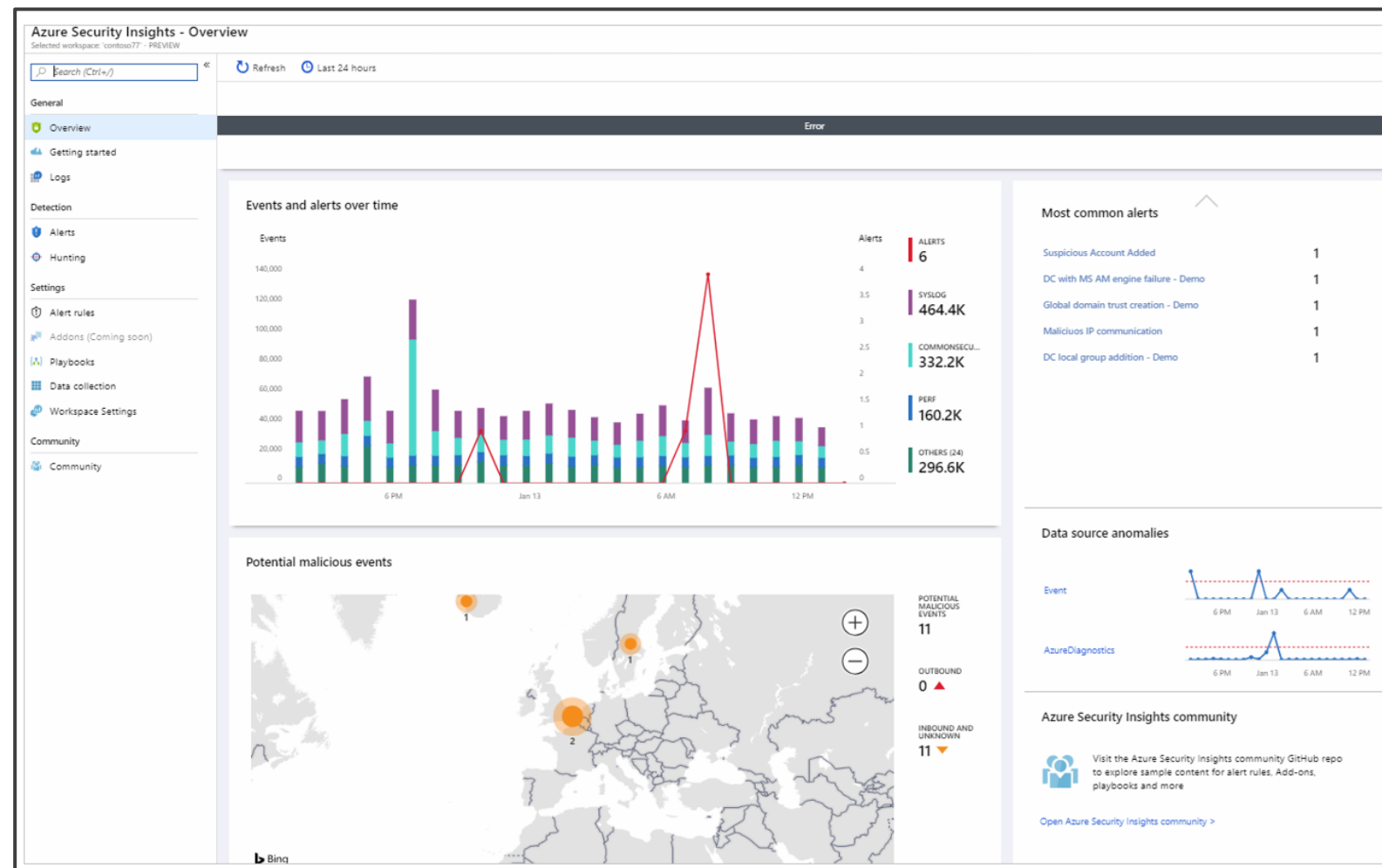
Monitoring data is collected automatically.



- **Platform metrics:** They are collected automatically.
- **Resource logs** – They are not collected by default. A user must create a diagnostic setting.
- **Activity log** – It is collected automatically.

Azure Sentinel

It is a built-in threat intelligence for detection and investigation.



- Collects data from devices, users, infrastructure, and applications
- Helps cloud and on-premises monitoring and management
- Investigates threats using AI

Application Monitoring

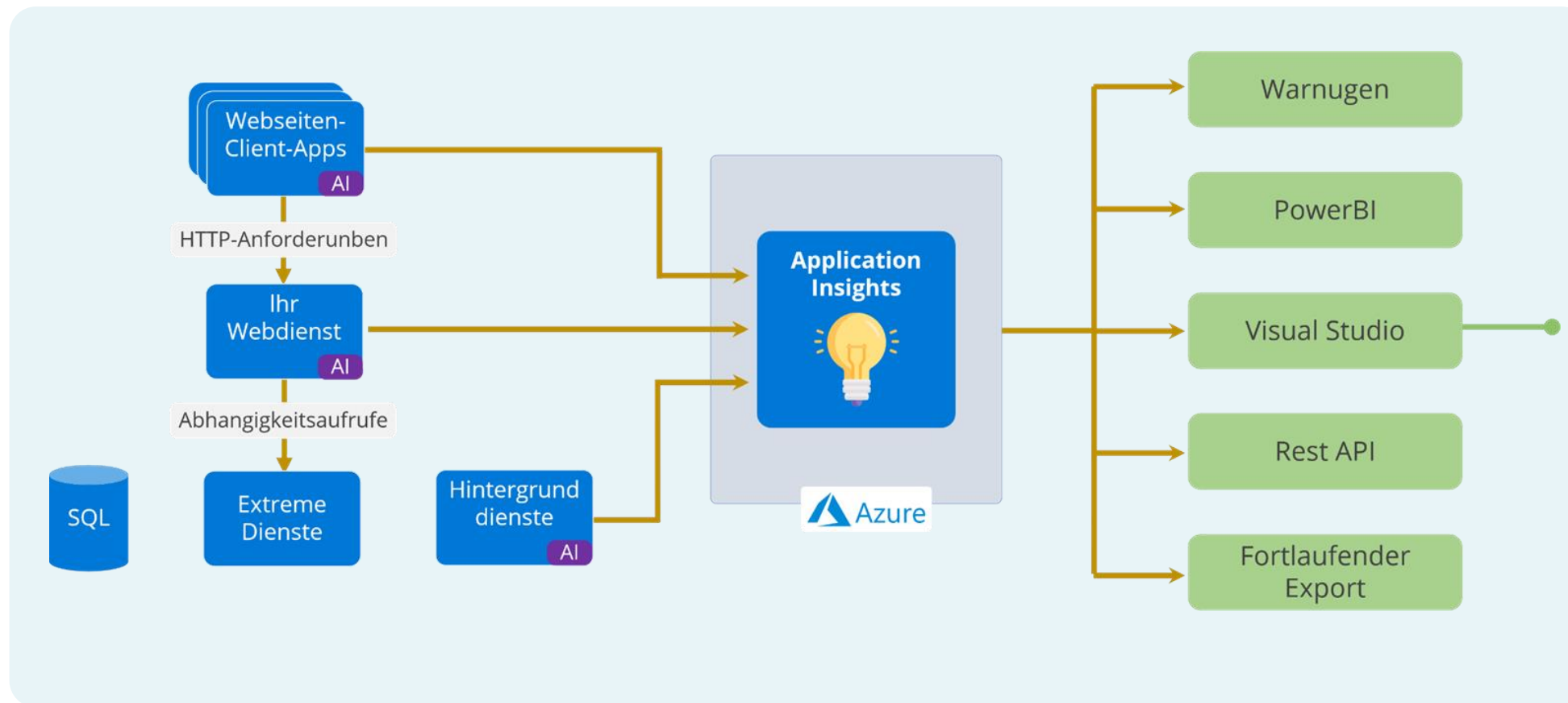
Connection points to a range of development tools are available in application insights.



Application insights keep track of user's web application availability, performance, and usage.

Application Monitoring

These are the different application insights:



Default dashboard with most important metrics

Smart detection

Usage analysis

Snapshot debugger

Performance statistics from a client and server

Platform Monitoring

These are the container insights:



- Clusters, nodes, and pods are visualized, and actionable information is provided.
- CPU, memory, and logs for individual Kubernetes pods are also available.
- Container logs are also collected.

Monitoring Best Practices

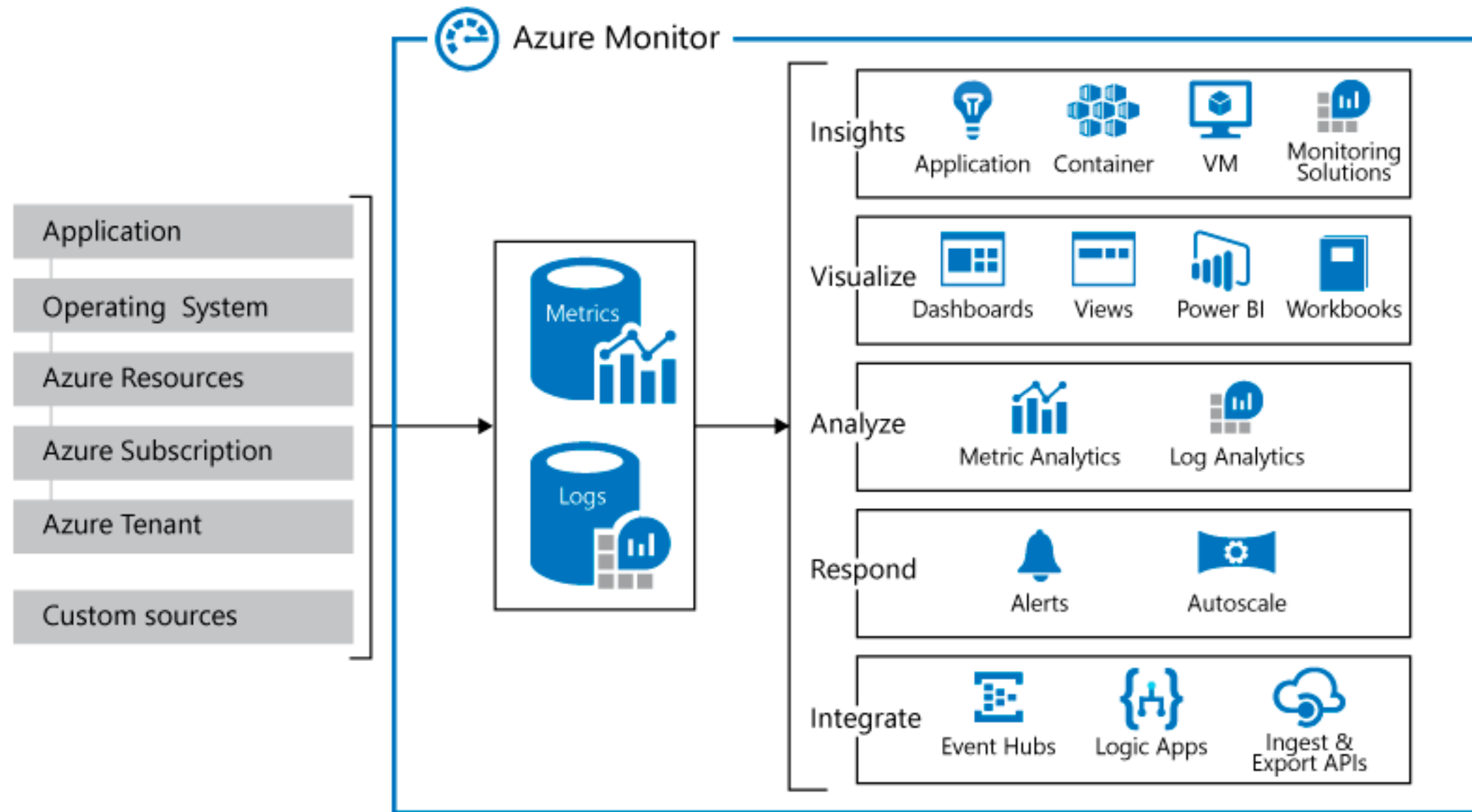
These are the best practices for monitoring:

- Ensures applications are performing as expected
- Ensures applications are as reliable as their underlying infrastructure
- Ensures quality through continuous deployment
- Prepares role-based dashboards and workbooks

Azure Monitoring

Azure Monitor Service

Azure includes multiple services that individually perform a specific role or a task in the monitoring space.



Key Capabilities

Azure includes multiple services that individually perform a specific role or a task in the monitoring space.

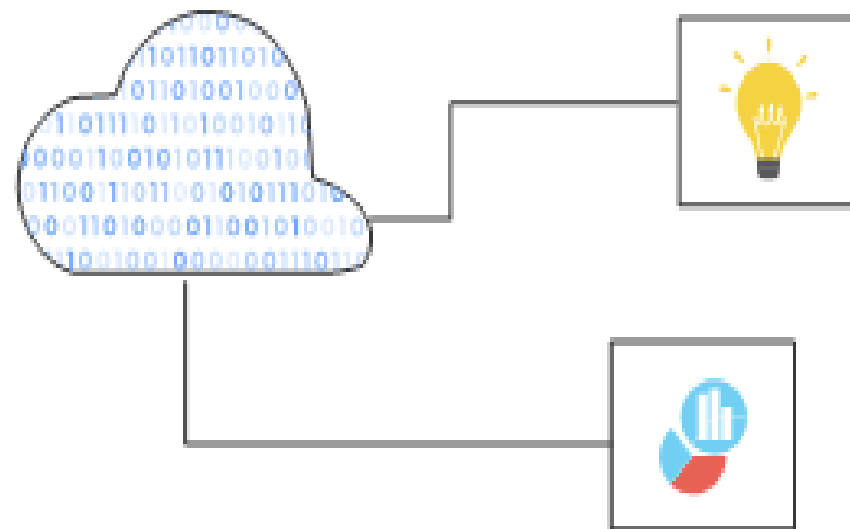


Monitor and Visualize Metrics

Metrics are numerical values available from Azure Resources that help the user understand the health, operation, and performance of the system.

Key Capabilities

Azure includes multiple services that individually perform a specific role or a task in the monitoring space.



Query and Analyze Logs

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

Key Capabilities

Azure includes multiple services that individually perform a specific role or a task in the monitoring space.

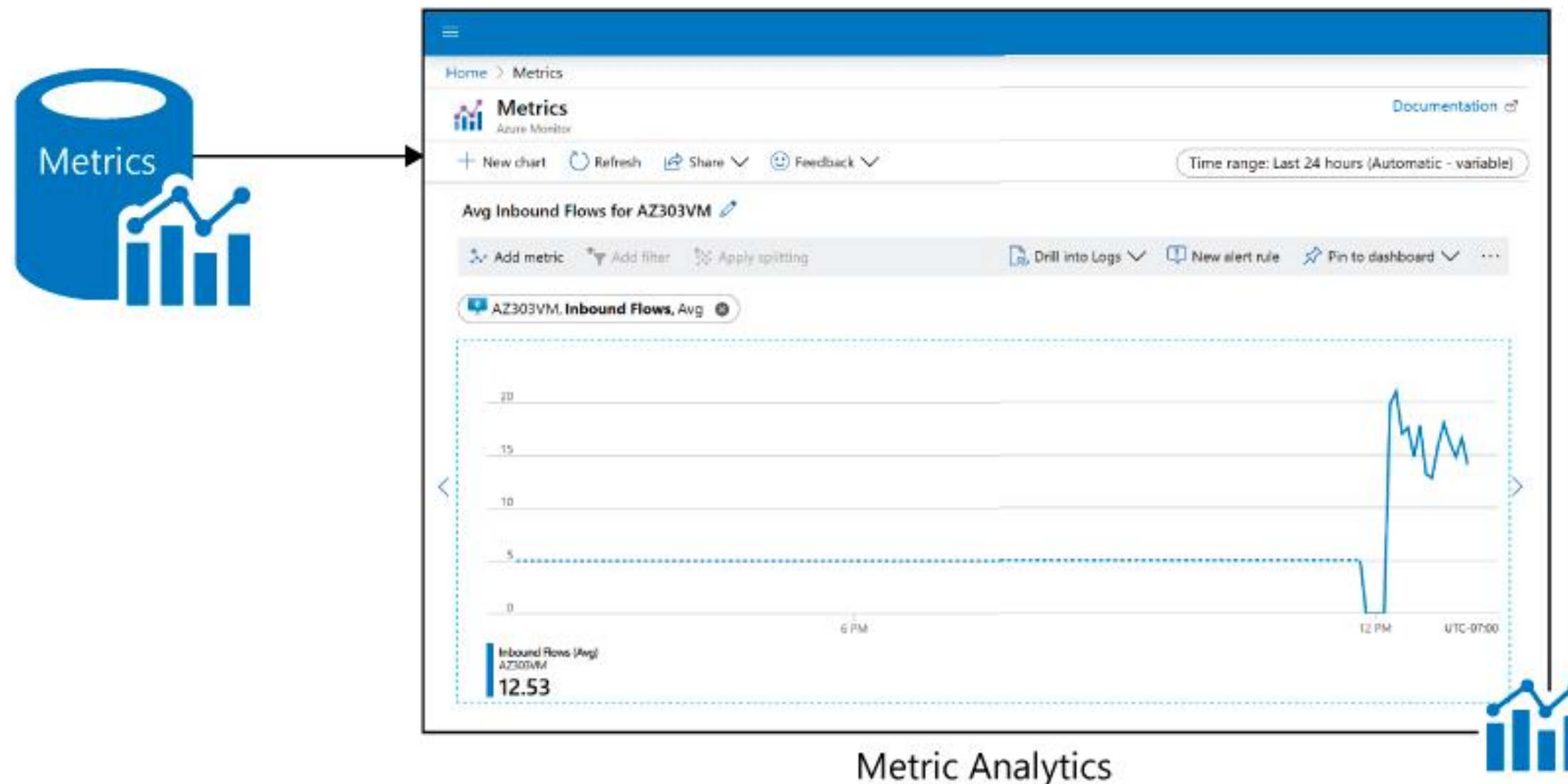


Setup Alerts and Actions

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

Monitoring Data Platform

Azure includes multiple services that individually perform a specific role or a task in the monitoring space.



Metrics

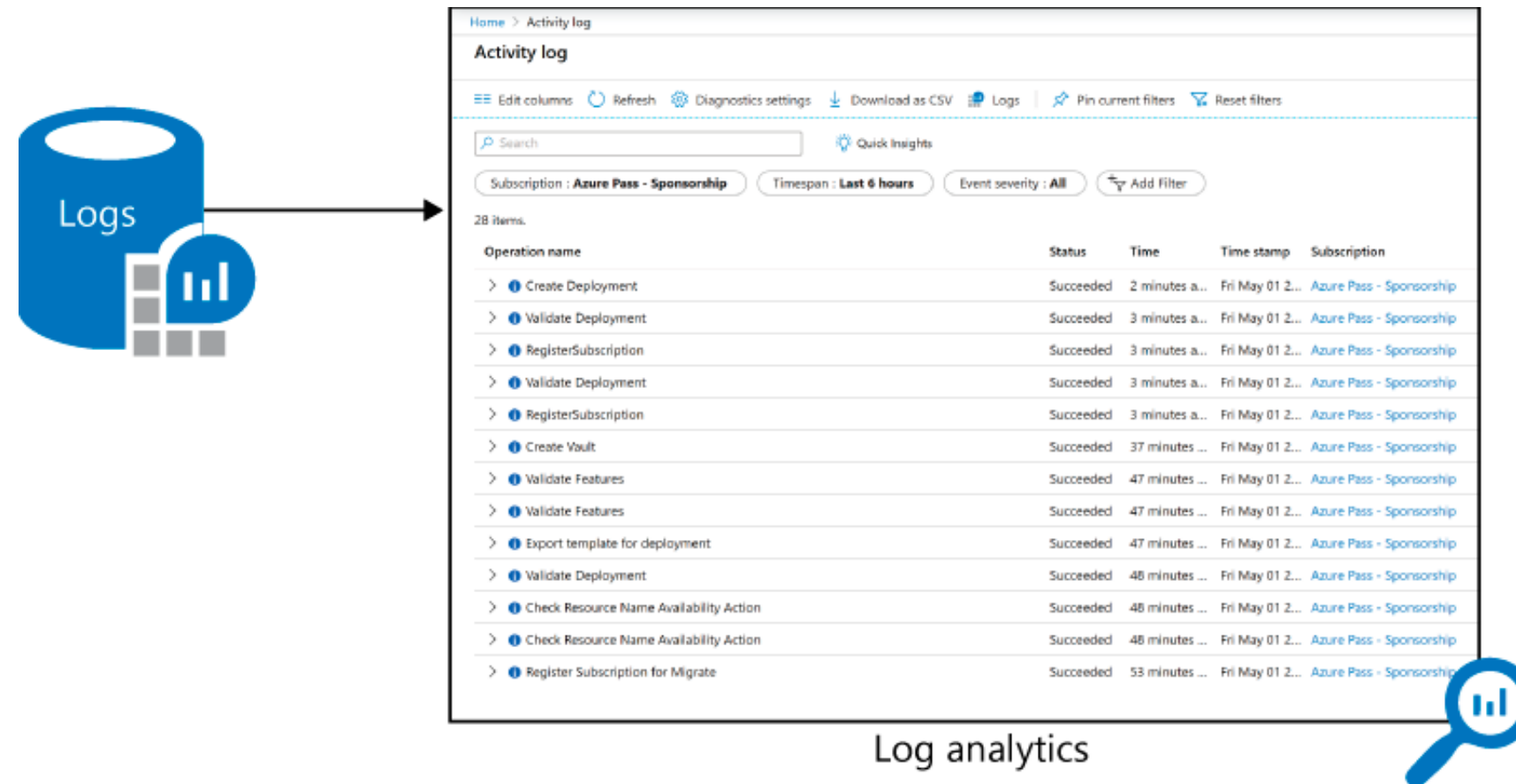
Metrics are numerical values that describe some aspect of a system at a point in time.



They are lightweight and capable of supporting near real-time scenarios.

Log Data

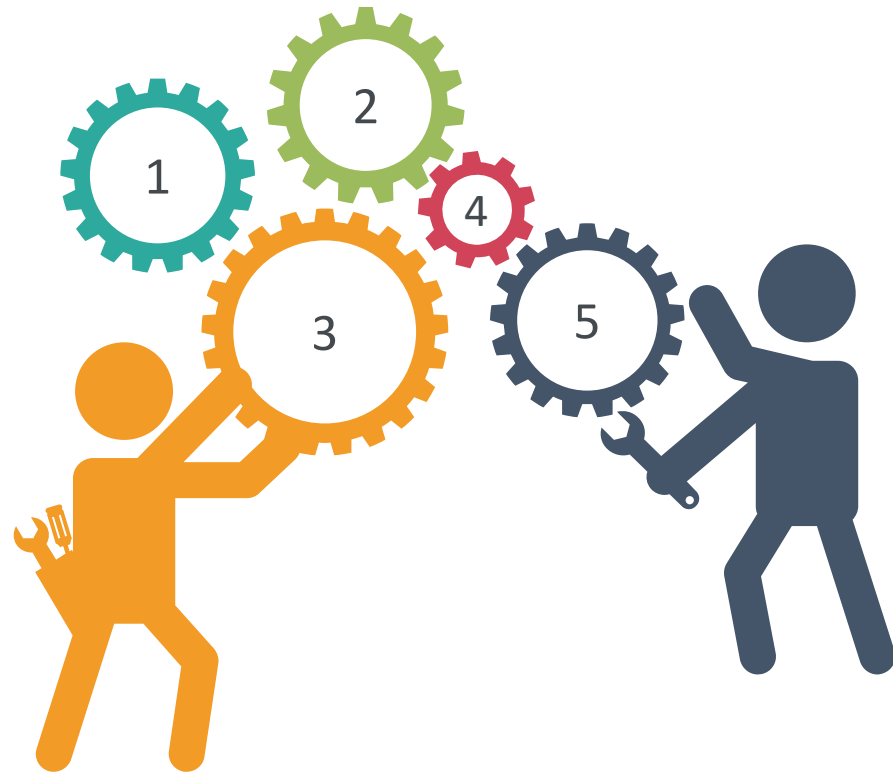
Logs contain different types of data organized into records with different sets of properties for each type.



Telemetry such as events and traces are stored as logs in addition to performance data so that it can be combined for analysis.

Data Types

Azure Monitor collects data from each of the following tiers:



Azure subscription monitoring data

Application monitoring data

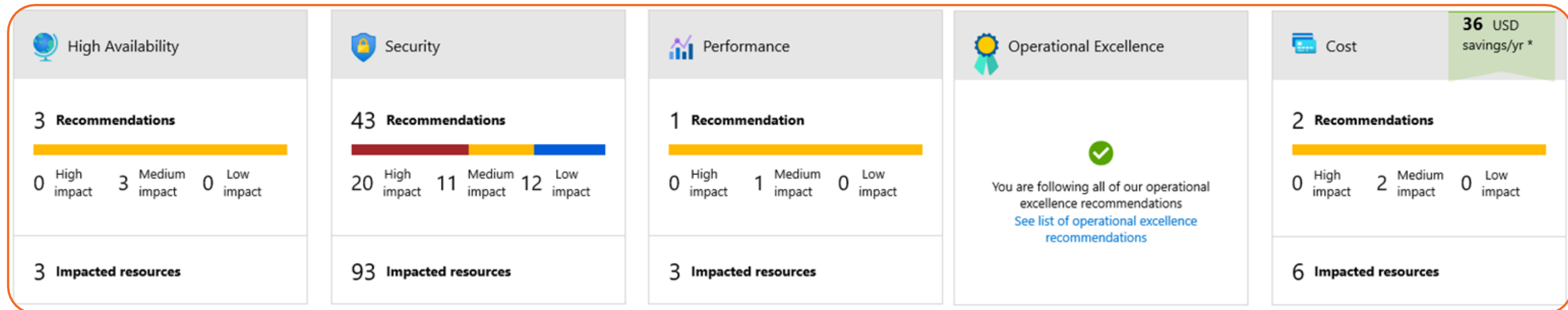
Guest OS monitoring data

Azure resource monitoring data

Azure tenant monitoring data

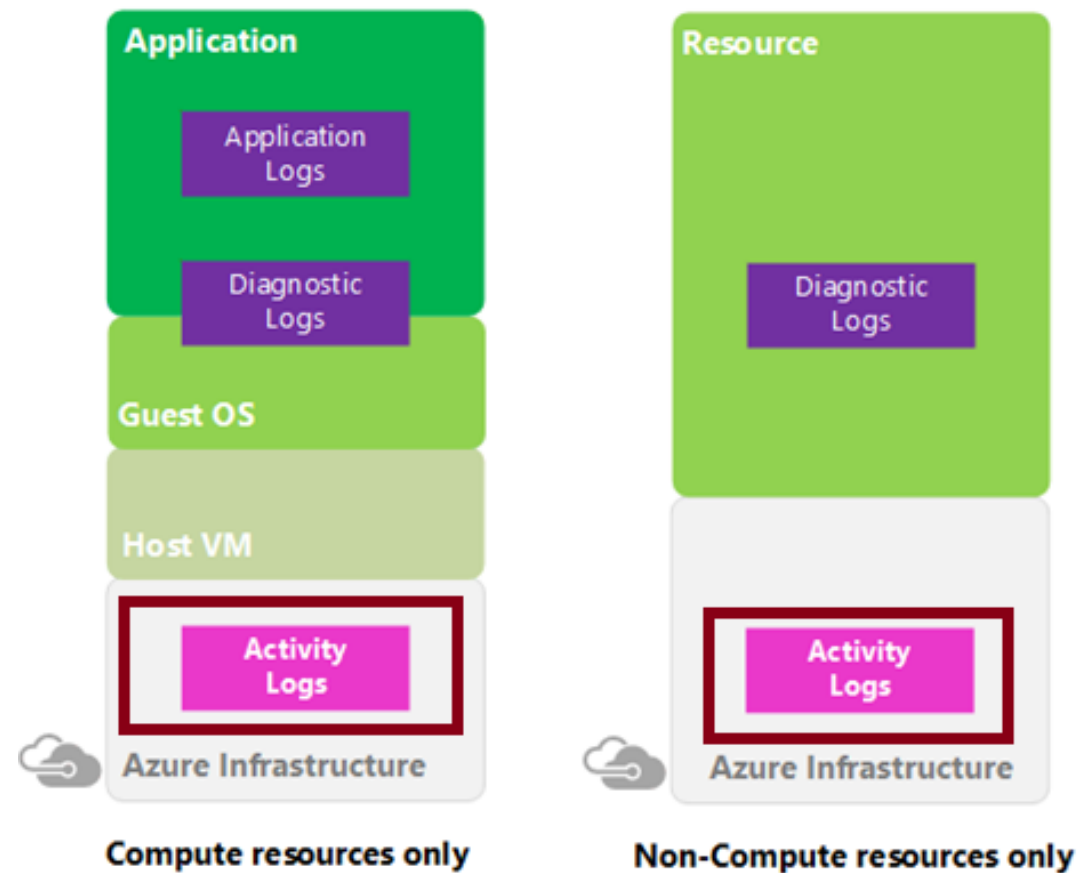
Azure Advisor

Azure Advisor is a personalized cloud consultant that helps follow best practices by optimizing Azure deployments.



Activity Log

Activity log is a subscription log that provides insight into subscription-level events that have occurred in Azure.



Activity log can determine:

- What operations (PUT, POST, DELETE) were performed on all resources?
- Who started the operation?
- When did the operation occur?
- What is the status of the operation?
- What are the values of other properties that might help in researching the operation?

Query the Activity Log

In the Azure portal, users can filter the Activity log by:

Subscription

Resource group

Event initiated by

Timespan

Resource name

Operation name

Event severity

Resource type

Search

App Service Diagnostic Logs

The Azure App Service has built-in diagnostics that can help users debug apps.



This service is not enabled by default.

Diagnostic Logs Types

There are two categories of Azure Web App diagnostic logs:

Application diagnostic logs:

- Contains information produced by the application code

Web Server diagnostic logs:

- Contains information produced by the web server that the web application is running on

Diagnostic Logs Types

There are three types of web server diagnostic logs that user can enable:

Web Server Logging

- Contains all HTTP events on a website and is formatted using the W3C extended log file format

Detailed Error Messages

- Contains information on requests that resulted in an HTTP status code of 400 or higher

Failed Request Tracing

- Contains detailed traces for any failed requests
- Contains traces for all the IIS components that were involved in processing the request

Log Structure : Log File Type and Location

Web server diagnostic logs are stored in different directories as shown below:

Web server logs

D:\Home\LogFiles\http\RawLogs\

Detailed error logs

D:\Home\LogFiles\DetailedErrors\

Failed request logs


D:\Home\LogFiles\LogFiles\W3SVC####\

Health and Availability Monitoring


Azure Status

Azure status provides a global view of the health of Azure services and regions.

Azure status

 RSS

Last updated 55 seconds ago

 **Services are operating normally.**


Status history >


Get a personalized view of the health of your Azure services


Go to your personalized dashboard >


Refresh every

2 minutes

 Good

 Warning

 Error

 Information

	Americas	Europe	Asia Pacific	Azure Government								
PRODUCTS AND SERVICES	NON-REGIONAL*	EAST US	EAST US 2	CENTRAL US	NORTH CENTRAL US	SOUTH CENTRAL US	WEST CENTRAL US	WEST US	WEST US 2	CANADA EAST	CANADA CENTRAL	BRAZIL SOUTH
COMPUTE												
Virtual Machines		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SAP HANA on Azure Large Instances		✓						✓				
Cloud Services		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Virtual Machine Scale Sets		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Functions		✓	✓	✓	✓	✓		✓	✓	✓	✓	✓

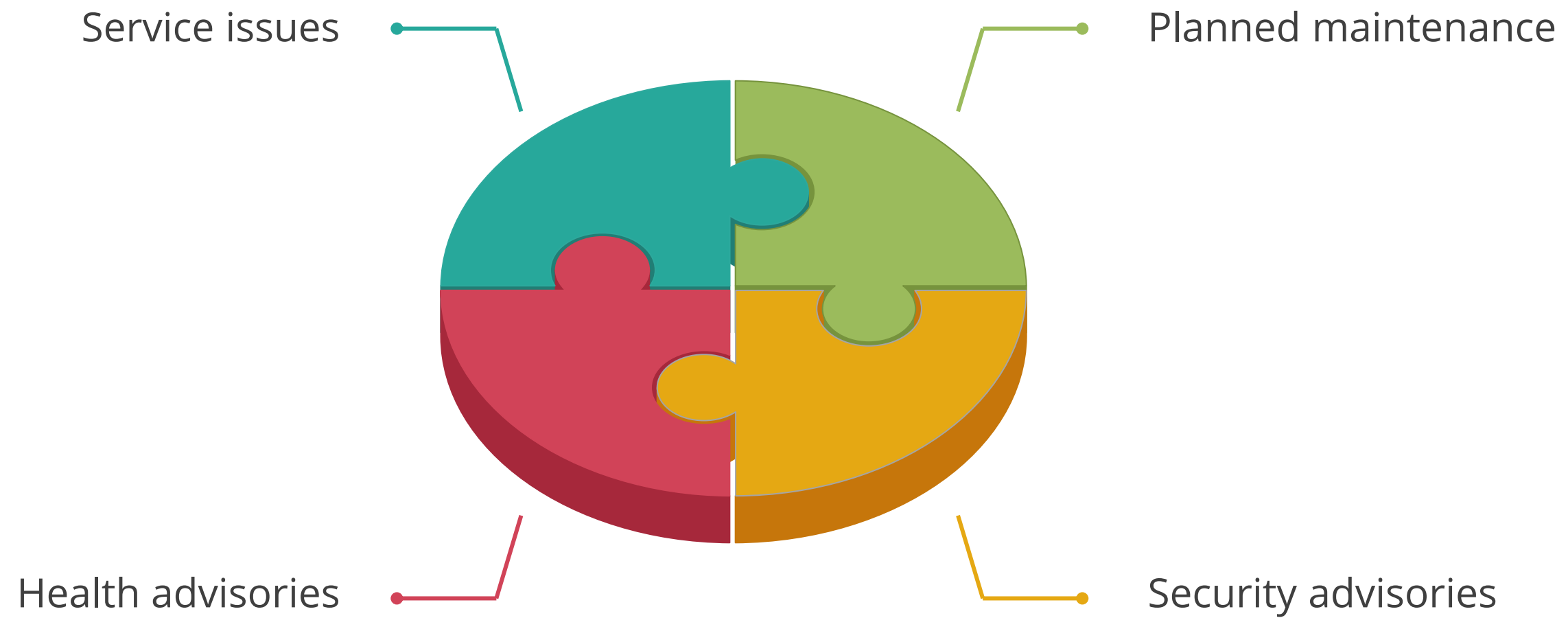
Azure Service Health



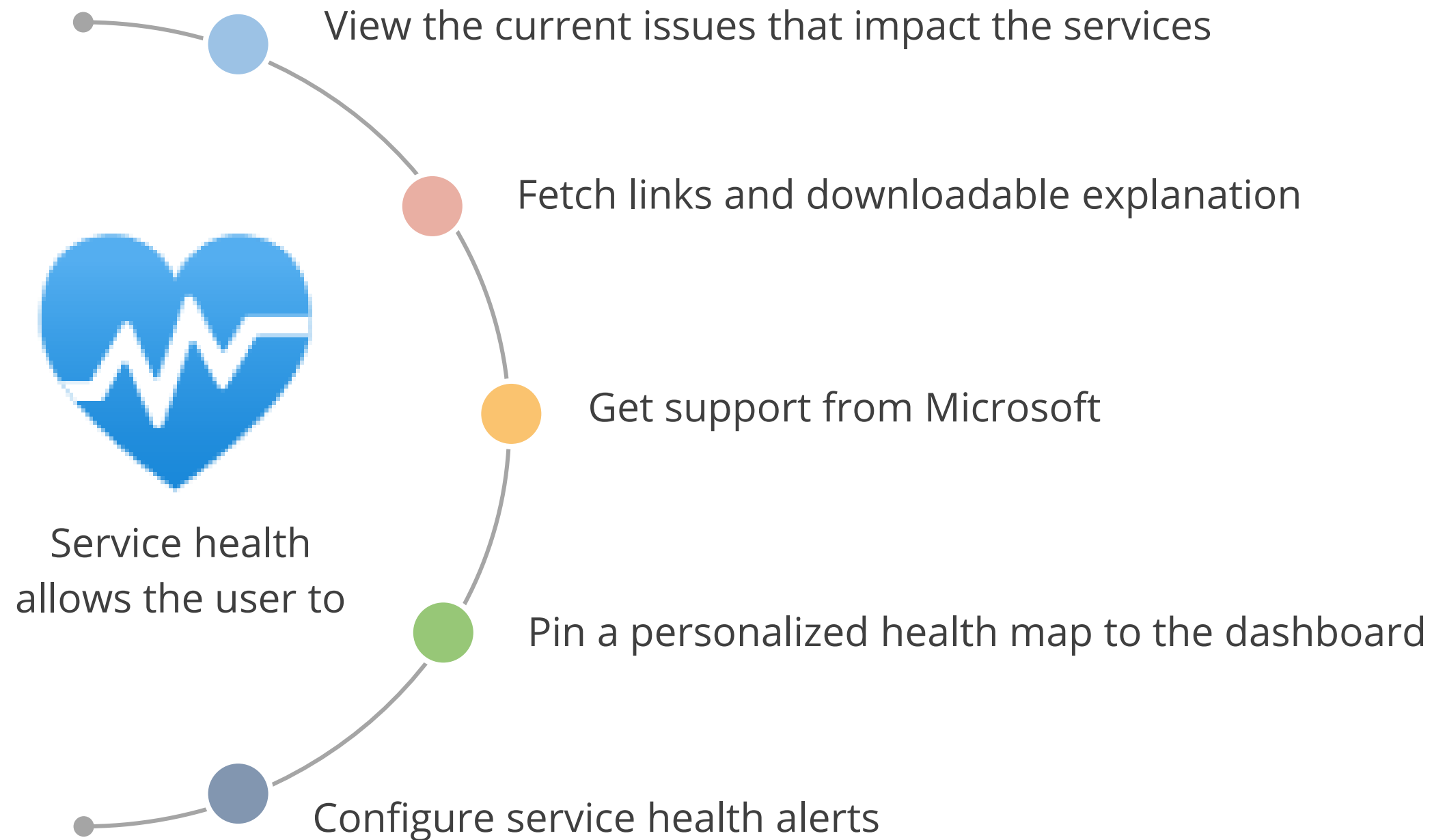
- When it comes to service availability, the Microsoft Azure platform is quite transparent.
- Service Health blade provides a global map view of regions with service issues, reviews planned maintenance, is informed of health advisories, and looks at the health history.

Azure Service Health

Service health events are as follows:

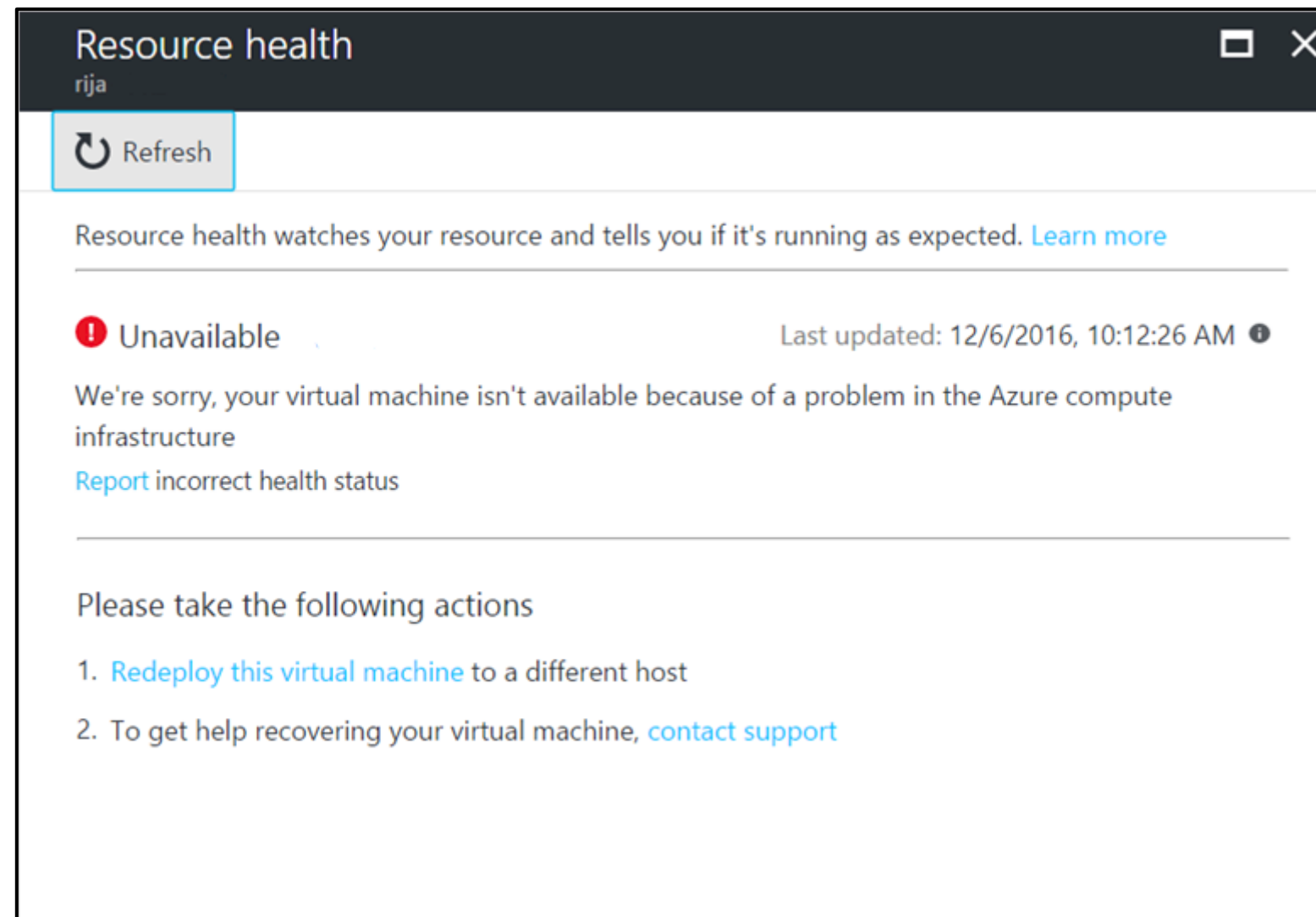


Azure Service Health



Azure Resource Health

Azure Resource Health helps diagnose and get support for service problems that affect Azure resources.



Azure Resource Health



- Resource definition and health assessment
- Health status
 - Available
 - Unavailable (includes platform events and non-platform events)
 - Unknown
 - Degraded
- Reporting of an incorrect status
- History information

Cost Monitoring

Monitoring Azure Costs

Cost monitoring is about establishing controls and business processes for reviewing the cloud spent to avoid any misuse and take advantage of new opportunities through flexibility provided by the cloud.



Cost Trade-offs

Consider these trade-offs between cost optimization and other aspects of design, such as security, scalability, resilience, and operability. An optimal design is not synonymous with a low-cost design. Low cost may incur additional risks.

Cost versus reliability

- Does the cost of high-availability components exceed the acceptable downtime?

Cost versus performance efficiency

Factors impacting performance:

- Fixed or consumption-based provisioning
- Azure regions
- Caching
- Batch or real-time processing

Cost Trade-offs

Cost versus security

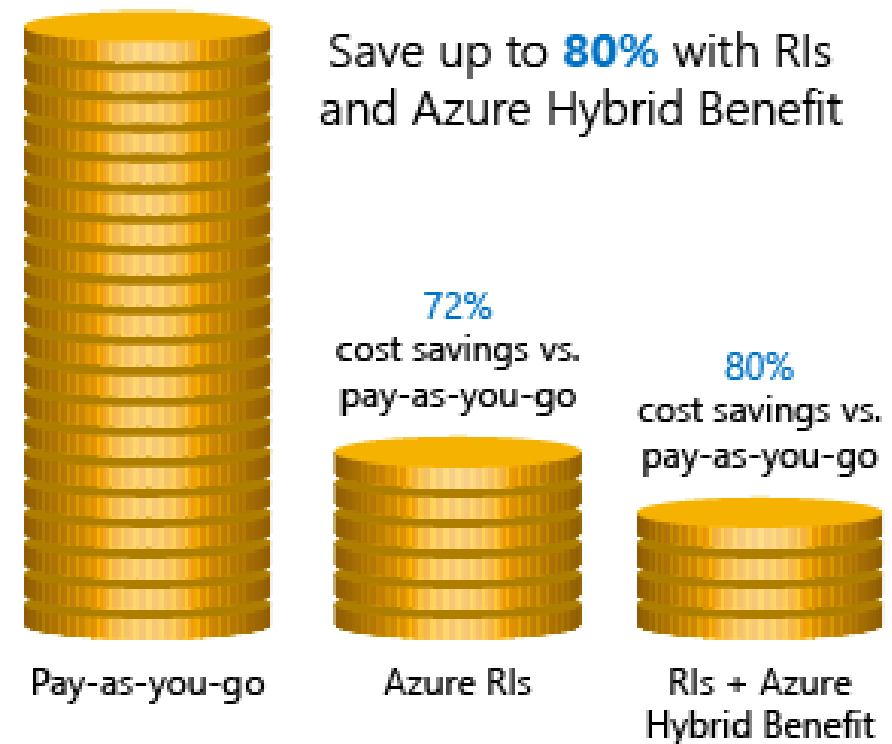
Increasing the security of the workload will increase the cost.

For example, for specific security and compliance requirements, deploying to differentiated regions will be more expensive. Premium security features can also increase the cost.

Cost versus operation excellence

Investing in systems monitoring and automation might increase the cost initially, but eventually, over a period, it can reduce cost.

Cost Savings



- **Azure Reservations:** These help users save money by allowing them to pay for services in advance.
- **Azure Hybrid Benefits:** With Software Assurance, a user can use on-premise licenses for Windows Server and SQL Server.
- **Azure Credits:** These are the benefit of a monthly credit that allows a user to try out, build, and test new Azure solutions.
- **Regions:** A user must choose low-cost locations and regions.

Report on Spend

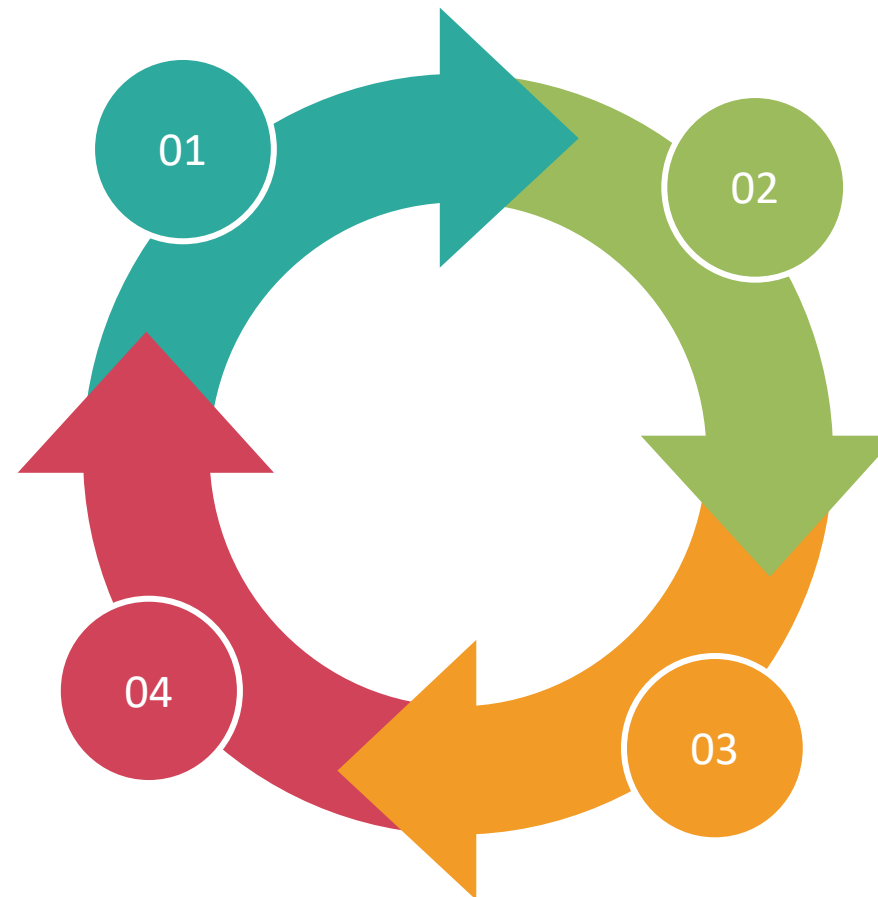
Azure provides tools to create cost reports:

Azure Advisor Cost Analysis tool

Provides an overview of spends over a period to help understand the spend trend

Consumption APIs

Are provided by Azure, so that a user can write custom tools and scripts to track costs over time



Azure Advisor recommendations

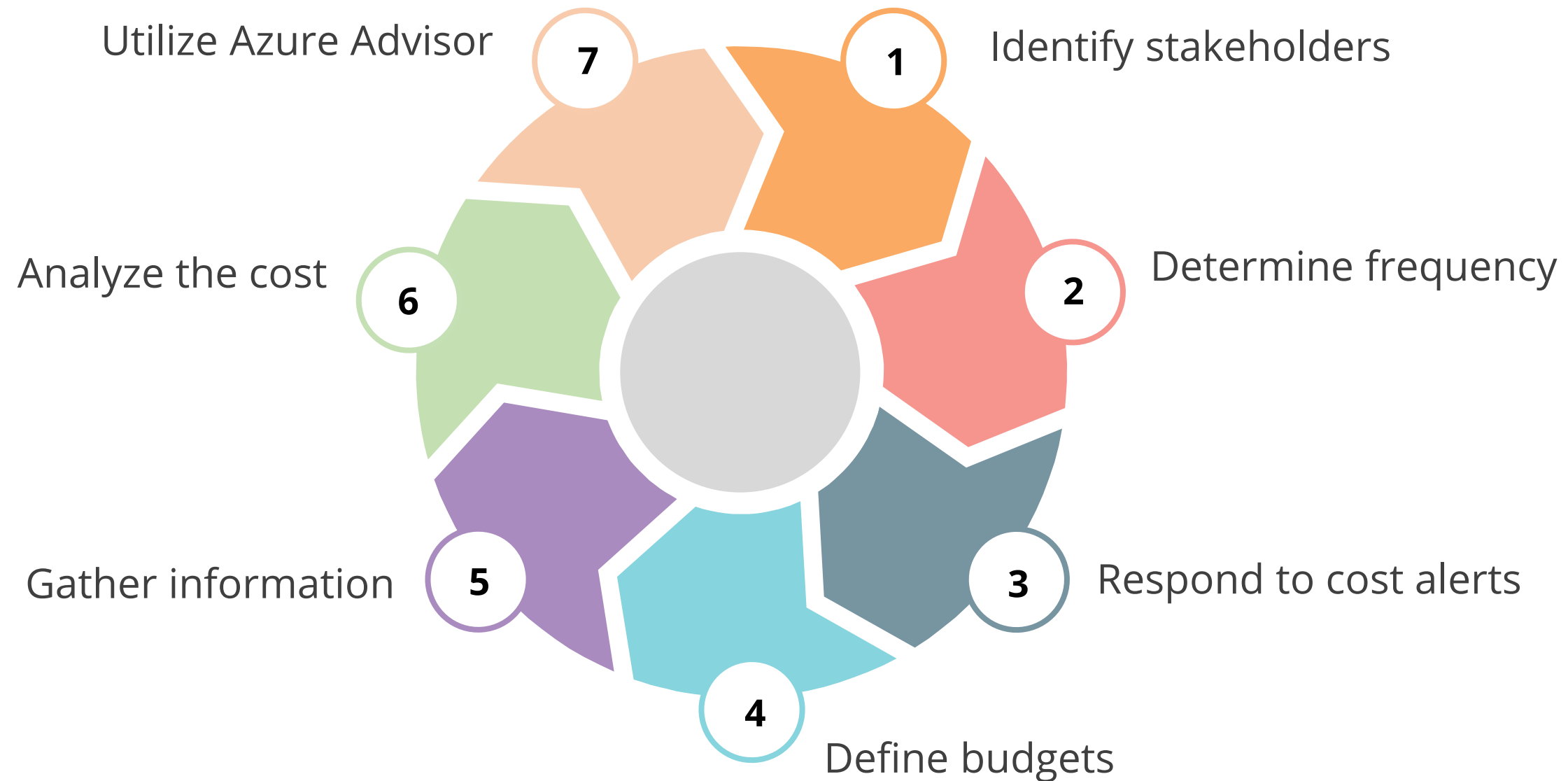
Highlights over-provisioned services and recommends ways to lower costs

Power BI Desktop

Connects to billing data from Azure Cost Management

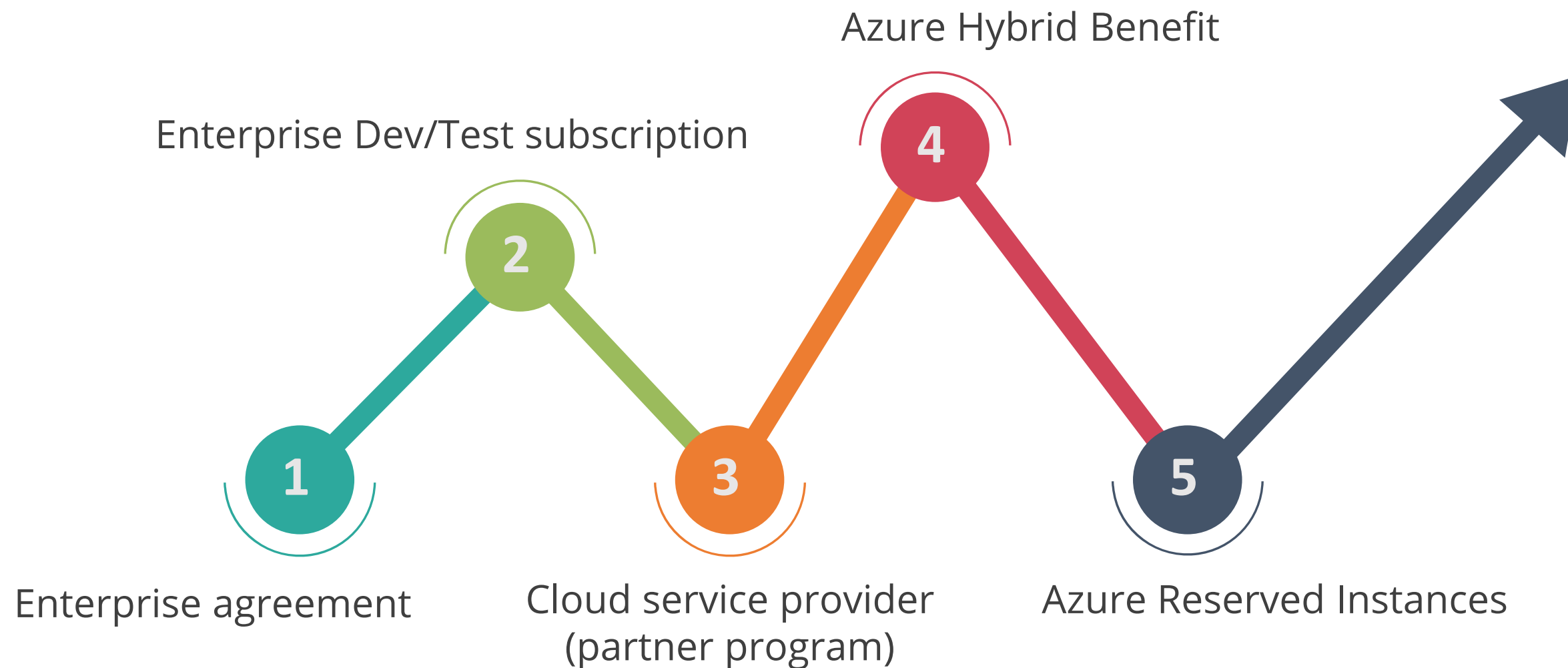
Monitoring Azure Costs

To monitor Azure cost, you need to:



Optimizing Azure Costs

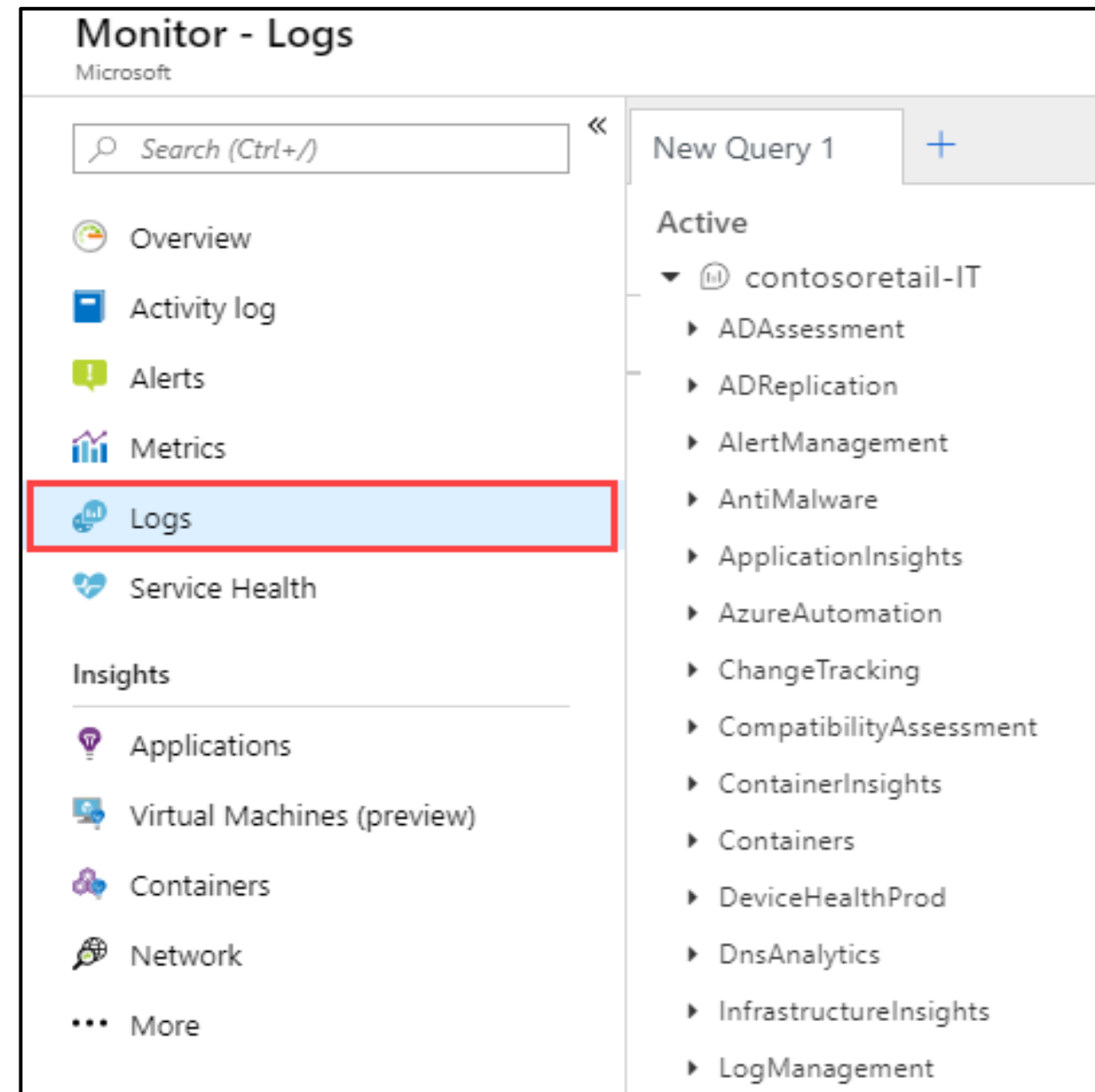
Consider the following methods of managing pricing:



Advanced Logging

Log Analytics

Log analytics help collect and analyze data generated in the cloud and on-premise systems.



Connected Sources

Connected sources are the computers and other resources that generate data collected by Log Analytics.

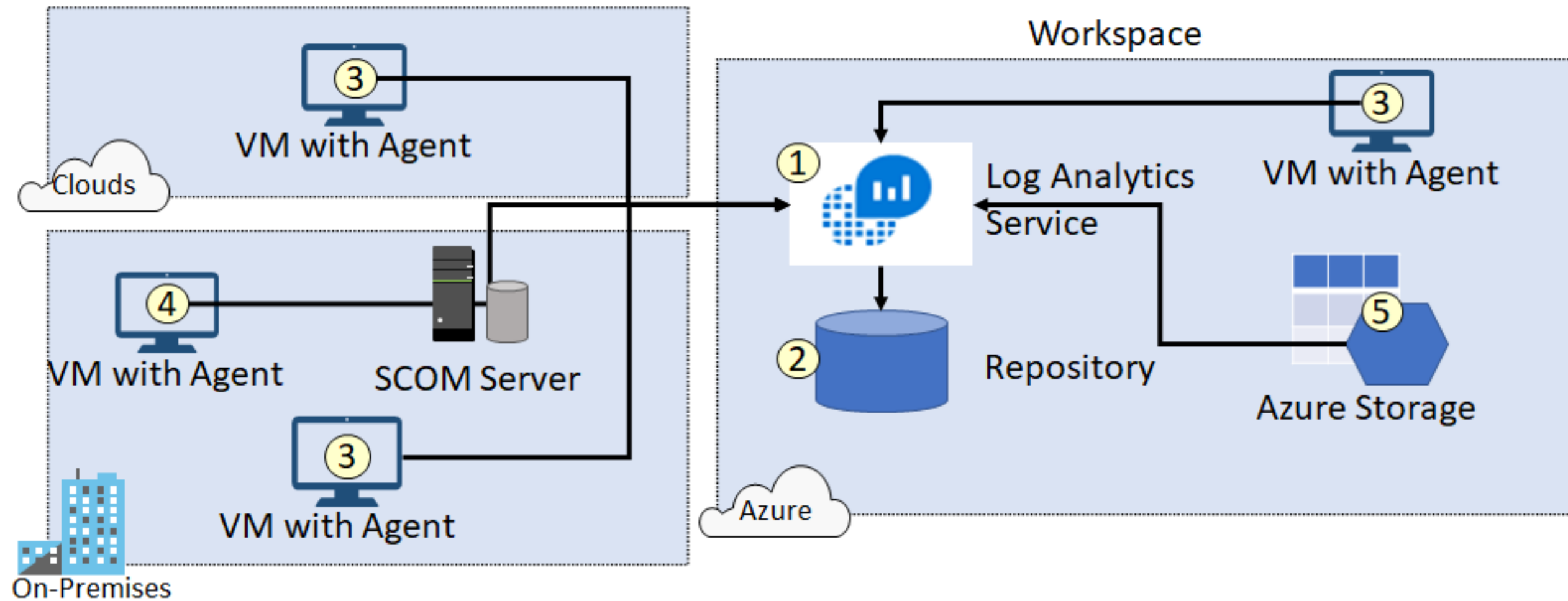


image source: <https://docs.microsoft.com/en-in/>

Data Sources

Data sources represent the data collected from connected sources.

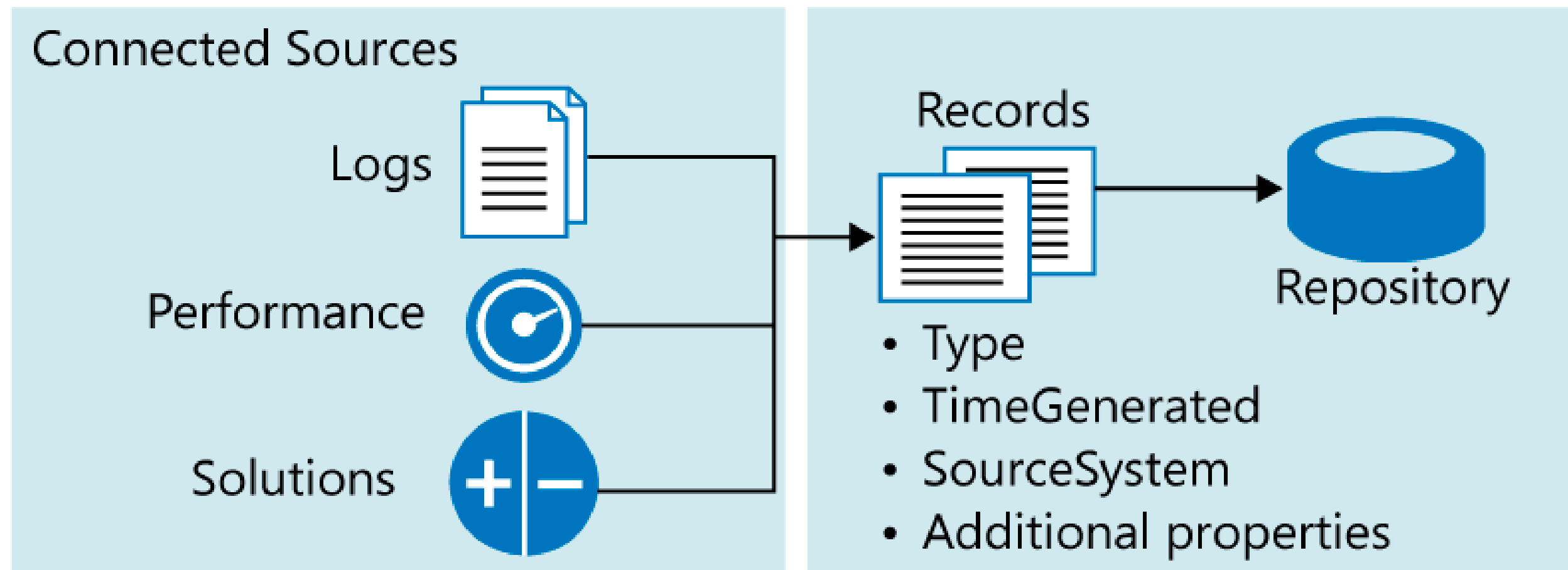


image source: <https://docs.microsoft.com/en-in/>

Log Analytics Querying

Log Analytics provides a query syntax to quickly retrieve and consolidate data in the repository.

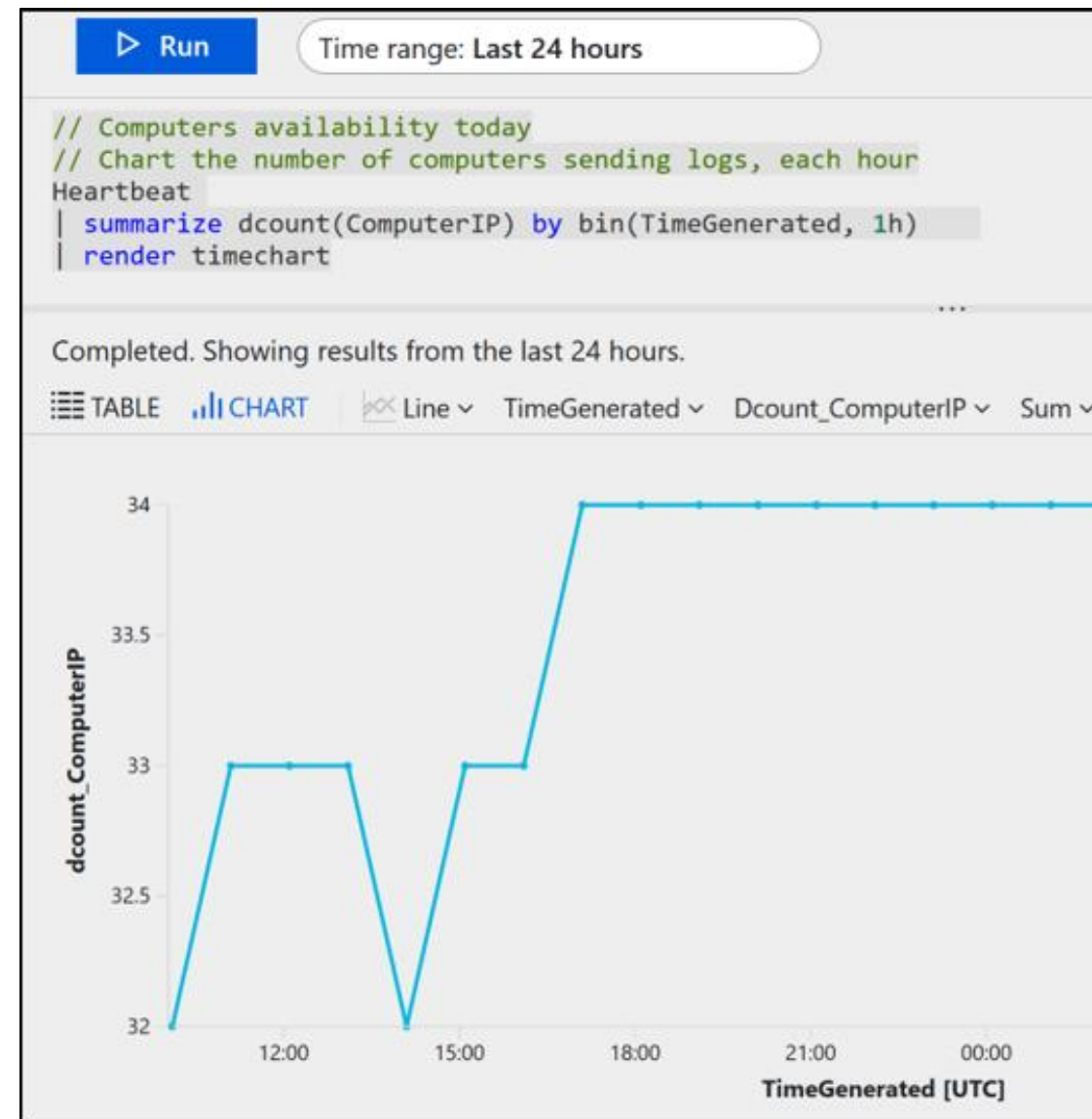


image source: <https://docs.microsoft.com/en-in/>

Query Language Syntax

A query's basic structure is a source table followed by a series of operators separated by the pipe character (|).

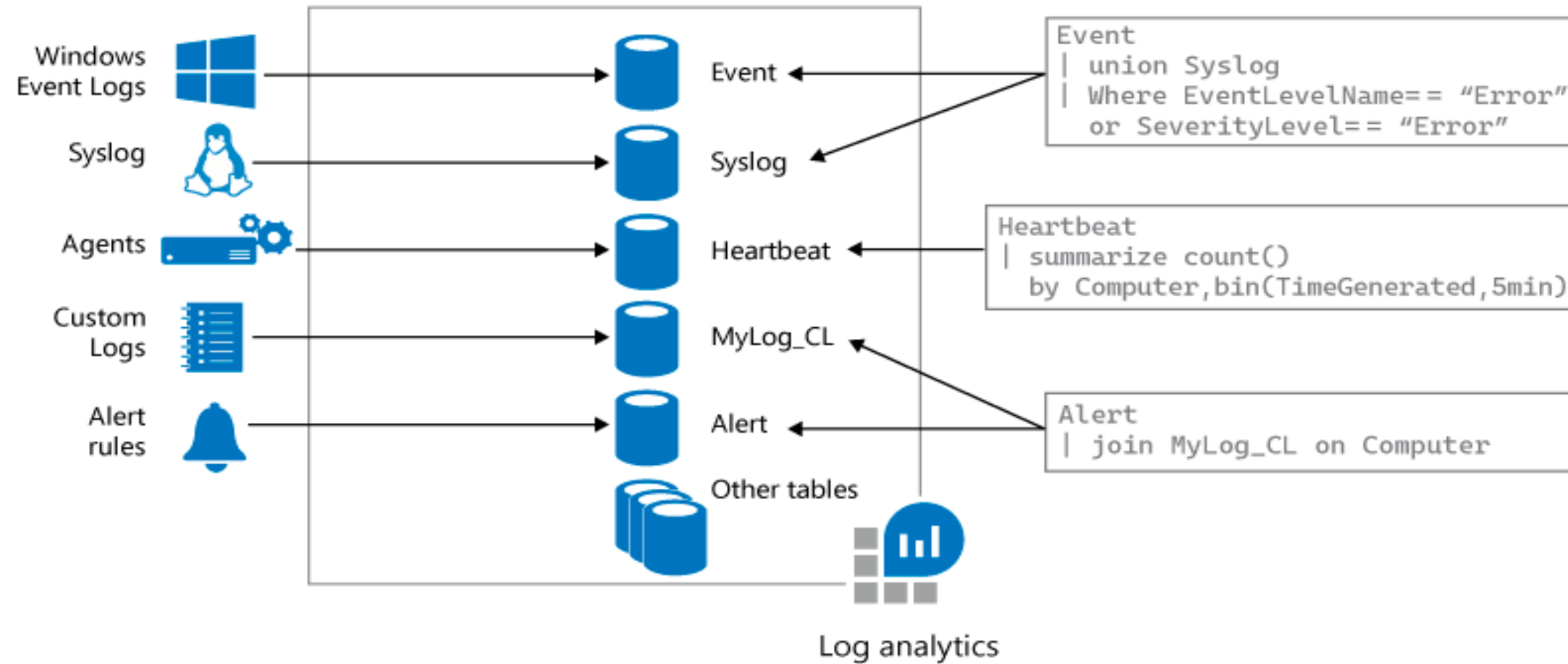
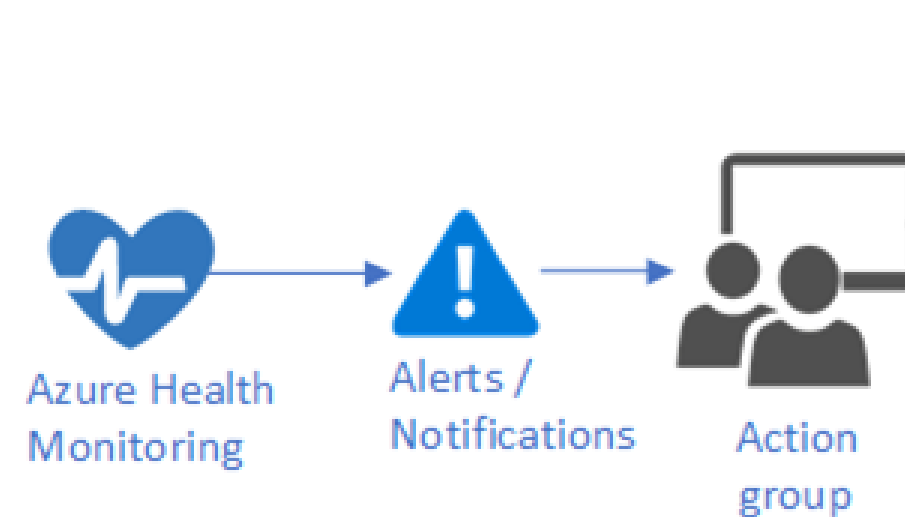


image source: <https://docs.microsoft.com/en-in/>

Choose a Mechanism for Event Routing and Escalation

Action Groups

An action group is a collection of notification preferences, defined by the owner of an Azure subscription.



Azure Monitor and Service Health alerts use action groups to notify users that an alert has been triggered.

Action Types

Add action group

Action group name * ⓘ
Sample action group ✓

Short name * ⓘ
SampleAG ✓

Subscription * ⓘ
Visual Studio Enterprise ▼

Resource group * ⓘ
Default-ActivityLogAlerts (to be created) ▼

Actions

Action name *	Action Type *
Unique name for the action	Select an action type ^

- Automation Runbook
- Azure Function
- Email Azure Resource Manager Role
- Email/SMS/Push/Voice
- ITSM
- LogicApp
- Secure Webhook
- Webhook

The seven action types in Azure portal are:

- Automatic Runbook
- Azure Function
- Email Azure Resource Manager role
- Email/SMS/Push/Voice
- ITSM
- Logic App
- Webhook

Alerts

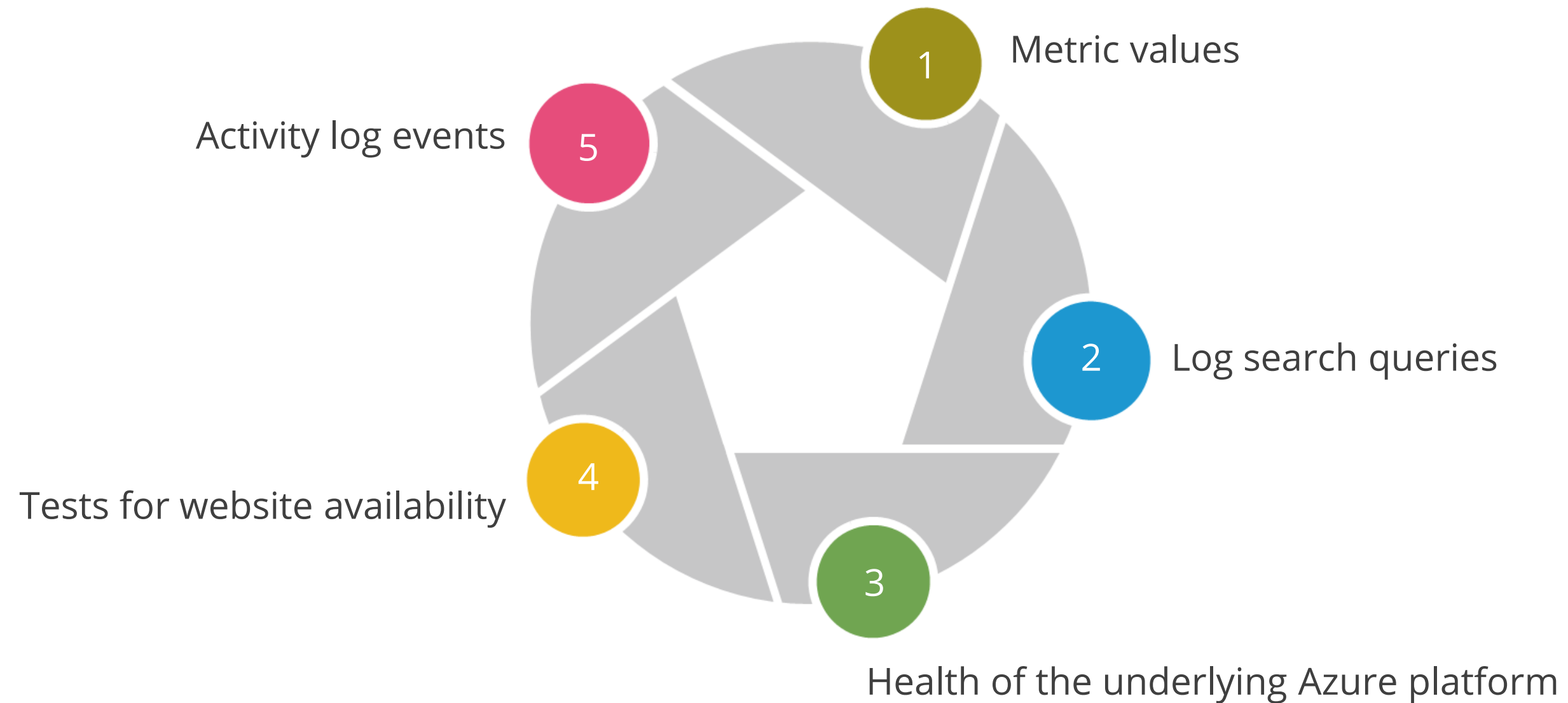
Alerts proactively notify a user when important conditions are found in the monitoring data.

Monitor alerts offer the following benefits:

- Better notification system
- A unified authoring experience
- Viewing of log analytics in the Azure portal
- Separation of fired alerts and alert rules
- Better workflow

Managing Alerts

Alerts can be set based on the following criteria:



Alert States

The key elements of alert states are:

New

The issue has just been detected and has not yet been reviewed.

Acknowledged

An administrator has reviewed the alert and started working on it.

Closed

The issue has been resolved. After an alert has been closed, the user can reopen it by changing it to another state.

Alert Rules

Alert rules are separated from alerts and the actions that are taken when an alert fires.



These are the key attributes of an alert rule:

- Target source
- Signal
- Criteria
- Alert name
- Alert description
- Security
- Action

Assisted Practice

Creating Action Groups

Duration: 10 Min.

Problem Statement:

As an Azure architect, you've been asked to provide your company with an Azure logging and monitoring solution that can be used by Azure Monitor and Service Health alerts to notify users when an alert has been triggered.

Assisted Practice: Guidelines

Steps to create an action group are:

1. Log in to your Azure portal
2. Search for and select Monitor
3. Select Alerts and then select Manage actions
4. Add an action group and fill in the fields



Assisted Practice

Azure Alerts

Duration: 10 Min.

Problem Statement:

As an Azure architect, you've been asked to provide your organization with an Azure logging and monitoring solution that can be utilized to warn you when issues with your infrastructure or application are discovered utilizing your Azure Monitor monitoring data. It should also enable you to spot and fix problems before your system's users become aware of them.

Assisted Practice: Guidelines

Steps to create Azure alerts are:

1. Log in to your Azure portal
2. Search for and select Monitor
3. Create an Azure alert



Assisted Practice

Azure Monitor

Duration: 10 Min.

Problem Statement:

As an Azure architect, you've been asked to create a proof of concept of monitoring virtual machine performance.

Assisted Practice: Guidelines

Steps to create Azure monitor are:

1. Deploying an Azure virtual machine
2. Creating a Log Analytics workspace
3. Enabling the Log Analytics virtual machine extension
4. Collecting virtual machine event and performance data
5. Viewing and querying collected data



Key Takeaways

- Azure Monitoring collects and analyzes data to assess the application's performance, health, and availability.
- Azure Resource Health helps diagnose and get support for service problems that affect your Azure resources.
- Log Analytics help collect and analyze data generated in the cloud and on-premise systems.
- An action group is a set of notification preferences set by the Azure subscription's owner.
- Alert rules are separated from alerts and the actions that are taken when an alert fires.



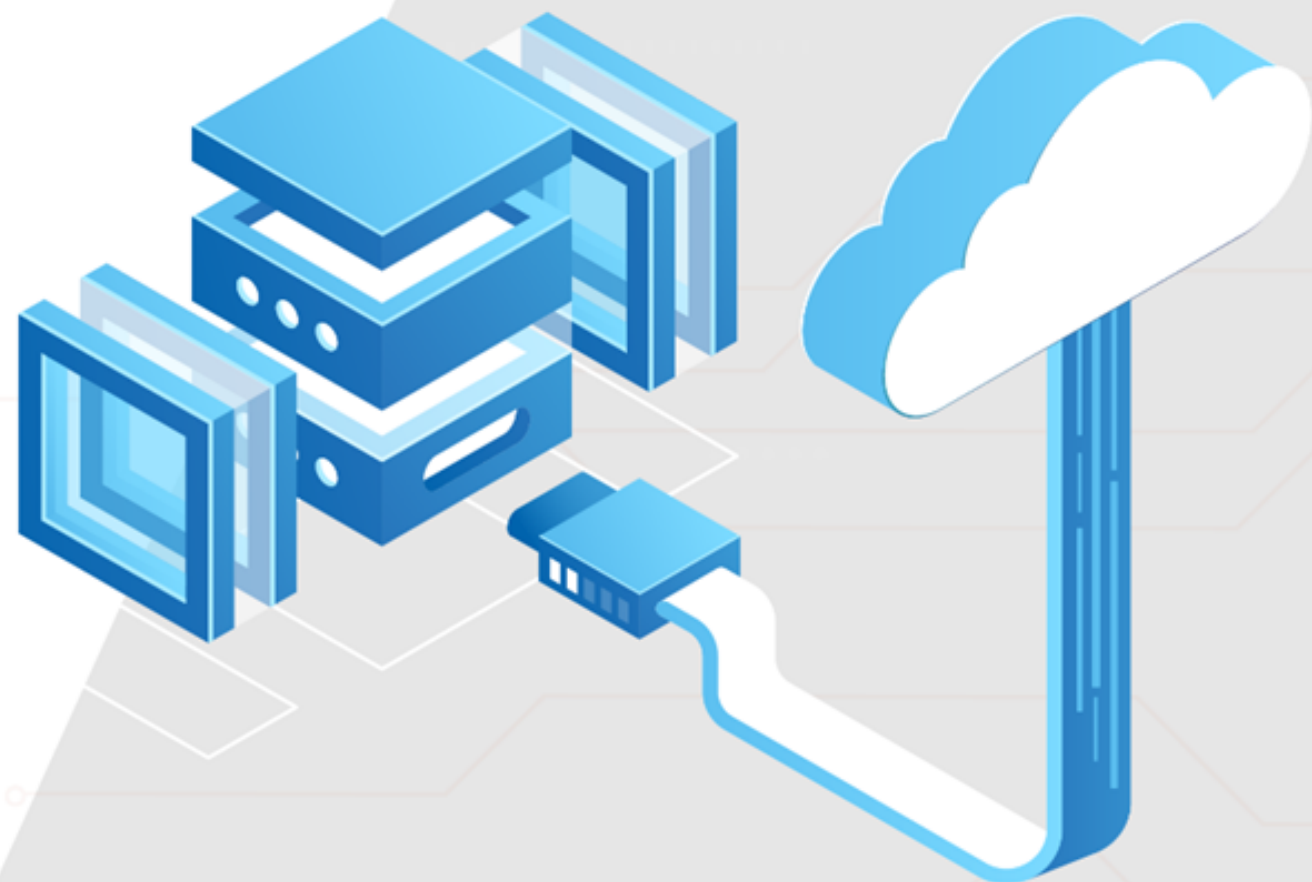


Project Agenda: To implement Azure Alert

Description: You have been given a project to design monitoring for a web application. You should be alerted whenever the HTTP 404 errors for the web crosses a threshold of 5. You also need to ensure that appropriate stakeholders are notified about the same. - monitoring – logging and monitoring.

Perform the following:

1. Going to the Azure Portal
2. Locating the Webapp to create an alert
3. Creating an Azure Alert



Thank you