Caltech | Center for Technology & Management Education

Post Graduate Program in Cloud Computing

Powered by simplilearn

Cloud Computing

Caltech | Center for Technology & Management Education

PG CC - Microsoft Azure Architect Technologies: AZ:303

Powerd by simplilearn

Implement cloud infrastructure monitoring

Learning Objectives

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

- Analyze Azure infrastructure security monitoring
- Monitor health and availability
- Initiate automated responses using action groups
- Configure and manage advanced alerts

A Day in the Life of an Azure Architect

You are working for an organization as a cloud operations manager.

You have been asked to suggest an azure solution that can help improve the availability and performance of your Azure applications and services.

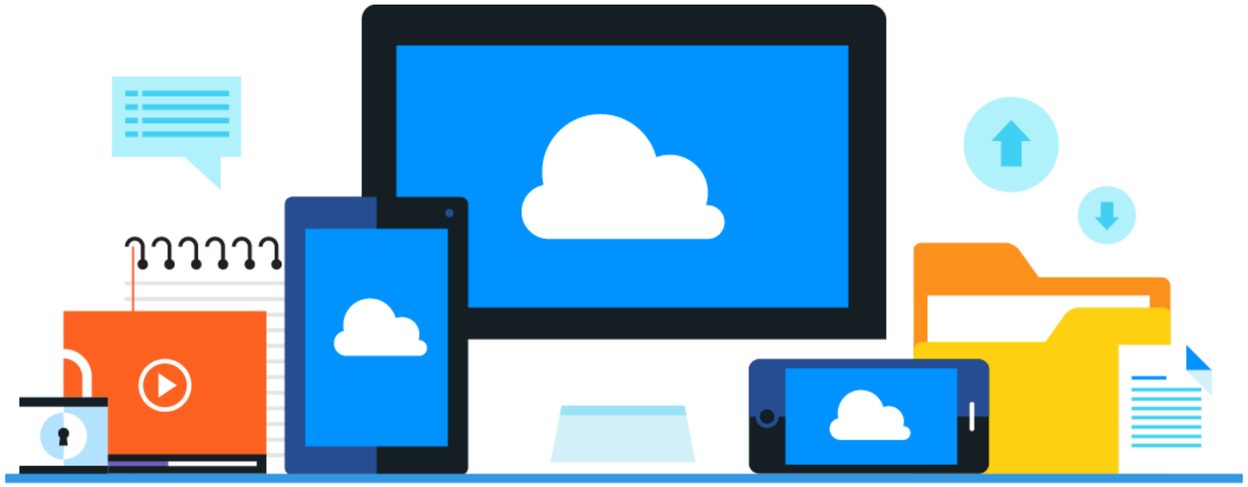
Also, based upon the performance your company should get notified when one of the metrics reaches a certain level. Basically, an alert should be triggered by Azure Monitor.

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

Azure Infrastructure Security Monitoring

Azure Monitoring

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

Security Posture

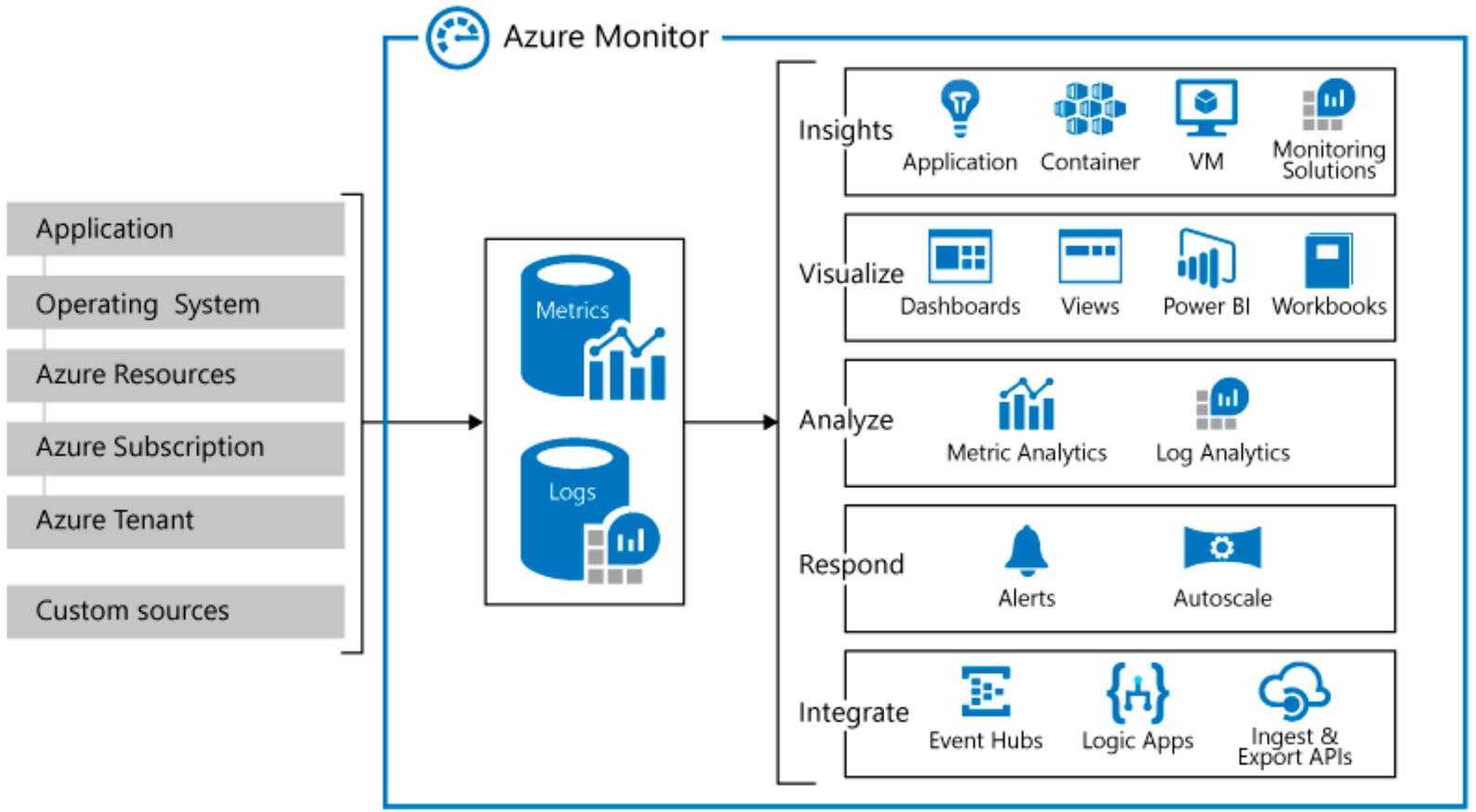
Azure Security Center enables a user to strengthen their security posture. It allows to view the security state of resources and any issues per resource type:

- Monitor computer resources and apps
- Monitor network resources
- Monitor data and storage resources
- Monitor identity and access resources

Azure Monitor

Azure Monitor Service

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



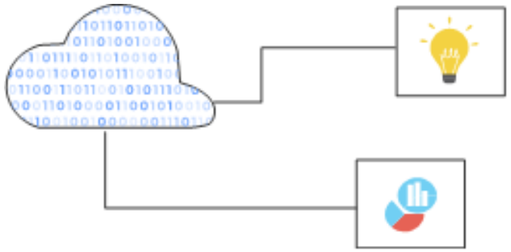
Key Capabilities

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 helping you understand the health, operation and performance of your system.

Explore Metrics



Query and Analyze Logs

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

Search Logs

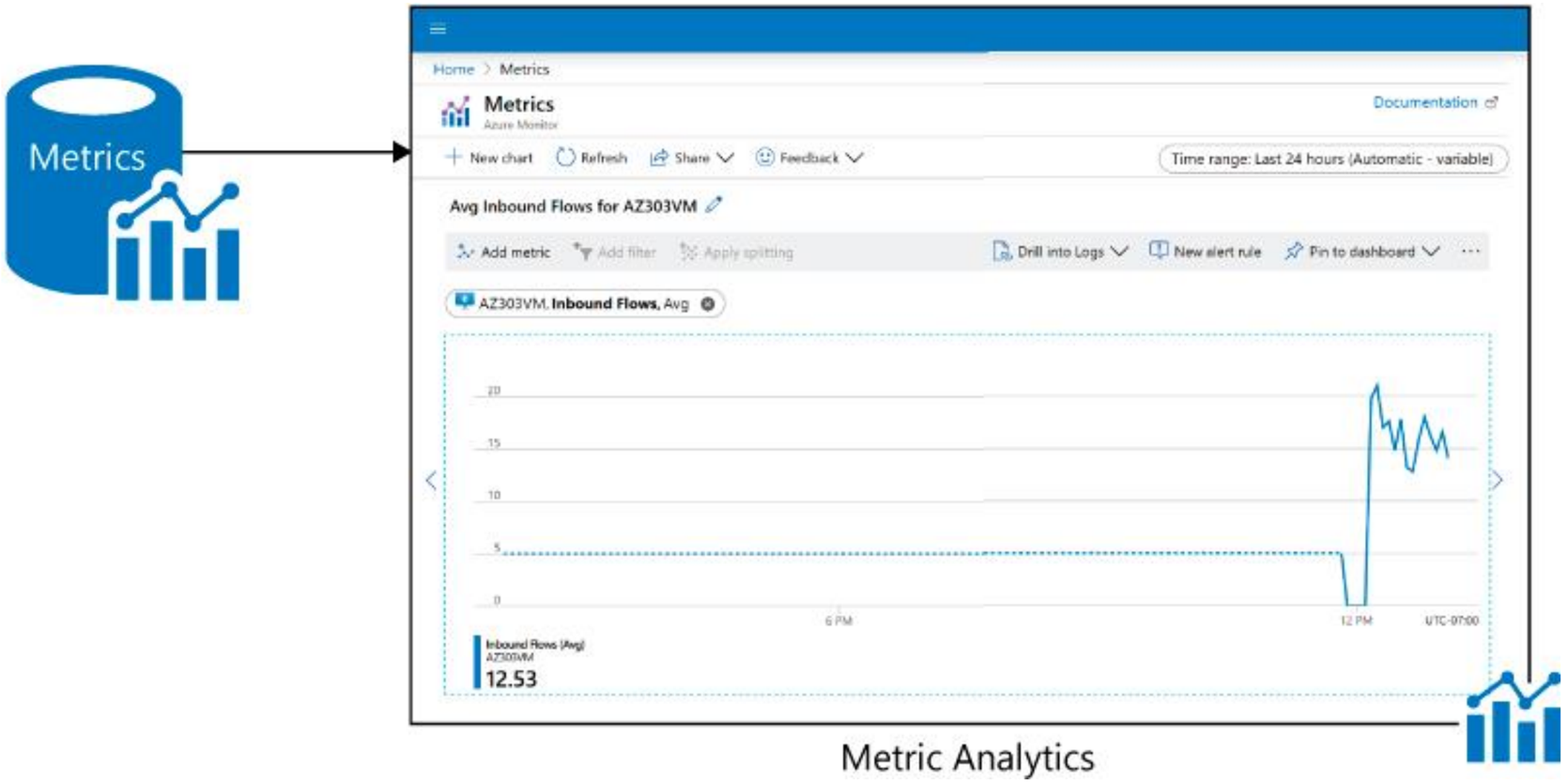
Setup Alerts and Actions

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

Create Alerts

Monitoring Data Platform

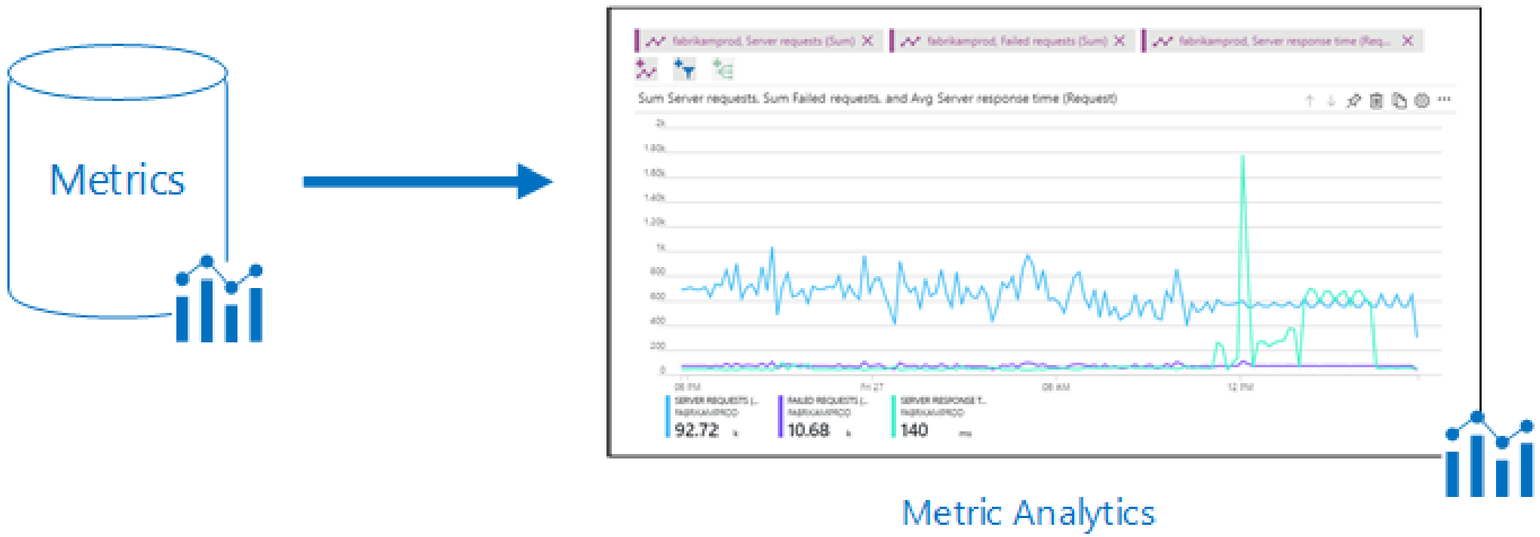
Azure includes multiple services that individually perform a specific role or a task in the monitoring space.



Metric Analytics

Metrics

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

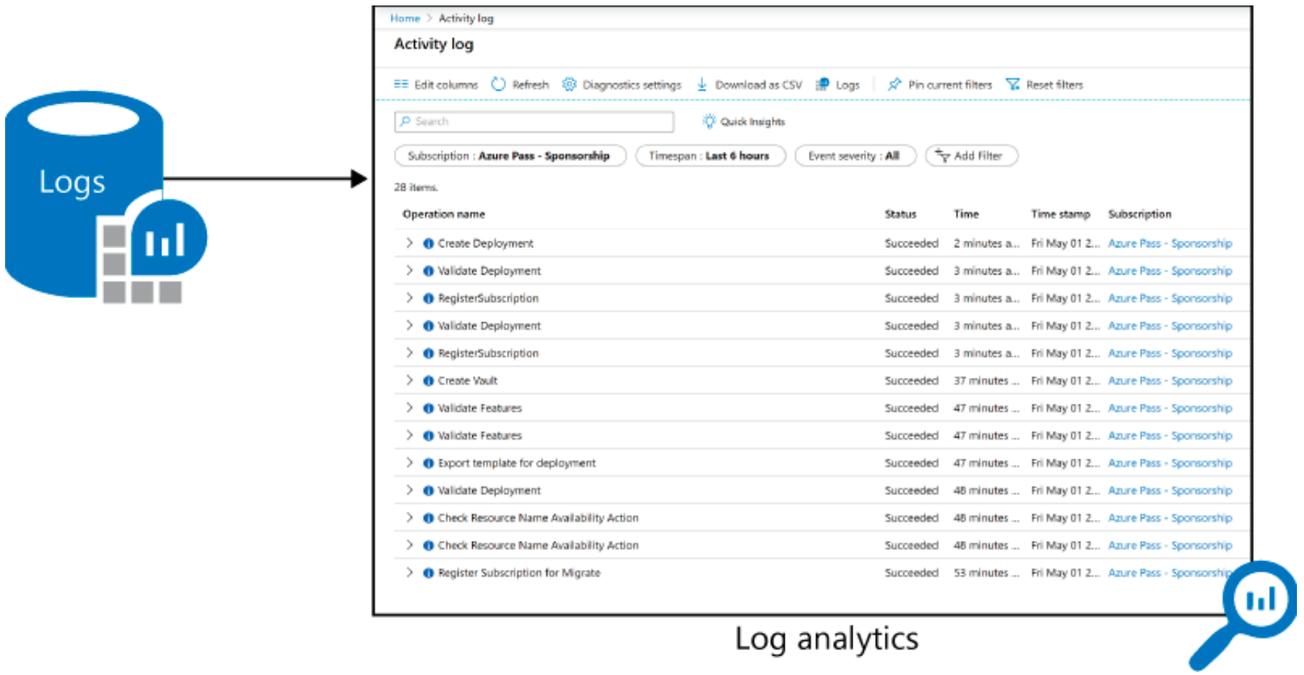


Metric Analytics

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 all be combined for analysis.

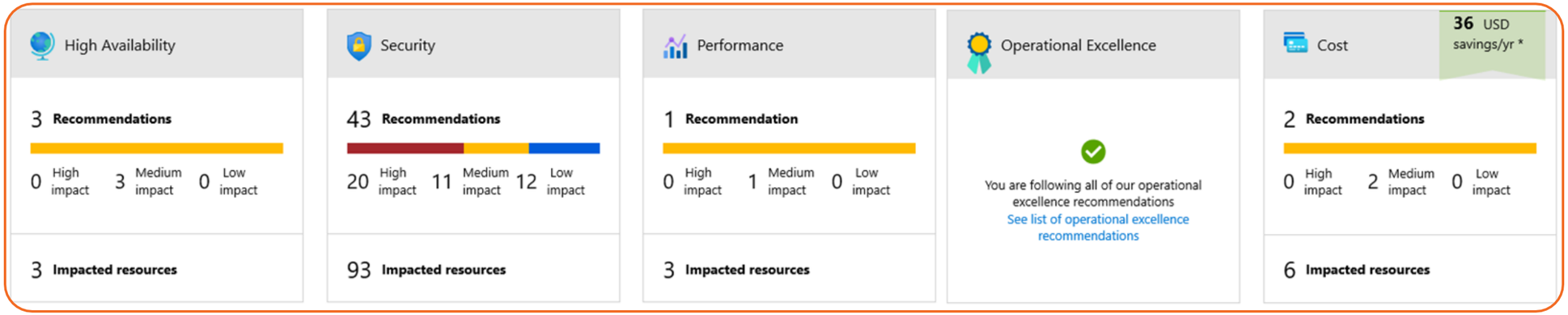
Data Types

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

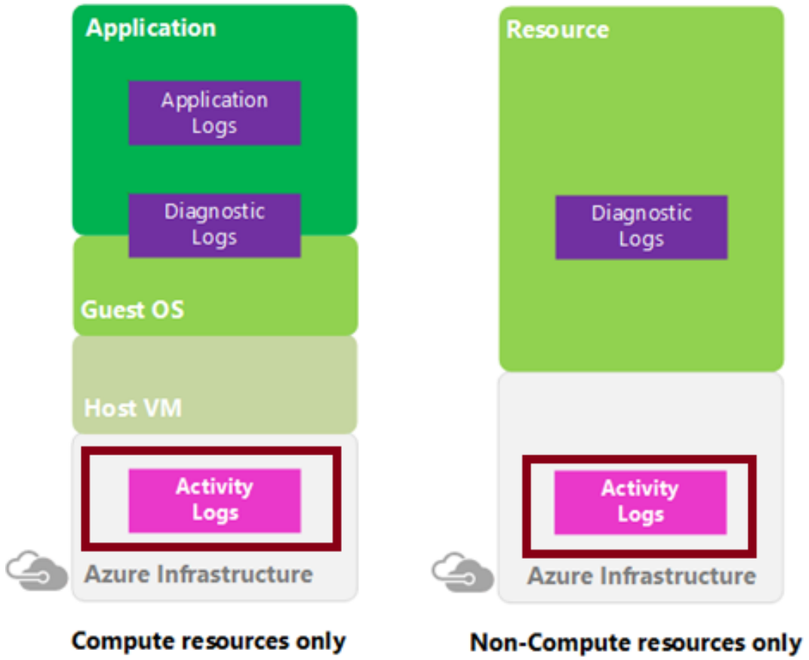
Azure Advisor

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



Activity Log

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

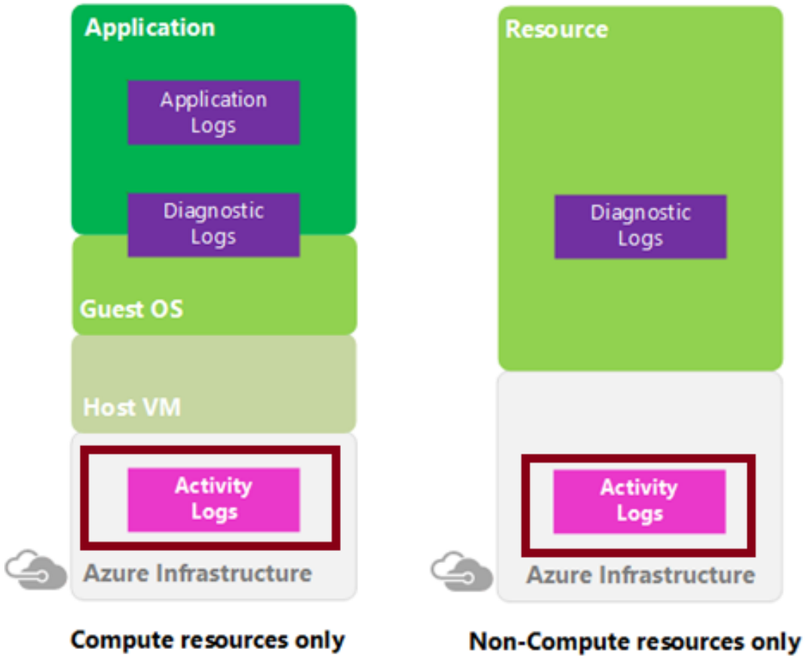


Activity log can determine

- 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 you research the operation?

Query the Activity Log

In the Azure portal, you can filter the activity log by the following filters:

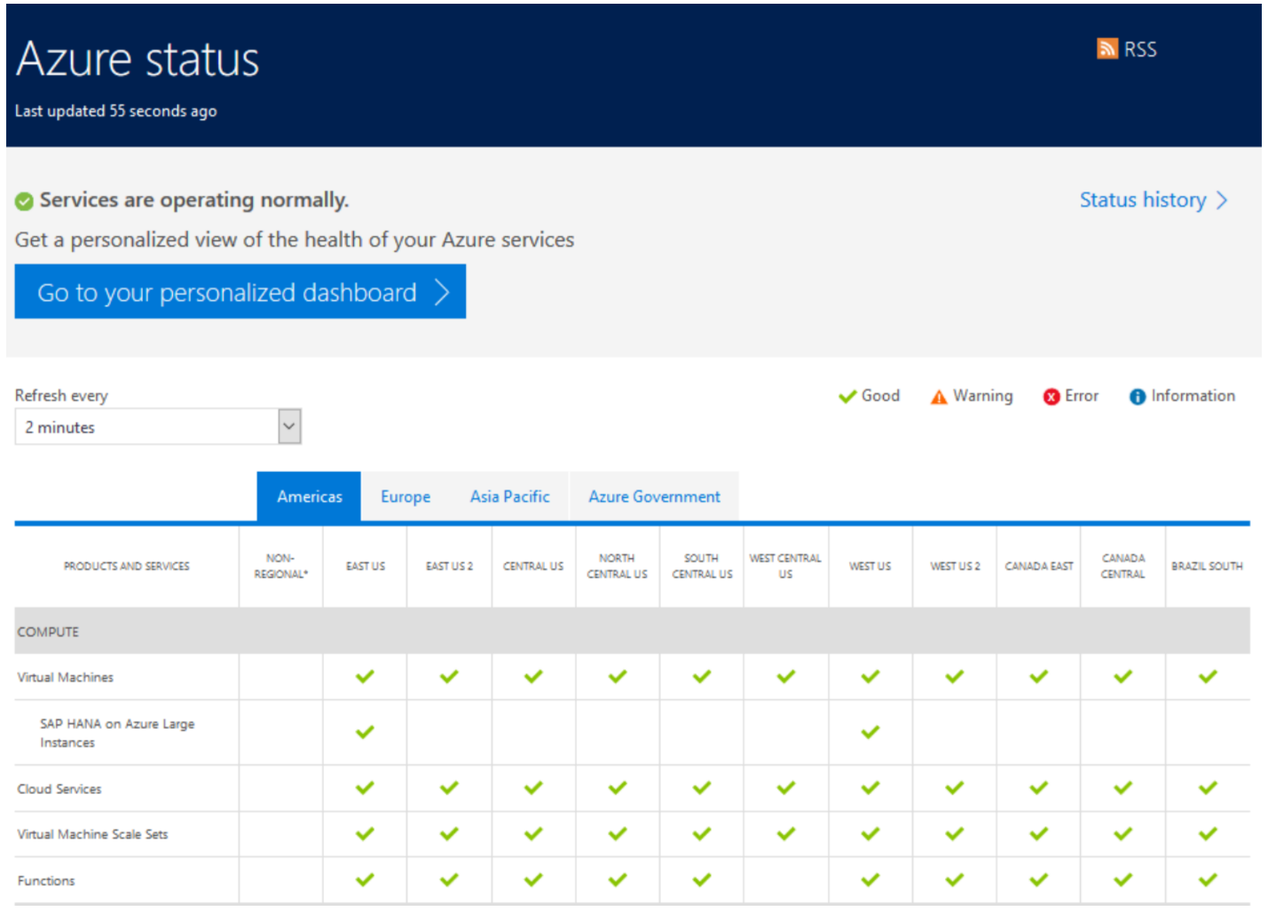


- Subscription
- Timespan
- Event severity
- Resource group
- Resource (name)
- Resource type
- Operation name
- Event initiated by
- Search

Health and Availability Monitoring

Azure Status

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

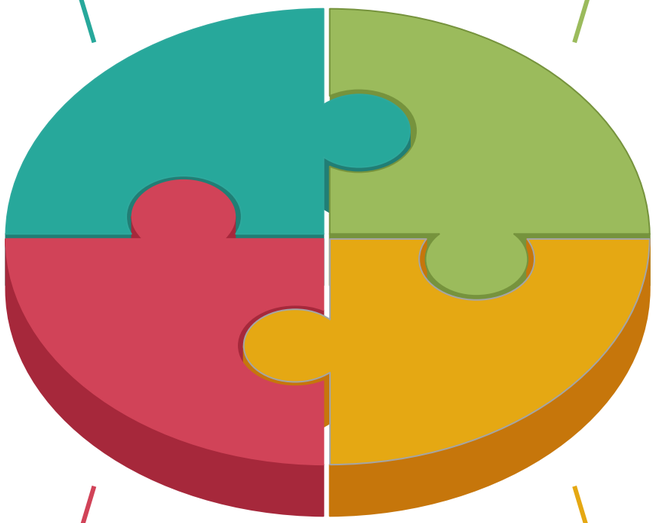


Azure Service Health

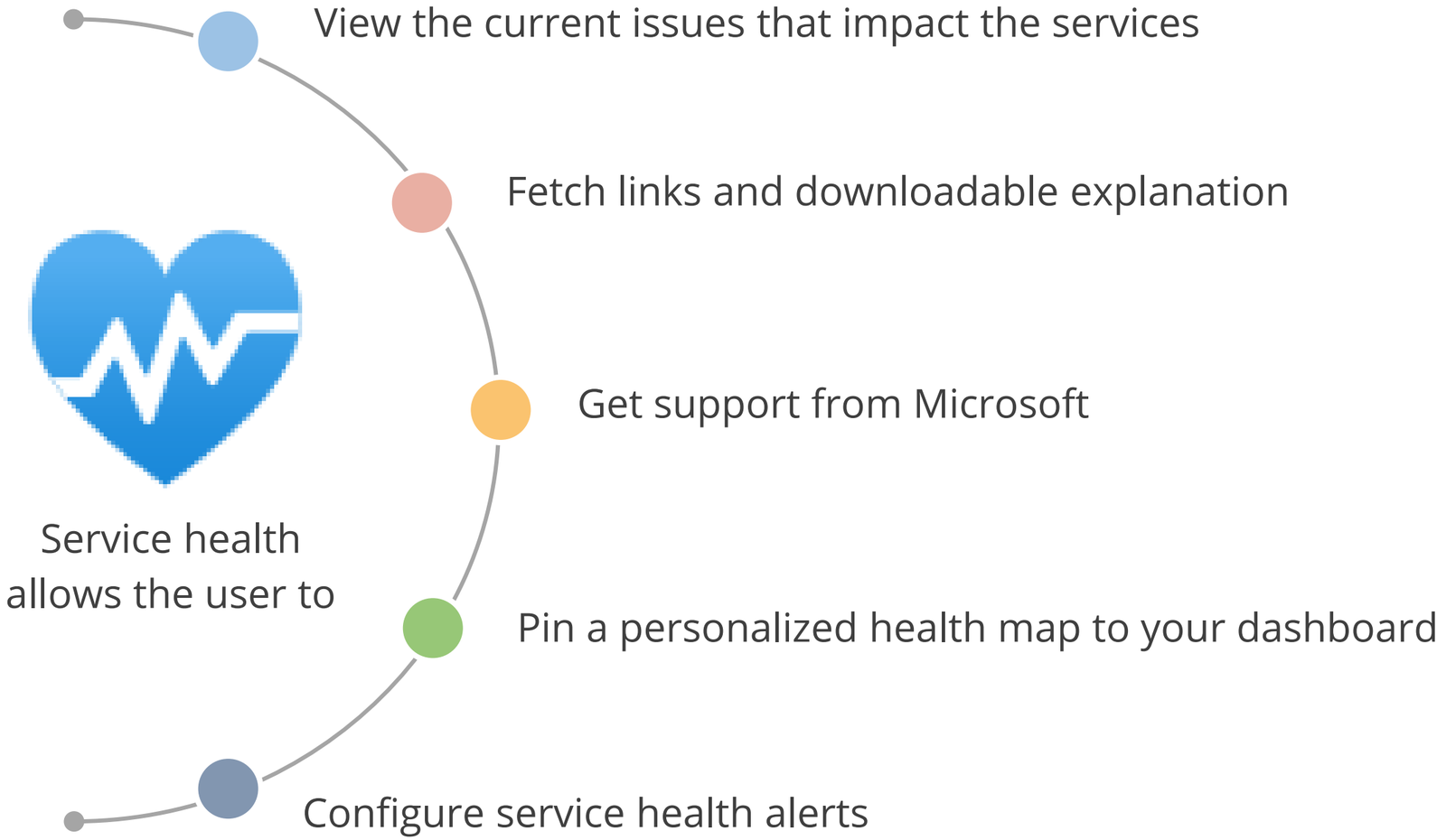
- When it comes to service availability, the Microsoft Azure platform is quite transparent.
- Service Health blade provides a global map view of regions with service issues, reviews planned maintenance, be informed of health advisories, and sees health history.

Azure Service Health

Service health events are as follows:

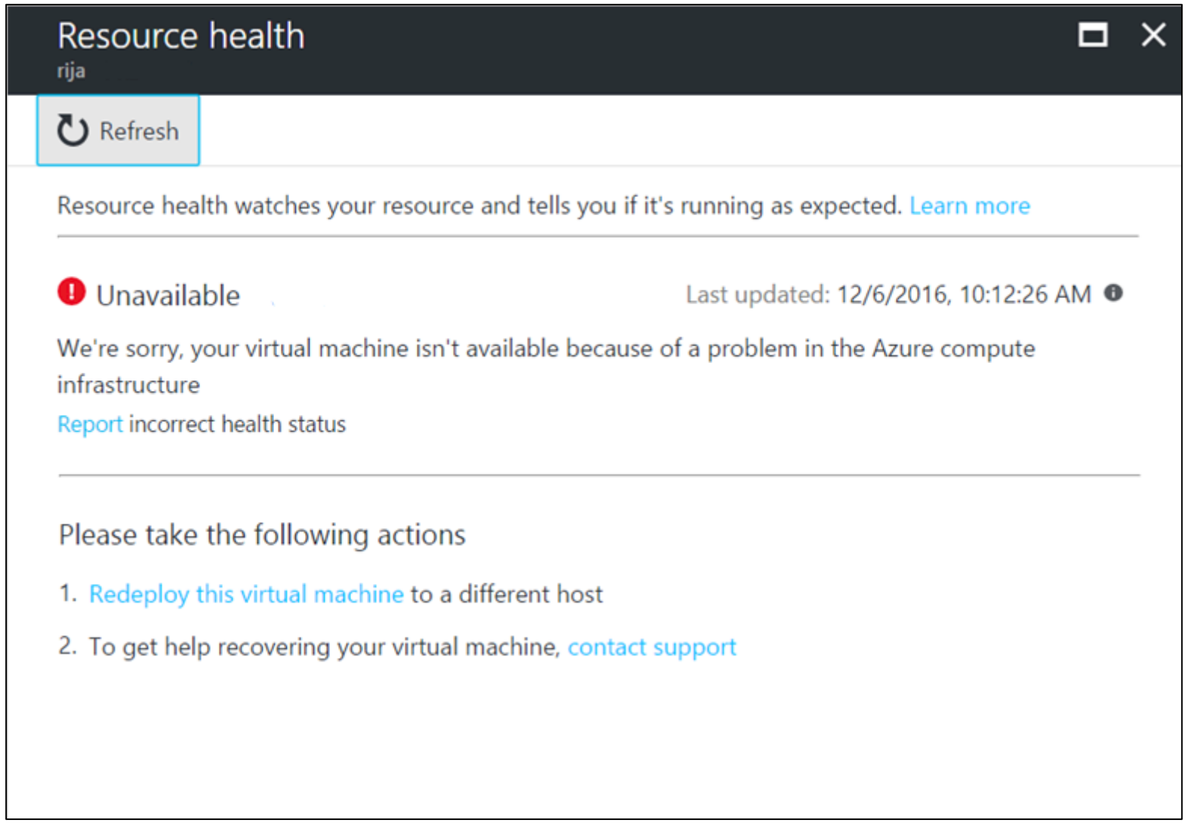


Azure Service Health



Azure Resource Health

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



Azure Resource Health

- Resource definition and health assessment
- Health status
  - Available
  - Unavailable (includes platform events and non-platform events)
  - Unknown
  - Degraded
- Reporting 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

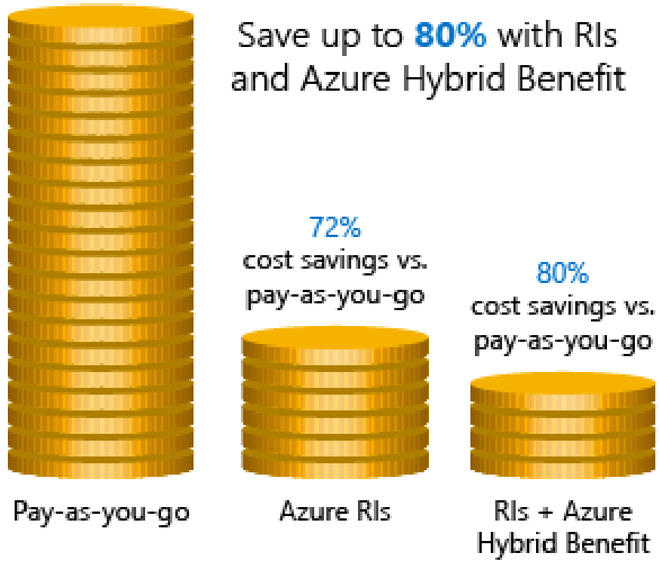
Increasing security of the workload will increase the cost.

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 over a period of time eventually reduce cost.

Cost Savings



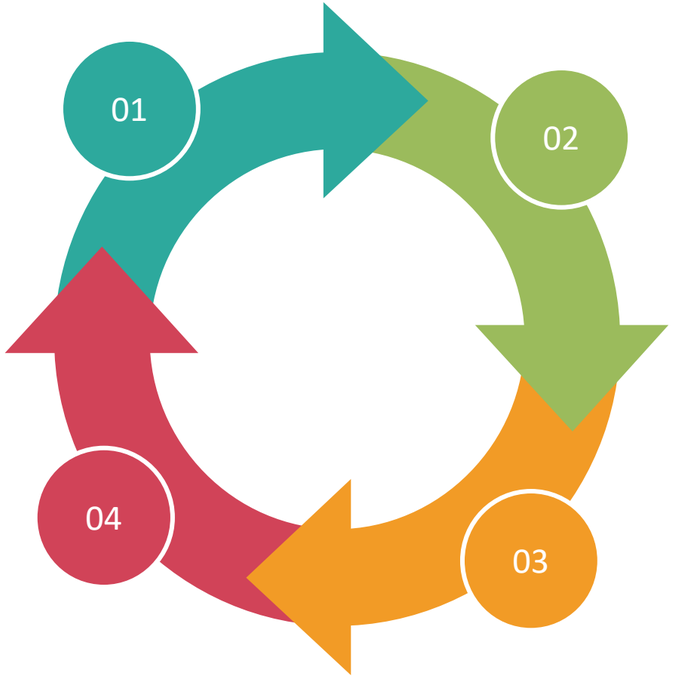
- **Azure Reservations:** helps you save money by allowing you to pay for services in advance
- **Azure Hybrid Benefits:** With Software Assurance, you can use on-premise licenses for Windows Server and SQL Server
- **Azure Credits:** Benefit of a monthly credit that allows you to try out, build, and test new Azure solutions
- **Regions:** 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



Azure Advisor recommendations

highlights over-provisioned services and recommends ways to lower costs

Consumption APIs

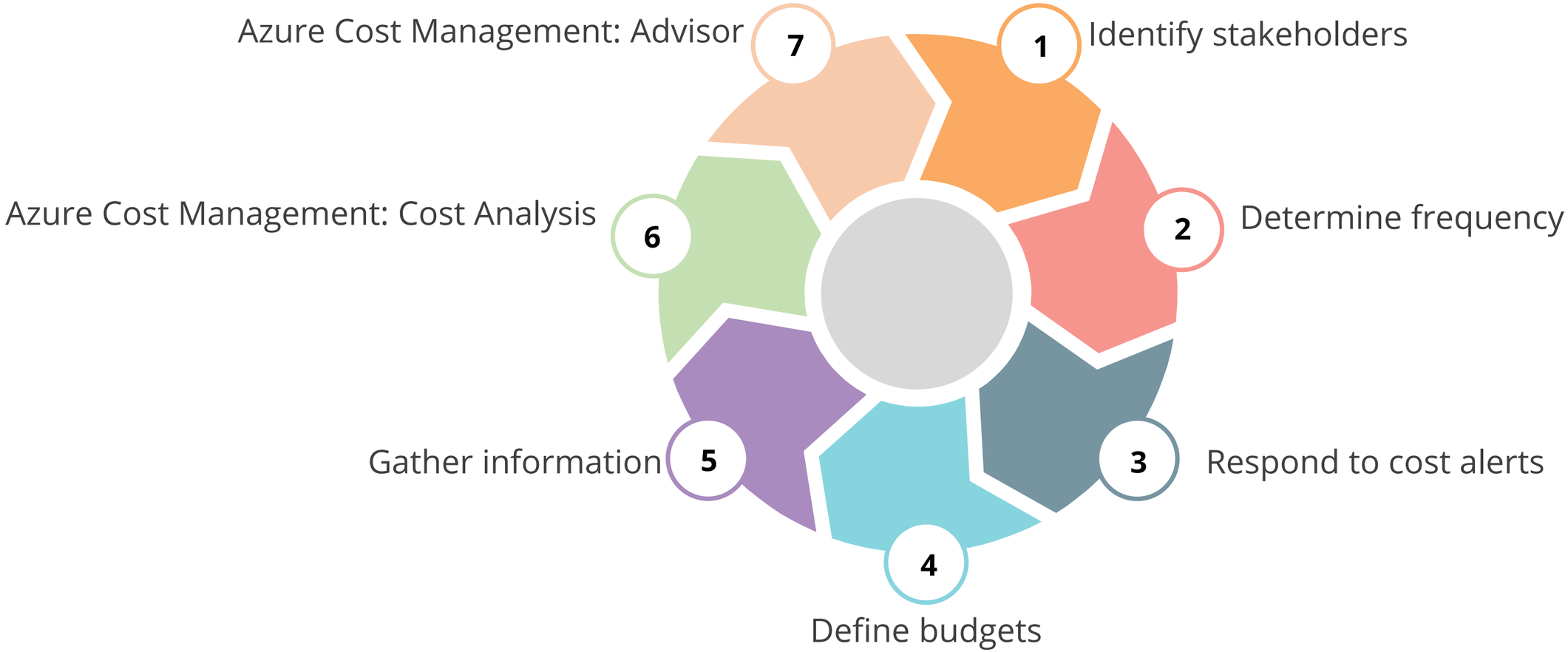
provided by Azure, so you can write custom tools and scripts to track costs over time

Power BI Desktop

connects to billing data from Azure Cost Management

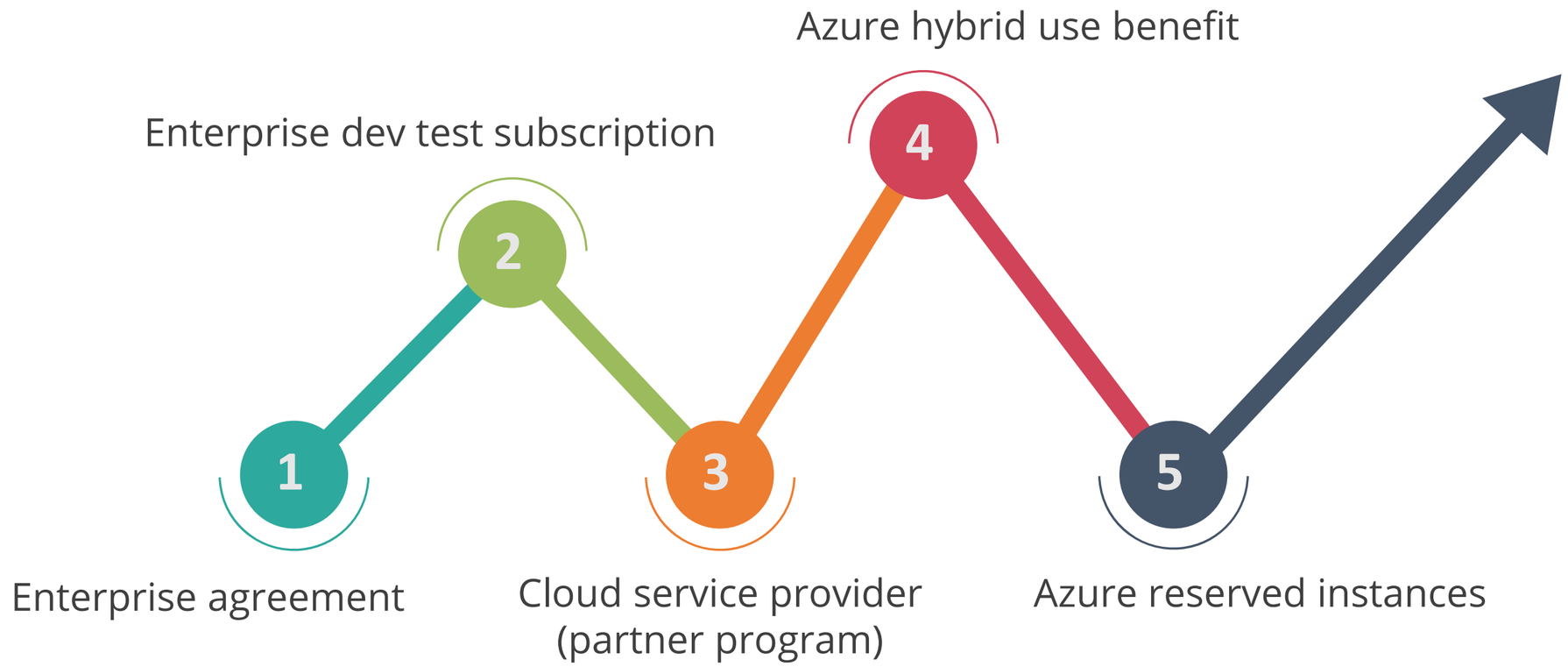
Monitoring Azure Costs

To monitor Azure cost, you need to:



Optimizing Azure Costs

Consider the following methods of managing pricing:



Assisted Practice

Azure Monitoring

Duration: 10 Min.

Problem Statement:

You've been given the task of setting up Azure monitoring in order to improve the availability and performance of your Azure applications and services.

Assisted Practice: Guidelines

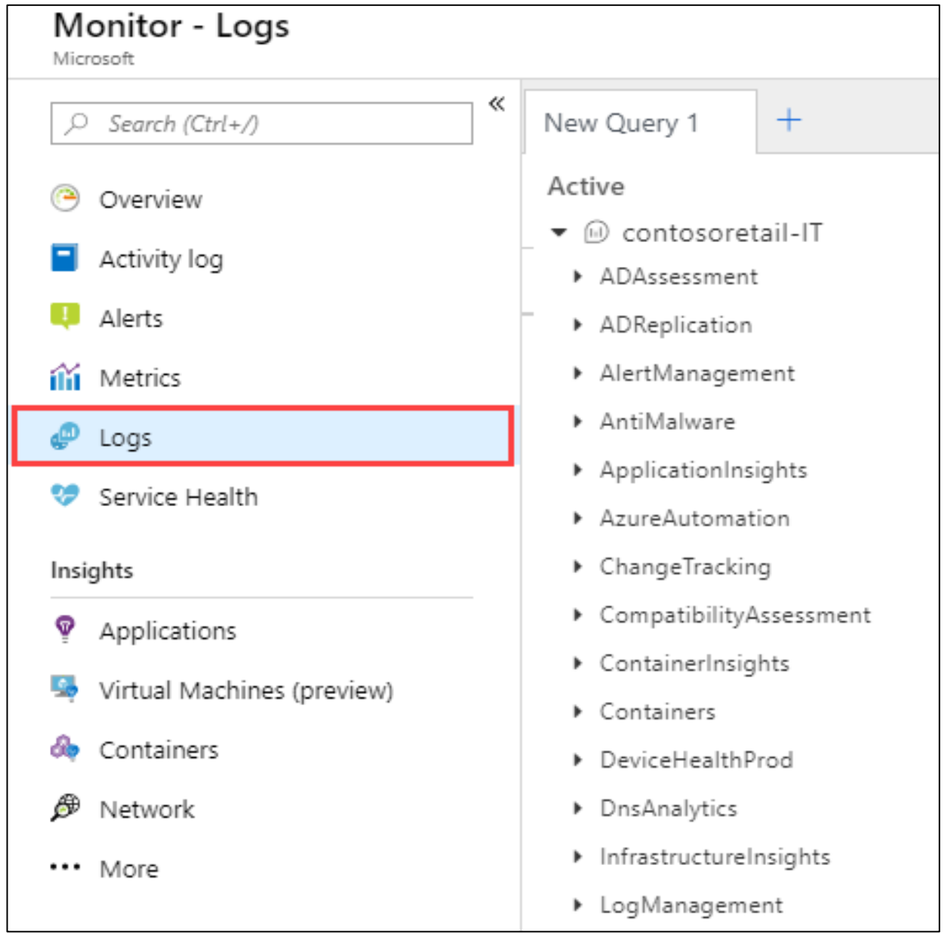
Steps to monitor Azure resource are:

1. Login to your Azure portal
2. Search for resources under subscription
3. Click on Monitoring on the overview page
4. Click on any of the Graph visible to open the data in the metrics explorer

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.

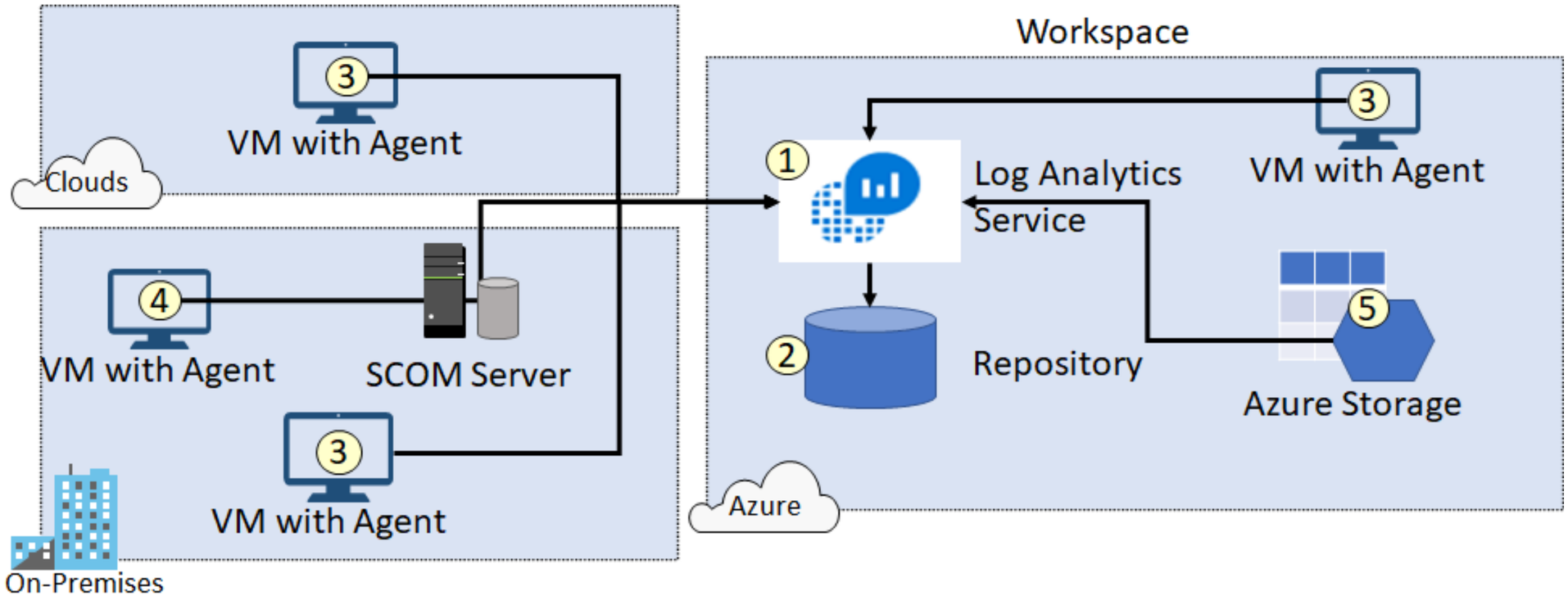


image source: https://docs.microsoft.com/en-in/

Data Sources

Data sources represent the data collected from connected sources.

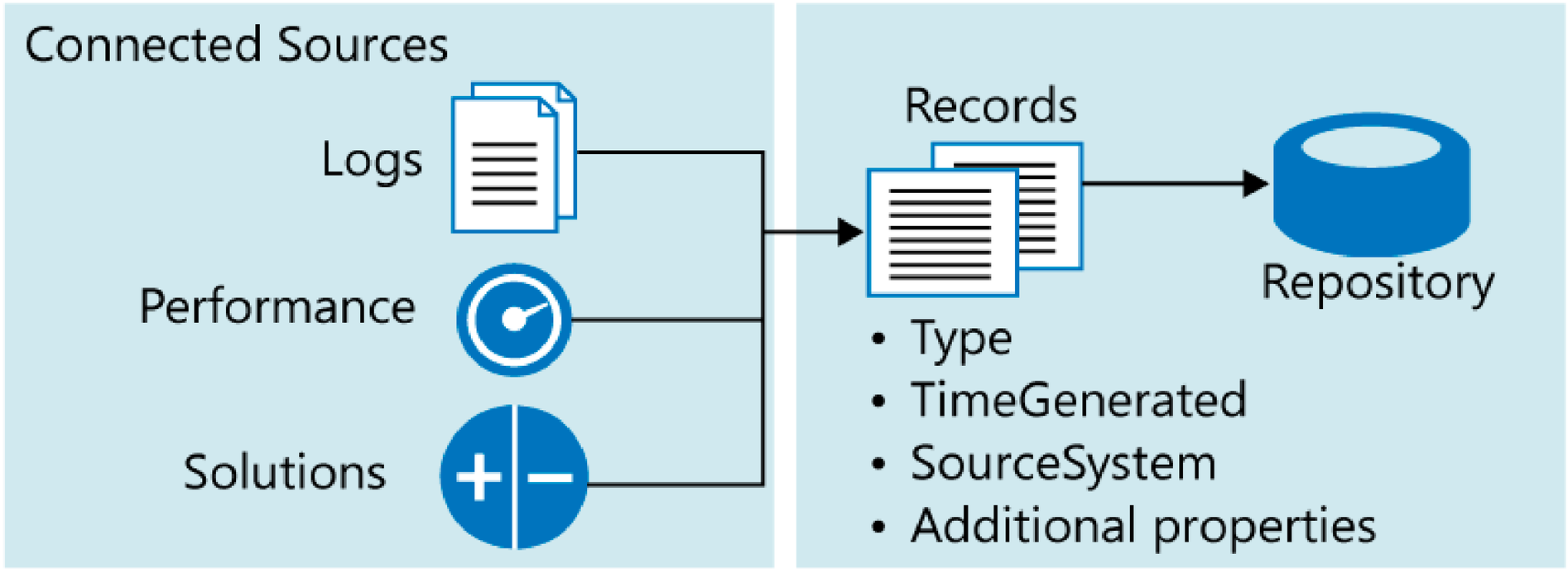


image source: https://docs.microsoft.com/en-in/

Log Analytics Querying

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

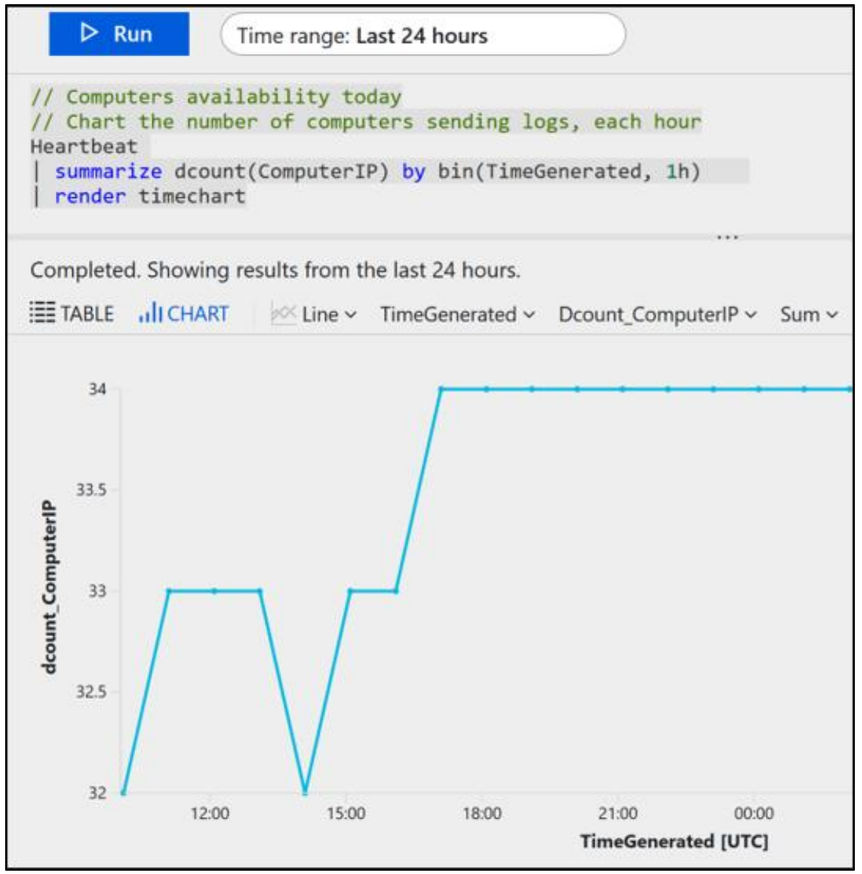


image source: https://docs.microsoft.com/en-in/

Query Language Syntax

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

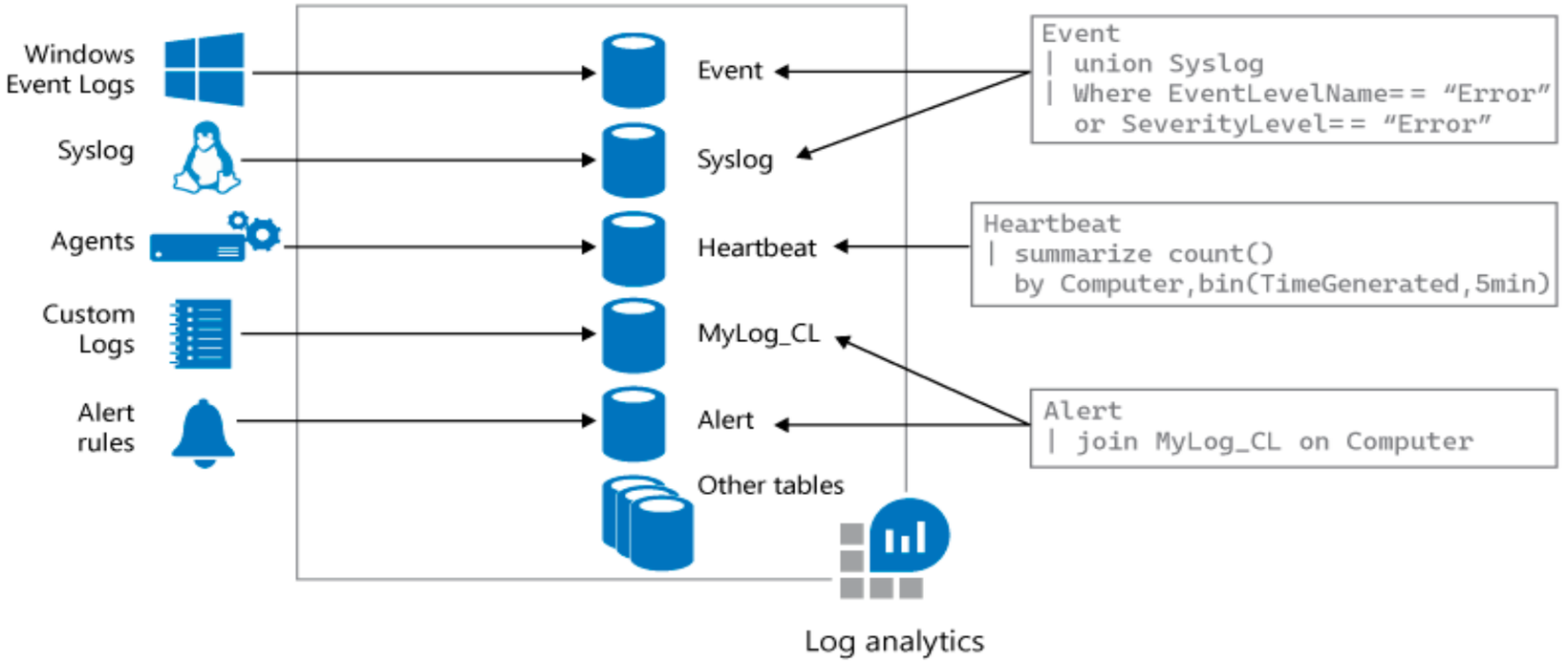
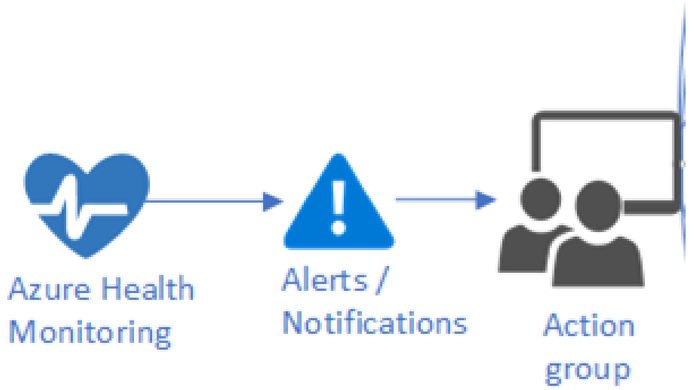


image source: https://docs.microsoft.com/en-in/

Action Groups

Action Groups

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

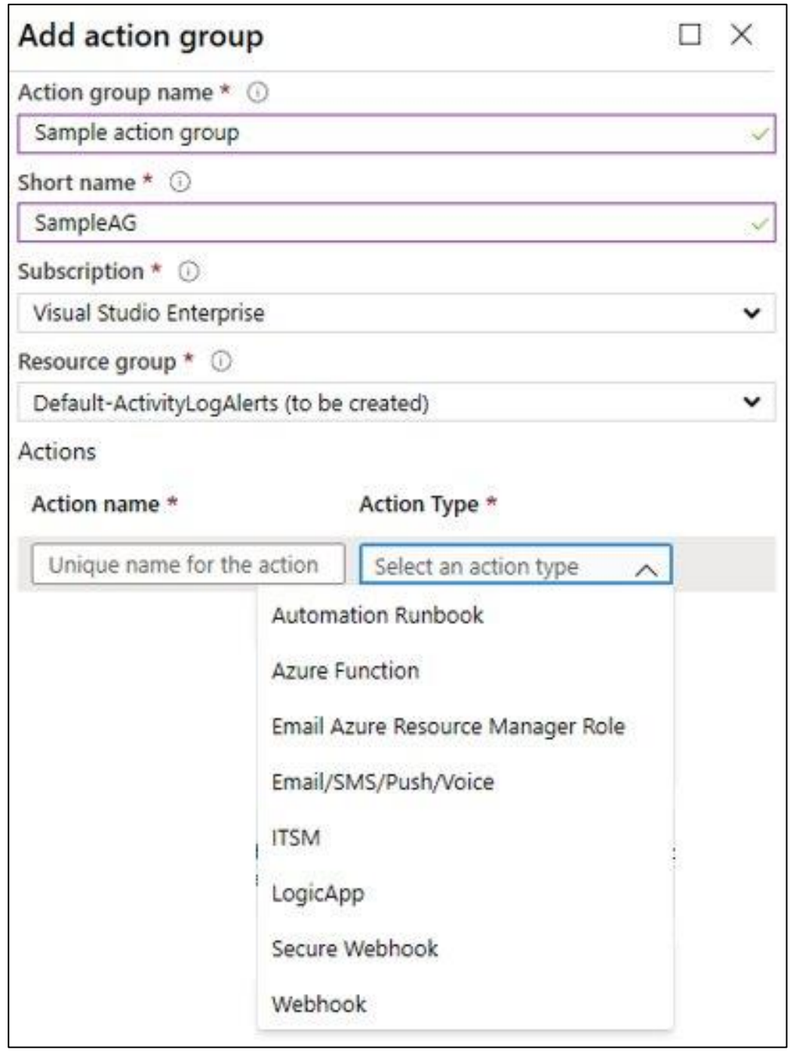


Azure Monitor and Service Health alerts use action groups to notify users that an alert has been triggered.

Action Types

The seven Action Types are listed:

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



Assisted Practice

Azure Action Groups

Duration: 10 Min.

Problem Statement:

You've been given the task of creating an Azure action group. This action group will be used to notify users that an alert has been triggered by Azure Monitor and Service Health alerts.

Assisted Practice: Guidelines

Steps to configure Azure Function App are:

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

Advanced Alerts

Alerts

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

Monitor alerts offer the following benefits

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

Managing Alerts

Alerts can be set based on

- Metric values
- Log search queries
- Activity log events
- Health of the underlying Azure platform
- Tests for website availability

Managing Alerts

Alert states include:

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

Azure Alerts **Duration: 10 Min.**

Problem Statement:

You've been assigned the task of creating an Azure alert to get notified when one of your metrics reaches a certain level.

Note: You can choose any of the resource metrics as per the availability to showcase this demo.

Assisted Practice: Guidelines

Steps to create Azure alerts are:

1. Login to your Azure portal
2. Search for and select Monitor
3. Create an Azure alerts

Assisted Practice

Log Analytics Workspace

Duration: 10 Min.

Problem Statement:

You've been given the task of creating a log analytics workspace that will be used by Azure Monitor Logs as well as Azure Security Center, Azure Sentinel, Application Insights, Service Map, and other Azure services.

Assisted Practice: Guidelines

Steps to configure Azure Function App are:

1. Login to your Azure portal
2. Creating Log Analytics workspaces
3. Adding required information on Log Analytics Workspace page

Key Takeaways

- Azure Monitoring collects and analyzes data to assess the application's performance, health, and availability.
- Azure includes multiple services that individually perform a specific role or task in the monitoring space.
- 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.

Implementing Azure Alerts

Duration: 25 Min.

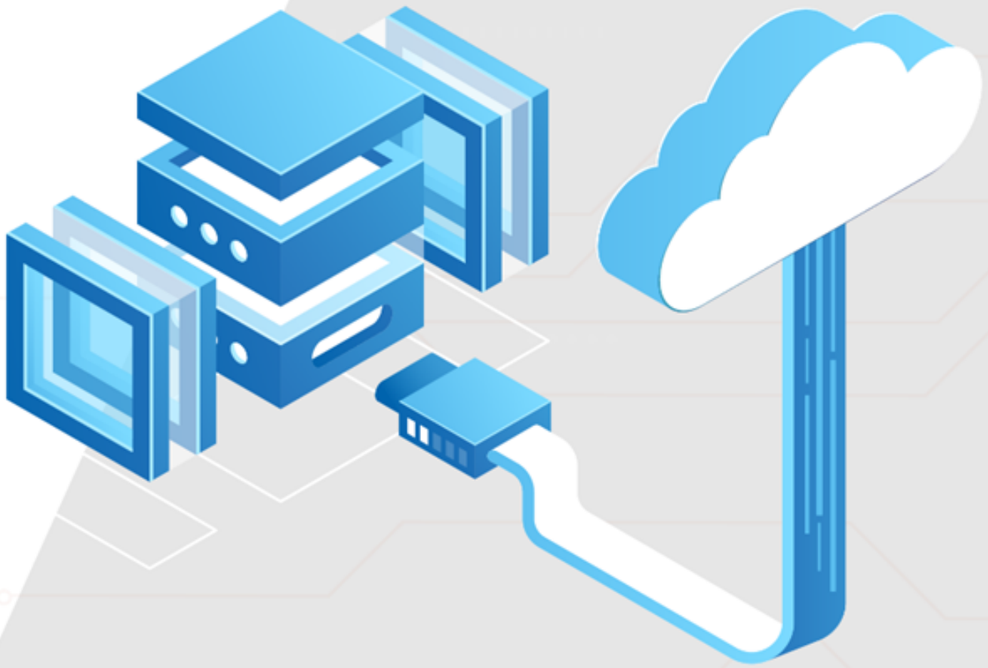
Project agenda: To implement Azure Alerts

Description: You have been given a project to create an alert for a web application (app service) whenever the CPU utilization for the Web App crosses a threshold of 75%. You also need to ensure that appropriate stakeholders are notified about the same. You will need to create an action group to configure notification.

Perform the following:

Create an alert for a web application by keeping the CPU utilization threshold as 75%.

LESSON-END PROJECT



Thank you