Cloud Computing

Caltech | Center for Technology & Management Education

Post Graduate Program in Cloud

Powerd by simplilearn

Caltech | Center for Technology & Management Education

AZ 304 - Microsoft Azure Architect Design

Powerd by simplilearn

Design a Solution for Logging and Monitoring

Learning Objectives

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

- Analyze levels and storage locations for logs
- Illustrate Plan for Integration with Monitoring Tools
- Recommend Database Service Tier Sizing
- Implement Appropriate Monitoring Tools for a Solution
- Configure a Mechanism for Event Routing and Escalation
- Recommend a Logging Solution for Compliance Requirements

A Day in the Life of an Azure Architect

You are working as an Cloud Architect in Eston Inc. The company uses multiple Azure subscriptions and has a wide portfolio of products deployed across all subscriptions.

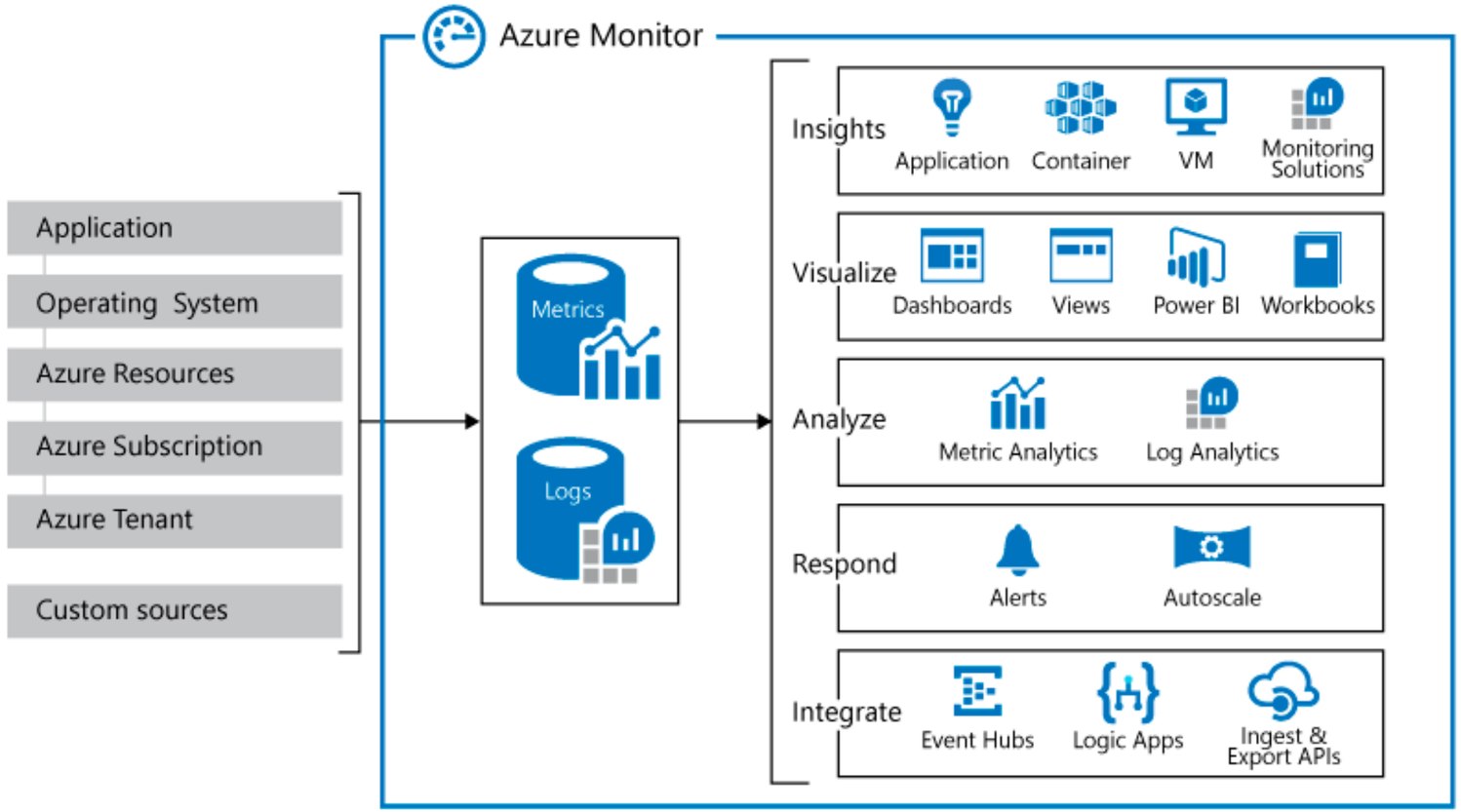
- You need to design a solution to generate a monthly report on all the resource deployments on a per subscription basis.
- Based on the monthly consumption, you also need to set up budget and alerts so that stakeholders can be notified about the costs incurred so far and forecasted pricing.

To achieve all of 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.

Determine Levels and Storage Locations for Logs

Azure Monitor Service

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



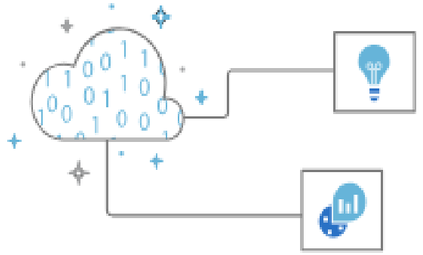
Key Capabilities

These are the key capabilities of azure monitor services:

Monitor & Visualize Metrics

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

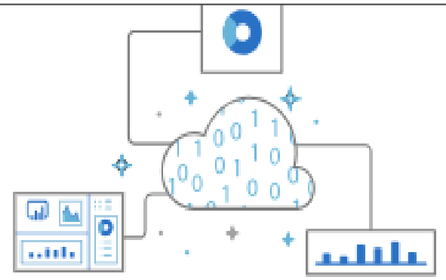
Explore Metrics



Query & Analyze Logs

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

Search Logs



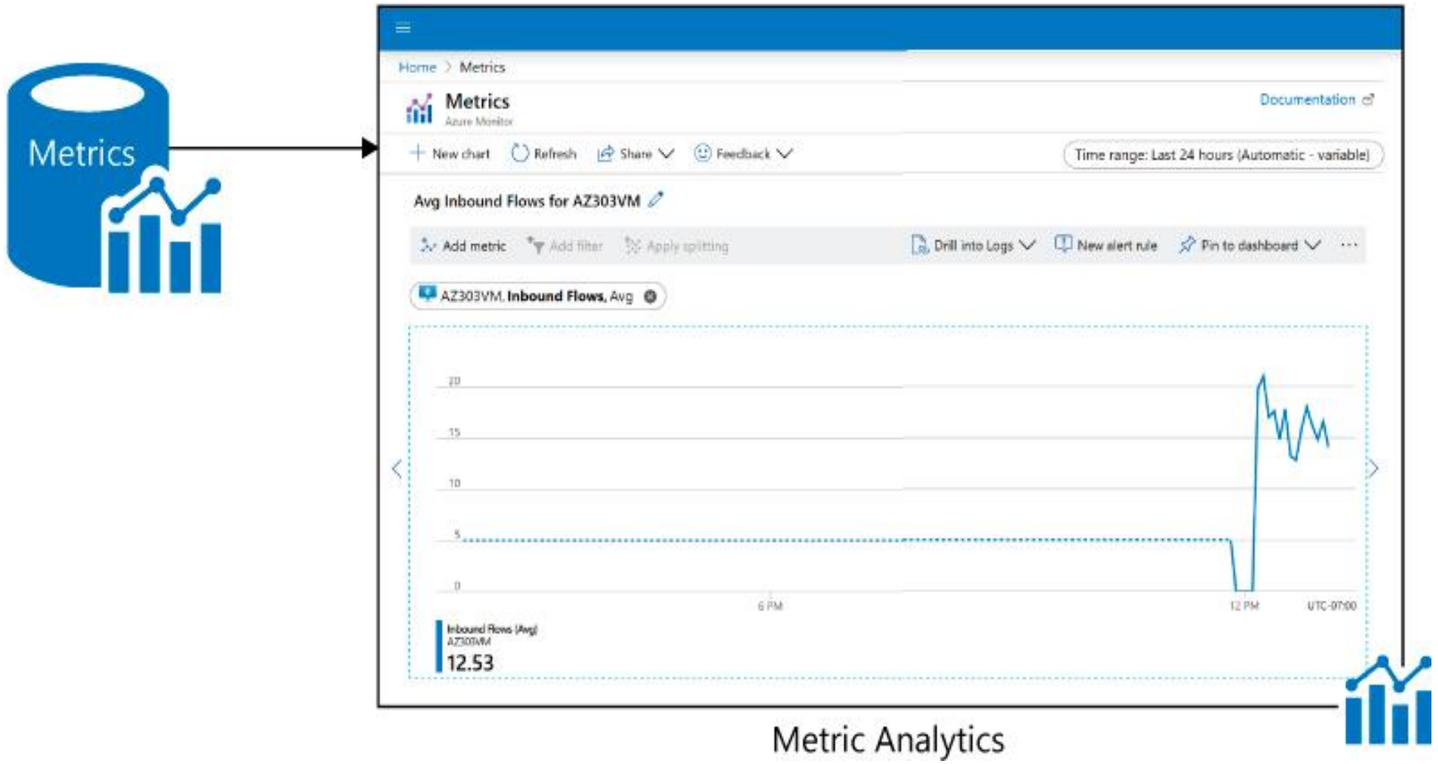
Setup Alert & Actions

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

Create Alert

Monitoring Data Platform

Relational databases organize data as a series of two-dimensional tables with rows and columns.

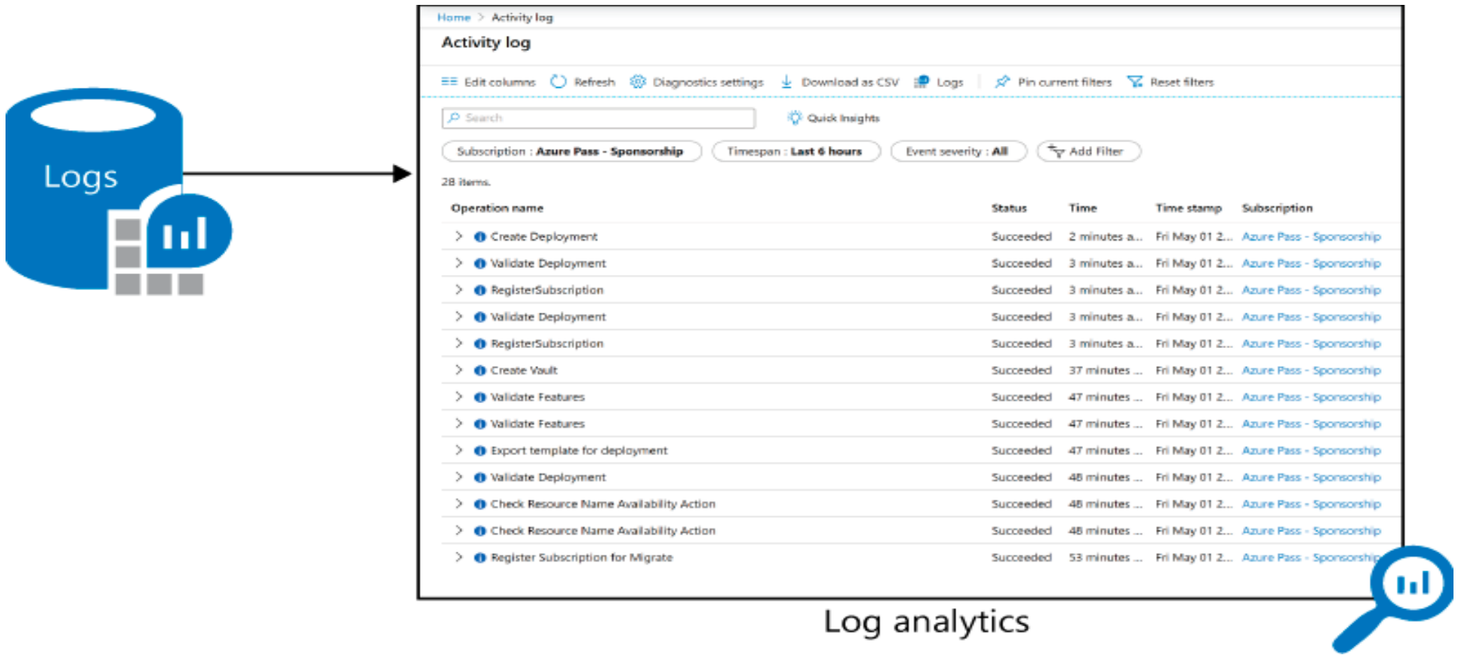


Metric Analytics

- Metrics
- Logs

Log Data

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

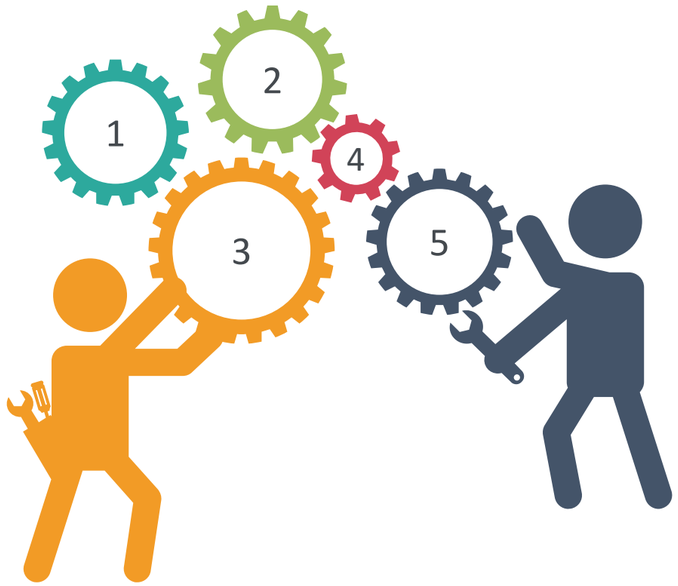


Log analytics

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

Data Types

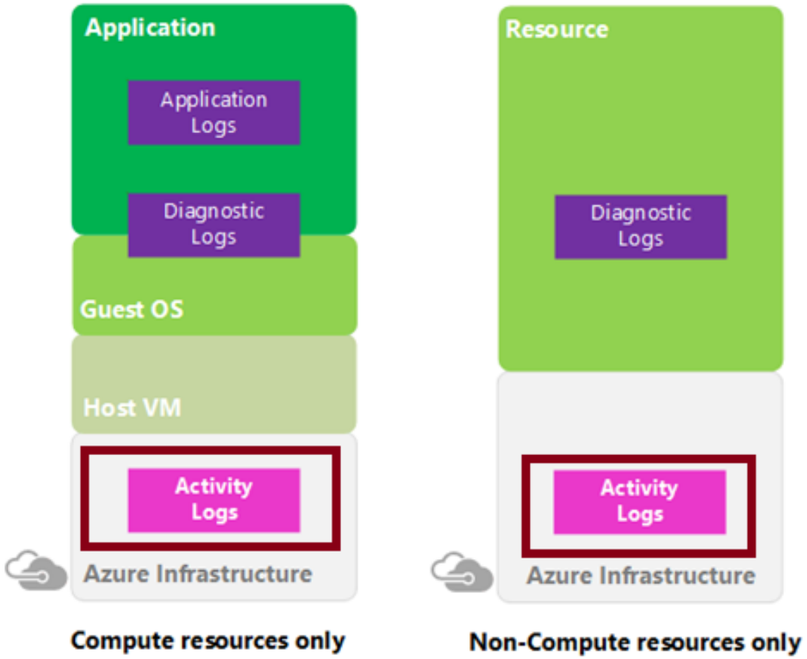
Azure Monitor collects data from each of the following tiers:



- Azure subscription monitoring data
- Application monitoring data
- Guest OS monitoring data
- Azure resource monitoring data
- Azure tenant monitoring data

Activity Log

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



Through activity logs, user can determine:

- What operations (PUT, POST, DELETE) were taken on all resources
- Who started the operation
- When the operation occurred
- The status of the operation
- The values of other properties that might help user research the operation

Query the Activity Log

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

App Service Diagnostic Logs

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

www.shutterstock.com · 1871168869

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.

Example : Exceptions raised by the application.

Web server diagnostic logs :

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

Diagnostic Logs Types

Three types of web server diagnostic logs can be enabled:

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 a HTTP status code of 400 or higher.

Failed Request Tracing

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

Log Structure : Log File Type and Location

Three types of web server diagnostic logs can be enabled:

Application logs:	D:\Home\LogFiles\Application\
Failed request logs:	D:\Home\LogFiles\LogFiles\W3SVC####\
Detailed error logs:	D:\Home\LogFiles\DetailedErrors\
Web server logs:	D:\Home\LogFiles\http\RawLogs\

Assisted Practice

Azure Monitoring

Duration: 10 Min.

Problem Statement:

You've been asked to provide your organization with an Azure logging and monitoring solution that will help you maximize the availability and performance of your apps and services as an Azure Architect.

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 Graphs visible to open the data in the metrics explorer

Assisted Practice

Diagnostic Settings

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 provides extensive diagnostic and auditing information for Azure resources and the Azure platform, as well as sending platform metrics and logs to various destinations.

Assisted Practice: Guidelines

Steps to configure diagnostic settings on the Azure portal are:

1. Login to the Azure portal at https://portal.azure.com
2. Click on Diagnostic settings
3. Click Add diagnostic setting

Assisted Practice

Log Analytics Workspace

Duration: 10 Min.

Problem Statement:

Demonstrate the Log Analytics Workspace, a unique workspace for analyzing Azure Monitor log data.

Assisted Practice: Guidelines

Steps to create log analytics workspace are:

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

Plan for Integration with Monitoring Tools

Azure Monitoring

Monitoring is the act of collecting and analyzing data to determine the performance, health, and availability of user application and the resources that it depends on.

Azure Infrastructure Monitoring

These are the types of azure infrastructure monitoring:

- 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

These are the types of 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

These are the types of 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

These are the types of 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

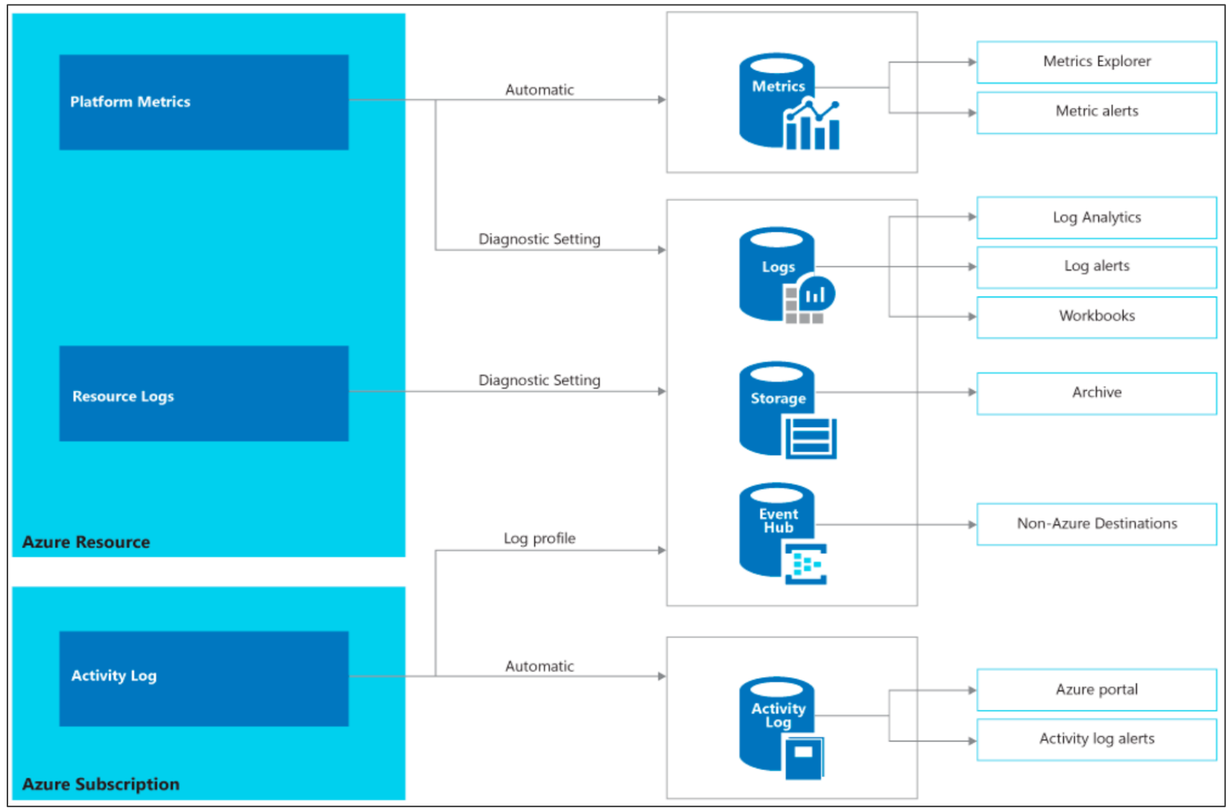
These are the types of azure infrastructure monitoring:

- 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 monitoring data:

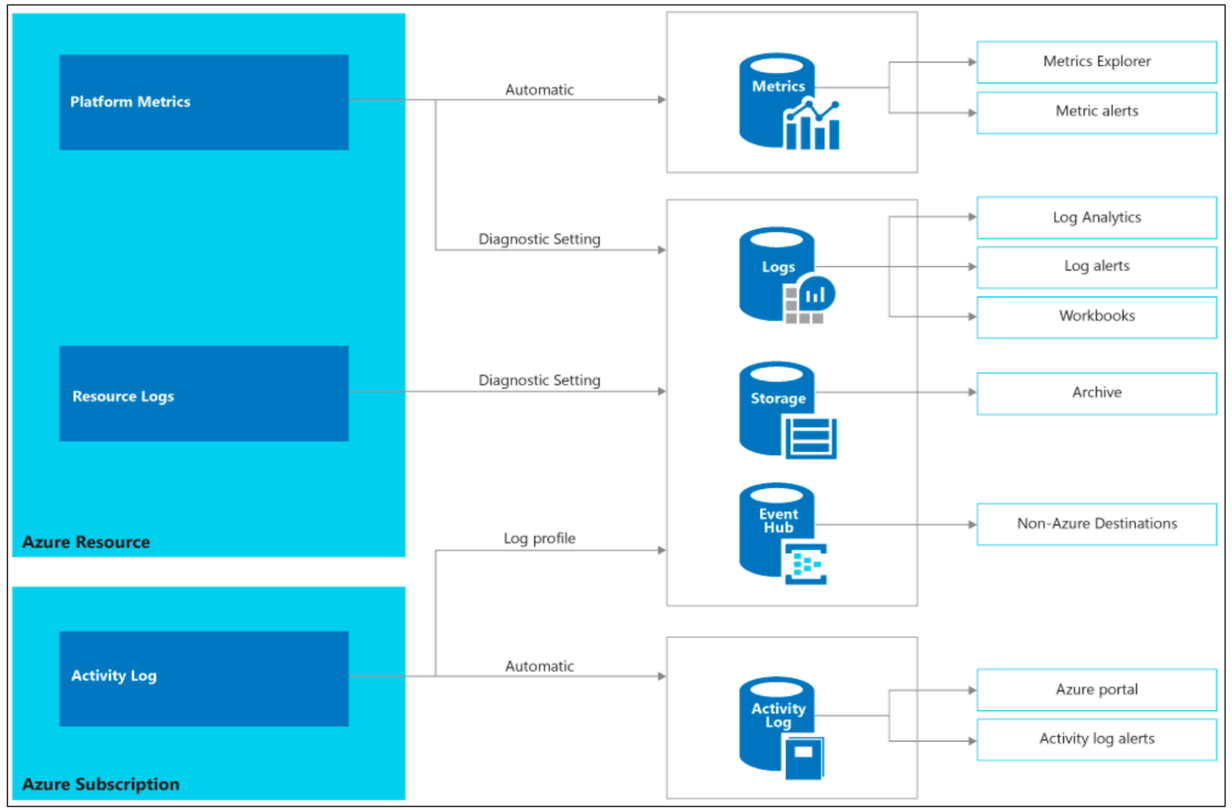


Platform metrics

Numerical values that are automatically collected at regular intervals and describe some aspect of a resource at a time.

Monitoring Data

These are the types monitoring data:

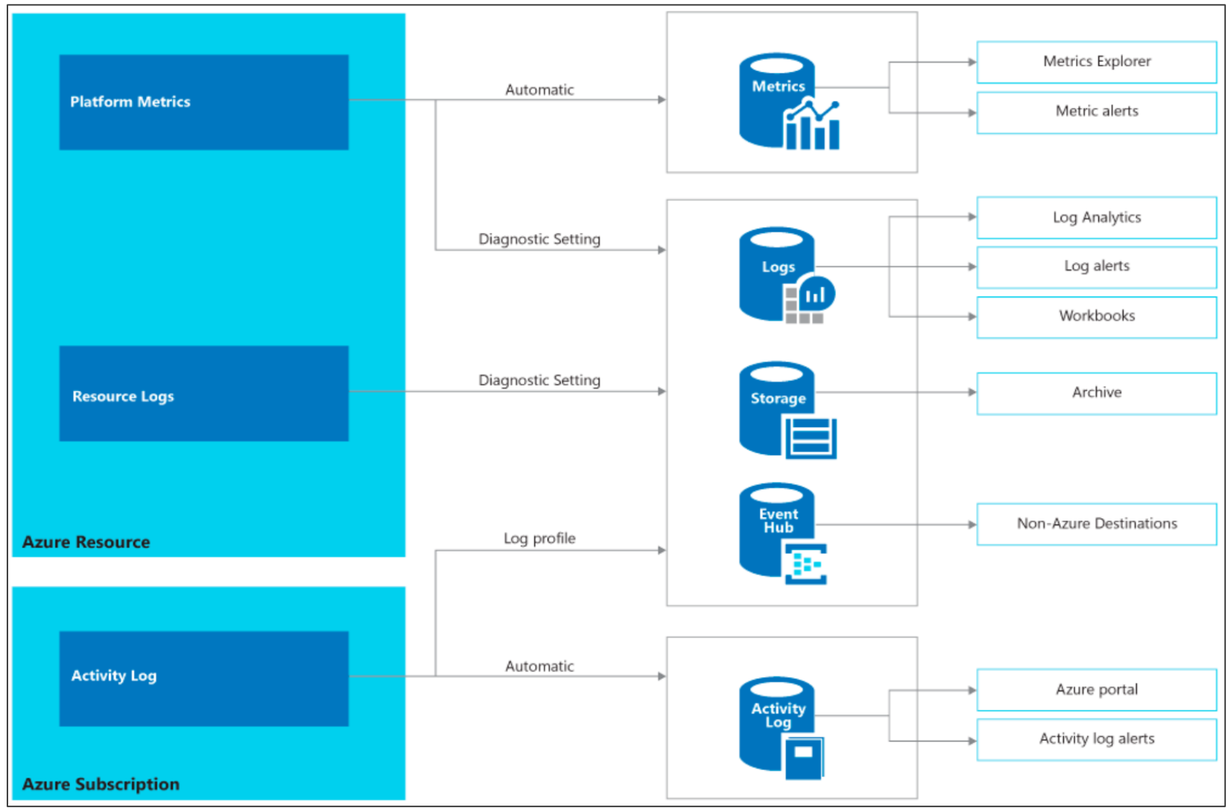


Resource logs

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

Monitoring Data

These are the types monitoring data:



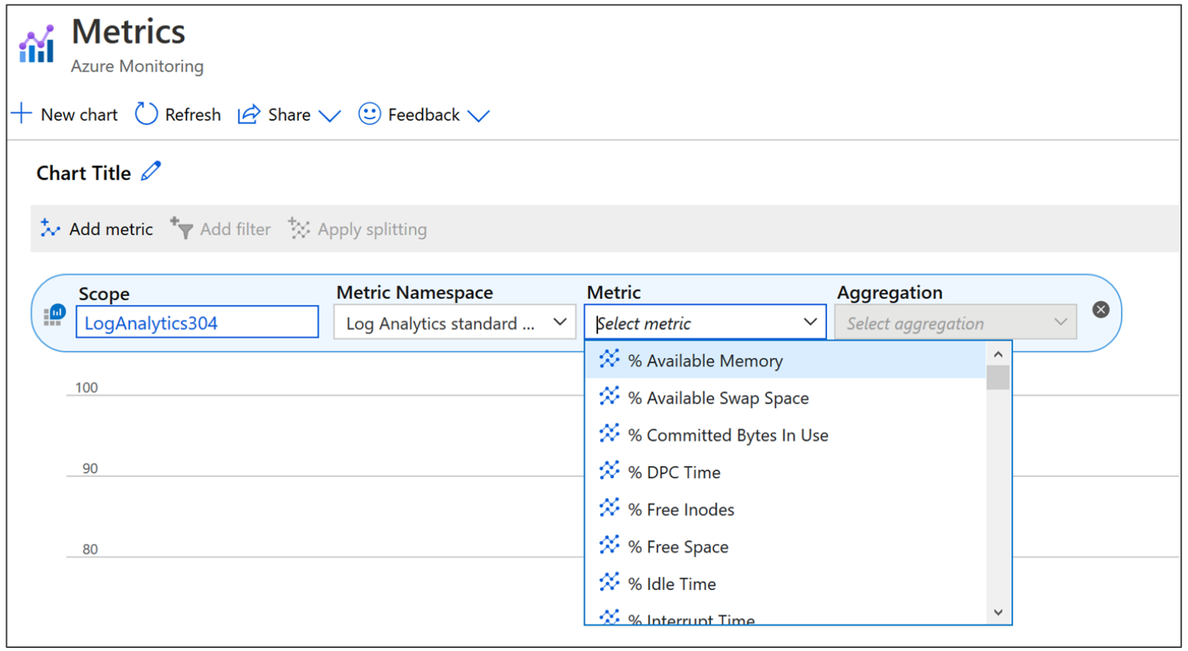
Activity log

Provides insight into the operations on each Azure resource in the subscription from the.

Example: creating a new resource or starting a virtual machine.

Configure Monitoring

Monitoring data is collected automatically



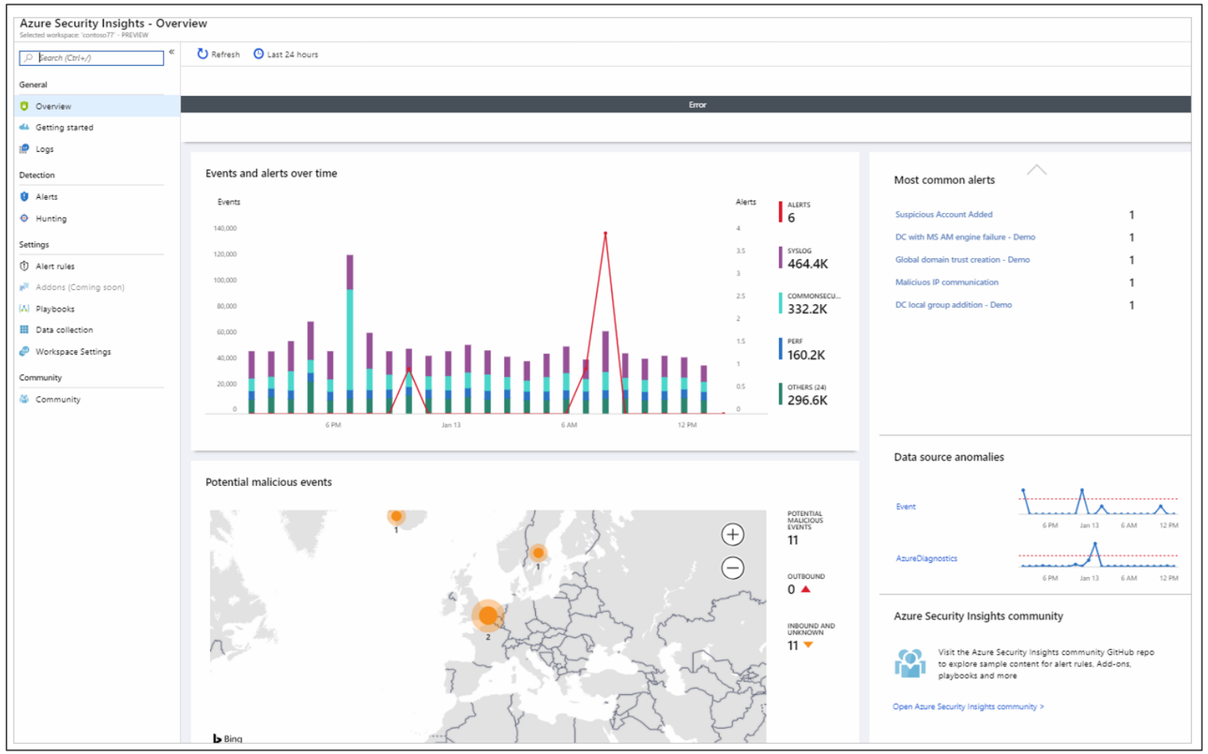
Platform metrics

Platform metrics are collected automatically

- **Resource logs** - diagnostic setting
- **Activity log** - The Activity log is collected automatically

Azure Sentinel

Built-in threat intelligence for detection and investigation.



- Collects data on the devices, users, infrastructure, and applications
- Cloud and on-prem monitoring/management
- Investigates threats using AI

Recommend Appropriate Monitoring Tools for a Solution

Monitoring Azure

Traditional application and infrastructure monitoring focus on whether the application is up and running or how fast it responds.

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

Monitoring Azure

Insights

- For specific Azure services, insights give a customized monitoring experience.
- They are simple to set up and give more visibility into the operation of crucial resources.

Application Monitoring

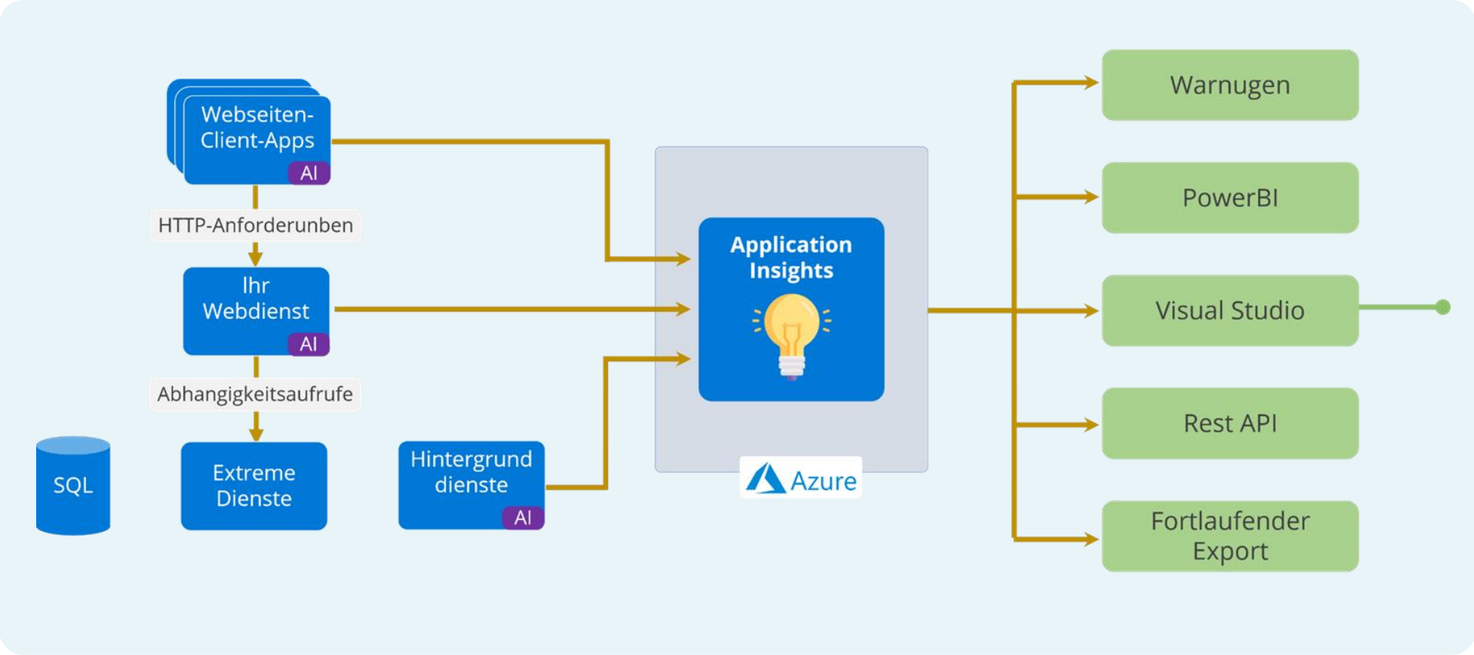
Connection points to a range of development tools are available in application insights.

Application insights keep track of user's web applications 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
- 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

Choose a Mechanism for Event Routing and Escalation

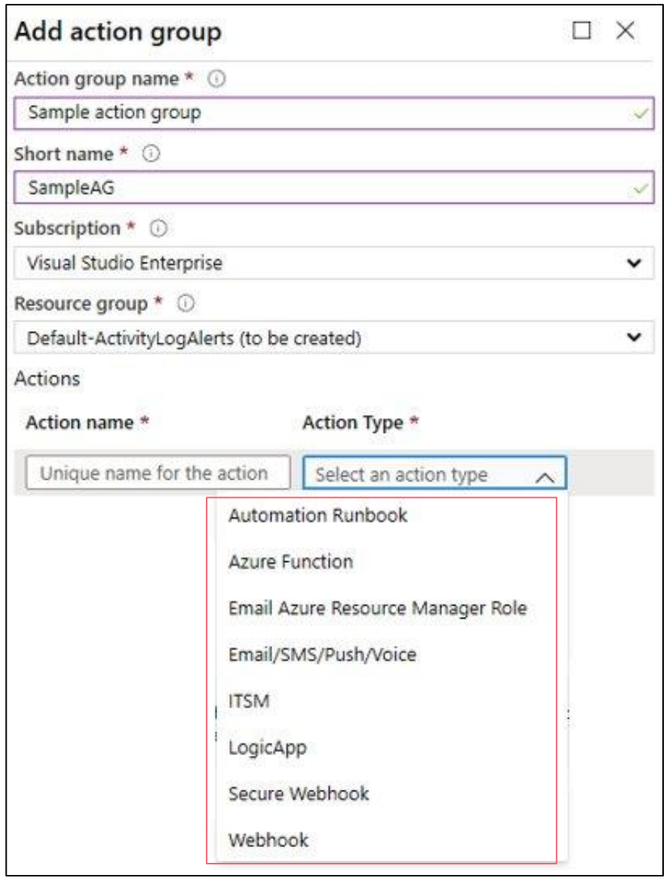
Action Groups

An action group is a set of notification preferences set by the Azure subscription's owner. Action groups are used by Azure Monitor and Service Health alerts to notify users when an alert has been triggered.

Action Types

The following action types are available to the owner:

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



Alerts

Alerts notify the user when severe events are identified in the monitoring data.

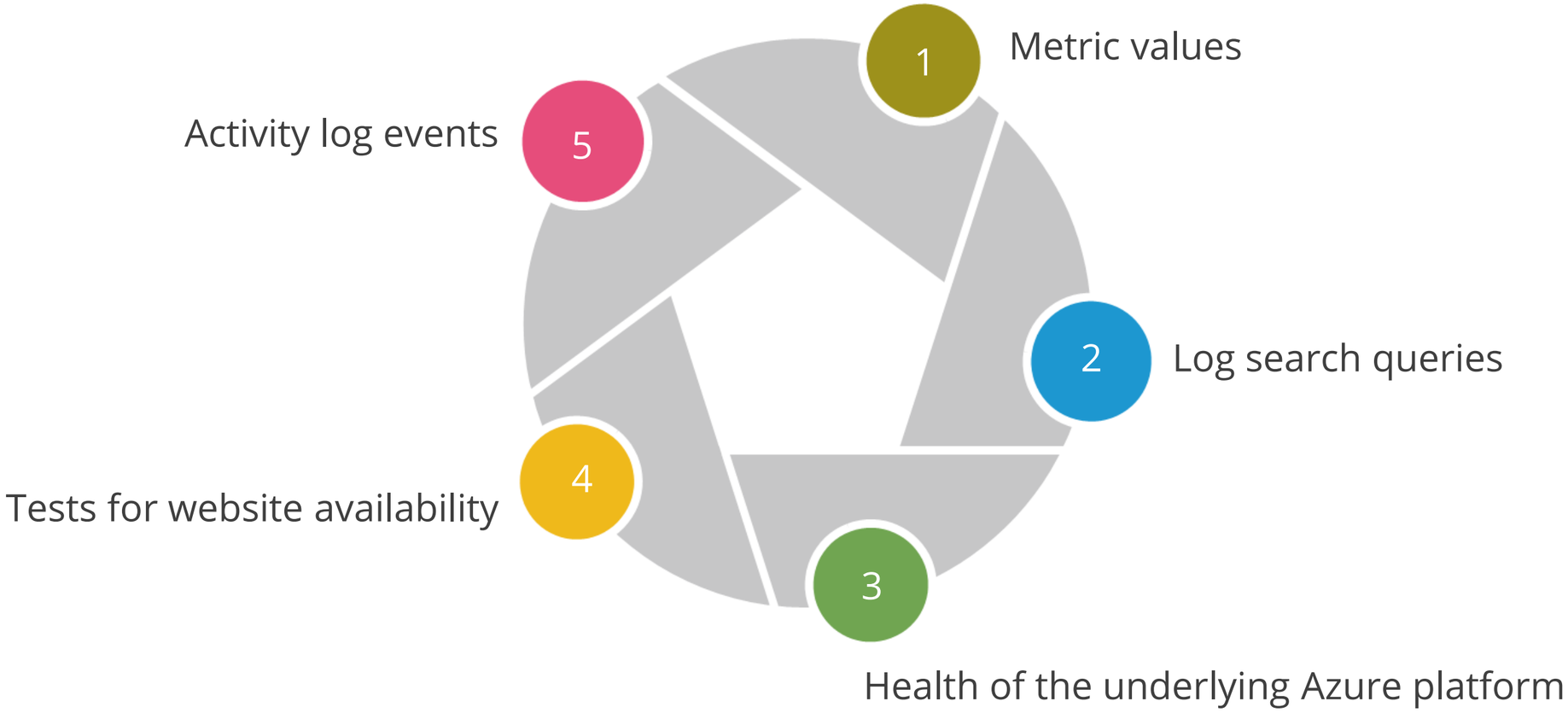
Benefits of Alerts

Monitor alerts offer the following benefits:

- Better workflow
- Better notification system
- Separate fired alerts and alert rules
- Unified authoring experience
- Log analytics in Azure portal

Managing Alerts

Alerts can be set based on the following criteria:



Alert States

The key elements of alert states:

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, you 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. Key attributes of an alert rule include:

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. 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

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

Recommend a Logging Solution for Compliance Requirements

Security Posture

It improves the posture and has a proactive strategy that audits the resources.

View the security state of resources and any issues per resource type:

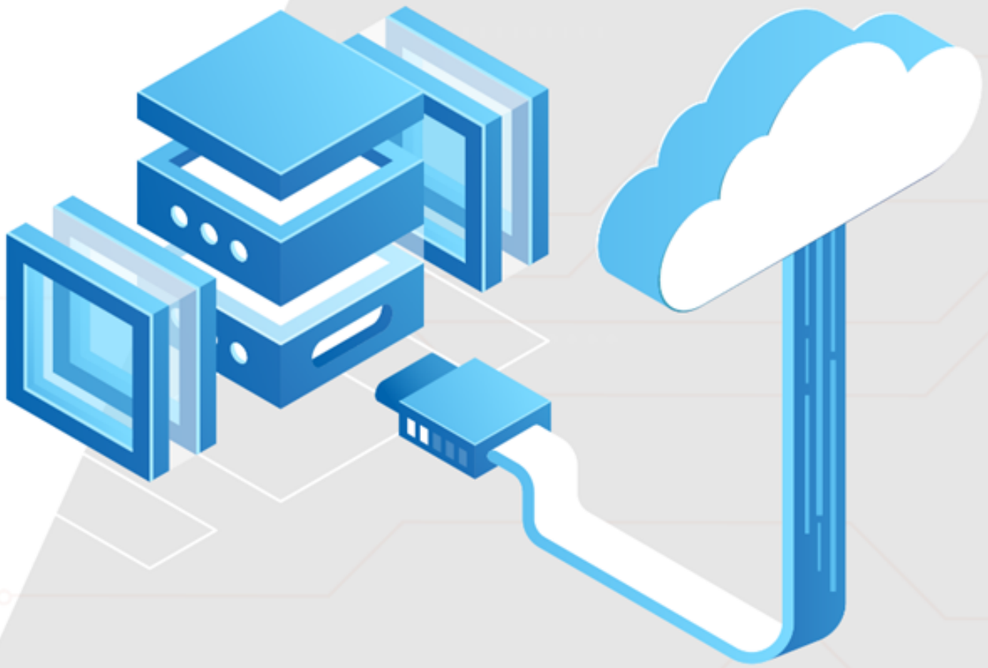
- Monitor computer resources and apps
- Monitor network resources
- Monitor data and storage resources
- Monitor user's identity and access resources

Azure Security Center

It manages infrastructure security from a centralized location, security of workloads on-premises or in the cloud, and monitors the health of resources and implements recommendations.

Key Takeaways

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



Thank you