Azure Monitoring

Agenda

- What is Azure Monitoring
- Monitor Azure environment
- Metrics
- Characteristics of Metrics
- Alerts
- Activity Log
- Diagnostic Logs
- Action Groups
- Service Health Notification
- SMS Alert
- Hands-On Lab

What is Azure Monitoring

- Azure Monitor is the platform service that provides a single source for monitoring Azure resources.
- Azure Monitor provides base-level infrastructure metrics and logs for most services in Microsoft Azure.
- Azure Monitor makes metrics available for many Azure resources.
- These metrics convey the performance and health of those resources.
- In many cases metric values can point to something being wrong with a resource.
- You can create metric alerts to monitor for abnormal behavior and be notified if it occurs.

Azure Monitoring: Monitor Azure environment

- There are a range of tools for monitoring, which work together to offer comprehensive monitoring and include:
  - **Azure Monitor**
    - It gives you access to performance metrics and events that describe the operation of the Azure infrastructure.
  - **Application Insights**
    - The Azure service that offers application performance monitoring and user analytics.
  - **Log Analytics**
    - It provides rich tools to analyze data across sources, allows complex queries across all logs, and can proactively alert on specified conditions.
    - You can even collect custom data into its central repository so you can query and visualize it.

Azure Monitoring: Metrics

- Azure Monitor enables you to consume telemetry to get into the performance and health of your workloads.

- The most important type of Azure telemetry data is the metrics (also called performance counters).

- Metrics are a valuable source of telemetry and enable you to do the following tasks:
  - Track the performance of your resource.
  - Get notified of an issue that impacts the performance of your resource.
  - Configure automated actions, such as autoscaling a resource or firing a runbook.
  - Perform advanced analytics or reporting on performance or usage trends of your resource.
  - Archive the performance or health history of your resource for compliance or auditing purposes.

Azure Monitoring: Characteristics of Metrics

Metrics have the following characteristics:

- All metrics have one-minute frequency.
- You receive a metric value every minute from your resource, giving you near real-time visibility.
- Metrics are available immediately.
- You can access 30 days of history for each metric.
- Some metrics can have name-value pair attributes called dimensions.
- These enable you to further segment and explore a metric in a more meaningful way.

Azure Monitoring: Alerts

- Alerts offer a method of monitoring in Azure that allows you to configure conditions over data and become notified when the conditions match the latest monitoring data.

- Azure uses the following terms to describe alerts and their functions:
  - **Alert**
    - Aa definition of criteria (one or more rules or conditions) that becomes activated when met.
  - **Active**
    - The state when the criteria defined by an alert is met.
  - **Resolved**
    - The state when the criteria defined by an alert is no longer met after previously having been met.
  - **Notification**
    - The action taken based off of an alert becoming active.
  - **Action**
    - A specific call sent to a receiver of a notification (for example, emailing an address or posting to a webhook URL). Notifications can usually trigger multiple actions.

Azure Monitoring: Activity Log

- The Azure Activity Log provides insight into subscription-level events that have occurred in Azure.
- This includes a range of data, from Azure Resource Manager operational data to updates on Service Health events.
- Using the Activity Log, you can determine the 'what, who, and when' for any write operations in your subscription.
- You can retrieve events from your Activity Log using the Azure portal, CLI, PowerShell cmdlets, and Azure Monitor REST API.
- You can use the audit logs to find an error when troubleshooting or to monitor how a user in your organization modified a resource.
- Activity logs are retained for 90 days.
- You can query for any range of dates, as long as the starting date is not more than 90 days in the past.

Azure Monitoring: Diagnostic Logs

- Azure resource-level diagnostic logs are logs emitted by a resource that provide rich, frequent data about the operation of that resource.

- Resource-level diagnostic logs differ from the Activity Log.
  - The Activity Log provides insight into the operations that were performed on resources in your subscription using Resource Manager, for example, creating a virtual machine or deleting a logic app.
  - The Activity Log is a subscription-level log. Resource-level diagnostic logs provide insight into operations that were performed within that resource itself, for example, getting a secret from a Key Vault.

- Resource-level diagnostic logs also differ from guest OS-level diagnostic logs.

- Guest OS diagnostic logs are those collected by an agent running inside of a virtual machine or other supported resource type.

Azure Monitoring: Action Groups

- You can configure a list of actions with action groups.
- These groups then can be used when you define activity log alerts.
- These groups can then be reused by each activity log alert you define, ensuring that the same actions are taken each time the activity log alert is triggered.
- An action group can have up to 10 of each action type.
- Each action is made up of the following properties:
  - **Name**
    - A unique identifier within the action group.
  - **Action type**
    - Send an SMS, send an email, call a webhook, send data to an ITSM tool, call an Azure app, or run an Automation runbook.
  - **Details**
    - The corresponding phone number, email address, webhook URI, or ITSM Connection Details.

Azure Monitoring: Service Health Notification

- Service health notifications are published by Azure, and contain information about the resources.
- Service health notifications can be informational or actionable, depending on the class.
- There are various classes of service health notifications:
  - **Action required**
    - Azure might notice something unusual happen on your account, and work with you to remedy this.
  - **Assisted recovery**
    - An event has occurred and engineers have confirmed that you are still experiencing impact. Azure engineering needs to work with you directly to restore your services to full health.
  - **Incident**
    - An event that impacts service is currently affecting one or more of the resources in your subscription.
  - **Maintenance**
    - A planned maintenance activity that might impact one or more of the resources under your subscription.
  - **Information**
    - Potential optimizations that might help improve your resource use.
  - **Security**
    - Urgent security-related information regarding your solutions that run on Azure.

Azure Monitoring: SMS Alert

- Action groups enable you to configure a list of receivers.
- These groups can then be leveraged when defining activity log alerts; ensuring that a particular action group is notified when the activity log alert is triggered.
- One of the alerting mechanisms supported is SMS; the alerts support bi-directional communication.
- A user can respond to an alert to:
  - **Unsubscribe from alerts**
    - A user can unsubscribe from all SMS alerts for all action groups, or a singular action group.
  - **Re-subscribe to alerts**
    - A user can re-subscribe to all SMS alerts for all action groups, or a singular action group.
  - **Request help**
    - A user can ask for more information on the SMS.

Hands-On Lab

Thank You