Document: AKS cluster monitoring

Tasks:

To ensure effective monitoring and alerting for the AKS cluster as a critical (backbone) part of the application deployment strategy. This ensures that the cluster runs smoothly, and potential issues are identified and addressed promptly.

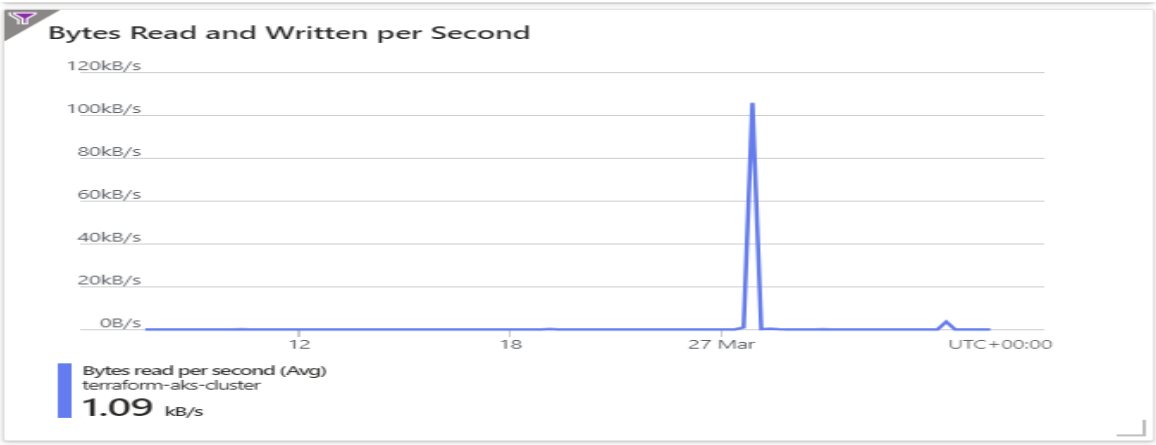
Steps:

1. Enabled Container Insights for the AKS cluster to collect real-time in-depth performance and diagnostic data for the efficient monitoring of the application performance and troubleshooting of issues. Note that enabling Container Insights is a key step in harnessing the full power of Azure Monitor for monitoring containerized workloads. Container Insights provides detailed metrics and insights into the performance and health of the AKS cluster. The following steps were taken to enable container insights:
    a. Enabled managed identity on the cluster using the following command: az aks update -g {resource-group-name} -n {aks-cluster-name} --enable-managed-identity
    Note: replace the placeholders with the resource group and cluster names. The --enable-managed-identity command allows the AKS cluster to use a Microsoft Entra ID identity instead of the Service Principal to authenticate with Azure services. To collect advanced data and metrics from the cluster, using Container Insights, the cluster needs to have managed identity enabled.
    b. Set the necessary permissions for the Service Principal using the following steps:
        i. Navigated to the Subscriptions web page, identifying my subscription called Hermas Amaewhule DevOps
        ii. From subscription web page accessed the Access control (IAM) page. Using the + Add -> Add role assignment button at the top of the page to add the following permissions:
            1. Monitoring Metrics Publisher: for granting permissions to publish monitoring metrics to Azure Monitor. This is important for applications and services that need to push metrics to Azure Monitor.
            2. Monitoring Contributor: To grant broad permissions for monitoring and managing monitoring resources in Azure, including permissions to read and write, monitoring settings, accessing monitoring data and managing monitoring resources.
            3. Log Analytics Contributor: Grants permissions to read and write access to Log Analytics workspaces. Includes permissions to query and analyze log data stored in those workspaces.
        iii. Assigned each of the above roles to your Service Principal application, in the Members page using the + Select members' button which opens a page for searching the Service Principal by name and selecting it.

    c. Then enabled Container Insights on the cluster as follows:
        i. Navigated to the AKS cluster's homepage and accessed the Insights tab within the Monitoring section.
        ii. Then click the Configure monitoring button to initiate the process of enabling Container Insights. This will be redirect to a configuration page to select the additional monitoring tools to enable for the cluster.
        iii. Select Enable container logs.

iv. Click Configure to confirm the setup. Note there, may be a delay in data visibility, and Container Insights won't offer historical data prior to activation. To start viewing data, you'll need to interact with the cluster, for example by redeploying your applications to it.

2. Created, configured, and saved the following charts in Metrics Explorer:
    a. Average Node CPU Usage: This chart allows you to track the CPU usage of your AKS cluster's nodes. Monitoring CPU usage helps ensure efficient resource allocation and detect potential performance issues.
    b. Average Pod Count: This chart displays the average number of pods running in your AKS cluster. It's a key metric for evaluating the cluster's capacity and workload distribution.
    c. Used Disk Percentage: Monitoring disk usage is critical to prevent storage-related issues. This chart helps you track how much disk space is being utilized.
    d. Bytes Read and Written per Second: Monitoring data I/O is crucial for identifying potential performance bottlenecks. This chart provides insights into data transfer rates.



3. Configured Log Analytics to execute and save the following logs:
    a. Average Node CPU Usage Percentage per Minute: This configuration captures data on node-level usage at a granular level, with logs recorded per minute.

```
// Kubernetes events
// Lists all the Kubernetes events.
KubeEvents
| where TimeGenerated > ago(7d)
| where not(isempty(Namespace))
| top 200 by TimeGenerated desc

// Avg node CPU usage percentage per minute
// For your cluster view avg node CPU usage percentage per minute over the last hour.
// To create an alert for this query, click '+ New alert rule'
//Modify the startDateTime & endDateTime to customize the timerange
```

Results | Chart

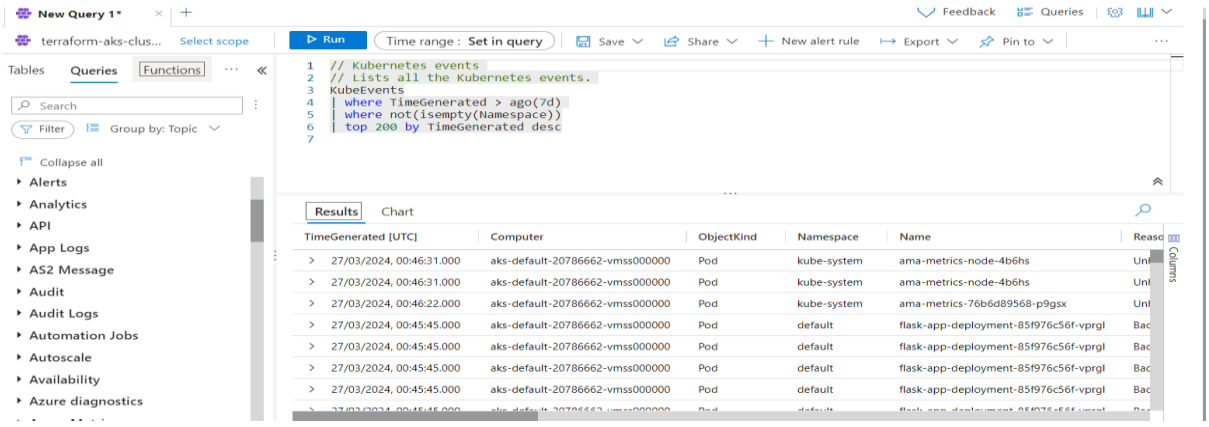
TimeGenerated [UTC]	ClusterName	_ResourceId	AggregatedValue
27/03/2024, 08:08:00.000	terraform-aks-cluster	/subscriptions/8ab233ac-c619-4888-bf7a-422ea867b8d8/resourcegroups/...	8.73
27/03/2024, 08:07:00.000	terraform-aks-cluster	/subscriptions/8ab233ac-c619-4888-bf7a-422ea867b8d8/resourcegroups/...	8.95
27/03/2024, 08:06:00.000	terraform-aks-cluster	/subscriptions/8ab233ac-c619-4888-bf7a-422ea867b8d8/resourcegroups/...	8.81333333333335
27/03/2024, 08:05:00.000	terraform-aks-cluster	/subscriptions/8ab233ac-c619-4888-bf7a-422ea867b8d8/resourcegroups/...	10.013333333333351
27/03/2024, 08:04:00.000	terraform-aks-cluster	/subscriptions/8ab233ac-c619-4888-bf7a-422ea867b8d8/resourcegroups/...	8.53666666666665
27/03/2024, 08:03:00.000	terraform-aks-cluster	/subscriptions/8ab233ac-c619-4888-bf7a-422ea867b8d8/resourcegroups/...	8.603333333333351
27/03/2024, 08:02:00.000	terraform-aks-cluster	/subscriptions/8ab233ac-c619-4888-bf7a-422ea867b8d8/resourcegroups/...	8.83

b. Average Node Memory Usage Percentage per Minute: Like CPU usage, tracking memory usage at node level allows you to detect memory-related performance concerns and efficiently allocate resources.

c. Pods Counts with Phase: This log configuration provides information on the count of pods with different phases, such as Pending, Running, or Terminating. It offers insights into pod lifecycle management and helps ensure the cluster's workload is appropriately distributed.

d. Find Warning Value in Container Logs: By configuring Log Analytics to search for warning values in container logs, you proactively detect issues or errors within your containers, allowing for prompt troubleshooting and issues resolution.

e. Monitoring Kubernetes Events: Monitoring Kubernetes events, such as pod scheduling, scaling activities, and errors, is essential for tracking the overall health and stability of the cluster.



4. Setup disk used percentage alarm: Set up an alert rule to trigger an alarm when the used disk percentage in the AKS cluster exceeds 90%. This alert is vital because it helps to proactively detect and address potential disk issues that could lead to performance degradation and service interruptions. The alert checks every 5 minutes and have a loopback period of 15 minutes. The alert is configured to send notifications to my email address, so I can determine what is the best strategy for responding to these alarms.

5. Modify memory and CPU alert rules: Adjusted the alert rules for CPU usage and memory working set percentage to trigger when they exceed 80%. CPU and memory are critical resources in the AKS cluster. When they are heavily utilized, it can lead to decreased application performance. By setting alert rules to trigger at 80%, one ensures that he gets notified when these resources are approaching critical levels.