**Questions – Level 2**

**Telemetry Data Collection - Types and Sources**

Metrics are used to monitor the performance of virtual resources, and logs are used to record events that happened on such virtual resources. The collection of metrics and logs should be done from multiple data sources that are related to multiple layers.

Yes/No

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Which layer can be a data source for telemetry data?

1. Azure Platform
2. Azure Resources
3. Operating Systems
4. Applications
5. **All answers are correct**

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

The Azure platform is the cloud environment, where we are creating all kinds of computing, networking and storage resources. Those resources are grouped into a variety of cloud services. In some cases, the issue we will see in a specific resource can be related to a problem in Azure services. In that case, we should be able to monitor the Azure platform in the **context** of our subscription and also be able to know about any configuration changes made to our Azure resources.

**Yes**/No

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Telemetry data collected from Azure resources is all about external operations performed on those resources.

Yes/**No (**Telemetry data collected from Azure resources is all about the internal operations of Azure resources for understanding what’s going inside those resources.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

A **metric** is a numerical value that describes some aspect of a system at a particular point in time. **Performance monitoring** is the collection of metrics in pre-defined intervals from multiple resource types and layers. Metrics are usually aggregated into higher time intervals. This process allows gradual reduction of data resolution over time, which is translated to less storage capacity.

**Yes**/No

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**A log** is a record created automatically to describe a specific event that happened over time. They are useful for **troubleshooting, debugging, and auditing**. Some logs are created and collected in pre-defined intervals (like every 5min), and some of them will be created sporadically when something is happening.

**Yes**/No

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Activity logs can be used to track **different types of activities** performed in Azure in the context of our subscription (subscription-level events). It can be activities that are performed by:

1. End-users
2. The Azure system
3. Answers 1 and 2

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Diagnostic logs provide insights into the operations that were performed **within the resource itself**.

**Yes**/No

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

In each VM, we will use some operating system, like Windows or Linux. That’s the **Guest OS.** The guest Operating system can provide additional or extended telemetry data based on metrics and logs. Guest OS metrics and logs are collected by the Azure “Diagnostics Extension” agent. This agent will monitor what’s going on inside the OS and send that telemetry data back to Azure Monitor.

**Yes**/No

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Automation**

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

In Microsoft Azure, the concept of thresholds management is called “**Alert rules**.” And the option to perform something is called “**Action groups**.” We, as end-users are responsible for creating an entity that is called an **alert rule**.

**Yes**/No

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

At the basic level, the definition of an alert rule includes the **target resource** and the **criteria** for alerting. The **criteria** are used to define the **scope and signals** available for alerting, and it can be almost any Azure resource.

Yes/**No (**The **target resource** is used to define the **scope and signals** available for alerting, and it can be almost any Azure resource).

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

An **action group** is a specific action taken automatically when an alert has been triggered. Action groups allow us to trigger one or more actions to notify others about an alert and also to solve it automatically.

**Yes**/No

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

An action group can be used only by one alert rule.

Yes/**No** (An action group can be used by many alert rules)

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

As part of an action group definition, we can use the **webhook** option to trigger a web-based API of an external service.

**Yes**/No

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Alarms created by alert rules will have three alarm states: New, Acknowledged, and Closed. An alert state is set by the users after it was created, meaning we can change it to “Acknowledged" or “Closed.”

**Yes**/No

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

The **monitor condition** of an alarm is a value being set by the system, which is updated by the underlying monitoring service that detected the issue. Monitoring condition supports two values – “fired” and “resolved.”

**Yes**/No

**Monitoring our Azure Solution**

Assuming a VM status is “stopped” while using a static public IP, what will be the “**Resource Health”** status reported by Azure?

1. Available
2. **Unavailable (**the VM as a resource was deallocated and it is not related to the public IP type)
3. Running

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Assuming I would like to know when a specific VM was deallocated and by whom, then I can use the information collected by the “Activity Logs.”

**Yes**/No

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Host-level metrics coming from the underline VM host infrastructure (like CPU utilization, disk, and network usage) requires a dedicated collection agent to be installed inside each VM.

Yes/**No** (host-level metrics coming from the underline VM host infrastructure are collected automatically by Azure)

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Logs can be collected into Azure Log Analytics workspace. Under the “**Workspace Data Sources,”** we will be able to check which resources are connected to our specific workspace.

**Yes**/No

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

We can query logs that are collected in Azure Log Analytics by using a dedicated query language which is called Kusto or KQL - **Kusto Query Language.** At the basic level, a Kusto query is a read-only request to process data and return results. The request is stated in plain text, using a data-flow model designed to make the syntax easy to read.

**Yes**/No

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Assuming you would like to query from the performance table the latest 100 records about a metric called “Processor” and organize them in descending order. What will be the Kusto query?

AzureActivity

| top 100 by TimeGenerated up

| search ObjectName == "Processor"

Perf

| top 100 by TimeGenerated desc

| where ObjectName == "Processor"

search in (AzureActivity) ObjectName == "Processor" | top 100

Perf

| where TimeGenerated > ago(100d)

| summarize max(Processor)

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Azure Monitor for VMs** is a tool to help us better manage a group of VMs and also get a deeper insight into the internal processes in each VM. It is out-of-the-box consolidated monitoring view dedicated to virtual machines. The “**Map” tab** can be used to display information on the internal processes that are running inside the VM. Also, it will show us how each process inside this VM is connected on the network level to other computers.

**Yes**/No

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*