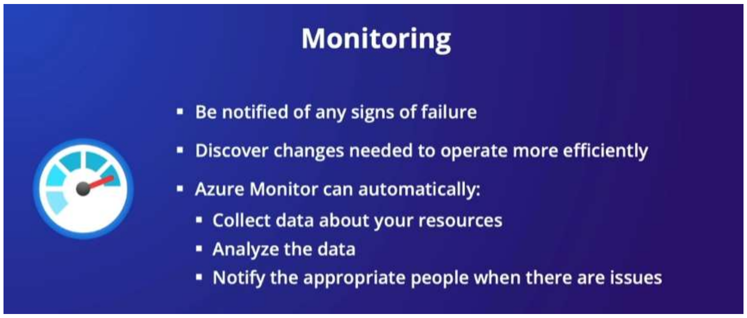
Azure Monitor metrics, logs and Alerts

Friday, April 28, 2023 9:42 AM

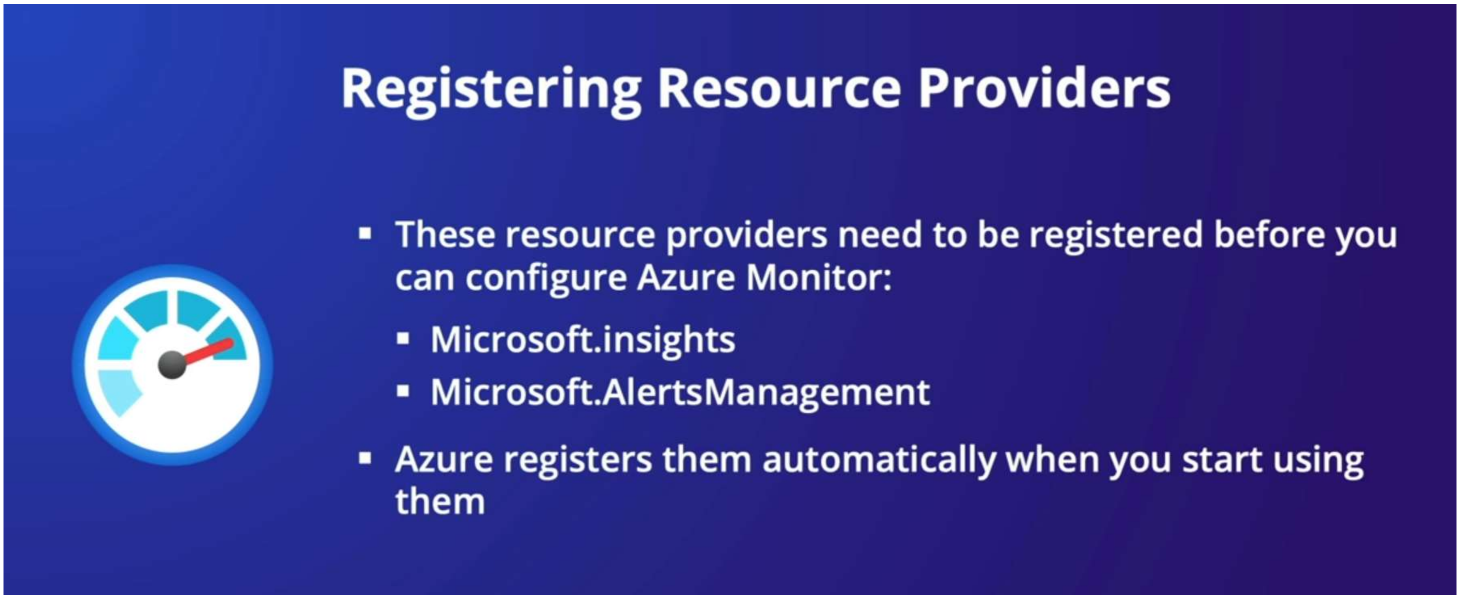


Monitoring

- Be notified of any signs of failure
- Discover changes needed to operate more efficiently
- Azure Monitor can automatically:
  - Collect data about your resources
  - Analyze the data
  - Notify the appropriate people when there are issues

Screen clipping taken: 4/28/2023 9:49 AM

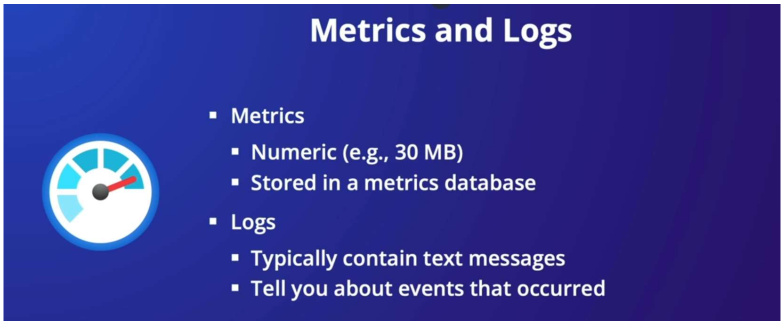
Capture some info without any config



Registering Resource Providers

- These resource providers need to be registered before you can configure Azure Monitor:
  - Microsoft.insights
  - Microsoft.AlertsManagement
- Azure registers them automatically when you start using them

Screen clipping taken: 4/28/2023 9:52 AM

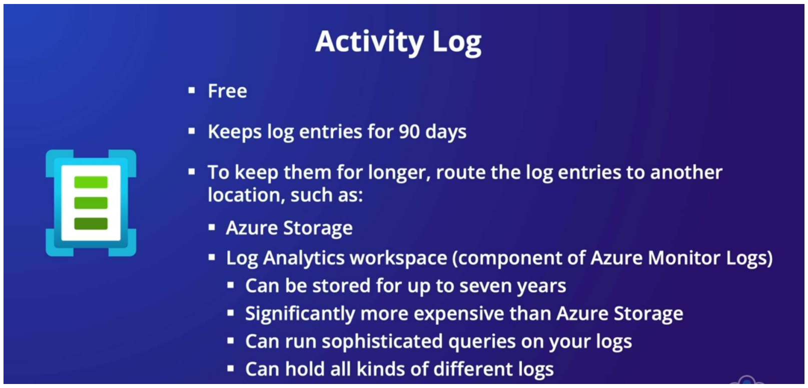


Metrics and Logs

- Metrics
  - Numeric (e.g., 30 MB)
  - Stored in a metrics database
- Logs
  - Typically contain text messages
  - Tell you about events that occurred

Screen clipping taken: 4/28/2023 9:52 AM

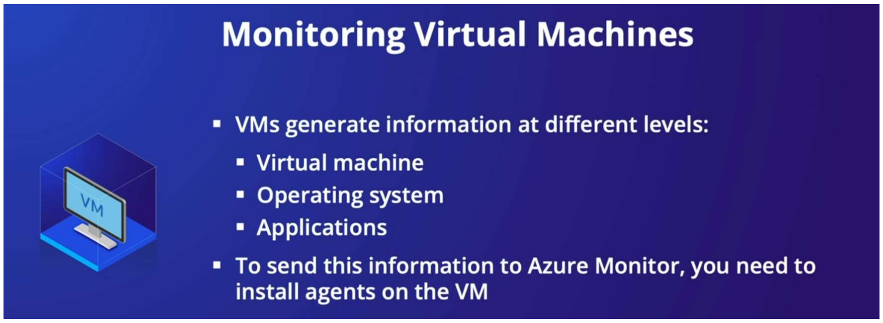
activity log → contains all of the subsc level events about your resource rather than events that happened within the resource.



Activity Log

- Free
- Keeps log entries for 90 days
- To keep them for longer, route the log entries to another location, such as:
  - Azure Storage
  - Log Analytics workspace (component of Azure Monitor Logs)
    - Can be stored for up to seven years
    - Significantly more expensive than Azure Storage
    - Can run sophisticated queries on your logs
    - Can hold all kinds of different logs

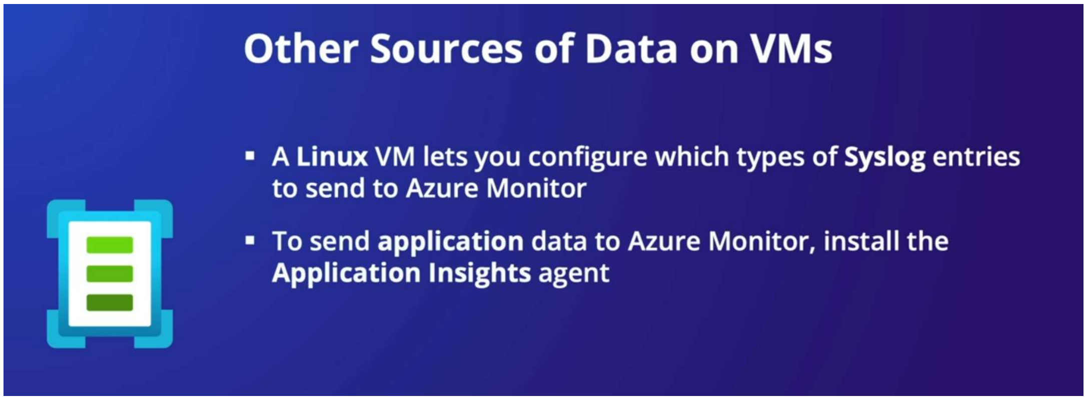
Screen clipping taken: 4/28/2023 9:57 AM



Monitoring Virtual Machines

- VMs generate information at different levels:
  - Virtual machine
  - Operating system
  - Applications
- To send this information to Azure Monitor, you need to install agents on the VM

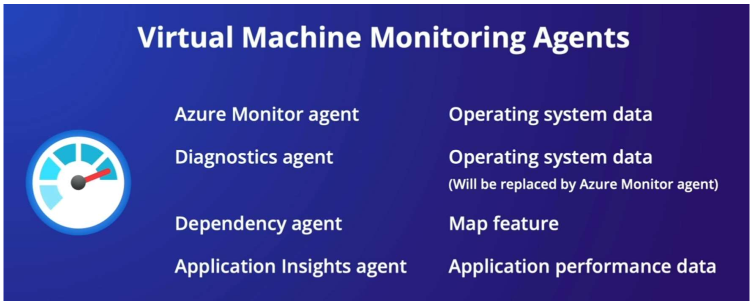
Screen clipping taken: 4/28/2023 10:14 AM



Other Sources of Data on VMs

- A **Linux** VM lets you configure which types of **Syslog** entries to send to Azure Monitor
- To send **application** data to Azure Monitor, install the **Application Insights** agent

Screen clipping taken: 4/28/2023 10:28 AM

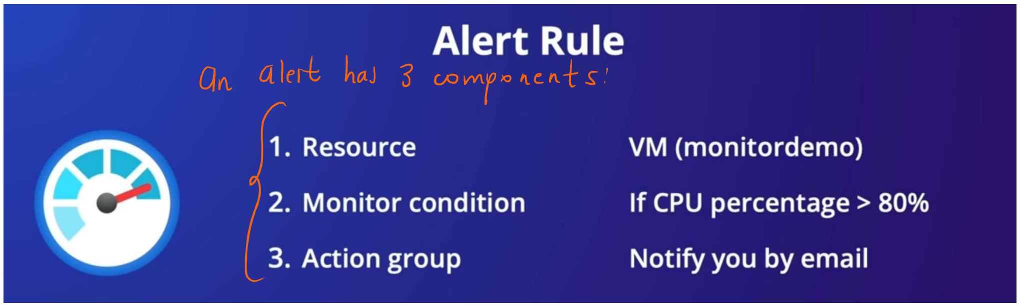


Virtual Machine Monitoring Agents

Azure Monitor agent	Operating system data
Diagnostics agent	Operating system data (Will be replaced by Azure Monitor agent)
Dependency agent	Map feature
Application Insights agent	Application performance data

Screen clipping taken: 4/28/2023 10:29 AM

Alerts
Screen clipping taken: 4/28/2023 9:57 AM

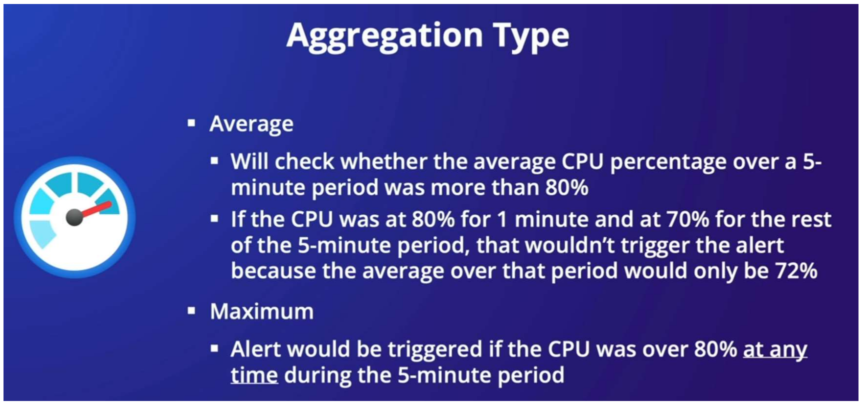


Alert Rule

an alert has 3 components!

1. Resource — VM (monitordemo)
2. Monitor condition — If CPU percentage > 80%
3. Action group — Notify you by email

Screen clipping taken: 4/28/2023 3:59 PM

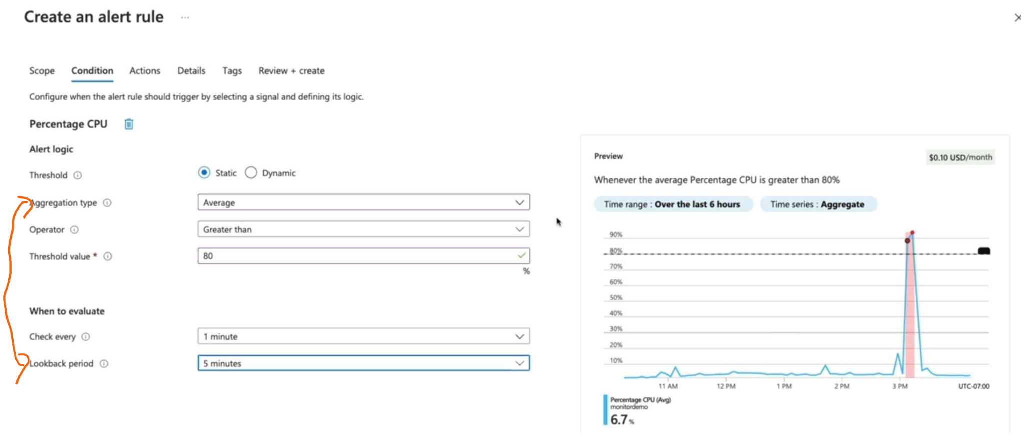


Aggregation Type

- Average
  - Will check whether the average CPU percentage over a 5-minute period was more than 80%
  - If the CPU was at 80% for 1 minute and at 70% for the rest of the 5-minute period, that wouldn't trigger the alert because the average over that period would only be 72%
- Maximum
  - Alert would be triggered if the CPU was over 80% at any time during the 5-minute period

Screen clipping taken: 4/28/2023 4:10 PM

Screen clipping taken: 4/28/2023 3:58 PM



Create an alert rule

Configure when the alert rule should trigger by selecting a signal and defining its logic.

Percentage CPU

Alert logic

Threshold: ● Static ○ Dynamic

Aggregation type: Average

Operator: Greater than

Threshold value *: 80 %

When to evaluate

Check every: 1 minute

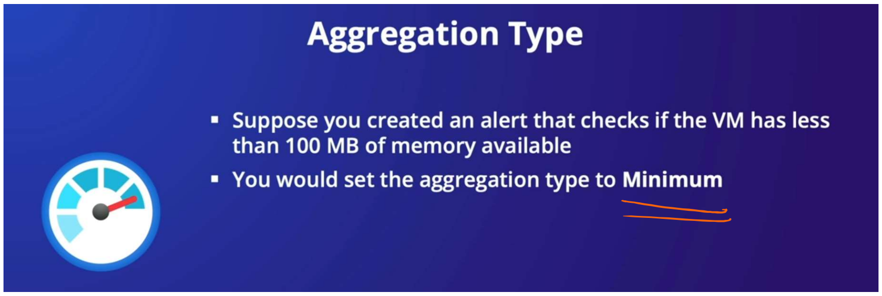
Lookback period: 5 minutes

Preview — $0.10 USD/month

Whenever the average Percentage CPU is greater than 80%

Time range : **Over the last 6 hours** — Time series : **Aggregate**

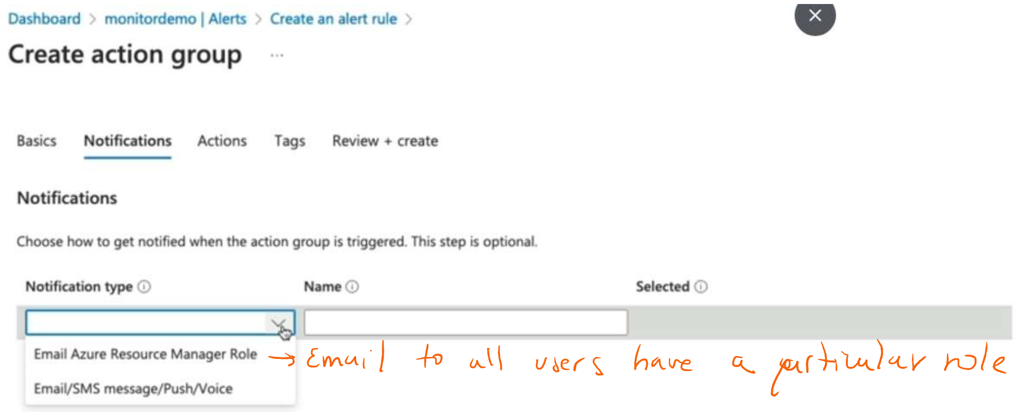
Screen clipping taken: 4/28/2023 4:13 PM



Aggregation Type

- Suppose you created an alert that checks if the VM has less than 100 MB of memory available
- You would set the aggregation type to **Minimum**

Screen clipping taken: 4/28/2023 4:15 PM



Dashboard > monitordemo | Alerts > Create an alert rule >

Create action group

Basics | **Notifications** | Actions | Tags | Review + create

Notifications

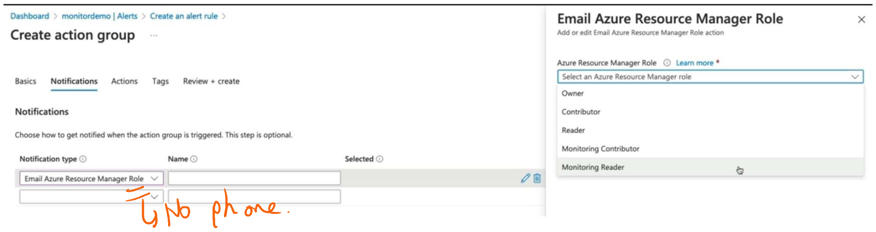
Choose how to get notified when the action group is triggered. This step is optional.

Notification type	Name	Selected

- Email Azure Resource Manager Role
- Email/SMS message/Push/Voice

→ Email to all users have a particular role.

Screen clipping taken: 4/28/2023 4:16 PM



Dashboard > monitordemo | Alerts > Create an alert rule >

Create action group

Basics | **Notifications** | Actions | Tags | Review + create

Notifications

Choose how to get notified when the action group is triggered. This step is optional.

Notification type	Name	Selected
Email Azure Resource Manager Role		

↳ No phone.

Email Azure Resource Manager Role

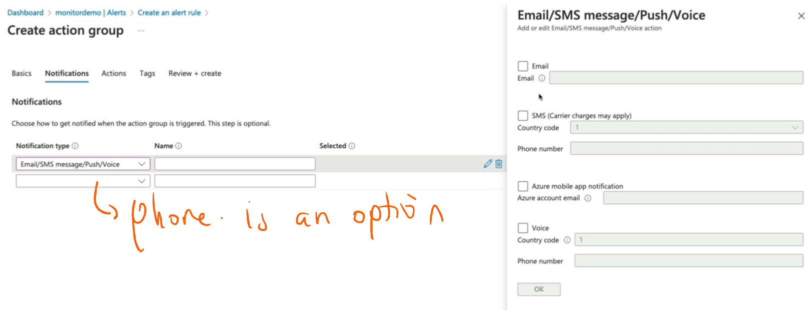
Add or edit Email Azure Resource Manager Role action

Azure Resource Manager Role ⓘ Learn more *

Select an Azure Resource Manager role

- Owner
- Contributor
- Reader
- Monitoring Contributor
- Monitoring Reader

Screen clipping taken: 4/28/2023 4:17 PM



Dashboard > monitordemo | Alerts > Create an alert rule >

Create action group

Basics | **Notifications** | Actions | Tags | Review + create

Notifications

Choose how to get notified when the action group is triggered. This step is optional.

Notification type	Name	Selected
Email/SMS message/Push/Voice		

↳ phone. is an option

Email/SMS message/Push/Voice

Add or edit Email/SMS message/Push/Voice action

□ Email

Email ⓘ

□ SMS (Carrier charges may apply)

Country code: 1

Phone number

□ Azure mobile app notification

Azure account email ⓘ

□ Voice

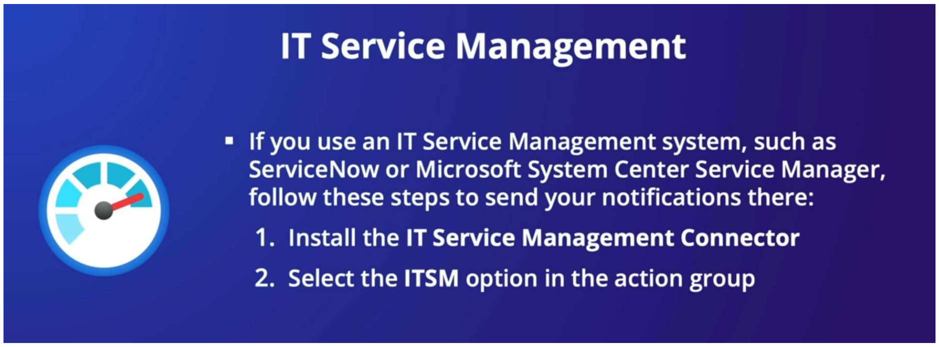
Country code ⓘ: 1

Phone number

OK

Screen clipping taken: 4/28/2023 4:18 PM

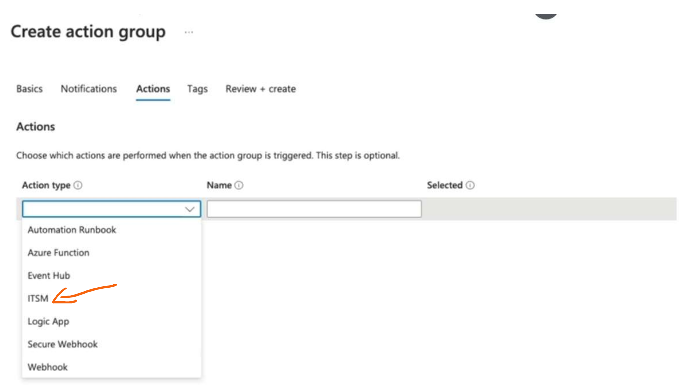
the disadvantage of doing it this way is that you'd have to enter this info manually. and you'd have to do this for every action group you created.



IT Service Management

- If you use an IT Service Management system, such as ServiceNow or Microsoft System Center Service Manager, follow these steps to send your notifications there:
  1. Install the IT **Service Management Connector**
  2. Select the **ITSM** option in the action group

Screen clipping taken: 4/28/2023 4:32 PM



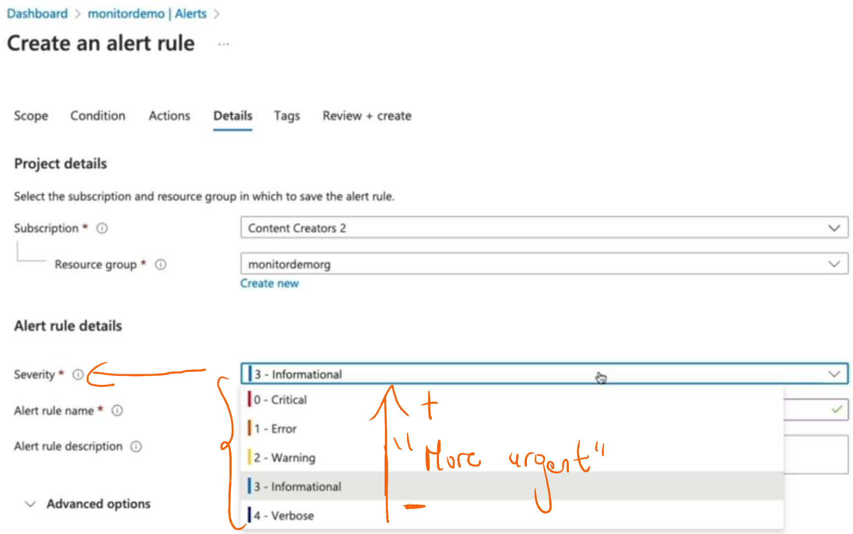
Create action group

Basics Notifications Actions Tags Review + create

Actions

Choose which actions are performed when the action group is triggered. This step is optional.

Screen clipping taken: 4/28/2023 4:33 PM



Dashboard > monitordemo | Alerts >

Create an alert rule

Scope Condition Actions Details Tags Review + create

Project details

Select the subscription and resource group in which to save the alert rule.

Subscription * : Content Creators 2

Resource group * : monitordemorg

Create new

Alert rule details

Severity * : 3 - Informational

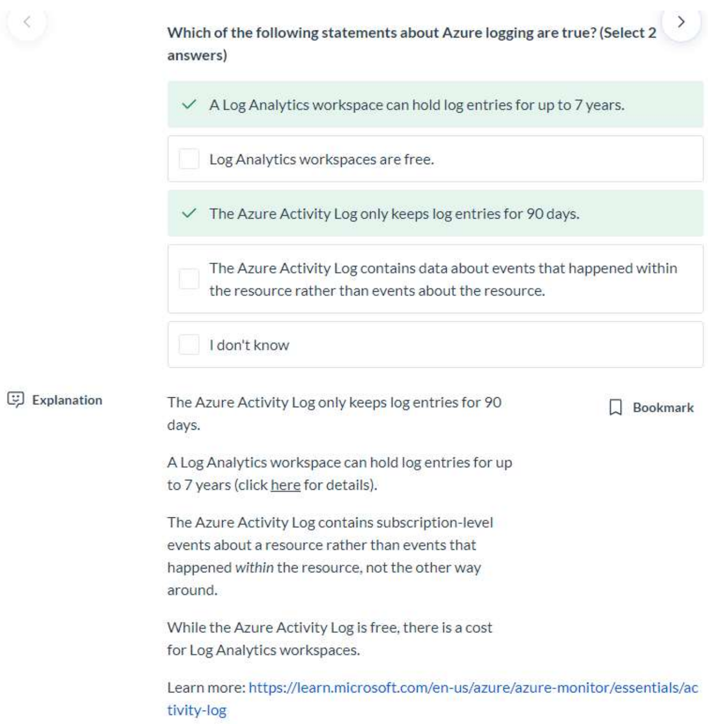
Alert rule name *

Alert rule description

Advanced options

Screen clipping taken: 4/28/2023 4:35 PM

You can edit the alerts.



Which of the following statements about Azure logging are true? (Select 2 answers)

- ✓ A Log Analytics workspace can hold log entries for up to 7 years.
- □ Log Analytics workspaces are free.
- ✓ The Azure Activity Log only keeps log entries for 90 days.
- □ The Azure Activity Log contains data about events that happened within the resource rather than events about the resource.
- □ I don't know

Explanation

The Azure Activity Log only keeps log entries for 90 days.

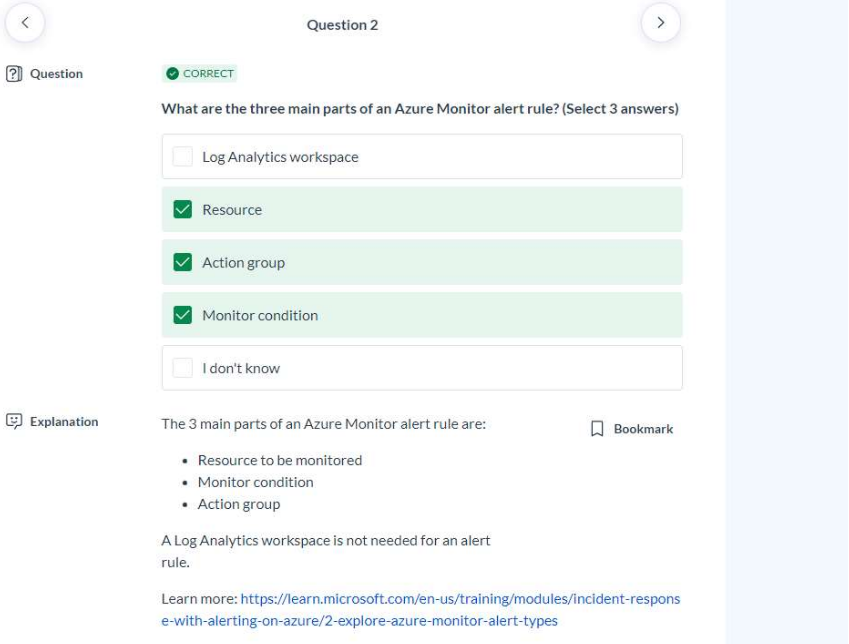
A Log Analytics workspace can hold log entries for up to 7 years (click here for details).

The Azure Activity Log contains subscription-level events about a resource rather than events that happened *within* the resource, not the other way around.

While the Azure Activity Log is free, there is a cost for Log Analytics workspaces.

Learn more: https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/activity-log

Screen clipping taken: 4/28/2023 5:58 PM



Question 2

Question

CORRECT

What are the three main parts of an Azure Monitor alert rule? (Select 3 answers)

- □ Log Analytics workspace
- ☑ Resource
- ☑ Action group
- ☑ Monitor condition
- □ I don't know

Explanation

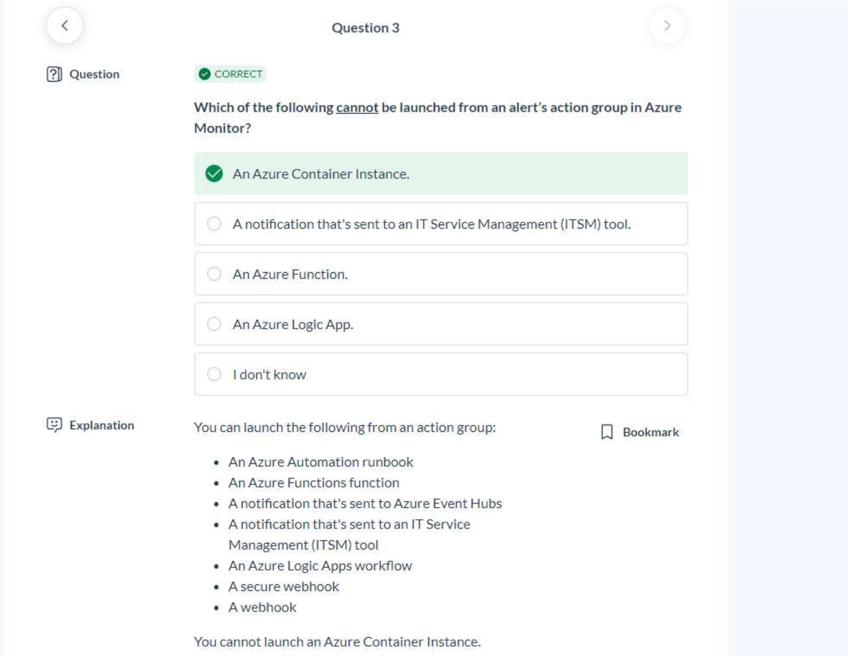
The 3 main parts of an Azure Monitor alert rule are:

- Resource to be monitored
- Monitor condition
- Action group

A Log Analytics workspace is not needed for an alert rule.

Learn more: https://learn.microsoft.com/en-us/training/modules/incident-response-with-alerting-on-azure/2-explore-azure-monitor-alert-types

Screen clipping taken: 4/28/2023 5:59 PM



Question 3

Question

✓ CORRECT

Which of the following <u>cannot</u> be launched from an alert's action group in Azure Monitor?

✓ An Azure Container Instance.

○ A notification that's sent to an IT Service Management (ITSM) tool.

○ An Azure Function.

○ An Azure Logic App.

○ I don't know

Explanation

Bookmark

You can launch the following from an action group:

- An Azure Automation runbook
- An Azure Functions function
- A notification that's sent to Azure Event Hubs
- A notification that's sent to an IT Service Management (ITSM) tool
- An Azure Logic Apps workflow
- A secure webhook
- A webhook

You cannot launch an Azure Container Instance.

Screen clipping taken: 4/28/2023 5:59 PM