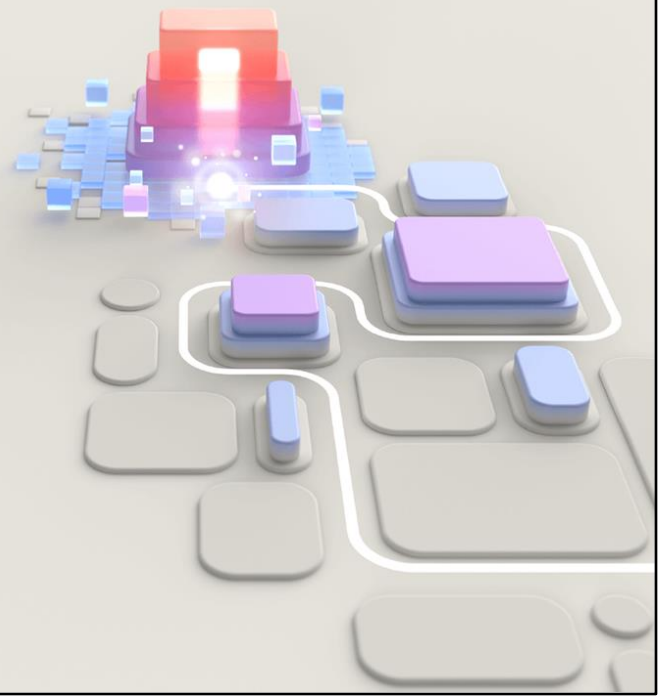
Microsoft

Azure Monitoring

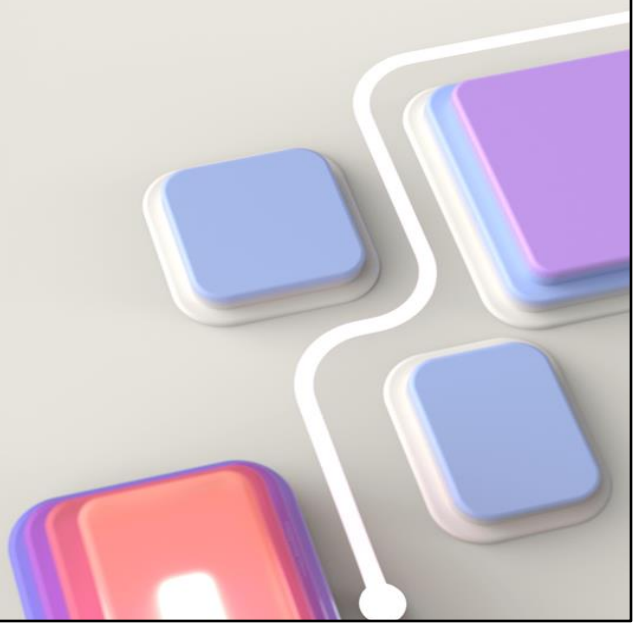


Learning Objectives - Administer Monitoring

- Configure Azure Monitor
- Improve incident response with alerting on Azure
- Configure Log Analytics
- Lab 11 – Implement Monitoring

This content is part of the AZ-104: Monitor and back up Azure resources (https://docs.microsoft.com/learn/paths/az-104-monitor-backup-resources/) learning path.

Configure Azure Monitor



Learning Objectives - Configure Azure Monitor

- Describe Azure Monitor Key Capabilities
- Describe Azure Monitor Components
- Define Metrics and Logs
- Identify Data Types
- Describe Activity Log Events
- Learning Recap

Monitor and maintain Azure resources (10–15%): Monitor resources in Azure

- Interpret metrics in Azure Monitor
- Configure log settings in Azure Monitor
- Configure and interpret monitoring of virtual machines, storage accounts, and networks by using Azure Monitor Insights

Describe Azure Monitor Key Capabilities

Monitor & Visualize Metrics

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

Explore Metrics

Core monitoring for Azure services

Query & Analyze Logs

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

Search Logs

Collects metrics, activity logs, and diagnostic logs

Setup Alert & Actions

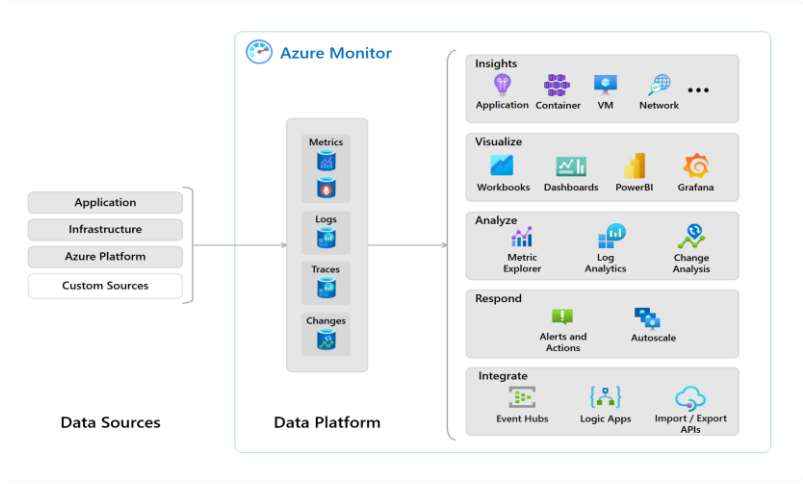
Alerts notify you of critical conditions and potentially take corrective automated actions based on triggers from metrics or logs.

Create Alert

Use for time critical alerts and notifications

Understand Azure Monitor Components

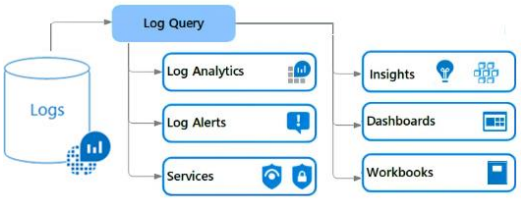
- Application monitoring data
- Guest OS monitoring
- Azure resource monitoring
- Azure subscription monitoring
- Azure tenant monitoring



What is Azure Monitor - https://docs.microsoft.com/azure/azure-monitor/overview

Sources of monitoring data for Azure Monitor - https://docs.microsoft.com/azure/azure-monitor/platform/data-sources

Define Metrics and Logs



- Metrics are numerical values that describe some aspect of a system at a point in time
- They are lightweight and capable of supporting near real-time scenarios

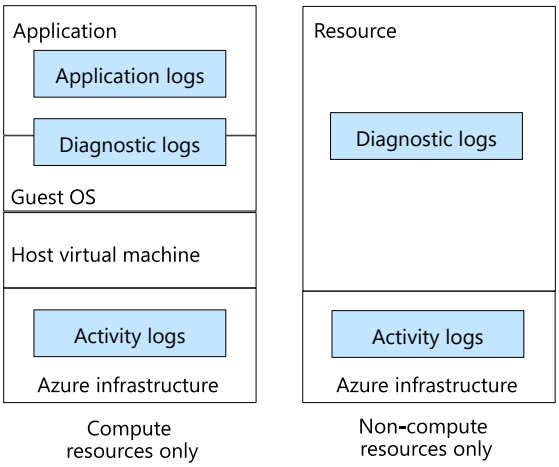
- Logs contain different kinds of data organized into records with different sets of properties for each type
- Telemetry (events, traces) and performance data can be combined for analysis

Metrics - https://docs.microsoft.com/azure/azure-monitor/platform/data-platform-metrics

Logs - https://docs.microsoft.com/azure/azure-monitor/platform/data-platform-logs

Describe Activity Log Events

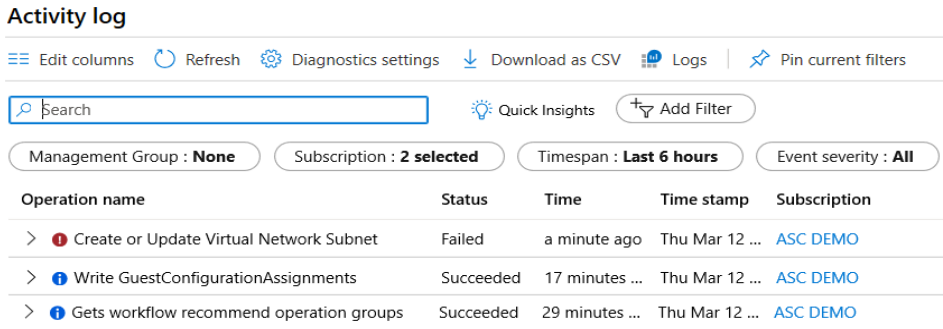
- Send data to Log Analytics for advanced search and alerts
- Query or manage events in the Portal, PowerShell, CLI, and REST API
- Stream information to Event Hub
- Archive data to a storage account
- Analyze data with Power BI



Azure Activity log - https://docs.microsoft.com/azure/azure-monitor/platform/activity-log

Send Azure Activity log to Log Analytics workspace using Azure portal - https://docs.microsoft.com/azure/azure-monitor/learn/quick-collect-activity-log-portal

Query the Activity Log



Filter by Management group, Subscription, Timespan, and Event Severity

Add a filter, like Event Category (Security, Recommendations, Alerts)

Pin current filters and download as CSV

Query the Activity Log in the Azure portal - https://docs.microsoft.com/azure/monitoring-and-diagnostics/monitoring-overview-activity-logs#query-the-activity-log-in-the-azure-portal

Learning Recap – Configure Azure Monitor

Check your knowledge questions and additional study

- Analyze your Azure infrastructure by using Azure Monitor logs (sandbox)
- Monitor your Azure virtual machines with Azure Monitor
- Monitor, diagnose, and troubleshoot your Azure storage (sandbox)

A *sandbox* indicates an additional hands-on exercise.

Additional questions in Office Forms - https://forms.office.com/Pages/ShareFormPage.aspx?id=v4j5cvGGr0GRqy180BHbR5NEFZBpuAZBgxPOGXi_gX5UOFlRUEszMlRFTkpFT0E3Q1oxRjlQVk81MS4u&sharetoken=8yKD9q6v9z0tcrXy3tS5&wdLOR=c3820A896-48CD-46AD-BE50-F09068C1280F

Name at least three data sources that can be used by Azure Monitor.

Answer: Azure Monitor can ingest many different data sources. Sources include application code, operating system, resource, subscription, and tenant data. You can even create your own custom data source. Data sources generally fall into two categories metrics and logs. Metrics are numerical values that describe some aspect of a system at a point in time. For example, virtual machine CPU

performance. Logs contain data organized into records with different sets of properties for each type. For example, the activity log shows subscription-level events. This includes such information as when a resource is modified or when a virtual machine is started.

Improve incident response with alerting on Azure

Improve incident response with alerting on Azure - Overview

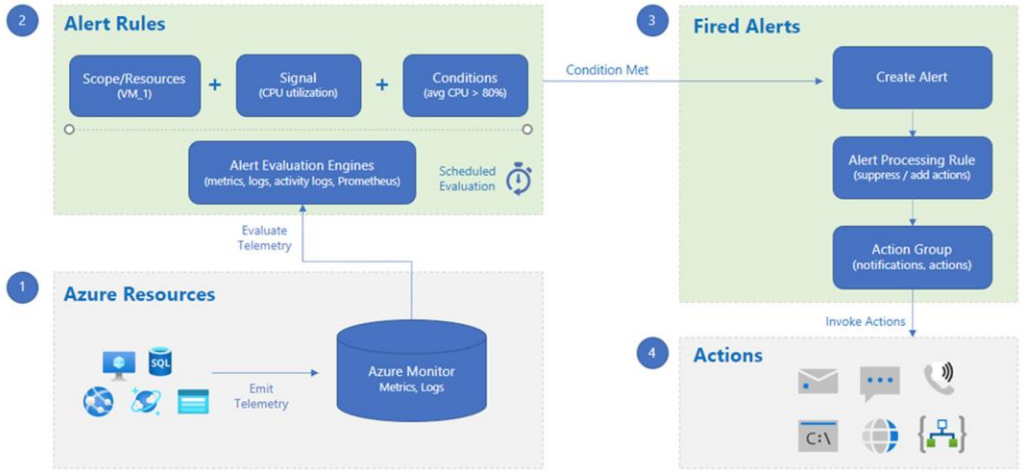
- Manage Azure Monitor Alerts
- Create Alert Rules
- Create Action Groups
- Demonstration – Alerts
- Learning Recap

Monitor and maintain Azure resources (10–15%): Monitor resources in Azure

- Set up alert rules, action groups, and alert processing rules in Azure Monitor

There is a new module for this is Improve incident response with alerting on Azure - Training | Microsoft Learn, https://learn.microsoft.com/training/modules/incident-response-with-alerting-on-azure/. The slides cover the certification topics and do not match the new module exactly. There are exercises in the new module that we are not using.

Manage Azure Monitor Alerts



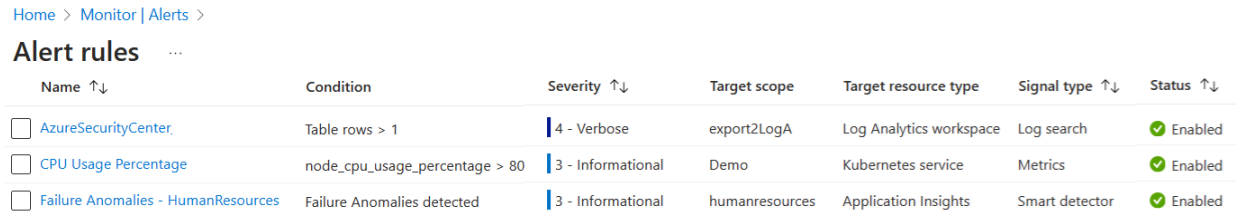
The new alerts experience in Azure Monitor - https://docs.microsoft.com/azure/monitoring-and-diagnostics/monitoring-overview-unified-alerts

Demonstration – Alerts

- Create and configure an alert rule
- Review alerts

Demonstration Azure Alerts - https://microsoftlearning.github.io/AZ-104-MicrosoftAzureAdministrator/Instructions/Demos/11%20-%20Administer%20Monitoring.html#configure-azure-alerts

Create Alert Rules



- Alert rules combine the resources to be monitored, the signal or data from the resource, and the conditions.
- You can enable recommended out-of-the-box alert rules in the Azure portal.

Respond to events with Azure Monitor Alerts - https://docs.microsoft.com/azure/azure-monitor/learn/tutorial-response

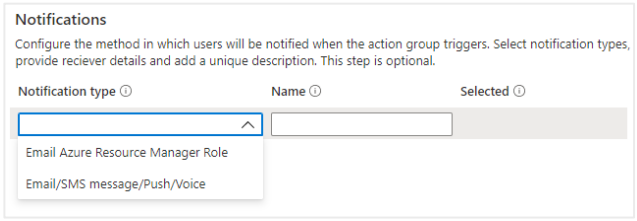
Create, view, and manage metric alerts using Azure Monitor - https://docs.microsoft.com/azure/azure-monitor/platform/alerts-metric

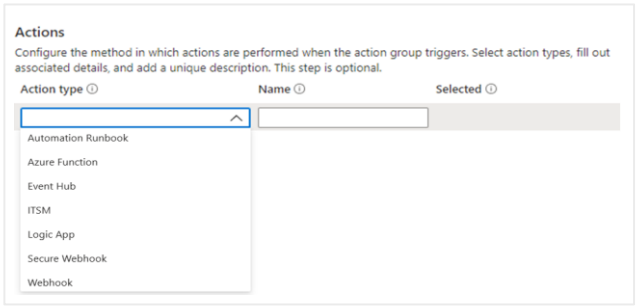
Recommended out-of-the-box alert rules - https://learn.microsoft.com/azure/azure-monitor/alerts/alerts-manage-alert-rules#enable-recommended-alert-rules-in-the-azure-portal

Create Action Groups

Defines a set of notifications and/or actions when an alert is triggered

You can add up to five action groups to an alert rule. Multiple alert rules can use the same action group.





Create and manage action groups in the Azure portal - https://docs.microsoft.com/azure/azure-monitor/platform/action-groups

Learning Recap – Configure Azure Alerts

Check your knowledge questions and additional study

- Improve incident response with alerting on Azure (sandbox)
- Configure for alerts and detections in Microsoft Defender for Endpoint
- Remediate security alerts using Microsoft Defender for Cloud

A *sandbox* indicates an additional hands-on exercise.

Additional questions in Office Forms - https://forms.office.com/Pages/ShareFormPage.aspx?id=v4j5cvGGr0GRqy180BHbR5NEFZBpuAZBgxPOGXi_gX5UOFlRUEszMlRFTkpFT0E3Q1oxRjlQVk81MS4u&sharetoken=8yKD9q6v9z0tcrXy3tS5&wdLOR=c3820A896-48CD-46AD-BE50-F09068C1280F

You need to configure several Azure alerts. How will you assign/notify the help desk personnel when an alert is triggered? What methods can be used to notify them?

Answer: The help desk personnel should be added to an action group. An action group is a collection of notification preferences. Alerts use action groups to notify users that an alert has been triggered. Various alerts may use the same action group or different action groups

depending on the user's requirements. Notification methods include push notifications to the Azure mobile app, email, SMS, and voice.

You are reviewing the Azure Monitor alerts page. What alert states (statuses) are possible?

Answer: There are three alert states *New*, *Acknowledged*, and *Closed*. *New* indicates an issue has been detected and hasn't been reviewed. *Acknowledged* indicates an administrator has reviewed the alert and started working on it. *Closed* indicates the issue has been resolved. You can reopen a closed alert if the issue returns.

Configure Log Analytics

Monitor and maintain Azure resources (10–15%)

Monitor resources by using Azure Monitor

- Configure and interpret metrics
- Configure Azure Monitor Logs

Learning Objectives - Configure Log Analytics

- Determine Log Analytics Uses
- Create a Workspace
- Query Log Analytics Data
- Structure Log Analytics Queries
- Demonstration – Log Analytics
- Learning Recap

Monitor and maintain Azure resources (10–15%): Monitor resources in Azure

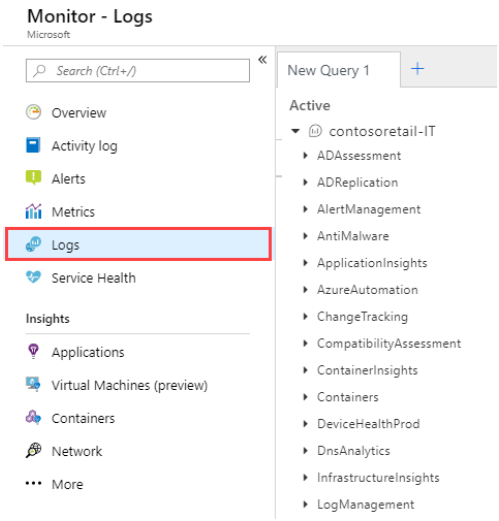
- Query and analyze logs in Azure Monitor

Determine Log Analytics Uses

A service that helps you collect and analyze data generated by resources in your cloud and on-premises environments

Write log queries and interactively analyze their results

Examples include assessing system updates and troubleshooting operational incidents



Overview of Azure Monitor agents - https://docs.microsoft.com/azure/azure-monitor/platform/agents-overview

Demonstration – Log Analytics

- Review built-in log queries
- Review the KQL language

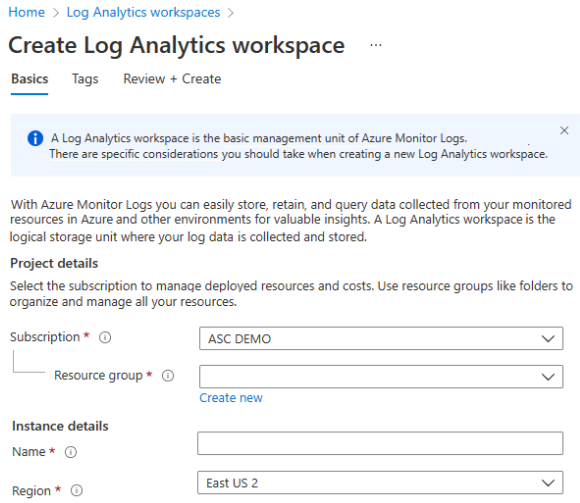
Demonstration Log Analytics - https://microsoftlearning.github.io/AZ-104-MicrosoftAzureAdministrator/Instructions/Demos/11%20-%20Administer%20Monitoring.html#configure-log-analytics

Create a Workspace

A workspace is an Azure resource and is a container where data is collected, aggregated, analyzed, and presented

You can have multiple workspaces per Azure subscription, and you can have access to more than one workspace

A workspace provides a geographic location, data isolation, and scope



Create a Log Analytics workspace in the Azure portal -https://docs.microsoft.com/azure/azure-monitor/learn/quick-create-workspace

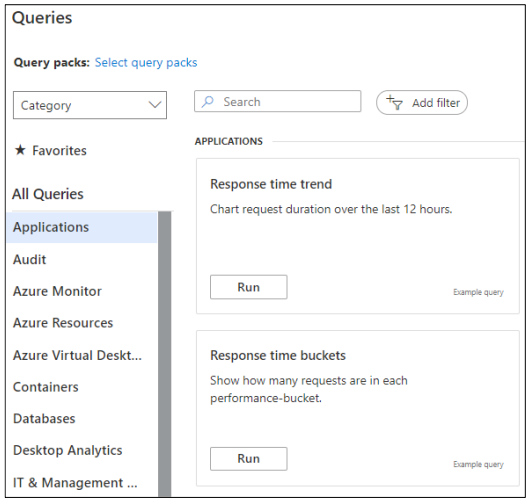
Query Log Analytics Data

Common queries and a query language (KQL) for custom searches

Quickly retrieve and consolidate data in the repository

Save or have log searches run automatically to create an alert

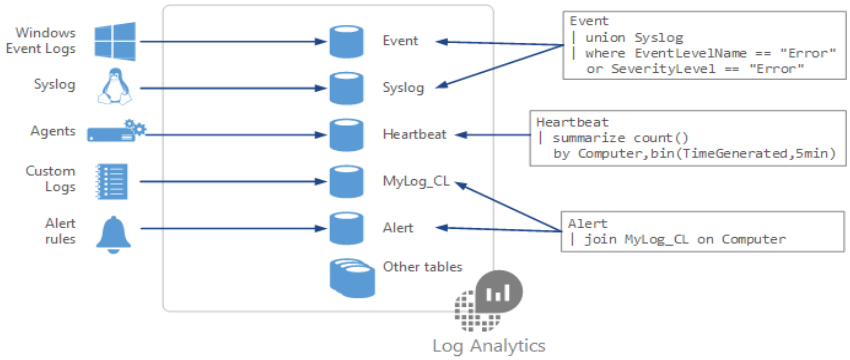
Export the data to Power BI or Excel



Overview of log queries in Azure Monitor - https://docs.microsoft.com/azure/azure-monitor/log-query/log-query-overview

Get started with log queries in Azure Monitor - https://docs.microsoft.com/azure/azure-monitor/log-query/get-started-queries

Structure Log Analytics Queries




```
Event
| where (EventLevelName == "Error")
| where (TimeGenerated > ago(1days))
| summarize ErrorCount = count() by Computer
| top 10 by ErrorCount desc
```


Azure Monitor log queries - https://docs.microsoft.com/azure/azure-monitor/log-query/query-language

Azure Monitor log query examples - https://docs.microsoft.com/azure/azure-monitor/log-query/examples

Learning Recap – Configure Log Analytics

- Write your first query with Kusto Query Language

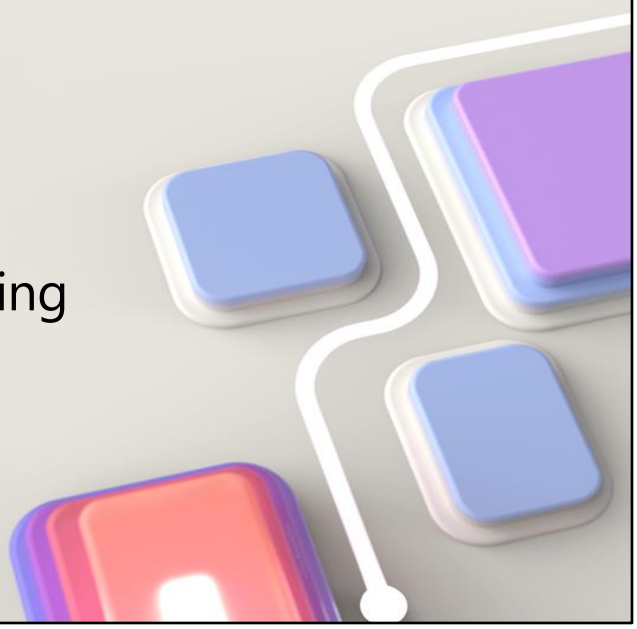
Check your knowledge questions and additional study

Additional questions in Office Forms - https://forms.office.com/Pages/ShareFormPage.aspx?id=v4j5cvGGr0GRqy180BHbR5NEFZBpuAZBgxPOGXi_gX5UOFlRUEszMlRFTkpFT0E3Q1oxRjlQVk81MS4u&sharetoken=8yKD9q6v9z0tcrXy3tS5&wdLOR=c3820A896-48CD-46AD-BE50-F09068C1280F

You would like to structure queries against the Windows Event log. Specifically, you would like to identify any errors. What product should you use? What query language is available to construct the query?

Answer: You should use a Log Analytics workspace. The workspace can receive data from the Windows Event log. The event records can then be visualized or queried. Azure uses the Kusto query language. Windows Event logs are stored in the Event table. to query the event table for errors, use this command: Event | where (EventLevelName == "Error").

Lab – Implement Monitoring



Lab 11 – Implement monitoring

In this lab, you learn about Azure Monitor.

You learn to create an alert to be sent to an action group.

You trigger the alert and check the activity log.

Job Skills

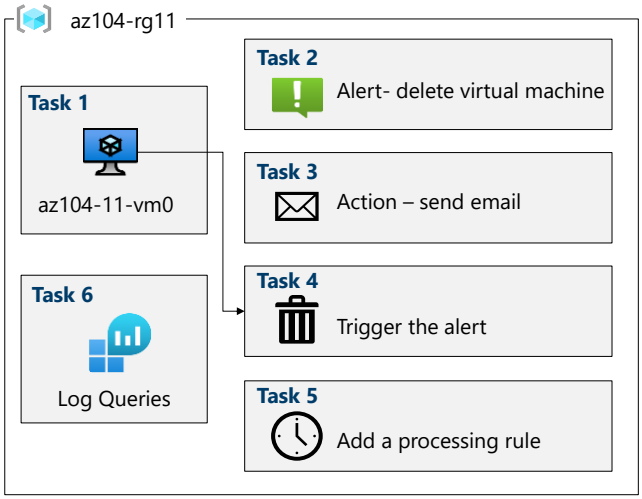
Task 1: Use a template to provision an infrastructure.
Task 2: Create an alert.
Task 3: Configure action group notifications.
Task 4: Trigger an alert and confirm it is working.
Task 5: Configure an alert rule.
Task 6: Use Azure Monitor log queries.

Next slide for an architecture diagram

This last lab is little shorter but puts together a practical example of monitoring.

Lab 11 - https://microsoftlearning.github.io/AZ-104-MicrosoftAzureAdministrator/Instructions/Labs/LAB_11-Implement_Monitoring.html

Lab 11 – Architecture diagram



End of presentation