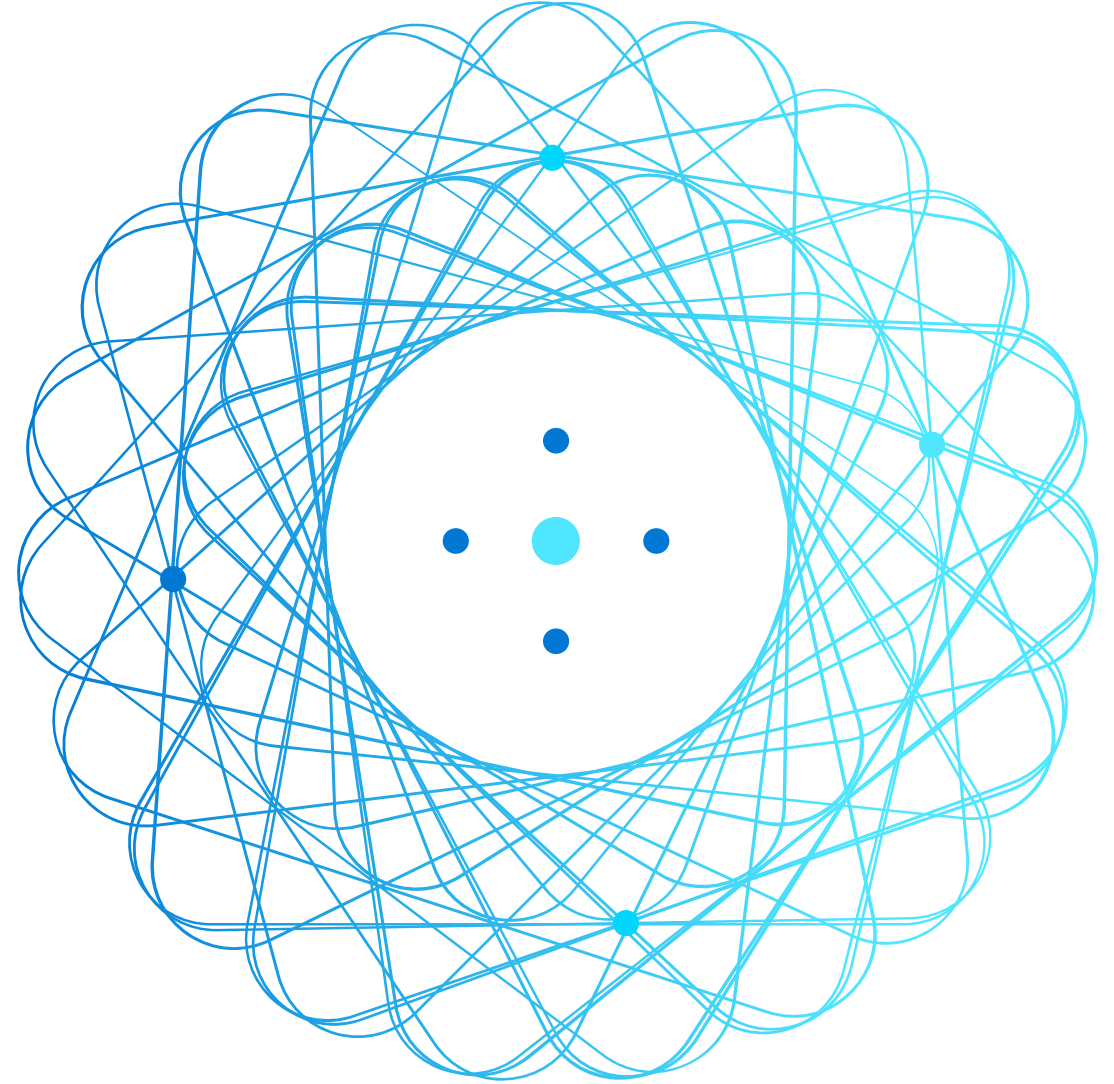# AZ-220T01
Module 09: Solution testing, diagnostics, and logging
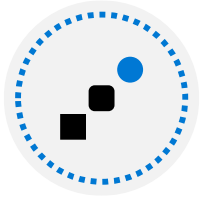
Lesson 1: Learning objectives
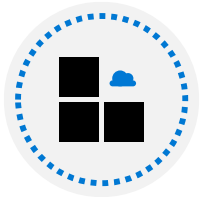
Module 9 – Learning objectives

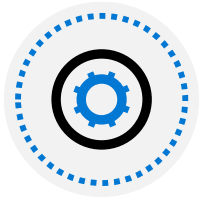Describe the options for monitoring and logging an Azure IoT solution

Configure Azure Monitor to support of an IoT solution

Configure IoT Hub Metrics to support of an IoT solution
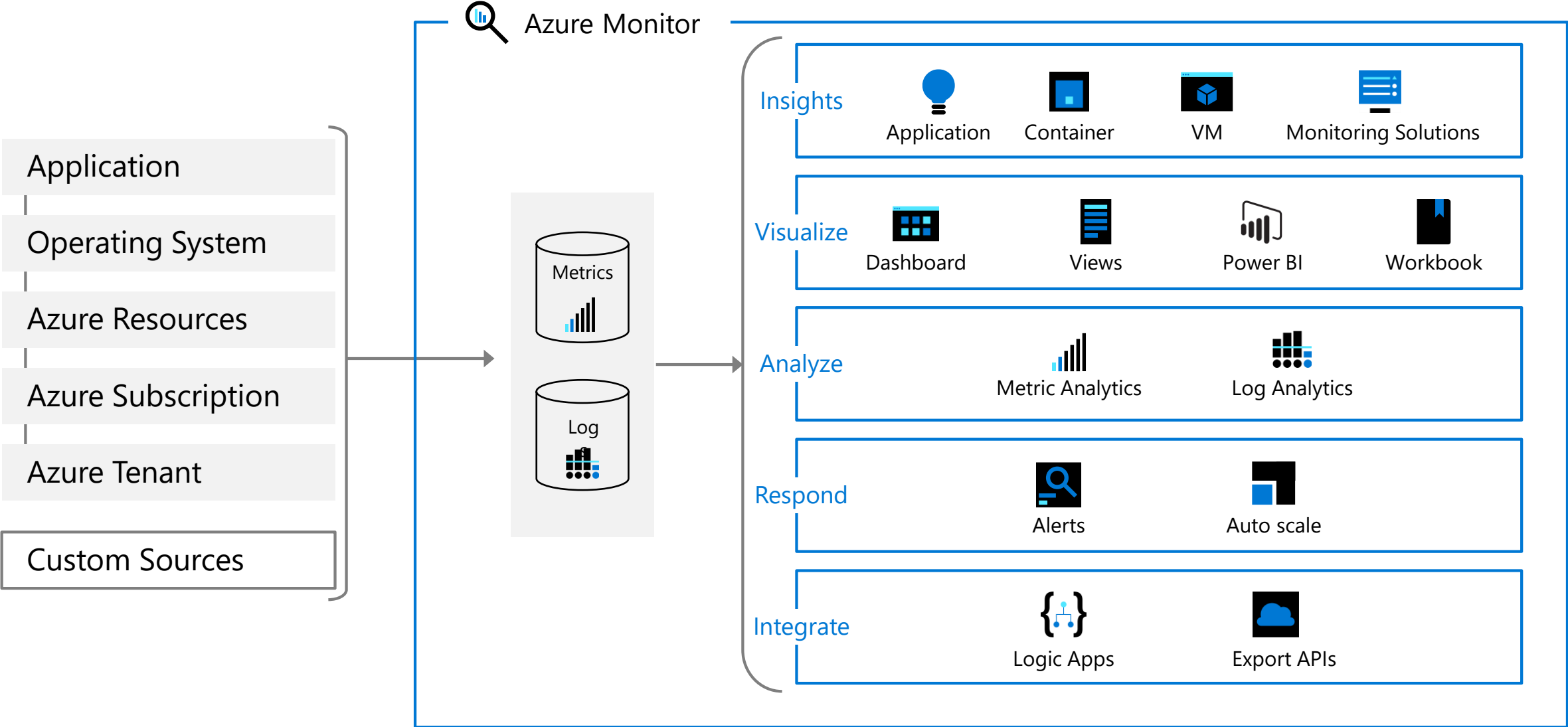
Implement diagnostics logging

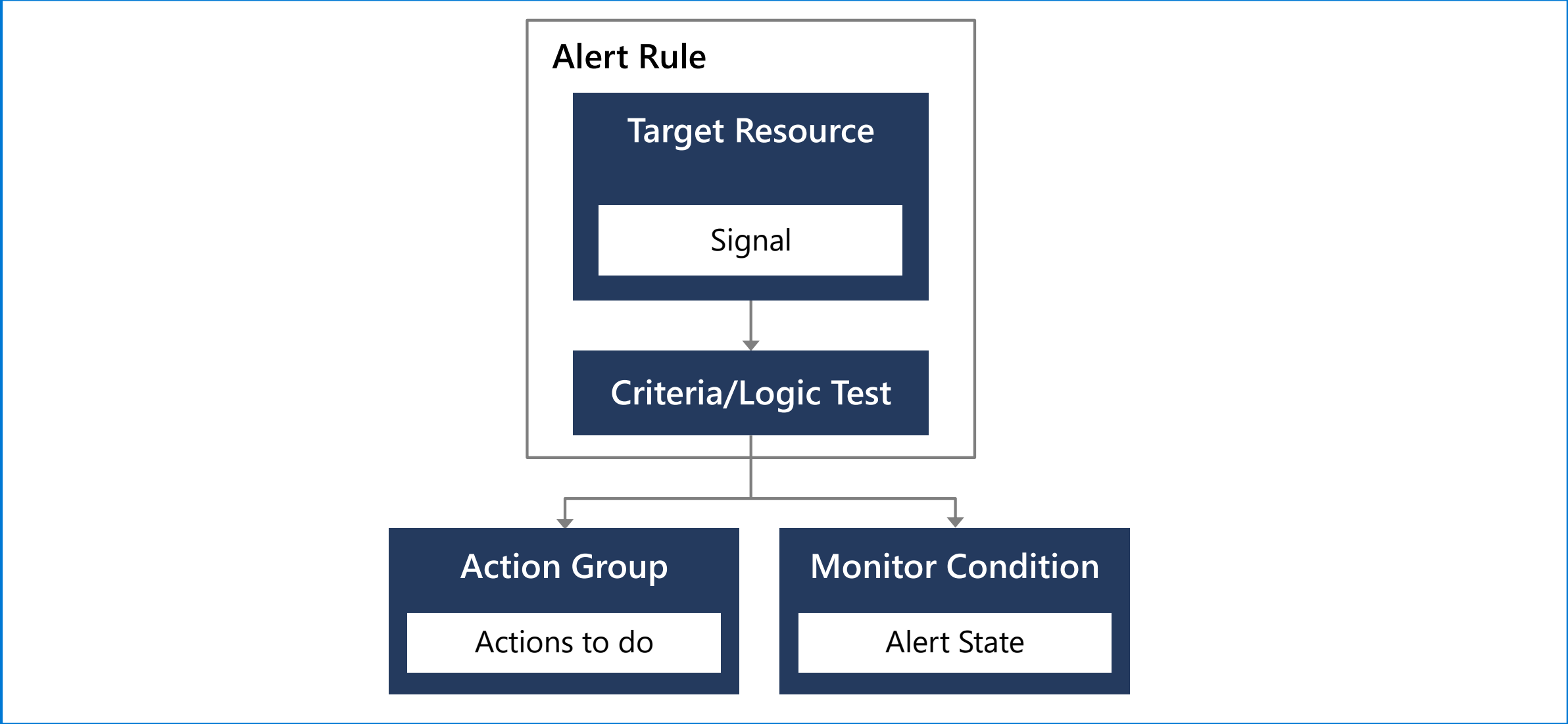Troubleshoot IoT device connection and communication issues

Lesson 2: Monitoring and logging

Azure Monitor

Azure Monitor

Sources (left column):
- Application
- Operating System
- Azure Resources
- Azure Subscription
- Azure Tenant
- Custom Sources

Data stores:
- Metrics
- Log

Insights:
- Application
- Container
- VM
- Monitoring Solutions

Visualize:
- Dashboard
- Views
- Power BI
- Workbook

Analyze:
- Metric Analytics
- Log Analytics

Respond:
- Alerts
- Auto scale

Integrate:
- Logic Apps
- Export APIs

Azure Monitor alerts

IoT Hub metrics

Diagnostics tools

Use Azure Monitor:

Understand the logs

Read logs from Azure Event Hubs

Use Azure Resource Health

Diagnostics tools

Use Azure Monitor:

Understand the logs

Read logs from Azure Event Hubs

Use Azure Resource Health

Diagnostics tools

Use Azure Monitor:

Understand the logs

Read logs from Azure Event Hubs

Use Azure Resource Health

Diagnostics tools

Use Azure Monitor:

Understand the logs

Read logs from Azure Event Hubs

Use Azure Resource Health

Device connection state and lifecycle notifications

Heartbeat Pattern – regularly timed device-to-cloud messages validating working connectivity

Device and Module Lifecycle Notifications – used for information on device and module identity creation and deletion:

Not seen by default

To see them, create a route and to set the Data Source equal to `DeviceLifecycleEvents` or `ModuleLifecycleEvents`

Quotas and throttling
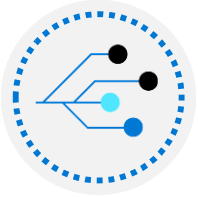
Operation throttles:

Throttling limits:
- Throttling is the same for all tiers
- Limits are based on the edition within the tier and the number of units

Traffic shaping:
- You can exceed the throttling limit for a short time
- After that, requests will be queued
- If too many requests are queued, messages start failing with a 429 error

Identity registry operations throttling exists because there are import and export capabilities for bulk at-once provisioning

Device connections throttling is around creation of a new connection, not around number of existing connections

Other limits

Lesson 3: Troubleshooting

Connection and retry patterns

Error patterns – the device SDKs process three categories of errors

1 *Network errors* – Disconnected sockets, name resolution errors

2 *Protocol-level errors* – Detached links, expired sessions

3 *Application-level errors* – Invalid credentials, service throttling

Retry patterns – the device SDKs have three retry policies

1 Exponential back-off with jitter

2 Custom retry policy (not in the C SDK)

3 No retry

Troubleshooting guide for D2C communication issues
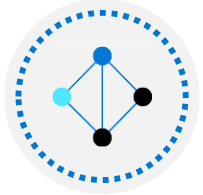
Cannot connect to your Azure IoT hub
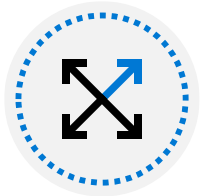
Not detecting disconnections

Failing to send some messages

Lesson 4: Module labs

Module 9 labs
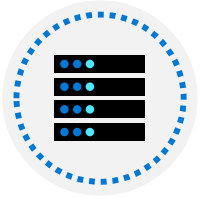
Lab 17: How to manage your Azure IoT hub

You will enable diagnostic logs and metrics

You will set up alerts for your metrics

You will download and run an app that simulates IoT devices connecting via X.509 and sending messages to the hub

You will run the app until the alerts begin to fire, and then observe the metrics and check the diagnostic logs

Lesson 5: Module 9 review questions

Module review: Question 9.1

A developer wants to track the total number of devices that are connected to IoT Hub. They also want to track the percentage of deployed devices that are connected at any given time.

What is the correct way to check the connected/disconnected state of a device?

Answer A:

Query the connectionState field of the IoT Hub identity registry.

Answer B:

Maintain a record of the last message received from each device.

Answer C:

Use device twin desired and reported properties that can be used to track connection state.

Module review: Question 9.2

A developer has detected instances when telemetry is not being received by IoT Hub. The issue always occurs during peak business periods. It appears that devices are connected to IoT hub when this issue occurs.

Which of the following statements about message throttling is correct?

Answer A:

The IoT Hub tier edition (1-3) determines the throttling limits that IoT Hub enforces on all operations.

Answer B:

All messaging attempts in excess of throttle limits are queued and eventually received.

Answer C:

IoT Hub caches incoming messages for later retrieval if the number of queued messages exceeds the queue size limit.

Module review: Question 9.3

What are the three retry policies that are supported by the IoT SDKs?

Answer A:	Answer B:	Answer C:
Scheduled retry, Custom retry, No retry	Exponential back-off, Custom back-off, No retry	Exponential back-off, Custom retry, No retry

Module review: Question 9.4

A developer is writing code that will implement the device connection "retry" pattern. The first step in the code is to detect an error.

What is the next step in the process that the code should implement?

Answer A:

Retry according to the specified retry policy.

Answer B:

Filter by error type and decide if a retry is needed.

Answer C:

Determine whether the error is an unrecoverable error.

Module review: Question 9.5

Which of the following statements about IoT Hub Metrics is correct?

Answer A:

IoT Hub metrics help to assess the overall health of the IoT Hub service.

Answer B:

IoT Hub metrics will help to assess the overall health of the devices connected to your IoT Hub.

Answer C:

IoT Hub metrics are disabled by default.

Module review: Question 9.6

What does Azure Monitor do to help manage an IoT solution?

Answer A:

It monitors the IoT devices.

Answer B:

It monitors the IoT device telemetry.

Answer C:

It monitors the IoT Hub.