

PRACTICE QUESTIONS

Linux Foundation / CNCF

MCPA

Model Context Protocol Associate

SHARED BY [u/tidyfox1977](#) on aiexamcerts

EDITION	Free Set 2
QUESTIONS	10
SHARED	October 18, 2026
EXAM	Linux Foundation / CNCF MCPA, Model Context Protocol Associate

Shared by [u/tidyfox1977](#) on aiexamcerts

10 practice questions for the Linux Foundation / CNCF MCPA exam, Model Context Protocol Associate, each followed by its answer and a short explanation. More free sets and the full practice exam:

aiexamcerts.com/linux-foundation-cncf/mcpa. Spotted a mistake? Email support@aiexamcerts.com with the exam code MCPA and the question number.

1. Which MCP method does a client call to discover which tools a server offers?

- A tools/list
- B tools/call, which invokes one specific tool with its arguments
- C resources/read, which returns the contents of a resource identified by a URI
- D prompts/get, which returns a rendered prompt template for the user to send

Answer: A

tools/list returns the available tools with their names, descriptions and input schemas, which is how a client discovers them. tools/call runs a tool, which comes after discovery. Reading a resource or fetching a prompt returns different primitives entirely.

2. Because MCP servers run locally, the specification makes every tool call safe, so no approval step is needed in the host.

- A True
- B False

Answer: B (False)

False. Local servers can still run destructive commands, leak data or be compromised, so the host should keep approval and least-privilege controls regardless of where the server runs. Local execution is not a security boundary by itself.

3. A data team wants a model to answer SQL questions over a warehouse with read-only access. Which design best fits MCP principles?

- A Give the server write credentials to the warehouse so it can tune the tables it queries
- B Give the server a full administrator account so that it can answer any question the user asks
- C Expose read-only query tools backed by a least-privilege database role with a row limit
- D Copy the entire warehouse into the model's prompt on every turn of the conversation

Answer: C

Read-only query tools with a least-privilege role and a row limit give the model what it needs while bounding the damage from a mistake or an injected instruction. Write credentials and administrator accounts give far more power than a read-only question needs. Copying the warehouse into every prompt is impractical and exposes data without any control.

4. In MCP, a server's reusable message templates that users select are called _____.

Answer: prompts

Prompts are user-controlled templates that a server publishes, often with arguments, and that a client can render into messages. They are distinct from tools, which the model invokes. Resources are the primitive for reading content by URI.

5. Which description best matches an MCP server?

- A The application that the user runs, which asks the model for answers on the user's behalf
- B A program that exposes tools, resources and prompts to clients over a transport
- C A network firewall that filters all traffic between the hosts on a corporate network
- D A database that stores the model's conversation history between different user sessions

Answer: B

An MCP server is a program that exposes tools, resources and prompts to clients over a transport such as stdio or Streamable HTTP. The application the user runs is the host, which is the most common confusion. A firewall and a conversation database are unrelated infrastructure components.

6. Which two transports are defined for MCP connections? (Choose two.)

- A stdio, which runs the server as a subprocess and exchanges messages over its standard input and output
- B Streamable HTTP, which uses HTTP requests with optional server-sent event streams for responses
- C A proprietary binary socket that exchanges protobuf messages only with its own clients
- D FTP with a fixed directory layout that clients poll for new files on a regular schedule
- E Email with a polling interval of one minute, carrying JSON-RPC messages as attachments

Answer: A, B

stdio and Streamable HTTP are the two transports defined for MCP, and both carry the same JSON-RPC messages. The proprietary socket, FTP and email options are not MCP transports, and they are plausible-sounding distractors. Choosing a transport changes how messages move, not what they say.

7. Which practice most reduces the risk of DNS rebinding attacks against a Streamable HTTP server running on a developer's machine?
- A Disabling TLS so that the browser can connect to the local server without certificates
 - B Allowing any origin so that every browser page can call the server without restriction
 - C Binding the server to all network interfaces so that remote clients can reach it easily
 - D Validating the Origin header and binding the server to localhost where possible

Answer: D

Validating the Origin header rejects requests from web pages that are not trusted, and binding to localhost keeps the server off the network. Allowing any origin or binding to every interface makes a rebinding attack far easier. Disabling TLS removes the transport protection rather than addressing the attack.

8. A customer support team wants a tool that issues refunds. Which control matters most before the call executes?
- A Sending the refund tool's schema to the model in a larger prompt for better accuracy
 - B Removing the tool description so that the model cannot see the refund tool at all
 - C Requiring explicit user or operator approval for a state-changing action such as a refund
 - D Caching each refund result in the model's context window so it can be reused later

Answer: C

A refund changes money and records, so an explicit approval step keeps a person accountable for the action. A larger schema prompt does not add any safety, and hiding the tool just makes it harder to use. Caching refund results in context does not control whether the refund happens.

9. A prompt in MCP can accept arguments, so the same template can produce different messages for different inputs.
- A True
 - B False

Answer: A (True)

True. Prompt definitions can declare named arguments, and prompts/get renders the template with the values the user supplies. This lets one reusable template serve many related tasks.

10. Which JSON-RPC error code means that the request named a method the server does not implement?

- A -32601, method not found
- B -32602, invalid params, meaning the parameters are missing or malformed for the method
- C -32603, internal error, meaning the server failed while processing a valid request
- D -32600, invalid request, meaning the message is not a well-formed request object

Answer: A

The JSON-RPC code -32601 signals that the method is not found on the server. Invalid params, which is the most tempting near-miss, means the method exists but its arguments are wrong. Internal error and invalid request describe different failures in processing or message structure.