

PRACTICE QUESTIONS

Linux Foundation / CNCF

MCPA

Model Context Protocol Associate

SHARED BY [u/Nifty-Widget-7044](#) on aiexamcerts

EDITION	Free Set 1
QUESTIONS	10
SHARED	October 18, 2026
EXAM	Linux Foundation / CNCF MCPA, Model Context Protocol Associate

Shared by [u/Nifty-Widget-7044](#) 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. The MCP principle of user consent and _____ means that users must approve data access and tool use.

Answer: control

User consent and control means people must explicitly approve how their data is accessed and which tools run on their behalf. Hosts are expected to present these decisions clearly. Consent alone without the ability to review or revoke access would leave users with little real control.

2. Which component connects directly to one MCP server and handles the protocol messages for that connection?
 - A The host application's user interface, which renders the chat window and its buttons
 - B The LLM provider's billing service, which meters tokens for each conversation separately
 - C The language model's tokenizer, which splits the text of each prompt into tokens
 - D The MCP client, which maintains one protocol session with a single server

Answer: D

The MCP client is the component that holds one session with one server and speaks the protocol on that connection. The host's interface, the billing service and the tokenizer do not manage protocol connections at all. The host can contain several clients, which is why the per-connection role belongs to the client.

3. An IDE assistant needs the current project's source files as context. Which primitive is the most natural way to expose them?
 - A Sampling, which lets the server write new files directly into the project folder
 - B Resources, identified by URIs that the client can read on request
 - C Elicitation, which asks the user to paste each source file into a text box
 - D Tool annotations, which mark every file in the project as read-only for the model

Answer: B

Resources are identified by URI and read by the client, which suits files that provide background context. Sampling asks for a model completion rather than writing files. Elicitation requests input from a user, and annotations describe tools, so neither exposes source files.

4. Which two statements about JSON-RPC requests in MCP are correct? (Choose two.)
- A A request carries an id so that the matching response can be correlated with it
 - B A notification carries an id and must receive a matching response from the other side
 - C Batch responses are required for every tools/list request that a client sends
 - D Requests can be sent by either side of the connection, client or server, depending on the method
 - E Method names must be written in uppercase letters so that the parser can match them

Answer: A, D

The id is how a response is matched to its request, and JSON-RPC is bidirectional, so servers can send requests such as sampling to clients. A notification has no id and receives no response, which makes option B wrong. Batch responses and uppercase method names are not MCP requirements.

5. Which MCP feature lets a server ask the host to run a language model completion on its behalf?
- A Roots, which list the filesystem boundaries that the server is allowed to access
 - B Sampling, which the host can review and approve before the completion is generated
 - C Resource templates, which describe the URI patterns the server uses for its resources
 - D Logging notifications, which record events on the server for later inspection by staff

Answer: B

Sampling lets a server request a completion from the host's model, and the host keeps the decision to approve it. Roots describe filesystem scope rather than model access. Resource templates and logging notifications have no role in asking for a completion.

6. Each MCP server exposes its capabilities during initialization, so a client uses only the primitive types that the server declared.
- A True
 - B False

Answer: A (True)

True. Capability negotiation tells each side which features the other supports, and a client should not assume a feature that was not declared. This is what lets old and new implementations interoperate safely.

7. Which operational use case benefits most from a server's ability to send progress notifications?
- A A one-line lookup that returns its result almost instantly without any waiting
 - B A static prompt template with no arguments that is rendered the same way each time
 - C A boolean check that always returns true and is never expected to take any time
 - D A long-running tool, such as a batch import, that reports its progress to the client while it runs

Answer: D

Progress notifications let a client show a user that a long-running operation is advancing, such as a batch import processing records. Instant lookups and fixed templates finish before progress would matter. A check that always returns true does no work worth reporting.

8. A client cancels a long-running request by sending a notification named notifications/_____.

Answer: cancelled (also accepted: canceled)

The cancellation notification tells the other side to stop work on a request that was previously sent. Because it is a notification, it does not get a response of its own. Sending a new request for the same work would leave the original one running.

9. Why does a careful host treat a tool's description as untrusted input?
- A Because a malicious server can place instructions in the description that try to steer the model
 - B Because descriptions are always stored in a binary format that the host cannot read
 - C Because descriptions are limited to a single word, so they carry too little information
 - D Because descriptions are shown only to the server developer and never reach the model

Answer: A

Tool descriptions are sent to the model, so a hostile server can use them to influence the model's choices, which is a form of prompt injection. Descriptions are text rather than binary, and they do reach the model because it chooses tools from them. Treating them as untrusted input is the defense.

10. Which MCP element is the AI application that runs the model and coordinates one or more clients?
- A A server, which exposes tools, resources and prompts to the clients that connect to it
 - B A transport, which carries the JSON-RPC messages between the two ends of a connection
 - C A host, which is the AI application that coordinates one or more clients
 - D A schema, which describes the JSON structure that a tool expects as its input

Answer: C

The host is the AI application, such as a desktop assistant or an IDE, and it coordinates the clients that connect to servers. A server supplies capabilities rather than coordinating anything, and the transport and schema are supporting parts of the protocol. Confusing the host with the server is the usual mistake.