+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 10/14/2026

Sign Up

MCPA Certification Training

3 days (21 hours)

Overview

Give your agent-based applications controlled access to your company's tools and data. Using the Model Context Protocol and an approach centered on clients, servers, and transports, learn how to design interoperable, secure integrations tailored to production constraints.

Our MCPA Certification Training: Hands-On prepares you for the official MCPA certification by combining an understanding of the protocol, guided exercises, and analysis of scenarios representative of the skills assessed on the exam.

You'll learn how to develop an MCP client, build a server that exposes tools and resources, and then connect external APIs to a workflow using a language model.

By the end of the course, you will be able to handle stateless requests, manage permissions, mitigate risks associated with tools, and diagnose integration errors.

The course also covers testing and observability, architectural choices, and catalog governance. Progressive workshops and a mock exam will help you solidify your exam preparation and apply what you've learned to your projects.

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

Objectives

- Explain the roles of hosts, clients, and servers in an MCP architecture and distinguish between tools, resources, and prompts

- Develop an MCP client integrated into a workflow using a language model
- Build an MCP server that exposes tools, resources, and external APIs
- Implement stateless interactions with metadata via queries and explicit application state
- Secure and test integrations with access controls, validations, and audit trails
- Prepare for the MCPA exam by analyzing scenarios and taking a mock exam

Target Audience

- AI Developer
- Backend developer
- Platform Engineer
- DevOps Engineer
- Software Architect

Requirements

- Experience programming with TypeScript and using a terminal
- Understanding of HTTP requests, REST APIs, and JSON structures
- Initial experience integrating an LLM via API and understanding how to call tools
- Basic knowledge of authentication, secret management, and authorization using OAuth

Technical Prerequisites

- Computer running Windows 11, macOS, or Linux with 16 GB of RAM recommended, a quad-core processor, and installation privileges
- Node.js 22.19 or higher environment with npm, Git, and Visual Studio Code installed
- Installation of MCP Inspector 2 and the MCP TypeScript 2 SDK with fixed dependencies in the learning environment
- Stable internet connection supporting the training services, packet logs, and APIs used, with access to a test language model
- To take the exam: a computer compatible with PSI Secure Browser, a webcam, a microphone, and a quiet, private space, following validation of the system requirements

MCPA Certification Training Program

[Day 1 - Morning]

MCP Fundamentals and Certification Guidelines

- Introduction to the MCP Fundamentals Certification Training: practical application and exam topics for the MCPA exam
- The role of MCP in agent-based systems and the responsibilities of hosts, clients, and servers
- Protocol primitives: tools, resources, prompts, and JSON-RPC exchanges

- Differences between MCP, direct APIs, plugins, RAG, and A2A-style inter-agent communication
- Use cases for development agents, enterprise data, and operational tools; ecosystem and adoption trade-offs
- Hands-on workshop: Explore a simple server with MCP Inspector, identify its capabilities, and interpret its exchanges based on MCPA preparation questions.

[Day 1 - Afternoon]

MCP clients and integration with LLM workflows

- MCP client responsibilities, server configuration, metadata per request, and optional capability discovery
- Invoking tools, reading resources, and using prompt templates
- Integration with an LLM application and coordination with agent frameworks
- Managing version compatibility, schema validation, errors, retries, and unavailable servers
- Client-side permissions, user approval, and analysis of the invocation cycle for review
- Hands-on workshop: Create a TypeScript client connected to an LLM workflow, call a tool, and handle a validation error as well as a simulated unavailability.

[Day 2 - Morning]

MCP Servers and Exposure of External Systems

- MCP server responsibilities, exposed capabilities, independent request processing, and local or shared execution
- Design of tool schemas, resource interfaces, prompt definitions, and structured output formats
- Adapting files, databases, and REST, GraphQL, or SaaS APIs to MCP capabilities
- Input validation, side effects, idempotency, pagination, rate limits, and partial failures
- Authentication of external services, least privilege, and choosing between MCP, direct API, RAG, and workflow automation
- Hands-on workshop: Build a server exposing a tool and a resource, integrate a and verify pagination, invalid inputs, and service errors.

[Day 2 - Afternoon]

Security, Authorization, and Governance

- Analysis of trust boundaries between users, clients, servers, tools, and data sources
- Distinguishing between authentication and authorization, secret management, and HTTP authorization with OAuth
- Risks of prompt injection, tool poisoning, data leaks, and dangerous actions

- Consent controls, approval of sensitive actions, execution isolation, and policy enforcement
- Security review of servers and catalogs, audit trails, and analysis of MCPA
- Hands-on workshop: Add authentication and restricted permissions to an HTTP server, enforce approval for a sensitive action, and verify the denial of unauthorized access.

[Day 3 - Morning]

Stateless protocol, transports, and extensions

- Stateless model from revision 2026-07-28: version, capabilities, and client information per request; optional discovery; and backward compatibility
- stdio and Streamable HTTP transports, responses limited to the request, streaming, and cancellation
- HTTP metadata and header-based routing for gateways, policies, and observability requirements
- Explicit application state via arguments and identifiers issued by the server, independent of transport sessions
- Multi-round-trip interactions, long-running processes, catalogs with cache hints, and boundaries between the protocol core and extensions
- Hands-on workshop: Implementing a stateless interaction with discovery, metadata per request, and explicit application identifiers, then verify its continuity across two server instances.

[Day 3 - Afternoon]

Reliability, architecture, and exam preparation

- Inspection of exchanges using MCP Inspector and diagnosis of issues related to transport, authorization, schema, and model integration
- Contract and regression testing: schemas, versions, edge cases, failures, and tool evolution, extensions, and models
- Integration observability: application logs, traces, metrics, and audit events without exposing secrets
- Stateless local, team, and enterprise architectures; integration with RAG, AI gateways, and CI/CD workflows
- Version governance and catalogs, trade-offs between performance, cost, caching, and reliability, adoption roadmap, and MCPA readiness strategy
- Hands-on workshop: Diagnose and instrument the built integration, propose its and conduct a timed mock assessment with a detailed feedback report.

Target Audience

This training is intended for both individuals and companies—large or small—seeking to train their teams in a new advanced IT technology or to acquire specific domain knowledge or modern methodologies.

Assessment upon enrollment

The pre-training assessment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency level across various types of technologies, as well as their expectations and personal goals for the upcoming training, within the limits imposed by the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for monitoring and ensuring the smooth running of the training session.

Teaching Methods

Hands-On Training: 60% Practical, 40% Theoretical. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the instructor—supported by examples and reflection sessions—and group work.

Assessment

At the end of the session, a multiple-choice quiz is administered to verify that participants have successfully acquired the skills.

Certification

A certificate will be issued to each trainee who has completed the entire training program.

Training organization registered under number 11 75 54743 75. This registration does not constitute state accreditation.
© Ambient IT 2015-2026. All rights reserved. Paris, France - Switzerland - Belgium - Luxembourg