

KOENIG SOLUTIONS · COURSE OUTLINE

Model Context Protocol Foundation

2 Days

DURATION

8

MODULES

48

TOPICS

RXM404

COURSE CODE

COURSE OVERVIEW

Agentic AI systems are only as useful as the data, tools, and systems they can reach. Connecting them to enterprise infrastructure safely is where most teams get stuck. The Model Context Protocol (MCP) gives developers a standard way to make those connections production-ready. Prepare to take on roles such as AI Systems Architect, Agentic Integration Engineer, or Platform and DevOps Lead for AI initiatives, with the skills to deploy secure agentic workflows in real-world environments. The Linux Foundation has partnered with the AI/ML experts at rx-m to offer this course to the community.

WHO THIS COURSE IS FOR

- For developers, data engineers, and platform, DevOps, and security teams building agentic AI applications. Also valuable for technical managers and architects planning AI integrations.

PREREQUISITES

- Programming experience, preferably in Python or JavaScript. Basic familiarity with LLM applications, APIs, and command-line development is recommended.

Lab Info

- An Ubuntu cloud instance is provided. Students need only the ability to ssh or browse to the instance.

LEARNING OBJECTIVES

What You Will Learn

- Build MCP clients and servers that expose tools, resources, and prompts, and connect them to external APIs, data, and enterprise systems. Then secure, debug, and harden those integrations for production.

8 Modules, 48 Topics

01

MCP Overview

TOPICS

- Why MCP matters for agentic AI systems
- MCP clients, servers, tools, resources, prompts, and transports
- How MCP differs from direct APIs, plugins, RAG, and A2A-style communication
- Common use cases for coding agents, enterprise data, workflow tools, and operations
- MCP ecosystem, adoption patterns, and integration tradeoffs
- LAB: Explore MCP basics with a simple studio-based client and server

02

MCP Clients

TOPICS

- Client responsibilities, per-request metadata, and optional capability discovery
- Invoking tools, reading resources, and using prompt templates
- Integrating MCP clients with LLM applications and agent frameworks
- Handling version compatibility, errors, retries, schema validation, and unavailable servers
- Client-side configuration, permissions, and user approval patterns
- LAB: Create an MCP client and connect it to an LLM workflow

03

MCP Servers

TOPICS

- Server responsibilities, exposed capabilities, and stateless request handling
- Designing tool schemas, resource interfaces, and prompt definitions
- Mapping local files, APIs, databases, and services into MCP capabilities
- Managing side effects, idempotency, input validation, and output formats
- Packaging and running MCP servers for local and shared environments
- LAB: Build an MCP server that exposes tools and resources

04

External APIs and MCP

TOPICS

- Wrapping REST, GraphQL, database, and SaaS APIs as MCP tools
- Translating API contracts into safe tool schemas and response formats
- Handling authentication, rate limits, pagination, and partial failures
- Designing least-privilege access for external service integrations
- Choosing between MCP, direct APIs, RAG, and workflow automation
- LAB: Expose a third-party or simulated API through MCP

05

MCP Security and Authorization

TOPICS

- Trust boundaries between users, clients, servers, tools, and data sources
- Authentication, authorization, least privilege, and secret handling
- Prompt injection, tool poisoning, data leakage, and unsafe action risks
- Approval flows, sandboxing, audit trails, and policy enforcement
- Security review patterns for MCP servers and tool catalogs
- LAB: Add authentication and approval controls to an MCP workflow

06

Stateless Protocol, Transports, and Extensions

TOPICS

- Per-request protocol version, client metadata, capabilities, and optional server discovery
- Studio and Streamable HTTP transport patterns, including request-scoped responses and cancellation
- HTTP metadata and header-based routing for gateways, policy, and observability
- Explicit application state through tool arguments and server-minted handles, not transport sessions
- Multi-round-trip interactions, long-running work, cacheable catalogs, and extension boundaries
- LAB: Build a stateless MCP interaction with discovery, request metadata, and explicit state

07

Debugging, Testing, and Observability

TOPICS

- Inspecting request metadata, client-server interactions, tool calls, and resource access
- Testing tool schemas, version compatibility, validation paths, edge cases, and failures
- Debugging transport, authorization, schema, and model-integration issues
- Logging, tracing, metrics, and audit events for MCP applications
- Regression testing MCP integrations as tools, extensions, and models change
- LAB: Debug and instrument an MCP client/server integration

08

MCP Architecture and Integration Strategy

TOPICS

- MCP reference architectures for local, team, and stateless enterprise deployments
- Integrating MCP with RAG, agent frameworks, AI gateways, and CI/CD workflows
- Versioning, compatibility, extension adoption, catalog management, and lifecycle governance
- Performance, cost, reliability, caching, and operational ownership tradeoffs
- Roadmap planning for MCP adoption across teams and platforms
- LAB: Design a production MCP integration architecture

WHAT IS INCLUDED

Everything You Need to Succeed

- Koenig course material for every module
- Hands-on exercises throughout the course
- Delivery by certified instructors and subject matter experts
- Course completion certificate from Koenig

ABOUT KOENIG

Who We Are

Established in 1993, Koenig Solutions is a globally recognised training provider with 35+ technology partnerships, 5,000+ training programmes and a network of certified instructors and subject matter experts, supporting individuals and enterprise teams worldwide.

FLEXIBLE DELIVERY

Learn the Way That Suits You

Classroom Training

Live Online Classes (ILO)

Fly-Me-A-Trainer (FMAT)

Flexi (Self-Paced)

1-on-1 Training

Ready to Get Started?

Talk to a learning advisor about schedules, group training and customised delivery.

[Visit koenig-solutions.com](https://www.koenig-solutions.com)

[✉ info@koenig-solutions.com](mailto:info@koenig-solutions.com)