MCP + Vector DB + A2A Flashcards

Generated: 2025-09-11 07:03 UTC

MCP + Vector DB + A2A Flashcards

Generated: 2025-09-11 07:00 UTC

Q: What is a Resource?
A: Read-only data endpoint for LLMs.
Code: `@mcp.resource def foo(): ...`

Q: How to secure a destructive tool?
A: Require role checks, confirmation prompts, logging.
Code: `@require_role("admin") @mcp.tool def delete_user(id): ...`

Q: What is a Vector DB used for?
A: Store embeddings and support fast similarity search for RAG.

Q: How to integrate Vector DB into MCP?
A: Expose a resource/tool that queries the index.
Code: `@mcp.resource def search(q): return vector_index.search(embed(q))`

Q: What is Google A2A?
A: Protocol for agents to discover peers, negotiate, and delegate tasks.

Q: How to ensure trust in A2A?
A: Mutual TLS, signed assertions, short-lived tokens, policy engine.