MCP Open Discovery v2.0 — Executive One-Pager

Container-first • Official MCP SDK

Production-ready MCP server for discovery, CMDB, and tool orchestration

What it is

A production-ready Model Context Protocol (MCP) server that unifies infrastructure discovery, lightweight CMDB, and tool orchestration. Built on the official MCP SDK with a dynamic tool registry and container-first deployment.

Why it matters

- Accelerates infrastructure visibility and inventory with minimal setup
- Centralizes discovery/monitoring actions behind a single secure endpoint
- Reduces operational toil via hot-reload tools and persistent CMDB
- Enterprise security: encrypted credentials, audit trails, least privilege

Key capabilities

- 57+ tools: Network, SNMP, Proxmox, Zabbix, Nmap, Credentials, Memory (CMDB)
- Dynamic registry with hot-reload (no restarts for updates)
- SQLite-backed CMDB: hierarchical CI keys, relationships, auto-save
- Multi-transport MCP server: HTTP, stdio; AMQP evaluated; container-first

Architecture

- Single MCP server instance; centralized tool registry
- Encrypted credentials + SQLite CMDB
- Capability-based security for privileged scans (no root)
- Health endpoint and structured logs for ops

Security & compliance

- AES-256 encrypted credentials with audit logging
- Input validation and defensive error handling
- Capability-based Docker security (NET_RAW, NET_ADMIN, NET_BIND_SERVICE)
- Designed for least privilege; supports at-rest encryption policies

Deployment & operations

- Docker Compose; Windows PowerShell script (rebuild_deploy.ps1)
- Health checks and logs; hot-reload for safe iteration
- Works locally, in CI, or in container platforms

Proof points

- 93% overall tool success across 57 tools
- Validated against Proxmox, SNMP devices, and Zabbix
- Persistent CMDB and dynamic registry at runtime

Get started

- Run: rebuild_deploy.ps1 on Windows
- Verify health on port 3000 and list MCP tools
- Add credentials and start discovery

This project was substantially coded with AI under human guidance and review. See README for architecture and security details.