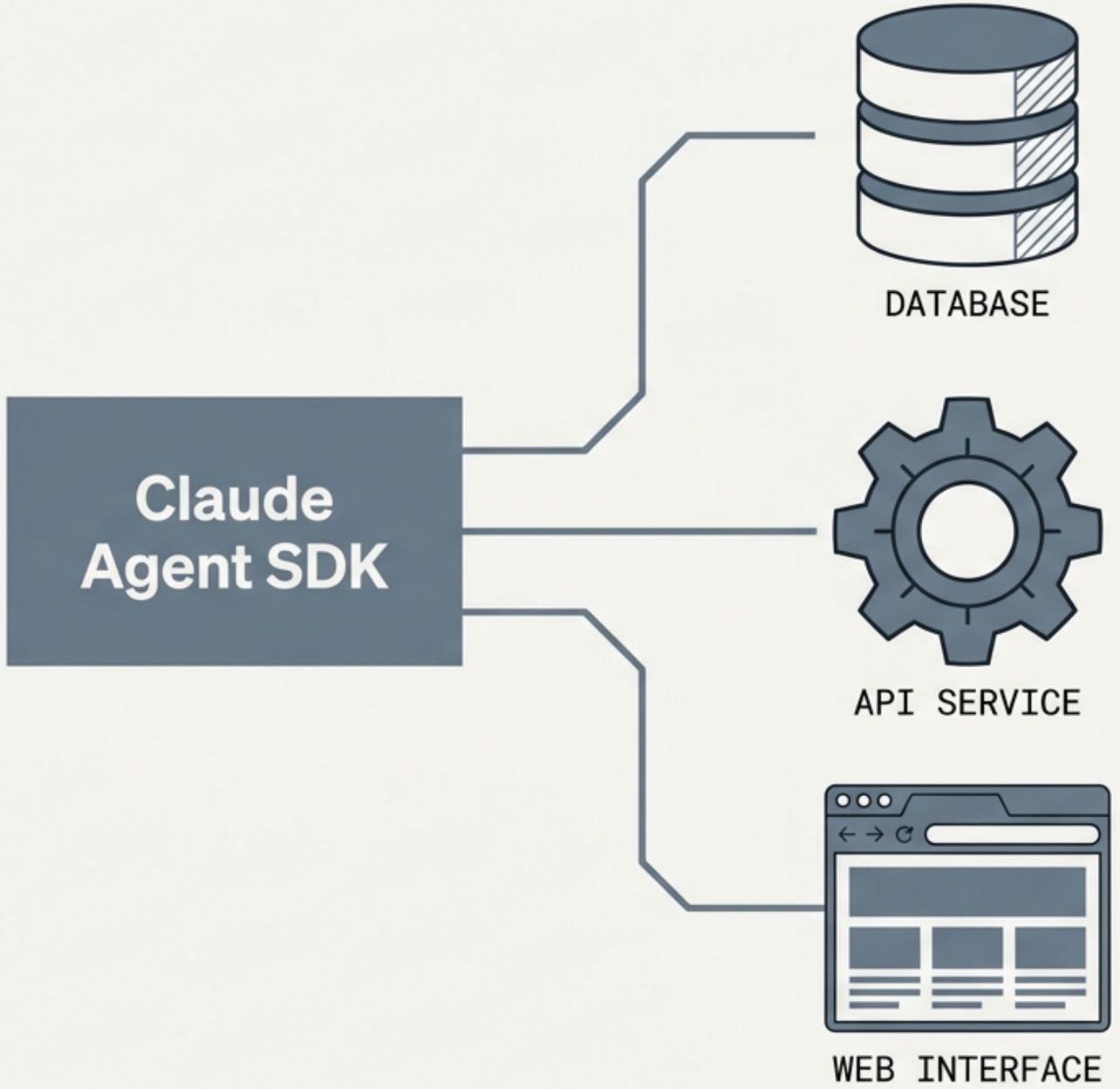
Orchestrating Multi-Server Agents

A visual guide to configuring the Model Context Protocol (MCP) Connector.

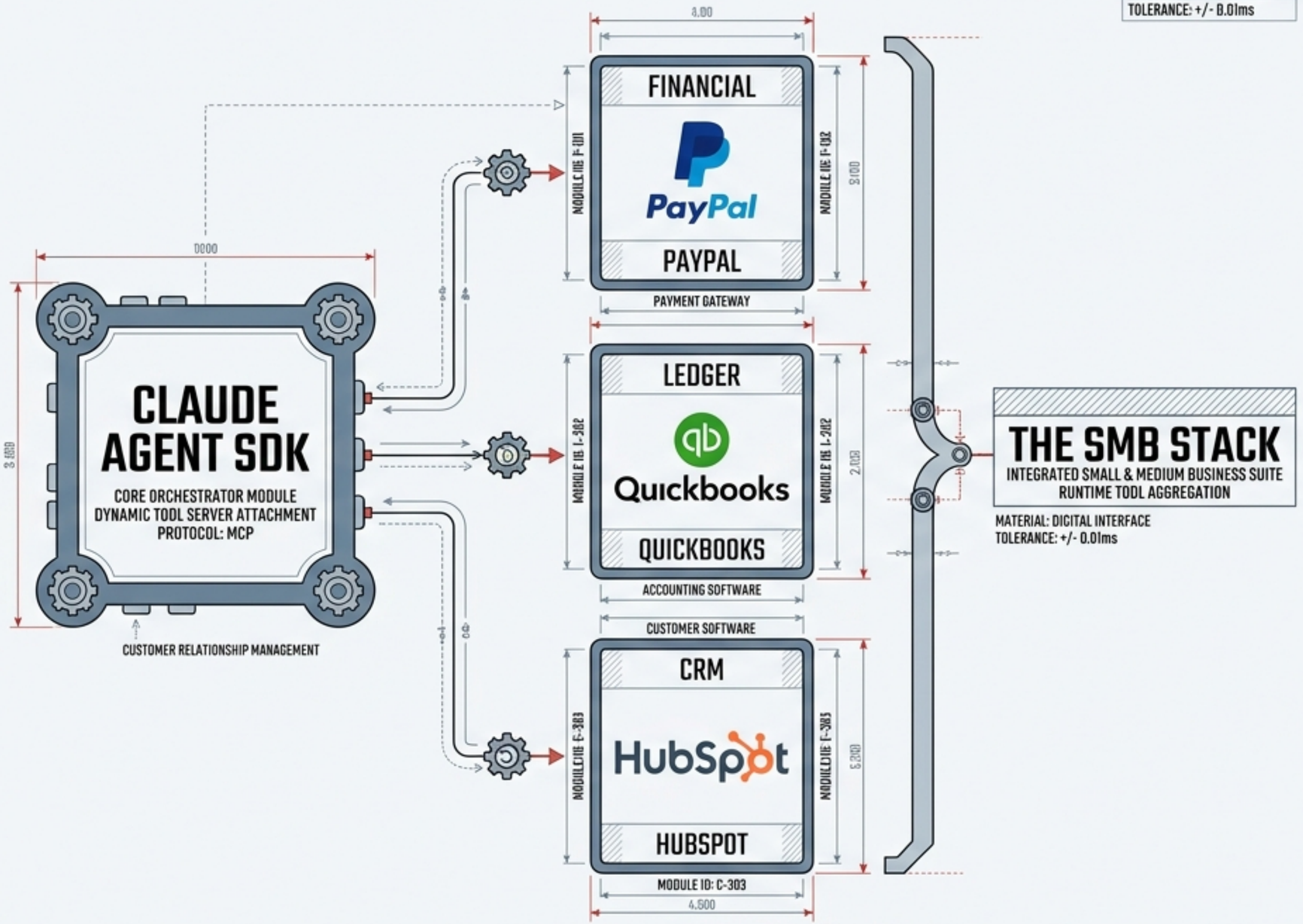
Updated for the May 2026 Claude Agent SDK release.

TAGS: Technical Blueprint | Infrastructure | Production Controls



RECONCILING DISPARATE SYSTEMS AT RUNTIME - MODERN SWISS ENGINEERING BLUEPRINT

MATERIAL: DIGITAL INTERFACE
TOLERANCE: +/- 0.01ms



RECONCILING DISPARATE SYSTEMS AT RUNTIME

THE CONCEPT:

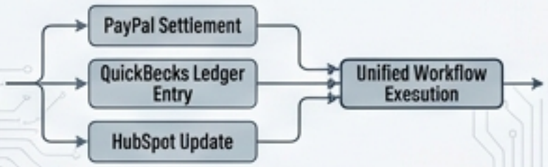
The MCP connector is a built-in mechanism for attaching external tool servers to an agent dynamically. it facilitates real-time, on-demand integration without pre-configuration, mirroring a mechanical coupling system.

THE PROTOCOL:

A standard epen protocol co-developed by Anthropic and the AI ecosystem. It defines a universal language for AI models to communicate with and control diverse software tools, ensuring interoperability across the assembly.

THE POWER OF COORDINATION:

A single query() can now reconcile a PeyPal settlement against a QuickBooks ledger, and trigger a HubSpot 'deal won' update simultaneously. This enables multi-step, cross-system workflows through unified command execution, akin to a synchronized multi-actuator operation.



PROJECT: CLAUDE AGENT SDK INTEGRATION
DRAWN BY: SWISS ENGINEERING GROUP
DATE: OCTOBER 26, 2023

DECONSTRUCTING THE MCP TOOL IDENTIFIER - MODERN SWISS ENGINEERING BLUEPRINT

mcp__github__list_issues

The Required Prefix.

The Server Key: Matches the name defined in the `mcpServers` configuration dictionary.

The Specific Tool: The exact function exposed by the remote server.

THE WILDCARD RULE

Passing `mcp__github__*` grants the agent access to the entire server cluster (e.g., `list_issues`, `search_issues`, `create_issue`).

PROJECT: CLAUDE AGENT SDK INTEGRATION
DRAWN BY: SWISS ENGINEERING GROUP
DATE: OCTOBER 26, 2023

THE TRANSPORT LAYER MATRIX - MODERN SWISS ENGINEERING BLUEPRINT

stdio

- **Type**: Local process servers.
- **Mechanism**: Spawns child process; communicates via stdin/stdout.
- **Use Case:** Development, npm/PyPI packages (e.g., local database).

HTTP

- **Type**: Stateless remote servers.
- **Mechanism**: Standard endpoint; no local installation required.
- **Use Case:** Cloud-hosted SaaS APIs.

SSE

- **Type**: Streaming remote servers.
- **Mechanism**: Server-Sent Events; SDK handles transparent reconnection.
- **Use Case:** Long-running queries, real-time data feeds.

PROJECT: CLAUDE AGENT SDK INTEGRATION		
DRAWN BY: SWISS ENGINEERING GROUP		
DATE: OCTOBER 26, 2023	REV: 1.0	SCALE: 1:1

The Permission Trap: Why acceptEdits Fails

Insight: MCP tools require explicit permission. Assuming acceptEdits auto-approves them will cause the agent to see the tools but refuse to call them.

default	Approves Nothing (Prompts user).	✗ **BLOCKS MCP**
acceptEdits	Approves File & Bash edits.	✗ **BLOCKS MCP**
bypassPermissions	Approves Everything.	✓ **DANGEROUS** (Disables safety checks)

The Fix:
`Use explicit grants via allowedTools: ['mcp__github__*']`

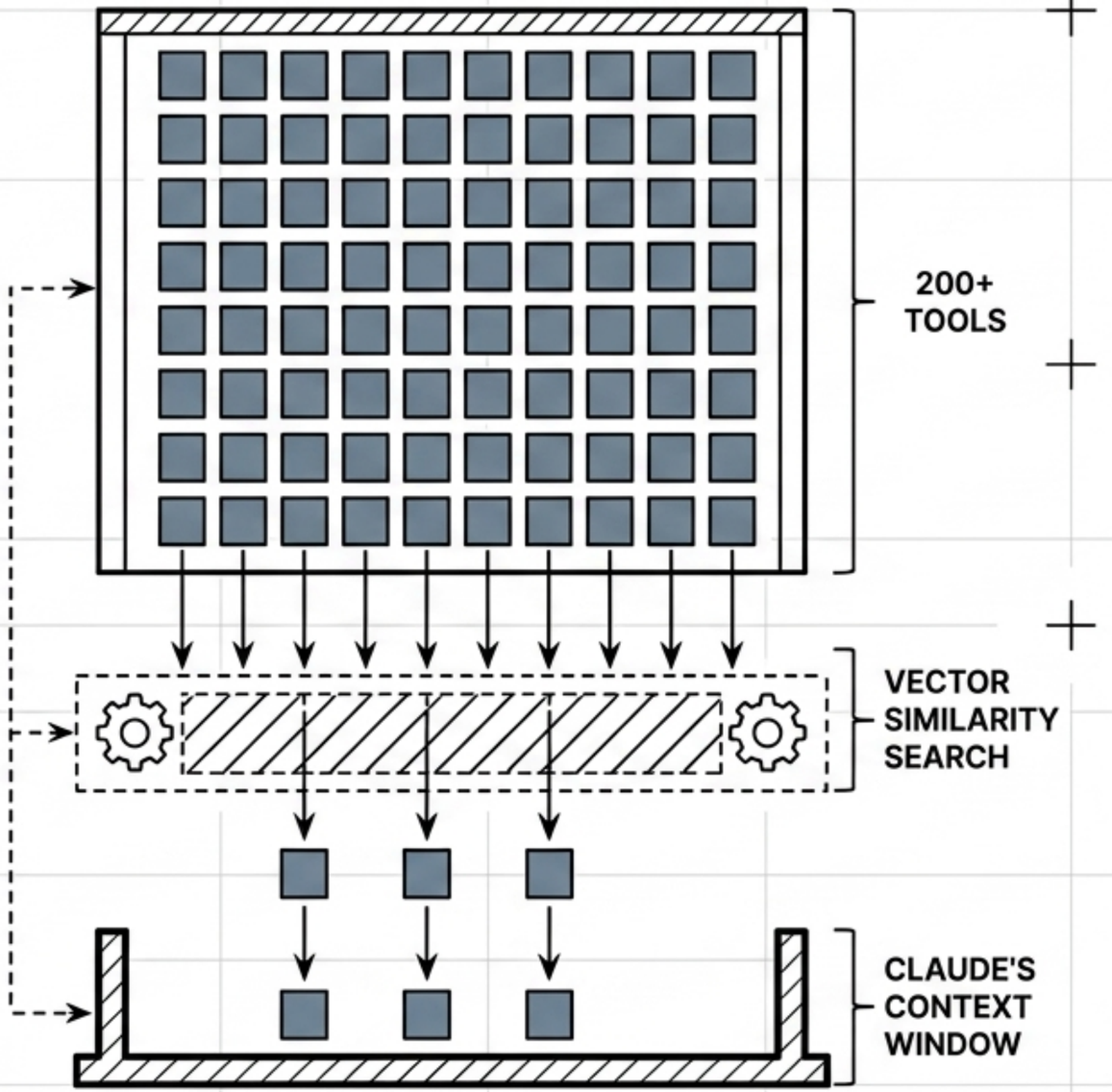
PROJECT: CLAUDE AGENT SDK INTEGRATION		
DRAWN BY: SWISS ENGINEERING GROUP		
DATE: OCTOBER 26, 2023	REV: 1.0	SCALE: 1:1

SCALING UP: DEFENDING THE CONTEXT WINDOW

THE PROBLEM: Attaching dozens of servers fills the context window with raw tool definitions before the agent even begins working.

THE SOLUTION: SDK Tool Search (Enabled by default).

MECHANISM: The SDK withholds all tool definitions, loading only the specific tools Claudo needs for the current turn based on vector matching.



PROJECT: CLAUDE AGENT SDK INTEGRATION		
DRAWN BY: SWISS ENGINEERING GROUP		
DATE: OCTOBER 26, 2023	**REV:** 1.0	S

Enterprise Configuration and Authentication

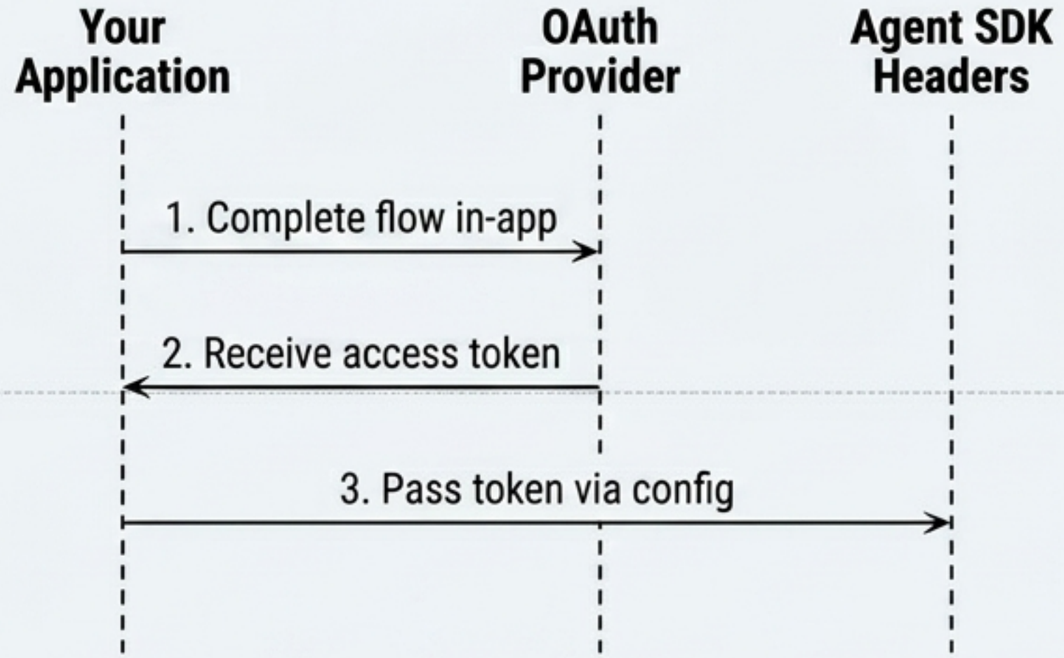
Declarative Infrastructure

.mcp.json

```
{
  "mcp": {
    "servers": {
      "database": {
        "command": "docker",
        "args": [
          "run",
          "-i",
          "--rm",
          "-e",
          "DATABASE_URL",
          "mcp/postgres"
        ],
        "env": {
          "DATABASE_URL": "${DATABASE_URL}"
        }
      }
    }
  }
}
```

Place .mcp.json at the project root. The SDK expands environment variables at load time, keeping hardcoded credentials out of your repository.

OAuth 2.1 Handling

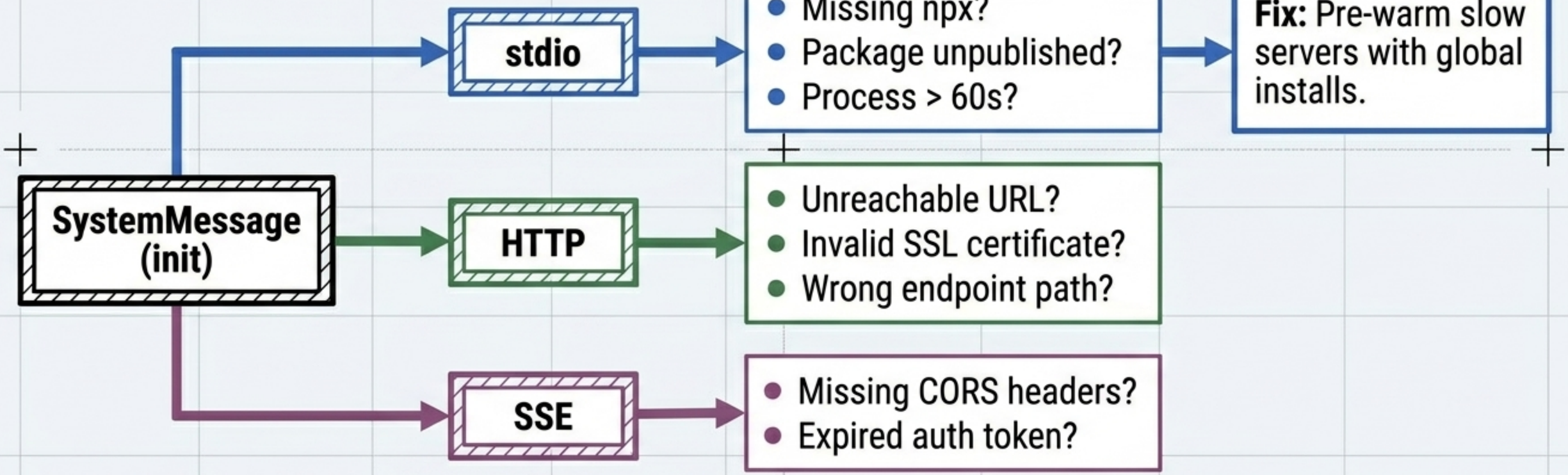


The Agent SDK does not handle OAuth flows. Manage token refreshes in your session initialization, never inside the agent loop.

PROJECT: CLAUDE AGENT SDK INTEGRATION		
DRAWN BY: SWISS ENGINEERING GROUP		
DATE: OCTOBER 26, 2023	**REV:** 1.0	S

The Diagnostic Tree: Catching Silent Failures

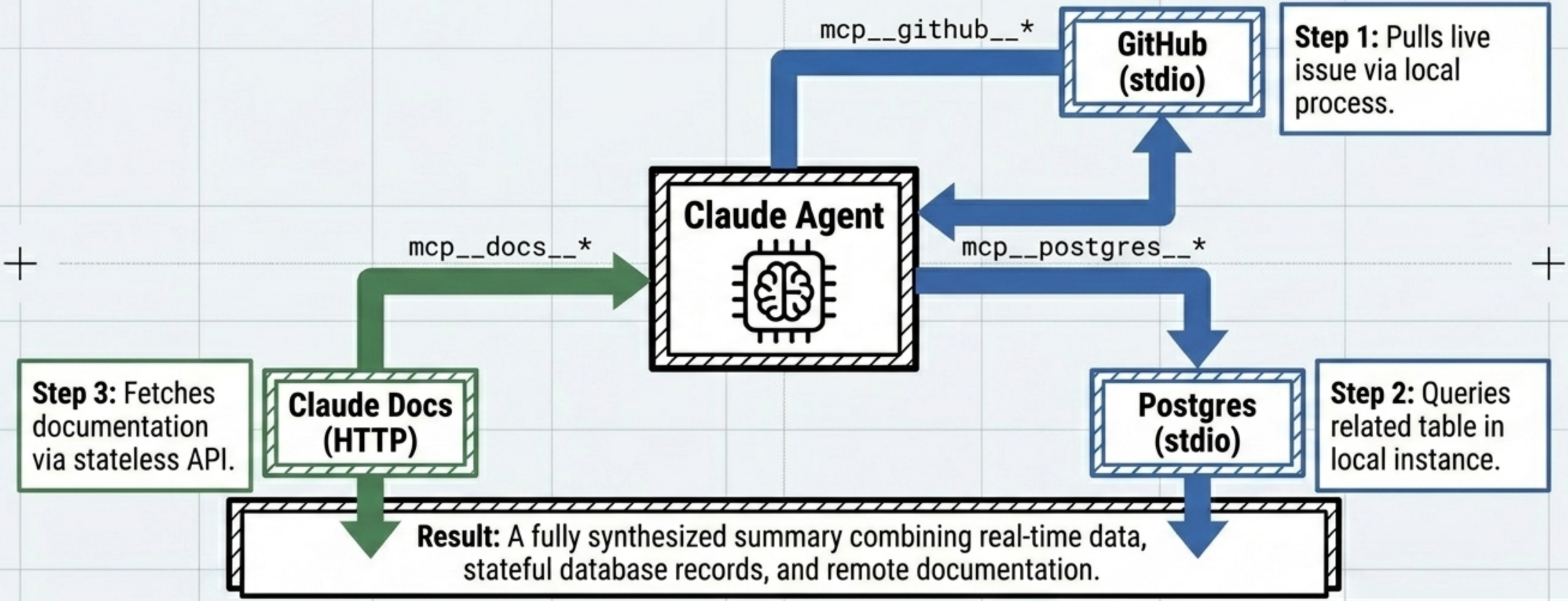
Crucial Rule: MCP servers fail silently. **Always** check the **init message status field** before the agent starts.



PROJECT: CLAUDE AGENT SDK INTEGRATION		
DRAWN BY: SWISS ENGINEERING GROUP		
DATE: OCTOBER 26, 2023	**REV:** 1.0	

The 3-Server Orchestration Blueprint

A single agent pulling live data, database records, and remote documentation simultaneously.



PROJECT: CLAUDE AGENT SDK INTEGRATION		
DRAWN BY: SWISS ENGINEERING GROUP		
DATE: OCTOBER 26, 2023	**REV:** 1.0	