VOLT ACTIVE DATA

Volt MCP Server

AI Assistants for Volt, Inside Volt's Own Security Model

AI assistants are now part of how engineering teams write and run software. On a Volt project they are useful only if they see the real schema, the real procedures and the real state of the cluster. They are safe only if they reach the database through the same accounts, roles and encryption as any other client.

Assistants Guess at Schema	One Shared Account	Laptop-Only Setup	Unencrypted Connections	Generic Volt Advice

Volt MCP Server is a Model Context Protocol server, built and maintained by Volt. It gives any MCP-capable assistant direct, permission-controlled access to a Volt cluster: to build applications against it, and to investigate how it is running.

How it works

The server runs in one of two ways. It runs locally, started by the assistant itself. A team runs it as a long-running service over Streamable HTTP, deployed from the Helm chart on Kubernetes, from the container image on a VM, or as a sidecar.

The MCP talks to the cluster over Volt's native client protocol, so no Volt Management Center (VMC) or JSON/HTTP endpoint is needed in the path. It exposes the database to the assistant as tools: SQL execution (including DDL), table and schema inspection, schema export, stored-procedure listing and invocation, system information, the @Statistics components, snapshot save and class loading.

Every call runs as a Volt user, so Volt's own authentication and role-based permissions decide what the assistant can do. Over HTTP, each MCP session can carry its own Volt credentials; locally, the server uses the account it was started with. Both connections, assistant to server and server to cluster, can be encrypted with TLS, and either can require mutual TLS.

The server ships with a built-in operations skill. It guides the assistant through diagnostics, such as XDCR problems, and sets explicit rules for when the assistant may apply a change and when it must propose the change for human approval. For application development, Volt also publishes Agent Skills (voltdb-development, voltsp, volt-kubernetes), free under the MIT license on GitHub.

What this means in practice

Build against the real database. The assistant reads the live schema and procedure list instead of guessing at them. With the voltdb-development skill loaded, the code it generates follows Volt's partitioning and procedure rules.

Investigate with real numbers. The @Statistics components are available as tools, so the assistant works from the cluster's own figures. The built-in operations skill steers the investigation and separates what the assistant may do from what it must propose.

Access you already control. The assistant gets exactly the permissions of the Volt user it runs as. Start with a read-only role: the tool set includes DDL, snapshot save and class loading, so write access should be a deliberate choice.

One server for the team. Run a single shared instance on Kubernetes from the Helm chart instead of a copy on every laptop, with each session using its own Volt credentials.

Architectural properties

- Model Context Protocol server; works with Claude Code and other MCP-capable clients
- **Transports:** stdio for local use; Streamable HTTP for a shared, long-running service
- **Connection:** Volt native client protocol; Volt Management Center (VMC) not required
- **Security:** Volt authentication and role-based permissions apply to every call; per-session Volt credentials over HTTP; TLS, optionally mutual, from assistant to server and from server to cluster
- **Tools:** SQL execution (including DDL), table and schema inspection, schema export, stored-procedure listing and invocation, system information, @Statistics components, user profile, snapshot save, class loading
- **Packaging:** container image, Helm chart for Kubernetes, JAR distribution
- **Built-in operations skill:** guided diagnostics (for example XDCR) with explicit apply-or-propose rules
- **Volt Agent Skills:** voltdb-development, voltsp, volt-kubernetes

Key outcomes

- A shorter path from schema to working application: assistants generate code against the live catalog with Volt's development skill loaded
- A faster first pass at diagnosis: the assistant reads the cluster's own statistics and follows Volt's operations guidance
- AI access that stays inside Volt's security model: Volt users, roles and TLS, with nothing new to administer
- One centrally deployed server for a team, instead of a copy per laptop

AVAILABILITY

Volt MCP Server 2.1 is available now as a free download from Volt, with a container image on Docker Hub. It works with Volt V15 and later; use with earlier Volt versions requires a license that includes the Active(MCP) feature.

Book a technical call voltactivedata.com/contact

Volt Active Data is the real-time decisioning layer for mission-critical systems.