MCP SERVER | NO CODE | CLOUD HOSTED

Starburst MCP

Query federated data lakes with natural conversation.

Starburst MCP connects your AI client directly to enterprise federated data lakes. It lets you run complex SQL queries against diverse sources like Snowflake and S3, check schemas, and manage access roles—all using natural conversation. You query massive, distributed datasets without ever leaving your chat window or needing multiple database connection tools.

A+ Quality Score 100/100

data-lake | federated-query | trino | data-engineering | sql-analytics | data-governance

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026
vinkius.com/mcp/starburst

SCAN TO VIEW

The connectivity layer between AI and the world's software.

Vinkius sits between AI and every application. All communication passes through Vinkius Cloud via the Model Context Protocol (MCP) — with governance, observability, and security at every layer.

Your AI Connections Run Through Vinkius Cloud

The world's largest managed MCP catalog

Vinkius is the connectivity layer where AI connects to the software your business already runs. We handle the hosting, the security, the credentials, the uptime — you get agents that actually do things.

We operate the world's largest managed MCP catalog. Major SaaS platforms, CRMs, databases, and cloud providers — running, monitored, production-ready. This MCP server is hosted and maintained by the Vinkius Cloud for AI Agents.

> *The agent doesn't manage credentials, doesn't manage uptime, doesn't manage security. Vinkius does.*
>
> — Architecture principle

Four Pillars of the Vinkius Runtime

01 — Security by design

Credentials stay encrypted at rest via AES-256. The AI agent never touches raw keys — they're injected into a sandboxed V8 isolate at runtime. Actions are logged, and connections have an emergency kill switch.

02 — Built on MCP Fusion

This MCP server was built with **MCP Fusion**, the open-source framework (Apache 2.0) that powers the entire Vinkius catalog. Schema-as-firewall strips undeclared fields, compiled PII redaction runs at zero overhead, and cryptographic lockfiles produce git-diffable audit trails.

03 — Deterministic observability

Eight immutable metrics per endpoint: request volume, p95 latency, error rate, active connections, cost attribution. A live payload feed logs every tool call with mutation detection.

04 — Autonomous operations

Servers are deployed, monitored, and patched autonomously. New capabilities and security patches ship weekly. Zero-downtime deployments ensure continuous availability across all managed MCP servers.

AES-256	Ed25519	24h TTL	V8 Isolate
Encryption at rest	PKI vault signatures	Ephemeral session keys	Sandboxed execution

One Token. Instant Access.

Every MCP server on Vinkius is accessed through a **Connection Token**. Tokens are generated in the cloud dashboard and produce a unique MCP endpoint URL. Paste this URL into any MCP-compatible client — no SDK required.

A single token can serve **multiple AI clients simultaneously**, or you can issue separate tokens per client for granular access control. Each token tracks its own request count, last activity timestamp, and can be individually enabled or revoked.

MCP ENDPOINT

```
https://edge.vinkius.com/{token}/mcp
```

Claude · Cursor · VS Code · Windsurf · Grok · Gemini

Security Is the Architecture

Security in Vinkius is not a feature — it's the foundation of the runtime. The gateway enforces multiple independent protection layers between AI agents and third-party APIs.

01 — Ed25519 PKI Vault

Every workspace has an Ed25519 Master Key. Session keys are generated ephemerally (24h TTL) and signed by the Master Key. Credentials never leave the vault boundary.

02 — V8 Isolate Sandboxing

Tool code runs inside isolated-vm V8 isolates with 64 MB memory caps and per-request timeouts. No filesystem access, no network access except through the SSRF-guarded fetch bridge.

03 — SSRF Guard

All outbound HTTP requests are DNS-resolved and validated before execution. Private IP ranges (10.x, 172.16-31.x, 192.168.x, AWS metadata 169.254.x) are blocked at the network layer.

04 — DLP & PII Redaction

A ResponseGuard pipeline intercepts every tool response. Configurable redaction patterns strip sensitive fields (emails, SSNs, card numbers) before data reaches the AI agent.

05 — Cryptographic Audit Trail

Every request is signed into a SHA-256 hash chain with Ed25519 signatures. Events form a tamper-proof, SIEM-exportable forensic record.

06 — Honeytoken Trap System

Phantom credentials are injected into isolated environments. If a honeytoken is used outside Vinkius infrastructure, the server is quarantined instantly.

Emergency Kill Switch

EU AI Act Art. 14(1) Compliant

The kill switch is an **emergency halt** mechanism — not a simple toggle. When triggered, it executes three actions atomically:

01 — Server deactivated

The MCP server is immediately taken offline across the entire cluster.

02 — All tokens revoked

Every connection token is invalidated. Total lockout — reconnection blocked until new tokens are issued.

03 — WebSocket connections killed

Active connections terminated via Redis pubsub broadcast. Propagates to every runtime node in the cluster.

Full Visibility. Zero Guesswork.

The Vinkius cloud dashboard includes a full MCP Governance suite — real-time analytics and security controls for production AI operations.

Control Plane

KPI dashboard with request volume, latency, success rate, token consumption, and AI-generated operational briefings.

Agent Activity

Which AI clients are connecting, how often, and what they're doing — real-time session tracking.

FinOps

Cost tracking per tool, payload compression savings, budget optimization signals, and consumption trends.

Tool Health

Slowest and most error-prone tools, with actionable root-cause insights and performance baselines.

Firewall & DLP

PII redaction activity, sensitive data protection counters, and security event timeline.

Incident Log

Error trends, failure rates, status-code breakdowns, and forensic audit trail access.

> Get started at **cloud.vinkius.com** — connect your AI agent in under 60 seconds.

Starburst MCP

6 tools available
Cloud-hosted on Vinkius

This MCP brings the power of enterprise data analytics into your conversational AI workflow. Instead of opening ten different dashboard tabs or writing boilerplate SQL connection scripts for every source, you talk to your agent and ask questions about your combined data lakes. Your client uses this MCP to figure out which sources are connected (like S3 or Snowflake) and lets you query them as if they were one giant database. You can run complex queries against the entire system, check what schemas exist across different departments, and even verify who has access to sensitive information. It's about making data governance and advanced querying feel natural. When working with other enterprise tools, Vinkius makes sure this MCP is available alongside thousands of others, so your AI client never gets stuck needing a new connection.

Core Capabilities

01 — Run complex SQL queries

You execute advanced SQL commands against massive data sources and receive structured results directly.

02 — Map connected databases

The system lists all the major data catalogs attached to your network, showing you where your data lives.

03 — Explore table structures

You drill down into specific databases to see exactly what schemas and tables are available for querying.

04 — Identify published datasets

The MCP lists all the pre-approved, structured data products ready for analysis across your enterprise.

05 — Check user permissions

You verify who has access to what by listing security roles and checking current assignments.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/mcp/starburst** — connect your AI agent in three steps.

01 First, you install the Starburst MCP connector, linking it securely to your active AI client.

02 Next, in the MCP settings, you provide your STARBURST_HOST and STARBURST_TOKEN to establish a persistent connection session.

03 Finally, you just ask your agent: 'Show me the top 10 rows from customer analytics.' The MCP handles the rest.

The bottom line is that this MCP turns complex, multi-step database interactions into simple conversation prompts.

Built For

This is for data professionals who spend too much time wrestling with connection strings and switching between dozens of specialized dashboard tools. It's the analyst who needs to check three different systems just to get a complete picture, or the engineer who dreads writing complex boilerplate code every single week.

Data Analyst

They use this MCP to explore massive federated datasets by simply asking for reports and executing complex SQL without building connection scripts.

Data Engineer

They rely on it to parse schemas, manage catalogs, and iterate over queries conversationally instead of writing detailed auditing code.

Data Governance Manager

They use this MCP to maintain oversight by verifying role assignments and checking internal data products without logging into multiple security consoles.

What Changes When You Connect

01 You get immediate visibility into your entire data landscape. Instead of manually checking multiple systems, running `list_catalogs` shows all connected sources in one go.

02 Complex reporting becomes simple talking. You write a prompt like 'top 10 customer records' and the agent executes it instantly using `execute_query`, getting structured results back.

03 Data governance is simplified. Need to know who can see payroll data? Use `list_roles` to review security assignments without logging into an admin portal.

04 Never get lost in your schema again. You can use `list_schemas` to drill down and map out exactly what tables exist inside a specific database structure.

05 Discover approved datasets easily. Instead of guessing which dataset is correct, run `list_data_products` to see every published data product ready for analysis.

Real-World Applications

Finding the source of truth for sales metrics

A Data Analyst needs to compare sales figures from the production system (Snowflake) against archived records (S3). Instead of writing a massive script with three connection points, they ask their agent. The MCP uses `list_catalogs` and then runs an `execute_query` across both sources, giving them one unified result set.

Auditing data access for compliance

A Governance Manager needs to prove that only the Finance team can view salary data. They prompt the agent to run `list_roles`, verifying that the 'analyst' role lacks permission, and then cross-reference this with active assignments.

Quickly diagnosing a broken report

A Data Engineer notices a dashboard is failing. They ask their agent to run `list_queries` to check recent failures, or use `get_query_details` to see exactly what parameters caused the failure in the last run.

Preparing for a new feature launch

The team needs a dataset combining marketing and sales data. They first use `list_data_products` to identify the existing components, then ask the agent to construct an `execute_query` that links them together.

Patterns to Avoid

Connecting system by system

✗ AVOID

Writing separate connection blocks for Snowflake and S3 just because you need data from both. This takes hours of boilerplate code.

✓ INSTEAD

Tell your agent to query the combined dataset. The MCP handles multiple sources automatically, so all you do is ask one conversational question using `execute_query`.

Forgetting current permissions

✗ AVOID

Writing a powerful query and running it only to find out later that your account doesn't have access to the required table.

✓ INSTEAD

Before writing code, always run `list_roles` and check the security assignments. This confirms you have the necessary access before wasting time on failed queries.

Not knowing what data exists

✗ AVOID

Opening a database console only to find dozens of schemas, none of which are clearly labeled or documented.

✓ INSTEAD

Start by running `list_catalogs` and then use `list_schemas` to systematically map out the available databases before you start building queries.

The Right Fit

Use this MCP if your core problem is querying data spread across multiple, diverse sources—like combining logs from S3 with structured data in Snowflake. You need natural language control over complex SQL and robust data governance checks using tools like `list_roles` or `list_data_products`. Don't use this if you simply need to send a message or manage user contacts; those are messaging MCPs. Also, don't use it if your only goal is simple document retrieval; for that, look at a dedicated knowledge base tool instead.

Data auditing and querying used to feel like an endless series of clicks.

Today, getting a full view requires logging into the data warehouse UI, running a query, downloading the CSV, then switching to the governance portal to check permissions, and finally opening the schema documentation just to figure out what column names mean. It's constant context switching.

With this MCP, you tell your agent exactly what data you need and from where. The AI client does all that cross-referencing—listing catalogs, checking schemas, running the SQL—and hands you a single answer.

Starburst MCP gives you immediate control over your data environment.

You no longer have to manually run `list_catalogs` and then drill down through multiple screens just to see what databases are even connected. The system maps it out for you automatically when you ask a general question.

It means your data exploration moves at the speed of thought, not the speed of clicking through a dozen different administrative dashboards.

Starburst MCP with 6 Tools

Use these tools to manage the structure of your data environment, from listing all connected catalogs to running specific SQL queries.

#	TOOL	DESCRIPTION
01	`get_query_details`	Retrieves specific information about a particular SQL query you ran.
02	`list_catalogs`	Lists all the main data catalogs available across your entire Starburst network.
03	`list_data_products`	Lists every published, pre-packaged analytical dataset ready for consumption.
04	`list_domains`	Shows the various domains that organize your data products.
05	`list_queries`	Retrieves a history of recent SQL queries executed in the system cluster.
06	`list_roles`	Displays all security roles defined across your organization's data environment.

See It in Action

Real prompts you can use once this MCP is connected to your AI agent through Vinkius Cloud.

U List all active operational catalogs across the current data lake instance, and fetch the underlying schematics of any source containing the designation 'finance' in its structure.

Parsing connection parameters effectively iterating across federated network protocols successfully maintaining persistent host authentication securely.

Catalogs Displayed: `hive`, `postgres_ops`, `finance_db`.

Extracting schematics specifically querying `finance_db`...
Schemas detected safely (`list_schemas`):
- `public`
- `payroll`
- `audit_logs`

Would you like me to execute a precise subquery mapping tables securely localized within `audit_logs` specifically utilizing advanced conversational routines accurately?

U Execute a query to retrieve the top 10 rows from the 'customer_analytics' table located in our 'production_hive' catalog.

Executing federated SQL query seamlessly...

Query Results (`execute_query`):
The top 10 rows from `production_hive.customer_analytics` have been successfully retrieved. The dataset includes fields such as `customer_id`, `purchase_history`, and `engagement_score`. Would you like me to aggregate this data safely?

U List all registered data products across the Starburst network and check current role assignments to ensure proper access.

Analyzing data products and roles securely within the Starburst ecosystem...

Data Products (`list_data_products`):
- `Marketing Insights Dashboard`
- `Global Sales Summaries`

Role Governance (`list_roles`):
Verified active assignments for `analyst_tier_1` and `data_governance_admin`. Access privileges align securely with enterprise standards.

Frequently Asked Questions

01 **How does Starburst MCP handle multiple database types?**

The MCP is designed to query federated data lakes. It connects to diverse sources like Snowflake and S3, allowing you to run a single query against all of them.

02 **Can I see which roles exist using Starburst MCP?**

Yes, running `list_roles` allows the agent to display every security role defined in your organization's data environment for auditing purposes.

03 **What is the difference between list_catalogs and list_schemas?**

Using `list_catalogs` shows the highest level of grouping (the entire database instance), while `list_schemas` lets you drill down to see the specific groups of tables within one catalog.

04 **Does Starburst MCP help with data discovery?**

Absolutely. By listing available data products using `list_data_products`, it helps you find pre-approved, curated datasets without knowing their exact location or schema name.

05 **What is the best way to check query history with Starburst MCP?**

You use the `list_queries` tool. This lets your agent retrieve a clean record of recent SQL queries executed in the cluster for review.

Go Live in 60 Seconds

Get your connection token from **cloud.vinkius.com**, then paste the endpoint URL into any MCP-compatible client.

YOUR MCP ENDPOINT

```
https://edge.vinkius.com/[TOKEN]/mcp
```

CLIENT	WHERE TO CONFIGURE
Claude AI	Profile → Customize → Connectors → "+" → Add custom connector → Paste endpoint
Cursor	Settings → Features → MCP Servers → "+ Add New MCP Server" → Type: SSE → Paste endpoint
VS Code	Ctrl/Cmd+Shift+P → "MCP: Add Server" → add `"starburst": { "url": "…" }`
Windsurf	MCP Settings → `mcp_settings.json` → Add endpoint URL
ChatGPT	Settings → Tools & plugins → Add MCP server → Paste endpoint
Gemini	Extensions → Add MCP Server → Paste endpoint URL

ASK AN AI ABOUT THIS

Let your preferred AI explain this MCP server

- Ask ChatGPT
- Ask Claude
- Ask Perplexity
- Ask Gemini
- Ask Grok

READY TO CONNECT

Starburst is live on Vinkius Cloud.

Get your connection token, paste it into your AI agent, and start building. No SDK. No deployment. Just results.

Start at cloud.vinkius.com →

INDEPENDENT PLATFORM DISCLAIMER

Vinkius is an independent platform and is not affiliated with, endorsed by, sponsored by, verified by, or otherwise authorized by Starburst. All third-party trademarks, logos, and brand names are the property of their respective owners. Their use in this document is strictly for informational purposes to identify service compatibility and interoperability.

DOCUMENT INFORMATION

Generated	June 2026
MCP Server	Starburst MCP
Server ID	`019d760d-3e66-71e5-8f6a-015ebd0e9756`
Platform	Vinkius Cloud for AI Agents
Endpoint	`https://edge.vinkius.com/{token}/mcp`

LICENSE & USAGE

This document is generated automatically by the Vinkius PDF Engine. Content reflects the MCP server configuration at the time of generation and may change as updates are deployed. For the most current information, visit vinkius.com/mcp/starburst.