

MCP SERVER

NO CODE

CLOUD HOSTED

CockroachDB Cloud MCP for AI Agents

Monitor Distributed SQL Cluster Health and Network Rules

CockroachDB Cloud MCP lets you manage your distributed SQL infrastructure entirely through natural conversation with your AI agent. You can list every cluster, check node health, audit network rules, and review management operations without ever opening the cloud console. It gives you full control over globally-scalable databases directly from your chat interface.

F Quality Score 3.6/100

distributed-sql

cluster-management

high-availability

scalability

database-monitoring

cloud-native



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.

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.

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.

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

Encryption at rest

Ed25519

PKI vault signatures

24h TTL

Ephemeral session keys

V8 Isolate

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.

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.

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.

06 — Honeypot Trap System

Phantom credentials are injected into isolated environments. If a honeypot 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.

FinOps

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

Firewall & DLP

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

Agent Activity

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

Tool Health

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

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.

CockroachDB Cloud MCP

8 tools available

Cloud-hosted on Vinkius

Connecting your CockroachDB Cloud account to an AI client means taking back time spent clicking through complex database dashboards. Instead of navigating provider consoles to check cluster status or network rules, you just talk to your agent. You can ask it to list all clusters across regions or pull up the details for specific nodes to see if they're running correctly. Need to verify who has access? Your agent pulls up user profile data instantly. If you need to audit recent changes, simply request a review of cluster operations. This MCP handles everything from checking encryption key metadata to reviewing network allowlist rules—all in plain language. For the full scope of connectivity, check out the Vinkius catalog; it connects your AI client to thousands of services like this one. It's about getting answers and taking actions without ever leaving your chat window.

Core Capabilities

01 — Get Cluster Details

Retrieve detailed information for any specific CockroachDB cluster.

02 — View User Profile

Fetch basic details about your authenticated user and organization.

03 — Audit Network Rules

List all network allowlist rules for a specific cluster to check connectivity security.

04 — Check Encryption Keys

List the Customer Managed Keys (CMKs) used to encrypt your cluster data.

05 — Identify Cloud Providers

See which cloud providers CockroachDB supports globally.

06 — List All Clusters

Get a complete list of every CockroachDB cluster you manage.

07 — Monitor Cluster Nodes

View all individual nodes within a specified cluster to assess their health and status.

One Click on Vinkius — From Prompt to Execution

Available at vinkius.com/mcp/cockroachdb-cloud — connect your AI agent in three steps.

- 01 Subscribe to the CockroachDB Cloud MCP in Vinkius and provide your API Secret Key.
- 02 Your AI client securely connects using the provided credentials, establishing a direct line to your database infrastructure.
- 03 You simply ask your agent questions—like 'Show me all clusters' or 'What are the current network rules?'—and it delivers structured data instantly.

The bottom line is that you manage complex, distributed databases using simple conversation and no manual console clicks.

Built For

Database Administrators (DBAs) who are sick of context switching between multiple cloud consoles. Cloud Engineers needing to audit regional deployments quickly. Security teams that must verify network allowlists or encryption keys on the fly.

Database Administrator (DBA)

Uses natural language to list all clusters and check node status, eliminating manual dashboard checks for health monitoring.

Cloud Engineer

Audits network allowlist rules or retrieves cluster details across multiple providers without having to log into the cloud console itself.

Security Analyst

Quickly reviews encryption key metadata and operational history of changes using plain chat commands, ensuring compliance.

What Changes When You Connect

- 01 Check cluster health instantly: Use the `list_cluster_nodes` tool to assess node status without logging into a dashboard.

-
- 02** Audit security rules easily: The `list_network_allowlist` tool lets you check connectivity rules in seconds, critical for security teams.
-
- 03** Track changes accurately: Running `list_cluster_operations` provides an audit trail of every scaling or upgrade action taken on your database.
-
- 04** Manage secrets without hassle: You can use `list_encryption_keys` to quickly view all Customer Managed Keys used for data encryption.
-
- 05** Understand scale: The ability to run `list_cockroach_clusters` gives you an immediate, comprehensive overview of your entire global footprint.
-

Real-World Applications

A new team member needs a cluster overview

Instead of spending an hour walking through the provider console to find all active databases, the engineer asks their agent to `list_cockroach_clusters`. The response immediately gives them a comprehensive list of every environment (Dev, Prod, Sandbox) and its region.

Post-incident review of database changes

After performance issues are reported, the DBA needs to know what changed. They use `list_cluster_operations` to pull up a timeline of recent management tasks, determining if a specific scaling event or upgrade was responsible.

Investigating unusual network access

The security team suspects unauthorized external connections. They ask the agent to `list_network_allowlist` for the production cluster. The agent returns a concise list of IP ranges, allowing them to verify if the suspicious activity originated from an unlisted source.

Verifying data compliance in different regions

A platform team needs to know what encryption methods are used across all deployments. They run the key listing tool (`list_encryption_keys`) and receive a clear inventory of CMKs, ensuring every cluster meets regulatory standards.

Patterns to Avoid

Manual Console Checking

X AVOID

A user logs into three different cloud provider consoles (AWS, GCP, Azure) and clicks through multiple tabs just to list all available clusters.

✓ INSTEAD

Just ask your agent to ``list_cockroach_clusters``. It aggregates the data from all providers in one chat response, saving you hours of clicking.

Guessing Connection Rules

X AVOID

A developer assumes a new service can connect because it used to work, and manually tries various IP ranges until the connection succeeds.

✓ INSTEAD

Always use ``list_network_allowlist`` first. This verifies exactly what IPs are permitted for the cluster before you attempt any deployment.

Ignoring Operational History

X AVOID

A DBA sees slow performance and immediately restarts services, without knowing if a recent version upgrade caused the issue.

✓ INSTEAD

Run ``list_cluster_operations`` to see the exact timeline of events. This helps you diagnose whether the performance dip correlates with a specific scaling or update action.

The Right Fit

Use this MCP if your primary pain point is context switching across multiple cloud provider dashboards while managing distributed databases. If you regularly need quick, comprehensive views of cluster topology, node health, network rules, or operational history via natural conversation, this tool is for you. Don't use it if you only need to write SQL queries—you still need a dedicated query execution environment for that. Also, don't rely on it for writing code; focus on monitoring and auditing. If your goal is deep architectural planning, you might need specialized modeling tools, but for day-to-day operational visibility, this MCP is the answer.

CockroachDB Cloud: Auditing Cluster Network Allowlist Rules with CockroachDB Cloud

Today, checking network access means logging into a dedicated cloud console. You have to navigate through security groups and networking tabs just to find the list of allowed IP addresses for your production cluster. It's tedious copy-pasting and clicking that risks missing an outdated rule or misinterpreting the output.

With this MCP, you simply ask your agent, 'What is the network allowlist for the Production database?' The agent runs `list_network_allowlist` and spits out a clean, current list of rules in plain text. You get immediate, verifiable clarity on who can talk to your cluster.

CockroachDB Cloud: Monitoring Distributed SQL Node Status with CockroachDB Cloud

Manually checking the health of dozens of nodes across different regions is a nightmare. You open one dashboard, check status; switch to another, check logs; repeat until you've seen everything. This process takes hours and requires deep console knowledge.

Now, just ask your agent to `list_cluster_nodes`. It pulls up the health status for every node in one go. This gives you an instant, aggregated view of the entire system, telling you exactly where the problem is without leaving your chat window.

CockroachDB Cloud: 8 Tools for Cluster Management and Auditing

These tools allow you to query details on cluster nodes, review security policies, and track operational changes in your CockroachDB environment using natural language.

#	TOOL	DESCRIPTION
01	<code>get_cluster_cloud_details</code>	Retrieves detailed information about a single specific cluster you own.
02	<code>get_my_cockroach_profile</code>	Pulls up basic details about your organization and user account settings.
03	<code>list_network_allowlist</code>	Provides a list of current network allowlist rules for a specified cluster.
04	<code>list_encryption_keys</code>	Lists all Customer Managed Keys (CMKs) used to encrypt your database data at the cluster level.
05	<code>list_supported_cloud_providers</code>	Returns a list of cloud providers that CockroachDB Cloud supports in various regions.
06	<code>list_cockroach_clusters</code>	Generates an exhaustive list containing all your existing CockroachDB Cloud clusters.
07	<code>list_cluster_nodes</code>	Shows a detailed list of every node that belongs to a specific cluster, including its status.
08	<code>list_cluster_operations</code>	Lists recent management operations performed on a cluster, such as scaling or version upgrades.

See It in Action

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

U What are all my active clusters and what region are they in?



Cluster Inventory Report

I found 4 distinct CockroachDB Cloud clusters:

- **Prod-US-East:** AWS, us-east-1. Status: **RUNNING**. Last check: 2 minutes ago.
- **Dev-Europe:** GCP, europe-west1. Status: **ACTIVE**. Last check: 5 minutes ago.
- **Sandbox-Asia:** Azure, eastasia. Status: **STANDBY**. Last check: 1 hour ago.
- **Global-Main:** AWS, us-east-1. Status: **RUNNING**. Last check: 2 minutes ago.

U Show me the last three changes made to the Global-Main cluster.



Cluster Operations Audit: Global-Main

Here are the most recent management operations:

1. **Type:** CLUSTER_SCALE | **Details:** Increased node count from 5 to 7. | **Time:** Oct 24, 2023 @ 10:00 AM EST.
2. **Type:** VERSION_UPDATE | **Details:** Minor version upgrade applied (v23.1 to v23.2). | **Time:** Oct 24, 2023 @ 8:30 AM EST.
3. **Type:** NETWORK_RULE_ADD | **Details:** Added rule for IP range 192.168.1.0/24. | **Time:** Oct 24, 2023 @ 7:00 AM EST.

U What are all the supported providers and my user profile?



Cloud Support & User Profile

Supported Providers: AWS, GCP, Azure, Oracle Cloud.

Your Account Details:

- Organization: GlobalTech Solutions Inc.
- User ID: jsmith@globaltech.com
- Role: Senior DBA
- Last Login: Today.

Frequently Asked Questions

01 How does the CockroachDB Cloud MCP help me monitor cluster nodes?

You ask your agent to list all nodes for a specific cluster. It gives you a real-time status report on every single node, telling you if they are healthy or struggling without opening any dashboards.

02 Can I use the CockroachDB Cloud MCP to check my network security rules?

Yes. You can run a command via your agent that lists all network allowlist rules for a cluster, letting you audit connectivity from one place in your chat window.

03 Is the CockroachDB Cloud MCP better than checking the cloud console?

It's much faster. Instead of switching between AWS and GCP consoles to find details, this MCP aggregates all that information into a single, conversational response for you.

04 What kinds of operational history can I check with CockroachDB Cloud MCP?

You can pull up the full audit trail. This includes records of cluster scaling events, version upgrades, and any other management task that occurred on your database.

05 Does this help me manage encryption keys in CockroachDB Cloud?







Absolutely. You can use the MCP to list all Customer Managed Keys (CMKs) used across your clusters, which is vital for compliance and security audits.

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 <code>"cockroachdb-cCloud": { "url": "..." }</code>
 Windsurf	MCP Settings → <code>mcp_settings.json</code> → 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

CockroachDB Cloud 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](https://cloud.vinkius.com) →

vinkius.com · support@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 CockroachDB Cloud. 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	CockroachDB Cloud MCP
Server ID	019d7575-c62c-7288-b8c6-7b09372301df
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/cockroachdb-cloud.