MCP SERVER | NO CODE | CLOUD HOSTED

Vultr MCP

Control bare metal and cloud networking via chat.

Vultr MCP gives your agent full control over cloud infrastructure, bare metal instances, and backups. Manage everything from account billing to rebooting servers—all through natural conversation. Stop switching between SSH sessions and web dashboards; handle complex networking setups and deployments directly within your AI client.

A+ Quality Score 98.33/100

vultr | bare-metal | cloud-hosting | infrastructure-as-code | server-management

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

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.

Vultr MCP

19 tools available
Cloud-hosted on Vinkius

Managing cloud resources usually means hopping between a dozen different tabs: the dashboard for billing, the terminal for reboots, and the network settings page for DNS records. This MCP changes that. Connect your Vultr account to any compatible agent and treat your entire infrastructure like a single conversation. You can list all bare metal instances across global regions or get the IPv6 details for a specific machine on the fly. Need to update BGP configurations or deploy an application from the Marketplace? Just ask. Because this MCP sits in the Vinkius catalog, you don't have to worry about integrating multiple service connectors; you connect once and gain access to high-performance infrastructure management instantly.

Core Capabilities

01 — Manage instance lifecycle

Start, stop, reboot, reinstall, or delete physical bare metal servers with simple commands.

02 — Handle networking configurations

Setup BGP settings and manage both IPv4 and IPv6 reverse DNS records for any instance.

03 — View account status and billing

Retrieve current account information, check the billing status, and list existing API keys.

04 — Backups and deployments

List available automated backups or browse the Marketplace to deploy one-click applications onto your setup.

05 — Create and control credentials

Generate new API keys and list all existing ones, ensuring controlled access across your infrastructure tools.

One Click on Vinkius — From Prompt to Execution

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

01 Subscribe to this MCP on Vinkius and provide your specific Vultr API Key.

02 Your agent uses the key to authenticate against the Vultr API, granting it permission to manage your resources.

03 You interact with it using natural language prompts like 'Reboot my primary web server in Frankfurt' or 'What is the billing status for this account?'

The bottom line is that you talk to your agent exactly how you talk to a teammate, and it handles the complex API calls needed to manage your entire cloud environment.

Built For

This MCP is for the DevOps Engineer who's tired of context switching between three different dashboards. It's for the Cloud Architect who needs instant visibility into BGP settings across global regions, and any Developer needing to manage API keys or deploy marketplace apps without leaving their IDE.

DevOps Engineer

You use it to check server statuses and reboot bare metal instances from your chat client instead of switching back to the terminal.

Cloud Architect

You inspect BGP settings and network configurations across multiple regions, consolidating complex networking data into one conversation thread.

Backend Developer

You manage API keys or list marketplace applications to set up automated deployment workflows for new services.

What Changes When You Connect

01 You instantly check the status of any machine, whether you need to `list_bare_metals` or just check if a specific server is running. No more logging into multiple dashboards for simple health checks.

02 Managing complex network settings used to mean jumping between DNS records and BGP consoles. Now, you can use tools like `setup_bgp` and `set_bare_metal_ipv4_reverse` conversationally. It's all one chat window.

03 Need to provision a new machine? Instead of clicking through five forms, simply ask the agent to `create_bare_metal`. It handles the entire lifecycle from request to ID assignment.

04 Don't lose critical access credentials. Use `list_api_keys` and `create_api_key` to manage your programmatic access points without leaving your workflow.

05 When a service fails, you don't need to guess what worked last time. You can use `list_backups` and then `get_backup` to pull up the exact restore point details instantly.

Real-World Applications

Need to isolate a failing service immediately

A developer notices high latency on their primary web server. Instead of manually SSHing into the machine and restarting services, they simply instruct their agent to `halt_bare_metal` on that specific instance, verifying connectivity with `get_account` status before proceeding.

Preparing a new data center connection

The Cloud Architect needs to ensure the new site has proper routing. They ask the agent to check `list_bare_metals`, then run `get_account_bgp` and finally execute `setup_bgp` to confirm all necessary routes are active.

Automating a dev environment update

The DevOps Engineer needs a fresh test server. They ask the agent to first run `create_api_key` for the automated pipeline, and then use the resulting credentials to `list_applications`, deploying 'Docker' instantly.

Restoring an account after misconfiguration

A system owner accidentally deleted a necessary server. They ask the agent to first check `list_backups` for viable restore points, and then use the relevant tool to restore or recreate the instance.

Patterns to Avoid

Manual dashboard hopping

✗ AVOID

A user needs to reboot a server. They open the web portal, find the machine's ID, click 'Actions', select 'Reboot,' and hit submit. This takes 4-5 clicks and requires context switching.

✓ INSTEAD

Just ask your agent: 'Can you `reboot_bare_metal` for the instance named Web-Frontend?' It handles the API call directly from your chat.

Guessing required permissions

✗ AVOID

A developer needs to write a script that interacts with Vultr, but they aren't sure if their current key has enough rights. They might end up creating a useless key or one that fails later.

✓ INSTEAD

First, use `list_api_keys` to see what you have. Then, ask the agent to help you generate a specific new key using `create_api_key` with only the necessary permissions.

Ignoring global network scope

✗ AVOID

A Cloud Architect needs to check BGP status for multiple sites but only checks one region's dashboard, missing critical cross-region routing errors.

✓ INSTEAD

Don't look at single dashboards. Ask the agent to `get_account_bgp`. It pulls your global account information in one go.

The Right Fit

Use this MCP if you need deep, low-level control over cloud infrastructure components—things like BGP setup, IPv6 reverse DNS records, or bare metal lifecycle management. If your job involves provisioning new servers, managing network routes, or handling account credentials programmatically, this is the right tool. Don't use it if all you need to do is view a single piece of data, like checking an

email balance (use a dedicated billing MCP for that). Also, don't use it just because you 'might' need to check a server status; only use it when you are ready to issue the command—like `reboot_bare_metal` or `halt_bare_metal`. When in doubt about connectivity, start by running `list_bare_metals`; that gives you the full inventory before you take action.

Infrastructure changes used to mean a lot of clicking and context switching.

Think about how you handle routine maintenance today. You log into the portal, check server A's status in one tab; then switch to the networking page to verify DNS records for B; next, you jump to the billing section just to confirm your API key limits are okay. It’s a painful dance of dashboards and copy-pasting IDs.

With this MCP, that whole process collapses into conversation. You simply tell your agent what needs doing—whether it's creating an account record with `create_bare_metal` or pulling the current billing status via `get_account`. It handles all the underlying clicks for you.

Vultr MCP gives you complete command control over bare metal and network settings.

The specific manual tasks that disappear are: navigating to the correct subnet panel, manually setting a reverse DNS record with `set_bare_metal_ipv4_reverse`, or figuring out which API key is active by running `list_api_keys`.

What's different now is speed and focus. You keep all your complex infrastructure management conversation in one place, letting the agent handle the heavy lifting across the entire Vultr environment.

Vultr MCP: 19 Tools for Cloud Management

These tools allow you to perform every major operation on your Vultr accounts, from managing API keys and listing backups to rebooting machines.

#	TOOL	DESCRIPTION
01	`get_bare_metal_ipv6`	Retrieves the IPv6 address information for a specific bare metal instance.
02	`halt_bare_metal`	Stops all operations and powers down a selected bare metal instance immediately.
03	`reboot_bare_metal`	Restarts the operating system on a specified bare metal machine.
04	`reinstall_bare_metal`	Wipes and reinstalls the operating system onto an existing bare metal instance.
05	`set_bare_metal_ipv4_reverse`	Configures or updates the reverse DNS settings for an IPv4 address on a machine.
06	`set_bare_metal_ipv6_reverse`	Configures or updates the reverse DNS settings for an IPv6 address on a machine.
07	`setup_bgp`	Sets up Border Gateway Protocol (BGP) routing necessary for advanced network connectivity.
08	`start_bare_metal`	Powers on a previously halted bare metal instance, bringing it back online.
09	`delete_bare_metal`	Permanently removes the specified bare metal instance from your account.
10	`list_backups`	Lists all available automated backup records for your infrastructure.
11	`list_bare_metals`	Retrieves a comprehensive list of every bare metal instance in your account.
12	`create_api_key`	Generates and provides a brand new API key for programmatic access to Vultr services.
13	`get_bare_metal_ipv4`	Retrieves the IPv4 address details associated with a bare metal instance.
14	`get_backup`	Fetches specific details about a single, targeted backup record.

#	TOOL	DESCRIPTION
15	`create_bare_metal`	Initiates the process of provisioning and creating a new bare metal machine.
16	`get_account_bgp`	Retrieves the BGP information for your entire Vultr account level.
17	`get_account`	Pulls all general billing and account profile details for your Vultr account.
18	`list_api_keys`	Shows a list of every existing API key attached to the account.
19	`list_applications`	Retrieves a catalog listing of available one-click marketplace deployment applications.

See It in Action

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

U List all my bare metal instances.

I've retrieved your bare metal instances. You have 2 active servers: 'DB-Primary' (ID: 550e8400) in New Jersey and 'Web-Frontend' (ID: 660f9511) in Tokyo. Would you like to see the IP details for one of them?

U Show my Vultr account and billing information.

Your account is currently active with a balance of $45.20. Your registered email is 'admin@example.com' and the account is in good standing. Would you like to check your BGP status as well?

U What marketplace applications are available for deployment?

I've listed the available applications. You can deploy 'Docker', 'WordPress', 'cPanel', or 'LAMP' as one-click apps, or choose from various Marketplace images like 'Plesk' or 'OpenVPN'. Which one would you like to deploy?

Frequently Asked Questions

01 **Can I use the Vultr MCP to manage multiple regions?**

Yes. The MCP allows you to list bare metal instances and perform actions like `reboot_bare_metal` across your global deployment without needing regional-specific credentials.

02 **How do I find out what tools are available in the Vultr MCP?**

All 19 specific tools, ranging from `list_backups` to `get_account`, are accessible. You just need to ask your agent for help or check the tool list.

03 **Does this MCP handle billing inquiries?**

It provides general account info using `get_account`. For specific, detailed invoice questions, you should consult Vultr's dedicated support channels.

04 **What is the difference between `halt_bare_metal` and `delete_bare_metal`?**

`Halt_bare_metal` powers down a machine temporarily while keeping its data intact. `Delete_bare_metal`, however, permanently removes the entire server from your account.

05 **I need to deploy an app; which tool should I use in Vultr MCP?**

You first run `list_applications` to see what one-click apps are available. Then, you ask the agent to deploy your chosen application.

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 `"vultr": { "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

Vultr 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 →

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 Vultr. 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	Vultr MCP
Server ID	`019e3907-973c-7271-b108-aea3aee22ddd`
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/vultr.