MCP SERVER | NO CODE | CLOUD HOSTED

Wasabi MCP

Govern Your Cloud Storage Assets via Chat

Wasabi MCP connects your AI agent directly to Wasabi Hot Cloud Storage. It lets you manage storage buckets, check object versions, and audit file access lists using natural conversation. Control where your data lives, list files within any bucket, or delete incomplete uploads—all without navigating a complex cloud console.

F Quality Score 3.89/100

s3-compatible | object-storage | data-residency | bucket-management | cloud-backup | data-archiving

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

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.

Wasabi MCP

10 tools available
Cloud-hosted on Vinkius

You can use this MCP to take full control of all your Wasabi assets through chat. Instead of clicking through confusing storage consoles, you simply tell your AI agent what you need done. You can check which physical region your data is stored in, verify if versioning is active on a bucket for protection against accidental deletions, or even find out exactly who has permissions to view specific files by checking the Access Control List (ACL). If you're used to managing cloud assets via dedicated scripting tools, this MCP offers that control but wrapped in natural conversation. When you connect through Vinkius, your AI agent becomes a hands-on administrator for your entire cloud storage setup. You can also manage containers themselves—create new buckets or permanently remove old ones—and run cleanup tasks to delete those 'fractured' file uploads taking up space.

Core Capabilities

01 — Manage Storage Containers

Create, list, and delete high-availability storage buckets in your account.

02 — Audit File Permissions

Retrieve the access control list (ACL) for any file to verify who has permission to view or edit it.

03 — Verify Data Location

Check the physical geographic region where a specific storage bucket is hosted, which is crucial for compliance.

04 — Track Object History

Activate or check object versioning on a bucket to protect against accidental overwrites and deletions.

05 — Browse Files in Buckets

List all files (objects) within a specific container, including their size and when they were last modified.

06 — Clean Up Uploads

Identify and permanently delete incomplete multipart uploads that are wasting storage space.

One Click on Vinkius — From Prompt to Execution

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

01 Subscribe to this MCP and provide your Wasabi Access Key, Secret Key, and Region credentials.

02 Connect the service to any compatible AI client, like Cursor or Claude.

03 Ask your agent natural language questions, such as 'List all buckets' or 'Check versioning on my main data bucket.'

The bottom line is you manage complex cloud operations by talking to your AI agent instead of clicking through a console.

Built For

This MCP is for the Data Engineer who spends too much time writing boilerplate scripts just to check permissions. It's for the DevOps professional who needs instant compliance checks on data residency. If you handle cloud infrastructure and need conversational control over your assets, this is for you.

Cloud Architect

Verifies that all storage buckets meet regional data residency requirements or provisions new containers in specific geographic locations.

Data Engineer

Browses entire datasets using list_bucket_objects to find files, checks the versioning status on critical buckets, and cleans up incomplete uploads via list_pending_multipart_uploads.

DevOps Professional

Automates tasks like calling create_storage_bucket or deleting_storage_bucket, and quickly audits file access by retrieving the object's ACL.

What Changes When You Connect

01 Compliance checks are instant. Instead of manually checking the console for data residency, simply ask your agent to run get_bucket_datacenter_location and confirm where your data sits.

02 You'll never lose a file again. Use enable_bucket_versioning to activate object versioning on critical buckets, protecting against accidental overwrites or deletions across your dataset.

03 Know exactly what you're deleting. Before running delete_storage_bucket, use list_storage_buckets and list_bucket_objects to see the contents and verify which files are safe to remove.

04 Save time auditing permissions. Running get_object_access_control on a file instantly shows who can access it, eliminating manual security checks for sensitive data.

05 Stay organized with cleanup tasks. Use list_pending_multipart_uploads to find those 'orphaned' uploads that take up space and need permanent deletion via delete_bucket_object.

Real-World Applications

Auditing a New Project's Data Residency

A Cloud Architect needs to confirm if all user data for a new EU client is physically stored in the European region. Instead of navigating compliance dashboards, they ask their agent to get_bucket_datacenter_location on the project bucket and verify the output matches the required geography.

Recovering from an Accidental Deletion

A Data Engineer accidentally overwrites a critical file. They immediately check the get_bucket_versioning_status and, finding it off, ask their agent to run enable_bucket_versioning before attempting any recovery.

Onboarding a New Team Member

A DevOps Professional needs to grant read-only access to a new team member for the 'user-logs' bucket. They use get_object_access_control on key files and then modify the permissions through their agent, ensuring least privilege.

Cleaning Up Test Environments

An IT Admin notices that old test data is accumulating and wasting money. They ask their agent to list_pending_multipart_uploads across several buckets, identify the junk uploads, and permanently delete them using delete_bucket_object.

Patterns to Avoid

Relying on GUI navigation

✗ AVOID

Spending thirty minutes clicking through Wasabi's web console tabs to find out if a specific bucket has versioning enabled.

✓ INSTEAD

Just ask your agent directly using get_bucket_versioning_status. It gives you the answer in one chat prompt, saving all that manual navigation.

Assuming empty containers

✗ AVOID

Trying to run delete_storage_bucket on a bucket they think is empty but actually still contains old logs.

✓ INSTEAD

First, use list_bucket_objects to confirm the container is truly empty. Once confirmed, you can safely call delete_storage_bucket.

Forgetting data location rules

✗ AVOID

Assuming that because they created a bucket in the US, all data will stay there when accessed by international staff.

✓ INSTEAD

Always verify compliance first. Use get_bucket_datacenter_location to confirm the physical region before moving any sensitive assets.

The Right Fit

Use this MCP if your primary workflow involves auditing, listing, or performing discrete administrative actions on cloud storage buckets and objects. It excels when you need to answer questions like 'What files are in X?' or 'Who can see Y?' without writing a script. Don't use it if you need continuous data streaming or real-time ETL pipelines; for those, stick to dedicated integration tools. However, if your goal is simply reading basic metadata that could be scraped via a public API endpoint, this MCP might be overkill. This tool shines

when the complexity comes from the *management layer* (permissions, versioning, location), not just the data retrieval itself.

The Manual Pain of Cloud Storage Management

Today, managing your cloud storage means logging into a complex web console. You jump between buckets, run different reports to check for orphaned files, and click through multiple menus just to verify if versioning is active or what the data residency status is. It's tedious, slow, and requires constantly switching context.

With this MCP, you talk to your agent instead. Instead of clicking around five tabs to find out who has access to a file, you simply ask, 'Who can view that object?' Your agent handles all the API calls behind the scenes and gives you a direct answer in chat. It’s instant control.

Get Instant Cloud Visibility with Wasabi MCP

The manual steps that disappear are checking permissions, listing objects, and confirming the bucket's physical location. You don't have to copy names from one screen into another to run a status check.

Now, your AI agent is your cloud storage administrator. It gives you immediate visibility over every object, permission, and container in your account. That’s how fast it should be.

Wasabi: 10 Tools for Cloud Infrastructure Management

Use these tools to create, delete, list, check permissions, and audit every aspect of your cloud storage infrastructure via chat.

#	TOOL	DESCRIPTION
01	`create_storage_bucket`	Creates a new, high-availability storage container in your configured Wasabi region.
02	`delete_storage_bucket`	Permanently removes an empty storage bucket from your account. Note: This action cannot be undone.
03	`delete_bucket_object`	Irreversibly deletes a single file from a specified container.
04	`enable_bucket_versioning`	Turns on object versioning for a bucket, which keeps copies of files when they change or are deleted.
05	`get_bucket_datacenter_location`	Retrieves the physical geographic location where an entire storage bucket is hosted.
06	`get_object_access_control`	Pulls the access control list (ACL) for a specific file to show who has permissions.
07	`get_bucket_versioning_status`	Checks if object versioning is currently turned on or off for your bucket.
08	`list_storage_buckets`	Lists all the storage buckets that are visible to your authenticated user account.
09	`list_bucket_objects`	Returns a list of files, showing their keys, sizes, and last modified dates within a bucket.
10	`list_pending_multipart_uploads`	Lists incomplete multipart uploads that are consuming storage space in your bucket.

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 storage buckets in Wasabi.

I found 3 buckets in your account: 'backups-2026' (Created: 2026-01-15), 'user-data-prod' (Created: 2025-11-20), and 'media-assets-global' (Created: 2026-02-10). Would you like to see the contents of any of these?

U What files are inside the 'backups-2026' bucket?

Searching 'backups-2026'... I found 5 objects: 'db-dump-jan.sql' (4.2 GB), 'logs-archive.zip' (850 MB), 'config-backup.json' (12 KB), and 2 others. I can pull the ACL or delete any of these for you.

U Is versioning enabled for my 'user-data-prod' bucket?

Checking status... No, object versioning is currently suspended for 'user-data-prod'. Would you like me to enable it now to protect your files from accidental overwrites?

Frequently Asked Questions

01 **How do I use the Wasabi MCP to check my data residency?**

You run get_bucket_datacenter_location on the specific bucket name. This tells you the exact physical geographic region where your stored data is hosted, which is essential for compliance.

02 **Can Wasabi MCP help me delete files from a bucket?**

Yes. You use delete_bucket_object to permanently remove a specific file, or you can run list_pending_multipart_uploads and then delete the whole incomplete upload.

03 **Is there a way to see all my buckets with Wasabi MCP?**

You simply call list_storage_buckets. This command returns a complete inventory of every bucket visible to your authenticated user account.

04 **Do I need to worry about versioning when using Wasabi MCP?**

It's wise to check the status first by calling get_bucket_versioning_status. If it’s off and you work with critical files, run enable_bucket_versioning immediately.

05 **How do I list all the files inside a container?**

You use list_bucket_objects, specifying the name of the bucket. This returns key information like file names, sizes, and when they were last modified.

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 `"wasabi": { "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

Wasabi 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 Wasabi. 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	Wasabi MCP
Server ID	`019d761f-24b5-7020-ba4c-4b46e95cfc4a`
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/wasabi.