MCP SERVER | NO CODE | CLOUD HOSTED

Amazon S3 MCP for AI Agents

Managing Cloud Object Storage Policies and Data Lifecycle

Amazon S3 MCP connects your AI agent directly to Amazon's cloud object storage, letting you manage data assets via conversation. You can audit bucket policies, create and delete buckets, list objects with their file sizes, and retrieve technical metadata without downloading files. It's full-spectrum control over your AWS data storage.

A+ Quality Score 100/100

object-storage | bucket-management | data-archiving | cloud-infrastructure | metadata | aws

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · JUNE 2026
vinkius.com/mcp/amazon-s3

SCAN TO VIEW

The infrastructure that powers AI agents in the real world.

Vinkius connects AI to the world's software through secure, enterprise-grade infrastructure — enabling real-world execution at scale, built on the Model Context Protocol (MCP).

Your AI Connections Run Through Vinkius Cloud

The world's largest managed MCP catalog

Vinkius is the cloud infrastructure where AI agents connect 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.

Amazon S3 MCP

10 tools available
Cloud-hosted on Vinkius

Need to handle complex cloud storage operations? This MCP gives your agent direct access to manage Amazon S3 environments. You can talk to it like you're talking to a senior DevOps engineer, and it handles the heavy lifting across your AWS infrastructure. Want to know what policies are attached to 'website-images-eu'? Just ask. Need to find all log files from last month? It lists objects in specific buckets, giving you file sizes and modification dates instantly. You can even delete unwanted data or upload new records directly. Because we host thousands of services, accessing this power through Vinkius makes sure your agent always knows exactly how to talk to Amazon S3.

It's built for deep control. Your AI client manages everything from auditing bucket access controls to retrieving object metadata—all through natural conversation.

Core Capabilities

01 — List and audit all storage buckets

Retrieve a list of existing Amazon S3 buckets, or check their specific policies and access control lists (ACLs).

02 — Create, modify, and delete buckets

Programmatically build new storage containers or remove old ones from your account.

03 — Upload and manage objects

Send files directly to S3 or delete individual object files you no longer need.

04 — List file contents and metadata

View all objects within a specific bucket, getting details like size and when the file was last modified.

05 — Review technical object headers

Get detailed metadata (like content type or headers) for an object without having to download the whole file first.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/mcp/amazon-s3** — connect your AI agent in three steps.

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

02 Your AI client authenticates using those credentials, giving it read/write access to your specified S3 account.

03 You simply tell your agent what you need—for example, 'Audit the public policies on my data lake'—and it executes the necessary AWS API calls.

The bottom line is: it connects your AI client directly to your cloud credentials so that conversation becomes direct action against your Amazon S3 buckets and objects.

Built For

This MCP is for the Cloud Engineer who can't afford downtime, the Security Analyst who needs constant compliance checks, or the DevOps Specialist tired of manual CLI scripts. If you manage critical data stored in S3, you need this.

Security Analyst

Auditing bucket access controls and checking policies to ensure sensitive data remains compliant and private.

Cloud Engineer

Automating the process of auditing multiple buckets, verifying object configurations across large-scale deployments.

DevOps Specialist

Running file cleanups or monitoring S3 policies to prevent data sprawl and ensure proper resource lifecycle management.

What Changes When You Connect

01 Audit bucket security instantly. Use `get_bucket_policy` or `get_bucket_acl` to confirm that public policies aren't accidentally exposed.

02 Automate file management using dedicated tools. You can use `list_objects` to find files and then `delete_object` to clean up old data, all through a simple chat command.

03 Verify object state without bulk downloads. Instead of downloading gigabytes, use `get_object_metadata` to check headers, size, or content type for specific items.

04 Build infrastructure faster. Use `create_bucket` and `list_buckets` together to script out the setup of new data environments with conversational prompts.

05 Control your data flow precisely. Need to upload a file? `put_object` handles the transfer, while `get_object_data` lets you retrieve it later.

Real-World Applications

Checking for exposed assets in a new environment

A security analyst asks their agent to 'Audit all buckets and show me any public read policies.' The agent uses `list_buckets` followed by `get_bucket_policy`, providing an immediate, centralized compliance report.

Cleaning up old log data in a data lake

A DevOps specialist asks the agent to 'Find all objects in the raw logs bucket that haven't been accessed since last quarter and delete them.' The agent uses `list_objects` for filtering, then triggers multiple `delete_object` calls.

Finding a specific file without guessing its name

A data scientist needs to check the size of '2026/Q1/transactions.csv' in a massive bucket. Instead of searching, they ask the agent to get object metadata, which returns the precise file size and headers.

Building out new storage architecture

A cloud engineer needs three separate buckets for development, staging, and production. The agent handles this with a single prompt: 'Create these three buckets,' automatically calling `create_bucket` multiple times.

Patterns to Avoid

Downloading everything to check metadata

✗ AVOID

Manually downloading 50GB of data just to verify the file type or size, which wastes time and bandwidth.

✓ INSTEAD

Instead, ask your agent to use `get_object_metadata`. It pulls technical details for every object without needing to download any actual content.

Assuming permissions are correct

✗ AVOID

Deploying a new bucket and forgetting to check if the necessary security policies (ACLs) were applied correctly.

✓ INSTEAD

Ask your agent to run `get_bucket_acl` or `get_bucket_policy` immediately after creation. This verifies compliance before any data goes in.

Managing files one by one

✗ AVOID

Needing to delete 20 old log files but having to run a separate command for each file.

✓ INSTEAD

Use the agent to list objects and then trigger deletions. The conversation handles the bulk operation, saving you dozens of repetitive steps.

The Right Fit

Use this MCP when your workflow requires deep interaction with Amazon S3 resources—like auditing security policies, listing object metadata, or performing mass file management. It's perfect for cloud engineers and security teams who need to treat storage infrastructure like a conversational API.

Don't use it if you simply need general AWS account information (that belongs in a broader IAM MCP). Also, if your primary task is data transformation or running complex ETL jobs, you should look into dedicated workflow orchestration tools. If you only need basic listing capabilities and never need to check policies or metadata, other simpler read-only connectors might suffice.

Amazon S3 MCP: Auditing Cloud Policies with S3 Buckets

Right now, checking the security of your storage means navigating through AWS consoles, clicking into every single bucket, and manually reviewing complex policy documents. You copy-paste rules between spreadsheets to see if everything is compliant, a process that's slow and prone to human error.

With this MCP, you just ask your agent: 'Check the policies for all my data buckets.' The system uses tools like `get_bucket_acl` and `get_bucket_policy` to pull every policy into one chat window. You get a clear summary of who can access what—no clicking required.

Amazon S3 MCP: Managing Object Lifecycle in Data Lakes

Before this, cleaning up data involved running complex CLI scripts that often failed halfway through, leaving you with partial deletions and incomplete file cleanup. You had to track every single object ID manually.

Now, your agent takes the complexity out of data hygiene. Tell it which objects need deleting or moving; it handles the listing (`list_objects`), verification, and deletion (`delete_object`) in a single conversation. It’s reliable.

Amazon S3 10 Tools for Cloud Bucket & Object Management

Use these tools within your agent to list buckets, upload files, check security policies, or retrieve object metadata on Amazon S3.

#	TOOL	DESCRIPTION
01	`list_buckets`	Lists all the S3 buckets currently in your account.
02	`create_bucket`	Creates a new, empty bucket within your S3 storage space.
03	`delete_bucket`	Permanently removes an existing S3 bucket.
04	`list_objects`	Retrieves a list of all files inside a specific bucket, optionally filtering by name prefix.
05	`get_object_data`	Downloads the actual content of an object file from S3.
06	`put_object`	Uploads a new object file into a specified bucket.
07	`delete_object`	Deletes an individual, specific object file from S3.
08	`get_bucket_policy`	Retrieves the formal security policy attached to a bucket.
09	`get_bucket_acl`	Checks the detailed access control list (ACL) for a specific bucket.
10	`get_object_metadata`	Fetches technical details and headers about an object without downloading its content.

See It in Action

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

U What are the policies on my production and staging buckets?

S3 Policy Audit Report

Here is the policy breakdown for your requested buckets:

BUCKET NAME	POLICY TYPE	STATUS
`prod-assets`	Bucket Policy	Public Read (WARNING)
`staging-logs`	ACLs Only	Internal Use Only

You should review the policy on `prod-assets` immediately.

U List all objects in 'data-lake-raw' and tell me which ones are the biggest.

Files Found (Filtered by Size):

- `2026/q3_report.zip` : 1.8 GB
- `metadata/config.json` : 4 KB
- `images/logo_v3.png` : 540 KB

The largest file is `2026/q3_report.zip`. Would you like me to retrieve its metadata?

U I need to create a new bucket for marketing assets and upload the initial files.

Action Plan Complete

1. Bucket `marketing-assets` successfully created.
2. Initial object `campaign_guide.pdf` uploaded (Size: 12 MB).
3. We've also set the default policy to private read, which is best practice.

Frequently Asked Questions

01 **How do I check if my S3 buckets are secure using the Amazon S3 MCP for AI Agents?**

You ask your agent to audit the bucket policies and ACLs. It retrieves these security settings instantly, showing you exactly what access controls are active on every resource.

02 **Can I use the Amazon S3 MCP for AI Agents to find a specific file's size?**

Yes. You ask it to list objects in a bucket and filter by metadata. It gives you the exact size, modification date, and headers without needing to download anything.

03 **What if I need to delete a bunch of old log files using Amazon S3 MCP for AI Agents?**

You simply tell your agent which objects or prefixes to remove. It manages the deletion process, preventing you from having to run multiple complex commands manually.

04 **Does this MCP handle creating new storage buckets in my AWS account?**

Yes. You can ask it to create brand-new S3 buckets and assign them initial configurations—it handles the whole setup process for you.

05 **Is Amazon S3 MCP for AI Agents good for data compliance checks?**

It's excellent. It lets you audit bucket policies and check access control lists (ACLs), which is essential for proving your cloud storage meets strict regulatory requirements.

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 `"amazon-s3": { "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

Amazon S3 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

DOCUMENT INFORMATION

Generated	June 2026
MCP Server	Amazon S3 MCP
Server ID	`019d754d-1102-730d-b2e0-322601223fc7`
Platform	Vinkius Cloud for AI Agents
Endpoint	`https://edge.vinkius.com/{token}/mcp`

LICENSE & USAGE