MCP SERVER | NO CODE | CLOUD HOSTED

Backup Coverage Audit MCP

Find protection gaps and storage waste in your backup environment.

Backup Coverage Audit MCP connects your AI agent directly to your backup infrastructure. It scans for unprotected assets, identifies failed or outdated backup jobs, detects redundant data consuming storage, and verifies that your retention policies are actually being followed.

A+ Quality Score 100/100

backup | audit | compliance | storage | reliability

MAINTAINED BY VINKIUS CLOUD FOR AI AGENTS · OCTOBER 2026
vinkius.com/en/ai-agent-connect/backup-coverage-audit

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.

Backup Coverage Audit MCP

4 tools available
Cloud-hosted on Vinkius

You shouldn't have to manually hunt through logs to find out why a critical database isn't being backed up. This MCP gives your AI agent the ability to audit your entire backup environment in seconds. Instead of running manual reports, you can ask your agent to find unprotected production folders or identify jobs that haven't run in days. It looks for the gaps that lead to data loss, like assets missing from your backup schedule, and the inefficiencies that drive up costs, like duplicate data sets sitting in different destinations. It also acts as a compliance watchdog by checking if your data is being purged according to your specific retention rules. You get a clear view of your operational risks and storage health without the manual heavy lifting.

Core Capabilities

01 — Gap Analysis

Your agent uses this to find critical assets that lack any backup protection.

02 — Job Health Monitoring

Your agent checks for failed or outdated backup jobs that violate your frequency requirements.

03 — Storage Optimization

Your agent identifies duplicate data sets to help reduce wasted storage space.

04 — Policy Verification

Your agent confirms that data retention and purging rules are being strictly followed.

One Click on Vinkius — From Prompt to Execution

Available at **vinkius.com/en/ai-agent-connect/backup-coverage-audit** — connect your AI agent in three steps.

01 Connect your preferred MCP-compatible client to Vinkius.

02 Grant the MCP access to your backup infrastructure.

03 Ask your AI agent to run specific audit tasks.

04 Review the findings for gaps, staleness, or redundancy.

Connect your AI client to the Vinkius hosted MCP to start auditing your infrastructure.

Built For

This MCP is built for technical teams managing large scale data protection environments.

Backup Administrator

Hands off the manual task of checking job status and retention compliance to the agent.

Infrastructure Engineer

Uses the agent to quickly identify unprotected assets or storage redundancies.

Compliance Officer

Relies on the agent to verify that data purging matches organizational policies.

What Changes When You Connect

01 Identifies unprotected assets before they cause data loss.

02 Reduces storage costs by finding duplicate data sets.

03 Detects failed backup jobs that fall outside of required windows.

04 Automates the verification of data retention and purging policies.

Real-World Applications

Security Gap Auditing

Your agent scans your environment to ensure every critical folder has an active backup job.

Storage Cost Reduction

You use the agent to find redundant data sets that are consuming unnecessary space across destinations.

Compliance Reporting

The agent verifies that your data retention policies are being strictly enforced.

Operational Health Checks

You ask your agent to find stale or failed backup jobs that need immediate attention.

Patterns to Avoid

Manual Log Hunting

AVOID

You spend hours scrolling through thousands of lines of backup logs to find one failed job.

✓ INSTEAD

Ask your agent to find failed or outdated jobs immediately using check_staleness_tool.

Blind Compliance Checks

AVOID

You assume your data is being purged correctly because the policy says it should be.

✓ INSTEAD

Use verify_retention_compliance_tool to confirm that your retention rules are actually being honored.

Ignoring Storage Bloat

AVOID

You keep adding more storage because you don't realize you're backing up the same data twice.

✓ INSTEAD

Run audit_redundancy_tool to find duplicate data sets and stop paying for wasted space.

The Right Fit

Connect this MCP if you manage large scale data protection environments and need to verify coverage without manual reporting. If you only manage a handful of local files, you don't need this. The decision depends on whether your current backup visibility requires manual intervention to find gaps.

4 Tools for Automated Backup Auditing

These tools let your agent scan for coverage gaps, monitor job health, and verify retention compliance.

#	TOOL	DESCRIPTION
01	audit_redundancy_tool	This tool finds wasted storage by identifying duplicate data sets across different destinations.
02	check_staleness_tool	This tool detects backup jobs that have failed to run or haven't completed within their required frequency.
03	verify_retention_compliance_tool	This tool checks that your backup retention rules are being honored and that old data is being purged correctly.
04	analyze_coverage_tool	This tool identifies which critical data assets are missing backup protection.

See It in Action

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

U Which folders are currently unprotected in the production environment?

The following folders in the production environment are unprotected: /data/finance/2023 and /logs/system_critical.

U Are there any stale backups older than 7 days?

Yes, the 'Daily_Database_Backup' is stale; its last successful completion was 10 days ago.

U Check if the retention policy 'POL-99' is being followed correctly.

Policy 'POL-99' is compliant. 150 items were correctly retained and 0 items were erroneously kept or deleted.

Frequently Asked Questions

01 **What can this MCP do for my backup environment?**

It audits your backup setup to find unprotected assets, failed jobs, redundant data, and retention policy violations.

02 **How does it help with storage costs?**

The audit_redundancy_tool finds duplicate data sets across different destinations so you can reclaim wasted space.

03 **Can I use this with Claude or Cursor?**

Yes, you can connect this MCP to any MCP-compatible client including Claude, Cursor, and Windsurf.

04 **How does it verify compliance?**

The verify_retention_compliance_tool checks if your data is being purged according to your defined retention rules.

05 **Does it find failed backup jobs?**

Yes, the check_staleness_tool identifies jobs that have failed or haven't run within their required frequency.

06 **How can I find unprotected data assets?**

You can use the `analyze_coverage_tool` to identify which critical folders or devices are missing active backup protection.

07 **How do I detect if my backups are outdated?**

Use the `check_staleness_tool` by providing a maximum age threshold in days to find backup sets that have not completed successfully within the required window.

08 **Can this tool help reduce storage costs?**

Yes, the `audit_redundancy_tool` identifies duplicate data sets across different destinations, allowing you to consolidate storage and reduce waste.

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 `"backup-coverage-audit": { "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

Backup Coverage Audit 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 Backup Coverage Audit. 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	October 2026
MCP Server	Backup Coverage Audit MCP
Server ID	`01a0ed97-e05f-712e-a005-c5e5441f29d1`
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/en/ai-agent-connect/backup-coverage-audit.