

MCP SERVER

NO CODE

CLOUD HOSTED

Checkmk MCP for AI Agents

Manage complex IT infrastructure monitoring and service alerts

Checkmk lets you manage your IT infrastructure monitoring through natural conversation. You can query service states, list host details, check configuration groups, or even activate pending changes—all directly from your AI client without opening the complex GUI.

F Quality Score 3.6/100

server-monitoring

infrastructure-management

network-monitoring

it-operations

real-time-metrics



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.

Checkmk MCP

8 tools available

Cloud-hosted on Vinkius

Managing a large server landscape usually means clicking through dashboards and running specific reports in a dedicated console. With this MCP, you talk to your agent instead. You get full control over your entire IT monitoring setup by asking questions like, 'What's wrong with the web servers?' or 'Show me all services on the database cluster.'

Your AI client handles the complex calls, giving you immediate status reports and diagnostic data right in your chat window. Need to audit which hosts belong to a specific group? Just ask. Want to push through configuration changes that are waiting for approval? It's one prompt away.

It takes the headache out of maintaining service visibility. Because this MCP is hosted on Vinkius, you connect once and gain access not just to Checkmk controls, but to thousands of other infrastructure tools your team needs.

Core Capabilities

01 — Check all monitored hosts

Retrieve a comprehensive list of every host currently being tracked by the system.

03 — Pull detailed machine configurations

Fetch in-depth, technical information about a single monitored server or appliance.

05 — Activate pending changes

Manually trigger the application of configuration updates across the monitored infrastructure.

02 — Diagnose service health on specific machines

Get real-time status and detailed metrics for services running on any given host.

04 — Review the entire monitoring structure

List and map out all configured folders, host groups, and service groups to understand your setup's architecture.

One Click on Vinkius — From Prompt to Execution

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

- 01** First, subscribe to this MCP and provide your Checkmk credentials, including the Username, Automation Secret, and Server URL.
- 02** Next, connect your preferred AI agent client. Your agent now has direct access to all of Checkmk's monitoring APIs through Vinkius.
- 03** Finally, simply ask a natural language question—like 'List all hosts that are critical'—and the agent performs the necessary checks and delivers an actionable report.

The bottom line is you stop navigating complex GUIs and start talking to your infrastructure monitoring system instead.

Built For

This MCP is built for operations teams, sysadmins, and network engineers who get tired of clicking through multiple dashboards just to check a single status. If you spend time copy-pasting host names or manually auditing service groups, this tool saves your day.

DevOps Engineer

Uses it to audit deployment environments quickly, listing hosts and verifying that services are running correctly after a push.

System Administrator

Manages routine maintenance by checking service states across groups or activating pending configuration changes without logging into the core monitoring GUI.

IT Operations Analyst

Quickly diagnoses issues for support tickets, retrieving specific plugin output and system metadata straight from their chat interface.

What Changes When You Connect

-
- 01 Don't open the GUI to check status. You ask your agent, and it runs commands like `list_checkmk_hosts` instantly, providing a list of all monitored servers.

 - 02 When troubleshooting, you don't waste time digging for data. Use the agent to run diagnostics by listing services on a host using `list_host_services`, getting immediate issue details.

 - 03 Need an audit trail? The MCP lets you map out your entire setup structure by calling functions like `list_checkmk_folders` and `list_service_groups` without navigating menus.

 - 04 Configuration changes are simple. Instead of a multi-step process, just ask the agent to activate pending changes using `activate_checkmk_changes` and watch it run.

 - 05 Get full context on any machine by running `get_host_details`. This pulls all core system metadata you need in one chat response.
-

Real-World Applications

Auditing service status across the environment

The ops analyst needs to verify if a critical application is running on every server. Instead of checking dozens of individual dashboards, they ask their agent to run ``list_all_monitored_services``, getting one consolidated report showing service health everywhere.

Investigating an intermittent server failure

A support team member hears about a slow machine. They use the MCP to first run ``list_checkmk_hosts`` to confirm the host is tracked, then use ``get_host_details`` to check core system metrics and plugin outputs for immediate clues.

Preparing for maintenance window changes

A DevOps engineer needs to push a new monitoring configuration. They use the MCP to list all relevant host groups (``list_host_groups``) and then trigger ``activate_checkmk_changes`` right from their agent, confirming deployment readiness.

Mapping out an unfamiliar monitoring setup

A new team member needs to understand the organizational structure. They ask their agent to call ``list_checkmk_folders``, followed by checking service groupings (``list_service_groups``), building a full architectural map via conversation.

Patterns to Avoid

Manually compiling status reports

X AVOID

Opening the web GUI, navigating to 'Hosts', finding 'web-01' and then opening its service tab. Copying three pieces of data into a spreadsheet.

✓ INSTEAD

Ask your agent to run ``list_host_services`` for that host. It gathers all necessary status information in one chat response, eliminating manual copy/pasting.

Forgetting which group a server belongs to

X AVOID

A user knows the server is related to finance but can't recall if it's in 'PCI-scope' or 'Internal'. They spend 15 minutes clicking through menus.

✓ INSTEAD

Use ``list_host_groups`` first. This lists all configured groups, letting you confirm the correct placement quickly before running diagnostics.

Relying on partial data views

X AVOID

Checking a host's status but missing critical system metadata like its OS version or associated service group details.

✓ INSTEAD

Always run ``get_host_details`` for the comprehensive view. This ensures you pull all core site information and organizational configurations in one go.

The Right Fit

Use this MCP if your workflow involves routine monitoring checks, auditing service groups, or activating configuration changes across

a large fleet of servers. It's perfect when you need to quickly pivot between checking hosts (`list_checkmk_hosts`) and reviewing specific services (`list_host_services`). Don't use it if you only need to manage credentials; those are better handled by dedicated vault tools. If your primary goal is solely understanding the deep technical details of a single machine, while `get_host_details` is useful, remember that this MCP doesn't replace specialized database querying tools.

Checkmk: Monitoring IT Infrastructure Service Health with AI Agents

Right now, checking the health of a distributed server environment means logging into complex dashboards. You click through host groups, drill down to individual services, and copy-paste status codes or metrics into an incident ticket. This process is slow, tedious, and prone to human error.

With this MCP, you just ask your agent. Instead of opening multiple tabs or clicking five times to check service states across a group, you prompt the system. The agent handles all the complex API calls—like listing services (`list_host_services`) and pulling metadata—and returns a clean summary right in the chat.

Checkmk: Controlling Server Configurations Using AI Agents

Making changes requires meticulous manual steps. First, you must check which folders are affected (`list_checkmk_folders`), then manually verify the target host groups, and finally, navigate to the change management section to hit the activation button.

This MCP streamlines that entire process into a single command. You tell your agent what needs updating, and it manages the prerequisite checks before executing `activate_checkmk_changes` . You get instant confirmation and zero clicks on the GUI.

Checkmk: 8 Tools for Real-Time Service Metrics & Diagnostics

These tools let you manage everything from listing all monitored hosts to activating pending system changes, giving your agent deep control over your Checkmk instance.

#	TOOL	DESCRIPTION
01	<code>activate_checkmk_changes</code>	Activates configuration changes that are currently pending in the Checkmk monitoring setup.
02	<code>get_host_details</code>	Retrieves detailed, technical information for any specific host you name.
03	<code>list_all_monitored_services</code>	Provides a complete list of all services running across every monitored host.
04	<code>list_checkmk_folders</code>	Lists all major configuration folders used to organize the monitoring structure.
05	<code>list_host_groups</code>	Retrieves a list of configured groups that contain multiple hosts.
06	<code>list_checkmk_hosts</code>	Lists every individual host currently under monitoring.
07	<code>list_service_groups</code>	Provides a list of service groups, helping you understand how services are organized.
08	<code>list_host_services</code>	Retrieves all monitored services associated with one specific host.

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 monitored hosts and tell me which ones are currently down.



Host Status Report

- `web-prod-01` : **UP** (Service: OK)
- `db-primary` : **UP** (Service: WARNING - Disk Space)
- `api-gateway` : **DOWN** ● (Status: Critical failure detected. Needs immediate attention.)
- `auth-replica` : **UP** (Service: OK)

I found 12 total hosts. `api-gateway` is the only one flagged as down.

U Show me all services running on 'web-prod-01' and tell me which ones are not OK.



Service Report for web-prod-01

SERVICE NAME	STATUS	METRIC VALUE
CPU Load	WARNING	4.5%
Filesystem /var	CRITICAL	98% full
Network Latency	OK	12ms

Action Required: The filesystem on `/var` is critical. You should check disk usage immediately.

U I need to see the details for the host 'db-primary' and list all services it runs.



Detailed Host Report: db-primary

- **Host ID:** 3a2b9c
- **Owner Group:** Database Team (ID: 5)
- **Uptime:** 14 days, 3 hours

Associated Services:

- PostgreSQL Replication (OK)
- Backup Agent (WARNING - Last run failed)
- Monitoring Agent (OK)

Frequently Asked Questions

01 How can Checkmk MCP help me monitor my servers without using the web interface?

You can manage everything conversationally. Instead of clicking around dashboards, you ask your agent to list hosts (`list_checkmk_hosts`) or check service groups (`list_service_groups`). It gives you real-time metrics and reports directly in the chat.

02 Can I use Checkmk MCP to activate changes on my infrastructure?

Yes, this is one of its key features. You simply ask your agent to trigger pending configuration updates using `activate_checkmk_changes`. It handles the activation run and reports success or failure immediately.

03 What if I need detailed info on just one server?

You don't have to guess. You can ask for specific host details using `get_host_details` for a single machine, pulling all core system metadata and configuration data in a structured report.

04 Is Checkmk MCP useful for auditing my monitoring setup?

Absolutely. The MCP lets you list the entire structure—like finding out every folder (`list_checkmk_folders`) or service group (`list_service_groups`)—giving you a full audit trail of your infrastructure organization.

05 Does Checkmk MCP help me troubleshoot live issues?







Yes. When an issue pops up, you can ask the agent to run diagnostics by listing services on that specific host (`list_host_services``), which retrieves plugin output and current states for immediate troubleshooting.

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>"checkmk": { "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

Checkmk 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 Checkmk. 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	Checkmk MCP
Server ID	019d756e-5096-723f-a765-112b35db0f24
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/checkmk.