

OPEN SOURCE

APACHE 2.0

MCP Gateway & AI Registry

Unified Control Plane for AI Agents, MCP Servers, and Agent Skills

MCP SERVERS

A2A AGENTS

AGENT SKILLS

ENTERPRISE READY

GitHub Repository

AWS Workshop

Last updated: May 19, 2026

The AI Asset Sprawl Problem

PROBLEM

Teams are building MCP servers, agents, and skills faster than anyone can track. Developers and agents need a curated list they can discover, trust, and use.

Even the registries themselves are sprawling -- AWS Agent Registry, Anthropic, Workday ASOR, per-LOB registries.

Every agent and developer has their own credentials to every server.

No way to tell if a newly added MCP server or skill is safe.

Agents can't discover tools at runtime, everything is hardcoded.

Rotating a credential or upgrading a server means touching every client.

SOLVED BY

Central registry with unified semantic search, trust badges, visibility controls, and star ratings across servers, agents, and skills.

Federation imports and syncs from external registries, and **P2P federation** links registry instances. One search surface across all of them.

Single gateway with **OAuth2 M2M** and **5 IdPs** (Keycloak, Entra, Okta, Auth0, Cognito).

Automatic security scanning (Cisco AI Defense) + **registration admission gate** + **audit logging**.

Intelligent tool finder + **semantic discovery API** for servers, agents, and skills.

Version routing (instant rollback) + **virtual MCP servers** + **centralized credential management**.

One control plane. Registry discovers and governs. Gateway connects and enforces.

Four Core Functions

Unified MCP Gateway

Centralized access point for multiple MCP servers with reverse proxy routing, SSL termination, and health monitoring.

MCP Server Registry

Register, discover, and manage MCP servers with unified governance, semantic search, and version routing.

Agent Registry & A2A Hub

Agent registration, discovery, and direct agent-to-agent communication via the A2A Protocol. Supports both A2A and non-A2A agents.

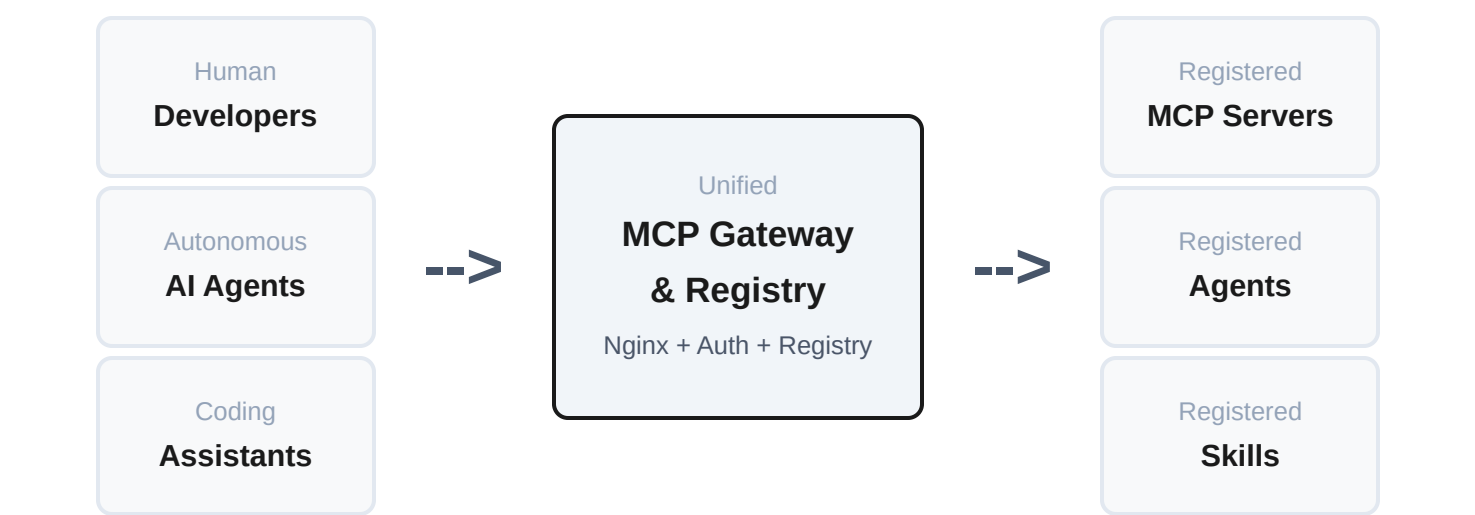
Skills Registry

Register, version, and discover reusable AI skills (SKILL.md) with security scanning, enabling skill sharing across agents and teams.

Platform Demo



Platform Architecture



Servers and agents can be hosted **anywhere**:

- AMAZON BEDROCK AGENTCORE
- AMAZON EKS
- OTHER AWS COMPUTE
- THIRD-PARTY SAAS

Skills are sourced from **GitHub or private Git repositories** (PAT or GitHub App auth, GitHub Enterprise supported).

Single connection point with **dual authentication** for human users and machine-to-machine agent flows.

Enterprise Security

Multi-Provider IAM Keycloak, Microsoft Entra ID, Okta, Auth0, and AWS Cognito with harmonized management API.	Fine-Grained Access Scopes define which servers, methods, tools, and agents each user or service account can access.	Security Scanning Cisco AI Defense integration for MCP servers and A2A agents with YARA pattern matching.
Audit Logging Comprehensive audit trails with credential masking, TTL retention, and SOC 2/GDPR compliance.	M2M Auth OAuth2 Client Credentials flow for AI agent identity with service accounts.	Static Token Auth API key access for CI/CD pipelines and trusted network environments without IdP setup.

Intelligent Discovery

Hybrid Search

- ◆ Vector similarity + keyword matching
- ◆ Unified search across servers, tools, agents, skills
- ◆ Name-boost for exact match relevance
- ◆ Tag-based and metadata filtering

Flexible Embeddings

- Local sentence-transformers
- OpenAI embeddings
- Amazon Bedrock Titan
- 100+ LiteLLM-supported providers

Agents discover tools at runtime via natural language -- **"find an agent that can book flights"**

Agent Registry & A2A Protocol

Agent-to-Agent Communication Direct peer-to-peer agent communication. Registry handles discovery, agents connect directly for low-latency interaction.	Semantic Agent Discovery Agents find collaborators via natural language queries. Dynamic composition based on capabilities, not hardcoded references.	Agent Skills Registry Register reusable SKILL.md instruction sets with security scanning, visibility controls, and star ratings.
--	---	--

Agents autonomously discover specialized agents for tasks they cannot handle, enabling **dynamic agent orchestration**.

Supply Chain Security: Cisco AI Defense

EXTERNAL INTEGRATION

Three open-source scanners automatically scan every MCP server, A2A agent, and Agent Skill before it reaches production.

MCP Scanner

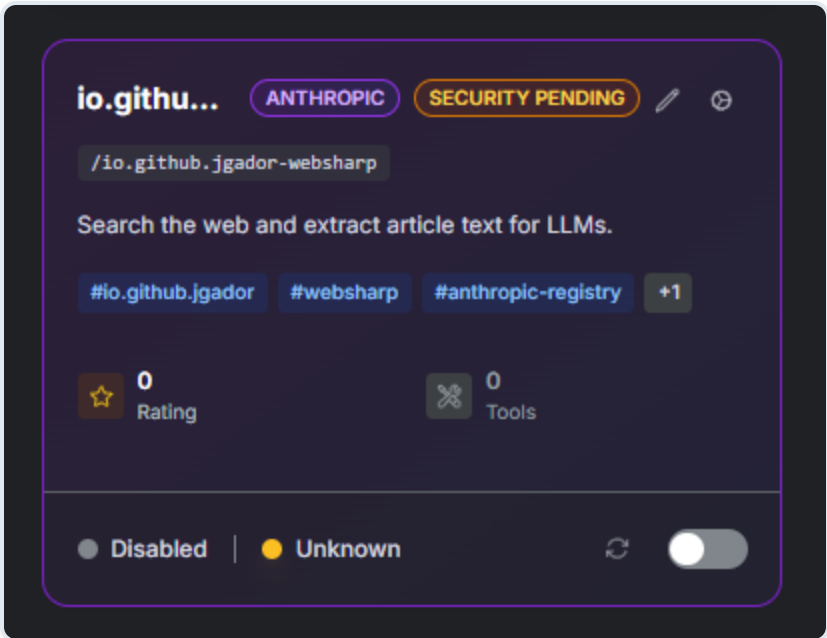
YARA pattern matching and optional LLM analysis for MCP server tool definitions. Detects injection, XSS, and hardcoded secrets.

A2A Scanner

Heuristic and spec validation for Agent-to-Agent protocol agents. Catches protocol violations and malicious behaviors.

Skill Scanner

Static and behavioral analysis of SKILL.md files. Detects prompt injection, privilege escalation, and social engineering.



Unsafe items are auto-disabled with a "security-pending" tag for admin review

Scan on registration, on-demand rescan, and periodic registry-wide audits -- powered by [cisco-ai-defense](#) open-source scanners

Agent Trust: Agent Name Service

EXTERNAL INTEGRATION

DNS + PKI for AI Agents -- just as SSL certificates let you trust websites, ANS lets you trust agents.

Structured Identity


Each agent gets an ANS Name and X.509 certificate issued by a Registration Authority.

Bring Your Own ANS ID

Owners link their ANS Agent ID to registry entries. Registry verifies via GoDaddy ANS API.

Production Resilience

Circuit breaker, retry with backoff, 6-hour background re-verification, and rate limiting.

 ANS integration showing trust badge on agent card

Verified agents display a trust badge with certificate details

IETF Internet-Draft (draft-narajala-ans-00) -- Powered by GoDaddy ANS, integrated into the open-source AI Registry

Federated Sources: Import from Anywhere

EXTERNAL INTEGRATION

Anthropic Registry

Import curated MCP servers from Anthropic's official registry at registry.modelcontextprotocol.io.

No Auth Required

Public API -- set `ANTHROPIC_REGISTRY_ENABLED=true` and go.

Selective or Full Import

Import specific servers by name or leave the list empty to sync all available servers.

Workday ASOR

Agent System of Record -- federate Workday-managed AI agents into the registry.

OAuth Integration

Secure token-based access with automatic credential management and 4-hour rotation.

A2A Agent Mapping

ASOR agents map to A2A Agent Cards with skills, capabilities, and provider metadata.

Others Coming Soon

The federation framework is extensible -- new sources plug in with a standard adapter interface.

Unified governance -- federated assets inherit the same scanning, RBAC, and audit policies as locally registered items

Registry Federation

P2P Federation

Bidirectional sync between registry instances with configurable sync modes: all, whitelist, or tag filter.

Anthropic Registry

Import curated MCP servers from Anthropic's official registry with full API compatibility.

External Sources

AWS Agent Registry, Workday ASOR, and Anthropic Registry -- federate assets from multiple external sources.

Registry Card

Standardized discovery via /.well-known/registry-card with capabilities, auth endpoints, and contact info.

Central IT aggregates across LOB registries -- LOBs inherit shared tools from a **central hub**.

AWS Agent Registry Federation

Federate MCP servers, A2A agents, and skills from AWS Agent Registry into the Gateway.

Multi-Registry Support

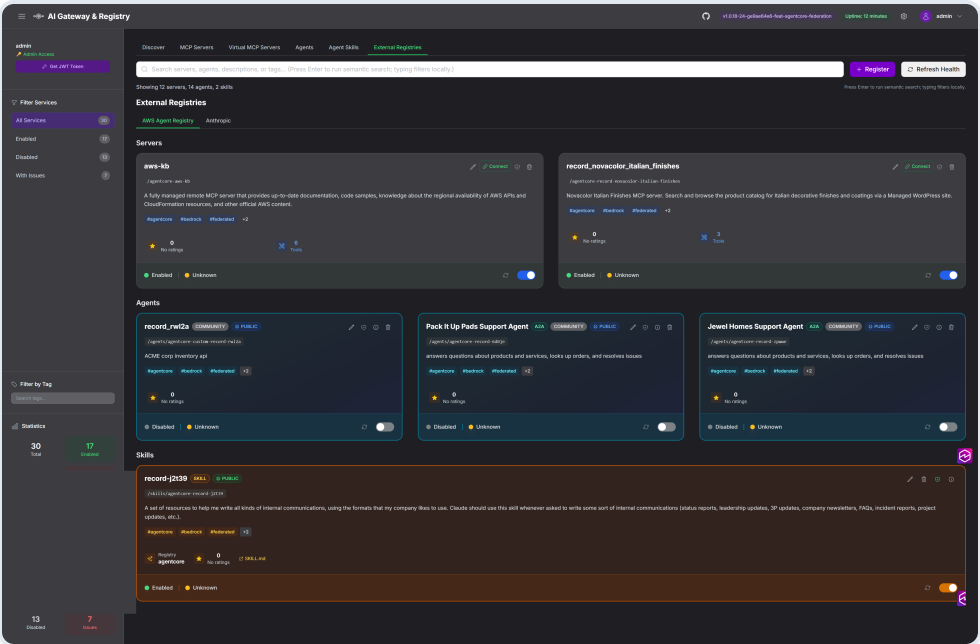
Add multiple registries from same or different AWS accounts and regions. Cross-account via IAM role assumption.

Selective Sync

Choose descriptor types (MCP, A2A, CUSTOM, AGENT_SKILLS) and status filters per registry.

Cascade Cleanup

Remove a registry and all its synced assets are automatically deregistered.



Federated assets from AWS Agent Registry in the External Registries tab

Enable with a single env var: `AWS_REGISTRY_FEDERATION_ENABLED=true` -- manage registries via UI, API, or CLI | [Watch Demo](#)

Virtual Servers & Version Routing

Virtual MCP Servers

- Aggregate tools from multiple backends
- Tool aliasing for naming conflicts
- Per-tool scope-based access control
- Session multiplexing (1:N transparent)
- 60s cached aggregation

Version Routing

- ◆ Multiple versions behind single endpoint
- ◆ Test with X-MCP-Server-Version header
- ◆ Instant rollback with one API call
- ◆ Deprecation lifecycle with sunset dates
- ◆ O(1) nginx map-based routing

Observability & Metrics

Grafana Dashboards

Real-time metrics for server health, tool usage, auth events, and system performance.

OTLP Push Export

Direct export to Datadog, New Relic, Honeycomb, or Grafana Cloud -- no OTEL Collector needed.

OpenTelemetry

Integration with Prometheus, CloudWatch, and other monitoring platforms via OTEL protocol.

Anonymous Telemetry

Privacy-first usage telemetry for adoption tracking. Non-sensitive metadata only. Opt-out with one env var.

Flexible Deployment

Amazon EKS (Kubernetes) Helm chart deployment on Amazon EKS for container orchestration at scale.	Amazon EC2 Traditional deployment on EC2 instances with Docker Compose. Complete setup guide from scratch.
Docker / Podman Pre-built Docker Hub images and rootless Podman support for macOS and Linux. One-command AI-assisted setup.	Amazon ECS Fargate Serverless containers with multi-AZ, ALB with HTTPS, auto-scaling, CloudWatch, and NAT Gateway HA. Full Terraform config.

3

AWS Deployment Targets

5

Identity Providers

700+

Passing Tests (22 releases)

Developer Experience

MCP Registry CLI Conversational interface for registry management with real-time token status and cost tracking.	IAM Settings UI Visual management of users, groups, and M2M service accounts with fine-grained permissions.	AI Coding Assistants Single config for VS Code, Cursor, Claude Code, and Cline with guided tool discovery.
Management API RESTful HTTP endpoints with Python client, type-safe interfaces, and comprehensive error handling.	Config Viewer Admin panel with 11 config groups. Export as ENV, JSON, TFVARS, or YAML for deployment automation.	Custom Metadata Rich metadata on servers and agents for team ownership, compliance tracking, and cost allocation.

What's New

- **Server-Side OAuth Session Store (1.24.1)**
Moves OAuth session payload out of browser cookie into MongoDB/DocumentDB with AES-GCM encrypted id_token. Eliminates cookie-size bug class for Entra users with large group memberships.
- **Local stdio MCP Server Registration (1.24.0)**
Register local stdio MCP servers and per-server custom HTTP headers, plus operator-configurable branding for the registry UI.
- **Cloud Detection, IAM Hardening, Splunk-Ready Logging (1.23.0)**
Auto-detect AWS/Azure/GCP deployments, harden IAM policies, and emit structured logs ready for Splunk and other SIEMs.
- **Group-Restricted Agent Visibility (1.0.22)**
Publishers can restrict visibility to specific IdP groups via visibility: group-restricted and allowedGroups, layered on top of IAM scopes. Works across all 5 IdPs.
- **Admin Data Export and Centralized Logging (1.0.21)**
Download 11 registry collections as JSON/ZIP. Production logging with MongoDB storage, log viewer UI, and admin REST API. ARM64 image support.
- **Registration Webhooks and Admission Gate (1.0.20)**
External gate for approve/deny on registration. Fire-and-forget webhooks to CMDBs, Slack, or CI/CD pipelines. Multi-key static tokens.
- **AWS Agent Registry Federation (1.0.19)**
Federate MCP servers, A2A agents, and skills from AWS Agent Registry. Multi-registry, cross-account, cascade cleanup. GitHub private repo auth for skills.
- **ANS Trust Verification + Auth0 IdP (1.0.18)**
PKI-based trust verification for agents via GoDaddy ANS. Green shield badge on verified agents. Auth0 added as the fifth IdP.

What's Next

- **1.24.2 (May 20): Patch Follow-Up to 1.24.1** Final cleanup items from the 1.24.1 auth-hardening release.
- **1.25.0 (May 23): Registry Hardening & Observability** MCP registration deduplication (#913), agent-card PATCH + async batch endpoint (#956), Prometheus /metrics endpoint (#867), dependency management for cards (#844), and the mcpgw -> airegistry-tools rename (#1020).
- **1.26.0 (May 29): Coding-Assistant OAuth Integration** All 7 phases of the coding-assistant OAuth umbrella (#988): PRM + AS metadata + WWW-Authenticate, Entra v1 scope verbatim pass-through, RFC 8707 resource enforcement, CIMD publisher and consumer, ID-JAG receiver, and the no-DCR decision doc.
- **1.27.0 (Jun 12): A2A Gateway & Registry Copilot** A2A reverse proxy gateway (#847) mirroring what the MCP gateway does for MCP servers, plus the embedded Registry Copilot chat assistant (#744).
- **Parking Lot** mcp-registry-discover skill + token-vending tool (#936), agent knowledge sharing, and 22 other ideas under community discussion.

Have a feature idea?

We build in the open. Tell us what you need.

Create an issue on GitHub →

Community Adoption

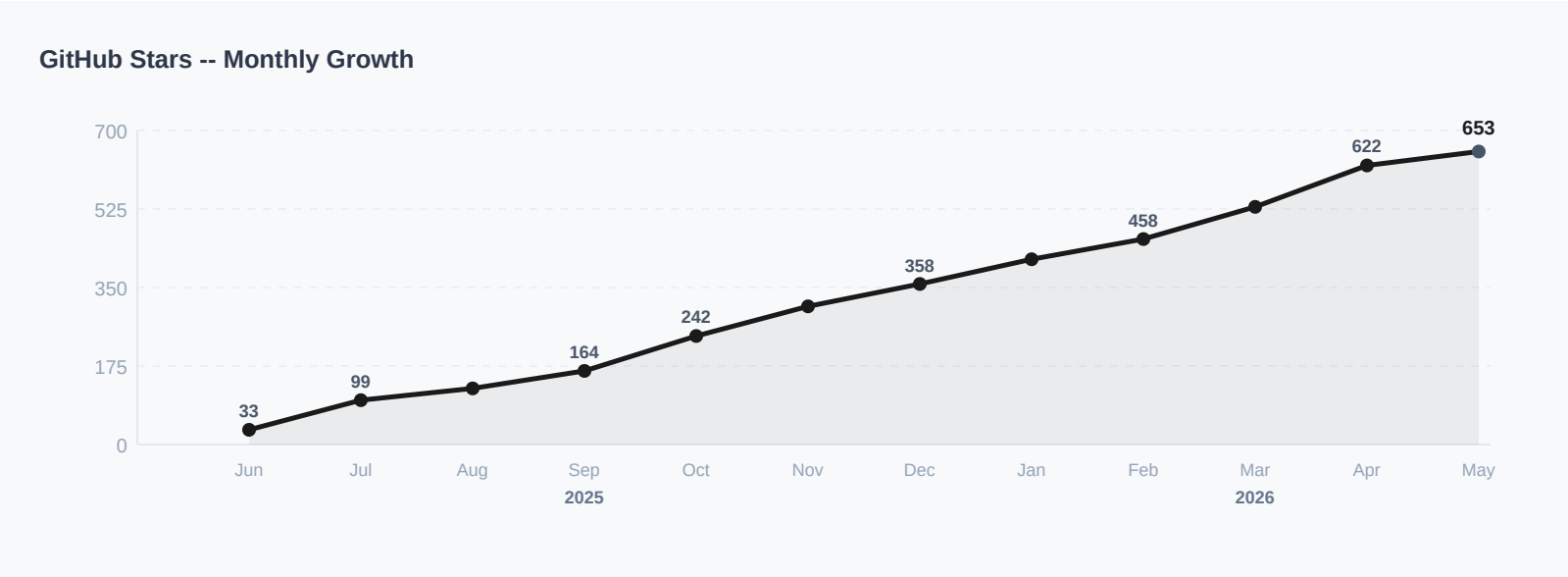
A community-driven project with growing momentum since June 2025

653
GitHub Stars

39
Contributors

171
Forks

~500
Persistent
Deployments



540
Merged PRs

347
Issues Closed

22
Releases

DAI/WAI 32%
Daily-active / 7d-alive

Kubernetes > Docker
among active customers

Listed on GoodAIIist — curated directory of top AI repositories

Customer Stories



We are collecting stories from teams
deploying AI Registry in production.

If your organization is using MCP Gateway Registry and would
like to share your experience, we would love to hear from you.

COMING SOON

[Share your story on GitHub Discussions →](#)

Featured Coverage

AWS MACHINE LEARNING BLOG

MAY 2026

Securing AI agents: How AWS and Cisco AI Defense scale MCP and A2A deployments

A joint AWS and Cisco perspective on how the MCP Gateway & Registry, combined with Cisco AI Defense scanners, secures the supply chain for MCP servers and A2A agents at enterprise scale -- covering registration-time scanning, runtime trust, and federation across AWS Agent Registry, Anthropic, and Workday ASOR.

[Read on aws.amazon.com](#) →

aws.amazon.com/blogs/machine-learning/securing-ai-agents-how-aws-and-cisco-ai-defense-scale-mcp-and-a2a-deployments/

Demo & Links



**Securing AI agents: How AWS and Cisco AI
Defense scale MCP and A2A deployments**

[AWS Machine Learning Blog -- joint AWS + Cisco perspective](#)



AWS Show & Tell

[YouTube -- MCP Gateway & Registry deep dive](#)



Live Demo

[Vidcast -- Hands-on walkthrough of the platform](#)



Roadmap

[GitHub Milestones -- Upcoming features and releases](#)

Scan to Get Started



github.com/agentive-community/mcp-gateway-registry

Open source, Apache 2.0 License

One AI Registry. Unified Control.

3

AWS Targets

ECS Fargate, EKS, EC2

5

Identity Providers

Keycloak, Entra ID, Okta, Auth0, Cognito

Open

Source

Apache 2.0 License

github.com/agentic-community/mcp-gateway-registry

Quick Start

Documentation

AWS Deployment

AWS Workshop

Demo Video

Community