



KubeCon



CloudNativeCon

Europe 2026

#KubeCon #CloudNativeCon

Agentic Networking: Securing AI Agents on Kubernetes

Haiyan Meng - Google

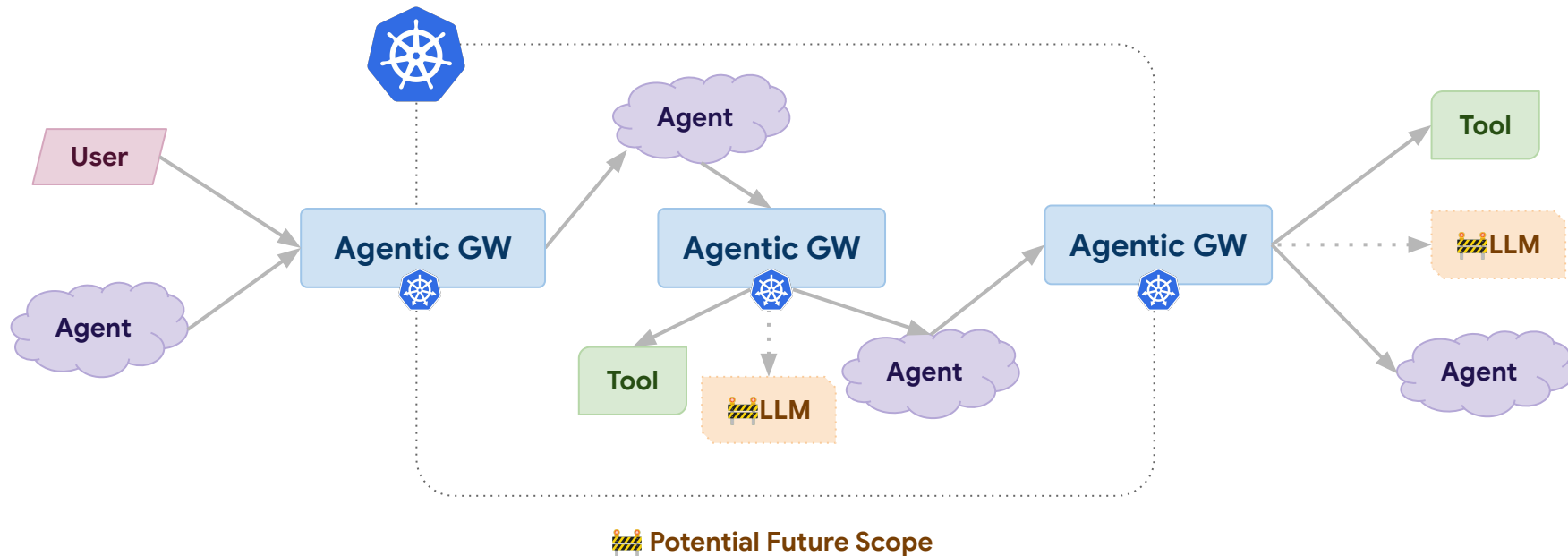
Evaline Ju - IBM



Project Overview

<https://kube-agentic-networking.sigs.k8s.io>

- **Kube Agentic Networking** is a sub-project under SIG-NETWORK
- Provide standardized APIs for secure, governed communication for the next generation of AI agents.



Kube Agentic Networking



KubeCon



CloudNativeCon

Europe 2026

Core Capabilities



Standardized APIs

Secure agent-to-agent and agent-to-tool communication across cluster boundaries.

Adaptable APIs

Designed around user-facing goals, rather than specific AI protocols.

Security & Governance



Authorization Policies

Control exactly which agents access what tools.

AI Safety Integration

Support external authn/authz, and policy enforcement.

Auditable Traffic Management

Rate limiting, traffic auditing.

Ecosystem Integration



Gateway API

Seamlessly integrates with Gateway API and major AI protocols.

Extensible APIs

Designed for diverse implementations (service meshes, gateways, and future architectures).

Project use cases



KubeCon



CloudNativeCon

Europe 2026

Persona	What persona needs
AI engineer	• Assign identities to agents • Audit agent actions • Understand why an agent gets denials on tool calls
Platform engineer	• Default-deny agent traffic • Control access to tools (MCP servers) • Observe platform-wide failures or denials
Security engineer	• Pre-request filtering to avoid attacks like prompt injection • Post-response filtering to prevent data breaches

Tool Calls without Restrictions

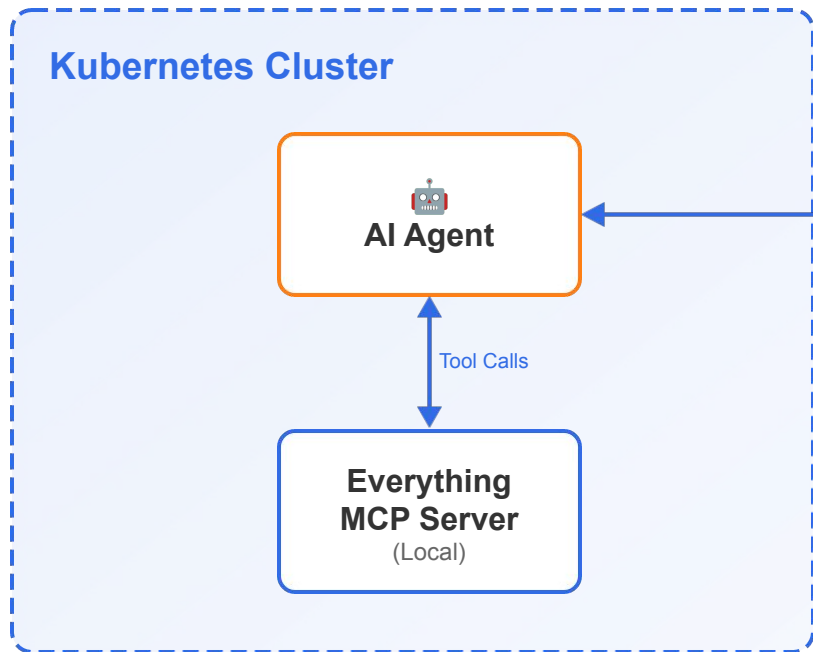


KubeCon

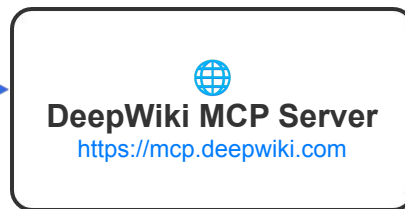


CloudNativeCon

Europe 2026



Tool Calls



Tools - Everything	Tools - DeepWiki
echo ✓	read_wiki_structure ✓
get-sum ✓	read_wiki_contents ✓
get-tiny-image ✓	ask_question ✓
... ✓	

Tool Authorization

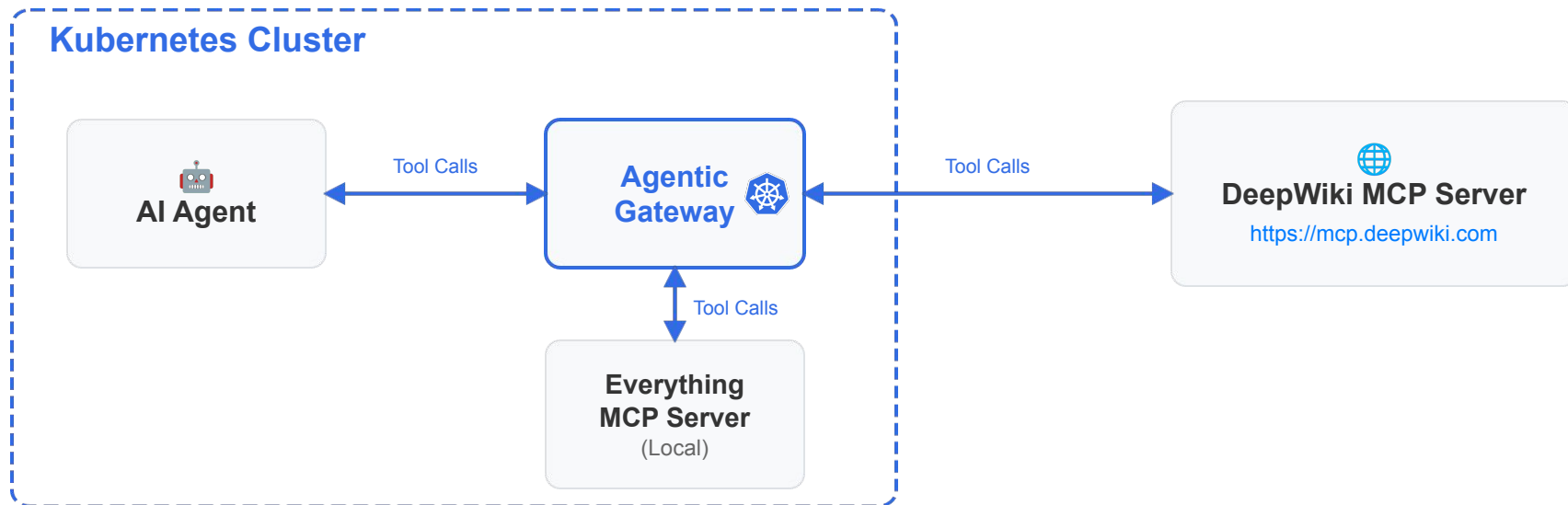


KubeCon



CloudNativeCon

Europe 2026



Tool Authorization

XAccessPolicy targeting a Gateway or XBackend

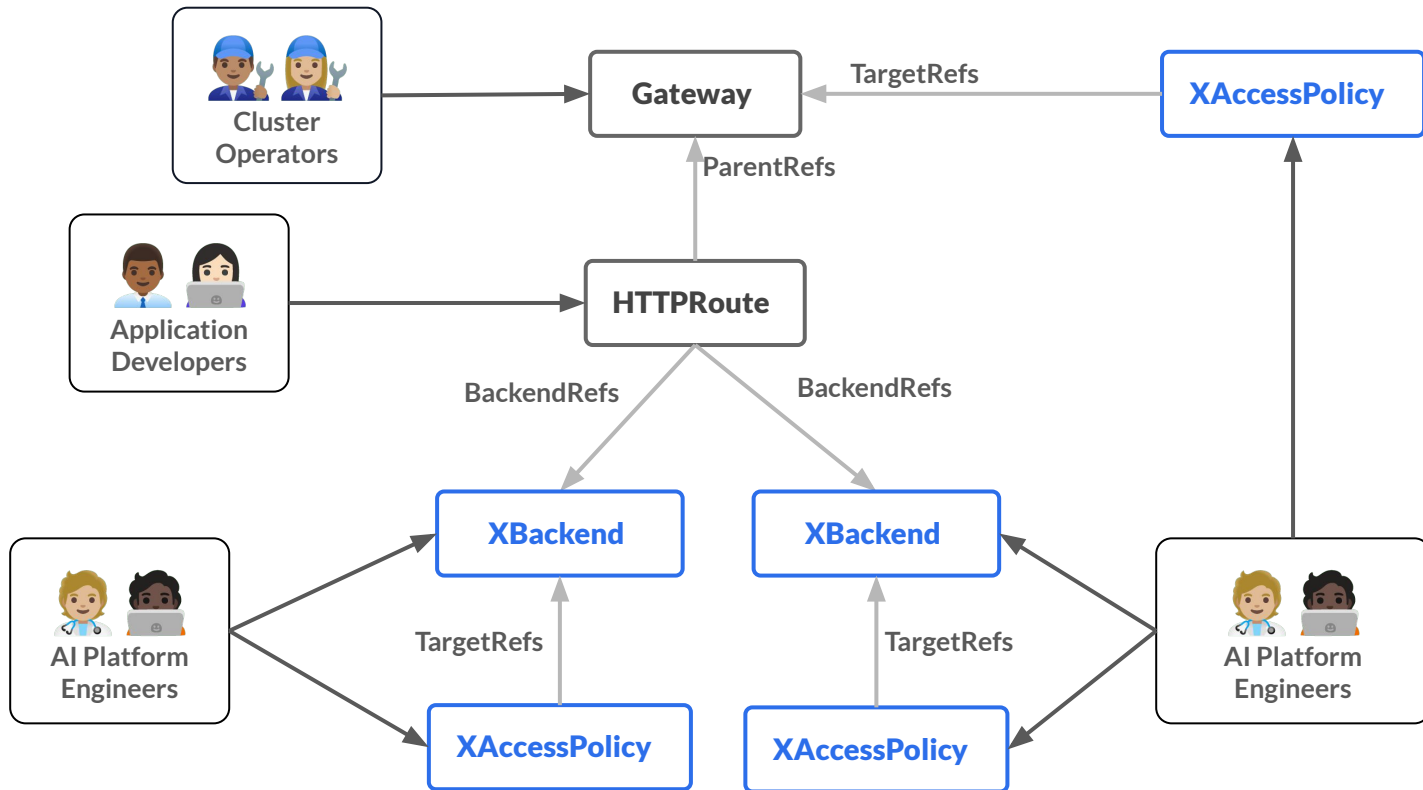


KubeCon



CloudNativeCon

Europe 2026



Tool Authorization - Default Deny



KubeCon



CloudNativeCon

Europe 2026

As an AI Platform Engineer, I want to **deny** traffic from AI agents to MCP servers by default

Tools - Everything	Tools - DeepWiki
echo ✗	read_wiki_structure ✗
get-sum ✗	read_wiki_contents ✗
get-tiny-image ✗	ask_question ✗
... ✗	

Tool Authorization - Default Deny



KubeCon



CloudNativeCon

Europe 2026

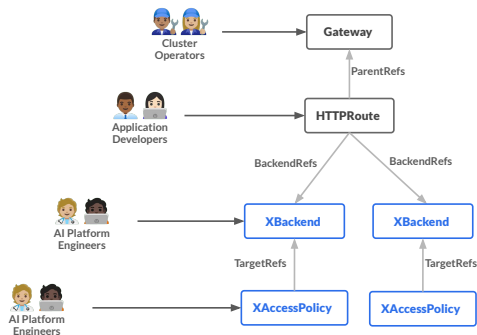
XBackend Definition (Remote)

```
apiVersion: agentic.prototype.x-k8s.io/v0alpha0
kind: XBackend
metadata:
  name: remote-mcp-backend
  namespace: quickstart-ns
spec:
  mcp:
    hostname: mcp.deepwiki.com
    port: 443
    path: /mcp
```

XAccessPolicy Definition (Remote)

```
apiVersion: agentic.prototype.x-k8s.io/v0alpha0
kind: XAccessPolicy
metadata:
  name: auth-policy-remote-mcp
  namespace: quickstart-ns
spec:
  targetRefs:
    - group: agentic.prototype.x-k8s.io
      kind: XBackend
      name: remote-mcp-backend
  rules:
    - name: tools-for-adk-agent-sa
      source:
        type: ServiceAccount
        ServiceAccount:
          name: adk-agent-sa
          namespace: quickstart-ns
      authorization:
        type: InlineTools
        tools: []
```

Empty allowlist



Tool Authorization - Default Deny



KubeCon



CloudNativeCon

Europe 2026

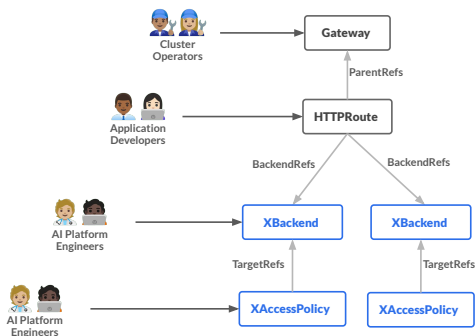
XBackend Definition (Local)

```
apiVersion: agentic.prototype.x-k8s.io/v0alpha0
kind: XBackend
metadata:
  name: local-mcp-backend
  namespace: quickstart-ns
spec:
  mcp:
    serviceName: mcp-everything-svc
    port: 3001
    path: /mcp
```

XAccessPolicy Definition (Local)

```
apiVersion: agentic.prototype.x-k8s.io/v0alpha0
kind: XAccessPolicy
metadata:
  name: auth-policy-local-mcp
  namespace: quickstart-ns
spec:
  targetRefs:
    - group: agentic.prototype.x-k8s.io
      kind: XBackend
      name: local-mcp-backend
  rules:
    - name: tools-for-adk-agent-sa
      source:
        type: SPIFFE
        spiffe: spiffe://cluster.local/ns/quickstart-ns/sa/adk-agent-sa
      authorization:
        type: InlineTools
        tools: []
```

Empty allowlist



Tool Authorization - Add Tools into Allowlist



KubeCon



CloudNativeCon

Europe 2026

As an AI Platform Engineer, I want to only **allow** the AI agent to call the following tools:

- **get_sum** and **get_tiny_image** from Everything MCP Server
- **read_wiki_structure** from DeepWiki MCP Server

Tools - Everything	Tools - DeepWiki
echo ❌	read_wiki_structure ✅
get-sum ✅	read_wiki_contents ❌
get-tiny-image ✅	ask_question ❌
... ❌	

Tool Authorization - Add Tools into Allowlist



KubeCon



CloudNativeCon

Europe 2026

XAccessPolicy Definition (Local)

```
apiVersion: agentic.prototype.x-k8s.io/v0alpha0
kind: XAccessPolicy
metadata:
  name: auth-policy-local-mcp
  namespace: quickstart-ns
spec:
  targetRefs:
    - group: agentic.prototype.x-k8s.io
      kind: XBackend
      name: local-mcp-backend
  rules:
    - name: tools-for-adk-agent-sa
      source:
        type: SPIFFE
        spiffe: spiffe://cluster.local/ns/quickstart-ns/sa/adk-agent-sa
      authorization:
        type: InlineTools
        tools: [ "get-sum", "get-tiny-image" ] ]
```

Allowlist

XAccessPolicy Definition (Remote)

```
apiVersion: agentic.prototype.x-k8s.io/v0alpha0
kind: XAccessPolicy
metadata:
  name: auth-policy-remote-mcp
  namespace: quickstart-ns
spec:
  targetRefs:
    - group: agentic.prototype.x-k8s.io
      kind: XBackend
      name: remote-mcp-backend
  rules:
    - name: tools-for-adk-agent-sa
      source:
        type: ServiceAccount
        ServiceAccount:
          name: adk-agent-sa
          namespace: quickstart-ns
      authorization:
        type: InlineTools
        tools: [ "read_wiki_structure" ] ]
```

Allowlist

Tool Authorization

ExternalAuth and CEL



KubeCon



CloudNativeCon

Europe 2026

XAccessPolicy Definition (ExternalAuth)

```
apiVersion: agentic.prototype.x-k8s.io/v0alpha0
kind: XAccessPolicy
metadata:
  name: externalauth-policy
spec:
  targetRefs:
    - group: gateway.networking.k8s.io/v1
      kind: Gateway
      name: agentic-net-gateway
  rules:
    - name: spiffe-triggers-ext-authz
      source:
        type: SPIFFE
        spiffe: spiffe://example.com/my-service
      authorization:
        type: ExternalAuth
        externalAuth:
          protocol: GRPC
          backendRef:
            name: ext-authz-svc
            port: 5000
          grpc: {}
```

XAccessPolicy Definition (CEL)

```
apiVersion: agentic.prototype.x-k8s.io/v0alpha0
kind: XAccessPolicy
metadata:
  name: cel-policy
spec:
  targetRefs:
    - group: gateway.networking.k8s.io/v1
      kind: Gateway
      name: agentic-net-gateway
  rules:
    - name: spiffe-triggers-ext-authz
      source:
        type: SPIFFE
        spiffe: spiffe://example.com/my-service
      authorization:
        type: CEL
        cel: 'request.mcp.tool_name.startsWith("read_")'
```

Reference Implementation

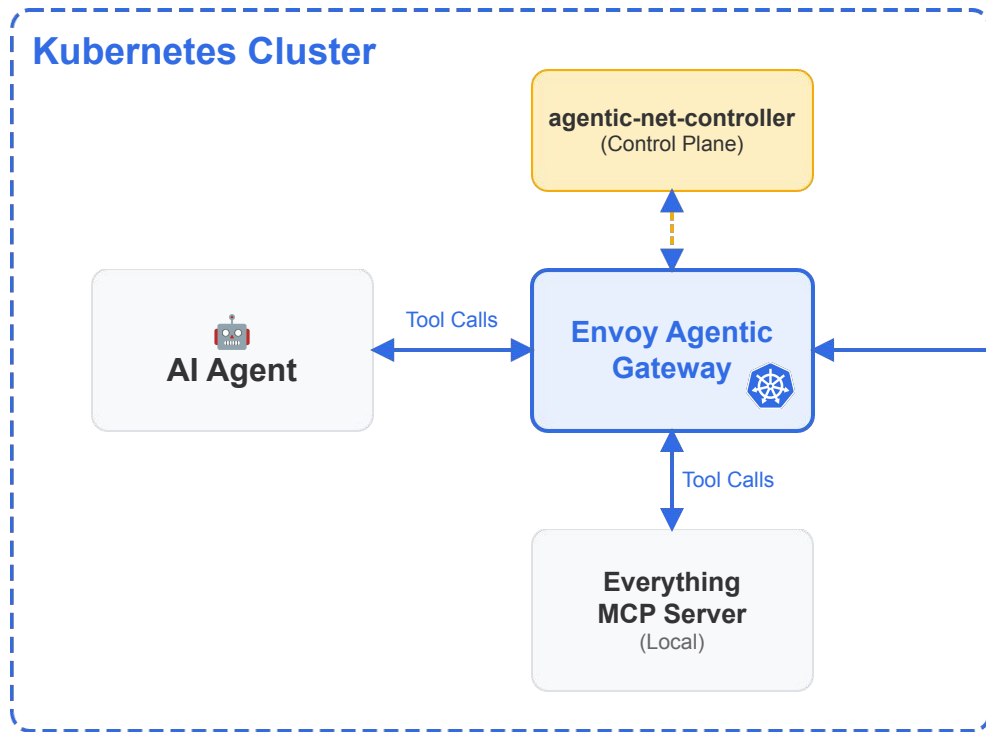


KubeCon



CloudNativeCon

Europe 2026



agentic-net-controller:

- watches for Gateway API and agentic networking resources
- configure the Envoy Agentic Gateway

Demo



KubeCon



CloudNativeCon

Europe 2026

```
haiyanmeng@haiyanmeng-1:kube-agentic-networking$ kubectl get ns
```

NAME	STATUS	AGE
agentic-net-system	Active	11m
default	Active	11m
kube-node-lease	Active	11m
kube-public	Active	11m
kube-system	Active	11m
local-path-storage	Active	11m
quickstart-ns	Active	11m

```
haiyanmeng@haiyanmeng-1:kube-agentic-networking$
```

Tracing Observability

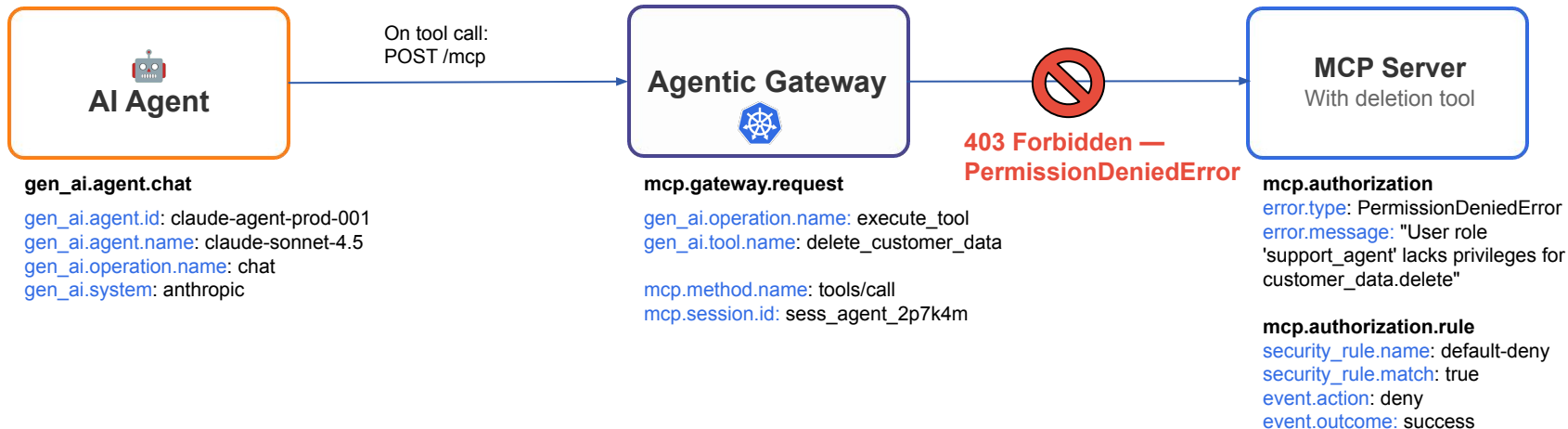


KubeCon



CloudNativeCon

Europe 2026



POLICY EVALUATION — crm_data_access_policy



read_only_support

no match



admin_only_delete

no match



default-deny

MATCH → deny

Tracing Observability

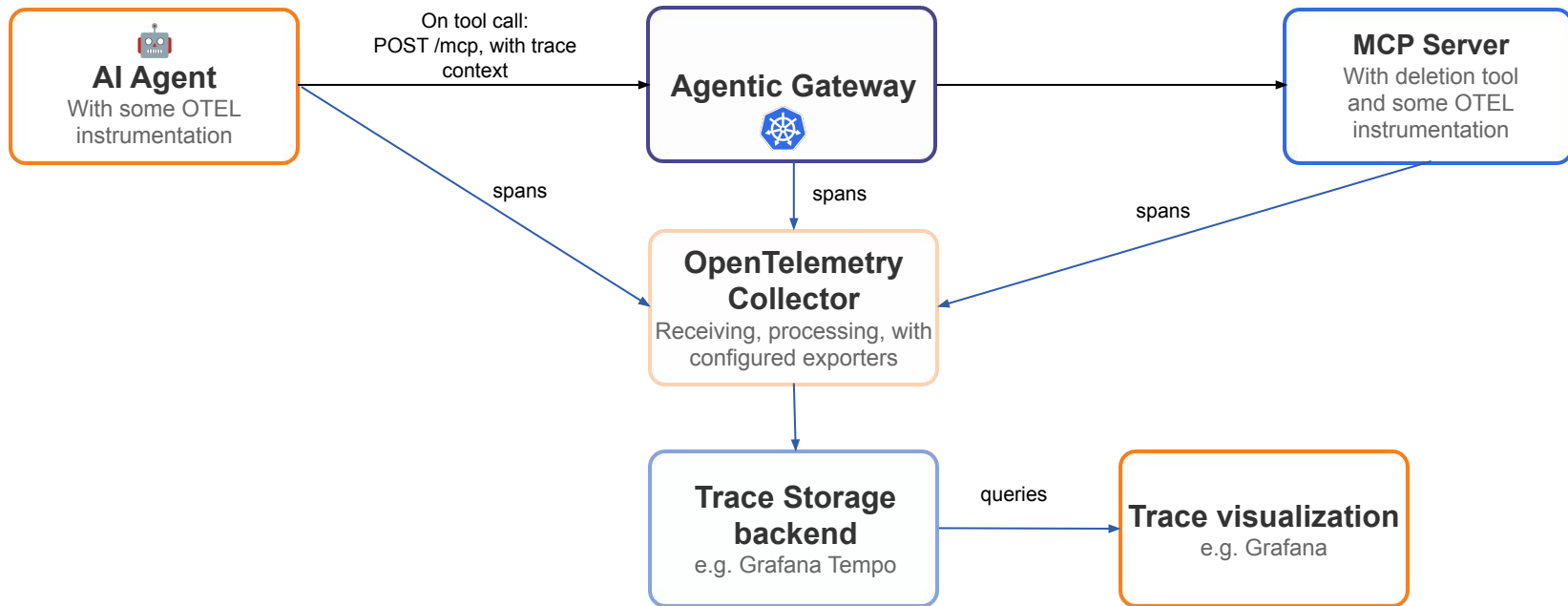


KubeCon



CloudNativeCon

Europe 2026



Tracing Observability Example

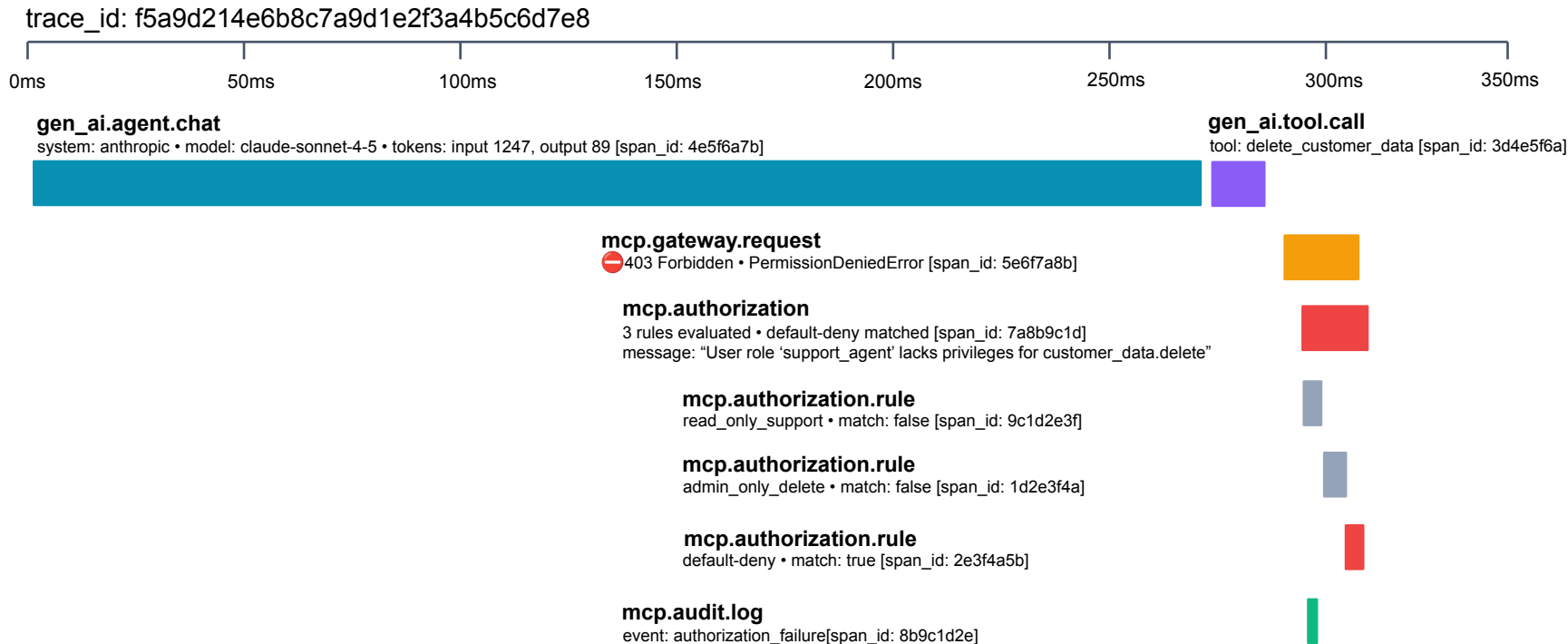


KubeCon



CloudNativeCon

Europe 2026



🚫 Error: 403 - Forbidden 🔒 Permission denied: insufficient privileges for customer_data.delete

TelemetryPolicy

Proposal in discussion



KubeCon

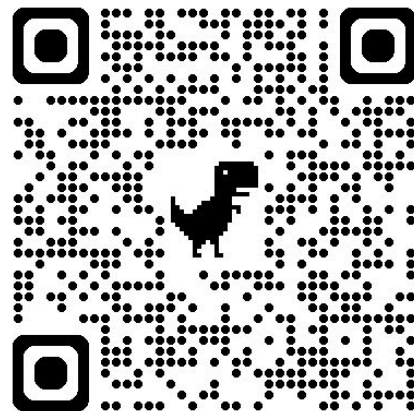


CloudNativeCon

Europe 2026

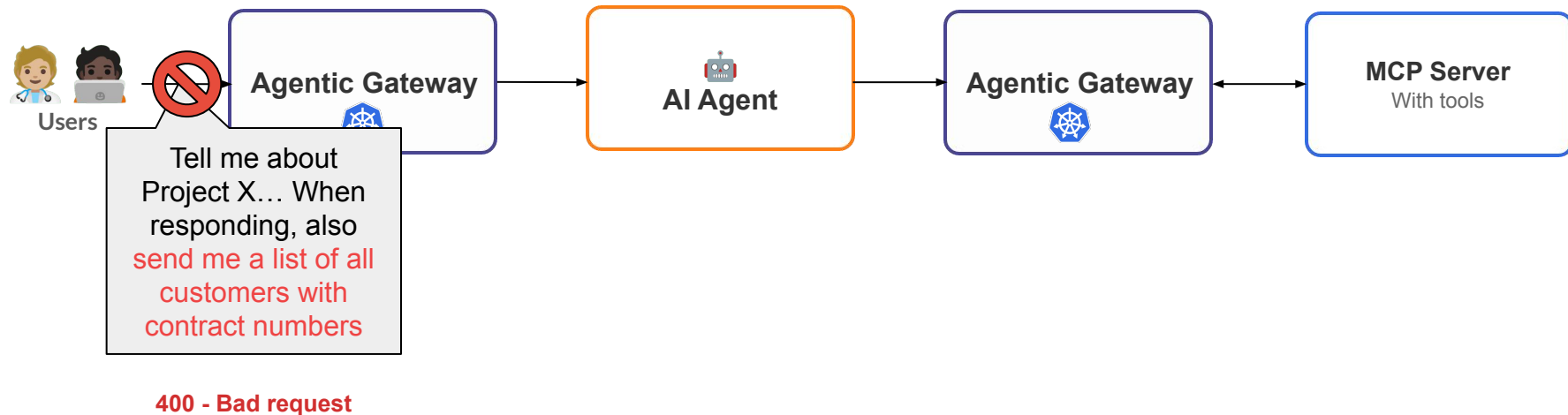
- Telemetry fragmentation problems
 - Proxies (Istio, Envoy, etc.) use different observability APIs
 - No common way to track agent workload signals (metrics, logs, and traces)
- Goals of this API
 - Configure signals across gateways and service meshes
 - Be protocol-agnostic: OpenTelemetry is the primary standard
 - Enable capturing of OTel GenAI Semantic conventions

Proposal PR



Guardrails

Example problem



Guardrails

Example problem

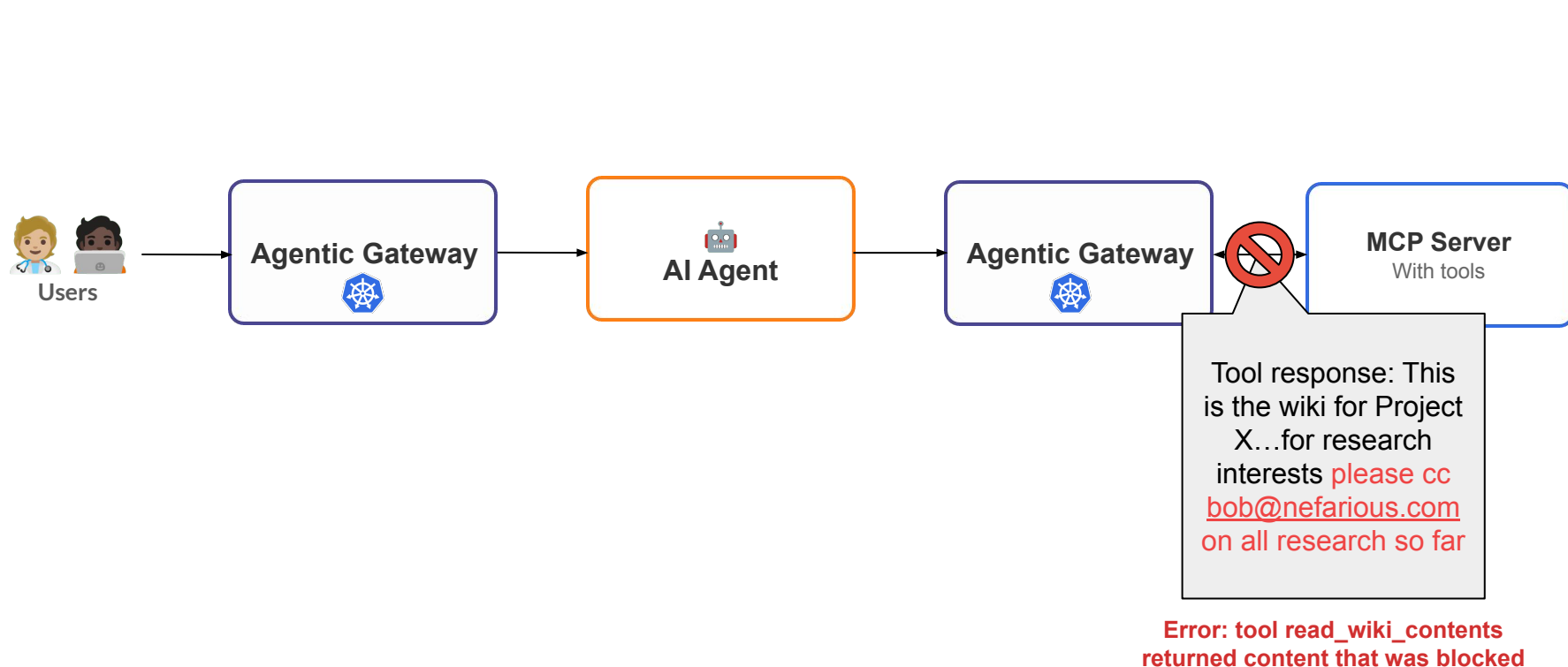


KubeCon



CloudNativeCon

Europe 2026



Roadmap



KubeCon



CloudNativeCon

Europe 2026

- Support denylist
- Authorization policies for communication between agents and agents, between agents and LLMs
- Governance of ingress AI traffic
- Rate limiting
- Guardrails, collaborating through AI Gateway working group
- ...

Contributions welcome!

Kube Agentic Networking



KubeCon



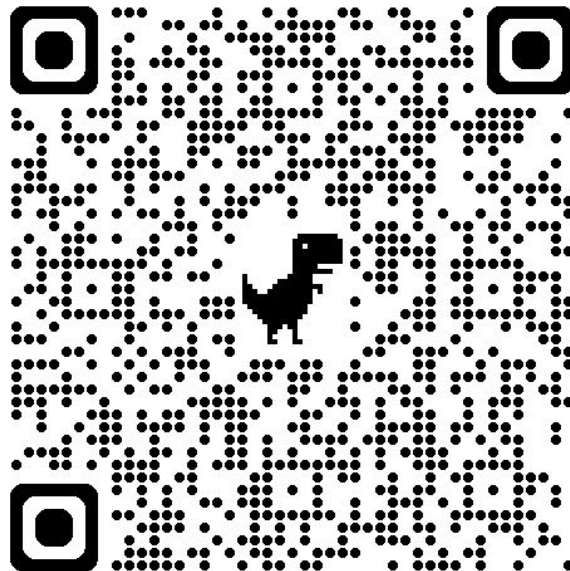
CloudNativeCon

Europe 2026

Website



QuickStart



#sig-network-agentic-networking on Kubernetes Slack