

AI Agent Hub



Overview

AI Agent Hub is JioCloud's centralized platform for managing, deploying, and monitoring AI agents across your enterprise. It provides a comprehensive ecosystem where Agent Admins and Agent Creators can onboard intelligent agents, configure their capabilities, and make them available to authorized users based on organisational hierarchy, projects, and user roles. With built-in security guardrails, Human-in-the-Loop (HITL) approval workflows, real-time observability, and an interactive Agent Playground, AI Agent Hub ensures enterprise-grade governance and control for all AI-driven operations-every time.

Key Features

- **Centralized Agent Management**
Unified dashboard to register, manage, and monitor AI agents across the organisation.
- **Agent Catalogue and Subscription**
Curated agent catalogue with flexible subscriptions by organisation, project, role, or group.
- **Agent Playground**
Interactive environment to test agent behavior and prompts before deployment.
- **Built-In Guardrails**
Runtime security and compliance controls to keep agents within organisational boundaries.
- **Role-Based Access Control (RBAC)**
Three-tier access model with fine-grained permissions for every agent.
- **Real-Time Observability**
Monitor agent invocations, success rates, failures, and execution metrics in real time.
- **Human-in-the-Loop (HITL)**
Built-in approval workflows for high-impact or irreversible agent actions.

Benefits

- **Peak Agent Performance**
Deploy agents with direct API access and zero middleware overhead.
- **Enterprise Governance**
RBAC and HITL ensure agents operate within defined enterprise policies.
- **Mission-Critical Readiness**
Guardrails and compliance checks meet enterprise security requirements.
- **Faster Time-to-Value (TTV)**
Pre-configured agents reduce time from idea to production deployment.
- **Consistent Observability**
Full execution telemetry for real-time debugging, audit, and optimisation.
- **No Configuration Delays**
Agents are ready to subscribe and invoke with zero infrastructure setup.

Technical Specifications

Database

Operating
System

Cloud (AWS /
Azure / GCP)

Kubernetes

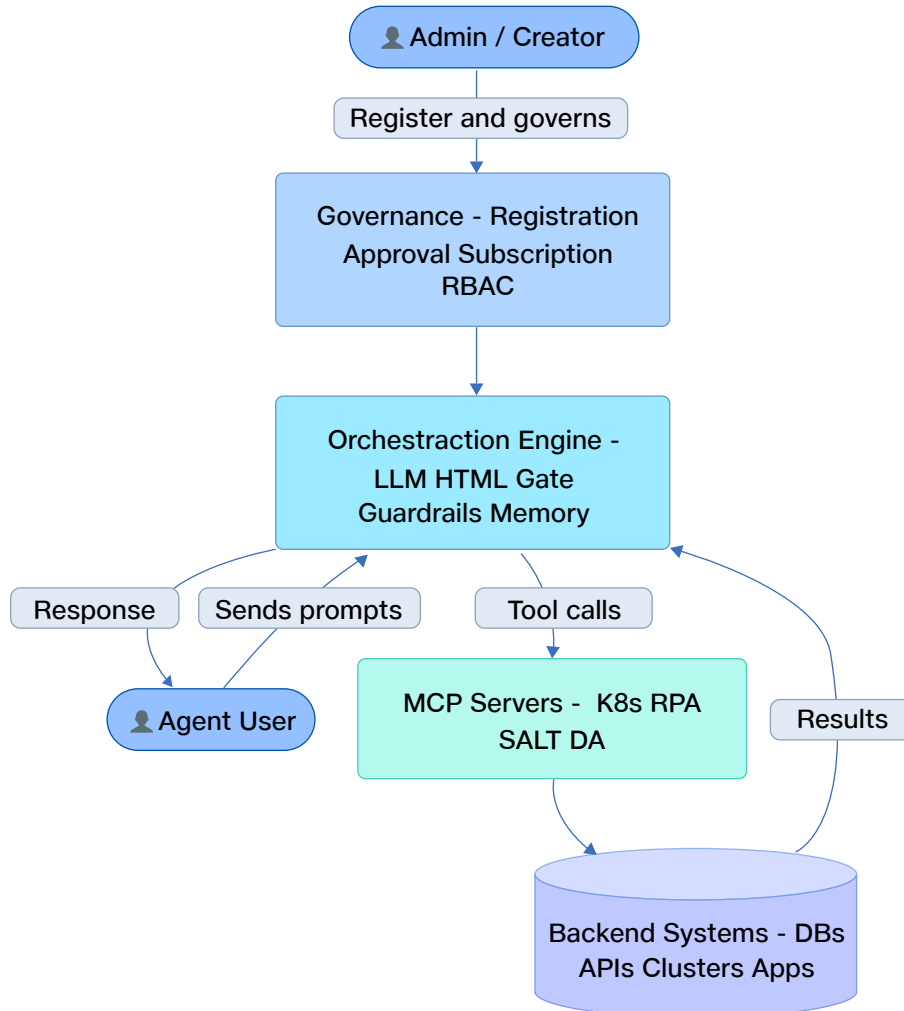
Middleware

Network
and APIs

Technical Specifications

Category	Specifications
Deployment Model	Cloud-hosted (JioCloud Platform)
Access Interface	Web Dashboard + REST API
User Roles	Agent Admin · Agent Creator · Agent User
Agent Registration	Multi-step wizard (5 steps)
Authentication	Basic Auth, API Key, OAuth
Observability	Real-time metrics, invocation history
HITL Support	Yes – configurable per agent
Guardrails	Built-in security and compliance checks
Deployment	SaaS – JioCloud CloudXP Platform

Architecture Diagram



Use Cases

- IT Operations Automation**
 Deploy AI agents to monitor, diagnose, and autonomously remediate infrastructure issues-spanning databases, operating systems, cloud platforms, and middleware-with full RBAC control and audit logging.
- Enterprise AI Governance**
 Centrally manage and govern all AI agents across business units with role-based permissions, HITL approval workflows, compliance guardrails, and complete invocation audit trails for regulatory adherence.
- Cloud and Kubernetes Operations**
 Enable autonomous Kubernetes cluster management, cloud resource optimisation, and real-time incident response with AI-powered agents-without jitter or infrastructure noise.