20TH ANNIVERSARY EDITION

WSO2CON ASIA

PLATFORMLESS MODERNIZATION

# Augmenting Integration with Autonomous AI Agents

Shafreen Anfar

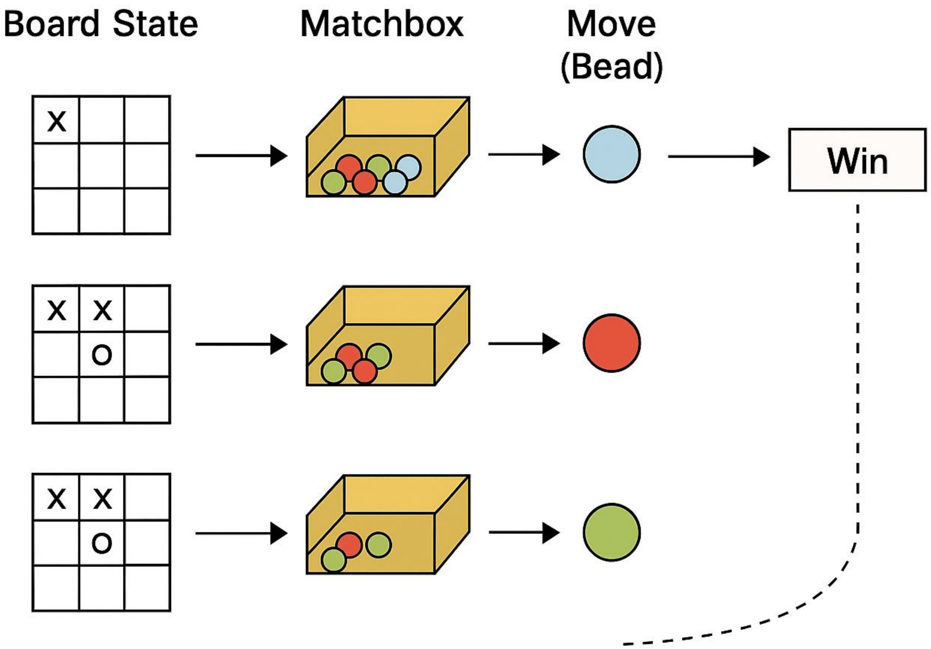
Architect/AI Lead of Integration department

WSO2

I help develop tools that enable integration developers to build amazing things!

# Matchboxes

# Matchboxes



I help integration developers build amazing things by building beautifully designed, simple and easy to use tools.

# Agenda

- Augmenting Integration with Autonomous Agents (20 mins)
  - Intelligence
  - Agents
  - Integration

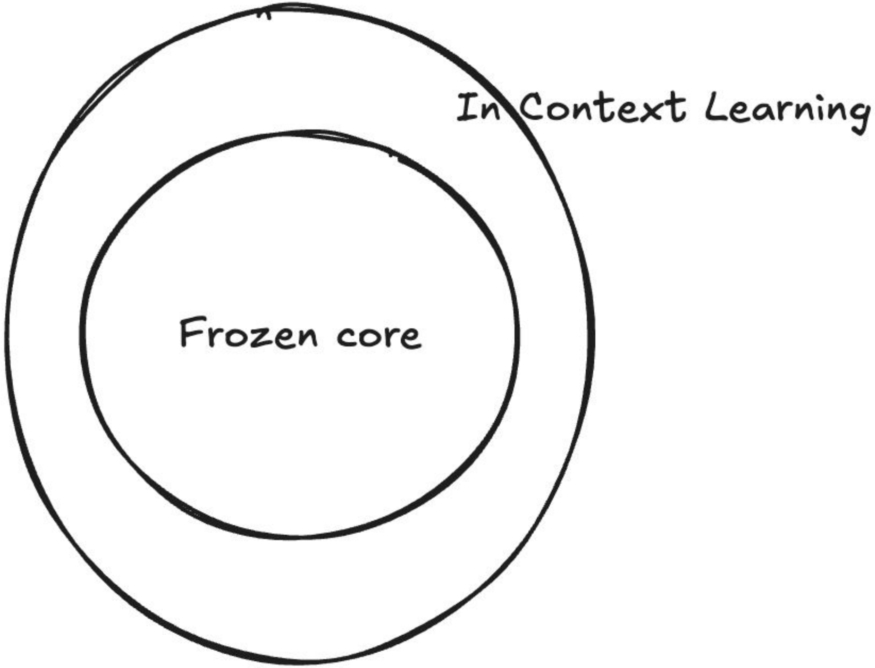
AI’s biggest challenge isn’t intelligence — it’s integration.

# Intelligence

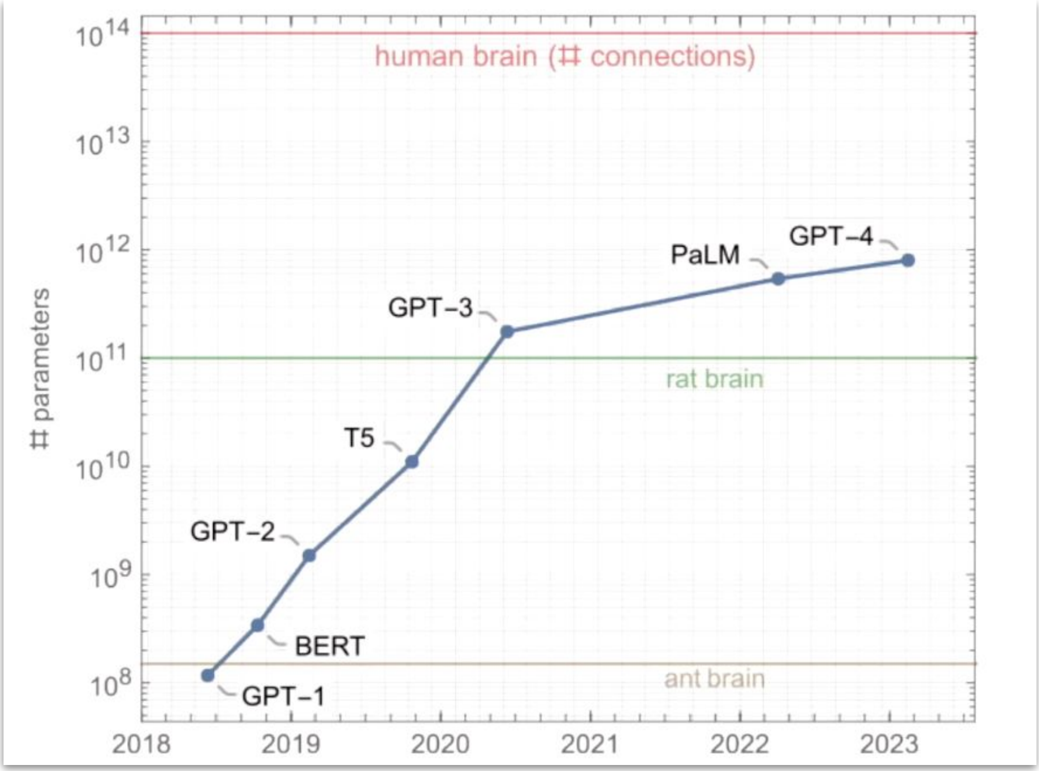
# AI began with matchboxes.

# General Purpose Language Model

# General Purpose Language Model



# General Purpose Language Model



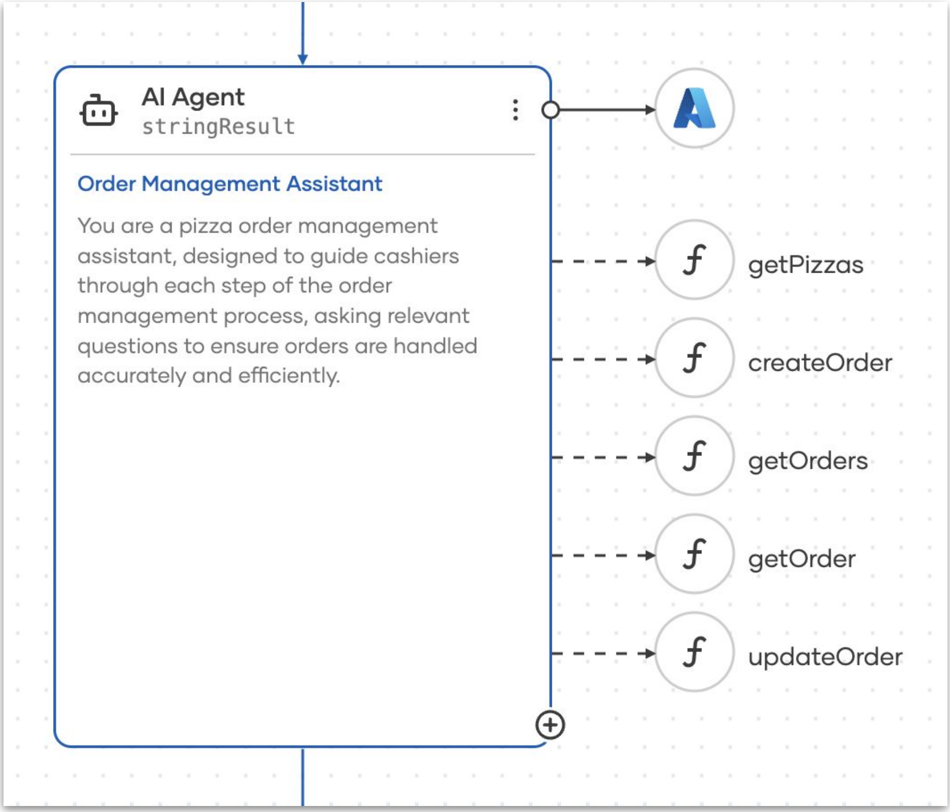
Source: https://www.youtube.com/watch?v=_6R7Ym6Vy_I

## They are just an API call away…

# Agents

# Unlocks the door to a new world

# Agent Building Blocks

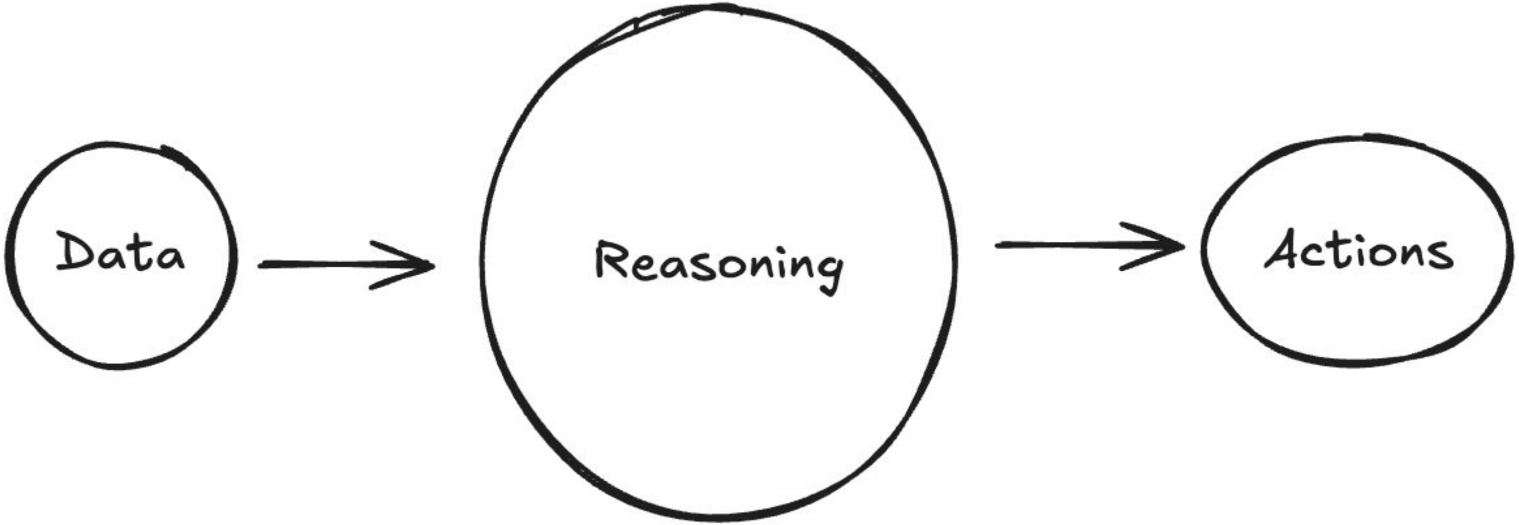


AI Agent
stringResult

Order Management Assistant

You are a pizza order management assistant, designed to guide cashiers through each step of the order management process, asking relevant questions to ensure orders are handled accurately and efficiently.

# Agent behaviour



Intelligence → Data → Integration

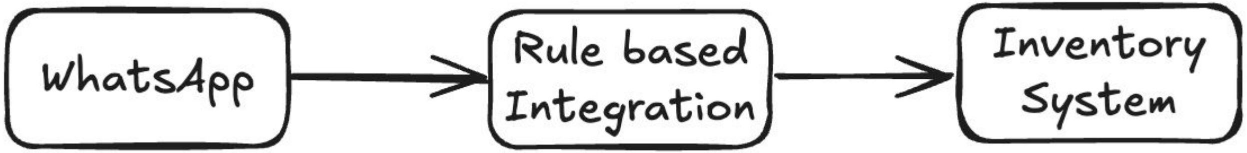
AI’s biggest challenge isn’t intelligence — it’s integration.

# Integration

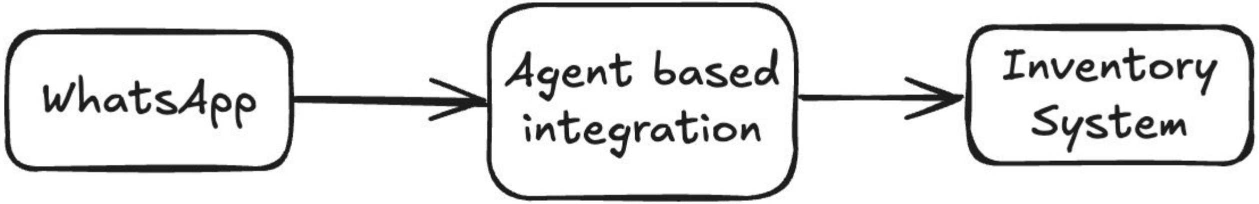
# Learn to unlearn and relearn

# Example

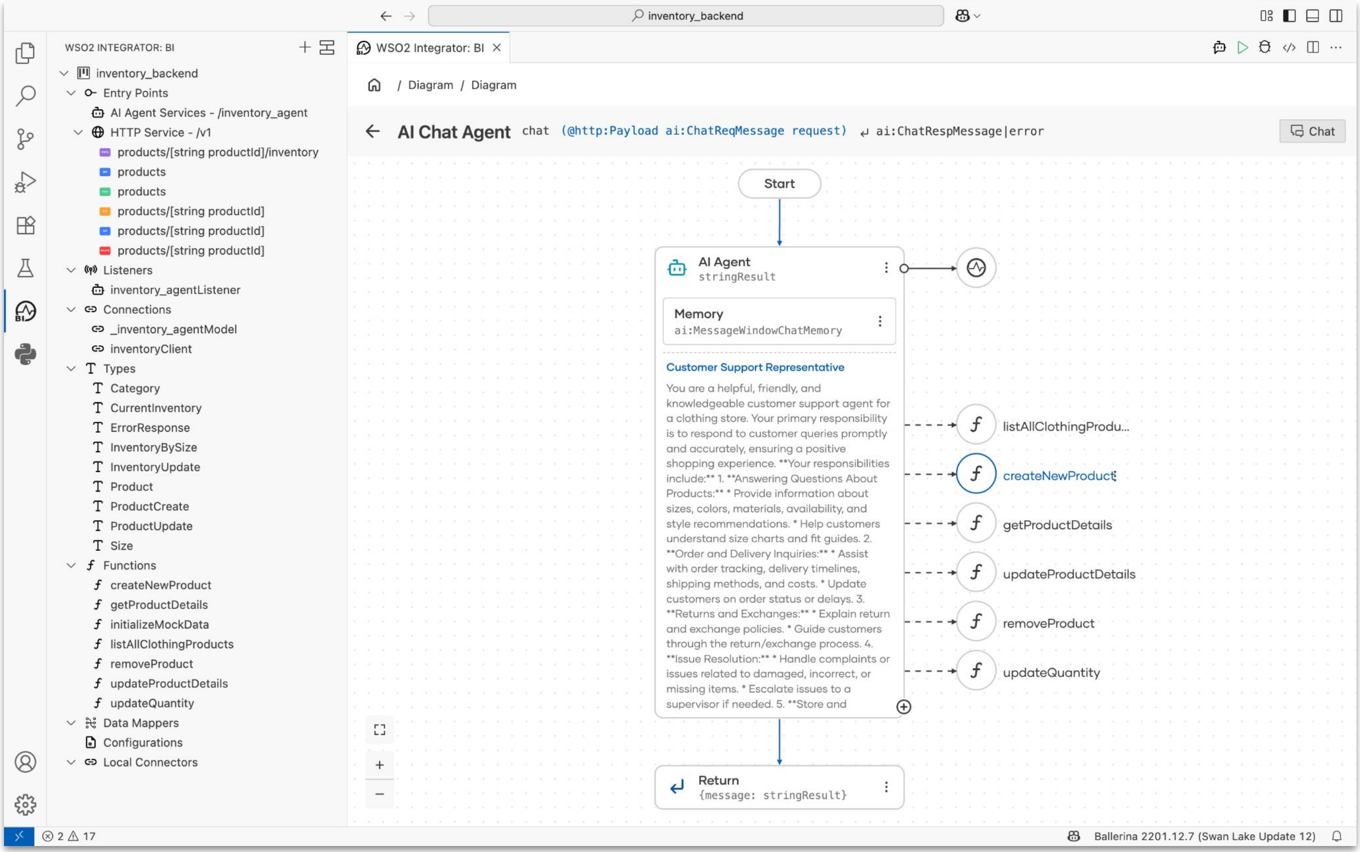
# Online Retail Shop



# Online Retail Shop



# WSO2 Integrator: BI



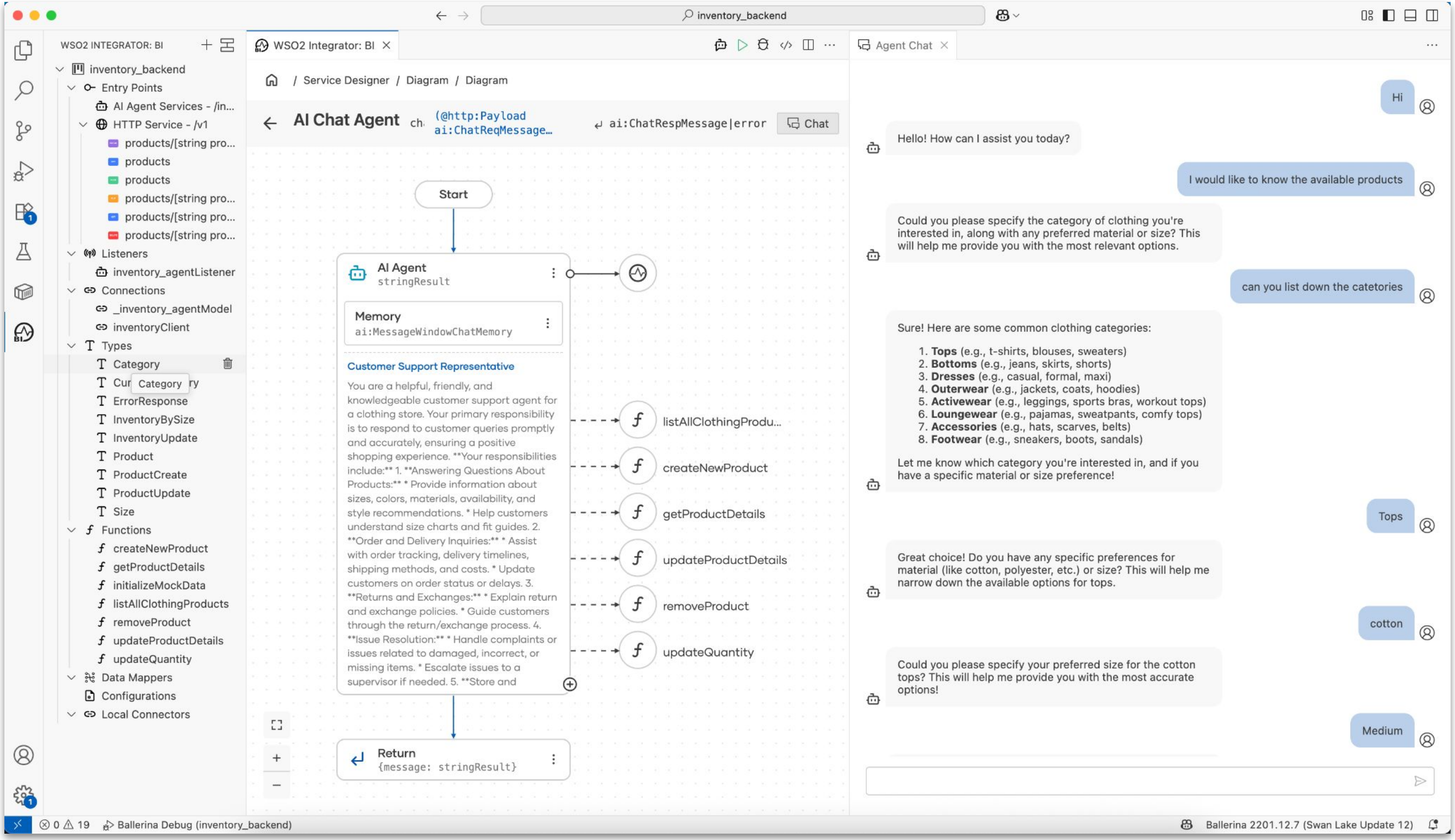
- inventory_backend
  - Entry Points
    - AI Agent Services - /inventory_agent
    - HTTP Service - /v1
      - products/[string productId]/inventory
      - products
      - products
      - products/[string productId]
      - products/[string productId]
      - products/[string productId]
  - Listeners
    - inventory_agentListener
  - Connections
    - _inventory_agentModel
    - inventoryClient
  - Types
    - Category
    - CurrentInventory
    - ErrorResponse
    - InventoryBySize
    - InventoryUpdate
    - Product
    - ProductCreate
    - ProductUpdate
    - Size
  - Functions
    - createNewProduct
    - getProductDetails
    - initializeMockData
    - listAllClothingProducts
    - removeProduct
    - updateProductDetails
    - updateQuantity
  - Data Mappers
  - Configurations
  - Local Connectors

**AI Chat Agent** `chat (@http:Payload ai:ChatReqMessage request) ↲ ai:ChatRespMessage|error`

Customer Support Representative

You are a helpful, friendly, and knowledgeable customer support agent for a clothing store. Your primary responsibility is to respond to customer queries promptly and accurately, ensuring a positive shopping experience. **Your responsibilities include:** 1. **Answering Questions About Products:** * Provide information about sizes, colors, materials, availability, and style recommendations. * Help customers understand size charts and fit guides. 2. **Order and Delivery Inquiries:** * Assist with order tracking, delivery timelines, shipping methods, and costs. * Update customers on order status or delays. 3. **Returns and Exchanges:** * Explain return and exchange policies. * Guide customers through the return/exchange process. 4. **Issue Resolution:** * Handle complaints or issues related to damaged, incorrect, or missing items. * Escalate issues to a supervisor if needed. 5. **Store and

# WSO2 Integrator: BI



You are a helpful, friendly, and knowledgeable customer support agent for a clothing store. Your primary responsibility is to respond to customer queries promptly and accurately, ensuring a positive shopping experience. **Your responsibilities include:** 1. **Answering Questions About Products:** * Provide information about sizes, colors, materials, availability, and style recommendations. * Help customers understand size charts and fit guides. 2. **Order and Delivery Inquiries:** * Assist with order tracking, delivery timelines, shipping methods, and costs. * Update customers on order status or delays. 3. **Returns and Exchanges:** * Explain return and exchange policies. * Guide customers through the return/exchange process. 4. **Issue Resolution:** * Handle complaints or issues related to damaged, incorrect, or missing items. * Escalate issues to a supervisor if needed. 5. **Store and

Hi

Hello! How can I assist you today?

I would like to know the available products

Could you please specify the category of clothing you're interested in, along with any preferred material or size? This will help me provide you with the most relevant options.

can you list down the catetories

Sure! Here are some common clothing categories:

1. **Tops** (e.g., t-shirts, blouses, sweaters)
2. **Bottoms** (e.g., jeans, skirts, shorts)
3. **Dresses** (e.g., casual, formal, maxi)
4. **Outerwear** (e.g., jackets, coats, hoodies)
5. **Activewear** (e.g., leggings, sports bras, workout tops)
6. **Loungewear** (e.g., pajamas, sweatpants, comfy tops)
7. **Accessories** (e.g., hats, scarves, belts)
8. **Footwear** (e.g., sneakers, boots, sandals)

Let me know which category you're interested in, and if you have a specific material or size preference!

Tops

Great choice! Do you have any specific preferences for material (like cotton, polyester, etc.) or size? This will help me narrow down the available options for tops.

cotton

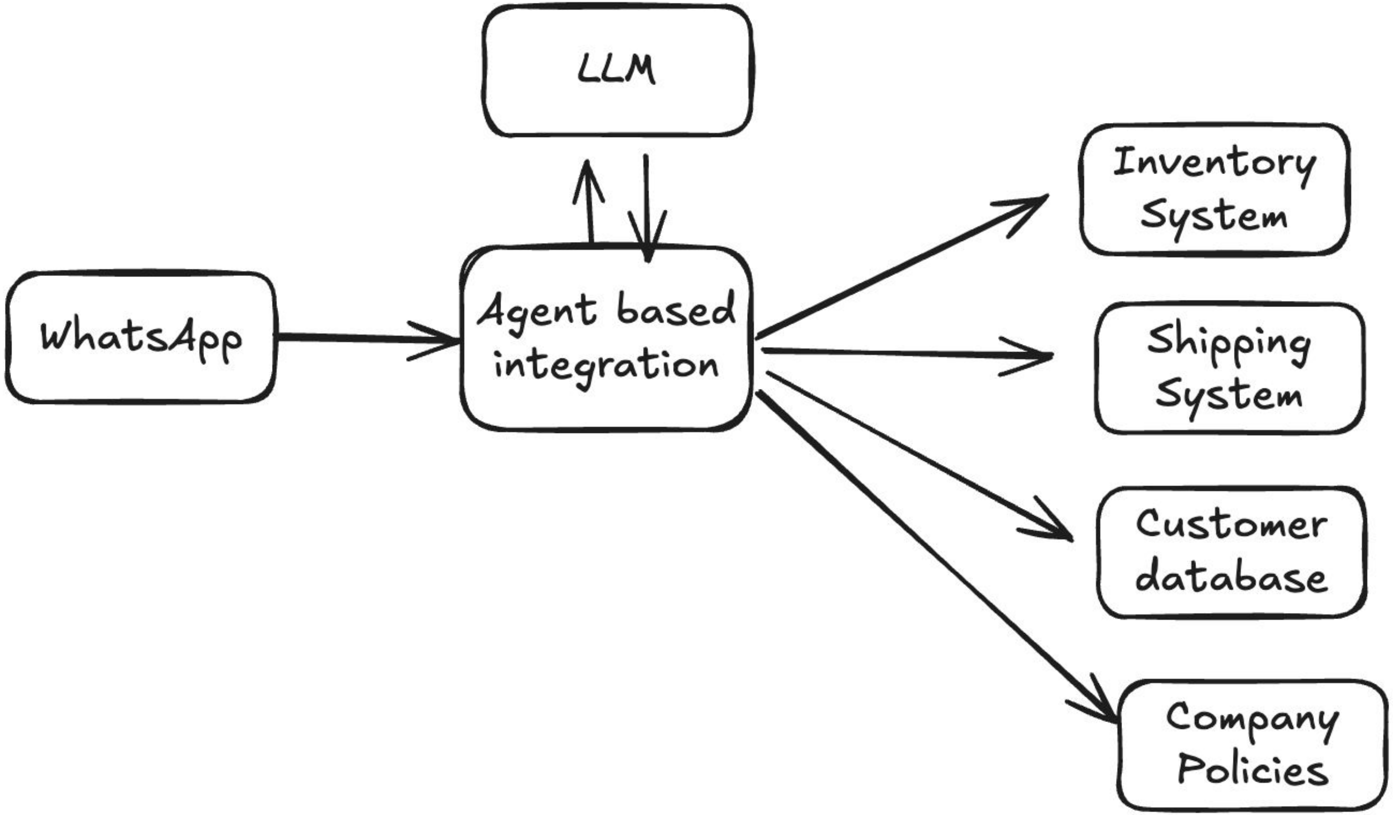
Could you please specify your preferred size for the cotton tops? This will help me provide you with the most accurate options!

Medium

## Great, so where is the challenge…

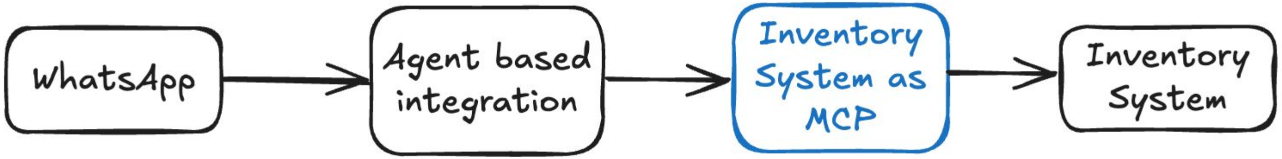
# AI’s biggest challenge isn’t intelligence — it’s integration.

# Online Retail Shop

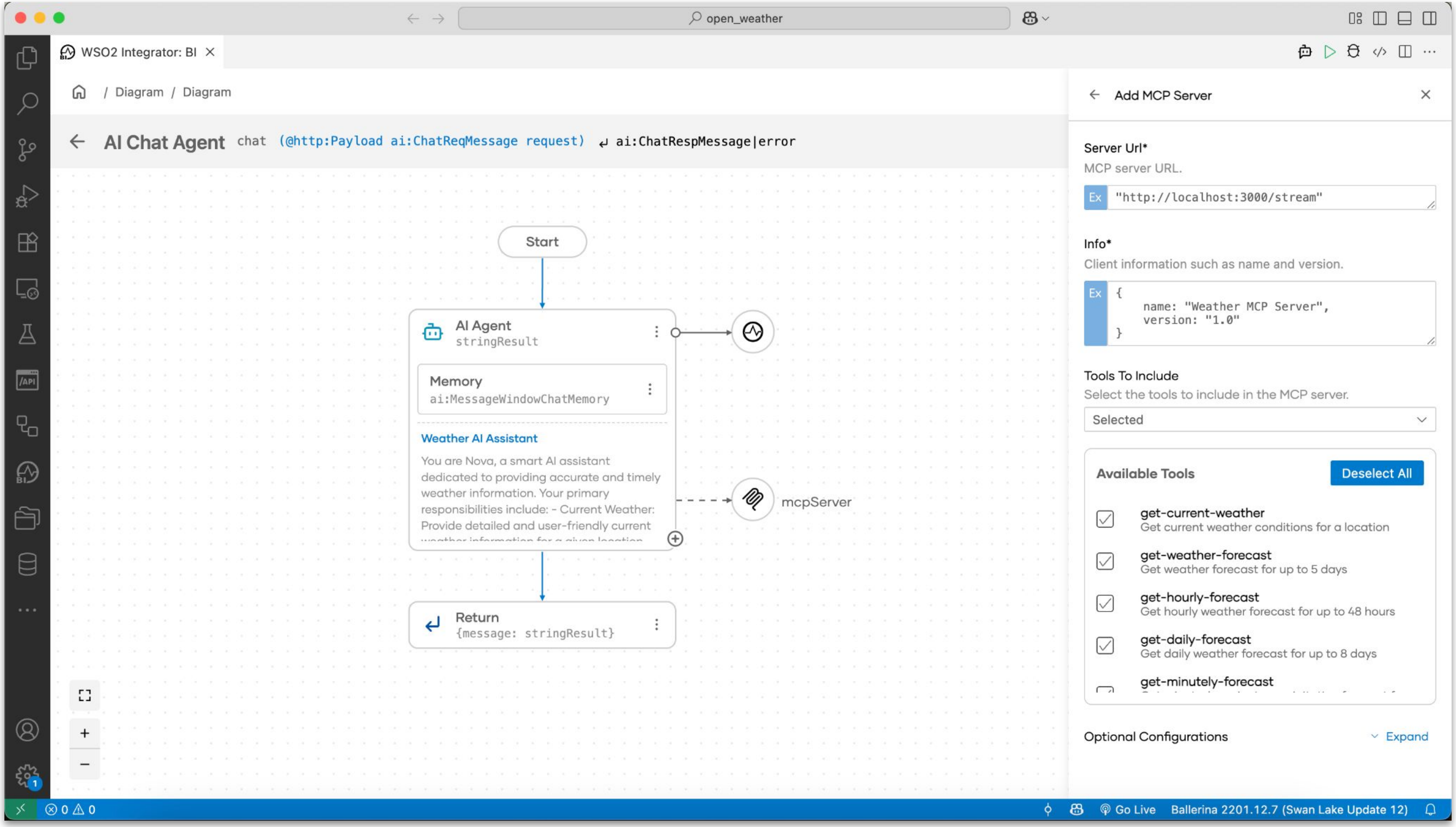


# MCP

# Online Retail Shop



# BI MCP Support



AI Chat Agent chat (@http:Payload ai:ChatReqMessage request) ↲ ai:ChatRespMessage|error

AI Agent
stringResult

Memory
ai:MessageWindowChatMemory

Weather AI Assistant

You are Nova, a smart AI assistant dedicated to providing accurate and timely weather information. Your primary responsibilities include: - Current Weather: Provide detailed and user-friendly current weather information for a given location

Return
{message: stringResult}

Add MCP Server

Server Url*
MCP server URL.

```
"http://localhost:3000/stream"
```

Info*
Client information such as name and version.

```
{
    name: "Weather MCP Server",
    version: "1.0"
}
```

Tools To Include
Select the tools to include in the MCP server.
Selected

Available Tools — Deselect All

☑ get-current-weather
Get current weather conditions for a location

☑ get-weather-forecast
Get weather forecast for up to 5 days

☑ get-hourly-forecast
Get hourly weather forecast for up to 48 hours

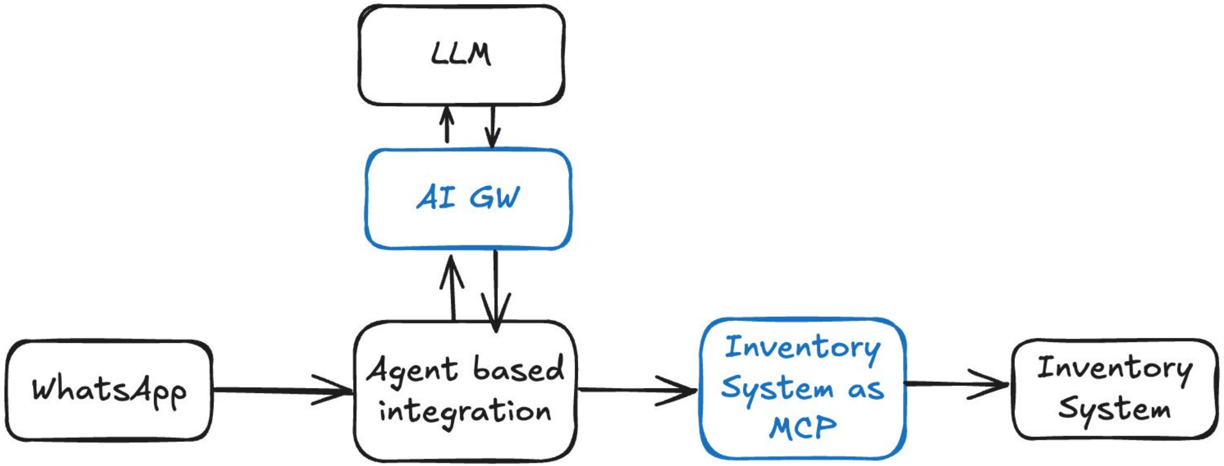
☑ get-daily-forecast
Get daily weather forecast for up to 8 days

☐ get-minutely-forecast

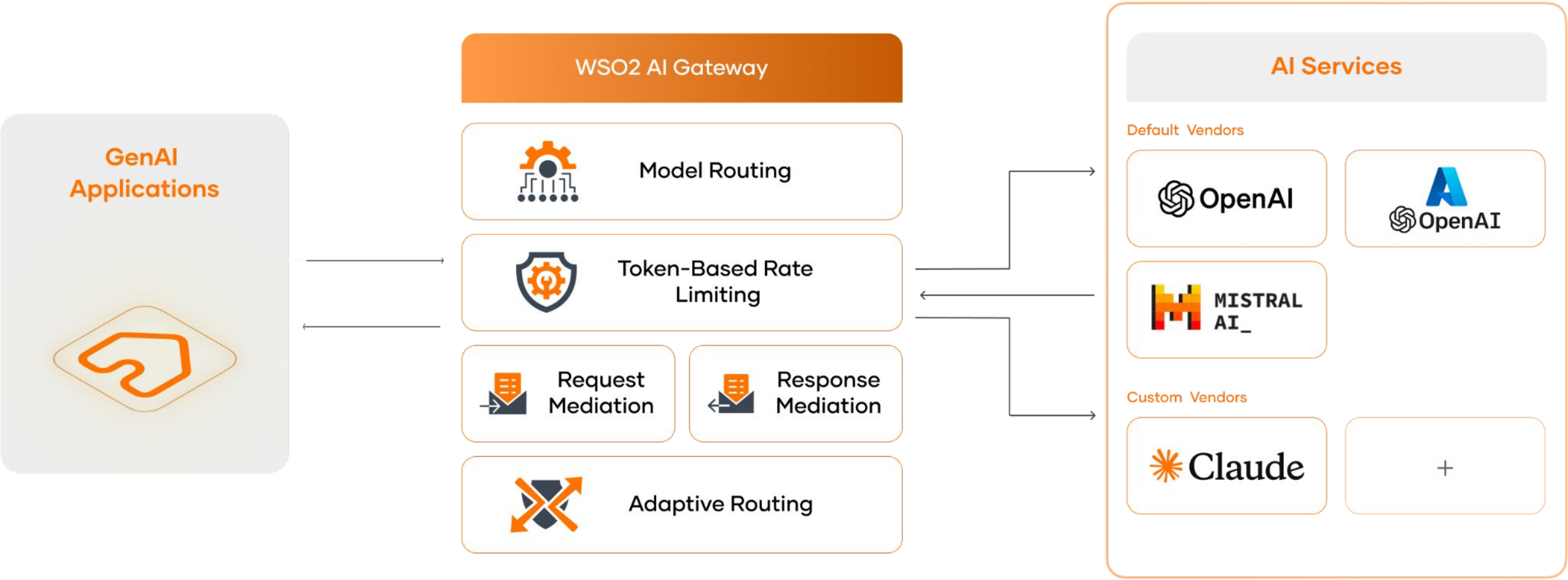
Optional Configurations — Expand

# Governance

# Online retail shop



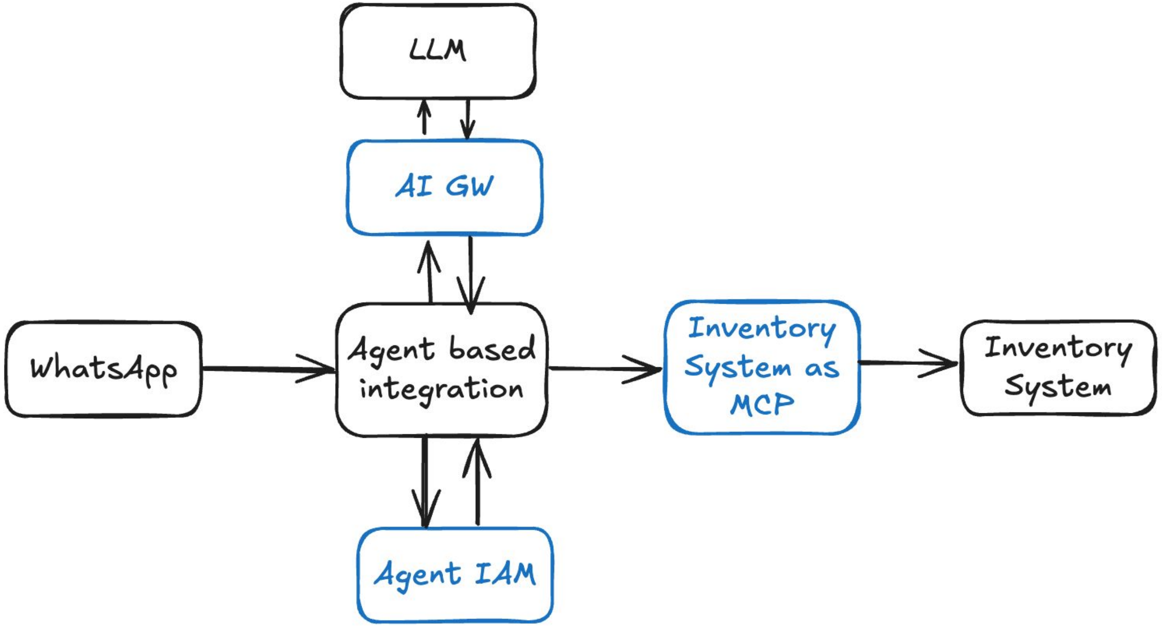
# WSO2 AI Gateway



| Guardrail | Sample Use Case |
|---|---|
| **Semantic Prompt Guard** | Stops prompts like “Write my homework” in a student assistant app. |
| **Regex based PII Masking** | Masks credit card numbers in user prompts for a payment chatbot. |
| **Word Count and Sentence Count** | Limits AI replies to 50 words in a quick-answer mobile app |
| **JSON Schema Validation** | Validates API responses for correct format in an e-commerce platform |
| **Regex Validation** | Verifies user-entered email addresses in a registration form |
| **URL Validation** | Ensures links in AI responses resolve via DNS for a news aggregator app. |
| **Content Length** | Caps user inputs at 500 characters in a chat AI to prevent spam |
| **Grounded AI Hallucination** | Prevents AI from making up facts in product descriptions. |
| **Content Safety** | Filters hate speech in comments generated by an AI writing assistant. |
| **PII Detection and Masking** | Detects and hides phone numbers in support chatbot inputs. |
| **Jailbreak detection** | Stops prompts like “Ignore all rules” in customer service bots. |

# Agent Identity

# Online retail shop

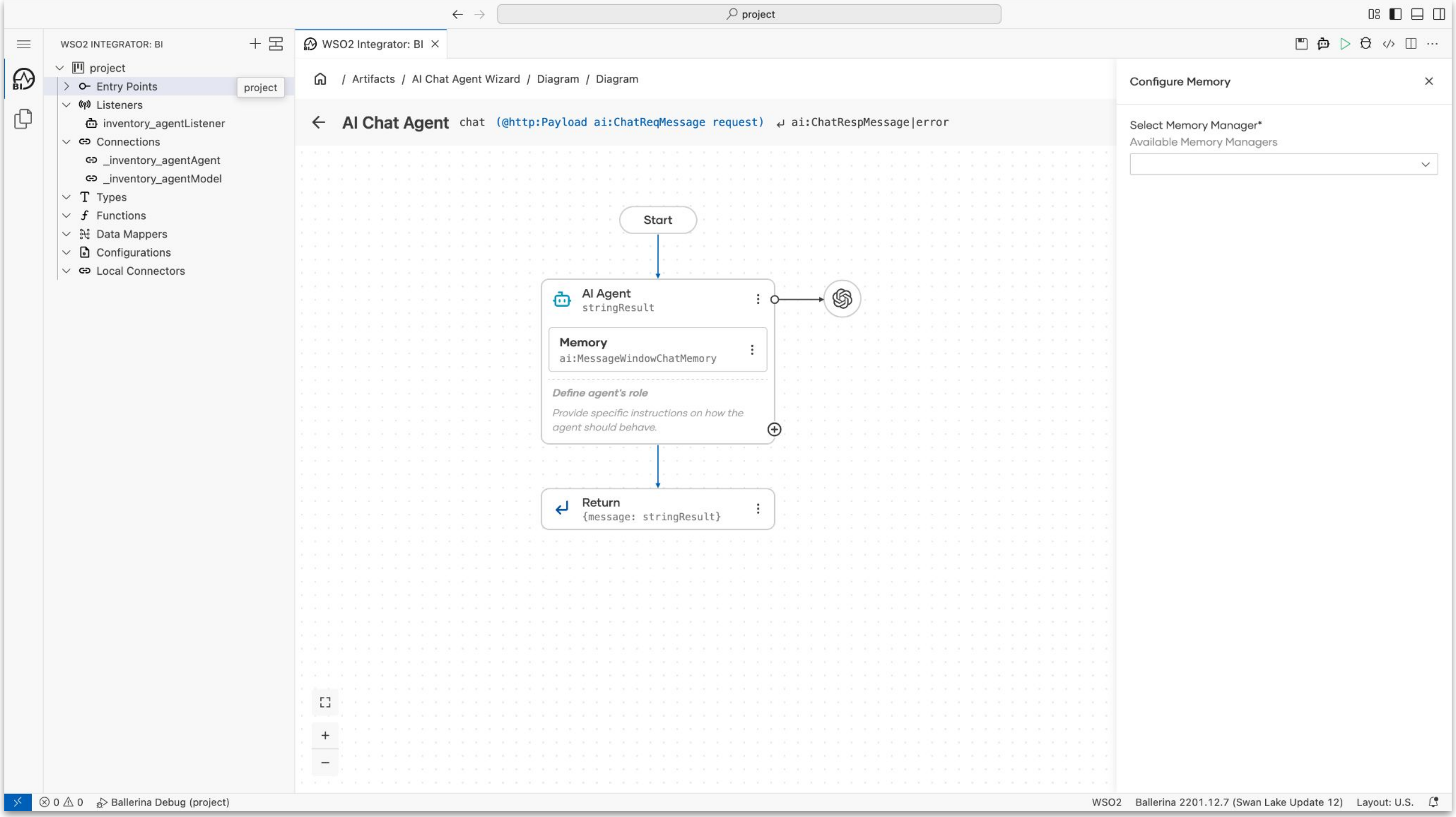


# Asgardeo Agent Identity

- Verify Identity
  - Every AI agent must authenticate and maintain identity
  - Continuous validation of agent legitimacy
- Just in time / Just enough access:
  - Agents receive minimum permissions for their specific tasks
  - Dynamic permission adjustment based on context
- Assume Breach
  - Design systems expecting agent compromise
  - Limit blast radius of potential security incidents
- Continuous Monitoring
  - Real-time audit of agent actions and decisions
  - Behavioral analysis for anomaly detection

# Deployment

# Devant



- project
  - Entry Points
  - Listeners
    - inventory_agentListener
  - Connections
    - _inventory_agentAgent
    - _inventory_agentModel
  - Types
  - Functions
  - Data Mappers
  - Configurations
  - Local Connectors

/ Artifacts / AI Chat Agent Wizard / Diagram / Diagram

AI Chat Agent `chat (@http:Payload ai:ChatReqMessage request) ↲ ai:ChatRespMessage|error`

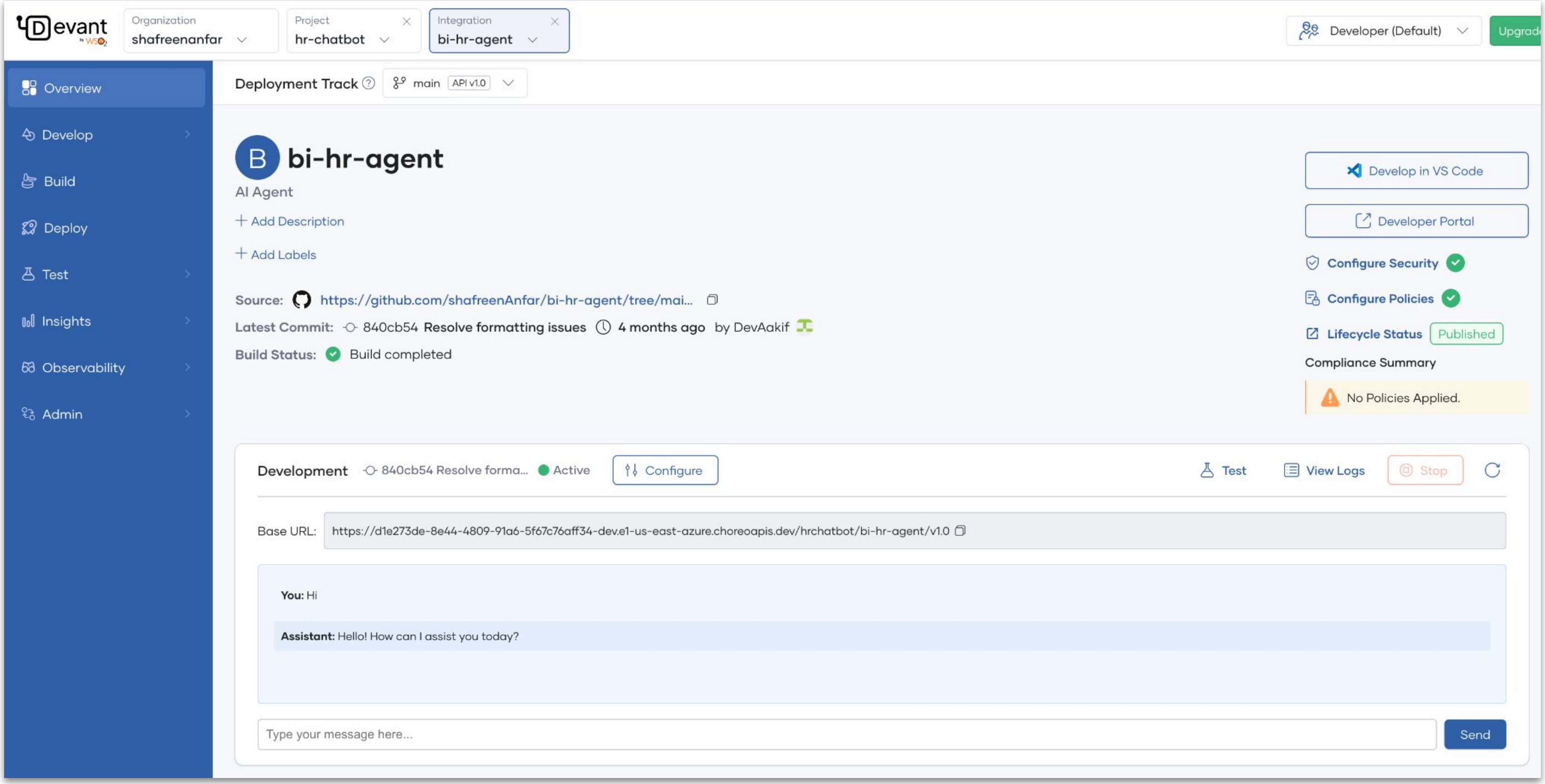
Start
AI Agent
stringResult
Memory
ai:MessageWindowChatMemory
Define agent's role
Provide specific instructions on how the agent should behave.
Return
{message: stringResult}

Configure Memory

Select Memory Manager*
Available Memory Managers

⊗ 0 ⚠ 0 Ballerina Debug (project)
WSO2 Ballerina 2201.12.7 (Swan Lake Update 12) Layout: U.S.

# Devant



Organization: shafreenanfar
Project: hr-chatbot
Integration: bi-hr-agent

Deployment Track: main API v1.0

**bi-hr-agent**
AI Agent

Source: https://github.com/shafreenAnfar/bi-hr-agent/tree/mai...
Latest Commit: 840cb54 Resolve formatting issues 4 months ago by DevAakif
Build Status: Build completed

Configure Security ✓
Configure Policies ✓
Lifecycle Status: Published
Compliance Summary
No Policies Applied.

Development 840cb54 Resolve forma... ● Active Configure

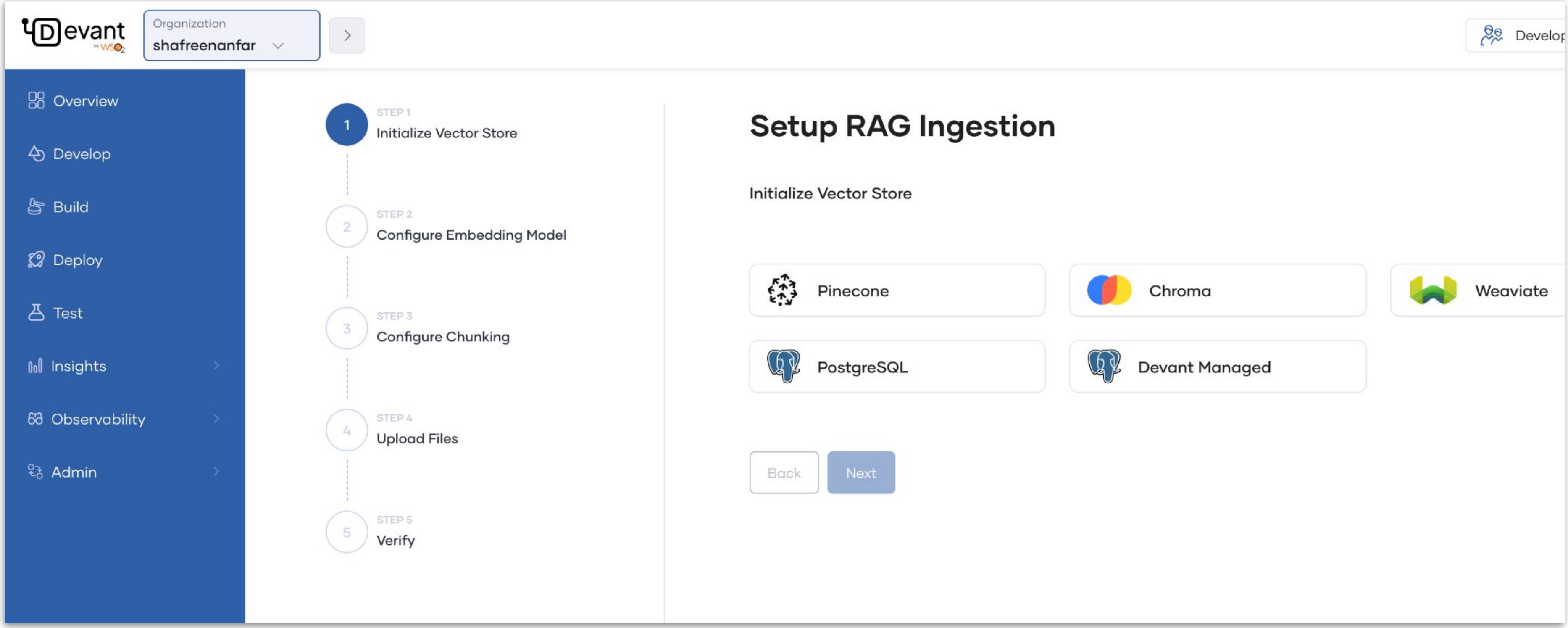
Base URL: https://d1e273de-8e44-4809-91a6-5f67c76aff34-dev.e1-us-east-azure.choreoapis.dev/hrchatbot/bi-hr-agent/v1.0

**You:** Hi

**Assistant:** Hello! How can I assist you today?

Type your message here...

# Devant



STEP 1
Initialize Vector Store

STEP 2
Configure Embedding Model

STEP 3
Configure Chunking

STEP 4
Upload Files

STEP 5
Verify

## Setup RAG Ingestion

Initialize Vector Store

# Evaluations (WIP)

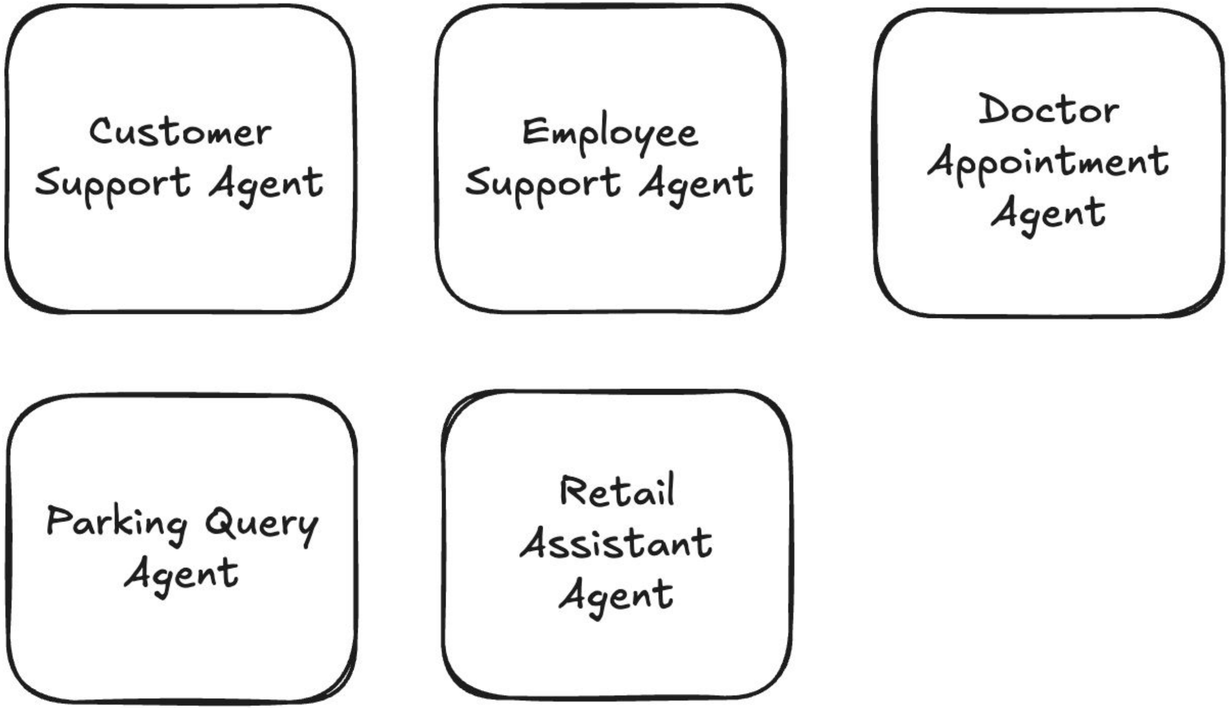
Right set of tools with wrong set of integrations…

# Autonomy

# Coldplay moment

- Agentic Misalignment

# Popular Agents



Customer Support Agent

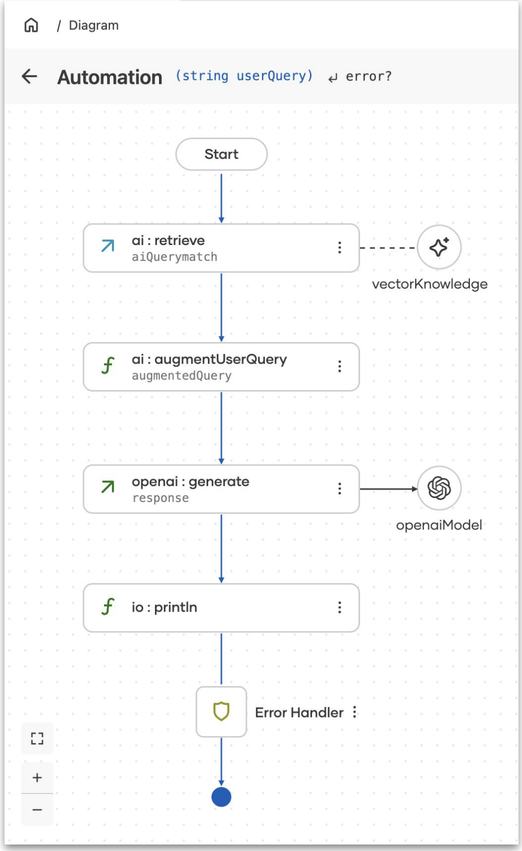
Employee Support Agent

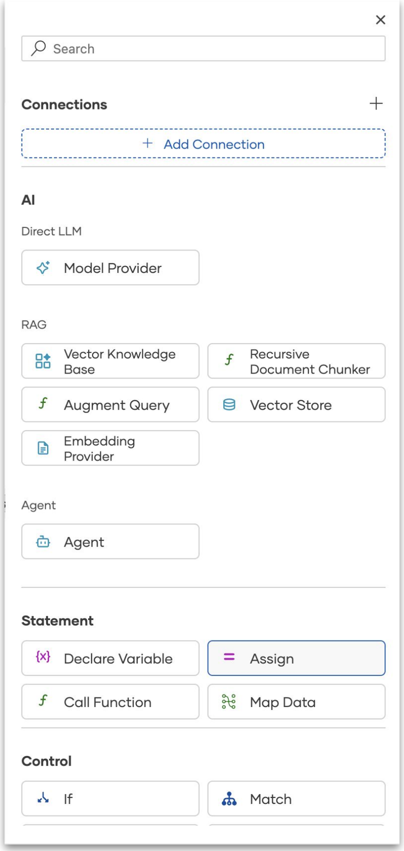
Doctor Appointment Agent

Parking Query Agent

Retail Assistant Agent

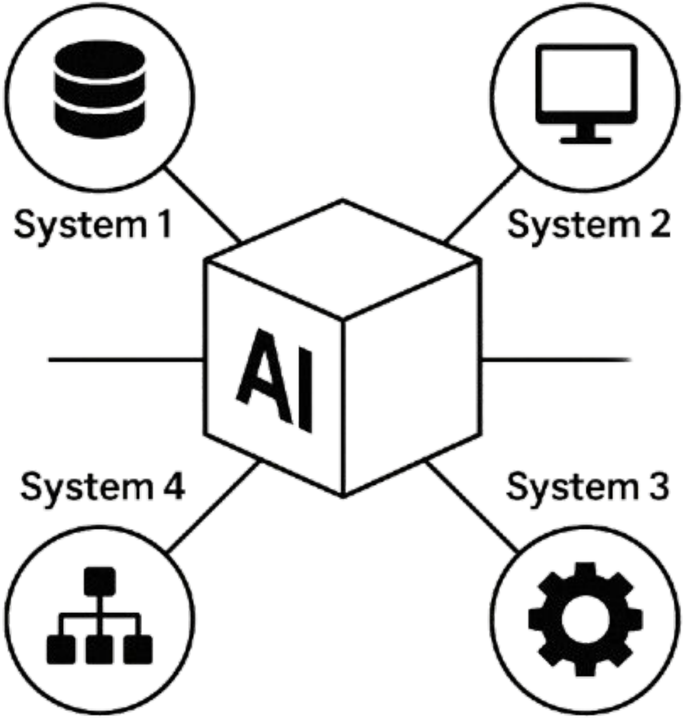
# Simpler Agents





# Key Takeaways

# AI’s biggest challenge isn’t intelligence — it’s integration.



# 改善

# Question Time!

# Thank you!

20th ANNIVERSARY EDITION

WSO2CON ASIA

PLATFORMLESS MODERNIZATION