A2AForge – Crafting Intelligent Cloud Agents with A2A and MCP

TEAM MEMBERS:

APURVA KARNE (018221801)

CHANDINI SAISRI UPPUGANTI (018228483)

HARSHAVARDHAN REDDY (018239936)

ROSHINI JOGA (0182211736)

Problem Statement

The Challenge in current Cloud Infrastructure Management :

- Cloud environments (AWS, Azure, GCP) are becoming **more complex and dynamic**.
- Managing EC2, S3, VPC, Lambda, IAM, etc., requires **specialized knowledge**.
- DevOps teams spend significant time on **manual, repetitive tasks**.
- Misconfigurations or human errors can lead to **downtime, security risks, or cost overruns**.
- There is **no unified, natural-language interface** for cloud operations.

A2AForge

What is A2AForge?

- A2AForge is an AI-powered **multi-agent automation system** that manages cloud infrastructure through **natural language commands**.

How It Works

- Converts user intent into actionable cloud operations
- Uses multiple specialized AI agents (EC2, S3, etc.)
- Agents communicate autonomously using **Google's A2A Protocol**
- Executes cloud tasks safely via **Anthropic's MCP tool integration**
- Leverages **OpenAI Agents SDK** for reasoning, delegation, and decision-making

Solution Highlights

- Reduces manual DevOps workload
- Minimizes configuration errors
- Enables conversational cloud management
- Scalable to any AWS service or cloud provider

What Makes A2AForge Unique?

1. Autonomous Multi-Agent Collaboration

- Agents communicate, delegate, and solve tasks without centralized control.
- EC2 Agent, S3 Agent, and future agents work together seamlessly.

2. Protocol-Driven Intelligence

- Uses **Google's A2A protocol** for agent-to-agent messaging.
- Integrates **Anthropic's MCP** to securely execute AWS operations.

3. Natural Language Cloud Management

- Users interact with AWS using **plain English** (e.g., "Create an EC2 instance").
- No need for CLI, console navigation, or scripting.

4. Modular & Extensible Architecture

- New agents (Lambda, RDS, IAM, CloudWatch) can be added easily.
- Highly scalable for enterprise-level cloud automation.

5. Production-Inspired Design

- Secure credential handling
- Region inference
- Real-world DevOps patterns mirrored in design

High-Level Architecture Overview

Core Components

- **Coordinator Agent -** Routes user requests, interprets intent, and assigns tasks to specialized agents.
- **EC2 Agent -** Handles EC2 lifecycle actions (create, stop, terminate, list).
- **S3 Agent -** Manages S3 bucket operations (create, list, delete, list objects).

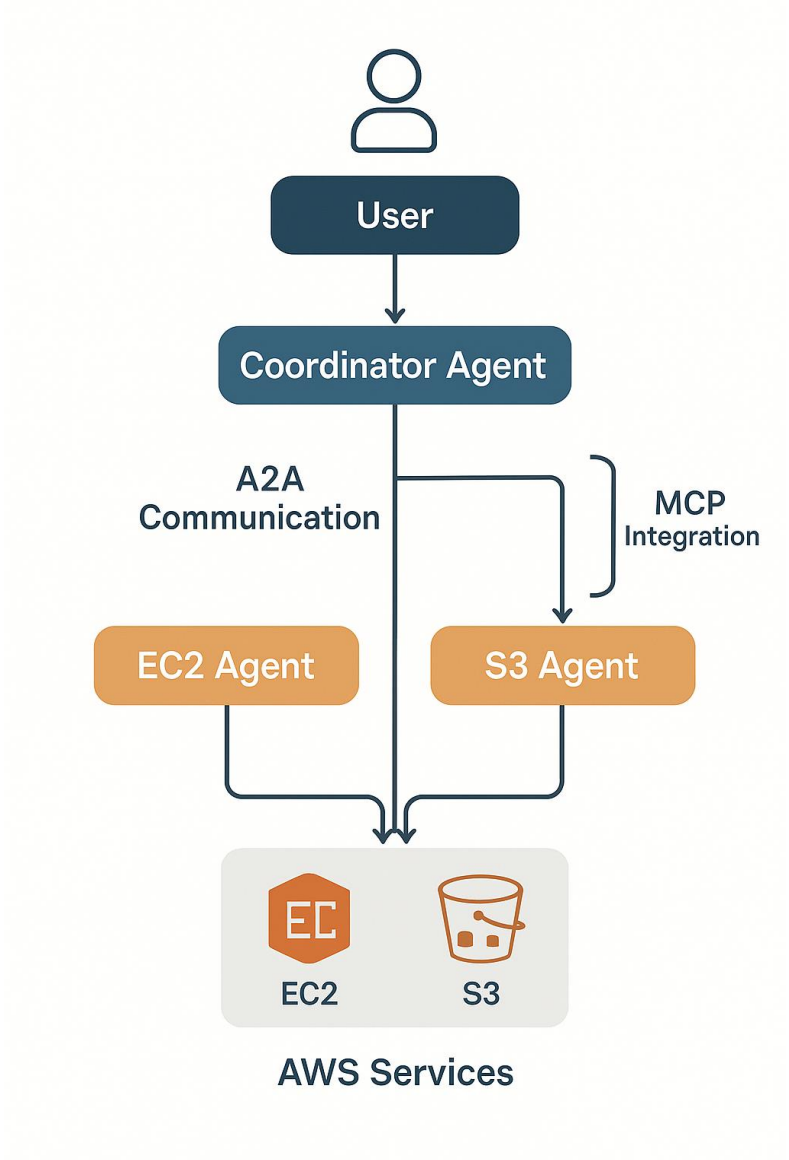
Supporting Technologies

- **A2A Protocol (Google):** Enables autonomous agent-to-agent communication.
- **MCP (Anthropic):** Provides secure tool access for real AWS operations.
- **OpenAI Agents SDK:** Powers reasoning, delegation, and tool-use decision-making.
- **Perplexity API:** Enhances natural language understanding.

System Flow (Simplified)

- User gives a natural language command
- Coordinator Agent interprets intent
- Coordinator dispatches task to EC2/S3 Agent
- Agent performs tool actions via MCP
- AWS executes the requested operation
- Response is returned to user

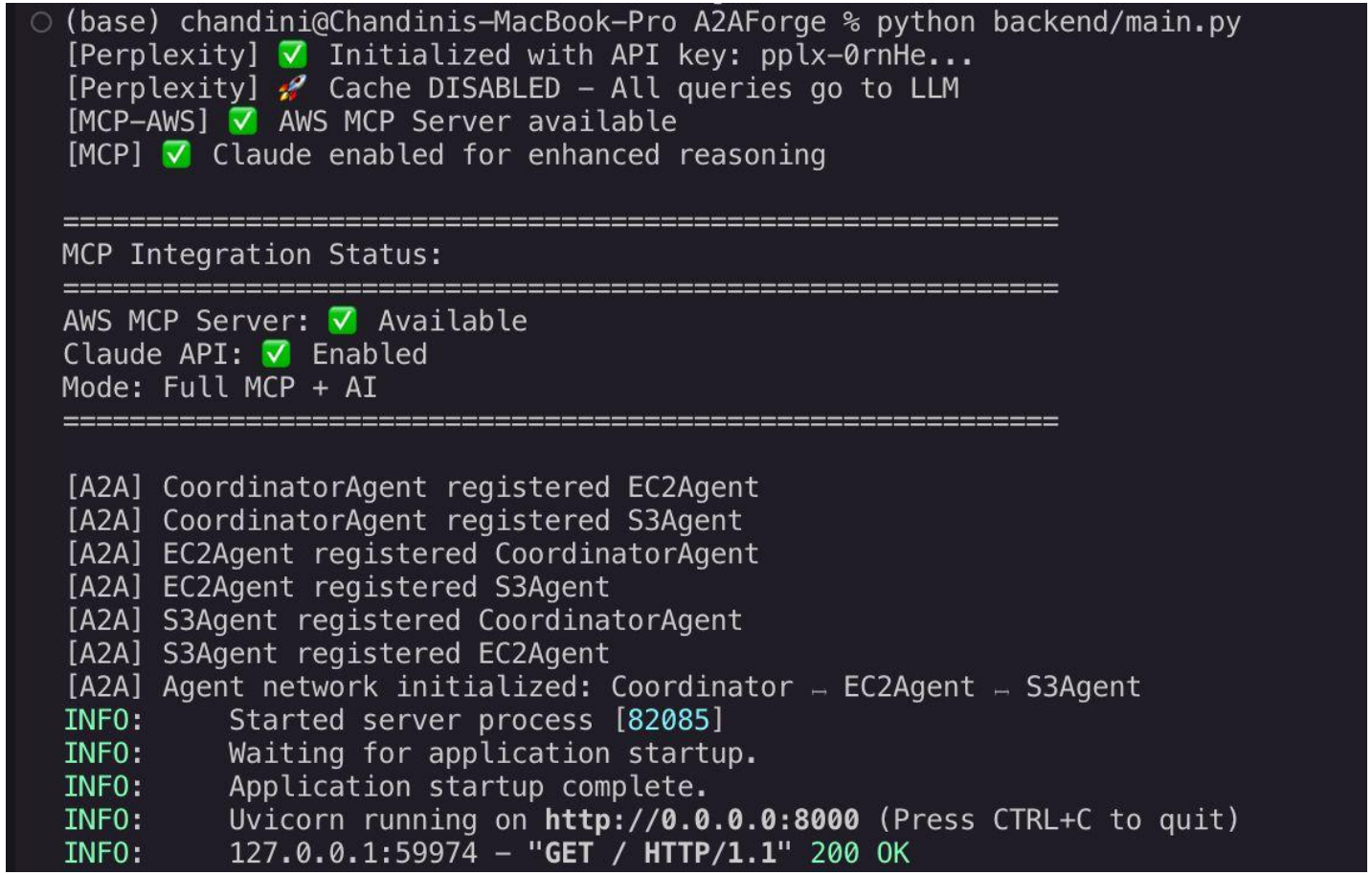
Architecture



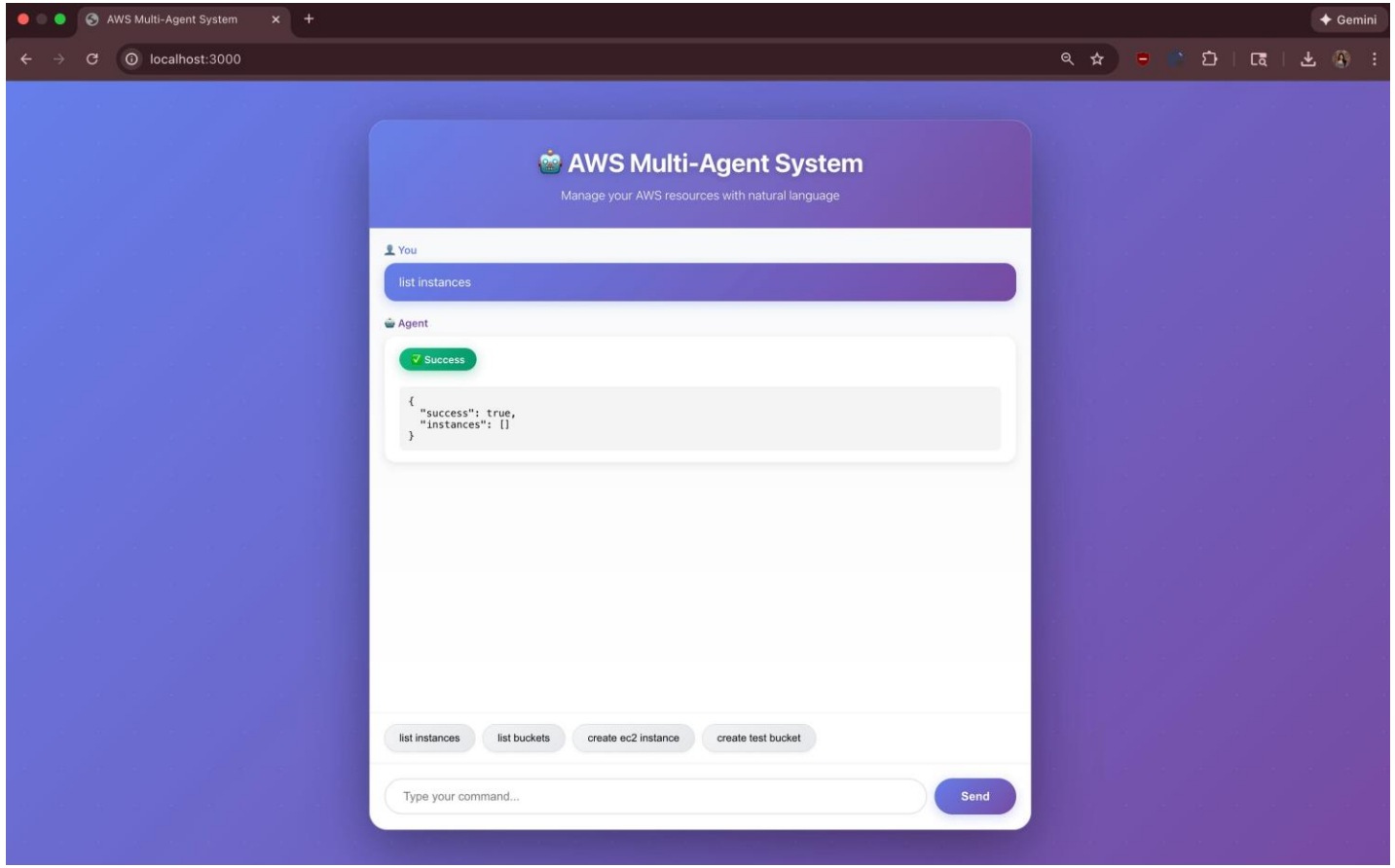
A2A Communication Flow

- **How Agents Communicate in A2AForge**
- **User Issues Command -** Natural language input (e.g., *“Create an EC2 instance.”*)
- **Coordinator Agent Interprets Intent -** Extracts required parameters, Determines which agent is responsible
- **A2A Message Exchange Begins -** Coordinator sends structured messages to EC2/S3 agents, Agents can request clarification or data from each other, Agents share context and collaborate autonomously
- **Tool Execution via MCP -** MCP allows agents to securely execute AWS actions, Ensures safe, isolated tool usage
- **AWS Performs the Operation**
- Example: Launch EC2, create S3 bucket, list resources
- **Final Response Returned to User**
- Clear, human-readable result

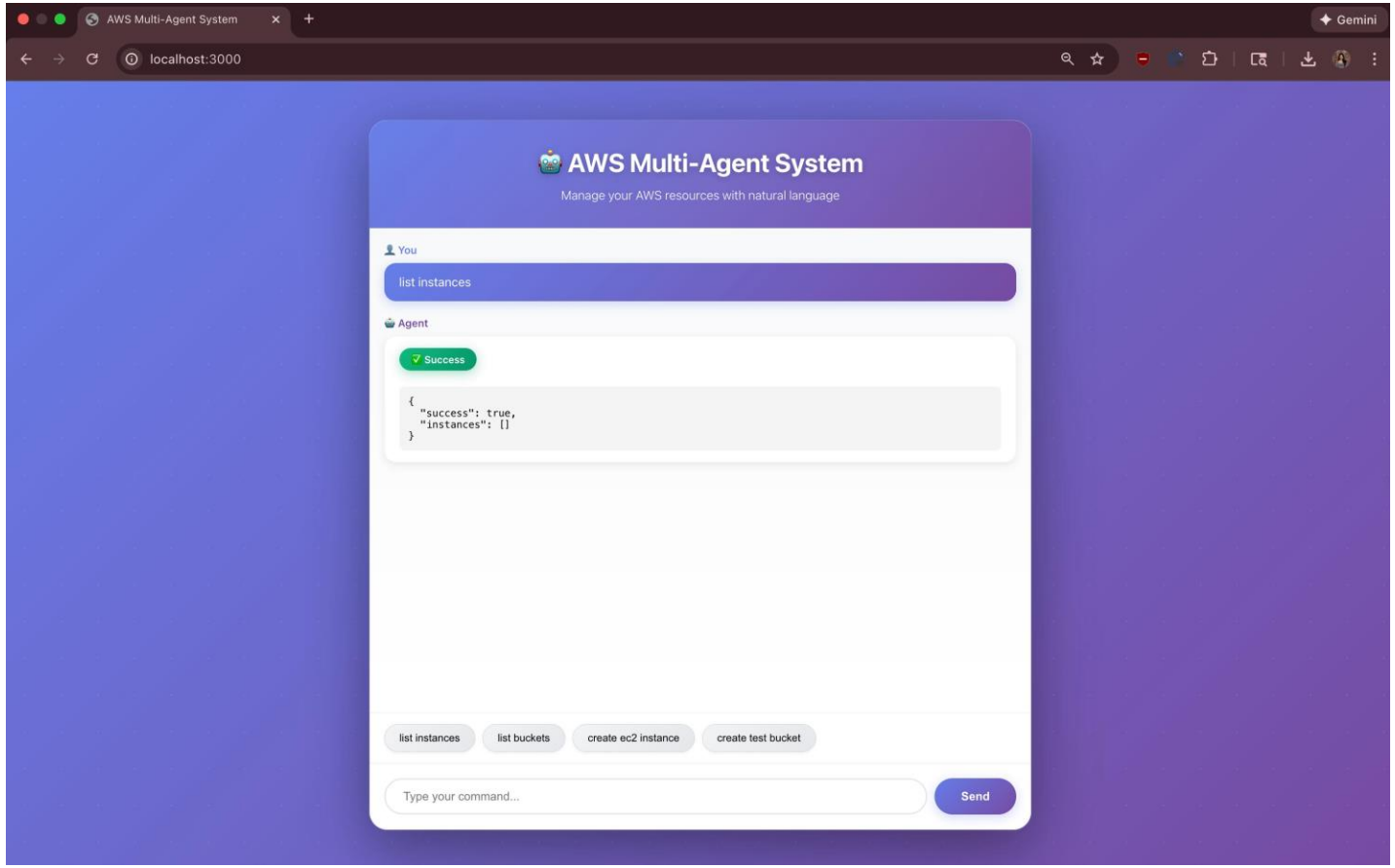
Output Screens



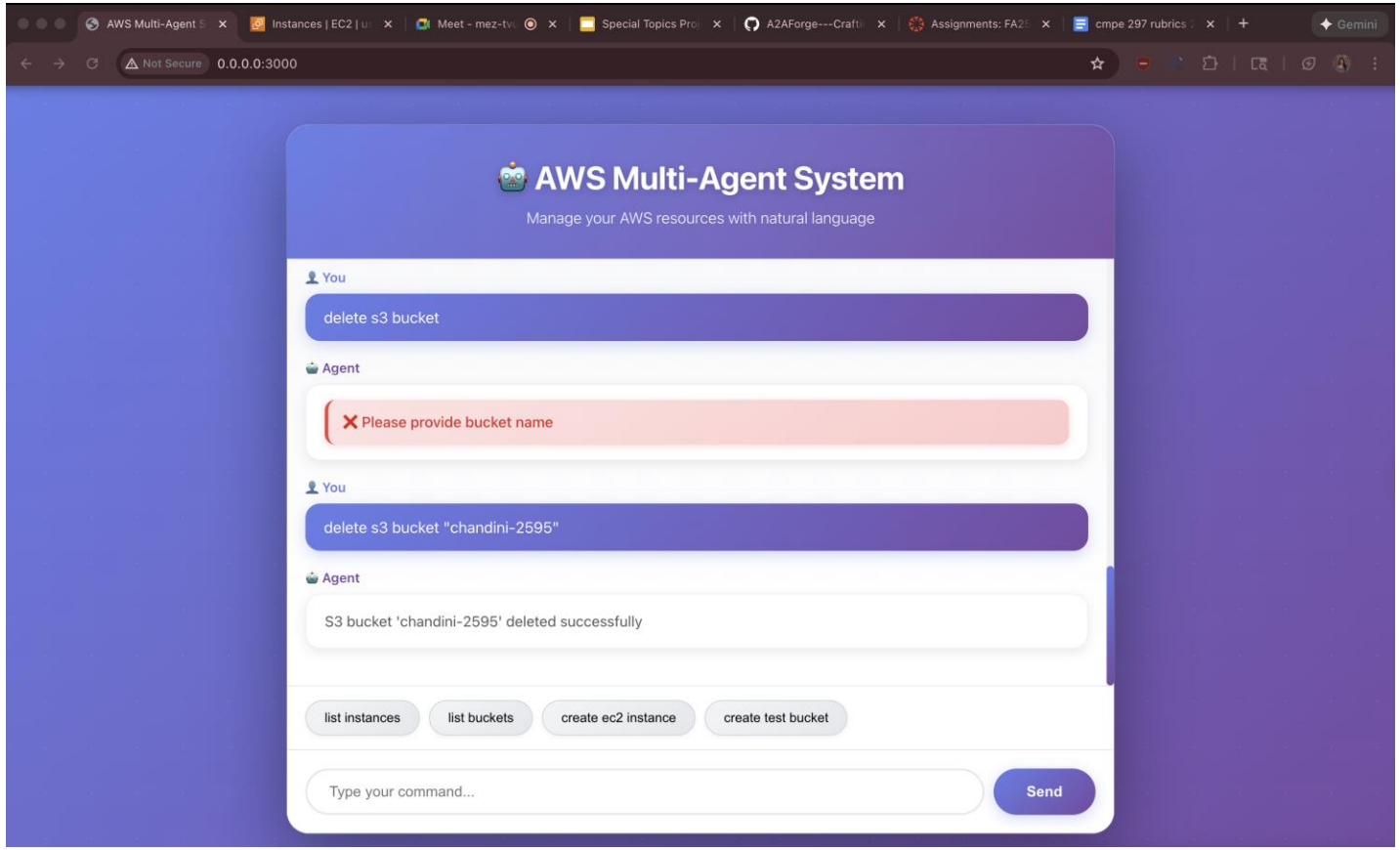
List Instances



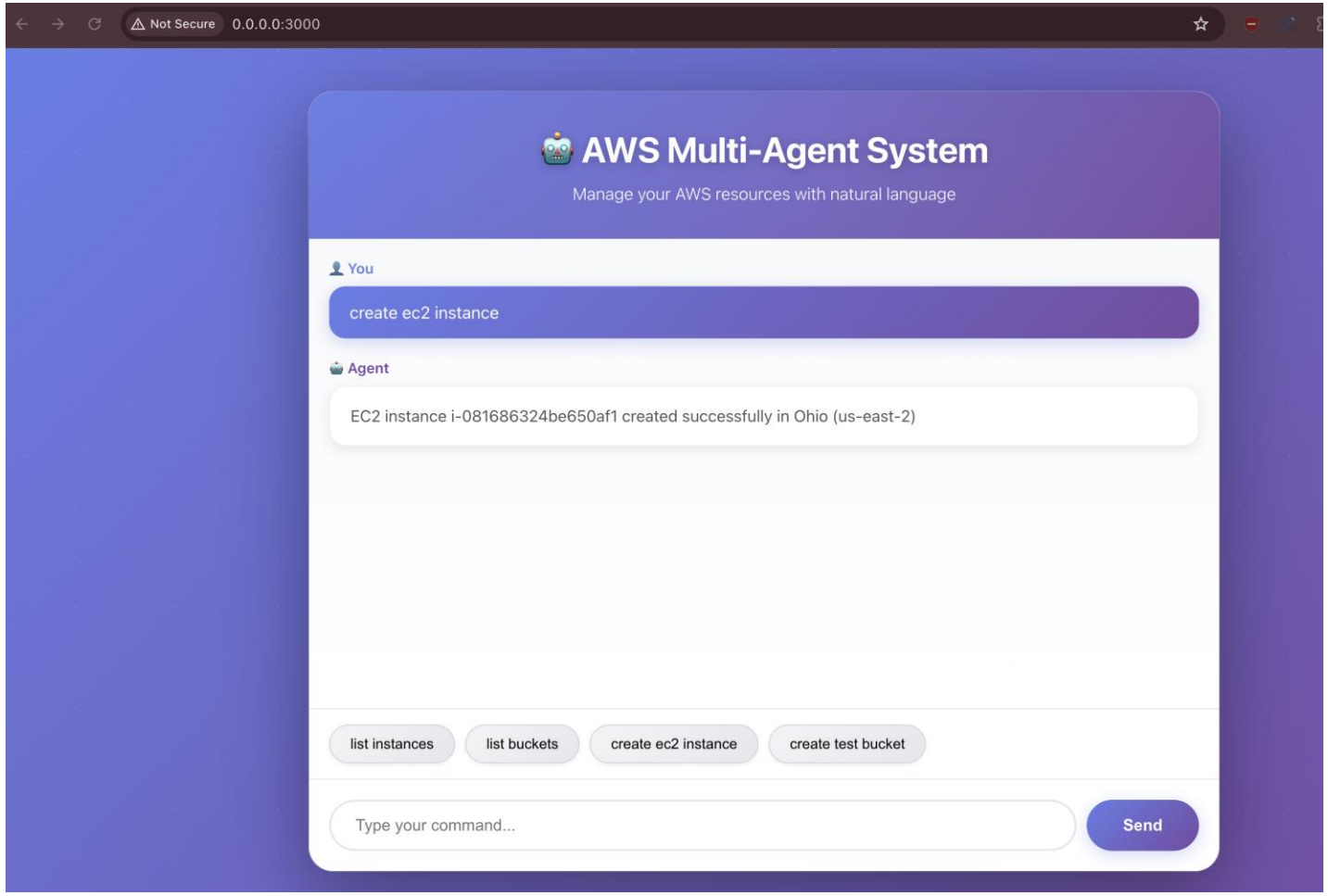
Create S3 bucket

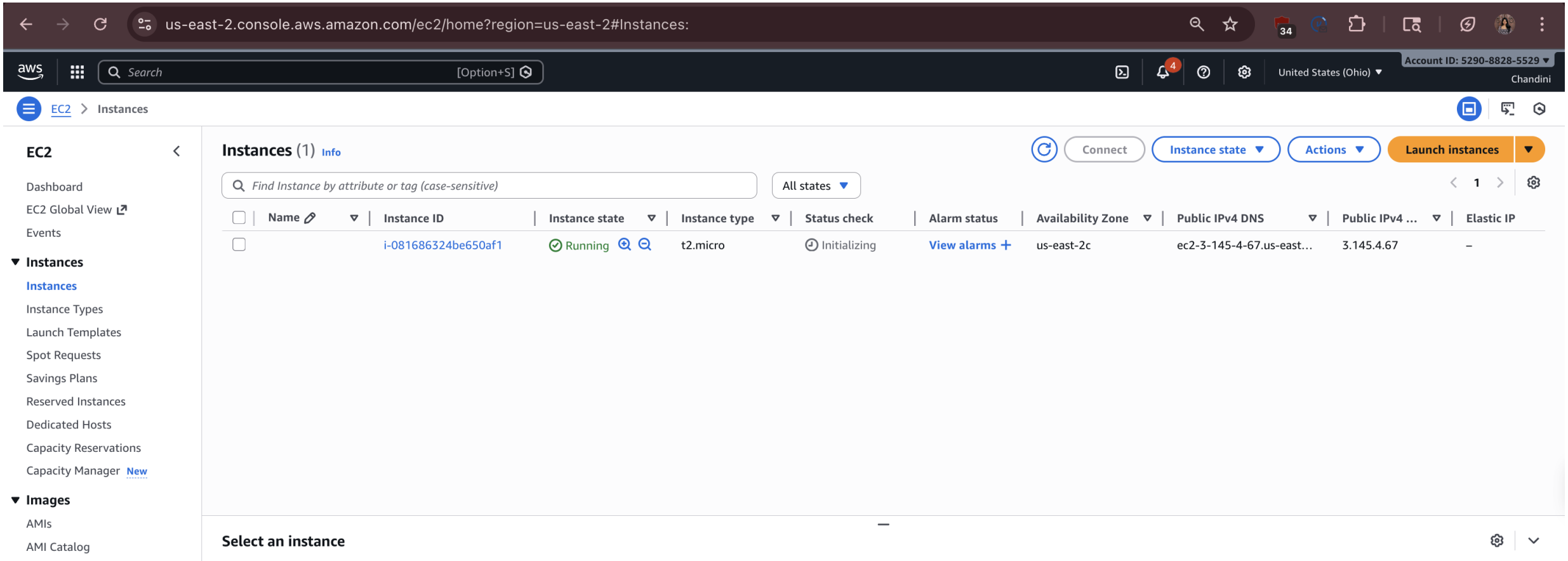


Delete S3 bucket

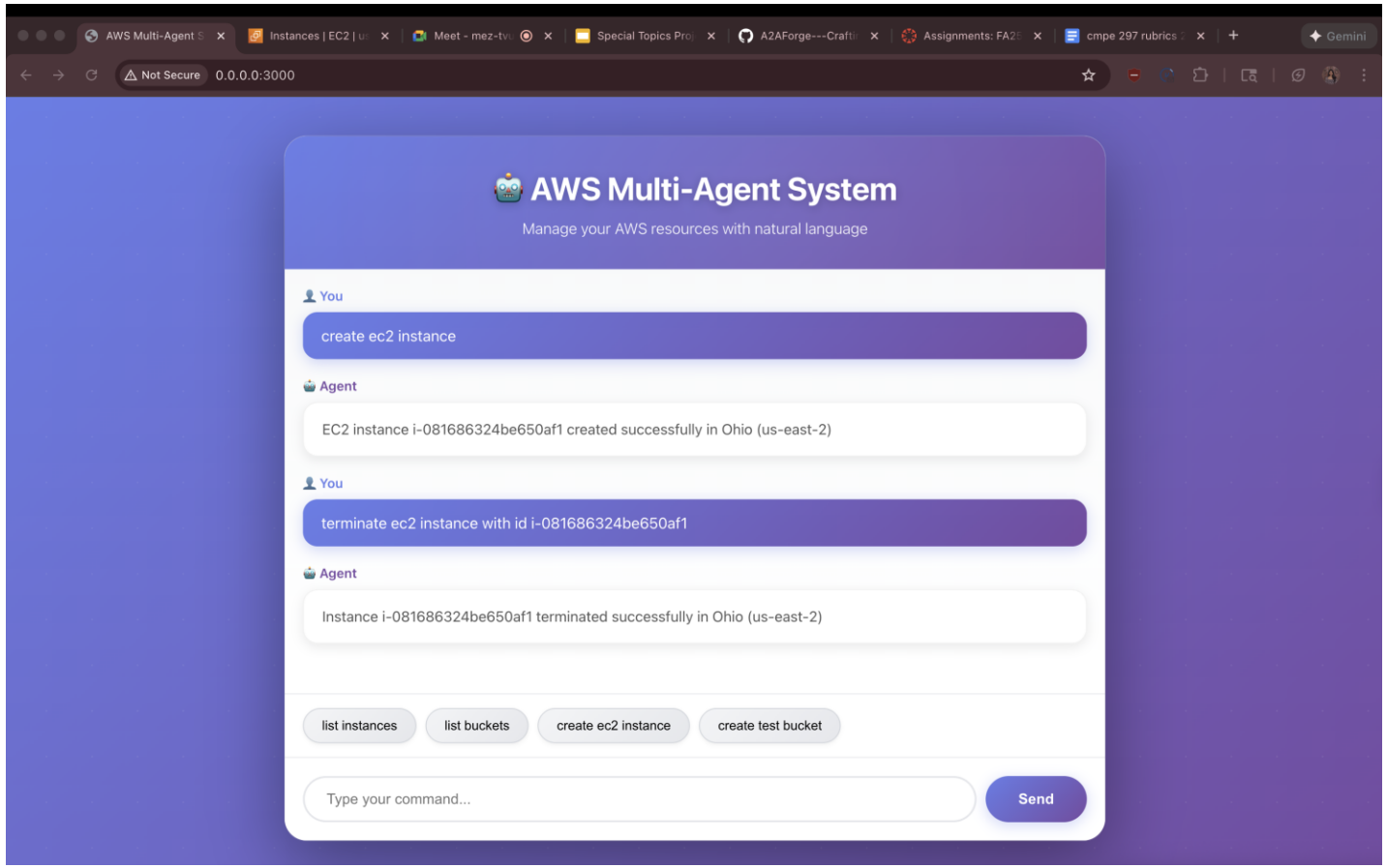


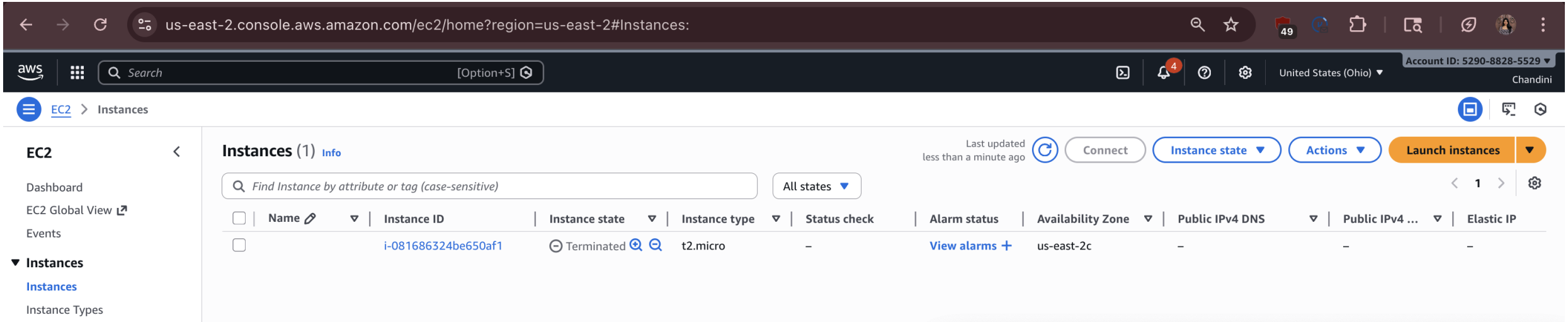
Create EC2 instance




us-east-2.console.aws.amazon.com/ec2/home?region=us-east-2#Instances:
aws
Search
[Option+S]
United States (Ohio)
Account ID: 5290-8828-5529
Chandini
EC2
Instances
EC2
Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Capacity Manager New
Images
AMIs
AMI Catalog
Instances (1) Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
1
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4 DNS
Public IPv4 ...
Elastic IP
i-081686324be650af1
Running
t2.micro
Initializing
View alarms
us-east-2c
ec2-3-145-4-67.us-east...
3.145.4.67
–
Select an instance

Terminate EC2 instance




us-east-2.console.aws.amazon.com/ec2/home?region=us-east-2#Instances:
aws
Search
[Option+S]
United States (Ohio)
Account ID: 5290-8828-5529
Chandini
EC2 > Instances
EC2
Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Instances (1) Info
Last updated less than a minute ago
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
1
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4 DNS
Public IPv4 ...
Elastic IP
i-081686324be650af1
Terminated
t2.micro
–
View alarms
us-east-2c
–
–
–

Conclusion

A2AForge: The Future of Cloud Automation

- Demonstrates how **multi-agent AI systems** can transform cloud operations
- Simplifies AWS management through **natural language interaction**
- Leverages **A2A protocol** and **MCP** to enable autonomous, collaborative agents
- Delivers a scalable, modular framework for EC2, S3, and future cloud services
- Reduces human effort, minimizes errors, and accelerates DevOps workflows

Key Takeaway

- **A2AForge proves that cloud infrastructure can be managed intelligently - not through commands, but through conversations.**

Looking Ahead

- Expanding agents (Lambda, IAM, CloudWatch, RDS)
- Advanced cost monitoring and rollback capabilities
- Secure, production-grade web UI
- Full multi-agent orchestration for enterprise DevOps

Thank you !