The Managed Harness

Define an agent. Skip the orchestration code.

Amazon Bedrock AgentCore

Elizabeth Fuentes Leone

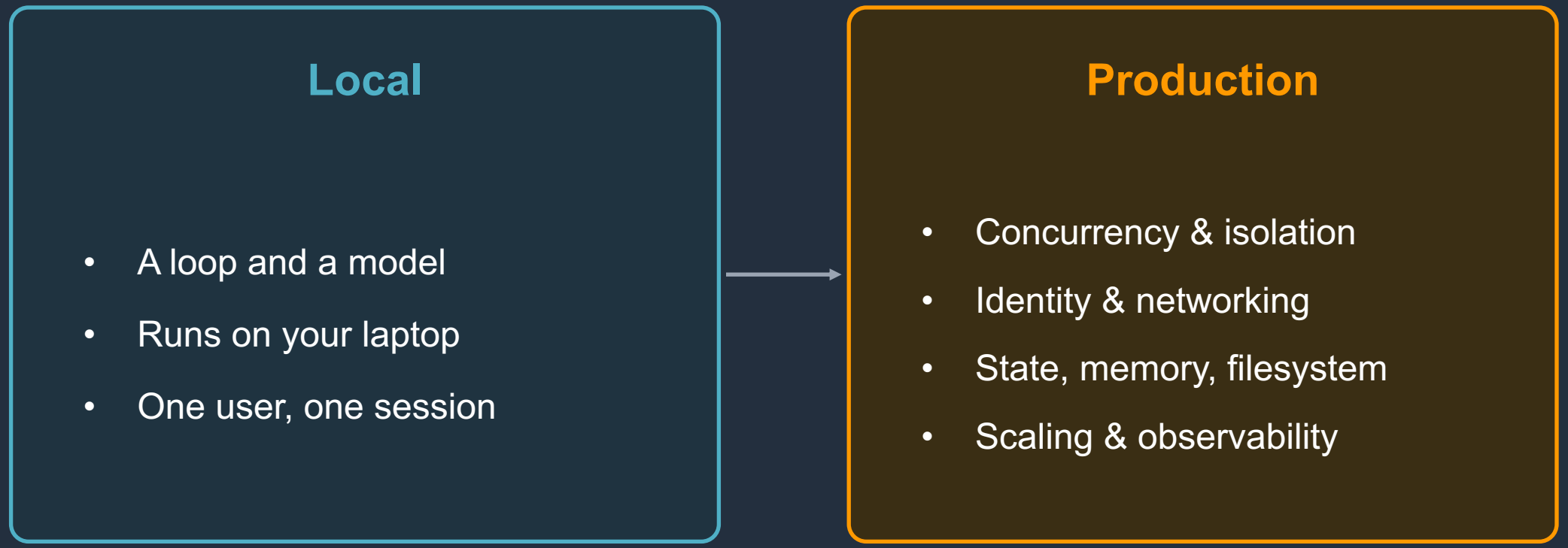
Developer Advocate @ AWS

GenAI · 107+ articles on dev.to · MS Data Science · EN/ES

The Agent Loop

What every agent needs to run

Local Is Easy. Production Explodes.



Until now, every team built this layer themselves.

What You Get Out of the Box

No orchestration code. Just config.

Isolated microVM

Own sandbox, shell, filesystem

Built-in Memory

Cross-session recall, zero config

Persistent Storage

Mount S3 / EFS, survives restarts

Switch Models Mid-Session

Swap model or prompt, no rebuild

Direct Shell Access

Run commands, write & execute code

It's Configuration, Not a Rewrite

Any Model

Bedrock, OpenAI, Gemini, any LiteLLM provider

Any Tool

Gateway, MCP servers, browser, code interpreter

Skills on Demand

Attach from Git, S3, or the curated AWS skills catalog

Traced Automatically

Every action, one unified observability view

Trying a different model or adding a tool is a config change.

Managed Harness in AgentCore

From idea to running agent in 3 steps

Define your agent

`model + tools + prompt`

Deploy

`agentcore deploy`

Invoke

`agentcore invoke`

Key Takeaways

Declare	Define the agent — model, tools, prompt — and skip the orchestration code.
Isolate	Every session runs in its own secure microVM with shell, filesystem, and memory.
Swap	Change model, prompt, or tools as a config change — no rewrite, no redeploy.
Operate	Versions, named endpoints, and automatic tracing make rollout and debugging safe.

Thank you!

Elizabeth Fuentes Leone

Developer Advocate @ AWS

Powered by open-source Strands Agents

Resources

bit.ly/4vXltMt

Blog & Socials

elifuentes.tech