

MYCLOUDSKILL · AI 101

AI for beginners

From "what is AI?" to letting Claude build
on AWS for you

Presented by Ganesh · Tamil Techies community



STEP 1 · WHAT IS AI?

AI = computers doing things that normally need a human brain



See

Face unlock



Hear

Voice assistants



Understand

Translate
languages



Decide

Netflix suggestions



Create

Write, draw,
compose

Old computers: follow rules

A person writes every step. If something new happens, the computer is stuck.

Modern AI: learns from examples

Like a child who learns "mango" by seeing many mangoes, not by reading rules. This is called **machine learning**.

Generative AI = AI that creates something new

Older AI

Recognizes and decides

"Is this email spam?" → Yes

Generative AI

Creates something brand new

"Write a birthday poem for Amma" → a new poem



Text



Images



Code



Music



Video

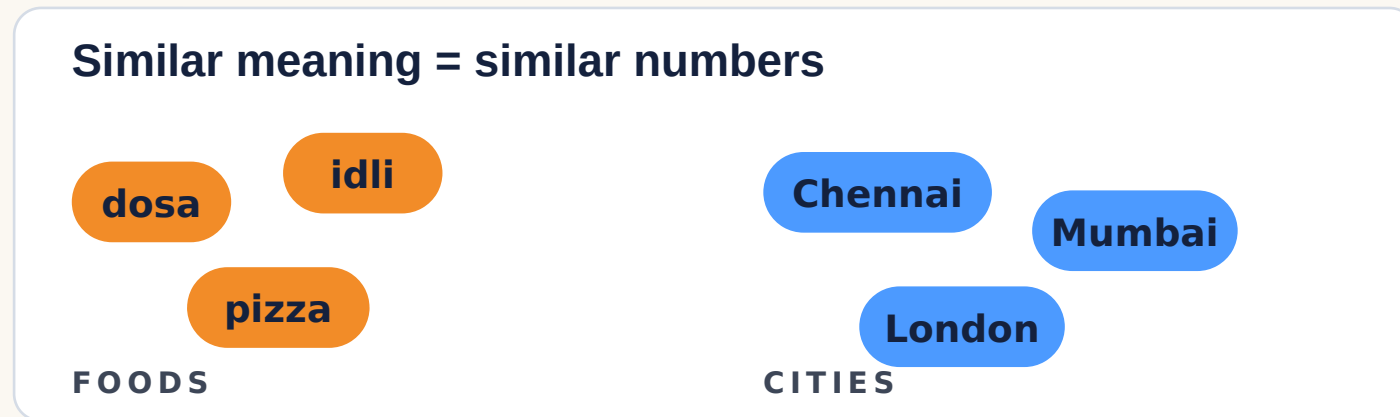
How? It studied millions of examples, so it can make new ones in the same style.

STEP 3 · HOW AI UNDERSTANDS

AI understands only one thing: numbers



"I love dosa" → pieces → numbers → meaning



Inside AI, it's all math

Numbers go in → math happens → numbers come out → turned back into words for you.

LLM: the brain inside ChatGPT, Claude and Gemini

L

Large

Learned by reading a huge library: much of the internet, books, articles

L

Language

Works with words: reads, writes, explains

M

Model

What's left after learning: billions of numbers

Its one skill: guess the next word

"Every morning I drink a cup of ____"



Pick one, add it, guess again. Very fast → full answers.

ChatGPT, Claude and Gemini: chat apps with an LLM brain



ChatGPT

by OpenAI · 2022

Started the AI boom. Hit 1 million users in 5 days.



Claude

by Anthropic · 2023

Strong at writing and coding. Anthropic created MCP. Our tool for this course.



Gemini

by Google · 2023

Built into Google products like Search and Gmail.

On their own, they can only chat. Give them **knowledge** and **tools**, and they can do real work. Let's see how →

RAG: let the AI look things up before it answers

Without RAG: a closed-book exam

The LLM answers only from memory. It doesn't know your files or today's news, and may guess wrong.

With RAG: an open-book exam

The AI first looks up the right pages in your documents, then answers from them.



1 · You ask

"What's our refund policy?"



2 · Find

Search your documents for the right pages



3 · Add

Hand those pages to the LLM with your question

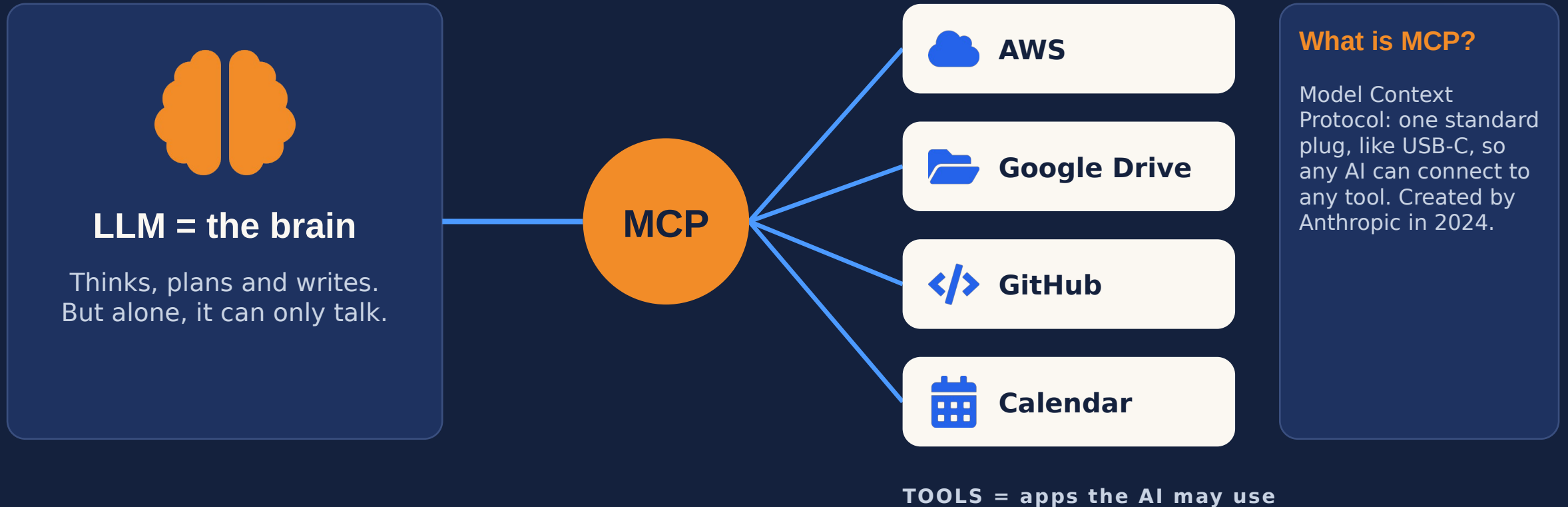


4 · Answer

Based on your documents, with sources

RAG = **R**etrieval (find) + **A**ugmented (add) + **G**eneration (answer)

The LLM is the brain. MCP connects it to tools.

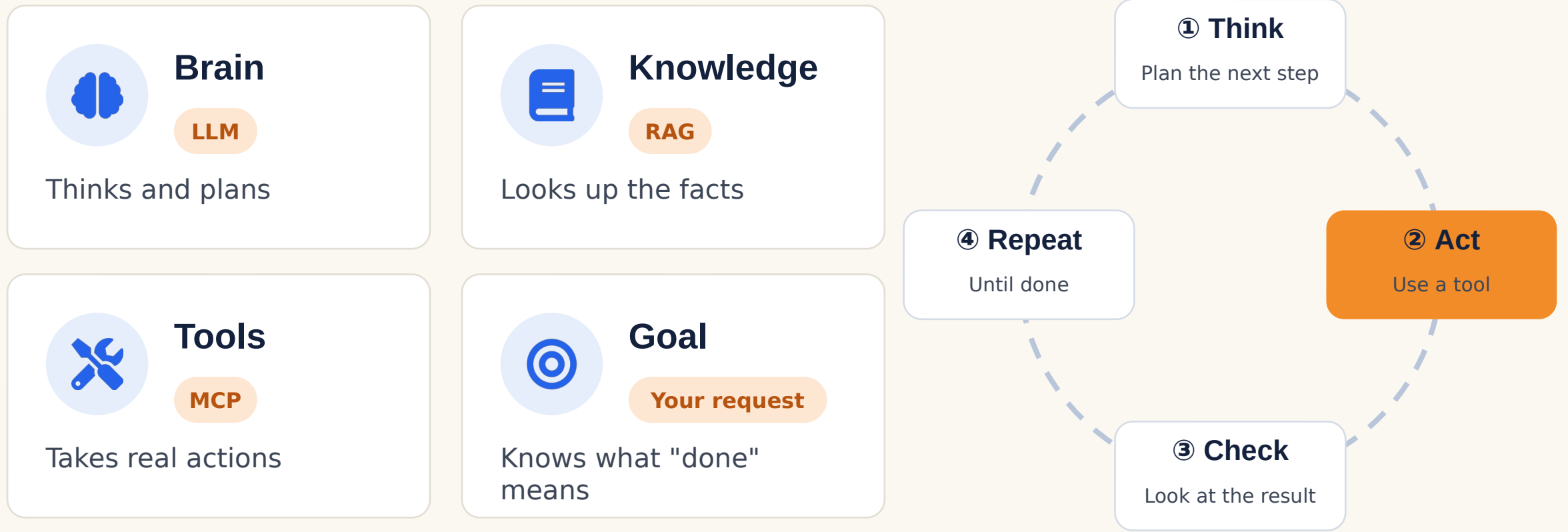


Brain (LLM) + nervous system (MCP) + hands (tools) = an AI that can actually do things

STEP 8 · WHAT IS AN AGENT?

Agent: an AI that gets the job done, step by step

A chatbot answers. An agent takes action, step by step, until the job is done.



The AI stack, explained like a human body



1 · LLM

= the brain

Understands, writes and reasons. Only knows what it learned in training.

In our course
Claude's model



2 · RAG

= brain + library

Looks up your documents before it answers.

In our course
Reading AWS docs before advising

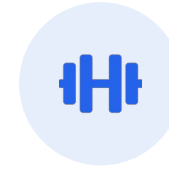


3 · MCP

= the nervous system

Carries signals between the brain and tools. One standard plug.

In our course
The AWS MCP Server



4 · Skills

= muscle memory

Saved know-how for tasks you repeat. Used only when needed.

In our course
"How we set up a website on AWS"



5 · Agent

= brain + hands

Plans the steps itself, then uses tools to act, not just answer.

In our course
Claude creating your S3 bucket

Brain thinks · library informs · nerves connect · muscle memory repeats · hands act

A good question gets a good answer

Weak prompt

“Write about S3.” → a vague, generic answer

Strong prompt

“You're an AWS trainer. Explain Amazon S3 to a complete beginner in 5 bullets, with one everyday example and one command I can try.”



Role

Tell it who to be: “You're an AWS trainer”



Task

Say exactly what you want done



Context

Who it's for and what you already know



Format

Bullets, a table, how long, an example

Not quite right? Just reply and refine — talking to AI is a conversation, not a one-shot search.

Use AI with your eyes open



Verify everything

AI can “hallucinate”: sound confident and still be wrong. Check facts, numbers and code.



Never paste secrets

No passwords, AWS access keys or bank details in a chat.



Protect personal data

Leave out other people's private information.



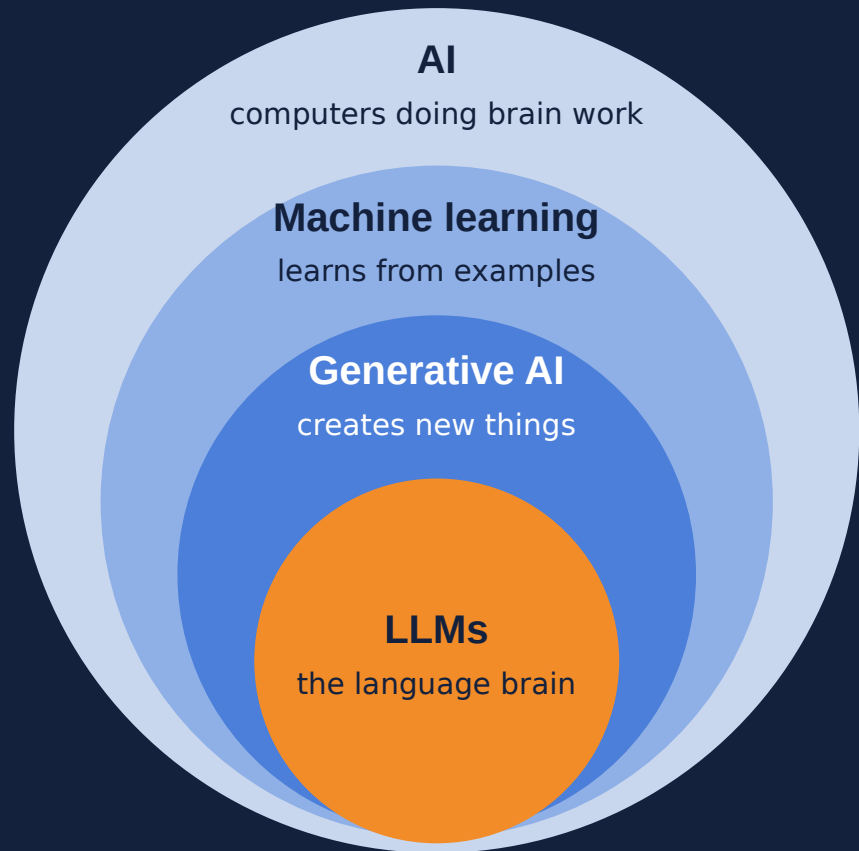
You make the call

AI suggests; you approve what actually happens — especially on AWS.

Think of AI as a smart new intern: fast and helpful, but you always double-check its work.

THE BIG PICTURE

Putting it all together



THE RECIPE FOR AN AGENT



LLM the brain: thinks and writes



RAG the library: looks things up



Tools via MCP nerves + hands: takes real actions



Skills muscle memory: know-how for repeat tasks



Your goal what "done" looks like

= an AI agent that gets real work done

Remember: it all runs on numbers. Next session: install Claude and build on AWS together. **Questions?**

Hands-on: Claude creates AWS resources for us

You



Claude (the brain)



AWS MCP Server (the tool)



Your AWS account

1 Install Claude Code

Claude Code = Claude on your computer, able to take actions. Paste into the **terminal** (the window for typing commands):

Mac / Linux

```
curl -fsSL  
https://claude.ai/install.sh |  
bash
```

Windows (PowerShell)

```
irm https://claude.ai/install.ps1  
| iex
```

Then type `claude` and sign in. Needs Claude Pro or higher.

2 Connect AWS MCP

One line gives Claude its AWS "hands":

```
claude mcp add aws-mcp  
https://aws-mcp.us-east-  
1.api.aws/mcp --transport http
```

First time: AWS asks you to sign in in your browser. The MCP server is free; you pay only for what you create.

3 Just ask

"Create an S3 bucket (a storage folder) called my-first-bucket."

Claude plans it, asks your OK, creates it, and confirms ✓

You approve every action, so nothing happens without your say-so.

Brain (Claude) + tool (AWS MCP) + goal (your request) = an AWS agent

The AWS MCP Server, at a glance

15,000+

AWS actions Claude can call

Free

no extra charge — pay only for what you create

May 2026

generally available from AWS



call_aws

Runs any AWS action, using your own permissions



run_script

Runs a short Python script in a safe sandbox



AWS docs

Reads the latest AWS documentation before it advises (RAG!)



Skills

Step-by-step playbooks written by AWS teams (muscle memory!)

Every call is logged in AWS CloudTrail, so you can always see what Claude did.

Two ways to connect — pick one



OAuth

Recommended for this course

- ✓ Sign in to AWS in your browser
- ✓ No AWS keys saved on your laptop
- ✓ Needs one IAM policy (Step 1)
- ✓ Works in Claude Code and Claude Desktop



SigV4 via proxy

Advanced

- ✓ Uses your AWS CLI sign-in
- ✓ Needs AWS CLI 2.32+ and uv
- ✓ Switch between several AWS accounts
- ✓ Runs a small helper on your computer

In class we use OAuth. Choose SigV4 only if you already use the AWS command line or manage several accounts.

Get ready before you connect



An AWS account

Set a billing alert first — Free Tier is enough



An IAM user, not root

We give it permissions in Step 1



Claude Pro or higher

Claude Code or Claude Desktop installed and signed in



SigV4 only: AWS CLI 2.32+ and uv

Check your version with: `aws --version`

SigV4 only

Install uv

```
# Mac / Linux
curl -LsSf https://astral.sh/uv/install.sh | sh
# Windows (PowerShell)
irm https://astral.sh/uv/install.ps1 | iex
```

Sign in to AWS and check it worked

```
aws login
aws sts get-caller-identity
```

Give your IAM user the right permissions

1 Allow AWS sign-in for MCP (required for OAuth)

```
aws iam attach-user-policy --user-name mcs-student \  
--policy-arn arn:aws:iam::aws:policy/AWSMCPSignInOAuthAccessPolicy
```

2 Start read-only — Claude can look around but can't change anything

```
aws iam attach-user-policy --user-name mcs-student \  
--policy-arn arn:aws:iam::aws:policy/ReadOnlyAccess
```

Prefer clicking? IAM → Users → your user → Add permissions → Attach policies directly → search each policy name.

Replace mcs-student with your IAM user name. Using a role instead? Use attach-role-policy.

Connect Claude Code to AWS

OAuth · recommended

Paste into your terminal — one line:

```
claude mcp add aws-mcp https://aws-mcp.us-east-1.api.aws/mcp --transport http
```

SigV4

Run aws login first, then:

```
claude mcp add-json aws-mcp --scope user '{"type":"stdio","command":"uvx",  
  "args":["mcp-proxy-for-aws-cli@latest","https://aws-mcp.us-east-1.api.aws/mcp",  
  "--metadata","AWS_REGION=us-east-1"]}'
```

Check it: `claude mcp list` · Run only ONE of the two commands above.

Or connect Claude Desktop

OAuth · recommended

- 1 Open Settings → Connectors
- 2 Choose Add custom connector
- 3 Paste this address:

```
https://aws-mcp.us-east-1.api.aws/mcp?oauth=initialize
```
- 4 Sign in to AWS when your browser opens

SigV4

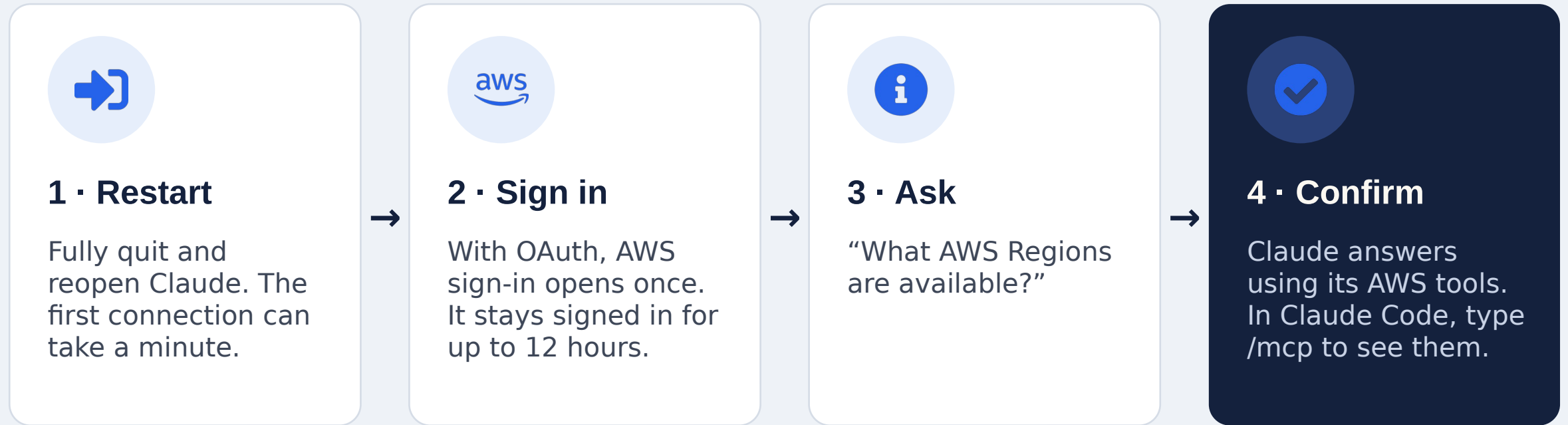
Edit `claude_desktop_config.json`

```
{
  "mcpServers": {
    "aws-mcp": {
      "command": "uvx",
      "args": [
        "mcp-proxy-for-aws-cli@latest",
        "https://aws-mcp.us-east-1.api.aws/mcp",
        "--metadata", "AWS_REGION=us-east-1"
      ]
    }
  }
}
```

Mac: ~/Library/Application Support/Claude/

Windows: %APPDATA%\Claude\ · then fully quit and reopen Claude

Check that it works



Connected? You've just given Claude its AWS “hands”. If not, see the troubleshooting slide.

Your first prompts — just ask



Read-only

“List my S3 buckets and the Region each one is in.”



Read-only

“Which EC2 servers are running right now, in any Region?”



Read-only

“How much did I spend on AWS last month, by service?”



Needs write access

“Create an S3 bucket called my-first-bucket and host a simple web page in it.”

Claude plans it → asks your OK → does it → confirms ✓

Stay safe before you let Claude build



Least privilege

Start read-only. Add write access per service, only when needed.



Read before you approve

Check what Claude plans to do before you click Allow.



Budget alert

An AWS Budgets alarm emails you before costs surprise you.



Audit trail

CloudTrail records every action the agent takes.



Golden rule

Claude can only do what your IAM user allows. Control the permissions, and you control the agent.

If something goes wrong

You see	What to do
400 error after AWS sign-in	Attach <code>AWSMCPSignInOAuthAccessPolicy</code> to your IAM user (Step 1)
<code>ExpiredTokenException</code>	Run <code>aws login</code> again, then restart Claude
<code>UnrecognizedClientException</code>	Run <code>aws sts get-caller-identity</code> ; if it fails, sign in again
<code>InvalidSignatureException</code>	Fix your computer's clock — it must be within 5 minutes of AWS time
AWS server doesn't show up	Check the settings file for typos, then fully quit and reopen Claude

WHAT'S NEXT

You're ready to build on AWS with Claude

1

Claude

the brain that plans

2

AWS MCP

the hands that act

3

You

the boss who approves

Keep learning: MyCloudSkill AWS certification cohorts · mycloudskill.com

Questions?

