



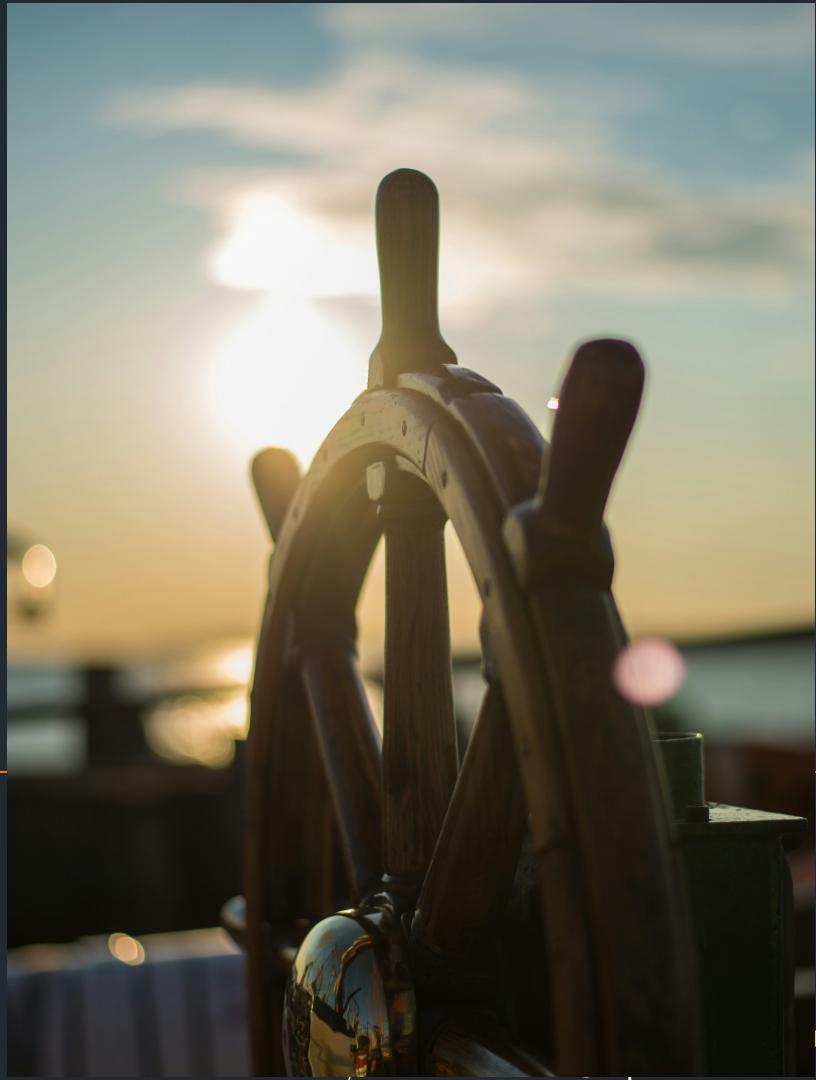
FRANCE API

Du design à la production:

**Meilleures pratiques pour la
gouvernance.**



Isabelle MAUNY - Field CTO

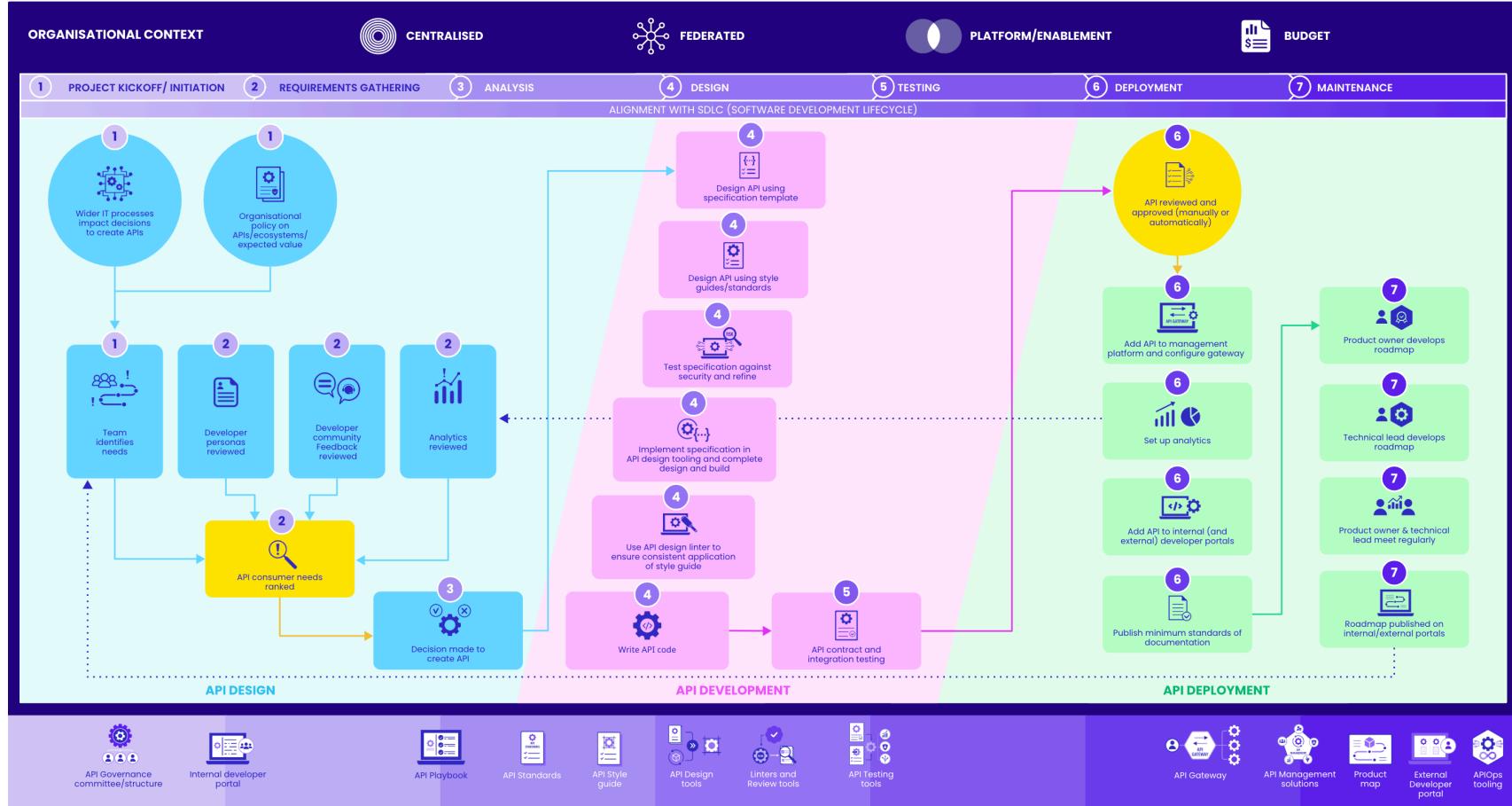


THINKING OF GOVERNANCE?

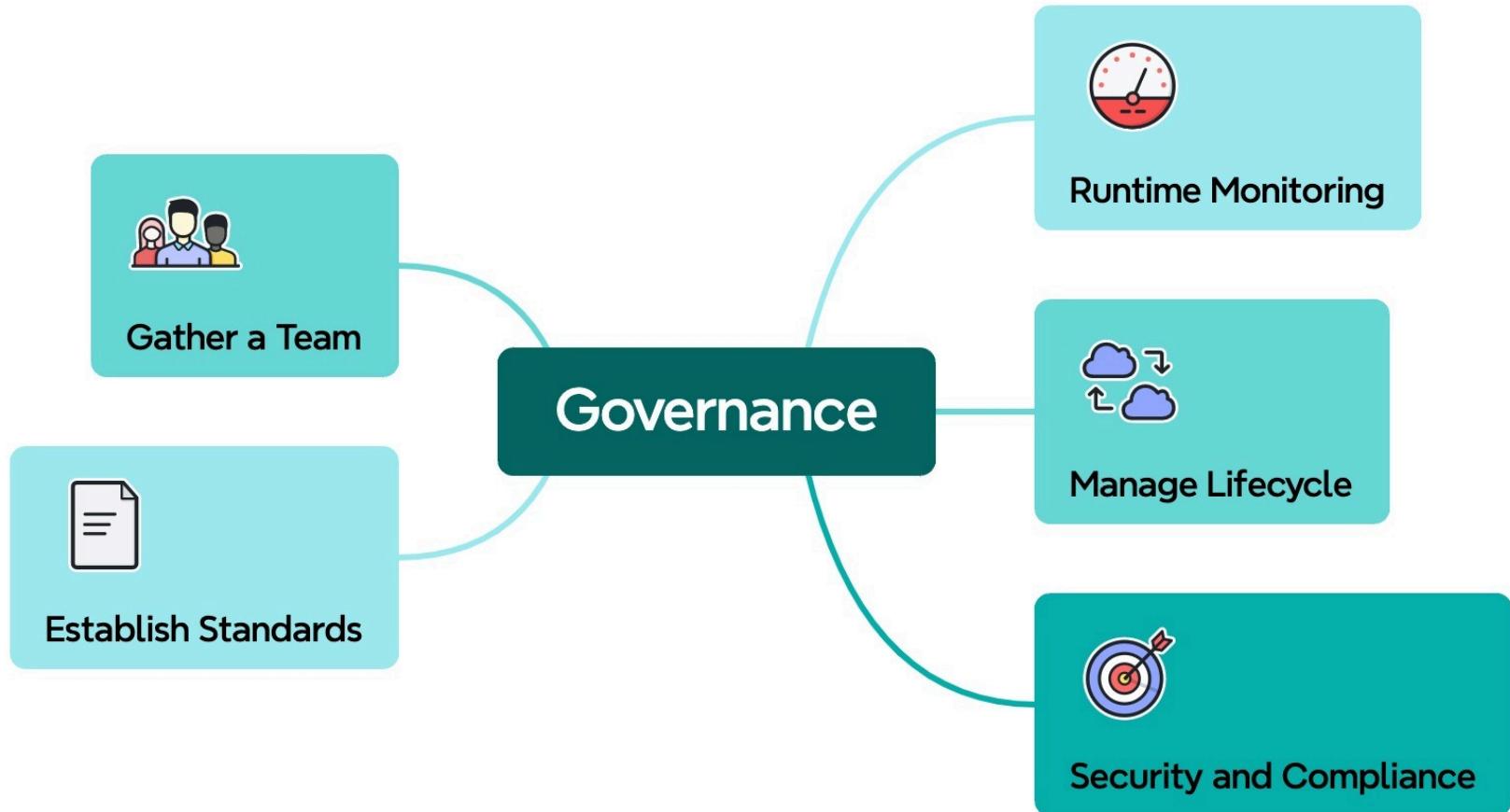


A cartoon illustration of a young boy with brown hair, wearing a white t-shirt, sitting in a dental chair. He is smiling broadly and giving a thumbs-up with both hands. In the background, there is a dental light fixture and a tray with various dental instruments like mirrors and探子. The background is a light blue with white sparkles.

**THINKING OF
GOVERNANCE** 😢



<https://platformable.com/products/api-governance>



DEV, ARCHITECTURE, SECURITY, OPS - YOU NEED EVERYONE!



IT ALL STARTS WITH GUIDELINES.. YOUR GUIDELINES!

adidas API Guidelines

[adidas API Guidelines](#)

GENERAL GUIDELINES

Introduction

API First

Contract

Immutability

Robustness

Common Data Types

Version Control System

Minimal API Surface

Rules for Extending

JSON

adidas API Guidelines



License [MIT ↗](#)

[Read online at GitBook ↗](#)

Motivation

The goal of this document is to facilitate the work and minimize the effort of all API users at adidas while protecting their investment and encouraging API First adoption.

These guidelines lay down the foundation for collaboration, stability, and extensibility.

**GOT A
PDF? AI TO
THE
RESCUE.**

(TOOK 2 ATTEMPTS
THOUGH)

Adidas API Guidelines to Spectral Rules

IM Adidas has provided a set of public guidelines here: <https://github.com/adidas/api-guidelines/tree/master/rest-api-guidelines> - Could you turn those into actionable spectral rules?

I'll fetch the Adidas API guidelines and convert them into actionable Spectral rules for you.

Fetched api-guidelines/rest-api-guid... github.com

Let me try to access the raw content directly:

Failed to fetch https://raw.githubusercontent.com/adidas/api-guidelines/master/rest-api-guidelines/index.json

Let me search for the Adidas API guidelines content:

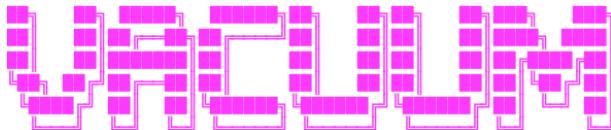
adidas api guidelines rest specifications 10 results

Sonnet 4

```
# Adidas API Guidelines – Comprehensive Spectral Ruleset
# Based on https://adidas.gitbook.io/api-guidelines/
extends:
  - [[spectral:oas, all], [spectral:asyncapi, all]]
documentationUrl: https://adidas.gitbook.io/api-guidelines/
functions:
  - kebab-case-check
  - camelCase-check
  - american-english-check
rules:
  # Disable some default rules that conflict with Adidas
  operation-tags: off
  operation-operationId: off
  operation-success-response: error
#
# =====
# CORE PRINCIPLES – OpenAPI Specification
# =====

adidas-api-description-required:
  description: "Every API MUST be described using Open"
  severity: error
```

ENFORCING STANDARDS



```
version: 0.17.0 | compiled: Sun, 08 Jun 2025 18:08:07 UTC
🔗 https://quobix.com/vacuum | https://github.com/daveshanley/vacuum
```

```
[INFO] Linting file 'OpenWeather.json' against 15 rules:
```

```
/Volumes/DATA/Projects/FranceAPI-2025/OASFiles/OpenWeather.json
```

Location	Severity	Message	Rule
OpenWeather.json:8:5	error	Declare intended audience of every server by defining servers{{property}} as true/false.	owasp:api9:2023-inventory-ac
OpenWeather.json:48:22	warning	Operation is missing {{property}}.	owasp:api8:2023-define-error-
OpenWeather.json:48:22	warning	Operation is missing {{property}}.	owasp:api8:2023-define-error-
OpenWeather.json:48:22	warning	Operation is missing {{property}}.	owasp:api8:2023-define-error-
OpenWeather.json:48:22	warning	Operation is missing {{property}}.	owasp:api8:2023-define-error-
OpenWeather.json:48:22	warning	Operation is missing rate limiting response in {{property}}.	owasp:api4:2023-rate-limit-re
OpenWeather.json:48:22	warning	Operation is missing rate limiting response in {{property}}.	owasp:api4:2023-rate-limit-re

```
Category | Errors | Warnings | Info
Validation | 1      | 6        | 0
```

```
Linting file 'OpenWeather.json' failed with 1 errors, 6 warnings and 0 informs
```

```
Error: failed with 1 errors
```

ENFORCING STANDARDS

PUBLISHER

WSO2 API MANAGER

OpenWeather :1.0

CREATED State

Current API ▾

Go To

Create New Version

Download API

Delete

Overview

Compliance

Develop

Portal Configurations ▾

API Configurations ⓘ ▾

Deploy

Deployments

Test

Try Out

Publish

Lifecycle

Search

Last updated: an hour ago

Compliance Summary

Policy Adherence



Followed (0)
Violated (2)
Pending (0)
Not Applied (0)

Ruleset Adherence



Passed (0)
Failed (4)
Unapplied (0)

Rule Adherence



Errors (3)
Warnings (20)
Info (0)
Passed (61)

ERRORS (3) WARNINGS (20) INFO (0) PASSED (61)

OWASP Top 10 (1) [API Definition](#) [View Documentation](#)

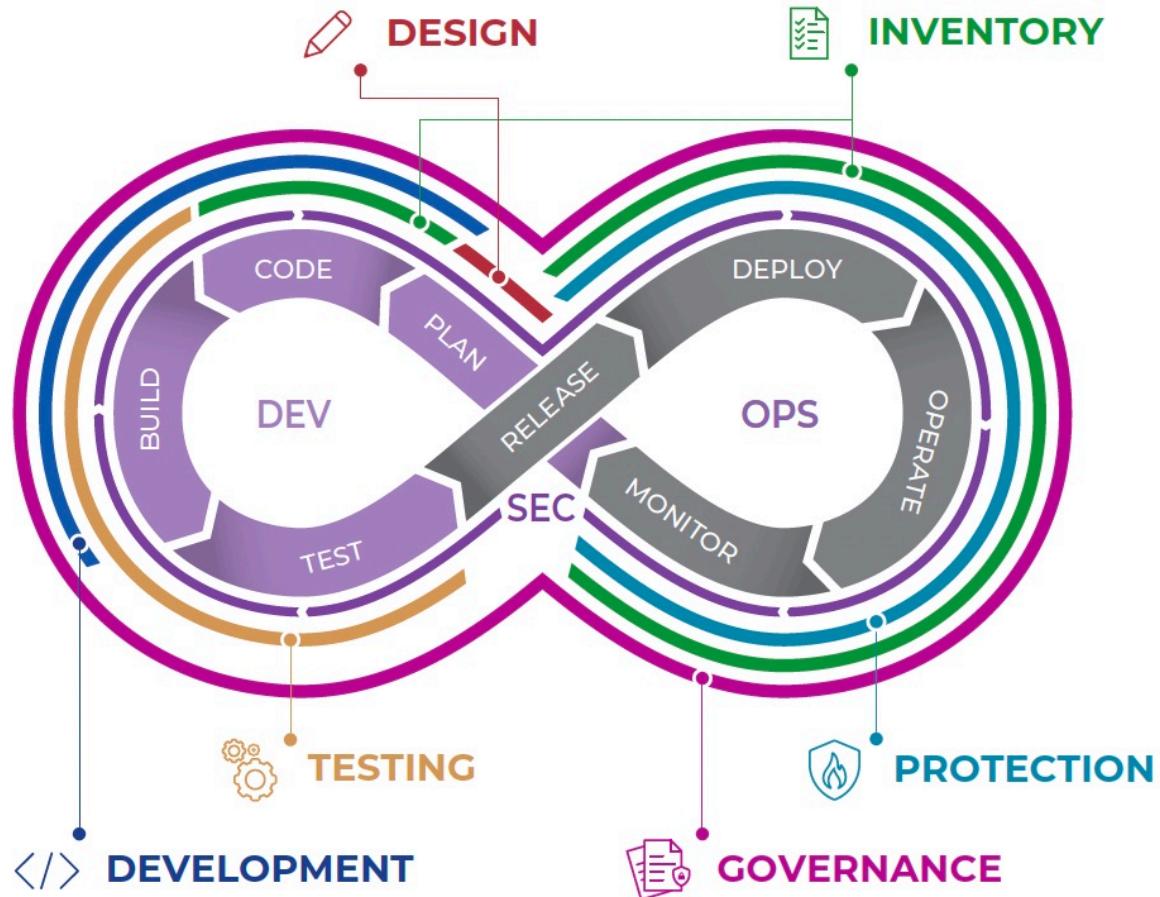
Adidas (1) [API Definition](#) [View Documentation](#)

WSO2 REST API Design Guidelines (1) [API Definition](#) [View Documentation](#)

DEMO TIME



**ACROSS THE
WHOLE
LIFECYCLE!!**





**TIME TO
AUTOMATE!**

WHAT DO WE AUTOMATE ?

- Compliance validation
- Breaking changes detection: **do we have a revision or a new version ?**
 - oas-diff (Azure)
 - wiretap (Quobix)
- **Security validations!!!**
 - OWASP Spectral rules as a base...

ERRORS == BUILD FAILED - FIX AND REPEAT

The screenshot shows a GitHub Actions run titled "GitHub Actions / Lint (push)" which failed 2 minutes ago. The "Lint (push)" job is highlighted. The run details include "Usage" and "Workflow file". Two annotations are displayed:

- Annotations**
 - Check warning on line 49 in OASFiles/OpenWeather.json**
github-actions / Lint (push)
owasp:api8:2023-define-error-responses-500
Operation is missing responses[500].
 - Check failure on line 9 in OASFiles/OpenWeather.json**
github-actions / Lint (push)
owasp:api8:2023-no-server-http
Server URLs must not use http://. Use https:// or wss:// instead.

A photograph of two young children, a boy and a girl, sitting at a desk and looking at a laptop screen. The boy on the left has his arms raised in excitement, while the girl on the right points her finger at the screen. They appear to be reacting to something on the computer.

DEMO TIME

THERE IS A MAJOR GOVERNANCE ISSUE IN THIS DEMO SETUP.
CAN YOU FIND IT?

(SECURE) CONTRACT TESTING!

- We have a contract with our **consumers**, are **we** respecting it?
- We have a contract with our **providers**, are **they** respecting it ?
- What if...
 - We get data we don't expect (format, value, extra properties, etc.)
 - Someone/something invokes a verb we don't support
 - What if...
- Base rule : 1 **Happy** test, 10 **Hacky** tests!
- **AUTOMATE THIS!!**
 - Schemathesis (Python framework)
 - Microsoft RESTler
 - 42Crunch Scan
 - It helps a lot to have examples!

DEMO TIME



```
isabelle@isabelle booking % uvx schemathesis run http://127.0.0.1:8080/openapi.json \
--header 'Authorization: Bearer secret-token' \
--output-sanitize false
[ Installed 54 packages in 38ms
Schemathesis dev
```

✓ Loaded specification from <http://127.0.0.1:8080/openapi.json> (in 0.66s)

Base URL: <http://127.0.0.1:8080/>
Specification: Open API 3.1.0
Operations: 3 selected / 3 total

✓ API capabilities:

Supports NULL byte in headers: ✘

► Examples (in 0.12s)

► 3 skipped

✗ Coverage (in 1.16s)

✓ 2 passed ✘ 1 failed

✗ Fuzzing (in 1.04s)

✓ 2 passed ✘ 1 failed

===== FAILURES =====

POST /bookings

1. Test Case ID: ltVHeP

- Server error

- Undocumented HTTP status code

Received: 500

TIME FOR API MANAGEMENT POLICIES

The screenshot shows the WSO2 API Manager Publisher interface. The top navigation bar includes the WSO2 logo, 'PUBLISHER', a search bar, and an 'ADMIN' dropdown. Below the header, the 'OpenWeather :1.0' API is selected, showing it was 'Created by: admin' and is in 'CREATED' state. The main content area is titled 'Policies' and displays two tabs: 'API LEVEL POLICIES' and 'OPERATION LEVEL POLICIES'. The 'API LEVEL POLICIES' tab is active, showing a policy for the '/Weather' endpoint. The 'Request Flow' section contains icons for 'AH' (Add Header) and 'LP' (Log Policy). The 'Response Flow' section contains an icon for 'RH' (Debug Request Flow). To the right, a 'Policy List' sidebar shows a list of common policies: 'Add Header v2', 'Log Policy v1', 'Add Query Param v1', 'Apply Accept Header v1', 'Change HTTP Method v1', and 'Debug Request Flow'.

Publisher

OpenWeather :1.0

Created by: admin

CREATED

Search

ADMIN

Current API

Go To

Create New Version

Download API

Delete

Last updated: 2 hours ago

Overview

Compliance

Develop

Portal Configurations

API Configurations

Runtime

Resources

API Definition

Endpoints

Local Scopes

Policies

Properties

Monetization

Deploy

Deployments

Test

Try Out

Publish

Lifecycle

Policies

API LEVEL POLICIES

OPERATION LEVEL POLICIES

API level policies will execute before operation level policies

/Weather

get /Weather

Request Flow

Response Flow

RH

Policy List

REQUEST RESPONSE FAULT

Add New Policy

Common Policies

AH Add Header v2

LP Log Policy v1

AQ Add Query Param v1

AA Apply Accept Header v1

CH Change HTTP Method v1

DR Debug Request Flow

BEST PRACTICES

- Policies Templates
- Managed in GIT
- Automatically applied via pipelines
- For higher environments (UAT, PrePro, Pro) - **No manual updates**

DEMO TIME



LIFE CYCLE MANAGEMENT

An AnthropicMessagesAPI :1.0.0
Created by: admin

PUBLISHED State

Current API ▾ Go To View in Dev Portal Create New Version Download API Delete

Last updated: a month ago

Lifecycle

PRE-RELEASED
PUBLISHED
DEPRECATED
RETIRED
BLOCKED
CREATED

Block Pre-Release Demote to Created Deprecate

History

User	Action	Time
admin	LC has changed from CREATED to PUBLISHED	a month ago

MONITORING

- You need to know everything about your API traffic:
 - Who calls you, from where, how often, what's the response time, which APIs are used, not used (!), which endpoints are used, not used (!), etc.
- Special attention to usage by version
 - V1 was deprecated. Can it be retired ?
 - V1 was retired. Why do we still have calls to it ????
 - Open door for hackers...



DEMO TIME



WHERE DO WE START ?

- Two approaches:
 - Test the full lifecycle on a smaller scope
 - Make one of the stages work well across the board (for example, design validation)



YEP - AND THIS JUST FOR APIs...

SEE YOU IN 2026 TO TALK ABOUT MCPs!



**TOUT EST AUTOMATISÉ.
SOUS CONTRÔLE.**



WSO2CONASIA

July 29–31, 2025 | Colombo, Sri Lanka

Platformless Modernization and Celebrating 20 Years of Global Impact

- Inspiring keynotes
- Focused agenda
- Interactive sessions
- Customer stories
- Look to the future
- Networking

Full Conference

LKR 50,000 (150 €)

Includes 3-day conference access (July 29–31), meals during conference hours, networking sessions, and entry to all social events.

Full Conference + 4 Nights' Accommodation

LKR 200,000 (600 €)

Includes everything in the Full Conference package, plus 4 nights' accommodation at the conference venue (July 28–August 1).

[Register Now](#)



Merci !



wso2.com

