

Porting APIs from v5 to API Gateway Service

Krithika Prakash, STSM - krithika.p@ibm.com

Jeremy Geddes, Technical Lead - jgeddes@us.ibm.com
API Connect & Gateways



IBM Cloud



Important Disclaimers

- **IBM Confidential.** Unless specifically advised otherwise, you should assume that all the information in this presentation (whether given in writing or orally) is IBM Confidential and restrict access to this information in accordance with the confidentiality terms in place between your organization and IBM.
- **Content Authority.** The workshops, sessions and materials have been prepared by IBM or the session speakers and reflect their own views. They are provided for informational purposes only, and are neither intended to, nor shall have the effect of being, legal or other guidance or advice to any participant. While efforts were made to verify the completeness and accuracy of the information contained in this presentation, it is provided AS-IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this presentation or any other materials. Nothing contained in this presentation is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software.
- **Performance.** Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.
- **Customer Examples.** Any customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth or other results.
- **Availability.** References in this presentation to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates

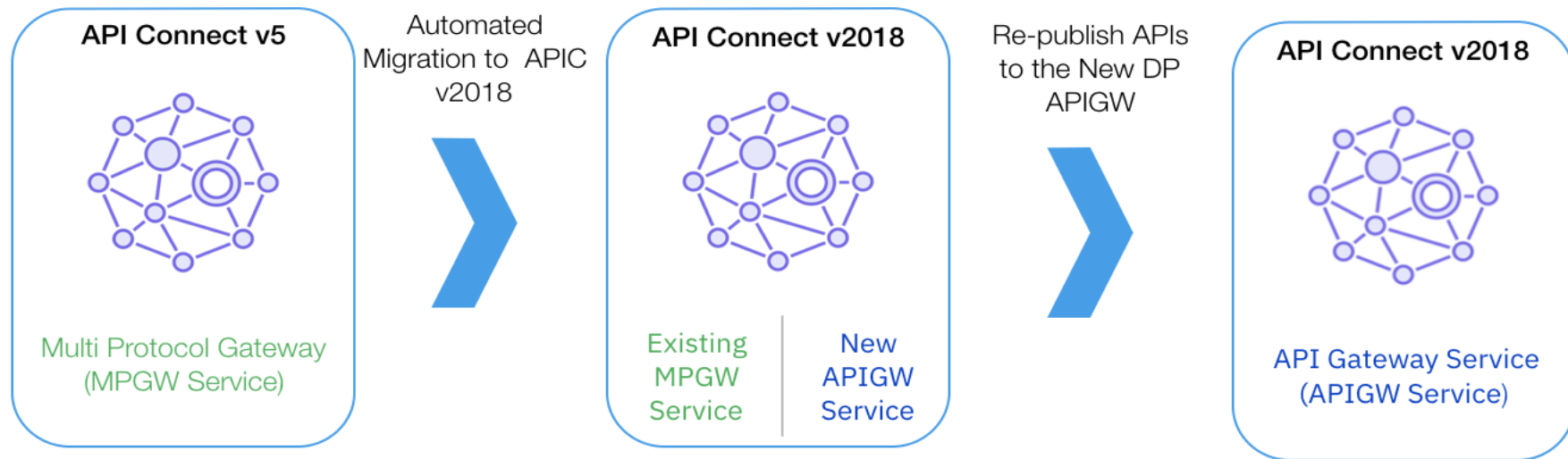
Trademark Acknowledgements

- IBM, IBM API Connect, IBM DataPower Gateway are trademarks of International Business Machines Corporation, registered in many jurisdictions
- Other company, product and service names may be trademarks, registered marks or service marks of their respective owners. A current list of IBM trademarks is available on the web at "Copyright and trademark information" ibm.com/legal/copytrade.html

Agenda

- Types of Gateway
- Migration paths
- High level architecture of v2018
- Key improvements in APIGW
- Porting from V5/V5C to API Gateway
 - Assembly Policies
 - OAuth Provider APIs to Objects
 - Custom Policies & Gateway Extensions in APIGW
- Open API V3 support
- Demo

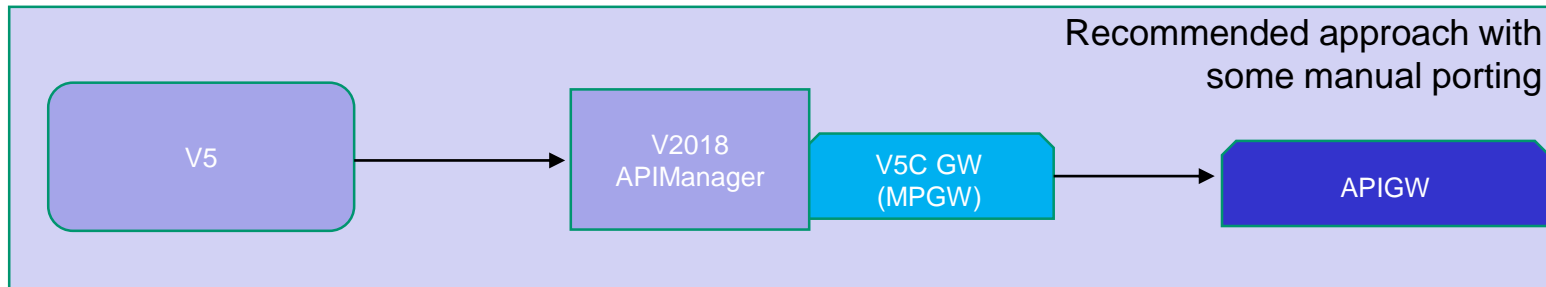
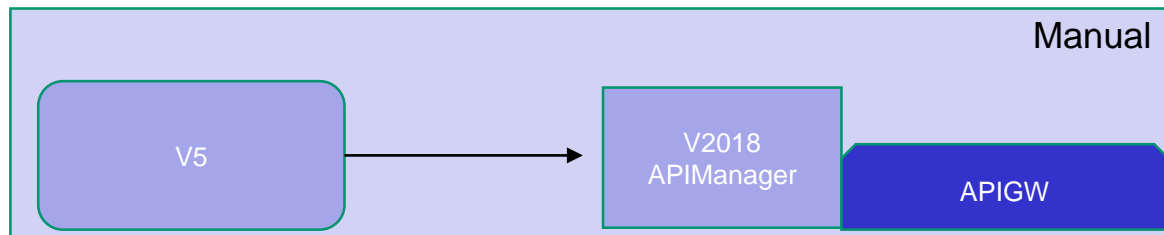
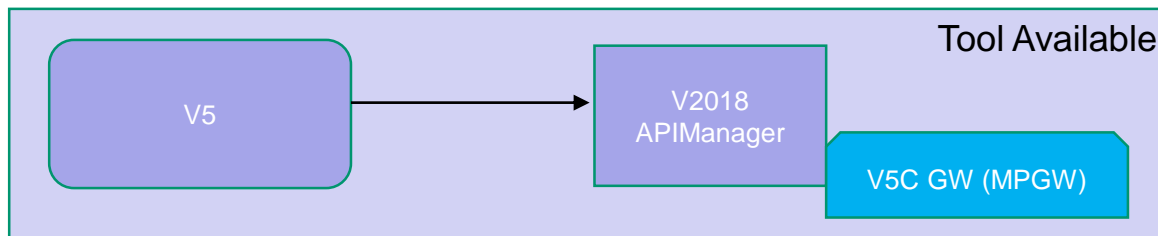
Types of Gateway – v5, v5c and APIGW



➡ **Migration tooling will automatically move APIs as-is to v2018 v5c (MPGW)**

➡ **Migration Tooling will NOT migrate APIs to the New APIGW Service.** Clients will port assembly and re-publish to API Gateway Service

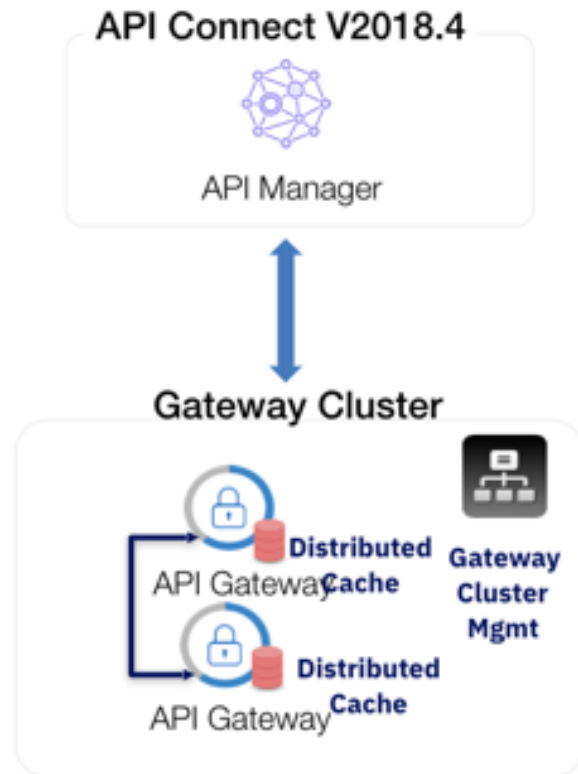
Migration Paths



Multi-cloud scalable API Manager & Gateway Architecture



- **Gateway Cluster management moved to the API Gateway** in API Connect V2018.4 from the API manager in API Connect V5



- **API Gateway Data Replication** performed between API Gateway members in API Connect V2018.4 instead of the API Manager in API Connect V5
- **Reduces the runtime dependency** between the API Gateway and API Manager in API Connect V2018.4

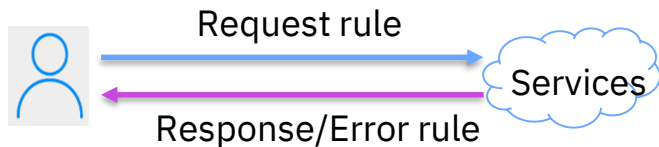
DataPower API Gateway Service: Secure & Performant APIs

- **Secure to the core** with self-contained signed & encrypted image to minimize risk, plus proven security policies to quickly protect APIs
- **Up to 5X increased performance** with natively built API Gateway using purpose-built technology for native OpenAPI/Swagger REST and SOAP APIs
- **Multi-cloud scalability and extensibility** to help meet SLAs and improve client user experience
- **Optimized drag & drop built-in policies** fully unleash the power of the gateway for security, traffic control and mediation including flexible OAuth, enhanced JSON & XML threat protection

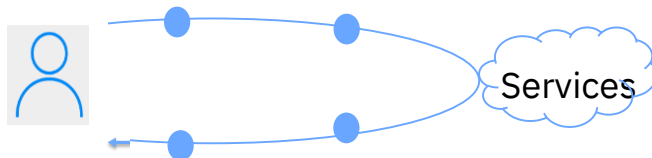


API Gateway Service

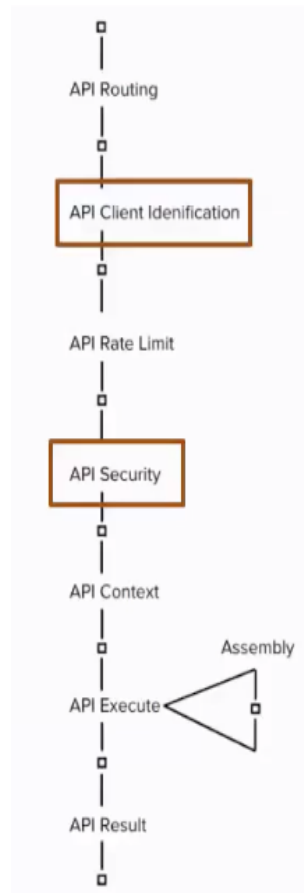
- APIGW was redesigned and reimplemented from scratch
- Natively written with no interpretive XSLT layer
- 5x increased performance
- Horseshoe request/response pattern
- WYSIWG (What you see in APIManager is what you get in DataPower)



VS



- API Application Type
- API Collection
- API Definition
- API LDAP Registry
- API Operation
- API Operation Rate Limit
- API Path
- API Plan
- API Rule
- API Schema
- API Security API Key
- API Security Basic Authentication
- API Security OAuth
- API Security OAuth Requirement
- API Security Requirement
- API Security Token Manager



Porting from V5/V5C to API Gateway

- Set gateway type to “datapower-api-gateway”
- Update Assembly policies
- Port OAuth Provider APIs to objects
- Port custom policies and gateway extensions
- Leverage added support for OpenAPI V3.

Gateway Type

Select the gateway type for this API

- ☐ DataPower Gateway (v5 compatible)
- ☒ DataPower API Gateway

Porting Assembly

- All policies have new Versions
- Switch replaces switch', 'operation-switch' & 'if'
- Enhanced Invoke policy with whitelisting and blacklisting support
- No proxy policy – replaced by invoke
- Enhanced Activity Log, CORS, Streaming
- New policies – user security, client security, API rate limit
- Gateway script and XSLT policies
 - » New functions and extensions
 - » Wrapper available (but could degrade performance)
 - » Refer to new message and context objects

<https://github.com/ibm-apiconnect/apigw/wiki/APIGW-Porting-Notes>

Assembly Policies v5/v6

Features	V5c	APIGW	First Release	Notes
Invoke	✓	✓	7.7.1.0	
Map	✓	✓	7.7.1.0	
Activity Log	✓	✓*	7.7.1.0	As API Property
JSON-to-XML	✓	✓	7.7.1.1	Requires Parse
XML-to-JSON	✓	✓	7.7.1.1	Requires Parse
Set Variable	✓	✓	7.7.1.1	
Throw	✓	✓	7.7.1.1	
JWT Generate	✓	✓	7.7.1.2	
JWT Validate	✓	✓	7.7.1.2	

Assembly Policies v5/v6

Features	V5c	APIGW	First Release	Notes
If / Switch / OperationSwitch	✓	✓	2018.4.1.0	As Switch
Gateway Script	✓	✓	2018.4.1.0	
Proxy	✓	✓	2018.4.1.0	As Invoke
XSLT	✓	✓	2018.4.1.0	Requires Parse
Validate	✓	✓	2018.4.1.0	Requires Parse
LTPA Generate	✓	×		
Redaction	✓	×		
Validate Username Token	✓	×		
OAuth	×	✓	7.7.1.0	
User Security	×	✓	7.7.1.0	
Parse	×	✓	7.7.1.1	

**Additional Policies
Releasing soon:**

1. Client Security
2. API Rate Limit

GatewayScript : New objects

Context

- context.message.getVariable()
- context.message.setVariable()
- context.request.body.readAsBuffer()
- context.request.body.readAsBuffers()
- context.request.body.readAsJSON()
- context.request.body.readAsXML()
- context.clear()
- context.get()
- context.set()
- context.request.headers
- context.request.header.get()
- context.reject()
- context.swagger.readAsJSON()

Message

- | | |
|---|--|
| <ul style="list-style-type: none">• message.body.readAsBuffer()• message.body.readAsBuffers()• message.body.readAsJSON()• message.body.readAsXML()• message.body.write()• message.header.get()• message.header.remove()• message.header.set()• message.getVariable()• message.setVariable()• message.headers• message.reasonPhrase | <ul style="list-style-type: none">• message.statusCode• message.body.readAsBuffer()• message.body.readAsBuffers()• message.body.readAsJSON()• message.body.readAsXML()• message.headers• message.header.get()• message.header.remove()• message.header.set()• message.reasonPhrase• message.statusCode |
|---|--|

https://www.ibm.com/support/knowledgecenter/en/SS9H2Y_7.7.0/com.ibm.dp.doc/context_apigw_js.html

https://www.ibm.com/support/knowledgecenter/en/SS9H2Y_7.7.0/com.ibm.dp.doc/multistep_js.html

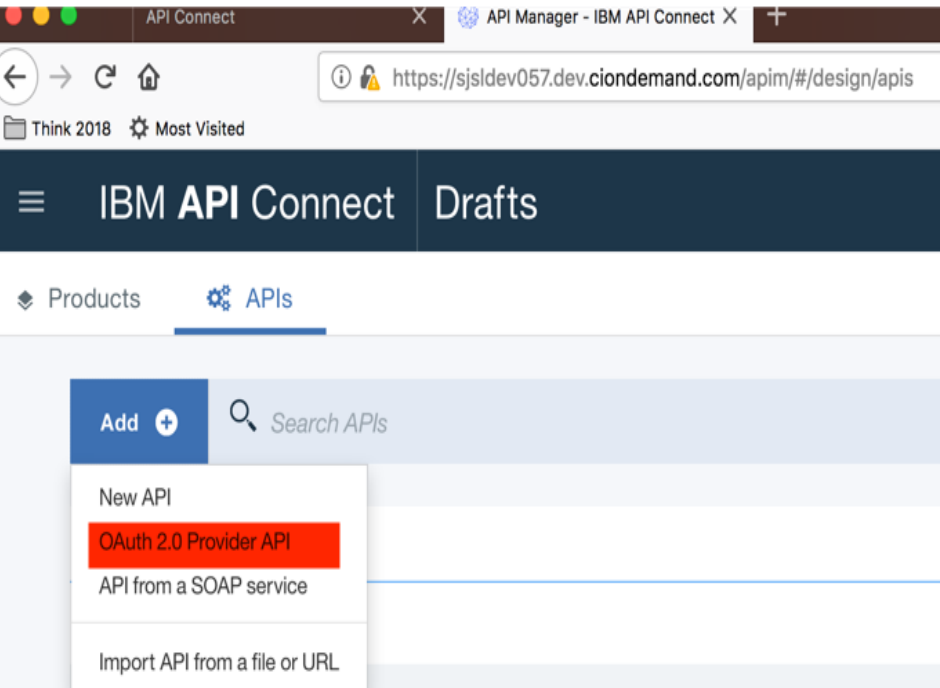
Porting OAuth Provider APIs to Objects

Steps

- Migrate V5 OAuth Provider API to v2018 OAuth Provider object
- OAuth Provider object has an underlying API
- Take advantage of the customizable Assembly
- Create and configure providers to a catalog
- Link the OAuth provider to the API using it - “x-ibm-oauth-provider”

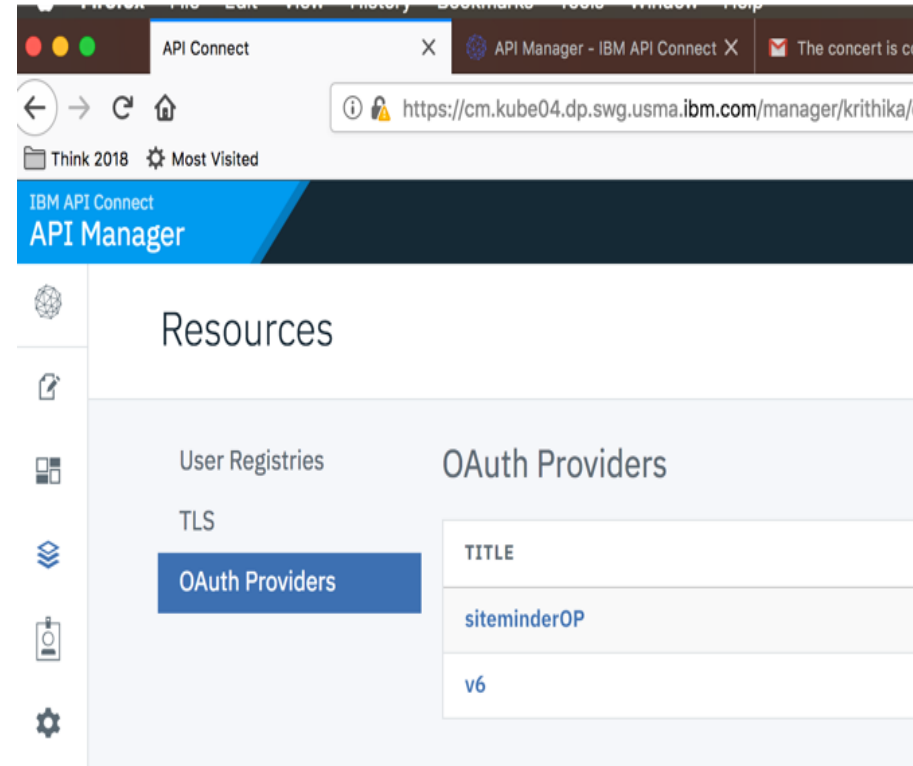
OAuth API → OAuth Object

v5



The screenshot shows the IBM API Connect v5 interface. The browser address bar displays the URL <https://sjsldev057.dev.ciondemand.com/apim/#/design/apis>. The main header includes the IBM API Connect logo and the word "Drafts". Below the header, there are tabs for "Products" and "APIs". The "APIs" tab is active, showing a search bar with the placeholder text "Search APIs" and a list of API creation options. The options are: "New API", "OAuth 2.0 Provider API" (highlighted in red), "API from a SOAP service", and "Import API from a file or URL".

v2018



The screenshot shows the IBM API Connect v2018 interface. The browser address bar displays the URL <https://cm.kube04.dp.swg.usma.ibm.com/manager/krithika/>. The main header includes the IBM API Connect logo and the word "API Manager". Below the header, there are tabs for "Resources" and "OAuth Providers". The "OAuth Providers" tab is active, showing a table with the following data:

TITLE
siteminderOP
v6

Native & Third Party Provider

Edit Native OAuth Provider

Info

Configuration

Scopes

User Security

Tokens

Token Management

Introspection

Metadata

OpenID Connect

API Editor

Configuration

Authorize path

/oauth2/authorize123

Token path

/oauth2/token

Supported grant types

☒ Implicit

☐ Application

☒ Access code

☐ Resource owner password

Supported client types

☒ Confidential

☒ Public

Edit Third Party OAuth Provider

Info

Endpoints

Scopes

Third Party OAuth Provider

OAuth providers can be created and managed in the following list.

Title

siteminderOP

Name

siteminderop

Gateway version

6000

Supported grant types

☒ Implicit

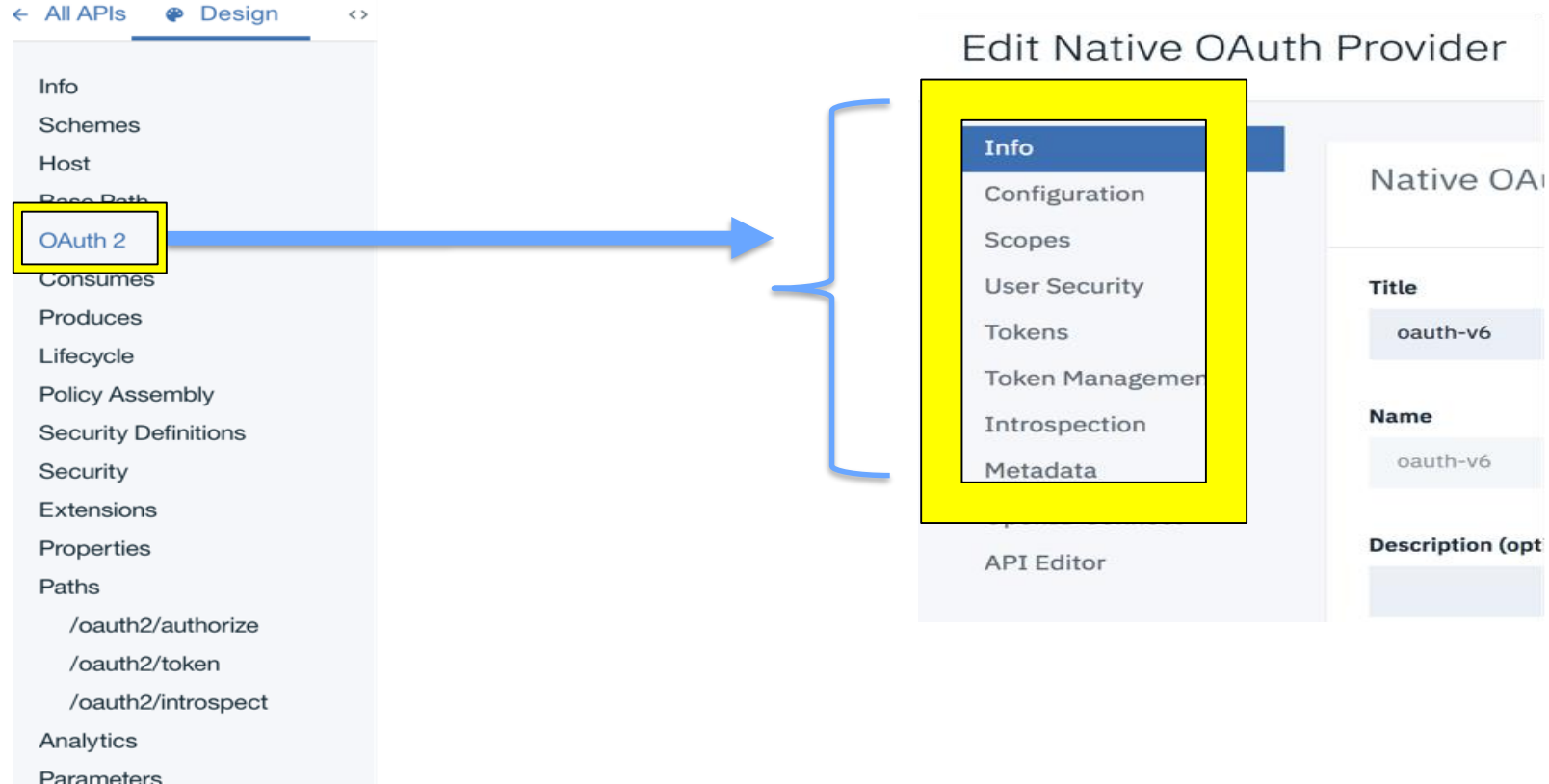
☒ Application

☒ Access code

☒ Resource owner password

☐ Enable debug response headers

V5 (OAuth2 section) ----- > V2018 OAuth object



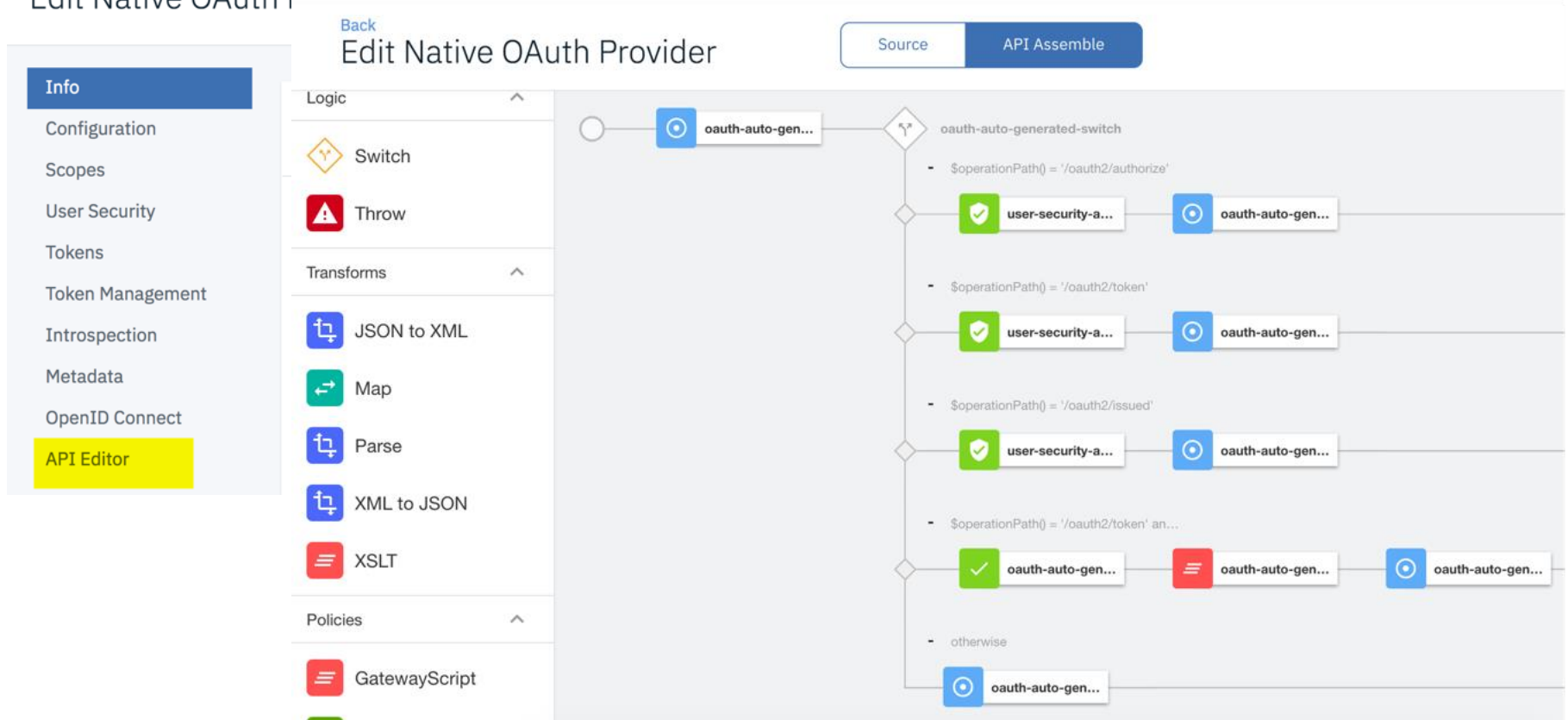
V5 Everything else ---->

V2018 Underlying API

The image shows a screenshot of the API Design console. On the left is a sidebar with a list of API components: Info, Schemes, Host, Base Path, Consumes, Produces, Lifecycle, Policy Assembly, Security Definitions, Security, Extensions, Properties, Paths, Analytics, and Parameters. A blue bracket groups the first 13 items. A blue arrow points from this group to the 'API Editor' tab in the 'Edit Native OAuth Provider' panel on the right. The 'Edit Native OAuth Provider' panel has a title bar and a list of tabs: Info (selected), Configuration, Scopes, User Security, Tokens, Token Management, Introspection, Metadata, and OpenID Connect. The 'API Editor' tab is highlighted with a yellow border. The 'Native OAuth Provider' panel shows fields for Title (oauth-v6), Name (oauth-v6), and Description (optional).

Customizable Assembly within OAuth Provider object

Edit Native OAuth Provider



Configure OAuth Providers in the Catalog

[Manage](#) / [Sandbox](#)
Settings

Overview

Gateway Services

Lifecycle Approvals

Roles

Onboarding

API User Registries

OAuth Providers

API Endpoints

TLS Client Profiles

Portal

Properties

OAuth Providers

Manage the OAuth Providers configured for API Manager

Edit

TITLE	TYPE
oauth-v6	Native

Link Provider to OAuth Security Definitions



API Security Definition

Name
oauth2

Description (optional)

Type
☐ API Key ☐ Basic ☒ OAuth2

OAuth Provider
v6

Flow
Implicit

Authorization URL
https://\$(catalog.url)/v6123/oauth2/authorize123

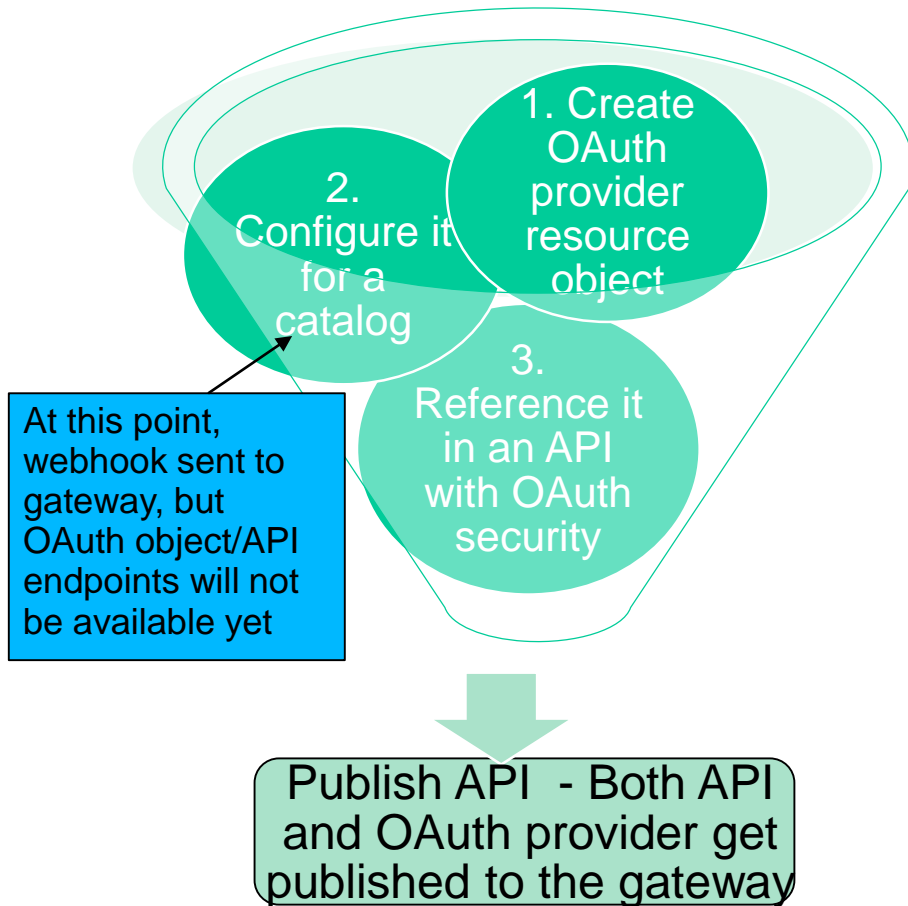
Advanced Scope Check
Default validator endpoint set by OAuth Provider: https://test.com

Scopes

NAME
openid
sample_scope_1

```
schemes:  
  - https  
basePath: /oauth-api-v6  
security:  
  - oauth-1:  
    - scope1  
securityDefinitions:  
  oauth-1:  
    type: oauth2  
    flow: accessCode  
    x-ibm-oauth-provider: oauth-v6  
    authorizationUrl: 'https://$(catalog.url)/oauth-v6/oauth2/authorize'  
    tokenUrl: 'https://$(catalog.url)/oauth-v6/oauth2/token'  
    scopes:  
      | scope1: This is scope1 description  
x-ibm-configuration:  
  phase: realized  
  testable: true  
  enforced: true  
  properties:  
    target-url:  
      value: 'http://example.com/operation-name'  
      description: The URL of the target service  
      encoded: false  
  cors:  
    enabled: true  
  application-authentication:  
    certificate: false  
  gateway: datapower-api-gateway
```

Publish sequence – onto Gateways



- Note : Unless the OAuth provider is used by at least one of the APIs in the Security Definition, the OAuth provider endpoints are not available in Gateway
- Any updates to OAuth provider or its underlying API will take effect immediately on the gateway (no need to republish once already configured in catalog and used by any API)
- Until the last API that uses an OAuth provider is published, the OAuth provider and its API also remain published in the gateway

Porting User Defined Policies in APIGW

- Converting User Defined Policies

- Available soon

- Basic Converting Policies Steps

- 1 - Import existing v5c policy, save, copy the config from DP
- 2 - create gateway script to call the rule

```
var ms = require('multistep');  
ms.callRule('saml-validation-policy-main', 'request', 'message', function(error)  
    { if (error) { throw error; } });
```

- 3 – Changed location of some common utils

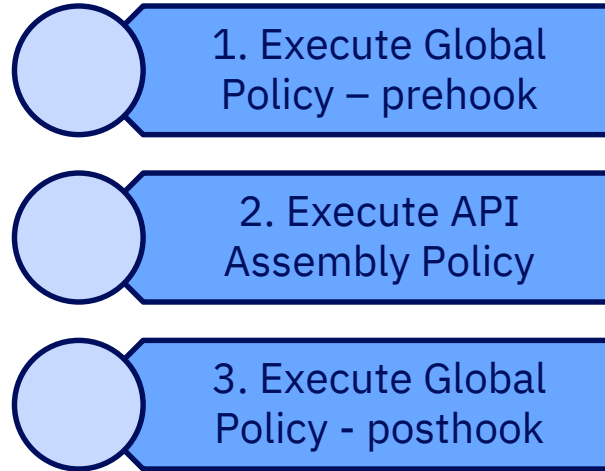
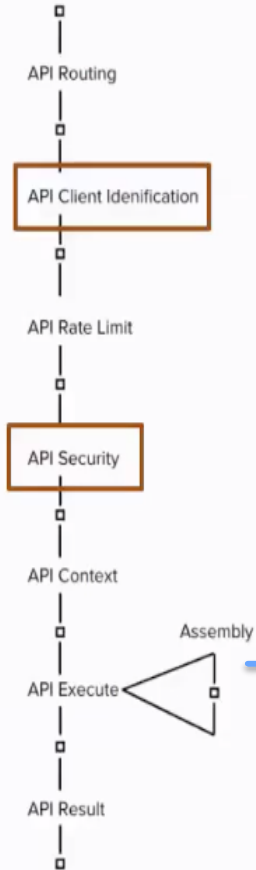
- local:///isp/policy/apim.custom.xsl to store:///dp/apim.custom.xsl
- local:isp/policy/apim.custom.js to require('apim');

- May need to do some marshalling to support the policies as some context was setup in V5.

Gateway Extensions in v5 → Global Policies in APIGW

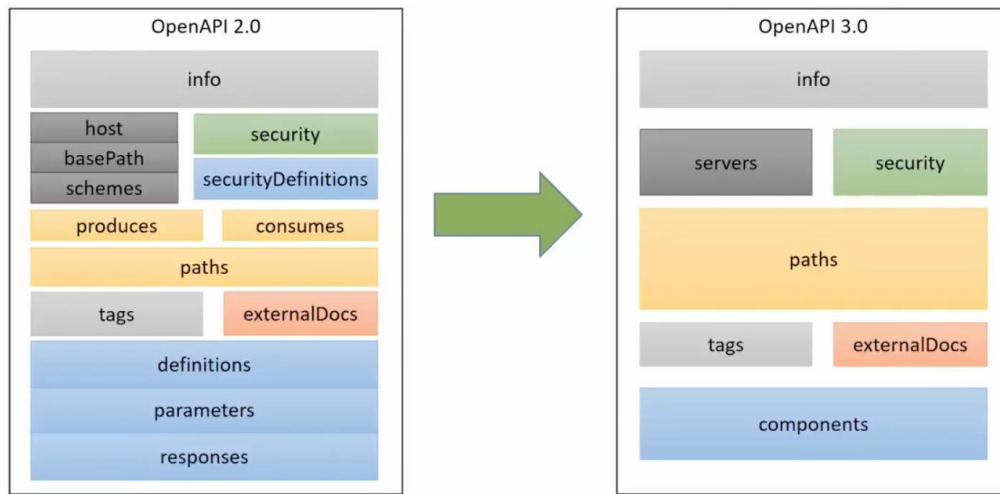
Sample policies that can benefit from being a global policies

- Kerberos policy using Gateway Script (Poc done for a customer)
- PingIdentity AI powered API security policy (Demoed at THINK 2019)
- Client Security policy to offload client authentication (available soon)



OpenAPI V3 Support

- Partial OAI3 support
 - Focused around Berlin Group PSD2 (OpenBanking)
- General Limitations
 - Single Server
 - Most policies
 - Limited to JSON Schema Version 4
- Currently CLI only



https://www.ibm.com/support/knowledgecenter/en/SSMNED_2018/com.ibm.apic.toolkit.doc/rapic_oai3_support.html

Demo

Thank You

