Integration Technical Conference 2019

Security Best Practice

API Connect & DataPower

Shiu Fun Poon, STSM shiufun@us.ibm.com
Krithika Prakash, STSM krithika.p@ibm.com

IBM **Cloud**

IBM

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

Security

- Availability
- Configurable
- Standard
- Ease of use
- Monitoring
- Resource consumption
- …

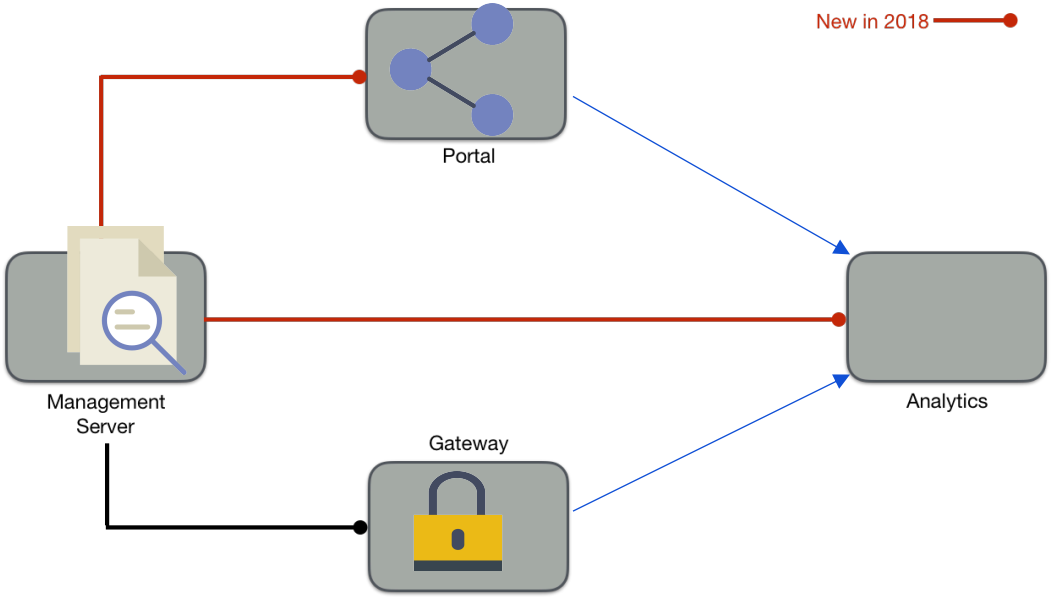
Security

le

e

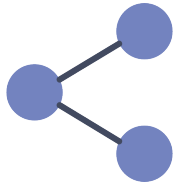
onsumption

API Security



API Manager:

- Plan/product design
- Policy administration
- API plan usage analytics
- API Governance
- **Security**



Developer portal:

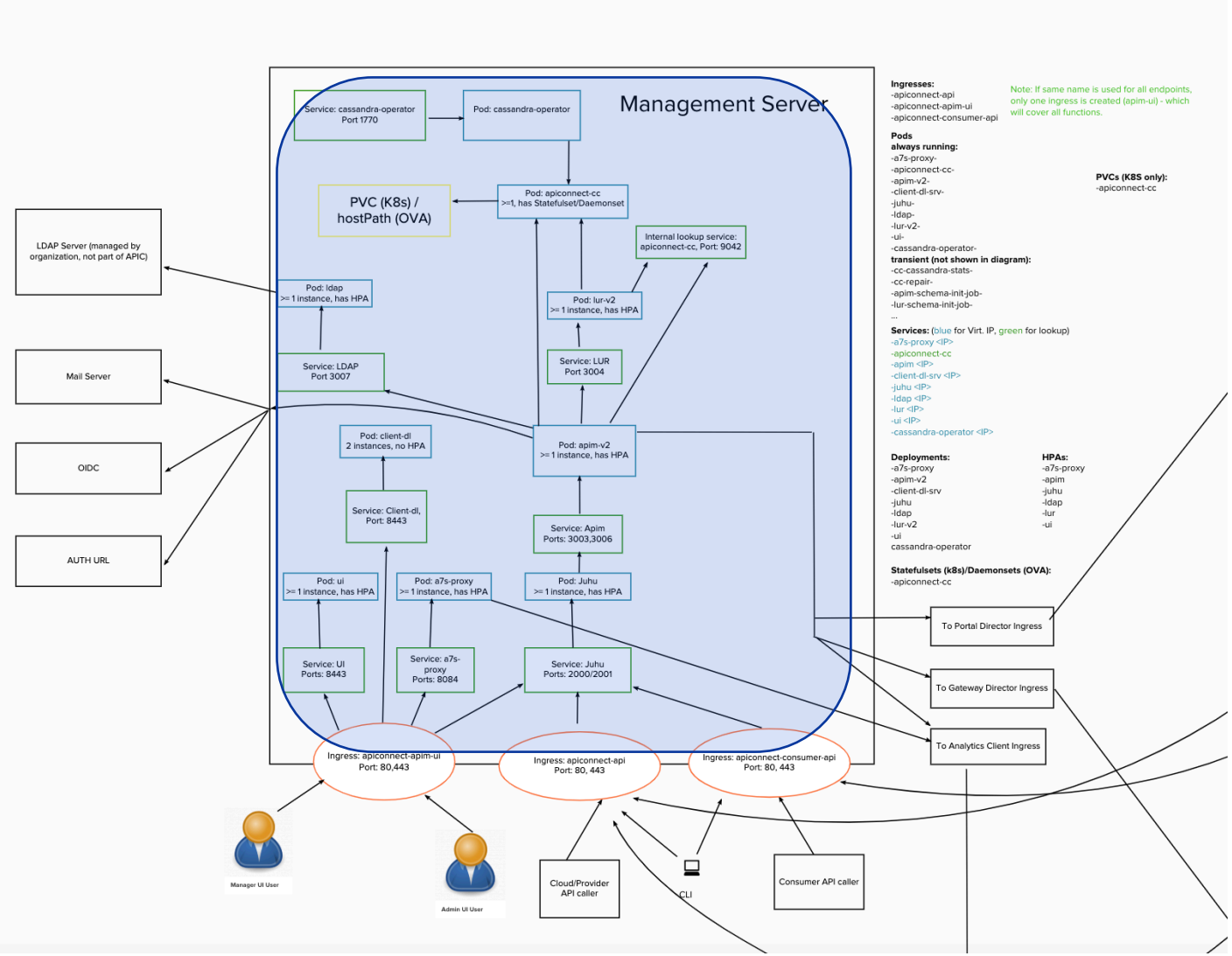
- API discovery
- Self subscription/administration
- Account usage analytics
- Monetization
- **Security**

API Gateway:

- Decoupling/routing
- Traffic management
- **Security**
- Translation

https://www.ibm.com/support/knowledgecenter/en/SSMNED_2018/com.ibm.apic.install.doc/capic_deploy_overview.html

Management Server



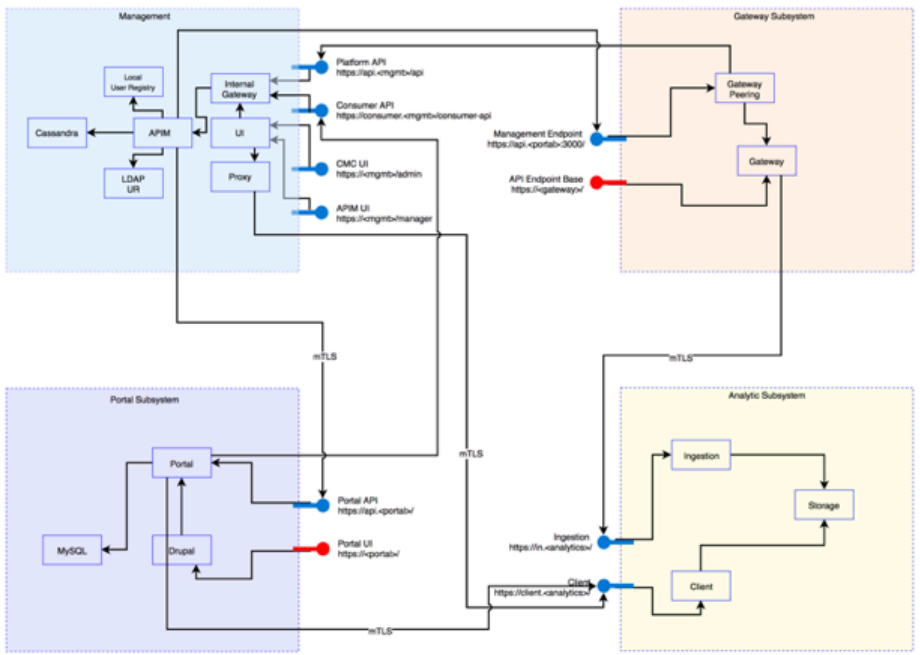
Service Name
r0dc9ac8ca3-cassandra-operator
r3383eaabb4-dynamic-gateway-service
r3383eaabb4-dynamic-gateway-service-ingress
r83f584144e-apic-portal-admin-all
r83f584144e-apic-portal-db
r83f584144e-apic-portal-db-all
r83f584144e-apic-portal-db-proxy
r83f584144e-apic-portal-director
r83f584144e-apic-portal-director-cluster
r83f584144e-apic-portal-nginx
r83f584144e-apic-portal-web
r83f584144e-apic-portal-web-cluster
r8be0d774b0-dynamic-gateway-service
r8be0d774b0-dynamic-gateway-service-ingress
r94a65033af-analytics-client
r94a65033af-analytics-ingestion
r94a65033af-analytics-mtls-gw
r94a65033af-analytics-operator
r94a65033af-analytics-storage
r94a65033af-es-data-persistence
r94a65033af-es-discovery
r94a65033af-es-master-persistence
rf01f435561-a7s-proxy
rf01f435561-apiconnect-cc
rf01f435561-apim
rf01f435561-client-dl-srv
rf01f435561-juhu
rf01f435561-ldap
rf01f435561-lur
rf01f435561-ui

APIc under the hook

- Internal services communicating vs mTLS
- Quorum, with 3 being the magic number
- APIc is the match maker, it introduces each subsystem to each others
  - APIM, Portal, Analytics, Gateway
  - How does APIM <-> Portal
  - How does APIM <-> Analytics
  - How does APIM <-> Gateway
  - How does Portal <-> Analytics
  - How does Gateway <-> Analytics
- Configurable, extensible

Micro services

```
~/dev/apim (⎈ ) kubectl get pods
NAME                                                  READY   STATUS    RESTARTS   AGE
r10b59f5d9f-dynamic-gateway-service-0                 1/1     Running   0          2d
r305ac78e55-a7s-proxy-5d44d6f74c-pvlrv                1/1     Running   0          2d
r305ac78e55-apiconnect-cc-0                           1/1     Running   0          2d
r305ac78e55-apim-v2-7ffdf57685-tgd48                  1/1     Running   0          1d
r305ac78e55-client-dl-srv-599dfd7cd5-st5v6            1/1     Running   0          2d
r305ac78e55-juhu-7bc8685c94-bdqnz                     1/1     Running   0          2d
r305ac78e55-ldap-7d95d4cdb6-qhppq                     1/1     Running   0          2d
r305ac78e55-lur-v2-57c578b76f-6j8hk                   1/1     Running   0          2d
r305ac78e55-ui-7d64db9797-zp2x5                       1/1     Running   0          2d
r3451a94256-analytics-client-85f6dc4d4f-j648q         1/1     Running   0          2d
r3451a94256-analytics-ingestion-6cd59476d8-zckh6      1/1     Running   0          2d
r3451a94256-analytics-mtls-gw-55f8957788-skwrx        1/1     Running   0          2d
r3451a94256-analytics-operator-6b595bffc7-rxgbr       1/1     Running   0          2d
r3451a94256-analytics-storage-coordinating-5c4b68c7cc-2n2bz   1/1     Running   1          2d
r3451a94256-analytics-storage-data-0                  1/1     Running   0          2d
r3451a94256-analytics-storage-master-0                1/1     Running   0          2d
r969ade2f3c-dynamic-gateway-service-0                 1/1     Running   0          2d
r973af30785-apic-portal-db-0                          2/2     Running   0          2d
r973af30785-apic-portal-nginx-58745777df-q97wh        1/1     Running   0          2d
r973af30785-apic-portal-www-0                         2/2     Running   0          2d
ra59641e274-cassandra-operator-59cf5b6d8f-4sxvm       1/1     Running   0          2d
~/dev/apim (⎈ )
```

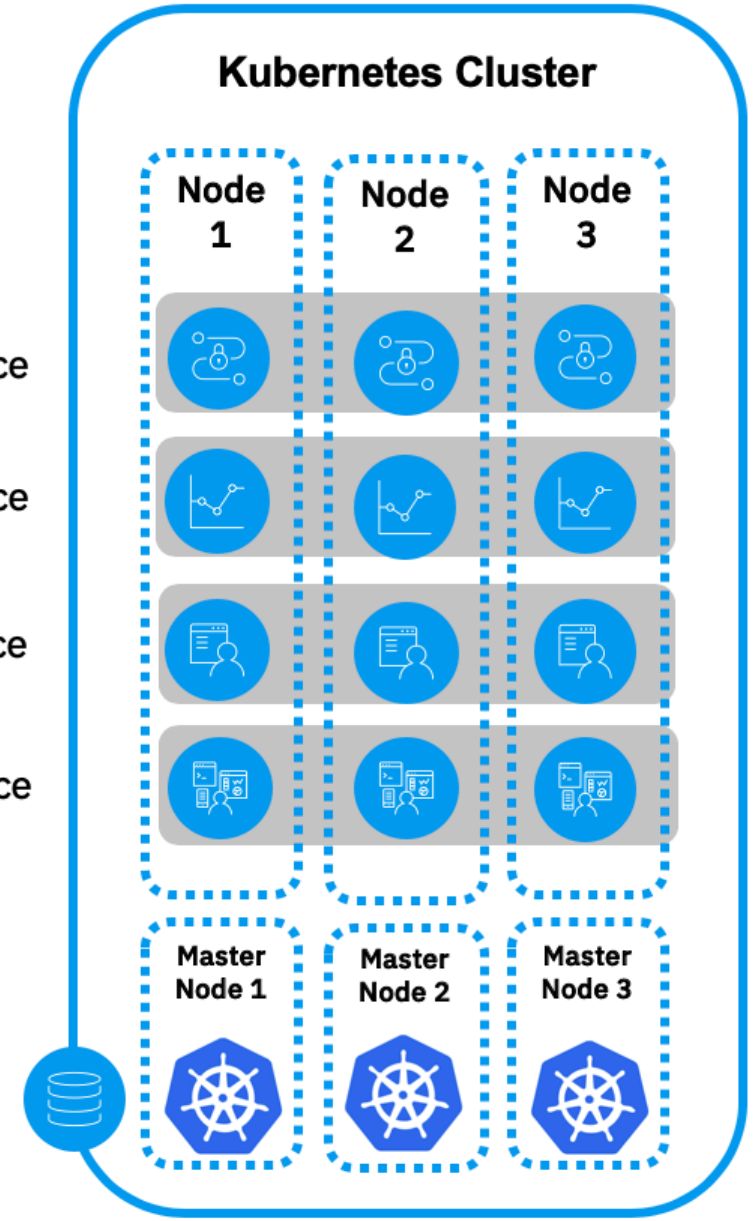


Gateway Service

Analytics Service

Portal Service

Management Service



APIC Connect White Paper: https://www.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=03023503USEN&

API Manager

- **User Registry support**
  - Authenticate URL
  - LDAP (supports group authentication)
    - Search DN
    - Compose DN
    - Compose UPN
  - Local User Registry (LUR)
    - Protection against timing attack
    - Protection against brute force attack
  - OIDC/Social Login (Federated Identity)
    - Portal
    - Admin/Provider Organization
    - OOTB : Google, Facebook, Linkedin, Slack, WindowLive, Github, Standard
    - Public Key for Code Exchange
    - Nonce
    - Proxy tokens

- How is OIDC/Social Login difference from v5
- Implication ?

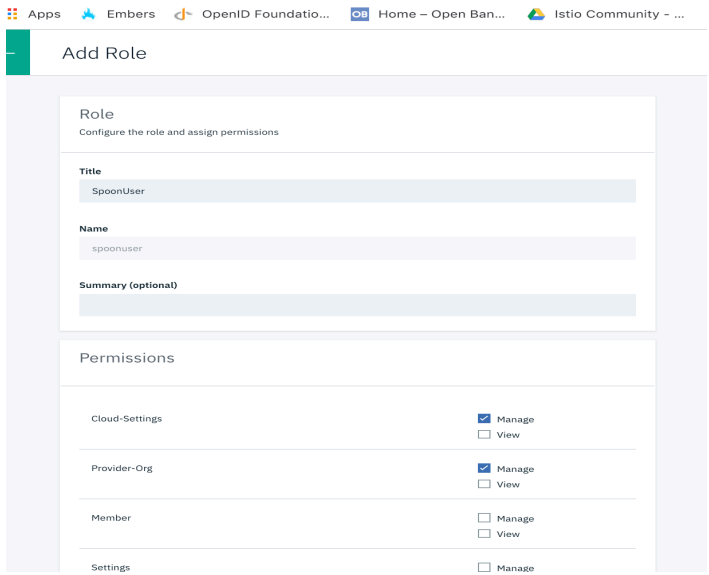
API Manager

- **User Registry support**
  - Authenticate URL
  - LDAP (supports group authentication)
    - Search DN
    - Compose DN
    - Compose UPN
  - Local User Registry (LUR)
    - Protection against timing attack
    - Protection against brute force attack
  - OIDC/Social Login (Federated Identity)
    - Portal
    - Admin/Provider Organization
    - OOTB : Google, Facebook, Linkedin, Slack, WindowLive, Github, Standard
    - Public Key for Code Exchange
    - Nonce
    - Proxy tokens

- How is OIDC/Social Login difference from v5
- Implication ?

API Manager

- **Token (JWT)**
  - OAuth 2.0 (no basicauth, no more cookie)
- **Role**
  - Custom role
- **Token ttl (invitation, oauth 2)**
  - ttl



- **Data at Rest**
- **Data at Transit**
- **Introduction of microservices to each others**
  - **Webhook**

API Manager

- API are published
  - Publish in openapi v2 format
    - apim vs consumer
  - WebGUI/toolkits/portal/BYO
  - RateLimit

[Drinking Our Own Champagne]

Get an access_token

access_token must contain the right sc

Permission is checked

Is token valid

Token contains necessary scope ?

Does User has the proper permission ?

```
#---------------------------------------------------------------------------
# User Registry Collection
#---------------------------------------------------------------------------
'/orgs/{org}/user-registries':

  description: The collection of User Registry operations

  parameters:
    - $ref: '#/components/parameters/org'

  post:
    summary: Create a User Registry object
    description: Create a User Registry object
    operationId: user_registry_create
    security:
      - oauth:
        - org:manage
    externalDocs:
      description: Additional documentation
      url: 'https://www.ibm.com/knowledge-center/api-connect/platform-apis/user-registry#create'
    requestBody:
      content:
        application/json:
          schema:
            $ref: '#/components/schemas/UserRegistry'
        application/yaml:
          schema:
            $ref: '#/components/schemas/UserRegistry'
    responses:
      '201':
        description: Successful create
        content:
          application/json:
            schema:
              $ref: '#/components/schemas/UserRegistry'
          application/yaml:
            schema:
              $ref: '#/components/schemas/UserRegistry'
        headers:
          Location:
            $ref: '#/components/headers/Location'
      5XX:
        $ref: '#/components/responses/Error'
```

Hardened Portal Security

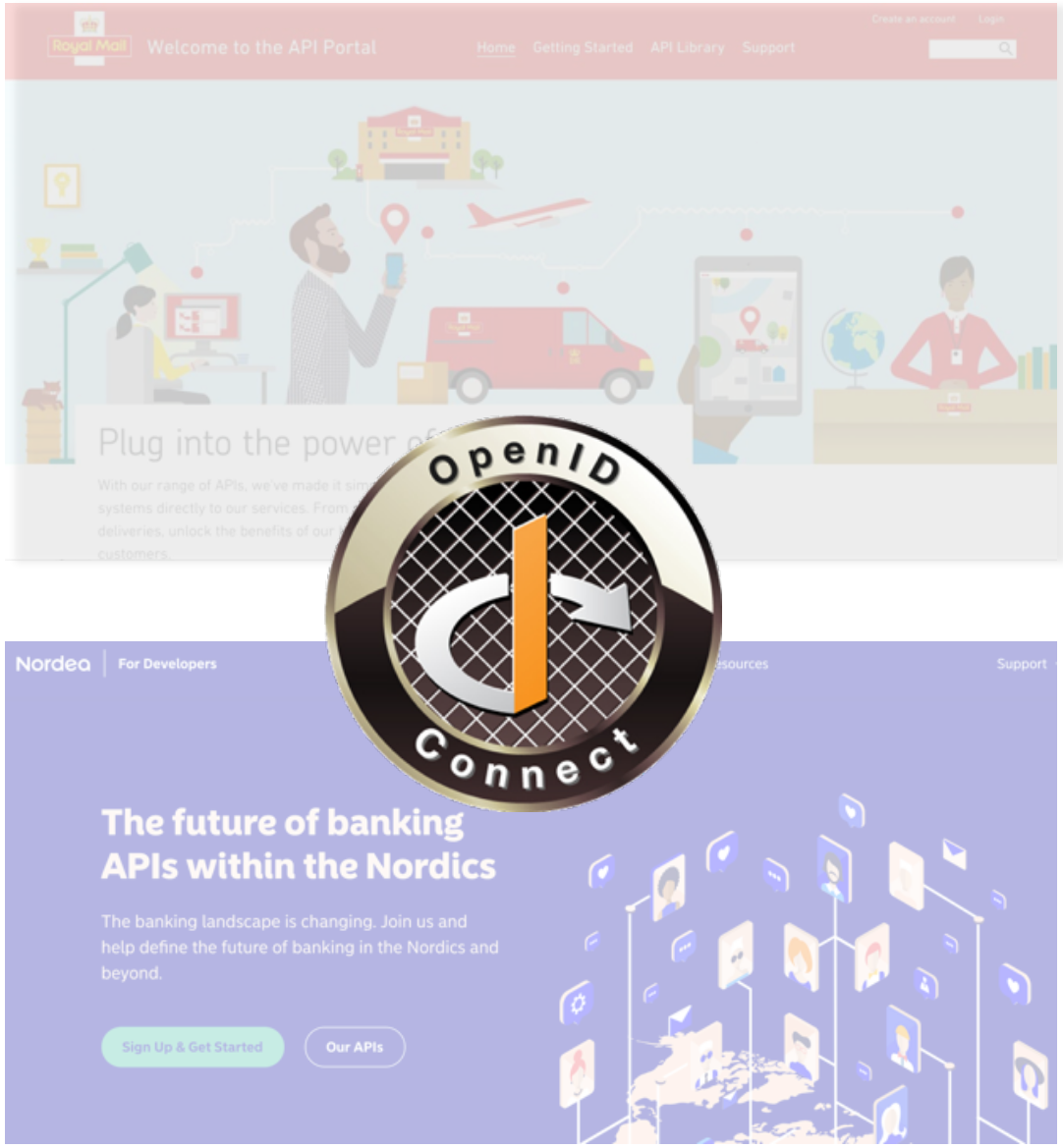
Supports OpenID Connect for accelerated developer on-boarding and social login

Enable PSD2/ Open Banking compliance to programmatically onboard consumers using REST Management APIs and OpenID Connect

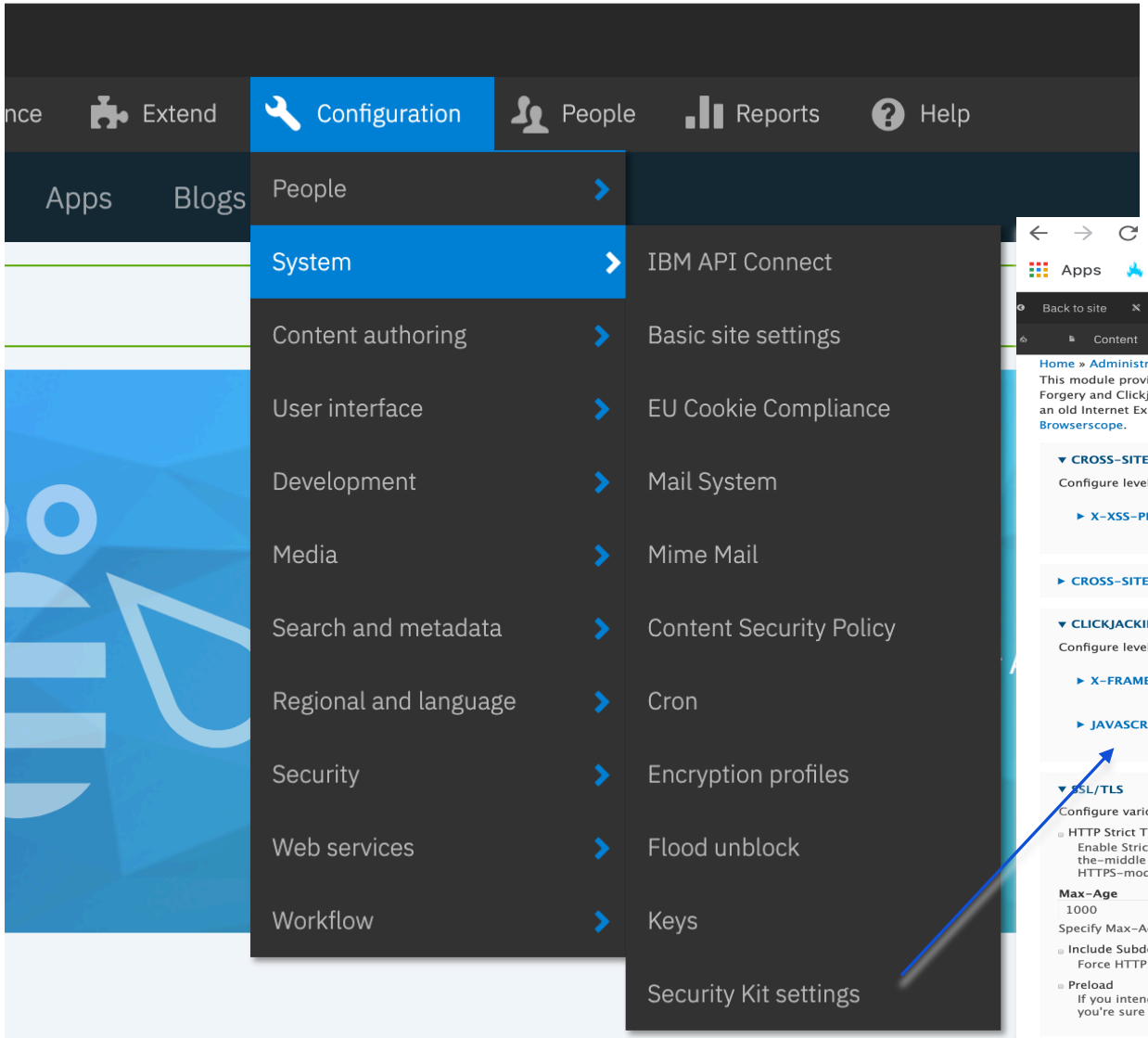
Enhanced spam protection against spam bots with CAPTCHA and honeypot

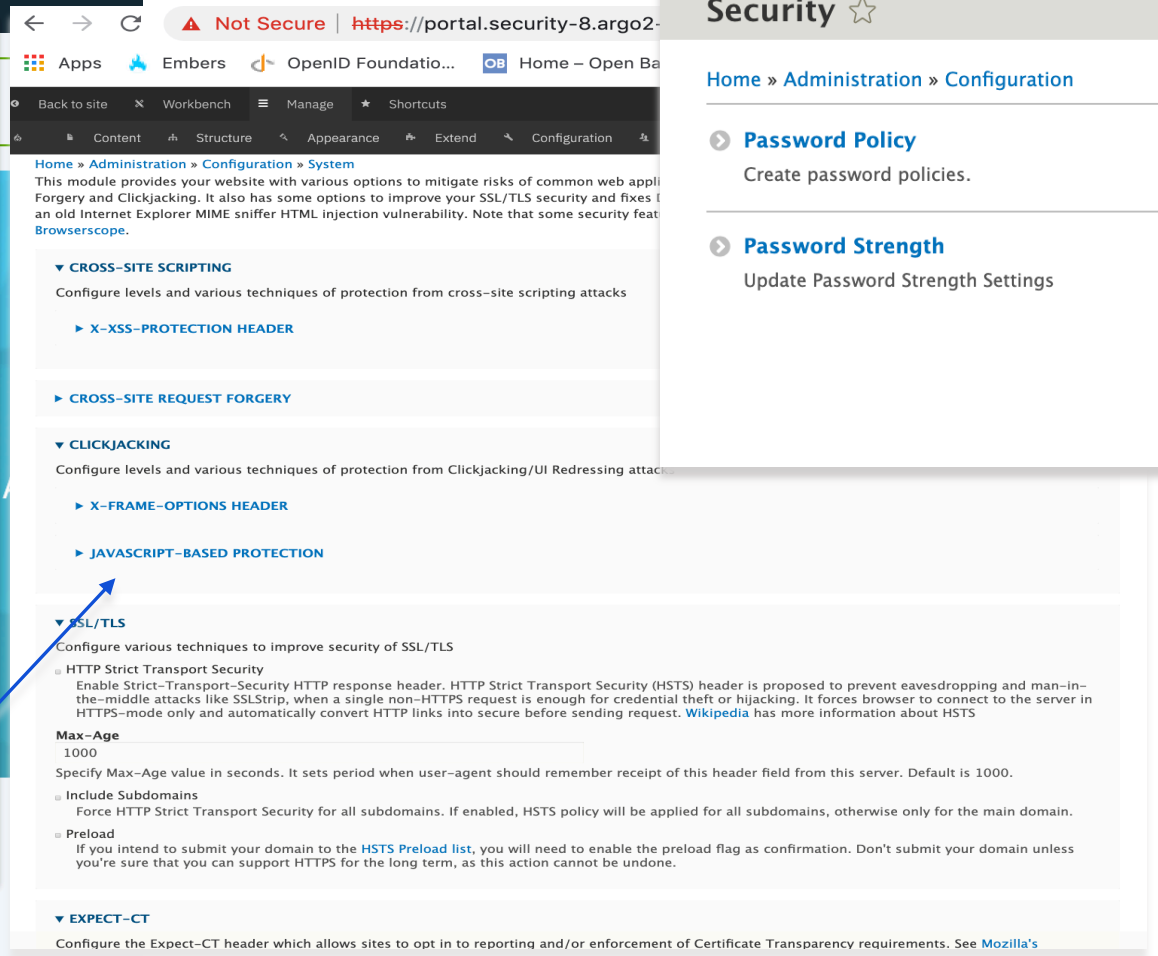
Detect and prevent malicious attacks with perimeter and DNS check

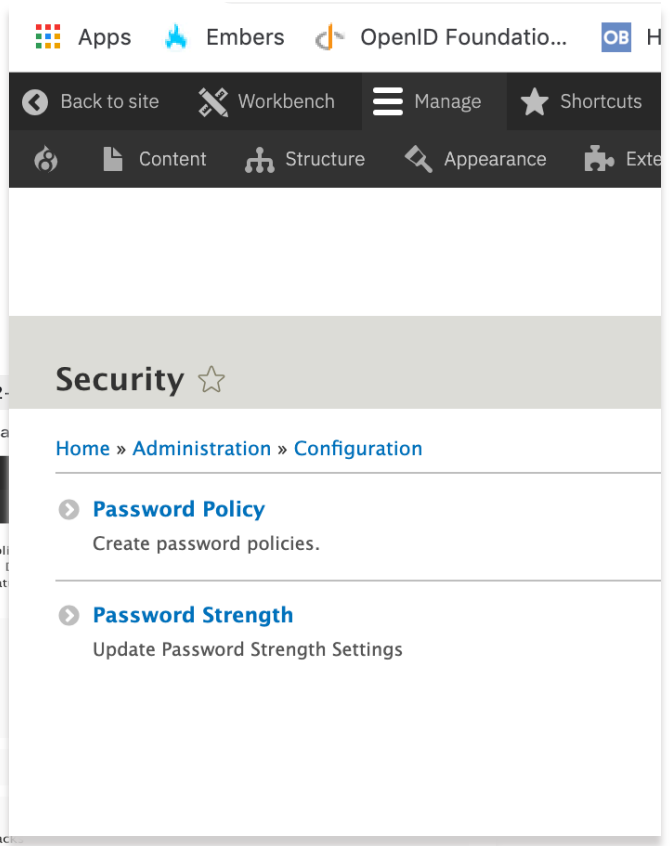
Detect and prevent flood attacks



Configure Portal Behavior







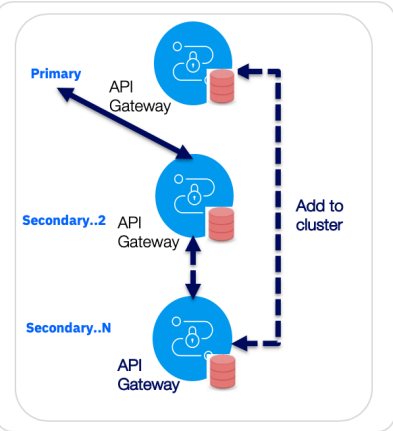
APIManager with Gateway

Runtime Scale for Usage Spikes

Scale API gateway clusters to adhere to SLAs and handle volume spikes

Autonomous gateway management, deploy gateways on multiple clouds without any operational impact

Self-healing gateways optimizing scaling for usage spikes to improve runtime resiliency



- **Gateway must be 24 * 7 (without API manager)**
- **API gateway introduce a gateway director manager**
  - Using clustering technology to track configuration from APIM
  - Heartbeat from APIm to make sure Gateway will have the latest information
  - 911 protocol to handle catastrophic failure
- **Gateway director allows auto scaling of the additional gateway**
  - Configuration/Key Materials
  - State of the processing

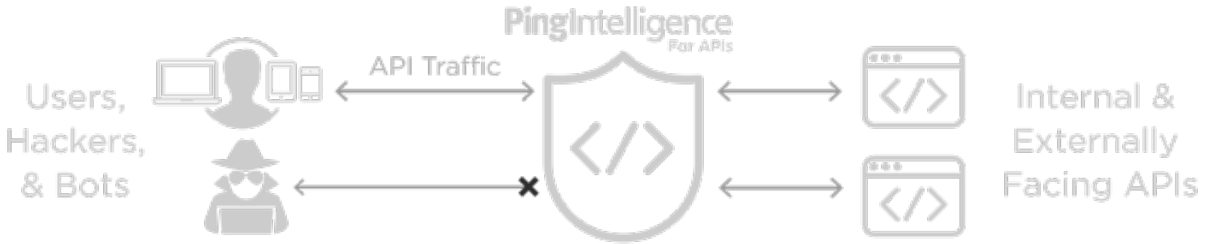
Performant and Secure

- **Istio Integration** for improved performance & security by passing API header and tokens into Istio
- **Open API V3 support** to meet security industry standards (i.e. PSD2) & improve reuse
- **OpenBanking & PSD2 Compliant** including flexible JWT and OAuth features
- **5X Improved Performance** with cloud-native API-centric Gateway Service
- **Fast Time to Value** through Out of the Box policies for API Gateway Service
- **Enterprise Specific Security Support** through OAuth flow customization
- **Expanded Security** with OIDC, CAPTCHA, Perimeter, DNS check on Portal, etc.

API Security leveraging AI and Machine Learning

Power your APIs with API Behavioral Security (ABS), integrated with Ping Intelligence to detect attacks against your APIs

+



Detect and block cyberattacks that target APIs, such as:

- Data, Application and System attacks
- API DDoS attacks
- Login Attacks (credential stuffing, fuzzing, stolen cookies & tokens)

Easily enable AI-powered threat protection on every API using Global Policy support

https://www.pingidentity.com/en/platform/api-security.html
https://developer.ibm.com/apiconnect/2019/02/12/ping-identity-and-ibm-partner-to-protect-against-api-cyberattacks/

Under the hook

Pre-req : ase-token

Global Policy (x-correlationid)

Pre-hook :

is request ok ?

authorization header ?

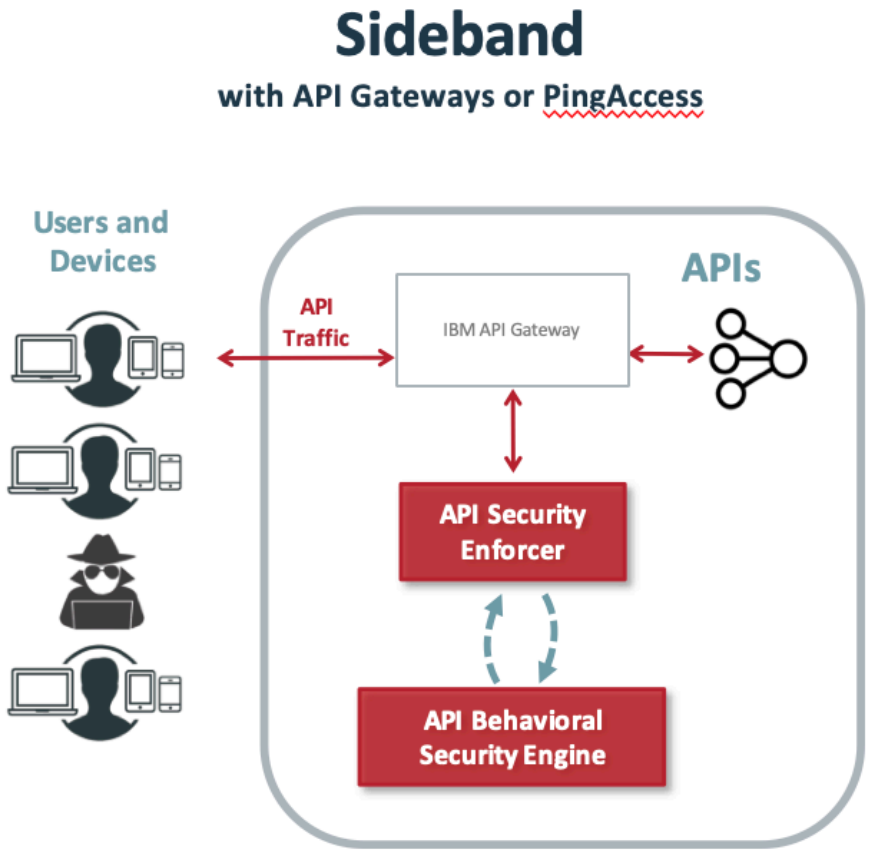
appId ?

cookie ?

Post-hook :

backend response

redact (record) for learning



Response Codes

#	Condition	Error Code
1	Good request (Normal User)	200 OK
2	Bad Request (Attacker)	403 Forbidden
3	Incorrect JSON format	400 Bad Request
4	Unknown API.	503 Service Unavailable
5	Authentication failure (ASE-Token)	401 Unauthorized

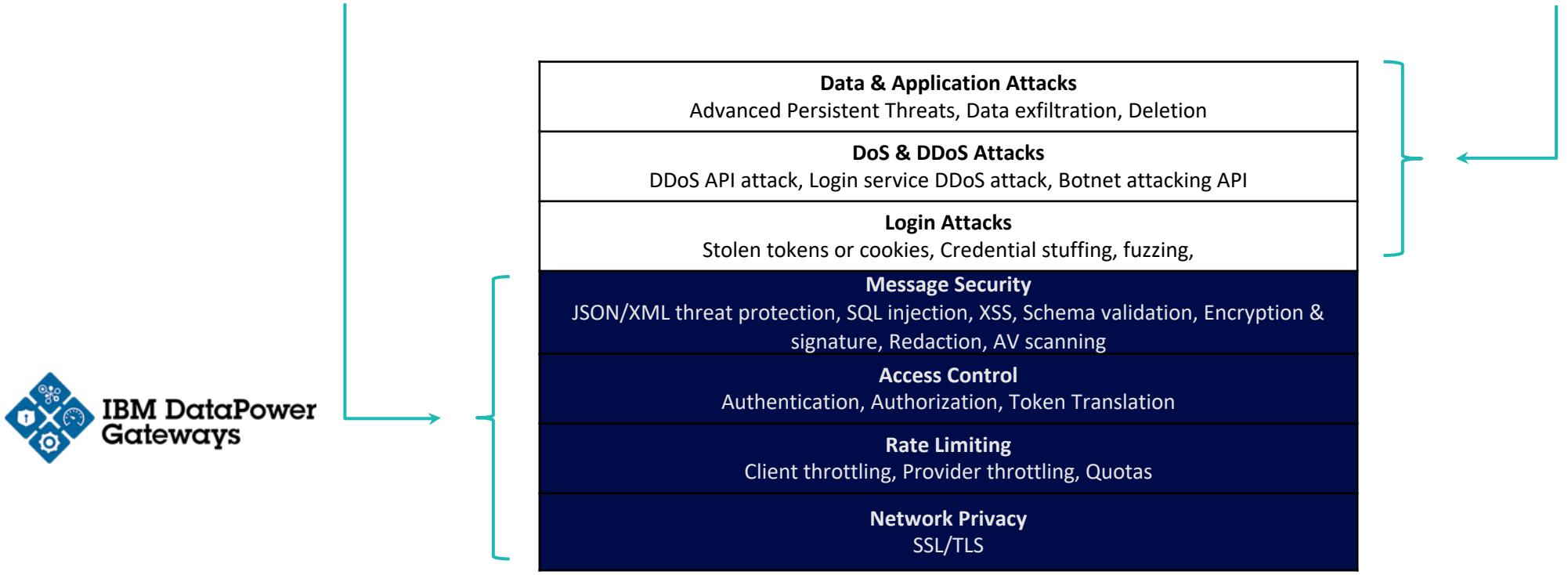
Comprehensive API Security with Ping and IBM

IBM API Connect

Scalable Multi-Cloud API Platform

PingIntelligence for APIs

AI-powered Threat Protection for APIs



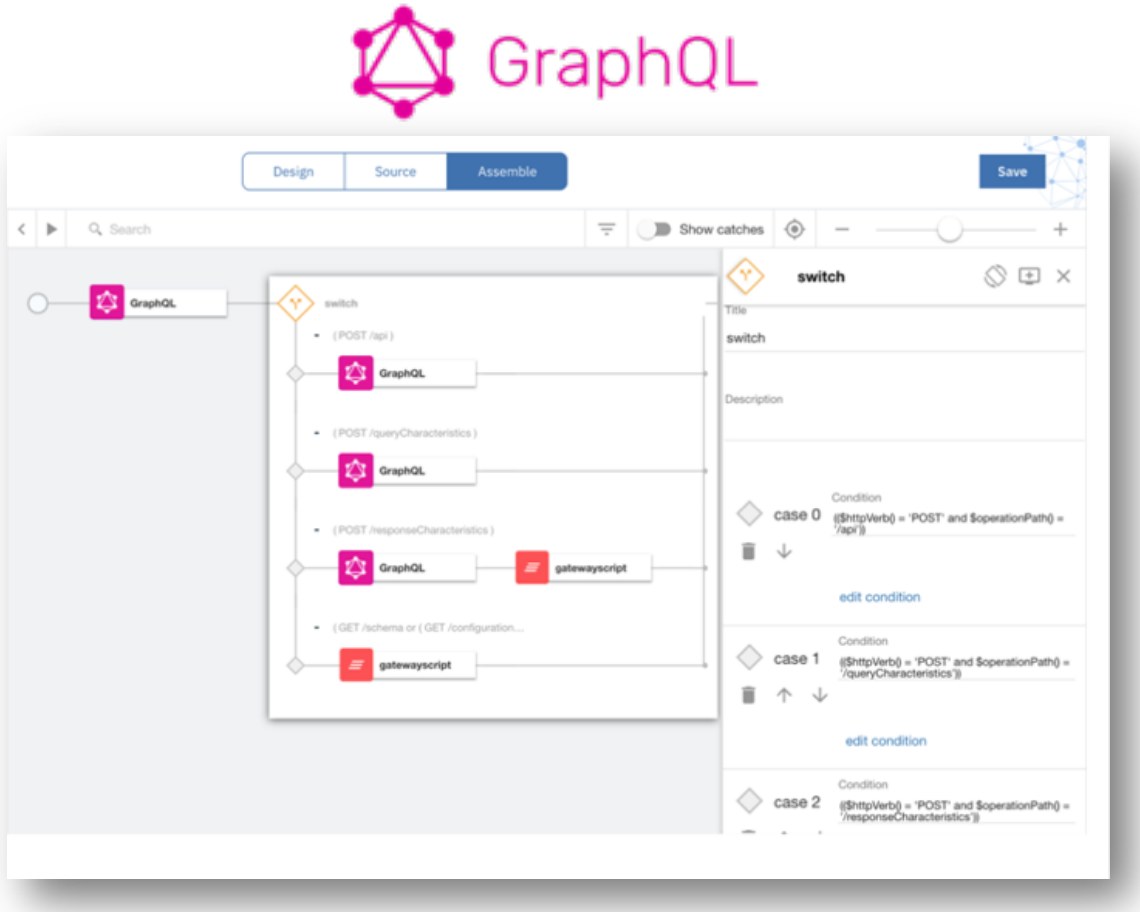
Secure & Manage GraphQL Endpoints

Next-Gen evolution of Gateway technology beyond Web services and REST with GraphQL support

Secure and Manage APIs with GraphQL backends, efficiently managing compute intensive services

Threat Protection against cyberattacks using advance query complexity analysis to prevent API-based attacks

Rate Limit GraphQL queries with consumer plans based on number of API calls & backend compute time



https://www.ibm.com/blogs/research/2019/02/graphql-api-management/
https://developer.github.com/v4/guides/resource-limitations/

GraphQL Endpoints security breakdown

1. Access Control
   - Who can access the data and what data
   - APIc
     - Client credential (application)
     - User credential (who)

2. Load Control
   - How much effort for the server to fulfill the request
     - Complexity
       - Type (object type)
       - Resolve
     - nesting

Cloud-Native API Gateway Service in DataPower

Up to 5X+ increased performance with natively built API Gateway using purpose-built technology for native OpenAPI/Swagger REST and SOAP APIs

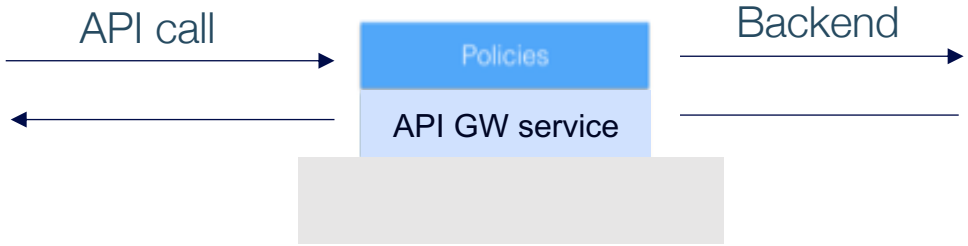
Multi-cloud scalability and extensibility to help meet SLAs and improve client user experience

Optimized drag & drop built-in policies for security, traffic control and mediation including flexible OAuth, enhanced JSON & XML threat protection

Secure to the core with self-contained signed & encrypted image to minimize risk, plus proven security policies to quickly protect APIs

Before: DP Multi protocol Gateway Service

New: Native API Gateway Service



Policies for Enforcement on API Gateway Service

Gateway Script and XSLT policy support provides flexible message mediation & dynamic security enforcement

Dynamic Routing support through Conditional Policy

Enforce strong security through Parse, JSON and XML Schema Validation policy

OpenID Connect support to enable banks to meet PSD2 / Open Banking regulations

OAuth Token revocation to enable self-service token management

Foundational	Security	Mediation
Invoke	API Key	Map
Activity Log	JWT Validate	JSON-XML
Rate Limit	JWT Generate	Gateway Script
Throw	OAuth Policy	XSLT
Set Variable	Parse (Threat Detection)	
Conditional	Validate	
	User Security	
	OpenID Connect	

Built-in policies

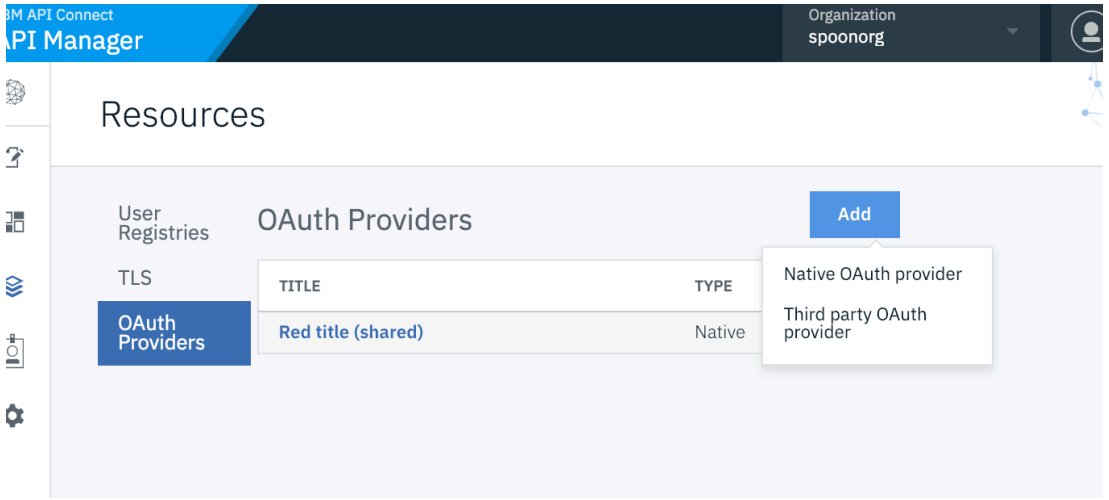
Meeting Security Needs through New Flexible OAuth Provider

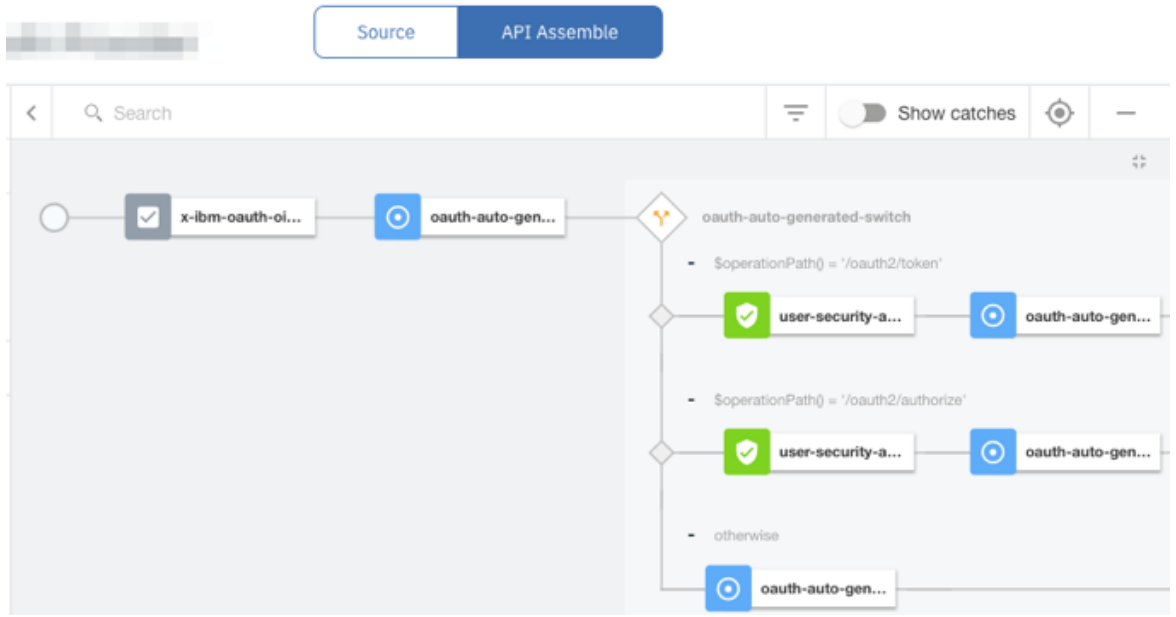
Rapid OAuth policy creation to quickly create OAuth provider security without deep security expertise

Improved governance capabilities on managing OAuth providers with flexible administrative access control to enforce enterprise standards

Ability to meet business demands with customizable OAuth assembly

New User Security policy to enforce authentication & authorization in API assembly, adapting to unique enterprise security needs





Feature list of OAuth in APIC V5, v2018+V5GW, v2018+APIGW

Features	V4	V5	v2018 + V5 CompatGW	v2018 + APIGW
Basic OAuth Support				
Distinct Client ids and Secrets	×			
Separate API	×			
Access Control	×	×		
Seamless packaging within product		×		
Tight coupling with Provider	×	×	*	
PKCE, Metadata, Token introspection, Revocation/Token Management, Advanced scope handling	×			
Customize OAuth Assembly	×	×	×	
Dynamic configuration updates	×	× **	× **	
Context variable driven	×	×	×	
Independent Resource Owner Security	×	×	×	
Out of the box OIDC support	×	× ***	× ***	
Out of the box JWT Authorization Grant	×	× **	× **	

* Tight coupling is only at the APIManager API level, not in the backend V5 Gateway
** Can be done with gateway extension
*** Supported by a set of rule in the assembly

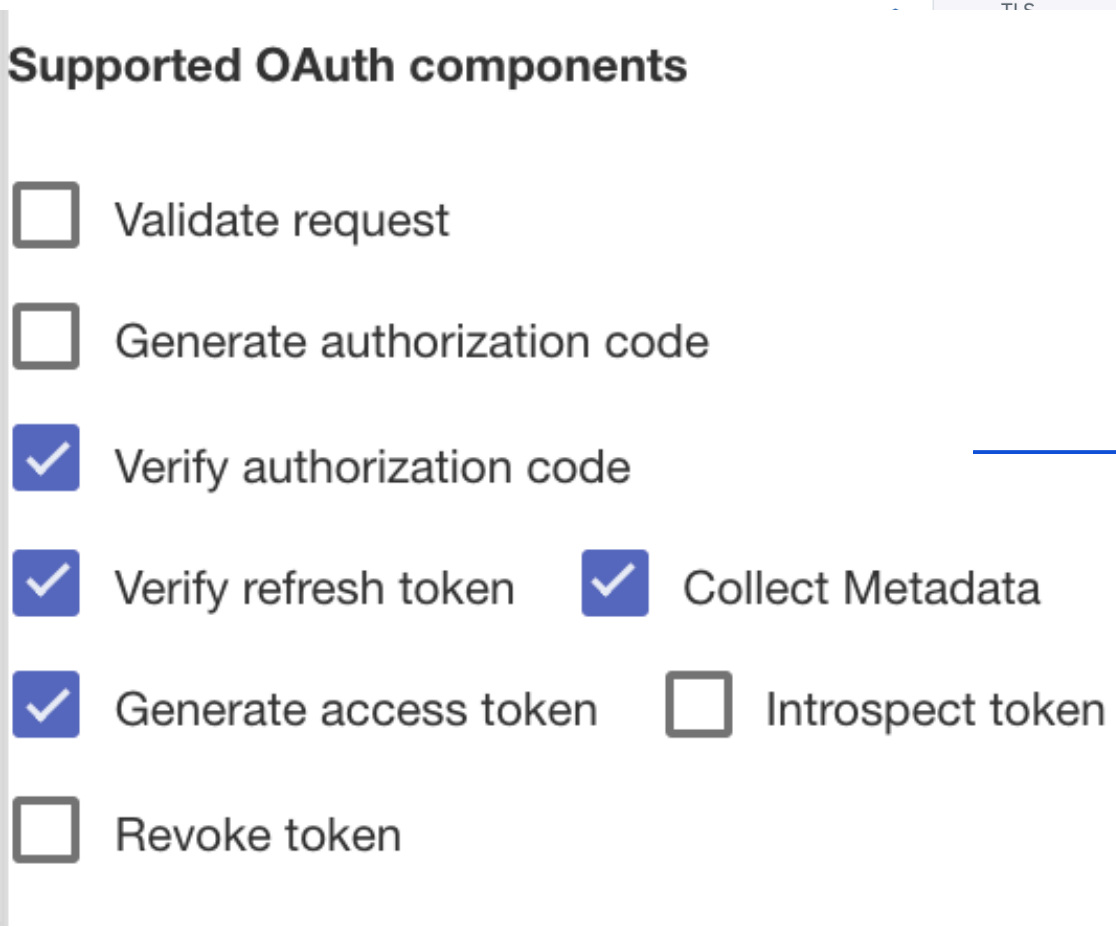
Meeting Security Needs through New Flexible OAuth Provider

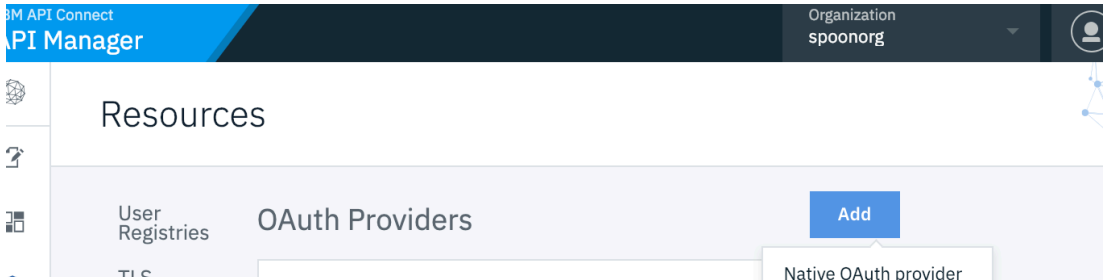
Rapid OAuth policy creation to quickly create OAuth provider security without deep security expertise

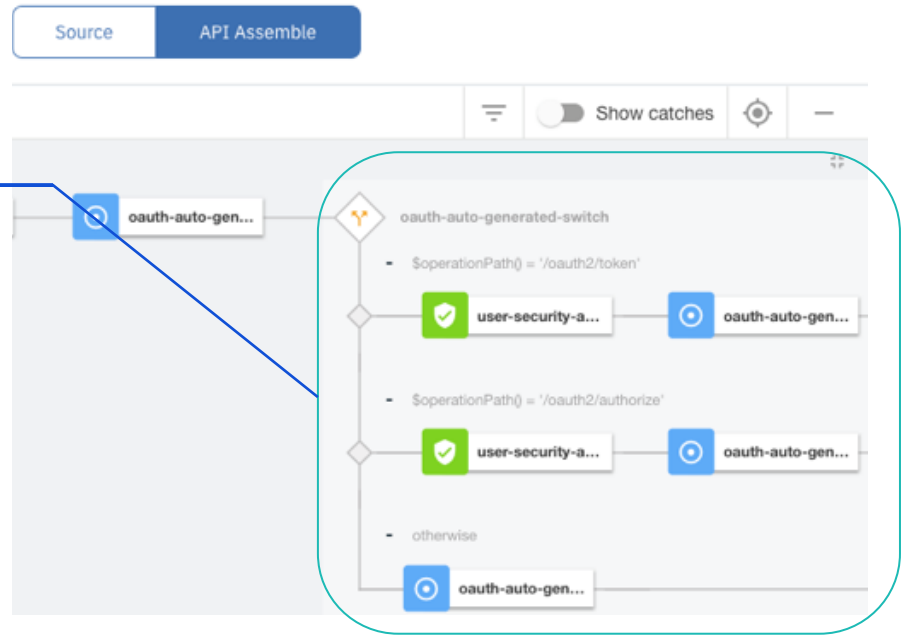
Improved gov
managing OAu
administrative
enterprise star

Ability to mee
customizable

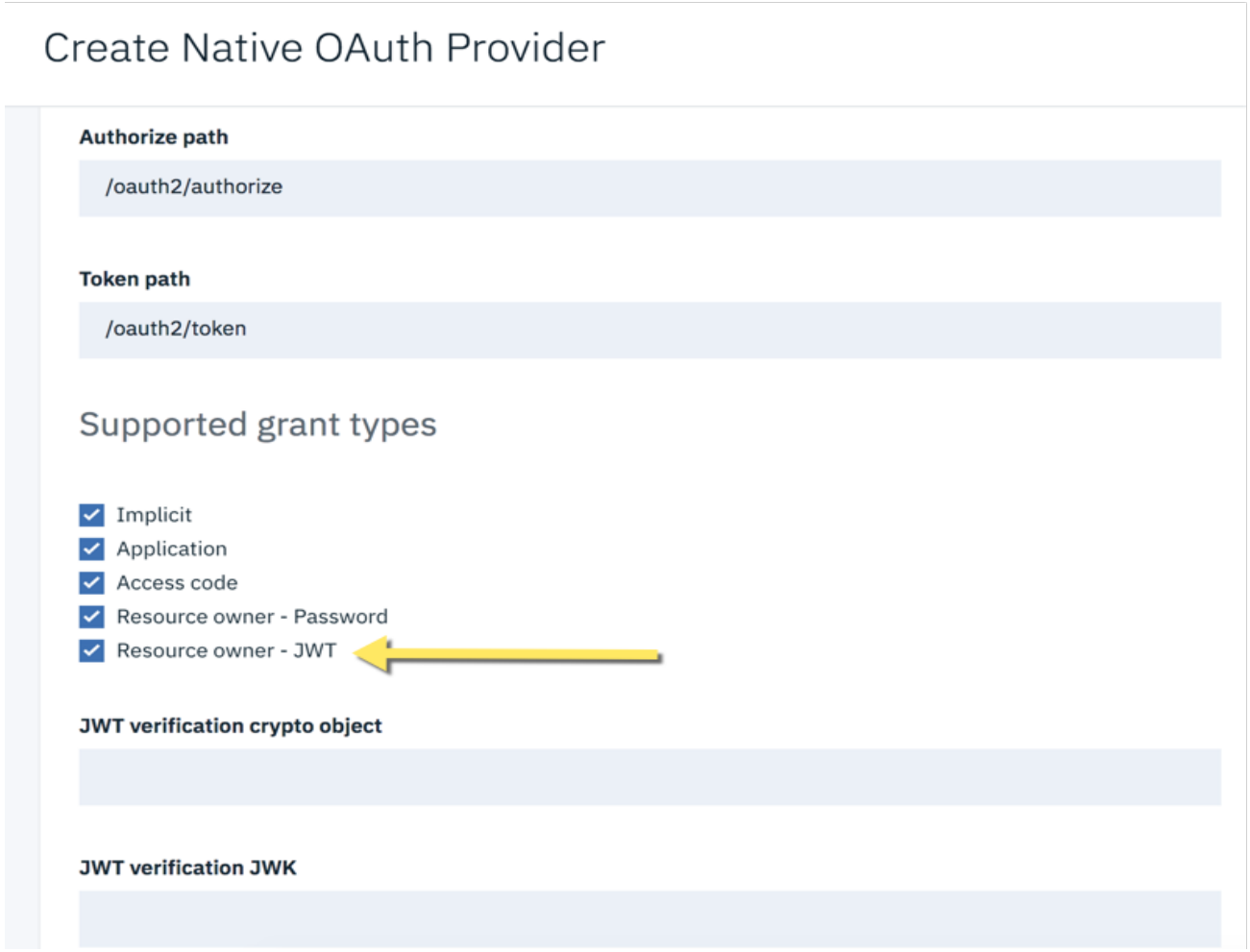
New User Se
authentication
adapting to ur



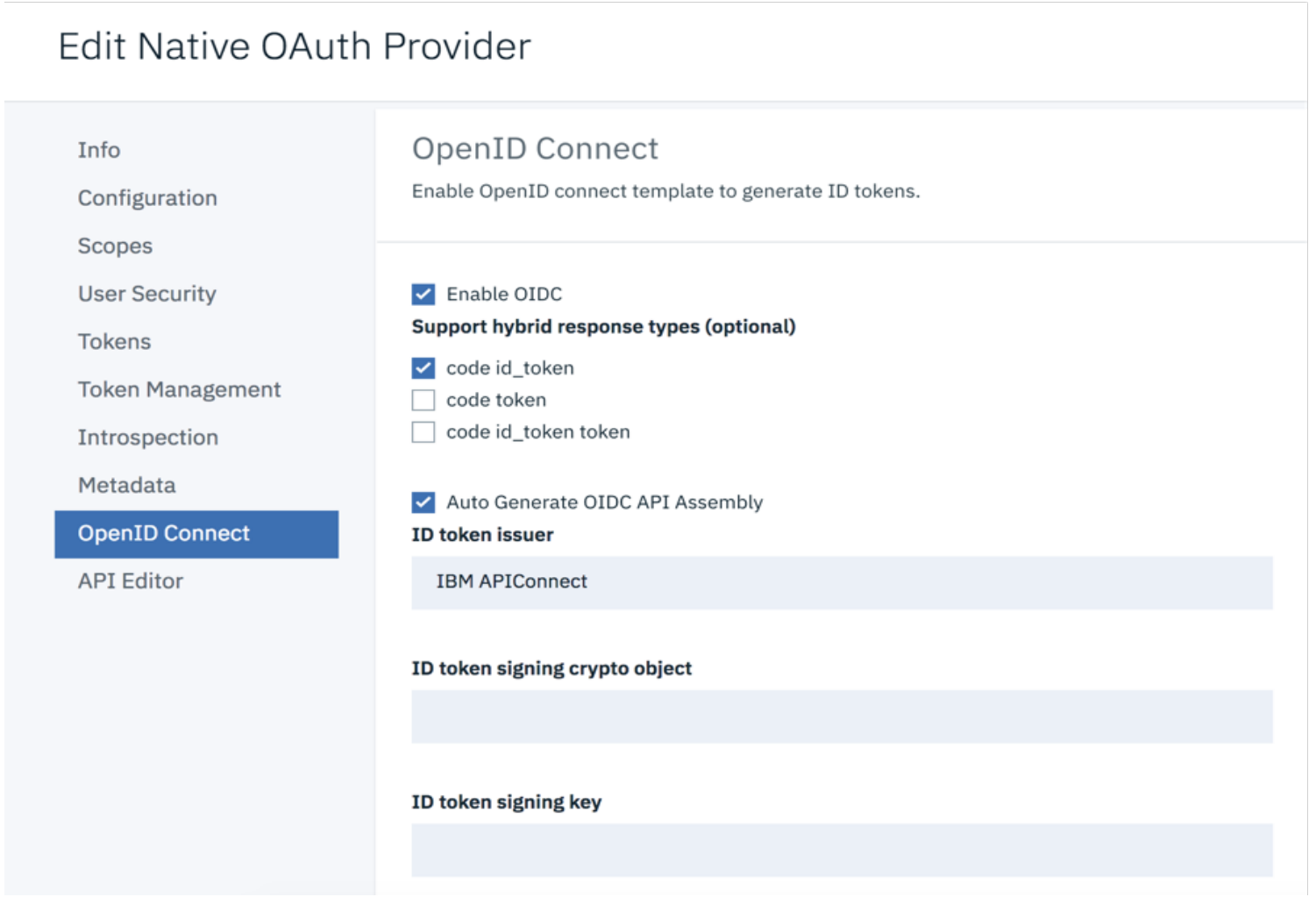




Out of the box JWT Grant Type Support



Out of the box OIDC Support



Customizable
Ease of use

- Crypto material on per OAuth native provider (vs gateway level)
- End user credential gathering (context variable) *
- Consent handling
- Global Policy (and thus inject context variable for processing) *
- Token handling (white listing)
- Flexibility
- ….

What should I do

- Monitoring IBM PSIRT for IBM APIC (APIm, Portal, Analytics), IBM DataPower
  - https://www.ibm.com/security/secure-engineering/process.html
- Timely upgrade/migration to a new version of firmware
- Balance your security needs vs platform offered (hardware vs ova vs docker vs ..)
  - How about cloud ? ICP ?
  - APIC Connect White Paper: https://www.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=03023503USEN&
- Security **vs** ease of use **vs** compatibility
- Performance/usage spike
- HA (rule of 3)
- Stateless (especially across Availability Zone)
- Gateway when used as part of APIC 2018, the configuration can be stored as in-memory (default) vs flash (persist)
  - Note that the sensitive information is available and exposed to the admin who has access to the gateway
  - Recommendation : in-memory

Gateway specific

- Is WebGUI needed for production (or any ports)
- Isolate application request traffic from admin request traffic
- Automate deployment (which APIc solves)
- Monitoring gateway (DataPower Operations Dashboard)
- Set up RBM
- Set up Backup administrator (do NOT loss password)
- ACL
- mTLS with your backend services (with right cipher, protocol 1.2, with EC, PFS)

Gateway specific

- Message validation (payload, size, nest level ..)
- Streaming vs no Streaming
- Payload redact
- SLM
- WhiteList vs BlackList
- Monitor tool (like DPOD), latency, cpu, memory ..

- Noisy neighbor (tenant vs application domain – work load isolation)
  - Different version of DP is running
  - Protect against noisy neighbor

Gateway specific

- GWS is expensive
- Context variable access is expensive
- Most of DP extension function is not available thru GWS
- Debug level is expensive (especially probe – payload sensitive data can leak)
- Log is best effort only (except audit event)
- By default, GW will ship what we consider as the secure setting
- Key material can be stored in local:///, this means the crypto material can be exported with domain export. Do consider keeping key material (especially private key and shared secret) in cert:/// sharedcert:///. Those 2 directories are with roach motel, the key material cannot be exported by GW. It can only be accessible thru secure backup and restore, which is protected by a couple keys, and only another DataPower can import and access the data. (roach motel model)
- Use HSM if paranoid is needed

From you, our audiences

- Your feedbacks ?
- What would you like to see ?
- What can you share with each others on your experience ? Good or Bad

Thank you. Merci. Gracias.

Thank You