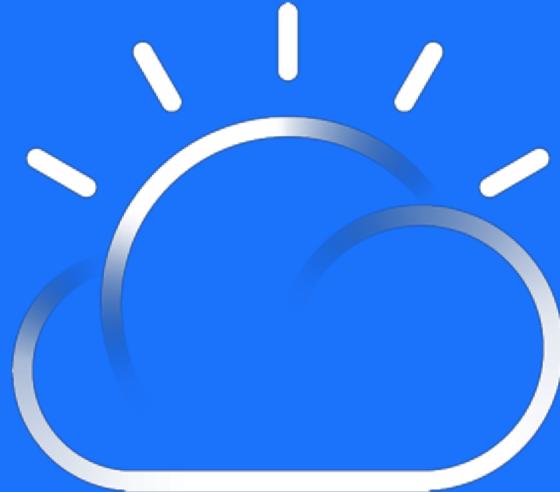


# API Connect & DataPower Extensibility



IBM Cloud

IBM

# Why Product Extensibility?

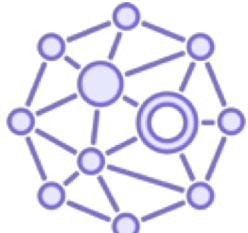
When considering a product purchase, evaluate a product under three main criteria's

1. [60%] Provides out-of-the box function to meet your business needs
2. [20%]: Provides roadmap for missing features
3. [20%]: *Is extensible to meet customize and meet your unique business requirements*

**Products exist to deliver market functionality** and don't expect them to completely provide individual business functionality



# IBM API Connect Components



IBM API Connect

Scalable Multi-Cloud API Platform



Management Service

API lifecycle management, governance & topology



API Gateway Service

Executes the API Transaction



Portal Service

Catalog of APIs and API subscription functions



Analytics Service

Collects data about the API transaction

# Agenda

- API Connect Installer
- API Manager
- API Gateway
- Analytics
- Developer Portal

# API Connect Installer & Helm Charts



**Helm charts package Kubernetes (k8) configuration** into a single archive, enabling tooling to deploy containers with user-driven values

- The APICUP installer creates subsystem Helm charts and k8 secrets for all subsystems.

```
// 1. Create helm charts based on apiconnect-up.yaml  
apicup subsys install mgmt --out=mgmt-out  
  
// 2. Modify helm charts  
  
// 3. Install management subsystem using modified helm charts  
apicup subsys install mgmt --plan-dir=./myProject/mgmt-out
```

- **Example:** Modify Kubernetes pod security policies to provide security that meets your enterprise security requirements

# API Connect Installer – Post Install Script



Each subsystem component allows you to run commands post-deployment

- Use extra-values file to modify configuration post-deployment

## **apiconnect-up.yaml**

```
apiVersion: v1
kind:
  apic.ibm.com/GatewaySubsystem
metadata:
  name: gateway
spec:
  CloudProperties:
    extra-values-file: gw-extras.yaml
```

## **apiconnect-up.yaml**

```
apiVersion: v1
kind:
  apic.ibm.com/ManagementSubsystem
metadata:
  name: manager
spec:
  CloudProperties:
    extra-values-file: manager-extras.yaml
```

## **gw-extras.yaml**

```
datapower:
  webGuiManagementState:
    "enabled"
  webGuiManagementPort: 9090
  webGuiManagementLocalAddress:
    0.0.0.0
```

## **manager-values.yaml**

```
apim:
  modes:
    standard:
      minReplicaCount: 1
      maxReplicaCount: 1
      minAvailable: 1
```

# Platform Scale & Flexibility with Microservices architecture

**Manage API Connect platform components** using Kubernetes management tools (ie kubectl)

**Individual scale platform components** to increase replica count seamlessly, including synchronization of data (ie kubectl scale <name> --replicas=4)

**Use built-in Kubernetes tooling (ie Istio)** to provide enhanced operational visibility, enabling easier integration with DevOps infrastructure

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

# Agenda

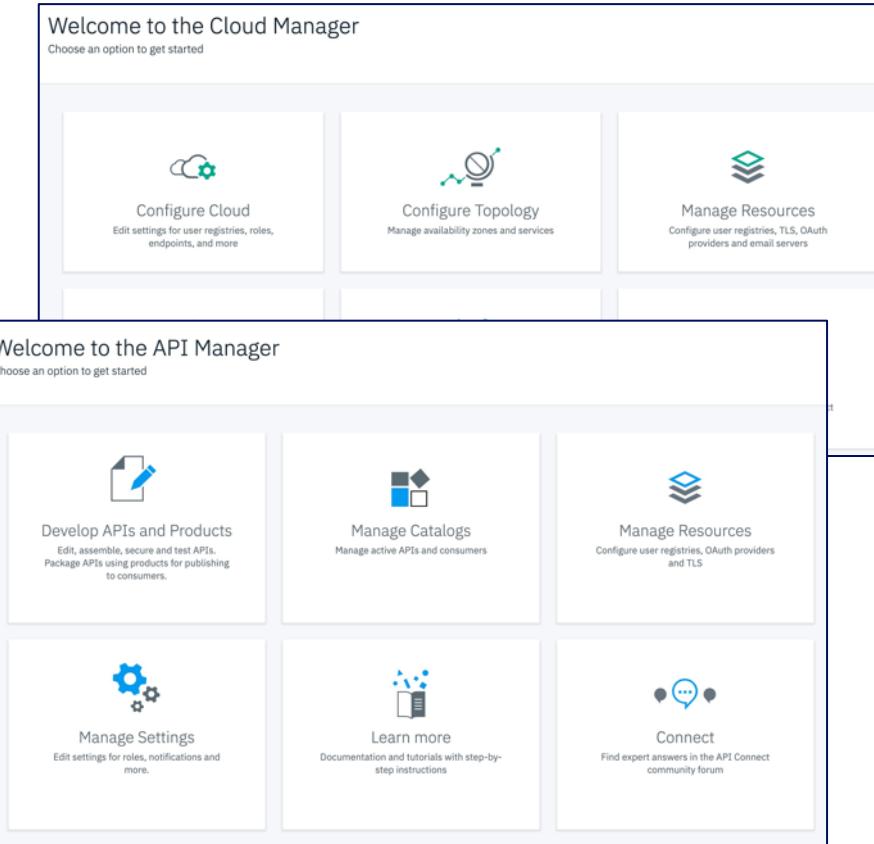
- API Connect Installer
- **API Management**
- API Gateway
- Analytics
- Developer Portal

# Extending Administrative Security for API Management Consoles

Accelerated on-boarding of (infrastructure) users, easily integrating with existing identity provider infrastructure

- **Supports OpenID Connect** for integration with identity systems with external logins
- **Using Authentication URL** to integrate with any third-party system over HTTP(s)
- **Integrate with existing LDAP repository** to provide consistent security policy enforcement

**Integrate with existing mail providers** to provide notifications for invites and approvals



# Use API Manager to catalog APIs

**API Manager allows you to catalog APIs**

to provide a single repository for API discovery

**Include API definitions** that exist without API enforcement or outside of the enterprise

- Available within the API Catalog and published into the developer portal



**API definition includes an Enforced flag**

to control whether API Gateway enforces API definition.

# Vendor Extensions

**Extensions to OpenAPI (Swagger) specification**  
to be referenced within the Open API definition

**Create a schema definition file** for an extension to support your API definitions with *custom fields*

**Dynamically influence API Gateway transactions**  
with data entered into *custom fields*

**Categorize and search custom fields** within the developer portal

## Extensions

Banking services

Branch type

ATM  
ATM  
Walk in  
Location

city

San Francisco

state

CA

citystate

San Francisco, CA

This is generated automatically from the previous two fields

# Agenda

- API Connect Installer
- API Management
- **API Gateway**
- Analytics
- Developer Portal

# Extend Gateway Behavior with Gateway Extensions

## Gateway Extensions are different between V5

MPGW and API Gateway service

- **V5 MPGW:** global rules executed at specific parts of the transaction
- **API Gateway:** modify DataPower configuration safely and managed across the deployment lifecycle

## Gateway Extensions contain DataPower API

Gateway CLI commands packaged within one or more .cfg files.

## Example Use Cases

- Modify default Gateway settings (ie timeouts)
- Package additional DataPower configuration outside of API Connect (eq MQ Queue Manager Object used within url-open)

## Change API Plan from Application to Client Id Scope

*mod-plan.cfg*

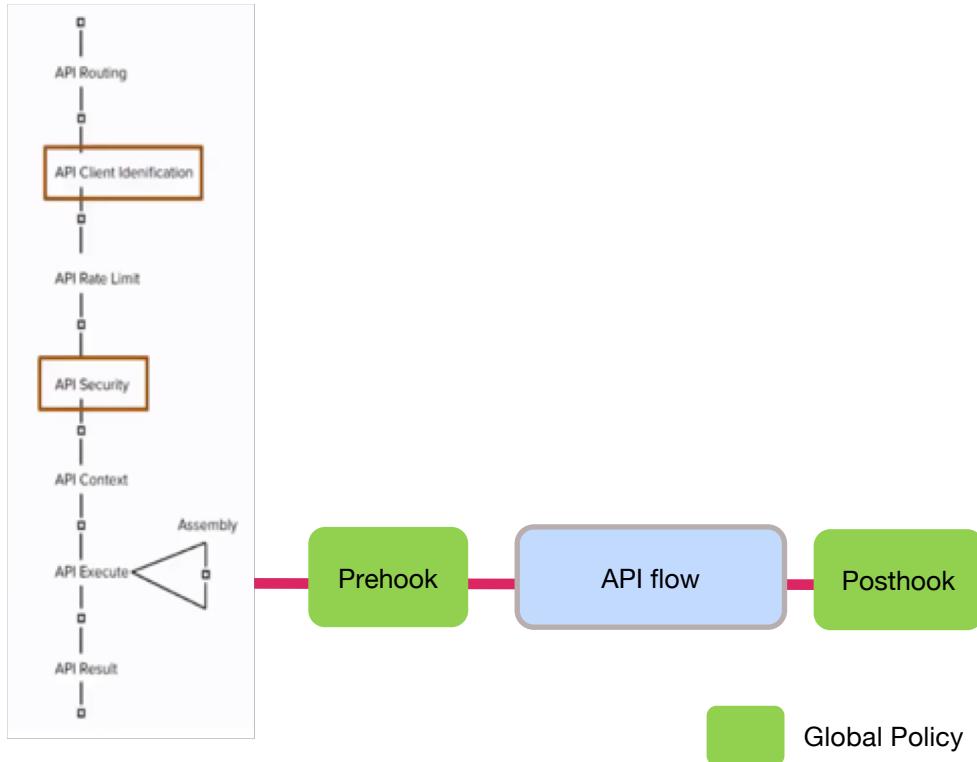
```
api-plan myorg_sandbox_financial-
services_1.0.0_basic
    rate-limit-scope per-client-id
exit
```

# Global Policies For Corporate Governance

**Enforce corporate standards**, e.g.  
security and logging, using different  
personas across multiple API definitions

**Global assembly flows** to enforce policies  
without changing individual API assembly  
definitions

**Any valid API Assembly policies** can be  
used as global policy pre or post hook  
actions



# Extend API Assembly with User Defined Policies

Create user-defined policies to extend built-in API Assembly policies, such as security, or routing of requests.

A user-defined policy is implemented as a DataPower processing rule

User-defined policies are configured within DataPower Web GUI

- Modify API Connect Gateway Service object with User-defined policies
- API Manager will dynamically discover policies and display it within API Assembly

The screenshot displays two main sections of the DataPower Web GUI:

**API Connect Gateway Service (bottom section):**

- Administrative state: enabled (radio button selected)
- Comments: (empty text field)
- Local address: 0.0.0.0 (text field), Select Alias (button)
- Local port: 3000 (text field)
- SSL client: gwd\_to\_mgmt (dropdown menu)
- SSL server: gwd\_to\_mgmt (dropdown menu)
- API gateway address: 0.0.0.0 (text field), Select Alias (button)
- API gateway port: 9443 (text field)
- Gateway Peering: apic (dropdown menu)
- V5 compatibility mode: (checkbox)

**User-defined policies (bottom section):**

- function-switch-on-author-01\_1.0.0
- function3\_1.0.0

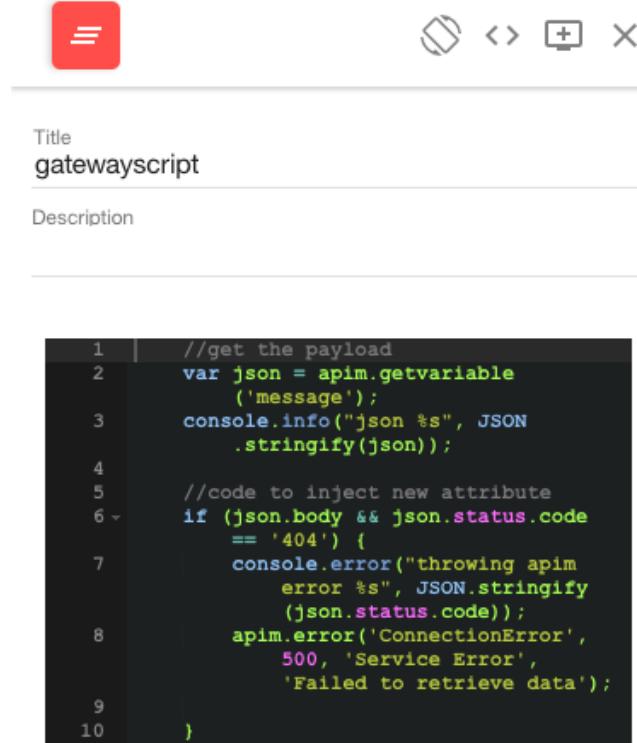
Both the "User-defined policies" section and the entire bottom panel are highlighted with a red border.

# GatewayScript for API Connect

Use **GatewayScript** to manipulate headers, payload or perform off-box calls using `url-open`.

**GatewayScript `multistep` module**  
allows you to call an existing DataPower processing rule

Use **context object** to access runtime context variables, payload & header information



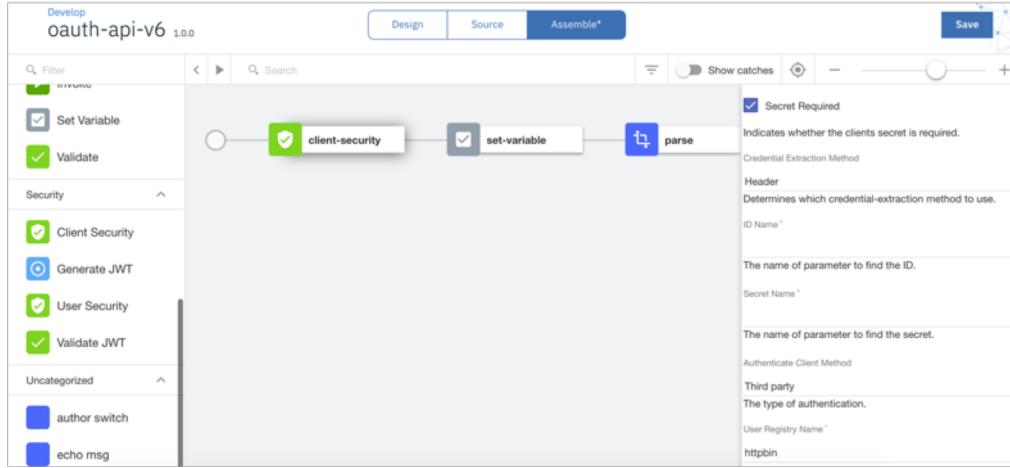
The screenshot shows a code editor interface with a red toolbar at the top. The title bar says "Title: gatewayscript". The code area contains the following GatewayScript code:

```
1 | //get the payload
2 | var json = apim.getvariable
   ('message');
3 | console.info("json %s", JSON
   .stringify(json));
4 |
5 | //code to inject new attribute
6 | if (json.body && json.status.code
   == '404') {
7 |   console.error("throwing apim
   error %s", JSON.stringify
   (json.status.code));
8 |   apim.error('ConnectionError',
   500, 'Service Error',
   'Failed to retrieve data');
9 |
10 }
```

# Customize Client Authentication – App Client Security Policy

## New Client Security Policy in API Gateway Service

- **Integrate with Third Party Providers** to authenticate using third-party Client ID and optionally Client Secret
- **Customize API Key Security requirements** (ie perform two-factor authentication with API Key validation and external source)

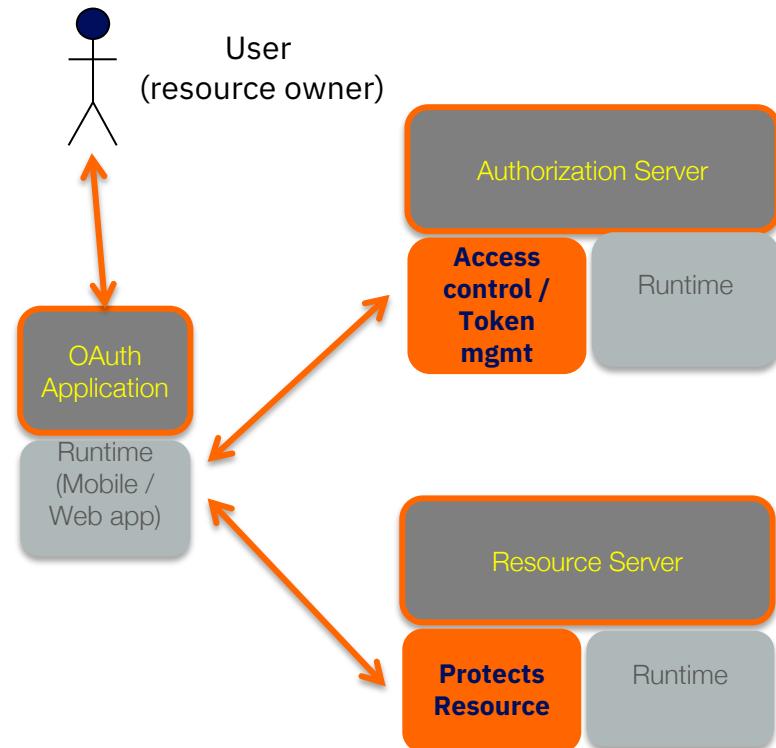


# API Connect OAuth Provider

**OAuth:** Allow you to share your resources with a third party application

**Authorization server:** validates resource owner credentials and generates authorization code and access token

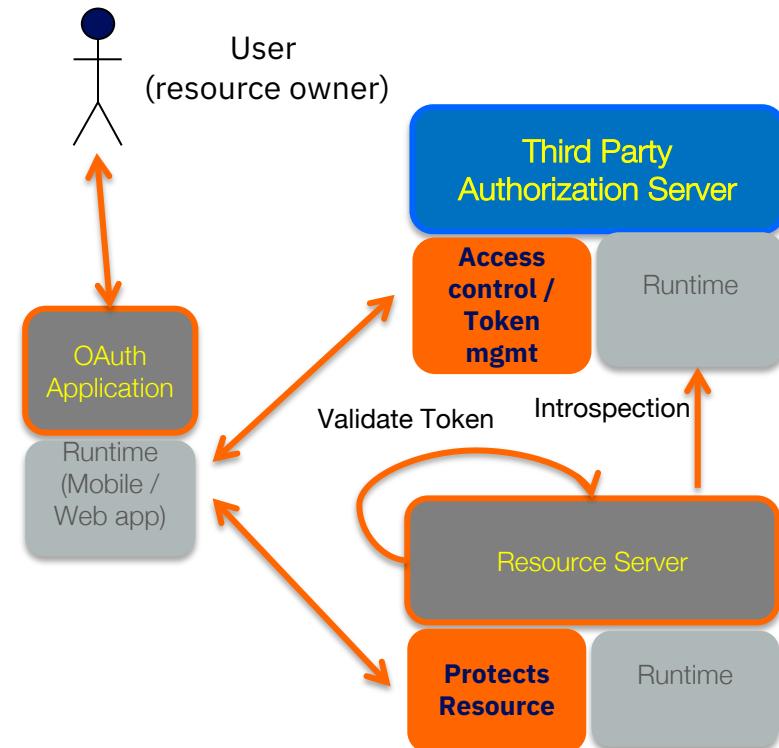
**Resource server:** protects backend API via an access token



# Third Party Provider - Offload OAuth Token Generation

**Authorization server:** Third-party OAuth server validates resource owner credentials and generates authorization code and access token

**Resource server:** Enforces access to API by introspection (validate access token with third party) or cryptographically validating token locally

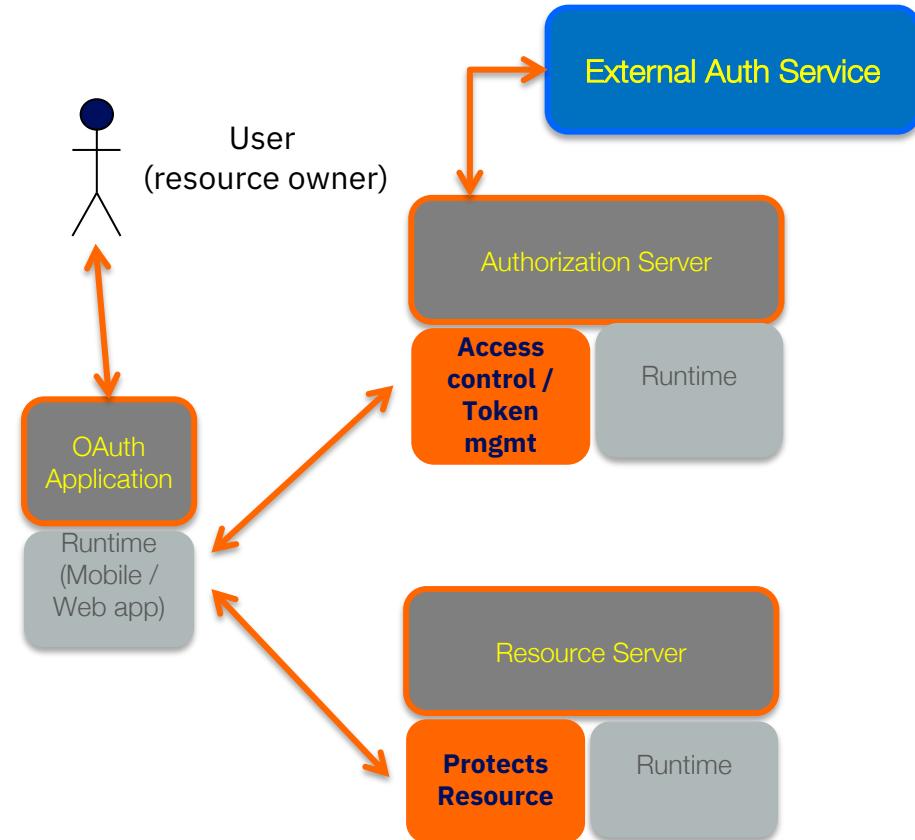


# Offload OAuth Resource Owner Authentication & Authorization

**Authorization server:** authentication / authorization of resource owner is performed using third-party authentication service

Generates authorization code and access token after successful authentication / authorization

**Resource server:** protects backend API via an access token



# OAuth Provider Extensibility

**Include custom metadata** within OAuth access token or payload

**Control user permissions with scopes** with scopes based on user / application to enforce stronger & flexible resource control at multiple levels

## OAuth Token Management & Lifecycle

- Use Refresh tokens to obtain a new access token w/o starting from scratch
- OAuth Token Revocation to revoke access tokens

### Metadata

Specifies whether and v

Collect metadata

#### Source

Authentication URL

External URL

### Advanced Scope Check before Token Generation

Specify the scope check endpoint where additional scope verification is performed in addition to the defined scopes.

Application scope check

Owner scope check

### Advanced Scope Check after Token Validation

Specify the scope check endpoint where additional scope verification is performed in addition to the defined scopes.

Enabled

# Agenda

- API Connect Installer
- API Management
- API Gateway
- **Analytics**
- Developer Portal

# Customize Analytics configuration file

**Offload analytics** to external logging infrastructure using logstash pipelines

**Customize Logstash pipelines** for enhanced data filtering when used with Kibana

**Modify Kibana index patterns** to manage fields available for creating dashboards

The screenshot shows the 'Management Endpoint' settings page. It includes fields for 'Endpoint' (set to `https://mystack-a7s-client.argo2-sl.dev.ciondemand.com`) and 'TLS Client Profile' (set to 'Analytics client TLS client profile'). A red box highlights the 'Advanced Analytics Configuration' button, which has a gear icon and the text 'Advanced Analytics Configuration'. Below this, there are sections for 'Kibana' (with 'Index Patterns' and 'Advanced Settings' buttons), 'API Connect', 'Ingestion', and 'Storage'.

# Agenda

- API Connect Installer
- API Manager
- API Gateway
- Analytics
- **Developer Portal**

# Customize Developer Portal

Custom Portal Theme

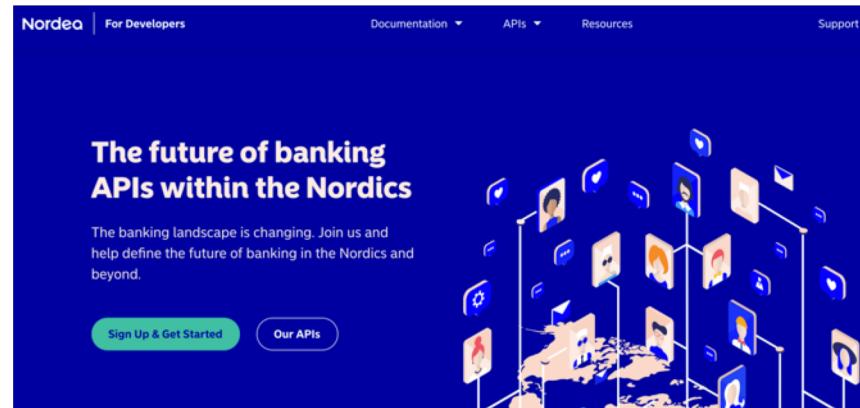
Control behavior with Configuration

Taxonomies, Images, attachment, new pages etc.

Custom fields to content types

Customize Layout with Twig template

Extend with Custom Modules



# Custom Theme Generation

Complete the form below and you will be presented with a custom sub-theme to download.

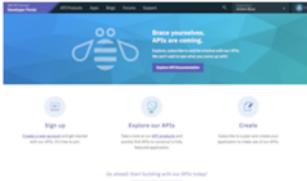
**Sub-theme name \***

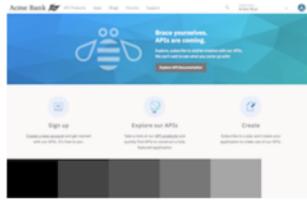
A custom theme name, for example: 'mycustom\_theme' or 'banka\_theme'. The name does not need to end in '\_theme' but it is a common convention.

**Sub-theme type**  
 CSS  
 SCSS

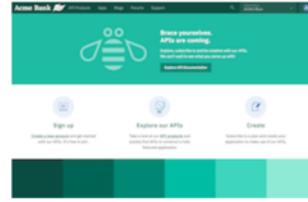
Your sub-theme can be setup to use either CSS or SCSS. SCSS is an extension to CSS and is for more advanced theme developers.

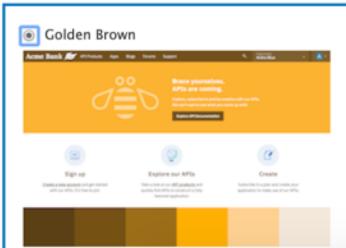
**Template**

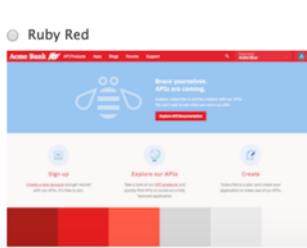
Default Connect Theme  


Business Mono  


Sapphire Blue  


Emerald Green  


Golden Brown  


Ruby Red  


# Notices and disclaimers

© 2018 International Business Machines Corporation. No part of this document may be reproduced or transmitted in any form without written permission from IBM.

## **U.S. Government Users Restricted Rights – use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.**

Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. **This document is distributed “as is” without any warranty, either express or implied. In no event, shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.** IBM products and services are warranted per the terms and conditions of the agreements under which they are provided.

IBM products are manufactured from new parts or new and used parts. In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply.”

**Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.**

Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.

References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.

Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.

It is the customer’s responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer’s business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer follows any law.

# Notices and disclaimers continued

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products about this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products.

Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. **IBM expressly disclaims all warranties, expressed or implied, including but not limited to, the implied warranties of merchantability and fitness for a purpose.**

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.

IBM, the IBM logo, ibm.com and [names of other referenced IBM products and services used in the presentation] are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at: [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

