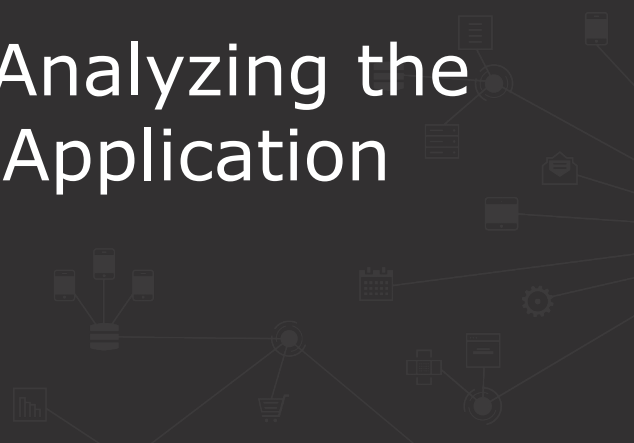


# Module 10

## Monitoring and Analyzing the Behavior of the Application Network

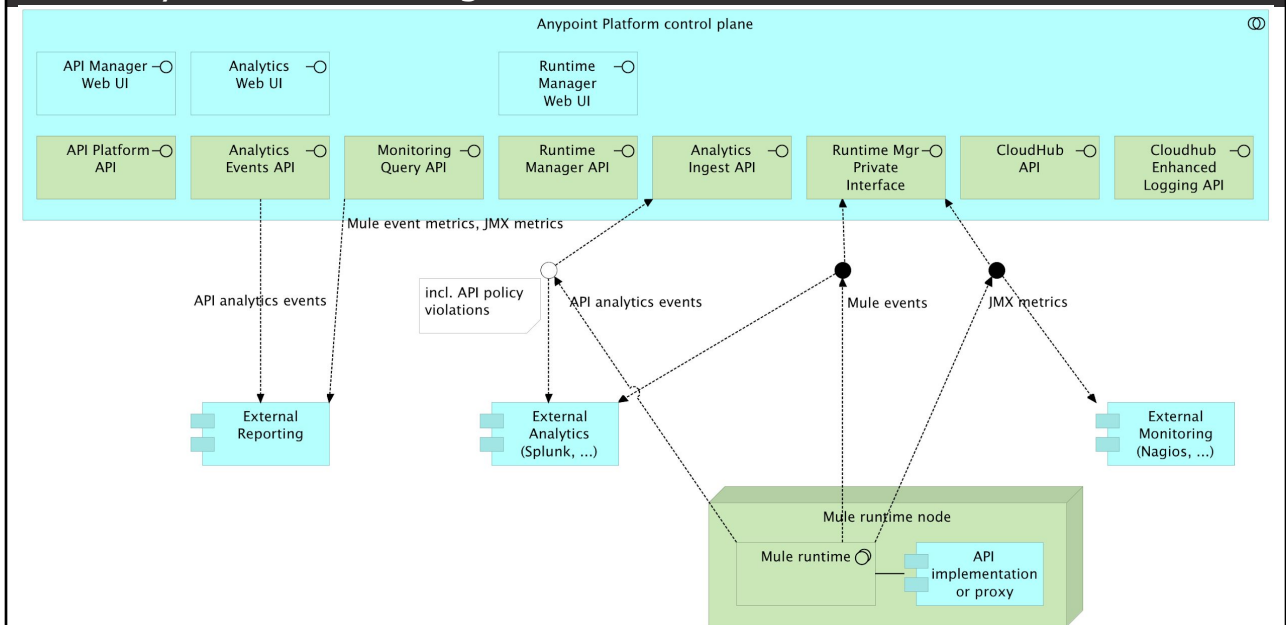
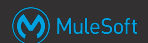


### Objectives

- Describe **origins of data** for monitoring, analysis and alerting
- Describe the **metrics** collected on the level of API invocations
- Describe the available **grouping** of API metrics for analysis
- Make use of options for performing **API analytics** in/outside of Anypoint Platform
- Define **alerts** for API invocations in all tiers of API-led connectivity
- Use metrics and alerts for **API implementations** to augment those for API invocations
- Recognize **operations teams** as stakeholder in API-related assets

# Understanding monitoring data flow in Anypoint Platform

## Data flows for Anypoint Platform monitoring, analytics and alerting



# Using Anypoint Analytics to gain insight into API invocations



## Metrics in Anypoint Analytics



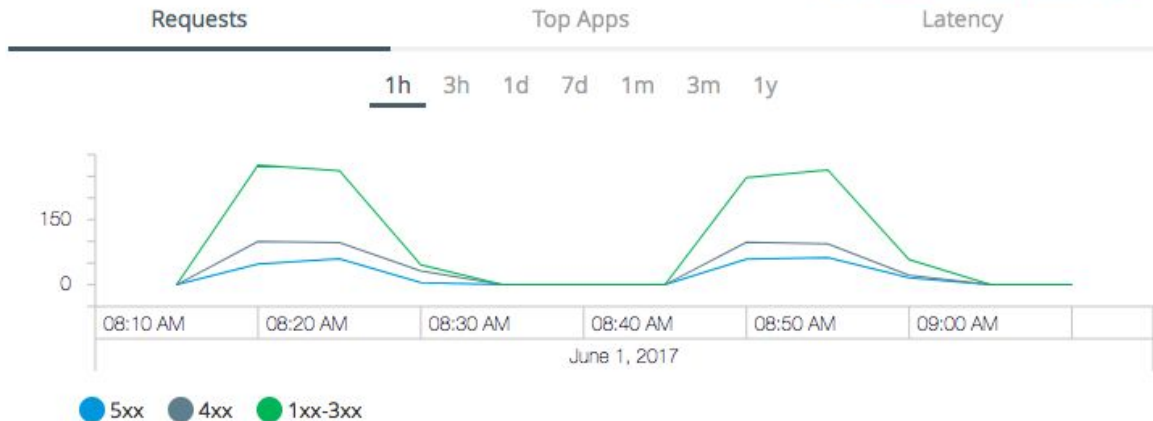
- **Number** of API invocations (requests)
  - Successful: **[100, 400)**
  - Unsuccessful due to a client error: **[400, 500)**
  - Unsuccessful due to a server error: **[500, 600)**
- Mean **response time** (average latency)
- Request and response **payload size**
- Properties of the **API client**:
  - Client ID (if registered), geographical location, OS platform, ...
- Properties of the **API invocation**:
  - resource path, HTTP method, ...
- Metrics can be **grouped** and displayed along various dimensions:
  - for one/all API(s) and one/all API client(s)
  - custom

## Metrics in Anypoint Analytics



**Number of API invocations** (requests) over time for a given API and all its API clients, grouped by HTTP status code class

[Analytics Dashboard](#) [Download CSV](#)

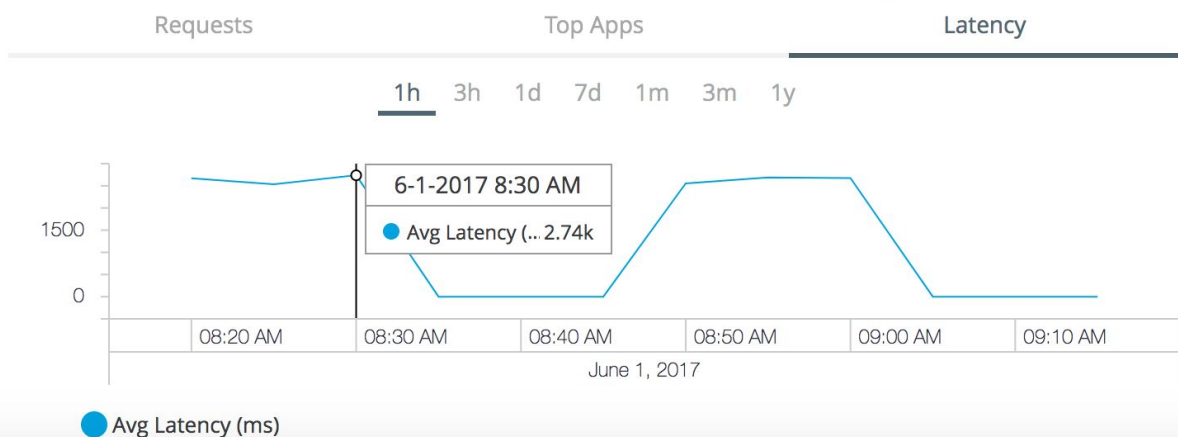


## Metrics in Anypoint Analytics

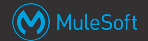


**Mean response time** (average latency) of API invocations over time for a given API and all its API clients and all HTTP status codes

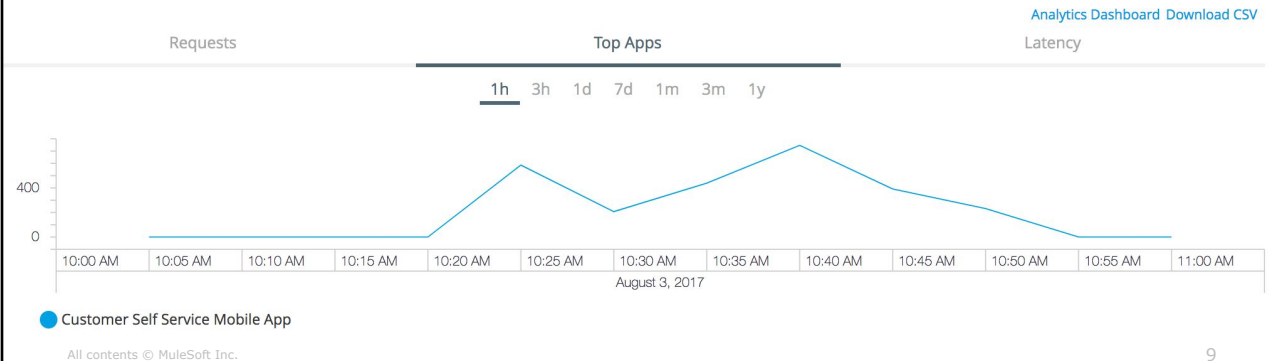
[Analytics Dashboard](#) [Download CSV](#)



## Analyzing API invocations to the "Mobile Auto Claim Submission EAPI"



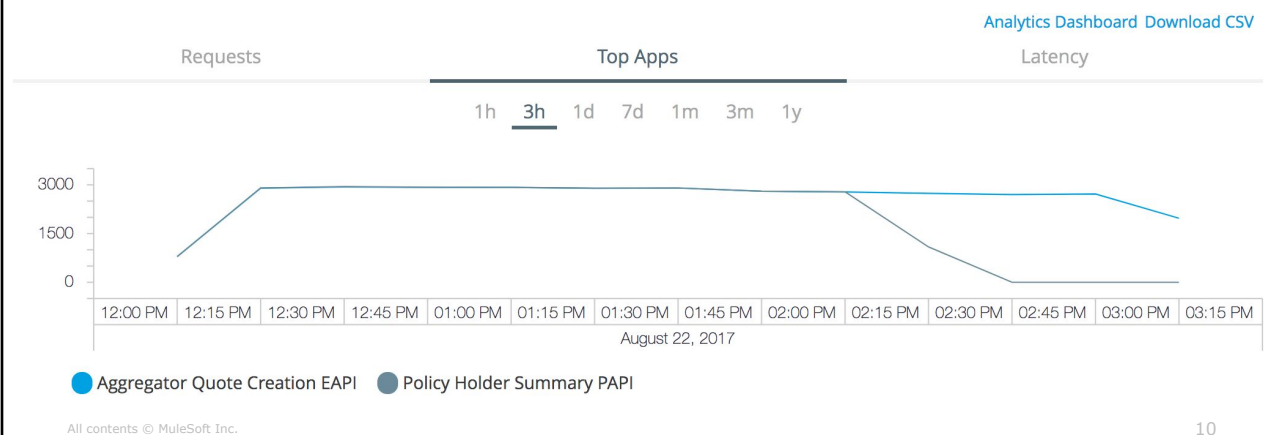
**Number of API invocations** (requests) over time to the "Mobile Auto Claim Submission EAPI", grouped by each of its top 5 API clients



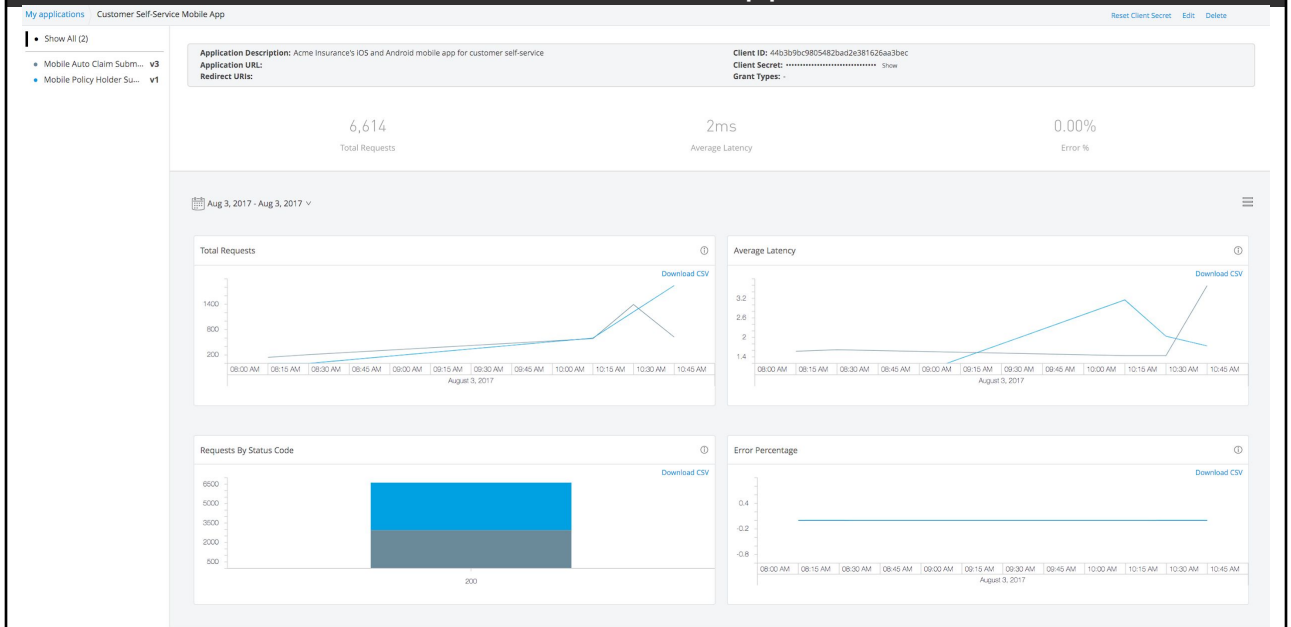
## Analyzing API invocations to the "Policy Holder Search PAPI"



**Number of API invocations** (requests) over time to the "Policy Holder Search PAPI", grouped by each of its top 5 API clients



# Analyzing API invocations from the perspective of the Customer Self-Service Mobile App



## Analyzing API invocations across the application network

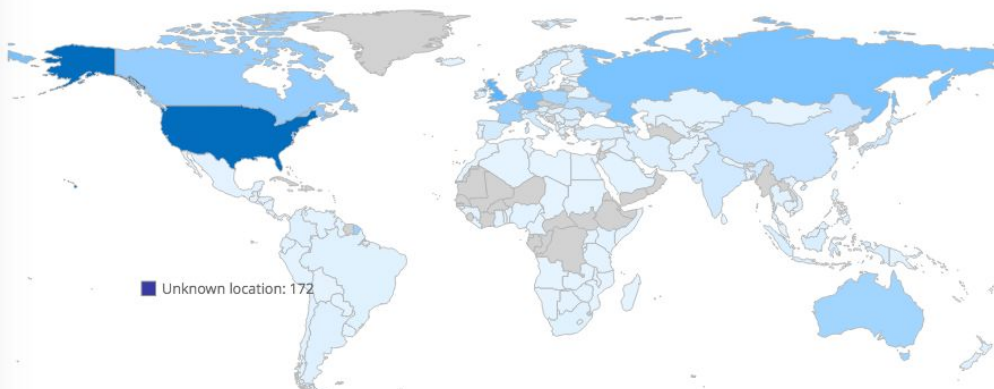


- **Anypoint Analytics** can perform standard and custom analyses across all API invocations in an application network:
  - **Interactive** exploration through drill-down
  - Definition of **custom charts and dashboards**
  - Definition of **custom reports**
  - Exporting all data underlying a graph to **CSV** files
  - Access to all data via Anypoint **Platform APIs**

## API invocation analysis by geography

**Number of API invocations** from all API clients to all Experience APIs, grouped by geography

Requests by Location

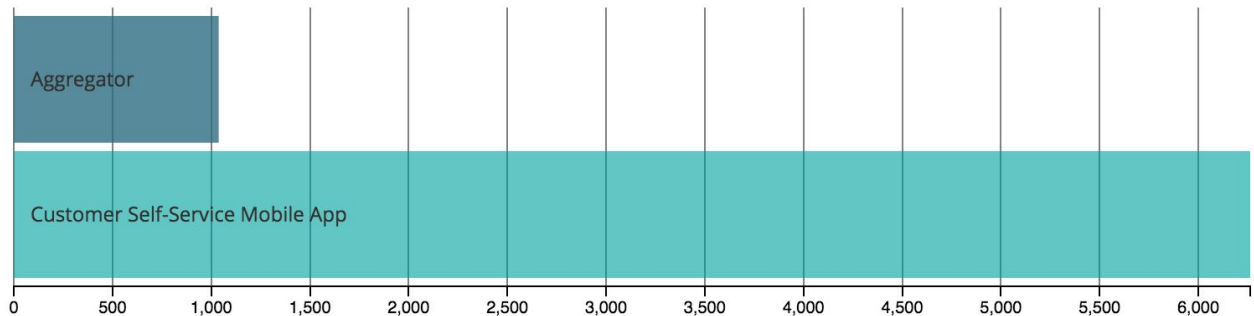


## API invocation analysis by API client



**Number of API invocations** to all Experience APIs, grouped by API clients, over the last hour

Requests by Application

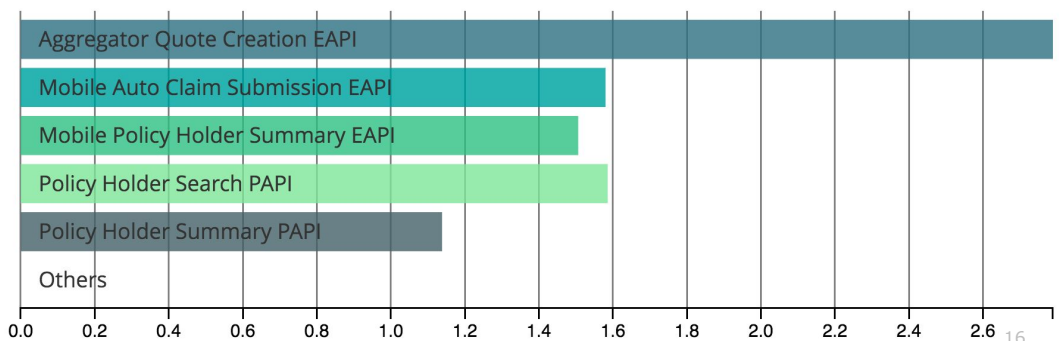


## API invocation analysis by response time



Custom chart showing **average (mean) response time** per API invocation in milliseconds for the top 5 slowest APIs, for the last 90 days

Average response time by API



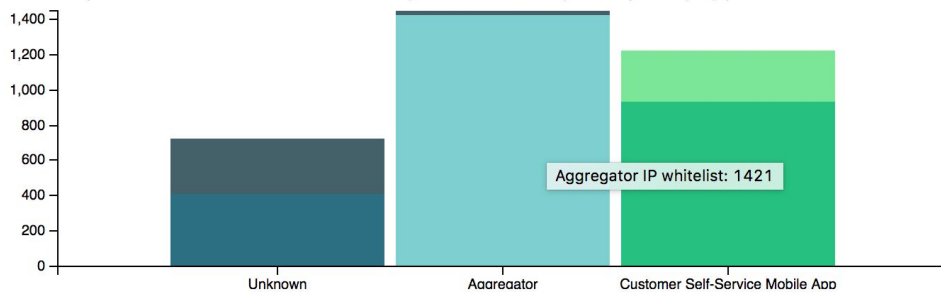


Custom chart showing **number of policy violations**, grouped by API policy and API client, over the last 90 days

Date Range: 1 Day ▾

## API Policy violations by API client

Groups the number of API Policy violations by the policy type and API client ID



All content

17

# Defining alerts for exceptional occurrences in an application network



# Introducing alerts at the level of API invocations



- **Alerts based on these metrics** of API invocations:
  - Number of **violations** of a given policy
  - Request count (**number of API invocations**)
  - **Response code** in given set of HTTP response status codes
  - **Response time** exceeding given threshold in milliseconds
- Alert is triggered **when** the metric
  - Falls above/below a **threshold**
  - For a given number of **time periods** of a given duration
- **C4E guideline:** alerts should at least cover:
  - All **violations of API policies**
  - All **violations of QoS guarantees** not explicitly captured in API policies

All contents © MuleSoft Inc.

19

# Defining alerts for "Policy Options Retrieval SAPI"



## Policy Options Retrieval SAPI v1

Actions ▾

API Status: ● Active    Asset Version: 1.0.0    Type: RAML/OAS

Implementation URL: <http://ans-policyoptionsretrieval-sapi.cloudhub.io/v1>

Consumer endpoint: <http://ans-policyoptionsretrieval-sapi.cloudhub.io/v1>

View API in Exchange >

View configuration details >

View Analytics Dashboard >

Add alert

Q Search

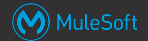
✕

Name	Type	Date modified	Date created	Enabled	
> Client not in Process API subnet for "Policy Options Retrieval SAPI"	Policy	1/17/18 6:32 PM	1/17/18 6:32 PM	Yes	<button>Edit</button> <button>Delete</button>
> SLA tier exhausted for "Policy Options Retrieval SAPI"	Policy	1/17/18 6:31 PM	1/17/18 6:31 PM	Yes	<button>Edit</button> <button>Delete</button>

All contents © MuleSoft Inc.

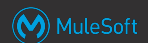
20

## Defining alerts for "Policy Options Retrieval SAPI"



- **SLA tier exhausted:**
  - Violation of **SLA-based Rate Limiting**, severity **Info**, > 60 violations for at least 3 consecutive 10-minute periods
  - Alerts when approx. **10%** of 1-second intervals are **above limit defined by SLA tier**
  - Also alerts on **invalid client ID/secret** supplied
- **Client not in Process API subnet:**
  - Violation of **IP whitelist**, severity **Critical**, > 1 violation for at least 3 consecutive 1-minute periods
- Could add alert for violations of **Spike Control**

## Defining alerts for "Policy Holder Search PAPI"



Policy Holder Search PAPI v1

Actions ▾

API Status: ● Active Asset Version: 1.0.3 Type: RAML/OAS

Implementation URL: <http://ans-policyholdersearch-papi.cloudhub.io/v1>

Consumer endpoint: <http://ans-policyholdersearch-papi.cloudhub.io/v1>

View API in Exchange >

View configuration details >

View Analytics Dashboard >

Add alert

Q Search

×

Name	Type	Date modified	Date created	Enabled	
> Client not in Experience API or Process API subnet for "Policy Holder Search PAPI"	Policy	1/17/18 6:39 PM	1/17/18 6:39 PM	Yes	<button>Edit</button> <button>Delete</button>
> Response time QoS guarantee violated by "Policy Holder Search PAPI"	Response Time	1/17/18 6:40 PM	1/17/18 6:40 PM	Yes	<button>Edit</button> <button>Delete</button>
> Throughput QoS guarantee exhausted for "Policy Holder Search PAPI"	Policy	1/17/18 6:38 PM	1/17/18 6:38 PM	Yes	<button>Edit</button> <button>Delete</button>

- **Throughput QoS guarantee exhausted:**
  - Violation of **Spike Control**, severity **Info**, > 60 violations for at least 3 consecutive 10-minute periods
  - Alerts when approx. **10%** of 1-second intervals are **above limit**
- **Client not in Experience API or Process API subnet:**
  - Violation of **IP whitelist**, severity **Critical**, > 1 violation for at least 3 consecutive 1-minute periods

- **Response time QoS guarantee violated:**
  - Severity **Warning**, > 6600 requests whose response time > 100 ms for at least 3 consecutive 10-minute periods
  - Alerts when approx. **1%** of API invocations (1% of  $1100 \times 60 \times 10 = 6600$ ) are **above limit** of 100 ms (twice the target median of 50 ms)
  - Note that **exact QoS guarantee** cannot be expressed in alert
    - median = 50 ms, maximum = 150 ms
- Should add alert for violations of **Client ID enforcement**

## Defining alerts for "Aggregator Quote Creation EAPI"

Aggregator Quote Creation EAPI v1

Actions ▾

API Status: ● Active Asset Version: 1.0.1 Type: RAML/OAS

Implementation URL: <http://ans-aggregatorquotecreation-eapi.cloudhub.io/v1>

Consumer endpoint: <http://ans-aggregatorquotecreation-eapi.cloudhub.io/v1> 

[View API in Exchange](#) >

[View configuration details](#) >

[View Analytics Dashboard](#) >

Add alert

Search

×

Name	Type	Date modified	Date created	Enabled	
> Response time QoS guarantee violated by "Aggregator Quote Creation EAPI"	Response Time	1/17/18 3:17 PM	1/17/18 3:17 PM	Yes	<button>Edit</button> <button>Delete</button>
> SLA tier exhausted for "Aggregator Quote Creation EAPI"	Policy	1/17/18 3:10 PM	1/17/18 3:10 PM	Yes	<button>Edit</button> <button>Delete</button>
> TLS mutual auth circumvented for "Aggregator Quote Creation EAPI"	Policy	1/17/18 3:11 PM	1/17/18 3:11 PM	Yes	<button>Edit</button> <button>Delete</button>
> XML attack on "Aggregator Quote Creation EAPI"	Policy	1/17/18 3:15 PM	1/17/18 3:15 PM	Yes	<button>Edit</button> <button>Delete</button>

All contents © MuleSoft Inc.

25

## Defining alerts for "Aggregator Quote Creation EAPI"

- **SLA tier exhausted:**

- Violation of **SLA-based Rate Limiting**, severity **Info**, > 60 violations for at least 3 consecutive 10-minute periods
- Alerts when approx. **10%** of 1-second intervals are **above limit defined by SLA tier**

- **TLS mutual auth circumvented:**

- Violation of **IP whitelist**, severity **Critical**, > 1 violation for at least 3 consecutive 1-minute periods

All contents © MuleSoft Inc.

26

- **XML attack:**

- Violation of **XML threat protection**, severity **Warning**, > 30000 violations for at least 3 consecutive 10-minute periods
- Alerts when approx. **5%** of requests (5% of  $1000 \times 60 \times 10 = 30000$ ) are identified as XML threats

- **Response time QoS guarantee violated:**

- Severity **Warning**, > 6000 requests whose response time > 400 ms for at least 3 consecutive 10-minute periods
- Alerts when approx. **1%** of API invocations (1% of  $1000 \times 60 \times 10 = 6000$ ) are **above limit** of 400 ms (twice the target median of 200 ms)
- Note that **exact QoS guarantee** cannot be expressed in alert

All contents © MuleSoft Inc. median = 200 ms, maximum = 500 ms

27

## Alerts on API implementations augment alerts for API invocations

The screenshot shows the MuleSoft Runtime Manager interface. On the left, a sidebar contains navigation links: PRODUCTION, Applications, Servers, Alerts, VPCs, and Load Balancers. The main area displays a table of alerts with columns for Name, Source, Condition, Severity, and Active. The first alert, 'Deployment failed to CloudHub', is selected, and its details are shown on the right. The details include the Name, Source, Condition, Severity, Created and Modified timestamps, and Recipients.

Name	Source	Condition	Severity	Active
Deployment failed to CloudHub	All CloudHub Applications	Deployment failed	Critical	Yes
High CPU usage on CloudHub	All CloudHub Applications	CPU usage - Cloudhub	Warning	Yes
High memory usage on CloudHub	All CloudHub Applications	Memory usage - Cloudhub	Warning	Yes
Unresponsive CloudHub Worker	All CloudHub Applications	Worker not responding	Warning	Yes

Property	Value
Name	Deployment failed to CloudHub
Source	All CloudHub Applications
Condition	Deployment failed
Severity	Critical
Created	Thu Jan 18 2018 08:37
Modified	Thu Jan 18 2018 08:37
Recipients	AnySurance Admin

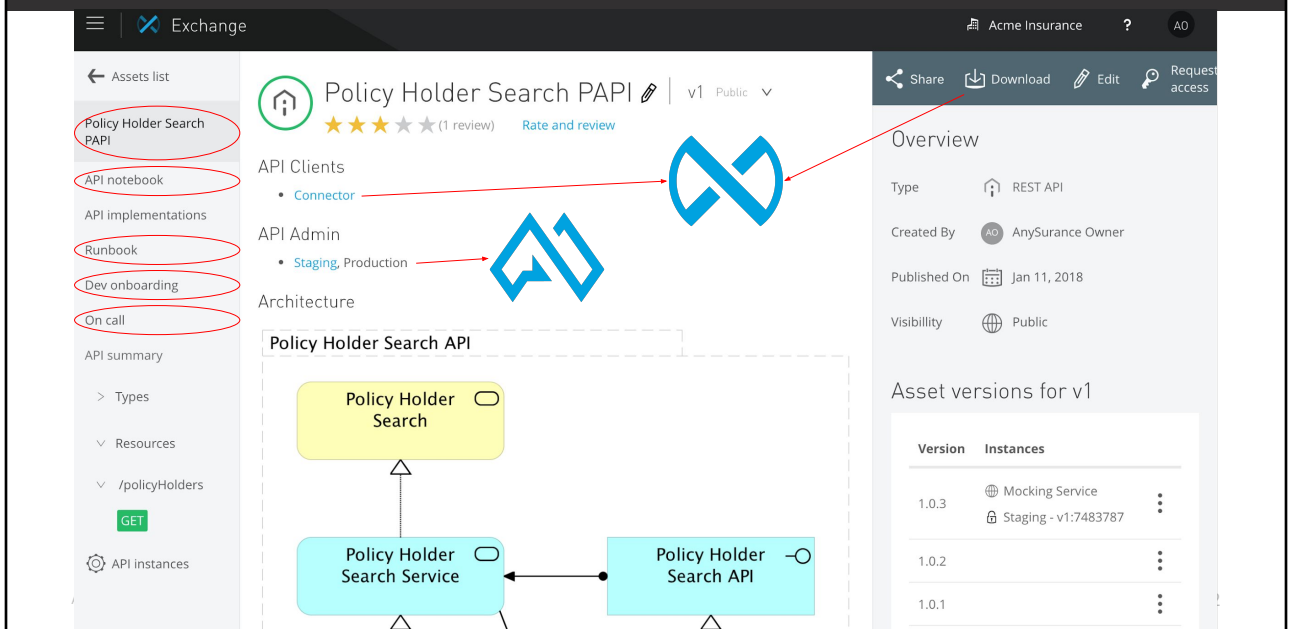
- Alerts for **API invocations** and **API implementations** complement each other
- If API implementation **crashes** but no API client invokes that API then no alert on the level of API invocations will be raised
  - But remember **auto-restart**
- Consistently high **CPU usage**
- **Deployment failures** in production and staging environments

## Organizing discoverable documentation for operations



- **Development teams** may also operate the APIs and API implementations they implement
  - Thereby become **operations teams**
- Operations teams **need**
  - **Dashboards and alerts**
    - **Runtime Manager, API Manager, Anypoint Analytics**
  - Custom-written **documentation**:
    - **Runbooks**: how to address **alerts**
    - **On-call registers**: **who** to contact
- Should be discoverable through **Exchange**

## Exchange entry is portal to API's documentation and assets

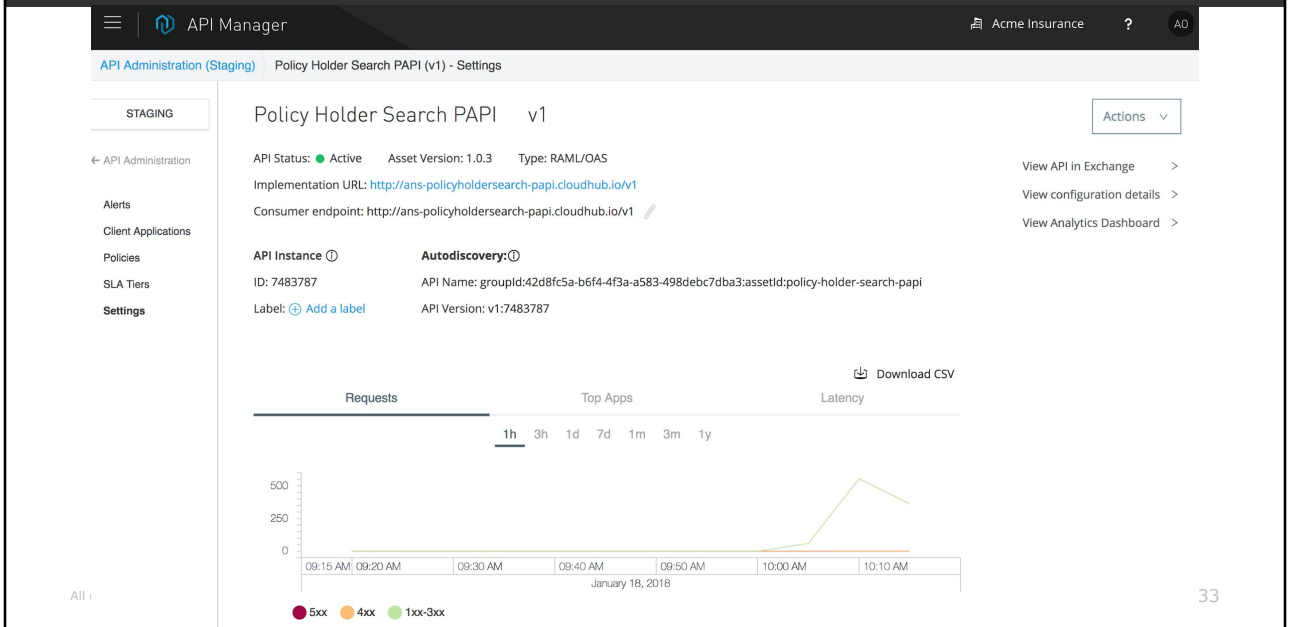
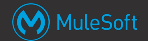


The screenshot shows the MuleSoft Exchange interface for the 'Policy Holder Search PAPI'. The left sidebar contains a list of assets, with 'Policy Holder Search PAPI' highlighted. The main content area displays the API details, including a rating of 4.5 stars (1 review), a 'Rate and review' link, and sections for API Clients (Connector), API Admin (Staging, Production), and Architecture. The Architecture section shows a diagram with three components: 'Policy Holder Search' (yellow box), 'Policy Holder Search Service' (light blue box), and 'Policy Holder Search API' (light blue box). The right sidebar shows the 'Overview' section, including the API type (REST API), created by (AnySurance Owner), published on (Jan 11, 2018), and visibility (Public). Below the overview is a table of asset versions for v1.

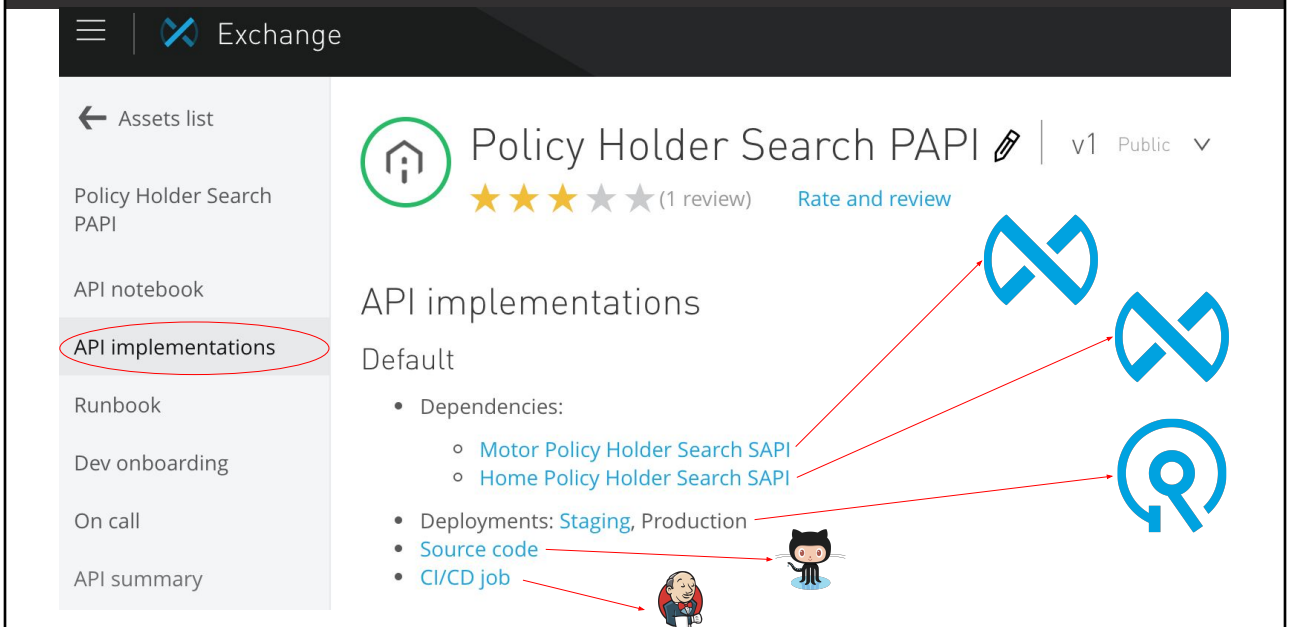
Version	Instances
1.0.3	Mocking Service Staging - v1:7483787
1.0.2	
1.0.1	



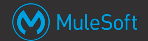
# Matching API Manager API administration entry



# Exchange entry section for API implementations



# Runtime Manager dashboard for matching CloudHub deployment of API implementation



Runtime Manager

Acme Insurance



AO

STAGING

● ans-policyholdersearch-papi



Applications

Dashboard

Insight

Logs

Application Data

Queues

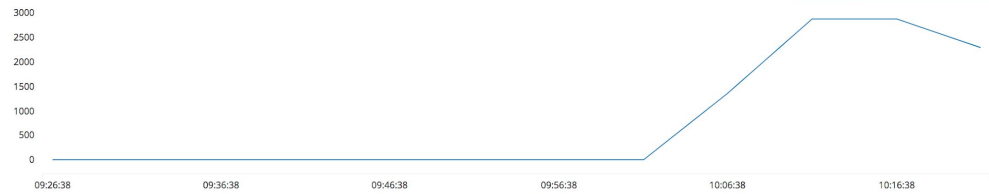
Schedules

Settings

Domain: [ans-policyholdersearch-papi.cloudhub.io](https://ans-policyholdersearch-papi.cloudhub.io) · Last Updated 2018-01-11 5:12:16PM · 1 micro worker, using 3.9.0

Mule messages

Last hour Last 24hs Last week



CPU

Worker 18.218.156.99



Memory

## Summary



- **Data** used in monitoring, analysis and alerting flows from Mule runtimes to external monitoring/analytics systems and/or Anypoint Platform
  - **Available via APIs** for external reporting
- Anypoint Platform collects numerous **metrics** for API invocations:
  - Response time, payload size, client location, ...
- Metrics can be **grouped** by API, API client or any of the other metrics
- Analyses targeted specifically at **API consumers** and clients

- Anypoint **Analytics** supports
  - Interactive analyses, custom charts and reports
  - Data download in CSV files and/or retrieval through Anypoint Platform APIs
- **Alerts** defined based on API invocation metrics:
  - Request count and time, response status code
  - Number of API policy violations
- Metrics and alerts for **API implementations** defined in Runtime Manager augment API invocations metrics and alerts
- **Operations teams** are important stakeholder in API-related assets: structure and link assets to support them