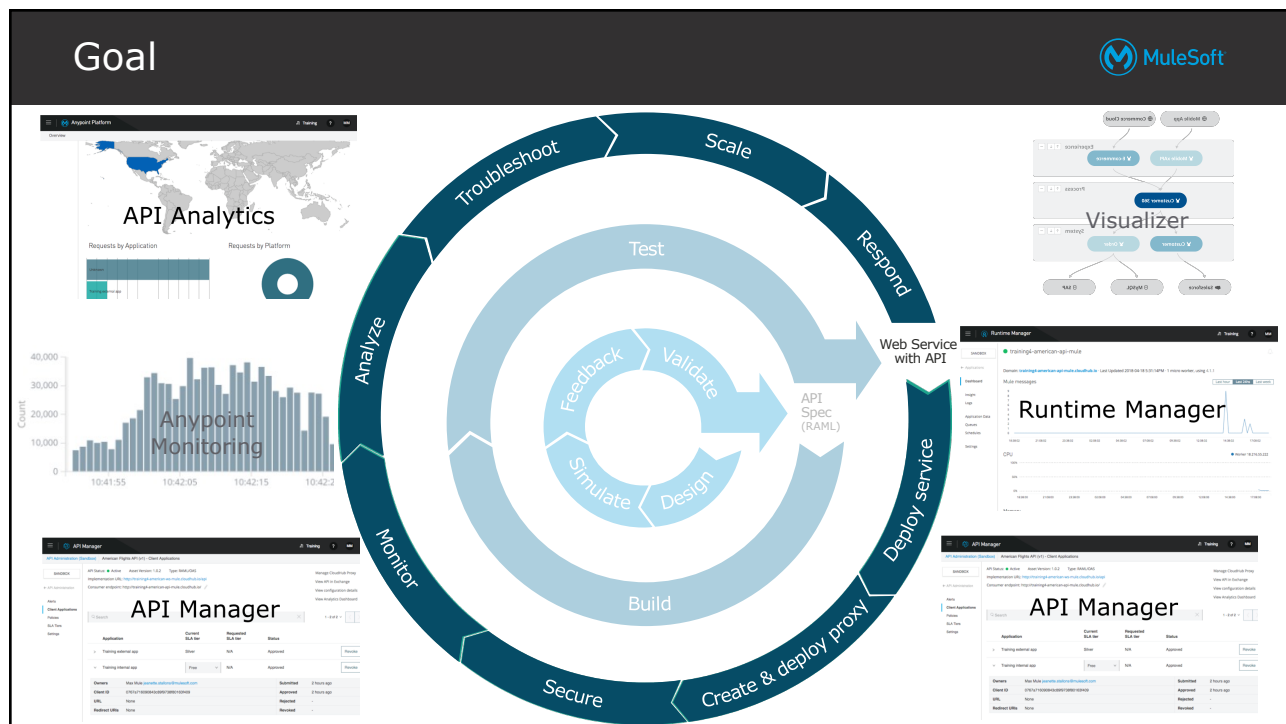




Module 5: Deploying and managing APIs

1



2

At the end of this module, you should be able to



- Describe the options for deploying Mule applications
- Deploy Mule applications to CloudHub
- Use API Manager to create and deploy API proxies
- Use API Manager to restrict access to API proxies

All contents © MuleSoft Inc.

3

3

Introducing deployment options



4

Deploying applications



- During development, applications are deployed to an embedded Mule runtime in Anypoint Studio
- For everything else (testing, Q&A, and production), applications can be deployed to
 - **CloudHub**
 - Platform as a Service (PaaS) component of Anypoint Platform
 - MuleSoft-hosted Mule runtimes on AWS
 - A fully-managed, multi-tenanted, globally available, secure and highly available cloud platform for integrations and APIs
 - **Customer-hosted Mule runtimes**
 - On bare metal or cloud service providers: AWS, Azure, and Pivotal Cloud Foundry
 - **Anypoint Runtime Fabric**
 - Customer-hosted container service of the runtime plane



CloudHub



Customer-hosted runtime



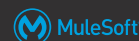
Runtime Fabric

All contents © MuleSoft Inc.

5

5

CloudHub benefits



- No hardware to maintain
- Continuous software updates
- Provided infrastructure for DNS and load-balancing
- Built-in elastic scalability for increasing cloud capacity during periods of high demand
- Globally available with data centers around the world
- Highly available with 99.99% uptime SLAs (service level agreements) <http://status.mulesoft.com/>
- Highly secure
 - PCI, HiTrust, and SSAE-16 certified

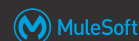


All contents © MuleSoft Inc.

6

6

Customer-hosted Mule runtimes



- Easy to install
- Requires minimal resources
- Can run multiple applications
- Uses a Java Service Wrapper that controls the JVM from the operating system and starts Mule
- Can be managed by
 - Runtime Manager in MuleSoft-hosted Anypoint Platform
 - Runtime Manager in customer-hosted Anypoint Platform
 - Anypoint Platform Private Cloud Edition

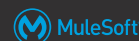


All contents © MuleSoft Inc.

7

7

Anypoint Runtime Fabric



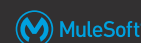
- A deployment model of the runtime plane
 - Container service that automates orchestration of apps and API gateways
 - Anypoint Platform control plane is still hosted by MuleSoft
- Runs on customer-hosted infrastructure
 - AWS, Azure, virtual machines (VMs) or bare-metal servers
- Main characteristics and capabilities
 - Security and reliability through isolation between applications
 - Re-deployments with zero downtime
 - Automated application failover through horizontal scaling
 - Run multiple versions of the Mule runtime
 - MuleSoft-supported containerized runtime images

All contents © MuleSoft Inc.

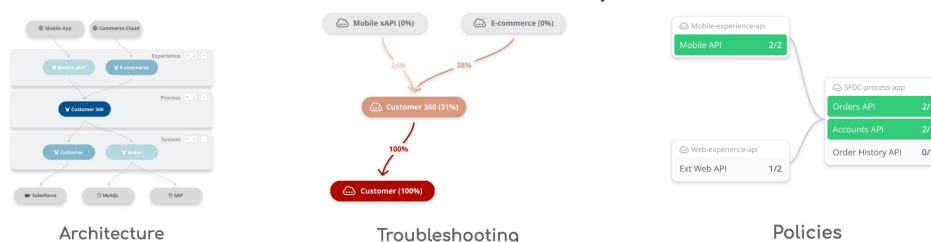
8

8

Viewing Deployed Applications with Visualizer



- Visualizer provides a real-time view into your application architecture in a context that best suits your role



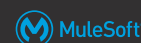
- Organizes APIs and applications into relational diagrams
 - Promotes best practices and layer-based architectural consistency
 - Pinpoints issues rapidly through root cause analysis
 - Enables visibility into the policy compliance of APIs
- Diagram data is secure and automatically & dynamically updated

All contents © MuleSoft Inc.

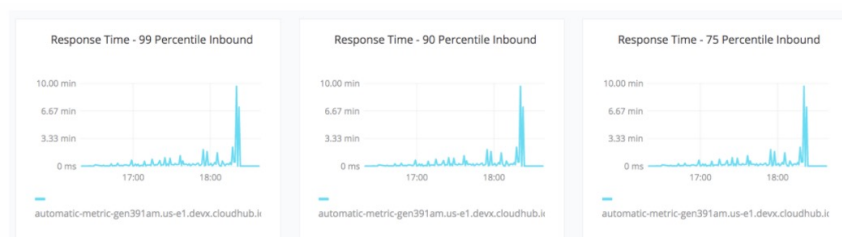
9

9

Understanding the State of Your Infrastructure with Anypoint Monitoring



- Anypoint Monitoring provides visibility into integrations across your app network



- Its monitoring tools are designed to reduce the time to identify and resolve issues by providing ways to
 - Aggregate and map metrics across dependent systems in real-time
 - Configure dashboards and alerts to reduce issue identification time
 - Store and search log data at scale

All contents © MuleSoft Inc.

10

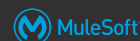
10

Deploying applications to CloudHub



11

Deploying applications to CloudHub



- Can deploy from Anypoint Studio or from Anypoint Platform using Runtime Manager
- You must set worker size and number
 - For apps deployed from Flow Designer, these values were set automatically

The screenshot shows the MuleSoft Runtime Manager interface. The application 'training4-american-ws-maxmule' is selected. The configuration is as follows:

Runtime	Properties	Insight	Logging	Static IPs
Runtime version: 4.3.0	Worker size: 0.1 vCores		Workers: 1	

Additional details visible in the interface:

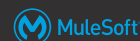
- Application File: training4-american-ws-v2.jar
- Last Updated: 2020-04-28 2:42:38PM
- App url: training4-american-ws-maxmule-us-e2.stgpx.cloudhub.io
- Settings: ☒ Automatically restart application when not responding
- Options: ☐ Persistent queues, ☐ Encrypt persistent queues
- Warning: Your current subscription allows only one worker per application

All contents © MuleSoft Inc.

12

12

Review: CloudHub workers



- A worker is a dedicated instance of Mule that runs an app
- Each worker
 - Runs in a separate container from every other application
 - Is deployed and monitored independently
 - Runs in a specific worker cloud in a region of the world
- Workers can have a different memory capacity and processing power
 - Applications can be scaled vertically by changing the worker size
 - Applications can be scaled horizontally by adding multiple workers

Worker size

0.1 vCores

0.1 vCores

500 MB memory

0.2 vCores

1 GB memory

1 vCore

1.5 GB memory

2 vCores

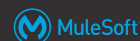
3.5 GB memory

4 vCores

All contents © MuleSoft Inc.

13

Walkthrough 5-1: Deploy an application to CloudHub



- Deploy an application from Anypoint Studio to CloudHub
- Run the application on its new, hosted domain
- Make calls to the web service
- Update an API implementation deployed to CloudHub

The screenshot shows the MuleSoft Runtime Manager interface. On the left is a sidebar with navigation links: SANDBOX, Applications (selected), Servers, Alerts, VPCs, and Load Balancers. The main area has a header 'Runtime Manager' with a search icon. Below the header is a 'Deploy application' button and a search bar labeled 'Search Applications'. A table titled 'All Applications (1)' shows one application with the following details:

Name ^	Server	Status	Runtime Version	Dat
training4-american-ws...	CloudHub	Started	4.3.0	20

At the top right of the main area, there is a link 'Switch back to cla...' and a status 'Update Available (0)'.

All contents © MuleSoft Inc.

24

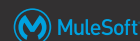
14

Creating API proxies

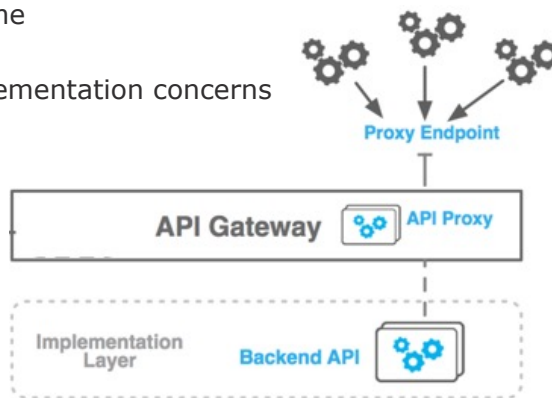


15

Restricting access to APIs



- An **API proxy** is an application that controls access to a web service, restricting access and usage through the use of an API gateway
- The **API Gateway** is a runtime designed and optimized to host an API or to open a connection to an API deployed to another runtime
 - Included as part of the Mule runtime
 - Separate licenses required
 - Separates orchestration from implementation concerns



All contents © MuleSoft Inc.

16

16

The API Gateway is the point of control



- **Determines which traffic** is authorized to pass through the API to backend services
- **Meters the traffic** flowing through
- **Logs** all transactions, collecting and tracking analytics data
- Applies runtime policies to **enforce governance** like rate limiting, throttling, and caching

All contents © MuleSoft Inc.

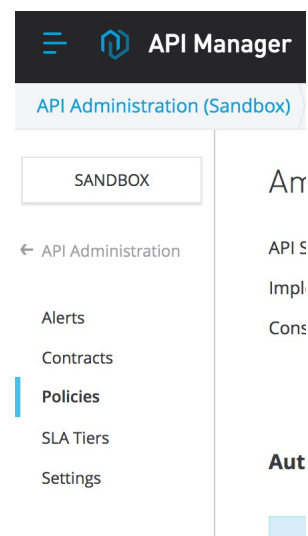
17

17

Using API Manager to manage access to APIs



- **Create** proxy applications
- **Deploy** proxies to an API Gateway runtime
 - On CloudHub or a customer-hosted runtime
- Specify throttling, security, and other **policies**
- Specify **tiers** with different types of access
- Approve, reject, or revoke **access** to APIs by clients
- **Promote** managed APIs between environments
- Review **analytics**

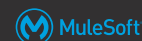


All contents © MuleSoft Inc.

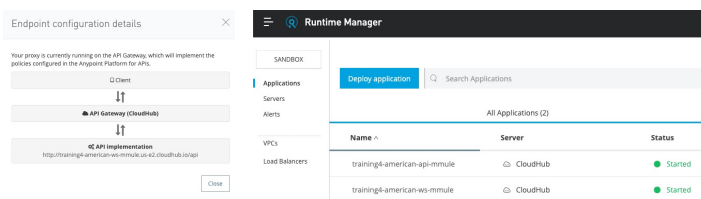
18

18

Walkthrough 5-2: Create and deploy an API proxy



- Add an API to API Manager
- Use API Manager to create and deploy an API proxy application
- Set a proxy consumer endpoint so requests can be made to it from Exchange
- Make calls to an API proxy from API portals for internal and external developers
- View API request data in API Manager.

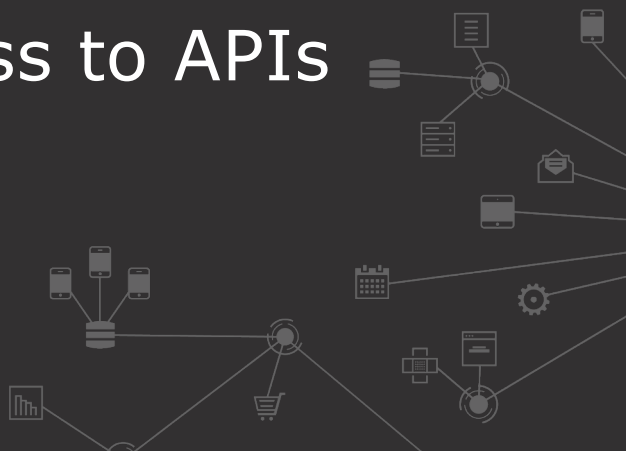


All contents © MuleSoft Inc.

19

19

Restricting access to APIs

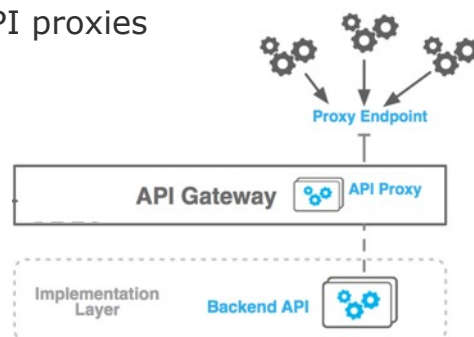


20

Restricting access to APIs



- Use **API Manager** to manage access to API proxies
 - Define SLA tiers
 - Apply runtime policies
- The **API Gateway** enforces the policies
- **API Autodiscovery** is a mechanism that enables a deployed Mule application to
 - Download policies from API Manager
 - Act as its own proxy

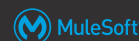


All contents © MuleSoft Inc.

21

21

Applying policies to restrict access



- There are **out-of-the box** policies for many common use cases
 - Rate limiting
 - Spike control
 - Security
- You can define **custom** policies (using XML and YAML)
- You can apply **multiple** policies and set the order
- You can define **automated** policies to comply with common requirements
 - Requires a MuleSoft-hosted control plane

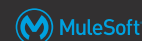
Client ID enforcement	JSON threat protection
Cross-Origin resource sharing	Basic Authentication - LDAP
OAuth 2.0 access token enforcement	Message Logging
Header Injection	Rate limiting
Header Removal	Rate limiting - SLA based
Basic authentication - Simple	Spike Control
IP blacklist	XML threat protection
IP whitelist	

All contents © MuleSoft Inc.

22

22

Using SLA tiers to restrict access by client ID



- A **Service Level Agreement** tier defines the # of requests that can be made per time frame to an API
 - Request approval can be set to automatic (free) or manual (for tiers that cost \$)

All contents © MuleSoft Inc.

23

23

Walkthrough 5-3: Restrict API access with policies and SLAs



- Add and test a rate limiting policy
- Add SLA tiers, one with manual approval required
- Add and test a rate limiting SLA based policy

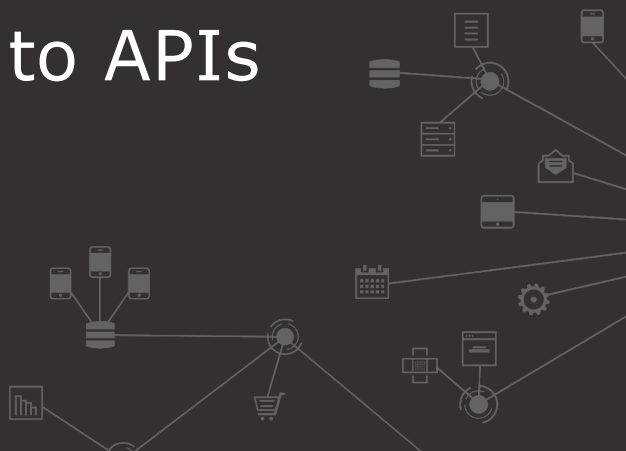
Name	Category	Fulfills	Requires
v1-Rate limiting - SLA based	Quality of service		SLA Rate Limiting - Client ID required

All contents © MuleSoft Inc.

24

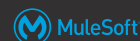
24

Granting access to APIs



25

Enforcing access to APIs using SLA tiers



- To enforce, apply an **SLA based** rate limiting policy
- SLA based policies require all applications that consume the API to
 - **Register** for access to a specific tier
 - From an API portal in private or public Exchange
 - **Pass their client credentials** in calls made to the API

Sandbox - Rate limiting - SLA based policy ▾

<http://training4-american-api-maxmule.us-e2.cloudhub.io/flights>

API is behind firewall ⓘ

Parameters Headers

☒ `</>`

Header name

client_id ⓘ

Parameter value

3c376d605d7f4a5b849e435729f6fe13 ⓘ

+ Add header

Send

All contents © MuleSoft Inc.

26

26

Requesting access to SLA tiers



- If an API has an SLA-based policy, a Request access button appears in API portal
- To request access, developer must belong to the Anypoint Platform organization and be logged in
- When developers request access, they must
 - Register/add an app to their Anypoint Platform account
 - Select a tier

The screenshot shows the 'Request API access' dialog in the MuleSoft API portal. The dialog is titled 'Request API access' and includes a 'Create a new application' link. It contains the following fields:

- Application:** Training external app
- API Instance:** American Flights API - Sandbox - Ra...
- SLA tier:** Silver

Below these fields is a table with the following data:

# of Reqs	Time period	Time Unit
1	1	Second

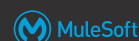
At the bottom of the dialog are 'Cancel' and 'Request API access' buttons.

All contents © MuleSoft Inc.

27

27

Approving SLA tier access requests



- For tiers with manual approval, emails are sent to the Organization Administrators when developers request access for applications
- Organization Administrators can review the applications in API Manager and approve, delete, or revoke requests

The screenshot shows the 'American Flights API' details in the MuleSoft API Manager. The API is active and has a version of 1.0.3. The table below shows the access requests for this API:

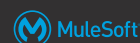
Application	Current SLA tier	Requested SLA tier	Status	Actions
> Training external app	Silver	N/A	Approved	Revoke Delete
> Training internal app	Free	N/A	Approved	Revoke Delete

All contents © MuleSoft Inc.

28

28

Walkthrough 5-4: Request and grant access to a managed API



- Request application access to SLA tiers from private and public API portals
- Approve application requests to SLA tiers in API Manager

The screenshot shows the MuleSoft API Manager interface. The top navigation bar includes 'API Manager', 'Training', and 'MM'. Below the navigation bar, there's a section for 'American Flights API v1'. The left sidebar contains links for 'API Administration', 'Alerts', 'Contracts', 'Policies', 'SLA Tiers', and 'Settings'. The main content area displays the API details, including its status (Active), version (1.0.2), and implementation URL. Below this, there's a table of API instance contracts.

Application	Current SLA tier	Requested SLA tier	Status	Actions
> Training external app	Silver <i>Applied</i>	N/A	Approved	Revoke Delete
> Training internal app	Free <i>Applied</i>	N/A	Approved	Revoke Delete

All contents © MuleSoft Inc.

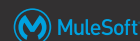
29

29

Adding client ID enforcement to API specifications

30

Adding client ID enforcement to API specifications



- You need to add client ID enforcement to the API spec for the
 - REST connector that is created for the API to enforce the authentication
 - Required headers to automatically show up in the API console so you don't have to manually add them for every call
- Instructions are in the RAML snippet for a policy in API Manager

Client ID based policies by default expect to obtain the client ID and secret as headers. To enforce this in the API definition a trait can be defined in RAML as shown below.

API level policies

Apply New Policy

Name	Category	Fulfills	Requires
> Rate limiting - SLA based	Quality of service	SLA Rate Limiting, Client ID required	API Specification snippet

API Specification snippet

RAML 0.8 RAML 1.0 OAS 2.0

```

traits:
  client-id-required:
    headers:
      client_id:
        type: string
      client_secret:
        type: string
    responses:
      401:
        description: Unauthorized, The client_id or client_secret are not valid or the client does not have access.
      429:
        description: The client used all of it's request quota for the current period.
      500:
        description: An error occurred, see the specific message (Only if it is a WSDL endpoint).
      503:
        description: Contracts Information Unreachable.

```

All contents © MuleSoft Inc.

31

31

Walkthrough 5-5: (Optional) Add client ID enforcement to an API specification



- Modify an API specification to require client id and client secret headers with requests
- Update a managed API to use a new version of an API specification
- Call a governed API with client credentials from API portals

Note: If you do not complete this exercise for Fundamentals, the REST connector that is created for the API and that you use later in the course will not have client_id authentication

```

1 #API: 1.0
2 title: American Flights API
3
4 types:
5   AmericanFlight: !include /exchange_modules/2637/
6
7 traits:
8   client-id-required:
9     headers:
10       client_id:
11         type: string
12       client_secret:
13         type: string
14     responses:
15       401:
16         description: Unauthorized, The client_id or
17         429:
18         description: The client used all of it's n
19       500:
20         description: An error occurred, see the spe
21       503:
22         description: Contracts Information Unreach
23
24 /flights:

```

Headers

COPY Text editor

client_id*

Value is required but currently empty.

client_secret*

Value is required but currently empty.

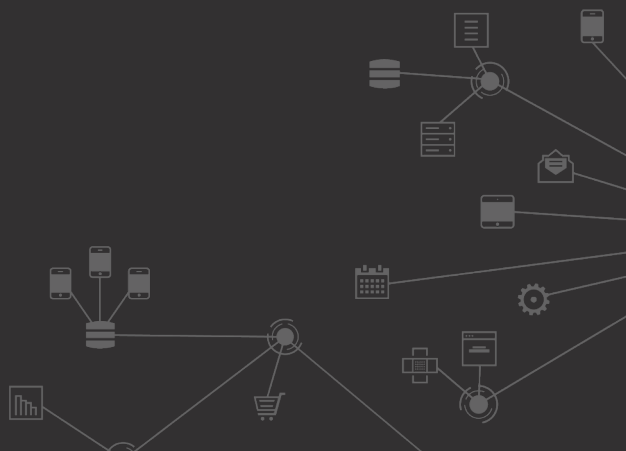
Add

Send

32

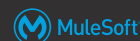
32

Summary



37

Summary



- Deploy applications to MuleSoft-hosted or customer-hosted Mule runtimes
- **CloudHub** is the Platform as a Service (PaaS) component of Anypoint Platform
 - Hosted Mule runtimes (workers) on AWS
- An **API proxy** is an application that controls access to a web service, restricting access and usage through the use of an API gateway
- The **API Gateway runtime** controls access to APIs by enforcing policies
 - Is part of the Mule runtime but requires a separate license

All contents © MuleSoft Inc.

38

38

Summary



- Use **API Manager** to
 - Create and deploy API proxies
 - Define SLA tiers and apply runtime policies
 - Anypoint Platform has out-of-the box policies for rate-limiting, throttling, security enforcement, and more
 - SLA tiers defines # of requests that can be made per time to an API
 - Approve, reject, or revoke access to APIs by clients
 - Promote managed APIs between environments
 - Review API analytics

All contents © MuleSoft Inc.

39

39

Anypoint Platform Operations training courses



- This module was just an introduction to deploying and managing applications and APIs
- Anypoint Platform Operations:
 - CloudHub
 - Customer-Hosted Runtimes
 - API Management



All contents © MuleSoft Inc.

40

40