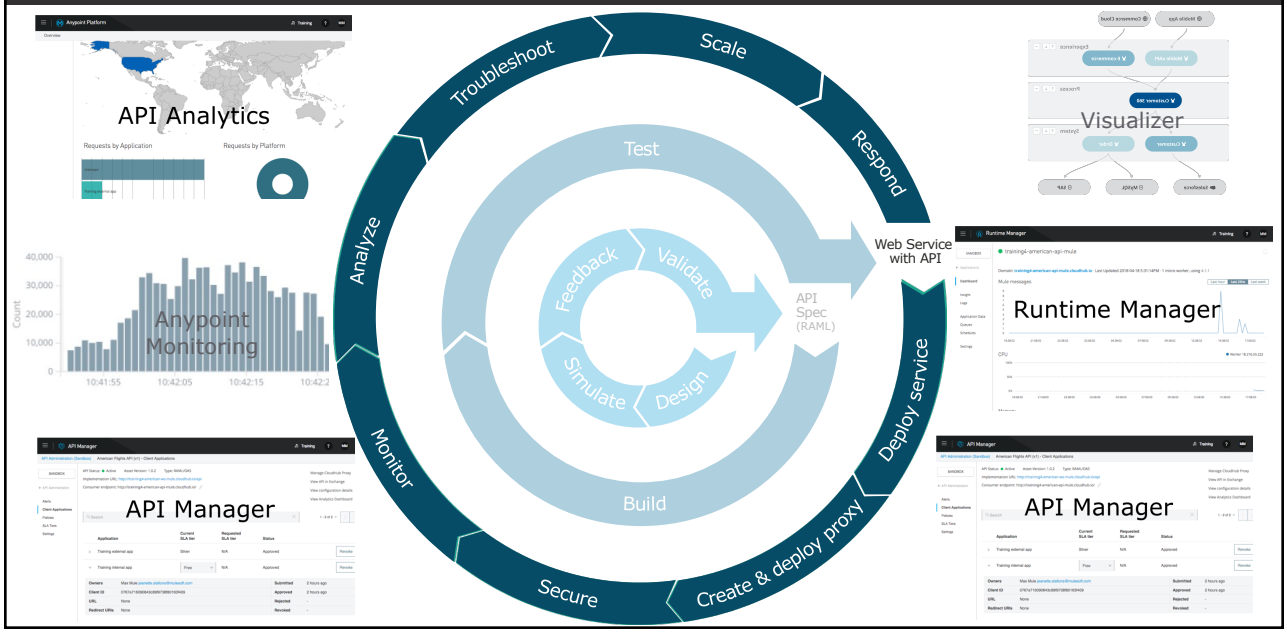
MuleSoft

Module 5: Deploying and managing APIs

1

Goal

MuleSoft



2

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

MuleSoft

- 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

3

Introducing deployment options

4

Deploying applications

MuleSoft

- 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

5

CloudHub benefits

MuleSoft

- 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

6

Customer-hosted Mule runtimes

MuleSoft

- 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

7

Anypoint Runtime Fabric

MuleSoft

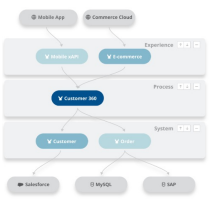
- A deployment model of the runtime plane
  - Container service that automates orchestration of apps and API gateways
  - Anypoint Platform control plane is still hosted by MuleSoft
- Runs on customer-hosted infrastructure
  - AWS, Azure, virtual machines (VMs) or bare-metal servers
- Main characteristics 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

8

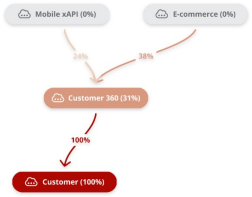
Viewing Deployed Applications with Visualizer

MuleSoft

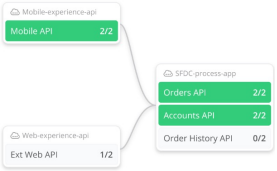
- Visualizer provides a real-time view into your application architecture in a context that best suits your role



Architecture



Troubleshooting



Policies

- 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

Understanding the State of Your Infrastructure with Anypoint Monitoring

MuleSoft

- 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

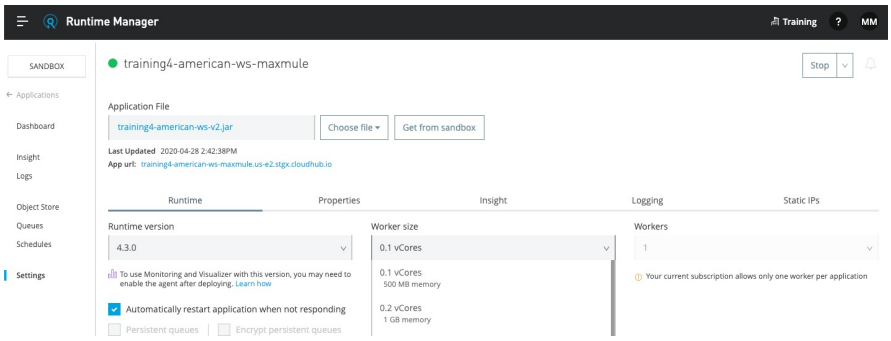
Deploying applications to CloudHub

11

Deploying applications to CloudHub

MuleSoft

- 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

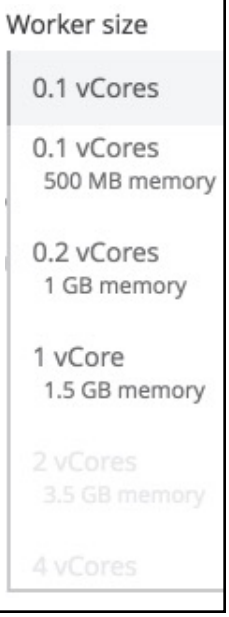


12

Review: CloudHub workers

MuleSoft

- 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

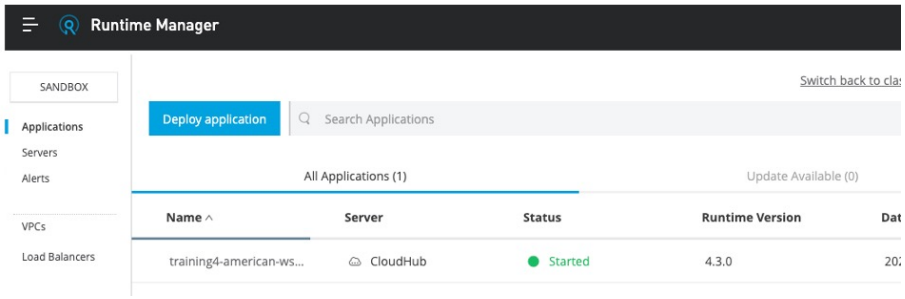


13

Walkthrough 5-1: Deploy an application to CloudHub

MuleSoft

- 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



14

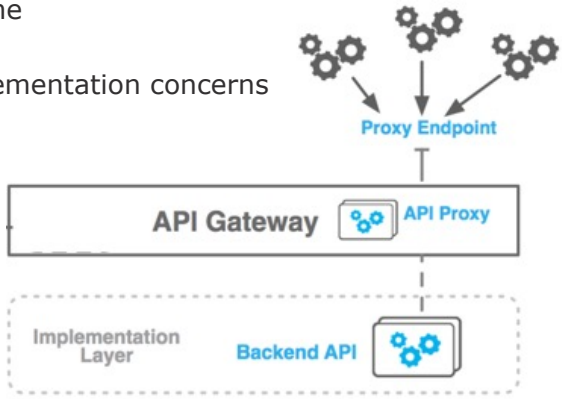
Creating API proxies

15

Restricting access to APIs

MuleSoft

- 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



16

16

The API Gateway is the point of control

MuleSoft

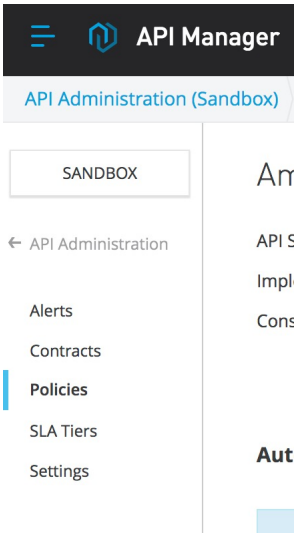
- **Determines which traffic** is authorized to pass through the API to backend services
- **Meters the traffic** flowing through
- **Logs** all transactions, collecting and tracking analytics data
- Applies runtime policies to **enforce governance** like rate limiting, throttling, and caching

17

Using API Manager to manage access to APIs

MuleSoft

- **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**

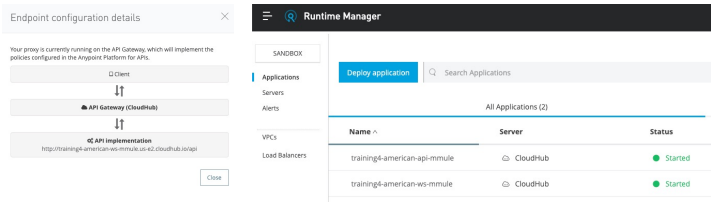


18

Walkthrough 5-2: Create and deploy an API proxy

MuleSoft

- 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.



19

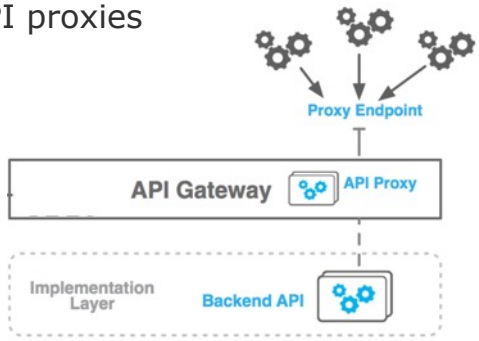
Restricting access to APIs

20

Restricting access to APIs

MuleSoft

- 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



Applying policies to restrict access

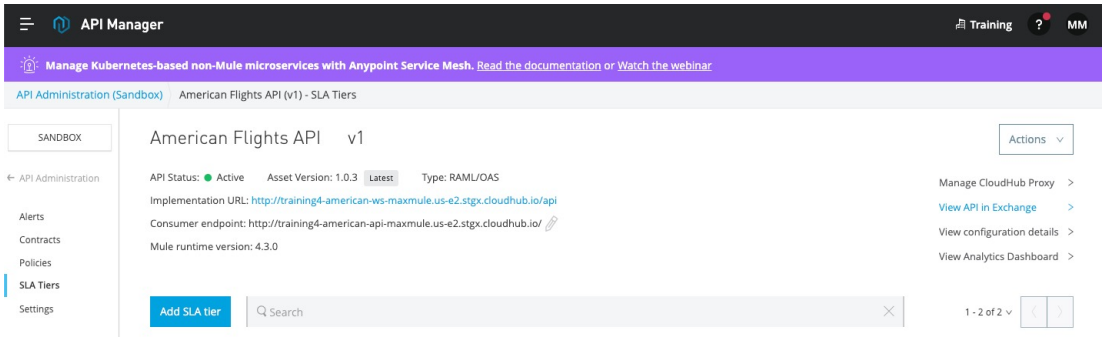
MuleSoft

- 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	

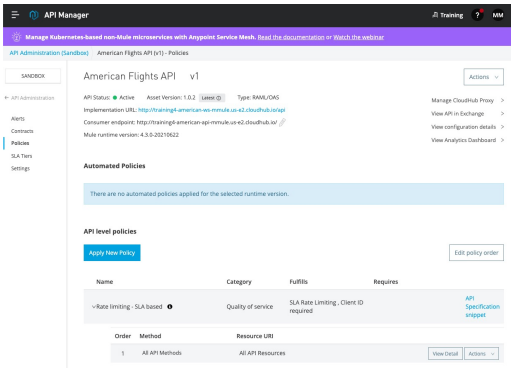
Using SLA tiers to restrict access by client ID

- A **S**ervice **L**evel **A**greement 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 $)



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



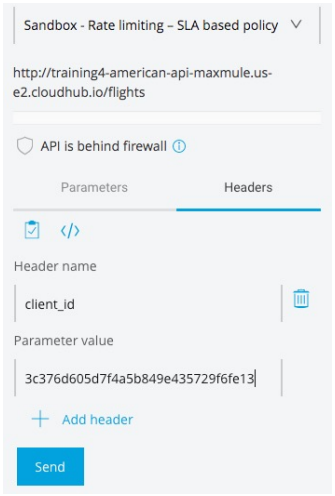
Granting access to APIs

25

Enforcing access to APIs using SLA tiers

MuleSoft

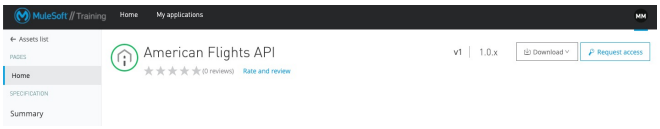
- To enforce, apply an **SLA based** rate limiting policy
- SLA based policies require all applications that consume the API to
  - **Register** for access to a specific tier
    - From an API portal in private or public Exchange
  - **Pass their client credentials** in calls made to the API



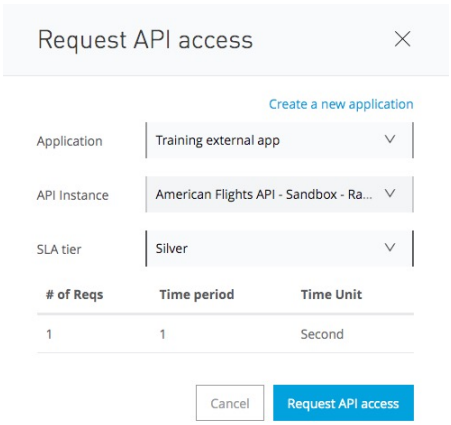
26

Requesting access to SLA tiers

- If an API has an SLA-based policy, a Request access button appears in API portal

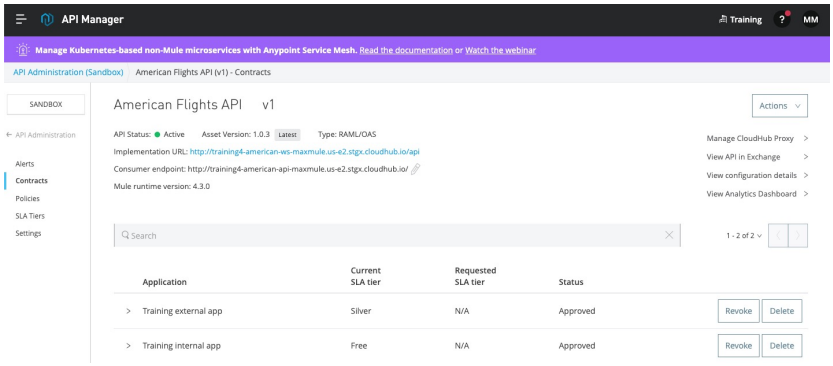


- To request access, developer must belong to the Anypoint Platform organization and be logged in
- When developers request access, they must
  - Register/add an app to their Anypoint Platform account
  - Select a tier



Approving SLA tier access requests

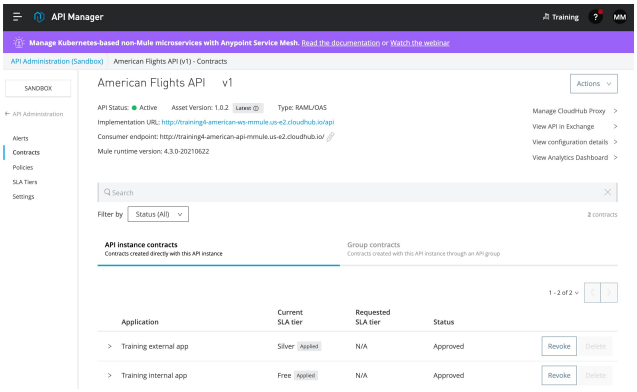
- For tiers with manual approval, emails are sent to the Organization Administrators when developers request access for applications
- Organization Administrators can review the applications in API Manager and approve, delete, or revoke requests



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

MuleSoft

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

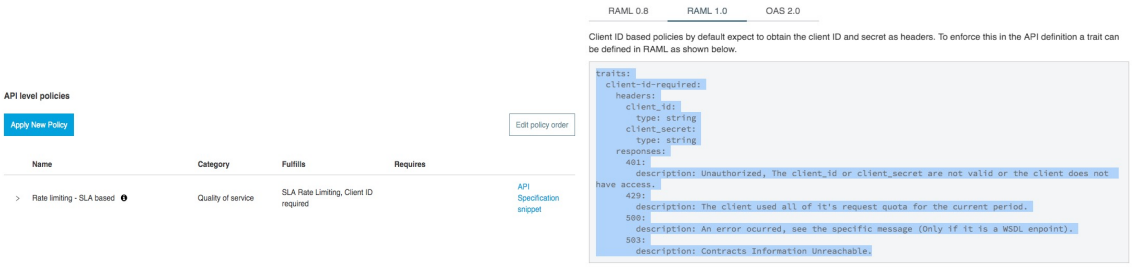


Adding client ID enforcement to API specifications

Adding client ID enforcement to API specifications

MuleSoft

- 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

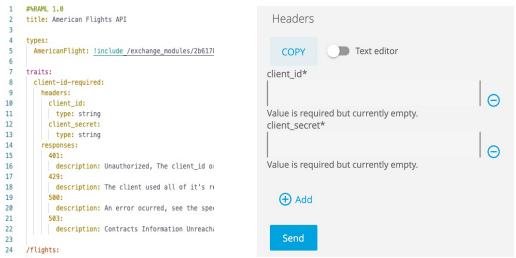


Walkthrough 5-5: (Optional) Add client ID enforcement to an API specification

MuleSoft

- 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



Summary

37

Summary

MuleSoft

- 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

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

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