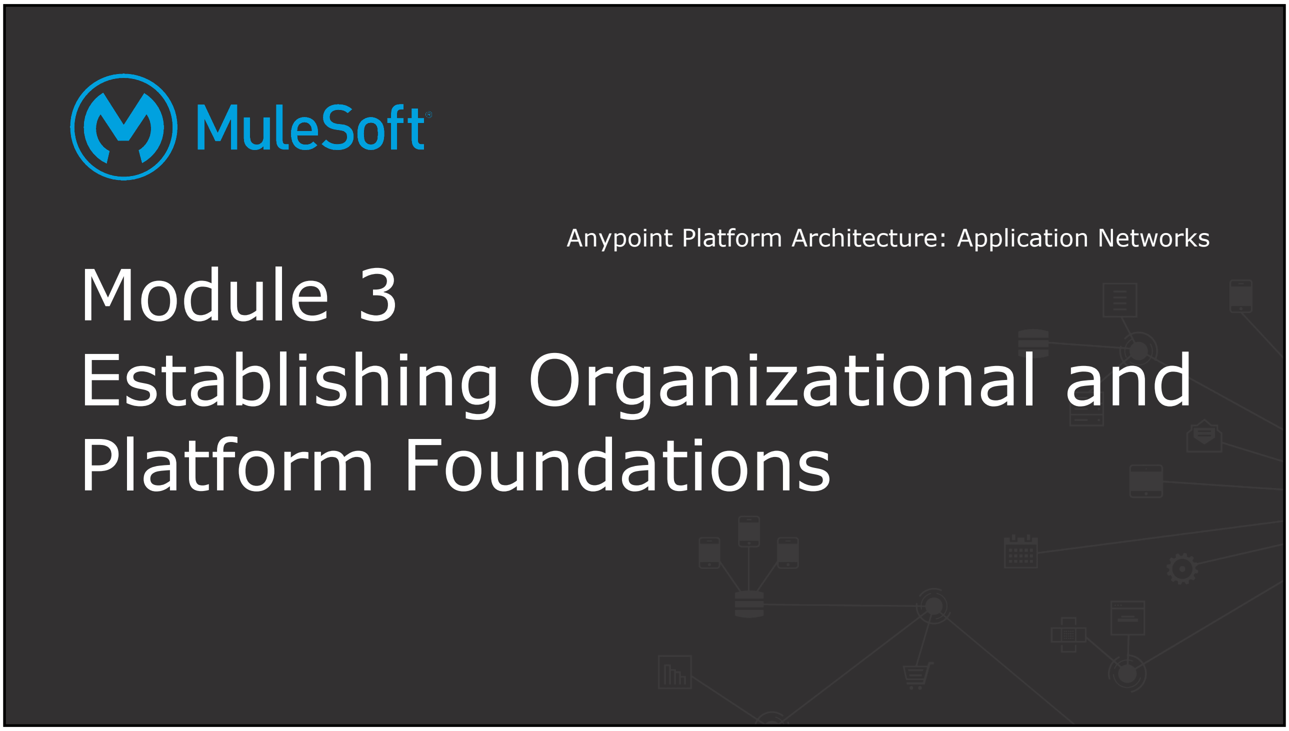
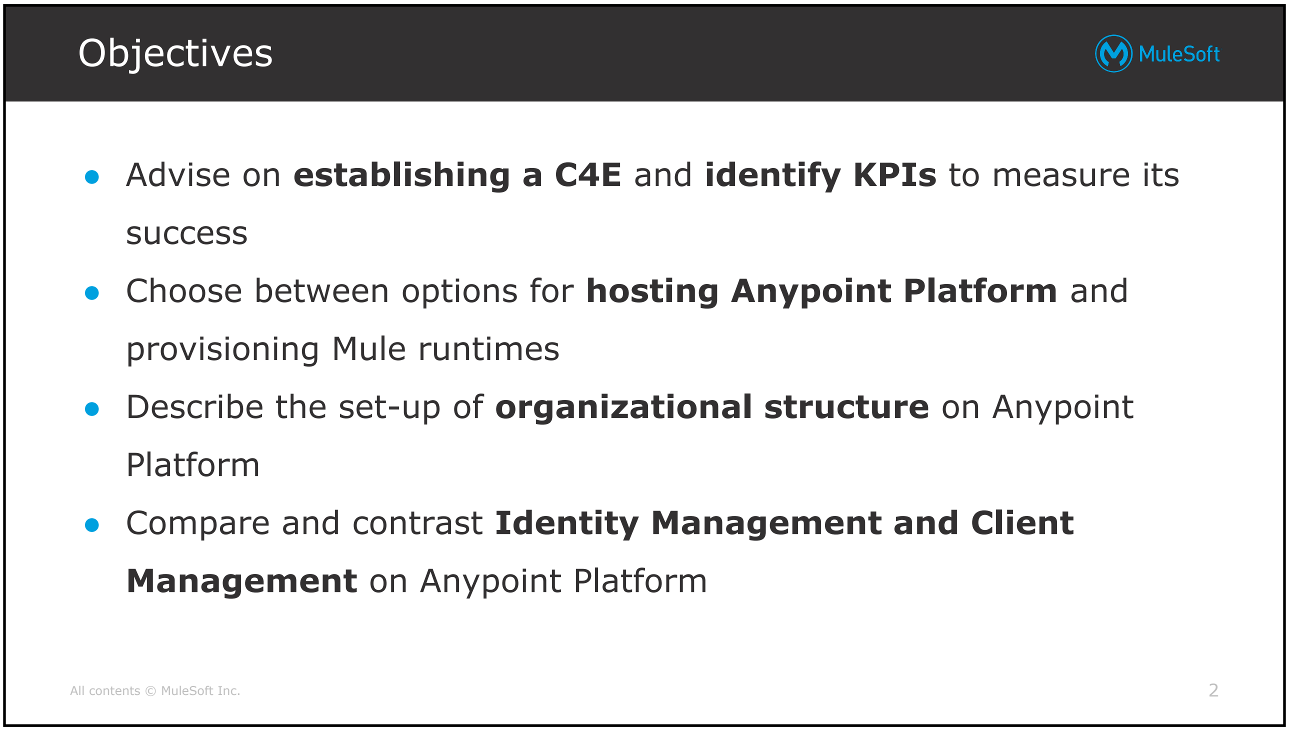


MuleSoft

Anypoint Platform Architecture: Application Networks

Module 3
Establishing Organizational and Platform Foundations



Objectives

MuleSoft

- Advise on **establishing a C4E** and **identify KPIs** to measure its success
- Choose between options for **hosting Anypoint Platform** and provisioning Mule runtimes
- Describe the set-up of **organizational structure** on Anypoint Platform
- Compare and contrast **Identity Management and Client Management** on Anypoint Platform

Establishing a Center for Enablement (C4E) at Acme Insurance

Assessing Acme Insurance's integration capabilities

MuleSoft

An assessment of Acme Insurance’s IT capabilities is performed:

- **LoBs** have history of **IT independence**
  - Strong IT skills, medium integration skills, no API-led connectivity know-how
- **Acme IT is small but enthusiastic** about application networks and API-led connectivity
- **DevOps** capabilities present in LoB IT and Acme IT
- **Corporate IT** lacks the capacity and desire to involve themselves directly in Acme Insurance’s Enterprise Architecture
  - But **corporate principles** must be followed

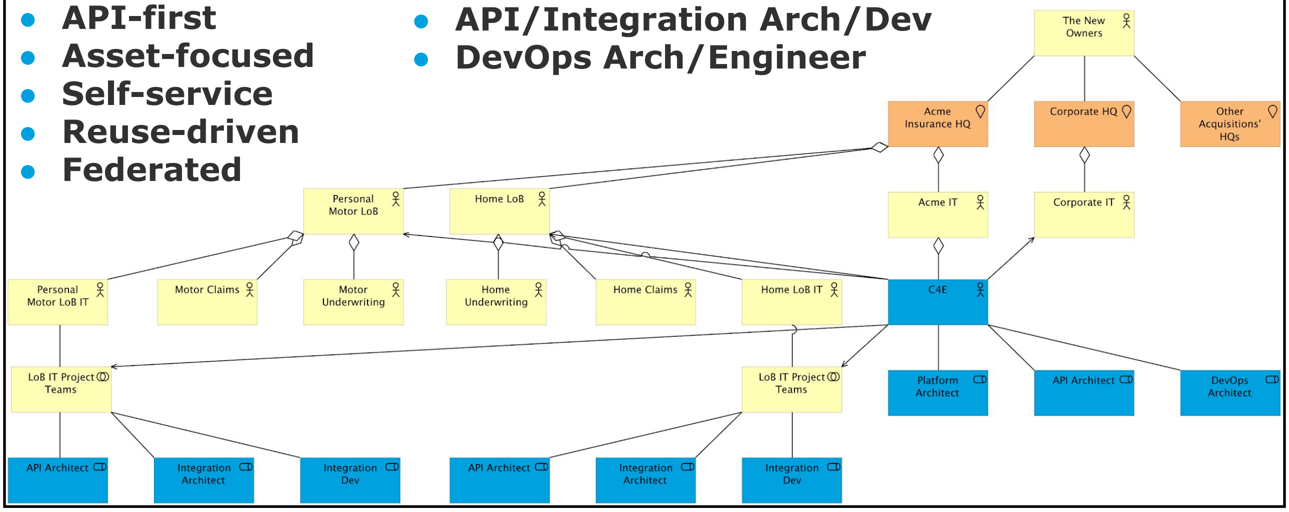
A decentralized C4E for Acme Insurance

Guiding principles:

- **Enable**
- **API-first**
- **Asset-focused**
- **Self-service**
- **Reuse-driven**
- **Federated**

Roles:

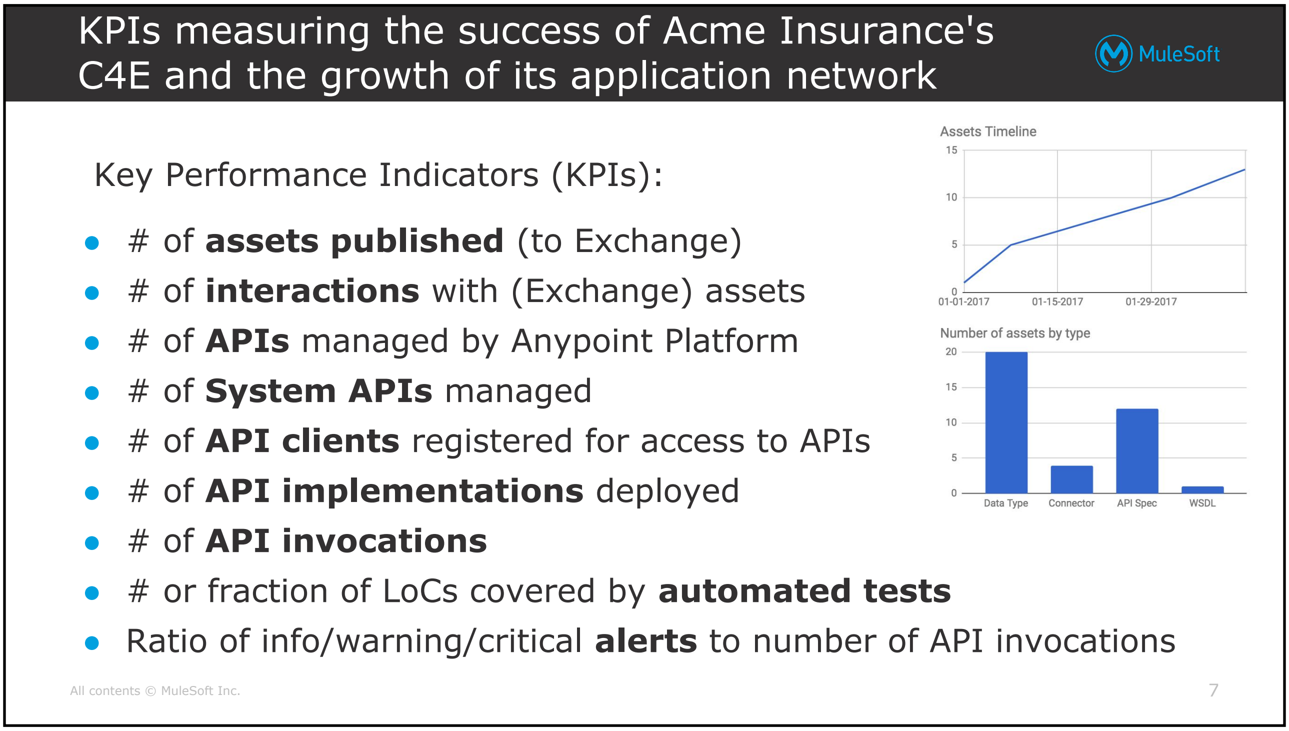
- **Plaform Arch**
- **API/Integration Arch/Dev**
- **DevOps Arch/Engineer**



Exercise: Measuring success of the C4E

Thinking back on the application network vision on the one hand, and the principles of Acme Insurance’s' C4E on the other hand:

1. Compile a **list of statements** which, if largely true, allow the conclusion that the **C4E is successful**
2. Compile a similar list that allows the conclusion that the **application network vision is being realized**
3. From these lists, extract a list of corresponding **metrics**

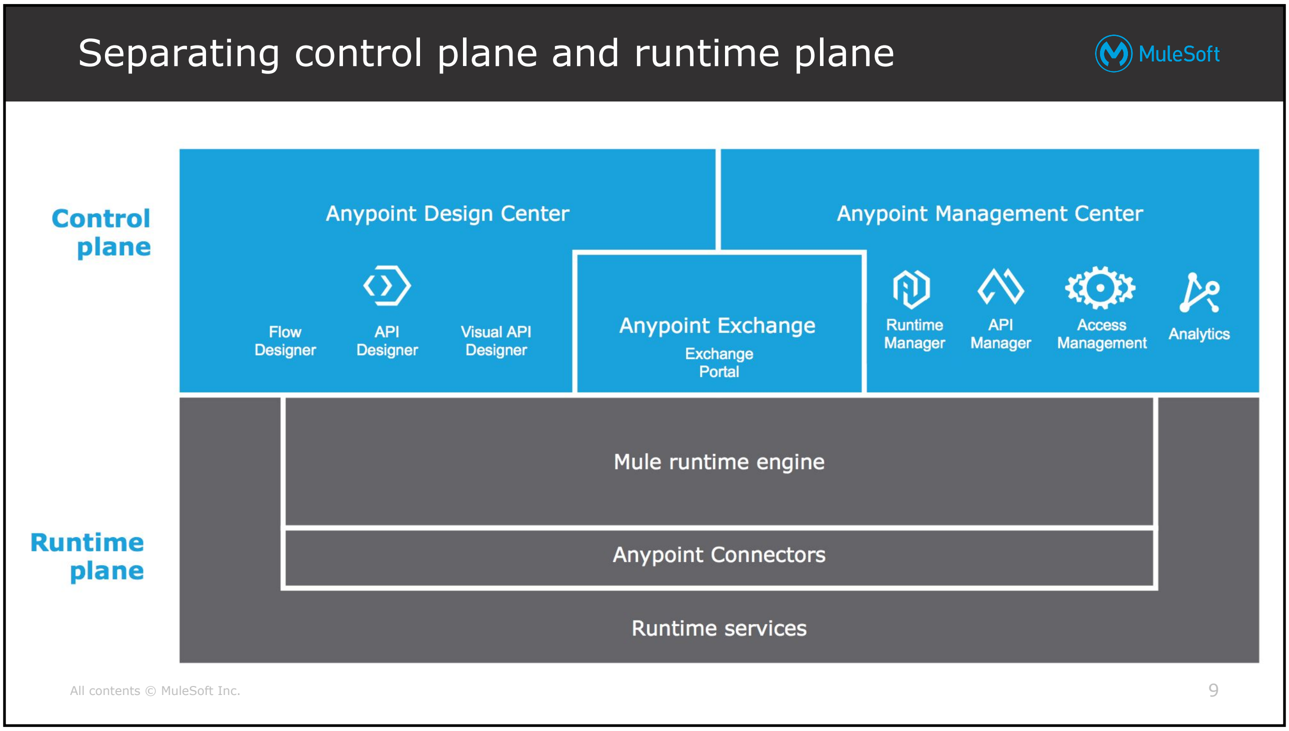


KPIs measuring the success of Acme Insurance's C4E and the growth of its application network

Key Performance Indicators (KPIs):

- # of **assets published** (to Exchange)
- # of **interactions** with (Exchange) assets
- # of **APIs** managed by Anypoint Platform
- # of **System APIs** managed
- # of **API clients** registered for access to APIs
- # of **API implementations** deployed
- # of **API invocations**
- # or fraction of LoCs covered by **automated tests**
- Ratio of info/warning/critical **alerts** to number of API invocations

Understanding Anypoint Platform deployment scenarios



Separating control plane and runtime plane

MuleSoft

Control plane

Anypoint Design Center

Flow Designer

API Designer

Visual API Designer

Anypoint Exchange

Exchange Portal

Anypoint Management Center

Runtime Manager

API Manager

Access Management

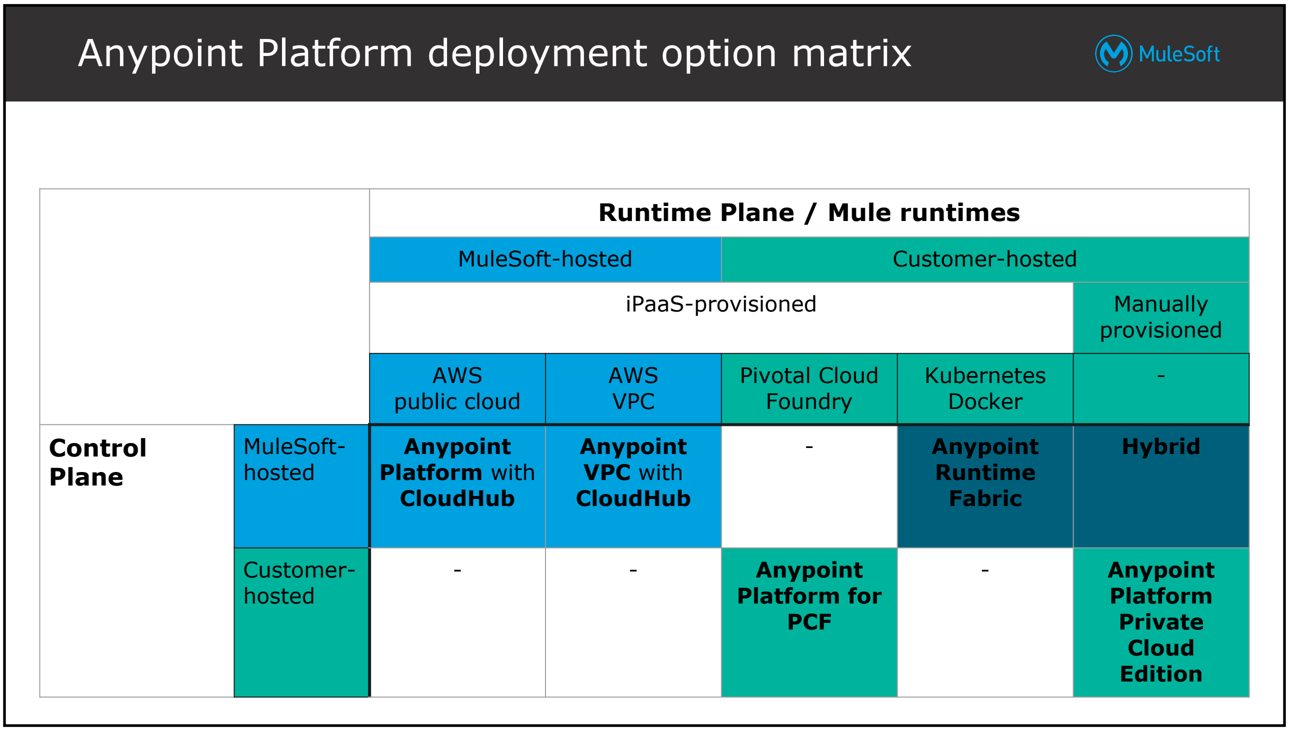
Analytics

Runtime plane

Mule runtime engine

Anypoint Connectors

Runtime services



Anypoint Platform deployment option matrix

MuleSoft

		Runtime Plane / Mule runtimes				
		MuleSoft-hosted		Customer-hosted		
		iPaaS-provisioned				Manually provisioned
		AWS public cloud	AWS VPC	Pivotal Cloud Foundry	Kubernetes Docker	-
Control Plane	MuleSoft-hosted	**Anypoint Platform** with **CloudHub**	**Anypoint VPC** with **CloudHub**	-	**Anypoint Runtime Fabric**	**Hybrid**
	Customer-hosted	-	-	**Anypoint Platform for PCF**	-	**Anypoint Platform Private Cloud Edition**

Deployment of control plane

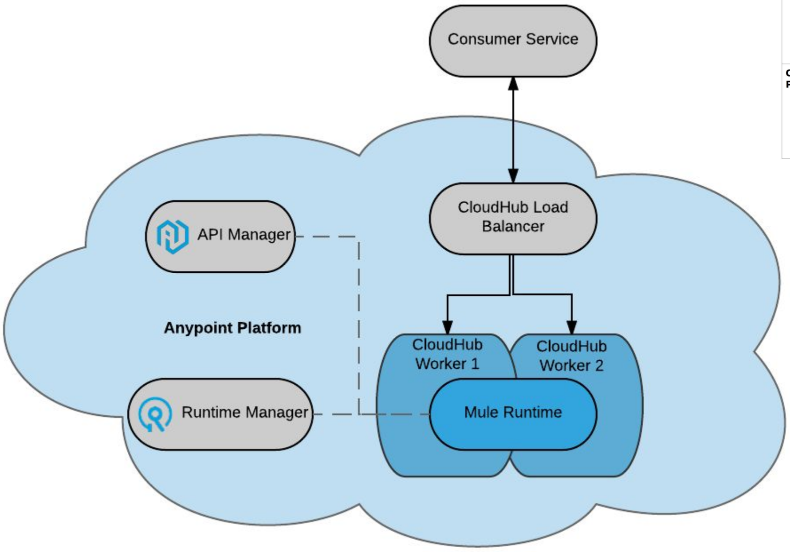
- **MuleSoft-hosted**
  - **Anypoint Platform**
  - AWS **regions**:
    - US East (N Virginia)
    - EU (Frankfurt)
- **Customer-hosted**
  - **Anypoint Platform Private Cloud Edition**

Deployment of runtime plane and Mule runtimes

- **MuleSoft-hosted**
  - In **public AWS** cloud: **CloudHub**
  - In **AWS VPC**: **CloudHub** with **Anypoint VPC**
  - AWS **regions**:
    - **US control plane**: US East/West, Canada, APac, EU (incl. London), S America
    - **EU control plane**: EU (Frankfurt, Ireland)
- **Customer-hosted**
  - **Manually provisioned** Mule runtimes: metal, VMs, on-premises, cloud, ...
  - **iPaaS-provisioned** Mule runtimes:
    - MuleSoft appliance: **Anypoint Runtime Fabric**
    - Customer-managed: **Anypoint Platform for Pivotal Cloud Foundry**

MuleSoft-hosted control plane and runtime plane with iPaaS functionality in public cloud

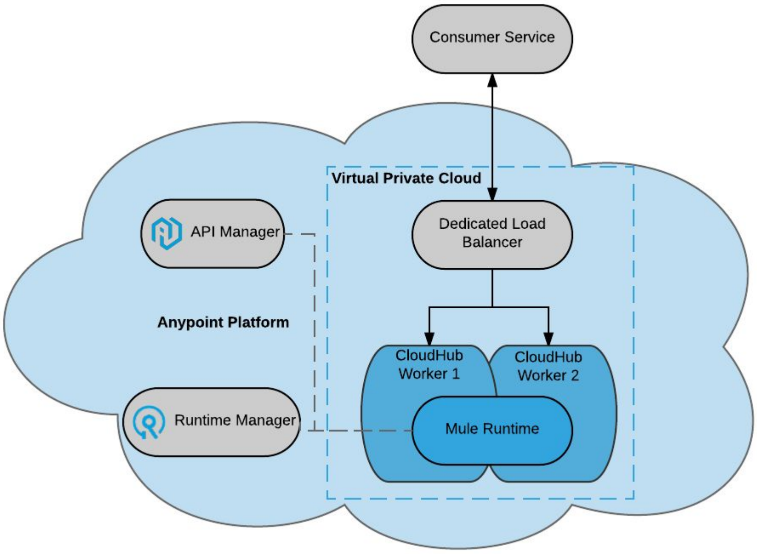
MuleSoft



		Runtime Plane / Mule runtimes				
		MuleSoft-hosted		Customer-hosted		
		iPaaS-provisioned				Manually provisioned
		AWS public cloud	AWS VPC	Pivotal Cloud Foundry	Kubernetes Docker	-
Control Plane	MuleSoft-hosted	**Anypoint Platform** with **CloudHub**	**Anypoint VPC** with **CloudHub**	-	**Anypoint Runtime Fabric**	**Hybrid**
	Customer-hosted	-	-	**Anypoint Platform for PCF**	-	**Anypoint Platform Private Cloud Edition**

MuleSoft-hosted control plane and runtime plane with iPaaS functionality in Anypoint VPC

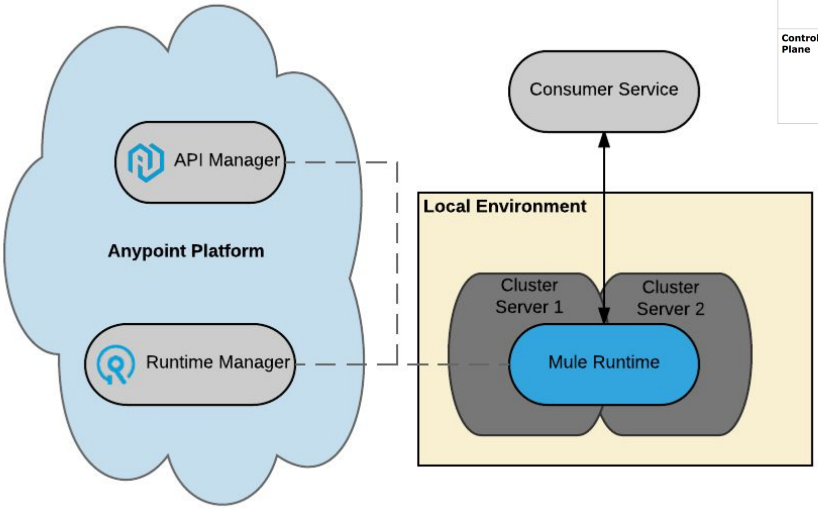
MuleSoft

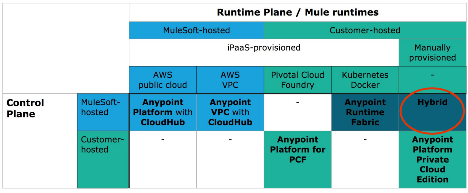


		Runtime Plane / Mule runtimes				
		MuleSoft-hosted		Customer-hosted		
		iPaaS-provisioned				Manually provisioned
		AWS public cloud	AWS VPC	Pivotal Cloud Foundry	Kubernetes Docker	-
Control Plane	MuleSoft-hosted	**Anypoint Platform** with **CloudHub**	**Anypoint VPC** with **CloudHub**	-	**Anypoint Runtime Fabric**	**Hybrid**
	Customer-hosted	-	-	**Anypoint Platform for PCF**	-	**Anypoint Platform Private Cloud Edition**

MuleSoft-hosted control plane and customer-hosted runtime plane without iPaaS functionality

MuleSoft

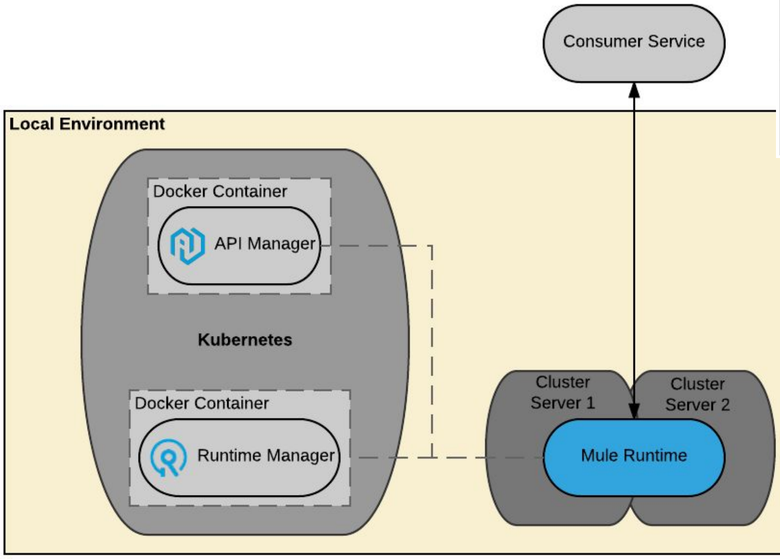


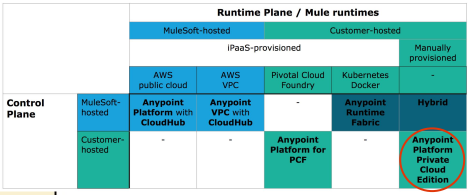


		Runtime Plane / Mule runtimes				
		MuleSoft-hosted		Customer-hosted		
		iPaaS-provisioned				Manually provisioned
		AWS public cloud	AWS VPC	Pivotal Cloud Foundry	Kubernetes Docker	-
Control Plane	MuleSoft-hosted	**Anypoint Platform** with **CloudHub**	**Anypoint VPC** with **CloudHub**	-	**Anypoint Runtime Fabric**	**Hybrid**
	Customer-hosted	-	-	**Anypoint Platform for PCF**	-	**Anypoint Platform Private Cloud Edition**

Customer-hosted control plane and runtime plane without iPaaS functionality

MuleSoft

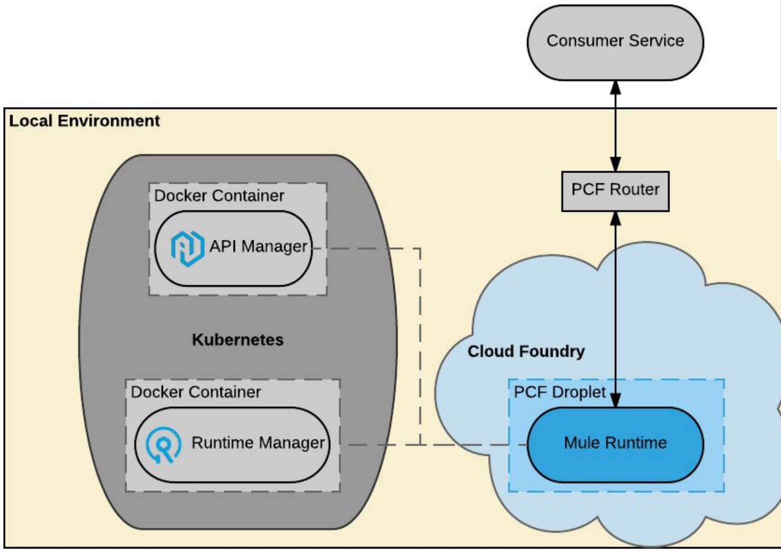


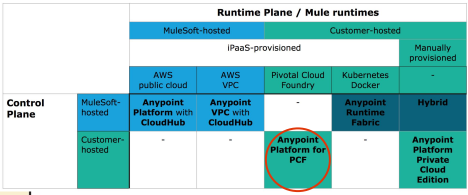


		Runtime Plane / Mule runtimes				
		MuleSoft-hosted		Customer-hosted		
		iPaaS-provisioned				Manually provisioned
		AWS public cloud	AWS VPC	Pivotal Cloud Foundry	Kubernetes Docker	-
Control Plane	MuleSoft-hosted	**Anypoint Platform** with **CloudHub**	**Anypoint VPC** with **CloudHub**	-	**Anypoint Runtime Fabric**	**Hybrid**
	Customer-hosted	-	-	**Anypoint Platform for PCF**	-	**Anypoint Platform Private Cloud Edition**

Customer-hosted control plane and runtime plane with iPaaS functionality on Pivotal Cloud Foundry

MuleSoft





		Runtime Plane / Mule runtimes				
		MuleSoft-hosted		Customer-hosted		
		iPaaS-provisioned				Manually provisioned
		AWS public cloud	AWS VPC	Pivotal Cloud Foundry	Kubernetes Docker	-
Control Plane	MuleSoft-hosted	**Anypoint Platform** with **CloudHub**	**Anypoint VPC** with **CloudHub**	-	**Anypoint Runtime Fabric**	**Hybrid**
	Customer-hosted	-	-	**Anypoint Platform for PCF**	-	**Anypoint Platform Private Cloud Edition**

Availability of Anypoint Platform components in different Anypoint Platform deployment scenarios

MuleSoft

Component	**MuleSoft-hosted Anypoint Platform**	**Hybrid**	**Anypoint Platform Private Cloud Edition**	**Anypoint Platform for Pivotal Cloud Foundry**
API designer	yes	yes	yes	yes
Flow designer	yes	yes	no	no
Access Management	yes	yes	yes	yes
Runtime Manager	yes	yes	yes	yes
API Manager	yes	yes	yes	yes
Analytics	yes	yes	no	no
Exchange	yes	yes	yes	yes
Anypoint MQ	yes	yes	no	no
iPaaS	yes (CloudHub)	no	no	yes

Exercise: Choosing between deployment scenarios

Reflecting on the various deployment scenarios supported by Anypoint Platform:

1. Discuss the characteristics of each scenario
2. For each deployment scenario, identify requirements that would clearly require that scenario

		Runtime Plane / Mule runtimes				
		MuleSoft-hosted		Customer-hosted		
		iPaaS-provisioned				Manually provisioned
		AWS public cloud	AWS VPC	Pivotal Cloud Foundry	Kubernetes Docker	-
Control Plane	MuleSoft-hosted	**Anypoint Platform** with **CloudHub**	**Anypoint VPC** with **CloudHub**	-	**Anypoint Runtime Fabric**	**Hybrid**
	Customer-hosted	-	-	**Anypoint Platform for PCF**	-	**Anypoint Platform Private Cloud Edition**

Solution: Choosing between deployment scenarios

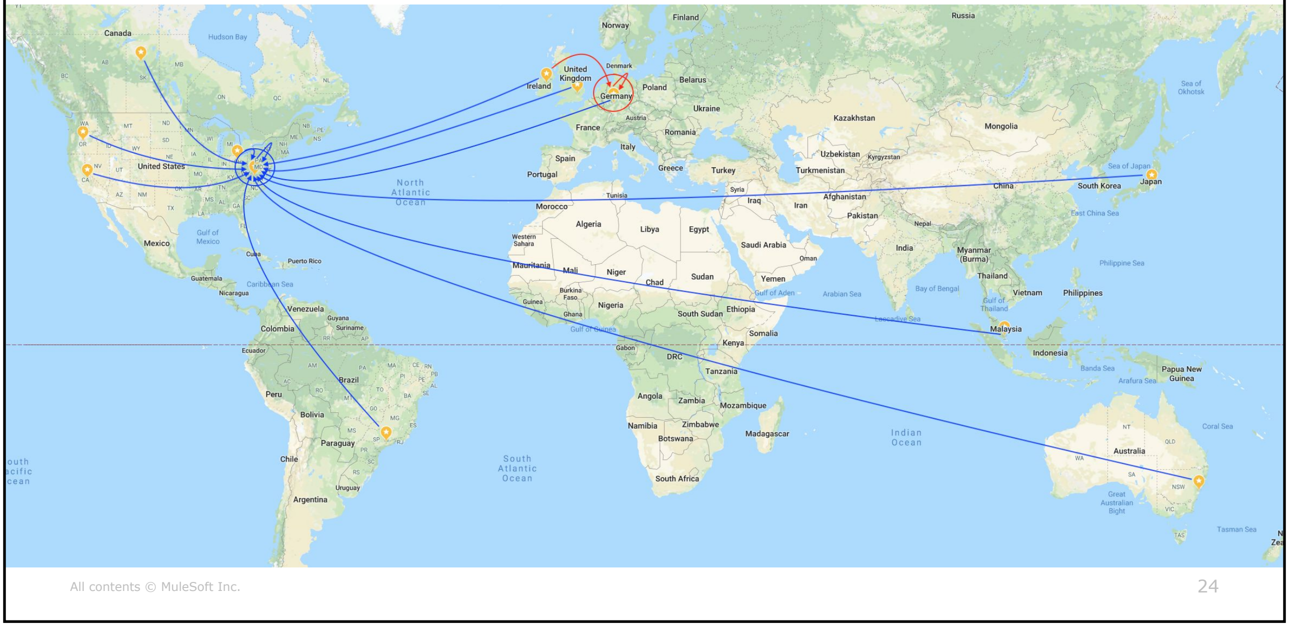
Evaluate scenarios along the following dimensions:

- **Regulatory** requirements of on-premises processing
  - Including meta-data about API invocations and messages
- **Time-to-market**
- **IT operations effort**
- Accessing **on-premises data sources**
- **Isolation** between Mule apps
- **Mule runtime tuning**
- **Scalability** of runtime plane
  - horizontal and vertical; static and dynamic
- Roll-out of **new releases**

Anypoint Platform data residency

- Location of **Mule runtime + integration logic** in Mule apps determine location and residency of all **data**
  - Message **payload** stays in Mule runtime
    - Possible exception (not by default): business events and Insight
  - **Persistent data** (ObjectStore, persistent VM queues, Anypoint MQ queues) in AWS region of runtime plane
- **Metadata incl. metrics** exchanged with Management Center
  - CPU/memory usage, message/error count, API name and version, geodata about the API client, HTTP method, violated API policy name, etc.
- **Mule apps** stored in Runtime Manager
- Typical **jurisdiction-local** deployments:
  - (EU/US control plane) + (EU/US or customer-hosted runtime plane)
  - Fully customer-hosted (Private Cloud Edition or for PCF)

MuleSoft-hosted control and runtime planes

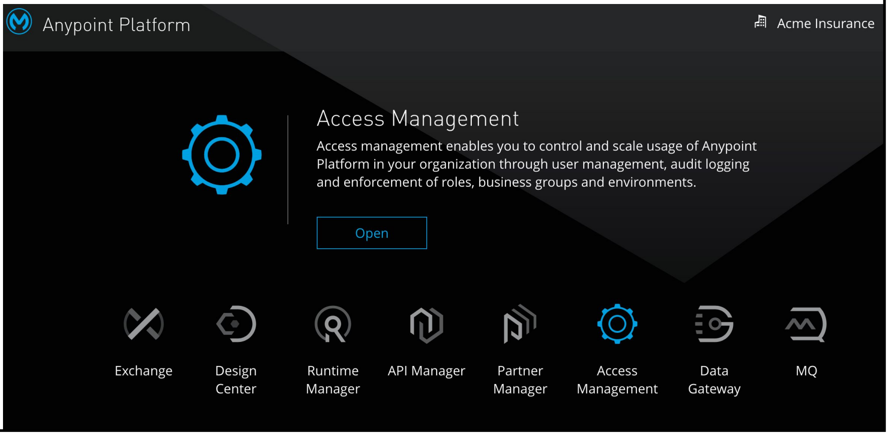


Onboarding Acme Insurance onto Anypoint Platform

Anypoint Platform Access Management

MuleSoft

- Controls access to **entitlements** in Anypoint Platform
- **Manage**
  - Business groups, users, roles and permissions
  - Environments
  - Other Resources



Anypoint Platform

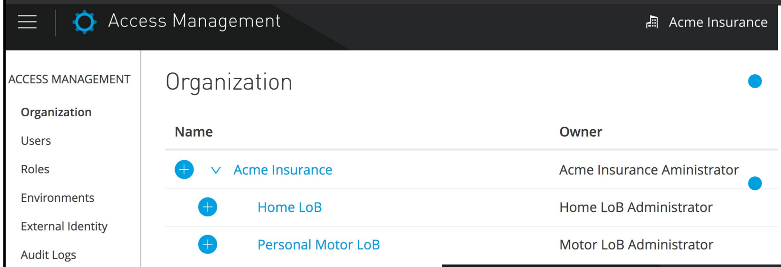
Acme Insurance

Access Management

Access management enables you to control and scale usage of Anypoint Platform in your organization through user management, audit logging and enforcement of roles, business groups and environments.

Anypoint Platform organizations and business groups

- **Organization**:
  - Administrative collection of resources and users
- **Business group**:
  - Sub-organization at any level



Access Management — Acme Insurance

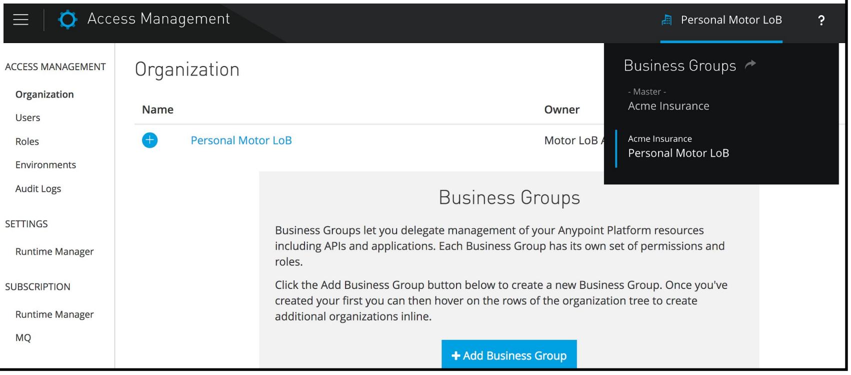
ACCESS MANAGEMENT
- Organization
- Users
- Roles
- Environments
- External Identity
- Audit Logs

SETTINGS
- Runtime Manager

SUBSCRIPTION
- Runtime Manager
- MQ

Organization

Name	Owner
Acme Insurance	Acme Insurance Aministrator
Home LoB	Home LoB Administrator
Personal Motor LoB	Motor LoB Administrator



Access Management — Personal Motor LoB ?

ACCESS MANAGEMENT
- Organization
- Users
- Roles
- Environments
- Audit Logs

SETTINGS
- Runtime Manager

SUBSCRIPTION
- Runtime Manager
- MQ

Organization

Name	Owner
Personal Motor LoB	Motor LoB A

Business Groups

- Master -
Acme Insurance

Acme Insurance
Personal Motor LoB

Business Groups

Business Groups let you delegate management of your Anypoint Platform resources including APIs and applications. Each Business Group has its own set of permissions and roles.

Click the Add Business Group button below to create a new Business Group. Once you've created your first you can then hover on the rows of the organization tree to create additional organizations inline.

+ Add Business Group

Identity Management vs Client Management

- **Identity Management** concerns users of Anypoint Platform
  - Human users of the Anypoint Platform web UI
  - Programmatic clients of Anypoint Platform APIs
  - Enables Single Sign-On (SSO)
  - Default: Anypoint Platform itself
- **Client Management** concerns API clients using OAuth 2.0
  - No default
- Anypoint Platform allows **one external Identity Provider each**
  - For Identity Management
  - For Client Management

Supported Identity Provider standards and products

MuleSoft

- For **Identity Management**:
  - Mapping of Anypoint Platform **roles to groups** in IdP
  - **OpenID Connect (OIDC)**
    - Implemented by PingFederate, OpenAM, Okta, ...
  - **SAML 2.0**
    - Implemented by PingFederate, OpenAM, Okta, Shibboleth, Active Directory Federation Services (AD FS), onelogin, CA Single Sign-On, ...
  - **LDAP**
    - Only on Anypoint Platform Private Cloud Edition
- For **Client Management** as OAuth 2.0 servers:
  - **OpenAM**
  - **PingFederate**
  - OpenID Connect Dynamic Client Registration (**OIDC DCR**)
    - Implemented by Identity Providers such as Okta and OpenAM

Selecting an Identity Provider for Acme Insurance

MuleSoft

- Currently Microsoft **Active Directory** (AD)
- Choose **PingFederate** as an Identity Provider ontop of AD
- Configure organization in MuleSoft-hosted Anypoint Platform to access on-premises PingFederate instance **for Identity Management**
- If OAuth 2.0 needed use same PingFederate instance **also for Client Management**

Summary

Summary

MuleSoft

- **Federated C4E** is established
  - **KPIs** to measure the C4E’s success are defined and monitored
- Anypoint Platform can be **hosted by MuleSoft or customers**
  - **Control plane** and **runtime plane**
- **Mule runtimes** can be **provisioned manually** or through **iPaaS**
- Not all Anypoint Platform **components** are available in all deployment scenarios
- Organization is **onboarded onto Anypoint Platform** using an external Identity Provider
- **Identity Management and Client Management** are clearly distinct functional areas supported by Identity Providers