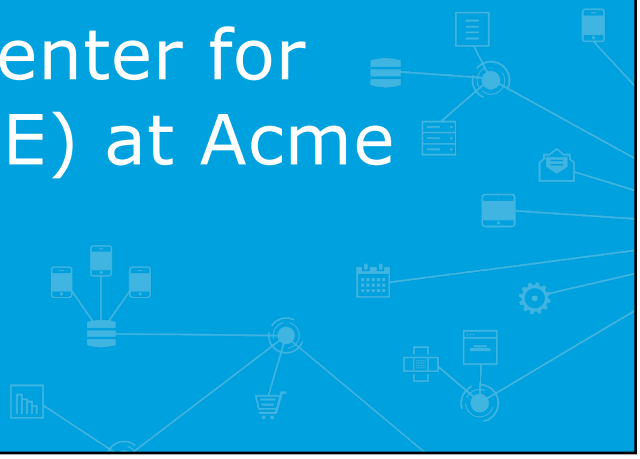
1

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

- 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

2

Section 1
Establishing a Center for Enablement (C4E) at Acme Insurance



3

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

4

4

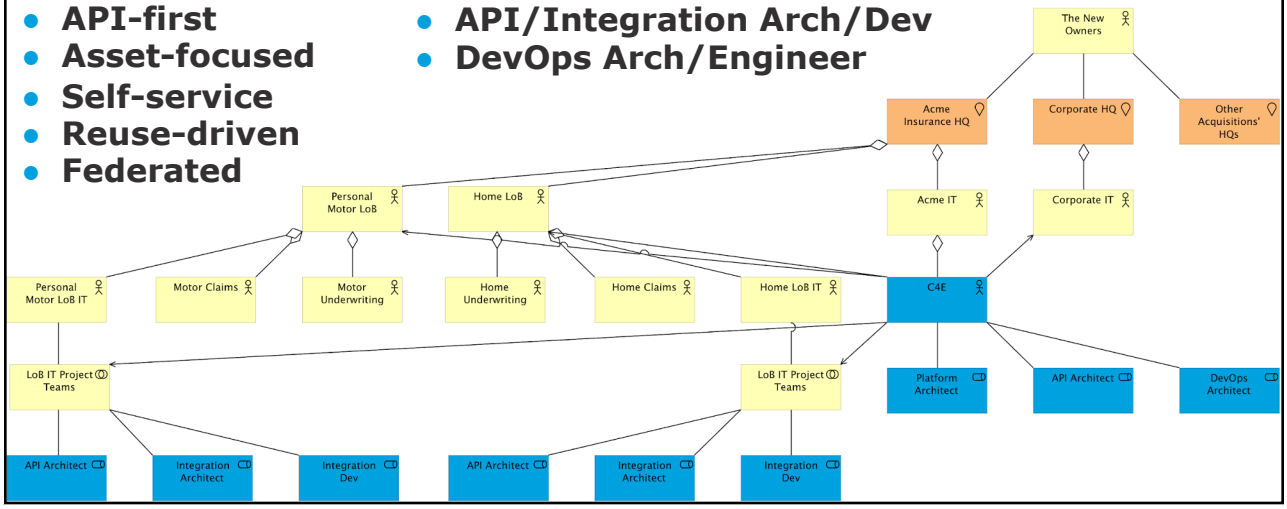
A decentralized C4E for Acme Insurance

Guiding principles:

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

Roles:

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



5

Exercise: Measuring success of the C4E

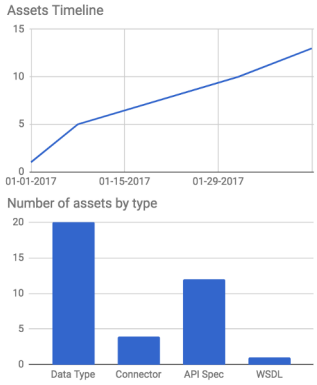
Thinking back on the application network vision on the one hand, and the principles of Acme Insurance's' C4E on the other hand:

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**

6

6

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



Key Performance Indicators (KPIs):

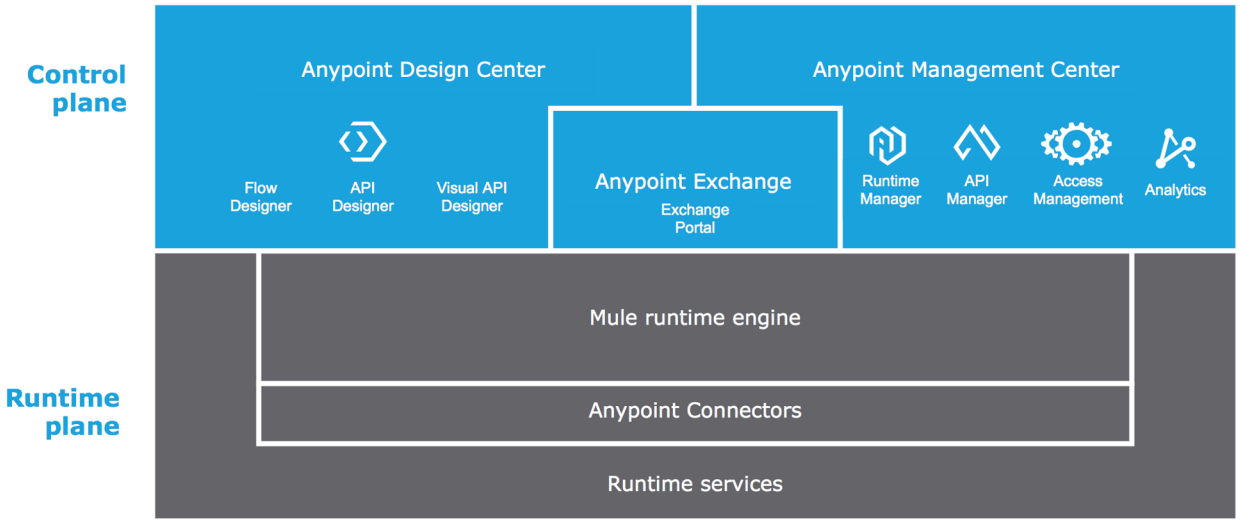
- # of assets published to Anypoint Exchange
- # of interactions with Anypoint Exchange assets
- # of APIs managed by Anypoint Platform
- # of API clients registered for access to APIs
- # of reused assets
- # of API implementations deployed to Anypoint Platform
- # of API invocations in a given period
- # or fraction of lines of code covered by automated tests in CI/CD
- # of automated scripts, reusable templates, … improving developer experience
- # or sum of alerts, production defects, total uptime, … measuring operational outcomes
- Fraction of API invocations that return HTTP 5xx responses
- Time to market (duration from specification to production deployment)

7

Section 2
Understanding Anypoint Platform deployment scenarios

8

Separating control plane and runtime plane



9

Anypoint Platform deployment option matrix

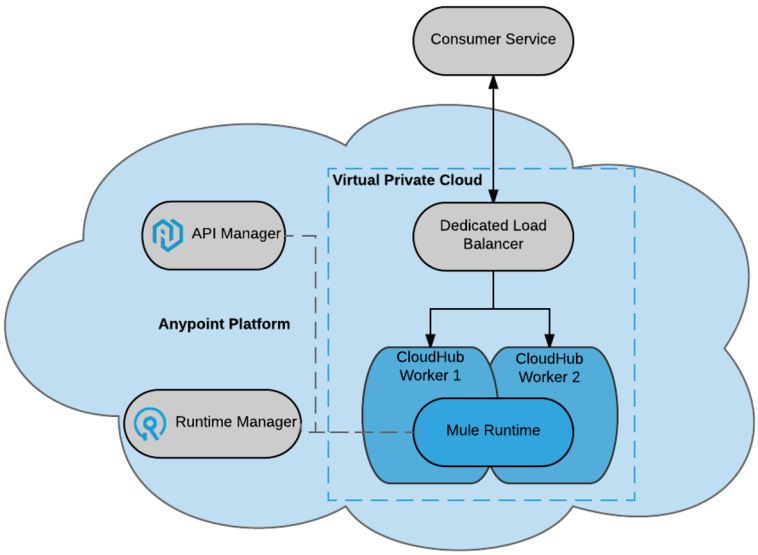
		Runtime Plane / Mule runtimes				
		MuleSoft-hosted			Customer-hosted	
		iPaaS-provisioned				Manually provisioned
		AWS public cloud	AWS VPC	AWS GovCloud	Kubernetes Docker	-
Control Plane	MuleSoft-hosted	**Anypoint Platform** with **CloudHub**	**Anypoint VPC** with **CloudHub**	**Mulesoft Government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

10

Deployment of control plane

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

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



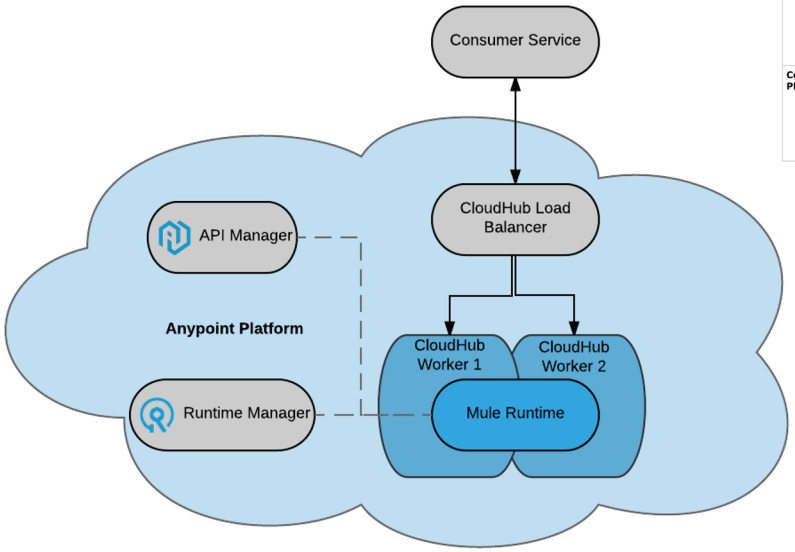
		Runtime Plane / Mule runtimes				
		MuleSoft-hosted				Customer-hosted
		iPaaS-provisioned				Manually provisioned
		AWS public cloud	AWS VPC	AWS GovCloud	Kubernetes Docker	-
Control Plane	MuleSoft-hosted	Anypoint Platform with CloudHub	Anypoint VPC with CloudHub	Mulesoft Government Cloud	Anypoint Runtime Fabric	Hybrid
	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)
  - In **AWS GovCloud**
- **Customer-hosted**
  - **Manually provisioned** Mule runtimes: metal, VMs, on-premises, cloud, ...
  - **iPaaS-provisioned** Mule runtimes:
    - MuleSoft appliance: **Anypoint Runtime Fabric on VM/Bare Metal**
    - Customer managed: **Runtime Fabric on Self-Managed Kubernetes**

13

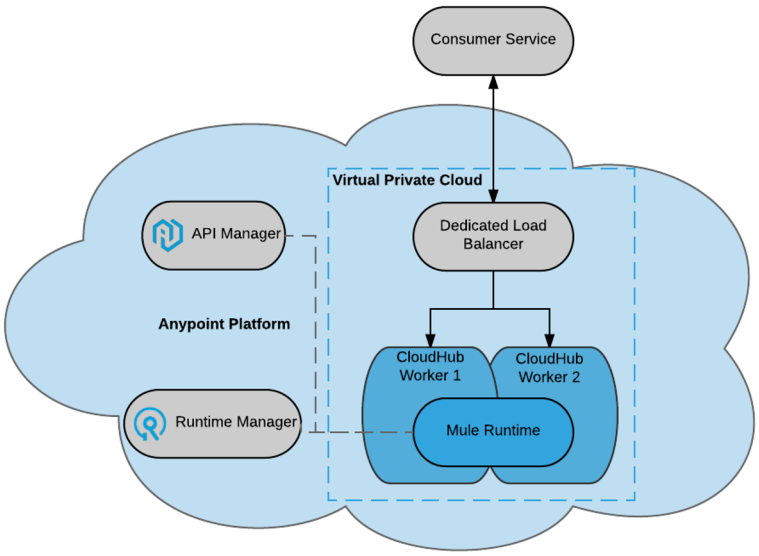
MuleSoft-hosted control plane and runtime plane with iPaaS functionality in public cloud



		Runtime Plane / Mule runtimes				
		MuleSoft-hosted				Customer-hosted
		iPaaS-provisioned				Manually provisioned
		AWS public cloud	AWS VPC	AWS GovCloud	Kubernetes Docker	-
Control Plane	MuleSoft-hosted	Anypoint Platform with CloudHub	Anypoint VPC with CloudHub	Mulesoft Government Cloud	Anypoint Runtime Fabric	Hybrid
	Customer-hosted	-	-	-	-	Anypoint Platform Private Cloud Edition

14

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

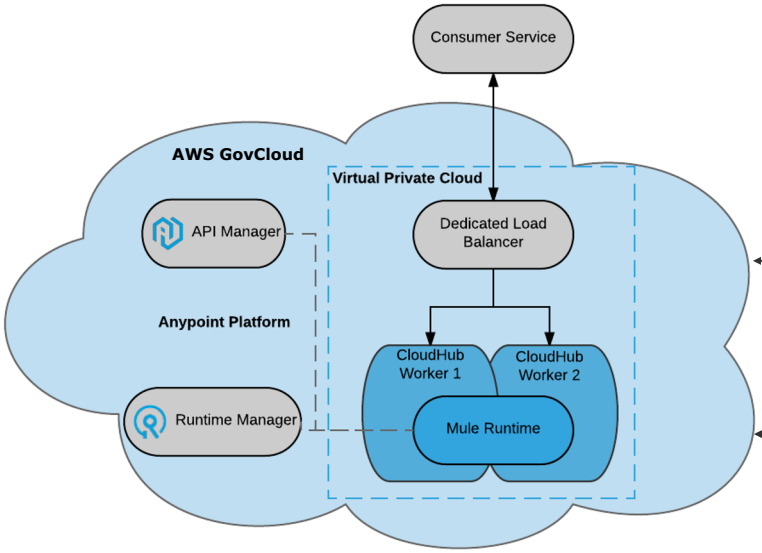


		Runtime Plane / Mule runtimes				
		MuleSoft-hosted				Customer-hosted
		iPaaS-provisioned				Manually provisioned
		AWS public cloud	AWS VPC	AWS GovCloud	Kubernetes Docker	-
Control Plane	MuleSoft-hosted	Anypoint Platform with CloudHub	Anypoint VPC with CloudHub	Mulesoft Government Cloud	Anypoint Runtime Fabric	Hybrid
	Customer-hosted	-	-	-	-	Anypoint Platform Private Cloud Edition

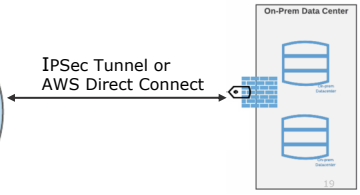
15

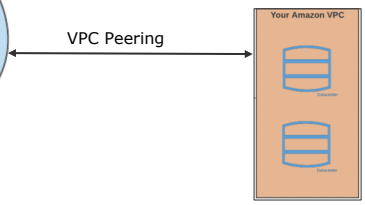
15

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



		Runtime Plane / Mule runtimes				
		MuleSoft-hosted				Customer-hosted
		iPaaS-provisioned				Manually provisioned
		AWS public cloud	AWS VPC	AWS GovCloud	Kubernetes Docker	-
Control Plane	MuleSoft-hosted	Anypoint Platform with CloudHub	Anypoint VPC with CloudHub	Mulesoft Government Cloud	Anypoint Runtime Fabric	Hybrid
	Customer-hosted	-	-	-	-	Anypoint Platform Private Cloud Edition

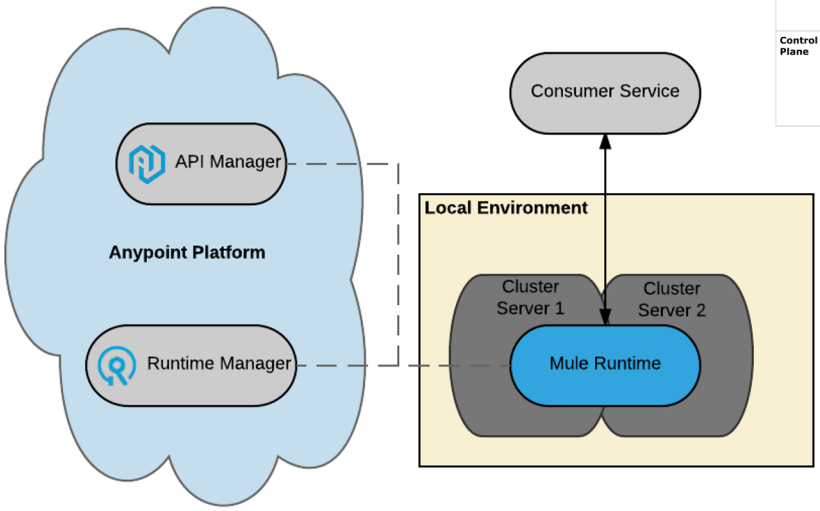




16

16

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

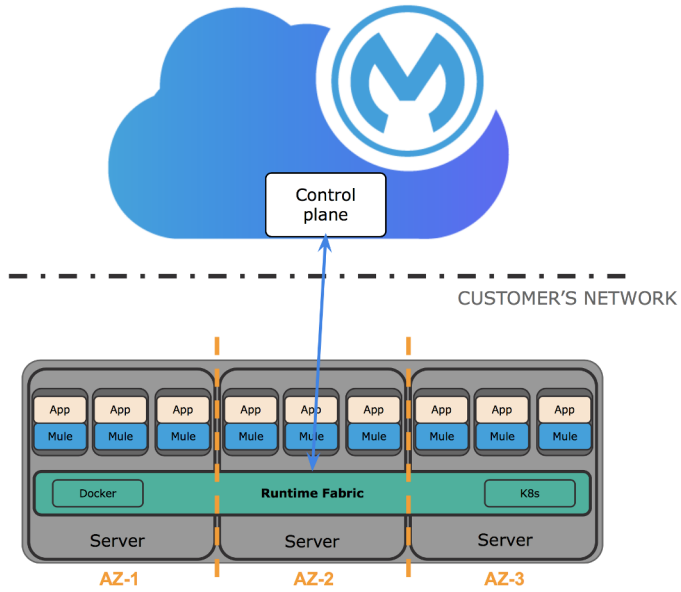


		Runtime Plane / Mule runtimes				
		MuleSoft-hosted				Customer-hosted
		iPaaS-provisioned				Manually provisioned
		AWS public cloud	AWS VPC	AWS GovCloud	Kubernetes Docker	-
Control Plane	MuleSoft-hosted	Anypoint Platform with CloudHub	Anypoint VPC with CloudHub	Mulesoft Government Cloud	Anypoint Runtime Fabric	Hybrid
	Customer-hosted	-	-	-	-	Anypoint Platform Private Cloud Edition

17

17

MuleSoft-hosted control plane and customer-hosted runtime plane with iPaaS functionality on Runtime Fabric



		Runtime Plane / Mule runtimes				
		MuleSoft-hosted				Customer-hosted
		iPaaS-provisioned				Manually provisioned
		AWS public cloud	AWS VPC	AWS GovCloud	Kubernetes Docker	-
Control Plane	MuleSoft-hosted	Anypoint Platform with CloudHub	Anypoint VPC with CloudHub	Mulesoft Government Cloud	Anypoint Runtime Fabric	Hybrid
	Customer-hosted	-	-	-	-	Anypoint Platform Private Cloud Edition

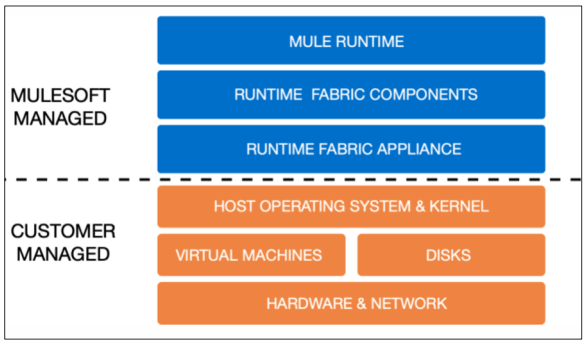
18

18

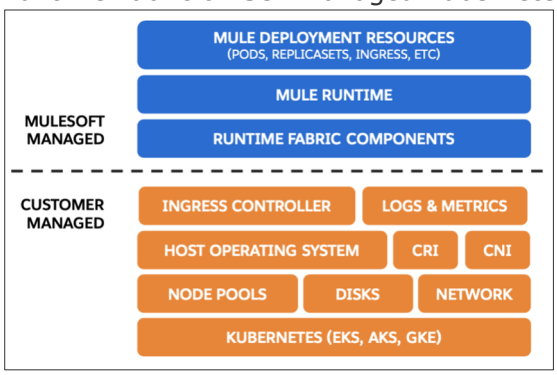
Runtime Fabric Shared Responsibility

MuleSoft

Runtime Fabric on VMs / Bare Metal



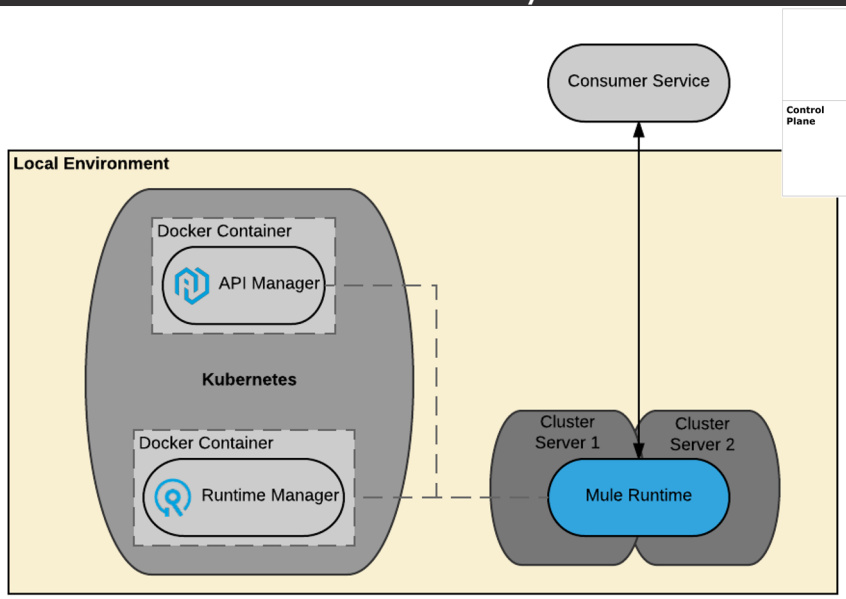
Runtime Fabric on Self-Managed Kubernetes

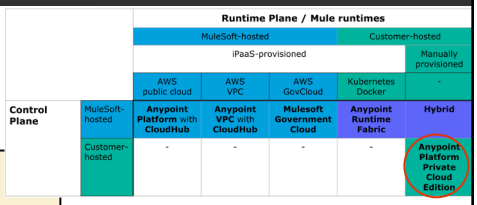


19

Customer-hosted control plane and runtime plane without iPaaS functionality

MuleSoft





20

Availability of Anypoint Platform components in different Anypoint Platform deployment scenarios

MuleSoft

Component	CloudHub	Hybrid	Runtime Fabric	Anypoint Platform Private Cloud Edition	Government Cloud
API designer	yes	yes	yes	yes	yes
Access Management	yes	yes	yes	yes	yes
Runtime Manager	yes	yes	yes	yes	yes
API Manager	yes	yes	yes	yes	yes
Anypoint Monitoring	yes	yes	yes	yes	no
Analytics	yes	yes	yes	no	no
Exchange	yes	yes	yes	yes	yes
Anypoint MQ	yes	no	no	no	no
iPaaS	yes	no	yes	no	yes

22

Exercise: Choosing between deployment scenarios

MuleSoft

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	AWS GovCloud	Kubernetes Docker	-
Control Plane	MuleSoft-hosted	**Anypoint Platform** with **CloudHub**	**Anypoint VPC** with **CloudHub**	**Mulesoft Government Cloud**	**Anypoint Runtime Fabric**	**Hybrid**
	Customer-hosted	-	-	-	-	**Anypoint Platform Private Cloud Edition**

23

Exercise: Choosing between deployment scenarios

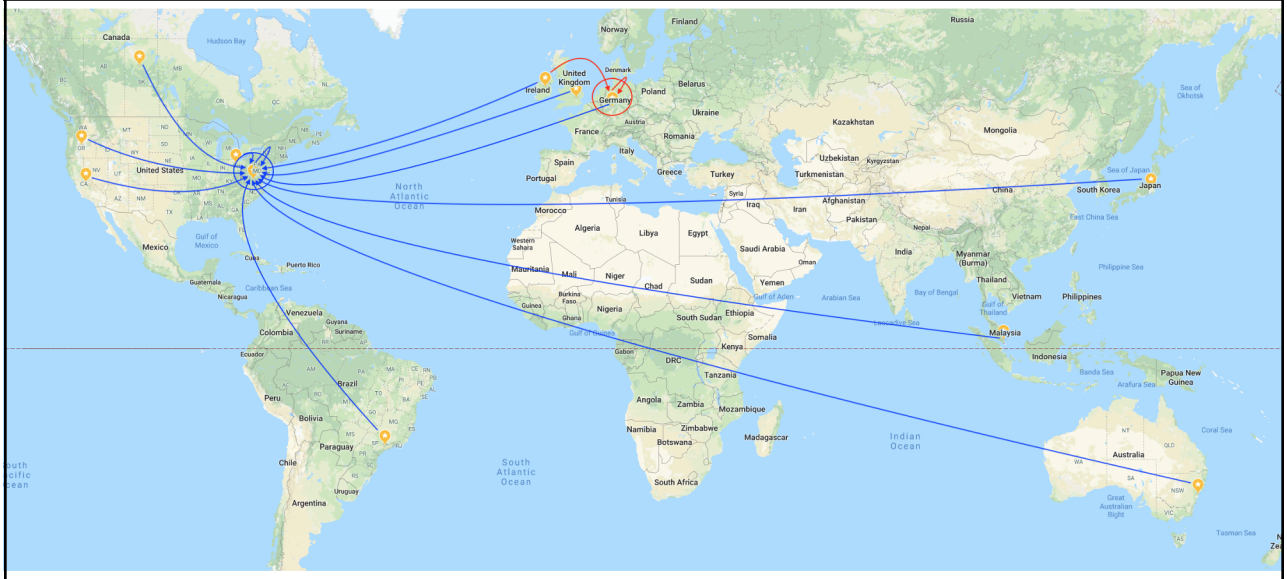
Evaluate scenarios along the following dimensions:

- **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



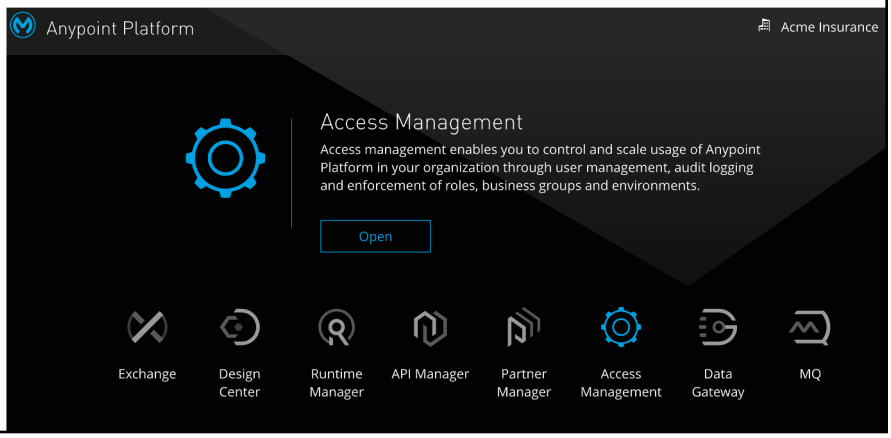
26

Section 3
Onboarding Acme Insurance onto Anypoint Platform

27

Anypoint Platform Access Management

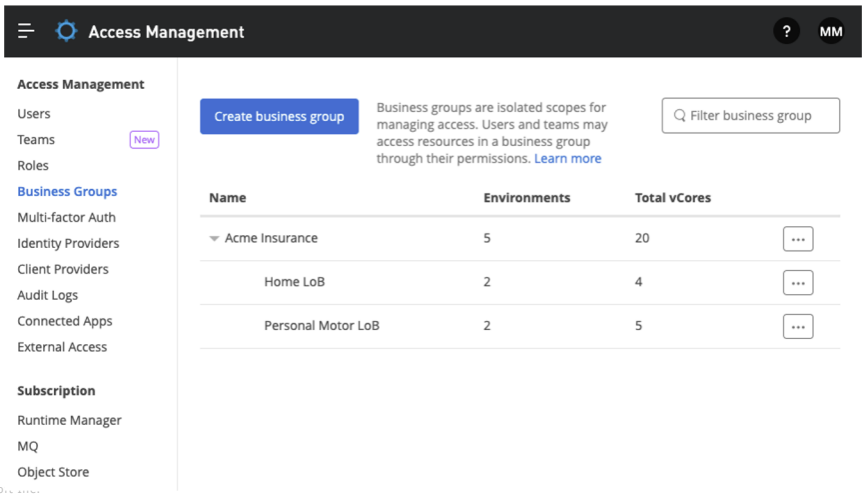
- Controls access to **entitlements** in Anypoint Platform
- **Manage**
  - Business groups, Teams, users, roles and permissions
  - Environments
  - Other Resources



28

Anypoint Platform Organizations

- **Organization**:
  - Administrative collection of resources and users



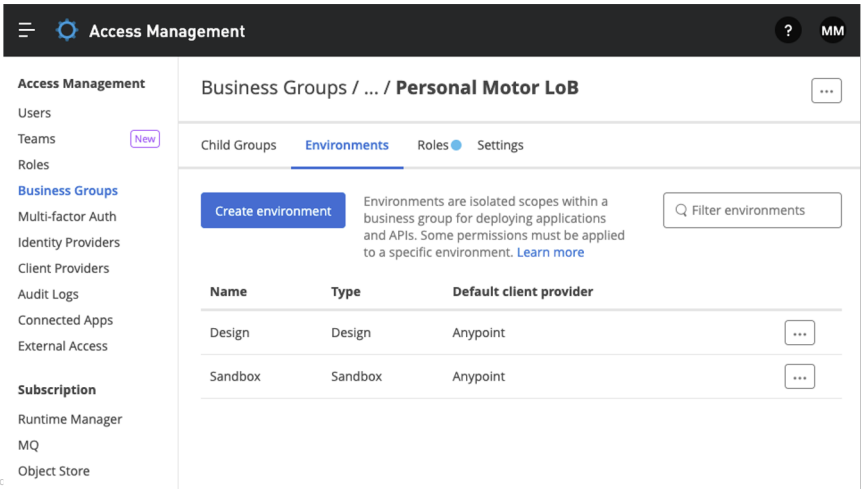
29

29

Anypoint Platform Business Groups

MuleSoft

- **Business Groups:**
  - Isolated scopes for managing resources and access



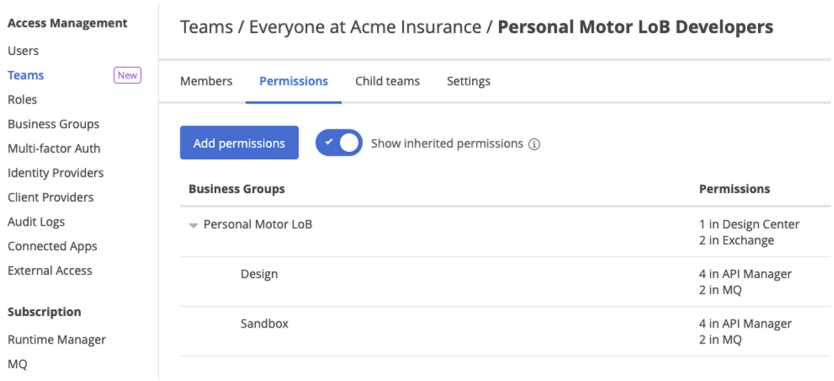
30

30

Introducing Teams: Scalable access management

MuleSoft

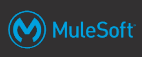
- **Teams:**
  - Users are assigned to one or more teams (All users belong to the Everyone team)
  - Permissions granted to a team are inherited by team members



31

31

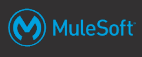
Introducing Teams: Scalable access management



- Like business groups, teams are created in a hierarchy
  - Unlike business groups, permissions inherit from parent to child teams
- Manage part or all of an Anypoint Platform Organization in one simple and global view
- Delegate team administration to other team members by designating them as team **maintainers**
- Manage user and team permissions across business groups in one place
- Share Exchange assets with entire teams rather than individual users

32

Identity 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
- Anypoint Platform also supports configuring one external Identity Provider

33

Client Management

Client Management concerns API clients using OAuth 2.0

- No default for OAuth 2.0 client management
- Anypoint Platform supports configuration of multiple external Client Providers for:
  - Different business groups
  - Different environments
  - Internal and external APIs and API clients

- When no external Client Provider is configured, Anypoint Platform acts as **internal Client Provider only for non-OAuth 2.0** Client ID-based policies like Client ID enforcement
  - See Module 5

34

Supported Identity Provider standards and products

- For **Identity Management**:
  - Mapping of Anypoint Platform **roles to groups** in IdP
  - **OpenID Connect (OIDC)**
    - Implemented by Salesforce Identity, PingFederate, OpenAM, Okta, ...
  - **SAML 2.0**
    - Implemented by PingFederate, OpenAM, Okta, Shibboleth, Active Directory Federation Services (AD FS), onelogin, CA Single Sign-On, …
    - supports rotation of SSO keys, thereby complying to security best practices
  - **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

35

Selecting an Identity Provider for Acme Insurance

- Currently Microsoft **Active Directory** (AD)
- Choose **PingFederate** as an Identity Provider on top 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**

36

Introducing Connected Apps

- The **Connected Apps** feature provides a framework that enables an external application to integrate with the Anypoint Platform using APIs through **OAuth 2.0** and **OpenID Connec**t
- Actions taken by connected apps are **audited**
- Supports the following use cases
  - **Organization Administrator** can control access by allowlisting apps, revoking access, and disabling this feature for the whole organization
  - An application **developer** can register new (and manage existing) apps
  - An **end user** can authorize apps to access particular information (e.g., assets in Anypoint Exchange)

37

Summary

38

Summary

- **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 and Client Providers

39