

Hybrid Enterprise API Deployment Patterns

Darko Vukovic
Director of Product Management
Oracle API Platform Cloud Service

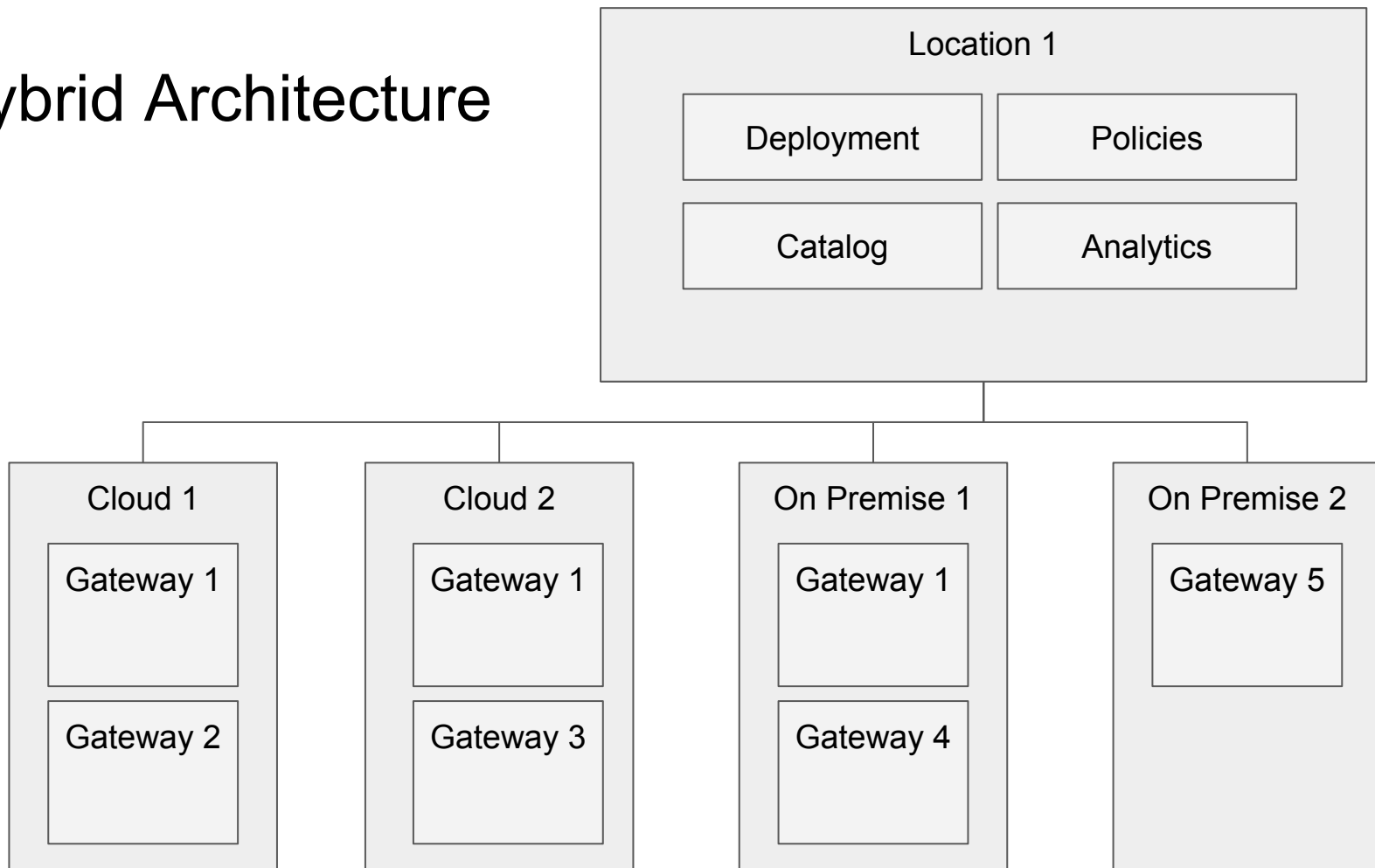
Agenda

- Terminology
- Hybrid API Architecture
- !Hybrid API Architecture
- Drivers for Hybrid Architecture
- API Deployment Topology Decisions
- 4 Enterprise Examples

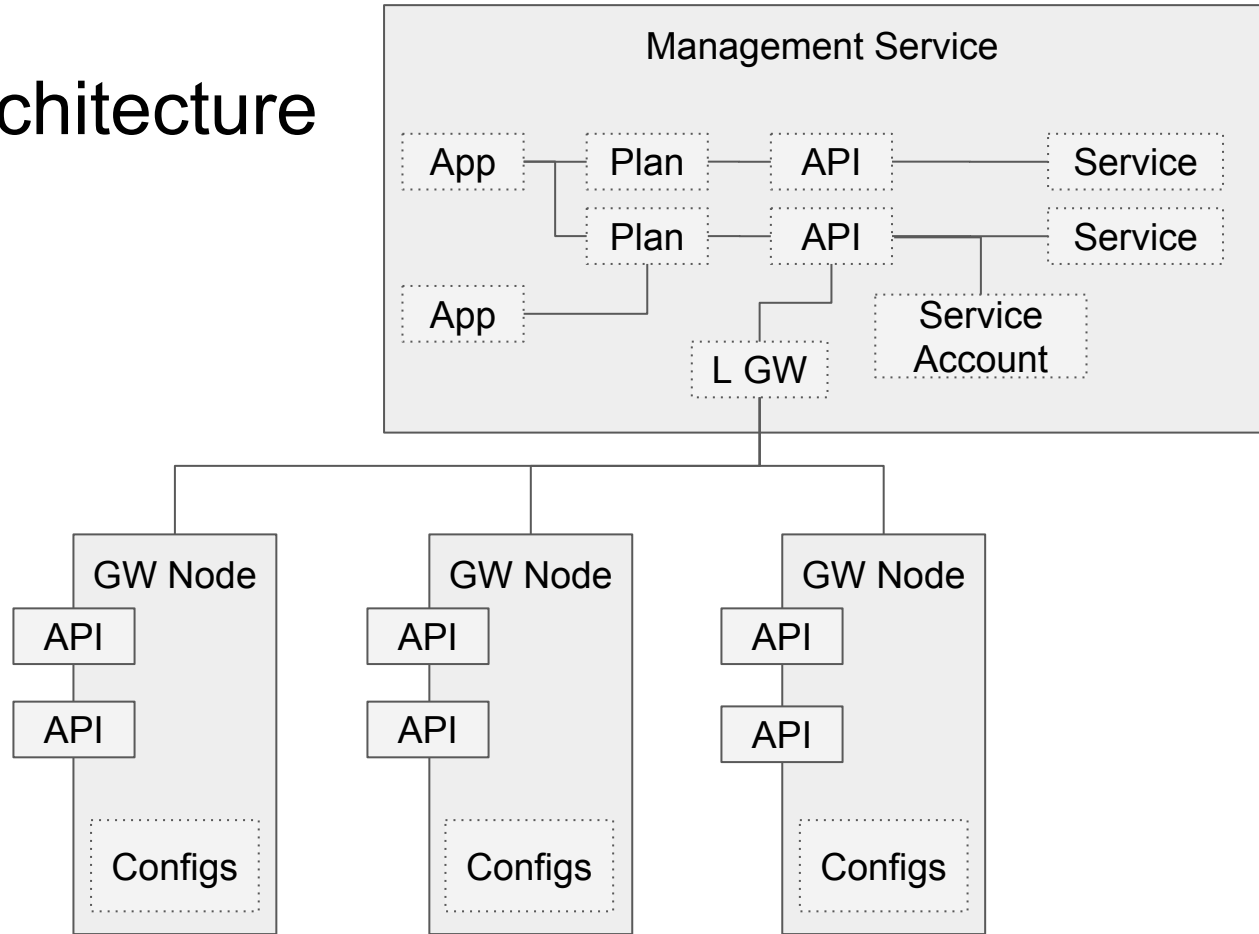
Component Terminology

Management Service	The source of truth system for all component state
Gateway	The runtime enforcement point for policies set in the management service
API	The endpoints exposed on the GW with a unique set of policy configurations
Service	The backend services to which successful requests are routed
Service Account	The credentials set by the GW to be used in accessing the service
Plan	Different tiers of access defined for different groups of consumers
Application	The identity of the requesting application

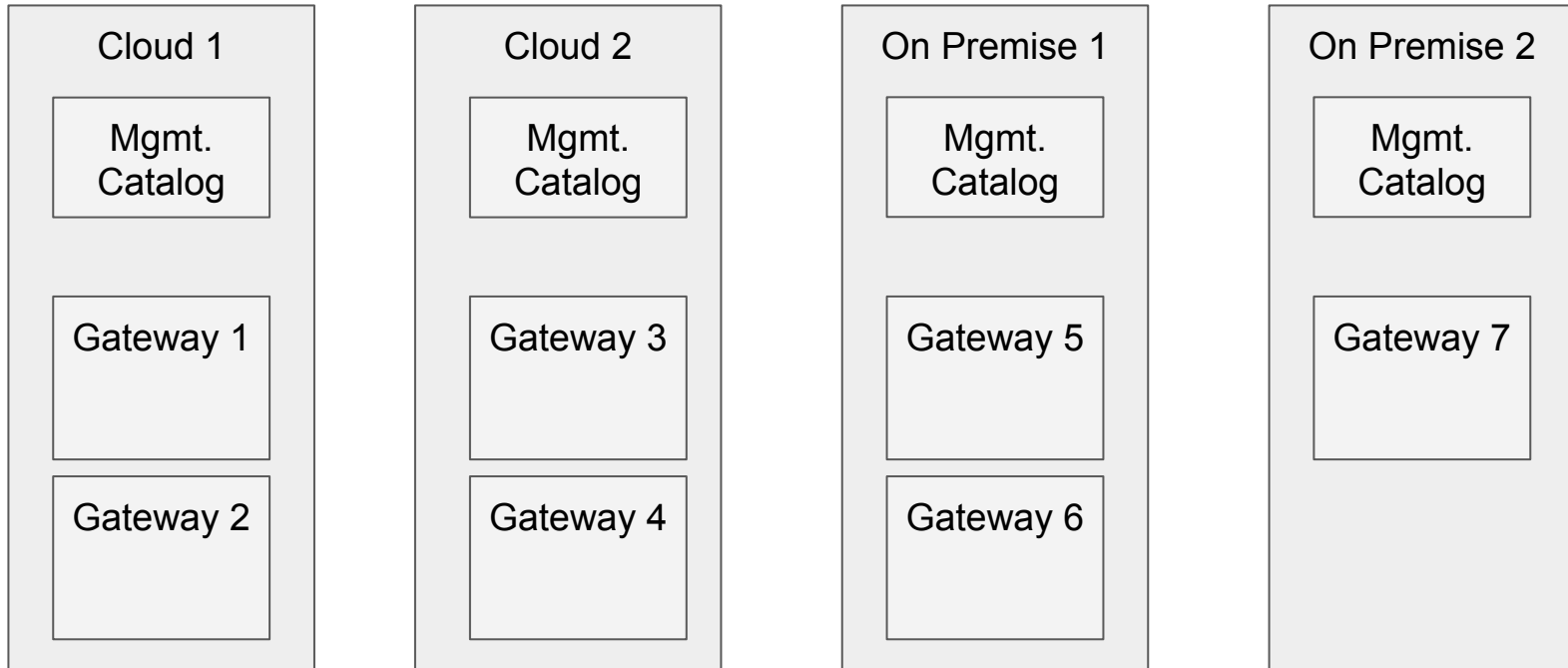
Hybrid Architecture



APIPCS Architecture



! Hybrid Architecture



Hybrid Drivers

- Situation:
 - 10,000s of employees across 10s of Business Units across the planet
 - Each business has its own regulations, competitors, customer profiles, business leaders
 - Generally collaboration between businesses is viewed as “low”
 - Generally large companies are perceived as “behind the times”

- Motivations:
 - Move “fast”
 - Hire the best talent
 - Cross sell
 - Manage cost
 - Achieve economies of scale

Management Service

Hybrid Impact

Option	Reason to do it	% customers	Things to watch for
One for whole company	<ul style="list-style-type: none">• Single API Catalog• Single Client IDs	~ 75%	<ul style="list-style-type: none">• Central Ownership Team
Production & Sandbox	<ul style="list-style-type: none">• Custom Policies• Training	~ 20%	<ul style="list-style-type: none">• Custom Policies from day 1?• Train with separate GW?
One per division (LOB P/L)	<ul style="list-style-type: none">• Future Divestitures• Separate Procurement• Secret Projects	< 5%	<ul style="list-style-type: none">• Separate LOB elsewhere?• Desire for common API catalog?
One per GW or IaaS	<ul style="list-style-type: none">• None - don't do it!	0%	<ul style="list-style-type: none">• Legacy thinking
One per Dev Team	<ul style="list-style-type: none">• None - don't do it!	0%	<ul style="list-style-type: none">• Misunderstanding of grants

Gateway Topologies

Hybrid Impact

Option	Reason to do it	% customers	Things to watch for
Managed by Central IT	<ul style="list-style-type: none">• Less training• Common infra• Tighter control on security & load	100%	<ul style="list-style-type: none">• Slower API Development• Bypassing of IT
Central IT Managed Prod/Pre Dev managed Dev/Test	<ul style="list-style-type: none">• Accelerated API development	*	<ul style="list-style-type: none">• Production Review Process
LOBs/Dev Managed	<ul style="list-style-type: none">• Decentralized Load Management• Faster Time to Value	*	<ul style="list-style-type: none">• Inconsistent security criteria• Compute/license cost

API Management Teams

Hybrid Impact

Option	Reason to do it	% customers	Things to watch for
Central API Management Team	<ul style="list-style-type: none">• High security requirement• Less training	50%	<ul style="list-style-type: none">• Slower time to value• Diminished concept testing & ideation
Automated, Template Driven, API Lifecycle	<ul style="list-style-type: none">• API standardization• Service deployment automation	10%	<ul style="list-style-type: none">• Premature automation• APIs as “endpoint” rather than “products”• Full lifecycle automation?
Product Managers, Developers, or Ops own APIs for their services	<ul style="list-style-type: none">• Time to value• Innovation• Ideation• Partnerships• APIs a “Product”	40%	<ul style="list-style-type: none">• Product education• Security & configuration reviews• Auditing

API Deployment Process

Hybrid Impact

Option	Reason to do it	% customers	Things to watch for
API Managers Deploy to All	<ul style="list-style-type: none">• Fastest time to value	0%	<ul style="list-style-type: none">• Training of API Managers• Security & load• Production monitoring
Production approval, Dev/Test Open	<ul style="list-style-type: none">• Central ops team• Security & load management• Time to value	80%	<ul style="list-style-type: none">• Prod guidelines communicated to API Managers
Production pull by GW Managers Dev/Test Open	<ul style="list-style-type: none">• Load Management• Out of Band Process	15%	<ul style="list-style-type: none">• Quality of process• Auditing
All Env Pull or Approval	<ul style="list-style-type: none">• Tight review process early in development	0%	<ul style="list-style-type: none">• Slow iteration & low GW Manager productivity
Externally Controlled and Automated	<ul style="list-style-type: none">• Infra automation• Fast iteration time	5%	<ul style="list-style-type: none">• Auditing• Whole lifecycle automation

Service Configuration

Hybrid Impact

Option	Reason to do it	% customers	Things to watch for
Managed by API Management team	<ul style="list-style-type: none">• Less training	50%	<ul style="list-style-type: none">• Service URL Changes• Communication between service ops and API Managers
Service Ops/Developers	<ul style="list-style-type: none">• DevOps ownership of services	30%	
Automated creation & update	<ul style="list-style-type: none">• Iteration speed• Provisioning speed• Lower risk of downtime	20%	<ul style="list-style-type: none">• Are all services automatable?

Service Accounts Identity Management

Hybrid Impact

Option	Reason to do it	% customers	Things to watch for
Managed by API Management team	<ul style="list-style-type: none">• Less training	60%	<ul style="list-style-type: none">• Service URL Changes• Communication between service ops and API Managers• Credential sharing method
Managed by Service Ops/Developer	<ul style="list-style-type: none">• DevOps ownership of services	20%	<ul style="list-style-type: none">• Credential sharing method
Managed by Identity Manager, Associated by Service Ops/Developer	<ul style="list-style-type: none">• Central IDM• Lower credential exposure risk	20%	
Automated Service Account Configuration	<ul style="list-style-type: none">• No credential exposure	0%*	<ul style="list-style-type: none">• Are all lifecycle functions automatable for each service type?

Plan Ownership

Hybrid Impact

Option	Reason to do it	% customers	Things to watch for
Managed by API Management team	<ul style="list-style-type: none">• Less training• Plans “access rights” to APIs	100%	<ul style="list-style-type: none">• Missed “API as a Product” opportunity
Managed by LOB “Biz Dev”	<ul style="list-style-type: none">• Business driven API strategy	*	<ul style="list-style-type: none">• Access & security configuration review

Client Application Identification

Hybrid Impact

Option	Reason to do it	% of customers	Things to watch for
Representing a client application	Default	90%	
Representing a partner	<ul style="list-style-type: none">• Partners don't want transparency• Partner rate limits to apply across all their apps	10%	
Representing a use case, region, user group,	<ul style="list-style-type: none">• Detailed analytics• Fine grain API access controls• Fine grain kill switch	0%	<ul style="list-style-type: none">• More complicated configuration• Misuse of user scopes

Example Customers

	Retail	Banking	Oil and Gas	Industrial
Annual Revenue	\$40 B	\$87 B	\$23 B	\$122 B
# of Employees	194,000	209,000	40,000	295,000
# of Business Locations	411	4,600	NA	NA
Platforms	AWS, Oracle, IBM, On-Premises	Private Clouds, On-Premises	Azure, AWS, Oracle, On-Premises	Azure, Oracle

Customer Example - Retail - Centralized

Component	Choice	Reason
Management Service	Production & sandbox	Common API catalog
Gateway Infra	Managed centrally	Lower costs from sharing GWs, central skill, automation
API Management	Both Central & LOB API Management Teams	Some LOBs want to hand the work over, others do not want to be dependent, use different IaaS/PaaS
API Deployment	Production Request Model LOB has right to deploy to DEV/Test	Separation of concerns for ITSEC. GW load management.
Service Management	Both Central & LOB API Management Teams	Team size
Service Accounts	Managed by Central API Team*	Security reasons, credentials exposure to LOB
Plans	Both Central & LOB API Management Teams	Team size.
Applications	Representing a Client Application	Partner is too coarse grained, better visibility

Customer Example - Banking - Decentralized

Component	Choice	Reason
Management Service	<u>One per LOB</u>	Each LOB is a separate business
Gateway Infra	Managed by Separate LOBs/Dev Teams	LOBs use different IaaS/PaaS
API Management	LOB Ops own APIs for their services	APIs used for access management
API Deployment	Production approval API Managers deploy to Dev/Test	Separation of concerns for ITSEC. GW load management.
Service Management	Service Ops/Developers	Delegated services ownership
Service Accounts	Service Ops/Developers	Delegated services ownership
Plans	Managed by LOB API Manager	APIs used for access management
Applications	Representing a Client Application	Standard approach

Customer Example - Oil and Gas - Mixed

Component	Choice	Reason
Management Service	Production & Sandbox	Common API Catalog
Gateway Infra	<u>Managed by Separate LOBs/Dev Teams</u>	Self Sufficient LOB Dev Teams, different IaaS/PaaS
API Management	LOB Dev/Ops	Manual, intend to automate
API Deployment	Production approval by Dev Management API Managers deploy to Dev/Test	- -
Service Management	LOB Dev/Ops	- -
Service Accounts	LOB Dev/Ops	- -
Plans	LOB Dev/Ops	- -
Applications	Mix of Client Application & Partner	Few partners want broad access rights

Customer Example - Industrial - Mixed

Component	Choice	Reason
Management Service	Production & Sandbox	API Management as a Service
Gateway Infra	Managed Centrally	GWs are part of “API Management” as a Service
API Management	LOB Ops	LOBs own their own services and access rights
API Deployment	Production Pull Model Managed Externally, LOB has right to deploy to DEV/Test	Have other systems for managing deployments & service requests
Service Management	LOB Ops	LOBs own their own services/accounts
Service Accounts	LOB Ops	- -
Plans	LOB Ops	- -
Applications	Representing a Client Application	Apps are internal only

Conclusions

- All large companies require hybrid topologies to a varying degree
- Industry domain doesn't matter for deployment topologies
- Size of company **may** lead to more complex topologies, does not have to
- How a company operates LOB/P&Ls matters for Management Service topology
- How a company operates dev team infrastructure determines GW topologies
- Maturity of API initiatives (width and depth) determines roles, processes, automation, and number of people involved
- Partner drive may lead to client applications representing partners

Implementing Oracle API Platform Cloud Service



<http://apiplatform.cloud/>