Towards a Comprehensive ONAP Operations Management Solution

Presenters: Ramki Krishnan (VMware), David Sauvageau (Bell Canada), Sastry Isukapalli (AT&T)

Key Demo Contributors:

Wind River: Gil Hellmann; Amdocs: Michael O'Brien

Collaborators:

VMware: Sumit Verdi, Xinhui Li, Danny Lin, Ramesh Tammana
Wind River: Gil Hellmann
AT&T: Bin Hu, Marco Platania
Bell Canada: Marc-Alexandre Choquette, David Sauvageau
Amdocs: Michael O'Brien

Primary Source: Kubecon Austin 2017 ONAP Mini Summit presentation “Open Source Cloud Native NFV Operations Management & Security: ONAP Perspective”
Other Sources: Material from various Kubecon Austin 2017 presentations on leading edge open source technologies for platforms & microservices

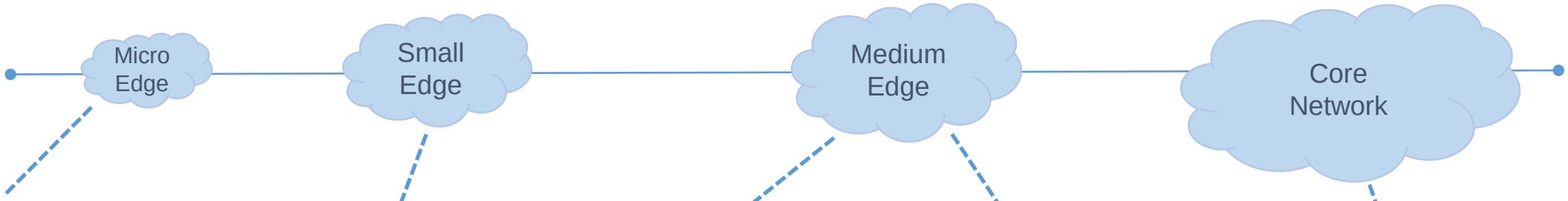
Agenda

- Use Cases – Edge → Core Deployment Profiles
- Cloud Native NFV/Edge Deployment Options
- ONAP Perspective
  - OOM Deployment Architectural Vision
  - Multi-vendor Demo
- Towards ONAP S3P and Beyond: Leveraging Advances in Service-Mesh Architecture
  - Examples of Technologies related to Stability & Security

Use Cases – Edge → Core Deployment Profiles

Key Industries:
Telco (e.g. NFV, 5G, and IoT),
Retail (e.g. IoT, Supply Chain)

Key Application Domains:
Surveillance (e.g. CCTV),
Telematics, Enterprise Security



Micro Edge Device
- Remote Radio Head
- Remote Radio Unit
- CPE / set top box

Runs a single instance, instance changes infrequently

Small Edge Device
- Retail Wi-Fi
- POS for a store
- Cell tower site

Multiple instances, instances change occasionally

Medium Edge Backhaul, **Critical Deployment**
- Cloud-RAN
- Big cell site
- National Broadband Network Point of Interconnect (NBN-POI)

Multiple instances, instances change daily

Medium Edge Backhaul, **Non-Critical Deployment**
- Big box retail
- Cloudlet

Multiple instances, instances change daily

Core Network
- Region DC
- IMS
- EPC Control Plane

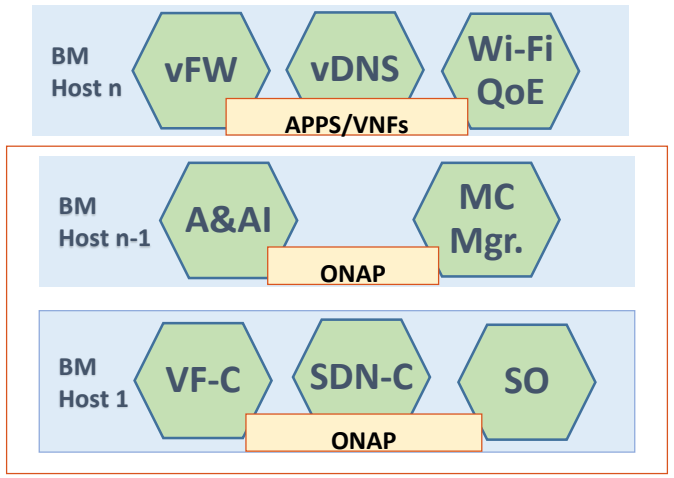
Thousands of instances, instances changing constantly

* Use cases were identified in OpenDev 2017

Cloud Native NFV/Edge Deployment Options

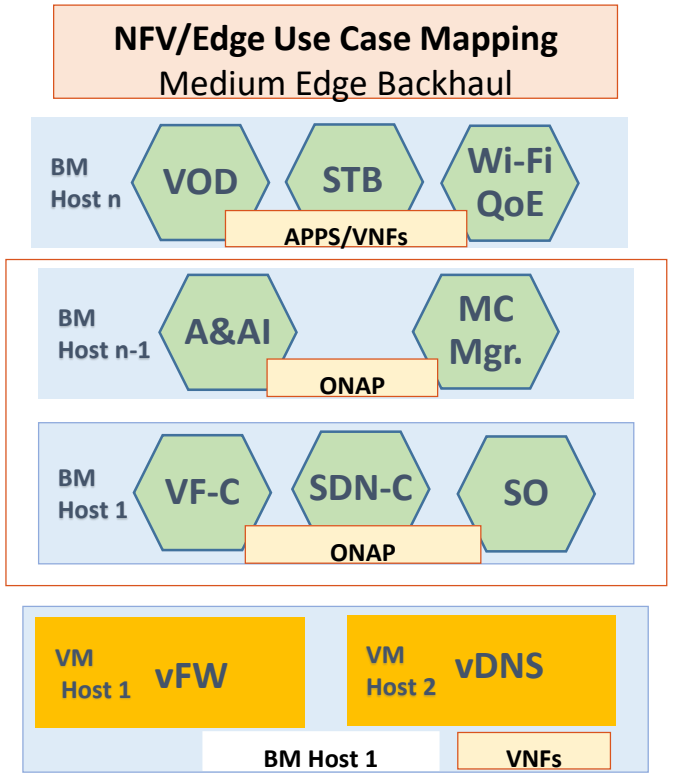
Bare Metal (Small Scale)

NFV/Edge Use Case Mapping
Micro Edge/Small Edge



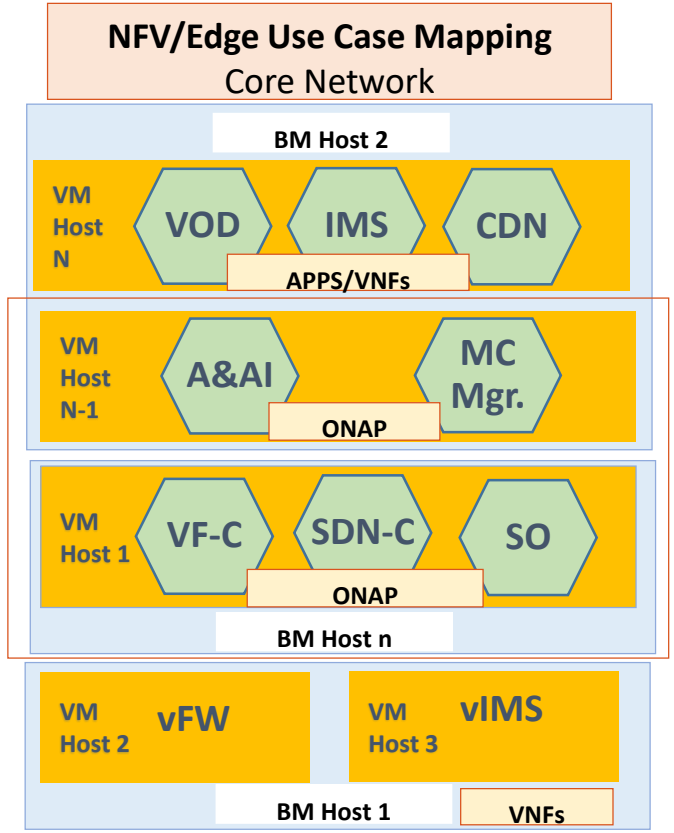
Hybrid (Medium Scale)

NFV/Edge Use Case Mapping
Medium Edge Backhaul



CaaS (Hyper Scale)

NFV/Edge Use Case Mapping
Core Network

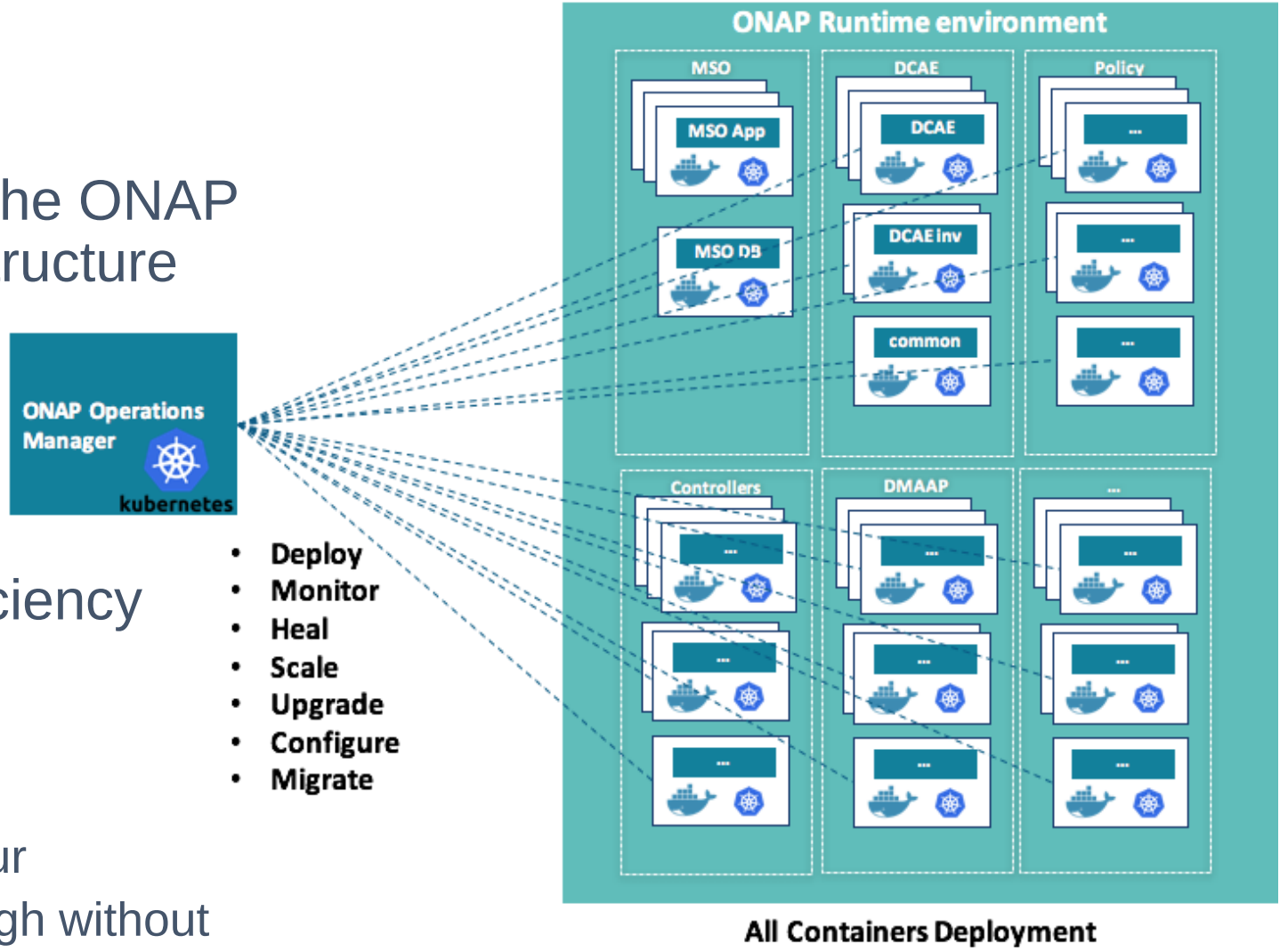


Source: ONAP Mini Summit in Kubecon 2017

Legend:
STB – Set Top BOX; EPG – Electronic Programming Guide; VOD – Video On Demand; IMS – IP Multi Media Subsystem
BM - Bare Metal; VM – Virtual Machine; Hybrid – Mix and Match VM and BM hosts;
CaaS – Container Orchestration on VM Hosts;
Containerized ONAP components – A&AI, SDN-C etc.

ONAP Operations Manager (OOM) Background

- ONAP on Containers (K8s)
- Supports Bare Metal or VM hosts
- Efficiently deploy, manage, operate the ONAP platform, its components, and infrastructure
  - Life-cycle Management
  - Hardware Efficiency
  - Deployment Speed
  - Cloud Provider Flexibility
- Deployment Speed & Hardware Efficiency (vs OpenStack deployment):
  - Memory: 200 GB vs 60 GB
  - Disk Space: ~ 1.3 TB vs 120 GB
  - Deployment time (US): 2 hours vs 1 hour
  - Deployment time (international): very high without mirrors

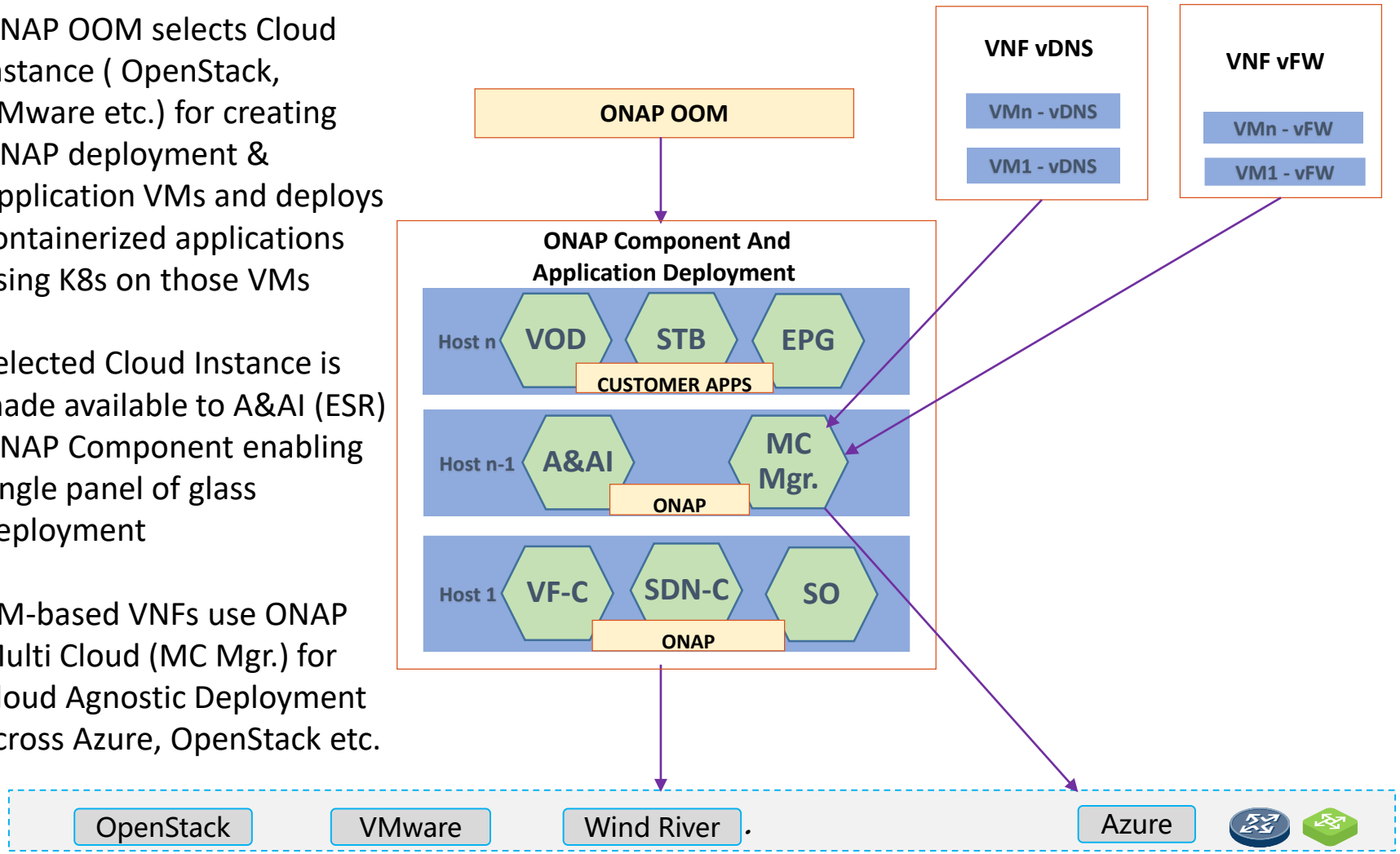


OOM Deployment Architectural Vision

ONAP OOM selects Cloud Instance (OpenStack, VMware etc.) for creating ONAP deployment & Application VMs and deploys containerized applications using K8s on those VMs

Selected Cloud Instance is made available to A&AI (ESR) ONAP Component enabling single panel of glass deployment

VM-based VNFs use ONAP Multi Cloud (MC Mgr.) for Cloud Agnostic Deployment across Azure, OpenStack etc.

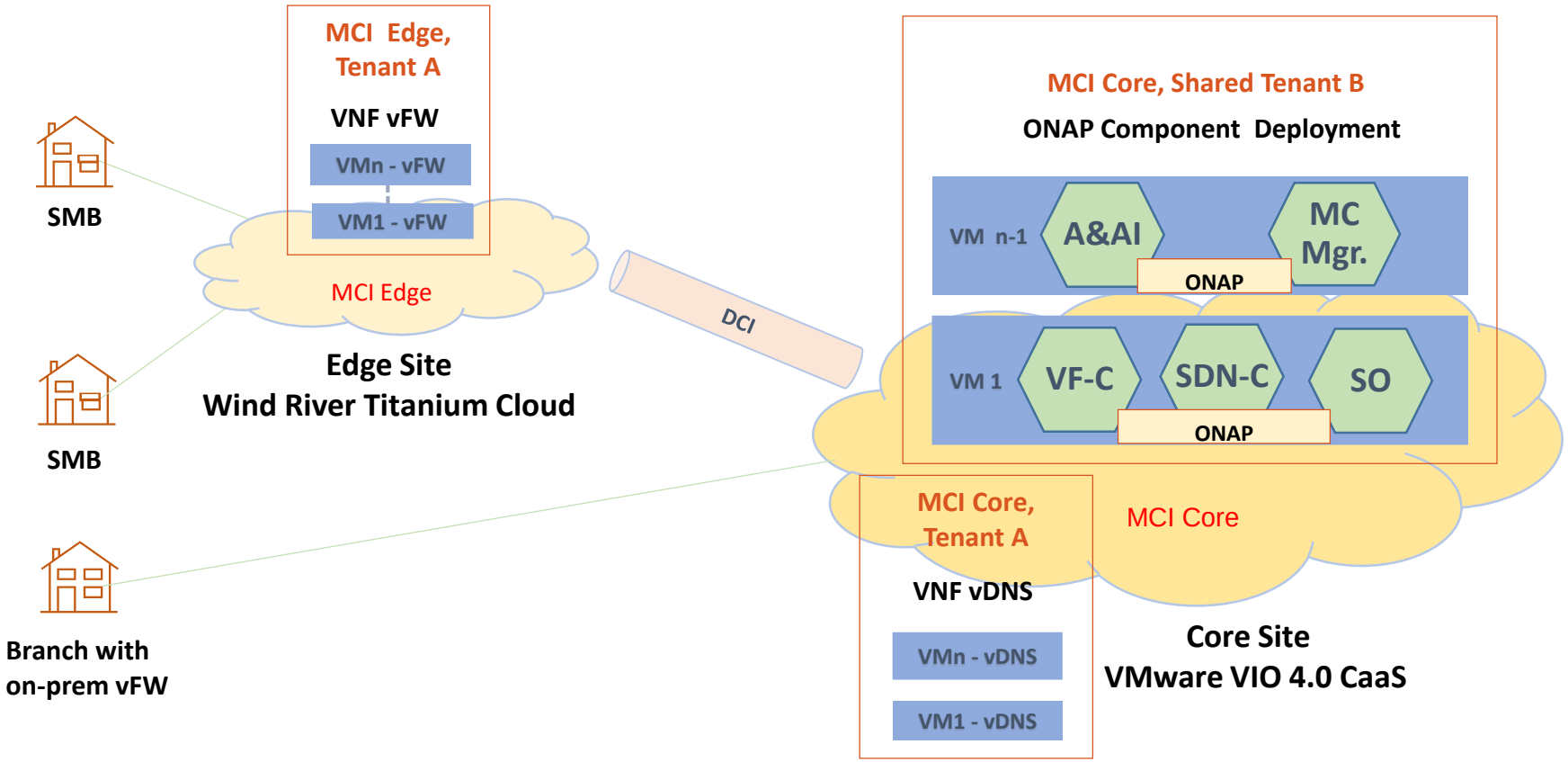


Flexible Architecture

Support Bare Metal, Hybrid and CaaS deployment options

Legend:
STB – Set Top BOX; EPG – Electronic Programming Guide; VOD – Video On Demand
Host – VM or Bare Metal

Multi-vendor Demo



CaaS - Simplifying Workload Management & Delivering Native Security

Single pane of glass deployment for Containerized Microservices and VM-based Applications/VNFs
Native HW security/isolation for all Components and VNFs

Pivotal Container Service

ONAP Multi Cloud

Cloud Agnostic VNF deployment across Wind River Titanium Cloud and VMware VIO

Multi Cloud Instance (MCI) Core (VMware VIO 4.0) - Core site with containerized ONAP component microservices deployed on VMs and vDNS VNF VMs
MCI Edge (Wind River Titanium Cloud) - Edge site with vFW VNF VMs

Admin deploys ONAP component microservices using ONAP OOM which leverages VMware VIO K8s running on VMware VIO VMs

WIND™
AN INTEL COMPANY

Multi-vendor Demo – More Details

- ONAP on VIO 4.0 – Container Orchestration
  - https://wiki.onap.org/display/DW/ONAP+on+VIO+-+Container+Orchestration

- Intel/Wind River/VMware lab on VIO 4.0 enablement
  - Work in progress

ONAP S3P: Leveraging Advances in Service-Mesh Architecture

Provides infrastructure level functionality for service discovery, load balancing, network flow, logging, tracing, etc. [adapted from Envoy documentation]

Service-Mesh architecture leverages design patterns for distributed systems such as:
(a) pluggable sidecars
(b) proxies for multiple aspects such as logging, metrics, and security tokens
(c) support for audit and compliance

Core service mesh: Istio, Linkerd
Identity and Authentication: SPIFFE/SPIRE, Vault
Visibility/Troubleshooting: OpenTracing, Jaeger, Zipkin
Service Discovery: Consul, Envoy
Policy-Based Network Security: Calico, Weave, Cilium
End-to-end Application Security: Twistlock, Aqua
Scalability/Stability: Prometheus, Istio

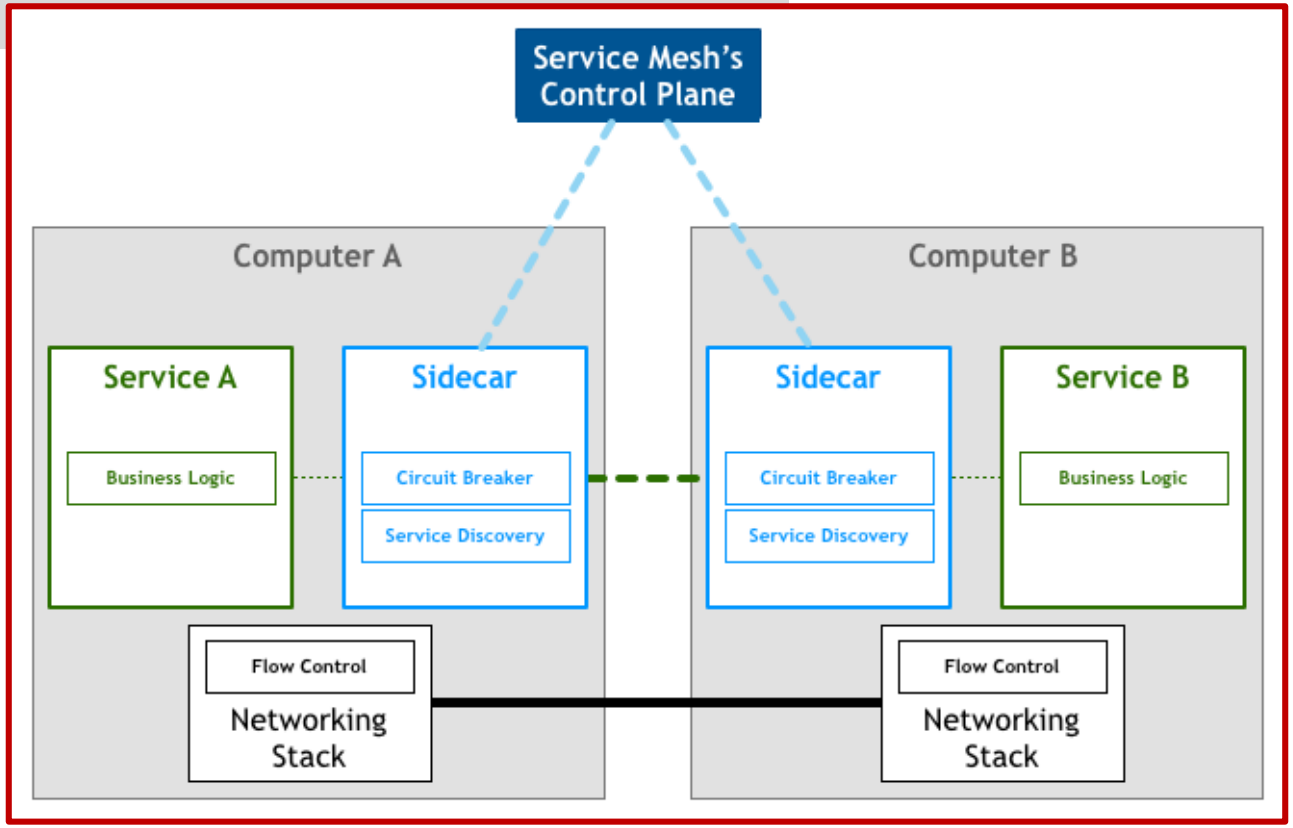


Image Source Philip Calcado, Bouyant Inc.
http://philcalcado.com/2017/08/03/pattern_service_mesh.html

S3P: Stability (Examples with Cloud Native Service Mesh Architecture)

Automatically maintain multiple versions

- Istio/Envoy service tags provide finer-grained routing (partitioning endpoints between A/B for A/B testing)
- Upgrades can be tested in real production environments without affecting services

Fault tolerance

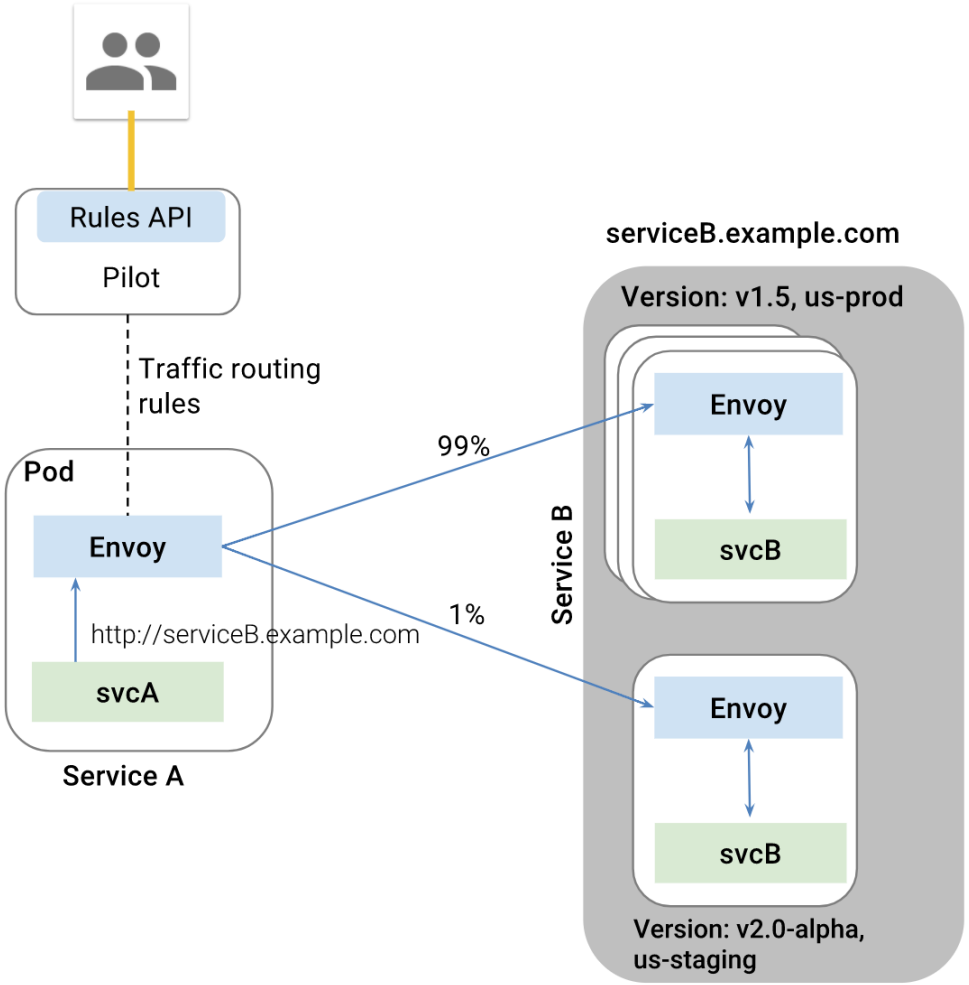
- K8S as a supervisor can restart containers
- Best practice: exit container with a proper return code
- Reduces retry error handling code in applications

Simpler architecture

- Reduces code changes and increases stability
- Most functionality in sidecar containers (infrastructure)
- Application is not aware of sidecars

Simple APIs like in Hadoop MapReduce Ecosystem

- User needs to implement just a mapper and a reducer
- Rest all is provided by Hadoop infrastructure



Service Versions

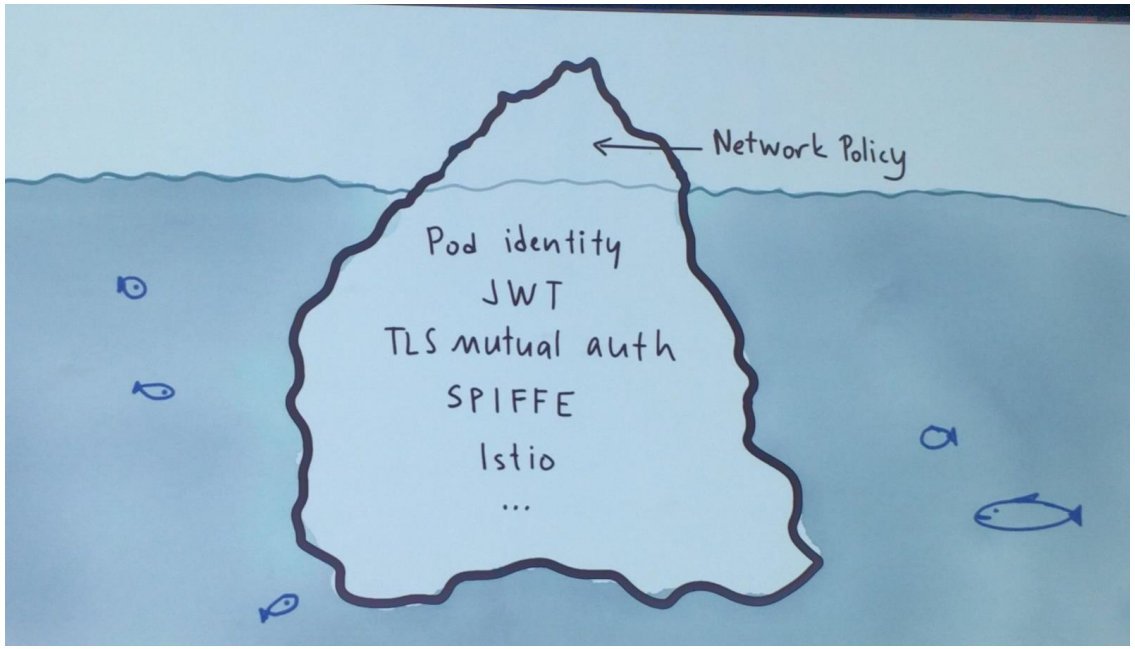
Source: Istio documentation
https://istio.io/docs/concepts/traffic-management/request-routing.html

S3P: Security (Examples with Cloud Native Service Mesh Architecture)

Traditional perimeter security via firewalls is not sufficient
- Often, more attacks originate from "inside”
- Definitions of "inside" and "outside" change dynamically

Specialized techniques for single type of security are not sufficient
- EBPF techniques can be used, but not sufficient

Requires mutual TLS between all segments (across each hop)
- Currently, often internal communication is not encrypted



Source: talk by Ahmet Balkan (Google) at Kubecon 2017
via Tweet from Evan Gilman (Scytale; @evan2645)

Policy based orchestration of network security
- Proxies within the control plane or as pluggable sidecars can be used

Authentication and secure service-to-service traffic management
- Secret management, regular rotation of credentials, bootstrapping credentials
- Compatibility with variety of external authentication systems

Example: Secure Production Infrastructure Framework for Everyone (SPIFFE/SPIRE)

BACKUP

NFV/Edge Deployment Options and Trade-Offs (General)

	Bare Metal (BM)	Hybrid (VM + BM)	CaaS (VM)
Base Architecture	Everything over K8s over bare metal hosts	Containerized applications on K8s cluster over bare metal hosts; Rest on VMs	Everything over VMs, including K8s clusters
Application/VNF Architecture	All applications and VNFs have to be containerized	Support containerized and VM-based Applications and VNFs	Support containerized and VM-based Applications and VNFs
Mixed Workloads	No Support for VM-based VNF/Application workloads	Supports containerized and non-containerized workloads	Supports containerized and non-containerized workloads

Note: VNFs can be potentially developed as native OS processes [NetBricks], but entails redevelopment of the entire stack and applications

NFV/Edge Deployment Options and Trade-Offs (Management)

	Bare Metal (BM)	Hybrid (VM + BM)	CaaS (VM)
Operational Simplicity	Single panel of glass deployment for containers	Independent management of Bare Metal and VM hosts	Single pane of glass deployment for containerized and VM-based Applications/VNFs
Mixed Hardware Portability	No hardware-independent abstraction for normalized capability and capacity metrics	Partial support (limited to VM-based Hosts)	VM-based Hosts provide normalized capability and capacity metrics across mixed hardware
Scalability	Dynamic scalabilty for containers	Scaling across bare metal & VMs requires major reconfiguration	Dynamic scalability of VM/Container workload capacity

NFV/Edge Deployment Options and Trade-Offs (Security)

	Bare Metal (BM)	Hybrid (VM + BM)	CaaS (VM)
Component/VNF Isolation	Security only via physical HW topology isolation	Additional security for specific VMs possible	Native HW security for all components and VNFs
Security Attestation (e.g. TPM, image integrity, etc.)	Cannot provide extra security for specific components/VNFs	Can provide extra security for VM based components/VNFs	Can provide extra security for any user-specified components/VNFs
Open Source Security	Relies purely on software security (base K8s security)	VM layer provides additional hardware security for VM based components/VNFs	VM layer provides additional hardware security for all components/VNFs