EOM (ECOMP Operations Manager)

Overview for ONAP Community

Habib Torab
Shrikant Acharya
Vijay Venkatesh Kumar

February 20, 2019
Topics

- Background
- What is EOM?
- Architecture
- Features highlights
- Edge Automation requirement coverage
- Delta compared to ONAP DCAE
The framework was initially designed and built for DCAE.
- It was expanded later and the same framework was used as the main “platform controller”.
- Initially 2 separate instances were used in AT&T: Root Node/ECOMP Controller & DCAE Controller.
- Root Node Controller was used to manage all platform applications with the exception of DCAE applications/mS.
- The architecture is centered around a top-level TOSCA-based orchestration using Cloudify.
- It leverages Cloudify plugins and supports deployment/management of platform workloads in different cloud environment.
- An AT&T contributed Helm plugin is used for helm-based deployments of core platform applications.
- This allows leveraging the helm charts created for platform applications in ONAP.
- Consul is another key subcomponent used for registration/discovery, health checks, and as a key/value store.
What is EOM?

- EOM: ECOMP Subsystem that deploys and manages the lifecycle of ECOMP and all software required to make it operational, including scaling and self-healing
- EOM merges the functionality of:
  - ECOMP-C developed by AT&T
  - DCAE-C developed by AT&T
  - DCAE-C from ONAP
  - ONAP OOM (TOSCA) & HELM Plugin
  - CCSDK (ONAP)
- Single code base
- Continuous process of insourcing/open-sourcing between ONAP and EOM

Motivation

- Three existing controllers, DCAE-C (ONAP), DCAE-C and ECOMP-C, shared several attributes:
  - Same root source code
  - Common platform components across multiple implementations
  - Similar functions: Onboard and manage microservice lifecycles
  - Maintaining two similar systems was inefficient in engineering & development effort, which had to be duplicated for both systems in many cases, and resource staffing
- Decision: Merge controllers
DBaaS

ECOMP Tenant Space
- MariaDB
- MySQL
- Cassandra
- MongoDB
- Elastic Search

A&AI Tenant Space
- Cassandra
- Zookeeper
- Music

DCP
- ORACLE

VMs
K8s
## EOM features – highlights

<table>
<thead>
<tr>
<th>Application Lifecycle Management</th>
<th>Efficient Operations</th>
<th>Resilience</th>
<th>Access Control</th>
<th>Security</th>
<th>DCAE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management of containerized &amp; non-containerized applications</td>
<td>Efficient installation of EOM Components</td>
<td>EOM Components Geo-Redundancy</td>
<td>AAF authentication</td>
<td>Secure communication via TLS using AAF certs</td>
<td>Onboarding/management of SDC (self-serve) microservices</td>
</tr>
<tr>
<td>Cluster Management, Bare metal K8s support</td>
<td>In-place upgrades of EOM components</td>
<td>EOM Components Local Redundancy</td>
<td>Cert management</td>
<td>Support multi-certs (Digicert, etc.)</td>
<td>Onboarding/management of non- SDC microservices</td>
</tr>
<tr>
<td>TOSCA &amp; Helm support</td>
<td>Blueprint context awareness</td>
<td>ECOMP Applications Geo-Redundancy</td>
<td>User role management</td>
<td>AAF namespaces for fine-grained role based authentication</td>
<td>CLAMP initiated microservices reconfiguration</td>
</tr>
<tr>
<td>Auto-recovery</td>
<td>Script for generation of blueprints for Kubernetes onboarding</td>
<td>DCAE microservices resilience</td>
<td>AAF role mapping to Kubernetes</td>
<td>Event Logging and Analytics</td>
<td>DTI initiated microservices reconfiguration</td>
</tr>
<tr>
<td>Multi-Site Management</td>
<td>Runtime configuration</td>
<td>Affinity/Anti-affinity</td>
<td>Application and microservices user roles via ECOMP Portal</td>
<td></td>
<td>Policy initiated microservice reconfiguration</td>
</tr>
<tr>
<td>Metrics management based on Prometheus/Grafana</td>
<td>Multiple plug-ins</td>
<td></td>
<td></td>
<td></td>
<td>DMaaP integration</td>
</tr>
<tr>
<td>Auto-Ticketing</td>
<td>DBaaS (MySQL, MariaDB, PostgreSQL, Cassandra, MongoDB)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Resilience

EOM supports a rich set of resilience capabilities for itself as well as onboarded applications/microservices:

**EOM components – Local resilience**

**EOM components – geo-resilience**

**DCAE resilience**

**EOM Applications resilience**
Resilience for containerized Components is achieved via pod replicas

Resilience for non-containerized EOM components is achieved by implementing redundant instances

- Cloudify 4.4, Consul, PostgreSQL, and the DBs (MariaDB, MySQL, Mongo, Elasticsearch and Cassandra) implement their own resilience architectures on their own clusters consisting of 2 or 3 nodes on VMs per site

Persistent storage is provided via Cinder volumes
- EOM is installed in two sites: in **active** mode in one site, **passive** in the other
- Global iDNS communicates with an end point at each site to determine which site is active
- Data in persistent storage at the passive site is continuously updated with data from the active site
- If the active EOM fails, the passive EOM becomes active and takes over operations until the first EOM recovers, when normal operation is resumed
ECOMP applications geo-resilience: active-passive

- **ECOMP Applications** (e.g., SO) are installed in two sites: In **active** mode in one site and **passive** in the other.
- An instance of **EOM** is present in each site: In **active** mode in one and **passive** in the other.
- The active EOM provides support for monitoring, healing and scaling the ECOMP Applications **at both sites**.
- Global iDNS communicates with an end point provided by each ECOMP Application to determine at which site the Application is active.
- Each ECOMP Application implements its own resilience architecture:
  - Local resilience is based on pod replicas.
  - Geo-resilience is achieved via HA Proxy/Global iDNS.
  - In the event of the active Application failing, the Application at the other site becomes active.
ECOMP Applications (e.g., SO) are installed in two sites: In active mode in one site and active in the other.

- An instance of EOM is present in each site: In active mode in one and passive in the other.
- The active EOM provides support for monitoring, healing and scaling the ECOMP Applications at both sites.
- Global iDNS communicates with an end point provided by each ECOMP Application for balancing the Application load between the active sites.
- In the event of the active EOM failing, the passive EOM becomes active and manages the ECOMP Applications at both sites until the first EOM recovers, when normal operation is resumed.
DCAE resilience (1 of 2)

Active Site

EOM Site 1
- EOM
- DCAE Central 1
  - PG-App
  - Docker Applications
  - DCAE microservices
  - DMaaP
- Regional DMaaP
- DCAE microservices
- Docker Applications
- DMaaP
- Regional DMaaP
- DCAE microservices
- Docker Applications
- DMaaP

Passive Site

EOM Site 2
- EOM
- DCAE Central 2
  - PG-App
  - Docker Applications
  - DCAE microservices
  - DMaaP
- Regional DMaaP
- DCAE microservices
- Docker Applications
- DMaaP
- Regional DMaaP
- DCAE microservices
- Docker Applications
- DMaaP

VMs K8s
DCAE resilience (2 of 2)

EOM Site 1

EOM Site 2

EOM

Active Site

Site Failed

DCAE Central 1

DCAE Central 2

PG-App

Docker Applications

CDAP Applications

HAProxy

DCAE microservices

DMaaS

Regional

DMaaS

DCAE microservices

Docker Applications

Docker Applications

Regional

DMaaS

DCAE microservices

Docker Applications

Docker Applications

HAProxy

DCAE microservices

VMs

K8s
Onboarding DCAE components via EOM

DCAE Platform components installed:
- Docker Cluster on DCAE Central and Regional sites
- PostgreSQL (Application)
- DMaaP on Central and Regional sites
- Kubernetes cluster on Central and Regional sites
- Ops Tools
<table>
<thead>
<tr>
<th>Category</th>
<th>Requirement Item</th>
<th>EOM Mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform (Day 0)</td>
<td>Day 0 Bootstrap process: Ability to create ONAP platform using a single script</td>
<td>EOM multi-site platform creation</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Ability to onboard management applications, deployed in cloud-regions, in ONAP-Central. Shall not have any expectations that all management applications are onboarded as a single bundle.</td>
<td>Allow new MS/applications/components to be onboarded independently</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Ability to compose multiple management applications to be part of one management bundle and defining the dependency graph of applications belonging to a bundle.</td>
<td>Supported through DCAE, SDC*, CLAMP</td>
</tr>
<tr>
<td>Instantiation</td>
<td>Ability to deploy management applications in selected cloud regions owned by ONAP operator</td>
<td>EOM WIP</td>
</tr>
<tr>
<td>Instantiation</td>
<td>Ability to deploy management applications in selected cloud regions not owned by ONAP operator, but has business relationship (Examples: Public Clouds or Edge Clouds owned by some other organization)</td>
<td>EOM PoC to support third party clouds</td>
</tr>
<tr>
<td>Run time</td>
<td>Ability to upgrade management application components without loss of functionality</td>
<td>Multi-site footprint &amp; in place upgrade</td>
</tr>
<tr>
<td>Run time</td>
<td>High availability of management applications in the cloud regions</td>
<td>Multi-site resilience (active-active, active-passive management applications)</td>
</tr>
<tr>
<td>Platform</td>
<td>Enable tiered approach to support the volume, scaling and geo-distribution of platform and management applications</td>
<td>EOM can be instantiated to support geographic distributed management</td>
</tr>
<tr>
<td>Platform</td>
<td>Multi-site support</td>
<td>Single instance of EOM can orchestrate multiple site and manage life cycle of onboarded management applications</td>
</tr>
<tr>
<td>Security</td>
<td>Namespace separation and resource management</td>
<td>EOM supported</td>
</tr>
</tbody>
</table>
Onboarding ECOMP applications

Execute Blueprints (Helm chart & values as input)

or

Application CI/CD

EOM

API Handler

Service Change Handler

Inventory (PG)

Deployment Handler

Cloudify

Policy Handler

Consul

Config Binding Service

Helm

Docker

CDAP

Kubernetes

Policy

cert

OpenStack

AIC/MSO

DTI

ECOMP Application Tier 2
Delta with ONAP DCAE

- EOM architecture is closely aligned to ONAP DCAE
  - Base platform components are already in ONAP
    - PolicyHandler, Deployment Handler, ConfigBindingService, InventoryAPI (available in R3)
    - Dashboard (Targeted R4)
  - DTI/handler – For dynamic reconfiguration of deployment component
  - Plugins/tools – To simplify monitoring of deployment components
  - Helm Chart support (Dublin)
  - Capability to Deploy DMaaS at edge
Monitoring EOM components & ECOMP applications

Monitoring of EOM Components and ECOMP Applications will be via a combination of several capabilities:

**Consul:**
1. Performs health check on EOM Components hosted in the K8s cluster as well as on VMs (e.g. Cloudify, PG) and sends alerts to DMaaP
2. Performs health check on ECOMP Applications hosted in their K8s cluster as well as on VMs (e.g. databases) and sends alerts to DMaaP

**Prometheus:**
1. Collects performance metrics from EOM Components hosted on their K8s cluster
2. Collects performance metrics from the K8s cluster hosting the ECOMP Applications
3. Collects health check information from Consul
4. Transmits the metrics collected by itself and the Consul health check data to Grafana

**Grafana:**
1. Produces visualizations (dashboards etc.) and alerts based on the data obtained from Prometheus and Consul

**Kubernetes**
1. Healthchecks the containers
2. Kube2PyConsul utility sends the health check status to Consul
Summary

- EOM meets critical Tier 1 service provider platform requirements:
  - Highly Resilient
  - High Capacity/Transaction volumes
  - Highly Scalable/geographically distributed (microservices, centers, ...)
  - Highly Flexible (wide range of databases, microservices, protocols, ...)
  - Fast/agile onboarding of microservices

- Addresses Edge Automation group objectives:
  - Controller alignment
  - Management application requirements

- ONAP adoption of EOM involves minimal efforts (DCAE+)
Questions?
## EOM and Edge Automation Requirements

<table>
<thead>
<tr>
<th>Category</th>
<th>Requirement Item</th>
<th>EOM Mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Platform (Day 0)</strong></td>
<td>Day 0 Bootstrap process: Ability to create ONAP platform using a single script</td>
<td></td>
</tr>
<tr>
<td>Onboarding</td>
<td>Ability to onboard management applications, that are to be deployed in cloud-regions, in ONAP-Central. Shall not have any expectations that all management applications are onboarded as a single bundle.</td>
<td>Allow new MS/applications/components to be onboarded independently</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Ability to compose multiple management applications to be part of one management bundle and defining the dependency graph of applications belonging to a bundle</td>
<td>Allow Service assurance flow composition and deployment of individual or group of component</td>
</tr>
<tr>
<td>Instantiation</td>
<td>Ability to deploy management applications in selected cloud regions that are owned by ONAP operator</td>
<td>Allow Service assurance flow composition and deployment of individual or group of component</td>
</tr>
<tr>
<td>Instantiation</td>
<td>Ability to deploy management applications that are ephemeral (example: Analytics applications)</td>
<td>Allow Service assurance flow composition and deployment of individual or group of component</td>
</tr>
<tr>
<td>Instantiation</td>
<td>Ability to deploy management applications in selected cloud regions that are not owned by ONAP operator, but has business relationship (Examples: Public Clouds or Edge Clouds owned by some other organization)</td>
<td></td>
</tr>
<tr>
<td>Instantiation</td>
<td>Support for deploying management applications independent of each other when there are no dependencies (no expectation that all management applications are brought up together).</td>
<td>Allow Service assurance flow composition and deployment of individual or group of component</td>
</tr>
<tr>
<td>Instantiation</td>
<td>Ability to deploy few management applications based on VNF instantiations and bring down when VNF is terminated</td>
<td>Dynamic deployment of MS based on xNF instantiation</td>
</tr>
<tr>
<td>Instantiation</td>
<td>Ability to apply configuration (Day 0 configuration) of management applications at the time of deployment</td>
<td></td>
</tr>
</tbody>
</table>
## EOM and Edge Automation Requirements

<table>
<thead>
<tr>
<th>Category</th>
<th>Requirement Item</th>
<th>EOM Mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instantiation</td>
<td>Support for various Day0 configuration profiles (e.g., different profiles for different cloud regions with differing capabilities)</td>
<td></td>
</tr>
<tr>
<td>Instantiation</td>
<td>Support for placement of management applications based on platform features (example: GPU, FPGA etc...)</td>
<td></td>
</tr>
<tr>
<td>Instantiation</td>
<td>Support for consistent Day0 configuration mechanisms - should be the same path as Day 2.</td>
<td></td>
</tr>
<tr>
<td>Run time</td>
<td>Support for Day 2 configuration of single or multiple instances of management applications in various cloud regions</td>
<td></td>
</tr>
<tr>
<td>Run time</td>
<td>Support for management applications depending on other management applications - Support for configuration (Day2 configuration) of provider services when the consuming service is being instantiated and removal of the configuration on provider services when consuming service is terminated (Example: When analytics applications are brought up, analytics/collection framework need to be updated with additional configuration such as DB table, Kafka topic etc...)</td>
<td>Dynamic topics(MR) and feeds(DR) provisioning and role assignment for MS</td>
</tr>
<tr>
<td>Run time</td>
<td>Support for Day 2 configuration (add/delete) of appropriate management applications upon VNF instantiation/termination (Example: configuration of analytics &amp; collection services when VNFs are brought up and removing the added configuration upon VNF termination)</td>
<td>Dynamic reconfiguration of MS based on xNF instantiations</td>
</tr>
<tr>
<td>Run time</td>
<td>Support for consistent Day 2 configurations across management components - should be the same path as Day 0.</td>
<td></td>
</tr>
<tr>
<td>Networking</td>
<td>Secure connectivity between central ONAP and management applications in cloud regions</td>
<td></td>
</tr>
<tr>
<td>Networking</td>
<td>Support for various connectivity protocols (Kafka, HTTP 1.1, 2.0, GRPC, Netconf etc...) between ONAP-Central and management components in cloud regions</td>
<td></td>
</tr>
<tr>
<td>Run time</td>
<td>Monitoring and visualization of management applications of cloud-regions along with ONAP components at the ONAP-Central</td>
<td>Complete view of MS and relation maintained at single/multisite K8S scenarios Health check of all deployment component to be available for CLAMP/external system</td>
</tr>
<tr>
<td>Run time</td>
<td>Scale-out of management application components at the cloud-regions &amp; traffic (transaction) distribution</td>
<td></td>
</tr>
</tbody>
</table>
# EOM and Edge Automation Requirements

<table>
<thead>
<tr>
<th>Category</th>
<th>Requirement Item</th>
<th>EOM Mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run time</td>
<td>Ability to upgrade management application components without loss of functionality</td>
<td>Multi-site footprint + in place upgrade capability available</td>
</tr>
<tr>
<td>Run time</td>
<td>High availability of management applications in the cloud regions</td>
<td>Multi-site resiliency (active-active, active-passive management applications)</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>Support for ONAP-compliant third party management applications that provide similar functionality as ONAP management applications. Some of the key aspects of ONAP-compliance include but are not limited to the following - API compatibility, Cloud Native Packaging in ONAP Helm chart format etc.</td>
<td></td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>Support management applications as containers</td>
<td></td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>Support management applications as VMs</td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td>Security and privacy aspects of management applications (To be expanded)</td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td>Access control management</td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td>Namespace separation and resource management</td>
<td></td>
</tr>
<tr>
<td>Instantiation</td>
<td>Support for MS deployment not binded to any VNF/service; these are application which are service agnostic can be managed by dynamic configuration rule to support different use cases</td>
<td></td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>Backward compatibility with existing application based on TOSCA</td>
<td></td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>Non-containerized management application support</td>
<td></td>
</tr>
<tr>
<td>Run time</td>
<td>Service registration, Alert monitoring and Ticket creation</td>
<td></td>
</tr>
<tr>
<td>Platform</td>
<td>Enable tiered approach to support the volume, scaling and geo-distribution of platform and management applications</td>
<td></td>
</tr>
<tr>
<td>Platform</td>
<td>CI/CD integration</td>
<td></td>
</tr>
<tr>
<td>Platform</td>
<td>Backup/Restore capabilities</td>
<td></td>
</tr>
</tbody>
</table>
Microservice Onboarding without ASDC
Microservice Onboarding with ASDC (self-service)
Microservice Deployment (via Dashboard)

EOM

Service Change Handler

Inventory (PG)

Deployment Handler

Cloudify

Consul

Config Binding Service

Helm

Docker

CDAP

Kubernetes

Policy

cert

OpenStack

OpenStack

AIC/MSO

DTI

Blueprints

K8s

Docker

Operations

Dashboard

ASDC

Blueprint

DMaP

Pick up Blueprint

Retrieve MS YAML files

Onboarding Developer

TOSCA Lab

JSON Component Spec

YAML Files

ASDC Catalog

Designer

ASDC Design Studio

Policy Handler

Operations

28

© 2017 AT&T Intellectual Property. All rights reserved. AT&T and the AT&T logo are trademarks of AT&T Intellectual Property.
Reconfiguration via DTI

EOM

DTI

Global DMaaP

A&AI

Inventory (PG)

Receipts

Service Change Handler

Blueprints

Deployment Handler

Cloudify

Consul

Config Binding Service

Helm

Docker

CDAP

Kubernetes

Policy

cert

OpenStack

OpenStack

AIC/MSO

Database

K8s

Docker

CDAP

Kubernetes

Policy

cert

OpenStack

OpenStack

AIC/MSO

Database

K8s

Docker

CDAP

Kubernetes

Policy

cert

OpenStack

OpenStack

AIC/MSO

Database

K8s

Docker

CDAP

Kubernetes

Policy
Policy Flow part 1 – Blueprint (with Policy ID) to Inventory