



UNICORN

*A Novel Framework for Multi-cloud Services
Development, Orchestration and Continuous
Management*

Manos Papoutsakis

paputsak@ics.forth.gr



<http://unicorn-project.eu>



[@unicorn_H2020](https://twitter.com/@unicorn_H2020)



European
Commission

Horizon 2020
European Union funding
for Research & Innovation



European
Commission

Horizon 2020
European Union funding
for Research & Innovation

Architecture and Technology Stack Overview



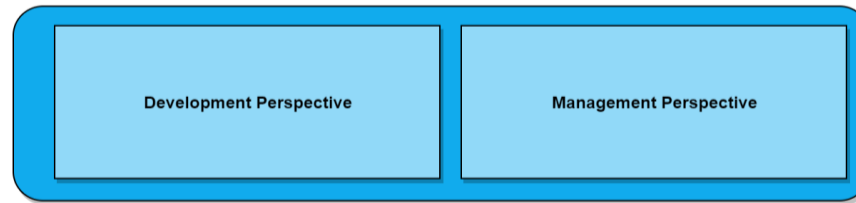
University
of Cyprus



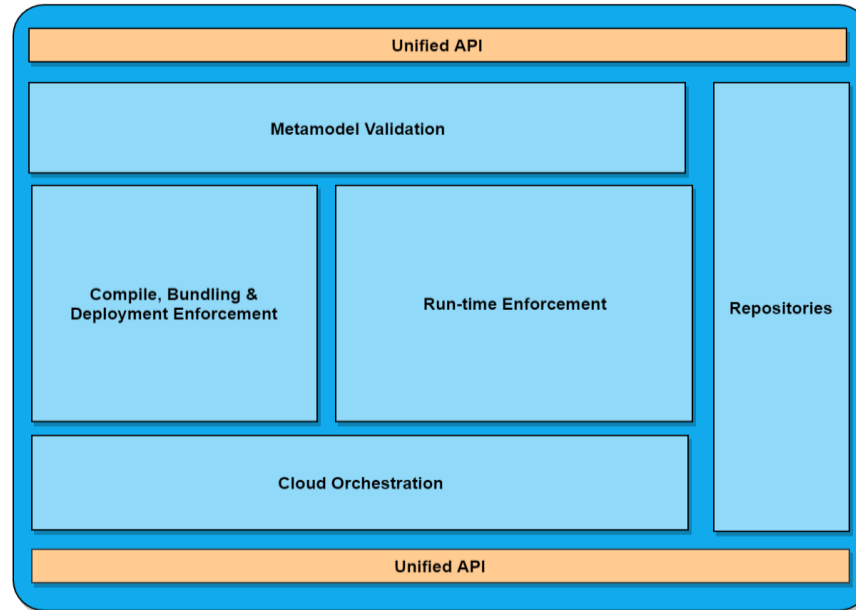
Steinbeis



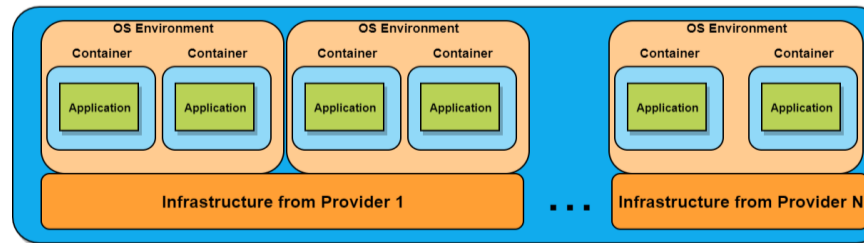
Unicorn Dashboard



Unicorn Platform



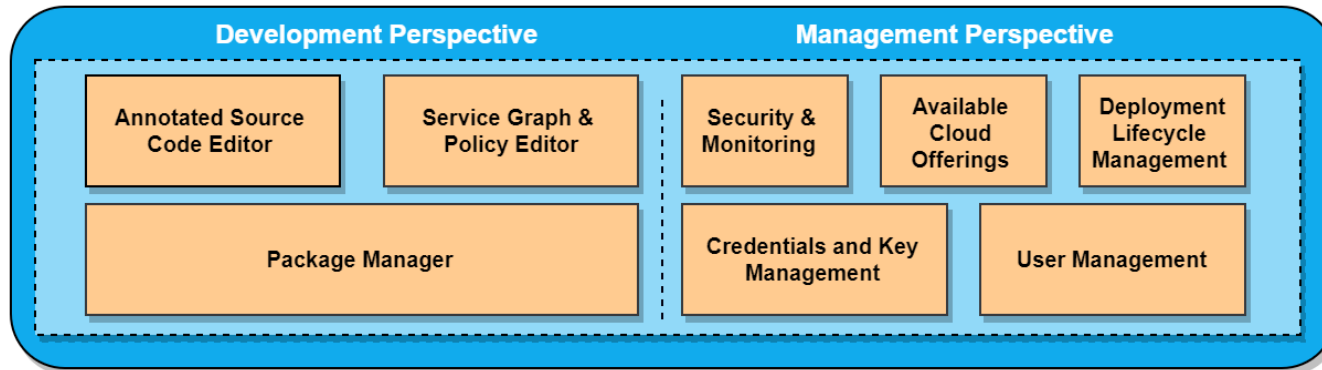
Multi-Cloud Execution Environment



Unicorn Dashboard

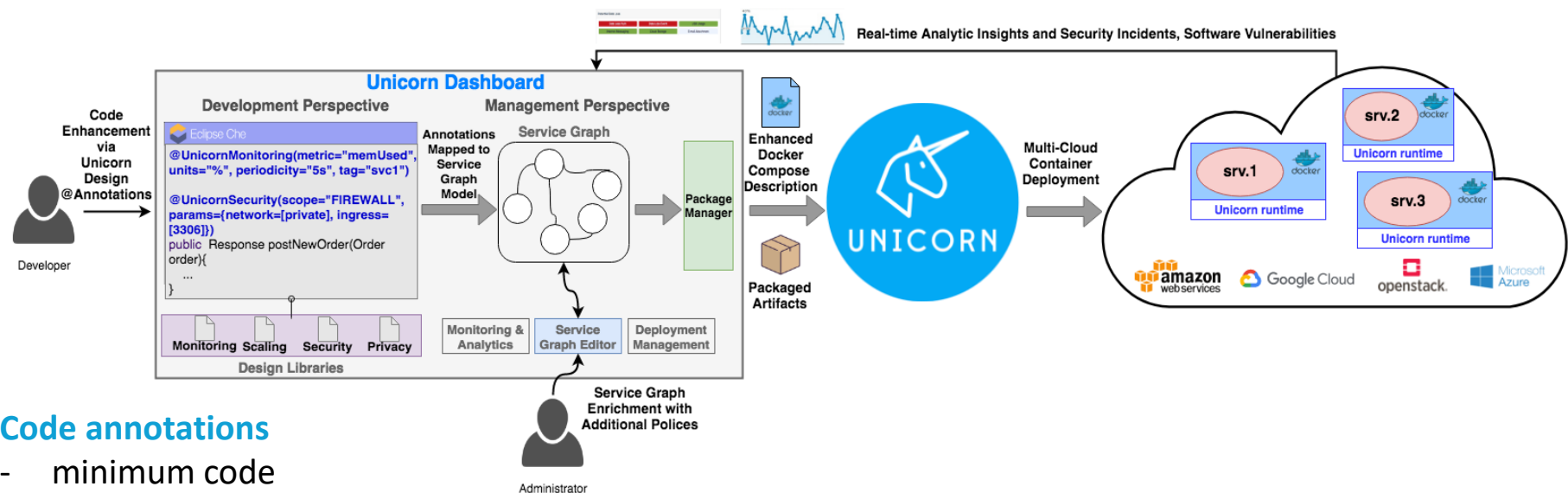
- Hosts the Unicorn **design libraries** for monitoring, elastic scaling, security enforcement and vulnerability assessment
- Provides the **packaging tools** for successful application deployment
- Provides **real-time incident notification** and **cost explorer**

Unicorn Dashboard



Unicorn Dashboard

One collaborative and unified environment to develop apps, share workspaces, ship coded artefacts to the cloud, and manage the entire deployment lifespan



Code annotations

- minimum code instruction
- hide operation complexity

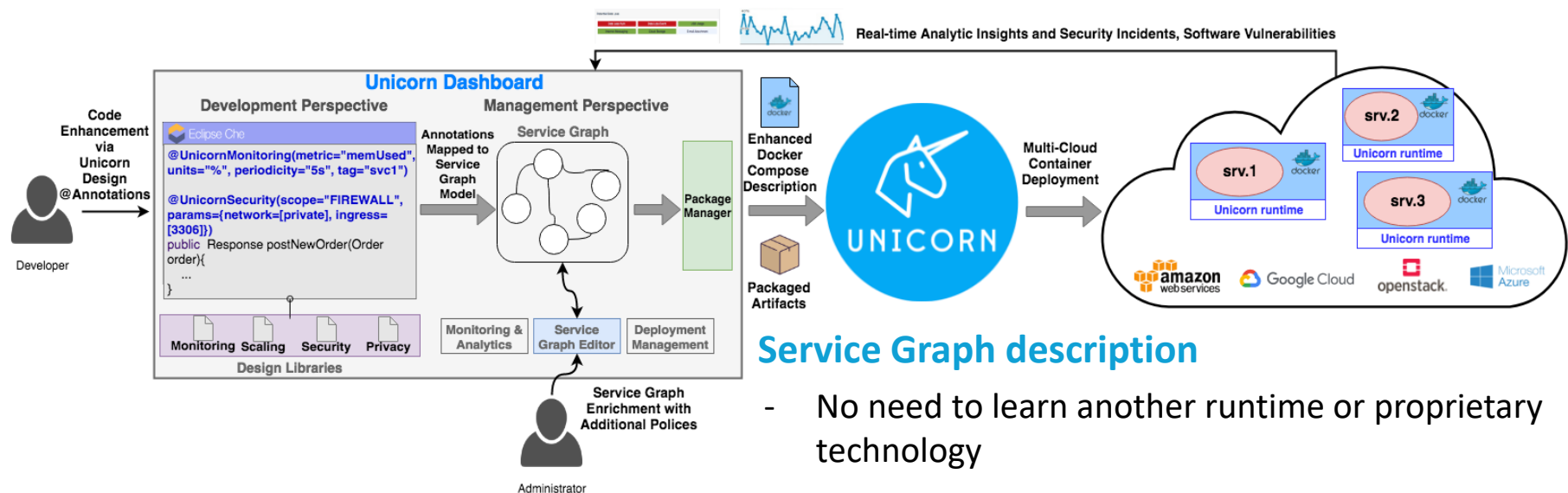
policy and
constraint
definition

Service graph enrichment

- alter or define new policies without coding

Unicorn Dashboard

One collaborative and unified environment to develop apps, share workspaces, ship coded artefacts to the cloud, and manage the entire deployment lifespan

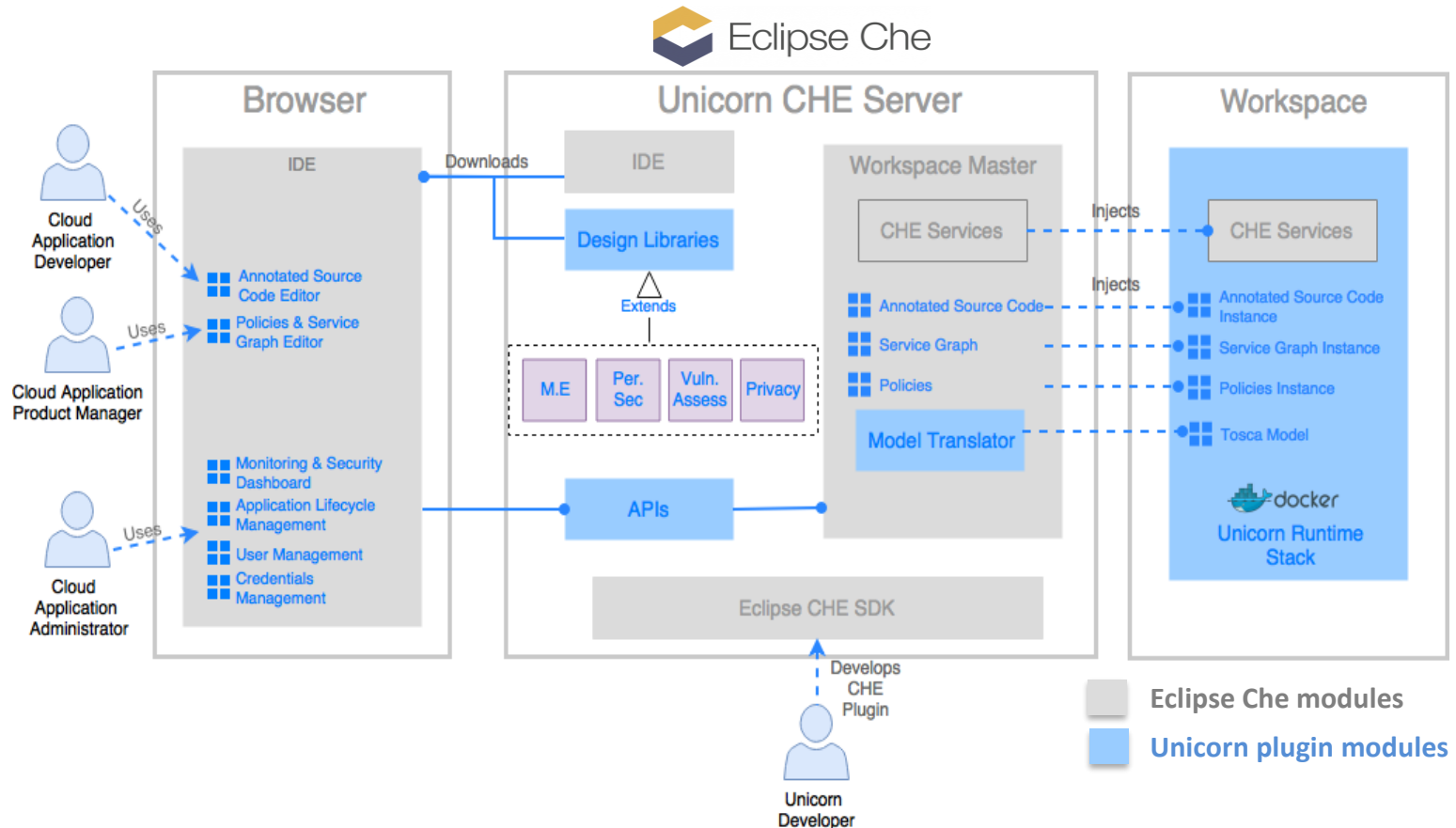


Service Graph description

- No need to learn another runtime or proprietary technology
- Enhanced **Docker Compose** description
- Description can still be used in any other Docker runtime but Unicorn policies will be ignored

Unicorn Cloud IDE Plugin

Developed for popular and open-source Eclipse Che ecosystem to support online and collaborative software development



Unicorn Platform

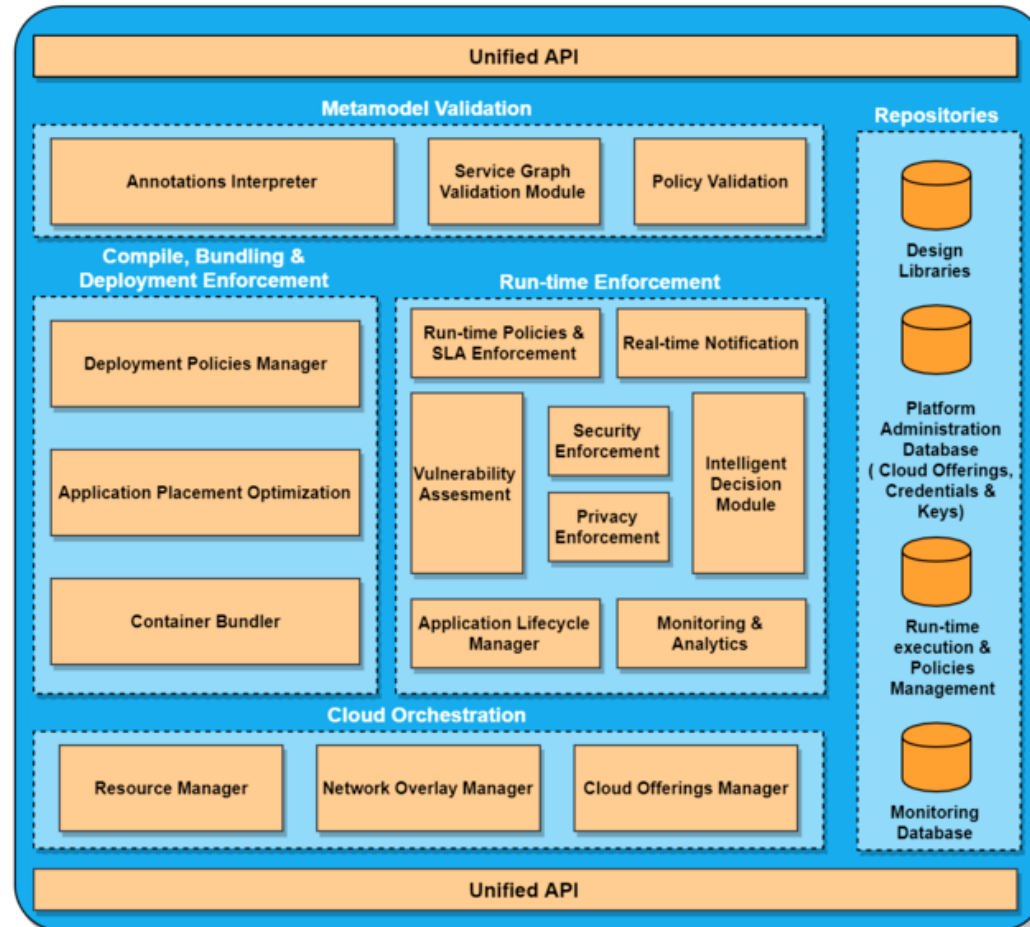
Link between Dashboard and Multi-Cloud Execution Environment.
Where the Unicorn business logic is applied.

Service graph validation

Detect antagonizing policy restrictions and circular dependencies

Runtime policy and constrain enforcement

Monitoring, auto-scaling, security and vulnerability assessment

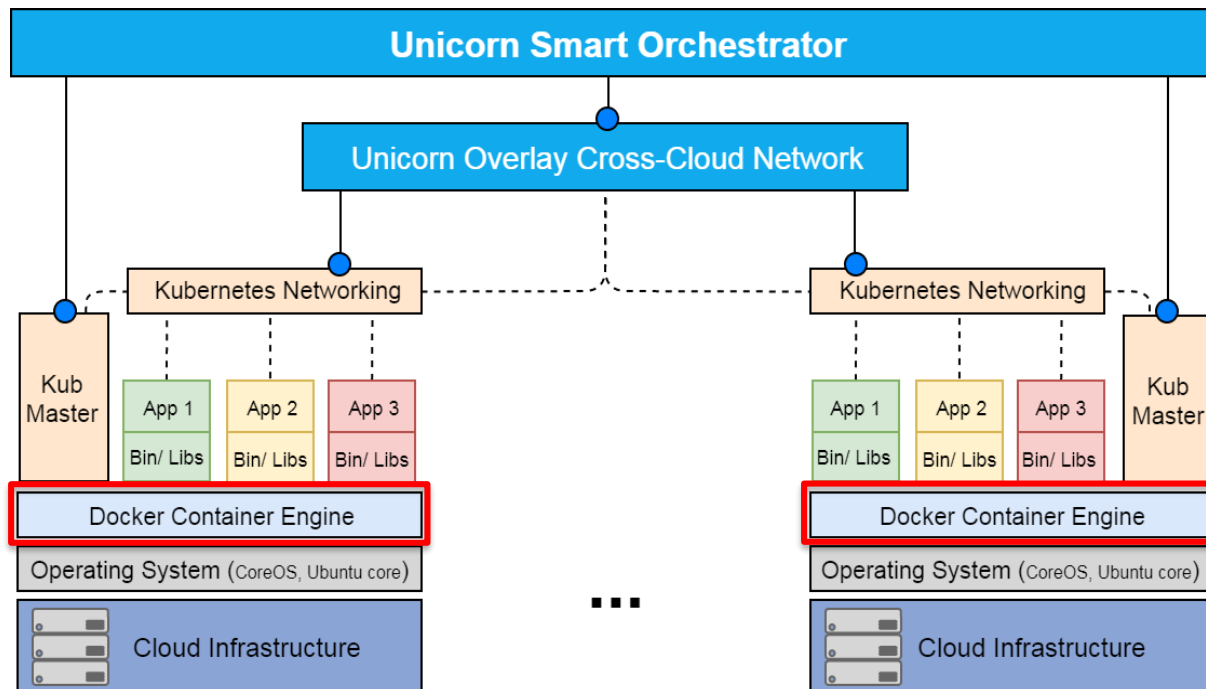


Code annotations
Interpretation and binding

Smart and interoperable orchestration
underlying programmable infrastructure, network fabric and multi-cloud containerized execution environment

Unicorn Technology Stack

All Unicorn apps are packaged and enabled by **Docker Runtime Engine** to create and isolate the containerized execution environment.



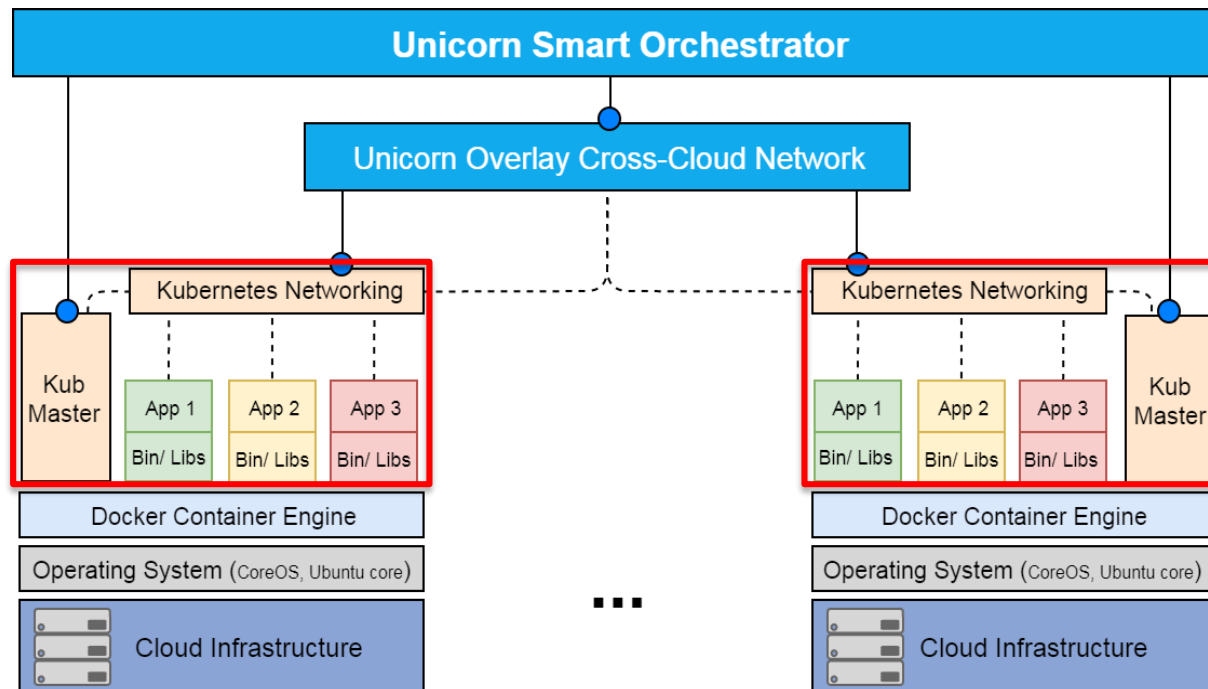
Docker Runtime Engine is sufficient for small deployments.

But...

Limited to a single host.

Unicorn Technology Stack

Kubernetes to support the orchestration of large-scale distributed containerized deployments spanning across multiple hosts.

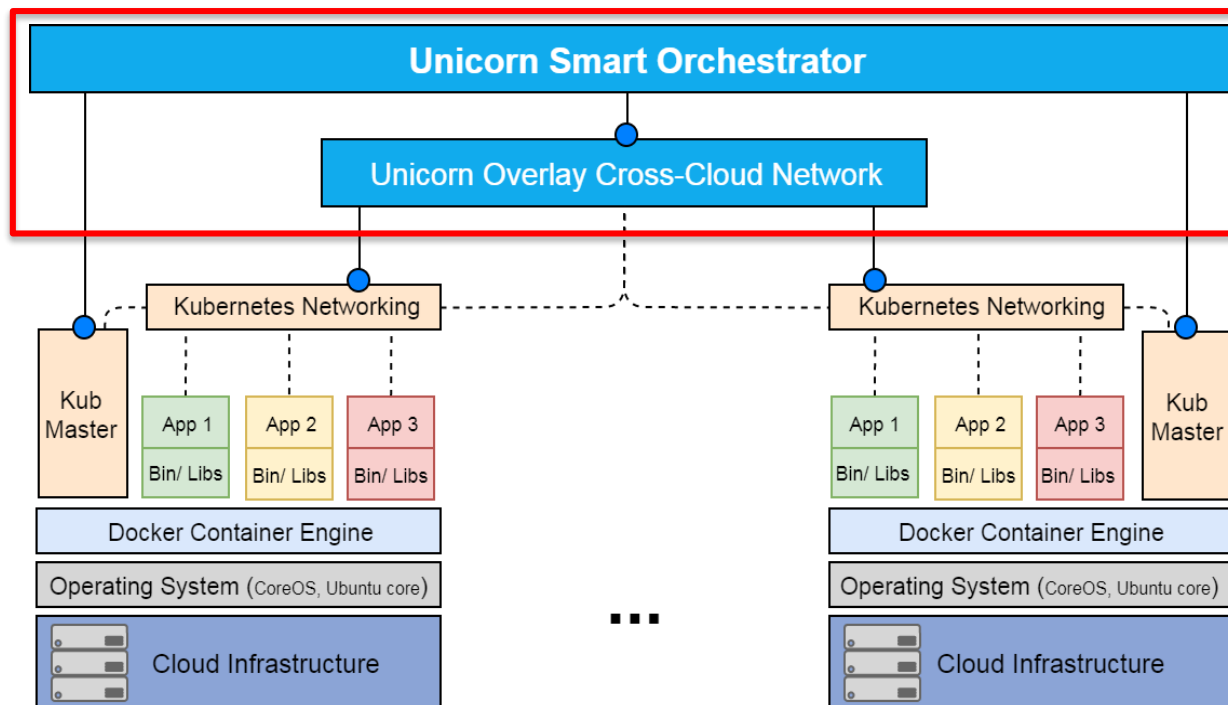


Kubernetes Limitations

- (De-)provisioning infrastructure resources.
- Auto-scaling.
- Cross-cloud deployments.

Unicorn Technology Stack

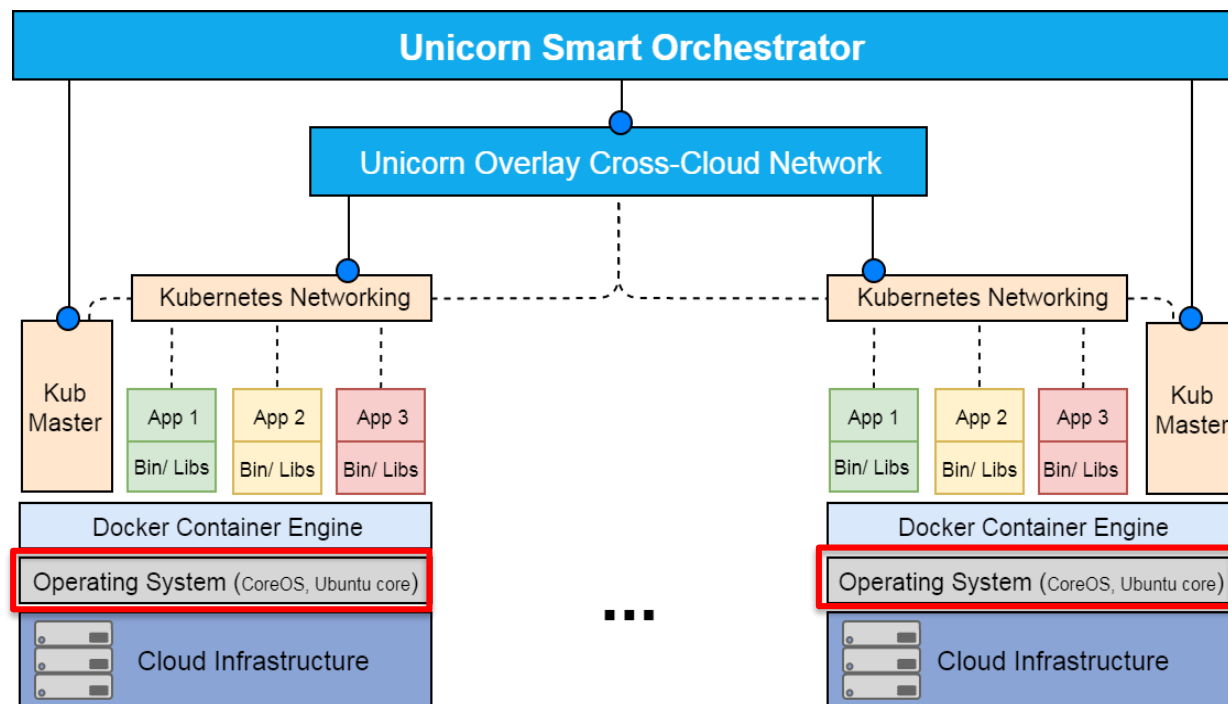
Unicorn Smart Orchestrator extends open-source Arcadia framework to enable Kubernetes across multiple cloud sites.



- Cloud adaptors to probe and program underlying infrastructure.
- Taps into auto-scaling offered by cloud offerings to estimate and assess app elasticity behavior and scaling effects.
- Cross-cloud network overlay management to reliably handle SDN accessibility.

Unicorn Technology Stack

Underlying kernel for the containerized environment is **CoreOS** which enables fast boot times and secure-out-of-the Docker runtime.



Unicorn “side-car” services

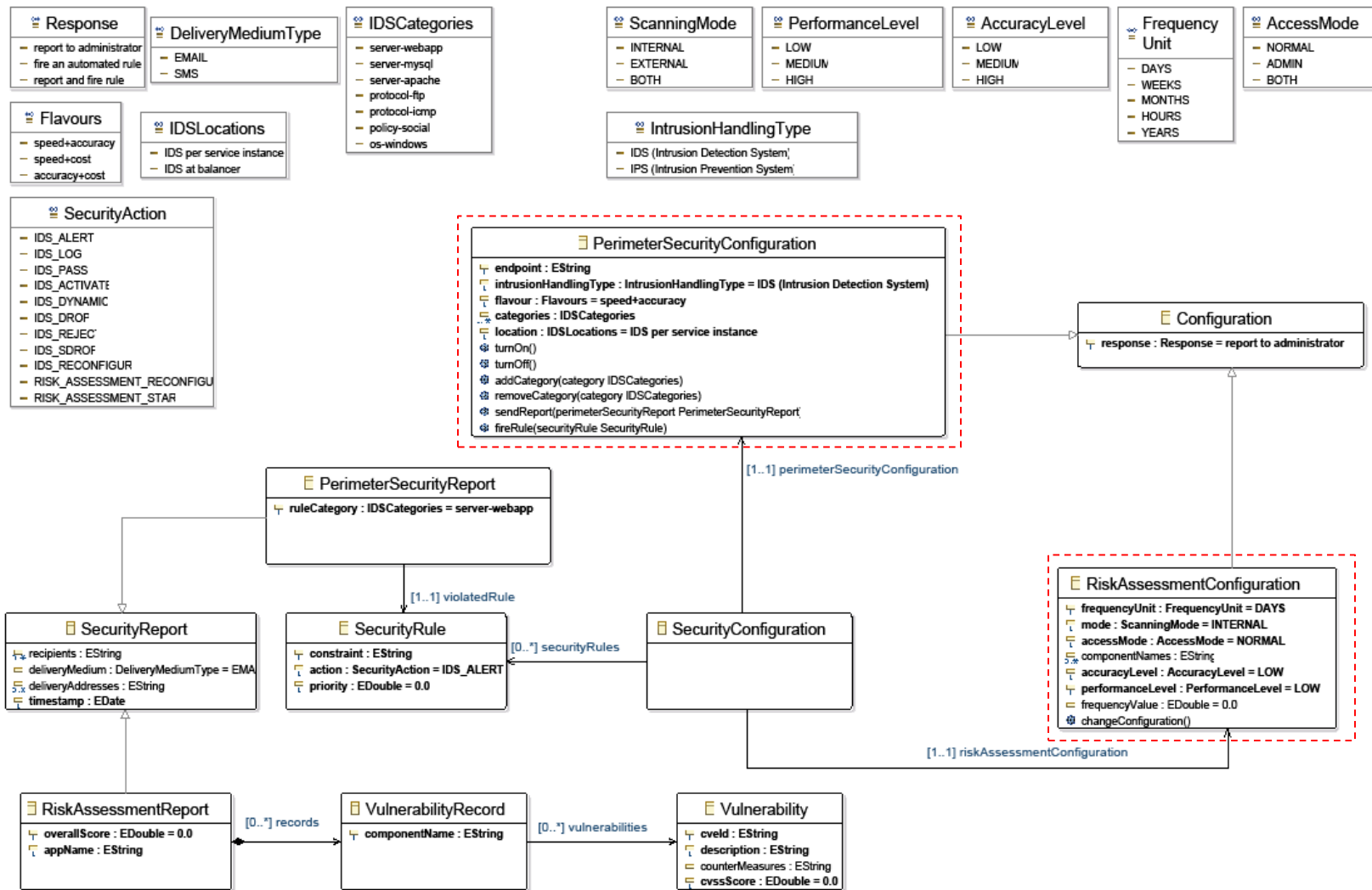
- Orchestrator service for HA host management.
- Low-cost and self-adaptive monitoring to reduce network traffic propagation.
- Security service to filter network traffic and apply privacy preserving ruling.

“Unicorn: A Novel Framework for Model-driven Security for Multi-cloud Services”

Goals of this research

- Drive the selection, tuning, and reconfiguration of security solutions to high-level user requirements
- Declarative specification of security requirements, configuration, reporting, event handling
 - Perimeter security
 - Continuous risk assessment
- Platform to translate requirements into appropriately configured cloud security solutions & deployments
- Automated DoS defense mechanism, elasticity driven
- Evaluation using GCP cross-region deployment

Security meta-model UML class



Modeled application



HTTP requests

SecurityConfiguration.xmi

- platform:/resource/vulnerability/model/SecurityConfiguration.xmi
 - Security Model WebAppSecurityConfiguration
 - Perimeter Security Configuration WebAppPerimeterSecConfig
 - Risk Assessment Configuration WebAppRiskAssessConfig
- platform:/resource/vulnerability/model/vulnerability.ecore

Ecore Problems

Property	Value
Categories	server-webapp, server-apache
Endpoint	
Flavour	speed+accuracy
Id	WebAppPerimeterSecConfig
Intrusion Handling Type	IPS (Intrusion Prevention System)
Location	IDS at balancer
Response	report and fire rule

Perimeter security configuration

SecurityConfiguration.xmi

- platform:/resource/vulnerability/model/SecurityConfiguration.xmi
 - Security Model WebAppSecurityConfiguration
 - Perimeter Security Configuration WebAppPerimeterSecConfig
 - Risk Assessment Configuration WebAppRiskAssessConfig
- platform:/resource/vulnerability/model/vulnerability.ecore

Ecore Problems

Property	Value
Access Mode	NORMAL
Accuracy Level	HIGH
Component Names	
Frequency Unit	WEEKS
Frequency Value	1.0
Id	WebAppRiskAssessConfig
Mode	INTERNAL
Performance Level	HIGH
Response	report to administrator

Risk assessment configuration

Apache2 HTTP server configured for CGI



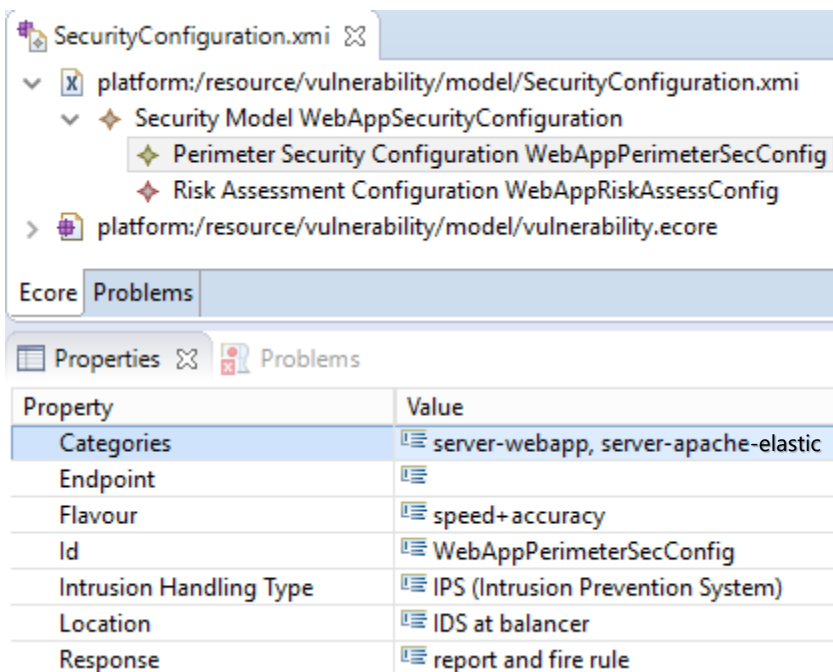
CGI Script

Application topology model (TOSCA, CAMEL, etc.)

CGI script performs computation for each HTTP request

Worker

Application security-configuration models



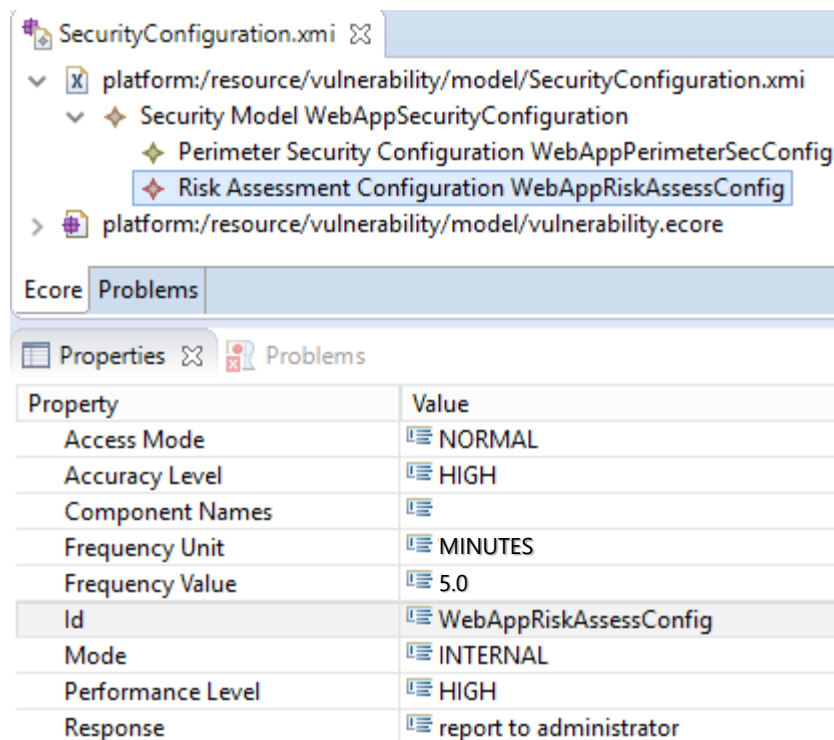
SecurityConfiguration.xmi

- platform:/resource/vulnerability/model/SecurityConfiguration.xmi
 - Security Model WebAppSecurityConfiguration
 - Perimeter Security Configuration WebAppPerimeterSecConfig**
 - Risk Assessment Configuration WebAppRiskAssessConfig
 - platform:/resource/vulnerability/model/vulnerability.ecore

Ecore Problems

Properties Problems

Property	Value
Categories	server-webapp, server-apache-elastic
Endpoint	
Flavour	speed+accuracy
Id	WebAppPerimeterSecConfig
Intrusion Handling Type	IPS (Intrusion Prevention System)
Location	IDS at balancer
Response	report and fire rule



SecurityConfiguration.xmi

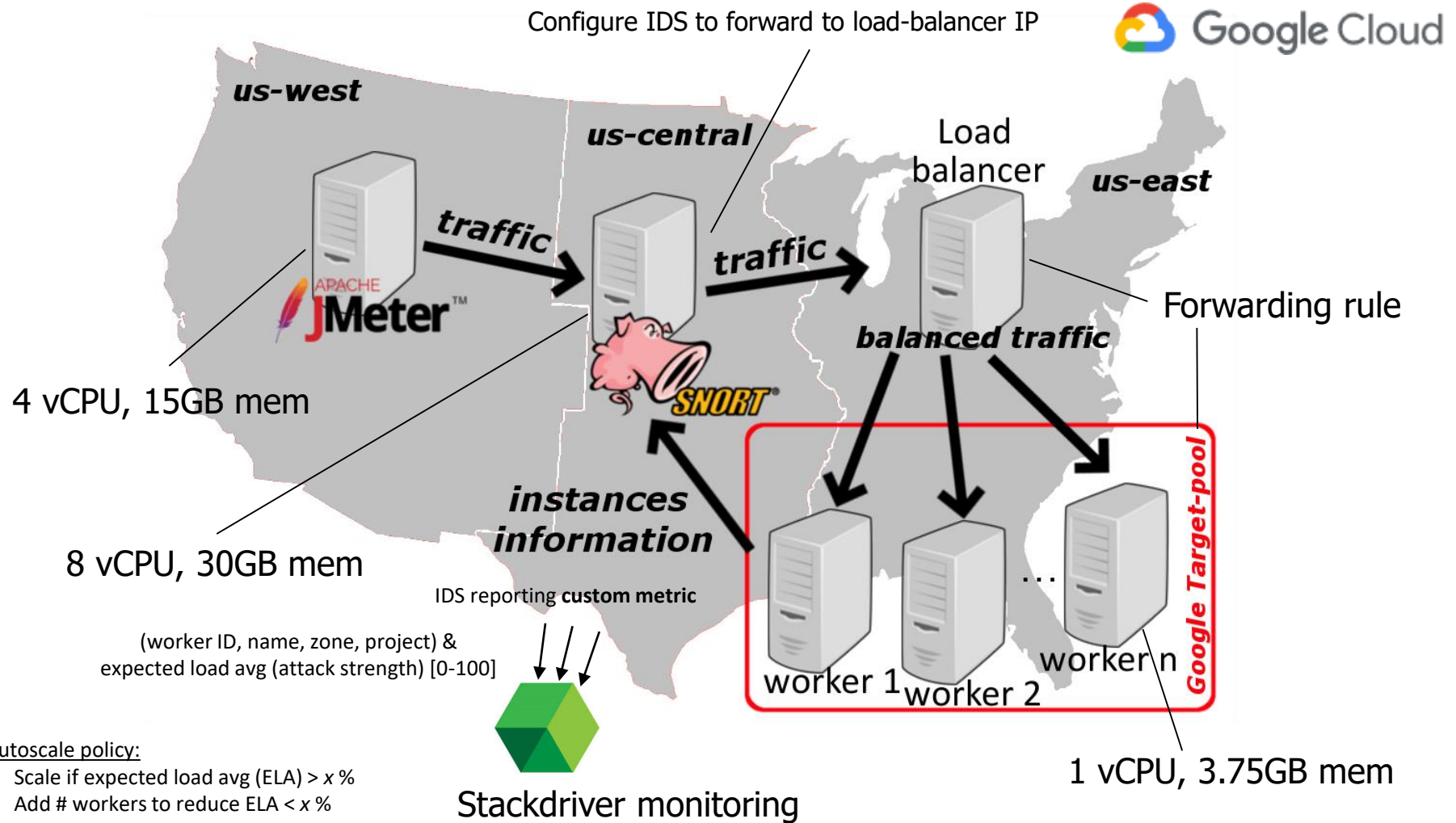
- platform:/resource/vulnerability/model/SecurityConfiguration.xmi
 - Security Model WebAppSecurityConfiguration
 - Perimeter Security Configuration WebAppPerimeterSecConfig
 - Risk Assessment Configuration WebAppRiskAssessConfig**
 - platform:/resource/vulnerability/model/vulnerability.ecore

Ecore Problems

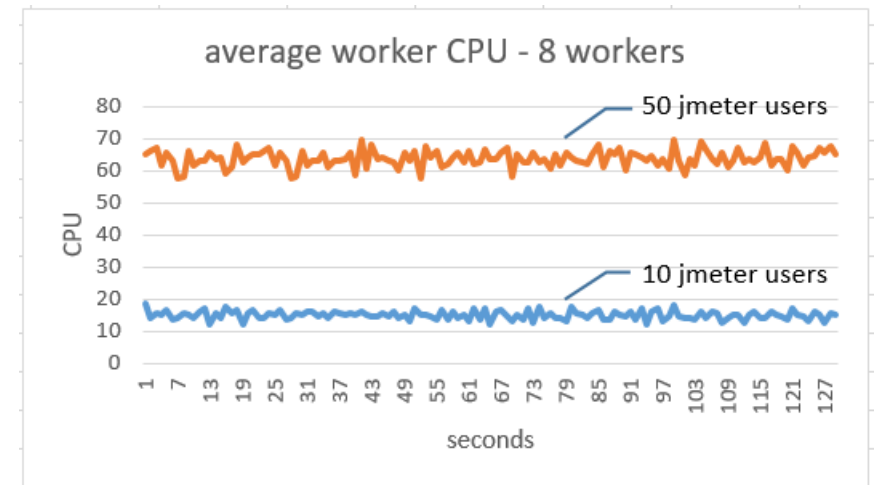
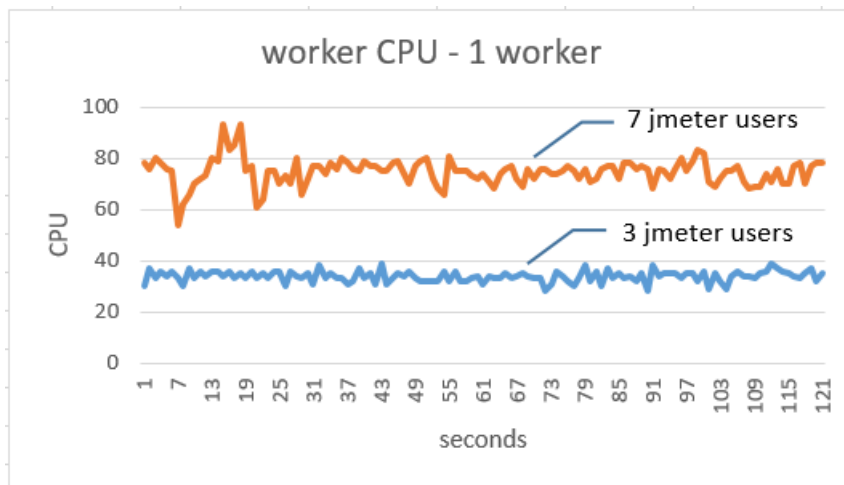
Properties Problems

Property	Value
Access Mode	NORMAL
Accuracy Level	HIGH
Component Names	
Frequency Unit	MINUTES
Frequency Value	5.0
Id	WebAppRiskAssessConfig
Mode	INTERNAL
Performance Level	HIGH
Response	report to administrator

Cross-region deployment



Average CPU utilization of application VMs (workers) under increasing load



- Degree of elasticity driven by prediction of load (CPU) placed by traffic
- Important to be able to predict imminent DoS attack and its strength

Thank you!

References

1. Manos Papoutsakis, Kyriakos Kritikos, Kostas Magoutis, and Sotiris Ioannidis.
Towards Model-Driven Application Security across Clouds.
In Proceedings of the 5th Workshop on CrossCloud Infrastructures & Platforms (CrossCloud'18).
ACM, New York, NY, USA, Article 2, 6 pages.
2. Trihinas, D.; Tryfonos, A; Dikaiakos, M. D., and Pallis, G.
DevOps as a Service: Pushing the Boundaries of Microservice Adoption.
IEEE Internet Computing, May/June 2018