Standards Adoption Deep Dive Workshop report: Measured Service, Monitoring and Advanced Security.

www.cloudwatchhub.eu|info@cloudwatchhub.eu |@cloudwatchhub

This document provides a summary report of the first of three Standards Adoption Deep Dive workshop, held at Cloudscape 2016 on 7 March 2016, in Brussels, Belgium

CLOUDWATCH2 has received funding from the European Union's Horizon 2020 programme - DG CONNECT Software & Services, Cloud. Contract No. 644748

CloudWATCH Mission

CloudWATCH2 takes a pragmatic approach to market uptake and sustainable competitiveness for wider uptake and commercial exploitation. It provides a set of services to help European R&I initiatives capture the value proposition and business case as key to boosting the European economy.

CloudWATCH2 services include:

- A cloud market structure roadmap with transparent pricing to enable R&I projects to chart exploitation paths in ways they had not previously considered, or help them avoid approaches that would not have been successful.
- Mapping the EU cloud ecosystem of products, services and solutions emerging from EU R&I projects. Identifying software champions and best practices in mitigating risks associated with open source projects, and ultimately, enable faster time-to-value and commercialisation.
- Impact meetings for clustering and convergence on common themes and challenges. Re-use of technologies will also be of paramount importance.
- Promoting trusted & secure services through roadshows and deep dive training sessions. Giving R&I initiatives a route to users at major conferences or in local ICT clusters.
- A portfolio of standards for interoperability and security that can facilitate the realisation of an ecosystem of interoperable services for Europe.
- Cloud interoperability testing in an international developer-oriented and hands-on environment. Findings will be transferred into guidance documents and standards.
- Risk management and legal guides to the cloud for private and public organisations to lower barriers and ensure a trusted European cloud market.

Disclaimer

CloudWATCH2 (A European Cloud Observatory supporting cloud policies, standard profiles and services) is funded by the European Commission's Unit on Software and Services, Cloud Computing within DG Connect under Horizon 2020.

Document Information Summary

Document title:	Standards Adoption Deep Dive Workshop report
Main Author(s):	Michel Drescher (UOXF), David Wallom (UOXF)
Contributing author(s):	
Reviewer(s):	Nicholas Ferguson, Trust-IT
Target audiences:	CloudWATCH2 consortium, The Cloud Interoperability Plugfest project, standards development organisations
Keywords:	Standards Development Organisations, Standards Setting Organisations, Standards implementing community
Deliverable nature:	Report
Dissemination level: (Confidentiality)	Public
Contractual delivery date:	
Actual delivery date:	
Version:	
Reference to related publications	CloudWATCH D2.4, CloudWATCH D4.3

1 Workshop report

The first of three standards adoption deep dive workshops was co-located with Cloudscape 2016 on 7 March 2016 in Brussels, Belgium.

This workshop was dedicated to continuing the successful work established during the first CloudWATCH project, and more specifically the final workshop conducted in September 2015[1]. Recapitulating the results and outcomes of that workshop:

> *"While the methodologies were generally accepted as sound and applicable, as described in D2.4 and D4.3* [of the CloudWATCH project]*, participants felt that the NIST characteristics of cloud computing used in the gathering of information should be revised. While it is certainly agreeable that Privacy characteristics should not be subsumed under "Advanced Security" (which is a characteristic that was present in a draft version of NIST SP 800-145), the workshop participants made it abundantly clear that NIST SP 800-145[2], even in a draft form, defines characteristics of only cloud computing, but at the same time, many more IT service characteristics are applicable that are not specific to Cloud computing."*

This also affected the definition of the second of three strawman profiles that were discussed at that workshop. Consequently, the first standards adoption deep dive workshop focussed on the following topics:

- Measured Service
- Monitoring
- Advanced Security

while paying attention to the different aspects of standardising on technical topics such as APIs and Information Models, and those of standardising policy, processes and procedures.

1.1 Deep Dive on "Measured Service" / Accounting

The primary use cases for measured services are stemming, not surprisingly, from the demand side, and similarly concern end users and resellers, however the main drivers for resource consumption and billing is the structure of the cost of service for service providers.

On the provider's side, three main drivers shape the cost of service. That is not to say that other costs are negligible, but these are much more under the control of service providers through internal processes and provisioning than the following drivers:

- **Ingress** – Data (both actual data, as well as application data, command and response instructions between user and cloud service) transmitted from external endpoints to within the boundaries of the CSP's data centre, measured at the exchange point between connectivity provider and Cloud Service Provider.
  Ingress typically does not incur service charges for the provider.
- **Resting** – Again, data of various kinds may be at rest within the provider's infrastructure, stored when it is not used (i.e. "at rest").
  Data at rest incurs *some* costs, namely for the maintenance of the portion of the infrastructure involved in the storage of the data.

[1] http://www.cloudwatchhub.eu/towards-secure-and-trusted-cloud-services-europe
[2] http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

- **Egress** – is the inverse of ingress, i.e. of all kinds that is transmitted from the CSP's data centre to external endpoints.
  Egress frequently incurs high cost on the cloud service provider, which are passed on to the consumer.

This applies to all service models, be it IaaS, PaaS or SaaS. However, while Ingress and Egress costs are fairly transparent and straight-forward, cost of service in the Resting phase is mostly variable and untransparent across Cloud Service Providers regardless of the service model. This is detrimental to the needs of other stakeholders in terms of service description transparency and comparability – including service costs.

The SLAReady project has established a Common Reference Model[3] to (partially) address this issue.

1.2 Deep Diving "Monitoring"

Unanimously, workshop participants identified Service Availability as the predominant use case for (Cloud) service monitoring. However, the semantics of Service Availability is noticeably different between service consumers and service providers. While service providers scope Service Availability across the entire service infrastructure that is offered to consumers, workshop participants characterise service consumers as discriminating between the "working" resources, i.e. those that they currently consume, and those that are available to them for rapid elasticity. These figures frequently do not add up, particularly for large public cloud providers where the amount of resources for an average service consumer is dramatically smaller than the entire service infrastructure on offer. The consequences are hidden in Service Availability numbers where an outage of a small part of a provider's infrastructure may not cause a dent in its overall availability calculations, but all the same may cause havoc on a consumer's own service offerings, or service components. It is therefore important to harmonise not only on common metrics, but also on the respective semantics. Harmonised/standardised monitoring metrics, particularly those commonly used in SLAs, also underpin better comparison between providers.

A new approach to reliability metrics is to break it up into per-feature/capability monitoring, since a common value may hide the real-life availability histogram across features. Such a histogram provides consumers with richer information upon which they may choose the most suitable Cloud Service Providers.

The participants also discussed the issue of provider-sourced monitoring vs. external monitoring, whether consumer-controlled or trusted third party provided. While either of the three approaches have their individual benefits and drawbacks, external monitoring may improve provider transparency and comparability, particularly on the interface level.

1.3 "Advanced Security": A wide spectrum of aspects

Based on a remote presentation given by CSA-delegate Damir Savanovic, workshop participants quickly subscribed to the notion of Advanced Security as having to include continuous monitoring (with varying frequencies) incorporating technical testing (automated technical tests similar to SW engineering unit tests) and periodic checks of policy/process related security controls: While technical security is testable and hence automatable, policy-level security requires external certification.

In general, this model resonates with external testing discussed for Monitoring (see above), but is constrained due to consumer's privacy levels, which typically reduce API visibility and access. Nonetheless, when embarking this direction, consumers must aspire to cover mission-critical aspects of a cloud provider's security in favour over completeness of security checks.

[3] http://www.sla-ready.eu/common-reference-model

In general, workshop participants agreed on the notion of Cloud Security being still in its early stages (comparable to Cloud Computing in its childhood time 5 – 10 years ago) with terms only vaguely defined, and very evasive dynamics. While it is true that the Cloud Computing market is growing more complex, Cloud security not only follows suit, but also grows in complicatedness.