Cloud Computing (IV)
Contrail Federations and SLA

SPD Course
19-20/05/2011
Massimo Coppola

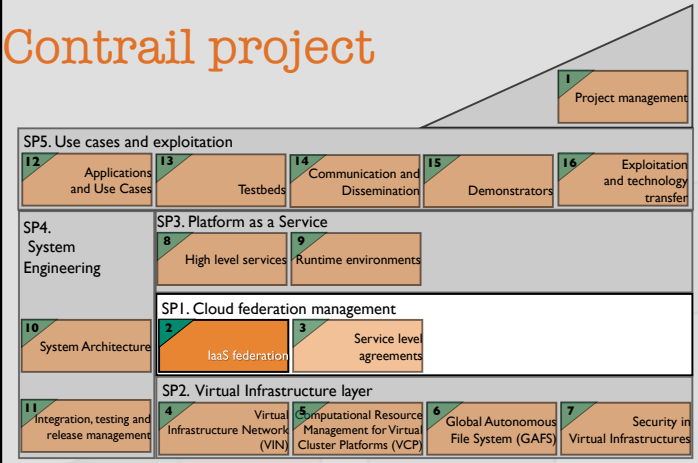
IaaS Federation
Objectives and Challenges & SLA management in Federations

Adapted from two presentations
by Massimo Coppola (CNR) and Lorenzo Blasi (HP)

contrail is co-funded by the EC 7th Framework Programme under Grant Agreement nr. 257438

http://contrail-project.eu

Contrail project



IaaS Federation

CONTRAIL Definition (Deliverable 2.1)

A CONTRAIL Federation integrates in a common platform multiple Clouds, of public and private kind.

User identities, data, and resources are interoperable within the federation, thanks to

- common supports for authentication and authorization
- common mechanisms for
  policy definition, *monitoring*, and *enforcing* of all aspects of QoS : SLA, QoP, etc.
- a common economic model

Federation Objectives

- Develop a Federation support that integrates and **actively coordinates SLA management provided by single Cloud providers**
- Do not disrupt provider's business model
  - Cloud administration **is not** Federation management
- Allow exploiting a Federation as a single Cloud
  - Cloudbursting to and from the Federation
- Federation Support must be scalable
  - Number of apps running, providers, resources, users

5

Service Level Agreements

- A **Service level agreement** is a part of a service contract where the level of service is formally defined (it's even on Wikipedia)
- *Formal* definition, part of a *contract*
  - A language to describe SLAs
  - Ways to measure the service level
  - Protocols to agree the SLA
  - Penalties when SLA is violated

6

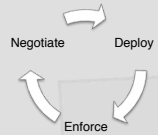
Service Level Agreements

- So far, especially in Clouds
  - performance, and sometimes availability
- Many more Service Quality aspects can be subject to SLAs, e.g.
  - Power consumption
  - Service Latency
  - Security and protection
  - Elasticity

7

SLA Objectives

- Support for the full life cycle of SLAs
  - Creation, instantiation and enactment of agreements at all levels of the Cloud services stack: infrastructure, IaaS federations, Platforms as a Service
  - Dynamic SLA negotiation, monitoring and enforcement



- Provide monitoring and accounting for Contrail services
  - Measure and record usage of resources per user and attribute that usage to the respective providers in the federation
  - Secure monitoring data distribution and aggregation
- Extend SLAs to QoP
  - Integrate QoP guarantee specification in SLAs, monitor and possibly enforce them

8

SLA Requirements summary

- Required QoS terms:
  - availability for VMs and data
  - network bandwidth
  - web response time, ...
- Required QoP terms:
  - *storage zeroing upon release*
  - encryption algorithms
  - access control policies
  - authentication and authorization requirements for services
  - logging policies
  - data segregation mechanisms
  - *data location*
  - recoverability
- Other requirements:
  - penalties for SLA violations
  - access control on map/reduce intermediate data
  - pub/sub for monitoring
  - keep history of monitored data
  - accounting and monitoring data isolation per user
  - support custom monitoring metrics and events
  - user to be notified of SLA violations
  - *automatic negotiation and automatic monitoring setup*
  - multi-turn negotiation and re-negotiation
  - negotiation timeout
  - access control on SLAs

9

Challenges / SLA lifecycle & QoP

- Offer SLAs at Federation level
  - SLA splitting/composition issues, split/migrate decisions and similar trade offs
  - SLA splitting in cloud-bursting scenarios
- Enforce QoS guarantees when lower layers don't offer any
  - guarantee support from WP4/WP5/WP5 still TBD
- Cost-based QoS enforcement
  - SLA offers the best possible quality at a predefined cost, monitoring is not (only) on QoS but also on cost (from accounting). Resource allocation is filtered at WP3 level and further provisioning requests are denied if their cost is not on budget
- Monitor offered QoP and enforce it
  - issues are: observability, security & privacy, Heisenberg / Uncertainty Principle…

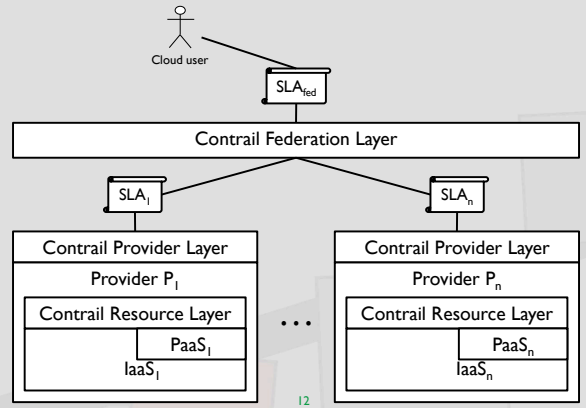
10

Challenges / Monitoring & Accounting

- Automatic monitoring setup from SLA definition
  - SLA specification language should be complete and precise enough (e.g. When, Which, Where, What, How [Sahai])
  - System should offer enough data from sensors and flexible aggregation / composition at SLA level
- Enable pay-per-use across different providers
  - Different providers may have different billing/charging models
  - The billing model of the provider must be configurable

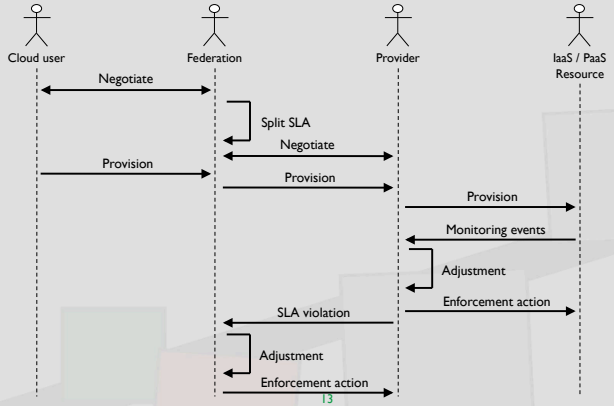
11

SLA Interaction Model



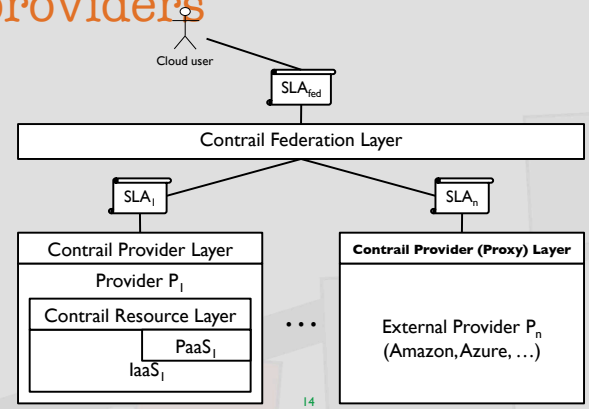
12

Interaction Model



13

Integrating external providers



14

State of the Art

- Several research fields are converging in SLAs
  - QoS for Networks, Computing and Storage
  - Quality of Protection (QoP) – Only recommendations, no real experiences
  - Monitoring
  - Accounting and Billing
  - SLA specification – WS-Agreement + extensions
  - SLA lifecycle – Extensions to WSAG for negotiation
  - SLA negotiation – Fully automated negotiation still not a reality
- SLAs are about:
  - Describing services
  - Expressing guarantees about services
- No support for SLA guarantees from commercial cloud providers
  - only for detailed service descriptions (Amazon)
  - or for specific prerequisites of guarantees (VMs in the same HW, Zones, etc)

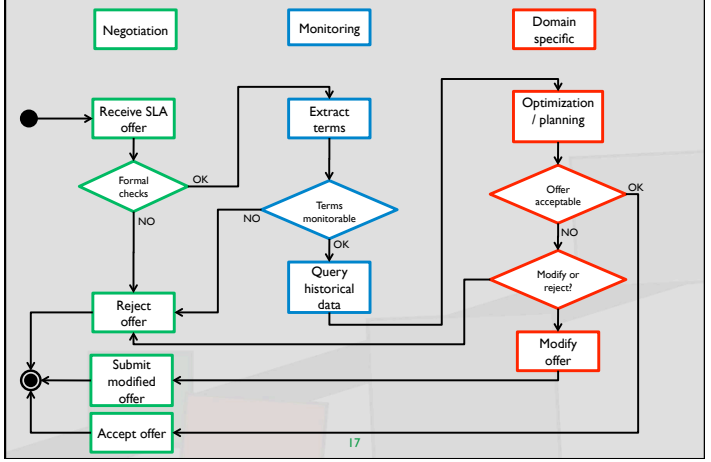
15

Our approach

- Reuse SLA@SOI framework as a starting point
  - Integration with Contrail internal interfaces and components
  - Integration with domain-specific reasoning/monitoring plugins
- Extend SLA@SOI with:
  - Federation support
  - QoP support
  - Integration of external providers
  - Reputation model for providers
  - Cost-based QoS enforcement

16

Negotiation from the provider's side as seen by SLA@SOI



Back to Cloud Federations

Federation Challenges

- Defining practical algorithms to tie together different providers
  - Define internal interfaces to allow federation level SLA management
  - Toward Network (inter & intra Cloud), Compute and Storage
  - The “Amazon way” won’t always solve the problem
- Define mechanisms for distributed monitoring of providers
- Define reputation of providers
- Contribute to the definition of SLA terms in order to simplify federation choices

Federation Challenges

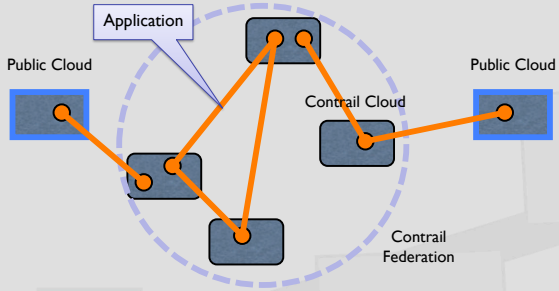
- Providing identity in federation vs. federated identity
  - We will need users, roles and some form of VO
  - Authorization and policies at the federation level
  - Leverage state of the art with respect to Security
- Providing distributed Federation access to ensure scalability → consistency / contention issues
- Identify technical solutions to provide federation support on “trusted & safe” resources

Federation Approach

- Allow applications to run across several Contrail providers by set up of
  1. SLA splitting
  2. Data, computation, network not from the same provider
  3. Multiple competing providers for all resources
- Develop algorithms to split user applications
- Multiple Aspects of QoS (SLA, QoP …) as terms and constraints
- Solution which integrates security and SLA
  → easy to reuse on top of other clouds
  → ease the adoption path

21

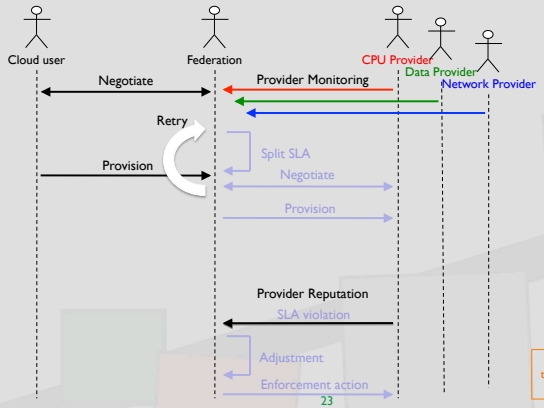
Federation Overview



- Exploiting multiple provider for a single application
- Application spans several resource, network and data providers

22

Interaction Model



See full description of the general approach in the SLA presentation

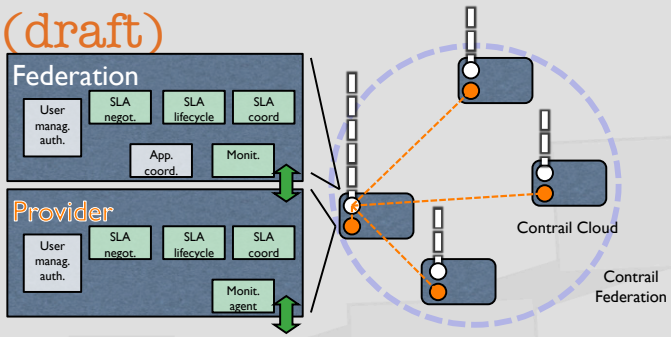
23

State of the Art

- Commercial platforms do not need to support federation of Clouds
  - Focus on availability and security (user managed networks)
  - SLA in terms of provided resources
  - Exploit strong assumptions on the hardware
- Open source solutions address different targets
  - Modularity and extendability (we can benefit)
  - Interoperability (we also target)
  - Support for heterogeneous federations is not a widespread aim
  - OpenNebula, Nimbus, OpenStack, Eucalyptus …

24

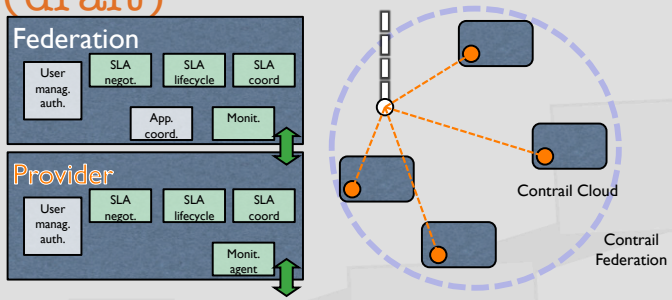
Federation Architecture (draft)



- SLA@SOI management of SLA applied to federation support
- SLA splitting + coordination of the application parts

25

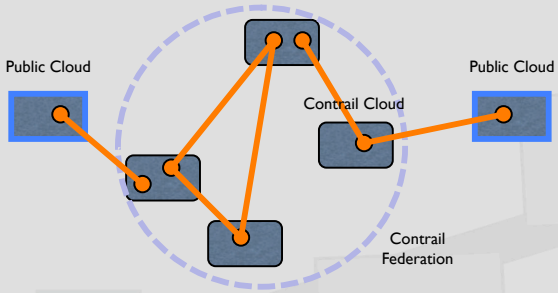
Federation Architecture (draft)



- Different options : centralized, distributed, hybrid
- Federation supprt should enjoy **trusted** resources

26

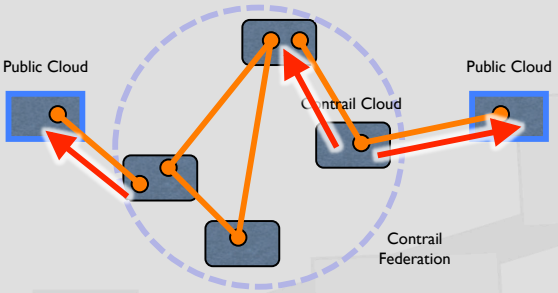
IaaS Federation in Contrail



- Improved SLA and QoS enforcement from Contrail Providers
- Single sign-on and IaaS management toward multiple providers

27

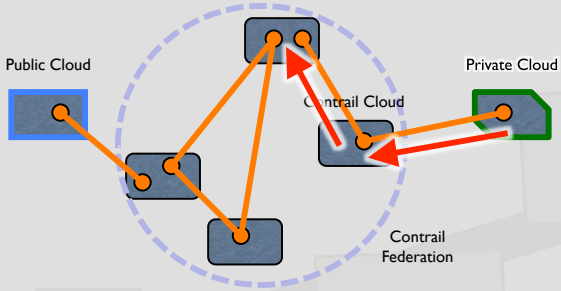
IaaS Federation in Contrail



- Cloudbursting exploiting federation resources *and* public Clouds
- Rely on accepted standards

28

IaaS Federation in Contrail



- Cloudbursting toward Contrail : Federation as a Cloud provider

29

Key features for federation support

- Scalability, security, resource use optimization, SLA monitoring and enforcement

- Provide access points
- Provide AAA checks
- Manage resource location from providers
- Manage resource selection
- Set up deployment on providers
- Monitor execution (SLA monitoring/enformcement)

30

Opportunities for Research

- Single versus multiple access points to federation
  - centralization bottleneck vs need for coordination
- Mechanism for coordination of access points
  - P2P/gossip mechanisms? but Security built-in!
- Resource allocation
  - Hierarchical, multiple-goal scheduling
  - Adaptive continuous resource management
- Complex application description
- SLA hierarchical management
  - SLA splitting and coordination

31

Next Steps

- Refine Federation requirements and Architecture
- Contribute to the overall CONTRAIL architecture
- Focus on core WPs (VIN, GAFS, VCP, Security)
- Federation-wide resource allocation, scheduling and QoS monitoring/enforcing algorithms
  - Development, Simulation
  - Formal validation of security properties

32