Usage Control in CONTRAIL Cloud

POFI 2011
Pisa, 9 June 2011

Paolo Mori
IIT - CNR
Agenda

• CONTRAIL project
• Usage Control Model
• Security Policy Language
• Usage Control System Architecture
CONTRAAIL Project
contrail is co-funded by the EC 7th Framework Programme

Funded under: FP7 (Seventh Framework Programme)
Area: Internet of Services, Software & virtualization (ICT-2009.1.2)
Project reference: 257438
Total cost: 11.29 million euro
EU contribution: 8.3 million euro
Execution: From 2010-10-01 till 2013-09-30
Duration: 36 months
Contract type: Collaborative project (generic)
Objectives

- Design, implement, validate and promote an open source software stack for Cloud federations
- Develop a comprehensive Cloud platform integrating a full IaaS and PaaS offer
- Allow Cloud providers to seamlessly integrate resources from other Clouds with their infrastructure
- Provide trusted Clouds by advanced SLA management
- Break the current customer lock-in situation by allowing live application migration from one cloud to another
CONTRAIL Federation

- A CONTRAIL federation integrates in a common platform multiple Clouds, both public and private.
- Coordinates SLA management provided by single Cloud providers.
- Does not disrupt providers' business model.
- Allows to exploit the federation as a single Cloud.
Expected Outputs

– A collection of infrastructure services
  • Virtual Infrastructure Networks
  • Virtual Cluster Platform
  • Globally Distributed File System
– Services to federate IaaS Clouds
  • Identity Management
  • Management of federation policies
  • SLA management
  • Autonomic resource management
– A collection of PaaS services to support Cloud applications
  • High throughput elastic structured storage
  • Automatic set-up and configuration of SQL servers
  • Geographically distributed key/value store
Expected Outputs (II)

- A collection of run-time environments
  - An efficient map-reduce implementation
  - Scalable hosting for service oriented applications
  - Autonomic workflow execution
- A collection of applications
  - Distributed Provisioning of Geo-referentiated Data
  - Multimedia Processing Service MarketPlace
  - Real-Time Scientific Data Analysis
  - Electronic Drug Discovery
CONTRAIL in a Nutshell

Cloud Federation Management SP1

Cloud User Interface + API

IaaS Federation (distr. registry, VO management, identity mgmt)

Integration, Validation and Testing SP4

High-throughput Electronic Drug Discovery

Distributed Provision of Georeferenced Data

Clouds for High-Performance Real-Time Scientific Data Analysis

Multimedia Processing Service Marketplace

Use cases and Exploitation SP5

Platform-as-a-Service SP3

Key-value store

Structured storage

SQL

Map/Reduce

Bag-of-Tasks

Web-servers

well known abstractions (POSIX API, x86 ISA, IP Network)

Network

Compute

Storage

Core Virtual Infrastructure Layer SP2

Providers
## Sub-projects and Workpackages

<table>
<thead>
<tr>
<th>SP5. Use cases and exploitation</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>12 Applications and Use Cases</td>
<td>13 Testbeds</td>
</tr>
<tr>
<td>14 Communication and Dissemination</td>
<td>15 Demonstrators</td>
</tr>
<tr>
<td>16 Exploitation and technology transfer</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SP4. System Engineering</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>10 System Architecture</td>
<td></td>
</tr>
<tr>
<td>11 Integration, testing and release management</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SP3. Platform as a Service</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>8 High level services</td>
<td>9 Runtime environments</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SP1. Cloud federation management</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2 IaaS federation</td>
<td>3 Service level agreements</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SP2. Virtual Infrastructure layer</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>4 Virtual Infrastructure Network</td>
<td>5 Computational Resource Management for Virtual Cluster Platforms</td>
</tr>
<tr>
<td>6 Global Autonomous File System</td>
<td>7 Security in Virtual Infrastructures</td>
</tr>
</tbody>
</table>
WP7

• Security in Virtual Infrastructure
  – Authentication
  – Usage Control
  – Compartmentalization and Isolation
  – Auditing
Usage Control Model
Usage Control Model

• Defined by R. Sandhu et. al.
  – The UCON Usage Control Model. ACM Trans. on Information and System Security, 7(1), 2004
  – ..... 

• Main novelties
  – New decision factors
  – Mutability of Attributes
  – Continuity of Enforcement
Example: onGoing Authorization

The right is granted without pre decisions, but authorization decisions are made continuously while the right is exercised

authorize(s,o): true
revoke(s,o): (usageNum(o) >10) and (s,t) in startT(o) with t min

preUpdate(startT(o)): startT(o) = startT(o) U {(s,t)}
preUpdate(usageNum(o)) : UsageNum(o)++

postUpdate(usageNum(o)) : UsageNum(o)--
postUpdate(startT(o)): startT(o) = startT(o) – {(s,t)} where (s,t) in startT(o) with t min
Access VS Usage Control

Decision

Pre decision

Ongoing decision

Access request

Usage

Before usage

Usage

After usage

Attr. update

Pre update

Ongoing update

Post update

Continuity of decision

Mutability of attributes

Time
Access VS Usage Control

Continuity of decision

Decision
Access request
Usage
Attr. update

Pre decision
begin
Usage
After usage

Pre update
Ongoing update
Post update

Mutability of attributes

Time

revocation
Access VS Usage Control

Traditional Access Control

Decision

Access request

Usage

Attr. update

Pre decision

Before usage

Pre update

Usage

After usage

Ongoing decision

Mutability of attributes

Continuity of decision

Time

Ongoing update

Post update
### UCON Core Models

<table>
<thead>
<tr>
<th>Decision Factors</th>
<th>Decision Time</th>
<th>Attributes Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auth</td>
<td></td>
<td>IMMUT</td>
</tr>
<tr>
<td>PRE</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>ON</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Obbl</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PRE</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>ON</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Cond</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PRE</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>ON</td>
<td>Y</td>
<td>N</td>
</tr>
</tbody>
</table>
Why Usage Control in CONTRAIL?

- Accesses to some resources last a long time (hours, days,..)
  - Run a Virtual Machine
  - Mount a Global File System on a Virtual Machine
  - Establish a virtual network connection
  - ...

- The factors that granted the access when it was requested could change while the access is in progress
  - User's reputation could decrease
  - Workload of resources could change
  - ...

- The security policy should be re-evaluated every time that factors change
  - An access that is in progress could be interrupted
Security Policy Language
UCON XACML Security Policy Language

• We are extending XACML language to implement UCON features:
  – Attributes update
  – Continuous control

• Preliminary work:
  – A proposal on enhancing XACML with continuous usage control features. CoreGrid ERCIM WG Workshop on Grids, P2P and Service Computing, 2009
UCON-XACML Policy Schema
Example of UCON-XACML policy

```xml
<?xml version="1.0" encoding="UTF-8" ?>


PolicyId="GeneratedPolicy" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:ordered-permit-overrides">

+ <Rule RuleId="LoginRule" Effect="Permit">

  + <Target>

    - <Condition FunctionId="urn:oasis:names:tc:xacml:1.0:function:double-greater-than"

      FunctionId="urn:oasis:names:tc:xacml:1.0:function:double-one-and-only">

      <SubjectAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#double"

        AttributeId="urn:iit:cnr:names:subject:reputation" Issuer="iit.cnr.it" />

  </Condition>

  </Target>

  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#double">0.9</AttributeValue>

</Rule>

+ <AttrUpdates>

  <Rule RuleId="FinalRule" Effect="Deny" />

</AttrUpdates>

</Policy>
```
UCON XACML Security Policy

• CONTRAIL supports security policies at different levels:
  – Federation level
  – Cloud Provider level
  – Interactions through attributes
Usage Control System Architecture
Security-Relevant Actions

• Are the action that are **relevant for system security**
  – Their execution must be controlled by the usage control system

• We are defining the set of security-relevant actions for each component of the CONTRAIL architecture, e.g.:
  – Federation Manager
  – VM manager
  – VIN
  – GAFS
  – VCP
  – …..
Example: VM Manager

• Security Relevant Actions:
  – Create a new VM Image
  – Start a VM
  – Stop a VM
  – Delete a VM Image
Usage Control System Architecture

• We are extending XACML architecture to deal with continuous policy enforcement
Usage Control System Components

- **Policy Enforcement Point**: intercepts the execution of security-relevant actions
- **Context Handler**: constructs XACML requests for the PDP, retrieves attribute values
- **Policy Decision Point**: evaluates the security policy to determine user's right to execute a security relevant action
- **Policy Information Point**: manages the attributes of users and resources
- **Policy Administration Point**: writes policies and make them available to the PDP
Policy Enforcement Points (PEPs)

- PEPs must be “embedded” in the architecture components that implement the security-relevant action (SRA) to:
  - Intercept the SRAs before their execution and suspend them
  - Ask the PDP to evaluate the security policy and wait for the decision
  - Enforce the decision of the PDP
    - resume the execution of the SRA
    - skip the execution of the SRA
    - ...
  - Interrupt the execution of the SRA that is in progress when requested by the PDP
  - Intercept the end of a SRA and communicate it to the PDP
contrail is co-funded by the EC 7th Framework Programme

Funded under: FP7 (Seventh Framework Programme)
Area: Internet of Services, Software & virtualization (ICT-2009.1.2)
Project reference: 257438
Total cost: 11,29 million euro
EU contribution: 8,3 million euro
Execution: From 2010-10-01 till 2013-09-30
Duration: 36 months
Contract type: Collaborative project (generic)