Federation and its security aspects

Contrail project & Koofr
Aleš Černivec & Luka Zakrajšek
XLAB & Koofr

Clouds


amazon
web services™


iCloud


talk
Google™ apps


rackspace®
the open cloud company

Clouds and Applications

- Selection of providers
- Each platform needs special deployment configuration
- Different platform, different UX
- Personalized images

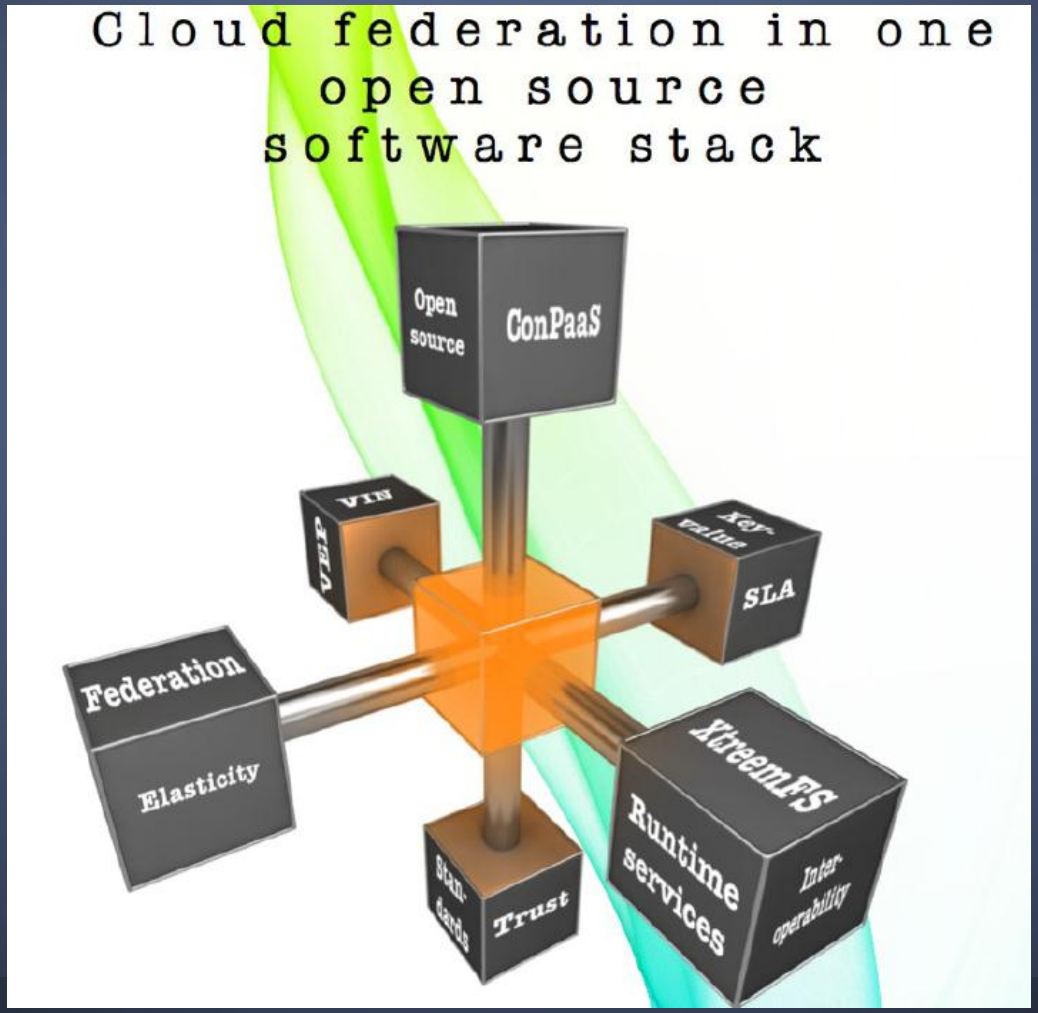
Federation of Clouds

- Abstraction of providers
- Selection and deployment
- Providing unified approach

Contrail Project

- FP7 EU Research project, 11 partners
- Integrated software stack
- Standard interfaces for cooperation and resource sharing within Federation of Clouds
  - integrated approach to virtualization (abstraction of IaaS)
  - unified way to describe and create an application on different IaaS providers
  - monitoring, accounting, billing

Federation and Applications

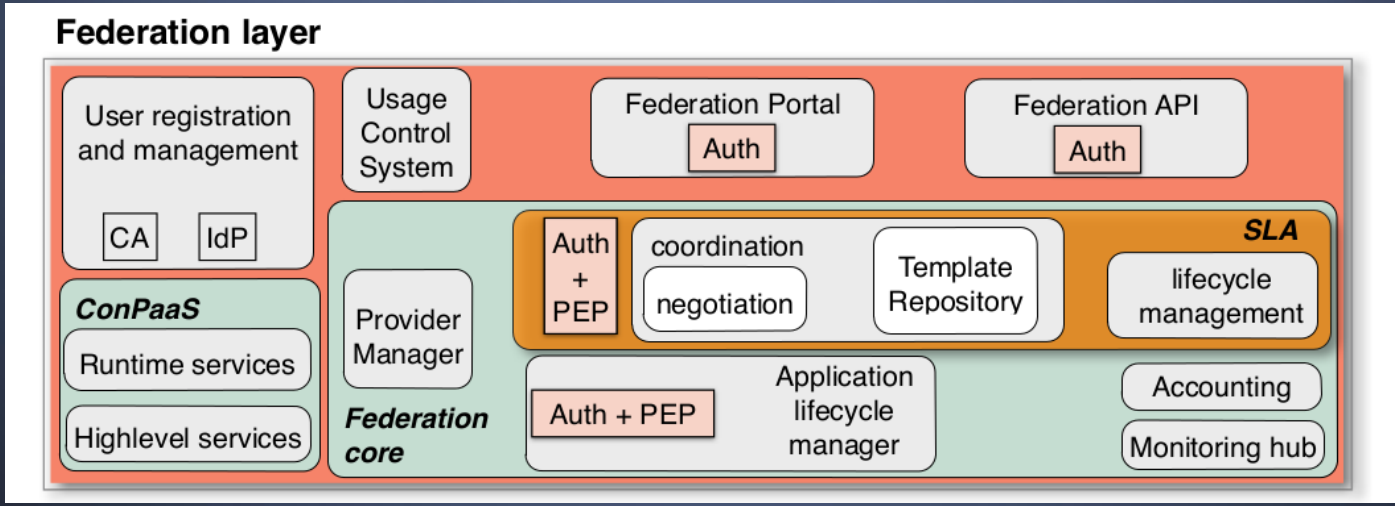


Contrail Layers

- Federation
- Provider
- Resource

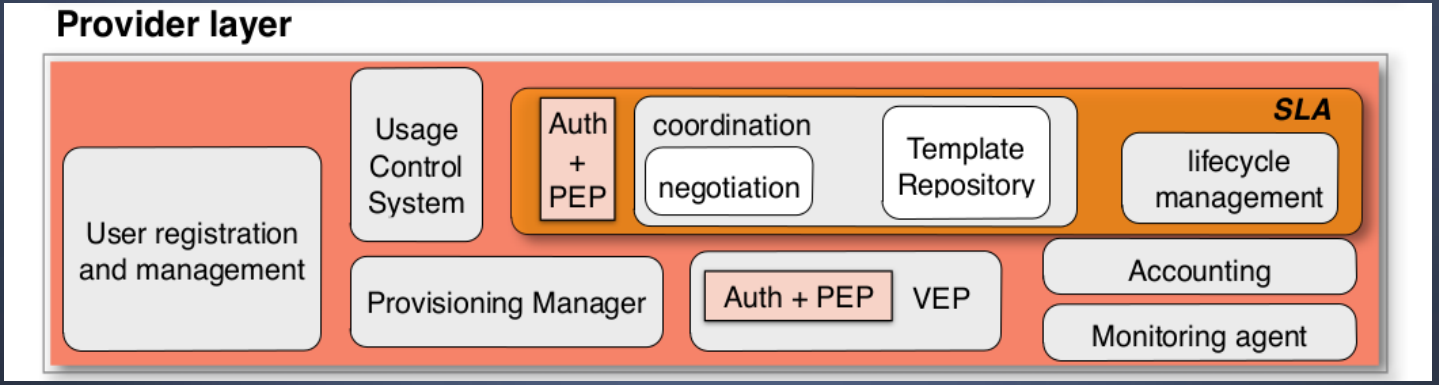
Contrail Layers - Federation

- Federation
  - Multiple access points
  - Services: Federation Portal, Federation API, Federation CA and IdP, ConPaaS



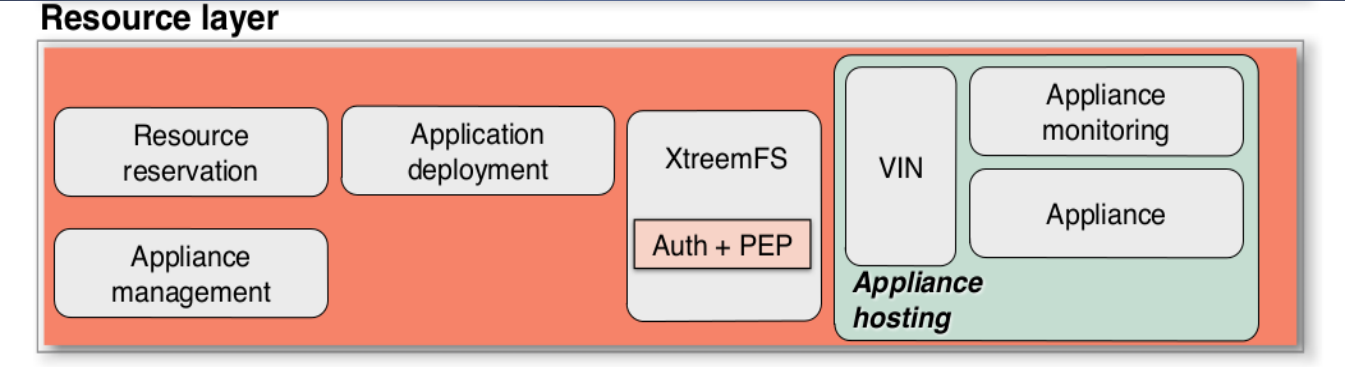
Contrail Layers - Provider

- Provider
  - Main interface: Virtual Execution Platform (VEP)
  - Other services: SLA, Monitoring, Accounting, Security (AuthZ, PEPs, UCON)

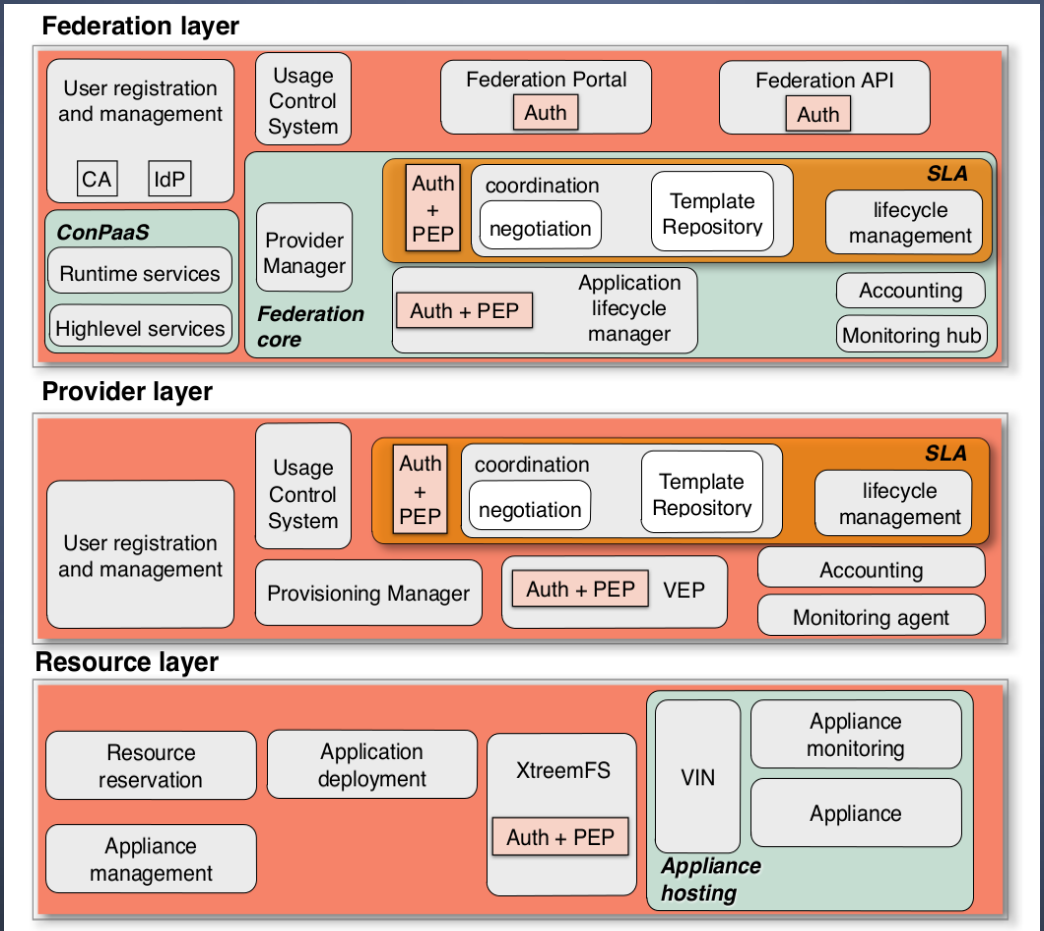


Contrail Layers - Resource

- Resource
  - Monitoring sensors, distributed file system (GAFS), security services, Virtual Infrastructure Network (VIN)



Contrail Software Stack



Application deployment

- Create an image, deploy the image or use existing one
- Describe the application
  - OVF
- Negotiate the provider
  - SLA: list of SLA terms
- Create the application
  - OVF + SLA = Deployment Doc

OVFs

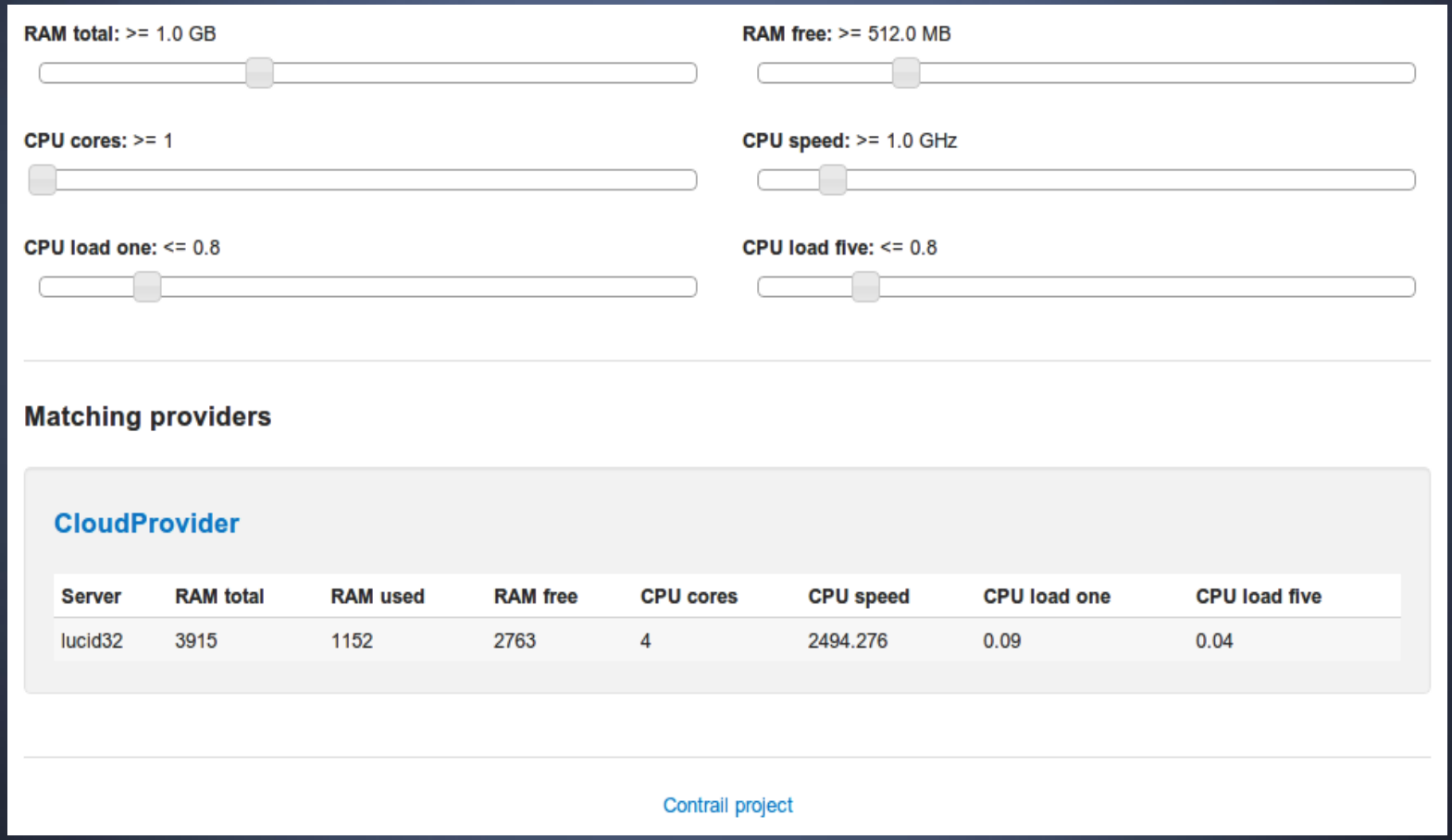
- References to VM‘s image
- Describe virtual disks
- Describe networks

```
<!-- References to all external files -->
   <References>
           <!-- Use existing ONE image ! -->
           <File ovf:id="dsl-1" ovf:href="/srv/one-images/dsl-1.qcow2.z" ovf:size="57359872" />
   </References>

   <!-- Describes meta-information about all virtual disks in the package.
           This example is encoded as a delta-disk hierarchy. -->
   <DiskSection>
           <Info>Describes the set of virtual disks</Info>
           <Disk ovf:diskId="dsl-1a" ovf:fileRef="dsl-1" ovf:capacity="1073741824"
                   ovf:populatedSize="157359872"
                   ovf:format="http://www.vmware.com/specifications/vmdk.html#streamOptimized" />
           <Disk ovf:diskId="dsl-1b" ovf:fileRef="dsl-1" ovf:capacity="1073741824"
                   ovf:populatedSize="157359872"
                   ovf:format="http://www.vmware.com/specifications/vmdk.html#streamOptimized" />
   </DiskSection>

   <!-- Describes all networks used in the package -->
   <NetworkSection>
           <Info>List of logical networks used in the package</Info>
           <Network ovf:name="private-lan">
                   <Description ovf:msgid="network.description">The network used to link the web s
```


SLA definition

- User selects an SLA template
- References the OVF
- Negotiate the terms of the SLA template
- Create an agreement
- User gets an SLA
- Uses it in the application deployment

Choosing the provider



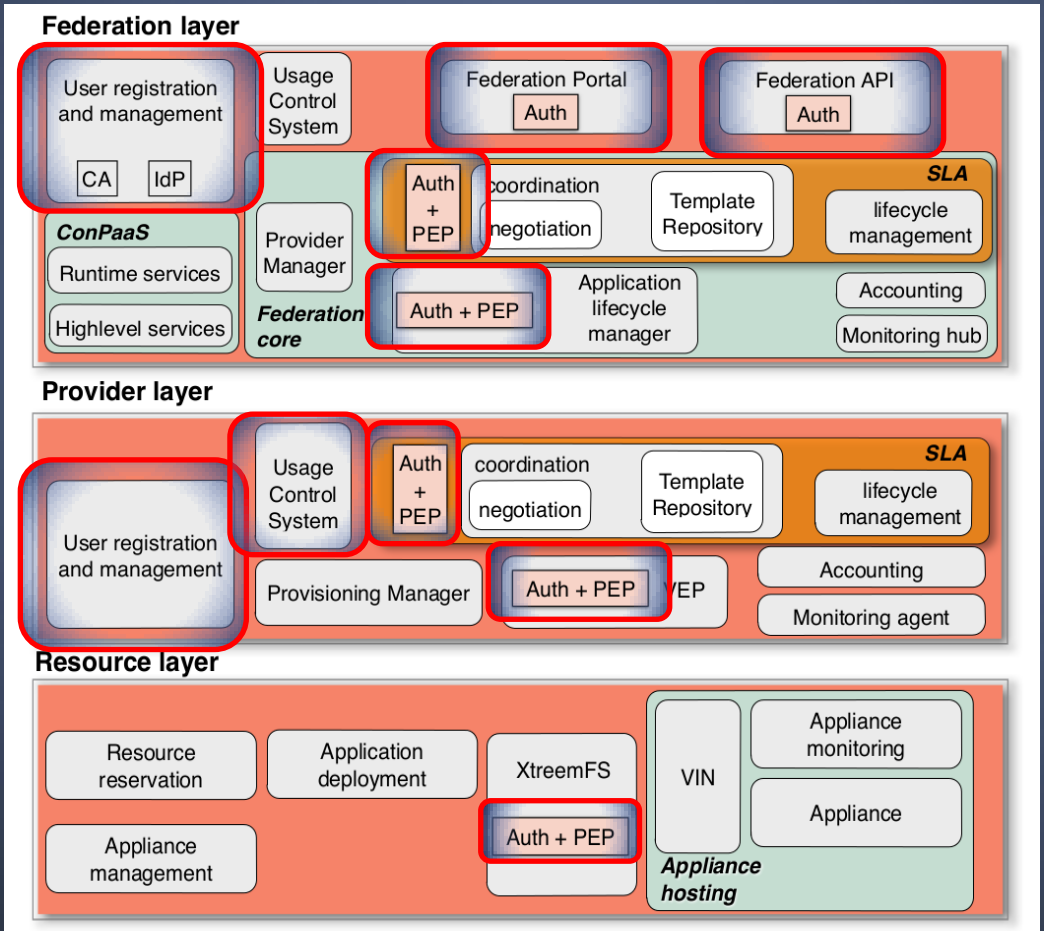
Negotiation process

- Demo

Federation and Security

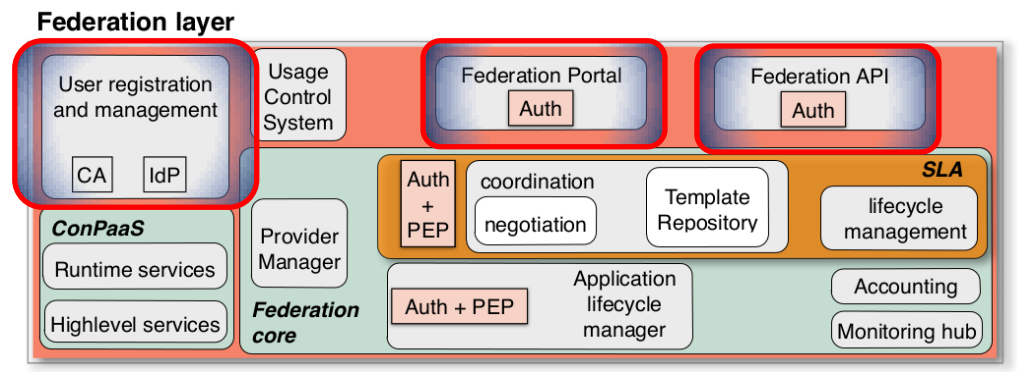
- AuthT: single sign-on, federated identity (SAML2, OpenID)
- AuthZ: usage control, policies (XACML)
- Delegation (OAuth2)

Contrail security components



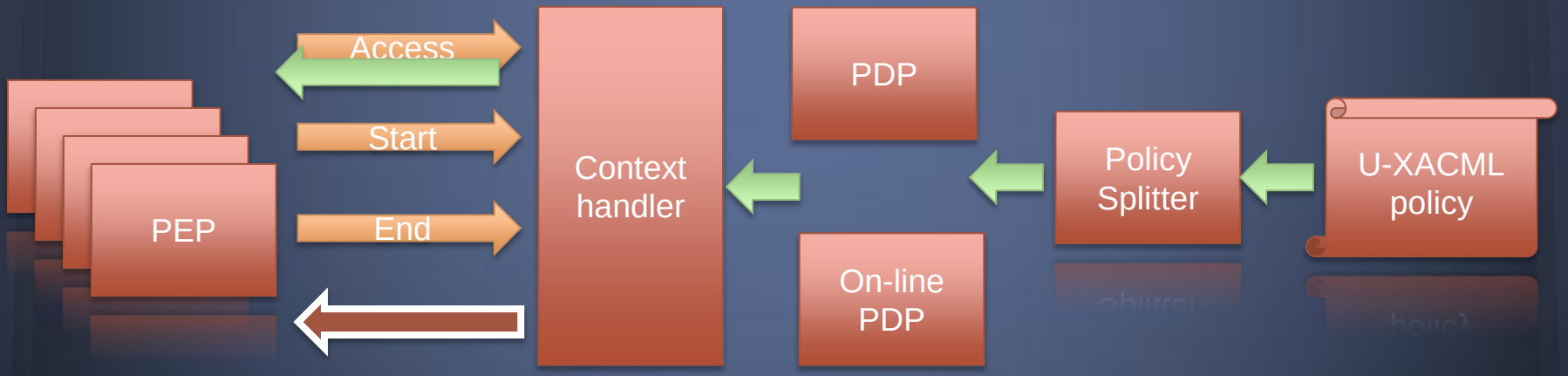
Authentication

- Web portal or CLI
- SSO and X509
- Support for federated id

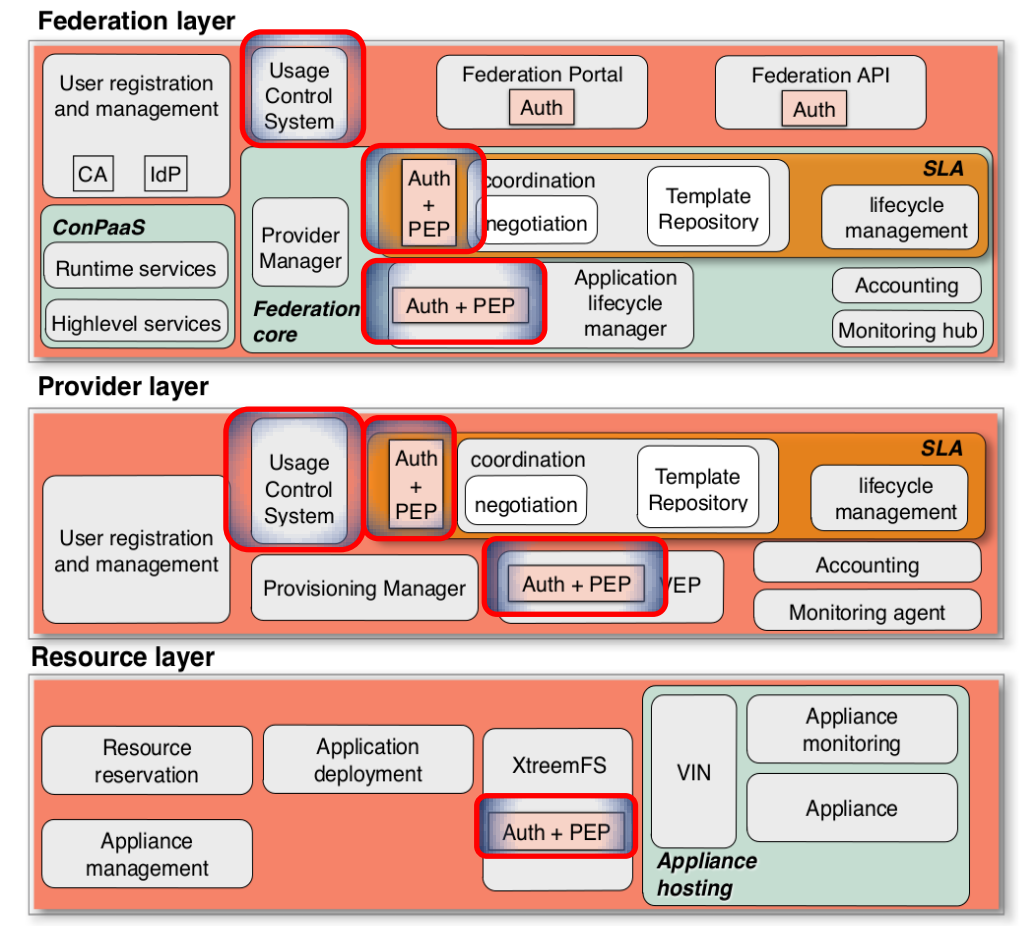


Usage Control - UCON

- Policies expressed using U-XACML
- On-line usage control



Usage Control - UCON

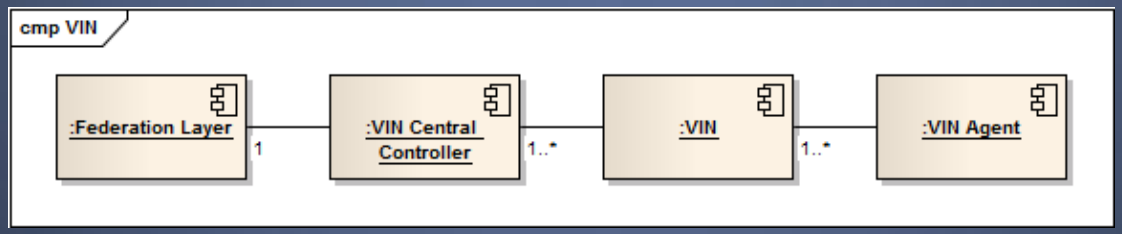


Delegation

- Core components access to users' resources
- Delegation use cases
  - Delegated user credentials to services
  - Delegation within VIN - Virtual networks
- OAuth2
  - Authorization grant (initial authZ step)
  - Client Credentials grant

Delegation and networks

- VIN
  - Elastic private networks within cloud application
  - Nodes, GAFS instances, physical machines
  - Scales, handles large networks

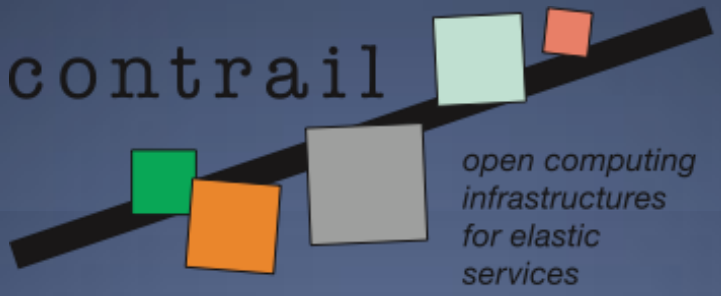


Storage

- How to transfer images to providers?
- Moving data between providers
  - Secure, efficient, API
  - Different (public/private) providers
- Provide unified access to the storage underneath
- Koofr – hybrid cloud storage interface

Project resources

- Source code in public SVN
- OW2 Jira for issue tracking
- DEB packages for Squeeze, up to Ubuntu 12.04 LTS
- Guides (Installation, Admin, User)
- http://contrail-project.eu
- http://contrail.projects.ow2.org/xwiki/bin/view/Main/Download



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)

Future development

- Full support for reservations and SLA terms
- Federation becomes a provider
- Federation accounting support
- Federation SLA violation handling
- Improved security (OAuth2 on all layers)
- Multiple federation nodes