RESERVOIR

Editorial

As the RESERVOIR project moves into its third and final year, this newsletter looks at some of the achievements that have taken place so far. Focus is also placed on the the importance of best practices and standards and how alliances between cloud computing interoperability and security standards groups have been formed. Finally we look at how cloud can both improve security and resilience and how it also raises specific challenges.

RESERVOIR – Two Years on

Since its launch in February 2008, the RESERVOIR project has defined a Reference Architecture for a next generation of Infrastructure as a Service (IaaS) Clouds capable of dealing with new requirements such as service-orientation (services managed as a whole, automating the services provisioning and scalability, and guaranteeing SLAs), separation between infrastructure and services, use of Open/Standard specifications, virtualisation technology independent, support for site federation (allowing private, public and hybrid Clouds), security and isolation reinforcement and use of utility computing business models.

Juan Caceras, Telefonica I+D (left), outlined some of the achievements of the project as it enters its third and final year at the recent Cloudscape II workshop which took place in February in Brussels. The project achievements were also highlighted in the following paper, published especially for the event and authored by Juan and Ignacio Llorente, UCM, Irit Loy, IBM and Philippe Massonet, CETIC.
RESERVOIR infrastructure management functions are structured in three layers, each dealing with different aspects of the Cloud:

- **Service Manager (SM)**
- **Virtual Execution Environment Manager (VEEM)**
- **Virtual Execution Environment Host (VEEH)**

Year 2 Achievements

The Service Manager (SM) is responsible for the instantiation of service applications (controlling the Service Lifecycle) and dynamically requesting virtualised resources to the underlying layer (VEEM), trying to avoid over/under provisioning and over-costs based on SLAs and business rules protection techniques. RESERVOIR proposes an integrated model to automate service deployment and scalability, including elasticity rules, SLA monitoring and protection, and business business-oriented directives.
Year 2 results include:

- Use of Distributed Management Task Force's (DMTF) OVF specification to declare the service architecture (set of virtual machines, networks and other virtualized resources) and extensions to it to define deployment directives and automatic scaling.
- Cloud Interface (SMI) to manage services "as a whole".
- Customisable Service Monitoring systems to support SLA protection.
- SLA Management model based on WS-Agreements.
- SLA Protection components based on elasticity rules and control theory.
- Accounting & Billing models for federated clouds.
- Access control and signing of OVF files with X509 based certificates.

Software prototypes have also been developed to support the research, and most of the components will be released as Open Source.

Virtual Infrastructure Manager (VEEM) are responsible for the placement of VEEs (Virtual Execution Environment, a generalisation of the Virtual Machine concept) into VEE Hosts (a generalisation of the concept of hypervisor or Java Virtual Machine Container manager).

Research activities conducted to meet the main challenges in Cloud infrastructure and federation operation include:

- Dynamic and scalable management of VMs and physical resources in data centres.
- Analysis of security functionalities of major cloud infrastructures and Open Source solutions.
- Virtual Resources provisioning and efficient local and cross-site placement algorithms to meet SLA commitments of service.
- Architectures for federation of sites to analyse the main challenges of cloud interoperation, regarding virtualisation, image, and network management, and performance evaluation of the proposed solutions.
- Provisioning algorithms across sites including the design, implementation, and evaluation of a framework for brokering (site selection) in federated clouds.
- Cloud API specification for virtual resource provisioning leading the Open Grid Forum's Open Cloud Computing Interface Working Group (OCCI WG).
- Plug-ins to access remote Clouds such as Amazon EC2, ElasticHost or RESERVOIR remote sites.

The Virtualisation Layer (VEEH) represents a virtualised resource that can host a certain type of VEEs (for example a physical machine with a hypervisor controlling it, or a Java Virtual Service Container). VEEH is also responsible for adding to the virtualisation platform the necessary functions (virtual network management, image storage, image live-migration, etc.).
VEEH supports the Hosting of Virtualised Resources. In order to support the required platform virtualization abstraction RESERVOIR has developed:

- Federated Network Service. VEEH's network service supports isolated virtual networks that span VEEHs and sites.
- Host-based parallel and distributed provisioning for elastic applications. The hosting platform is responsible for VEE provisioning (as opposed to the management). Furthermore, a VEEs that are generated from the same template image may be provisioned in parallel on different VEEHs.
- Live Migration with non-shared storage and/or subnet. Allows transparent VEE migration to any VEEH, in the Site, regardless of the target VEEH network or storage configurations.
- Federated Monitoring Service. The VEEH monitoring service supports asychronous monitoring of the VEEHs, their VEEs and the applications running inside the VEEs.

Conclusions

Most of the RESERVOIR's research results have been published as scientific papers, open specifications and Open Source software. In particular, Telefónica I+D has created Claudia for publishing SM components, UCM is evolving Open Nebula, IBM is contributing to the KVM Community and UCL has created and released The Lattice Monitoring Framework for federated Clouds. RESERVOIR is also actively contributing to Standardisation Bodies such as OGF with the Open Cloud Computing Interface working group (OCCI-WG) and DMTF with the Cloud Incubator working group. Therefore, the combination of open standards and open source software will assist future research on Cloud Computing. This is some of the return on investment of RESERVOIR's contribution to the economic and scientific development within the European Union.

Finally, as RESERVOIR commences on the final year of the project, coordinator Eliot Salant underlines the importance of sustaining the progress made so far. "*In its third and final year, RESERVOIR research will be concentrating on solving the general case of cloud federation. Additionally, we will be actively pursuing exploitation activities to guarantee that the RESERVOIR legacy will live on.*"

RESERVOIR Reports and publications are available here.

Go back to top

Building Alliances for Standards

Best practices transformed into standards for interoperability are seen as central to pervasive adoption at an accelerated pace. Standards in the ICT industry serve to enable interoperation between consumers of similar product and services from different providers, giving the consumer the freedom to choose offerings that meet their current business needs. Open standards are also important to accelerating the growth of important new markets where consumers can rapidly adopt new ideas and innovate in their businesses. Products and Services are differentiated by the

performance relative to the prices they set. This gives the consumer choice and ultimately drives competition among service providers.

The advent of cloud computing has brought into play new standardisation efforts in a surprisingly positive and co-ordinated way prompted by a recognised need to build strategic alliances across Standardisation Development Organisations (SDOs), share knowledge and ultimately develop a complementary standards framework.

Interoperability is important to users and RESERVOIR is working closely on standard interfaces for the remote management of cloud infrastructures, working with various standards bodies including DMTF and OGF between the Virtual Infrastructure Management and the Cloud Management layers. The validation and use of open interface standards by RESERVOIR aims to promote adoption by Cloud customers.

Recently this work has been made easier following the alliance between cloud computing interoperability and security standards groups. This has seen the Data Management Task Force (DMTF), Open Grid Forum's Open Cloud Computing Interface working group (OCCI), the Cloud Security Alliance, the Storage Networking Industry Association and the Object Management Group, join forces to address cloud services interoperability and portability. As cloud computing develops increasing numbers of proprietary and open application programming interfaces (API) are being proposed to provide management, security and interoperability among IaaS services, including Amazon.com Inc.'s Elastic Compute Cloud API, VMware Inc.'s DMTF-submitted vCloud API, Sun Microsystems' Open Cloud API, Rackspace US Inc.'s API, and GoGrid Cloud Hosting's API. In order to address such diversity, a cloud standards wiki has been developed in order to highlight Standards groups working with Cloud and to track their progress.

Market forces, consumer demand and economics eventually will pare down these standards players, analysts say; in the meantime, consumers will use a variety of interfaces to interact with cloud services. In addition, a new class of cloud service brokers probably will emerge to abstract incompatible APIs and provide a seamless interface in advance of a common cloud API, according to the Cloud Security Alliance.

Go back to top

Security and Risk Assessment for Cloud Computing

"The information risk management factors one must consider when leveraging cloud computing – especially legal and regulatory compliance issues – represent unchartered territory for many enterprises." – Joshua Davis, Director of Information Security & Compliance, Qualcomm

Discussions on security and cloud computing need to be multi-perspective, exploring how cloud can both improve security and resilience on the one hand, and how it raises specific challenges on the other. New insights in this respect have been delivered by a study and report on Cloud Computing Security Risk Assessment spearheaded and published by the European Network and Information Security Agency (ENISA) with the support of a group of experts, including representatives from enterprise and from RESERVOIR **Philippe Massonet**, CETIC. The study is an independent, in-depth analysis outlining several information security benefits and key security risks of cloud computing, along with a set of practical guidelines.

Security Benefits

Cloud computing can bring clear benefits and has a significant potential to improve security and resilience. Cloud computing security can also benefit from the economies of scale provided by cloud computing as all kinds of security measures are cheaper when implemented on a large scale. Cloud computing can also be a marker differentiator. This is because customers can compare and select services based on the quality of protection provided.
Cloud providers can offer value-add by:

- Hiring highly qualified security personnel to develop and deploy scalable security infrastructures.

- Supplying open and standardized interfaces to managed security services for high-quality security.
- Dynamically scaling defensive resources on demand for a high level of resilience even when under attack enabled by the rapid scaling of resources.
- Providing audit, evidence gathering and forensic analysis services.
- Bringing more timely and effective updates on security patches.
- Offering as a service the hardening of customer virtual machines and application of security patches.

Best practices encompass audits and Service Level Agreements (SLAs) to foster better risk management practices capable of dealing with potential penalties for SLA breaches and resulting impact on reputation. Another point for consideration regards resource concentration. While this can be attractive to attackers, it brings advantages of cheaper physical access control per unit resource and an easier and cheaper application of a comprehensive security policy.

Technical Security Risks

Technical risks identified include:

- Resource exhaustion caused by under or over provisioning.
- Isolation failures due to resource sharing & multi-tenancy leading to a breach of confidentiality.
- Malicious insider activity resulting in breach of confidentiality, integrity and availability of data & services.
- Management interface risk linked to remote access over the Internet & browser vulnerabilities leading to unauthorized access.
- Data leakage on upload/download.
- Insecure or ineffective deletion of data.
- Distributed or economic denial of service.
- Conflicts between customer hardening procedures and cloud provider procedures.

Legal & Policy Framework

"Regulatory agents, government and standards bodies need to enforce a legal framework that allows people to be accountable for a breach of confidentiality and loss of data to build a trusted environment where customers can move data outside their corporate domain. We have a long way to go along this road, and industry cannot go it alone, so we need European Union and government involvement." – Fabrizio Gagliardi, Microsoft Research & Chair of the Industry Expert Group

The ENISA Security Risk Assessment has identified a number of policy and organizational risks applicable to Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS):

- Vendor lock-in.
- Loss of governance because the user cedes control to provider on several issues that can affect security.
- Compliance challenges resulting from failure to conduct audits.
- Potential loss of business reputation due to resource sharing & co-tenant malicious activities.
- Cloud service failure or termination, acquisition by another provider.
- Shift in strategy that may put at risk some of the agreements on which a cloud client relies.

Additionally, in the context of service chains partially outsourced to cloud providers, any failure could have a snowball effect with significant economic loss.
In terms of legal risks, the ENISA Study has pinpointed the following:

- Subpoena and e-Discovery due to seizing cloud shared resources containing data of many customers.
- Managing customer data in multiple jurisdictions.
- Data protection risks.
- Licensing risks.

Government clouds will entail many non non-technical challenges, such as legal liabilities, legal electronic discovery and auditing. Data privacy and security is a particular issue from a government perspective. Tim Willoughby, Irish Local Government Computer Services Board, says "*the fear is data privacy and data security, the mobility of data across borders and sovereignty of data. At the moment these are really perceived barriers because not many governments are using cloud".* In Willoughby's mind, there is a growing need for governments to pursue focused discussions with vendors and service deliverers on such issues.
Concerted effort is needed on several fronts, encouraging standardised approaches at government level on the one hand and administrative and policy reform on the other

to ensure a level playing field and an environment consonant to cloud computing. The security benefits and risks of cloud computing are described in more detail in the following reports which are both available on the ENISA web site: Cloud Computing Security Risk Assessment & Cloud Computing Information Assurance Framework"

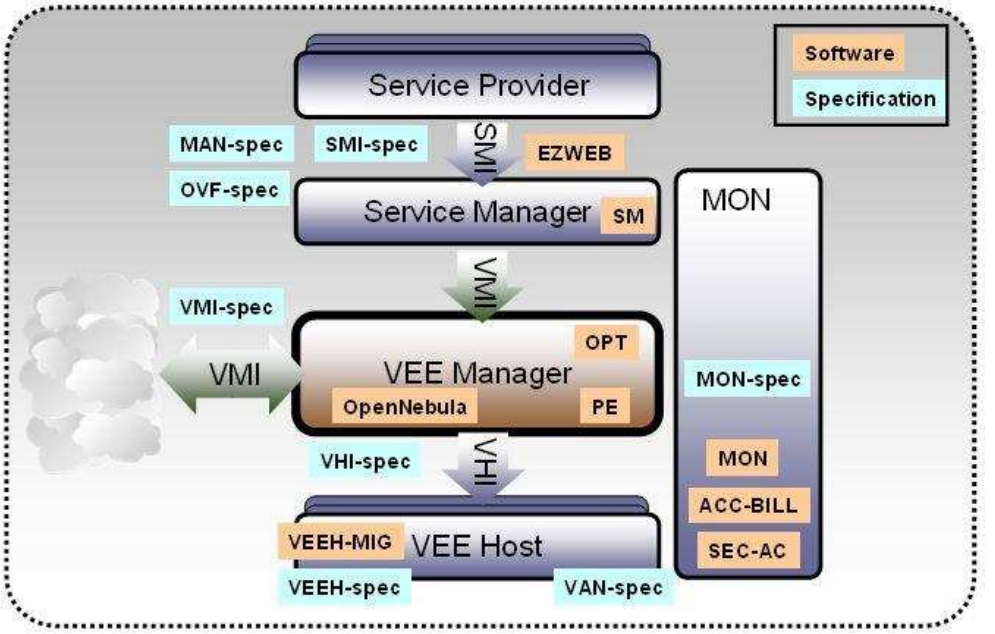
Acknowledgements

We would like to thank the ENISA Team, especially Daniele Catteddu and Giles Hogben, who coordinated and edited the reports.

Go back to top

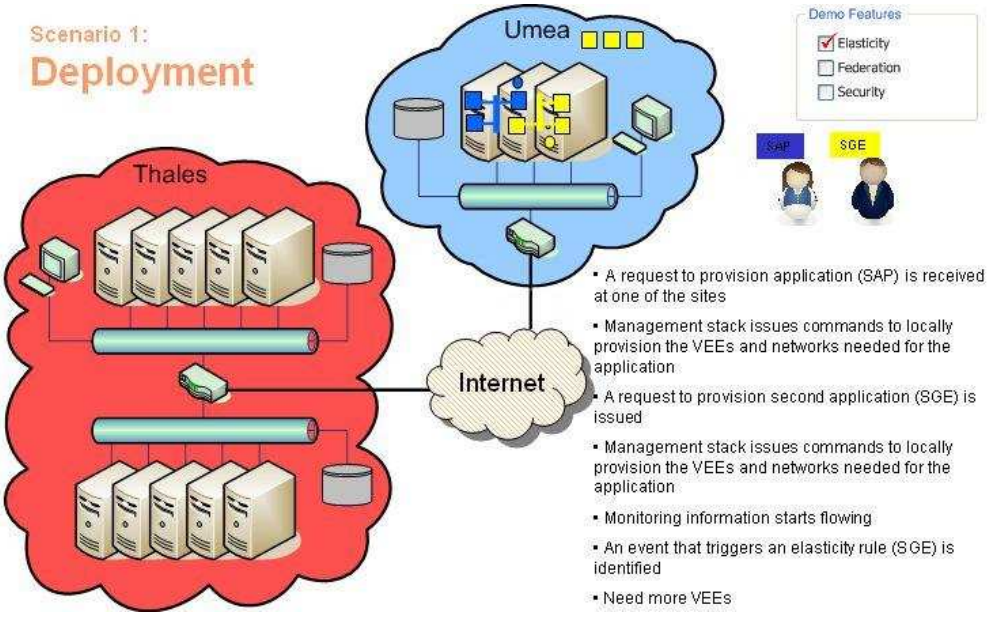
RESERVOIR Demo Now Online

The latest RESERVOIR demo shows how complex multi-tier applications can be securely deployed on a federated Cloud infrastructure. It demonstrates how virtualization and business service management techniques can be used to transparently provision and manage resources and services on an on-demand basis at competitive costs with high quality of service.



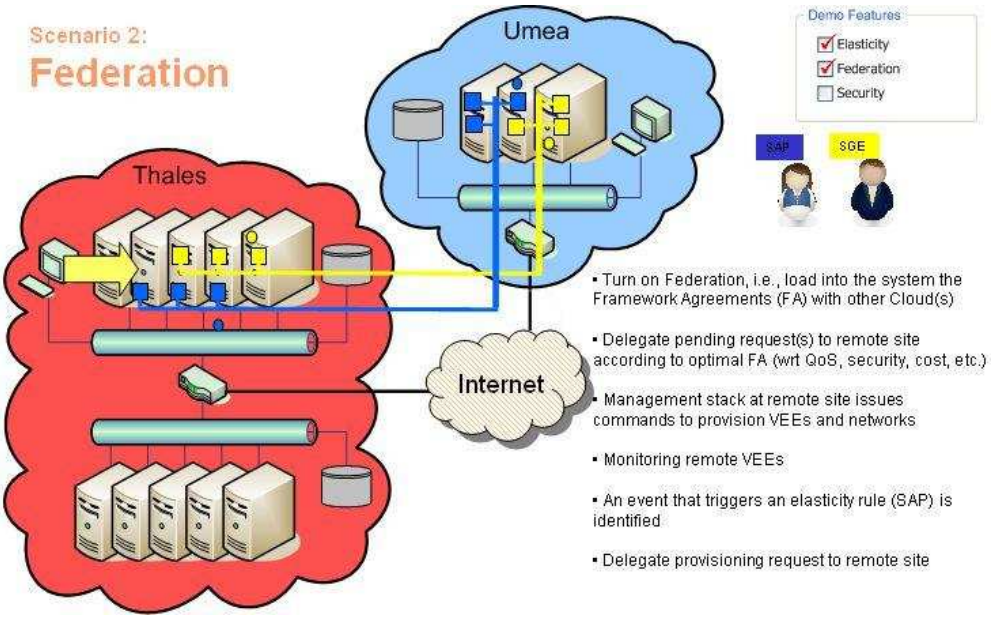
The RESERVOIR Framework

The demonstration consists of four scenarios.
The first scenario shows automated elastic deployment, auto-configuration and auto-scale of multi-tier applications from SAP, SUN and THALES.



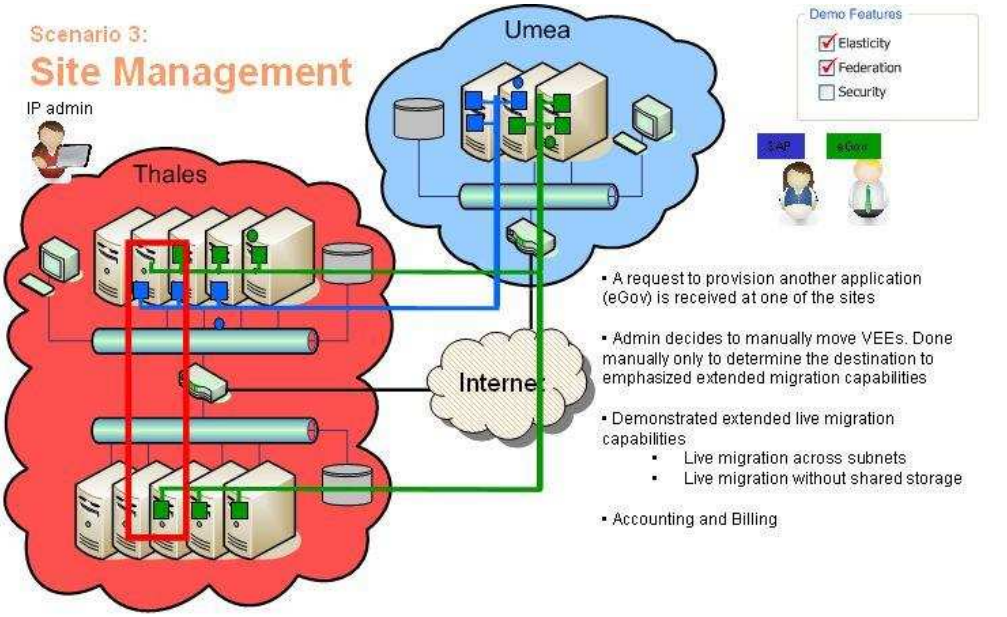
RESERVOIR Deployment scenario

The second scenario shows how federation can extend Cloud size by using remote resources for elasticity and deployment. It highlights cross-site placement, cross site virtual private networks and cross site monitoring.



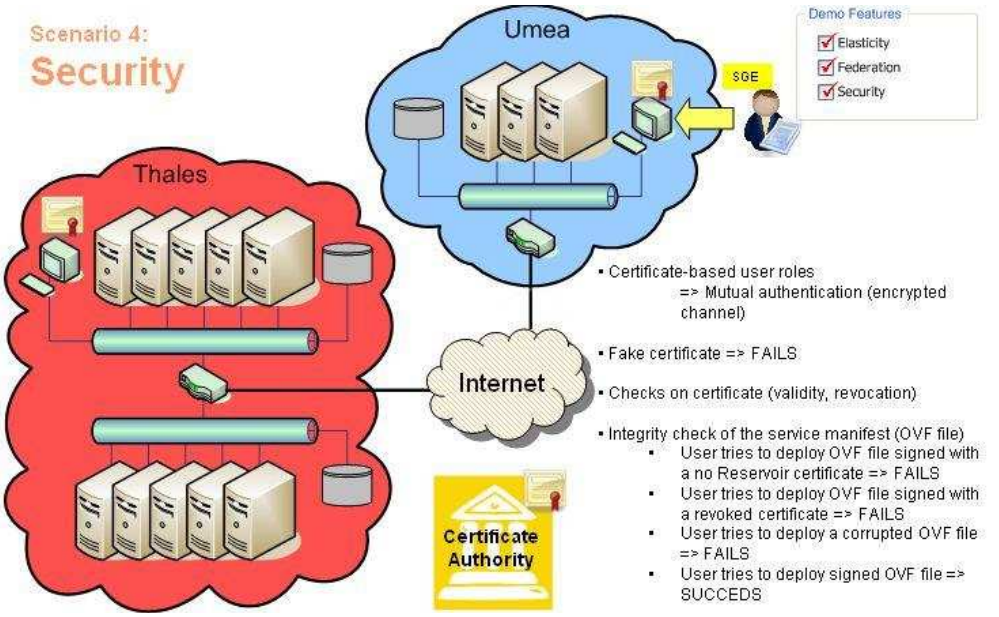
RESERVOIR Federation scenario

The third scenario demonstrates live migration capabilities across subnets without shared storage, and describes how cross site accounting and billing is performed.



RESERVOIR Site Management scenario

The fourth scenario highlights secure access to the Cloud by showing how certificates and role based access control are used.



RESERVOIR Security scenario

It is envisioned that the RESERVOIR innovation is to serve the European community in the development of next generation data centres demonstrating quantified and significant improvements in service delivery productivity, reducing software complexity and costs, expediting time-to-market, improving reliability and enhancing accessibility of consumers to government and business services.

Download the RESERVOIR Demo

Go back to top

RESERVOIR Training

RESERVOIR Training offers insight into the RESERVOIR framework, a collection of open source software, open specifications and publications produced by the project and available for download here. Information is given on the architecture, individual RESERVOIR components, and how to integrate them to build an open source cloud infrastructure. Training also aims to teach users how to create service definitions and submit them to a RESERVOIR infrastructure for deployment.

The next main training session will be at the **Second Service and Software Architectures, Infrastructures and Engineering (SSAIE) Summer School** - **June 28-July 2, 2010 - Heraklion, Crete.**

Further details on RESERVOIR training can be found here - http://www.reservoir-fp7.eu/index.php?page=training

Go back to top

RESERVOIR on the Road

Internet of Services - Technical Collaboration meeting for FP6 & FP7 projects
19-20 October 2010, Diamant Center, Auguste Reyerslaan 80, 1030 Schaarbeek, Brussels, Belgium

This event is organised by the European Commmission and co-hosted by **RESERVOIR** and the EC-funded project **Deploy**. The event will see the participation of representatives from FP6 and FP7 projects in the area of Software & Services, Grid and Software and Service Architectures and Infrastructures, as well as those seeking collaboration in this area or who wish to contribute to the Future Internet Assembly or NESSI.

Event objectives:

- Consolidating the collaboration activities among the projects in order to build an even stronger community; to include the newly started projects in Collaboration Working Groups.
- Providing new projects the opportunity to understand key results of established projects/collaboration working groups in order to facilitate reuse of these results
- Offering established projects/collaboration working groups the opportunity to exploit their results better by finding synergies with new projects
- Achieving a better understanding of the results of the FP6 & FP7 projects in the "Internet of Services" area

Look out for more event information on the RESERVOIR website.

RESERVOIR at Cloudscape Workshop

More than 120 participants joined Cloudscape-II to continue to explore the guiding principles which surround the importance of interoperability and the openness necessary for the development of grid-infrastructures as well as for the advent of cloud. Global standardisation efforts are a key priority and were highly promoted at the event.

RESERVOIR played a major role at Cloudscape-II with 2 presentations and a member of the Panel Discussion on Future Considerations, Achievements and Challenges:

- RESERVOIR Project: Major Achievements – Juan Careres, Telefonica
- RESERVOIR: The SAP use case – Maik Lindner, SAP Research
- Panel Member – Ignacio Llorente, UCM

Download the Cloudscape Executive Report

RESERVOIR at the Future Internet Assembly and NESSI Projects Summit

RESERVOIR presented its latest findings and achievements at both the Future Internet Assembly (FIA) April 15-16, 2010 and the NESSI Projects Summit on April 12-13, 2010 which were both held in Valencia, Spain. The project demonstrated how complex multi-tier applications can be securely deployed on a federated Cloud infrastructure. It showed how virtualization and business service management techniques can be used to transparently provision and manage resources and services on an on-demand basis at competitive costs with high quality of service.

RESERVOIR was organised an information stand at the FIA and participated with a number of presentations at both events:

- RESERVOIR – Service Computing Clouds – Benny Rochwerger, IBM
- Benefits of being a NESSI Strategic Project – Yaron Wolfsthal, IBM
- Infrastructure layer SLA@SOI and RESERVOIR – Philippe Massonet, CETIC
- Providing Infrastructure as a Service with a federated RESERVOIR Infrastructure – Michael van de Borne, CETIC

Go back to top