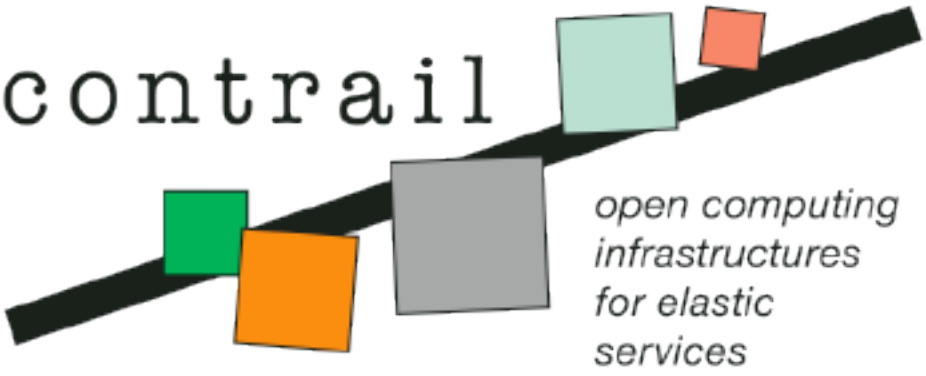
# Contrail White Paper




# Overview of the Contrail system, components and usage

**Bringing data centre style versatility to the Cloud**

**Second edition**

January 2014

**http://contrail-project.eu**

The Contrail project is managed by the Contrail consortium.
Contrail is partially funded by the FP7 Programme of the European Commission under Grant Agreement FP7-ICT-257438.

Version II 1.5 2014-01-20

# [preface]

## Contrail - Bringing data centre versatility to the Cloud

Cloud computing has developed fast over the past years. However, what it exactly is and how it can help your business is not always obvious. This White Paper provides a global overview of Contrail and is intended for IT managers that want to quickly get an idea about how they can take advantage of federated clouds at an Infrastructure-as-a-Service or Platform-as-a-Service level. In this White Paper we describe how the software that is being developed by the Contrail project can bring data centre style versatility to the Cloud that includes scalability, flexibility, security, and reliability. In this context a Cloud can be a private, public or hybrid Cloud. A Cloud can be a set of infrastructures (Infrastructure-as-a-Service) or platforms (Platform-as-a-Service) managed as one single entity by system management software, commonly referred to as Cloud middleware (OpenNebula, OpenStack, etc.). Contrail also enables and supports Software-as-a-Service (SaaS). SaaS itself is not in the scope of Contrail.

Contrail focuses on several aspects that will make cloud computing more versatile:

- Contrail provides federation of all types of Clouds
- Contrail provides  Cloud interoperability
- Contrail provides federated identity management, security and SLA support
- Contrail provides an industry grade Cloud file system
- Contrail provides Platform-as-a-Service layer, allowing easy management and deployment of applications and data storage.

In several use cases Contrail demonstrates how this technology can be used to set up distributed cloud environments that offer the kind of versatility that today can only be found in data centres.

# [table of contents]

# [introduction | about the cloud]

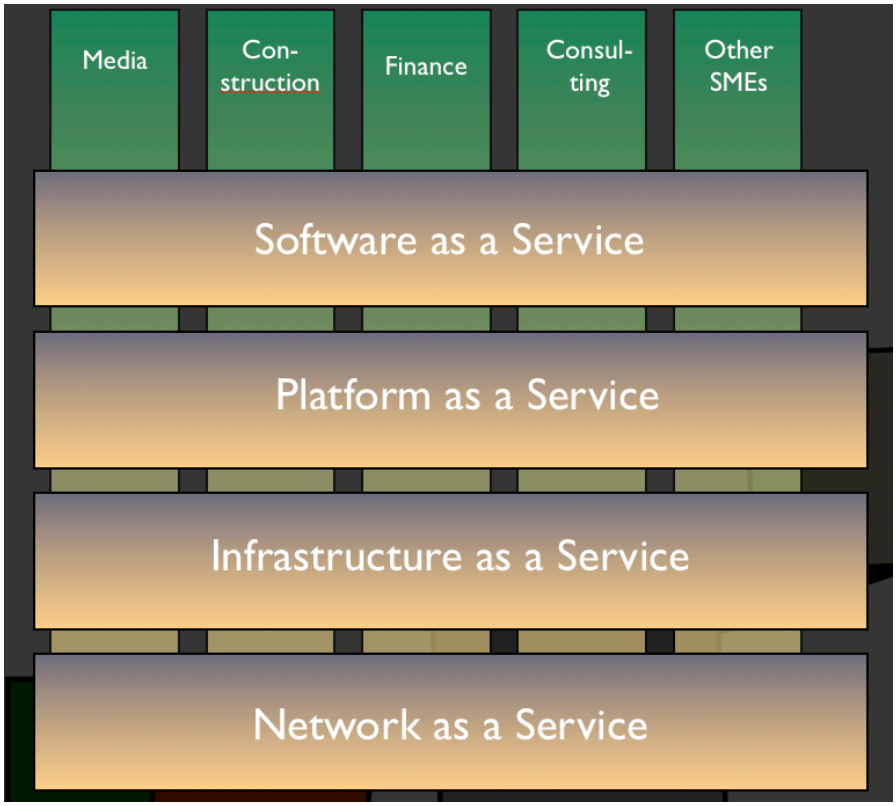
Today, almost anyone is running applications “In the Cloud”, and Cloud computing has become big business. However, running applications in the Cloud - Software-as-a-Service (SaaS) as it is commonly called - is just one part of Cloud computing.

Beneath this Software-as-a-Service, there are several other layers of Cloud computing. There is the Platform-as-a-Service layer. What you get as service here is a computing platform. This could be a PHP web platform or an SQL database. This layer is typically used by application developers or providers that provide Software-as-a-Service to the masses.

But in the end all of it needs computers to run on. This is provided by the next Cloud level: the Infrastructure-as-a-Service layer. Here the offer is a Virtual Machine or many Virtual Machines, that each are complete systems, working under Windows, MacOS or Linux. Infrastructure-as-a-Service is the alternative to buying your own machine(s).

There are some more Cloud Computing layers that recently gained interest. Networking-as-a-Service is one of them.

From a business perspective Cloud computing is about renting software and infrastructure instead of buying it. So you pay as you use. Cloud computing is also about reducing complexity of maintenance of IT. You do not have to maintain systems yourself. You just use them and always have the most recent version available. Because you rent hardware and software, you can easily rent more when you need it, and release it again when you do not need it anymore. This is what is called elasticity.



# [introduction | opportunities]

First and foremost inspiration for decision makers to turn to the Cloud is changing investment costs into renting cost, thus freeing up capital. Migration to the Cloud saves cost on in-house IT infrastructure, maintenance, and licenses. And that is not a vague promise, it's a fact. 97 percent of SMEs that have put some operations in the Cloud report they got what they wanted in terms of cost savings and increased flexibility (CompTIA survey 2011). Yet less than 50 percent of small business owners do expect cost savings from a switch to Cloud (Newtek survey 2011).

This comes as no surprise. Cloud opportunities are less evident than they appear. And they are flanked by Cloud threats. Since both lack common understanding, the uncertainty of economics and the fear of the unknown make business owners wait to see which way the cat jumps. Their fear to act upon the provided Cloud opportunities is not helping the economy.
Rather than budget driven migration, opportunity driven innovations could propel SMEs into the auspicious environment of the Cloud. Let's investigate the opportunities.

### Flexibility, agility, scalability

Virtualization technology makes the Cloud tremendously flexible. In a matter of minutes you can multiply capacity, improve performance or share resources and data.

### Availability

Cloud availability comes in two ways: in accessibility and in capacity. You can use your Cloud resources from wherever you are and you can choose to use it as much as you like.

### Speed to implement

No slower than you set up your Cloud services you are up and running. Business start-ups with brilliant ideas accelerate from nil to 100 virtual machines in a day. And 200 the next. And maybe 3000 the week after?

### Efficiency

From a global point of view, Cloud outsmarts all other solutions because resources are shared optimally.

### Cost reduction

With the Cloud there is no need for upfront investments in hardware, software and IT staff. You pay for what you use. So you can free up capital and can use it in another way.

Depending on your requirements the list of opportunities and advantages can grow or shrink. And maybe that is the biggest advantage of Cloud. Because so does your use of the Cloud.

# [introduction | common problems]

Of all barriers that Cloud critics can raise, security is the most heard of. You have to depend on your Cloud provider's security standards, or suffer the lack thereof. Yes, your corporate data seems easily accessible in the Cloud. But perhaps the average on-premise infrastructure is not much more secure, and only feels safer.
Less prominent is the fact that Cloud services, other than the easy to use SaaS solutions, demand for highly capable staff and continuous monitoring. And the Cloud is not that homogenous as one would wish, so for each and every new Cloud environment a new set of interfaces has to be developed. Let us investigate the common Cloud problems.

**Vendor lock-in**

Most vendors want you to use their Cloud; their specific implementation of a Cloud layer. There is no easy way to switch from one Cloud vendor to the other. If you want to change vendors you need to adapt to a new management interface to manage your Cloud applications; you have to adhere to a different security model, you have to use different storage structures and data access methods. Another critical problem for business is relying on a Cloud provider which might run out of business and you cannot escape easily this situation.

**Data control, transparency and monitoring**

Where's your data? Who owns it? Who else has access to it? Can you get it back? And can you monitor the performance of your Cloud service? For many organizations these are critical issues. A special problem is posed by legal issues. If you cannot control where your data is actually located, it may well be on a server to which foreign government officials have access.

**Reliability, availability**

Cloud availability is typically lower than what is offered by large data centres. Can you always access your Cloud services? Can your users? Even the largest Cloud providers occasionally have times their service is not available. And how redundant is your data. How soon can you recover?

**Security and identities**

How many different usernames and passwords do you have on the Internet? Probably too many. Cloud computing makes it even worse, because you need to get an "identity" on each Cloud service. Your identity needs to be secured. And your data needs to be secured too, since it is no longer protected by being on a local machine in your office. Security policies and identity management still are far from standardized in the Cloud.

**Service Level Agreements (SLAs)**

When your business depends on the availability of your applications and your data, you want to be sure you and your users can (nearly) always use it. However, Service Level Agreements (SLAs), for Cloud services are either non-existent or very basic.

**Difficult to set up and administer**

For a local machine in your office, your local system administrator knows what to do. IT is a relatively static environment. Providing services in the Cloud is much more dynamic. It requires a set-up that is more complex. The environment changes when the Cloud provider upgrades or changes his systems. System administration in the Cloud requires a different set of skills.

# [introduction | common answers]

Surely Cloud providers are eager to subduct the common obstacles for Cloud users. But the fact is: they are not that easy to tackle. So what are the common answers you get today when you ask for solutions to the common Cloud problems?

### Vendor lock-in

There is not a real answer to this yet. Some companies offer an interface to several Cloud providers. Advantage is that you can use resources from several Cloud providers, be it most of the time in a rather primitive way, but still: you get locked in by the company that offers the Cloud interface.

### Control your own data

Some companies now offer the service that they promise to store data in data centres in a specific region of the world, say Europe. However, this is not very fine grained, unless you go to a local data centre yourself, but then it is not the Cloud anymore, is it? Who really has access to your data often remains unclear.

### Service availability

For high availability, you have to pay more, sometimes so much more that it makes sense to either just buy your own systems or go to a regular data centre. Or you can choose several Cloud providers and distribute data and services by hand, taking care you always have a shadow service running. Which makes things rather complicated.

### Security

There is not much you can do about multiple sign-ons and security vulnerabilities. There are some efforts, like OpenID to move towards simplifying identity management, but it is all very much in its infancy.

### Monitoring

To know what is really happening with your services, applications and data in the Cloud, you need to set up extensive monitoring and notification services. Different solutions are available, but they come at a cost.

Cloud computing offers ample opportunities, but all in all, with current Cloud computing offerings the issues, problems and uncertainties impede many businesses in the adoption of Cloud technology. And that is where Contrail comes in.

# [introduction | contrail vision]

Contrail tackles a number of the problems in today's Cloud computing. As a result you will have access to a a Cloud environment as versatile as if it were your own data centre.

So, Contrail brings data centre versatility to the Cloud by developing a software stack that enables:

Vendor lock-in: **Federation**
Federation is at the heart of Contrail. Federation allows to combine services from different Cloud providers and use them as one federated set of services. You get to combine the best services.

Data control, transparency and monitoring**: Federated Identity management**
Identity management is federated. This means you only need one set of credentials, for instance a single username/password to use all the different services from the different providers. As a result security is also federated: a user may use his preferred means of identification, Contrail will translate it into the credentials a Cloud provider needs.

Service Level Agreements: **Contrail SLAs**
Services level agreements are federated. The user only has to express his service level requirements once. Contrail then decomposes and translates it to requirements that can be matched with individual resource providers' offerings.

Reliability, availability: **XtreemFS File system**
Availability of data and services is improved by using a reliable and distributed Cloud file system as basis of the storage.

Difficult to set up and administer: **ConPaaS**
The federated services can be packaged in an easy to use Platforms-as-a-Service. These platforms can use the complex federated Cloud, but the complexity is shielded from the user that only sees familiar platforms.

Difficult to set up and administer: **VEP Interoperability**
An interoperability layer is used to ease the management of the infrastructure and the deployment of the application.

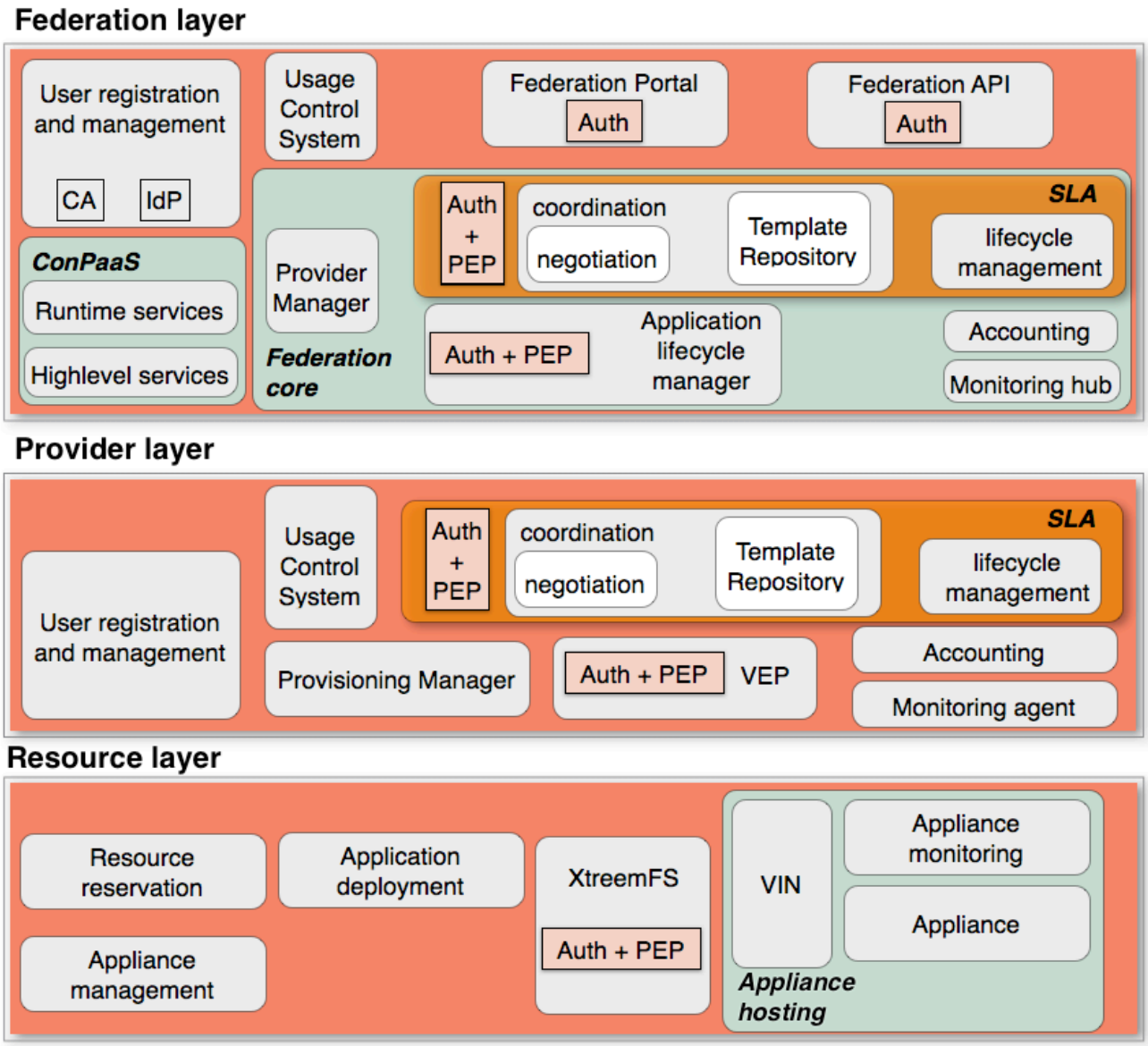
All these aspects lead to a federated Cloud in which you can put your trust. A Cloud that delivers what it promises; where your data is always available, and where you can choose the options that fit your needs and budget.

Contrail is delivered as open source software and supported by several service companies that can help you with setting up and maintaining Contrail based federated Clouds.

# [contrail architecture | system overview]

| Contrail component | What this component does | What you need before you can install it | How it fits in Contrail | Can be used independently from Contrail |
|---|---|---|---|---|
| Contrail PaaS (ConPaaS) | Platform-as-a-Service for web applications (Java, PHP), NoSQL, SQL, Task Farming, MapReduce. | Access to Amazon EC2 or a working OpenNebula cloud. | Builds on XtreemFS to store data and applications. Interfaces with the federation layer. | yes. |
| Contrail XtreemFS | Highly available cloud file system with policy-based customization e.g., to control the placement of data. | File system clients are available for Linux, MacOSX and Windows. Can also be used in Hadoop or directly through client libraries for Java and C++. | Can be used as a component at several levels, PaaS and IaaS, where reliable storage is needed. | yes. |
| Contrail Security | Federated support for identity management. Security for SLA support. | | Provides federated identity management for users and resources providers. Provides security at all levels of the federation. | yes. |
| Contrail SLA Manager | Definition of SLAs at federation and provider level. SLA-based provider selection / brokering. SLA monitoring and enforcement. | Cloud Federation, VEP. | Provides SLA definition, negotiation, monitoring and enforcement at all levels of the federated Cloud. | Yes, but the Cloud provider API must be adapted to the VEP's one. |
| Contrail VEP | Virtualized Execution platform. | IaaS infrastructure with resource providers using OpenNebula or other supported Cloud. | Virtualizes resource providers at the IaaS level and presents them to the PaaS level. | VEP can work as a standalone component. |
| Contrail VIN | Virtualized Infrastructure Network. | IaaS infrastructure with resource providers using OpenNebula or other supported Cloud. | It integrates (federated) IaaS resources of an application by providing a virtual private network. | VIN could be integrated in other Cloud solutions. |
| Contrail Federation | Integrates all components of Contrail into a single federated cloud. | Cloud providers. | Turns a number of individual Clouds from resource providers into a single Cloud. Allows users to execute services on this federated Cloud. | Federation is a core Contrail service, that can be used as a separate component by relying on SLA technology and the availability of suitable Cloud providers. |

# [contrail architecture | system diagram]



# [technology overview]

Contrail is a Cloud software stack of components that are designed to work together to combine a number of independent clouds into one integrated federated cloud. Users can for instance submit work to the cloud federation and let the federation decide to which resource provider it should be sent for execution. The placing is decided by means of Service Level Agreements (SLAs). The user can define the SLA for his/her work. The federation can split work, if possible, and split the associated SLAs, thus distributing the work over the resource providers that (best) meet the SLAs.

The Contrail Federation layer builds on top of the Virtual Execution Platform (VEP) layer. VEP provides an integrated standard view of the resources layer. It can be considered as a kind of virtualisation of a cloud.

The data in a Contrail federated Cloud are stored on a file system designed especially for the Cloud. XtreemFS, as this Cloud file system is called, can handle and distribute data on widely dispersed centres. It is designed for high availability, even in the case of not too reliable networks and data centres. Data can be placed in specific centres or specific countries, depending on the user requirements.

In a federated cloud, often different networks with different address and naming schemes are used. The Virtual Infrastructure Network component of Contrail combines these networks into one virtual network. This frees the user from the burden of configuring networks on different Clouds and adapting his applications to them.

Together, these components provide an Infrastructure-as-a-Service view of a set of federated Clouds to a user. In addition there is a Contrail Platform-as-a-Service component, called ConPaaS that provides an even higher level of abstraction. Here, typically an application developer can compose an application consisting of several parts, such as PHP, Java, SQL, NoSQL. The deployment is done automatically on the Federated Cloud by the ConPaaS software.

When one is using several clouds in one federation, managing the identity is important to the user and his applications: you do not want to login to five different Clouds all with different user names and passwords before being able to submit some work to the Cloud federation. Also the security of the user's actions and data and security of the providers and their resources needs to be respected. Contrail Security (ConSec) has been developed to handle this.

To demonstrate the use of the complete Contrail stack, it has been implemented in several use cases. One is available on-line as a fully functioning "Demonstrator". In these uses cases all the components work together with application specific software,

The Contrail stack federates existing Clouds that are built by Cloud management software. Contrail fully supports OpenNebula based Clouds and to some extent OpenStack Clouds.

ConPaaS can be used independently of the other Contrail components on top of Amazon EC2 too. Most other components of Contrail are designed in such a way they can be used in other settings outside a Contrail federated Cloud. Some are widely used already, such as XtreemFS, others are being deployed in recently started research projects.

Contrail components are available in open source.

# [contrail paas | conpaas]

ConPaaS, integrated runtime environment for elastic Cloud applications

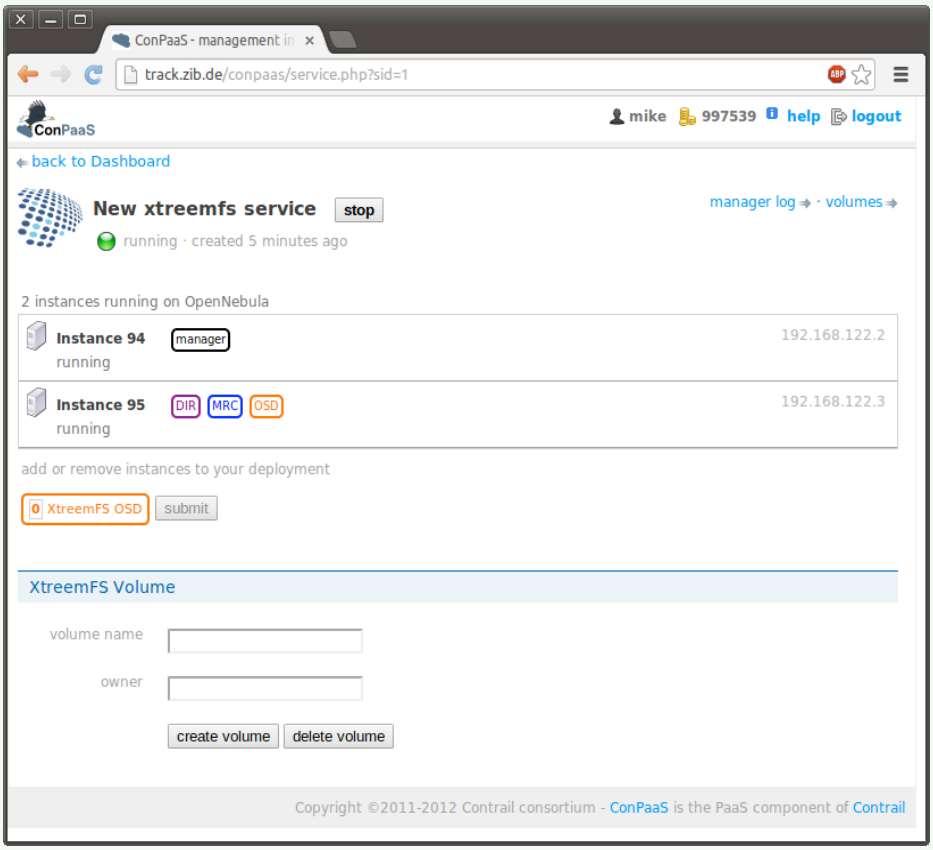
## Cloud issues addressed

When you have a new idea for an Internet based business, you need to write an application, make sure you have a database for transactions and other information, and a place to run it so your customers can access it. The “place to run” today is in the cloud. You can get virtual machines and manage them quite easily. But putting your application and databases in there can be difficult when you need many load balanced virtual machines.

So somewhere in the cloud lies an abundance of computer capacity. It offers both storage and computing power. It is available, scalable and right there for grabs. Or isn't it?

Well, it is, but it is not so easy to get your web application or service running in a cloud environment. Setting up and configuring your desired environment requires specialized skills and precise coding. And for each and every new infrastructure (on the web or elsewhere) you would need to adapt to different specifications. And once you're up and running comes the monitoring and maintenance. Let us face it: deploying your application in the cloud is rather complicated, time-consuming and costly.

That was before ConPaaS. The Contrail Platform-as-a-Service is an open source environment for easy application hosting in the federated cloud.




The Contrail web front-end

## Contrail Solution

Contrail's PaaS component provides a zero-configuration running and load-balancing of a set of applications and databases. You can compose your complex application out of these basic building blocks.

ConPaaS today runs on top of Amazon EC2 and OpenNebula based clouds and Contrail federated clouds. To use ConPaaS, you need to install the ConPaaS user portal only once. For EC2, ConPaaS AMIs are being provided, for OpenNebula clouds, VM images can be built easily following the provided scripts.

ConPaaS makes it really simple to get your application running in the cloud. Click a few buttons, actually specifying your needs, and you're on. Need more servers? You can add any number on the fly. And of course it's just as easy to scale down. ConPaaS is very simple to use and it makes 'your platform' totally scalable. And it is open source and thus extensible.
Contrail PaaS includes many components and services that can be used:

1. Generic ConPaaS components include:
- Web GUI
- Service core,
- Common functionality

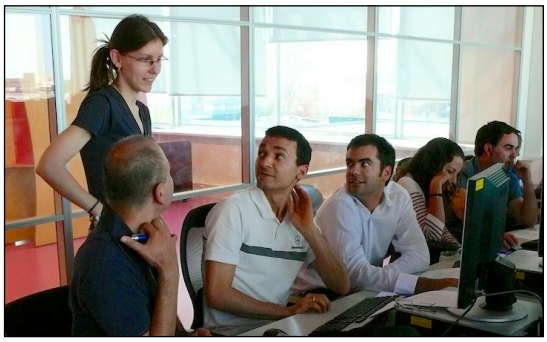
2. ConPaaS services include:
- Web hosting: static files, PHP, and Java Servlets
- MySQL database
- Scalarix key-value store (NoSQL database)
- MapReduce
- TaskFarming (Bag-of-tasks)
- XtreemFS files service

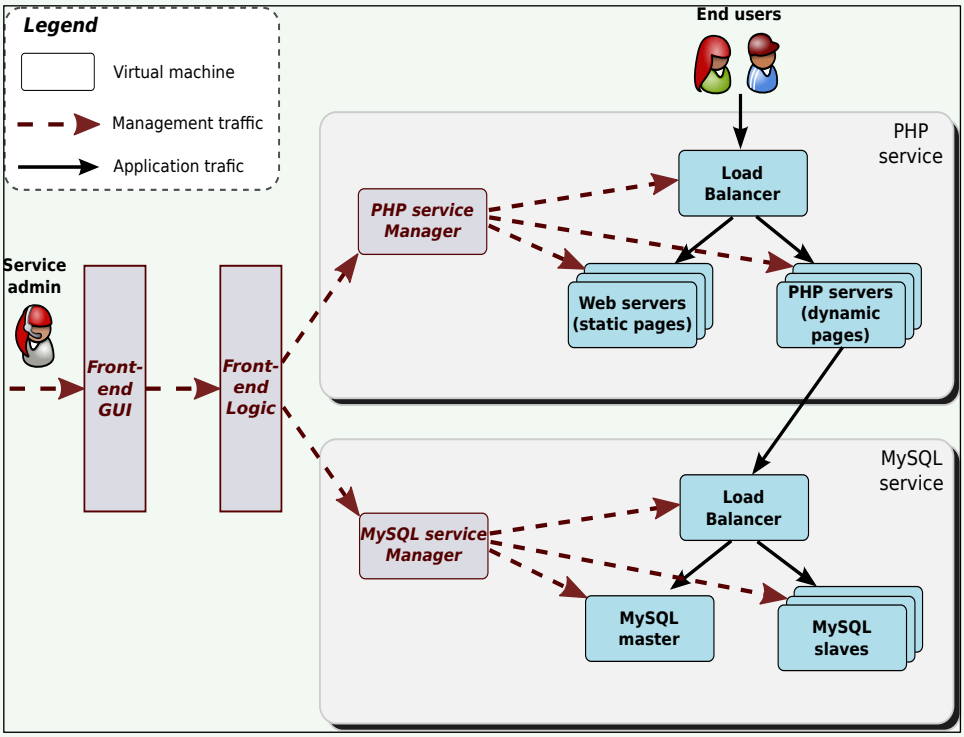

If more functionality is needed, one can develop new services and register them with the ConPaaS framework.

The MySQL and XtreemFS services allow for persistent storage. You can save and resume an application's configuration with manifests.

The ConPaaS functionality makes it suited for both web applications and HPC environments. For web applications all basic building blocks, including SQL databases and programming tools are present. As an example the implementation of a Word Press powered website is given.
For High-Performance Computing (HPC). the task farming service (Bag-of-Tasks) and the Hadoop data service provide building blocks for high-throughput applications.

The PaaS services managed by ConPaas can be enforced by SLA agreements. This provides elasticity and resource provisioning to guarantee performance at lowest possible cost.






ConPaaS web application architecture

ConPaaS is fully integrated with the XtreemFS Cloud file system. ConPaaS can be used to manage an XtreemFS set-up. In summary:

1. The ConPaaS Service
- Creates and manages XtreemFS deployments in the cloud
- Easy to use web-frontend

2. Features of ConPaaS XtreemFS management
- Manage DIR, MRC and OSD nodes
- Dynamically scale XtreemFS by adding/removing virtual machines as needed
- Volume management
- Policy management
- Replication
- Replica Selection
- OSD Selection

## More information

ConPaas information on the Contrail portal: http://contrail-project.eu/conpaas
ConPaaS online is an online public test bed. It is free to test for everyone: https://online.conpaas.eu
For the latest ConPaaS developments and downloading the public domain software: http://conpaas.eu

# [contrail xtreemfs]

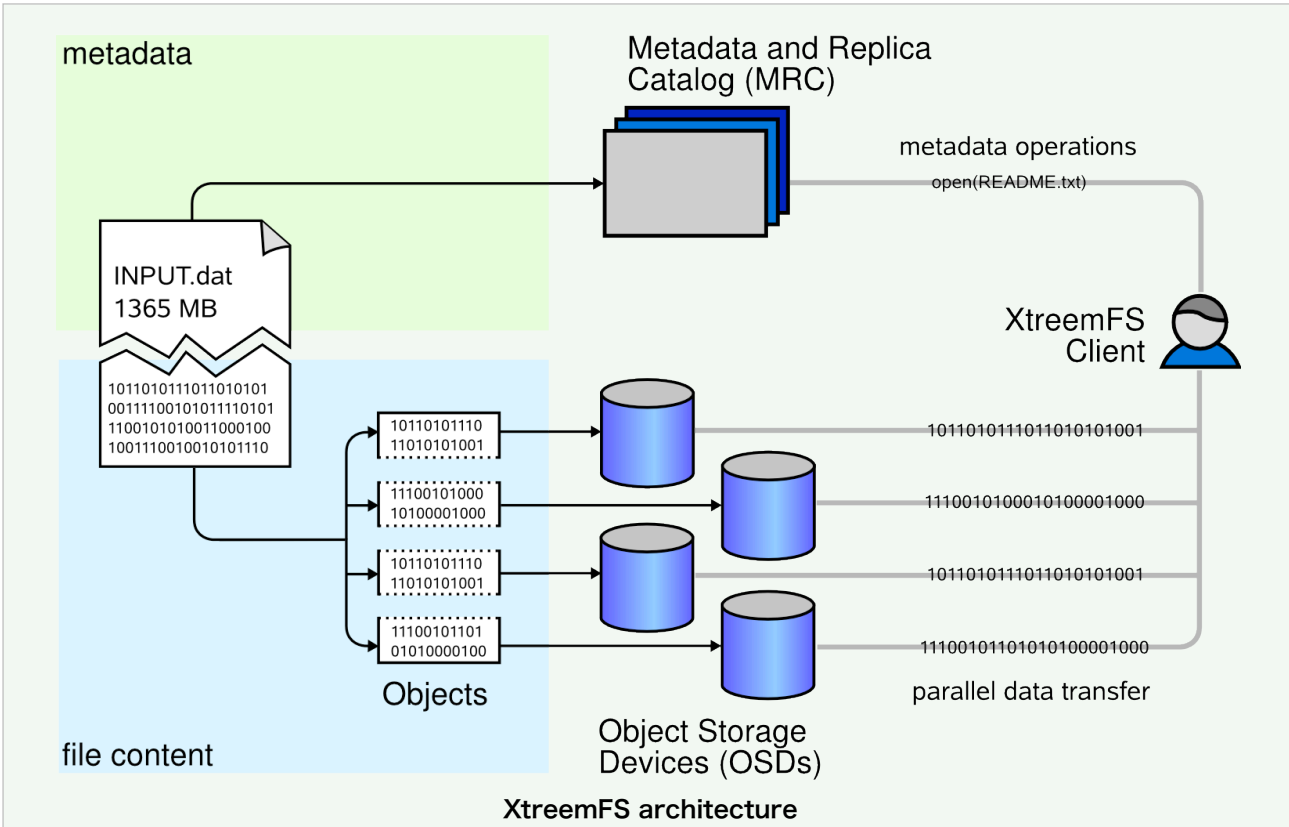
A distributed and replicated file system for the Cloud

## Cloud issues

Cloud computing is distributed computing. This requires seamless integration and availability of data in many (physical) places. For users the seamless and fast access part is important. For data providers, protection of data and providing the right levels of access counts. For infrastructure administrators, manageability of data and infrastructure is important. But overall it is reliability that counts: despite the distributed nature of the storage and the sometimes unreliable Cloud and networking infrastructure, the data has to be there when the user's application needs it. And it has to stay available when the application is active, even if some networking nodes or file servers crash.

## Contrail's Solution

Contrail's file system, XtreemFS, is a secure and fault-tolerant file system for the cloud. It has been designed to store peta-scale data volumes across large numbers of distributed servers, while it behaves like a local file system with POSIX® semantics from a user's point of view.




XtreemFS architecture

XtreemFS has been specifically tailored to the use in cloud computing environments. The modular design makes it possible to start with a small-scale installation and scale it out when necessary. Its integrated security infrastructure allows to share storage resources between multiple users in a secure and isolated manner. Replication ensures availability and safety of all data at any time.

One of the core features of XtreemFS is its ability to replicate files over WANs while guaranteeing their consistency. Replication algorithms are designed for dealing with large latencies and complex failure scenarios like network splits. Storage servers are aware of the state and recency of the files they store.

XtreemFS offers different kinds of replication: Read-only File Replication and Read-Write File Replication; and it has features for Replica Placement and Selection.

Read-only file replication provides an efficient mechanism to distribute large volumes of write-once data in a CDN-like manner. Data transfers are performed asynchronously between all replicas using peer-to-peer mechanisms. This allows replicas to be accessed while they are created, and allows to prioritize the transfer of important parts of the file to the new replica.

Read-write replication ensures strong replica consistency without write-once restrictions. Internally, it resorts to a primary backup scheme with automatic primary fail-over. Read-write replication ensures that files can be read and written as long as a majority of all replicas remain available.

Metadata Replication: Since metadata and file content are managed separately in XtreemFS, metadata is replicated independently. Metadata replication ensures safety and high availability of metadata in the event of downtimes of metadata servers.

The placement and selection of file replicas in XtreemFS is policy-driven. Users can define policies that restrict the creation of replicas to certain servers. Similarly, policies define the preferred order in which clients attempt to access existing replicas.

In addition to this core functionality, XtreemFS offers a wide range of additional features:

- Striping: XtreemFS can spread chunks of a single file across multiple storage servers, thus increasing throughput when accessing large files.
- Client-side Metadata Caching: XtreemFS clients can maintain a local metadata cache to ensure low-latency access to metadata.
- Snapshots: XtreemFS can record consistent snapshots of volumes.
- Checksums: Storage servers are capable of calculating and verifying checksums whenever data is read or written, so as to detect corruptions of file content.
- Hadoop Support: XtreemFS can be accessed by Apache Hadoop applications through an HDFS adapter.
- Monitoring: XtreemFS installations can be easily monitored with third-party monitoring tools like Ganglia and Nagios through an SNMP-based monitoring service.

Some examples of use cases for XtreemFS are efficient storage and distribution of VM images and storage of Cloud user data.

For efficient storage and distribution of VM images XtreemFS provides the scalability to accommodate vast amounts of large virtual machine images for a cloud. Immutable VM images can be replicated to multiple sites in a particularly efficient manner, which allows different clients to access different replicas in parallel, thus balancing load and reducing startup times of distributed cloud applications. Also images with copy-on-write (CoW) format, which have a static part are supported.

For storage of Cloud user data there are many cloud storage solutions - but only few provide POSIX file system semantics! Ideally, users can run their applications on a cloud without major modifications. XtreemFS provides the same guarantees as a local file system when files are accessed, even if accesses are directed to different replicas. Furthermore, XtreemFS can use a shared pool of storage resources for the data of many different users while protecting the interests of individual users in terms of privacy and isolation.

There are several features that make XtreemFS specifically suitable for Cloud computing environments. One of them is XtreemFS' POSIX® compatibility that provides the same interface and operation semantics as a common local Linux file system. Applications can thus use XtreemFS without having to be adapted to a specific storage subsystem.

XtreemFS supports elasticity. Servers can be easily and dynamically added to an XtreemFS installation in order to increase storage and I/O capacity of the file system. This can happen at any time without having maintenance downtimes. Newly added servers are immediately integrated in the system.

Data safety is inherent to XtreemFS that provides robustness in the event of storage device failures by means of replication. Maintaining multiple replicas of files and metadata ensures data safety even if underlying storage devices take physical damage.

High Availability makes it suitable for larger environments. In peta-scale storage installations, hardware failures and downtimes are the norm rather than the exception. XtreemFS transparently resorts to available replicas of files and metadata if individual servers become unavailable. XtreemFS supports off-site replication over wide area networks to ensure availability even in the event of downtimes of entire data centres.

XtreemFS comes with an integrated security infrastructure that protects data from unauthorized access. SSL connections ensure that data transfers between clients and servers are encrypted. X.509 certificates enable a secure authentication of individual users. POSIX® permissions and ACLs provide the basis for a fine-grained access control to different data volumes.

Extensibility is a last feature that makes XtreemFS Cloud ready. Most behavior in XtreemFS can be controlled by means of policies. Examples are authentication and authorization of users, placement of files and replicas, and selection of replicas. In addition to using predefined policies, XtreemFS offers a plug-in mechanism to support custom user-defined policies.

XtreemFS is available for Linux (openSUSE, SLE, Fedora, CentOS, RHEL, Mandriva, Debian, Ubuntu, Gentoo), Mac OS X and Windows.

## More information

XtreemFS information on the Contrail portal: http://contrail-project.eu/xtreemfs
For the latest XtreemFS developments and downloading the public domain software: http://xtreemfs.org

# [contrail federation]

## Cloud issues addressed

Today's Clouds all run in isolation. Combining services from several clouds has to be done by hand, by writing scripts that are difficult to maintain. Credentials have to be entered many times, as each Cloud has different authentication procedures. Combining different services automatically would give flexibility to users to customize the Cloud according to their business needs.

Both Cloud providers and their users would really be pleased to use the cloud with one identity, having Cloud capacity made to measure, dynamically scaled to suit the tasks and with automatic SLA management. And it would drastically boost the use of cloud solutions.

But it can't be done yet. It's not a homogenous Cloud we're dealing with. The Cloud is as versatile as you can imagine. Deploying the current Cloud needs customization to various providers and users unavoidably get entangled in commitments to particular providers, that lock them in for strategic purposes. Within the context of evolving Cloud technology this market situation impedes the desirable evolution to a common, integrated Cloud.

Ideally, one could merge all Clouds, allowing for individual providers' business models and yet coordinate SLA management provided by single Cloud providers. It would be a federated Cloud and it is at hand.

## Contrail's Solution

Contrail enables interoperability amongst Cloud providers. The best provider for the job, according to the requirements and type of application, is dynamically chosen and for any one job, providers can be combined. Operations can be migrated, scaled and secured. And with all this the Contrail federation also handles SLA management. Contrail turns multiple heterogeneous Clouds into one federated Cloud that can be exploited as a single Cloud.

Contrail federation provides the following functionality:

- Dynamical match between job and provider(s)
- Deployment in time and at runtime
- Allowing provider collaboration
- Migration and elasticity
- Security and privacy framework
- Quality of Service: Minimal SLA support
- SLA, Quality of Protection and other
- Provider selection and integration
- Enforced mechanisms
- Interoperability
- Federation as a mediator and a 3rd party for security and SLA management
- Basic adapters for XtreemFS, SLA, VEP and VIN.
- Runtime state watcher image manager - complete version
- Complete SLA support
- Complete adapters for: SLA, XtreemFS, provisioning manager (PM), and VIN full PaaS support

Federating the Cloud with Contrail will lower the barriers for Cloud providers, big or small, and Cloud users alike and greatly improve usability and reliability.

# [contrail | sla manager]

## Cloud issues addressed

The growth of cloud providers in the last few years, both in terms of number of players and of differentiation of offered services, forces companies to deal with a not trivial selection problem. Ever existing cloud brokers don't offer an effective solution to the issue of identifying the ideal cloud provider for each application of their customers.

Different cloud providers may have different interfaces to specify requirements, and not all of them provide automatic quotation for a required user configuration. Interacting with different providers by hand to find the best and cheapest one for a given application is a complex and time consuming task.

## Contrail's Solution

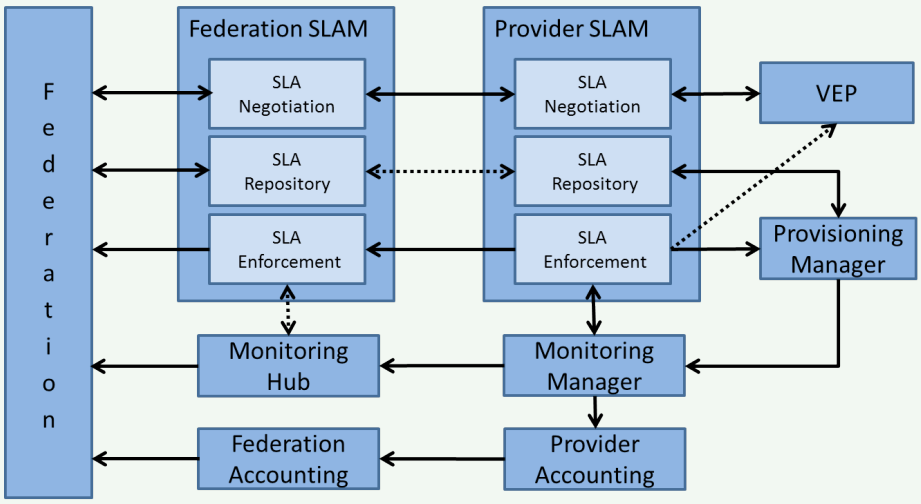
The Contrail federation SLA Management layer automates the provider comparison and selection task and hides to the final user the complexity of interacting with multiple cloud providers.

The Contrail SLA Management layer allows expressing user requirements about application Quality of Service (QoS) in a uniform way. The same SLA syntax is used by all cloud providers in the federation, enabling it to negotiate with and to compare multiple providers. To enable negotiation interoperability of different cloud providers with the Contrail federation, a SLA Management layer is added to each provider. Contrail SLA Management is based on SLA@SOI and extends it by integrating with Open Virtualization Format (OVF): a pair OVF-SLA is used to describe the application.

SLA terms that are supported by Contrail include specific characteristics defining the configuration of each VM, such as the amount of memory or the number of virtual cores, but also terms related to application setup, such as the possibility to reserve resources; there are terms affecting performance, such as the possibility to co-locate in the same physical host different VMs that must exchange large amounts of data, and even terms important at a legal or privacy level, such as those defining the geographical location of resources.

## Features

- SLA template repository
- Automatic multi-step SLA negotiation
- SLA-based provider selection
- SLA monitoring and violation detection
- Support for defining enforcement rules
- Geographic and security-level SLA terms
- Reservation and VM-placement SLA terms
- Support for elasticity / automatic scaling




Contrail Multi-level SLA Management architecture

# [contrail security | consec]

Federated Cloud security and federated identity management

## Cloud issues addressed

Security forms an important part of the Contrail Cloud infrastructure software stack. This is partly to address existing general security concerns in distributed collaborations, such as for a resource provider: "how do I know who my users are?", or for a user: "how do I protect my data against being modified/ stolen?", or concerns specific to the Cloud, such as "how do I know where my data is?" and "how do I know I can trust the provider?". Most commonly a user's identity has to be known to the resource provider in a way it allows him to determine whether to grant access to resources or not. In a federated Cloud, each resource provider can have his own set of identity checking rules and tools. That rather complicates things.

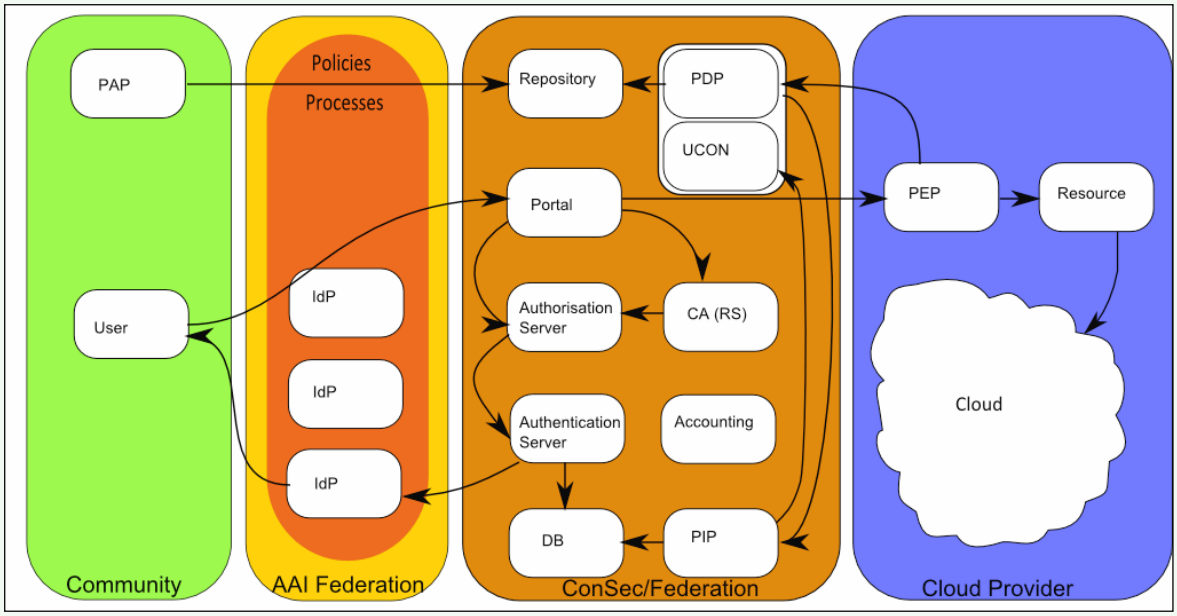
## Contrail's Solution

The aim of Contrail Security (ConSec) is to provide a means for users to use external identities to authenticate to service providers: any acceptable external identity can be used to identify users to any internal service managed by the federation.

The user thus gets single sign-on: an identity used for other purposes can be used with any federation resource, and, depending on the timing and technology used, he will only need to log in once.

The advantage for the federation operator is that they do not need to worry about allocating (and resetting) user passwords and keeping account records up to date. Finally, the resource provider gets at least an extra level of assurance, that authentication data used by the user for other resources is less likely to be shared with other users, and may even be subject to federation policies.

The diagram below, at a high level, sketches the advantages of ConSec (the third box ). From left, we have the user's community, either based on a Contrail use case or another collaboration in another project, the role the user adopts when making use of cloud resources.




ConSec federated security architecture

The yellow box denotes the identity management federation, wherein acceptable use policies are defined, and identities are managed. In the simplest case, it could just be a single identity provider, such as a public cloud or social network identity.

In the more complex cases, they could be a full national identity management federation with rules and processes, and the IdP would be provided by the user's employer or university, thus providing a high level of assurance. ConSec is able to simultaneously manage credentials at a different level of assurance, passing the information to the resource.

The third box is ConSec itself, which is managing most of the complexity of the authentication and authorisation; and finally, the fourth box represents the resource, with enforcement of access control and access to the resource as well.


One thing is solving problems for Contrail, another thing is to provide reusable and sustainable code which solves problems for others as well. Like many other parts of Contrail, ConSec aims to be modular, so components can be replaced, left out, reused, upgraded, etc. Indeed, ideally ConSec would provide a framework which enables any e-infrastructure provider to make use of federated (i.e., external) identity management. Whenever possible, ConSec itself is built out of standard components using standard protocols.

In practice, multiple technologies are combined to solve problems. The user's initial interaction with the service is via a portal, and authentication is usually web-based, using either OpenID or SAML SSO (such as Shibboleth).

Within the federation, everything is SOA, and REST web services are used. In order to carry authorisation information with the HTTP headers, we use OAuth2 to delegate the rights to access federation-level services on behalf of users.

The portal will then typically choose to create an X.509 certificate which it manages on behalf of the user: this is because the OAuth2 access token carries little information, because services are not in general web services based; because not all services can validate an access token; and because we need more fine grained authorisation data.

The users generally never see the certificate, but it is used to access services on their behalf, and the embedded authorisation assertion is used to check the access control via a standard XACML framework. Contrail moreover has implemented an extension to the PDP, called UCON in the diagram (for "usage control") which can re-evaluate an access control decision when the values of attributes change.

If the decision also changes, the PEP is notified of the change, and can suspend or terminate cloud activities. This is useful for "volatile" attributes, such as reputation and the remaining funds in prepaid accounts.

# [contrail virtual execution platform | vep]

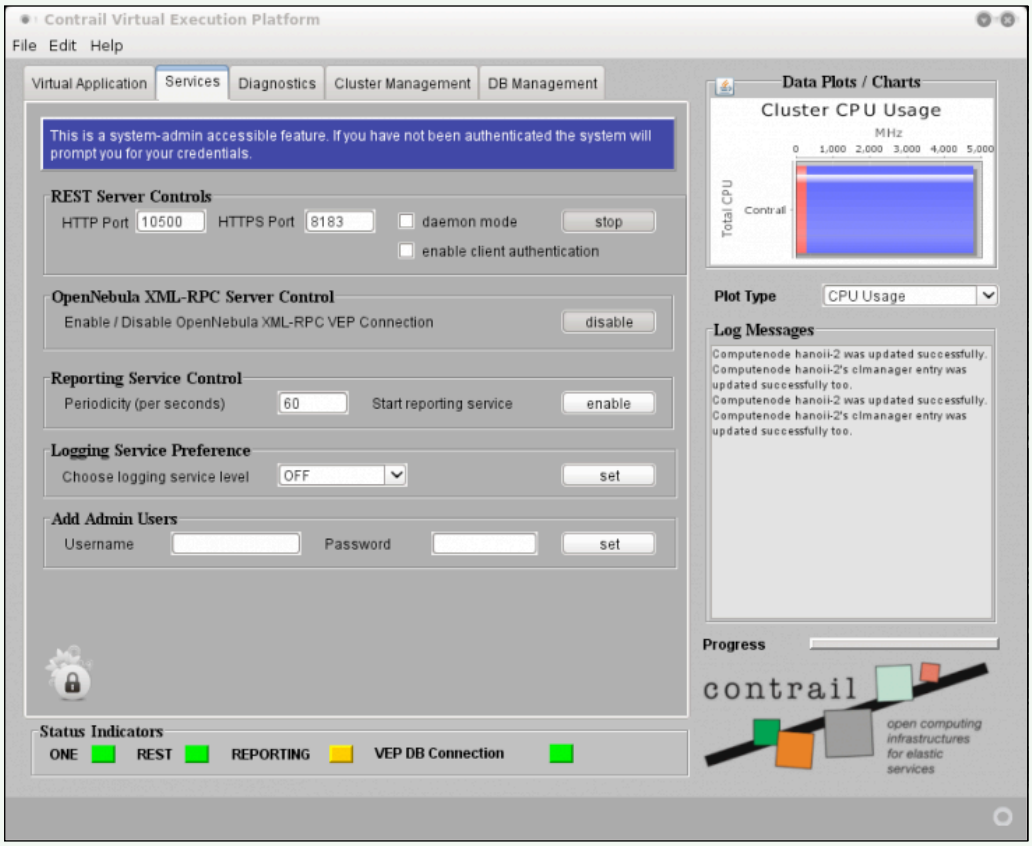
## Cloud issues addressed

A typical Virtual Execution Platform uses open standards, provides support for SLA negotiation and elasticity via advanced reservation and also provides monitoring data to higher level services. It manages computational resources in the Cloud(s), integrates both file storage and remote client machines.
VEP provides the proper means for interoperability and easy management of the resources at the IaaS level, hiding all the complexity. Moreover it is SLA aware and it is an important component to deploy application requirements.

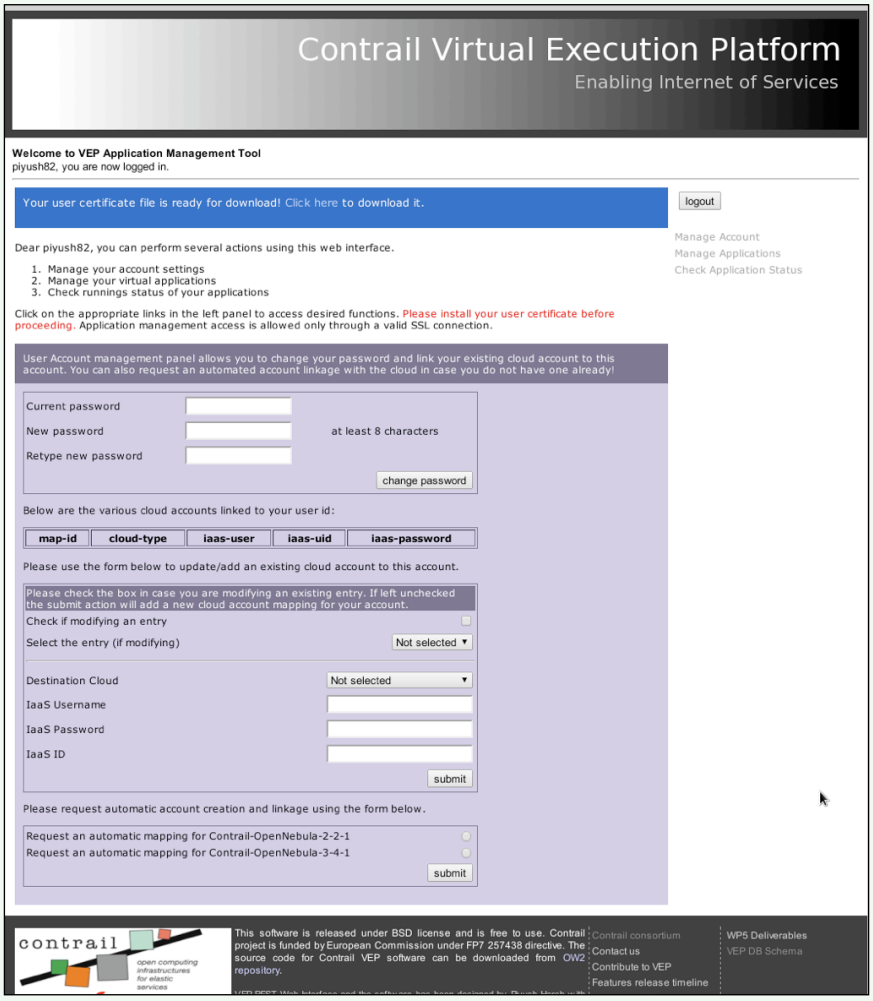
## Contrail's Solution

Virtual Execution Platform (VEP) is a software that links the cloud provider's computational resources to the Contrail (or any other) cloud federation. It is a key software component that enables the provider's participation in the federation and allows the federation to provision resources for deploying end-users' cloud applications.

VEP is a cloud middleware software that interfaces multiple Infrastructure as a Service (IaaS) clouds and presents end-users with an interface facilitating easy deployment and application life cycle management of distributed applications made up of several inter-networked virtual machines.




VEP can manage multiple Clouds




**VEP management interface**

Applications to be deployed are described using DMTF's Open Virtualization Format (version 1.1.0) standard. The software allows the deployment of any standard OVF application and full lifecycle management of the application after deployment until its termination on the provider's cloud.
The software can also be used independently. It provides a simple yet feature complete REST api to enable ease of development by any cloud application developer.

Standards and interoperability support includes:

- Interoperable hardware resource provisioning via a simple interface (GUI or CLI)
- Open Virtualization Format (OVF) support for application description
- Cloud Infrastructure Management Interface (CIMI) for managing the Cloud infrastructure
- Forthcoming OCCI support for IaaS interaction

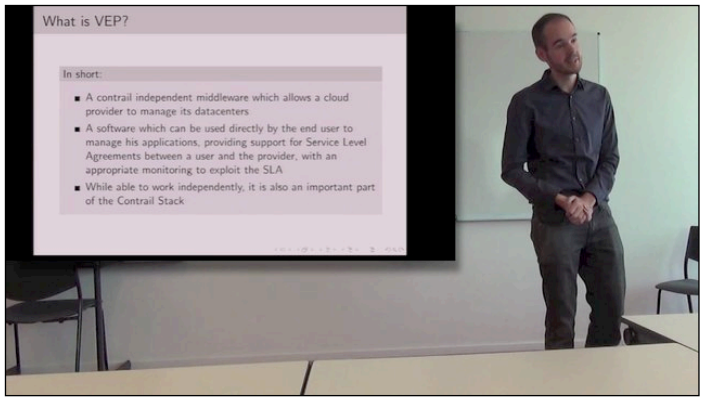
VEP offers administrators of data centres, a GUI to configure available IaaS resources, define data centre structure, and manage users. The data centre structure is exploited by VEP to enforce placement constraints on the resources before application deployment. Administrators can monitor resource usage and users' consumption.

There are several innovative aspects of VEP when deploying distributed applications in IaaS Clouds. Quick deployment is one of them: users only need to submit an OVF document describing the whole application, then VEP is in charge of allocating resources and initialize the application.
VEP can also take care of advance reservation: VEP can negotiate the availability of the resources explicitly requested by the users before application deployment. VEP is SLA aware: users can specify constraints on physical resources (ex. placement, type, size,...) which can be negotiated based on their availability in the data centre. Elasticity is also supported by VEP: adding or removing VMs is easy by submitting new requests or can be enforced by SLAs. Portability is resulting from VEP that hides the complexity of heterogeneous IaaS Clouds.

VEP can also work together with XtreemFS to manage remote storage.

In summary, VEP is available in open source and follows open standards:

- Under new BSD license
- IaaS supported: OpenNebula
- It follows the the DTMF, OVF and CIMI standards
- Coming soon: OpenStack and Amazon EC2
- VEP includes an OAuth client to retrieve a delegated certificate to use inside the created VMs




## More information

VEP information on the Contrail portal: http://contrail-project.eu/vep
For the latest VEP developments and downloading the public domain software: https://project.inria.fr/vep/

# [contrail virtual infrastructure network | vin]

## Cloud issues addressed

In today's Clouds, hardware systems are virtualized into Virtual Machines (VMs). The networking addresses for these Virtual Machines are provided by the resources providers, e.g. the Cloud providers. When federating multiple resources from multiple Cloud providers, also the networking has to be abstracted - virtualized - as do the resource providers. An important feature is the isolation and compartmentalization of the applications.

## Contrail's Solution

VIN integration in the Contrail software stack serves as enabler for other Contrail components. It virtualizes the network and the resource providers, generating a virtualized infrastructure.
The Virtual Infrastructure Network allows authenticated and encrypted communication via IPSec and the possibility to choose the level of protection. Virtual networks are dynamically created per user/application and contain a control network. Also the VIN serves within a Cloud and extends to other infrastructures (for Cloud federation), to a global cloud file system (Contrail XtreemFS), and to external machines.

- Integration with VEP,
- XtreemFS,
- security prototypes

VIN is an integrated part of the Contrail infrastructure, connecting virtual machines under control of VEP and the Contrail security services, with XtreemFS and external machines.

# [summary overall contrail stack]

## Contrail current release

Contrail has been developed over three years. There have been several releases over those years.

The latest additions to the Contrail stack include:

- Support for external Identity Providers (for example allowing login over Google)
- Support for SAML (exchange of attributes during login)
- Support for OAuth2 standard (securing API with OAuth tokens between the component calls)
- Authorization Server (fine grained control of token usage for the users and administrators)
- Dynamic-CA (for temporary services such as software defined networks or SDNs for applications)
- Bug fixes of existing components

The Contrail stack provides the building blocks that enable fine-grained security and which are used in the final release of the Contrail platform. The developers demonstrate the usage of external Identity Providers with a Single Sign On (SSO) feature and the usage of OAuth tokens.

| Contrail component | Latest release highlights |
|---|---|
| Contrail PaaS (ConPaaS) | Platform-as-a Service for Web applications (Java, PHP), NoSQL, SQL, Task Farming, MapReduce. MySQL Cluster and integration with VEP and VIN. |
| Contrail XtreemFS | Cloud high availability file system. With localization based storage. No single point of failure anymore. Integration with Hadoop and a Windows client. |
| Contrail Security | Federated support for identity management. Security for SLA support. |
| Contrail SLA | Definition of SLAs at federation level. Monitoring of SLAs. SLAs available with support at the provider level. |
| Contrail VEP | Virtualized Execution platform. OCCI based REST interface. |
| Contrail VIN | Virtualized Infrastructure Network. |
| Contrail Federation | Integrates all components of Contrail into a single federated Cloud. Integrated with Contrail PaaS. |

# [contrail usage overview]

Since the Contrail platform is a basic software infrastructure, it is difficult to directly show its potential stand-alone. Hence we developed use cases that illustrate the use and benefits of several components and the complete Contrail stack.

The Contrail Use Cases are the reference applications that have been developed and deployed on the Contrail framework, in order to evaluate, test, and demonstrate the full set of technological features and functionalities developed in the research part of the project. The selection of the use cases has been driven by scientific, technical and business considerations. Factors that have been taken into account, include heterogeneity of market scenarios, complementarities of the sectors addressed, and relevance at both industrial and scientific level.

Additional effort has been done to further expand one of the use cases - a Multimedia Marketplace - into a large, full scale market oriented "Demonstrator" that is fully open to final users. In that real production scenario, almost all critical aspects of the technology developed by Contrail have been tested under heavy load conditions, and information on performance, scalability, security, and usability issues has been collected and reported.

The demonstrator environment has been set up and linked from the Contrail public portal, where interested users can find relevant information, run the Demonstrator Use Case and could fill in an online questionnaire regarding quality evaluation, thus providing the opportunity to collect feedback from early adopters, in general from all people, including content and technology providers that have access to the environment and can participate in installing, configuring, and deploying Contrail components.

In addition to the use of Contrail components by the project itself in the use cases, there is also uptake by organisations outside Contrail. Examples are security components that are used in the European e-Infrastructure that supports eScience, and use of components in recently started R & D projects.

# [demonstrator | multimedia market place]

## Problem addressed

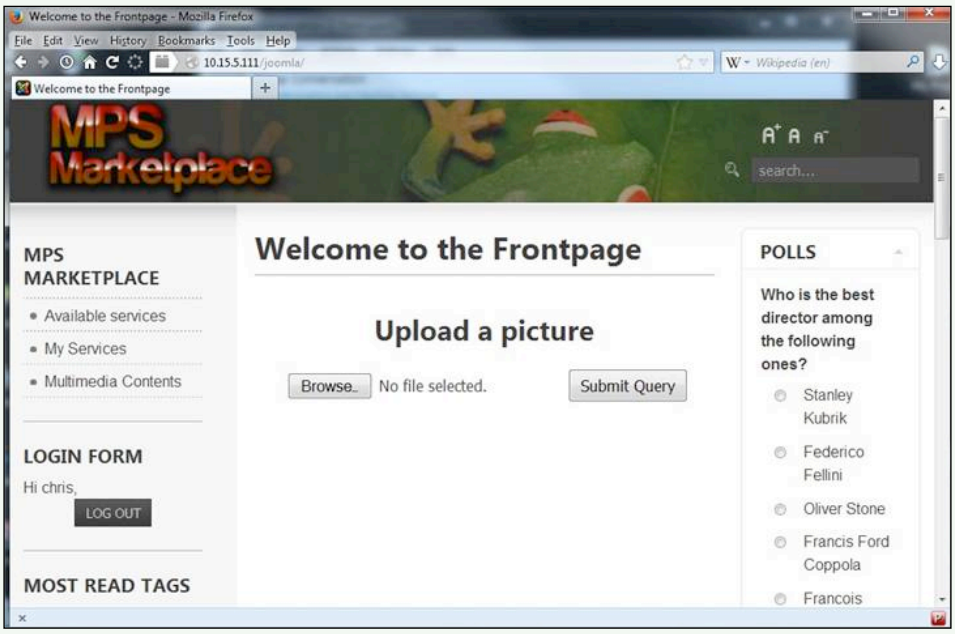
Online buying of multimedia content, like movies and audio, is common use today. Mostly this is done through stores. But these are rather limited. Search facilities for the user are limited to key words or simple browsing; moreover, tags manually assigned to contents are often not reliable, thus further impairing the precision of search results. While Query by Humming technologies are being successfully used in some music marketplaces, Query By Image Content technologies (used for instance in many simple free reverse image search engines) haven't been widely applied yet for improving the internal searches of Multimedia Marketplaces, in particular for videos.

From the multimedia providers' standpoint - regardless the existence of advanced content search services offered to their customers or not - the problems to be addressed in the application deployment concern scalability, elasticity, performance, security, and reliability. Deploying a multimedia service on the cloud is a clever option in order to satisfy the need of elastic and scalable resources, and together it also offers all the benefits of a pay per use model (no investments in infrastructure), but current cloud IaaS aren't a solid solution for other critical issues: reliability of the storage and of the running instances, overall security of the infrastructure, and quality of service.

Finally, a dynamic multimedia market place can interact with Content providers, offering pure multimedia contents, and Technology providers, offering adaptation and transformation services. While Content providers need trustable storage infrastructures to preserve their data, because their business comes from the commercial value of the contents they sell, Technology Providers need most of all computing power, so their major requirements are for elasticity, CPU performance and quality of service.

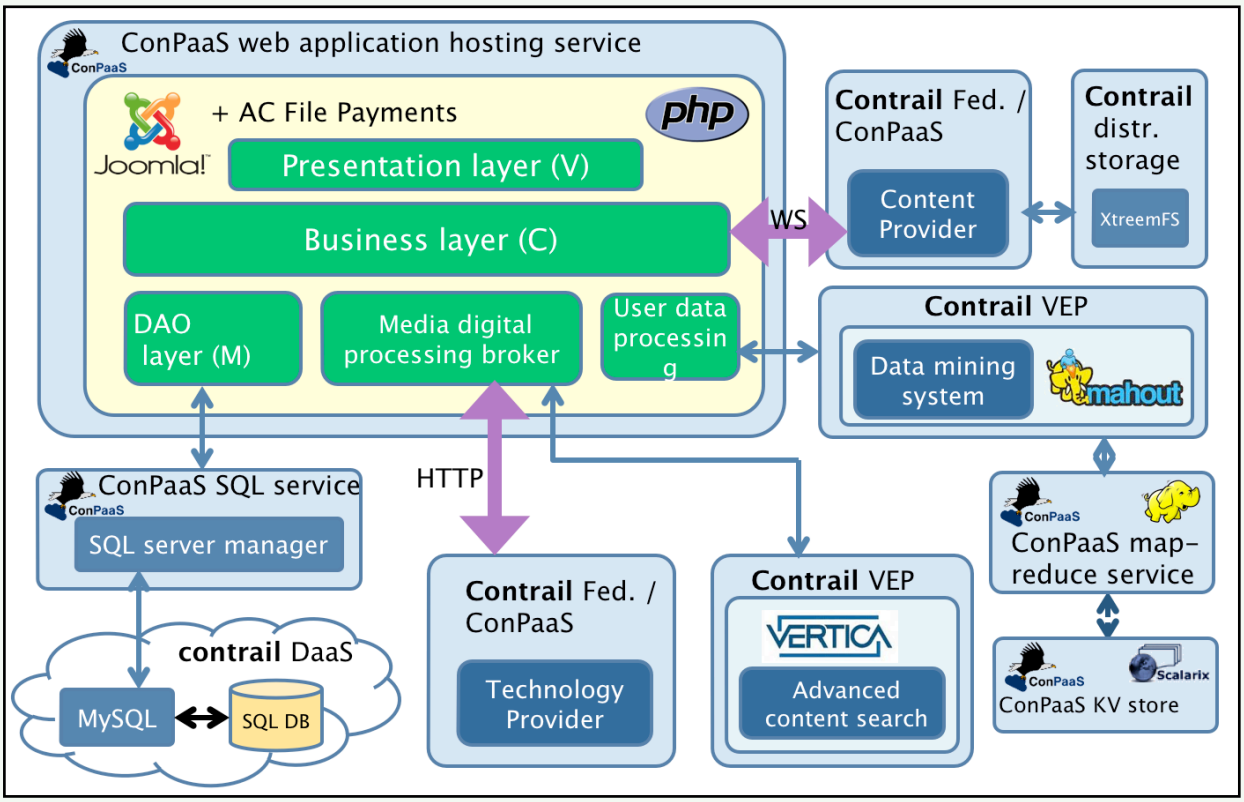
## Contrail's solution

Contrail technology enables the implementation of a dynamic multimedia market place. It will use the Contrail Federation components to allow Content and Technology providers to interact with each others' offerings, providing aggregated and focused content to a user. Contrail XtreemFS will assure the availability




Contrail Demonstrator: view of the Marketplace front page

of content for all the providers involved. Reliability of applications will be guaranteed by ConPaaS and VEP. These aspects, and more, will be negotiated and enforced by a SLA component. Contrail technology wil also be used to implement more advanced and refined search methods for the users, in particular MapReduce will be used by the data mining component responsible for content proposition purposes and VEP will support the scalability needed for demanding software in computational terms, such as face recognition processes inside videos.




**Contrail Demonstrator: overview of the Architecture**

The multimedia market place needs to be elastic and scalable. The market place is expected to grow. This requires an automatic scalability of all its services and components. Contrail PaaS can enable platform elasticity. The Marketplace and the technology providers can use elastic MapReduce services.

Contrail allows a real dynamic market place to be put in place at lower costs. It will allow multimedia technology providers to sell their services immediately without the need to invest in development of final products accessible by end users.

Similarly, content providers will be able to focus on their core business (contents), preserving their data in reliable storage services. Reliability will involve not only storage but also virtual machines, and proper SLAs will allow enforcing this important requirement for all the providers.

In the real production scenario, almost all critical aspects of the technology developed by the Project have been tested under heavy load conditions, and information on performance, scalability, security, and usability issues has been collected and reported so that corrective actions and fine tuning of the Contrail framework can be accomplished. The Multimedia Marketplace has been chosen as the “Demonstrator”.

A Demonstrator Environment has been set up and linked from the Contrail public portal, where interested users can find relevant information, run the Demonstrator Use Case and fill in an online questionnaire

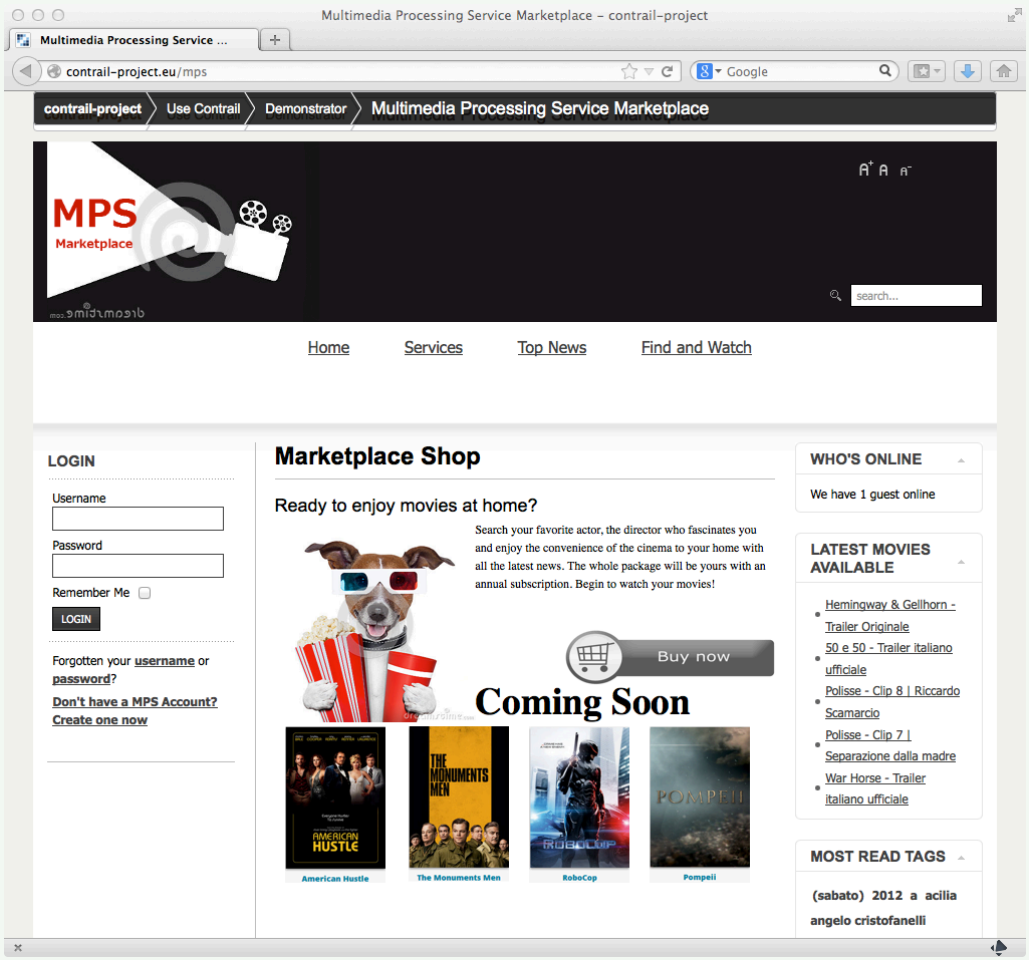
regarding quality evaluation, thus giving chance to collect feedback from early adopters, in general from all people, including Content and Technology Providers for the selected Use Case, that have access to the environment and can participate in installing, configuring, deploying Contrail components.

## Benefits of using Contrail

There are several benefits for using Contrail in this case. Resiliency and distribution of multimedia contents spread through different clouds will be easily managed and enhanced with the use of XtreemFS features.

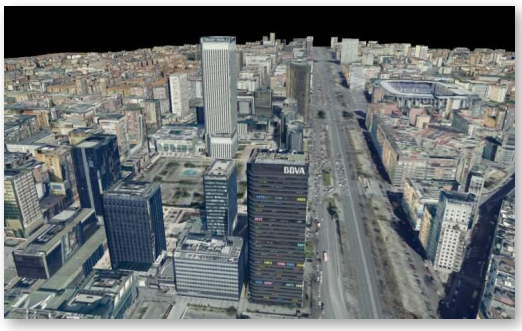
Protection of data is guaranteed not only by (QoP) rules, but also because all data channels are encrypted to preserve confidentiality, with the ability to enforce location on users' data, thus satisfying legal constraints on data storage, such as geographical location.

Finally, this solution enables interoperation of Contrail clouds with OpenStack based clouds, which is a de-facto standard worldwide with thousands of working instances, in this way providers that already manage OpenStack infrastructures can easily join the Contrail federation.



# [use case | distributed provision of geo-referenced data]

## Problem addressed




Map sites are among the most popular services available on the Web today: people use them for locating places, planning trips, finding points of interest and so on. Maps would be even more useful if they could be augmented dynamically with all kinds of location specific data, so the map user can make his specific selection and combination. This data can be provided by many different data providers. Although there are some map providers that offer access to data providers, they mainly are located outside Europe and use closed source platforms. Hence there is a need for a European based open source platform for geo-referenced data. However, the use case does not use open source technology only and it is not bound contractually to use it.

## Contrail's solution

The Distributed Provision of Geo-referenced Data implements a 3D Virtual Tourist Guide (VTG) through Web access to interactive digital maps and geo-referenced multimedia content.
Users can zoom maps on a specific area of the globe and visualize them at different levels of detail, depending on available detailed information about the region. Layers can cover the territory partially or completely.

Added value is given by Points Of Interest (POIs) related to tourism (like hotels, restaurants, museums), historical information about monuments or places, weather forecasts, images shared by users, etc.
The Virtual Tourist Guide service relies on the concept of Federation offered by the Contrail framework. It enables an open and distributed platform where companies and institutions, that are willing to share their maps or geo-referenced content, are allowed to add new terrain layers and POIs to VTG infrastructure. This will greatly enrich the quality of experience of the final users.

The service is managed by an Application Provider that monitors the quality of the overall service. Several Data Providers (including both Content Providers and Spatial Data Infrastructures) can join the service federating their private or public IT infrastructure: still maintaining full control over their data they can provide geo-spatial data and geo-referenced content from different sources to a single viewing environment.

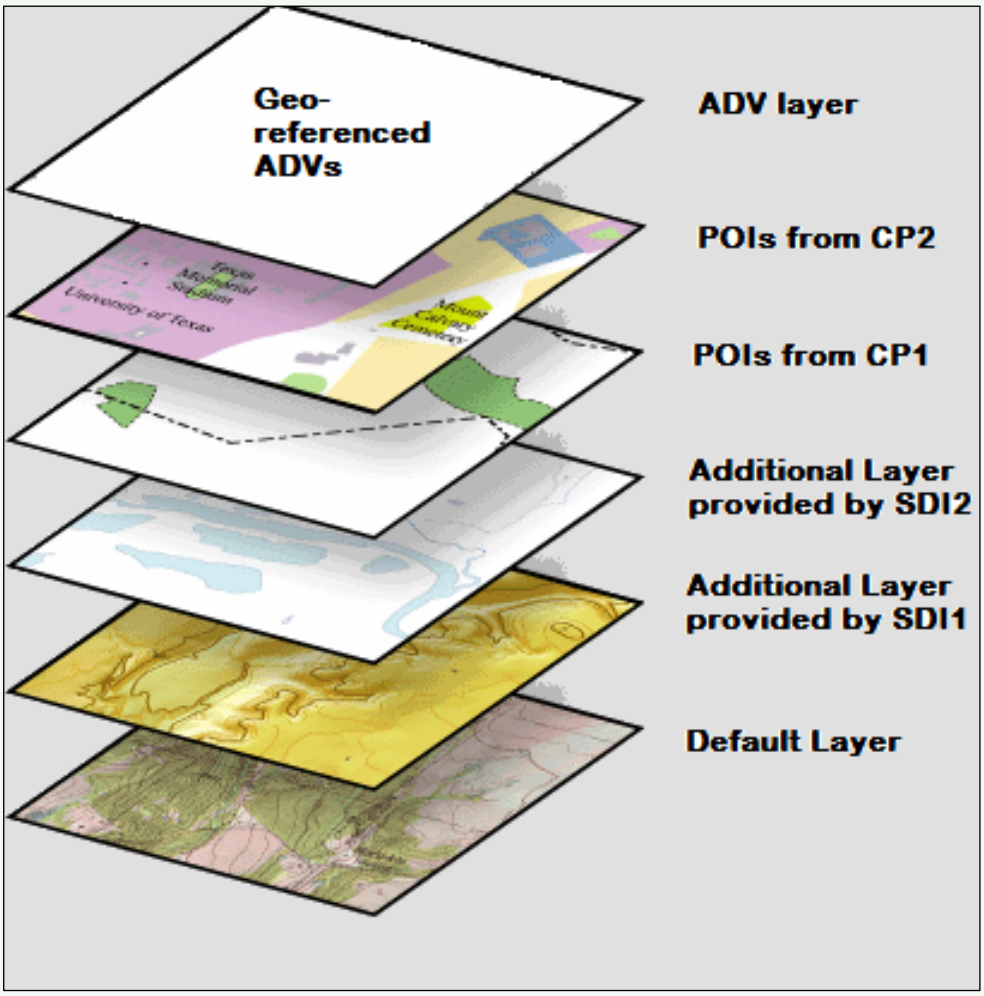
Main features of VTG are:

- User-friendly interface for an immersive navigation experience
- Search and fly to geographic location
- Dynamic activation of POIs

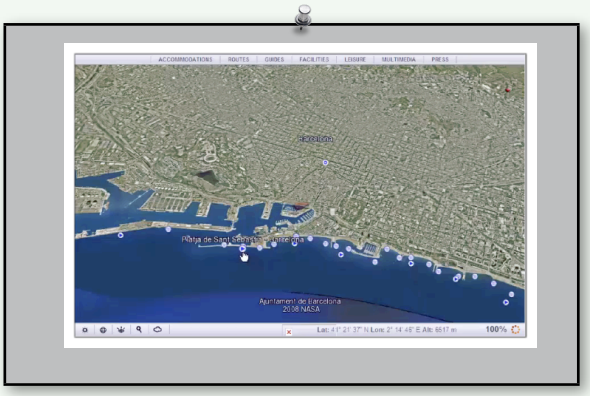
Data Providers are encouraged to contribute their services, since the Contrail technology guarantees a high level of security, protection, and reliability in data storage and management. The VTG platform could lower the initial investment needed for Data Providers: they could rent IT infrastructure from a Cloud provider in the Contrail Federation or they could easily federate their own private/public Cloud with Contrail. Quality of Service (QoS) is assured by transparent scalability and elasticity mechanisms provided by Contrail Federation.

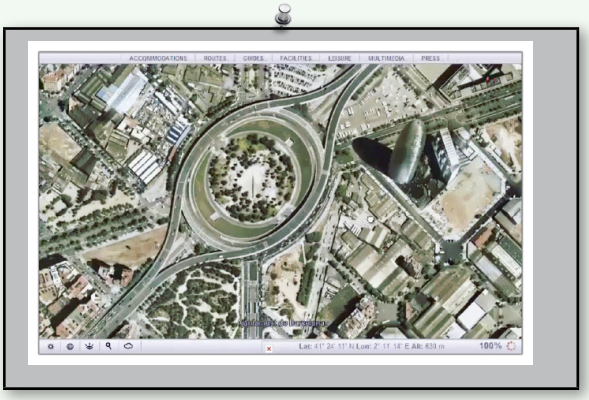
## Benefits of using Contrail

- Dynamic platform with open API's that can be easily joined by data and content providers.
- Locality of data assured: content providers can tell where their data may be used and by which user categories, thus keeping full control on them.
- Protection of data is guaranteed not only by Quality of Protection (QoP) rules, but also all data channels are encrypted to preserve confidentiality.
- Resiliency and distribution of Geodata and PoI data can be easily managed and enhanced with the use of XtreemFS features.
- This solution enables interoperation of Contrail clouds with OpenStack based clouds, which is a de-facto standard worldwide with thousand of working instances. In this way providers that already manage OpenStack infrastructures can easily join the Contrail federation.




Architecture layers

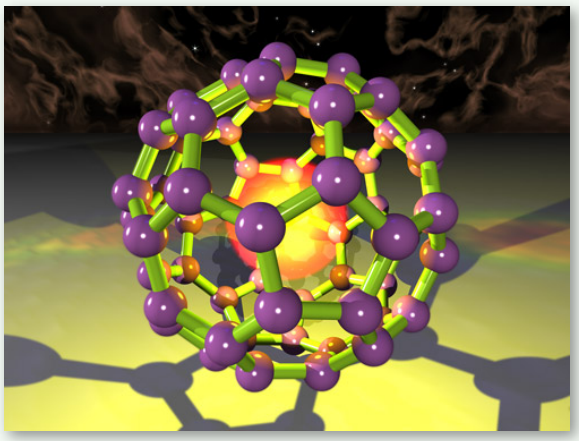


Snapshots from the system

# [use case | scientific data analysis]

## Problem addressed

Some scientific experiments are time consuming, hazardous, or expensive. Hence in these cases, it makes sense to prepare the experiments first "in silico": i.e. run simulations on computers, until the parameters space has been narrowed down to a small interesting set of parameters that can be used in a real experiment. Then a limited experiment can be conducted. Modeling a small angle neutron scattering experiment studying the structure of proteins is the simulation Contrail focuses on in this use case. This simulation software today however, runs on specific systems, that are not dynamically scalable.

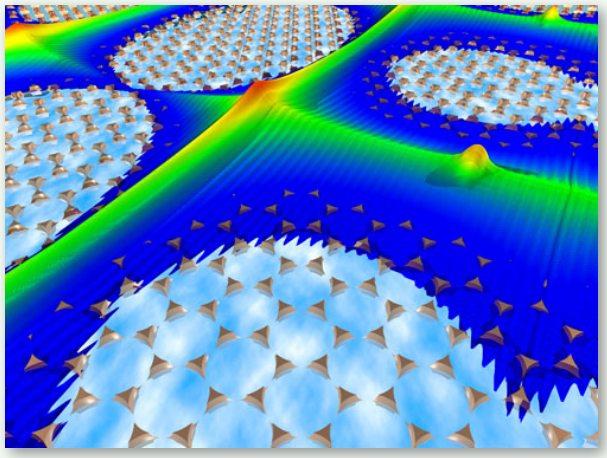


## Contrail's solution

Contrail will be used to implement a complete simulation environment for neutron scattering experiments. (From the ISIS neutron scattering facility, http://www.isis.stfc.ac.uk).The simulation itself will be implemented in a Contrail PaaS environment. Because simulations can sometimes exist of a dynamically changing number of sub-simulations that can run in the hundreds, elasticity as provided by Contrail is important.

## Benefits of using Contrail

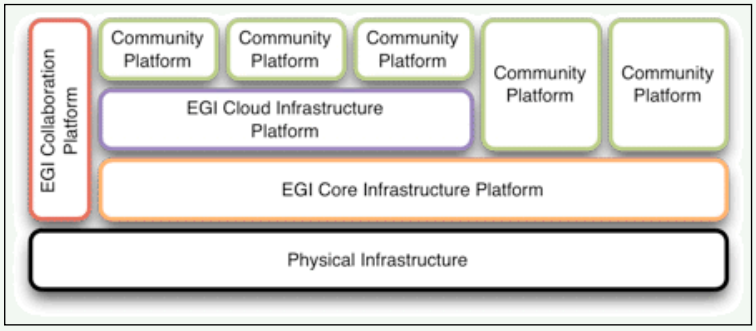
The outcome of using Contrail is a flexible, scalable simulation platform, which will also be applicable for other scientific simulation experiments.



# [contrail uptake]

Contrail components are beginning to be widely used all across Europe.

- Pan-european Cloud and Big data e-Infrastructure EGI and EUDAT are using the ConSec security tools
- The Dutch e-Health Community Cloud Dutch Health Hub is using ConPaaS and XtreemFS as part of a test bed
- Several recently started European and national R&D projects are using Contrail components




# [contrail uptake | egi/eudat]

EGI/EUDAT are large e-Infrastructures for e-Science in Europe. e-Infrastructures help European scientists to share data and computing resources in a transparent way.

The EUDAT project aims to support data management for research with an e-Infrastructure. The user communities themselves are quite diverse and are typically themselves distributed across multiple institutes: CLARIN works with linguistics; ENES is climate modelling; EPOS is Earth observation; VPH is the virtual physiological human; LIFEWATCH works with biodiversity. On top of this, new user communities are interested in using the e-Infrastructure and in contributing to the collaboration.

EGI.eu is a not-for-profit foundation established under Dutch law to coordinate and manage the European Grid Infrastructure (EGI) federation on behalf of its participants: National Grid Initiatives (NGIs) and European International Research Organisations (EIROs).

EGI offers a federated Cloud to scientists: a single, standards-based, open system to federate academic clouds from multiple providers, offering scalable computing resources with increased flexibility. Advanced compute capabilities are made available for research, virtualised resources to run different environments, cloud storage for easier sharing of data, and a number of support services to ensure applications run as efficiently as possible.

EGI and EUDAT are working together to create one federated identity management system for the e-Infrastructures in Europe.

## Use of Contrail components

The Contrail/EUDAT collaboration has been mainly in the area of federated identity management, and, more generally, building federations to support research. Users use either OpenID or national Shibboleth federations, and internally services will be built with iRODS and GridFTP, so the X.509 certificates generated internally by ConSec are an excellent match.

Indeed, the EUDAT project evaluated a number of different tools for building federated identity management, and chose ConSec as the one to proceed with. It should be noted though, that at the moment of writing EUDAT has not made an official decision as how to implement federated AAI: while ConSec is running in the EUDAT infrastructure, the project still depends on portal integration effort from their user communities.

## Benefits for Contrail

Although EUDAT has required a little reprioritising of the work in Contrail, and have required extra support for the installation and configuration of ConSec they have also contributed to the work, by evaluating the software and updating documentation and installation instructions; they have been active in the dissemination of the results, and in practical applications of ConSec (ie., applied to diverse user communities).

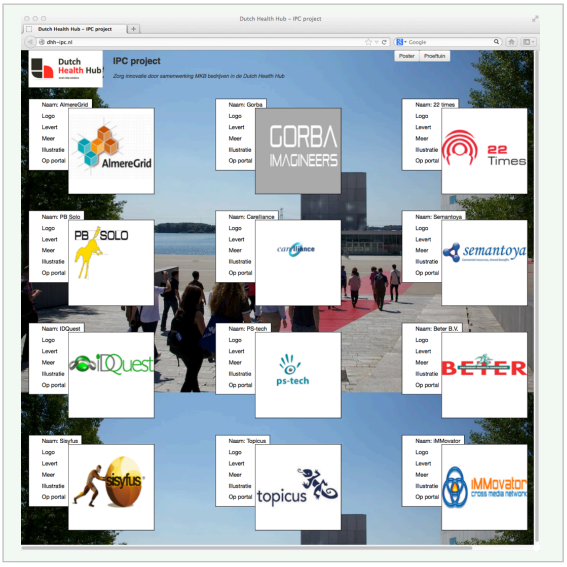
## More information

EUDAT is described at http://eudat.eu
EGI is described at http://egi.eu

# [contrail uptake | Dutch Health Hub]

The Dutch Health Hub aims to provide seamless, standard access to big medical data in the Netherlands by creating a market place on top of a Big Data infrastructure. This enables reuse and combination of data. This allows companies to offer new services to a wider audience. The Dutch health Hub is a combination of Big Data and Cloud computing.

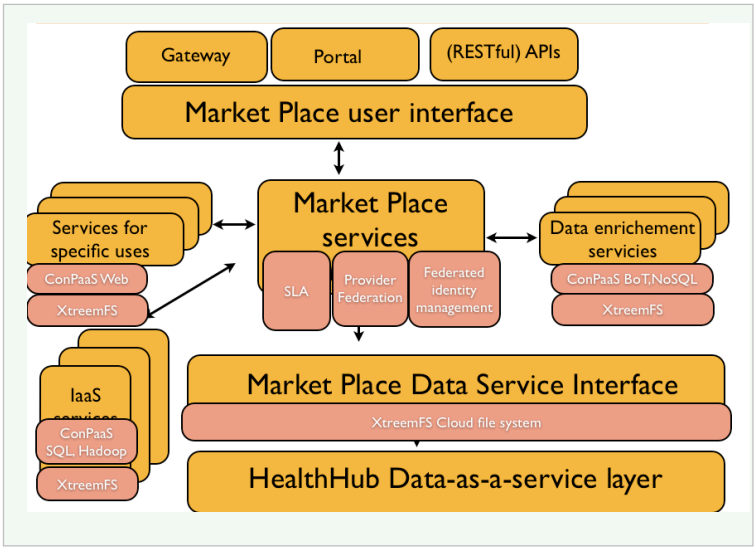
The architecture of the Dutch Health Hub IPC is based on standards and conforming to the NIST Cloud Computing Reference Model.




The Dutch Health Hub Market place is especially important for SMEs. SMEs offer distinct relatively specialized services
In a market place setting they can more easily reach customers.
The market place also offers the possibility to combine services. Other players in the Dutch Health Hub are medical centres, hospitals, HPC and cloud centres, and IT companies.

The market place is a platform in this sense that it looks like a Platform-as-a-Service based on an Infrastructure-as-a-Service layer. This maps well onto the Contrail architecture.
There should also be a role/service in the market place that certifies services. Certification increases confidence.

An application provider on the Dutch Health Hub has a complex application that consists of a number of simple applications that can run on one or more Cloud providers. The application provider makes this available to application users on the Market place, the federated Cloud. The application user submits the complex application on the Market Place, the federated Cloud, indicating with SLAs the performance that is needed.
The Cloud federation decomposes the run time application according to the SLAs and submits it to the Cloud providers that provide services according to the SLAs. This is a kind of orchestration of services.




The federated identity management service takes care the security and identity constraints are met.

In the DHH-IPC testbed, the overall structure of the market place resembles that of the media market place use case of Contrail. XtreemFS is deployed as a Cloud based file system that connects storage providers across the country.

ConPaaS is deployed to test managing services provided by SMEs.

## More information

The Dutch health Hub IPC test bed portal is described at http://dhh-ipc.nl

# [contrail uptake | projects]

New research projects are continuing where other projects stop. Hence from successful projects technology is used in new projects as this is considered stat-of-the-art. Contrail uptake in several new R&D projects has already started. Here we describe some important examples/

## Harness

The Harness project integrates heterogeneous hardware and network technologies into data centre platforms. This is vastly increasing performance, reducing energy consumption, and lowering cost profiles for important and high-value cloud applications including real-time business analytics and the geosciences.

Contrail components used in Harness include ConPaaS and XtreemFS.

## COMMIT

COMMIT is a public-private research community in the Netherlands, with many subprojects. One of these is ICT challenge, a project which is to ease the management of highly complicated scientific computing infrastructures by effectively shielding the user from the low-level complexity. The project will investigate how to design a programmable e-Science architecture while describing the infrastructure components and optimize them for typical usage scenarios.

ConPaaS is used in COMMIT.

## eBADGE

eBadge is an EU funded project with the objective of proposing an optimal pan-European Intelligent Balancing mechanism, which is also able to integrate Virtual Power Plant Systems by means of an integrated communication infrastructure that can assist in the management of the electricity Transmission and Distribution grids in an optimized, controlled and secure manner.

eBadge's aim of balancing the European electricity market brings great value to Europe because it enables the market to function more efficiently and with less wastage. In addition to that it also holds the potential for lowering the costs of balancing services throughout Europe to the benefit of European business and civil society alike. Thus eBadge leads the way to a sustainable Europe - both when it comes to keeping costs as well as resource spenditure at reasonable levels.

eBadge empowers consumers to participate and engage in the energy market of tomorrow - it supports the transition from being a consumer to being a prosumer.

eBadge intends to use the whole contrail stack for deployment of images.

## More information

eBADGE is described at http://www.ebadge-fp7.eu/
Harness is described at http://www.harness-project.eu/
COMMIT is described at http://www.commit-nl.nl/

# [open source]

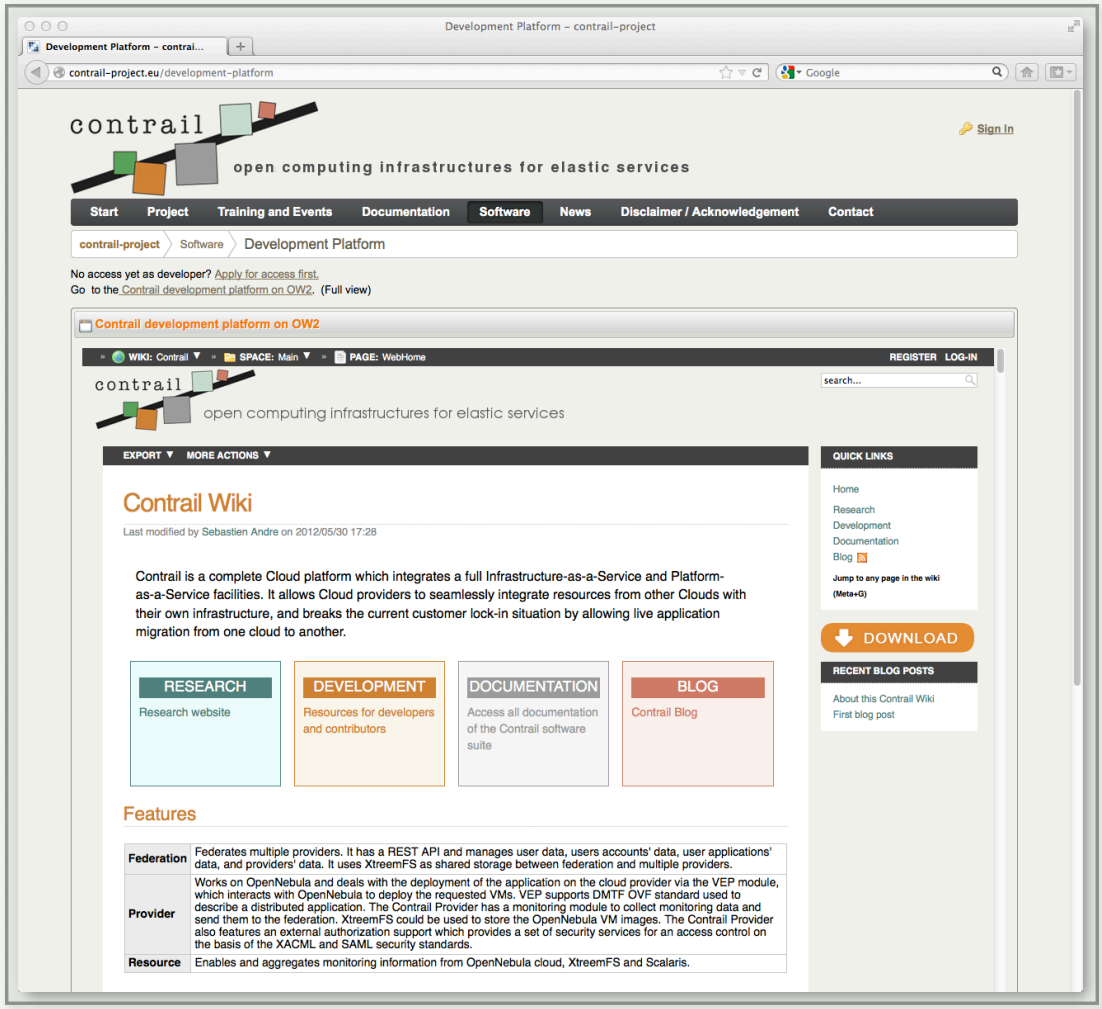
Contrail components and the overall Contrail software system are available as Open Source. They are hosted on the OW2 open source platform that specializes in infrastructure software. Apart from the software that is available as source code and binary downloads, there are mailing lists and chat channels for developers. There is also a technical Wiki with documentation.

Open Source is interesting, but only if it is backed by service companies that are committed to supporting businesses that want to use Contrail or its components. XLAB from Slovenia, HP from Italy, Genias Benelux from the Netherlands, and Linagora from France are experienced service companies supporting Contrail.

## Prerequisites

Contrail assumes there are basic Clouds available. In the current release, these have to be implemented using OpenNebula or OpenStack. If you want to install a Contrail component, like for instance ConPaaS, it may be worth to install an OpenNebula Cloud as part of your business. Contrail XtreemFS as a basic file system, does not need OpenNebula per se. You can run it on any Linux, MacOSX and Windows system.

**OW2 hosts the Contrail development and download website**




OW2

OW2 is an independent, global, open-source software community. The goal of OW2 is to promote the development of open-source middleware, generic business applications, cloud computing platforms and to foster a community and business ecosystem.

OW2 developments follow a flexible, component-based approach. Components developed under the OW2 umbrella range from specific software frameworks, protocols and applications through to integrated, service-oriented platforms. OW2 focuses on infrastructures.

The Contrail middleware stack is developed and maintained using the OW2 tools and communities. The main software repository holding the Contrail components and a Wiki describing Contrail can be found on OW2.

Contrail has also contributed with presentations to several OW2 organised events.

After the end of the Contrail project, the software will remain available at OW2 and thanks to the open source nature can be maintained and further improved.

## OpenNebula

Contrail has worked together with other partners in the OpenNebula community to further improve and enhance OpenNebula, especially concerning Cloud federation.

## OpenStack

Several components of Contrail are able to work together with OpenStack Clouds.

## More information

OW2 is described at http://http://ow2.org/
Contrail page on OW2: http://contrail.projects.ow2.org/xwiki/bin/view/Main/WebHom

http://contrail-project.eu