Contrail: A reliable and trustworthy cloud platform

[Extended Abstract]

Roberto G. Cascella Christine Morin Piyush Harsh Yvon Jegou
INRIA Rennes - Bretagne Atlantique
France
{roberto.cascella, christine.morin, piyush.harsh, yvon.jegou}@inria.fr

1. INTRODUCTION

The advent of cloud computing is a new opportunity for companies to rely on highly dynamic distributed infrastructures to offer services to their customers. While major companies might prefer to own the infrastructure to have full control on the data and applications, SMEs look with interest to cloud technology since they cannot afford the initial barrier cost to enter the market. In this perspective the advantages of cloud computing are well known: on-demand self-service; broad network access; resource pooling to optimize usage of provider resources; rapid elasticity to dynamically adapt the allocated resources to the customer needs; and measured service to provide performances guarantees and support the pay-per-use model [3]. Although this market is in rapid expansion, this growth may soon be hindered by user concerns such as lock-in within a single commercial offer (which reduces the necessary competition between many infrastructure providers), ownership and privacy issues of the data stored in the cloud, and the lack of performance predictability of current clouds. As such, it is not yet clear whether cloud computing can offer a valid and dependable alternative to private data centers for business applications, given their strong requirements in terms of availability, reliable application execution, and security.

Implementing a *dependable* cloud is both a challenging task and an important feature to make cloud computing trustful to run business applications. This implies ensuring the availability of the computation resources and having strict guarantees in terms of quality of service (QoS) and quality of protection (QoP) that users and organizations should be able to specify and monitor for creating their business on top of a cloud infrastructure, possibly owned by a third party. Other major issues are *legal* requirements for data: they cannot be stored anywhere for legal jurisdiction implication or they need to have specific privacy issues to stick with company or country legislation.

Contrail [1] is an open source integrated approach to virtualization, which aims at offering Infrastructure as a Service services (IaaS), services for federating IaaS clouds, and Contrail Platform as a Service services (ConPaaS) on top of federated clouds. In Contrail, the user is relieved from managing the access to individual cloud services providers and can focus on specifying the service or application deployed over a multitude of heterogeneous cloud providers. These providers can implement a different cloud technology, have different hardware, or offer different type of guarantees.

Contrail offers performance (QoS) and security (QoP) guarantees via SLA enforcement, and a scalable management of the computing resources via an interoperable Federation. The Federation service is the interface with the user, who needs to submit the description of the distributed application, along with its runtime configuration, and specify the requirements in terms of OVF [2] and SLA documents respectively. Then, the Federation ensures that the providers' resources are utilized as needed for offering an elastic, dependable, and trustworthy cloud service to customers.

Contrail supports dependability by providing these novel features both at the federation and provider level. This guarantees the development of trusted and reliable applications.

2. CONTRAIL ARCHITECTURE

Figure 1 depicts the Contrail architecture. The federation layer is the entry-point for users, who register and authenticate to use the Contrail services. The way the Contrail Federation is conceived enables seamless access to the resources of multiple cloud providers, avoiding potential vendor lock-in for the end users. It reaches a high degree of interoperability by managing private or public cloud providers' resources regardless of the technology implemented or hardware. The degree of interoperability and features that the Federation can exploit depends on the specific functionalities implemented at the cloud provider. Interoperability is achieved through the Contrail Virtual Execution Platform (VEP), an open source technology implementing standards that exploits resource virtualization to provide virtualized distributed infrastructures for deployment of end-user applications independently from the underlying platform.

Contrail enables users to deploy distributed applications on demand on different cloud providers by only interacting with the Federation, via the submission and negotiation of the terms of SLAs. The selection of the most suitable cloud providers is done based on the resources available, the expressed SLA terms for QoS and QoP, and the *reputation* of the providers, i.e., matching the level of performance and trustworthiness required by the application. The Federation then proceeds to negotiate proper SLA terms with each provider in a transparent way for the users.

EWDCC '12, May 8, Sibiu, Romania.

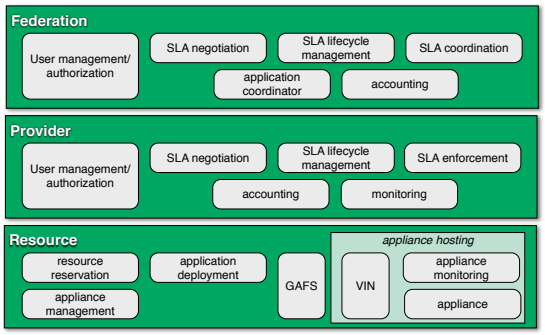

Figure 1: Contrail architecture

Proper authorization and security mechanisms are enforced primarily at the federation layer to guarantee quality of protection (QoP): each application runs in a *isolated* environment via a dedicated secured virtual network (VIN in Figure 1) to meet privacy requirements. Monitoring and auditing are performed during application execution to ensure that there is no violation of the SLA. To prevent a potential violation or implement fault tolerance, the Federation via the VEP can take a snapshot of the application and proactively decide to migrate the whole or part of the application to another provider if more resources are needed to satisfy the QoS. In such a scenario, Contrail technology is able to satisfy the user needs for the deployment of elastic and salable applications guaranteeing performance dependability and fault tolerance.

The provider layer implements the business part of a cloud provider: negotiation with the Federation and enforcement of the SLA, monitoring of the applications and accounting. The resource layer is in charge of managing the physical resources of a cloud provider. Contrail provides a reliable and highly available storage service, named Global Autonomous File System (GAFS). On the one hand, GAFS is used to store VM images and system logs; on the other hand it provides scalable Storage as-a-Service to cloud users and applications. Most important is the possibility to specify the level of protection of the stored data and the location of the storage due to specific legal requirements. These requirements are critical to make the provider resources trustworthy, making cloud computing suitable to run the users' businesses safely.

Contrail technology also deploys ConPaaS services [4], which are self-managed, elastic, and scalable. A ConPaaS service can deploy itself on the cloud, monitor its own performance, and increase or decrease its processing capacity by dynamically (de-)provisioning instances of itself in the cloud. The tight integration with the Federation will ensure that a ConPaaS service can be deployed over different cloud providers to guarantee elasticity within the constraint of the negotiated SLA, which specifies the QoS terms. Hence, ConPaaS services will integrate security and availability guarantees for a reliable execution.

3. RESEARCH CHALLENGES

Customers rely on cloud computing as an external source for their data management and processing. Major requirements of business applications are security, availability of the resources, and reliability of the cloud providers for deploying applications, i.e., dependability. Contrail tackles each of these challenges for a dependable cloud.

Availability.

Availability of the resources is important to meet the requirements of business applications. Sharing cloud resources with other users exposes the customers and the cloud provider to possible misuse of the resources, which might not be anymore available in case of outages or network misconfiguration. Contrail addresses these issues by ensuring proper isolation of the applications and control over the access to the resources. Moreover, implementing elasticity of cloud services requires cloud providers to allocate on-demand resources which might not be temporary available. In this case, the Contrail Federation service can take over and locate resources in an alternative cloud provider to meet the customers' requests.

Reliability and performance guarantee.

On the one hand a cloud provider should contractually reach the application performance objective to ensure a reliable application execution. On the other end, the provision of new resources to meet this objective should be done at the minimum cost for the customer. Contrail uses SLAs to negotiate Quality of Service (QoS) terms; the Federation is then in charge of locating the best cloud provider and monitoring the applications.

Security and trustworthiness.

Customers rely on the cloud to run their applications and store their data. Thus, both of them must be adequately protected against unauthorized access or modification. Authentication and authorization are two essential characteristics to identify users and protect their applications and data from others or even the cloud provider itself. These are integrated in the Contrail Federation service which implements a proper security support. Linked to security is the need to meet legal requirements, such as location of data storage or location of the used computing resources. Contrail uses SLAs to make the customers specify the Quality of Protection (QoP) terms. The Contrail Federation then selects the most reputable providers to deploy the application.

4. CONCLUSION

Contrail is a new open source system that aims at facilitating the deployment of distributed business applications by implementing a dependable platform. Contrail provides security mechanisms, specific performance guarantees via SLAs, and interoperability for deploying reliable applications in a dynamic and heterogeneous environment.

5. ACKNOWLEDGMENTS

This work is partially funded by the FP7 Programme of the European Commission in the context of the Contrail project under Grant Agreement FP7-ICT-257438. The authors would like to thank the Contrail Consortium members.

6. REFERENCES

[1] Contrail project. `http://contrail-project.eu/`.

[2] *Open Virtualization Format Specification*. DMTF Standard, 2009.

[3] P. Mell and T. Grace. The NIST definition of Cloud Computing, version 15.

[4] G. Pierre et al. Conpaas: an integrated runtime environment for elastic cloud applications. In *ACM/IFIP/Usenix Middleware*, 2011.