TClouds — Trustworthy Clouds

TRUSTWORTHY OPENSTACK PROTOTYPE

www.tclouds-project.eu

Security Threats in Cloud Computing

Cloud computing is one of the most promising technologies these days since it allows a user to access a potentially unlimited set of virtualized resources but, at the same time, raises new security issues that are not present in the case of an ad-hoc infrastructure. In particular, the development of cloud computing frameworks freely available as open source software, is typically focused on functionality and scalability rather than security.

Trustworthy OpenStack is a prototype resulting from a cooperative effort that increases the robustness and the security of the software framework, with benefits for the customers and for the cloud provider. It brings together several security enhanced subsystems.

Trustworthy OpenStack

Trustworthy OpenStack is an improvement of the standard OpenStack framework for the management of an Infrastructure as a Service (IaaS) cloud environment that enhances its security in different dimensions: trust and integrity, confidentiality, resilience and audit.

These objectives are reached through four security extensions consisting of integrated subsystems of the TClouds platform.

Figure 1 shows the architecture of Trustworthy OpenStack: Cloud Node 0 is the Cloud Controller while the other nodes are simply providing the Virtual Machine (VM) instances. Cloud Interface consists of the tools (API and web-based application) needed to manage the cloud. In the figure there are also depicted the TClouds subsystems that form the four security extensions described below.

Secure Logging and Log Resiliency. Implemented by the LogService and the CheapBFT subsystems, it provides by design integrity, confidentiality and resilience of the log entries created by OpenStack components. The cloud administrator can access the log entries inside the logging sessions and, for each session, verify their integrity through the Dashboard, the standard web-based management interface for OpenStack.

Advanced VM Scheduling. Implemented by Access Control as a Service (ACaaS), it provides an enhancement to the Scheduler, through the filter mechanism. It allows the definition of arbitrary properties for the cloud nodes in the form of key-value pairs and additional requirements for the customers to choose when instantiating a VM: only the cloud nodes that have the required propert(ies) set to the required

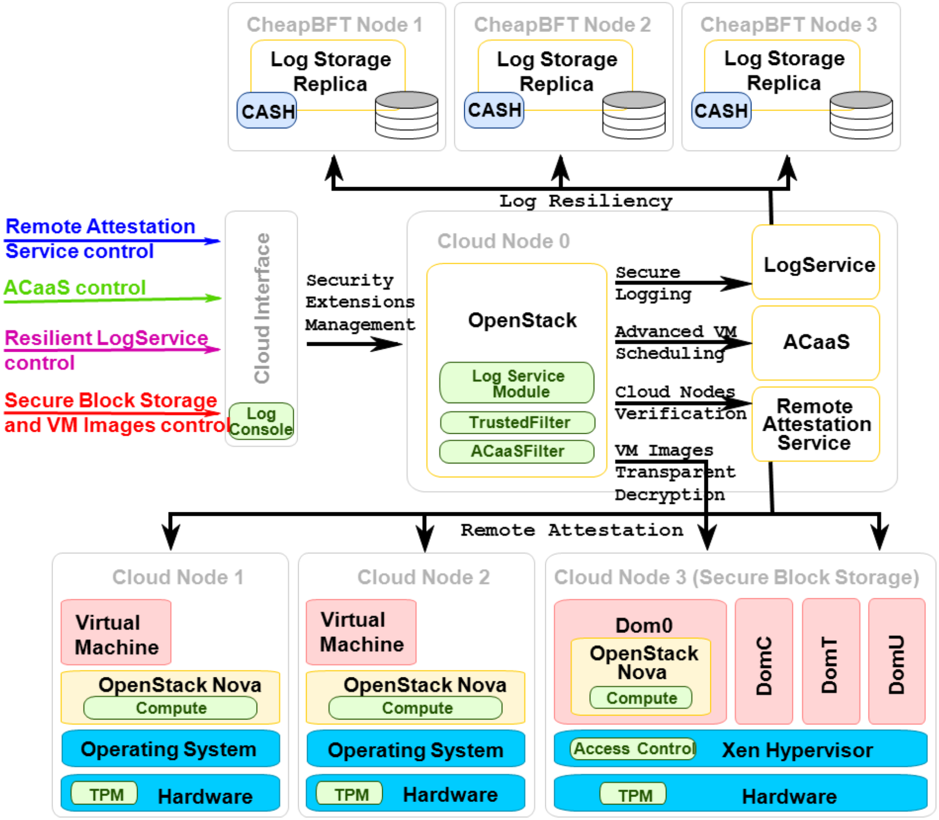

Figure 1: Architecture of Trustworthy OpenStack

value(s), will be selected for the deployment of the VM.

Cloud Nodes Verification. Implemented by Remote Attestation (RA) Service subsystem, it also provides an enhancement to the Scheduler, again through the filter mechanism. It works similarly to the *Advanced VM Scheduling* extension, whereas the allowed property for the nodes (and the requirement for the VM(s) to be deployed) is the node integrity level that can assume one out of five values. The integrity level represents the summary of the integrity state of a node and may indicate that all running software is recognized as being part of a Linux distribution and all related packages are up-to-date. Or, that some packages related to the running software are not updated, because improvements or security-critical bug fixes are available. The integrity level may also indicate that not all running software is recognized as being part of the distribution. This security extension allows the customer to select the nodes for deploying a VM in a pool of Trusted Nodes - since the integrity state information of the nodes is collected through Trusted Computing technologies.

Transparent Encryption. Exploiting the cryptography-as-a-service component, the system encrypts data in VM instances and block-storage devices. It provides a secure mechanism to store the VM images encrypted and to decrypt/encrypt them on-the-fly using customer keys protected from a malicious cloud administrator by means of Trusted Computing technologies.

Upcoming Security Extension

Trusted Virtual Domains (TVDs). Implemented by Ontology-based Reasoner subsystem, it provides a way to logically group together VMs belonging to a single customer (while possibly running on different nodes) and make them communicate to each other freely and be isolated from VMs of other customers. A customer may own many TVDs. A basic support for TVDs is already present, through the Quantum component, in the Folsom release of the standard OpenStack. This TClouds extension builds on Quantum and enforces the isolation through confidentiality and integrity of the communications using secure protocols like IPsec.

Further Information

Further information about *Trustworthy OpenStack* can be found under Deliverable „D2.4.2—Initial Component Integration, Final API Specification, and First Reference Platform".

Disclaimer

The TClouds project has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement number ICT-257243.

TClouds at a glance

Project number:
257243

TClouds mission:

- Develop an advanced cloud infrastructure that delivers computing and storage with a new level of security, privacy, and resilience.
- Change the perceptions of cloud computing by demonstrating the prototype infrastructure in socially significant application areas.

Project start:
01.10.2010

Project duration:
3 years

Total costs:
EUR 10.536.129

EC contribution:
EUR 7.500.000

Consortium:
14 partners from 7 different countries.

Project Coordinator:
Dr. Klaus-Michael Koch
coordination@tclouds-project.eu

Technical Leader:
Dr. Christian Cachin
cca@zurich.ibm.com

Project website:
www.tclouds-project.eu