1 Executive Summary

The Problem: multiple types of Cloud needs and procurement procedures may reduce efficiency of IT infrastructure and increase information security risks at Agency level

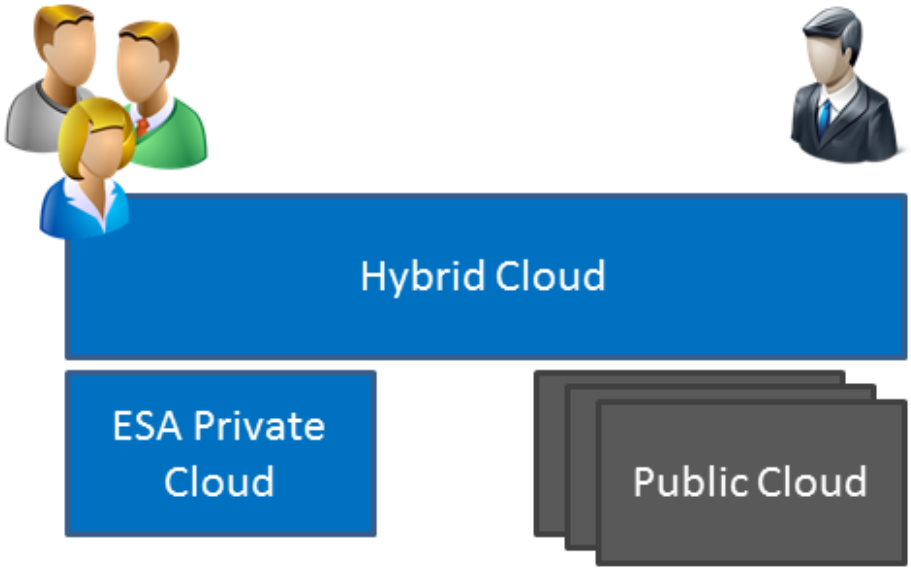
ESA has currently a mixture of fixed physical and virtual infrastructure. There are some activities which already make use of dynamic infrastructure (private cloud) for their own needs but this is a minority and still in the early phases. On the other hand, the Gaia mission is using public (Amazon) cloud services for data processing.

With this GSP study, ESA wanted to capture the business needs and Infrastructure as a service (IaaS) requirements for 10 activities that had expressed interest in the Cloud and design one common IaaS blueprint for all of them, which would allow to simplify the Agency's IT infrastructure and future IT procurements. The domains investigated within the Agency were:

- Provision of corporate IT for the entire Agency
- SAP business services
- Document management with Prisma
- Grid computing and VM management with SSEP
- Virtual Infrastructure for Integration and Validation of EO PDGS services
- Mission data processing for Gaia and Euclid
- Provision and management of VMs for developing and testing mission operations' ground applications and simulation frameworks
- Executing computationally heavy Space Weather models

Ten sets of IaaS requirements were captured covering technical, operations, governance and security requirements. The common requirements were then formulated that would serve as the driver for the common IaaS blueprint.

The Solution: a single hybrid IaaS cloud which the most demanding ESA programmes can use



Public and private clouds offer different benefits. Hybrid clouds offer the best of both worlds, as they allow users to switch as needed, at the cost of higher complexity in the design. This study has opted for a Hybrid cloud design, with a private ESA cloud as one of the cloud service providers.

Within ESA users can thus access clouds of different types through the hybrid cloud. The private clouds can be from different ESA sites and across different public cloud providers.

Given ESA's requirements, the most suitable product for Hybrid Cloud management is the DELL Multi Cloud Manager (formerly known as Enstratius). As Enstratius has now been bought by DELL it has a guaranteed future. It is also being used within ESA pilots within the Helix Nebula European Cloud project. It is also the only major cloud management software vendor to support European clouds such as CloudSigma out of the box.

The UI of the solution will be web-based. The selected cloud manager already provides a large set of UIs which should be reused. At the same time the need to remain flexible in extending the system later as well as the integration of multiple systems into the final solution Enstratius means that a UI mash up is desirable. Liferay was selected to be used for the UI mach-up.

The ESA Private Cloud is based completely on the VMware vCloud Suite product, including the vCenter Operations Management solution. The implementation is thus solely a deployment and configuration of the vCloud solution within ESA.

The platform virtualization for ESA Private Cloud is done by VMware vSphere. The core VMware vSphere components are the VMware vSphere Hypervisor ESXi and VMware vCenter Server & vCloud for management and Orchestration.

The hypervisors are deployed in a cluster configuration and can scale up to 32 nodes per cluster. The cluster allows dynamic allocation of resources, such as CPU, memory, and storage. The cluster also provides workload mobility and flexibility with the use of VMware vMotion and Storage vMotion technology.

Although all kinds of x86 servers could be used to provide more power to our private could implementation, Rack Based Servers, Blade enclosure servers or vBlock like servers enclosures are suggested. This kind of enclosures unify the infrastructure components and enable to obtain better performance and less power consumption, simple configurations and better management. In any case hardware shall be VMware compatible. vSphere supports multiple and different kind of hardware to be used over time. Also, more hardware could be added without downtime to running servers. Hardware will be deployed in at least 2 locations. In this case one vCenter Common virtual datacentre would expand over both sites and manage both vSphere clusters.

According to ESA requirements of approximately 1000 vCPU (similar in compute power to state of the art CPU cores) and taking a conservative virtualization ratio (1:7 ratio) a total of 130-144 physical cores total compute power configuration is needed. 1 TB RAM memory per physical node should be configured to have a total cluster size of 12TB. Each cloud node shall have capacity for at least two dedicated 10Gb Ethernet cards for virtual machines operation. In addition to production networking cards two more 10Gb Ethernet dedicated cards for VM management and motion are recommended.

Such a solution, together with a set of best practices identified for configuring the Solution will satisfy the security requirements captured during the study.

A common framework for Cloud governance and information security policies to ease procurement procedures and systematically mitigate security risks

Because of the increasing adoption of Cloud computing technologies within certain ESA programmes, draft governance and information security policies were written, with the aim of extending existing policies to address the risks related of using and procuring Cloud solutions and services.

In summary, the governance policy consists of the following main components:

- A Governance Board which consists of members of the already existing IGB CC WG group with overall responsibility for the Governance of Cloud Computing usage Agency-wide
- A set of five key underpinning pillars of the policy: Technical, Legal, Procurement, Compliance and Security, for which each has an assigned member within the Governance Board (with the possibility one member may cover a number of areas
- A Governance Cycle of four key phases: Policy Creation and Refinement, Procurement, Operations and Compliance
- The ESA Cloud Procurement Pack (ECPP) which contains a number of materials and tools to assist programmes with procuring and managing during operations of Cloud Computing resources

The Framework aims to ensure a lightweight process is in place to support programmes looking to make use of Cloud Computing.

A Security Approval and Accreditation process was outlined, according to which CIS may not enter operation prior to receiving an Interim-Authority-to-Operate or full Accreditation. Moreover a continuous risk management process was elaborated based on the Plan-Do-Check-Act cycle.