Design and Requirements, Cloud&Heat SafeCloud-based storage platform

D5.1

Project reference no. 653884

August 2016

Horizon 2020
European Union funding
for Research & Innovation

Document information

Scheduled delivery	01.09.2016
Actual delivery	15.09.2016
Version	1.1
Responsible Partner	Cloud&Heat Technologies GmbH

Dissemination level

Public

Revision history

Date	Editor	Status	Version	Changes
31.05.2016	L. Yazdanov	Draft	0.1	Initial version
17.06.2016	L. Yazdanov	Draft	0.2	Added content from (Cloud&Heat)
29.06.2016	L. Yazdanov	Draft	0.3	Added content to Section 2
01.07.2016	S. H. Totakura	Draft	0.4	Revised version
02.07.2016	H. Mercier	Draft	0.5	Revised version
04.07.2016	K. Tarbe	Draft	0.5.1	Revised version
24.07.2016	L. Yazdanov	Draft	0.6	Addressed comments from reviewers
24.08.2016	H. Mercier	Draft	0.7	Complete revision
29.08.2016	L.Yazdanov	Draft	0.8	Addressed comments from reviewers
30.08.2016	R. Barbi	Draft	0.8.1	Revised version
30.08.2016	H. Mercier	Final	1.0	Final version
15.09.2016	L. Yazdanov	Final	1.1	Minor changes discussed during the SafeCloud Fall 2016 Munich meeting

Contributor

L. Yazdanov (Cloud&Heat)
S. H. Totakura (TUM)

Internal reviewers

K. Tarbe (Cyber)
S. H. Totakura (TUM)
R. Barbi (UniNE)
H. Mercier (UniNE)

Acknowledgements

This project is partially funded by the European Commission Horizon 2020 work programme under grant agreement no. 653884.

More information

Additional information and public deliverables of SafeCloud can be found at http://www.safecloud-project.eu

Glossary of acronyms

Acronym	Definition
IaaS	Infrastructure as a Service
SaaS	Software as a Service
VM	Virtual machine
WAN	Wide Area Network

Table of contents

Executive summary

This document describes the use cases of Cloud&Heat products that will exploit the security and privacy features developed in the context of the SafeCloud project. The deliverable is structured as follows. Section 1 presents a general overview of the SafeCloud framework described in deliverables D1.1, D2.1, D3.1 and D4.1. Section 2 describes the SafeCloud-based storage platform that will be deployed on the Cloud&Heat infrastructure. It gives an overview of two Cloud&Heat storage products (Cloud Block Storage, SafeCloudBox), including product context description, functions, expected users, and constrains. Section 2 also presents product use cases and their integration within the SafeCloud framework. Finally, Section 3 defines the Cloud&Heat requirements for the SafeCloud framework with respect to the use cases and integration scenarios described in Section 2.

1 SafeCloud Framework

The section gives an overview of the Safecloud framework presented in deliverables D1.1, D2.1 and D4.1.

1.1 SafeCloud Architecture

The framework consists of three separate layers, each providing solutions in their own domain. The solutions provide different security guarantees at different costs. Generally, stricter security guarantees impose greater limitations or performance costs on the applications. The three layers of the SafeCloud framework are secure communications, secure storage and secure queries. Cloud&Heat aims to exploit two layers of the SafeCloud framework: secure communication and secure storage.

The secure communications layer provides solutions that improve the security aspects of communication channels over untrusted environments. We provide three solutions for this layer. First, the vulnerability-tolerant channels solution provides communication channels that are built on multiple redundant security mechanisms to ensure that failure of any one mechanism does not cause a security failure in the channel. Second, the protected channels solution introduces multiple methods to reduce the risk of fake certificates used by the parties. It defends against port scans and discovery of the network infrastructure. Third, the route-aware channels solution deploys methods to improve confidentiality and detect route hijacking. All of the solutions are built on top of the Java secure socket API. Cloud&Heat plans to implement cross data replication of the Cloud Block Storage. With the help of private communication middleware, the company wants to increase security measures against man-in-the middle attacks.

The secure storage layer consists of solutions that provide confidentiality and integrity guarantees for data stored in an untrusted environment. The secure block storage and the distributed encrypted filesystem give similar secure storage benefits but with different level APIs. The long-term distributed encrypted archival solution provides an entangled immutable data store for protection against tampering and censorship. It is exposed to applications as a REST API. Cloud&Heat considers to offer storage services that would allow customers to store private data on the cloud. However, customers are usually reluctant to store their data on the cloud due to insufficient data security. So we expect that the secure storage layer will provide the necessary confidentiality and integrity features.

1.1.1 Private Communication Middleware Architecture

The secure communications layer of SafeCloud is implemented as Private Communications Middleware. The middleware is used for all network communications between components of the SafeCloud architecture. Deliverable D1.1 describes this architecture layer in depth. To summarize, the middleware takes care of keeping these communications safe and private by providing three layers of protection:

1. The communications are made vulnerability-tolerant by encrypting the data of the channel with more than one crypto-suite such that a flaw/weakness in one crypto-suite will not break the confidentiality of the channel.
2. Communications between SafeCloud end-points are secured by authenticating the end-points using public-key infrastructure (PKI). To defend against man-in-the-middle attacks by a rogue certification authority during end-point authentication, the validity of certificates is checked against a notary. Additionally, the hosts running SafeCloud components are defended against vulnerability scanning

methods using secure port-knocking mechanisms which only allow connections from authenticated clients.

3. Communications are protected from metadata analysis by splitting them across multiple routes. This way, an attacker needs to acquire more than one vantage points to successfully analyse the communication. Additionally, end-to-end route monitoring employed by the middleware alerts the communication end-points when route properties have drastically changed, indicating a potential attack to hijack the communication route.

1.1.2 Storage architecture

As described in deliverable D2.1 and delivered at Month 6, the storage architecture provides three solutions in increasing levels of sophistication: secure block storage, a secure data archive, and a secure file system.

The **secure block storage** solution consists of a data store that can store raw data under a given key. In that respect, it behaves akin to a key/value store but provides additional mechanisms to ensure data security and integrity (using cryptographic techniques), as well as *explicit placement* of data items. As a matter of fact, being able to place different parts of data items in various geographical locations within distinct administrative domains is the key to provide privacy in the SafeCloud platform. The secure block storage operates locally, on a per node basis, and there are typically several instances per data center. Orchestration between these instances is performed by separate components that can explicitly place data items on individual instances of the block storage.

The **secure data archive** builds on top of the secure block storage and supports secure storage of documents over many distributed instances of data stores. Documents are redundantly stored and protected against tampering using coding and entanglement techniques, i.e., they are encoded and combined with previous documents to ensure that no party can modify or delete them (without affecting a significant portion of all other documents). The data stored in the system is immutable, as the key idea behind entanglement is to persist documents over the long term. In other words, this solution supports archival storage. Modifications to existing data can be implemented on top of the long-term distributed encrypted document storage by the means of a versioning, i.e., by inserting a new version of a previous document under the same name but a with different version identifier.

The **secure file system** provides a file system API on top of the secure block storage. It supports secure reading and writing of files that are geographically distributed across data centers, and hence deals with mutable data. The file system is optimized in terms of latency and throughput for sequential accesses. Placement of data in the file system can be guided by policies that express security or dependability requirements (e.g., replication degree, disaster tolerance against whole data center failure, geo-localization in a given set of countries, etc.). As the file system is accessible locally from clients, it requires a local component to execute directly on the client machines.

2 SafeCloud-based storage platform

This chapter presents the use cases of two storage products from Cloud&Heat – Cloud Block Storage that belongs to the family of IaaS products and SafeCloudBox that can be delivered in the form of SaaS to the end users. The goal of this chapter is to derive relevant requirements to be addressed by the SafeCloud platform from the perspective of the end-user that wants to use storage resources offered by Cloud&Heat with confidentiality, integrity and availability guarantees.

2.1 Cloud&Heat Storage Products

In the context of the SafeCloud project, Cloud&Heat aims to improve its existing storage offerings and attract new customers by providing a use case demonstration of the SafeCloud SafeCloudBox that will be deployed on the Cloud&Heat infrastructure. In this section we present two storage products that will exploit the security and privacy features provided by the SafeCloud project.

2.1.1 Cloud Block Storage

Product context
The company delivers computing resources to IaaS customers in the form of VM. A Cloud&Heat VM is an emulated computer running on a real computer somewhere in the cloud, which the customers can use much like a physical machine. Cloud&Heat offers VMs with Linux operating system, different number of processor cores, and with different amount of storage.

The storage in the VM is ephemeral. This means that if the VM terminates, the data stored in the VM is lost. The termination of a virtual machine, in the physical world, can be thought of as destroying the computer. To avoid losing data, one should attach persistent block storage to the VM.

Cloud Block Storage is the persistent storage solution offered by Cloud&Heat. One can consider it has a hard disk that can be attached to a server. In addition to data persistence, Cloud Block Storage provides data redundancy. At Cloud&Heat we apply triple data replication.

In the current version of Cloud Block Storage, the data is replicated across several racks that reside in the same data center. Such design allows us to avoid running data replication over an external network (WAN). Hence, we can provide higher performance and minimize the risk of data being accessed by third-parties. However, the downside of the approach is the lack of disaster recovery mechanism that would allow us to quickly restart customers' VMs from another data center.

To address the aforementioned problem, the company aims to perform cross data center Cloud Block Storage replication by exploiting the security features provided by SafeCloud. The focus will be put into providing privacy features and acceptable performance when the data is transferred over WAN.

Product capabilities/functions
Cloud Block Storage is a IaaS product from Cloud&Heat that delivers on demand storage resources to end users that can be consumed by the Openstack Nova. The storage provides end users with a self-service™ API to request and consume those resources without

requiring any knowledge about where their storage resources are actually deployed. The product has the following features:

- Persistent storage. The data stored on the block storage provisioned volumes is always available regardless of the state of a running VM.
- Data redundancy. All customer data stored on Cloud Block Storage volumes is replicated three times.
- Data snapshotting. Customer can take a snapshot to return to the previous state of a volume.
- Adjustable QoS levels. Volumes can be associated with different service levels. For example, we can deliver higher performance for privileged users and lower performance for non-privileged ones.
- Disaster recovery. In case of data center downtime, customer's VMs can be launched from another data center.

User characteristics

Cloud Block Storage is mainly targeted for IaaS users. The users represent different organizations and individual users that would like to host their infrastructure on our cloud.

Constraints

When deployed, the Cloud Block Storage should be compliant with regulations on personal data protection. Legal recommendations presented in deliverable D2.3 should be taken into consideration.

2.1.2 SafeCloudBox

Product context

Many companies and users are now facing *the Dropbox problem*. Employees use Dropbox for file sharing, synchronization and mobile access, but IT departments need to maintain control over the security and location of their data. There may also be regulatory restrictions which create the need for a secure, self-hosted solution that has the same file sync and share features as those from the public domain.

Considering the issues posed by popular cloud-based storage platforms, we envision a high demand for storage services with enhanced security and privacy features. In particular, Cloud&Heat focuses on solutions that would allow users to keep using cloud-based storage without giving up privacy and security. In addition, users should be able to control data-placement policies.

The main focus of Cloud&Heat is delivering IaaS solutions. Moreover, we believe that customers should have an option to use the infrastructure they trust. We therefore propose to install the SafeBox on the infrastructure that is controlled by the customer. It could be the central file sharing server of a company, the personal laptop of a customer or a VM running on a trusted cloud. The SafeCloudBox would allow users to communicate with Cloud&Heat data centers and perform secure reading and writing of data.

There are several use cases for SafeCloudBox. The cloud backend can be used as an extension of local storage, provide data mirroring (storing one copy of local data on a cloud), data archiving, data replication (storing many copies of local data on a cloud). By setting up a storage policy customers can reduce costs associated with cloud storage. For

example, data mirroring requires three times less cloud storage in comparison to triple data replication.

Cloud&Heat has highly distributed data centers, and for a given customer the network performance highly depends on the location of the chosen data center. Therefore, we believe that our customers should have the option to define data placement policies. For example, data can be stored on the closest data center or on the data center that has the highest bandwidth.

Product capabilities/functions
The following features are provided by SafeCloudBox:

- Two data access methods. Users can access data from a web interface and an on-device client application.
- Support for file operations. Allows to store, create, share documents.
- It allows to assign storage quota. A system administrator can limit the storage capacity available to a user.
- Data replication. To guarantee disaster tolerance against whole data-centre failure, the data is replicated with respect to defined replication parameters across different data centers.
- Data mirroring. Users keep a copy of the local storage data on the cloud.
- It works as storage extension. If the local data size exceeds a user defined threshold, then it is stored on the cloud. One can consider local storage as cache.
- Archiving. Users can store older files versions on the cloud to reduce the local data storage consumption.
- Control over data placement. Data should be stored at user-defined locations.
- Optimization for high performance. Data can be stored on the data centers with the lowest communication latency or the highest bandwidth for each customer.

User characteristics
The target users of SafeCloudBox are organisations and individuals that want to keep data safe and secure on our cloud.

Constraints
When deployed, the SafeCloudBox should be compliant with regulations on personal data protection. Legal recommendations presented in deliverable D2.3 should be taken into consideration.

2.2 Cloud&Heat use cases

2.2.1 Overview

This section presents an overview of the Cloud&Heat use cases and their actors. Cloud Block Storage use case is presented in Figure 1. In Figure 2 we present SafeCloudBox use case. Along with the use cases diagrams we provide detailed description of each use case.

2.2.2 Cloud Block Storage use case

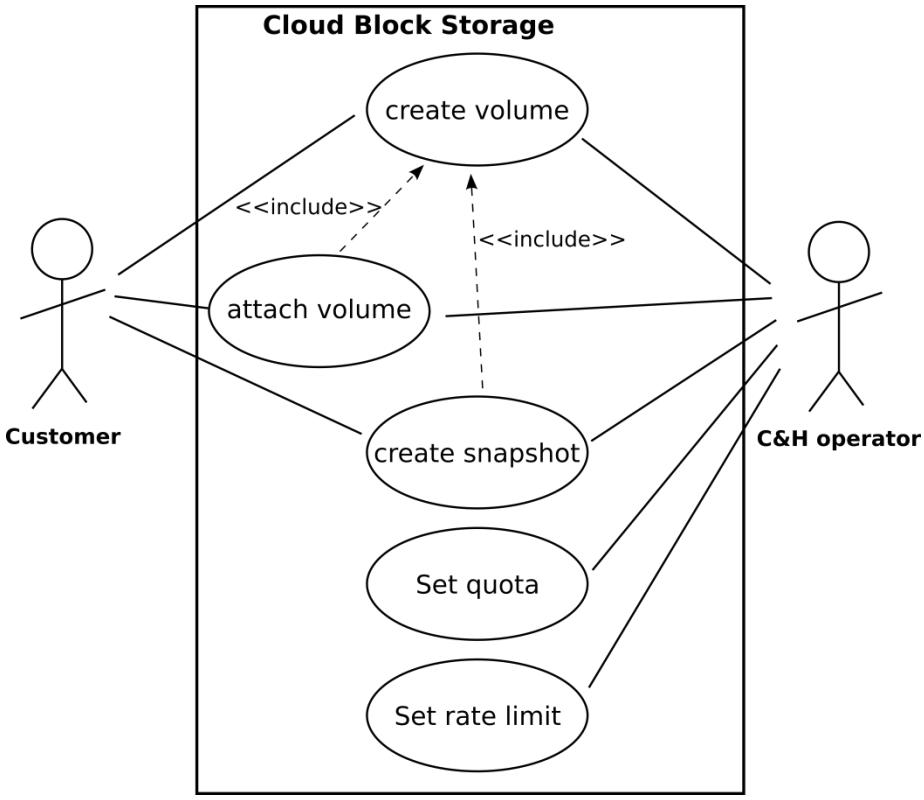

Figure 1: Cloud Block Storage use cases diagram.

We have two actors that are involved in Cloud Block Storage use case:

- Customer. A person that uses IaaS products and interacts with Cloud&Heat dashboard user interface.
- Cloud&Heat operator. A responsible person from Cloud&Heat that takes care of different cloud management operations including setting up users accounts, creating and attaching volumes, applying capacity and performance limits to customer's volumes.

2.2.3 Cloud Block Storage use case description

Use-case:create volume
Brief Description: a customer wants to create a persistent storage for a VM.
Actors: the customer.
Preconditions: the customer has access credentials.
Basic Flow:

1. the customer log in Cloud&Heat interface
2. the customer creates the volume

Alternate Flows:

1. flow:
   - in step 1 the customer cannot log in due to wrong credentials
   - the customer re-enters access credentials
   - the customer log in successfully and starts from step 2 in Basic Flow
2. flow:
   - in step 2 the requested volume size exceeded assigned quota
   - the customer requests the quota extension
   - the quota is extended and the customer restarts from step 2 in Basic Flow

Exception Flows:

- the network connection fails
- volume creation process reports an error state

Postconditions: the volume with specified size is created.

Use-case: attach volume

Brief Description: a customer or an operator needs to attach volume to a VM.
Actors: the customer/operator.
Preconditions: the volume has been already created.
Basic Flow:

1. the customer/operator log in Cloud&Heat interface
2. the customer/operator selects the target VM
3. the customer/operator attaches the volume to a VM

Alternate Flows:

1. flow:
   - in step 1 the customer/operator cannot log in due to wrong credentials
   - the customer/operator re-enters access credentials
   - the customer/operator log in successfully and starts from step 2 in Basic Flow
2. flow:
   - in step 2 the VM has not been created yet
   - the customer/operator creates the VM
   - the VM is created and customer/operator starts from step 2 in Basic Flow
3. flow:
   - in step 2 the customer/operator selects wrong VM
   - the customer/operator detaches the volume and starts from step 2 in Basic Flow

Exception Flows:

- the network connection fails
- volume attachment process reports an error state

Postconditions: the volume is attached.

Use-case: set quota

Brief Description: a customer requests to increase cloud block storage quota.
Actors:the operator.
Preconditions: the operator has an account on Cloud&Heat.
Basic Flow:

1. the operator log in Cloud&Heat interface
2. the operator sets specified quota

Alternate Flows:

1. flow:
   - in step 1 the operator cannot log in due to wrong credentials
   - the operator re-enters access credentials
   - the operator log in successfully and starts from step 2 in Basic Flow
2. flow:
   - in step 2 the operator sets wrong quota value
   - operator restarts from step 2 in Basic Flow

Exception Flows:

- the network connection fails
- the process of updating quota reports an error

Postconditions: the **specified quota is assigned**.

Use-case: set rate limit
Brief Description: an operator needs to associate customer's volume with certain service level.
Actors: the operator.
Preconditions: the operator has an account on Cloud&Heat.
Basic Flow:

1. the operator log in Cloud&Heat interface
2. the operator sets specified rate limit

Alternate Flows:

1. flow:
   - in step 1 the operator cannot log in due to wrong credentials
   - the operator re-enters access credentials
   - the operator log in successfully and starts from step 2 in Basic Flow
2. flow:
   - in step 2 the operator sets wrong rate limit value
   - the operator restarts from step 2 in Basic Flow

Exception Flows:

- the network connection fails
- the process of updating quota reports an error

*Post**c**onditions*: the specified limit is assigned.

Use-case:create snapshot
Brief Description: a customer wants to create a volume snapshot.
Actors: the customer.
Preconditions: the customer has access credentials.
Basic Flow:

1. the customer log in Cloud&Heat interface
2. the customer creates a snapshot

Alternate Flows:

1. flow:
   - in step 1 the customer cannot log in due to wrong credentials
   - the customer re-enters access credentials
   - the customer log in successfully and starts from step 2 in Basic Flow

Exception Flows:

- the network connection fails
- snapshot creation process reports an error state

*Post**c**onditions*: the snapshot is created.

2.2.4 SafeCloudBox use case

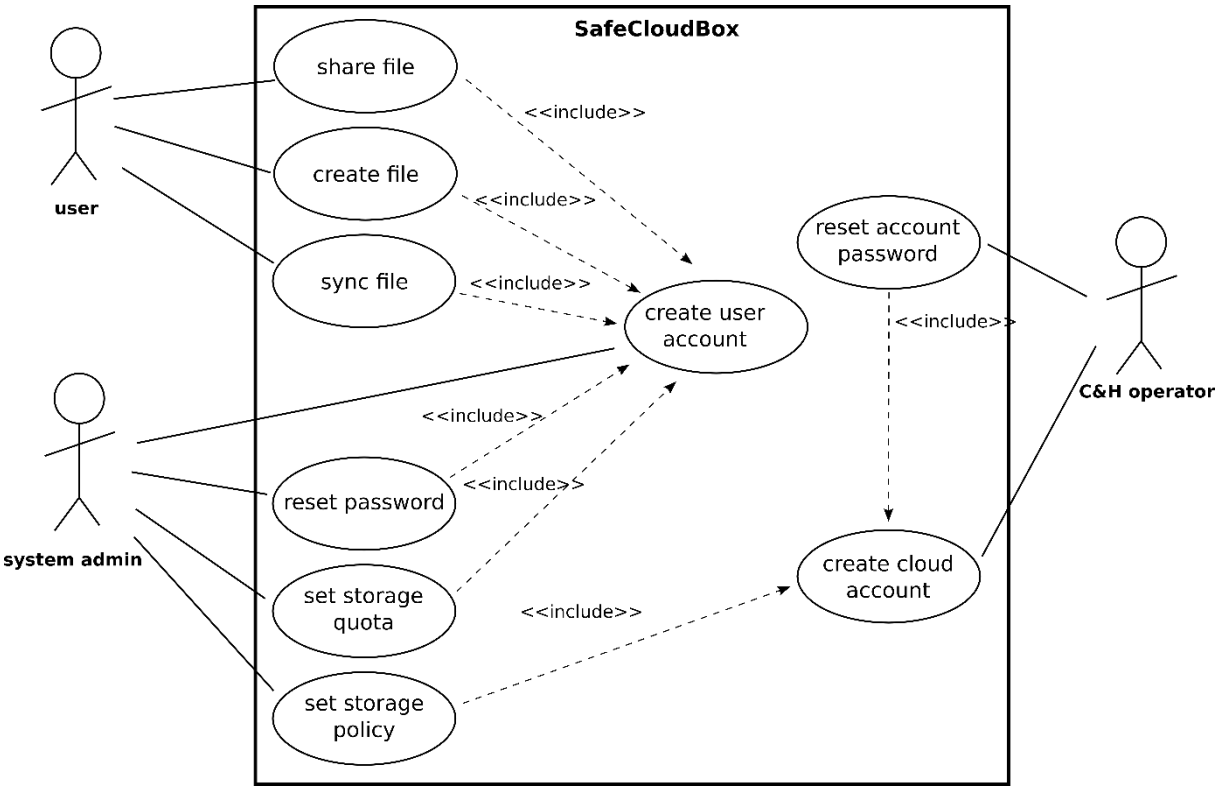

Figure 2: SafeCloudBox use cases diagram.

SafeCloudBox use case has three actors:

- User. A person that uses SafeCloudBox to securely store, sync and share file on our cloud.
- System administrator. A person that configures secure file system policies, creates user accounts to access SafeCloudBox.
- Cloud&Heat operator. A responsible person from Cloud&Heat that takes care of different cloud management operations including setting up cloud user accounts.

2.2.5 SafeCloudBox use case description

Use-case: create cloud account
Brief Description: system administrator requests access to the cloud backend storage.
Actors: Cloud&Heat operator.
Preconditions: the operator has access credentials.
Basic Flow:

1. the operator log in in Cloud&Heat interface
2. the operator creates a cloud user account

Alternate Flows:

1. flow:
   - in step 1 the operator cannot log in due to wrong credentials
   - the operator re-enters access credentials
   - the operator log in successfully and starts from step 2 in Basic Flow
2. flow:
   - in step 2 the operator detects that the account already exists
   - the operator stops the use case execution

Exception Flows:

- the operator cannot log in, the interface is not accessible

- the system fails to create the account

Postconditions: the account for the user is created.

Use-case: set storage policy
Brief Description: system administrator wants to set storage policy (e.g. local data mirroring, archiving, replication factor, data placement).
Actors: the system administrator.
Preconditions: the administrator has access to the SafeCloudBox interface.
Basic Flow:

1. the administrator log in to SafeCloudBox server
2. the administrator sets the required storage policy

Alternate Flows:

1. flow:
   - in step 1 the administrator cannot log in due to wrong credentials
   - the administrator re-enters access credentials
   - the administrator log in successfully and starts from step 2 in Basic Flow
2. flow:
   - in step 2 access credentials to the cloud are missing
   - the administrator finds that the policy has been already set
   - the administrator stops execution

Exception Flows:

- the administrator cannot log in, the interface is not accessible
- the policy cannot be set, secure file system reports an error

Postconditions: the storage policy is set.

2.2.5.1 Use-case: set storage quota

Use-case: set storage quota
Brief Description: limit the storage capacity available to the user.
Actors: system administrator.
Preconditions: the administrator has access to the SafeCloudBox interface.
Basic Flow:

1. the administrator log in to SafeCloudBox interface
2. the administrator sets storage quota

Alternate Flows:

1. flow:
   - in step 1 the administrator cannot log in due to wrong credentials
   - the administrator re-enters access credentials
   - the administrator log in successfully and starts from step 2 in Basic Flow
2. flow:
   - in step 2 the user does not exist
   - the administrator creates an user and start from step 2 in Basic Flow

Exception Flows:

- the administrator cannot log in, the interface is not accessible
- the requested quota exceeds local storage size

Postconditions: the quota is set.

Use-case: create a file
Brief Description: a user wants to create a file.
Actors: the user.
Preconditions: the user has access to the SafeCloudBox interface.

Basic Flow:

1. the user log in to SafeCloudBox interface
2. the user creates a file

Alternate Flows:

1. flow:
   - in step 1 the user cannot log in due to wrong credentials
   - the user re-enters access credentials
   - the user log in successfully and starts from step 2 in Basic Flow
2. flow:
   - in step 2 the file cannot be created, user's storage quota needs to be increased
   - the user requests quota extension
   - the administrator extends the quota and the user starts from step 2 in Basic Flow

Exception Flows:

- the user cannot log in, the interface is not accessible

Postconditions: the file is created.

2.3 Integration with the SafeCloud framework

To increase the level of security and privacy offered to its customers, Cloud&Heat plans to deploy products that will exploit the features of the SafeCloud framework. We consider two integration scenarios, one for each of the products.

2.3.1 Cloud Block Storage

For customers that have strict availability requirements, Cloud&Heat will offer the Cloud Block Storage service with a disaster recovery option. Whenever a data center is down, the customers can be quickly redirected to another available data center. To provide this feature, the set of data centers will be enhanced with cross data center replication. The replication requires data transfer over WAN, which is vulnerable to attacks. Hence, Cloud&Heat will exploit the SafeCloud private communication middleware to ensure secure data transfer. Private communication will provide protected channels that limit the availability and visibility of a service to authorized clients. In particular, Cloud Block Storage will use advanced port knocking techniques. The technique relies on PKI-based certificates, and Cloud&Heat will use internal certificate authority (CA) to certify the keys.

Figure 3 presents the integration scheme of Cloud Block Storage using the SafeCloud framework. The secure file system uses the block storage service as a storage backend. The block storage services of individual data centers perform data transfer using the private communication middleware developed by the consortium. Finally, Cloud Block Storage users interact over the standard dashboard (and command line) interface provided by Cloud&Heat.

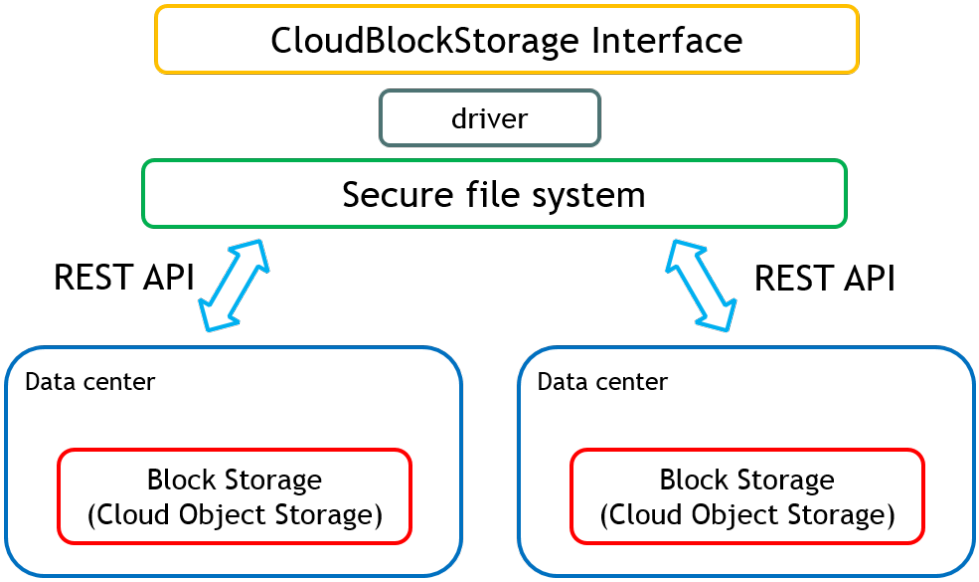

Figure 3: Cloud Block Storage.

2.3.2 SafeCloudBox

Cloud&Heat aims to increase the adoption of its storage infrastructure by offering a SafeCloudBox product that can provide a Dropbox-like interface. In comparison to the popular service, we propose to run SafeCloudBox on the customer side. It could be either trusted cloud or office servers. The process of storing and retrieving data on the cloud will be implemented using the SafeCloud Secure File System as shown in Figure 4. The file system will encrypt and send data to the cloud. The data is secured by the SafeCloud private communication middleware exploited by the Cloud Block Storage. The Secure File System should provide an interface to specify storage policies such as replication factor, data location, and data archiving. As a storage backend the file system uses Cloud Object Storage service offered by Cloud&Heat data centers.

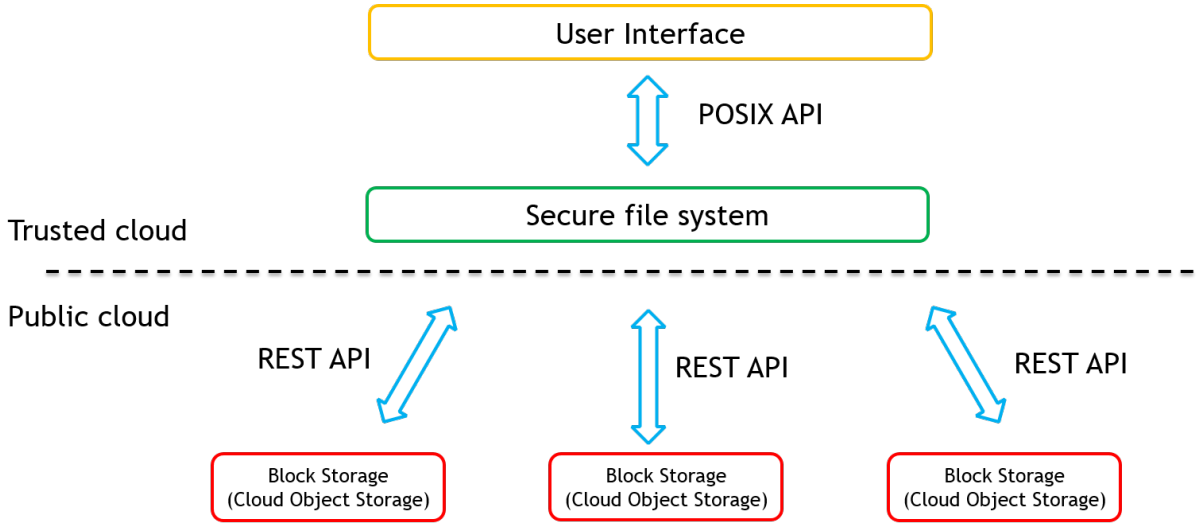

Figure 4: SafeCloudBox integration.

3 Cloud&Heat requirements

3.1 Functional requirements

In this section, we present functional requirements that need to be addressed by the SafeCloud framework to ensure privacy, integrity and security of the data that is stored and processed in the Cloud&Heat infrastructure.

Data-Location-Definition: The SafeCloud framework shall give the possibility to constrain the location of the resources to country boundaries.

Real-Time-Definition: The SafeCloud framework shall give the possibility to manage the real-time guarantees of the computation / storage / network resources. Management shall include the definition of predictable and bounded computation / communication / storage access times.

3.2 Non-functional requirements

3.2.1 Security

- **GDPR-Compliance**: The SafeCloud framework shall be compliant with the EU General Data Protection Regulation [GDPR16].
- **Secure-Resources-Access:** The SafeCloud framework shall give access to its resources only to the authorized user.
- **Secure-Data-Handling**:
    - The SafeCloud framework shall guarantee that data cannot be interpreted by unintended parties.
    - The SafeCloud framework shall guarantee that data cannot be interpreted in transit.
    - The SafeCloud framework shall guarantee that data may not get tampered with, and that integrity of data is maintained.
    - The SafeCloud framework shall ensure that all privacy-sensitive information (e.g., user name, date of birth) is not exposed (e.g., via logging).

3.2.2 Reliability

- **Data-Location-Guarantees**:
    - The SafeCloud platform shall guarantee to store data within the prescribed legal boundaries.
    - The SafeCloud platform shall guarantee to process data within the prescribed legal boundaries.
- **Availability-Storage-Guarantees**: The SafeCloud platform shall guarantee storage availability up to 99.999%.

3.2.3 Interface requirements

- **File Storage**: The SafeCloud platform shall provide interface to define storage policy. The policy defines how many copies will be stored on the cloud. If the users want to use the cloud as an archival storage, then they should be able to set the threshold that defines when the data is stored on the cloud.

4 Conclusion

In this deliverable we have presented the design and requirements of the Cloud Storage Platform that will be deployed on the Cloud&Heat data center infrastructure. We have given an overview of the SafeCloud framework, presented the Cloud&Heat use cases based on two products, and described their integration within the framework.

5 References

[GDPR16] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) http://data.europa.eu/eli/reg/2016/679/oj