
MSE CComp SEC 1 – Security for Clouds

Martin Gwerder
Marcel Graf

Table of Content

- Recap
 - Data Protection Laws
 - Comparison Traditional vs Virtual Datacenter
- Securing a Cloud
 - Identity and Access Management (IAM), Authentication, Authorization and Transaction Audit
 - Virtualization Environment
 - Physical Security
 - Interface Security
 - Computing Virtualization Security
 - Network Security
 - Data Isolation, Protection and Confidentiality Protection
- Processes
 - Security Coordination, Operational Security; Incident Management
 - Disaster Recovery
 - Service Security Assessment and Audit
- Standard compliance
 - Interoperability, portability and reversibility

Context

- Always keep in mind that a cloud is not just the virtualisation (NIST criteria)
- May be based on Type 1-3 hypervisor or a container
- A cloud platform is typically shared among multiple players which distrust each other. These parties are (in order to be cost effective) at least one cloud service provider and multiple customers.
- Sharing resources and measures to exploit synergy (such as memory/storage deduplication or cache sharing) augment attack surface.
- A cloud is not weaker in terms of security. It is just more complex and adds thus more points we have to think of. Generally the implementation of a cloud is underestimated security wise and thus weaker.

Swiss Federal Act on Data Protection of 1992

Art. 4 Principles

- 1 Personal data may only be processed lawfully.
- 2 Its processing must be carried out in good faith and must be proportionate.
- 3 Personal data may only be processed for the purpose indicated at the time of collection, that is evident from the circumstances, or that is provided for by law.
- 4 The collection of personal data and in particular the purpose of its processing must be evident to the data subject.
- 5 If the consent of the data subject is required for the processing of personal data, such consent is valid only if given voluntarily on the provision of adequate information. Additionally, consent must be given expressly in the case of processing of sensitive personal data or personality profiles.

Art. 6 Cross-border disclosure

- 1 Personal data may not be disclosed abroad if the privacy of the data subjects would be seriously endangered thereby, in particular due to the absence of legislation that guarantees adequate protection.
- 2 In the absence of legislation that guarantees adequate protection, personal data may be disclosed abroad only if:
- a. sufficient safeguards, in particular contractual clauses, ensure an adequate level of protection abroad
 - b. the data subject has consented in the specific case
 - c. the processing is directly connected with the conclusion or the performance of a contract and the personal data is that of a contractual party
 - d. disclosure is essential in the specific case in order either to safeguard an overriding public interest or for the establishment, exercise or enforcement of legal claims before the courts
 - e. disclosure is required in the specific case in order to protect the life or the physical integrity of the data subject
 - f. the data subject has made the data generally accessible and has not expressly prohibited its processing
 - g. disclosure is made within the same legal person or company or between legal persons or companies that are under the same management, provided those involved are subject to data protection rules that ensure an adequate level of protection.
- 3 The Federal Data Protection and Information Commissioner (the Commissioner, Art. 26) must be informed of the safeguards under paragraph 2 letter a and the data protection rules under paragraph 2 letter g. The Federal Council regulates the details of this duty to provide information.

Comparison of Physical vs Virtual Datacenters

Physical

- Physical presence in the location may be required to destroy, remove, copy or damage assets.
- Privileged access to root consoles or similar is only available on premises.
- Image copies of machines are hard to reuse as only seldom the same HW is available upon failure.
- Access control is easy as there are physical access controls installed on premise.
- Location of physical machine is always known
- Network boundaries are physical and may not be bridged by accident.
- A normal “full breach” of a physical machine only discloses the data of the respective system.
- Hardware failure of a host affects just one system. The failed system may require hours to days to recover.
- Redundancy must be explicitly built.

Virtual

- Assets are destroyed, removed, copied over networks.
- Privileged access is available over the network.
- Image copies allow to recover or copy any machine on any infrastructure within minutes.
- Access control is hard as network access is broadly available and thus needs to be separated into admin and “regular” traffic.
- Location of a virtual machine is volatile and may change during operation.
- Network boundaries are logical and may be bridged or even breached without visible impact.
- A normal “full breach” of a cloud host discloses the data of many systems (either full host or full cluster).
- Hardware failure of a host affects many systems. The failed systems may recover within minutes
- Redundancy (on HW level) is implicitly available.

- Clouds have typically not just one authentication and authorization source. A common, assessed trust model has to be applied on all authentication and authorization sources.
- Access management to a cloud needs to cover more levels than in a regular datacenter. Levels may be: Hardware access, full virtual infrastructure control, full virtual infrastructure access, partial virtual infrastructure control, and partial infrastructure access. Furthermore the regular access control to system and data is still required.
- A common IAM is a “must” in a cloud. It is the foundation for a successful audit.
- Important to remember: An Identity Management System combines typically *multiple* sources of *authentication and authorization* sources to a single (meta) source. The original sources do typically not trust each other. This meta source may then be subdivided again according to requirements.

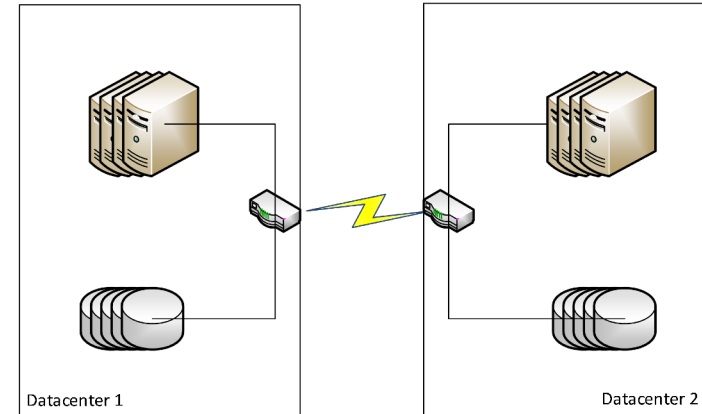
Virtualization environment: Physical environment

- Physical security is required in a cloud environment on the same technological level as in a traditional datacenter.
- Important to note:
 - The likelihood of a breach is in both cases the same
 - The impact of a physical breach is typically the same or higher.
- In order to guarantee availability we still need to have multiple sites

Securing a Cloud

Virtualization environment: Physical environment – Example

- VM storage is typically coupled asynchronously or even periodically mirrored. Synchronous replication is very hard and expensive to achieve.
- Host clusters typically do not span multiple physical datacenters or they are likely to break redundancy on VM level.
- An outage of a physical host is typically recovered within minutes automatically without significant data loss on disk (memory may be lost).
- An outage of a datacenter is typically recovered within hours with typical loss of up to 24 hours of data (due to mirroring) and failover and fall back are typically manual.



Virtualization environment: Interface Security

- Access to logical interfaces (typically root consoles or switches with specific VLANs) needs to be restricted in a cloud as in physical environments. The complexity is typically higher as a cloud combines multiple legal entities.
- VLANs of multiple customers must be streamlined. This may be hard to fulfill and is usually done by giving access over VLAN synonyms instead of the regular numbers.
- Access to root consoles and interfaces may be subdivided further within a cloud service customer.

Virtualization environment: Computing Virtualization Security

- Hypervisors must shield the (sometimes overcommitted) computing resources from attacks.
- Ideally a cloud provider provides basic security such as anti malware on host level
- Sharing resources in overcommitted systems may result in security relevant data exposures. Some of the exposures (e.g. RAM or disk) may be addressed by zeroing. However, in some cases such as a cache this does not work. Most of the known, general attacks on virtualization systems do address this vector.
Typically used vectors are:
 - Timing information from other virtual machines and their core adherence
 - Timing information when accessing Cache
 - Timing information when writing to deduped memory or storage
- Hardware security features are typically not available in today's cloud environment (or badly supported).

Securing a Cloud

Virtualization environment: Network security

Traditionally multiple networks have to be physically separated on a host.

- **Guest networks**

Although segregation within guest networks is very important these networks are considered the last sensitive ones in terms of security.

- **Admin network**

This network port allows privileged access to the full environment without tenant restrictions. Therefore access to this network should be limited to a very restricted set of users.

- **Heartbeat network**

The heartbeat network is used to exchange heartbeat information within nodes. As reliability of these connections is vital for the proper functioning of a virtualization cluster this interface is kept physically separated from other networks or sometimes combined with the admin networks (depending on the number and kind of users on the admin network).

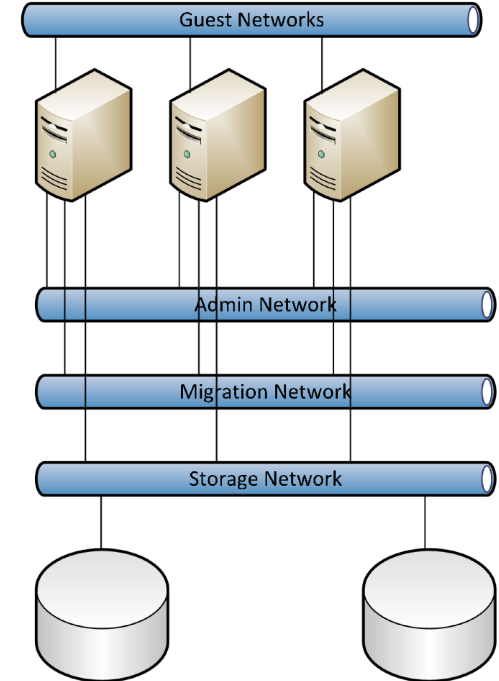
- **Migration networks**

As this network contains the unencrypted VM images or CPU states (in case of fault tolerant nodes). This network is highly sensitive and bandwidth-intensive. Physical medium should never be shared as saturating the media may heavily affect negatively neighboring networks.

- **Storage network** (includes regular and backup networks)

This network should be separated from any client traffic as here pass typically unencrypted VM content. Even encrypted the VM content is typically considered very sensitive and thus needs to be separated from other traffic.

This is a high-bandwidth network. Same arguments as above apply.



Security coordination, Operational security, and Incident management

While these criteria do apply to all (cloud and non-cloud) infrastructures, implications may be a bit different on cloud systems:

- Data Isolation

Data isolation is usually done on a per-tenant basis in cloud environments. An isolation using encryption is typically not regarded sufficient as this would leak meta information.

- Data protection

This is done by encrypting disks and backups and applying ACLs or encryption to data structures within a cloud.

- Confidentiality protection


It is important to verify that confidentiality protection is not outlevered by a cloud system (e.g., securely wiping data in a VM-level should have similar effects on the physical system).

Security coordination, Operational security, and incident management

- It is important to understand that security coordination, operational security, and incident management become more complex as multiple legal entities are involved in such a process. *Liability* or *impact* become weak terms as they heavily depend on the point of view.
- Operational security is not as easy to achieve as in physical environments. There are always multiple players of possibly different legal entities involved and not all players have the same access to information. Communication becomes therefore a key in cloud security and incident management.




- Fast and possibly automated disaster recovery is a key strength of a cloud system.
- Please note that not all type of strategies lead to the same level of disaster resilience. For example:
 - Types:
 - Image backup
Quickly allows to reinstall a machine. Typically no or limited access to files and only full backup strategy available. Hard to compress without knowledge of the underlying FS.
 - File backup on guest system
Allows single file restore. Does typically not cover vital parts of the OS (e.g., partition table). Consistency problems remain the same but are slightly different as the timespan to be covered for a file backup is typically higher.
- Please note that some systems require considerably more time when booting from scratch than to recover from a partial outage (e.g. Microsoft Active Directory). It might sometimes be advisable to keep at least one instance of a redundant system on a physical system.

- While clouds cover the regular services just as in a normal datacenter they got additional risks due to their «self service»-nature
- Audits may span multiple legal entities.

- Cloud services are interoperable only in limited ways. While VM migration within a cluster is «daily business», a migration between two clouds (of same or different type) requires usually a set of common factors.
- Please differentiate:
 - Online interoperability
Capability to move a *running* virtual machine between clouds 
 - Offline interoperability
Capability to move a *stopped* virtual machine between clouds
 - Physical-to-virtual (P2V) and virtual-to-physical (V2P)
Capability to convert a physical machine into a virtual one and the reverse

Standard Compliance

Common Disk File formats

- VMDK
Initially developed by VMware. Part of OVF. Supports thin and thick provisioning. 
- QCOW2
Main disk file format for QEMU. Supports thin provisioning, AES encryption, copy-on-write and transparent decompression. 
- VDI
Developed by Innotek for Oracle VirtualBox. Supports thin and thick provisioning.
- VHD
Developed by Connectix. Mainly used in Microsoft Virtual PC. Supports thin and thick provisioning.
- RAW
A disk represented as bunch of blocks without any additional structure. This format does not support thin provisioning, deduplication, or similar features.
- FVD 
Developed by IBM for QEMU. Supports deduplication of content across VMs (Meta container)