

Research report Data Centre Virtualisation

Author: Gergely Somogyi (Student number: 1814098)

Institute: University of Wales – Trinity Saint David

Course: BSc Cloud Computing, Year 3, Term 5

Module: Data Centre Virtualisation (ACUA6001_LON)

Lecturer: Koushik Modak

Contents

1. Introduction	3
2. Scenario 1 - Report one	4
2.1. Virtualized data centre	4
2.2. Design and architecture	4
2.3. Resources	5
2.4. Hypervisor.....	6
2.5. Operating a data centre	7
3. Own data centre	7
3.1. Installation	7
3.2. Operation.....	7
3.3. Monitoring.....	8
4. Recommendation	9
5. Scenario 2 – Report 2.....	10
5.1. Introduction	10
5.2. Security measures.....	10
5.3. SAN importance	11
5.4. Threatening	11
6. References.....	13

1. Introduction

My goal in this research report is binary: one, to I write a recommendation for UWTSD how to virtualise its central IT operation and second, write a report about security policy and its influence on the organisational design at ABC Data Ltd.

Report one

At first, I glance what the virtualized data centre requirements are, mentioning its architecture, design, hypervisor`s, physical limitations, energy supply, scalability, and sustainability. Also present the benefits and drawbacks of a virtualized data centre compare a non-virtualized one`s. So far, the report is mainly theoretical, pathfinding what leads closer to the solution. Second, I investigate an own running data centre-based scenario: what is the specification if an institution runs and maintains its own data centre. Then look through the elements and fulfilments of an outsourced data centre, when a third party responsible to manage the data centre. Last two chapter more focused on practical parts, but not ignore the general theoretical notes about solution features. After I brief what written before I give my recommendation to UWTSD regarding virtualization.

Report two

ABC Data Ltd. is an organisation using virtualised technology to provide a virtualised data centre solution for fee paying customers. My report is focusing to explain the importance of security measures. I write about what security measures should imply for all stakeholders who regarding to ABC Data Ltd. Then look through what kind of threatening`s would face a virtualized data centre. Finally mention that a well-designated storage area network (SAN) how to help and avoid these threatening`s, and how big role a proper disaster recovery plan plays in a company`s life such as ABC Data Ltd.

2. Scenario 1 - Report one

2.1. Virtualized data centre

The main goal of a data centre is to provide better and more secure IT services to users. The rapid growth of data demand challenges IT staff all over the globe. The main objectives to use virtualized data centres are as follows:

- “The isolation of environments in a consolidated structure
- The aggregation of discrete resources into a shared pool
- The simplification of operational procedures, preferably with the enablement of automation technologies” [2]

Data centre virtualisation is an operation of designing, evolving, and deploying it on a virtualization environment. This process results in a virtualized, cloud and collocated virtual/cloud data centre. The existing data centre facilities are used to provide multiple data centres on the same physical framework, to gain better performance and reduce operating costs.

2.2. Design and architecture

To design a data centre first consider its requirements:

- “Cloud Servers, i.e. the Virtual Machines created on VMware or Hyper-V hypervisors with redundancy.
- Virtual Switches, switch-like devices that can be used to create private networks between the various servers.
- Public IPs, to grant external (WAN) access.
- Unified Storages, virtual storage units to have a shared space between the various Cloud Servers.
- Balancers, which can be used to distribute the workload balancing between two or more Cloud Servers (with identical configuration settings and stored data).”[6]

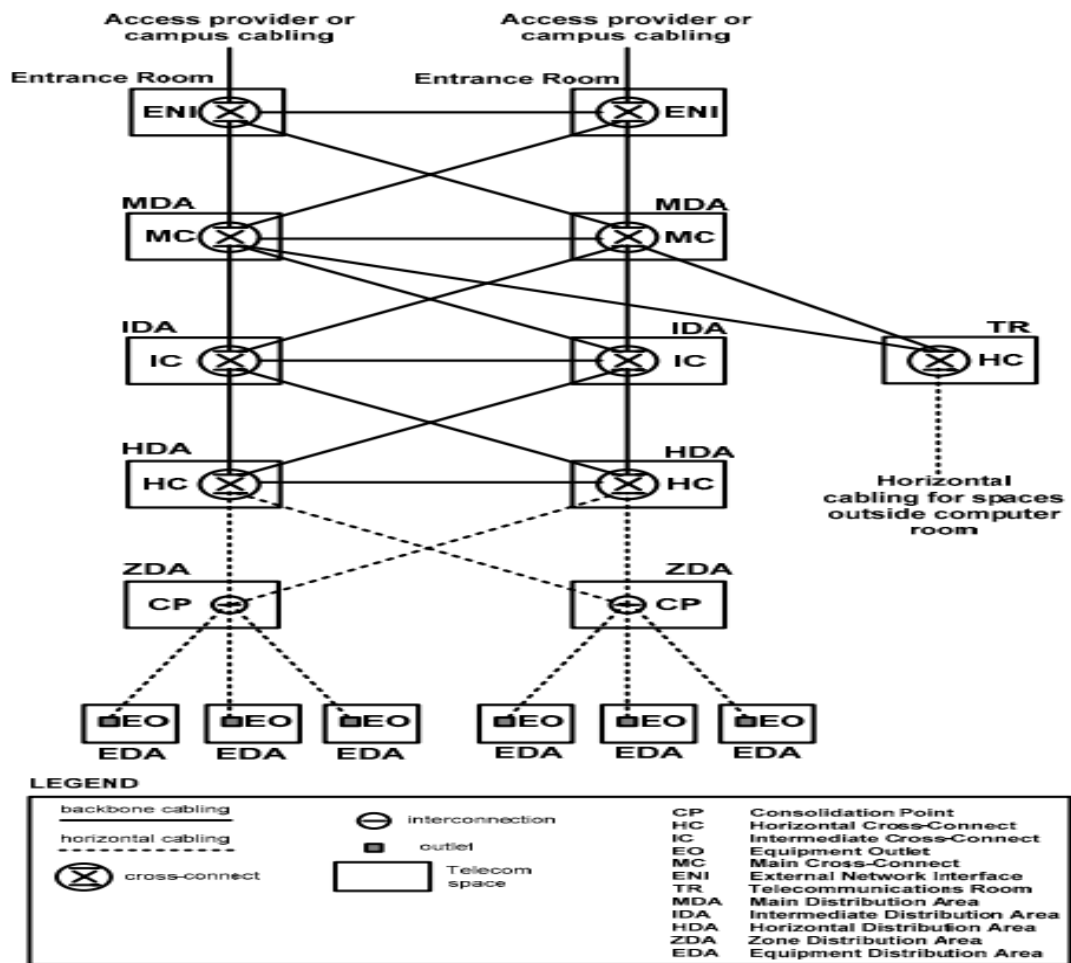


Figure #1: Example of data centre topology – Source: [5]

2.3. Resources

The success of the solution is due to the following main aspects:

- Easy operation;
- Less hardware, less failure;
- Flexible scalability and flexibility: the desired computing and storage needs can be efficiently expanded.
- An upgradeable platform that is time-resistant, maximizing the return on TCO / ROI costs, as it can support growing micro-service architectures and containerization technologies in addition to server virtualization and the applications running on it, but also collaboration with cloud-based services is far from the capabilities of the system.

“Those available services allowed me to build a Data Centre based on a typical edge-origin architecture featuring the following elements:

- 1 pfSense Firewall and VPN Server (one of the two Aruba Cloud standard firewall VM templates, the other one being Endian)
- 1 NGINX Reverse Proxy on a CentOS 7.x virtual machine

- 1 IIS Web Server on a Windows Server 2016 virtual machine
- 1 SQL Server Database on a second Windows Server 2016 virtual machine
- 1 NGINX Web Server on another CentOS 7.x virtual machine
- 1 MariaDB Database on a third CentOS 7.x virtual machine”[6]

2.4. Hypervisor

There are two types of hypervisor exist:

- Type 1: running directly on premise’s hardware
- Type 2: running on a host operation system

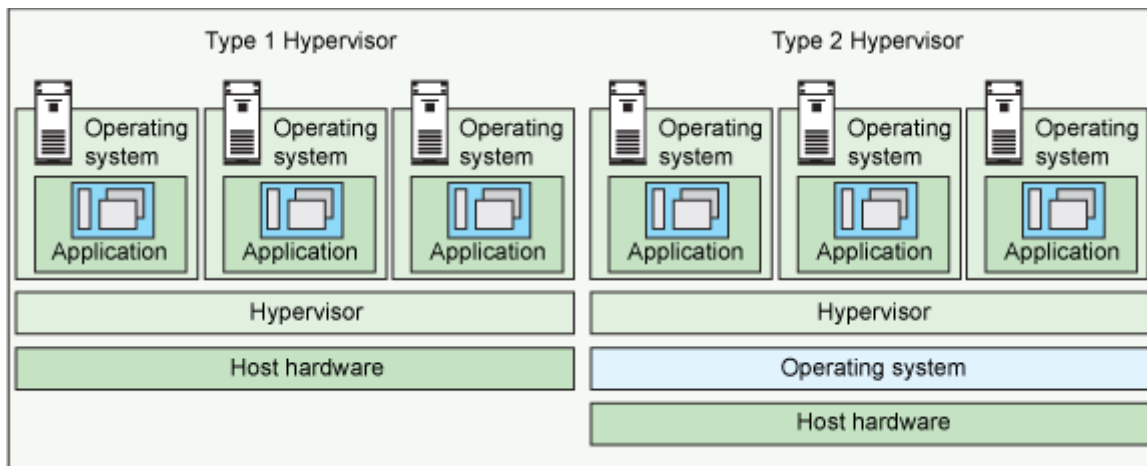


Figure #2: Type 1 and Type 2 hypervisor, source: www.ibm.com

Hypervisor Type	Benefits
Type 1	- Much better performance - Reduced resource usage - Better firmware location security - Runs virtualized production environments - Need active administration
Type 2	- Plain set up - Simple managing - Software-based virtualization is compatible with wide range of hardware - No need dedicated admin - Test multiple operating systems - Full access to Windows or Linux drivers

2.5. Operating a data centre

Users access the applications on a virtual machine running on one of the physical servers located in the data centres and upload their data to the cloud. It is becoming less and less important for them exactly in which data centre, on which storage the data was saved. Virtualisation has resulted in a significant change in the structure of data centres. This can be observed in physical infrastructure, network configuration, and application performance. The physical infrastructure is based on modular cabling systems, which typically provide fibre optic and structured copper cable connections for high-density and high-speed network devices. The increased bandwidth demand reaches 10, 40 or even 100 Gbps. Each application must receive the bandwidth that is essential to it and minimize packet loss, latency, and changes in the order in which packets arrive at their destination. Application performance is affected by the physical infrastructure and network configuration but is highly dependent on other elements of the application infrastructure, such as program code, the server, and the client. Applying appropriate measurement solutions during the installation and operation of data centres is essential to ensure the expected SLA (Service Level Agreement).

3. Own data centre

3.1. Installation

In the final phase of installing physical cabling systems, it is necessary to certify that they meet industry standards. It will then be determined whether the contractor has complied with the installation instructions for the standard component cable system. The customer can verify its compliance based on the measurement report. Once the network active devices have been physically installed and configured, it is essential to examine the network configuration and performance, considering the network requirements of the applications to be installed. In this way, problems can be avoided during live operation, which can easily lead to a deterioration in the quality of services or, in critical cases, downtime.

3.2. Operation

In many cases, there are physical problems with the operation of data centres caused by poor patch cables, interfaces, or other physical elements. Faults can be quickly identified and rectified with suitable cable analysers and testers. The occurrence of higher-level events can also be said to be commonplace. This includes Ethernet technology, which forms the basis of data centre-level operation of data centres, or IP, which is responsible for proper traffic management, and TCP, which provides applications with reliable data transfer between

endpoints. The qualitative and quantitative composition of application traffic, as well as their relative proportions, is important information for data centre operators. Even with proper planning, the performance requirements of a given application may be higher than expected, or its traffic may be moving in the wrong direction, and unwanted traffic may appear on the network. Traffic analysis provides an effective solution to these challenges.

3.3. Monitoring

A feature of network management systems is that they can provide continuous monitoring of the physical elements of the network but are less effective when they are not specifically caused by a physical failure or the combined effect of several failures. In this case, it is advisable to use debugging and troubleshooting solutions that can detect the root of the problem, investigate the affected area as needed, make appropriate recommendations for troubleshooting, and document the survey in a clear, graphical, and textual format. IT operators know that there may be several triggers behind the cause experienced by users, which can be related to network and application performance. This requires the use of appropriate application and network performance monitoring systems that can be easily integrated into existing management and /or operating systems. This allows them to quickly get an answer to which element of the application infrastructure (network, server, client, or application) is causing the slowdown.

The new generation servers used today are much larger and have more resources than running a single or just a few services on them. The creation of server virtualization provided an opportunity to run multiple virtual entities on a single physical server at the same time, thereby increasing the number of services running on the physical machine and the utilization of hardware. With virtualization, we achieved the computing capacity that used to require many separate servers in a significantly smaller physical location and using much less kW of electricity and cooling energy. However, to implement and operate said function, it is not enough to have only servers, we need data storage and a fast network to which all servers have access. The central element of the convergent system thus obtained, the storage unit, is accessed by the servers through a “dedicated” network designed and operated for this purpose.

On Hyper-Converged Infrastructure (HCI) systems, the main purpose of which is to connect embedded disks in physical servers to a RAID array using software (each vendor's own product) so that the required storage capacity is created and distributed between, so there is no need for a dedicated storage system or SAN architecture. The term hyper thus means that in addition to virtualization, even additional functions can be entrusted to individual servers, more precisely to a multi-server hyperconverged system. In addition to virtualization, storage, compression, replication, and some other functions are provided by “mini software” running on servers. Servers used in these systems incorporate components specified by the manufacturer to ensure reliable operation, i.e., 99.999% availability. To build most hyperconverged systems, you will need at least 3 servers, which can be expanded to 64 nodes, or some systems above, and run up to 1000 virtual machines in such an environment. Of course, there is also an HCI solution designed for remote sites, here two physical machines are enough.

4. Recommendation

Select the way of virtualization of an organisation is a hard task. Considering the goal, the budget, the resources, and the time frame, make this decision difficult. Sum up all the details about UWTSD IT department`s challenging:

- 5 different campus, 5 location
- About 10 000 students, wavering in every term
- 24/7 availability of student application, with peak periods of access such as examination periods, enrolment periods
- Sensitive and confidential data handling and storing such as student personal details, reports, dissertations, marks and results
- Possible online education periods, with short time implementing
- Updating all the courses related data`s
- Running e-library

The recommended solution is a SaaS service. A software what contains all requirements: applications, analytic tools, virtual hosts, operating system with provided facilities: data centre, network components, server, and storage. Microsoft Azure meets the requirements.

5. Scenario 2 – Report 2

5.1. Introduction

Today, all security professionals know that maximum protection cannot be achieved, or only to a small extent, with individually and separately applied technical solutions. In contrast to the cost of building and operating systems, it is worthwhile to look for and apply smart and intelligent solutions in the field of integrated protection systems as well. In terms of security a data centres have two aspect of safety measures: physical and non-physical. Physical means to protect the facility`s physical infrastructures and the networks physical parts. Non-physical means the security of the data`s and software`s.

5.2. Security measures

The challenges of integrating security subsystems:

- Quick reaction
- Reducing security risk
- Flexible operation
- Efficient and standard operation,
- IoT explosion

Despite the declining operating budgets, the control and automatic operation of integrated safety systems can be implemented with ever higher levels of availability, energy efficiency and comfort requirements. The surveillance system we supply is a flexibly configurable building management system that can be used to ensure the safety and comfort of people and the efficient operation of buildings and equipment efficiently and reliably. Surveillance software provides managers and managers of all levels with a well-designed, web-like interface that makes it easy to monitor and control one or more buildings. Alternatively, the software allows remote or partially automatic control and monitoring of the facility. The system is based on a client / server architecture and runs on the industry-accepted multi-user, multi-tasking Microsoft Windows Server operating system. Applications running on the server communicate with local controllers and manage a real-time and relational database.

Operators can perform a variety of building management tasks on workstations:

- View and manage alerts
- Timed activities
- Configure the hardware and software components of the connected controllers in the database
- View, manage, and evaluate data collected by various controllers

- Retrieve special screens, cardholder information, and photos from the server
- Making photo ID cards
- Integration
- Access control systems
- Video surveillance system
- Fire alarm, evacuation, property protection system
- Monitoring and optimizing energy consumption
- Lighting control
- Enterprise management systems (eg SAP, PeopleSoft)
- Time and attendance systems
- Maintenance system

5.3. SAN importance

The Storage Area Network consists of SAN subsystems and switches. Devices that contain hard disks are organized into a kind of network through fast connection, and this subnet is available to the servers through the switches. Due to the transparent implementation, there is no wasted capacity, and in the case of record management and transaction management, this solution is unbeatable in speed. An additional benefit of a well-designed network is increased security - you can even create a geographically extensive SAN system that, if properly mirrored, can guarantee data security in the event of an unforeseen disaster.

Some advantages of a SAN:

- Reliable disaster recovery
- Centralized and responsive backup
- Improved data security

Secure data release is also important for use and the company. Administrators can back up storage space with block-level and incremental-level backups. With SAN, it is possible to recover data from multiple applications in the event of any type of disaster. On SAN's switches various type of security measures is possible such as ACL, ADS, isolating users, and departments by virtual SAN, and encrypting data.

5.4. Threatening

A data centre like ABC Data Ltd must face many kinds of possible cyber-attack. The few most common kind of attacks are:

Denial-of-Service Attacks (DoS or DDoS): A DDoS attack is when an attacker floods a network or server with a large amount of traffic to make it impossible for it to function. Such attacks are most used to disable certain websites or applications for days or even longer. **Protection:** Firewall and ISP protection to filter and monitoring traffic, rate limiting, blackhole routing.

Brute Force Attacks: exploiting a weak or common password to gain unauthorised access to then network. Protection: password length and complexity, limit login attempt, two factor authentications.

DNS Infrastructure Exploits: kind of cyber-attack that feats the weakness or vulnerability in domain name system. A few types of DNS attack are Zero-Day attack, Fast Flux DNS, DNS Spoofing. Protection: using SSL certificates, Virtual LANs for transmitted data, OS and all application software are updated.

Web Application Attacks: Injection attacks can be used not only to log in to the application without knowing the username and password, but also to reveal private, confidential, or sensitive information or even to hijack an entire server. Two most common type: SQL injection and cross-sit scripting. Protection: educate users on phishing techniques, input validation.

6. References

- [1] M. Arregoces and M. Portolani, Data center fundamentals. Indianapolis, Ind.: Cisco, 2004.
- [2] G. A. A. Santana, Data center virtualization fundamentals. 2014.
- [3] S. Pham, 2020. [Online]. Available: https://blogs.vmware.com/networkvirtualization/2020/07/securing-data-center.html/?src=ps_5fabcc77c07d7&cid=7012H000001KT05&gclid=bd6e89ba009b1d573ea1e92af8de6826&gclsrc=3p.ds&mssclkid=bd6e89ba009b1d573ea1e92af8de6826. [Accessed: 04- May- 2021].
- [4] B. Felter, "What Are the Most Important Data Center Security Standards", Vxchnge.com, 2019. [Online]. Available: <https://www.vxchnge.com/blog/data-center-physical-security-standards#:~:text=%20Important%20Data%20Center%20Security%20Standards%20%201,than%20a%20simple%20locked%20door.%20Manned...%20More%20>. [Accessed: 04- May- 2021].
- [5] Telecommunications Infrastructure Standard for Data Centers. Arlington: TELECOMMUNICATIONS INDUSTRY ASSOCIATION Standards and Technology Department, 2012.
- [6] "How to create a secure virtualized Data Center on Aruba Cloud Pro", Ryadel, 2021. [Online]. Available: <https://www.ryadel.com/en/aruba-cloud-pro-create-data-center-vpn-tutorial-guide/>. [Accessed: 04- May- 2021].
- [7] G. Smith, "8 Steps to Building a Modern Datacenter", www.wired.com, 2018. [Online]. Available: <https://www.wired.com/insights/2013/06/8-steps-to-building-a-modern-datacenter/#:~:text=8%20Steps%20to%20Building%20a%20Modern%20Datacenter%201,in%20datacenters%20are%20ending.%20...%20More%20items...%20>. [Accessed: 04- May- 2021].
- [8]"The Advantages of a Storage Area Network (SAN)", BECA, 2019. [Online]. Available: <https://www.becacorp.com/the-advantages-of-a-storage-area-network/#:~:text=The%20advantages%20of%20a%20SAN.%201%201.%20Reduces,Increased%20scalability.%205%205.%20Reliable%20disaster%20recovery.%20>. [Accessed: 04- May- 2021].
- [9] K. Cross, "The Top 5 Data Center Threats You Need to Know", Infosecurity Magazine, 2014. [Online]. Available: <https://www.infosecurity-magazine.com/opinions/the-top-5-data-center-threats/>. [Accessed: 04- May- 2021].
- [10]"What is DDoS Attack?", www.cloudflare.com, 2021. [Online]. Available: <https://www.cloudflare.com/en-gb/learning/ddos/what-is-a-ddos-attack/>. [Accessed: 04- May- 2021].
- [11] I. Rehman, "What Is A Brute Force Attack?", The Official Cloudways Blog, 2018. [Online]. Available: <https://www.cloudways.com/blog/what-is-brute-force-attack/>. [Accessed: 04- May- 2021].

[12]"Most Common Web Application Attacks and How to Defend Against Them", EC-Council Official Blog, 2021. [Online]. Available: <https://blog.eccouncil.org/most-common-web-application-attacks-and-how-to-defend-against-them/>. [Accessed: 04- May- 2021].