



Assignment Title: **A research report on Data Centre Virtualization**

Module Title: **ACUA6001 Data Centre Virtualization**

Lecturer: **Koushik Modak**

Student Number: **1815743**

Student: **Anghel Sandra-Stefania**

## Abstract

*The aim of this report is to present an overview of virtualisation and its benefits and to identify the advantages of using cloud solutions offered by Amazon Web Service instead of building an on-premises data centre. On top of it, the report will focus on the importance of security policies and how the security is increased by using Storage Area Network.*

**Keywords** – *on-premises data centres, cloud services, Amazon Web Services, Storage Area Network, virtualisation, hypervisors, scalability, efficiency, energy consumption, fault tolerance, security*

## Table of content

|                                                        |    |
|--------------------------------------------------------|----|
| Introduction.....                                      | 1  |
| Research Methodology .....                             | 2  |
| Literature Review .....                                | 2  |
| Benefits of Virtualisation.....                        | 6  |
| Implementation of Cloud Computing in organisation..... | 6  |
| Scenario 1: UWTSd.....                                 | 8  |
| Scenario 2: ABC Data Ltd .....                         | 16 |
| Conclusion .....                                       | 20 |
| References.....                                        | 21 |

## List of figures

|                                                                                |    |
|--------------------------------------------------------------------------------|----|
| Figure 1: Services offered by IaaS, PaaS, and SaaS .....                       | 2  |
| Figure 2: High-level diagram of storage virtualisation.....                    | 3  |
| Figure 3: High-level diagram of network virtualisation .....                   | 3  |
| Figure 4: Data Centre common components.....                                   | 4  |
| Figure 5: Hypervisor type 1 and Hypervisor type 2 diagram representation ..... | 5  |
| Figure 6: 7- Tiles Aisle Pitch .....                                           | 9  |
| Figure 7: AWS global infrastructure map.....                                   | 9  |
| Figure 8: AWS data centre in Didcot.....                                       | 10 |
| Figure 9: AWS Auto Scaling.....                                                | 11 |
| Figure 10: AWS availability zones and fault tolerance.....                     | 12 |
| Figure 11: Physical security layers .....                                      | 13 |
| Figure 12: Zero-Trust model .....                                              | 13 |
| Figure 13: AWS equipment for physical security.....                            | 15 |
| Figure 14: AWS perimeter security.....                                         | 15 |
| Figure 15: AWS solar farm .....                                                | 16 |
| Figure 16: Example of data centre access ticket.....                           | 18 |
| Figure 17: SAN Component Layers [24] .....                                     | 19 |
| Figure 18: LUN Zoning and Masking [24].....                                    | 20 |

## List of tables

|                                                                           |   |
|---------------------------------------------------------------------------|---|
| Table 1: Comparison between hypervisor type 1 and hypervisor type 2 ..... | 5 |
|---------------------------------------------------------------------------|---|

# Introduction

The need of storage and processing data has a long history, starting with the period of World War II, when in 1946, the United States Army was able to store its artillery range tables using the first general-purpose computer ENIAC (Electronic Numerical Integrator and Computer) invented by John Mauchly and Presper Eckert.

The evolution continued with the invention of programmable processor by Intel, in 1971. It was a processor used to customized multiple electronic devices. In the same period, Xerox Alto was the first machine that supported graphical UI and large internal memory storage and ARCnet built the first LAN (Local Area Network), able to connect up-to 255 devices.

The most remarkable period was represented by the appearance of personal computers and Network File Systems protocol which highlighted the 1980s as the “boom” of computer industry. From that moment the users can access files over the network as they did on a local storage.

But local storages weren't enough, and businesses needed a dedicated space where they can store and process large amount of data. The beginning of 1990s period marked the appearance of the data centre concept as a solution of co-locating and interconnecting multiple servers in the same “room” capable to solve the businesses' requirements [1] [2]. Miniman [3] defined a Data Centre as being the physical place where multiple dedicated servers for storing and computing data are connected. However, the businesses' needs, and the technologies have changed, and a data centre is no longer just a “room”. Building a data centre requires a detailed analysis of the physical building location, building and floor layout, electrical and mechanical system, security regulations, cost, and scalability and can cause an increased cost and effort [3]

Nowadays, as an effective alternative to traditional on-premises data centres, multiple cloud providers offer cloud solutions, but businesses need to decide which approach is suitable based on their needs and based on a detailed analyse which includes aspects as cost, design, scalability, availability, performance, efficiency, and security.

## Research Methodology

In this report, the solutions for the two required scenarios, were formulated using a qualitative research method. The following questions were addressed:

- How virtualisation works and what it's benefits?
- What are the considerations of using cloud solutions instead of building on-premises data centres?
- How security can be ensured in a on-premises data centres and how Storage Area Network security works?

These questions are the foundation for performing exploratory research on existing on-premises data centres, existing solutions offered by Amazon Web Services cloud provider and security benefits that Storage Area Network has and the importance of security policies.

## Literature Review

Data Centres contains components and technologies like computing, storage and network hardware, virtualisation, automation and are designed using a modular architecture to support high-availability, scalability, performance, automation, and increased security.

Virtualisation is the technology that creates a virtual representation of the physical hardware able to run multiple virtual machines. Each virtual machine is an isolated software that contains an operating system and a set of applications. [4] However, it is essential to understand that virtualisation can be implemented on different levels which results in a set of virtualisation's types:

- Cloud virtualisation [5]

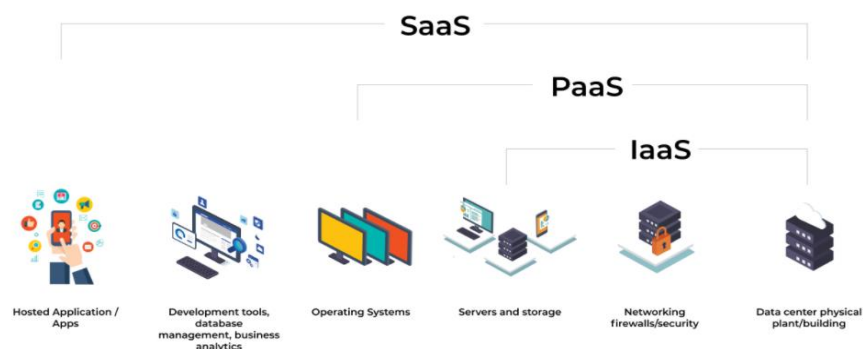


Figure 1: Services offered by IaaS, PaaS, and SaaS

This type of virtualisation became very popular in the last years, as many cloud providers offers services organized as Infrastructure as a Service (IaaS): virtual servers, storage devices or networks; Platform as a Service (PaaS): virtual deployment tools and solutions, databases; Software as a Service (SaaS): known as the most abstract set represented by the software applications that can be directly used on the cloud.

- Storage virtualisation [6]

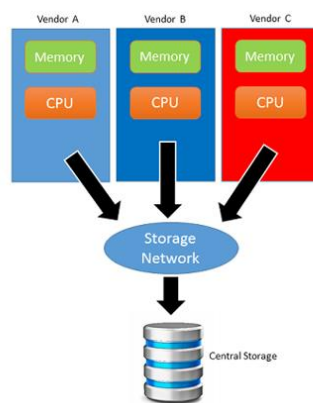


Figure 2: High-level diagram of storage virtualisation

Using storage virtualization, all the storage units are centralized, accessed, and manage from a single storage device. This central location is known as “single shared pool” used by each virtual machine to access the storage based on it’s need. The usage of storage resources is maximized across the network.

- Network virtualisation [7]

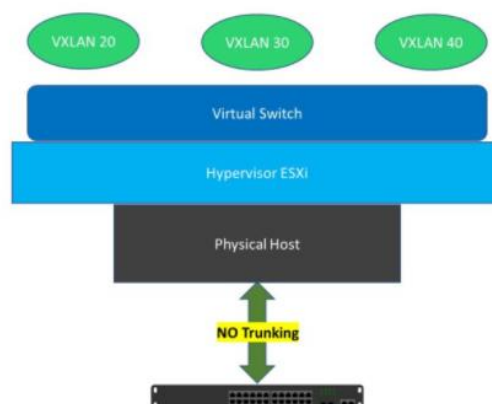


Figure 3: High-level diagram of network virtualisation

In the network virtualisation, the hardware (routers, connections, switches etc) are virtualized into the hypervisor and the administrator can manage them using direct access to the physical hardware. This type includes *software-defined networking* (SDN) responsible for virtualizing the control plane which is controlling the network traffic routing and *network function virtualization* (NFV) which refers to firewalls, traffic analysers or load balancers.

Figure 4 illustrates common data centre' components.

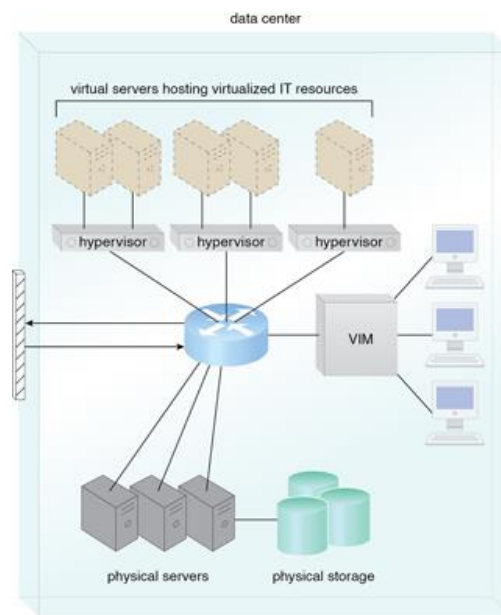


Figure 4: Data Centre common components

One of the most important components is represented by the hypervisor. A hypervisor is defined as a software responsible for creating virtual machines. There are two types of hypervisors: type 1 (also called “bare-metal” hypervisor) and type 2 (also called “hosted” hypervisor). The main difference between them is represented by the way that they run. Type 1 hypervisor runs directly on the underlying physical hardware having direct access to CPU, memory, and storage. On the other hand, type 2 hypervisor runs directly on the host operating system.

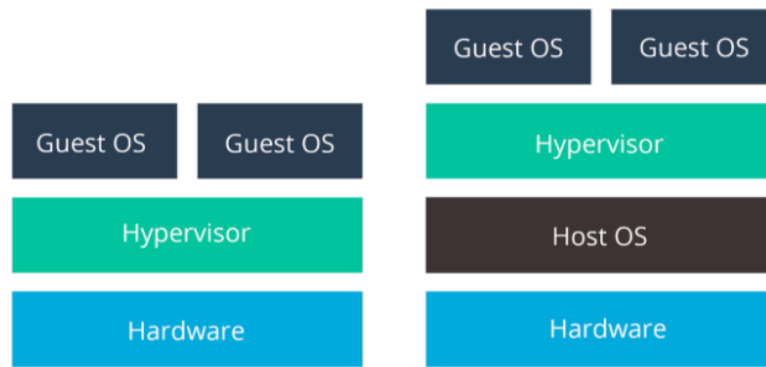


Figure 5: Hypervisor type 1 and Hypervisor type 2 diagram representation

Every virtual machine created has its own operating system (called “guest” operating system) and set of applications. [8] [9]

| Criteria                | Type 1 hypervisor                                        | Type 2 hypervisor                                                                           |
|-------------------------|----------------------------------------------------------|---------------------------------------------------------------------------------------------|
| <b>Known as</b>         | Bare-metal or Native                                     | Hosted                                                                                      |
| <b>Running location</b> | Directly on the underlying physical hardware             | On an operating system                                                                      |
| <b>Virtualisation</b>   | Hardware virtualisation                                  | OS virtualisation                                                                           |
| <b>Operation</b>        | Guest OS and applications run on the hypervisor          | Runs as an application on the host OS                                                       |
| <b>Speed</b>            | Faster                                                   | Slower because of OS’s dependency                                                           |
| <b>Performance</b>      | Higher performance as there is no need of a middle layer | Slower because of existence of the middle layer represented by the host OS                  |
| <b>Security</b>         | Increased security                                       | Less secure as the host OS can be affected which results into the hypervisor to be affected |
| <b>Examples</b>         | VMWare ESXi<br>Microsoft Hyper-V<br>Citrix XenServer     | VMWare Workstation Player<br>Microsoft Virtual PC<br>VirtualBox                             |

Table 1: Comparison between hypervisor type 1 and hypervisor type 2

## **Benefits of Virtualisation**

Even if we are talking about on-premises or cloud-based virtualisation, it comes with a set of benefits [9]:

- Resource efficiency

Without virtualisation, each server requires its own physical hardware (CPU, RAM etc.) that needs to be purchase and configured. In most cases, it is not used on its maximum capacity and has operating systems (OS) limitations as the applications can run only on the OS installed on the server.

- Easier management

Administrators can easily define a set of virtual machines where the processes of deployment and tools configurations can be automated. Also, the security is increased as the same policies are applied against all resources.

- Reduce or eliminate downtime and reduce cost

This benefit is essential for business continuity. If the businesses' requirements are changes and additional resources are needed, they can be provided without no downtime by adding additional virtual machines. Cost is also reduced, as there is no need of up-front physical resources purchased and once a resource is no longer needed it can be easily released.

- Energy Savings

In the context of global environment where the energy consumption becomes a concern, virtualisation can bring a huge impact as the need of power and cooling is considerable reduced. VMWare mentioned [a] than the energy consumption might be decreased by 80% using virtualisation solutions.

## **Implementation of Cloud Computing in organisation**

A massive migration to Cloud Computing technologies was observed during the last years. Businesses started to take advantage of the benefits exposed by different cloud providers like Amazon Web Services, Microsoft Azure, Google Cloud, Salesforce, or IBM Cloud. Instead of building their own data centres, the organisations are using the cloud infrastructure and services which has a considerable impact on different aspects such as [10] [11]:

- Cost

The organisation is not needed to buy physical equipment and it can directly use the cloud resources only when they need them following a model called “pay-as-you-go”.

- Scalability

The organisation can increase or decrease resources based on their business needs. For example, if a website has an increased number of sales during a period, then additional virtual machines can be quickly spin up and once the period is over, they can be released. This ensures business continuity without additional physical hardware purchased.

- Backup and disaster recovery

Cloud providers offers multiple regions, pair-regions, and availability zones. Data is replicated in different data centres, and it is quickly restored after a disaster event. Based on Salesforce report, 20% of cloud consumers has disaster recovery in less than 4h, comparing with only 9% of the on-premises data centre costumers.

- Security

Security is a critical aspect for any business. Cloud providers have more dedicated security teams and expertise, and they are constantly investing and following the best practices and regulations. Non-cloud customers can ensure the same level of security but with an additional cost and effort.

These are only several of the benefits that are taking in consideration for the businesses to migrate to cloud. For a new organisation, might be easier to just start with a cloud solution instead of building its own data centre. On the other side, existing businesses need to make a detailed analysis before deciding to migrate to cloud. This analysis includes and is not limited to:

- Identify the reason and needs for migrating to cloud
- Choose the cloud environment (cloud provider, cloud model)
- Determine the price of the migration (use pricing calculators offered by chosen cloud provider)
- Decide the migration strategy (known as six Rs of migration) which includes [12]:
  - Rehosting - the on-premises environment is copied in cloud. This might be the fastest solution, but can bring limitations in the future

- Replatforming - a combination of rehosting and changes to accommodate cloud requirements
- Repurchasing - applications are moved to new cloud services (mostly in Software as a Service scenarios. For example, a Customer Relationship Management software is moved to Salesforce)
- Refactoring - rebuilding applications. This might be a longer solution but you a bigger flexibility in the future
- Retiring - during the analysis phase, the business might identify applications that are no used and they can be excluded from the migration
- Retaining – this strategy comes in place when the applications are not ready for being migrated, because of different reasons (e.g., compliance compatibility) and the migration is postponed for a later review

A business should decide to migrate to cloud only if it makes sense and brings benefits.

## **Scenario 1: UWTSD**

UWTSD is presenting the following case study: *“UWTSD have decided to virtualise its central IT operation and to build a virtualised Data Centre to centralise UWTSD’s servers and services.”*

The proposed solution for UWTSD is based on a detailed analysis between the option of creating its own data centre or the option of using the services provided by Amazon Web Services (AWS) cloud provider. This analysis includes considerations as physical limitations, scalability, fault tolerance, security, and energy consumption.

### **Physical limitations**

UWTSD has one of the options to create a physical data centre. This option is possible with a detailed analysis and plan. One of the main considerations is represented by the physical location of the data centre. The best practices suggest avoiding high-risk areas where natural disasters (earthquakes, avalanches, hurricanes or very high or very low temperatures) can happen. The area shouldn’t be highly populated, and energy and water utilities are mandatory. The building’s structure is also an important criterion, as it needs to be high enough, with sizeable floors and a small number of windows where the racks will be installed. The racks are organized based on “7-tile aisle pitch” arrangement [13] [14].

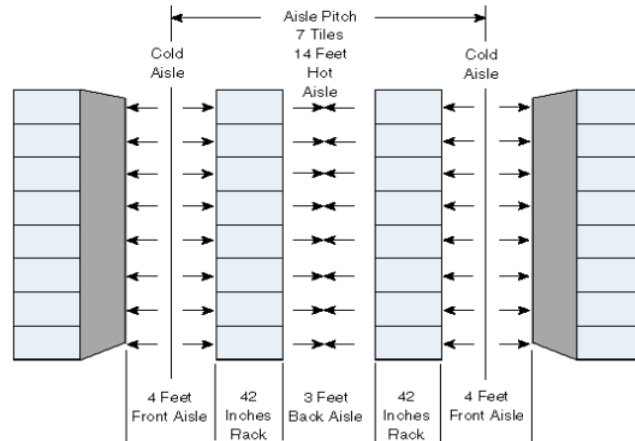


Figure 6: 7- Tiles Aisle Pitch

The construction material is essential. Wood might be acceptable if it is protected against fire with special resistant paint, but ceramic bricks' structure is recommended. Beside the location and the building structure, the organisation should analyse the space around the physical building as the fireworkers must have easy access ways.

On the other hand, all these aspects will become no longer a concern for UWTSD if they are using Amazon Web Services data centres. AWS has one of the largest infrastructures, globally distributed in 26 regions [15].



Figure 7: AWS global infrastructure map

UWTSD can choose the closest location and take advantages of multiple availability zones without having additional concerns in case of a disaster. Even in London region AWS launched in 2016, a data centre with three availability zones. On top of it, AWS is a dedicated cloud provider and which a considerable experience in building the high-quality data centres [16].



Figure 8: AWS data centre in Didcot

## Scalability

Scalability is one of the essential characteristics that a data centre must meet. It doesn't refer only to hardware, but also includes aspects as network, space, or essentials systems (cooling system, power system). As already mentioned, the business should consider physical space scalability. Based on the providing extension approach, scalability has two types:

- Vertical

Vertical scalability is ensured by addition additional compute power to existing resources, but it has the disadvantage that the hardware should be stopped, which results into increase downtime for the business's systems.

- Horizontal

Horizontal scalability is ensured by adding additional resources. For example, the power system can be horizontally scaled by adding more generators or uninterruptible power supply sources.

Based on the business's needs different combinations of scalability approaches (e.g., vertical scaling for some resources and horizontal scaling for others) can be implemented, but they are coming with the same disadvantage of increased cost and might result in unused resources. UWTSD should have a string prediction strategy to identify the business's requirements and possible peak activities [1].

By using AWS, UWTSD can quickly and easily access all the resources that the business needs in any situation by deploying thousands of new servers in several minutes. AWS provides Auto Scaling which scales or release the resources based different metrics and rules as performance, load which brings a huge improvement of cost and reduce the energy consumption [17].

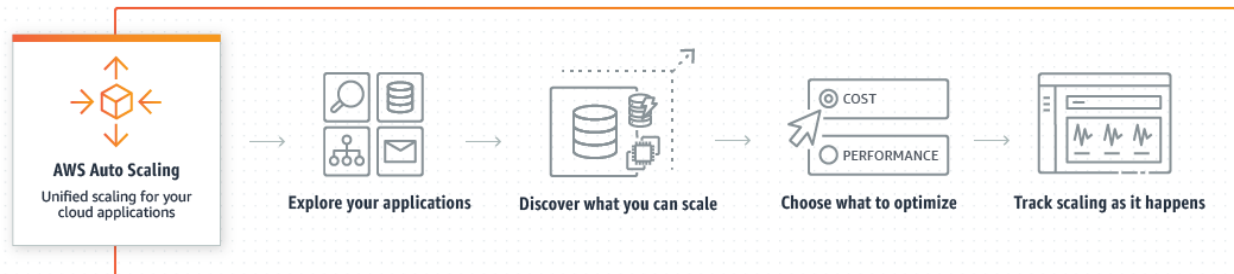


Figure 9: AWS Auto Scaling

AWS Auto Scaling is free, and the customer pays only for the resources that are used following a pay-as-you-go model.

### **Fault tolerance**

Fault tolerance is a concept that describe how quickly systems response and continue to operate when one or multiple failures occurs. There are multiple tiers of fault tolerance determined as a report between the time of downtime in a year: tier 1 – 28.8hours/year, tier 2 – 22 hours/year, tier 3 – 1.6 hours/year and tier 4 – 0.4 hours/year. For UWTSD would be difficult to achieve a low-level downtime without an increased cost. For example, for achieving tier 1, the cooling system should maintain a temperature of 21 to 23 degrees Celsius, and the emergency power system should come in place in less than 20 minutes [13].

AWS provides services that are ideal for building a fault-tolerance systems without up-front cost and capable to automatically operate. Several of these services are Amazon Elastic Compute Cloud (provides compute resources and use Amazon Machine Image to easily scale multiple instances), Auto Scaling (provides additional resources despite of the failure scenario) or Amazon Elastic Block Store (provides block storage volumes that are automatically replicated). On top of it, AWS provides regions and availability zones (collection of logically grouped data centres). Because these are independent and isolated means that each has its own source of power, cooling, internet connection which increase the availability even in case of a disaster [18] [19].

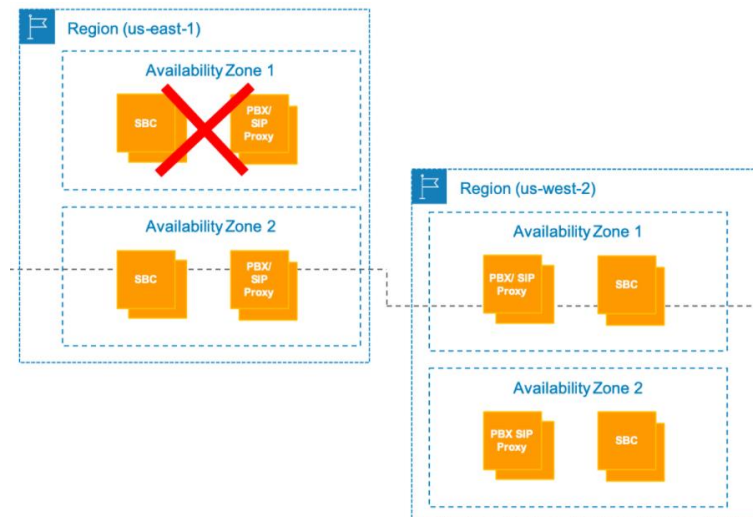


Figure 10: AWS availability zones and fault tolerance

## Security

### UWTSD

Security has always a substantial impact in businesses. Being a university, UWTSD records a diversity of information from personal data about employees and students to financial information about budgets or salaries. All those are sensitive and become a critical target for cyber-attacks. UWTSD must ensure security on both physical and digital levels.

Physical security implemented when the data centre is built and it has three levels: perimeter, facility, and computers room security.

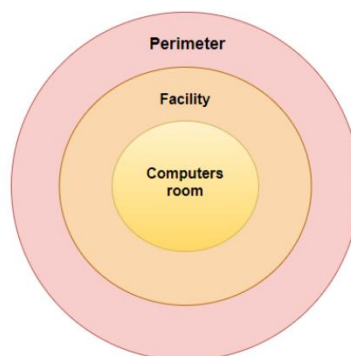


Figure 11: Physical security layers

The area where the data centre is located, should be permanently monitored using video and audio surveillance systems and dedicated security teams that do regular patrols. The access into the data centre area should have security gates and a good visibility and lighting. All the external and internal doors should have alarms and identity check equipment. Microsoft proposed a model called “Zero Trust” model, which provides a set of recommendations that can be implemented by UWTSD to obtain an increased level of security.

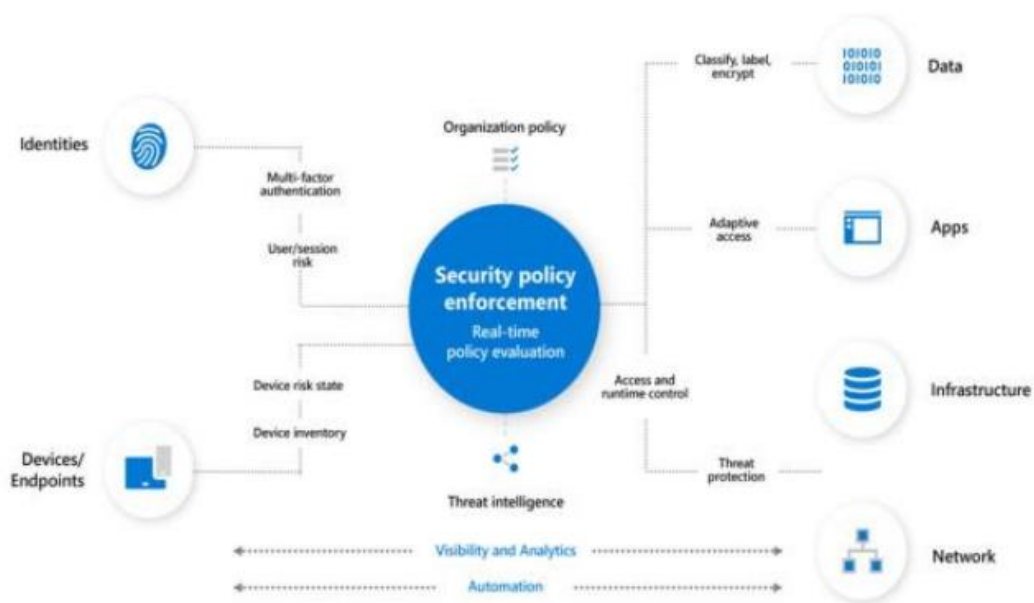


Figure 12: Zero-Trust model

UWTSD should identify the members that are allowed to access the data centre, perform background checks for employees and produce an access list with each individual role or authorization level. This list should be periodically reviewed [20]. The next level is represented by facility security involves the usage of card swipes or biometrics checks. Zero Trust model suggest the usage of face recognition mechanism and multi-factor authentication. Computers room is even more restricted to a dedicated list of members (e.g., maintenance team or internal IT team) and it should be carefully approved by the data centre manager.

On top of it, other procedures should be established. For example, when an employee leaves the UWTSD organisation, an “exit procedure” should be applied. The access list is reviewed,

the employee is removed from it, the security card or the access keys are collected, and the biometric records are removed.

As mentioned, physical security is just one of the concerns. Once it is provided, then the data should be protected from a digital perspective. All the network traffic should be protected by the firewalls, and it should be monitored and analysed to detect any unexpected incoming or outgoing data packages or possible security breaches. A password strategy should be implemented by policies (strong password rules, regular change password policies etc.) Data should be encrypted at rest and in transit and the access to it is determined based on roles and policies.

UWTSD should implement data centre automation processes to be able to continually monitor and report security events.

AWS has already in place a very strong security defence strategy and they significantly invest in large teams of experts in cybersecurity. Physical access is restricted following the best practices and measures [21].



Figure 13: AWS equipment for physical security



Figure 14: AWS perimeter security

There are security gates, video surveillance and even biometric scanners and any maintenance operation is strictly supervised. The employees' badges contain chips to be authenticated. Even if the physical security layer is bypassed, then additional layers as encryption (using multiple layers of encryption), replication or data anonymity. Authentication attacks are constantly analysed and mitigated using firewalls, VPN protocols, password reset policies, DDoS defence, key vaults, or role-based access control. It means AWS is not only protect the physical building, but also the infrastructure and the data. It detects vulnerability and provides patches. AWS monitors 24/7 their infrastructure. All those security aspects might be difficult to implement by UWTSD in the context of a on-premises data centre as they required dedicated cybersecurity teams, dedicated guards, surveillance and security equipment, a constant monitoring of any further possible cyberattacks which results into increased cost (up-front but also operational cost) and higher risk of security breaches.

Security is also one of the six pillars presented in AWS Well-Architected Framework which helps the cloud architects to define the most secure, performant and efficient architecture which shows the high attention that AWS pays to security.

### **Energy consumption**

Energy produces a considerable cost for the UWTSD if they own an on-premises data centre. Based on the statistics, currently the data centres are using 12% of the UK energy, but on the other hand Amazon has the main target to use 100% renewable energy by 2025. This commitment came in place in 2014. One year later, they founded Amazon Solar Farm in US

Virginia which was expected to produce solar energy in year equivalent with the energy consumed by 15000 US homes. In 2016 Amazon launched Amazon Wind Farm Fowler Ridge in US Indiana generating wind power. The same year comes with another five solar farms across Virginia. In 2018 Amazon had already 50% renewable energy usage. Amazon continued to develop new projects in Ireland, Sweden, Spain, China, Australia and in 2020 extended even more in Europe and South Africa. Currently Amazon has 232 projects globally [22].



Figure 15: AWS solar farm

Taking in consideration all mentioned aspect, using outsources solution as Amazon Web Services would be considered a better and more efficient solution of UWTSD.

## Scenario 2: ABC Data Ltd

ABC Data Ltd. is presenting the following case study: *“ABC Data Ltd. is an organisation that has 3 physical data centres offering a single reliable data centre using virtualised technology to provide a virtualised data centre. The data centre offers cloud storage and virtualised services for fee paying customers. ABC’s physical locations are connected by fibre high-bandwidth broadband connections, and they mirror each other’s data storage for resiliency. The organisation provides secure, safe storage and services to its customers at a premium price. For this to happen the security, hardware services and storage systems have been carefully designed.”*

ABC Data Ltd. has on-prem data centres which makes the organisation fully responsible for ensuring the security. As already mentioned, security has multiple layers and must cover all aspects from perimeter to data security and must be clearly defined in a set of data centre security policies as following [23]:

### **Physical security**

- All data centres physical areas are permanently monitoring using video cameras
- Only authorized member can access the data centre perimeter
- All data centre doors (internal or external) are monitored and alarmed
- Security patrols should be regularly performed
- Smoking, alcohol, drugs, and other combustible materials are totally prohibited
- Eating is allowed only into dedicated area
- Usage of camera or video devices is prohibited unless there is a specific reason and written approval

### **Personal authorization**

Background checks and confidentiality agreements are mandatory for each member.

Also, the organisation should define different levels of authorization:

- Level 3 authorization can be granted to data centre managers, staff, or technical team (members responsible for electrical and cooling systems, network connectivity or the layout of the data centre). Members with level 3 authorization can access the data centre without being escorted or assisted.
- Level 2 authorization can be granted to members that are responsible for physical maintenance. They are not authorized to perform any modifications without informing level 3 staff.
- Level 1 authorization can be granted to part time employees. They must be escorted by at least level 2 member.
- Visitors
  - They must be escorted and documented when they enter and exit the data centre.
  - A visit must be scheduled with at least 24h in advanced and it must be approved by the data centre manager
  - Tour visitors must be relatively small

Those permissions should be written into an access list, and it must be constantly updated and reviewed. Any additional access should come with a ticker that will be accepted by the data centre managers.

**Subject:** Customer # 00101 Access Ticket for 12/20/09

**Access Ticket:**

**Customer # 00101 ; ABC Corporation**

Name and vendor: **John Doe (IBM Technician)**

Task being performed: **Working on the IBM Storage Array.**

Start Date\Time: **12-20-2009 at 01:00 PM**

End Date\Time: **12-20-2009 at 05:00 PM**

Location of Task: **ABC Corporation's cage in Data Center**

Escorted or Not Escorted: **Will need to be escorted to cage (not on access list)**

Figure 16: Example of data centre access ticket

## Equipment installation/removal

- All equipment installation should be monitored and coordinated by the data centre manager and the data centre technical team
- Removal will be denied without the existence of a removal form completed and approved by the manager

## Network security

Nowadays, companies are fighting against multiple types of attacks that targets the network like packet sniffing, password attack, port redirection attack, IP spoofing etc. and ensuring the network security is critical. The security policy must include:

- Firewalls installed following Zero Trust model
- Permanent network vulnerability scanning
- Intrusion Detection and Prevention
- Regular Penetration Tests

## Data security

Once all the other layers of security are covered, the last but not the least in terms of importance layer is represented by the data itself.

- Data should be encrypted at rest and in transit
- Data backup and recovery strategies

- The organisation should follow the data privacy regulations (e.g., General Data Protection Regulation)

ABC Data Ltd. is using Storage Area Network which is based on Fibre Channel technology and was recognized as offering a great security level.

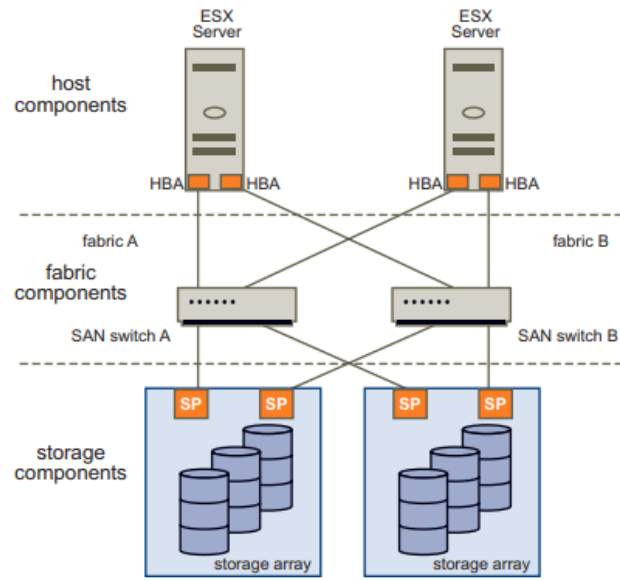


Figure 17: SAN Component Layers [24]

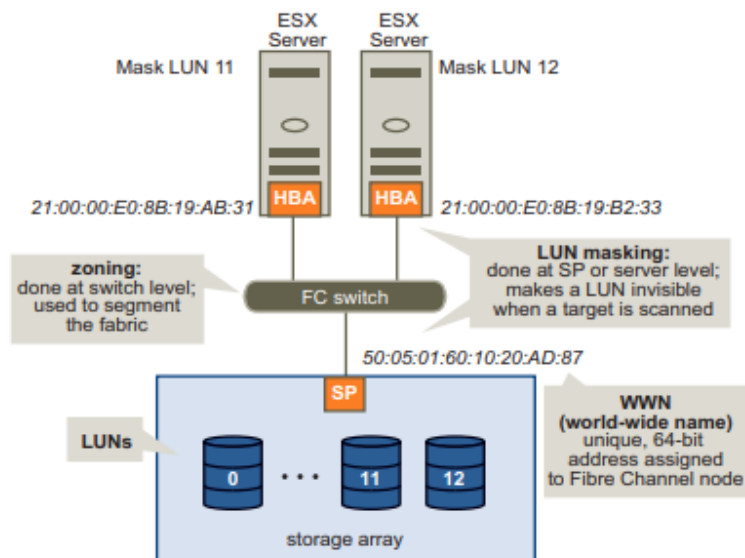


Figure 18: LUN Zoning and Masking [24]

It has the main advantage as not being directly connected to the Internet which reduced the chance of a network security breach. SAN components include fabric configurations servers which allows only authorized and trusted devices and have a strong management access control mechanism that mitigates the threats caused by unauthorized access.

The organisation can define a list of switches which must be authenticated using a certificate before being added into the fabric and ports dedicated to each world-wide name (WWN) used to uniquely identify the host-bus adapter (HBA) from where the request is send into the fabric switches.

On top of it, SAN comes in place with another two concepts: LUN (Logical Unit Numbers) Masking and Zoning which bring an additional layer of security. LUNs are designed to be visible only for the host that has it assigned. Also, zoning is designed to provide access only for the authorized devices, or devices defined in the same zone, which reduce the risk of losing the data when it is transferred between devices with different operating systems.

SAN has also a native support for disaster recovery. Even if the disaster was natural or produced by a person, the data can quickly recover, and it also offers immutable snapshots which is an efficient technology that allows a quick data backup [24].

## **Conclusion**

In this report, an overview of how virtualisation is working and what benefits it brings to businesses was presented.

The two scenarios were analysed and in conclusion for UWTSD would be more efficient to use services offered by Amazon Web Services cloud provider instead of building their own data centre.

The most evident aspect is that building an on-premises data centre has a high level of complexity, an increased cost and requires additional resources and expertise.

ABC Data Ltd. organisation has already in place three on-premises data centres and security is a critical aspect. A list of policies was provided and those need to be applied across all data centres to ensure a high-level security.

## References

- [1] H. Scott, Building a Modern Data Center, Principles and Strategies of Design, Bluffton: ActualTech Media, 2016.
- [2] IBM Corporation, Introduction to Storage Area Network, SAN, San Jose: IBM Corporation, 1999.
- [3] S. Miniman, “The Data Center: Past, Present and Future,” 2014.
- [4] H. Singh, Next-Gen Virtualization, Hoboken, NJ: John Wiley & Sons, Inc, 2019.
- [5] S. Tripathy, “IaaS vs PaaS vs SaaS: A Complete Overview,” Virtasant, 09 03 2021. [Online]. Available: <https://www.virtasant.com/blog/iaas-vs-paas-vs-saas-a-complete-overview>.
- [6] “A Brief History of the Data Centre,” 17 Ways Pty Ltd, [Online]. Available: <http://17ways.com.au/Library/CEO/A%20Brief%20History%20of%20the%20Data%20Centre.html>.
- [7] iponwire, “Virtual Network and Network Virtualization in easy words,” 31 10 2020. [Online]. Available: <https://iponwire.com/virtual-network-and-network-virtualization/>.
- [8] ResellerClub, “Type 1 and Type 2 Hypervisors: What Makes Them Different,” 24 05 2019. [Online]. Available: <https://medium.com/teamresellerclub/type-1-and-type-2-hypervisors-what-makes-them-different-6a1755d6ae2c>.
- [9] M. Portnoy, Virtualization Essentials, Second Edition, Indianapolis, Indiana: John Wiley & Sons, Inc, 2016.
- [10] Salesforce, “12 Benefits of Cloud Computing,” Salesforce, [Online]. Available: <https://www.salesforce.com/products/platform/best-practices/benefits-of-cloud-computing/>.
- [11] IBM Corporation, “The Benefits of Cloud Computing, A new era of responsiveness, effectiveness and efficiency in IT service delivery,” Somers, NY, 2009.
- [12] S. Orban, “6 Strategies for Migrating Applications to the Cloud,” Amazon Web Services, 01 11 2016. [Online]. Available: <https://aws.amazon.com/blogs/enterprise-strategy/6-strategies-for-migrating-applications-to-the-cloud/>.
- [13] P. Massiglia, Storage Area Network Essentials, New York: Wiley Computer Publishing, 2002.
- [14] Sun Microsystems Inc, “Site Planning Guide for Entry-Level Servers Version 1.4,” 2014. [Online]. Available: <https://docs.oracle.com/cd/E19095-01/sfv890.svr/816-1613-14/index.html>.
- [15] Amazon Web Services, Inc, “Regions and Availability Zones,” [Online]. Available: [https://aws.amazon.com/about-aws/global-infrastructure/regions\\_az/](https://aws.amazon.com/about-aws/global-infrastructure/regions_az/).
- [16] H. Menear, “AWS is building its next hyperscale data centre in Didcot,” 05 02 2021. [Online]. Available: <https://datacentremagazine.com/data-centres/aws-building-its-next-hyperscale-data-centre-didcot>.
- [17] Amazon Web Services, Inc, “AWS Auto Scaling,” [Online]. Available: <https://aws.amazon.com/autoscaling/>.
- [18] Amazon Web Services, Inc, “Fault-Tolerant Components on AWS,” 2019. [Online]. Available: <https://d1.awsstatic.com/whitepapers/aws-building-fault-tolerant-applications.pdf>.
- [19] Amazon Web Services, Inc, “Use Multiple Availability Zones,” [Online]. Available: <https://docs.aws.amazon.com/whitepapers/latest/real-time-communication-on-aws/use-multiple-availability-zones.html>.

- [20] Microsoft Corporation, “Evolving Zero Trust, how real-world deployments and attacks are,” 11 2021. [Online]. Available: <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWJJdT>.
- [21] Amazon Web Services, Inc, “Learn how we secure AWS data centers by design,” [Online]. Available: <https://aws.amazon.com/compliance/data-center/>.
- [22] Amazon Web Services, Inc, “Sustainability in the Cloud,” [Online]. Available: <https://sustainability.aboutamazon.com/environment/the-cloud?energyType=true>.
- [23] DataSite, “DataSite Data Center Policies & Work Rules,” [Online]. Available: <https://www.datasitecolo.com/wp-content/uploads/2018/08/DataSite-Data-Center-Policies-04-06-2018.pdf>.
- [24] VMware, Inc, “SAN Conceptual and Design Basics,” [Online]. Available: [https://www.vmware.com/pdf/esx\\_san\\_cfg\\_technote.pdf](https://www.vmware.com/pdf/esx_san_cfg_technote.pdf).
- [25] N. Bhatt, “Global Information Assurance Certification Paper,” SANS Institute, 2003.