Al-Aqsa University

Faculty of Computers and Information Technology

Department Networks and Mobiles Technology

Build proposed disaster recovery solution for the data center in khan Younis municipality via Microsoft azure cloud computing infrastructure

بناء حل مقترح للتعافي من الكوارث لمركز البيانات في بلدية خانيونس عبر البنية التحتية للحوسبة السحابية

(Microsoft azure)

A graduation project submitted in partial fulfilment of the requirements for the degree of Bachelor of Networks and Mobiles Technology

By

Rawan Maisara ALKahlut Tasneem A. M. Abuobaid

Supervisor

Hazem Al-Baz

June 2022

A verse from the Holy Quran

قال تعالى:

(يَرْفَعِ اللَّهُ الَّذِينَ آمَنُوا مِنكُمْ وَالَّذِينَ أُوتُوا الْعِلْمَ دَرَجَاتٍ ۚ وَاللَّهُ بِمَا تَعْمَلُونَ خَبِيرٌ)

صدق الله العظيم

المجادلة, الآية: (11)

DEDICATION

To the one who cried out in yearning to meet us, to the teacher, the honest and trustworthy, the seal of the prophets and messengers, Muhammad (peace be upon him).

May God extends the life of my loving father, who worked hard and hard to enjoy comfort and satisfaction for me, to the pure hand that removed the thorns from the road in front of me, to the one who taught me to give without waiting, to whom I proudly bear his name, may God prolong his life.

To the soul that inhaled its air, and walked with its supplications, to the inability of words to find a description that fulfils its right, to the source of tenderness, loyalty, and love, to my dear mother, may God grant her long life.

To those who are closer to me than my soul, to those who share a mother's bosom with me, to those from whom I draw my intention and my determination, my dear brothers.

To my relatives and everyone who stood by my side and supported me in completing this modest research.

To the seas of science that made ships from their knowledge to achieve our dreams, dear doctors.

How many sacrifices for the sake of science, religion, and country?

To all of you... I dedicate this humble work.

ACKNOWLEDGEMENTS

Oh God, praise be to you whose beginning has not run out and its end is not interrupted. Oh God, thank God, you deserve praise, worship, and thanks. Praise be to God who fills the heavens and the earth, and praise be to God who made our path easy and directed with success and hope, and prayers and peace be upon the purest of the prophets with an enlightened face.

Words and phrases race together to thank you. If you say thank you, then my thanks will not suffice for you, based on the saying of our Noble Messenger, may God's prayers and peace be upon him: "He who does not thank people does not thank God." (Al-Tirmidhi, 403/3: Hadith No. 1954).

My words are incapable of thanking the one who illuminated our paths with the light of science and hope, my distinguished doctors at the Faculty of Computers at Al-Aqsa University, and I remember in particular Dr. Hazem Al-Baz, may God preserve him, for his kindness in supervising my project and the engineer. Sahar Abu al-Khair, may God preserve her, for her kindness in supervising my project, and for what overwhelmed me with the abundance of her knowledge, her beautiful patience over my mistakes, and those who advised me, and her good treatment of me regardless of the number of questions that were uttered. I ask God to give them their life and health.

I would also like to extend my sincere thanks to the engineers in Khan Yunis Municipality, specifically Eng. Mazen Tabash, head of the computer department in the municipality of Khan Yunis. Many thanks to them.

And I will never forget the great share, my university, Al-Aqsa University that has embraced us throughout the past academic years, in recognition of virtue and gratitude, so I thank you all.

Abstract

The main goal of our project is to facilitate the process of disaster recovery and maintain a reduction in the proportion of financial losses and data loss in the event of a disaster and prepare the municipality in the event of natural disasters, wars, technical or human errors through prior planning for the method of disaster recovery and dealing with it with the least losses and as quickly as possible.

Through our project, we studied the municipality's situation and anticipated the worst possible scenarios. We worked on creating the first disaster recovery plan in the municipality to help them recover step by step. We found improvement solutions to weaknesses. The municipality's infrastructure helps the system recover quickly and with minimal data loss. We worked on finding solutions that target them. Reducing the time of business interruption in the municipality and implementing these solutions in an experimental environment, we chose cloud computing to implement this, and we applied a group of technology to the same infrastructure to achieve the goals of disaster recovery within the data center. Another center is in a geographical area far from the state. Data is transferred synchronously between the two sites and we used some technology to automatically transfer between the two sites and transfer services to the other site and provide services through it

In the future, we will be keen to increase the level of safety in the data center, develop a disaster recovery plan according to developments and updates in the municipality, and implement all practical aspects of the real environment of the project.

Within our project, there will be a time plan showing what has been achieved, developed, and followed up step by step.

Finally, the writing of the project report was completed and implemented in a practical way, thanks to God and the efforts of our supervisor, thanking him for his effort in following up and supervising our project.

الملخص

هدفنا الأساسي من مشروعنا تسهيل عملية التعافي من الكوارث والحفاظ على تقليل نسبه الخسائر المالية و فقدان البيانات عند حدوث كارثة وتهيئه البلدية في حال حدوث كوراث طبيعية أو حروب او اخطاء فنيه او بشرية من خلال التخطيط المسبق لطريقة التعافي من الكوراث والتعامل معها بأقل الخسائر وبأسرع وقت ممكن.

من خلال مشروعنا درسنا حالة البلدية و توقعنا أسوء السناريوهات الممكن حدوثها وعملنا على انشاء اول خطة تعافي من الكوارث في البلدية لتساعدهم على التعافي خطوة بخطوة وأوجدنا حلول تحسينيه لنقاط الضعف البنية التحتية للبلدية تساعد النظام على التعافي بأسرع وقت وقت وبأقل فقدان للبيانات وعملنا على ايجاد حلول هدفها تقليل وقت انقطاع الاعمال في البلدية وتنفيذ هذه الحلول على بيئة تجريبيه واخترنا الحوسبة السحابية لتنفيذ ذلك وطبقنا مجموعة من التكنولوجي على نفس البنية التحتية لتحقيق الاهداف التعافي من الكوارث في داخل الداتا سنتر وعند حدوث كارثة تدمر الداتا سنتر عملنا على ايجاد حلول لهذه الحالة عن طريق بناء داتا سنتر اخر في منطقة جغرافية بعيدة عن الدولة يتم نقل البيانات بشكل متزامن بين الموقعين واستخدمنا بعض التكونولجي لتحويل اتوماتك بين الموقعين ونقل الخدمات الي الموقع الاخر وتقديم الخدمات من خلاله.

وفي المستقبل سوف نحرص على زيادة مستوى الأمان في الداتا سنتر و تطوير خطة التعافي من الكوراث حسب التطورات والتحديثات في البلدية وتنفيذ جميع الجوانب العملية على البيئة الحقيقة للمشروع.

وضمن مشروعنا سيكون هناك خطة زمنية مبينة لما تم انجازه وتطويره وتتبعه خطوة بخطوة.

واخيرا تم الانتهاء من كتابة تقرير المشروع وتطبيقه بشكل عملي بفضل الله وجهود مشرفنا شاكرين له مجهوده في القيام على المتابعة والاشراف على مشروعنا.

Table of Contents

Acronyms

abbreviation	term	description
VM	Virtual machine	Simulation of a specific computer system, where this virtual machine or virtual machine works based on the computer structure and the supposed working method of this computer device that is being simulated, is usually achieved through computer hardware or computer program software dedicated for this purpose.
DR	Disaster recovery	enable the organization to regain use of critical systems and IT infrastructure as soon as possible after a disaster occurs.
DRP	disaster recovery plan	formal document created by an organization that contains detailed instructions on how to respond to unplanned incidents such as natural disasters, power outages, cyber-attacks, and any other disruptive events.
cloud DR	cloud disaster recovery	strategies and services enterprises apply for backing up applications, resources, and data into a cloud environment.
RPO	Recovery Point Objective	describes the interval of time that might pass during a disruption before the quantity of data lost during that period exceeds the Business Continuity Plan's maximum allowable threshold
RTO	Recovery Time Objective	duration of time and a service level within which a process must be restored after a disaster to avoid unacceptable consequences associated with a break in continuity.
ISO	International Organization for Standardization	A standards-setting organization that includes representatives from several national standards organizations.
HA	High availability	A feature of a system that aims to ensure an agreed level of operational performance.

DC	Datacenter	A huge center consisting of many huge servers, and primary and backup power supplies. It is connected to the Internet at very high speeds. It is also often in a private building equipped with equipment such as temperature control, fire extinguishing devices, electricity regulation, and high-security specifications. Also, it is not easy or simple.
AD	Active Directory	database and set of services that connect users with the network resources they need to get their work done.
DNS	Domain Name System	A system that stores information related to Internet domain names in a decentralized database on the Internet.
IP	Internet Protocol	The digital identifier for any device connected to an information network that operates on the Internet protocol package, whether it is a local network or the Internet.
DHCP	Dynamic Host Configuration Protocol	DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks.
Saas	Software as a service	software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted
Paas	Platform as a service	cloud computing model where a third-party provider delivers hardware and software tools to users over the internet. Usually, these tools are needed for application development.
Iaas	Infrastructure as a Service	cloud computing service model using which computing resources are hosted in a public, private, or hybrid cloud. It provides you with high-level APIs used to dereference various low-level details of underlying network infrastructure like backup, data partitioning, scaling, security, physical computing resources, etc. A hypervisor, such as Xen, Oracle VirtualBox, Oracle VM, KVM, VMware ESX/ESXi, or Hyper-V runs the virtual machines as guests. Pools of hypervisors within the cloud operational system can support large numbers of virtual

		machines as well as the ability to scale services up and down according to customers' varying requirements.
TB	terabyte	A terabyte is a unit of measurement for a computer's storage capacity.
NIC	Network interface controller	A computer component, without which the computer cannot connect to any network on the Internet, which allows the user of the computer to communicate with other computers through a computer network

CH01: INTRODUCTION

1.1 OVERVIEW:

In the last period, Khan Yunis municipality witnessed an obstacle in accessing some services due to some disasters that led to the noticeable suspension of some services

Proceeding from this fact and based on our belief in the importance of facilitating the provision of services to customers around the clock, a plan was reached to recover from disasters and develop the Khan Yunis municipality system by providing several services and solutions that help in that.

1.2 DEFINE THE PROBLEM

At present, in the twenty-first century, the world was exposed to the Corona pandemic, and all work and services in all public and private sectors, including Khan Yunis Municipality, were suspended, and it was difficult to continue work without a disaster recovery plan.

In addition, during the years 2021 and 2022 there was Israeli aggression on the Gaza Strip, which led to the lack of continuity of work due to the difficulty of going to the workplace, so it was necessary to develop an alternative plan to continue the work in the event of a catastrophic situation.

Therefore, we, Al-Aqsa University students, presented this idea by implementing a disaster recovery plan through the cloud.

1.3 RESEARCH AIM

Our plan aims to ensure business continuity in Khan Younis Municipality over time without wasting data. After the implementation of our project, it will be a very important technological addition to the municipality of Khan Yunis due to the lack of a similar application in the municipality. It will also save economically and provide material costs without wasting resources. The project also aims to integrate technology into practical life.

1.4 MODERNITY AND CONTRIBUTIONS

Our idea was implemented for the first time in the municipality of Khan Yunis (disaster recovery plan) to save time, reduce loss, waste data, and business continuity when a particular disaster occurs without waiting for a long time, making sure that none of the data is lost and none

of it is lost. It also allows the owners of the municipality to have all the details of the data centre and maintain it in the event of a malfunction.

1.5 RESEARCH OBJECTIVES:

Our plan aims to ensure business continuity in Khan Younis Municipality over time without wasting data. After implementing our project, you will be able to:

• Facilitate problem-solving when a catastrophic situation occurs through the disaster recovery plan

• Providing a data centre in a safe area to operate in parallel when a malfunction occurs in the municipality's data centre

• Cost savings

• Continuity of work. Customers can reach out at any time

• Flexibility and higher performance

1.6 TIME PLAN

In this part, we will show the implementation path of our project according to the timeline shown in Figure (1).

	Task Mo	Task Name	Duration	Start	Finish
1		Team selection	4 days	Mon 10/4/21 8:00 AM	Thu 10/7/21 5:00 PM
2		Choose an idea	10 days	Thu 10/7/21 8:00 AM	Wed 10/20/21 5:00 PM
3		Find sources	181 days	Thu 10/21/21 8:00 AM	Thu 6/30/22 5:00 PM
4		Choose a place	5 days	Sun 4/3/22 8:00 AM	Thu 4/7/22 5:00 PM
5		Infrastructure Study	33 days	Mon 4/4/22 8:00 AM	Wed 5/18/22 5:00 PM
6		System Analysis	64 days	Wed 5/18/22 8:00 AM	Mon 8/15/22 5:00 PM
7		We discovered weaknesses	11 days	Thu 6/30/22 8:00 AM	Thu 7/14/22 5:00 PM
8		Work disaster recovery plan	44 days	Sun 7/3/22 8:00 AM	Wed 8/31/22 5:00 PM
9		We found solutions	20 days	Wed 6/15/22 8:00 AM	Tue 7/12/22 5:00 PM
10		Choose the right solution	5 days	Wed 7/13/22 8:00 AM	Tue 7/19/22 5:00 PM
11		Apply the solution to azure	3 days	Wed 7/20/22 8:00 AM	Fri 7/22/22 5:00 PM
12		Building the first site in East US	2 days	Wed 7/27/22 8:00 AM	Thu 7/28/22 5:00 PM
13		Install the required services	2 days	Thu 7/28/22 8:00 AM	Fri 7/29/22 5:00 PM
14		Building the second site in UAE North	2 days	Thu 8/4/22 8:00 AM	Fri 8/5/22 5:00 PM
15		Install the required features	2 days	Fri 8/5/22 8:00 AM	Sat 8/6/22 5:00 PM
16		Create 2 web servers	2 days	Sat 8/6/22 8:00 AM	Mon 8/8/22 5:00 PM
17		Create settings for load- balancer between servers	2 days	Sat 8/6/22 8:00 AM	Mon 8/8/22 5:00 PM
18		load balancer test	2 days	Sat 8/6/22 8:00 AM	Mon 8/8/22 5:00 PM
19		Connectivety check between the two sites	2 days	Sun 8/7/22 8:00 AM	Mon 8/8/22 5:00 PM
20		Install failover cluster	2 days	Mon 8/8/22 8:00 AM	Tue 8/9/22 5:00 PM
21		Check the components of the sites	1 day	Tue 8/9/22 8:00 AM	Tue 8/9/22 5:00 PM
22		Create a strutch cluster	2 days	Mon 8/29/22 8:00 AM	Tue 8/30/22 5:00 PM
23		Create rules fileserver	2 days	Tue 8/9/22 8:00 AM	Wed 8/10/22 5:00 PM
24		Create a folder to share	2 days	Tue 8/9/22 8:00 AM	Wed 8/10/22 5:00 PM
25		Create a replication on the domain controller	2 days	Thu 8/11/22 8:00 AM	Fri 8/12/22 5:00 PM
26		Create replication at the storage level	4 days	Wed 8/31/22 8:00 AM	Sat 9/3/22 5:00 PM
27		Documentation preparation	39 days	Fri 7/15/22 8:00 AM	Wed 9/7/22 5:00 PM
28		Final presentation preparation	4 days	Sat 9/3/22 8:00 AM	Wed 9/7/22 5:00 PM

Figure 1 1Project time plan

CH02 BACKGROUND

2.1 OVERVIEW

In this chapter, we will present the theoretical part of the project, identify the concepts and simply clarify them.

2.2 HIGH AVAILABILITY

2.2.1 WHAT IS HIGH AVAILABILITY ARCHITECTURE?

A high-available architecture is when there are several different components, modules, or services that work together to maintain optimal performance, irrespective of peak-time loads.

In its purest sense, this system allows businesses to work continuously without failure over a given period. Many businesses can't afford even a minute of downtime. Considering that data is the lifeblood of many businesses, even just a short period of downtime can be incredibly costly.

Note: High availability is often measured in the percentage of time that a service is available to users. According to the Microsoft Network Developer Glossary, for a server to be considered "highly available", it needs to achieve 99.999% network uptime.[44]

2.2.2 WHAT IS HIGH AVAILABILITY?

High availability (HA) is the ability of a system to operate continuously without failing for a designated period. HA works to ensure a system meets an agreed-upon operational performance level. In information technology (IT), a widely held but difficult-to-achieve standard of availability is known as five-nines availability, which means the system or product is available 99.999% of the time.

Highly available systems must be well-designed and thoroughly tested before they are used. Planning for one of these systems requires all components to meet the desired availability standard. Data backup and failover capabilities play important roles in ensuring HA systems meet their availability goals. System designers must also pay close attention to the data storage and access technology they use.[44]

2.2.3 WHAT IS HIGH AVAILABILITY?

High availability is a characteristic of a system that aims to ensure an agreed level of operational performance usually uptime for a higher than normal period[42]

Availability %	Downtime per year	Downtime per month	Downtime per day
99%	3.65 days	7.31 hours	14.40 minutes
99.9%	8.77 hours	43.83 minutes	1.44 minutes
99.99%	52.60 minutes	4.38 minutes	8.64 seconds
99.999%	5.26 minutes	26.30 seconds	864.00 milliseconds

Table 1 High availability and down time

High availability mainly depends on RTO, RPO, and SLA

2.2.4 SLA (SERVICE LEVEL AGREEMENT)

service - level agreement (SLA): defines the level of service expected by a customer from a supplier, laying out the metrics by which that service is measured, and the remedies or penalties, if any, should the agreed - on service levels not be achieved. Usually, SLAs are between companies and external suppliers, but they may also be between two departments within a company.[45]

2.2.5 RPO & RTO

RPO: Recovery Point Objective: Recovery Point Objective (RPO) describes the interval of time that might pass during a disruption before the quantity of data lost during that period exceeds the Business Continuity Plan's maximum allowable threshold or " tolerance".

RTO: Recovery Time Objective: The Recovery Time Objective (RTO) is the duration of time and a service level within which a business process must be restored after a disaster to avoid unacceptable consequences associated with a break in continuity. In other words, the RTO is the answer to the question: " How much time did it take to recover after notification of business process disruption? "

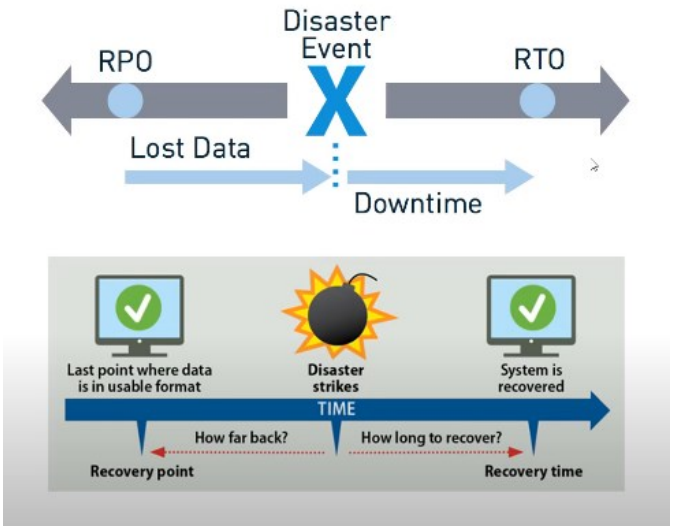

Figure 2 RPO & RTO IN Disaster Event

To improve any system, you need to identify the following requirements and calculate them in numbers for the system. It requires knowing the market value of the business and calculating the amount of the business loss in Downtime. It defines the basic functions of the business and the importance and priority of each service to determine the appropriate solutions for the state of the system that aims to reduce RTO and RPO, for example, solutions to reduce RPO We need to create a disaster recovery site for replication to transfer the changes that occur to the data directly to another site

Solutions to reduce RTO We need to reduce several solutions including cluster, load balance ...

Note that all these techniques are very expensive, so you must determine the priority of the business and determine the loss in the event of downtime to determine the appropriate technology.

2.2.6 HOW DOES HIGH AVAILABILITY WORK?

Systems can't be available 100% of the time, so true high-availability systems generally strive for five nines as the standard of operational performance.

The following three principles are used when designing HA systems to ensure high availability:

Single points of failure. A single point of failure is a component that would cause the whole system to fail if it fails. If a business has one server running an application, that server is a single point of failure. Should that server fail, the application will be unavailable.

Reliable crossover. Building redundancy into these systems is also important. Redundancy enables a backup component to take over for a failed one. When this happens, it's necessary to ensure reliable crossover or failover, which is the act of switching from component X to component Y without losing data or affecting performance.

Failure detectability. Failures must be visible and, ideally, systems have built-in automation to handle the failure on their own. There should also be built-in mechanisms for avoiding common cause failures, where two or more systems or components fail simultaneously, likely from the same cause.

To ensure high availability when many users access a system, load balancing becomes necessary. Load balancing automatically distributes workloads to system resources, such as sending different requests for data to different services hosted in a hybrid cloud architecture. The load balancer decides which system resource is most capable of efficiently handling which workload. The use of multiple load balancers to do this ensures no one resource is overwhelmed.

The servers in an HA system are in clusters and organized in a tiered architecture to respond to requests from load balancers. If one server in the cluster fails, a replicated server in another cluster can handle the workload designated for the failed server. This sort of redundancy enables failover where a secondary component takes over a primary component's job when the first component fails, with a minimal performance impact.

The more complex a system is, the more difficult it is to ensure high availability because there are simply more points of failure in a complex system.[46]

2.2.7 HA TECHNOLOGIES & LEVELS

- Cables.
- Power Supply, UPS & Generator.
- NIC Teaming. (Network)
- Network Devices. (Switch, Router, Internet, Firewall)
- Servers (HW).
- HDD RAID (storge)
- Cluster (application, OS).
- Load Balance (server, services).
- Storage.
- Backup.
- Replication.

- DR.

The following table shows disasters that occur at the level of hardware, software, and networks, and it shows the techniques of high availability and how to solve the problem of failure:

Scenario	How to cover it
Windows Or Linux OS Corruption	Cluster, Snapshot, Repair OS, DR, Restore from Backup.
Application Corruption	Application Cluster, Restore Configurations, Reinstall App. DR.
Database Corruption (Oracle or SQL)	Cluster D8, Node in DR, Restore De, Fully DR
Application Cluster Failure	Have Multi-Node, and LNB, Fix App, Restore, DR
VMware Virtual Machine Corruption	Restore from Backup or DR for this VM only
VMware vSphere ESXi Failure	VMware Cluster or FT
VMware vCenter Failure	HA for vCenter or Move to DR.
Backup Application Failure	Rebuild Backup App
Backup Data Failure	Work from 2nd Copy from Different media or Tapes.
Metro Cluster Failure	Stop Replication, Reconfigure it.
Replication Service Failure	Reconfigure the Replication tools.

Table 2 Software Scenario

Scenario	How to cover it
Network Cable Failure	Multi NIC with Multi Cable and Enable Teaming
Network Card Failure	Multi NIC with Multi Cable and Enable Teaming
HBA Cable Failure	Multi HBA with Multi Cable and Apply Zoning
HBA Card Failure	Multi HBA with Multi Cable and Apply Zoning
Power Cable Failure	Multi Power Cables or more connect with Multi Power Supply
Power Supply Failure	Multi Power Cables or more connect with Multi Power Supply
Internal HDD Server Failure	Configure H/W RAID
Server H/W Failure	Build Server Cluster
Blade H/W Failure	Build Have Multi Internal Redundancy (Network, Power, HDD, Server Node) if all Failures you can move to DR or another Blade on the same site.
Fabric Switch Failure	2 Fabric Switches
Storage HDD Failure	Configure H/W RAID
Storage Fiber Cable Failure	Storage Have Multi HBA Card
Storage HBA Failure	Storage Have Multi HBA Card
Storage Node Failure	Storage Have 2 Storage Processors Nodes.
Fully Storage H/W Failure	Restore from Backup to another Storage or Move to DR site.
Air condition	Have Another Air Condition
UPS Failure	you con work by Generator
Generator Failure	it's the last stage if lost all Public Power then UPS Generator you must move to DR.
Public Power Failure	you can work by UPS and Generator

Table 3 Hardware Scenario

COMPONENT AND DEPENDENCIS

Components that the application or service directly depends on and that the system usually requests during the installation of the application or service

Dependencies The application or service depends on it indirectly. If a failure occurs in it, the work of the service or application will stop

Component	Dependencies
Hard ware	Spam Solution
CAS server	Storage
HUB server	Server, network
Edge server	IP, Vlan, Firewall
OS	mail box database
DNS	Active directory

Table 4 Example:(Mail server)

2.2.8 REQUIREMENTS OF A HIGHLY AVAILABLE ARCHITECTURE

There are several different requirements that you'll need to maximize durability and high availability. These include:[46]

2.2.9.1 CLUSTER

A group of servers that provide the same service to protect the services provided to the client. Each server is named a node. When any node is damaged, the service is not lost, but another node is running. It is one of the first steps before building a disaster recovery site. One group can contain 16 or 32 nodes that deal with failure. At the level of the operating system, applications, servers, and services.

A high availability cluster will utilize multiple systems that are already integrated, so should a failure cause one system to fail, another can be efficiently leveraged to maintain the continuity of the service or application being used.

The high availability load balancing cluster plays a crucial role in preventing system failures. Having a load balancer in place essentially distributes traffic across different web nodes that are serving the same website or application users. This reduces the pressure on any one server, allowing each cluster to work more optimally while allowing traffic only to be sent to healthy servers.

2.2.9.1.1 HOW DOES A CLUSTER WORK?

The user only sees one node for a cluster that manages your traffic on the servers.

The cluster contains a quam or a file share witness in Microsoft. It can be a small server or a service on the Active Directory. It is in its place the brain of a Cluster called a handprint through which I can monitor active and passive servers by sending impulses to the servers.

If he sends 3 pulses and does not receive a response, another node from the cluster will be activated and your traffic will be transferred to another server. This process is called failover.

2.2.9.1.2 WHEN REPAIRING A NODE, YOU HAVE TWO OPTIONS:

- node continues to provide the service if it contains the same capabilities
- Converting the service to the first node and the process is called fall-back, either manually or automatically, and the best option is to manually switch because qurm checks work at the network level and cannot verify the validity of the service, so it is preferable to check manually

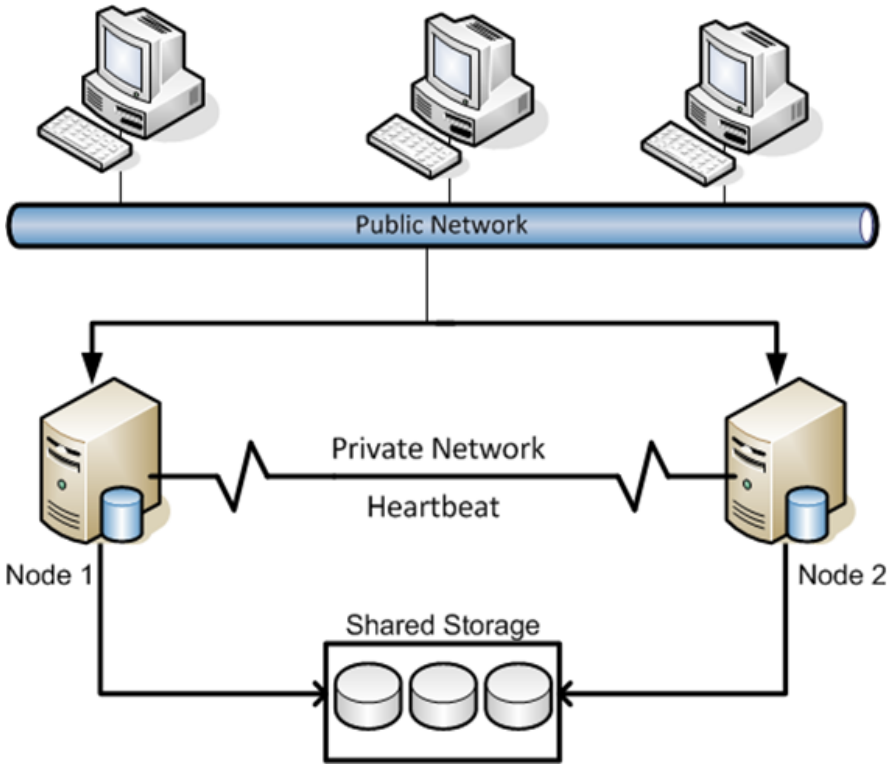

Figure 3 Failover Cluster

2.2.9.1.3 WHAT AND HOW DOES CLUSTER WORK?

It is applied to two different sites in different places, usually, the second site is the disaster recovery site, and each site contains special storage. A replication is made between these storages that are implemented at the LAN level. When a change occurs to the data on the first site, the change is transferred directly to the second site and made sure that it is written, and when the

replication process fails on the second site, the data is deleted from the two sites. There are two types:

- Synchronize :need a very fast connection with No more than 5-10 latency It is used in banks and with sensitive data RPO = 0
- A Synchronize :The data is stored on the first site and a period is specified before the changes are transferred to the second site. It does not matter the amount of latency between the two sites and is used with fewer data. RPO = specific time period

Note: The stretch cluster is expensive and needs an additional enterprise license and needs storage that supports replication.

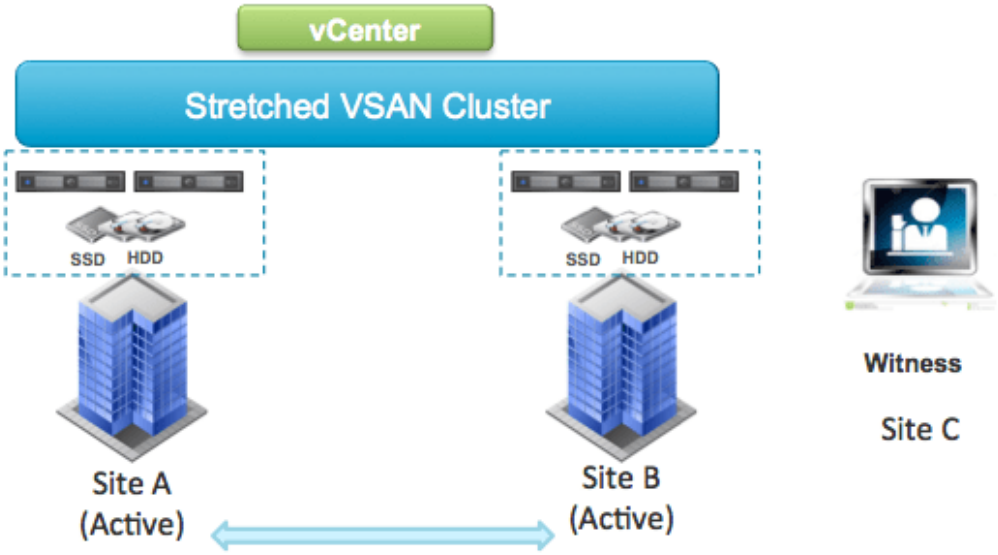

Figure 4 Stretched Cluster

2.2.9.1.4 THERE ARE MANY DIFFERENT TYPES OF CLUSTERS. COMMON TYPES INCLUDE:

- load sharing clusters, which divide work among the members.
- high availability clusters, where back-up nodes take over when primary nodes fail.
- information sharing clusters, which ensure the dissemination of information throughout a network.

2.2.9.1.5 THERE ARE TWO FUNDAMENTALLY DIFFERENT APPROACHES TO TAKE TO HIGH AVAILABILITY:

Active/Stand-By: The system is divided into active and stand-by nodes. The incoming requests are partitioned among the active nodes. The stand-by nodes are idle until an active node fails, at which point a stand-by node takes over his work.

The incoming requests are partitioned among all of the available nodes. If one node fails, his work will be redistributed among the survivors.

2.2.9.1.6 SHARED-NOTHING VS. SHARED-DISK CLUSTERS

A general rule that's followed in distributed computing is to avoid single points of failure at all costs. This requires resources to be actively replicated or replaceable, without a single factor being disrupted should the full service go down.

Imagine if you had fifty running nodes that were powered by one database. If one node fails, it will not have an impact on the persistent state of others, irrespective of the number of running nodes.

But should the database fail, the entire cluster will go down, making the database a single point of failure. This is referred to as a shared disk cluster.

On the other hand, should each node maintain its database, a node failure will not impact the entire cluster. This is referred to as a shared-nothing cluster.

2.2.9.2 REPLICATION

Transfer of changes that occur in a site such as (operating system, application, ...) on another site Transfer of changes takes place according to the RPO & RTO schedule

2.2.9.2.1 TYPES OF REPLICATIONS:

- Synchronize: Any data on the first site is written on the second site first and then written on the first site, RPO = 0, usually in banks and financial transactions
- A synchronized: This is going to be your session every week or 30 minutes, it is scheduled by the network administrator according to the size of the change that occurs + the bandwidth on the connection. If I want less time, I must provide the bandwidth, and to increase the bandwidth, I must make sure that there is a strong infrastructure

Amount of data loss = time of last replication - when the disaster occurred

2.2.9.2.2 REPLICATION LEVELS:

- Application level: Like SQL without equipment and interference from people, replication is done automatically within the application
- OS level: At the level of the operating system, use a software application, in case there are any additions, it will be used on the second site
- VM level: Able to transfer the entire VM and move it to another site such as Veeam It is the most widely used and is used to transfer data as a block level system
- storage level: All changes that occur are transferred to Storge, which is the most expensive because it requires an Enterprise license

The appropriate type of data center is selected according to the type of service provided, and more than one can be combined Type

2.2.9.2.3 REPLICATION SITE

- On the same data center, in case there is a problem on one server, it will be transferred to the other server at no time cost
- to two Data centres close together. In the event of a stretch cluster, I will be able to make a sync because they are connected to fibber
- on-premise with Cloud (Hybrid)

It differs from the backup in that the server run cannot do back-up and the server is running.

2.2.9.3 LOAD BALANCING

Distributing loads between more than one server. Allocates resources intelligently according to algorithms.

2.2.9.3.1 HOW IT WORKS:

When there are many requests on the server from users, the loads are distributed over more than one server, because if the load on the server increases, a very slow or a crash occurs for the system, it provides another server, and also if one of the server's malfunctions, the requests are transferred to other servers

2.2.9.3.2 HOW ARE THE USERS DISTRIBUTED?

Requests are received through a server and a VIP is created so that requests are distributed to the servers responsible for load balancing. The distribution is done through many algorithms, the appropriate ones are chosen according to the requirements of the institution

2.2.9.3.3 TYPES OF LOAD BALANCING:

1- Network Layer Algorithm (Layer 4)

How will he know who the server is running or not? Creates a session between the servers, when the server is down in the network, the requests are transferred to the other server automatically

2- Application Layer Algorithm (Layer 7)

The first type determines whether the server is running or not, through its activity on the network, but it may be working on the network and the service is off.

This type checks the port that provides the service if it down transfers the request to the other server:

Load Balancers	Cluster Module
Load Balancers distribute the processing load among the group of servers.	A cluster is a group of servers that run as if they were a single entity.
Load balancing can be simpler to deploy with different types of servers	It usually requires identical servers within the cluster
Load balancers require additional networking expertise for managing the different types of connected servers	Server clusters are more self-contained and managed by a controller automatically
Load balancers can operate independently of the destination servers and thus consumes fewer resources.	Cluster modules require node managers and node agents to communicate within the cluster which occupies bandwidth and processing on the servers
Relatively less resilient Load Balancing for applications eg. -While doing transactions If one server fails, the customer has to re-enter data again from the start as the user state will be lost.	Server clusters are more resilient for applications eg. -If any server got failed during the transaction, another server within the cluster will work and the customer will complete the transaction.

Table 5 Difference between Cluster module and load balancer

2.2.9.4 VIRTUALIZATION

- In the past, when downloading some services together, this resulted in a conflict, so each service of them needed a different server and it led to a waste of resources
- For virtualization, the problem was solved. It exploited the resources by making a program that helps to divide the resources of the Host operating system over more than one guest.
- To develop the second step and to provide more resources, the operating system was integrated with the virtualization program, and it was named Hyper-V

2.2.9.4.1 FEATURES:

- Provide high availability, when a malfunction occurs in one machine, you can move to another machine
- I can run more than one operating system on the same host
- Any attack on a particular dishonour does not affect the neighbourhoods that, in the case of communication between them, provides for the principle of isolation. There are certain advantages to virtualization. Monitor the guest's condition. When a dishonour takes large resources and needs other resources, but the server is unable to meet its needs, this dishonour will be transferred to a server else

2.2.9.5 STORAGE

A group of storage units that are treated as a single partition, with high availability. Dependency is available when there is a malfunction inside the hard drive. Data is not lost. There is no other copy of it on hard drives. These features are provided through RAID.

2.2.9.5.1 RAID TYPES:

- RAID0 When a hard drive fails, Dependency is not available
- RAID1 When a failure occurs, one copy is available
- RAID5 Data is distributed to all existing hard drives. If one fails, there is another copy. In case of failure 2, all data is damaged.

Differences in size, availability, and read and write speed. The connection in Strung through Viber is different from the network Switch Connecting to Storge is different from the normal Switch in the network It works on a different protocol than TCP / IP.

Note: the scale storage Depends on i/o, not storage size

2.2.9.5.2 STORGE CONCEPT:

A group of hard drives form an assembly called a shelf, and there is a RAID between them that is implemented by software Normally, there is more than a shelf in the data center, so there is a storage processor controller

It is the brain of the Storge that contains (the operating system through which a RAID is made, which contains a cache to speed up reading and writing)

Communication takes place between the storage and the servers. Zoning is done through a switch for police work so that the servers are linked to the private part of them.

There is a problem with the multibuys connection method that is solved through a small program provided by Vendor

2.2.9.5.3 HOW TO PARTITION STORAGE:

RAID is a pool that contains more than one lun that is distributed to different servers. It will appear inside the server as a partition. RAID can be divided into more than one lun or dealt with as one.

It is possible to make more than one shelf for a pond, and it can be of different types

Storage is made, consisting of more than one type of hard, your lesson. Each type is a pond, and a vertical pond is made that contains all the types of hard found in the storage.

2.2.9.5.4 HOW IS IT USED:

Taking advantage of I / o data is transferred between types of hard disks according to their need for I / o occurs automatically

2.2.9.5.5 WHY IS THERE CASH IN THE BRAIN STORAGE:

When you write data, it is written first on the cache and after you transfer it to the hard disk, the process of reading and writing speeds up and provides performance. The larger the cache size, the faster the process and contains a battery.

2.2.9.5.6 STORGE FEATURES:

- It can do replication on another site automatically
- Provide data compression & deduplication, especially if the data is cold
- Snapshot on a long level

2.2.9.6 BACKUP

Backup refers to the copying of physical or virtual files or databases to a secondary location for preservation in case of equipment failure or catastrophe. The process of backing up data is pivotal to a successful disaster recovery plan.

Enterprises back up data they deem to be vulnerable in the event of buggy software, data corruption, hardware failure, malicious hacking, user error, or other unforeseen events. Backups capture and synchronize a point-in-time snapshot that is then used to return data to its previous state.

Backup and recovery testing examines an organization's practices and technologies for data security and data replication. The goal is to ensure rapid and reliable data retrieval should the need arise. The process of retrieving backed-up data files is known as file restoration.

The terms data backup and data protection are often used interchangeably, although data protection encompasses the broader goals of business continuity, data security, information lifecycle management, and prevention of malware and computer viruses.

2.2.9.6.1 THE IMPORTANCE OF DATA BACKUP

Data backups are among the most important infrastructure components in any organization because they help guard against data loss. Backups provide a way of restoring deleted files or recovering a file when it is accidentally overwritten. In addition, backups are usually an organization's best option for recovering from a ransomware attack or a major data loss event, such as a fire in the data center.

2.2.9.6.2 WHY DO YOU NEED A BACK-UP?

System failure, database, power failure, ransomware, virus, delete files in these cases, the data has been completely lost. We need a backup to solve the problem

2.2.9.6.3 BACKUP PLAN AND STRATEGY? (1, 2, 3)

3- Make 3 copies of the data

2- We copy the data on different media

1- One outside the site cloud, DR

2.2.9.6.4 TYPES OF SOLUTION BACKUP?

- software backup solution is easier and faster used by large and medium companies
- hardware backup solution is cheaper used by small companies

2.2.9.6.5 BACKUP MEDIA?

- Storge is the best type because it is the fastest and has high performance. It is used in weekly, monthly, and daily copies
- Tab Library, the oldest type of backup, is slower than Storge. It can change the hard drive used in an out-site backup used for storing data in the long run.
- It is used as a backup outside the company

2.2.9.6.6 HOW DO YOU DETERMINE THE APPROPRIATE BACK-UP FOR YOUR COMPANY?

- Compatibility check.
- Is it hard ware or software?
- What operating systems will it support?
- Is it possible to back up all my apps?
- How to backup an element or block.

2.2.9.6.7 SHOULD YOU SPECIFY A POLICY:

- Several backup times on the level of the day, month, and year.
- How long do you save the data before deleting it, according to the business?
- A sheet is made for all the back-up data.

2.2.9.6.8 TYPES OF BACKUPS?

- full Take a full copy.
- proactive works constantly, in the event of a change, a back-up occurs immediately.
- Incremental daily differences from previous days.
- differential Today's version and all versions after the full back-up.

2.2.9.6.9 BACKUP FEATURES?

- Data compression saves space.
- Deduplication Take one copy of the block for a duplicate.
- indexing Interested in the restoration process, research work inside the back-up.
- Add daily backup to the Full version to save time, performance, and size.
- Encryption.
- scheduling.
- Restore by the user.

- Reports aimed at reaching the highest performance and modifying weaknesses.

2.2.9.7 RESTORE

The most important step is to test the restorer every period.

2.2.9.7.1 WHY DO WE NEED A RESTORE?

To access data after a disaster event you lost it. Restore levels are very important to understand to obtain the correct data

2.2.9.7.2 LEVEL RESTORE

- an item
- File
- Folder
- Operating system
- VM
- Applications
- configurations
- SQL query
- email
- Database
- Server

When defining recovery strategies, the organization must consider the issues

- income
- insurance coverage
- Resources
- technology
- data
- Suppliers
- Compatibility requirements

The recovery strategy must be approved by the management and this strategy must be consistent with the objectives of the place, once a disaster recovery strategy is developed and approved, it can be translated into a plan.

2.3 DISASTER RECOVERY

2.3.1 TYPES OF DISASTERS TO CONSIDER FOR YOUR DISASTER RECOVERY PLAN

To successfully recover from a disaster, businesses need to identify the types of disasters that could most impact the organization, and then build a DR plan around response to those events. The 3 main types of disasters are Natural Disasters, Physical Disasters & Technology-Based Disasters.

2.3.2 Types of Disasters

There are three categories of disasters we'll cover in this blog:

- Natural Disasters
- Physical Disasters
- Technology-Based Disasters

DR plans need to be more fluid than just focusing on technology failure. The thing with DR planning is that no two organizations are ever exactly alike. Think specifically about what your organization might classify as a disaster.

2.3.2.1 Natural Disasters

Natural disaster data recovery: Natural Disasters could include the following:

- Fire to one of your branches or offices
- Physical loss of a data center
- Storms impacting infrastructure
- Pandemics or other health issues for your staff

How should I respond to Natural Disasters?

Establish New Ways of Working

With Natural Disasters the focus is often going to be on establishing new ways of working and communicating. The pandemic is a great example of this. For most organizations, their routers, servers, workstations, and other technology didn't just die one day. Rather, the impact led to people changing the way they worked, often utilizing different devices than before, connecting to servers and applications through remote means, and establishing new security procedures, among other things.

2.3.2.2 Physical Disasters

- General infrastructure failures, such as loss of power or water
- A facility problem, such as a burst pipe or a collapsed roof
- Break-ins or physical security breaches
- Heating and cooling issues could make a workplace unusable

What's the impact of Physical Disasters on my organization?

Like Natural Disasters, Physical Disasters will also have an impact on where and how you work.

Sometimes a physical disaster such as a loss of power could simply require the organization to have people work from home for a short period. Other times, depending on your assets, you may have to relocate not only your people but also your technology infrastructure. And in the case of heating/cooling issues, a Physical Disaster could lead to a Technology Disaster, so while people can still work, there could be a huge impact looming.

How should I respond to Physical Disasters?

Know How to Recreate Your Work for the Short and Long Term

With Physical Disasters, it's important to understand not just how to recreate your work temporarily, but for how long. If there is a major power grid failure, likely, that this kind of disaster will only last for a relatively short period, and your focus on recovery should be short-term and temporary. But more significant physical disasters, such as a collapsed roof, may take months to resolve. Based on your impact analysis, you'll want to determine both temporary and long-term adjustments.

Know What Third-Parties You'll Need to Interact With

You also need to be aware of the third parties you need to interact with in the event of one of these disasters. If your HVAC fails, making your server closet too hot for operation, you must know immediately who your HVAC vendor is and how to contact them. Furthermore, your service agreements with these third-party providers need quality service level agreements that reflect your responsiveness needs in a disaster. These vendors can also provide input on expectations of what might happen in the event of a disaster

2.3.2.3 Technology-Based Disasters

Technology-Based Disasters could include the following:

- Ransomware and Malware incidents

- Server hardware failure
- Third-party SaaS/Cloud failure
- Data and security breaches
- Loss of data through corruption, failure, or viruses
- Phishing incidents
- Network infrastructure failure
- Major ISP outages

How should I respond to Technology Disasters?

Develop Your Response Plan and Contingencies

Once you have identified the potential technology issues that could arise to the level of disaster, you should develop your response plan and contingencies specific to those items.

This includes knowing who is on your response team, including third-party vendors and resources to help you procure any technology needed to resolve and restore systems to pre-disaster levels.

Create a Communications Plan for Staff & Vendors

Communications need to be put in place to your staff as well as other third parties when a technology disaster strikes.

Think about which of your customers, partners, lawyers, etc. may become a stakeholder, not just during the disaster, but also in the aftermath if there is liability involved.

2.4 DISASTER RECOVERY PLAN

2.4.1 WHY IS A DISASTER RECOVERY PLAN IMPORTANT?

Many disastrous events can lead to significant amounts of downtime for small businesses and large enterprises alike. Thriving businesses can occasionally absorb a few hours of downtime, but major disasters lead to major losses. Those who do not have a disaster recovery plan in place for business continuity risk unrecoverable loss. So that's why we are here to take a look at the different types of disaster recovery plans available.

Data from Gartner shows that businesses in the United States experience 87 hours of downtime each year on average. Yet, major natural disasters such as hurricanes and snowstorms can cause hundreds of hours of downtime. For example, Hurricane Sandy caused about 240 hours of downtime in Maryland and West Virginia, and 337 hours of downtime on Long Island.

Gartner estimates that downtime costs businesses $5,600 per minute on average, making it an obnoxiously expensive occurrence. Fortunately, businesses have options to mitigate the cost of a disaster. Experienced managed IT service providers (MSP) allow businesses to implement a comprehensive disaster recovery (DR) plan as part of their business continuity strategy.

2.4.2 WHAT IS A DISASTER RECOVERY PLAN?

The institution's Resumption works quickly after an unplanned accident ,Helps solve data loss and system restore so you can perform after an accident even if it's running at a minimum level .It consists of precautions to minimize the effects of a disaster so that you can continue to work and quickly resume mission-critical functions.

2.4.3 BEFORE THE PLAN

Business process analysis, business impact analysis, risk analysis, and identification of recovery goals. There is more than one disaster recovery plan that can be planned and we are now focusing on the data center disaster

2.4.4 ELEMENTS OF A DISASTER RECOVERY PLAN

One of the ways a municipality can protect itself from disaster is to create and implement a disaster recovery plan that addresses any type of disaster that can address any type of disaster and should be easy to follow and understand and be customized to meet the individualط needs of the organization Typical elements of the institution include the following:

1. Create a disaster recovery team. The team will be responsible for developing, implementing, and maintaining the DRP. A DRP should identify the team members, define each member’s responsibilities, and provide their contact information. The DRP should also identify who should be contacted in the event of a disaster or emergency. All employees should be informed of and understand the DRP and their responsibility if a disaster occurs communication plan should explain how to handle external communication and internal.
2. The first thing is to take the time and analyse all the potential factors that could be disturbing your work flow. Once you've done your research, it's time to create a different recovery plan for each of these scenarios. For example, cyber-attacks are becoming more prevalent and likely to occur, and unfortunately, the average firewall is not that strong enough to protect against most of them.

Thus, look at the possibility of a cyber-attack more intensely than would, for example, a tsunami. You can choose to encrypt data and secure devices. Try to understand

the weaknesses that exist within your systems, as these are the entry points that a hacker will use to gain access.

a. The best way is to keep yourself updated about the many schemes that hackers use. You can avoid the majority of malware infections and phishing scams.

b. The business impact analysis helps determine where to focus disaster recovery and identifies threats and vulnerabilities that can disrupt the operation of the systems and processes described.

c. The RTO and RPO of an organization will almost certainly influence its recovery strategy and the expenses associated with it.

3. Determine critical applications, documents, and resources. The organization must evaluate its business processes to determine which are critical to the operations of the organization. The plan should focus on short-term survivability, such as generating cash flows and revenues, rather than on a long-term solution of restoring the organization's full functioning capacity. However, the organization must recognize that some processes should not be delayed if possible. One example of a critical process is the processing of payroll to reduce the overall cost of a disaster recovery strategy, it is best to stratify the applications. The higher level reserved for mission-critical applications will require disaster recovery technology based on continuous real-time data replication. The middle tier may require a snapshot-based application, and finally, the lower tier may have a simple file-level backup system.

4. Specify backup and off-site storage procedures. These procedures should identify what to back up, by whom, how to perform the backup, the location of the backup, and how frequently backups should occur. All critical applications, equipment, and documents should be backed up. Documents that you should consider backing up are the latest financial statements, tax returns, a current list of employees and their contact information, inventory records, and customer and vendor listings. Critical supplies required for daily operations, such as checks and purchase orders, as well as a copy of the DRP, should be stored at an off-site location.

5. Test and maintain the DRP. Disaster recovery planning is a continual process as risks of disasters and emergencies are always changing. It is recommended that the organization routinely tests the DRP to evaluate the procedures documented in the plan for effectiveness and appropriateness. The recovery team should regularly update the DRP to accommodate changes in business processes, technology, and evolving disaster risks.

Management plan	Communication plan
Focus on protecting sensitive data during the event and defines the scope of actions to be taken during the incident and include the roles and responsibilities of the incident response team Disaster recovery focus Define recovery goals and steps to take to return the organization to operating condition after an accident	The next and crucial step is to identify those who need to be updated once disaster strikes. Engineers, Support, line managers, etc. will be involved in performing the actual disaster recovery and the communication plan should explain how to handle external communication and internal communication regarding crises.

Table 6 Management plan VS Communication plan

It is very important that when a disaster occurs, you are transparent about:

- What happened
- What steps are being taken to resolve the issue
- How you will determine the root cause
- How the business will adjust to avoid future incidents

Plan out Potential Limitations Caused by the Disaster

Your plan to respond to these Technology Disasters should also include expectations about restoration time for backup systems, limitations to your work due to technology failure, and details about any compliances or regulations by which your organization needs to abide.

Keep in mind, that it may not be possible to make every disaster recovery situation a positive experience. Your goal is to minimize the impacts of a technology failure by being reasonably prepared to respond and limiting the consequences.

2.5 DISASTER RECOVERY SITE

One of the key elements in any Disaster Recovery plan is the selection of a secondary site for data storage to help prevent data loss in the event of cyber-attacks or a natural disaster. DR software will extract critical business data from this secondary site and restore it to primary servers in the event of a major system failure. Three major types of disaster recovery sites can be used: cold, warm, and hot sites.

2.5.1 WHAT ARE THE THREE TYPES OF CLOUD COMPUTING SITES?

Disaster Recovery Site Types: Cold Computing Sites - the most simplistic type of disaster recovery site. A cold site consists of elements to provide power and networking capability as well as cooling. It does not include other hardware elements such as servers and storage. The use of a cold site is very limiting to a business since before it can be used, backup data along with some additional hardware must be sent to the site and installed. This will impede workflow.

Warm Computing Sites - contain all the elements of a cold site while adding to them additional elements including storage hardware such as tape or disk drives along with both servers and switches. Warm sites are "ready to go" in one sense, but they still need to have data transported to them for use in recovery should a disaster occur.

Hot Computing Sites - a fully functional backup site that already has important data mirrored to it. This is the ideal disaster recovery site but can be challenging to attain.

2.5.2 WHY ARE DISASTER RECOVERY SOLUTIONS IMPORTANT?

1. Network Downtime Is Expensive

If your employees or customers lose access to business-critical applications and data, there will be a direct impact on productivity and revenue. Let’s say your business has 100 employees, the average hourly revenue is $1,500 and the backup data set amounts to 2 TB. Given these parameters, a full restore from a local backup would take over 8 hours. The associated downtime cost would amount to $34,000 in lost revenue. Modern BCDR products offer the ability to run applications from backup instances of virtual servers. This allows users to continue operations while primary application servers are restored.

2. Data Backup Isn't Sufficient on its Own

You’d be hard-pressed to find a business today that doesn’t conduct some form of data backup. But what happens if your primary servers are irrevocably damaged? That's why it's essential to send copies of business data offsite. Modern BCDR products can run applications from backup instances of virtual servers, and some can extend this capability to the cloud. This approach is frequently called cloud DR or disaster recovery as a service (DRaaS). The ability to run applications in the cloud while onsite infrastructure is restored is widely considered to be a game-changer for disaster recovery. Backup and business continuity are not the same - and your business needs both.

3. Data Disasters Take Many Forms

Most IT downtime is a result of common, everyday actions like accidental (or intentional) data deletion, damage to computer hardware, and poor security habits. For example, a recent OWI Labs survey found that 81% of respondents occasionally or regularly log into public wife, despite security risks. A ransomware attack or virus can halt operations just as easily as a natural disaster. These are typically the result of human error but are preventable with BCDR planning and ongoing employee training.

4. Business Continuity Impacts Everyone

Ensuring access to applications and data following a disaster is just one piece of a successful BCDR strategy. Thorough BCDR planning should assess your business as a whole, and many planning efforts begin with an impact analysis or risk assessment. These studies can reveal weaknesses in your business's ability to continue operations. BCDR is a company-wide responsibility, and failure to protect your business from human error and system failures can be detrimental. Fortunately, by working with a skilled Managed Services Provider (MSP), you can avoid the fallout of poor BCDR planning. If you're looking for more information about BCDR strategies, or are interested in a risk assessment, reach out to I Corps for a free consultation.

2.6 STORAGE

2.6.1 TYPES OF DATA AND THEIR STORAGE

When it comes to data storage, all data isn't equal. After all, the data you use daily don't need the same level of protection or ease of access as long-term hot storage vs. cold storage backup. A large percentage of a business' data remains unleveraged due to data management and security challenges, which highlights the need to implement a data storage strategy.

2.6.2 WHAT IS HOT STORAGE?

The term “hot storage” refers to data that must be accessible immediately. This is a good option if the data is mission-critical and you can't wait for it when you need it. How fast the data can be accessed depends on how many routes it needs to take to reach its destination. Data processed closest to the source offers the fastest speed. Information that has further to go to reach its destination will be slower.

Information with the hottest storage requirements may use solid-state drives, which are intended for reduced latency and greater transactional rates than traditional hard drives. On the other hand, hard disk drives are better suited to circumstances where the drive is heavily utilized because of its superior resilience in the face of frequent read/write cycles.

2.6.3 WHERE IS HOT STORAGE INFORMATION LOCATED?

Hot archival information is located in an edge-storage configuration. In this approach, files are stored on servers within close range of their intended user population. This provides better network latency and bandwidth when accessing these resources from remote locations—especially at peak times when traffic is highest.

2.6.4 THE BENEFITS OF HOT STORAGE

Hot data archival technology uses non-volatile memory. Information stored will not be lost even in the event of a power outage. Its speed makes it ideal for a variety of use cases. Additional benefits include:

- Real-Time Processing: Hot data can be utilized in real-time processing applications that require fast response times such as CRM, ERP, and e-commerce platforms
- Reliability: Information is stored on SSDs, which are more reliable than HDDs. Hot storage is backed up more frequently than cold archival. Thus, there is less risk of losing important information in the event of business disruption.
- Speed: The faster storage speeds allow information to be accessed quickly

2.6.5 WHAT IS COLD STORAGE?

Information that is rarely used or accessed is a good candidate for cold archival. This is typically information that must be retained for compliance purposes. The information is often stored long-term and sometimes indefinitely. Cold archival is cheaper and slower than hot archival.

2.6.6 WHEN TO USE COLD STORAGE

A common use case for this type of storage is archived projects. Archived project documents don’t need to be accessed frequently. However, companies may want to refer to them later for research or reference. Storing legal and HR information is another use case. Often these departments have long-term archival requirements. Cold archival keeps this information available for audits.

2.6.7 THE BENEFITS OF COLD STORAGE

There is no need to pay premium prices for data that doesn't require frequent access. Cold archival is a way to save money. Additional benefits include:

- Stores inactive data more economically
- Reduces costs
- Simplifies archival option
- Meets regulatory requirements efficiently
- Prevents overloading primary repositories with inactive data

2.6.8 WHAT IS WARM STORAGE?

Warm data archival caches less frequently accessed information to avoid spikes in demand. Data stored here are updated every few hours, days, weeks, months, or years depending on the frequency specified. It allows companies to have access to their most recent files without having to perform frequent backups. Warm data archival may include cloud-based backup services to free up space on an organization's primary servers and archival systems that are cheaper but not online all the time.

2.6.9 WHEN TO USE WARM STORAGE

Use this form of archival for information that doesn't require frequent access. Examples include data for statistical modeling or time series forecasting. Another example is for data that needs to be replicated and synchronized across multiple servers.

A common scenario for warm archival is to bridge data access after mergers and acquisitions. Mergers and acquisitions often lead to separate archival infrastructures with incompatible file formats. Warm archival acts as a bridge by providing read-only access using one format while storing files originating from both legacy systems on tape.

2.6.10 THE BENEFITS OF WARM STORAGE

Warm data is much easier to back up. The backups must only encompass the changes made since the last full one. Restoring from backup is also easier with warm data archival. Information in warm archival is already online and waiting in its original location after being restored. Warm archival uses "chunking," which makes restoring data faster than cold archival.

2.7 Cloud

2.7.1 WHAT IS THE CLOUD?

The cloud servers that are accessed over the Internet, and the software and databases that run on those servers.

Cloud servers are located in data centres all over the world. By using cloud computing.

The cloud enables users to access the same files and applications from almost any device, because the computing and storage take place on servers in a data center, instead of locally on the user device.

For businesses, switching to cloud computing removes some IT costs and overhead: for instance, they no longer need to update and maintain their servers, as the cloud vendor they are using will do that. This especially makes an impact on small businesses that may not have been able to afford their internal infrastructure but can outsource their infrastructure needs affordably via the cloud. The cloud can also make it easier for companies to operate internationally because employees and customers can access the same files and applications from any location.

Users access cloud services either through a browser or through an app, connecting to the cloud over the Internet — that is, through many interconnected networks — regardless of what device they are using.

2.7.2 WHY IS IT CALLED 'THE CLOUD'?

"The cloud" started as a tech industry slang term. In the early days of the Internet, technical diagrams often represented the servers and networking infrastructure that make up the Internet as a cloud. As more computing processes moved to this servers-and-infrastructure part of the Internet, people began to talk about moving to "the cloud" as a shorthand way of expressing where the computing processes were taking place.

2.7.3 WHAT ARE THE MAIN SERVICE MODELS OF CLOUD COMPUTING?

- Software-as-a-Service (SaaS): Instead of users installing an application on their device, SaaS applications are hosted on cloud servers, and users access them over the Internet. Examples of SaaS applications include Salesforce, Mail Chimp, and Slack.

- Platform-as-a-Service (PaaS): In this model, companies don't pay for hosted applications instead, they pay for the things they need to build their applications. PaaS vendors offer everything necessary for building an application, including development tools, infrastructure, and operating systems, over the Internet. PaaS examples include Heroku

and Microsoft Azure.

- Infrastructure-as-a-Service (IaaS): In this model, a company rents the servers and storage they need from a cloud provider. They then use that cloud infrastructure to build their applications. IaaS providers include Digital Ocean, Google Compute Engine, and OpenStack.

2.7.4 WHAT ARE THE DIFFERENT TYPES OF CLOUD DEPLOYMENTS?

cloud deployment types have to do with where the cloud servers are and who manages them.

The most common cloud deployments are:

- Private cloud: A private cloud is a server, data center, or distributed network wholly dedicated to one organization.

- Public cloud: A public cloud is a service run by an external vendor that may include servers in one or multiple data centres. Unlike a private cloud, public clouds are shared by multiple organizations. Using virtual machines, individual servers may be shared by different companies, a situation that is called "multitenancy" because multiple tenants are renting server space within the same server.

- Hybrid cloud: hybrid cloud deployments combine public and private clouds, and may even include on-premises legacy servers. An organization may use its private cloud for some services and its public cloud for others, or it may use the public cloud as a backup for its private cloud.

- Multi-cloud: multi-cloud is a type of cloud deployment that involves using multiple public clouds. In other words, an organization with a multi-cloud deployment rents virtual servers and services from several external vendors. Multi-cloud deployments can also be hybrid clouds and vice versa.

2.7.5 HOW IS THE CLOUD DIFFERENT FROM THE TRADITIONAL CLIENT-SERVER MODEL OF THE INTERNET?

The Internet has always been made up of servers, clients, and the infrastructure that connects them. Clients make requests of servers, and servers send responses. Cloud computing differs from this

model in that cloud servers aren't just responding to requests they're running programs and storing data on the client's behalf.

2.7.6 WHAT ABOUT CONTAINERS? ARE CONTAINERS IAAS, PAAS OR SAAS?

Like virtual machines, containers are a cloud virtualization technology. They are part of the PaaS (Platform-as-a-Service) cloud model. Virtualization for containers occurs one abstraction layer up from where it occurs for virtual machines, at the operating system level instead of at the kernel level (the kernel is the foundation of the operating system, and it interacts with the computer's hardware). Each virtual machine has its operating system kernel, but containers on the same machine share the same kernel.

2.7.7 AWS vs. Azure: Understanding the Key Differences

Azure and AWS are two of the world's leading cloud solutions, differing on several key parameters.

Cloud computing allows users to rent their IT infrastructure instead of buying it. Customers choose to access and pay for computing power provided by service providers like AWS and Azure online or in the cloud, rather than investing extensively in databases, software, and hardware.[37]

- Amazon Web Services (AWS), is a subsidiary of the eCommerce and technology giant Amazon. It offers over 200 services from data centres worldwide and has millions of users across start-ups, large enterprises, and leading government agencies. [37]

- Microsoft Azure, often known as Azure, is another top cloud computing service. It aids in the management of applications through Microsoft-operated data centres. The platform provides many cloud services including analytics, computing, storage, and networking. Azure, like AWS, has an extensive toolkit that is constantly growing and has been the industry leader in cloud computing for more than ten years.[37]

AWS and Azure resemble each other in terms of basic features and functionalities however, they differ in other aspects.[37]

	AWS	Azure
Computing power	AWS leverages EC2 tailored to customer needs.	Azure users are given the option of creating a VM from a virtual hard disc (VHD).
Cloud storage offerings	AWS has services like AWS S3, EBS, and Glacier.	Azure Storage Services offers Blob Storage, Disk Storage, and Standard Archive.
Privacy and security enforcement methods	AWS performs an excellent job of selecting secure alternatives by default, ensuring enhanced privacy.	Azure is protected by a dedicated Cloud Defender service, an AI-powered tool.
Ease of use and documentation model	AWS provides a feature-rich and user-friendly dashboard, along with extensive documentation.	Azure keeps the account information in one place, although its documentation system is less intuitive and search-friendly.
Licensing and license mobility	AWS licenses are more configurable and feature-rich.	Azure provides more software as a service (SaaS) feature and is easier to set up for Windows administrators.
Networking	Users can build private networks using AWS' VPC.	Azure relies on a VPN
Machine learning (ML) modelling	AWS' Sage Maker gives total freedom and flexibility in creating ML models.	Azure ML Studio is primarily focused on providing a codeless experience through drag-and-drop elements.

Table 7 AWS VS. Azure

CH03: LITERATURE REVIEW

3.1 OVERVIEW

In this chapter, we present the previous studies that we passed during the search and browsing process. We looked at nearly 35 disaster recovery plans and disaster recovery strategies uploaded online.

We have selected some plans and studies and studied them in detail in terms of their features and some of the points that we have criticized considering them to be avoided in our application.

It should be noted that some previous studies have a direct and indirect relationship in our application of the disaster recovery plan, which helped in collecting data that helps

In the analysis and construction of the system in addition to the data obtained by the project team from the interviews. The project team spotlight the following studies:

3.2 DISASTER RECOVERY MANAGEMENT WITH POWERSHELL PSDRM

Zavala, Shashidhar, Varol, and Zhou [41] obtained that the custom program design to produce a standardized approach to disaster recovery is "PowerShell Disaster Recovery Management" (PSDRM), using PowerShell as a back-end method for performing Disaster Recovery steps such as creating a clone copy of a system shutting it down and deploying it to an isolated network to segment the system to prevent conflicting IP conflicts.

The next piece highlights a front-end executable system that Read-Host Switch input parameter, used for invoking a read line of input which prompts the user for an entry attached with a switch parameter for menu-like commands.

The switch data then has combinations of actions that perform cloning a system, migrating between hosts from a VCenter managed server, performing a shutdown of VM, creating a snapshot, disconnecting network drives, and these actions are mirrored for a Hyper-V infrastructure.

The final piece is the executable that performs different scenarios from a menu item for example Snapshot Function, Clone Function, Migrate VM, Power On, Power Off, and Clean Up.

The objective of these actions provides a method of cloning a machine to a sideloaded Host dedicated to storing running machines on a segmented network.

The infrastructure runs a three Host system, and two are for Host redundancy for migration and provides continuity during maintenance and the third Host is reserved for disaster recovery provided an attack occurs such as ransomware, then what has occurred is a sideloaded hot spare outside of the scenarios then used for cloning and testing of a valid running VM.

The executable includes a selection for what type of system so that it associates the right commands for the associated system giving the user an all-in-one box solution for different virtualized systems as in VMWare or Hyper-V. Different scenarios are required for forensic evidence when an attack has occurred so creating a snapshot to save the machine's volatile state is crucial for investigative measures so the machine can be shut down and cloned for deployment to the third host reserved for restoring cloned machines in a network isolated environment with a restorable snapshot.

A menu item to perform these combination actions are used for simple iteration from non-technical users such as "ANOMALY – SNAPSHOT_ISOLATE" which performs a combination of the functions associated with capturing the machine's volatile state and deploying on an isolated network.

3.3 DISASTER RECOVERY SYSTEM AND SERVICE CONTINUITY OF DIGITAL LIBRARY:

Yuncai Wang in [40] obtained that the disaster recovery system is an integral part of the digital library information security system.

Compared with traditional methods of disaster recovery, the effect of a remote disaster recovery system is more tangible. With the constant renewal of equipment, upgrade of software, and perfection of maintenance measures, the RDRS will play a greater role in disaster recovery.

Large-scale replication to the cloud can be accelerated and automated through disaster recovery. Continuous data replication ensures real-time data synchronization and reduces switching window frames by happening in the background without software interruptions or performance issues one strike. Highly automated machine conversion and orchestration processes reduce the risk of human error during migration turnarounds. Once the migration is complete, no compatibility issues and minimal IT skills are required. The image below shows the disaster's Detailed recovery process.

3.5 ONLINE DATA BACKUP AND DISASTER RECOVERY TECHNIQUES IN CLOUD COMPUTING:

K. R. Singh in [39] obtained that presented backup and recovery techniques that have been developed in the cloud computing domain.

that these techniques have their advantages and disadvantages All these approaches can provide the best performances under all uncontrolled circumstances such as cost, security, low implementation complexity, redundancy, and recovery in a short period.

Similarly, in the list of techniques for maintaining the cost of implementation, SBBR focuses on cost reduction.

however, fails to concentrate on the optimization concept and redundancy.

With an entirely new concept of virtualization REN cloud also focuses on low-cost infrastructure with complex implementation and low-security levels.

3.6 SUMMARIZE AND DISCUSS THE STUDIES

After reading and understanding the previous studies and deducing some information from them in table [6], we will present the advantages of each of the previous studies to clarify them in a simplified manner.

Disaster Recovery Management with PowerShell PSDRM	Disaster Recovery System and Service Continuity of Digital Library	Online Data Backup and Disaster Recovery Techniques in cloud computing
Ease of implementation	using disc protection technology RAID	Privacy and ownership.
overall simplicity	equipment from power surges	Relocation of servers to the cloud.
Cost		Data security.
management consistency		Reliability.
scalability time		Cost-effectiveness.
application compatibility		Appropriate Timing.
		Privacy and ownership.

Table 8 Advantages of each of the previous studies

CH04: Methodology

4.1 OVERVIEW

The success of our project depends largely on the practical study methodology used in the study; In this chapter, we will explain the methodology chosen to build our project as required with its main phases and describe what needs to be done in each phase. We will discuss the advantages and disadvantages and consider why this methodology was chosen, how choosing the right model will affect project progress and quality, and how choosing the right model will help us achieve the project's objectives.

4.2 What is Waterfall Project Management?

Waterfall model: In the waterfall model, each stage must be completely completed before the next one begins. At the end of each phase, a review takes place to determine if the project is on the right path and whether or not to continue or discard the project.

The waterfall approach is among the oldest project management techniques. It consists of sequential phases that map out every essential step of a project.[38]

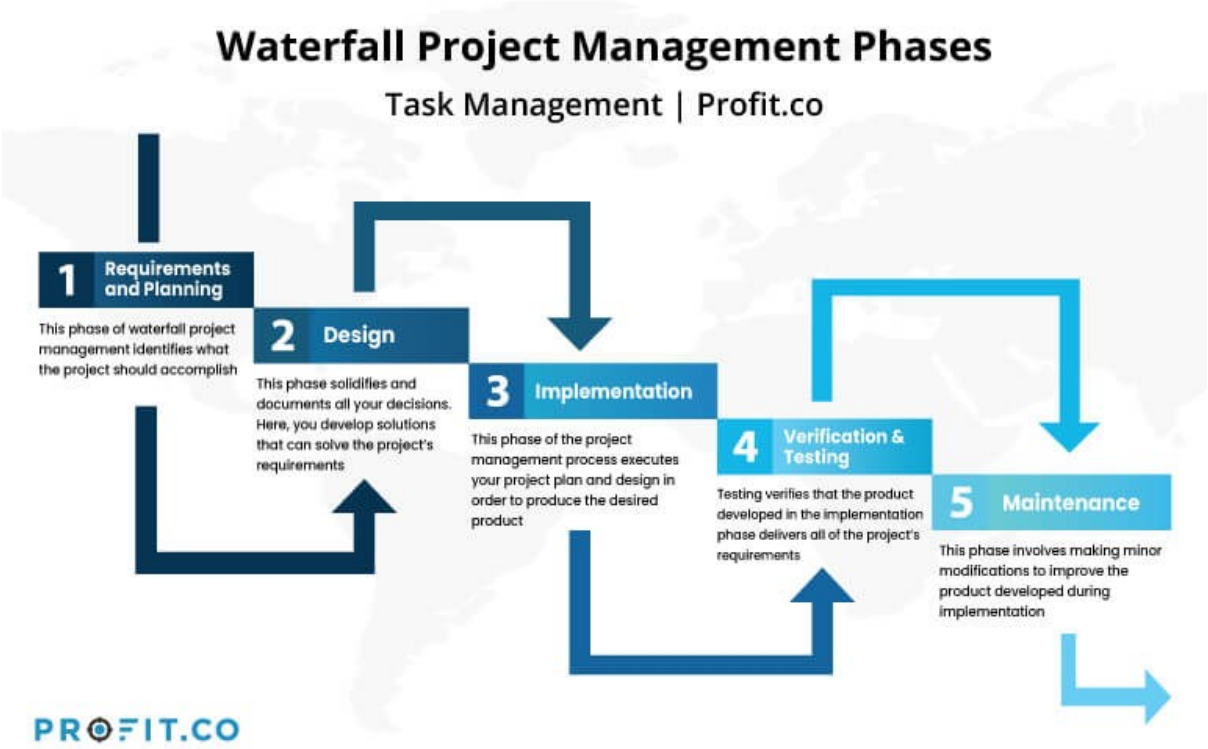

Figure 5 Phases of Waterfall

Each step of the methodology depends on the step that precedes it, so it is not possible to move to the next step without completing the previous step.

4.3 Waterfall project management stages

The stages of waterfall project management vary from project to project. But in general, you can group waterfall approach activities into five phases: planning, design, implementation, verification, and maintenance.[38]

1. Requirements and planning

The requirements and planning stage of the waterfall methodology in our project determine what the project should do. Through the methodology, we try to understand the requirements of the project based on what the Khan Yunis Municipality needs. This stage includes defining and describing the project, assumptions, dependencies, quality metrics, and schedule.[38]

2. design

The design phase solidifies and documents all assumptions and suggestions. In this case, we develop solutions that can solve the project requirements. The best way to do this is to note all the actions that are taken to deliver the scope of the project to its full implementation.

The design covers the project schedule, budget, and objectives, and you can think of the design as a blueprint or roadmap for the complete project.[38]

3. Implementation

The implementation phase implements your project plan and design to produce the required product.

Implementation takes a large part of waterfall project management. Everything that happens during this stage must be carefully documented.[38]

4. Verification / Test

The test verifies that the final project developed in the implementation phase fully meets the requirements of the project. If not, the project team should review the project from Phase 1 to determine what went wrong.[38]

5. Maintenance work

The maintenance phase extends beyond the five phases of project management into the life of the project. This stage includes making minor modifications to improve the project that was developed during implementation and performing other routine maintenance tasks. It also works on modifying the project from errors that were not discovered during the implementation of the project.[38]

4.4 Advantages and Disadvantages of Waterfall Project Management

Benefits and advantages of waterfall project management:[38]

1. Simplicity in training

The waterfall approach focuses on thorough documentation, making it easier for new team members to follow the project's progress. The new members can refer to the documentation to catch up on the project.

2. Proof of progress

Waterfall project management clearly defines the project's milestones in the requirements and planning phase. It is easier to identify the project's progress by reviewing these milestones. The distinct steps of the technique also clearly indicate how close the project is to completion.

3. Easy management

Waterfall-based projects are easy to manage because of their linear nature, and it is easier to identify the project's progress at any given time. If changes occur, you can easily refer to the waterfall documentation to see how you can address them.

4. It saves money and time

The waterfall approach emphasizes conceptualization and detailed documentation. The two activities better prepare for executing a project correctly in its first trial. Understanding the project's needs and implementation plan from early on can save you the time, money, and effort that would arise from revisions.

Disadvantages of the waterfall project management approach:[38]

1. Inflexible and resistant to change

The waterfall approach consists of sequential steps that pour into each other. So, the outcomes of one phase of the project are necessary to move on to the next phase. Changes in one phase imply that the whole waterfall process needs a review. This makes the management style difficult to change.

2. Focuses on one phase at a time

Phases of the waterfall approach are linear and sequential. No two processes can run simultaneously. This can be disadvantageous if personnel required for an early phase is backlogged, and the project grinds to a halt because of it.

4.5 Waterfall vs. Rapid Development

The waterfall project remains relevant despite new rapid management techniques like agile development. The waterfall approach focuses on the step-by-step implementation of a project. In contrast, agile project management focuses on iterative, shorter project cycles that deliver a working prototype to the client.[38]

The project team continuously improves this prototype until the project is complete. Both techniques have benefits when utilized correctly. The waterfall approach will serve you well if you stick to traditional project management. But if you're going to combine the old and the new, a hybrid waterfall methodology would be an excellent place to start your implementation.[38]

CH05: PROPOSED SOLUTION

5.1 OVERVIEW:

In this chapter, we will clarify the municipal system and the weaknesses that were discovered during our visit to the municipality and answer inquiries in addition to the proposed solution and how to implement it by presenting it with a simplified explanation by analysing the system and its requirements and then designing and implementing the proposed system and verifying the validity of the system.

5.2 GENERAL EXPLANATION OF THE MUNICIPAL SYSTEM:

The municipality's data center contains Firewall, Core Switch, and 5 servers. Each server provides several services for employees within the municipality. These servers serve 250 employees. A daily backup of the virtual machine is transferred to another place through the Veeam program according to a scheduling system. Through a wireless network, the other place contains two servers and qnap, and the raid5 system is applied to them to preserve them from corruption as high availability, and also the data is transferred daily and uploaded to the iDrive cloud.

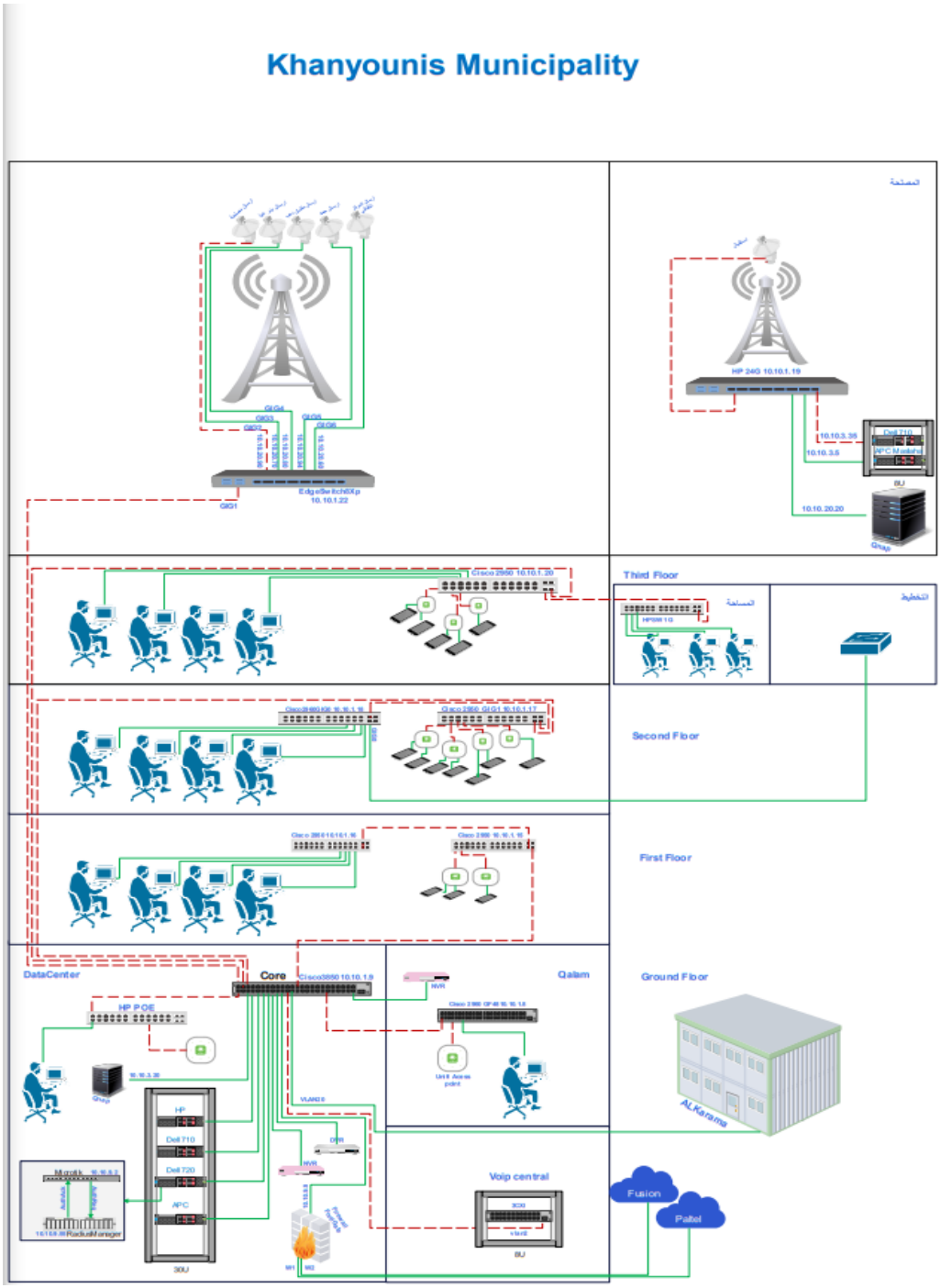

Figure 6 Infrastructure of Khan Younis Municipality

5.3 SYSTEM ANALYSIS

A general explanation of the municipal system showing the details of the data center and the services it provides and the percentage of the effect of business continuity in each service:

5.3.1 SERVER INFORMATION:

Server1	Location: municipal
	Server Model: DEL R710
	Operating System: ESXi 6
	CPUs: Xeon (E5645)
	Memory: 80 G
	Total Disk: 1.5 T
	IP Address: 10.10.3.33
	NIC: 4

Table 9 Server 1

Server2	Location: municipal
	Server Model: DEL R720
	Operating System: ESXi 6
	CPUs: Xeon (4110)
	Memory: 64 G
	Total Disk: 2.5 T
	IP Address: 10.10.3.34
	NIC: 4

Table 10 Server 2

Server3	Location: municipal
	Server Model: HP ProLiant DL300
	Operating System: ESXi 6
	CPUs: Xeon (4110)
	Memory: 50 G
	Total Disk: 2 T
	IP Address: 10.10.3.35
	NIC: 4

Table 11 Server 4

Server4	Location: municipal
	Server Model: HP workstation
	Operating System: windows server 2016
	CPUs: Xeon (E3 1225)
	Memory: 24 G
	Total Disk: 9.5 T
	IP Address: 10.10.3.33
	NIC: 4

Table 12 Server 5

5.3.2 DETAILS OF THE VIRTUAL MACHINE AND THE SERVICES IT PROVIDES:

VM	Service	Job	priority
01	Oracle test	Testing	31%
02	Query	Control of indoor and outdoor wireless units	31%
03	Block shadi	Blockchain Check	31%

Table 13 Server 1

VM	Service	Job	priority
01	File server	Personnel files, correspondence, PDF files, and all employee documents	50%
02	Oracle DB	Other municipal data Citizen's subscriptions and bills	100%
03	Data Giss database	A plan for all Khan Yunis services location GPS	50%
04	ArcGIS	shape charts	50%

Table 14 Server 2

VM	Service	Job	priority
01	VCenter management	virtual machine management	0%
02	Torit server	Download crack programs	0%
03	Este node management server	Antivirus for 250 devices	0%
04	DMA radios	internet authentication	10%
05	Kaspersky	Server antivirus	0%
06	S4	Printer server	10%

Table 15 Server 3

VM	Service	Job	priority
01	Server backup	Veeam backup and replication	50%

Table 16 Server 4

VM	Service	Job	priority
01	Prig	Network Monitor	60%
02	DNS, DHCP	Routing devices and allocating network addresses	100%
03	Windows 3cx	VoIP server	50%
04	Windows Deployment	Windows Download Services for Employees' Devices	25%
05	Web server	internal applications	25%
06	Windows sharing	work remotely	5%
07	API	Intermediary between database and applications	100%
08	Developer 12/cApi	web logic for API oracle	25%
09	Microtia	Internet service control	10%
10	Test hardware	Server troubleshooting	0%

Table 17 Server 5

Priority services to maintain the continuity of its work:

01	**DNS, DHCP**	**Routing devices and allocating network addresses**	**100%**
01	Oracle DB	Other municipal data Citizen’s subscriptions and bills	100%
03	Data Giss database	A plan for all Khan Yunis services location GPS	50%
02	API	Intermediary between database and applications	100%
04	ArcGIS	shape charts	50%
03	Windows 3cx	VoIP server	50%
01	File server	Personnel files, correspondence, PDF files, and all employee documents	50%

Table 18 Priority services

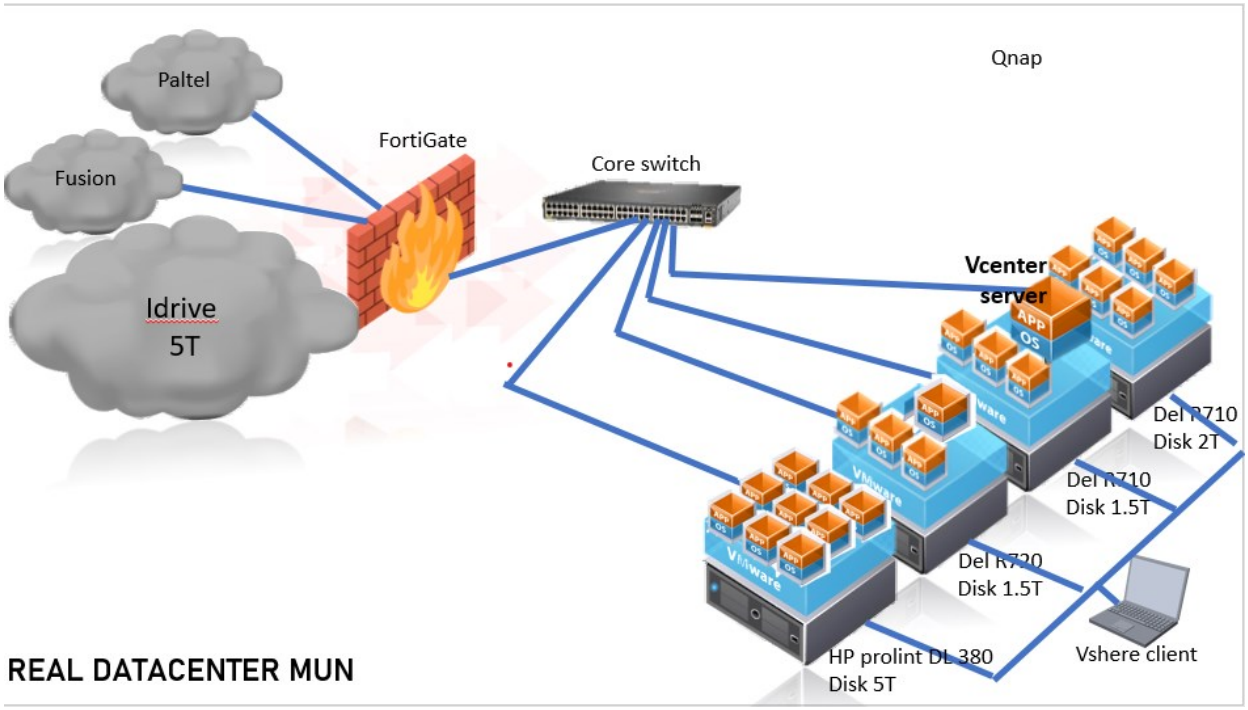

Figure 7 REAL DATACENTER MUN

5.4 SYSTEM PROBLEMS IN KHAN YOUNIS MUNICIPALITY:

- The failure of any virtual machine leads to a prolonged downtime
- Host failure results in the inability to access services provided by virtual machines
- The backup plan is weak
- Loss of data when disasters occur according to the timing of the disaster
- Big downtime when disaster strikes
- Storing the backup outside the organization leads to an increase in RTO when the system is restored
- There is no shared storage on the servers

5.5 WEAKNESSES IN KHAN YOUNIS MUNICIPALITY:

- qnap storage slow storage and restore
- Not using HA services in VCenter
- No disaster recovery plan
- There is no strategy for recovering from disasters
- There is no backup copy in the same place
- No shared storage on servers

5.6 DETERMINE RECOVERY TIME OBJECTIVE (RTO) AND A RECOVERY POINT OBJECTIVE (RPO)?

- Targeted duration of time between the event of failure and the point where operations resume => Open
- the maximum length of time permitted that data can be restored from => open
- lost data => must by zero

5.7 HOW DID WE DEFINE THE BACKUP STRATEGY?

- ✓ Understanding the infrastructure
- ✓ Determine the RTO, the RPO of the municipality
- ✓ Proposing strategic solutions
- ✓ Choosing the most appropriate strategy

Over the past few months, we have developed many appropriate and inappropriate solutions for the municipality's situation. We will mention them now, and we will compare the solutions and choose the best ones.

5.8 WE WILL START WITH SOLUTIONS THAT REDUCE DISASTERS WITHIN THE DATA CENTER

5.8.1 Solution 1

Migrate 22virtual machines to two servers, each server with 11 virtual machines Create Server Mirroring on other servers

What Does Server Mirroring Mean?

Server mirroring is a process in network management through which a replica of a server is continuously created on run time.

Server mirroring is a technique used for business continuity, disaster recovery, and backup. Duplicating the entire contents of a server on another remote or in-house server allows data to be restored if the primary server fails.

In simple terms, it looks like looking in a mirror and can be seen, but not the original. Two or more servers with identical online content and synchronized updates, except the main server, are called mirror servers.

Server mirroring is primarily implemented to create a fault-tolerant and redundant server computing infrastructure.

Besides backup and disaster recovery, server mirroring is also used in load balancing by providing identical data for fast downloading to remotely connected users.

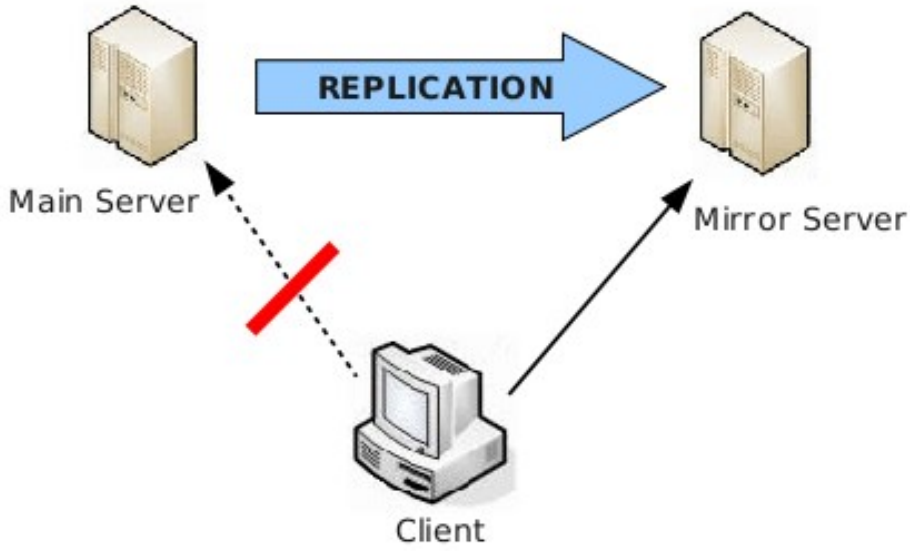

Figure 8 REPLICATION

The performance of a local mirror server depends on the following:

- Number of endpoints that it serves
- Network bandwidth
- Frequency of updates
- You can deploy multiple mirror servers to accommodate large environments.

Requirements that must be met to implement the mirror of the servers

- ✓ The physical servers of the brand are identical
- ✓ The server version is the same
- ✓ There is shared storage on the servers or used freeness
- ✓ There is a connection between servers

Solution 2**(Using Veeam backup and replication)**

DEFINITION

Veeam Backup & Replication

One of the first vendors to develop backup software for virtual machines, backup apps fail to recognize the difference between a physical server and a virtual server.

Backups are image-based and can be created from snapshots on Dell EMC, Hewlett Packard Enterprise, NetApp, and Nimble Storage arrays.

Veeam Backup & Replication Instant recovery feature

With Instant Recovery, an entire machine can be restored from backup in a matter of minutes.

In addition to backing up and recovering VMs, Veeam Backup & Replication can protect and restore individual files and applications for environments such as Exchange and SharePoint. It can also provide transaction-level restores of Oracle and Microsoft SQL databases.

Some of these features include a scale-out backup repository, instant file-level recovery, remote office/branch office support, and Sure Backup technology that tests VM backups to ensure data recovery. A Veeam Cloud Connect feature provides secure cloud backups, and the software has fully integrated cloud disaster recovery.

The Veeam software is available in free and paid editions: Veeam Backup Free provides a subset of the features and functionality of the Veeam Enterprise Plus paid edition.

Veeam Backup & Replication v12 focuses on security.

How do Backup and Restore of Failover Clusters work?

To process a cluster with Veeam Agent for Microsoft Windows, you must complete the following tasks:

In Veeam Backup & Replication, create a protection group that includes Active Directory objects and add to this protection group one of the following types of objects:

- Cluster account of the failover cluster whose data you want to back up.
- Active Directory container that includes this cluster account.

In Veeam Backup & Replication, configure a Veeam Agent backup job for a failover cluster. To add a failover cluster to the backup job, do the following:

At the Job Mode step of the New Agent Backup Job wizard, select Failover cluster.

At the Computers step of the wizard, add to the job the cluster account that you added to a protection group in step 1. Alternatively, you can add to the job a container or protection group that includes this cluster account.

IMPORTANT:

If a backup task within a Veeam Agent backup job that processes a failover cluster completes unsuccessfully or a new node is added to a cluster, Veeam Agent will create a full backup of all shared disks of the cluster during the next backup job run.

You cannot create per-machine backup files with a Veeam Agent backup job that processes failover clusters because of cluster limitations. The backup job with failover clusters in the backup scope creates a separate backup file for each cluster.

Data Restore from Failover Cluster Backups.

You can perform data restore tasks with failover cluster backups created by Veeam Agent. For example, you can restore entire volumes or individual folders and files from such backups.

Consider the following:

- When you restore data of a failover cluster, make sure that the cluster is added to the Veeam Backup & Replication inventory as part of a protection group.
- When you restore data of a failover cluster with shared disks, Veeam Agent does not restore data of a disk witness. During volume restore for shared disks of a cluster, the disk witness is not displayed at the Disk Mapping step of the Volume Restore wizard.
- Backup Copy from Failover Cluster Backups
- You can perform data copy tasks with failover cluster backups created by Veeam Agent to a secondary location.

When you copy failover cluster backups, consider the following:

The network traffic will be higher compared to the traffic sent during the Veeam Agent backup job run.

If you copy a failover cluster backup in the immediate mode, the job ignores the Use per-machine backup files option enabled for the backup repository and creates a single backup copy file for each cluster. If you copy a failover cluster backup in the periodic mode, the job will create backup copy files as set for the backup repository.

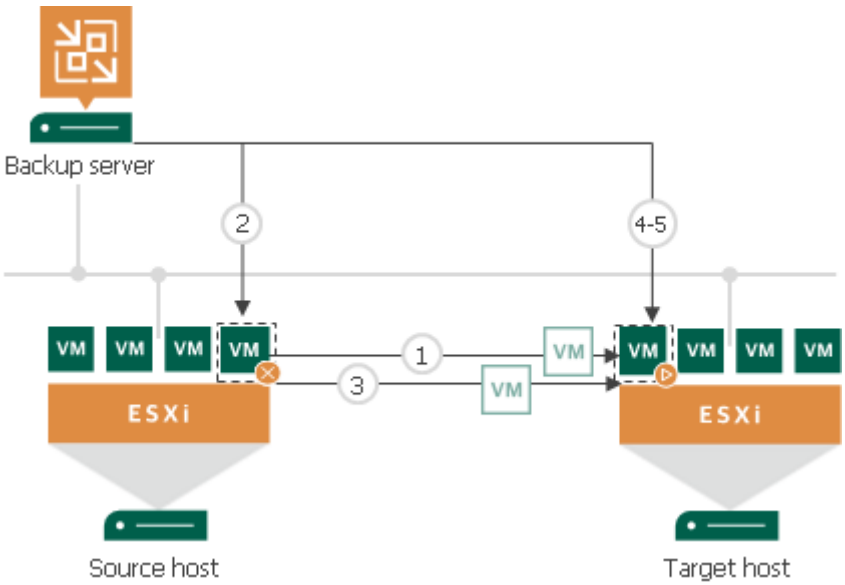

Figure 9 Requirements that must be met to implement Veeam Backup & Replication failover

- ✓ The physical servers of the brand are identical
- ✓ The server version is the same
- ✓ There is a connection between servers
- ✓ Provide a separate server for Veeam backup and replication

Through this solution, we can solve the problem of unavailability of storage on the same site, which leads to quick access to the backup and when both servers are not available, the backup server can prepare for the task

Solution 3: (Failover Clustering in Windows Server 2019)

A failover cluster is a group of independent computers that work together to increase the availability and scalability of clustered roles (formerly called clustered applications and services). The clustered servers (called nodes) are connected by physical cables and by software. If one or more of the cluster nodes fail, other nodes begin to provide service (a process known as failover). In addition, the clustered roles are proactively monitored to verify that they are working properly. If they are not working, they are restarted or moved to another node.

Failover clusters also provide Cluster Shared Volume (CSV) functionality that provides a consistent, distributed namespace that clustered roles can use to access shared storage from all nodes. With the Failover Clustering feature, users experience a minimum of service disruptions.

Failover Clustering has many practical applications, including:

Highly available or continuously available file share storage for applications such as Microsoft SQL Server and Hyper-V virtual machines

Highly available clustered roles that run on physical servers or on virtual machines that are installed on servers running Hyper-V

In Windows Server 2019, there are two components of the system that have their quorum mechanisms:

- ✓ Cluster Quorum: This operates at the cluster level (i.e., you can lose nodes and have the cluster stay up)
- ✓ Pool Quorum: This operates on the pool level (i.e., you can lose nodes and drives and have the pool stay up). Storage pools were designed to be used in both clustered and non-clustered scenarios, which is why they have a different quorum mechanism.

Cluster quorum recommendations

- ✓ If you have two nodes, a witness is required.
- ✓ If you have three or four nodes, the witness is strongly recommended.
- ✓ If you have five nodes or more, a witness isn't needed and doesn't provide additional resiliency.
- ✓ If you have internet access, use a cloud witness.
- ✓ If you're in an IT environment with other machines and file shares, use a file share witness.

How to cluster quorum works

When nodes fail, or when some subset of nodes loses contact with another subset, surviving nodes need to verify that they constitute the majority of the cluster to remain online. If they can't verify that, they'll go offline.

But the concept of majority only works cleanly when the total number of nodes in the cluster is odd (for example, three nodes in a five-node cluster). So, what about clusters with an even number of nodes (say, a four-node cluster)?

There are two ways the cluster can make the total number of votes odd:

First, it can go up by adding a witness with an extra vote. This requires user set-up.

Or, it can go down one by zeroing one unlucky node's vote (happens automatically as needed).

Whenever surviving nodes successfully verify, that they are the majority, the definition of majority is updated to be among just the survivors. This allows the cluster to lose one node, then

another, then another, and so forth. This concept of the total number of votes adapting after successive failures is known as a Dynamic quorum.

Dynamic witness

Dynamic witness toggles the vote of the witness to make sure that the total number of votes is odd. If there are an odd number of votes, the witness doesn't have a vote. If there is an even number of votes, the witness has a vote. Dynamic witness significantly reduces the risk that the cluster will go down because of witness failure. The cluster decides whether to use the witness vote based on the number of voting nodes that are available in the cluster.

Dynamic quorum works with a dynamic witness in the way described below.

Dynamic quorum behaviour

- ✓ If you have an even number of nodes and no witness, one node gets its vote zeroed. For example, only three of the four nodes get votes, so the total number of votes is three, and two survivors with votes are considered a majority.
- ✓ If you have an odd number of nodes and no witnesses, they all get votes.
- ✓ If you have an even number of nodes plus a witness, the witness votes, so the total is odd.
- ✓ If you have an odd number of nodes plus witnesses, the witness doesn't vote.

Dynamic quorum enables the ability to assign a vote to a node dynamically to avoid losing the majority of votes and to allow the cluster to run with one node (known as last-man-standing). Let's take a four-node cluster as an example. Assume that a quorum requires 3 votes.

5.9 EXPLAIN HOW FAILOVER OCCURS IN FAILURES

All nodes vote and the witness votes, so the majority is determined out of a total of 5 votes. After one failure, you're in Scenario 4. After two simultaneous failures, you skip down to Scenario 2.

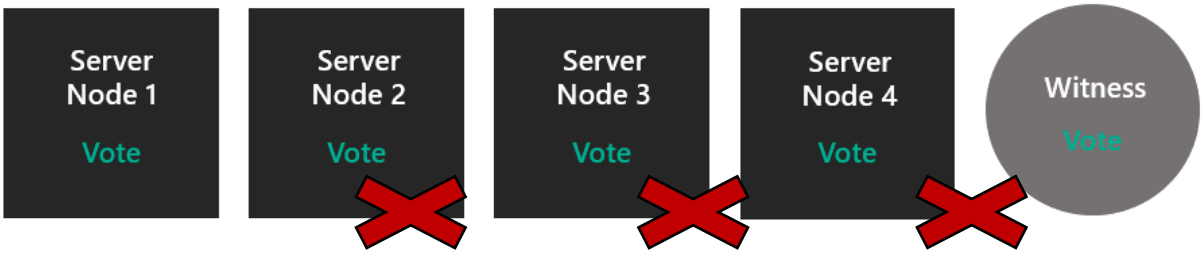

Figure 10 Failover Cluster

- Can survive one server failure: Yes.
- Can survive one server failure, then another: Yes.
- Can survive two server failures at once: Yes.

Implementation requirements

- ✓ All servers are the same version of Windows 2019.
- ✓ all hardware must be certified for the version of the windows server.
- ✓ the computer contains the same or similar components.
- ✓ complete failover cluster solution must pass all tests in the validate a configuration wizard.
- ✓ If you are using iscasi, each network adapter must be assigned either a network connection or the iscasi protocol, not both.

A table showing an evaluation of the proposed solutions :

#	Description of the solution	Evaluation
Solution 1	Server mirroring in the same site	The following solution is very suitable, but the municipality does not have storage in the same place, and this is a prerequisite for the success of the operation
Solution 2	Veeam backup and replication	It is the appropriate solution for the municipality's situation. All its requirements are available, but it may need a license for some services to complete the work
Solution 3	Failover Clustering in Windows Server 2019	The next solution is a suitable solution for the municipality because all its requirements are available and it is easy, cheap, and low cost

Table 19 Poposed Solutions

The last solution is to improve the infrastructure and take advantage of the features that are available in it, such as exploiting the advantages of VMware vSphere VMware vSphere provides IT administrators with several tools to prevent host failure, which we will mention now:

1. vSphere vmotion

vSphere vmotion enables zero-downtime, live migration of workloads from one server to another so your users can continue to access the systems they need to stay productive.

Perform Live Migrations

VMware vSphere lives migration allows you to move an entire running virtual machine from one physical server to another, with no downtime. The virtual machine retains its network identity and connections, ensuring a seamless migration process. Transfer the virtual machine's active memory and precise execution state over a high-speed network, allowing the virtual machine to switch from running on the source vSphere host to the destination vSphere host. This entire process takes less than two seconds on a gigabit Ethernet network. Live migration allows you to:

- ✓ Automatically optimize virtual machines within resource pools.
- ✓ Perform hardware maintenance without scheduling downtime or disrupting business operations.
- ✓ Move virtual machines away from failing or underperforming servers.

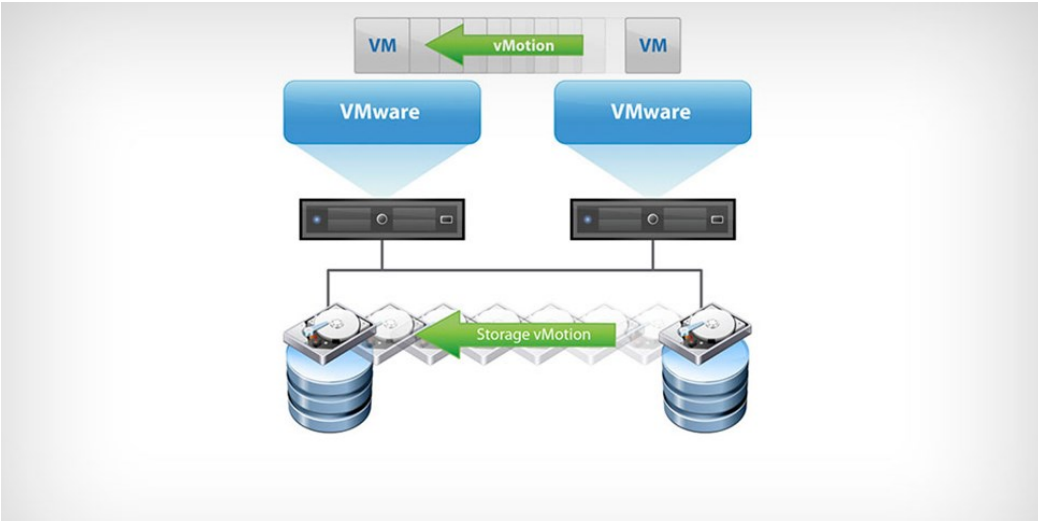

Figure 11 VMware vSphere

VMware HA to optimize and balance workloads

VMware HA is a technology that protects applications against host server failure. If the VM on which an application is running fails, then the VM is automatically restarted on another host. VMware HA can provide availability for nearly any application, but it's particularly well suited for applications that lack native HA capabilities.

VMware HA works by monitoring the host servers within a resource pool to ensure that the system can detect each host's heartbeat. An agent running on the host produces the host's heartbeat. If VMware HA fails to detect a host's heartbeat, then it assumes that the host has failed. VMware HA then takes corrective action by automatically restarting the VM on another host within the resource pool.

Among VMware HA's key features is its ability to automatically detect a server failure and automatically restart a VM. Additionally, VMware HA performs resource checks to make sure that sufficient capacity will be available when a VM needs to fail over to another host.

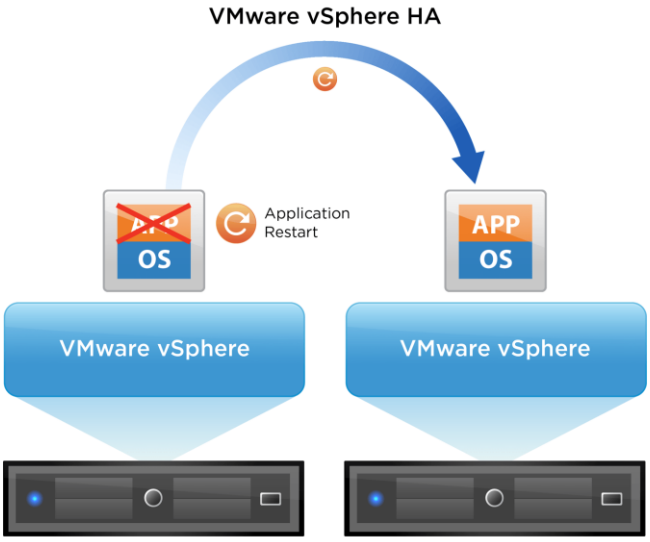

Figure 12 VMware HA

2. vSphere Fault Tolerance (FT)

VMware vSphere Fault Tolerance (FT) provides continuous availability for applications (with up to four virtual CPUs) by creating a live shadow instance of a virtual machine that mirrors the primary virtual machine. If a hardware outage occurs, vSphere FT automatically triggers failover to eliminate downtime and prevent data loss. After failover, vSphere FT automatically creates a new, secondary virtual machine to deliver continuous protection for the application.

provides a higher level of business continuity than vSphere HA. It works by creating a duplicate (secondary) copy of the virtual machine on a different host and keeping the two VMs in sync. The secondary VM can immediately take over in the event of an ESXi host failure and the entire state of the virtual machine will be preserved.

Because FT provides zero downtime and zeroes data loss, it is usually used for business-critical applications that must be available all the time. It is also sometimes used for applications that have no native capability for clustering.

vSphere FT also has some disadvantages. Here are the main ones:

- increased resource usage. An FT-protected VM will use twice as many resources. For example, if the primary VM uses 2GB of RAM, the secondary VM will also use 2GB of RAM.
- only virtual machines with a single vCPU are compatible with Fault Tolerance.
- hosts must be licensed for vSphere FT.
- the VM must not have any snapshots.

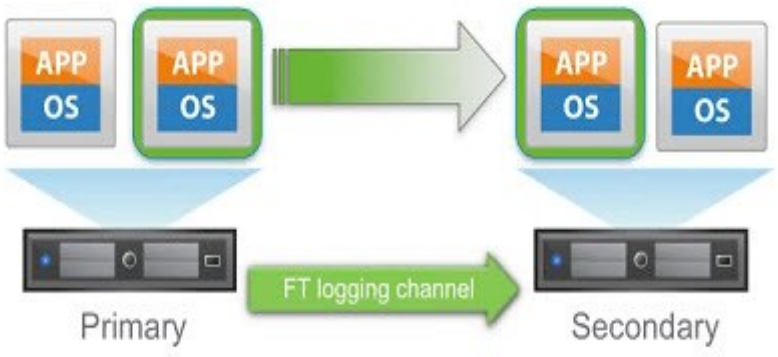

Figure 13 FT VMware

3. Distributed Resource Scheduler

VMware designed DRS to ensure optimal VM performance. VMware DRS achieves this by automatically distributing VMs across vSphere hosts based on workload characteristics. This ensures that VMs equitably consume the host resources and that a single host in a cluster isn't carrying a disproportionate share of the workload.

DRS can use other factors beyond host capacity when balancing VM workloads. For instance, DRS respects affinity and anti-affinity rules. Admins can also configure DRS to optimize power consumption. If DRS detects that the available host resources exceed the VM requirements, it can automatically place hosts in standby mode to reduce power consumption. Admins can then bring those same hosts back online if their resources are later needed.

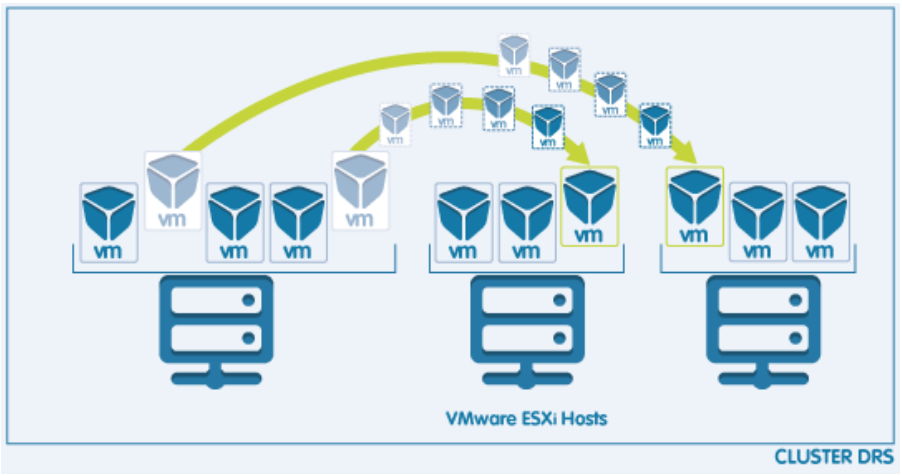

Figure 14 DRS VMware

CH06: RESULTS AND DISCUSSION

6.1 RESULTS

1. Reduce recovery point objective by replication of Active directory and synchronize replication on storage.
2. reduce downtime
3. no lost data
4. improve resilience by a failover cluster, load balancer, DR, replication, and stretch cluster.
5. apply high availability on level datacentre by building disaster recovery site
6. recovery time objective =1 by load balancer on a web server
7. There is no centralization and reliance on a distributed system

6.2 VALIDATION AND VERIFICATION

We will start by checking all the practical results through the screenshot of the process of testing the results

1. first test results: replication active directory
    a. Server in the first data centre with active directory installed it .local

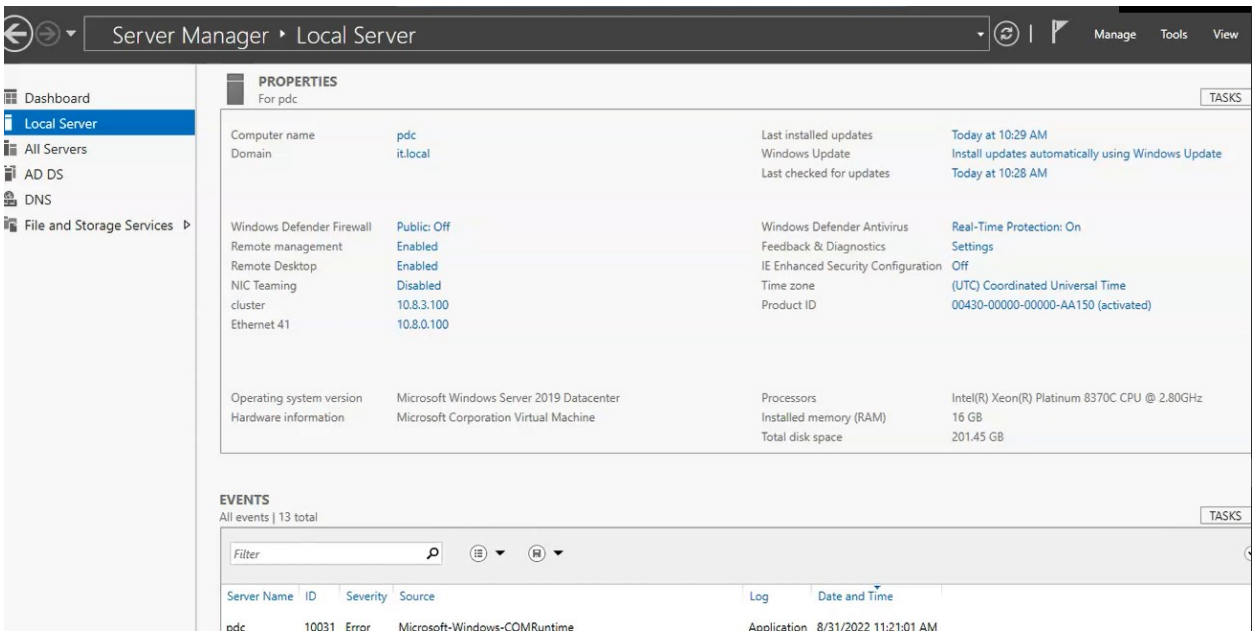

Figure 15 Datacenter1

b. The server in disaster recovery installed an additional active directory added to the active directory (it. local)

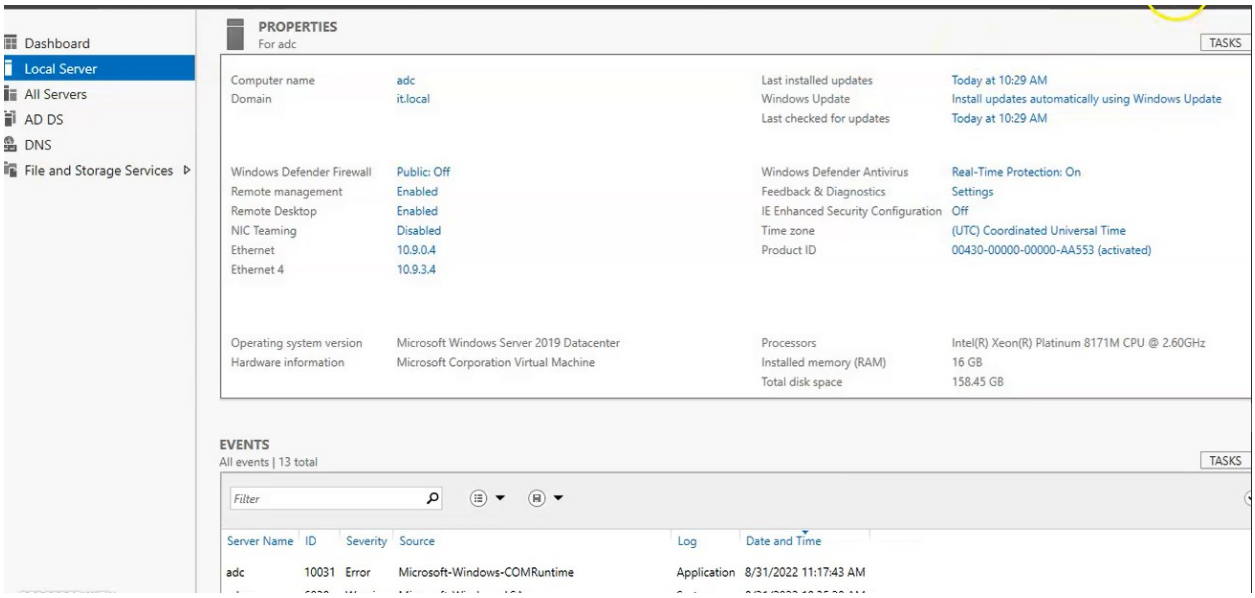

Figure 16 Datacenter2

c. The result of linking the two sites and adding add to PDC

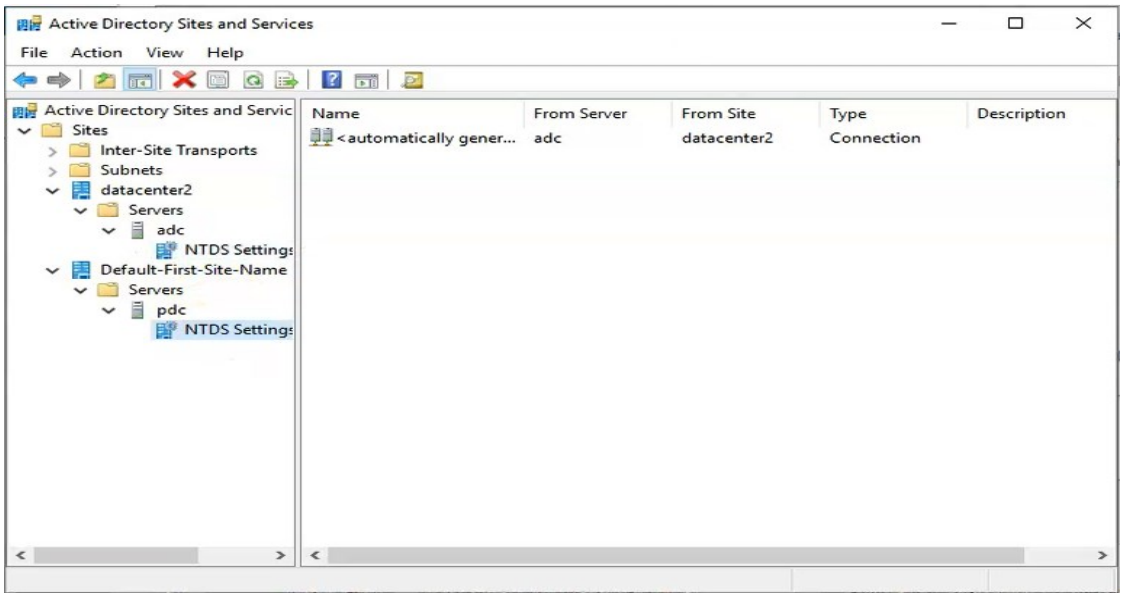

Figure 17 Join two datacenter

d. To check the replication process we will add a new user name test 1

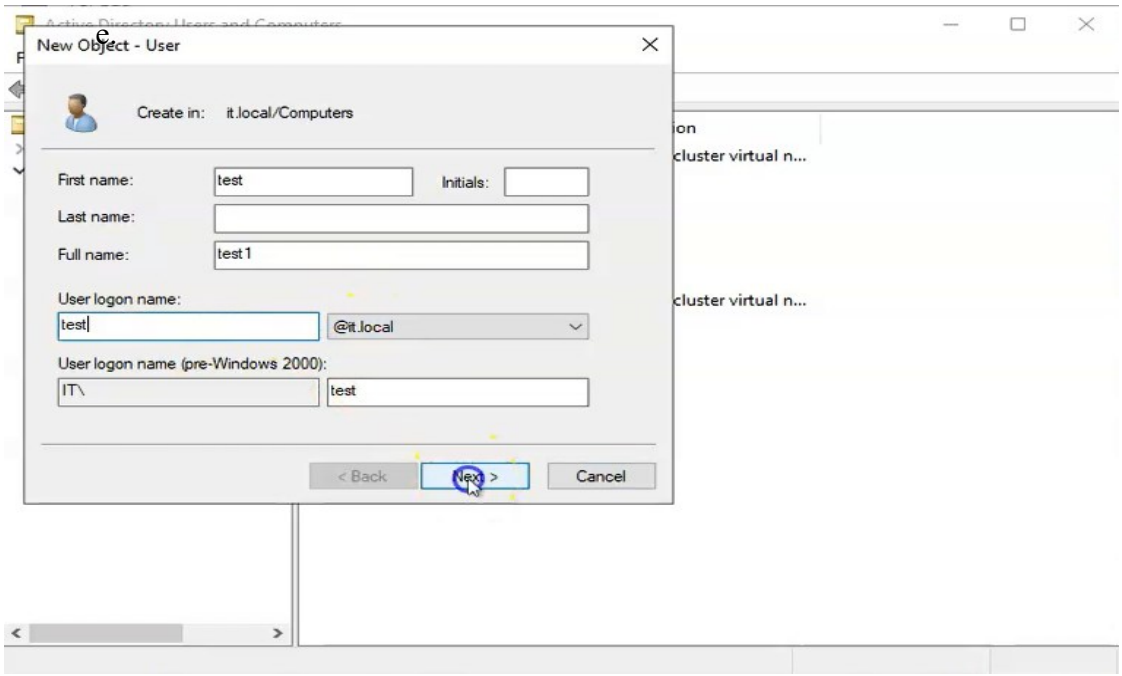

Figure 18 Add user on datacenter1

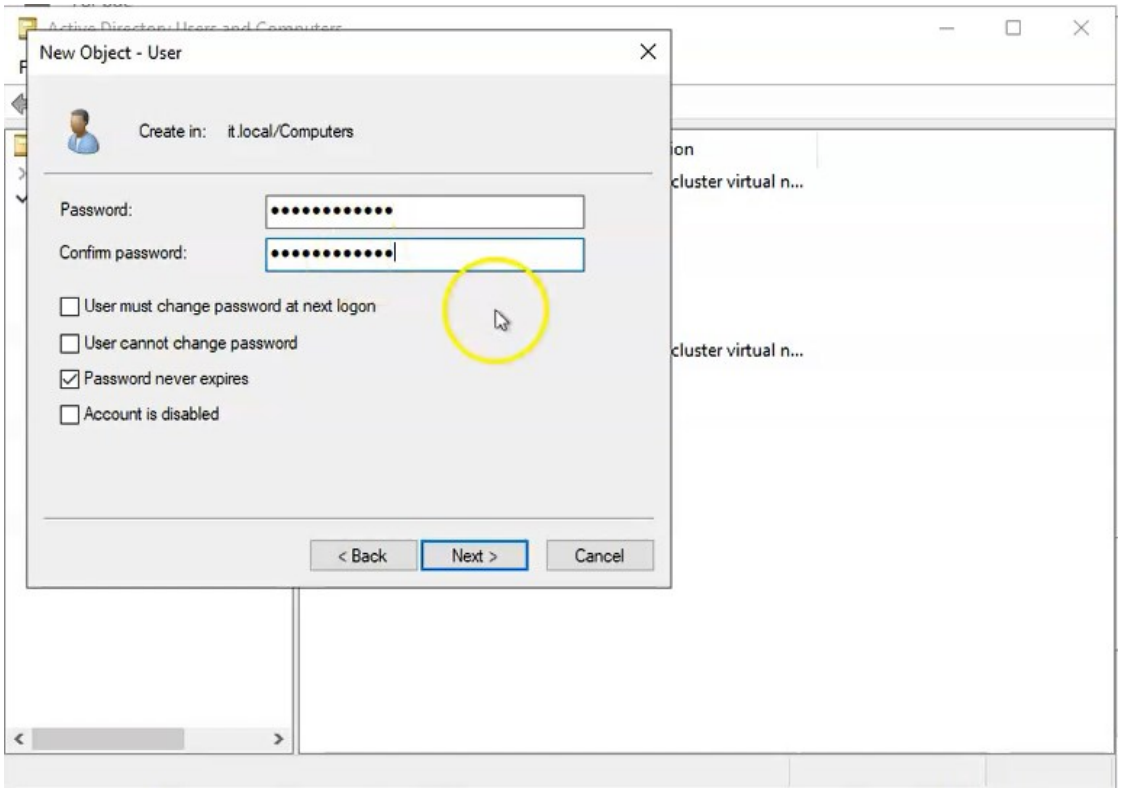

Figure 19 Add user on datacenter1

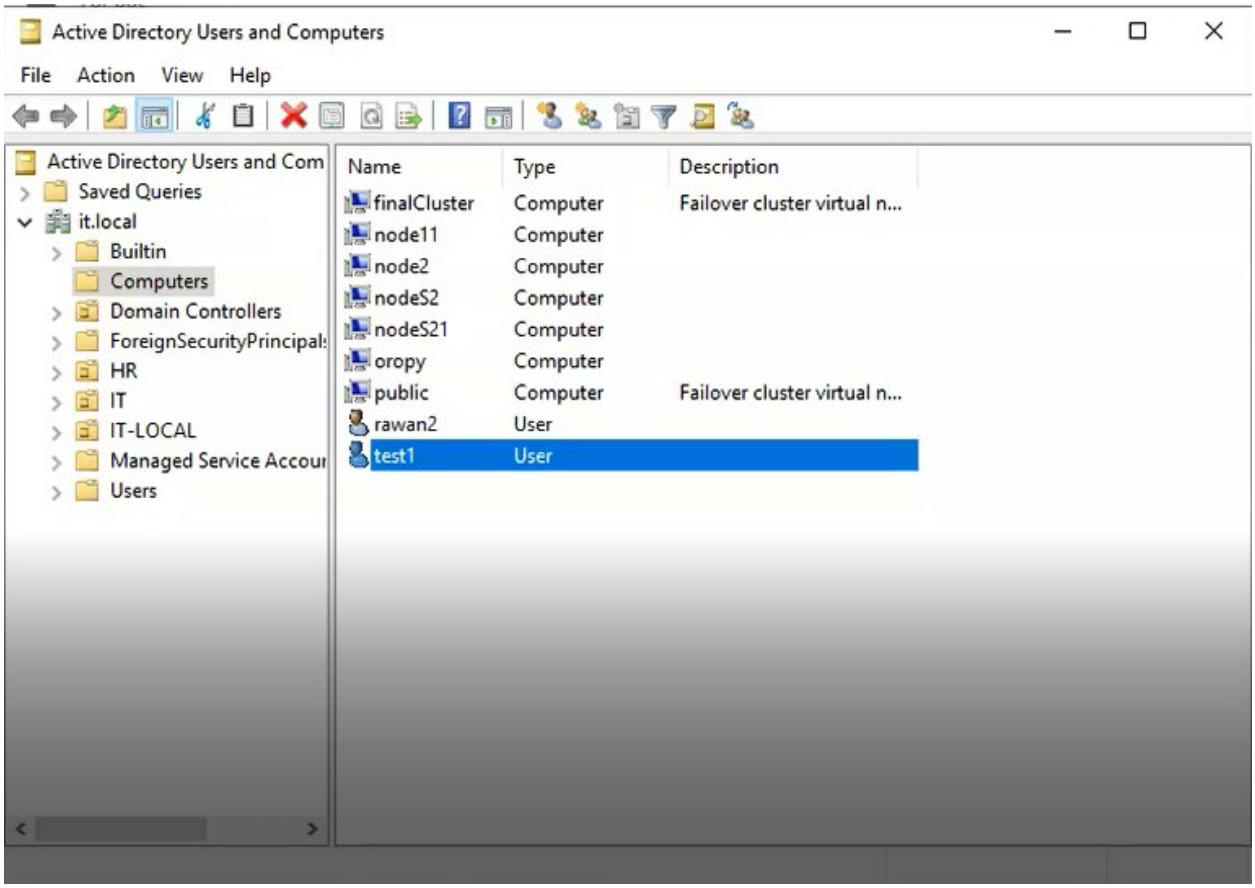

Figure 20 Add user on datacenter1 successfully

f. To speed up the data transfer process we apply replica now

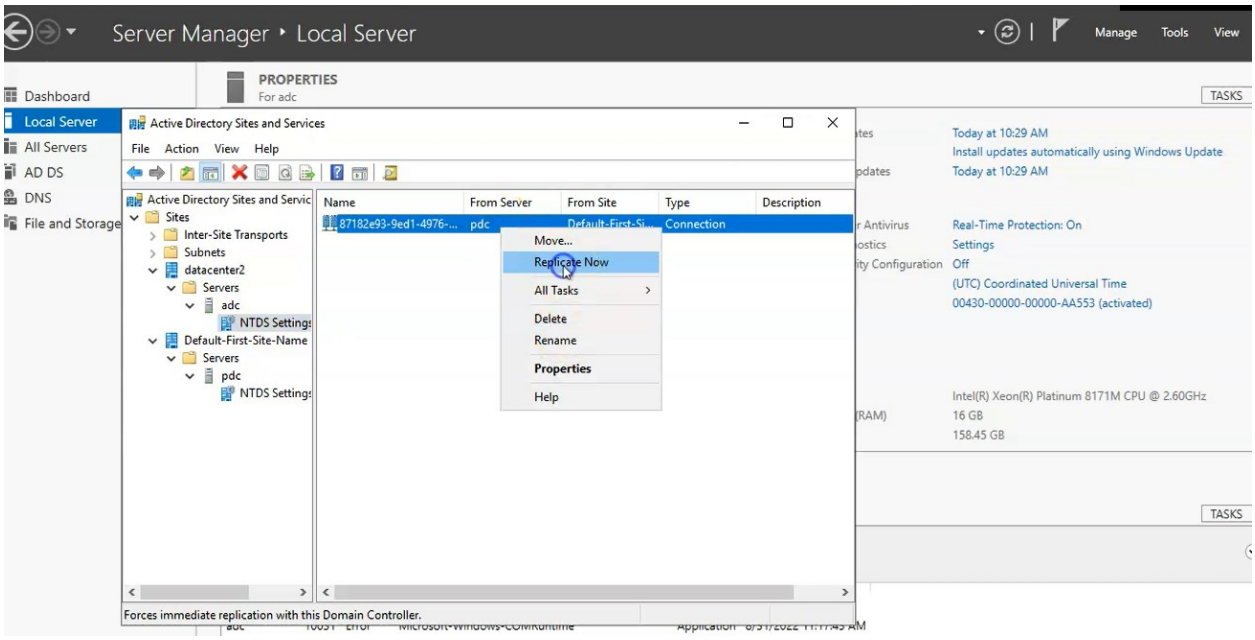

Figure 21 Replica

Successful replication of disaster recovery

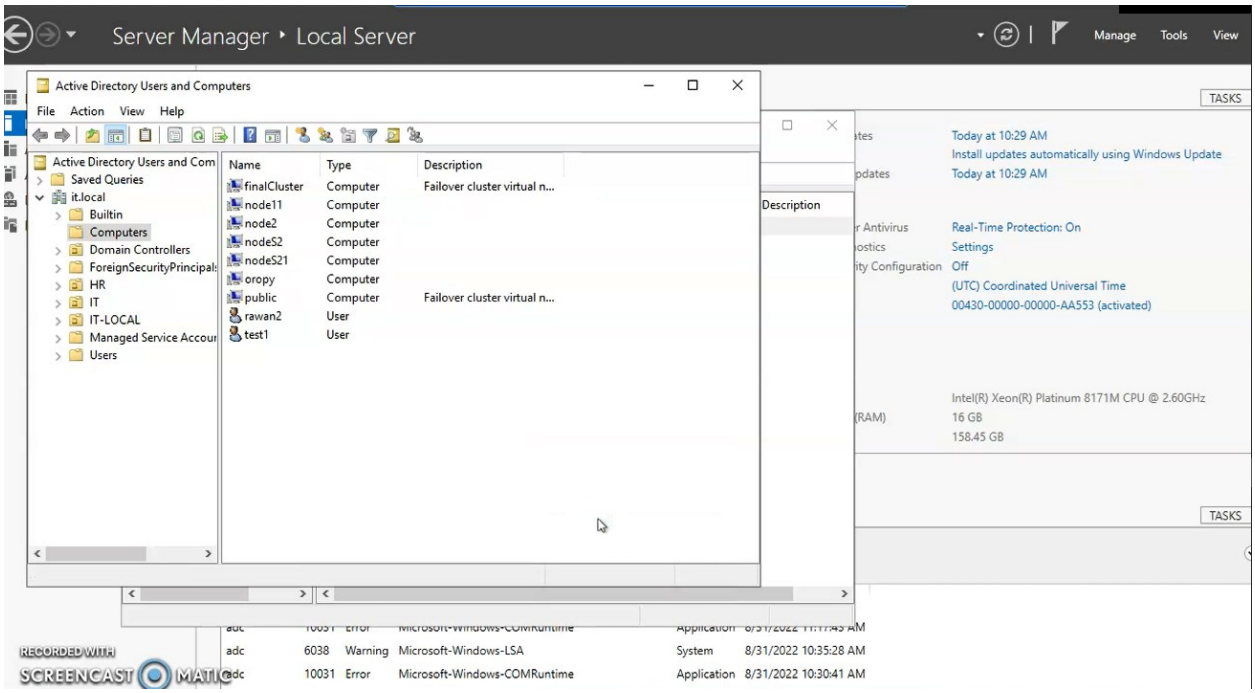

Figure 22 Successful replication

2. second test result: load balancer on the web server
    a. Install load balancer on server

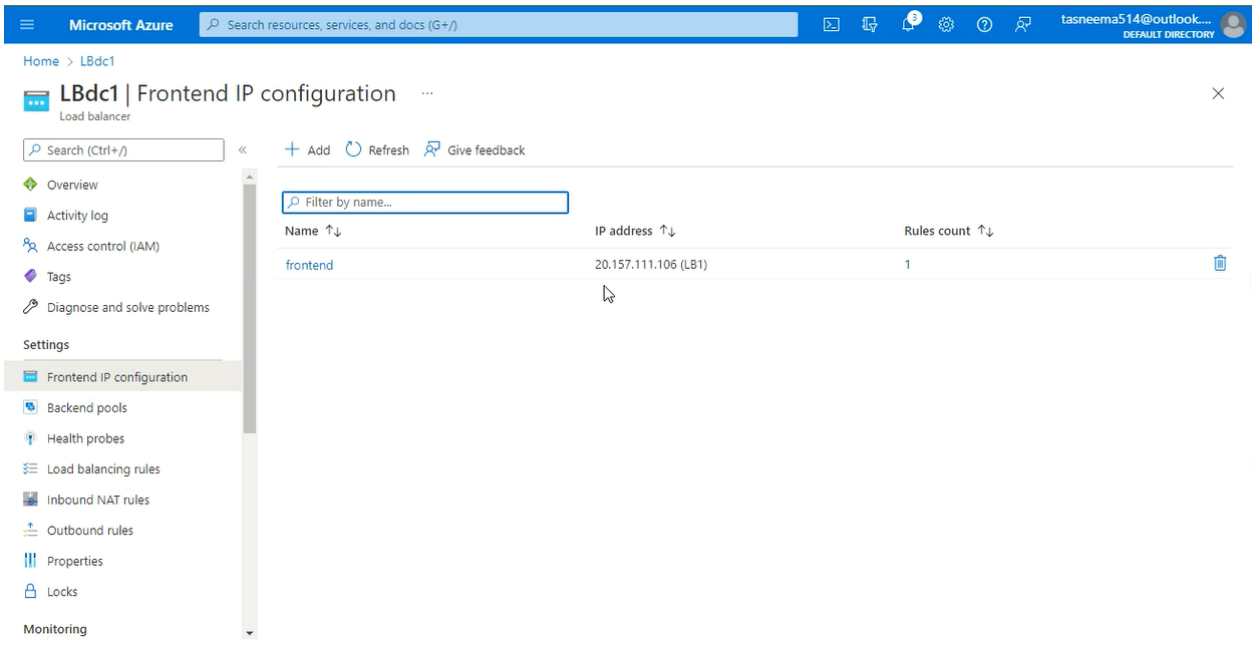

Figure 23

    b. Open the website of the site on the browser through a public address

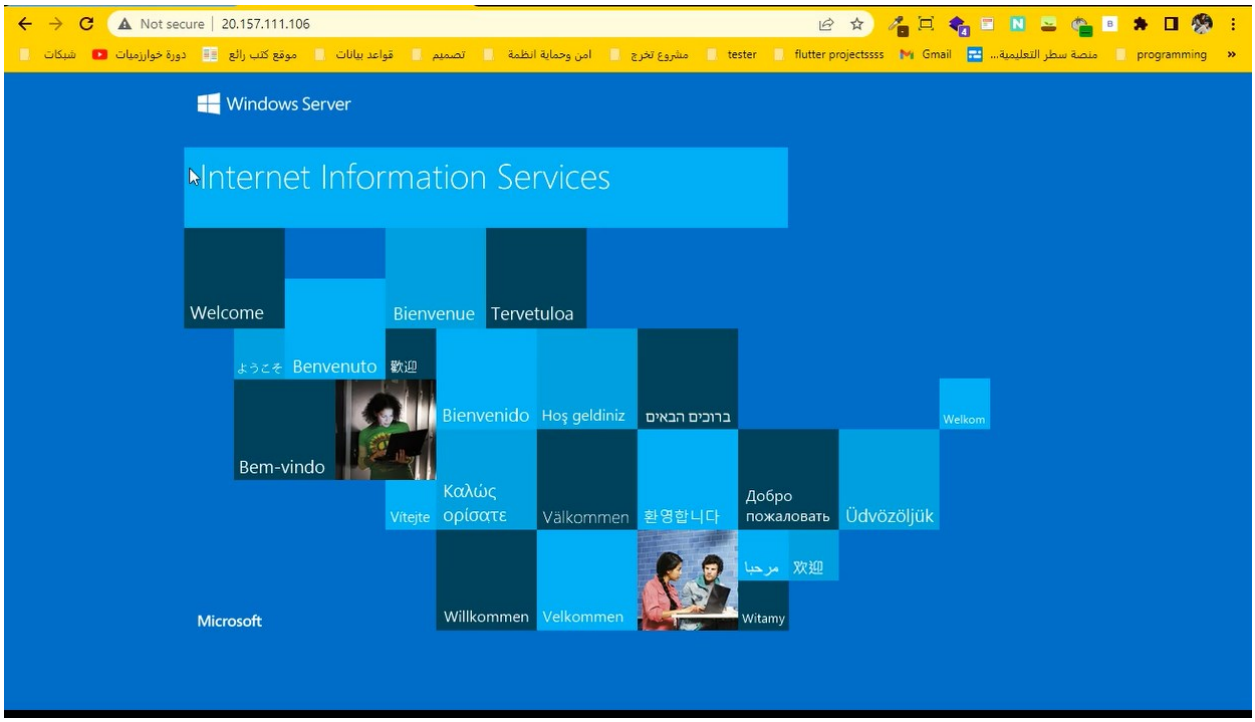

Figure 24

c. The first server providing the service stopped

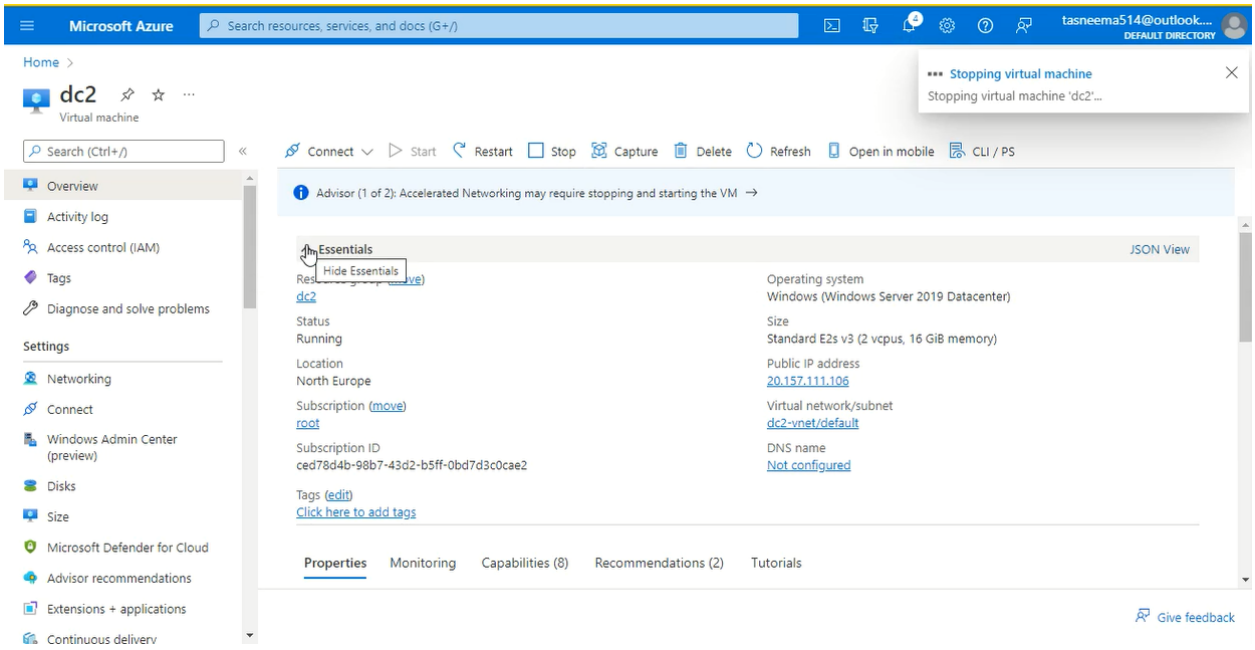

Figure 25

d. Wow, the site is still up and running!

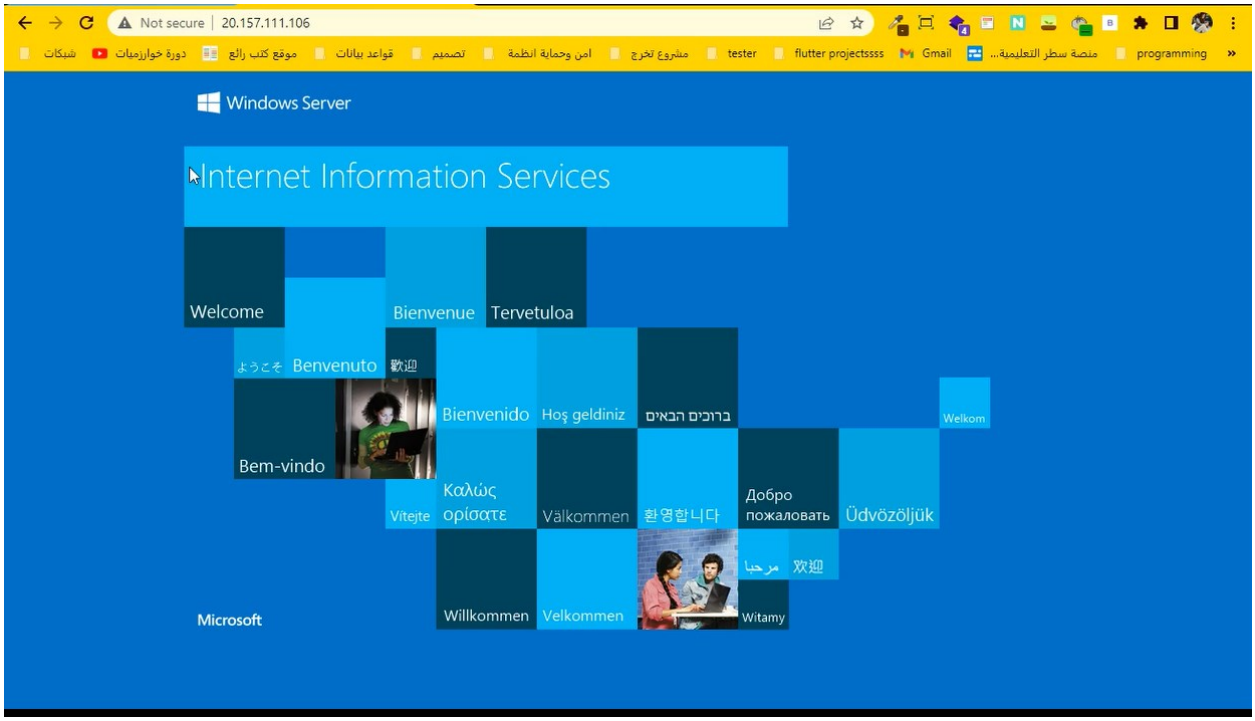

Figure 26

3. Third test result: failover cluster on a file server on the same site

    a) Create an active directory server(node11) and server(node2) and install the file server on nodes

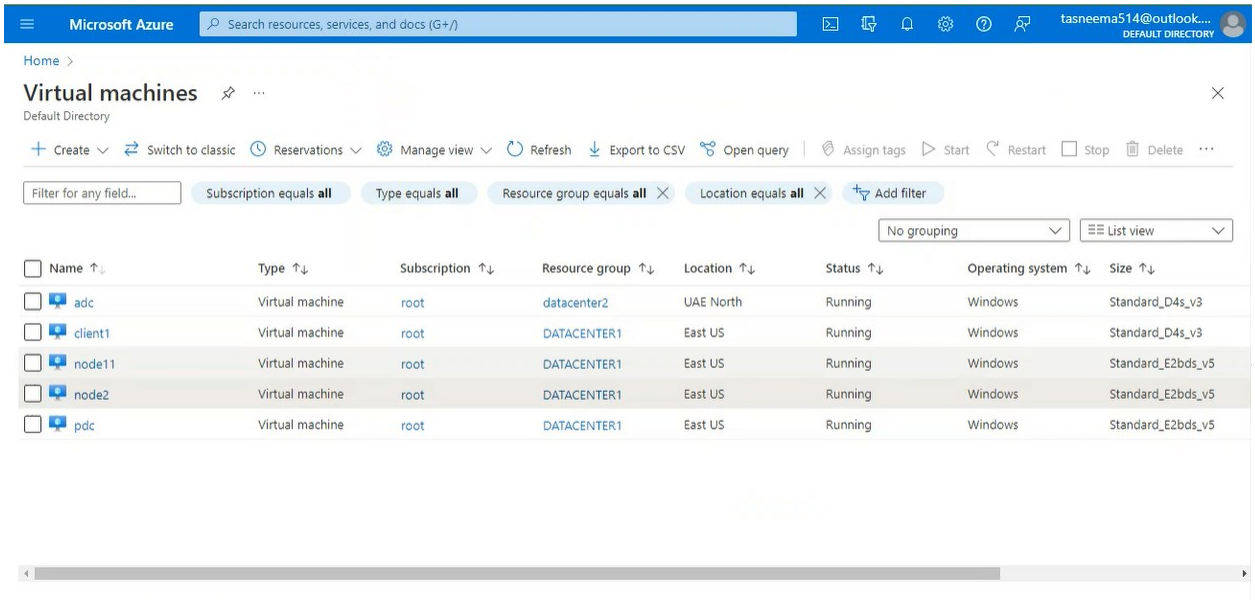

Figure 27

    b) shared storage on node 2 and node 11

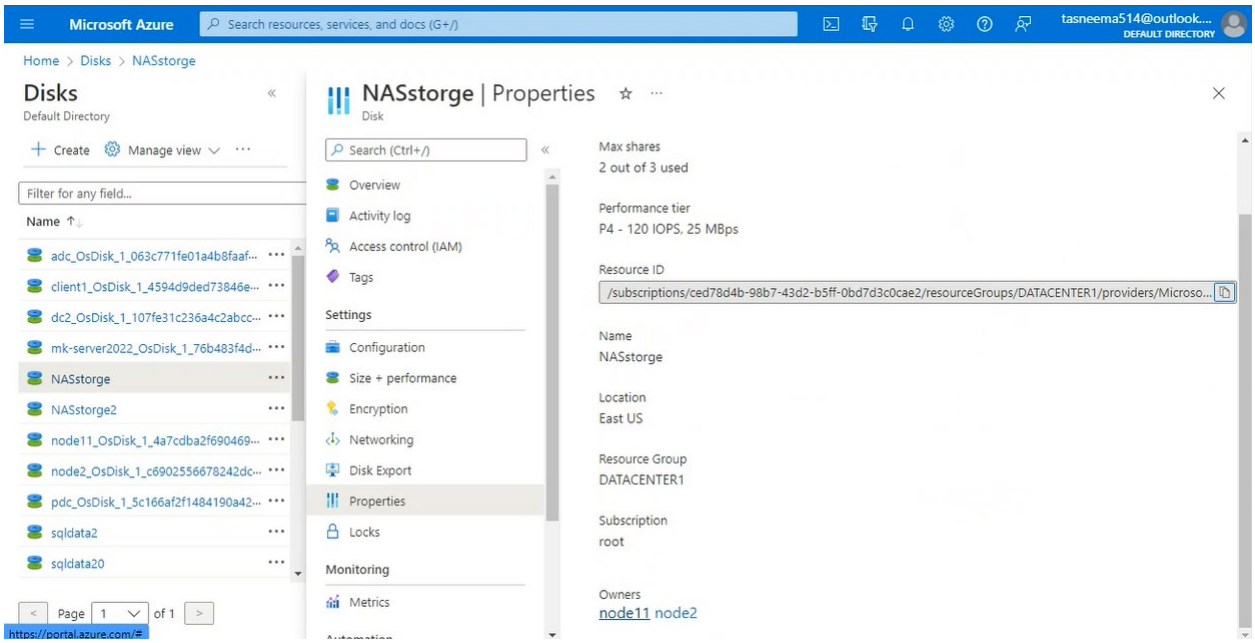

Figure 28

c) Node2 offers a file server service

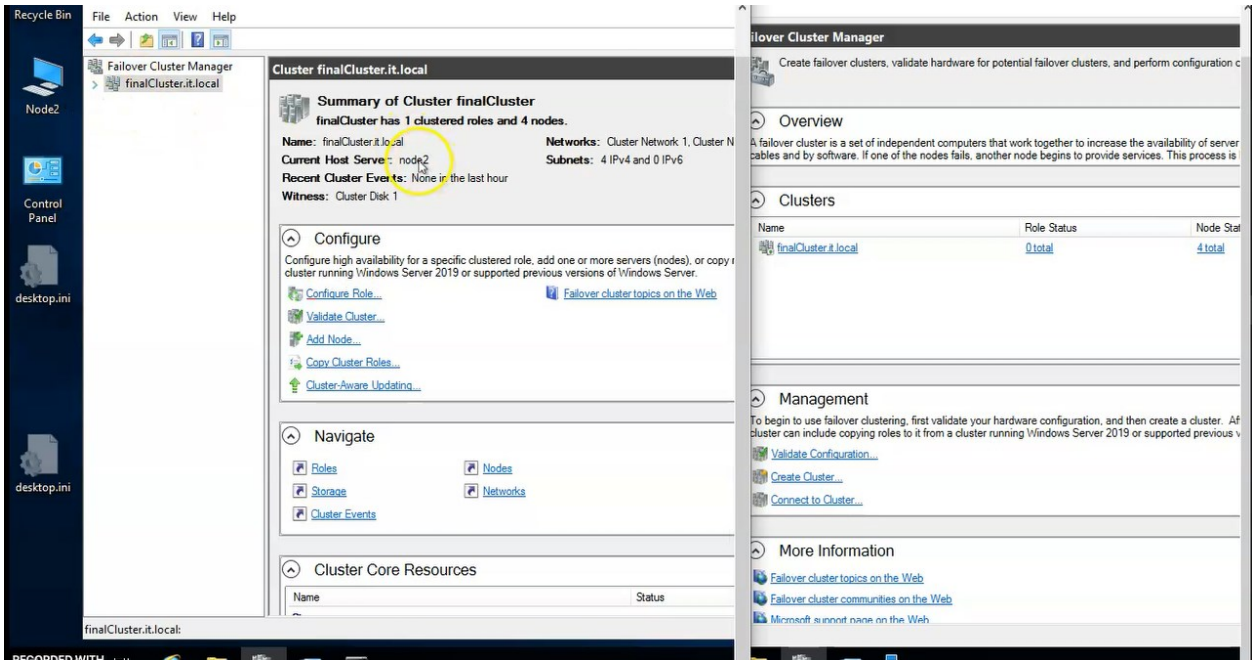

Figure 29

d) All nodes joined in a failover cluster

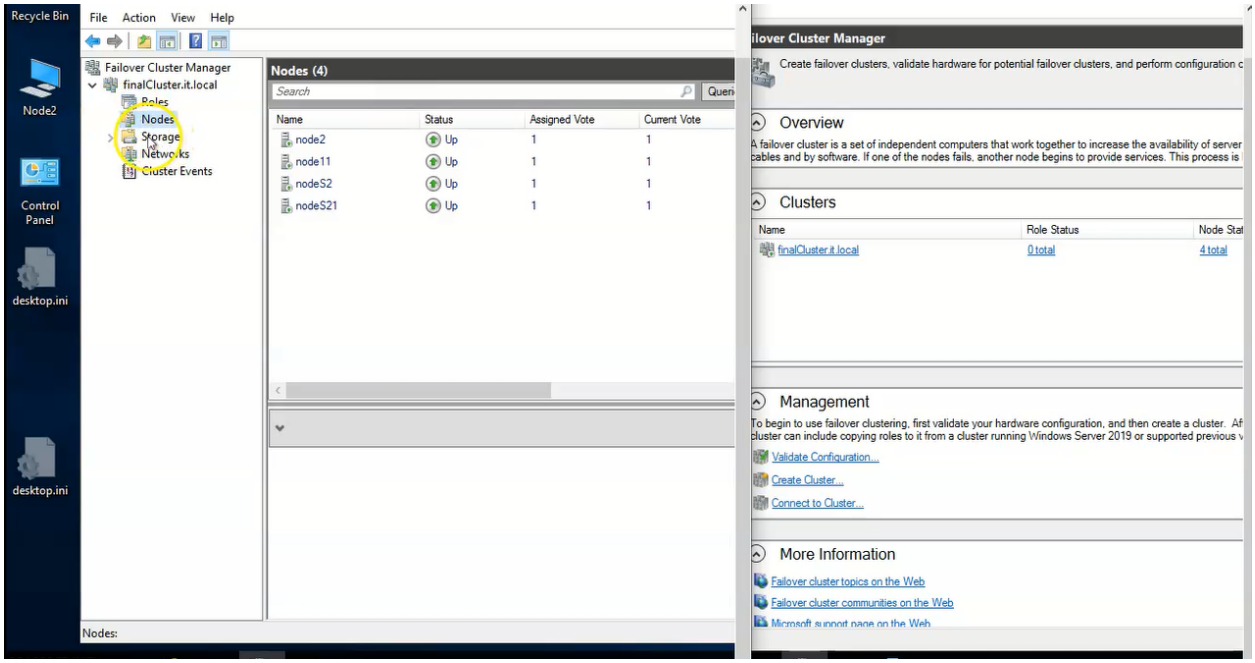

Figure 30

e) Add folder file server on shared storage

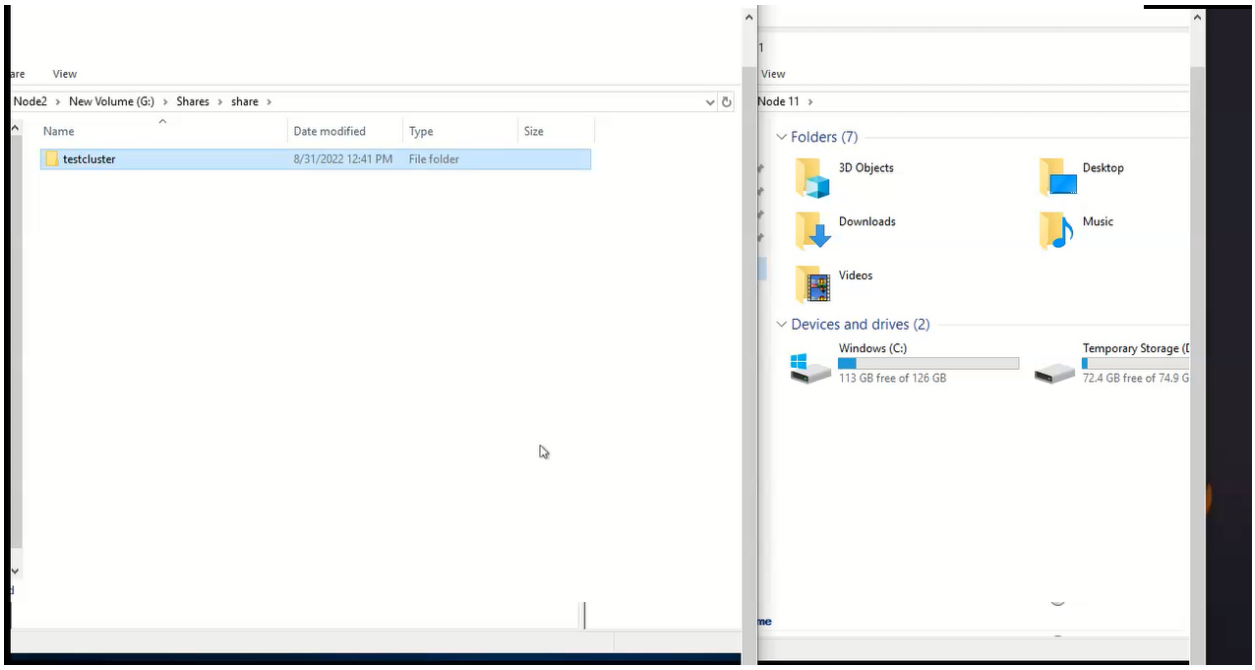

Figure 31

e. stop VM node 2

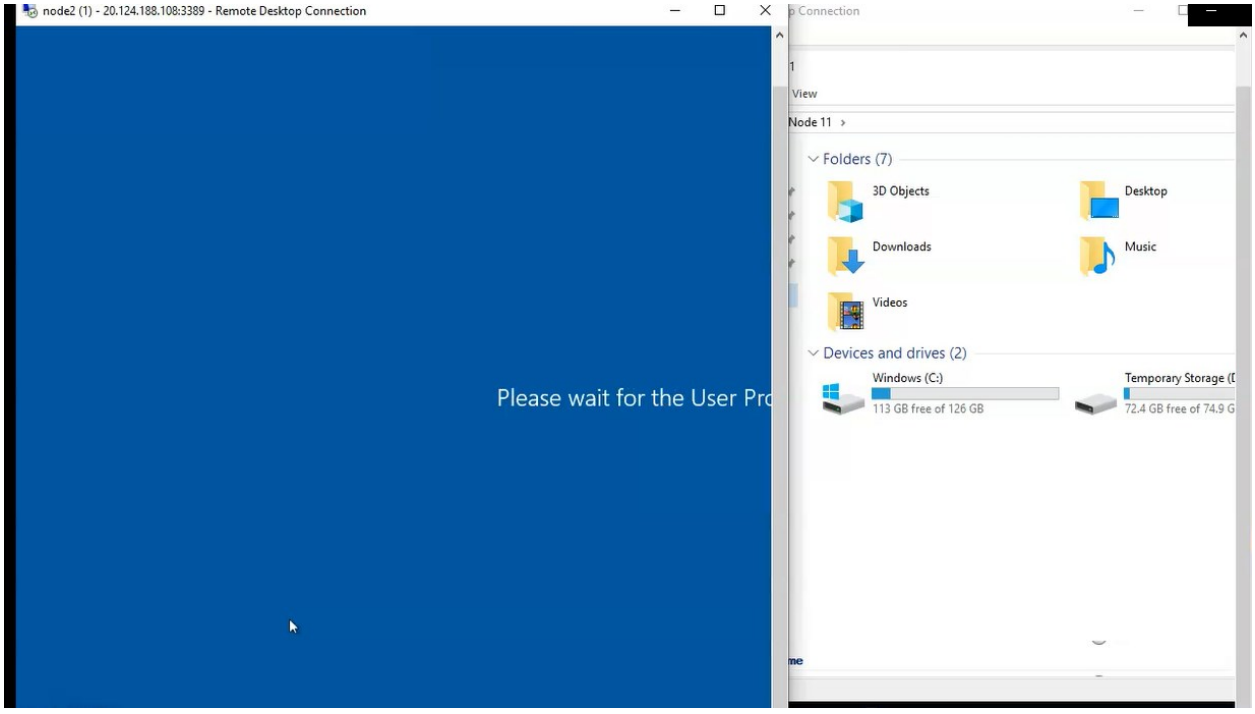

Figure 32

h) failover cluster succeeded in converting traffic to Node11

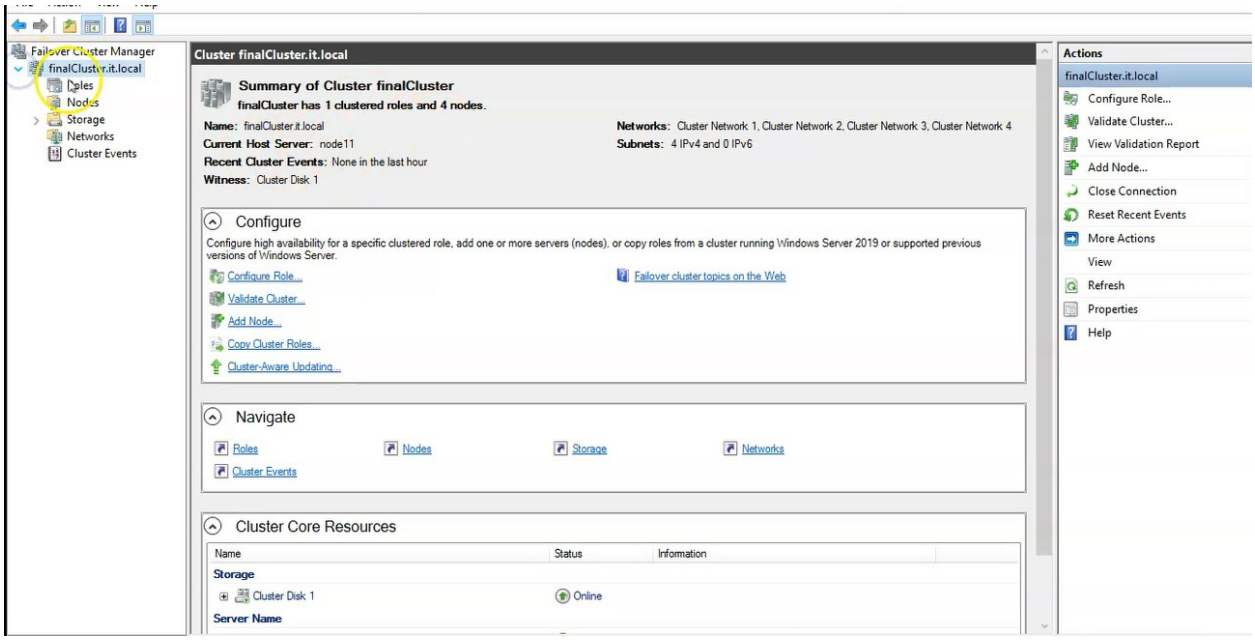

Figure 33

4. structure cluster and storage replica

a) Build disaster recovery site (site1 and disaster recovery)

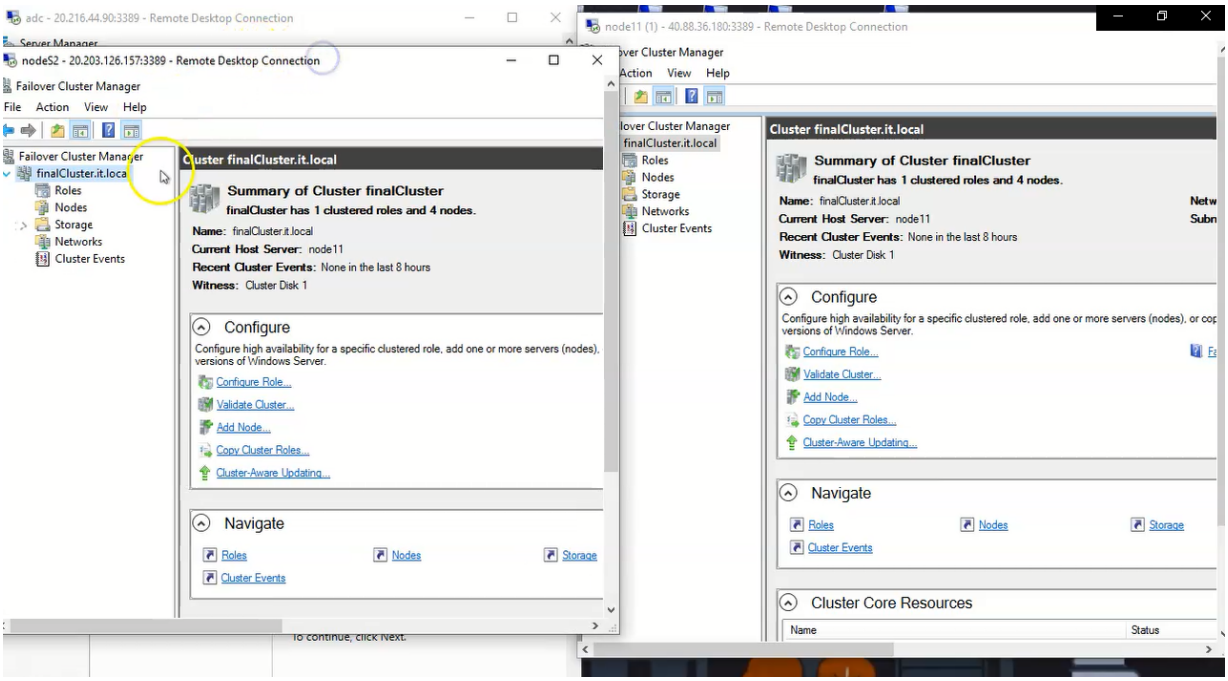

Figure 34

b) Turn off all servers of the first site

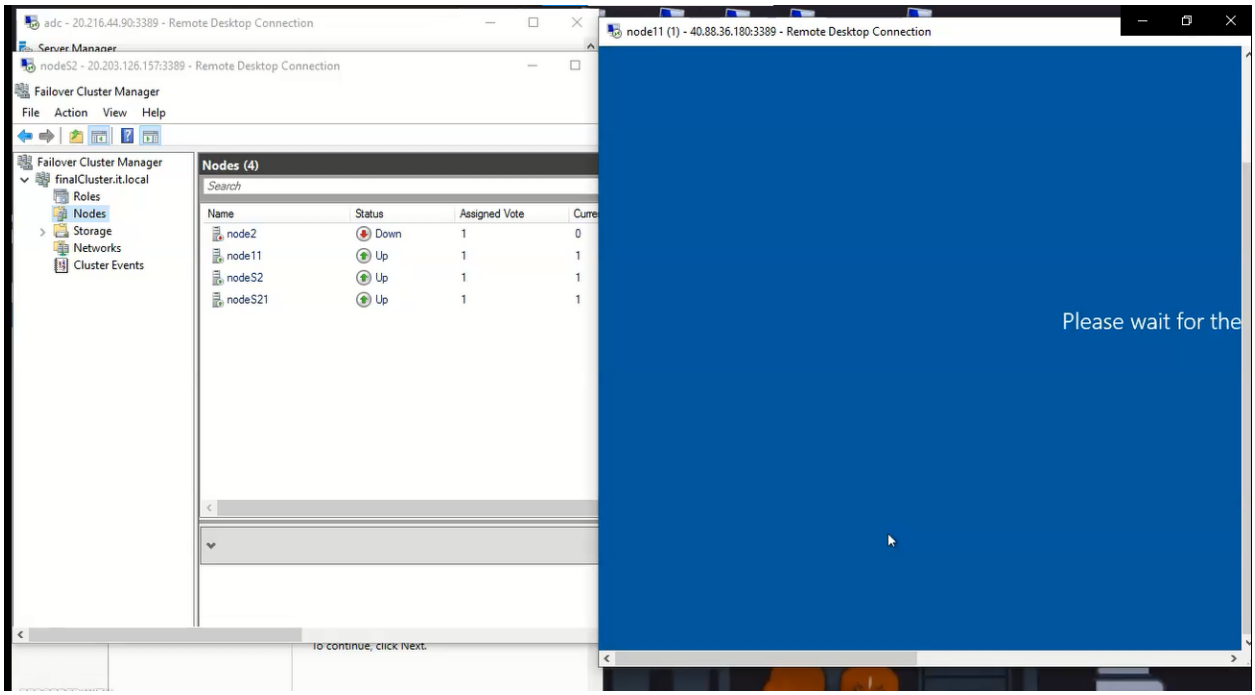

Figure 35

c) hot disaster recovery runs automatically

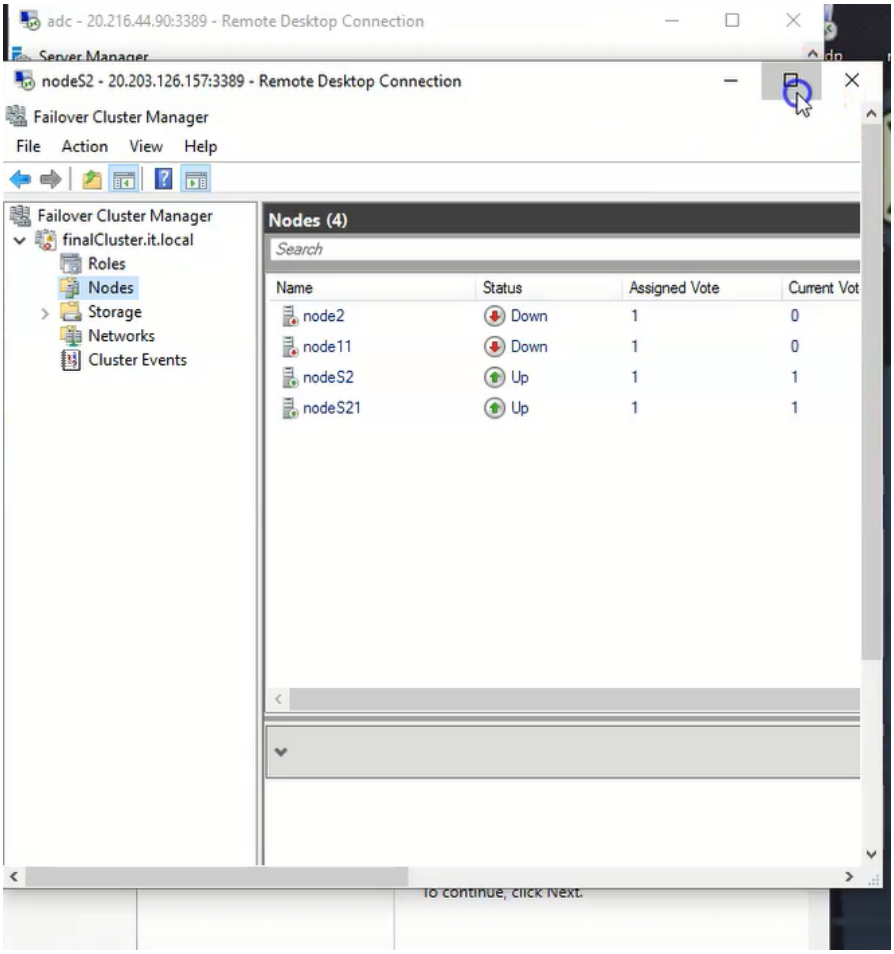

Figure 36

d) The service has been transferred to an automatic disaster recovery server

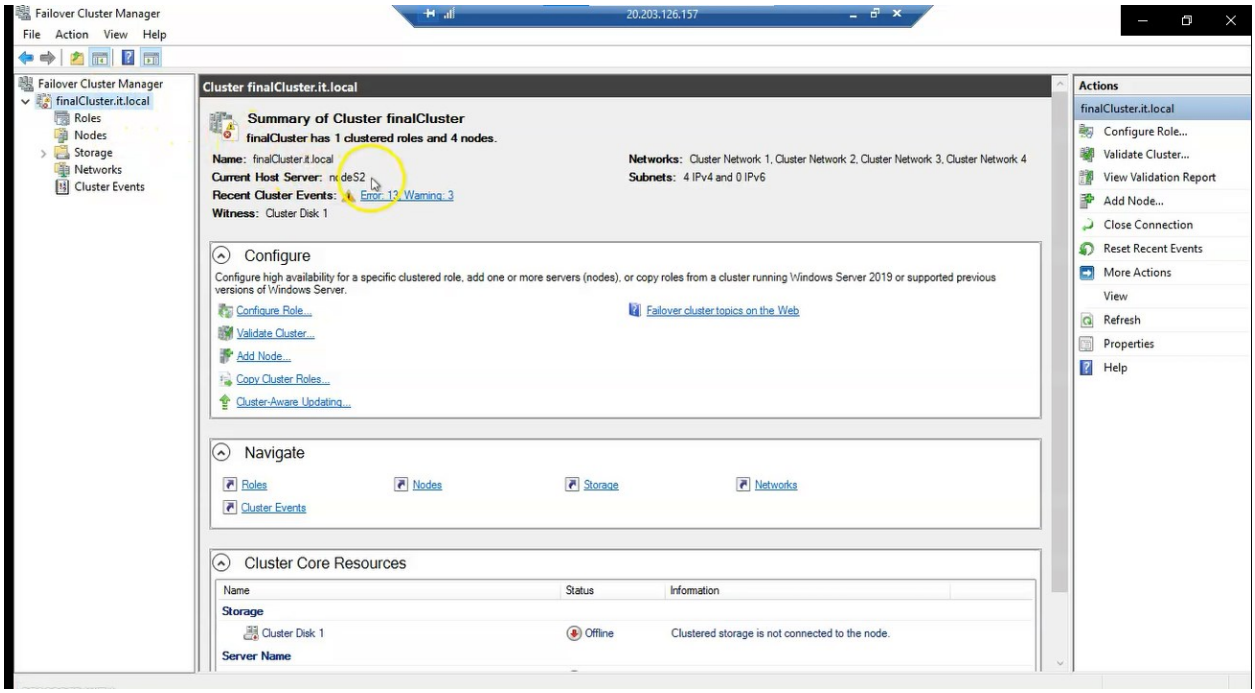

Figure 37

e) A replication test file has been created

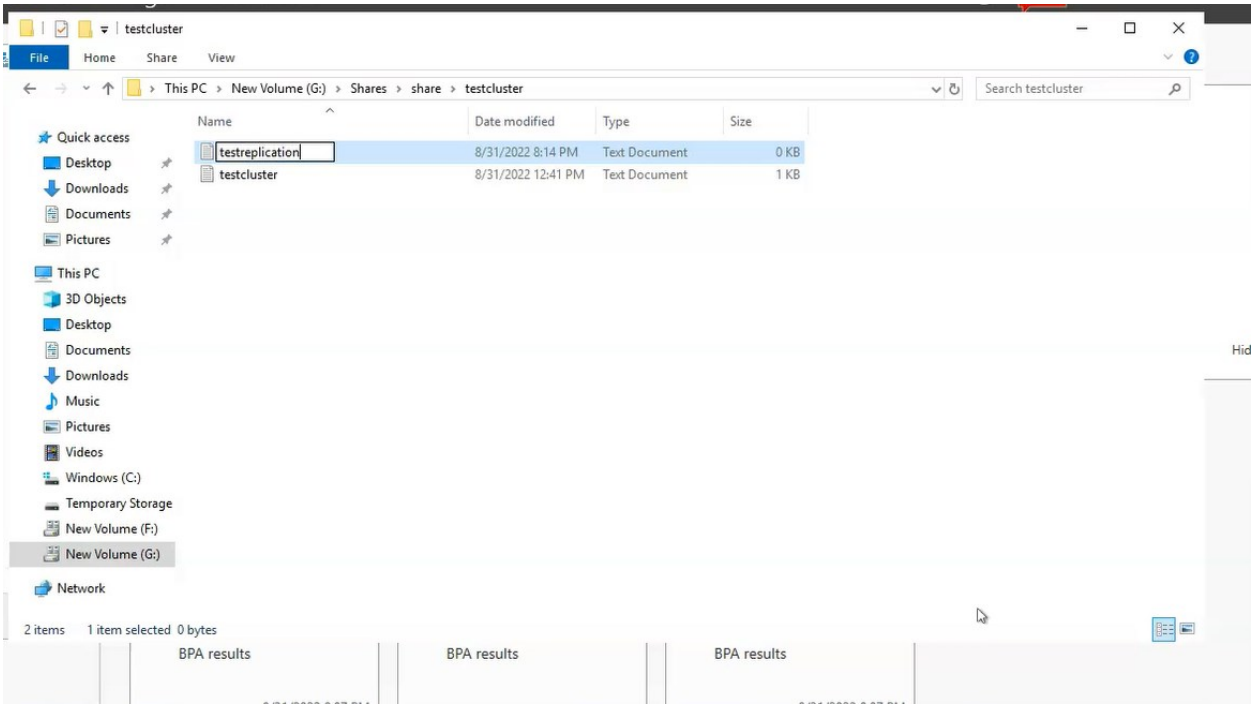

Figure 38

f) The file appeared on the main site storage after restoring the site

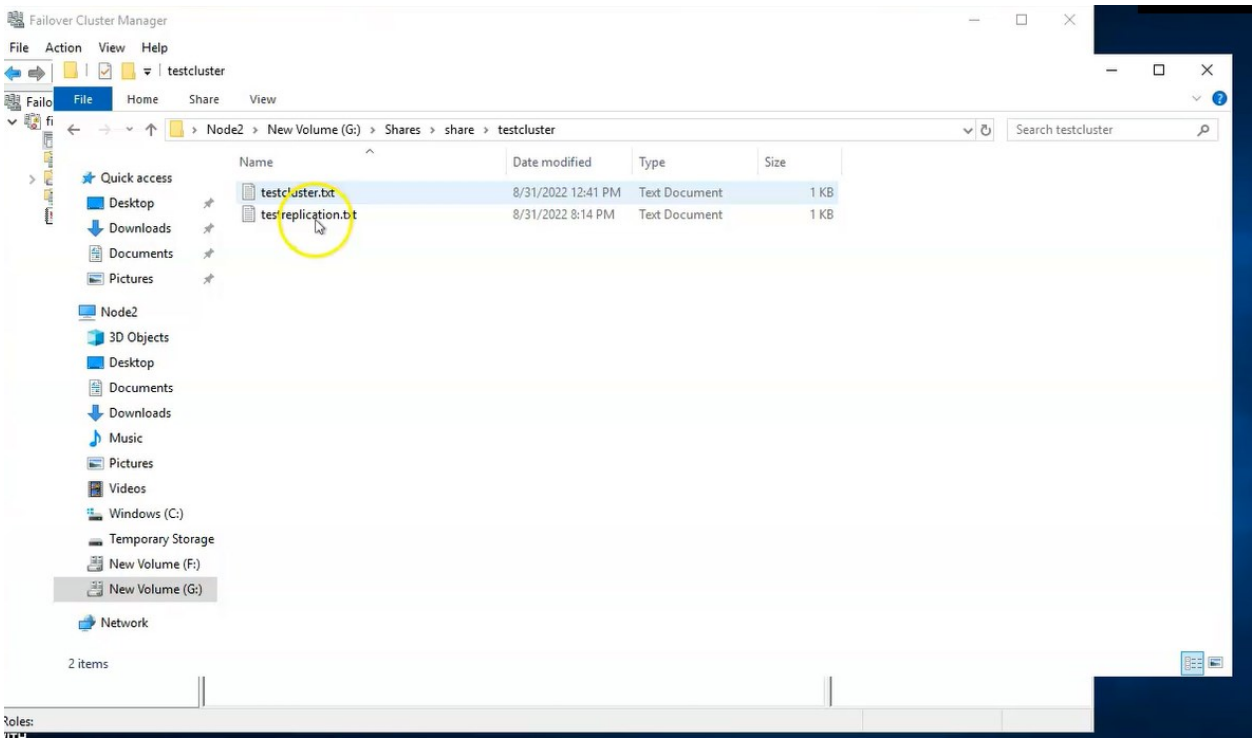

Figure 39

Ch07: Summary and future work

7.1 OVERVIEW

In this chapter, we will have reached the end of writing about our project, and we will make a comprehensive summary of the project and focus on mentioning the future works that we will develop to complete our educational and scientific careers.

7.2 CONCLUSION

In conclusion, the main goal of our project is to facilitate the matter for those in charge of the business in Khan Yunis municipality, to save time and effort, and not to cause financial loss or waste of data. And prepare the municipality in the event of natural disasters or disasters in wars or technical or human errors and planning how to deal with them with the least loss And as soon as possible

Through our project, we reached the following results: Developing the first disaster recovery plan and building a website on the cloud to maintain business continuity in the municipalities and a technological application to maintain the permanent availability of the municipality and reduce downtime and access to no data loss and reduce disaster recovery time through the application of some technology

In the future, we will try hard to develop it and preserve it from the shortcomings, update it according to the capabilities, and develop it as a preventive plan to maintain the continuity of work before it occurs, and we will apply the practical aspect to the real environment of the municipality.

Within our project, there will be a time plan showing what has been achieved, developed, and followed up step by step.

Finally, the writing of the project report was completed and implemented practically, thanks to God and the efforts of our supervisor, and we thank him for his efforts in following up and supervising our project.

7.3 RECOMMENDATIONS

1. Commit to implementing a disaster recovery plan as needed
2. Application of replication to maintain business continuity and not waste data
3. Developing the backup strategy and trying to implement a plan (3-2-1) for the back-up

4. Continuing to develop a disaster recovery plan
5. Write down all the disasters that will occur in the coming period and take the initiative in finding a solution to the problem and write it down in the plan
6. Provide shared storage on the main site
7. Create a plan that includes the financial and operational costs of the data centre

7.4 FUTURE WORKS

1. Improve the level of security in the network.
2. Application of replication to other services such as database service.
3. HA application on vSphere and vCenter.
4. Develop a disaster recovery plan according to site updates.
5. Attempting to connect the on-premise site to the cloud by firewall.
6. Suggesting more effective solutions and applying them to the municipality's environment.
7. Practical application of our final project to the municipal environment.
8. Apply the disaster recovery plan to all sectors in the Gaza Strip.

References

[1] SADOS, “types of disaster recovery plans,” SADOS Team, 13 July 2020. [Online]. Available: https://sados.com/blog/types-of-disaster-recovery-plans/. [Accessed 24 February 2022].

[2] J. Sipple, “5 ELEMENTS OF A DISASTER RECOVERY PLAN – IS YOUR BUSINESS PREPARED?,” MKS&H, 5 Jun 2021. [Online]. Available: https://mksh.com/5-elements-of-a-disaster-recovery-plan-is-your-business-prepared/. [Accessed 5 April 2022].

[3] IBM, “Example: Disaster recovery plan,” IBM, 8 March 2021. [Online]. Available: https://www.ibm.com/docs/en/i/7.1?topic=system-example-disaster-recovery-plan. [Accessed 19 March 2022].

[4] cristie, “The Importance of Replication In Your Disaster Recovery Strategy,” Cristie Software, 8 April 2020. [Online]. Available: https://www.cristie.com/news/the-importance-of-replication-in-your-disaster-recovery-strategy/. [Accessed 18 March 2022].

[5] C. Tozzi, “Data Backup vs. Disaster Recovery: Yes, There’s a Big Difference,” precisely, 9 May 2020. [Online]. Available: https://www.precisely.com/blog/data-availability/data-backup-vs-disaster-recovery. [Accessed 3 May 2022].

[6] JO, “Backup and Disaster Recovery Explained,” colocationamerica, 16 January 2020. [Online]. Available: https://www.colocationamerica.com/blog/data-backup-and-disaster-recovery. [Accessed 14 March 2022].

[7] INAP, “Backups vs. Disaster Recovery: The Ultimate Guide,” INAP THINKIT, 4 JAN 2021. [Online]. Available: https://www.inap.com/blog/backups-vs-disaster-recovery/. [Accessed 2 MAY 2022].

[8] P. Rummery, “Choosing the right disaster recovery for your business,” computerweekly, 10 Feb 2020. [Online]. Available: https://www.computerweekly.com/feature/Choosing-the-right-disaster-recovery-for-your-business. [Accessed 8 April 2022].

[9] P. Crocetti, “The top backup and disaster recovery services of 2020,” techtarget, 14 Feb 2021. [Online]. Available: https://www.techtarget.com/searchdatabackup/feature/The-top-backup-and-disaster-recovery-services-of-2020?_gl=1*1wf8ntl*_ga*NTE4MzcwMjMwLjE2NDE0Njk5NTg.*_ga_TQKE4GS5P9*MTY0MTQ2OTk1NS4xLjEuMTY0MTQ3MDAxMC4w&_ga=2.20172730.308902527.1641469958-518370230.1641. [Accessed 13 Feb 2022].

[10] ICORP, “3 Step Guide to Choosing the Right Disaster Recovery Solution,” ICORPS TECHNOLOGIES, 27 July 2021. [Online]. Available: https://blog.icorps.com/choosing-a-bcdr-solution. [Accessed 15 Feb 2022].

[11] A. Meesum, “How to Choose the Right Backup and Disaster Recovery Plan for Snowflake,” phdata, 1 March 2022. [Online]. Available: https://www.phdata.io/blog/choosing-the-right-snowflake-disaster-and-recovery-plan/. [Accessed 4 May 2022].

[12] J. McGroary , “How to Choose the Right Disaster Recovery Solution for Your Business Needs & Budget,” clearcomit, 6 may 2021. [Online]. Available: https://www.clearcomit.com/how-to-choose-the-right-disaster-recovery-solution-for-your-business-needs-budget/. [Accessed 7 April 2022].

[13] Ali, “How to Manage Data: Disaster Recovery as a Service vs BaaS & IaaS,” cyberfortress, 24 may 2021. [Online]. Available: https://www.offsitedatasync.com/blog/choosing-the-right-service. [Accessed 2 Feb 2022].

[14] A. Marget, “PO and RTO: What Are They and How to Calculate Them,” unitrends, 14 oct 2021. [Online]. Available: https://www.unitrends.com/blog/rpo-rto. [Accessed 15 March 2022].

[15] c. ayuya, “Cloud Disaster Recovery Best Practices,” enterprise storage forum, 4 November 2021. [Online]. Available: https://www.enterprisestorageforum.com/backup/cloud-disaster-recovery-best-practices/. [Accessed 29 march 2022].

[16] D. robb, “Best Enterprise Backup Software & Solutions 2022,” enterprise storage forum, 9 april 2021. [Online]. Available: https://www.enterprisestorageforum.com/products/best-enterprise-backup-solutions/. [Accessed 18 feb 2022].

[17] EES, “Cloud Disaster Recovery Best Practices,” eescorporation, 30 Dec 2021. [Online]. Available: https://www.eescorporation.com/cloud-disaster-recovery-best-practices/#. [Accessed 31 Jan 2022].

[18] Sangay, “Cloud Computing Disaster Recovery DR Dr Sanjay P,” slidetodoc, 14 Aug 2010. [Online]. Available: https://slidetodoc.com/cloud-computing-disaster-recovery-dr-dr-sanjay-p/. [Accessed 7 may 2022].

[19] B. Martin, “Disaster Recovery Plan Strategies and Processes,” sans, 5 March 2002. [Online]. Available: https://www.sans.org/white-papers/564/. [Accessed 17 March 2022].

[20] veeam, “Veeam: How to design and implement a policy-based SLA backup system – Part V – Monitoring the Veeam Backup & Replication environment with Veeam ONE,”

jorgedelacruz.uk, 13 March 2020. [Online]. Available: https://jorgedelacruz.uk/2020/03/13/veeam-how-to-design-and-implement-a-policy-based-sla-backup-system-part-v-monitoring-the-veeam-backup-replication-environment-with-veeam-one/. [Accessed 15 march 2022].

[21] C. Pietschmann, "Properly Shutdown Azure VM to Save Money," build5nines, 27 March 2020. [Online]. Available: https://build5nines.com/properly-shutdown-azure-vm-to-save-money/. [Accessed 11 April 2022].

[22] microsoft, "About Site Recovery," 14 Jun 2020. [Online]. Available: https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-overview. [Accessed 2 july 2022].

[23] A. Learn, "Understanding Azure Pricing Calculator in less than 10 minutes," Azure Learn, 10 March 2020. [Online]. Available: https://www.youtube.com/watch?v=ho9LJf_M_II. [Accessed 30 May 2022].

[24] U. Inc., "Changed Block Tracking (CBT) & Data Recovery: What You Need to Know," Unitrends Inc., 19 Feb 2016. [Online]. Available: https://www.youtube.com/watch?v=md5nTJUY5rA. [Accessed 22 May 2022].

[25] Azure, "Cost recommendations," 28 June 2022. [Online]. Available: https://docs.microsoft.com/en-us/azure/advisor/advisor-reference-cost-recommendations. [Accessed 30 June 2022].

[26] azure, "Availability options for Azure Virtual Machines," 19 Oct 2021. [Online]. Available: https://docs.microsoft.com/en-us/azure/virtual-machines/availability. [Accessed 25 June 2022].

[27] azure, "Domain Name System (DNS)," 11 Janu 2022. [Online]. Available: https://docs.microsoft.com/en-us/windows-server/networking/dns/dns-top. [Accessed 24 june 2022].

[28] S. Kuehn, "Video 4 of the Azure VMware Solution Zero to Hero Series!," 11 Nov 2021. [Online]. Available: https://techcommunity.microsoft.com/t5/itops-talk-blog/video-4-of-the-azure-vmware-solution-zero-to-hero-series/ba-p/2928613. [Accessed 25 July 2022].

[29] UNDP, "Disaster Recovery Plan," 10 DEC 2021. [Online]. Available: https://popp.undp.org/_layouts/15/WopiFrame.aspx?sourcedoc=/UNDP_POPP_DOCUMENT_LIBRARY/Public/ICT_Business%20Continuity%20Management_Template%20Annex%207%20

-
%20ICT%20Disaster%20Recovery%20Plan.docx&action=default&utm_source=EN&utm_medium=GSR&utm_content=U. [Accessed 18 MAY 2022].

[30] TEMPLAET, "DISASTER RECOVERY PLAN TEMPLATE," 1 MARCH 2020. [Online]. Available: https://www.disasterrecoveryplantemplate.org/download/disaster-recovery-plan-template-basic/. [Accessed 16 MAY 2022].

[31] "Disaster Recovery Plan Template," 1 APRIL 2019. [Online]. Available: https://www.disasterrecoveryplantemplate.org/. [Accessed 16 MAY 2022].

[32] I. Disaster, "IT Disaster Recovery Planning: A Template," 2 APRIL 2019. [Online]. Available: https://www.microfocus.com/media/unspecified/disaster_recovery_planning_template_revised.pdf. [Accessed 27 MAY 2022].

[33] T. Hanna, "The 11 Best Free Disaster Recovery Plan Templates Online," 1 JUNE 2022. [Online]. Available: https://solutionsreview.com/backup-disaster-recovery/the-best-free-disaster-recovery-plan-templates-online/. [Accessed 29 MAY 2022].

[34] "vSphere vMotion," vmware, [Online]. Available: https://www.vmware.com/products/vsphere/vmotion.html. [Accessed 11 Sep 2022].

[35] B. Lee, "VMware vMotion vs Storage vMotion," vembu, 9 May 2018. [Online]. Available: https://www.vembu.com/blog/vmware-vmotion-vs-storage-vmotion/. [Accessed 9 Sep 2022].

[36] C. BasuMallick, "AWS vs. Azure: Understanding the Key Differences," spiceworks, 28 April 2022. [Online]. Available: https://www.spiceworks.com/tech/cloud/articles/aws-vs-azure/. [Accessed 29 Aug 2022].

[37] "amazons aws vs microsofts azure areversal of roles coming soon," seekingalpha Amazons, 26 Aug 2014. [Online]. Available: https://seekingalpha.com/article/2452995-amazons-aws-vs-microsofts-azure-a-reversal-of-roles-coming-soon?source=acquisition_campaign_google&utm_source=google&utm_medium=cpc&utm_campaign=14823831578&utm_term=128719140158^dsa-1427141793820^^549166468495^^^g. [Accessed 8 Sep 2022].

[38] J. Welch, "The 5 Phases of Waterfall Project Management," profit, [Online]. Available: https://www.profit.co/blog/task-management/the-5-phases-of-waterfall-project-management/. [Accessed 7 Sep 2022].

[39] K. R. S. K. Sharma, “ONLINE DATA BACKUP AND DISASTER RECOVERY TECHNIQUES IN CLOUD COMPUTING:,” semanticscholar, 2012. [Online]. Available: https://www.semanticscholar.org/paper/Online-Data-Back-up-and-Disaster-Recovery-in-Cloud-Sharma-Singh/35b3cf66df5322d9b9d5739e133c49de5026451b. [Accessed 25 Aug 2022].

[40] S. Sivankalai, “DISASTER RECOVERY SYSTEM AND SERVICE CONTINUITY OF DIGITAL LIBRARY,” Hindustan University, Nov 2021. [Online]. Available: https://www.researchgate.net/publication/357174336_Disaster_Recovery_System_and_Service_Continuity_of_Digital_Library. [Accessed 23 Aug 2022].

[41] S. Zavala , N. Shashidhar , C. Varol and B. Zhou , “Disaster Recovery Management with PowerShell PSDRM,” 4 Jun 2022. [Online]. Available: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1022&context=sais2022. [Accessed 20 Aug 2022].

[42] B. Lutkevich, “high availability (HA),” techtarget, [Online]. Available: https://www.techtarget.com/searchdatacenter/definition/high-availability. [Accessed 2022].

[43] J. Noonan, “High Availability Architecture Demystified,” redis, 1 July 2022. [Online]. Available: https://redis.com/blog/high-availability-architecture/. [Accessed 15 Aug 2022].

[44] “High availability,” wikipedia, [Online]. Available: https://en.wikipedia.org/wiki/High_availability. [Accessed 10 Aug 2022].

[45] “What is an SLA? Best practices for service-level agreements,” [Online]. Available: https://www.cio.com/article/274740/outsourcing-sla-definitions-and-solutions.html. [Accessed 7 Aug 2022].

[46] “Best practices for high availability,” redis, [Online]. Available: https://redis.com/blog/high-availability-architecture/.