IT INFRASTRUCTURE RECOVERY STRATEGIES

Flamur Gogolli
IT INFRASTRUCTURE RECOVERY STRATEGIES

Bachelor Degree

Flamur Gogolli

October / 2012
Pristine
University for Business and Technology
Faculty of Computer Science and Engineering

Bachelor Thesis
Academic Year 2011 - 2012

Student: Flamur Gogolli

IT INFRASTRUCTURE RECOVERY STRATEGIES

Supervisor: Dr. Edmond Hajrizi

October / 2012

This thesis is submitted in partial fulfillment of the requirements for a Bachelor Degree
ABSTRACT

By taking into consideration the importance of IT services and servers in everyday business processes, the availability of these services is crucial for the functionality of the business. Given the importance that today’s technology gives to the IT, the uptime of these services can be translated to the “uptime of the business”. Thus, a Recovery Strategy of IT Services is highly crucial for an IT Departments everyday operations, as disasters are naturally unpredictable and unavoidable.

This thesis as the title states will produce and explain a practical approach to a Recovery Strategy for an IT Infrastructure by using a case study of two imaginary companies. The proposed infrastructures were taken as an example of infrastructures of similar size companies, and as such the developed Recovery Strategies can be applied to those companies as well. The scope of this thesis will be to restore the services, systems and sites in case of a failure in one of these levels. All of these failures will be summarized using the term disaster. This thesis will not be discussing or studying the network architecture recovery or the inter-connections required between the main site and the disaster recovery site.

In order to have a functional disaster recovery, the first and crucial building block is having a backup of the company data. As such, we will create a fully functional and dependable Backup Strategy for these imaginary companies. Additionally, duplicates of company data will be saved in the Disaster Recovery Site to enable restore of data, upon total loss of the main site, as well as in the second case, a duplicate will be made in an online storage space provider.

Additionally, to decrease the possible downtime in case of a failure, we will give an implementation plan for high-availability solutions for all of the high priority services offered in the first case study’s infrastructure, such as: domain authentication services, email services, file sharing services and databases. The second company will outsource their important services online.

Last but not least, a written Recovery Strategy should be compiled that will serve as a walkthrough guide in case such a disaster occurs. We will be giving a flowchart description of these steps for the first case study, but a full document stating a tested and verified version of all these steps should be written by the IT Departments of both companies.

Finally, as a wrap up to this thesis, we will give a summary of all the points discussed throughout this document with a final conclusion of the possible IT Recovery Strategies.
ACKNOWLEDGMENT

I started my Undergraduate Studies in the University of Pristina, Faculty of Electrical and Computer Engineering, in the Department of Computer Engineering. At the beginning of the second semester, I also started working as an IT Officer in the Ombudsperson Institution in Kosovo. After working there for 4 years and almost finishing my Bachelor Studies, on 2006, I changed jobs and got accepted in the Systems Administrator position in the Post and Telecommunications of Kosovo, one of the biggest companies in country.

Because of starting my new job and a number of other reasons I was not as active in my studies as I should have been, and this lack of activity went on for another 5 years, until the September of 2011, when I decided to transfer my studies to the University for Business and Technology (UBT), Department of Computer Science and Engineering. After an evaluation of my application, I was transferred to be a new student, with 13 more exams until earning my Bachelor’s Degree. I would like to take this opportunity to acknowledge and thank all of the UBT Staff starting from the Rector himself, who was also one of my Professors, and continuing with all the Lecturers, Assistants and the rest of the staff for providing such a professional and educational environment enabling students to grow both academically and professionally through their studies.

This thesis would not be possible without the help of my supervisor, Dr. Edmond Hajrizi, to whom I owe great gratitude and thankfulness. He has always been friendly, helpful and ready to contribute his time and knowledge in helping me create a professional thesis similar to other top level university papers.

Last but not least, I would like to thank my family for supporting me and my desire to work in the IT field since my childhood, without the help of who I would have not been who and what I am today.
CONTENTS

List of Figures ......................................................................................................................... v
List of Tables ............................................................................................................................ v
Glossary of Terms .................................................................................................................. vi
1 Introduction ......................................................................................................................... 1
2 Literature Review ............................................................................................................... 6
3 Problem Statement ............................................................................................................. 7
4 Methodology ....................................................................................................................... 8
5 Case Study A - KIT ............................................................................................................... 9
   5.1 KIT Backup Strategy .................................................................................................... 11
      5.1.1 Windows Server Backup ...................................................................................... 11
      5.1.2 Symantec BackupExec ....................................................................................... 12
   5.2 KIT Disaster Recovery Site Configurations ................................................................. 15
      5.2.1 Windows Server Backup and Symantec Backup Exec in DRS ....................... 16
      5.2.2 Domain Controller in DRS ................................................................................ 17
      5.2.3 Microsoft Exchange in DRS ............................................................................... 17
      5.2.4 File Server in DRS ............................................................................................. 19
      5.2.5 Database Server in DRS .................................................................................... 20
      5.2.6 Standby Server for Virtualization in DRS ........................................................... 21
      5.2.7 High Availability of Services ............................................................................. 22
      5.2.8 The final KIT IT Infrastructure ........................................................................... 23
   5.3 KIT Recovery Strategy ................................................................................................. 25
6 Case Study B – CBT .......................................................................................................... 27
   6.1 CBT Backup Strategy ................................................................................................. 28
   6.2 CBT Disaster Recovery Configuration ......................................................................... 29
   6.3 Using Online Services for CBT Infrastructure .......................................................... 29
      6.3.1 Email Services Online ......................................................................................... 30
      6.3.2 Web Application Server Online .......................................................................... 30
      6.3.3 Space Storage Online ......................................................................................... 30
6.4 The final CBT IT Infrastructure ................................................................. 31
6.5 CBT Recovery Strategy ........................................................................... 32
7 Analysis and Comparison of Case Studies ............................................... 34
8 Discussions and Conclusion ................................................................... 35
9 Appendix A ............................................................................................... 36
10 References ............................................................................................... 37
LIST OF FIGURES

Figure 1 KIT Server and Network Infrastructure at HQ Site ......................................................... 9
Figure 2 Windows Server Backup Procedure for KIT Server .......................................................... 12
Figure 3 Symantec BackupExec Configuration for KIT Servers ..................................................... 13
Figure 4 Windows Server Backup and Symantec BackupExec in HQS and DRS ...................... 16
Figure 5 KIT Exchange Front-End and Back-End Configuration ..................................................... 19
Figure 6 KIT Distributed File Service Configuration ................................................................. 20
Figure 7 SQL Failover Active/Passive Cluster Configuration ......................................................... 21
Figure 8 KIT IT Final Infrastructure (HQS & DRS) .......................................................................... 23
Figure 9 CBT IT Infrastructure ...................................................................................................... 27
Figure 10 Final CBT IT Infrastructure .......................................................................................... 31

LIST OF TABLES

Table 1 KIT Infrastructure Equipment Roles and Descriptions ..................................................... 9
Table 2 Windows Server Backup Locations and Schedule ............................................................. 12
Table 3 Symantec Backup Exec Configuration for KIT Servers ..................................................... 14
Table 4 Final KIT IT Equipment Role & Description List ............................................................... 24
Table 5 CBT IT Infrastructure Roles & Descriptions ..................................................................... 28
Table 6 Final CBT IT Infrastructure .............................................................................................. 32
<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active/Passive Cluster</td>
<td>A Windows Cluster Service with ONLY one active and one or more passive nodes, of which at one certain time only one can be active at all times.</td>
</tr>
<tr>
<td>Append</td>
<td>Ability to add data to an existing file, folder or tape.</td>
</tr>
<tr>
<td>Backup Set</td>
<td>A set of backup files, disks or tapes that altogether form a consistent backup of a certain resource's data.</td>
</tr>
<tr>
<td>Client Access Server Role</td>
<td>A role within Exchange Server that enables users to access their mailboxes through Outlook Web App/ Outlook Web Access as well as mail clients like Microsoft Outlook.</td>
</tr>
<tr>
<td>Differential Backup</td>
<td>A backup method that makes a copy of all the files and folders that are selected within a resource since the last Full Backup.</td>
</tr>
<tr>
<td>Disaster</td>
<td>Failure of a service, server or site caused by unpreventable and unpredictable reasons.</td>
</tr>
<tr>
<td>Disaster Recovery Site</td>
<td>A company site, which holds some or all of the needed hardware and software to replace the main site in case of a failure.</td>
</tr>
<tr>
<td>Domain Controller</td>
<td>Server hosting the Domain Services used for authenticating users.</td>
</tr>
<tr>
<td>Downtime</td>
<td>Time for which a service or server has been down and not offering services.</td>
</tr>
<tr>
<td>Failback</td>
<td>The ability to restore the responsibility of active node to the node that has previously failed in the event that node is back online.</td>
</tr>
<tr>
<td>Failover</td>
<td>The ability to shift the responsibility of active node to a passive node in the event of a failure of the current active node.</td>
</tr>
<tr>
<td>Full Backup</td>
<td>A backup method that makes a copy of all the files and folders that are selected within a resource.</td>
</tr>
<tr>
<td>High Availability</td>
<td>An implementation of a service or a system which can survive the failure of one or more nodes and continue serving its end-users by passing the responsibilities to other nodes in the group.</td>
</tr>
<tr>
<td>Hub Transport Role</td>
<td>A role within Exchange Server that handles the sending and receiving of emails between users and between our domain and other domains.</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Incremental Backup</td>
<td>A backup method that makes a copy of all the files and folders that are selected within a resource since the last Full or Incremental Backup, whichever was done last.</td>
</tr>
<tr>
<td>Instance</td>
<td>A working online copy of a resource, e.g. database, IP address, domain name and such other resources.</td>
</tr>
<tr>
<td>Mailbox Role</td>
<td>A role within Exchange Server which saves the Exchange Information Store - the database that Exchange uses to store user mailboxes and emails.</td>
</tr>
<tr>
<td>Network Load Balancing</td>
<td>A feature within Windows that represents more than one physical machine with one single IP address and domain name, thus balancing the network and service load of user requests between those two or more servers.</td>
</tr>
<tr>
<td>Overwrite</td>
<td>The ability to replace an existing file with the same name and path with another file.</td>
</tr>
<tr>
<td>Recovery</td>
<td>Ability to restore a service or server to a fully functional state.</td>
</tr>
<tr>
<td>Redundancy</td>
<td>Possibility of having dual copies of hardware or software parts of a system, to avoid single points of failure.</td>
</tr>
<tr>
<td>Service</td>
<td>A software or a group of softwares that offer a certain service to the end-user.</td>
</tr>
<tr>
<td>Single Point of Failure</td>
<td>A hardware, software or physical location which has the only copy of a working part of the Infrastructure and the failure of which part causes the failure of the whole service, server or site.</td>
</tr>
<tr>
<td>Site</td>
<td>A physical location with all the standard hardware and software requirements to enable a full functioning of an IT Infrastructure.</td>
</tr>
<tr>
<td>System</td>
<td>A server or a group of hardware equipment that enable the functionality of a service.</td>
</tr>
<tr>
<td>Uptime</td>
<td>Time for which a service or server has been up and running.</td>
</tr>
</tbody>
</table>
1 INTRODUCTION

For many years now, Information Technology has been one of the biggest enablers for businesses and the services they offer. Almost everything that businesses do, no matter the department, country or line of business they are in, in some or more often most of their processes are dependant of some kind of IT Technology, be it a phone, laptop, computer, server, network, desktop or web application, email or other types of technology like production robotics. As such, the availability of these technologies directly means the availability of business processes, which in the end offer the business services. Thus, in case those technologies are unavailable, so will the business services. And if a business can’t offer services then it means it can’t make money, which is a direct contradiction with the concept of business.

Because the IT Technology has a very wide range of products and technologies, and since this thesis should rather be concentrated on a specific topic, in this document we will only be discussing the Recovery Strategies for IT Servers and Services offered by them as well as the hardware directly connected to the functionality of these services. This thesis will not be discussing or taking into consideration the recovery strategies for Network Connections between different servers or server sites and their interconnectivity with client computers. It will be assumed that these strategies are or will already be in place and will provide all the necessary ground required to build the System Recovery strategies to be used in case of service or server failure.

Speaking of System Recovery strategies, this document will concentrate on three types of failures that can occur in an IT Infrastructure and will outline the procedures for recovering from these failures. These three types of failures are:

➢ Service is Down
➢ System is Down
➢ Site is Down

In the first case, when the service is down, it is a System Administrators job to ensure a fully functional service, but even if and when the issue is fixed, it would have still caused a possible downtime which is not good for business. To avoid this kind of possible downtime, this thesis will look at high-availability solutions for the high priority services in the infrastructure, thus, highly reducing system downtime from the first type of failure.
When the system is down, the System Administrator will still be dependent on the high-availability solutions to maintain service availability, until the failed system is back up and running.

And for cases when the whole site is down, which is a rather rare but possible failure mostly caused by some type of natural or human disaster which probably could cause the longest downtime, the System Administrators need to revive all of the servers and services in the main site, while highly depending on the highly-available parts of the system to be functional until a full recovery of the main site is made.

We will summarize all these three types of failures and we will use the term disaster to describe them, since this term has been used in the IT world for a long time now to explain situations when there was unplanned downtime of servers and services which could not be predicted or prevented. There are different ways of using the term disaster in IT, like operational disasters or disaster recovery strategy. [1]

In order to have a high level Recovery Strategy from any type of disasters, a company needs to have a geographically dispersed infrastructure spanned in between many locations with each offering some kind of recovery options for other sites technologies. But unless you’re a multi-million international company with offices around the globe, this kind of approach is costly and not exactly cost effective, so in most cases, most companies have one main site, where they have their main IT Infrastructure and a similar copy of the main sites infrastructure in a second site, which is normally called a Disaster Recovery Site. These two sites will normally be used to create some kind of high availability solution for IT Services offered in the main site, so that in case of a disaster, that servers copy will become functional and continue offering services until the main site’s node is back online.

Apart from high availability solutions, the second site will also have duplicate copies of the main site’s data, the ability to restore full functionality of servers and services in case of a failure, which means either idle or utilized physical servers which would replaces the functionality of the failed nodes and will have the necessary inter-connections to start offering full services for high-priority services and low-downtime offering for lower priority services.

Apart from having an up and running always-on disaster recovery site, a company can also decide to outsource the hosting of their internal high-priority services to Online Hosting companies, and thus shift the recovery responsibilities to them. In addition to disaster recovery, these service providers also offer high availability of these services. Also, companies can decide to save a copy of their company data online, thus they would always
have an up to date version of data that they could use to recover from any type of disasters. [2]

Throughout this document we will be looking at all these scenarios and will outline a Recovery Plan which could be used to avoid downtime and enable full recovery of services down to the last minute of operations. We will illustrate this plan through the use of two case studies from two fictional companies with a small to medium size IT Infrastructure.

This thesis is organized into ten chapters and the list below gives a short description of the contents for each of them:

- Introduction – gives a brief introduction regarding the thesis and the concepts used throughout this thesis.
- Literature Review – gives a short description of the literature used in compiling this document.
- Problem Statement – outlines the problems on which the study of this thesis is based and intends to solve together with the aim and a list of objectives.
- Methodology – gives a description of the research methodologies used in compiling the information and basing the study of this thesis.
- Case Study A - KIT – is the first of the two main parts of the document, where an imaginary infrastructure is used as a case study example in testing and solving the problems stated in the third chapter and thus creating a disaster recovery strategy for similar use cases in real world scenarios. This chapter is organized into the following subchapters:
  - KIT Backup Strategy – defines the Backup Strategy used by IT Department of the imaginary organization named KIT using Windows Server Backup and Symantec BackupExec.
  - Disaster Recovery Site Configuration – outlines all of the configuration changes both in hardware and software level made both in Main Site and the Disaster Recovery Site, to enable safe faster recovery times by making duplicates of backup data and shortest downtime possible by the use of high availability solutions and recovery procedures.
✓ Recovery Strategies – defines the document that should be compiled by the KIT IT Department to outline all of the steps required to recover from all sorts of disasters that can occur in KIT’s IT Infrastructure. A visual representation of these steps can be found in the flowchart given as Appendix A.

➢ Case Study B – CBT – is the second of the two main parts, where another imaginary infrastructure is taken into consideration as a case study example for on how another company decided to solve the problems stated in the third chapter of this thesis and finalized their Infrastructure with new upgrades in addition to the Disaster Recovery Plan. This chapter is organized into the following subchapters:

✓ CBT Backup Strategy – defines how CBT implemented their Backup Strategy by using external hard disk drives for the backup of data.

✓ CBT Disaster Recovery Configuration – defines the configuration that CBT has used in implementing their Disaster Recovery site and how this has affected their Infrastructure Configuration.

✓ Using Online Services for CBT Infrastructure – defines CBT’s strategy in moving some of their high-priority services, like email services, hosting of their Online Training Platform and renting Online Disk Space to the cloud service providers.

✓ The final CBT IT Infrastructure – gives a final layout of the CBT IT Infrastructure including the services in the cloud and those on-premises.

✓ CBT Recovery Strategy – defines a short description of the CBT’s Recovery Strategy that only covers the recovery of internal services like DC, SQL and SharePoint servers, while the Online Service Providers will be responsible for the recovery of the CBT’s hosted services.

➢ Analysis and Comparison of Case Studies – gives an analysis and comparison of these two case studies together with their strong and weak points. A conclusion on which one to choose in between those two strategies is also given in the last paragraph of this chapter.
Discussions and Conclusion – is one of the most important parts of this thesis giving a conclusion of the whole study made through this paper and discussing further options for future similar studies.

Appendix A – represents a graphical flowchart that summarizes the steps required to be performed by KIT System Administrators to overcome possible disasters in the systems and recover the servers and services to a fully functional level.

References – gives a list of references of information used in compiling this thesis and as such allows further studies on this subject by publicly showing the sources of information.
2 LITERATURE REVIEW

This thesis studies the topic of Recovery Strategies for IT Infrastructures that companies in the today’s IT world see as one of the unavoidable and very important topics that should be considered when making an overall Infrastructure Plan. As such, this topic has had and will continue to have a large volume of documents that describe these concepts and technologies. But even though this topic is widely discussed, those sources of information rather offer models of written strategic plans than actual implementation plans, as each company should consider their recovery procedures based on the types of hardware and software infrastructure that they have implemented in their IT Sites.

Further in this document, we have used information which comes from different sources, mainly the TechNet articles for Microsoft Technologies and Products, Symantec BackupExec Administrator’s Guide for Symantec BackupExec Suite, and books that elaborate the topics of this thesis, such as High-Availability, Disaster Recovery, Online Service Providers and Backup Strategies. Those books are very good sources of technical information, and they give a good foundation and further details for these technologies.

The parts of the information from the above sources has been analyzed and only parts of the information that deal directly with the proposed case studies and that apply to the proposed infrastructures have been taken into account. The reason for choosing those specific books in comparison to the rest of the bibliography available in these fields is that those books are one of the top rated books in that certain field’s readings.

As a conclusion, even though this topic has been overly and deeply discussed, the literature for the topic of Disaster Recovery has had some major changes, with the introduction of Cloud Services and this new field of IT will shift many of the current IT concepts to mean different things or include further features compared to the current concepts and technologies. While the first Case Study of this thesis looks at the more traditional Disaster Recovery concepts, the second case study will give an insight to the Cloud technologies in a real life world implementation and how they would affect the Disaster Recovery strategies of companies.
3 PROBLEM STATEMENT

Based on today’s IT Policies having a resilient infrastructure with the most possible uptime, ideally reaching 100%, is a very serious and important issue. Infrastructure Engineers and Architects always build an IT Infrastructure based on a number of factors with reliability and scalability being in the top of the group, as they directly affect the uptime of that Infrastructure.

The reason for such importance comes from the fact that in today’s business world, all of the services offered by the companies have some kind of technology behind them that allows them to function, and the lack of these technologies, means lack of the ability to offer such services, and as such lack of availability of services means lack of income.

The above mentioned concept translates directly into the IT Department’s responsibility in providing these technologies with the least possible downtime of these servers and services or the underlying technologies.

The aim of this Bachelor Thesis is to define the types of disasters that can occur in an infrastructure, which would cause possible downtime of servers and services and the recovery strategies used to recover these services to a fully functional state. As part of this aim, we will fulfill the following objectives:

✓ Recovery of servers and services into fully functional state based on the priority factor with the shortest possible downtime, depending on the type of disaster.

✓ Creation of a Disaster Recovery site and elimination of all single points of failure in all important servers and services.

✓ Backup Data from last two weeks saved in Disk Storage, Archived Backup Data saved for unlimited periods on tapes with a duplicate version in Disaster Recovery Site.

✓ High availability of high-priority services and servers, such as Domain Controllers, Email Servers, Database Servers and File Storage.

Upon the completion, all of the above objectives and the aim of this Thesis shall be completed. This will be tested and proved by the use of a case study, reflecting the infrastructure pre- and post-implementation of the recovery strategies.
4 METHODOLOGY

When writing a thesis in a technical subject, it is unavoidable to use all the research methodologies available, since in one part of the document or another, there will always be a comparison of technologies, products or procedures in both quantitative and qualitative aspects and then as a practical example of the implementation of these technologies and products and procedures we will have a case study of a real life scenario.

As such, the Qualitative and Quantitative Research Methodologies were used in compiling procedures that would be used for backup and restore of services, servers and sites having in mind the shortest possible recovery time but still finding a cost and space effective method for saving data. We are all aware of the fact that, shortest recovery time comes with highest amount of data, as there will always be duplicate data part of many different full backups, but when restoring those items, the backup software is aware of their location and doesn’t have to search through many backup sets to find and restore those items. Also, these methodologies were used in finding a cost effective solution in creating highly-available services while decreasing the data traffic and the investments necessary in having lowest downtime possible for servers and services.

The Case Study methodology was used to develop two practical Recovery Strategies which could apply to many different organizations with similar IT Infrastructures. By the use of this methodology, we can assure that those strategies are more than just an action plan sitting on a piece of paper, but we actually test and prove that they’re functional and could be safely used in a real life scenario, should a disaster occur.

Finally, we could say that by using the mixture of these methods in compiling this thesis, we have assured a working combination of theory and practice in producing usable and real life results.
5 CASE STUDY A - KIT

Based on the fact that Computer Science and IT are practical fields, it is just natural that a thesis in these fields would serve a practical purpose or would be based on a practical example. By taking such a practical example, we will build our first case study of this thesis by considering an IT Infrastructure of a medium sized enterprise with around 2,000 employees and we will consider the IT Recovery Strategies that would be required to have the highest possible uptime of servers and services.

We will first give an introduction to the proposed infrastructure of an imaginary medium size company named KIT (Kosovo’s IT – a company that produces hardware and software required by different industry and business lines) that would suit the needs of its employees. Please find below a picture of this company’s IT Infrastructure and a description of its servers and services.

![KIT Server and Network Infrastructure at HQ Site](image)

Table 1 KIT Infrastructure Equipment Roles and Descriptions

<table>
<thead>
<tr>
<th>Nr.</th>
<th>Name</th>
<th>Roles</th>
<th>Server Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>KITDC</td>
<td>Domain Controller</td>
<td>Domain Controller for the KIT AD and DNS Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DNS</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>KITEXFE</td>
<td>Exchange Front End</td>
<td>Exchange Outlook Web Access</td>
</tr>
<tr>
<td>3</td>
<td>KITEXBE</td>
<td>Exchange Backend</td>
<td>Exchange Information Store</td>
</tr>
<tr>
<td>Nr.</td>
<td>Name</td>
<td>Roles</td>
<td>Server Description</td>
</tr>
<tr>
<td>-----</td>
<td>--------</td>
<td>--------------------------------</td>
<td>---------------------------------------------------------</td>
</tr>
<tr>
<td>4</td>
<td>KITFS</td>
<td>File Server</td>
<td>Public Folders and File Sharing</td>
</tr>
<tr>
<td>5</td>
<td>KITDB</td>
<td>Database Server (SQL)</td>
<td>SQL Database Server for Company Application</td>
</tr>
<tr>
<td>6</td>
<td>KITAS</td>
<td>Application Server (Web) MySQL</td>
<td>Web Application Server with local MySQL Database</td>
</tr>
<tr>
<td>7</td>
<td>KITPS</td>
<td>Print Server DHCP</td>
<td>Print Sharing Server and DHCP Server</td>
</tr>
<tr>
<td>8</td>
<td>KITPR</td>
<td>Proxy Firewall / Gateway</td>
<td>Web Access Proxy and Firewall/Gateway to Internet</td>
</tr>
<tr>
<td>9</td>
<td>KITRT</td>
<td>Main Router</td>
<td>Main Router for KIT Network</td>
</tr>
<tr>
<td>10</td>
<td>KITSSW</td>
<td>Server Switch</td>
<td>Server LAN Switch</td>
</tr>
<tr>
<td>11</td>
<td>KITUSW</td>
<td>User Switch</td>
<td>User LAN Switch</td>
</tr>
</tbody>
</table>

As a first point, in order to achieve any type of recovery in an IT Infrastructure, KIT needs to have a fully functional and tested backup strategy. This strategy should include all of the important servers and services in KIT’s IT and both retention policy and recovery time of these services should be considered when building this strategy. In the next subchapter, we will take a look at KIT’s Backup Strategy for each of the servers and services. After all, you can buy and replace all of the hardware damaged by the disaster - the only thing that you cannot buy is data.

Additionally, as it can be seen from the diagram and table above, the KIT’s IT Infrastructure is located in one central location, the HQ site (HQS), which from a disaster recovery point of view can be seen as a single point of failure. To avoid such situations, KIT will build a second site in City Z, which will represent a city in the same country as the main site and we will call that the Disaster Recovery Site (DRS). The location for the DRS should have a distance of at least 100 kilometers from the main site (depending on the country – it could be even more) and should be one in a location with the least known history of natural disasters and the possibility of offering the required physical and technical infrastructure. [1]

Thus, further in this chapter we will first describe the new hardware and software configurations that will make use of the DRS, by providing high availability to most of KIT’s IT Services based on their priority and desired uptime.
5.1 KIT Backup Strategy

Since most of KIT’s IT Servers and Services are Windows Server based, they will have dual backups based on two products, the Windows Server Backup (WSB) and there will be an additional server which will use Symantec’s BackupExec Suite (SBE), which is the current leading IT Backup Solution in the world. Each of these backup methods will be described further in this chapter including all of the technologies and servers involved in archiving of data as well as the schedule and type of backups used.

5.1.1 Windows Server Backup

Since all of the servers in KITs infrastructure are installed with Microsoft Windows 2008 R2 OS, we will be using scripts and scheduled backups based on Windows Server Backup service to create the first layer of protection for these servers and services in case of a disaster. The reason behind this comes from the fact that with Windows 2008 R2, Microsoft introduced a new Server Recovery method called Bare-metal Recovery, which enables for any server with Windows Server Backup, to be restored to the same or other hardware, from ground up, which is why it’s called bare-metal, meaning you only need the hardware and the backup files, to restore the server to a fully functional state as the snapshot taken by the backup. [3]

The above mentioned fact is the reason we will be using Windows Server Backup in our strategy, since it provides the easiest and safest method to restore the Operating System and any System files residing on the System Drive to the exact same state of the time of backup.

As it can be seen from the diagram and table below, each of the KITs Windows Servers is backed-up locally using WSB daily at 4am and then this backup is duplicated to a central location in KITDC. Windows Server Backup uses a unique incremental technology, which automatically manages the backup storage and creates full backups itself thus, when restoring a server all we need to do is define the timestamp to which we want to restore the server and WSB automatically does the rest of the work by compiling a mixture of full and incremental backups into a single restorable full backup.
Table 2 Windows Server Backup Locations and Schedule

<table>
<thead>
<tr>
<th>Nr.</th>
<th>Name</th>
<th>Primary WSB Location</th>
<th>Duplicate WBS Location</th>
<th>Backup Type</th>
<th>Schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>KITDC</td>
<td>Local Backup Disk</td>
<td>WBS Disk in KITDC</td>
<td>Full / Inc</td>
<td>Daily 12am</td>
</tr>
<tr>
<td>2</td>
<td>KITEXFE</td>
<td>Local Backup Disk</td>
<td>WBS Disk in KITDC</td>
<td>Full / Inc</td>
<td>Daily 6am</td>
</tr>
<tr>
<td>3</td>
<td>KITEXBE</td>
<td>Local Backup Disk</td>
<td>WBS Disk in KITDC</td>
<td>Full / Inc</td>
<td>Daily 4am</td>
</tr>
<tr>
<td>4</td>
<td>KITFS</td>
<td>Local Backup Disk</td>
<td>WBS Disk in KITDC</td>
<td>Full / Inc</td>
<td>Daily 12am</td>
</tr>
<tr>
<td>5</td>
<td>KITDB</td>
<td>Local Backup Disk</td>
<td>WBS Disk in KITDC</td>
<td>Full / Inc</td>
<td>Daily 2am</td>
</tr>
<tr>
<td>6</td>
<td>KITAS</td>
<td>Local Backup Disk</td>
<td>WBS Disk in KITDC</td>
<td>Full / Inc</td>
<td>Daily 2am</td>
</tr>
<tr>
<td>7</td>
<td>KITPS</td>
<td>Local Backup Disk</td>
<td>WBS Disk in KITDC</td>
<td>Full / Inc</td>
<td>Daily 6am</td>
</tr>
<tr>
<td>8</td>
<td>KITPR</td>
<td>Local Backup Disk</td>
<td>WBS Disk in KITDC</td>
<td>Full / Inc</td>
<td>Daily 6am</td>
</tr>
</tbody>
</table>

5.1.2 Symantec BackupExec

As can be seen from the subchapter above, Windows Server Backup provides a pretty good method of backing up servers and services, but only down to the Operating System (OS) level. Windows Server Backup is not aware of services or other forms of backup, thus a
backup of only service data is not possible as WBS only operates in file system level. Additionally, since disk space used for backups is finite, saving older backups becomes impossible, since we would need to add disk space all the time, to be able to accommodate all backup data. Since disk space and hard disk drives are not exactly cheap as a technology, we have to use the Backup Tape archiving technology, which is a cheaper and cost effective for archiving data. But, since Windows Server 2008 R2 doesn’t provide built-in support for tape drives that would be used for archiving backups, we will need to use a commercial software product to suit these needs. [3]

Thus, we will be using Symantec BackupExec (SBE), which is one of the leading Backup Software Suites used by IT Departments worldwide at the moment. This Backup Suite will be installed on a new server which will be named KITBS and it will be connected to a disk pool with enough space to accommodate the backups of KIT Servers which will be backed-up using SBE. Additionally, the KITBS will be connected to a Tape Library with two LTO5 Drives, which will be used to archive the backup data onto tapes, which can be saved for a longer period of time. The following diagram and table will describe how SBE is configured for each of the KIT servers and services including all of the backup locations, schedules and retention policies.

Figure 3 Symantec BackupExec Configuration for KIT Servers
As can be seen from the above table, SBE will be used to backup only certain servers whose service resources can be backed up separately from the operating system, since WSB is used to backup their system resources. The table’s columns are pretty self-explanatory, but we will give a short description of each of them below:

- **Name** – defines the Server Name whose resources are being backed up by SBE
- **Backup Resource** – defines the server resource type that is backed-up by SBE
- **Backup Location** – defines the folder in KITBS used to save backup data for that resource
- **Retention Policy** – defines the period of time for which the backup files from that resource will be safe from *overwrite* (OW) and the period for which they be allowed to be *append* (AP) to existing backup sets. Overwrite means we lose that data, since it is replaced by newer data of the same resource, while, append means that one single backup set will contain all the data from the append period specified.
Backup Type & Schedule – The letter at the front of each row in the cell defines the backup type, where F stands for Full Backup, I for Incremental Backup and D for Differential Backup. The second part of the letters and numbers defines the days on which and the time at which these types of backups are performed. As such, MWF8pm means the backup will be performed on Monday-Wednesday-Friday nights at 8PM; similarly, TTS2am means Tuesday-Thursday-Saturday at 2am and WFSM2am means Wednesday-Friday-Sunday-Monday at 2am; while M-F12am means the backup will be performed every working day, Monday to Friday at 12am.

Duplicate Location – defines the location where archiving will be made. In our case we will be using our tape library with LTO5 Drives, which is the current fastest and biggest available tape drive technology in the market.

Duplicate Retention – defines our Retention Policy for Duplicate Backup data that is saved in the LTO5 Tapes. Since this is an archive backup, we would like to save this data for an unlimited amount of time, which is why OW period is Unlimited (UN) and also we would like to include as much data as a tape can hold, which is why also the AP period is Unlimited.

This backup strategy has been complied having in mind the best possible recovery time for the KIT Servers and services and as such, in case of a failure, these servers and services will be restored and up and running as soon as possible. [4]

With a backup strategy as mentioned in this and the previous subchapter, KIT Infrastructure has a solid recovery perspective upon the failure of a server or a service. But this strategy also has its downsides, such as in case the HQS goes down, so does everything in the KIT IT Infrastructure as all of the data, archives and servers are in one main site. The following subchapter will give an insight on the changed configurations after KIT has built the DRS and how this new site gives additional recovery options to the KIT Infrastructure.

5.2 KIT Disaster Recovery Site Configurations

As mentioned above, the Disaster Recovery Site will be built in City Z, by fulfilling all of the necessary Server Room standards such as: raised floor, cabling, power, cooling, backup power sources, fiber optic network links with the HQ Site and other similar physical requirements. but a description of all these technical features is out of the scope of this thesis, so we will assume that all of those standards were taken into consideration in the finishing of the new DRS. HQS and DRS will be interconnected with a fiber optic leased
line providing enough bandwidth and connectivity for the traffic passing between these two sites.

Below we will explain how the DRS has changed and modified the configuration of each of the services in HQS, based on their priority and their need to have a DRS component to achieve a faster recovery time, in case of a disaster.

5.2.1 Windows Server Backup and Symantec Backup Exec in DRS

After the creation of the DRS, one of the main tasks is to make duplicate copies of all of the backup data onto the DRS, thus creating redundancy in case of a failure in HQS. As such, a second server named KITDRBS will be placed in DRS, and it will be connected to a disk pool big enough to store all of the WSB and SBE Backups of at least the last two weeks. Additionally, a second Tape Library will be placed in DRS and will be connected to KITDRBS, where a second copy of all the data will be made. As such, in case of disaster and a failure of the whole HQS, a copy of tapes will still be existent in DRS.

The following diagram illustrates the changes made to the Backup Strategy and Infrastructure, including the duplicate jobs required to save a copy of the data in the DRS.

Figure 4 Windows Server Backup and Symantec BackupExec in HQS and DRS
5.2.2 Domain Controller in DRS

Apart from having a duplicate copy of all the backup data, in case for any type of failure, a second Domain Controller is crucial, thus we will be creating a second DC in DRS. This second DC won’t be used for authentication of users as it will make un-needed use of the leased lines between the HQS and DRS while still using a slower connection than that of the LAN. Thus, this DC will only accept updates and synchronization information from the HQS having all of the up-to-date data that will be used upon a failure on the main site. [5]

Additionally the second DC will also have a DNS Service running, which will have an up-to-date version of all the DNS Zones in the KITDC server, which will be used as the authoritative DNS Server in case of a failure of the HQS Site, but it won’t be serving any requests until manually allowed to do so by the IT Administrators in KIT, which shall happen only if the HQS is unavailable. [6]

5.2.3 Microsoft Exchange in DRS

With the introduction of Exchange 2010, Microsoft also introduced a new way of defining and separating Exchange 2010 Mail Server Roles. The three main roles are: Mailbox (MBX) Server, Client Access Server (CAS) and Hub Transport (HT) Server Roles. According to most technology specialists, including the Microsoft Advisors, MBX should be installed separately in a server, while the CAS and HT roles can be installed in the same server. Based on this strategy, KIT already has one Exchange Back-End (BE) Server and one Exchange Front-End (FE) Server. These are the pre-Exchange 2010 concept names, where servers were divided between Front-End which was the server answering to the customer requests and Back-End being the server holding the databases, but it still applies to the implementation strategy in place in KIT so we will be using these terms to define the Exchange Roles in KIT Servers. Thus, Front-End Servers will have the CAS and HT roles, while the Back-End Servers will have the MBX role. [7]

After the implementation of the DRS, the Exchange Server configuration will change to offer better recovery options. Thus, KIT will implement an additional FE and an additional BE server, which will replace each other in the event of a failure. Having two additional servers tremendously shortens the recovery time for such a high-priority service like the Email Servers.

With Exchange 2010, among other features, Microsoft introduced the Database Availability Group (DAG) concept, which represents a Cluster Server built inside of Exchange, which
would have *failover* and *failback* capabilities for Exchange Mailbox Stores in between two MBX role servers. This enables having two exact functional copies of the Exchange Database in two different servers in two different locations, thus if the primary site fails, we will have an up and running second copy which automatically enables itself as the Authoritative Mailbox Server in the organization.

Even if there are two mailbox servers that replace each other upon failure, starting with the Exchange 2010, the users connect to their mailboxes through the CAS server role and not through the MBX server role, as was previously. This places an additional importance on the CAS server, apart from just enabling access to the Outlook Web App (or Outlook Web Access as was previously) shortly known as OWA, which represents the method of accessing your mailbox through the web browser. Thus, we will need to have two FE servers in order to have redundancy in accessing the CAS and HT roles. But having two separate servers, means having two different server names, thus accessing these servers will require two different URLs which would be a hassle for the users. By making use of the Network Load Balancing (NLB) feature of Windows Server, we will enable both these servers to be represented by a single IP address and URL name, which in turn enables users to access the FE service without actually being aware of which physical server they are accessing. [8]

After the above mentioned changes, we will have a fully redundant Exchange Server infrastructure both in Front-end and Back-end. The following diagram illustrates the physical and logical configuration of these servers.
5.2.4 File Server in DRS

The File Server service is used to enable user access to common file shares and files where all of the company users need access to. Depending on the folders and files, we will have specific permissions for each of them down to the lowest level, depending on the importance and privacy of the data as well as the organizational structure and rank of each of the employees and their need to access this data to perform their everyday duties. Having access to this data at all times is very important for KIT employees as that’s where they find some of the most important information in performing their duties.

Having in mind what’s stated above, having a fully redundant File Server which is available at all times is of high-importance for the KIT Infrastructure. But technology being what it is, having a 100% uptime on a single server is physically impossible, as there will always be needs to restart servers due to physical interventions, software updates, power cuts and all sorts of other reasons. Even though Distributed File Systems (DFS) has been around as a technology for quite a long time, Windows Server 2008 R2 has introduced many new improvements to this service, and we will be implementing this free Windows
feature to replicate our File Share data between two different servers, one being in HQS and one in DRS. By doing this, we will have an almost exact copy of all the File Server data in our second site, as the replication service runs continuously enabling a last minute up-to-date version of the data in the main site. The following diagram illustrates the Distributed File Service Configuration in KIT IT Infrastructure.

![DFServiceConfiguration](image.png)

**Figure 6 KIT Distributed File Service Configuration**

The DFS Service also creates something called a namespace, which in turn creates a unique access name for the File Share data, thus even if the first server goes down, the second server will automatically resume control of the shares and will provide access to the users, thus the users won’t feel that they have switched to a second file server. They will still be using the same path to access the file share, even if the access actually goes to the File Server in DRS. [9]

### 5.2.5 Database Server in DRS

Similarly to having recovery options for other services, we will implement an Active/Passive Failover Cluster for the SQL Server in our main site, which is used as a database server for our company application. To prevent possible downtime of this service, after the installation of the Failover cluster, the database instance will be represented with a unique server and instance name, while the whereabouts of this service will depend on the cluster service. [10]
As can be seen from the implementation diagram from above, we will implement an Active/Passive cluster, in which case only one of the servers will have an active copy of the database which will be served to users using the cluster service unique instance name. The other server will only hold a passive copy of the database with all the up-to-date data. These two servers will communicate with each other through what’s known as a heartbeat connection, which enables them to check the health of the other node in the cluster. In the event that one node can’t access another, it will assume that this node is down and will resume control of the database instance thus becoming the active node in the cluster. When the second node of the cluster comes back online, it will first check if the other node is serving as an active node in the cluster. If so, it will automatically set itself as the passive node on the cluster and depending on the failback policy, will await the time when it gets to be the active node again. In the case of both nodes going down, the first node to come back online will be the active cluster node. [11]

### 5.2.6 Standby Server for Virtualization in DRS

Even though having a stand-by server which does nothing could seem like a bad investment idea, in case of a failure, each company will require the shortest possible recovery time. To have a fully functional infrastructure with all the services we will need to have a server where we could restore each of these services.
We already have some recovery options for our high-load services but we still have a few services which don’t require very strong physical machines but are still important for our infrastructure. To provide recovery options for these services as well, we will provide *virtual servers* where we will restore these services upon the failure of the HQS. The Windows Server 2008 R2 Hyper-V feature enables virtualization of server hardware to provide one or more virtual servers, where we could better utilize the physical hardware by sharing it among these virtual servers called *virtual machines*. The physical server that we will use will have enough physical resources to enable full functionality of all these services without any glitches. [12] [13]

5.2.7 High Availability of Services

In the previous subchapters we have described how the creation of the DRS has allowed us to change the configurations of our servers and services, in order to achieve better recovery options. But since highest possible uptime is our primary target, these services also need to be *highly-available*. High availability is the concept that describes a service that most ideally will never go off and will never stop serving user requests, even in case of failures. [2]

By reducing single points of failure in servers and services, we will reach a solid level of high-availability for these services. Even though we have reduced single points of failure, our infrastructure will still be prone to service failure upon multiple physical failures. That means, if both our HQS and DRS sites fail, we won’t be able to provide any of our services. To reach highest levels of high-availability, a company needs to have multiple versions of data and servers running in many different sites, thus reducing the chance of full failure, even in case of multiple hardware or software failures, but this requires a multiplication of our IT investments since we will need to buy a hardware infrastructure similar to our configuration in the HQS and implement these configurations in more than one site. [1]

After the full implementation of the above mentioned services and servers in our DRS, the highly available servers and services in our infrastructure are:

- Active Directory Service
- Exchange CAS and HT Roles
- Exchange MBX Roles
➢ DFS File Service

➢ SQL Failover Cluster

We did not mention the WSB & SBE Backups and the Virtualization Servers in the high availability list, as these features need manual intervention in order to be back to a fully functional state and as such don’t represent a highly available service.

5.2.8 The final KIT IT Infrastructure

The implementation of the DRS has enabled us to reach better recovery options and high availability in some of our high priority services, but this was only possible by making high level physical and logical changes to our IT Infrastructure. The following diagram and table explain these changes and give a final layout of KIT IT Infrastructure.

![Figure 8 KIT IT Final Infrastructure (HQS & DRS)](image-url)
**Table 4 Final KIT IT Equipment Role & Description List**

<table>
<thead>
<tr>
<th>Nr.</th>
<th>Name</th>
<th>Roles</th>
<th>Server Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>KITDC</td>
<td>Domain Controller</td>
<td>Domain Controller for the KIT AD and DNS Server</td>
</tr>
<tr>
<td>2</td>
<td>KITDRDC</td>
<td>DR Domain Controller DR DNS DR DHCP</td>
<td>Domain Controller for the KIT AD, DNS &amp; DHCP Server in DRS</td>
</tr>
<tr>
<td>3</td>
<td>KITEXFE</td>
<td>Exchange Front End</td>
<td>Exchange Outlook Web Access</td>
</tr>
<tr>
<td>4</td>
<td>KITDREXFE</td>
<td>Exchange DR Front End</td>
<td>Exchange Outlook Web Access in DRS</td>
</tr>
<tr>
<td>5</td>
<td>KITEXBE</td>
<td>Exchange Backend</td>
<td>Exchange Information Store</td>
</tr>
<tr>
<td>6</td>
<td>KITDREXBE</td>
<td>Exchange DR Backend</td>
<td>Exchange Information Store in DRS</td>
</tr>
<tr>
<td>7</td>
<td>KITFS</td>
<td>File Server</td>
<td>Public Folders and File Sharing</td>
</tr>
<tr>
<td>8</td>
<td>KITDRFS</td>
<td>File Server</td>
<td>Public Folders and File Sharing in DRS</td>
</tr>
<tr>
<td>9</td>
<td>KITDB</td>
<td>Database Server (SQL)</td>
<td>SQL Database Server for Company Application</td>
</tr>
<tr>
<td>10</td>
<td>KITDRDB</td>
<td>DR Database Server (SQL)</td>
<td>SQL Database Server for Company Application in DRS</td>
</tr>
<tr>
<td>11</td>
<td>KITAS</td>
<td>Application Server (Web) MySQL</td>
<td>Web Application Server with local MySQL Database</td>
</tr>
<tr>
<td>12</td>
<td>KITPS</td>
<td>Print Server DHCP</td>
<td>Print Sharing Server and DHCP Server</td>
</tr>
<tr>
<td>13</td>
<td>KITPR</td>
<td>Proxy Firewall / Gateway</td>
<td>Web Access Proxy and Firewall/Gateway to Internet</td>
</tr>
<tr>
<td>14</td>
<td>KITDRHV</td>
<td>DR Hyper-V Server</td>
<td>Virtualization of Low Priority KIT Services in DRS</td>
</tr>
<tr>
<td>15</td>
<td>KIRBS</td>
<td>Symantec BackupExec</td>
<td>Symantec BackupExec Server</td>
</tr>
<tr>
<td>16</td>
<td>KITDRBS</td>
<td>Symantec BackupExec DR Windows Server Backup DR</td>
<td>Symantec BackupExec Server in DRS Windows Server Backup Storage in DRS</td>
</tr>
<tr>
<td>17</td>
<td>KITRT</td>
<td>Main Router</td>
<td>Main Router for KIT Network</td>
</tr>
<tr>
<td>18</td>
<td>KITDRRF</td>
<td>DR Router &amp; Firewall</td>
<td>Main Router &amp; Firewall for DRS</td>
</tr>
<tr>
<td>19</td>
<td>KITSSW</td>
<td>Server Switch</td>
<td>Server LAN Switch for HQS</td>
</tr>
<tr>
<td>20</td>
<td>KITDRSSW</td>
<td>Server Switch</td>
<td>Server LAN Switch for DRS</td>
</tr>
<tr>
<td>21</td>
<td>KITUSW</td>
<td>User Switch</td>
<td>User LAN Switch</td>
</tr>
</tbody>
</table>
5.3 KIT Recovery Strategy

The implementation of all the steps described in the previous chapters and subchapters gives a very solid foundation that enables the recovery of the IT Infrastructure in case of a disaster, but the ability in doing so, doesn’t actually create a Recovery Strategy. It is one of the very important duties for all the IT Departments to have a written and fully tested Recovery Strategy, which explains all of the steps necessary to recover from any type of failure of the IT Infrastructure. Appendix A of this thesis gives a flowchart of the steps necessary to be taken to recover from any type of disaster. We will give a short description of these steps in this subchapter.

We will start by the most feared but the less possible disaster, when because of a natural disaster or some kind of big human error, the whole HQS goes down. This could happen because of a fire, earthquake, or any other form of disaster. In case this happens, what the System Administrators first need to do is to perform a bare metal restore of the Windows Server Backup of the KITBS to a physical or virtual server in DRS. After this, the Catalog files that contain all the necessary information about all the backup sets are restored to the server, so the server can be aware of what each backup set contains. After this, the data storage which holds these backup files should be mounted to that server. Now we have the necessary infrastructure required to start restoring all of the required servers or services.

This is also the case when a disaster happens to a single server which causes it to fail. When a server goes down, we will firstly need to perform a bare metal restore of the server by using the Windows Server Backup. After this restore, the server will return to the last minute state as it was before the last backup. In most cases, unless there are very crucial configuration changes after the backup, this version of running system shall be ready to get back to fully functional state. In order to achieve this state, in most cases, all that system needs is a last version of the service data.

And in case just a service fails, but the server and the site are still functional, then all that is required is a restore of the last version of the data that we have backed-up and the service should resume its functions as it was since the last backup.

Since we will have high-availability features on most high-priority services, the failure of a service, server or even HQS won’t require a full restore. It will rather require the restore of the server node which will serve as a passive node, until it receives an up-to-date version of all the necessary data of the service and then it can resume functionality as the active node of the service, in order to provide higher connectivity speeds and less utilization of high-cost leased lines. A full restore would only be required in case both of the nodes of a
service are down and a full service restore is required. In this case, the main node will first be restored, and then the second node will have a bare metal restore, so the high availability of the service is fully functional again.

In the worst case scenario, when both the HQS and DRS fail for whatever reason, in case the company has a triple copy of the backup data, after an initial procurement and physical installation of the hardware infrastructure, we can use the Windows Server Backups and BackupExec Backups to fully restore the infrastructure, based on the steps outlined in Appendix A and this subchapter.
CASE STUDY B – CBT

Our second case study will be based on the IT Infrastructure of a company called Center for Business and Technology (CBT), which is a company that provides trainings and consultancy services in the field of IT as well as in Business Administration and Finance. CBT has 15 permanent employees, while also employs temporary trainers, external consultants. Additionally, apart from the On-Premise Trainings, where CBT usually has around 100 active students every month, the company also provides an Online Web Portal, offering recorded and live online trainings to interested parties through subscriptions or per training basis. One of the benefits of taking on-premise training in this company is that you get a 1 year free membership to this online knowledgebase, with a possibility of extension.

Even though this company has a very appealing company profile the IT Infrastructure of this company started small and then has been added building blocks through time as the company grew and earned more value and customers. Below is a diagram and a table representing the initial IT Infrastructure of CBT together with a description of roles of each building block.

![CBT IT Infrastructure Diagram](image)

**Figure 9 CBT IT Infrastructure**
Table 5 CBT IT Infrastructure Roles & Descriptions

<table>
<thead>
<tr>
<th>Nr.</th>
<th>Name</th>
<th>Roles</th>
<th>Server Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CBTDC</td>
<td>Domain Controller DNS &amp; DHCP</td>
<td>Domain Controller for the CBT AD and DNS Server</td>
</tr>
<tr>
<td>2</td>
<td>CBTMAIL</td>
<td>Mail Server</td>
<td>Exchange Information Store</td>
</tr>
<tr>
<td>3</td>
<td>CBTSQl</td>
<td>Database Server</td>
<td>SQL Database Server for SharePoint Server</td>
</tr>
<tr>
<td>4</td>
<td>CBTSHP</td>
<td>SharePoint Server</td>
<td>SharePoint Web Server hosting Internal Applications</td>
</tr>
<tr>
<td>5</td>
<td>CBTWEB</td>
<td>Web Server &amp; Database Server</td>
<td>Web Server hosting the Online Training Platform</td>
</tr>
<tr>
<td>6</td>
<td>CBTROFW</td>
<td>Main Router</td>
<td>Main Router for CBT Network</td>
</tr>
<tr>
<td>7</td>
<td>CBTSW</td>
<td>Server Switch</td>
<td>Server LAN Switch</td>
</tr>
<tr>
<td>8</td>
<td>CBTCLSW</td>
<td>Classroom Switch</td>
<td>Student Classroom LAN Switch</td>
</tr>
<tr>
<td>9</td>
<td>CBTOFSW</td>
<td>Office Switch</td>
<td>Employee Office Switch</td>
</tr>
</tbody>
</table>

Even though the current CBT IT Infrastructure is functional and covers the needs of the company, after an internal assessment made by the IT Specialists working for the company, as internal or external staff, a decision was made to make the IT Infrastructure more resilient to failures and keep in step with the newest technologies. As such, after an initial planning and testing, the new infrastructure was implemented by using new server hardware for all the services. The next subchapters will give detailed information about the new infrastructure implemented by CBT.

6.1 CBT Backup Strategy

As could clearly be seen from the above diagram and table, CBT Infrastructure had no backup server or backup plan and no central backup of the data was being made. This was a very important issue and was considered top priority in the list of changes that had to be made by CBT to ensure a resilient infrastructure.

As such, a new backup server named CBTBAK was implemented and by using Windows Server Backup, the CBT Servers were being fully backed up to an external disk connected to the backup server. The reasons for using external disk drives instead of an archive Tape Backup comes from the fact that CBT uses only Windows Server Backup and doesn’t have a software suite that supports Tape Storage. Additionally, the prices for disk drives seem to
be similar to the tapes and since CBT has less data to backup, this seemed like a feasible solution to the IT Department of the company.

After a further consideration of backup and recovery strategy, a decision was made that only one copy of data doesn’t represent a failsafe protection in case of a disaster. As such, multiple copies of backup data were being made. Further in this case study we will look at a detail to how and where this backup data was being saved.

6.2 CBT Disaster Recovery Configuration

Apart from having a main site, CBT has decided that as part of their Disaster Recovery Strategy, they will have a rented office space, in City X, which is 50kms away from the CBT Main Office, which they will use as a Disaster Recovery Site. This site will have an active and ready Internet connection, which in case of the disaster could be used to start offering the services needed, upon the failure of the main site.

This second site will also have a safe box which will be used to keep a copy of the older backup data from the main site. Thus, every week, the System Administrator of CBT will bring a filled external disk, with older backup data to the Disaster Recovery site and these disks will be kept safely in the safe box. In case of a disaster, this backup data can be used to revive all the failed CBT Servers and Services. [1]

Apart from the copies of backup data, the older server hardware that was replaced by the upgrade was moved to this DR site. These servers still offer enough hardware resources that could be used to host the failed services, until a full recovery of the main site is made. These servers will have no OS installed and no data stored in them, but in case of a disaster, the Windows Server Backups from the external disks can be used to restore the main site’s services to the last point of backup available in DR. [2]

6.3 Using Online Services for CBT Infrastructure

After the technical assessment made on the CBT’s IT Infrastructure, the IT and Management Teams have decided to make use of Online Services to host some of the company’s applications and services, be it internal or external. As such, CBT has decided to outsource the hosting of two important services in their infrastructure, the E-Mail service and the web server hosting the online training platform. Additionally, CBT will buy Online Storage Space that will be used to keep a last copy of each day’s backup data.
6.3.1 Email Services Online

After an assessment of the options available both in technical and economical aspect, the email service was moved to the Google servers through the use of the Google Apps for Education program, which CBT qualified for, since it is an educational institution with the required registration certificate and status. Thus, CBT would offer email services to the internal and external employees as well as current and past students, through the use of one of the today’s number one email platforms in the IT World, for free. Apart from the email services, this platform would also offer some collaboration sites, Google Apps for accessing and editing documents online, training calendars, online storage space through Google Drive that internal and external users will use to save their important files and also advanced email features, which would be administered by the CBT System Administrators, such as email retention, archiving, legal hold and other features as offered by Google. The authentication services for emails will still go through the internal Domain Controller which is responsible for user accounts and this authentication information is shared with Google through a safe and secure connection. [14]

6.3.2 Web Application Server Online

Hosting a web application in an in-house web server is a cost effective strategy, but in case that this web server has a lot of traffic and requires more bandwidth, it would be a better strategy to move the hosting of this web application in an online web server hosting platform, as these companies they offer additional features both in security and reliability apart from the standard requirements of a web server for a fairly cheap and affordable price.

Thus, after an assessment of options and technologies, CBT decided to move the hosting of their Online Trainings Web Application to the HostGator servers, one of the number one hosting services in the world. As such, HostGator would be the responsible party for the uptime and functionality of this Online Training Platform, by offering the required hardware, bandwidth and availability solutions. [15]

6.3.3 Space Storage Online

Even though CBT has dual copies of backup data, in case of a disaster in the main site, CBT will only have a one week old backup in the DR site, since the backup disks are transferred there on a weekly basis. To avoid this kind of situation, CBT has decided to buy 2TB of Online Storage Space through their subscription to Google Apps for Education. By
using this space, CBT will daily upload all of the backup data from that day, to this online storage and as such, in case of a disaster, CBT would always have a last day version of the data online. This disk space is disaster-free since, Google is the responsible party for the safe keeping of this data. [16]

6.4 The final CBT IT Infrastructure

After the full implementation of the IT Infrastructure Upgrade Plan, now CBT has moved their Email Services and Web Application Services online, has created a passive but ready to use Disaster Recovery Site and has created a Backup Strategy with multiple copies of data being saved in more than one location, including a version saved in an online storage space. After these changes, the following diagram and table give a layout of the final CBT IT Infrastructure.

Figure 10 Final CBT IT Infrastructure
Table 6 Final CBT IT Infrastructure

<table>
<thead>
<tr>
<th>Nr.</th>
<th>Name</th>
<th>Roles</th>
<th>Server Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CBTDC</td>
<td>Domain Controller</td>
<td>Domain Controller for the CBT AD and DNS Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DNS &amp; DHCP</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>CBTSQL</td>
<td>Database Server</td>
<td>SQL Database Server for SharePoint Server</td>
</tr>
<tr>
<td>3</td>
<td>CBTSHP</td>
<td>SharePoint Server</td>
<td>SharePoint Web Server hosting Internal Applications</td>
</tr>
<tr>
<td>4</td>
<td>CBTBAK</td>
<td>Windows Server Backup</td>
<td>Backup Server for CBT Infrastructure</td>
</tr>
<tr>
<td>5</td>
<td>CBTROFW</td>
<td>Main Router</td>
<td>Main Router for CBT Network</td>
</tr>
<tr>
<td>6</td>
<td>CBTSSW</td>
<td>Server Switch</td>
<td>Server LAN Switch</td>
</tr>
<tr>
<td>7</td>
<td>CBTCLSW</td>
<td>Classroom Switch</td>
<td>Student Classroom LAN Switch</td>
</tr>
<tr>
<td>8</td>
<td>CBTOFSW</td>
<td>Office Switch</td>
<td>Employee Office Switch</td>
</tr>
<tr>
<td>9</td>
<td>Google Apps</td>
<td>Email Services, Google Apps</td>
<td>Online Service offering advanced e-mail features, online</td>
</tr>
<tr>
<td></td>
<td>for Education</td>
<td>Email, Email Vault</td>
<td>office documents and user storage space</td>
</tr>
<tr>
<td>10</td>
<td>HostGator</td>
<td>Web Application Server</td>
<td>Web Hosting Service for Online Training Web App</td>
</tr>
<tr>
<td>11</td>
<td>Google Drive</td>
<td>Backup Storage Space</td>
<td>Space used to save a copy of the latest backup data on a</td>
</tr>
<tr>
<td></td>
<td>Backup Space</td>
<td></td>
<td>daily basis</td>
</tr>
<tr>
<td>12</td>
<td>Spare Servers</td>
<td>Recovery Servers</td>
<td>Powered Off Idle Servers used in case of a Disaster</td>
</tr>
<tr>
<td>13</td>
<td>Backup Drives</td>
<td>Backup Data</td>
<td>Copies of archived Backup Data kept safely in DR</td>
</tr>
</tbody>
</table>

6.5 CBT Recovery Strategy

By outsourcing their email services and web hosting services, CBT has moved the Disaster Recovery responsibilities from their internal IT Staff to the online companies that host these services. Apart from hosting this data, it is the sole responsibility of these companies to offer highly available services and recovery of data and services in case of a failure of their servers.

CBT will be responsible for providing a working Domain Controller which will be used to authenticate users’ on-premise and online, through the shared secure connector with Google, is also responsible for maintain the availability of the internal SharePoint Server, which the company uses for hosting a custom built web application for administering their internal workflow and services.
Through the use of multiple copies of backup data, CBT can restore these internal services to either the same or another physical server, in case of a failure of the original server and service, or restore the functionality of these servers and services in the spare servers that are kept in the DR site. Older archived backups will still be available in the DR Site, while the latest version of the backup can always be accessed through Google Drive space. Google will be the party responsible for the safe keeping of the copies of backups of CBT Infrastructure saved in their servers. All of the above steps will be outlined in the Recovery Strategy document written by the CBT IT Staff and will be tested twice annually for consistency and updated accordingly.
7 ANALYSIS AND COMPARISON OF CASE STUDIES

In the above two chapters, we gave two examples of companies with IT Infrastructures, and how these two companies decided to change their infrastructures to make them resilient of three different types of failures that could occur, that we called disasters.

In the first case study, the company called KIT created a fully functional and tested backup strategy, which is the first step necessary to be able to recover any type of failure. As a second step, they created a Disaster Recovery Site, and used this site to build a high-availability solution of all of their high priority services. This way, in case of any type of disaster they would have the highest possible uptime by the automatic failover and failback of important services, until a recovery of the passive node was made. Additionally, they extended their backup strategy to create duplicate copies of the backup data from the main site, that in case of any type of disaster, they would have copies of all archive backups in the DRS. Last but least, they created a Disaster Recovery Plan, which would was tested and its functionality was ensured, and thus it would be used in case of a disaster as a walkthrough of all the steps needed to be taken to recover from that disaster.

In the second case study, CBT took a different path in their upgrade strategy, in making their infrastructure more prone to failures. After an initial hardware upgrade of existing servers, they outsourced the most important services to Online Service providers, thus shifting recovery responsibilities to these companies instead of their internal IT staff. This way, instead of a costly investment for building a fully functional highly available disaster recovery site, they would pay for the services of hosting these internal applications, while not having to worry about their recovery strategies. The only internal services that CBT is responsible in recovering in case of a disaster are the internal Domain Controller and the web and database servers used by the SharePoint Server that hosts a tailor-made internal web application.

As can be seen from above, these two companies took two different paths in making sure that their infrastructure could survive an IT Disaster, and these strategies were build taking into consideration a number of factors, such as: recovery time, availability of services, uptime, cost, location of data and implementation investments for disaster recovery sites. These factors were seen and considered differently by these two companies, based also on their company strategies and investment plans.

From a technical point of view, both these strategies are correct and can be implemented, as such, with the analysis of these two case studies, we could conclude that they are both valid paths for building a recovery strategy and should be taken into consideration.
Throughout the chapters and subchapters of this thesis we explain what IT Departments should do, in order to be able to recover from different types of disasters that could happen to their IT Infrastructures. These procedures could be summarized in these four tasks:

➢ Have a Disaster Recovery Site with all the necessary equipment and connections.

➢ Offer highly-available services to prevent downtime even in case of disasters.

➢ Have a fully functional and at least dual-copy backup of all the corporate data and their archives in both main site and the disaster recovery site and ideally a third in safe and secure location used for archiving.

➢ Have a written and fully tested Recovery Strategy, which shall be used as a walkthrough guide in the event of a disaster.

But fulfilling these tasks doesn’t ensure a fully functional strategy which can be used at all times. Since technologies change all the time, and since consistency of data is the crucial factor in the success of a recovery plan, this plan should be consistently tested and updated to adapt the changes in the infrastructure. Additionally, it is always better to develop a failure prevention plan rather than a recovery plan, thus, it is crucial that we eliminate all single points of failure both in hardware and software level for our high priority servers and services. By reducing these single points of failure and by using the high-availability features of important services, we can always recover from hardware and software errors with the lowest possible downtime.

Another important consideration is having multiple copies of data, which is the most important building block of any recovery plan. Thus, in case of a disaster that causes total or partial data loss, we can always recover our IT Infrastructure to the point of the last successful backup.

Last but not least, considering the technology advancements of today, companies can consider Cloud Solutions as one of the possible and highly successful parts of their IT Recovery Plans. By moving their services and saving their data in the cloud or even building a DRS in the cloud, we can be sure that our data is safe and that in case of a disaster; we can have an up and running infrastructure in the shortest possible time. As such, the responsibility for data and infrastructure safety is moved to the Cloud Services Provider as stated in the signed Service Level Agreement (SLA).
KIT Disaster Recovery Plan

Type of Disaster

HQS Down

Restore KITBS from Windows Server Backup (Bare Metal Recovery)

Resource Down

BackupExec – Job Setup

Restore Tasks – New Job

Select Server and the Resource to be restored

Select the Restore date from data in DR Folders

Type of Resource

KitFS or KitDRFS

KitDB or KitDRDB

Type of Last Backup

FULL

Restore only the last FULL Backup

DIFF

Restore the Full Backup and then the last DIFF Backup

INC

Restore the last FULL Backup and then all the INC Backups until the last one

Exchange BE Servers

Select DAG Server Group

Select Mailbox Store to be restored

DIFF

Restore the FULL Backup – Settings: Microsoft SQL: Leave the database non-operational

Select Mailbox Store to be restored

DIFF

Restore the FULL Backup – Settings: Microsoft SQL: Leave the database non-operational

DIFF

Take existing destination database offline

Run Now
10 REFERENCES


