KARELIA UNIVERSITY OF APPLIED SCIENCES
Information Technology

Lassi Latva-Nirva

BACKUP AND DISASTER RECOVERY IN WINDOWS ENVIRONMENT

Thesis
April 2019

Karelia
AMMATTIKORKEAKOULU

THESIS
APRIL 2019
Degree Programme in Information Technology

Tikkarinne 9
80200 JOENSUU
+358 13 260 600

Author
Lassi Latva-Nirva

Title
Backup and Disaster Recovery in Windows Environment

Commissioned by
Karelia UAS

Abstract

The primary goal of this thesis was to research, test and compare Windows Backup Role and Veeam Backup Agent. This thesis gives the reader a general idea of what type of backups there are and how different kind of solutions can be implemented in an environment.

Backup and Disaster recovery have a vital role in daily IT operations. Backups define major aspects of a business continuity plan in an enterprise. It is critical that the solutions work and constant improvement to the backup solutions is made to ensure that files or even whole servers can be recovered safely and within the time window.

This thesis consists of two parts. The first focuses on the theory and history of backups and disaster recovery. The second part tests backup and disaster solutions used at the enterprise level. Two backup solutions were tested, and various measurements were taken and compared. Some values that were analyzed were the backup time, time of recovery and use of resources and computing power when working on a backup. This experiment was performed in a lab environment.

Language

English

Pages 67

Keywords

Karelia, backup, recovery, research, Windows Server 2012 R2, Veeam

Table of Contents

Abbreviations and Terms

Endpoint Device

An endpoint device is a device usually used by end users. These devices can be, for example, computers, printers, and mobile phones. Nowadays people can connect household devices to the network, which means that even a fridge can be an endpoint device. They are called endpoint devices because they sit at the edge of a network.

HDD

Stands for the Hard Disc Drive, and it is the component for storing data. Unlike SSD, HDD is mechanical.

SSD

Stands for a Solid-State Drive, sometimes called solid-state disc, although SSDs do not have physical discs. It is a component to store data. SSDs have faster read and write times compared to HDD.

RAID

Stands for Redundant Array of Independent Disks. RAID is data storage technology that combines multiple physical or virtual discs in one or more logical units. There are various types of RAID, most are there to protect against for system failure, but some are there to increase performance. There is also hardware and software RAID. However, a RAID is not a backup solution, and it is not a good idea to use it as one.

CPU

Stands for Central Processing Unit and is the component that controls and executes commands.

Disaster Recovery

Disaster recovery (DR) is an area of security planning that aims to protect an organization from the effects of significant adverse events.

1 Introduction

Enterprises from small to large need backups of their data on a regular basis. Disasters do occur, and that makes backup and disaster recovery procedures a critical part of business IT. The backup system acts as a vital system in case of a data loss due to a human error, virus or a component failure [1]. The loss of data can turn out to be expensive, and the company might have to face legal charges [2].

With fast changing technologies, there is a need for cost-effective and low burden backup solutions. Cisco summarizes it well, the absence of a backup operation scheduled to take place in an enterprise may have a tremendous financial impact on the enterprise due to the cost of recreating lost data, possible legal charges and loss in productivity which the downtime creates. [3]

The primary purpose of this thesis was to study and test out different methods of backing up and recovering after an unexpected event. After the theory section, each chapter contains testing results of different servers tested with different techniques. This thesis focus is on how to backup servers and how much resources each method uses, giving some insight into other related topics as well.

Usually, networks varying from the size of the company include these four components: endpoint devices, switches, servers and routers. Endpoint devices are, for example, handheld devices like smartphones or tablets. Desktop computers and laptops are also categorized in the endpoint devices category, also not narrowing out other devices like printers or other network connected smart devices. This thesis covers servers only, giving the reader a possibility to learn more about backing up servers and help choose a proper backup and recovery measure for their company or apply these recommendations at home.

2 History of Disaster Recovery & Backup

Computer data develops fast nowadays. In the past, there was not a lot of data in the world, and people had no expectations of a possibility for immediate availability. For the first backups, big reels of magnetic tape were used to backup data. PCs could also process punch cards and paper tape. [4]

The first backup media ever created were the punch cards in 1951. Then in the 1960s came the magnetic tapes which are still in use today. Magnetic tapes were faster and had more capacity since one single roll of magnetic tape could hold 10 000 punch cards. It soon became popular and held its place as the best backup medium until the 1980s.

The first hard drive was invented in 1956 by IBM. It was called the IBM 305 RAMAC. The reason why hard drives were not used to back up data before the 1980s, was that they were expensive, large and had low capacity. In the 1980s, hard drives were considered an excellent choice to backup data. However, in the early 1990s, they became a real alternative for tape backups. Even today companies decide if to use tapes, discs or both [5]. Most enterprises have both. The data size has grown a lot since the 1950s. Megabytes have turned into gigabytes which have increased into terabytes and petabytes in recent times [6].

3 Backup Media Types

Different backup media types are explained in this chapter. Also, the advantages and disadvantages are presented.

3.1 Hard Drives and Disk-to-Disk Backup

Backing up data on a hard drive is the most common backup method. It is cheap, lots of data can fit on the hard drive, and hard drives can be used to build a RAID array. On the other hand, drives produce heat and have a high failure rate. Compared to tapes hard drives are more efficient and faster than tapes. [7]

There are some advantages and disadvantages, these are the benefits:

- RAID
- cheap
- size
- capacity.

These are the disadvantages:

- high failure rate
- heat.

3.2 Portable Drives

Backing up data on portable hard drives is also an option. Portable hard drives are easy to store and have the same possibilities and disadvantages that standard hard drives have. Portable drives are also great for their portability [8].

There are some advantages and disadvantages, these are the benefits:

- easy to store
- capacity
- cost-effective
- portability.

These are the disadvantages:

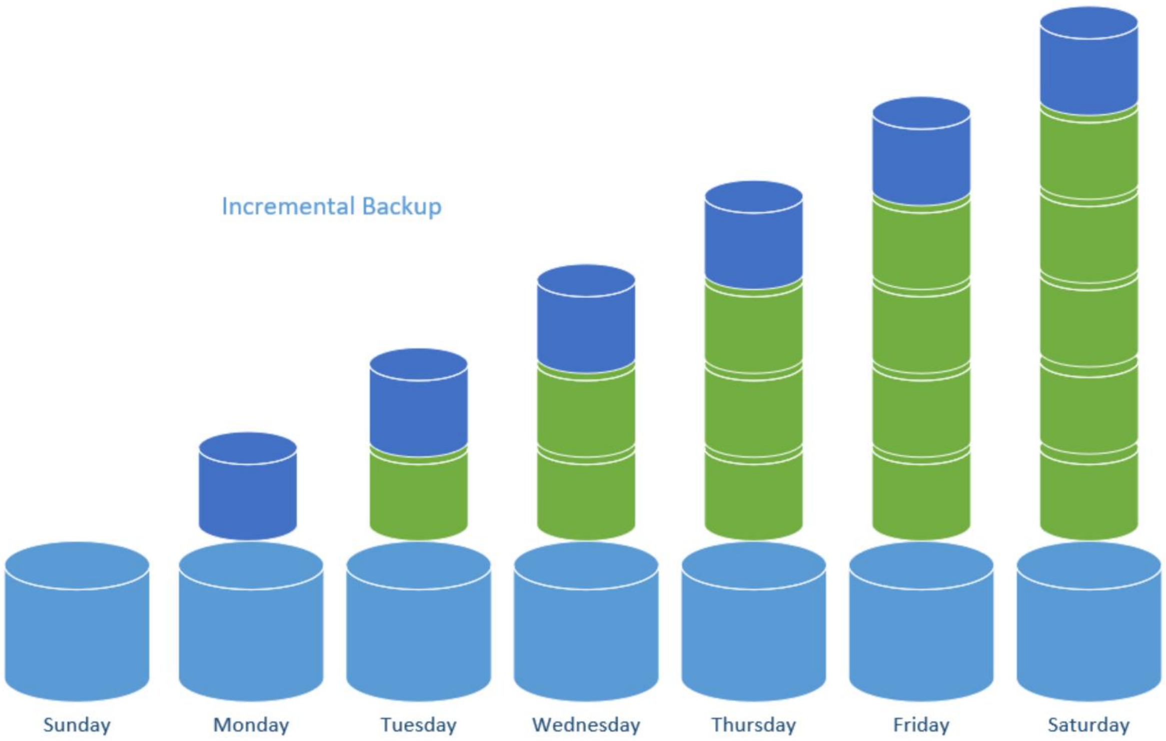
- high failure rate
- heat.

4 Backup Methods

There are many different options when backing up data. Here are some basic guidelines, however, some do not work in certain types of environments. Daily backups need to be made on critical data. At least one copy of the recovery media should be at the site for quick access. Extra duplicates of the backup should be taken to increase redundancy in case of environmental disasters like fire, flood or theft. To avoid theft, store the backup media in a locked safe. Encrypting backup files increase data security in case of theft. Keep backup devices and servers stored in a server room with access to IT personnel only. Daily backups schedules can be made to reduce the manual work on the IT staff. [9]

4.1 Incremental Backup

Incremental backup is a process, where only the changes and newly added data are backed up. After the full backup has finished, the incremental backup schedule can start. Demonstrated in Picture 1 below. By scheduling an incremental backup to run every day, data will always be up to date, and there will be no duplicate data. Standard types of incremental backups are a full synthetic backup, block-level incremental backup, byte-level incremental backup, incremental forever backup, multi-level incremental backup to name a few. [10]



Picture 1. Incremental backup. (Picture: Lassi Latva-Nirva).

There are some advantages and disadvantages, these are the benefits:

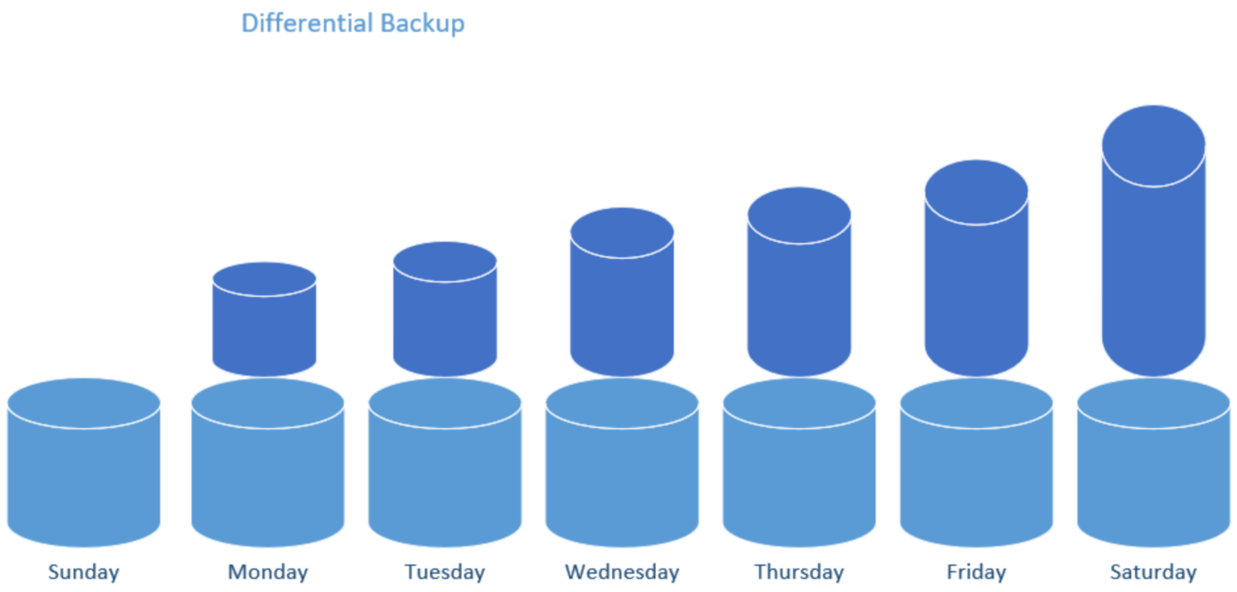
- fast backup method
- no duplicate data.

These are the disadvantages:

- slow to restore
- more complicated restore
- a full backup is needed to perform a complete restore.

4.2 Differential Backup

A differential backup is a process, where all changes and newly added data from the last full or differential backup are backed up, and each differential backup is merged into next day's differential backup copy, which makes the restoration process faster [11]. This is demonstrated in Picture 2 below.



Picture 2. Differential backup. (Picture: Lassi Latva-Nirva).

There are some advantages and disadvantages, these are the benefits:

- fast backup method
- faster restore time.

These are the disadvantages:

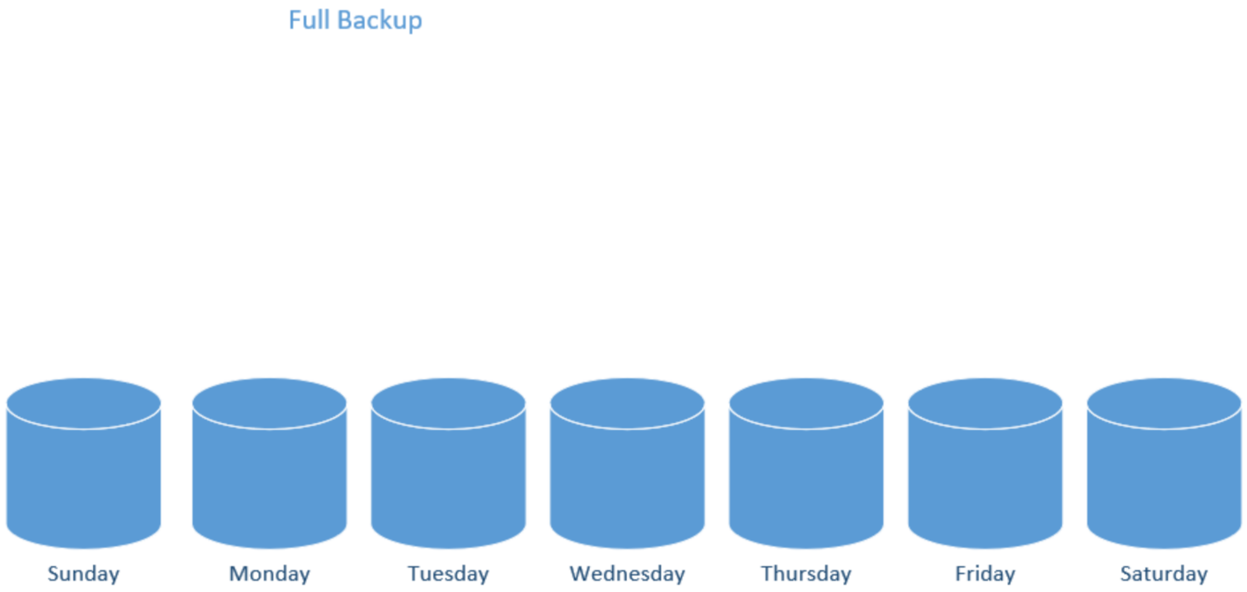
- creates many duplicates
- a full backup is needed to perform a complete restore.

4.3 Full Backup

A full backup is a process, where all files and folders are backed up. A full backup is usually made as an initial backup and re-made again depending on the backup schedule and window set. Some companies perform full backups weekly, bi-weekly or monthly. Full backup takes the most space to store. This is demonstrated in Picture 3 below. Full backup works as a base for other backup methods which means that other methods rely on it. [12]

Full backup copies everything from the server and that is why it takes the most time to backup and lots of storage space depending on the amount of the data on the server. It is also the safest way to back up anything. Recovering from a full backup is the easiest, most reliable and fastest way to get the server back online.

In the author's opinion, a full daily backup is not a big issue nowadays. The reason for that is that the recovery media are now cheaper than before, but still, it is a lot cheaper to use a different method for a daily backup.



Picture 3. Full backup (Picture: Lassi Latva-Nirva).

There are some advantages and disadvantages, these are the benefits:

- easy to maintain

- easy to manage
- less risk of losing data.

These are the disadvantages:

- takes much space to store
- backup can take a long time to run
- backups the same files already backed up previously.

4.4 Full Backup and Incremental Backup

When comparing full backup and incremental backup first a full backup is made. After the full backup, an incremental backup starts as scheduled. A full backup is made again after a set of incremental backups. To restore, the latest full backup and all the incremental backups after that are required to restore any data. [13]

When compiling these two different backup technics, the advantages of the full backup and the incremental backup are gained. Backups will complete faster and require fewer storage media to store the backup.

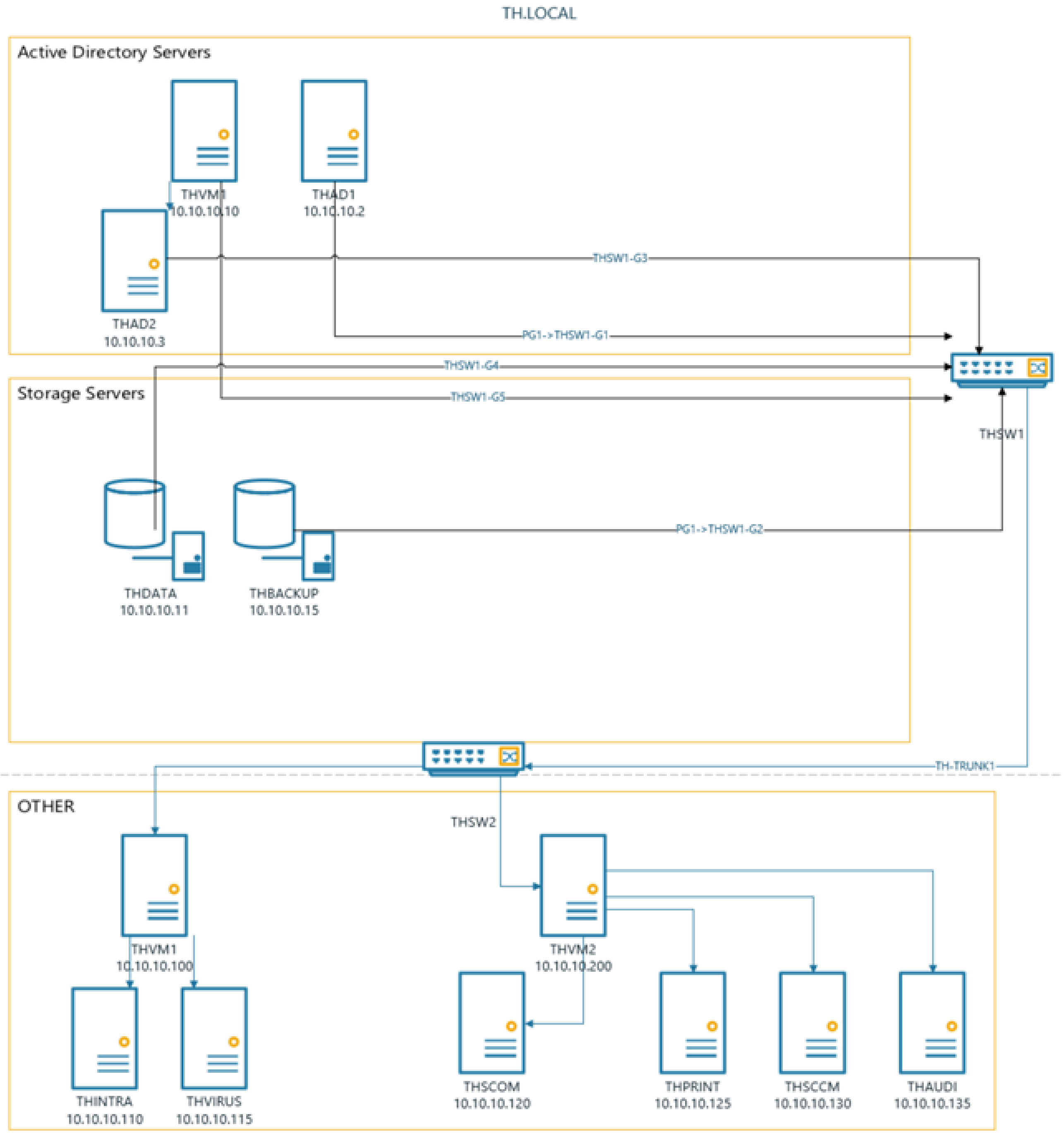
4.5 Synthetic Full Backup

A full synthetic backup is a variation of an incremental backup. Synthetics compile into full backups by connecting incremental and full backups. The incremental backups consist of updates only [14].

5 The Test Environment

The test environment consists of 500 machine created users. This thesis is limited to studying only three business critical servers. The test environment does have other roles and servers running as well. In Picture 4 can be seen all the servers of TH.local. All the physical servers run Windows server 2012 R2 Datacenter edition.

The business requirements are that the data and applications are accessible for 24 hours a day, every day of the year. It is critical due to these requirements that the environment runs on a high-availability platform. It is also crucial that the disaster recovery plan is in place.



Picture 4. TH.Local environment. (Picture: Lassi Latva-Nirva).

Research conducted by Tech-Pro research shows that 69% of the storage technologies in use 2015 was local technologies, such as external hard drives. SAN and NAS solutions were 63% and 61% and the fourth used were tapes. Cloud was not that popular during the research, but it has gained popularity in the past three years. According to the study, the pain points in major storage solutions are the cost and requirement for higher capacity. In

37% of the companies, IT vice president or director usually purchased the storage hardware and software for the environment. The person specialized in storage and backups did this only in 9% of the companies [15].

6 The Test Equipment

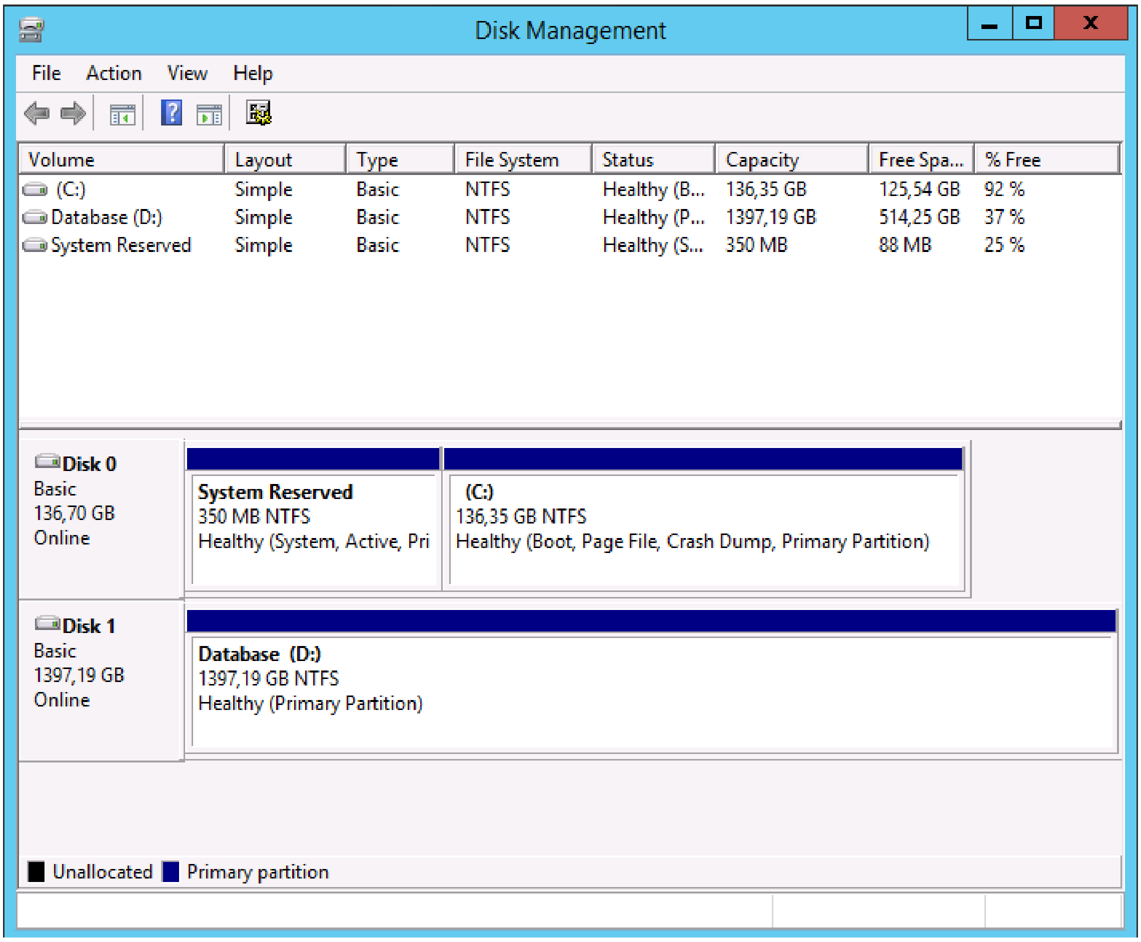
In this chapter, a closer look at the environments servers is taken. Only the servers used in testing are presented.

6.1 THBACKUP

Backup server, named THBACKUP is running Windows Server 2012 R2 Datacenter edition. Processors are two Intel(R) Xeon(R) E5620 2,40GHz processors. There are 16 gigabytes of RAM installed. The main role of this server is to act as the backup server in the TH.local domain.

6.1.1 Disk Setup

On this server C: is made of two disks that are mirrored, with one spare. D: is in raid five with three drives and one spare. In Picture 5 shows Disk Management from THBACKUP.



Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free
(C:)	Simple	Basic	NTFS	Healthy (B...	136,35 GB	125,54 GB	92 %
Database (D:)	Simple	Basic	NTFS	Healthy (P...	1397,19 GB	514,25 GB	37 %
System Reserved	Simple	Basic	NTFS	Healthy (S...	350 MB	88 MB	25 %

Disk 0
Basic
136,70 GB
Online

System Reserved
350 MB NTFS
Healthy (System, Active, Pri

(C:)
136,35 GB NTFS
Healthy (Boot, Page File, Crash Dump, Primary Partition)

Disk 1
Basic
1397,19 GB
Online

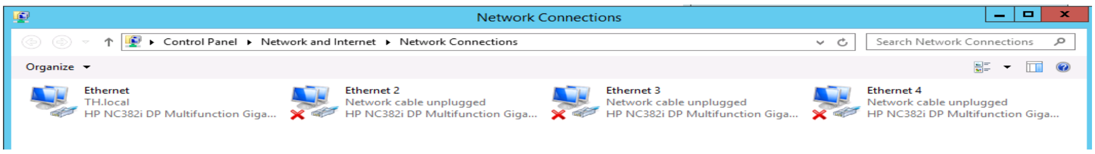
Database (D:)
1397,19 GB NTFS
Healthy (Primary Partition)

■ Unallocated ■ Primary partition

Picture 5. Disk Management window on THBACKUP server. (Picture: Microsoft Windows Server 2012 R2).

6.1.2 Network Setup

The server has four Ethernet ports, but only one is in use at the moment. Adding a NIC-team to the server would increase reliability. In Picture 6 shows the list of the installed network connections.



Network Connections
Control Panel ▸ Network and Internet ▸ Network Connections
Search Network Connections
Organize

Ethernet
TH.local
HP NC382i DP Multifunction Giga...

Ethernet 2
Network cable unplugged
HP NC382i DP Multifunction Giga...

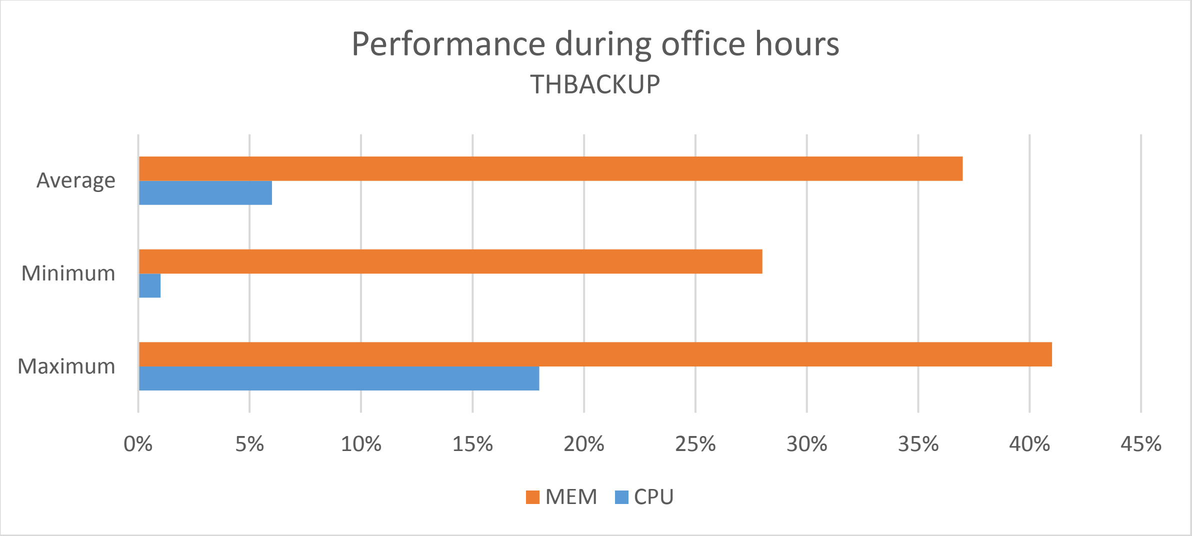
Ethernet 3
Network cable unplugged
HP NC382i DP Multifunction Giga...

Ethernet 4
Network cable unplugged
HP NC382i DP Multifunction Giga...

Picture 6. Network Connections window on THBACKUP server. (Picture: Microsoft Windows Server 2012 R2).

6.1.3 Performance During Working Hours

The server uses about 6% of its processing power during office hours and 37% of its memory on average, as can be seen in Picture 7 below. The server has enough capacity to perform other roles as well, but the main purpose of this server is to act as the backup storage server.



Picture 7. Performance during office hours on THBACKUP. (Picture: Lassi Latva-Nirva).

6.1.4 Backup Schedule

In this environment, backup runs from Monday to Friday every day at 23:00. Windows Server Backup does not support incremental backups, so full backup runs every day. For Veeam full backup is run every Sunday at 18:00 and incremental backups daily from Monday to Friday.

The server is backed up to either an external hard drive or THDATA server. There are six generations of backups made weekly. After one week the weekly backups are removed from storage. A monthly backup runs every 30th day of the month. Storing time for monthly backups is one year. A yearly backup is made 1.1.20xx and stored for seven years at the time.

There are four types of backup schedules set for THBACKUP:

- local backup to external HDD, created with Windows Server Backup
- network share backup, created with Windows Server Backup
- local backup to external HDD, created with Veeam Agent
- network share backup, created with Veeam Agent.

6.1.5 Recovery Time Objective

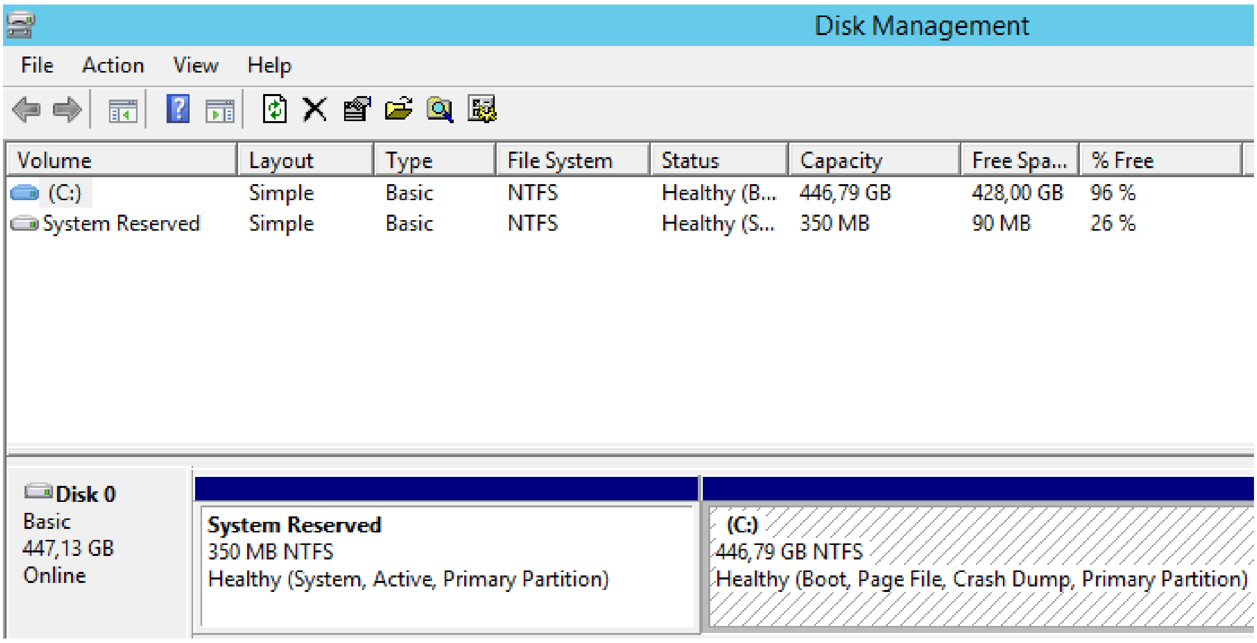
Availability is critical for backup server, restore should start immediately, and the server recovered as soon as possible. The time window for recovery is 13 hours.

6.2 THAD1

System THAD1 is one of the AD servers in TH.local domain, with 8GB of memory and AMD FX(TM)-6300 Six-Core Processor. THAD1 is running Windows Server 2012 R2 Datacenter edition. The primary role of this server is to act as a main Active Directory server.

6.2.1 Disk Setup

There is no RAID configured for THAD1. The operating system is running on one 470GB solid-state drive. Picture 8 shows the Disk Management window for THAD1.



Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free
(C:)	Simple	Basic	NTFS	Healthy (B...	446,79 GB	428,00 GB	96 %
System Reserved	Simple	Basic	NTFS	Healthy (S...	350 MB	90 MB	26 %

Disk 0
Basic
447,13 GB
Online

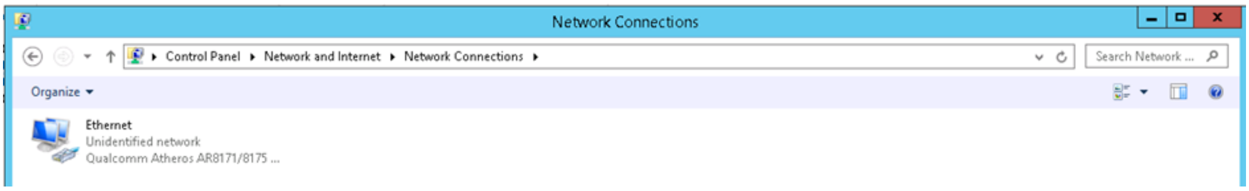
System Reserved
350 MB NTFS
Healthy (System, Active, Primary Partition)

(C:)
446,79 GB NTFS
Healthy (Boot, Page File, Crash Dump, Primary Partition)

Picture 8. Disk Management window on THAD1 server. (Picture: Microsoft Windows Server 2012 R2).

6.2.2 Network Setup

There is only one ethernet port on the server installed. If there were more network cards, NIC-teams could be made to improve reliability and performance on the server. Picture 9 shows the Network Connections on the THAD1 server.



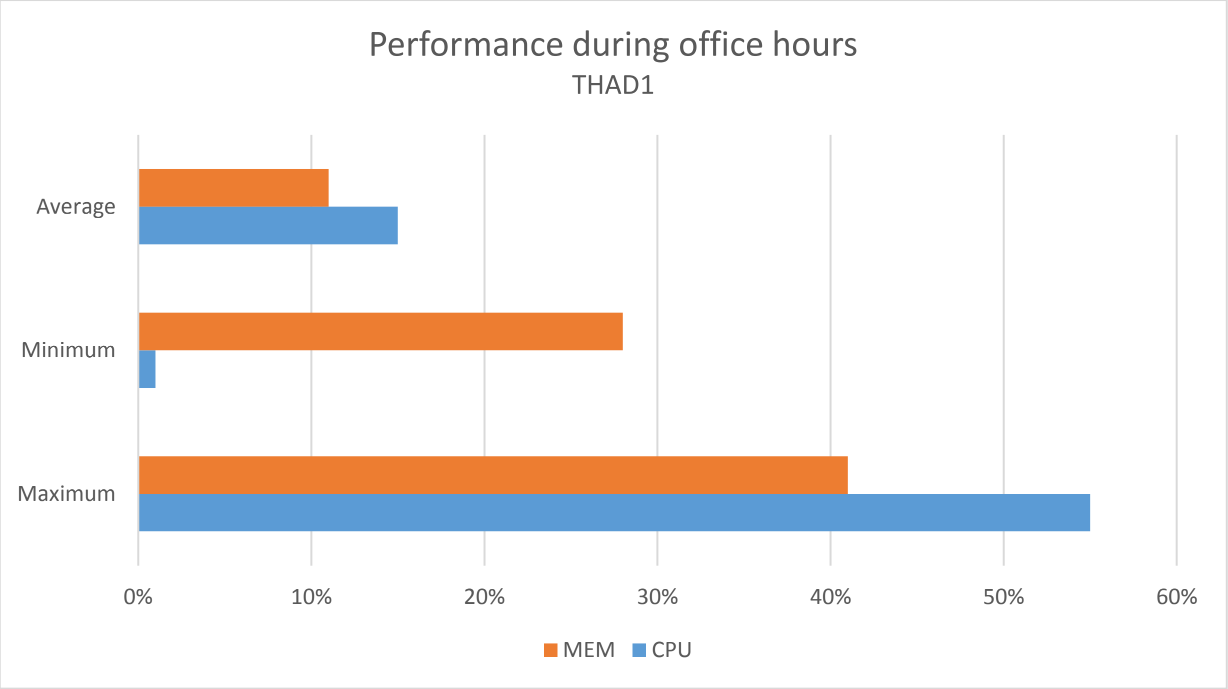
Network Connections
Control Panel ▸ Network and Internet ▸ Network Connections ▸
Search Network ...
Organize ▾

Ethernet
Unidentified network
Qualcomm Atheros AR8171/8175 ...

Picture 9. Network Connections window on THAD1 server. (Picture: Microsoft Windows Server 2012 R2).

6.2.3 Performance During Working Hours

The server uses about 15% of its processing power during office hours and 11% of its memory on average. Picture 10 shows the graph of performance during office hours.

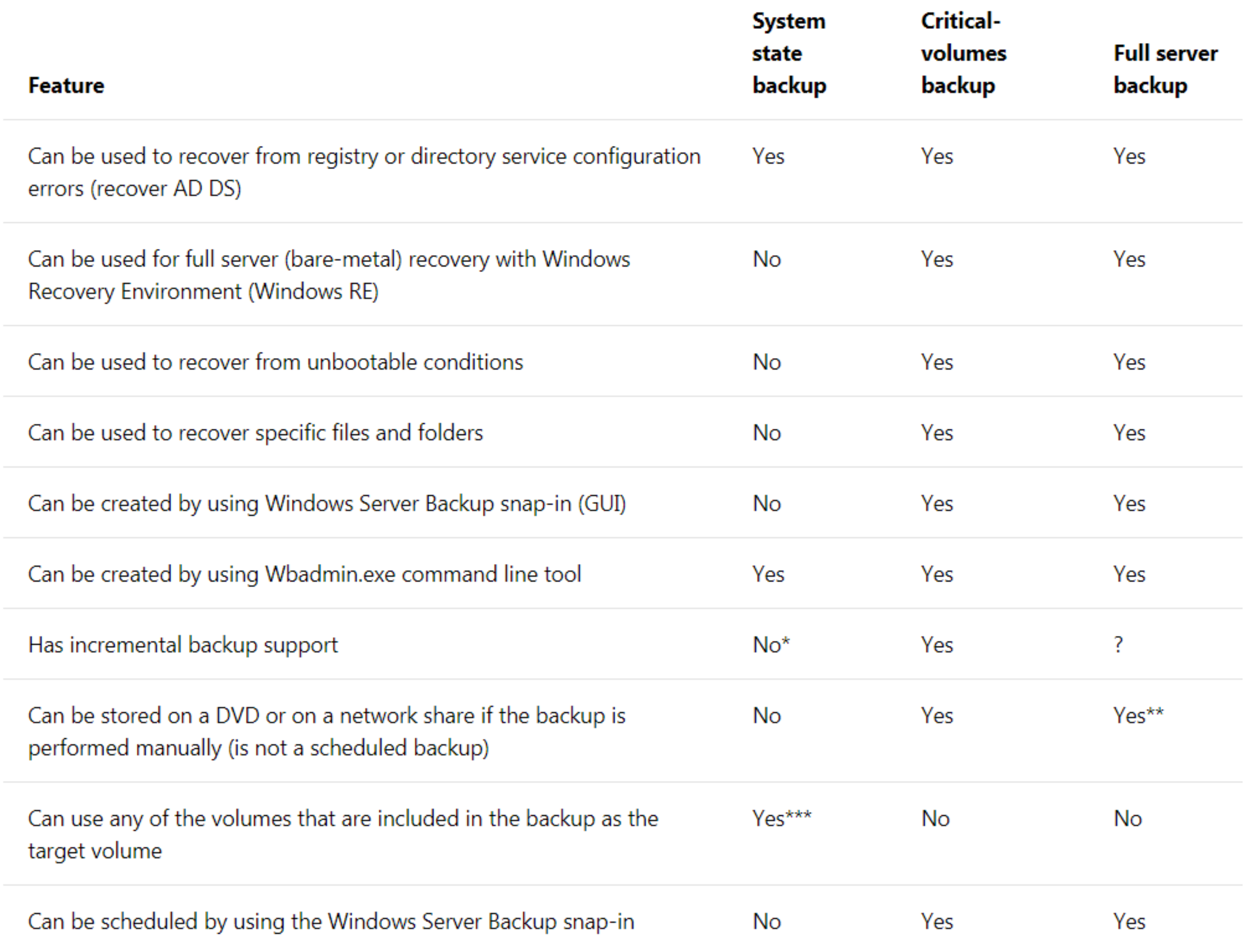


Picture 10. THAD1 server performance under workday load. (Picture: Lassi Latva-Nirva).

6.2.4 Backup Schedule

When backing up an Active Directory Server, some things are not so straightforward. It is possible to use the Windows Server Backup tool or some other solution. For example, the server has to restart into active directory recovery mode, and after the recovery, the forest will take a few steps to get fully recovered. Some backup solutions do not require such things but to avoid failures in the future it might be a good idea sometimes to build a new server and replicate the Active Directory from another Active Directory server in the domain. In Picture 11 below can be seen what is backed up and what is not when backing up with Windows Backup Role.

To use Windows Server Backup tools, Windows Server Backup Features are needed. There are two possibilities, the Windows Server Backup with a graphical user interface which is available on the Administrative Tools menu or the Command-line tool without the graphical user interface. This option uses PowerShell. Both of these options can be used to take backups; in this thesis, the graphical version is in use.



Feature	System state backup	Critical-volumes backup	Full server backup
Can be used to recover from registry or directory service configuration errors (recover AD DS)	Yes	Yes	Yes
Can be used for full server (bare-metal) recovery with Windows Recovery Environment (Windows RE)	No	Yes	Yes
Can be used to recover from unbootable conditions	No	Yes	Yes
Can be used to recover specific files and folders	No	Yes	Yes
Can be created by using Windows Server Backup snap-in (GUI)	No	Yes	Yes
Can be created by using Wbadmin.exe command line tool	Yes	Yes	Yes
Has incremental backup support	No*	Yes	?
Can be stored on a DVD or on a network share if the backup is performed manually (is not a scheduled backup)	No	Yes	Yes**
Can use any of the volumes that are included in the backup as the target volume	Yes***	No	No
Can be scheduled by using the Windows Server Backup snap-in	No	Yes	Yes

Picture 11. Use this picture to determine which backup type to use. (Picture: Microsoft).

The frequency of backups depends on criteria that vary for own Active Directory environments. In most Active Directory environments multiple changes happen during the day. Users, administrators and servers and computers running in the network create changes. These changes can be to the group policy or adding a new machine or user to the domain, also when the password has changed. In most working places the password has to be replaced every 30 days. So in a large company with many users, there is a good chance that somebody has a password change or account might expire which creates a change in Active Directory every single day.

In this environment, backup runs from Monday to Friday every day at 18:00. Windows Server Backup does not support incremental backups, so full backup runs every day. Windows Server Backup can take System state backup which includes all the files that are required to recover AD DS. Such as Active Directory Domain services database and the System Volume, as well all registry settings on the computer. The server can also take Critical volumes backup, which includes all system state files. For Veeam full backup is run every Sunday at 17:00 and incremental backups daily from Monday to Friday.

The server is backed up to either an external hard drive or THBACKUP server. There are six generations of backups made weekly, and storing time for them is a month. A yearly backup is made 1.1.20xx and stored for seven years at the time.

There are four types of backup schedules set for THAD1:

- local backup to external HDD, created with Windows Server Backup
- network share backup, created with Windows Server Backup
- local backup to external HDD, created with Veeam Agent
- network share backup, created with Veeam Agent.

6.2.5 Recovery Time Objective

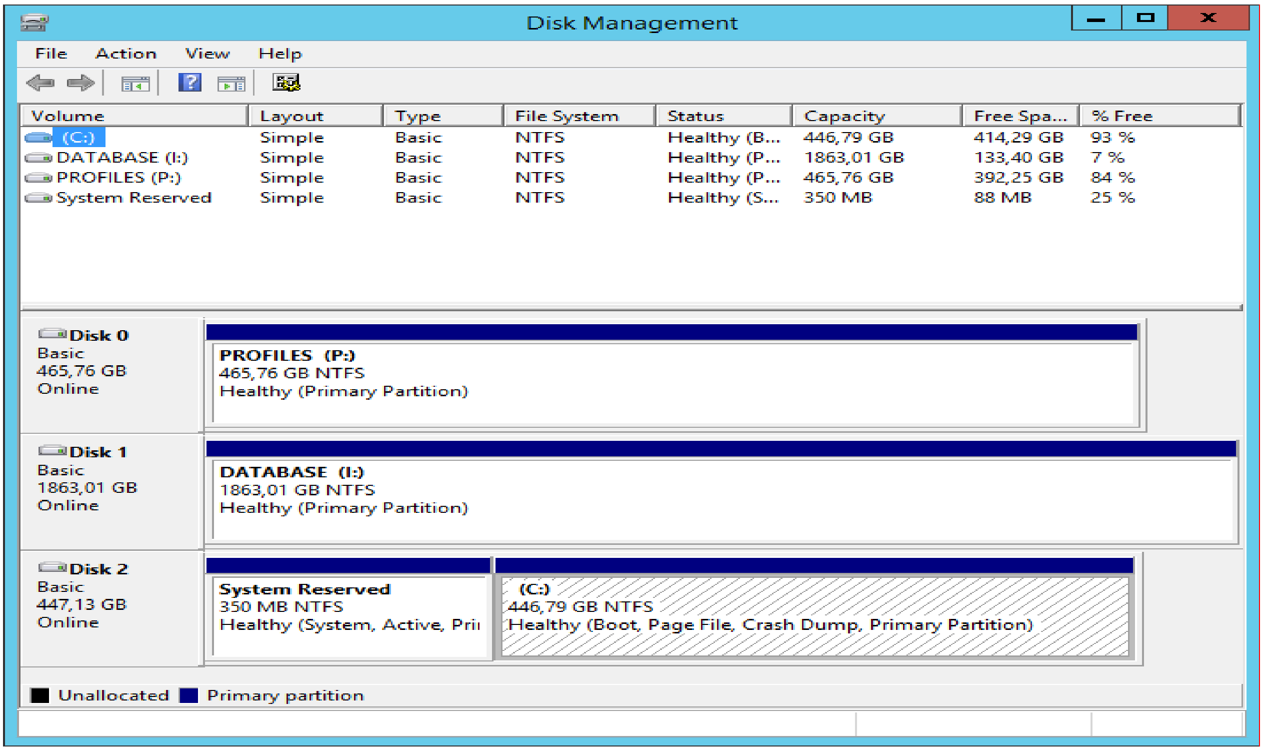
Availability is critical for an AD-server, restore should start immediately, and the server recovered as soon as possible. The time window for recovery is six hours.

6.3 THDATA

Acting as a file server, THDATA runs Windows Server 2012 R2 with 16GB of memory and an Intel(R) Core(TM) i5-4590 CPU. THDATA also stores the backups taken from THBACKUP.

6.3.1 Disk Usage

There is C: drive configured from two Solid State drives that are in RAID 1. There are also four disks that have been set in RAID 5 and is used for Database I: drive. I: is for storing public files and backups taken from THBACKUP. The last one Disk 0 P: Profiles is for User profiles this has been created from two solid state drives like C: drive. Refer to Picture 12 below for more information.



Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free
(C:)	Simple	Basic	NTFS	Healthy (B...	446,79 GB	414,29 GB	93 %
DATABASE (I:)	Simple	Basic	NTFS	Healthy (P...	1863,01 GB	133,40 GB	7 %
PROFILES (P:)	Simple	Basic	NTFS	Healthy (P...	465,76 GB	392,25 GB	84 %
System Reserved	Simple	Basic	NTFS	Healthy (S...	350 MB	88 MB	25 %

Disk 0
Basic
465,76 GB
Online

PROFILES (P:)
465,76 GB NTFS
Healthy (Primary Partition)

Disk 1
Basic
1863,01 GB
Online

DATABASE (I:)
1863,01 GB NTFS
Healthy (Primary Partition)

Disk 2
Basic
447,13 GB
Online

System Reserved
350 MB NTFS
Healthy (System, Active, Pri

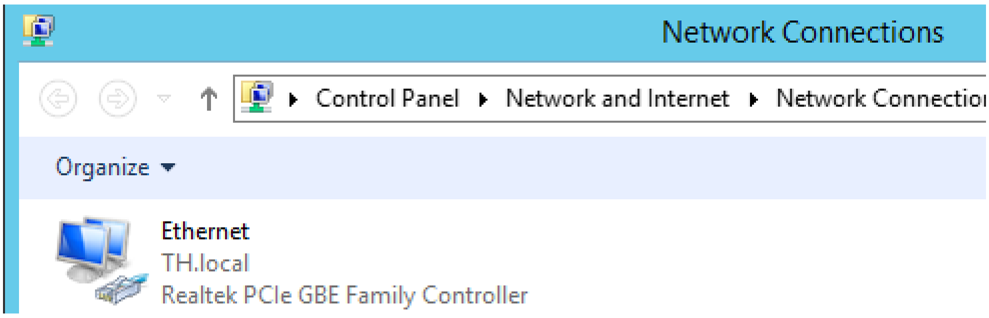
(C:)
446,79 GB NTFS
Healthy (Boot, Page File, Crash Dump, Primary Partition)

■ Unallocated ■ Primary partition

Picture 12. Disk Management windows of THDATA server. (Picture: Microsoft Windows Server 2012 R2).

6.3.2 Network Setup

There is only one Ethernet port on the server installed. If there were more network cards, NIC-teams could be made to improve reliability and performance on the server. Picture 13 shows the Network Connections on the THDATA server.

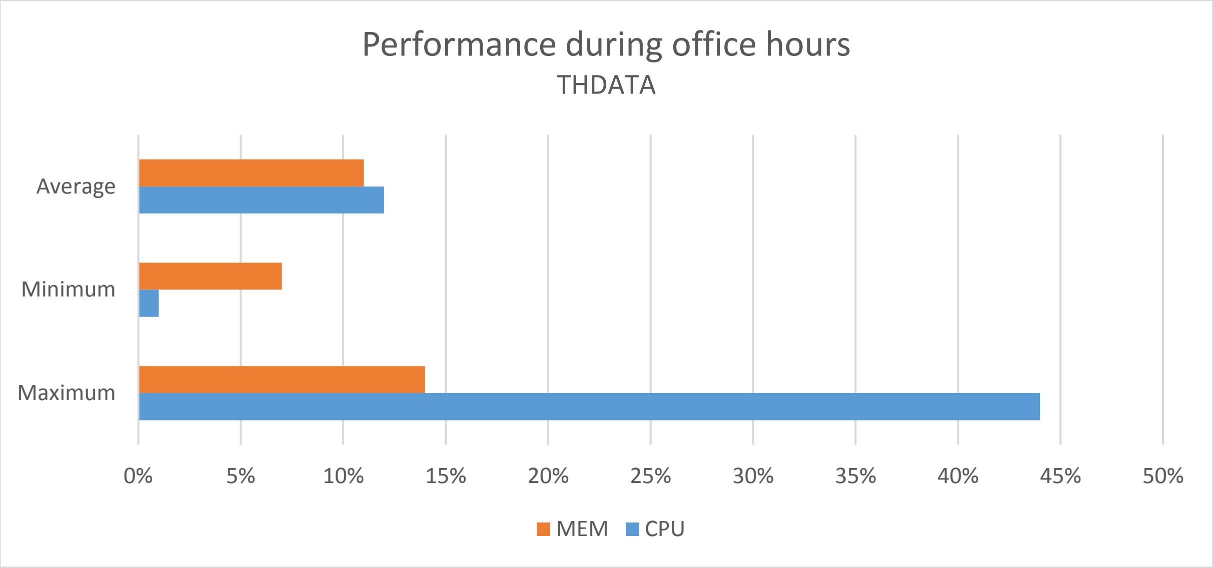


Ethernet
TH.local
Realtek PCIe GBE Family Controller

Picture 13. Network Connections on THDATA server. (Picture: Microsoft Windows Server 2012 R2).

6.3.3 Performance During Working Hours

The server uses about 12% of its processing power during office hours and 11% of its memory on average. Picture 14 shows the graph of performance during office hours.



Picture 14. Performance during office hours on THDATA server. (Picture: Lassi Latva-Nirva)

6.3.4 Backup Schedule

Backup runs from Monday to Friday every day at 19:00. Windows Server Backup does not support incremental backups, so full backup runs every day. For Veeam full backup is run every Sunday at 16:00 and incremental backups daily from Monday to Friday.

The server is backed up to either an external hard drive or THBACKUP server. There are six generations of backups made weekly, and storing time for them is a month. A yearly backup is made 1.1.20xx and stored for seven years at the time.

There are four types of backup schedules set for THDATA:

- Local backup to external HDD, created with Windows Server Backup

- Network share backup, created with Windows Server Backup
- Local backup to external HDD, created with Veeam Agent
- Network share backup, created with Veeam Agent

6.3.5 Recovery Time Objective

Availability is critical for File-server, restore should start immediately, and the server recovered as soon as possible. The time window for recovery is four hours.

7 Results of Backup Testing

The testing methods used vary depending on a device and the goal. The CPU, memory, disk and network usage are measured. Furthermore, the time to take a backup and the time of recovery is measured.

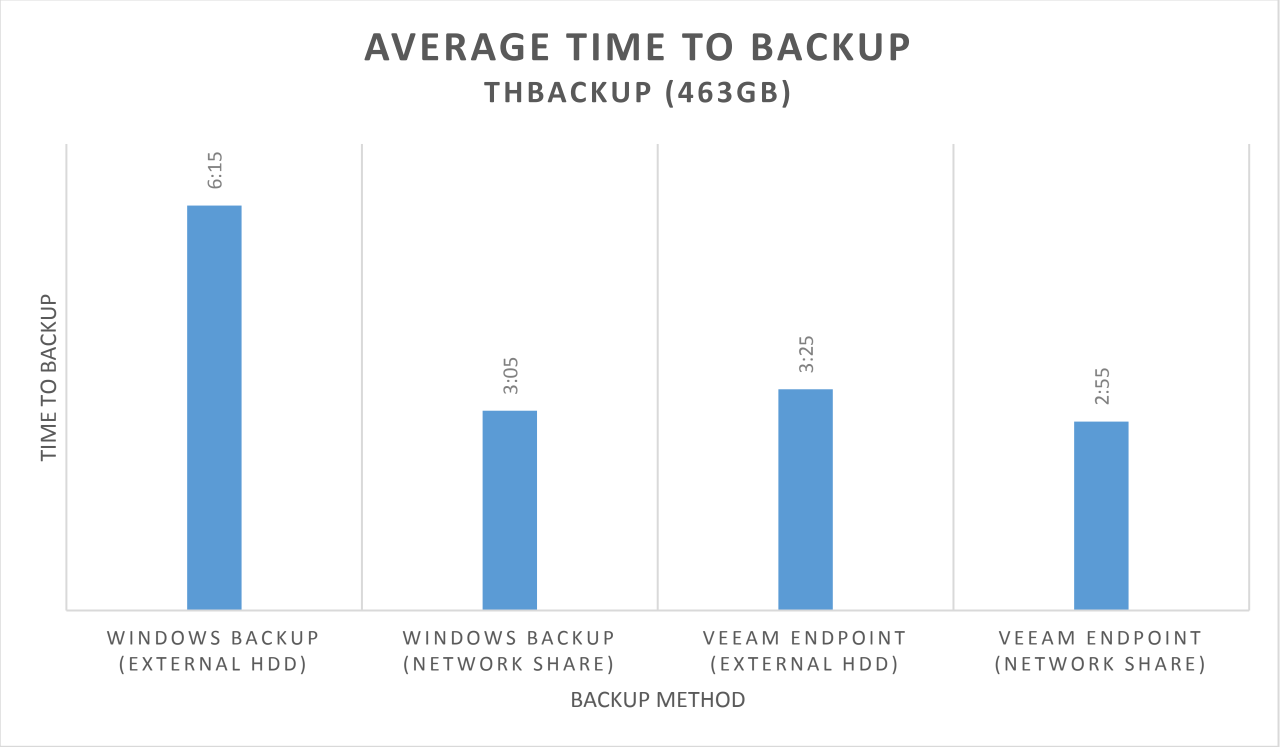
7.1 THBACKUP

The backup was run a total of 264 times during the six month testing period. It is simulating the backup schedule mentioned in chapter 6.1.4. Windows backup role does not support incremental backups, so it is deployed as a full backup.

Backup is fully automated using any of the methods. Backups are not encrypted. Encryption is possible when changing the setting.

7.1.1 Average Backup on THBACKUP Server

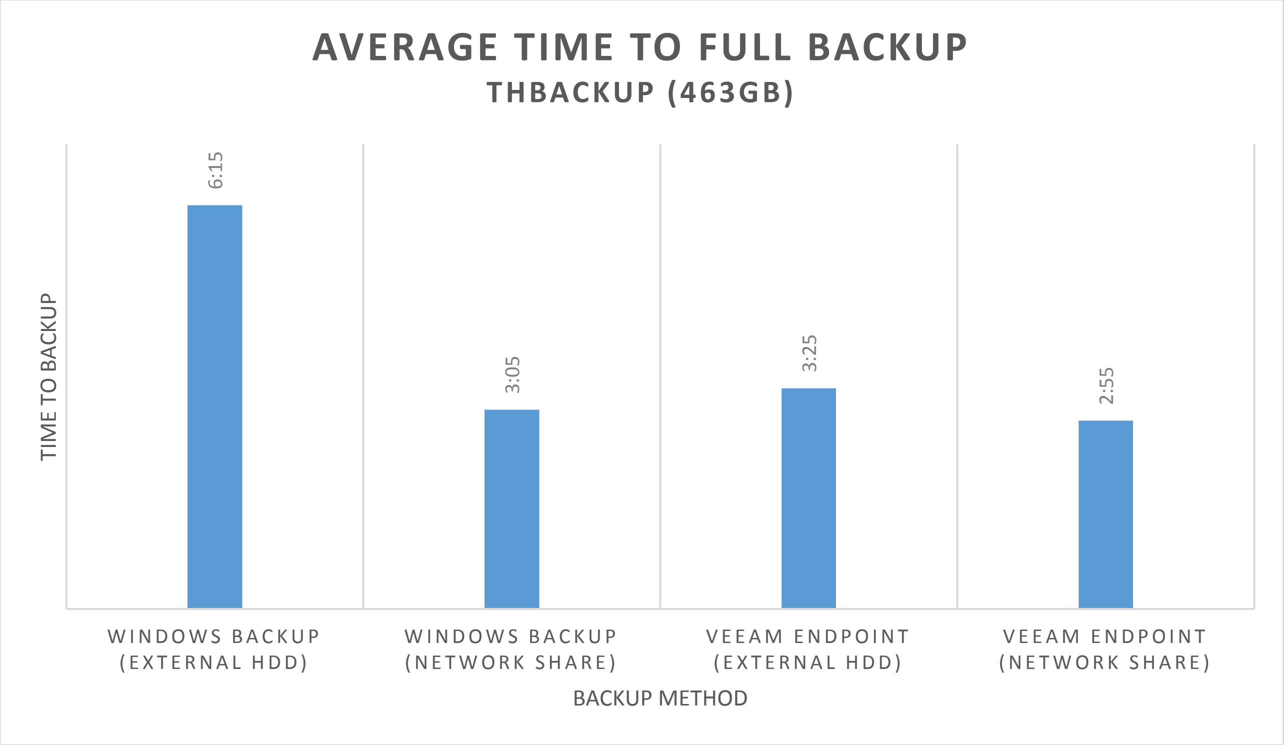
Results show that the fastest way to back up the THBACKUP server was with the Veeam agent that stored the backup on THDATA server. With an hour and one minute later backup using the Veeam agent that backed up data on the external hard drive was complete. The slowest backup method that took six hours and 15 minutes was when using the Windows Backup role to backup on the external hard drive. As shown in Picture 15 the average times have a big difference when backing up large amounts of data.



Picture 15. THBACKUP servers average backup times. (Picture: Lassi Latva-Nirva).

7.1.2 Full Backup on THBACKUP Server in Average

Results show that when taking a full backup on THBACKUP server, the fastest way is to make a backup with Veeam Agent and use a network share, in this case, our THDATA server. As the Picture 16 shows, the fastest backup was made in two hours and 55 minutes as the slowest was the Windows Backup role with the completion time of six hours and 15 minutes.

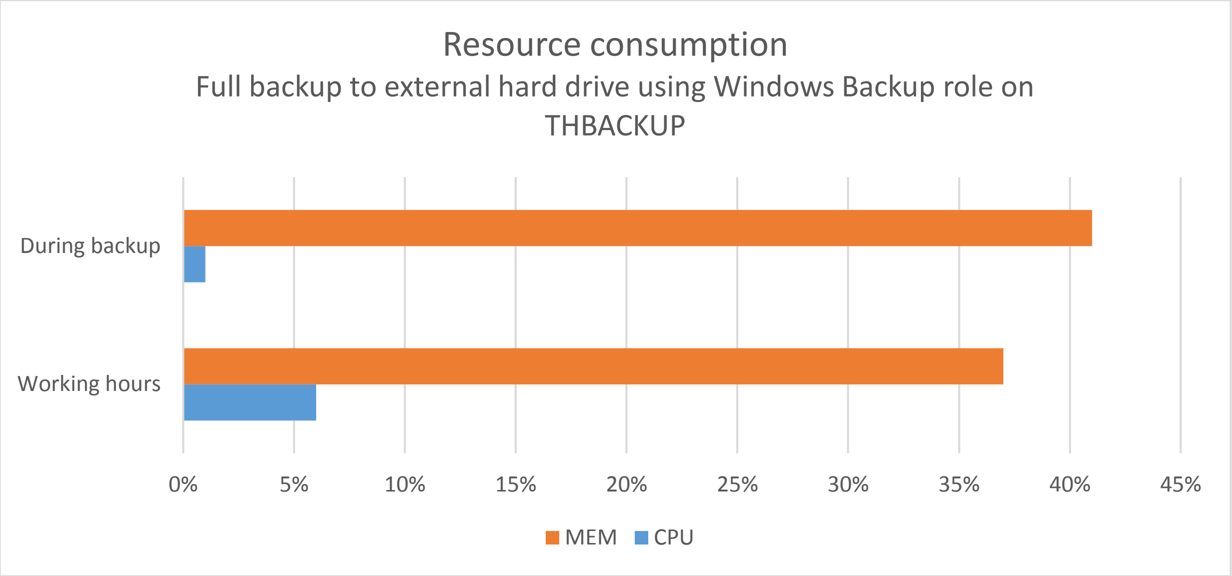


Picture 16. THBACKUP servers average full backup times. (Picture: Lassi Latva-Nirva).

7.1.3 Full Backup on THBACKUP With Windows Backup to External HDD

The first test method was carried out to take a full backup with the Windows backup role and backing up data on an external hard drive, and the results can be seen in Picture 17.

There was no effect on the CPU performance during the backup; it was even lower than during the office hours. Processor usage stayed at 1% during the full backup and memory was also quite stable at 41%.



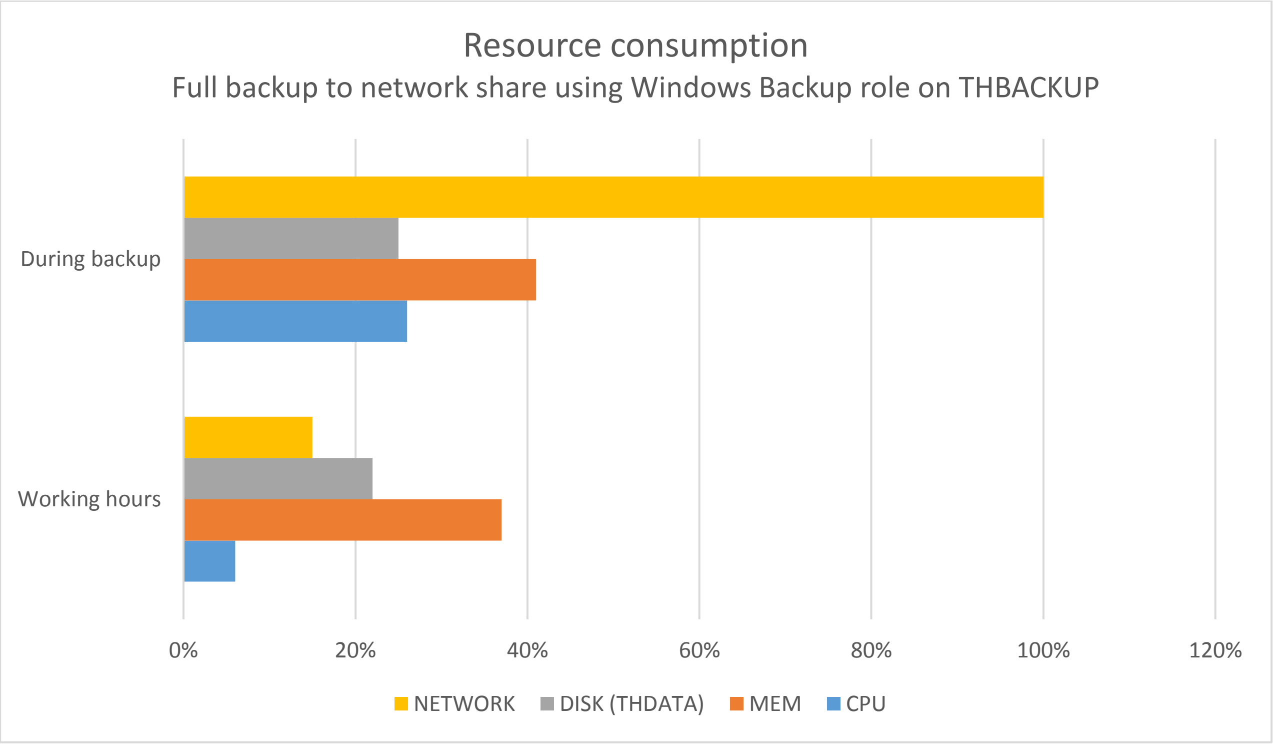
Picture 17. Resource consumption while using method one to run a full backup on THBACKUP server. (Picture: Lassi Latva-Nirva).

In Picture 17, the behavior of CPU and memory utilization of the THBACKUP server can be seen. These are the average values of the five sets of fifty test batches performed. Both CPU and memory utilization have not been impacted too much under backup load. This experiment has been made during working hours and outside working hours. The test users did not report anything during the backup time of six hours and 15 minutes when the test was taken during office hours with higher loads. Looking at Picture 17, it can be stated that the CPU had less utilization when creating a backup than during the office hours though both are under 10% of the CPU utilization values at both times. The test values were gathered with a performance monitor on the Windows Server. With this setup, it seems that it is entirely safe to take a backup during the office hours.

7.1.4 Full Backup on THBACKUP With Windows Backup Role to a Network Share

The second test method was carried out to take a full backup with the Windows backup role and backing up data on the network share. The network share was on THDATA which had a one-gigabyte connection. The results can be seen in Picture 18.

The measurement is made the same way as mentioned in the first test method. This time the disk usage and network have been taken into account when transferring files over the systems. The CPU utilization has been impacted, and there is a clear change in the network load. Memory usage was the same as in the first test type. Looking at Picture 18 can be clearly stated that CPU and network utilization have increased. Resource monitor gave values that marked CPU utilization in the ambit of 1-26% and network utilization in the range of 95-100% which caused concern because, during the over three-hour backup, the whole network was jammed. Logging in took serval minutes, and transferring files was impossible. If this had been a real office and not a test site, almost a whole working day would have gone by with users unable to work. Things might be different if the network was more capable of handling the moving of large backups.

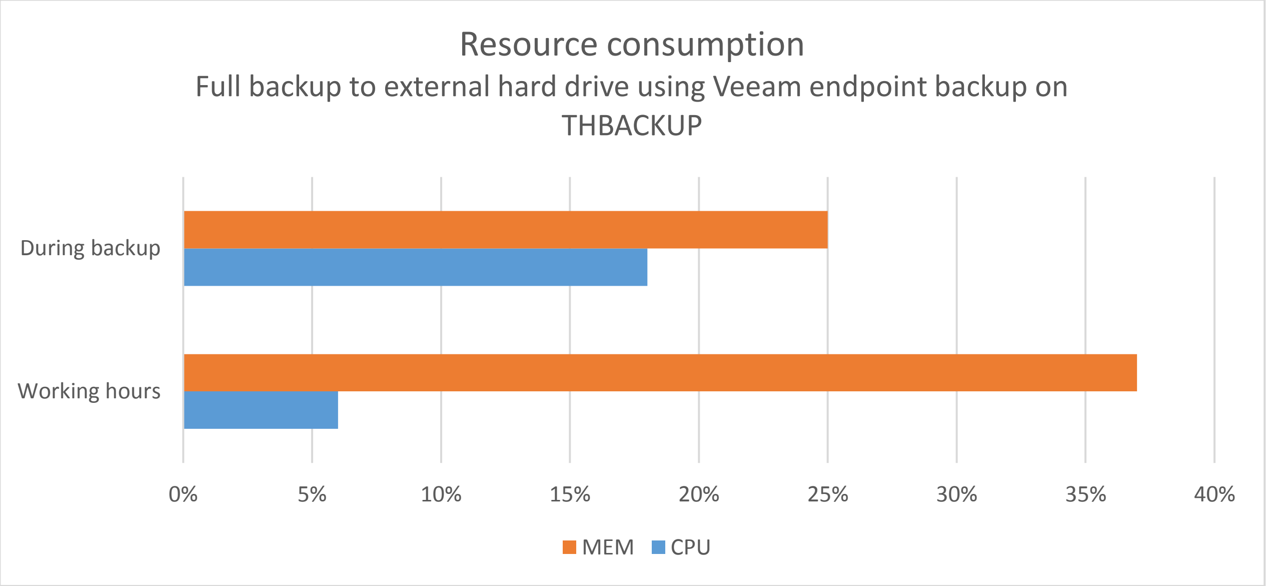


Picture 18. Resource consumption while using method two to run a full backup on THBACKUP server. (Picture: Lassi Latva-Nirva).

7.1.5 Full Backup on THBACKUP With Veeam Endpoint Backup to External HDD

The third test method was to take a full backup with the Veeam Endpoint backup and back up data on an external hard drive.

In Picture 19, the behavior of the CPU and memory utilization of the THBACKUP server can be seen. These are the average values of the five sets of fifty test batches performed, and the remaining 16 tests were used as checksums. It can be stated that during the backup the server had less memory utilization than during working hours or the previous two test methods. Values range between 18%-37% whereas the performance of the server during office hours is over 35% at most of the time. The Windows backup role may have more impact on the memory when the Veeam relies on CPU performance which is increased when compared to the working hour's load.



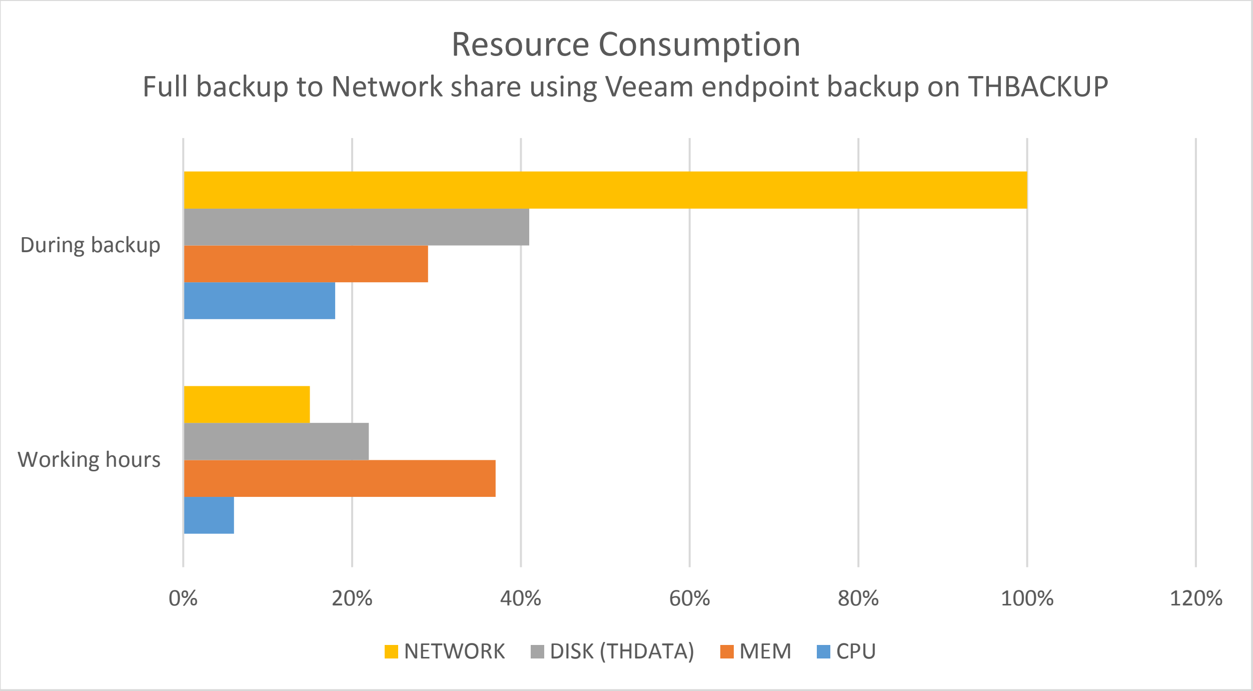
Picture 19. Resource consumption while using method three to run a full backup on THBACKUP server. (Picture Lassi Latva-Nirva).

In conclusion, there was minimal effect on the server performance, and the test users did not report anything during the backup time of three hours and 35 minutes. With this setup, it seems that it is entirely safe to take a backup during the office hours. These values were made with the Windows servers performance tool.

7.1.6 Full backup on THBACKUP with Veeam Endpoint to a Network Share

The final test method was to take a full backup with the Veeam Endpoint backup and back up data on the network file share.

In Picture 20 below, there was minimal effect on the server performance during the backup. Processor usage varied from 1% to 18%, and memory usage was a little less than during working hours load and a few percentages more than during method three.



Picture 20. Resource consumption while using method four to run a full backup on THBACKUP server. (Picture: Lassi Latva-Nirva).

7.2 THAD1

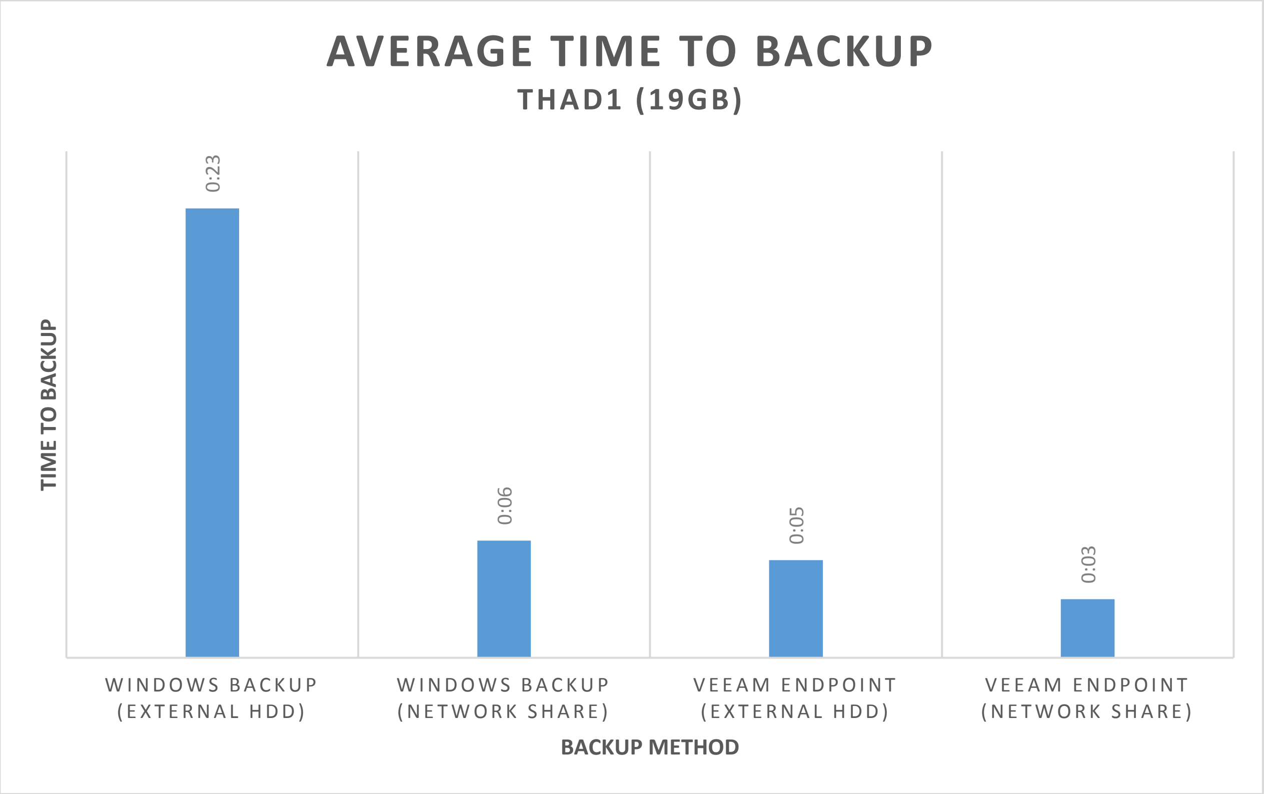
A full backup was carried out 264 times and the average of each 50 test batches was taken. The over going 14 values were used as a checksum. The tests were performed during the six month testing period. It is simulating the backup schedule mentioned in chapter 6.2.4. Windows backup role does not support incremental backups, so it is deployed as a full backup. Backup failed once on every type of run due to corrupted data, which was removed, and after that backup was run successfully.

Backup is fully automated using any of the methods. Backups are not encrypted. Encryption is possible when changing the setting.

7.2.1 Average Backup on THAD1 Server

On all of the tests of a full backup, Windows backup to External HDD was exceedingly time-consuming when compared to any other test methods, where the time taken was between three to six minutes in a range in average. With Veeam the time lies between three minutes and five minutes, with not much difference. With Windows backup role the time lies between six and 23 minutes.

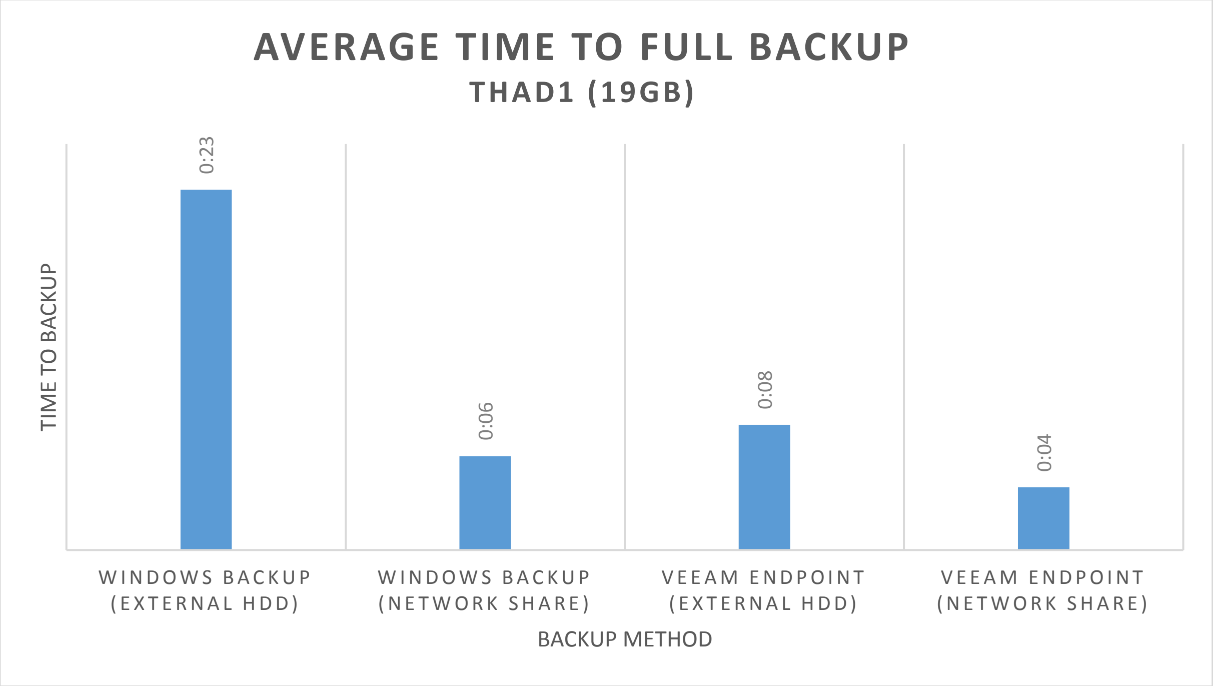
Results show that it requires less time if the backup is taken with Veeam agent that stores the backup on THBACKUP server since it is the fastest way to back up the THAD1 Active Directory server. Not far behind, with a two-minute difference came the Veeam agent that backed up data on the external hard drive. The backup method that required the most time, 23 minutes was using the Windows Backup role to backup on the external hard drive. The values plotted for all the test methods can be shown in Picture 21.



Picture 21. Time to backup THAD1 server on average. (Picture: Lassi Latva-Nirva).

7.2.2 Full Backup on THAD1 Server in Average

The time taken to carry out Full backup operation in Windows Backup role to external Hard drive was unquestionably higher when compared to the time taken on any other method with the same amount of data being backed up. The average values are used to plot the graph in Picture 22. Results show that when taking a full backup on THAD1 Active Directory server, the fastest way is to make a backup with Veeam Agent and use a network share, in this case, THBACKUP server. The quickest backup was made in four minutes as the slowest was the Windows Backup role with the completion time of 23 minutes, which means that the difference between most time consuming and the fastest backup was 19 minutes.

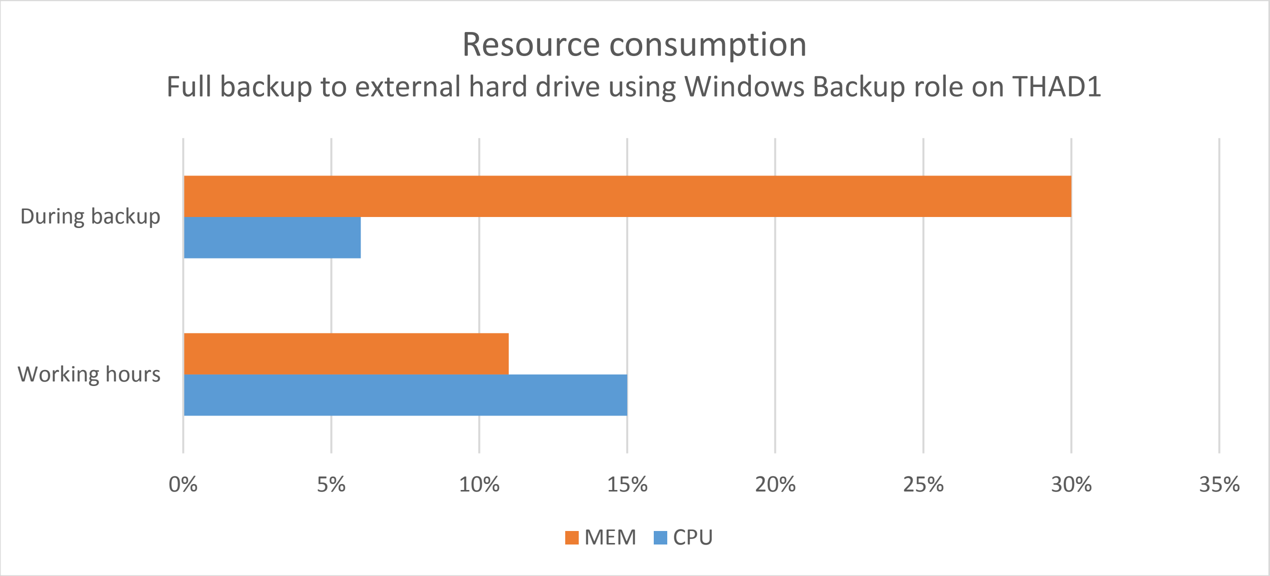


Picture 22. Time to run a full backup on THAD1 server on average. (Picture: Lassi Latva-Nirva).

7.2.3 Full Backup on THAD1 with Windows Backup to External HDD

The first test method was to take a full backup with the Windows backup role and backing up data on an external hard drive.

As Picture 23 below shows, there was minimal effect on the server performance during the backup. Processor usage was again lower than during the average office hours. And memory was quite stable at 29%-31%.



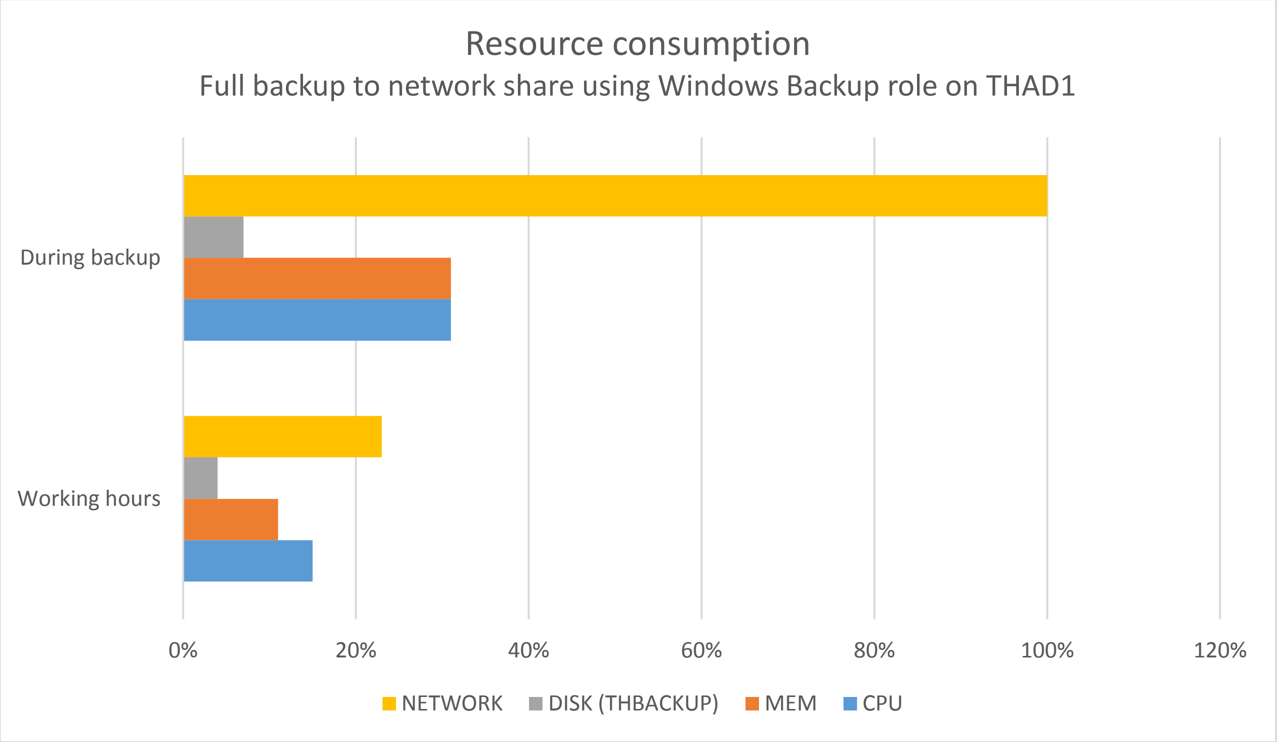
Picture 23. Resource consumption while using method one to run a full backup on THAD1 server. (Picture: Lassi Latva-Nirva).

From these results, it is noticeable that Windows backup role relies more on memory than CPU performance. The resource utilization effect on the server was comparatively low compared to working hours, and the test users did not report anything during the backup time of 23 minutes. With this setup, it seems that it is entirely safe to take a backup during the office hours.

7.2.4 Full Backup on THAD1 with Windows Backup Role to a Network Share

The second test method was to take a full backup with the Windows backup role and backing up data on the network share. The network share was on THBACKUP which had a one-gigabyte connection.

In conclusion, CPU performance was increased, but it did not cause any failures or other trouble. The memory stayed the same as in method one. What caused concern was the network latency. As Picture 24 demonstrates, during the six-minute backup, the whole network was jammed again. Logging In took serval minutes, and transferring files was impossible. Even of it was just a six-minute outage it was found very annoying amongst the users. It is not recommended to use this backup method during the office hours if the network link is only one gigabyte.

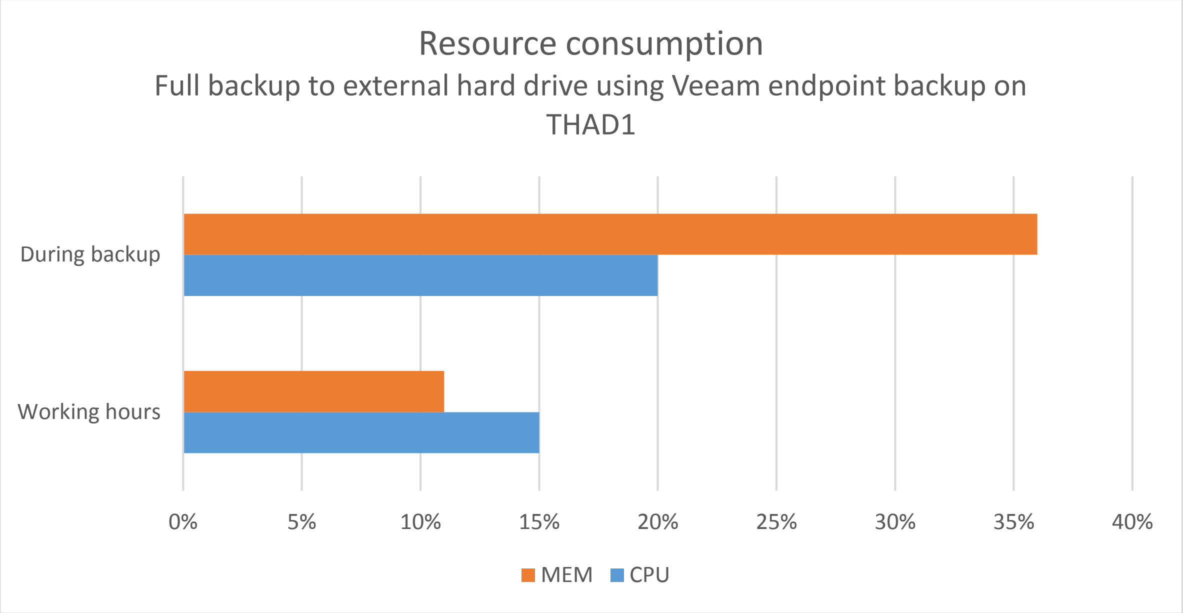


Picture 24. Resource consumption while using method two to run a full backup on THAD1 server. (Picture: Lassi Latva-Nirva).

7.2.5 Full Backup with Veeam Endpoint Backup to External Hard Drive

The third test method was to take a full backup with the Veeam Endpoint backup and back up data on an external hard drive.

As Picture 25 below shows, CPU usage was slightly increased during the backup compared to average working hours consumption. Memory usage was higher like in the second test method.



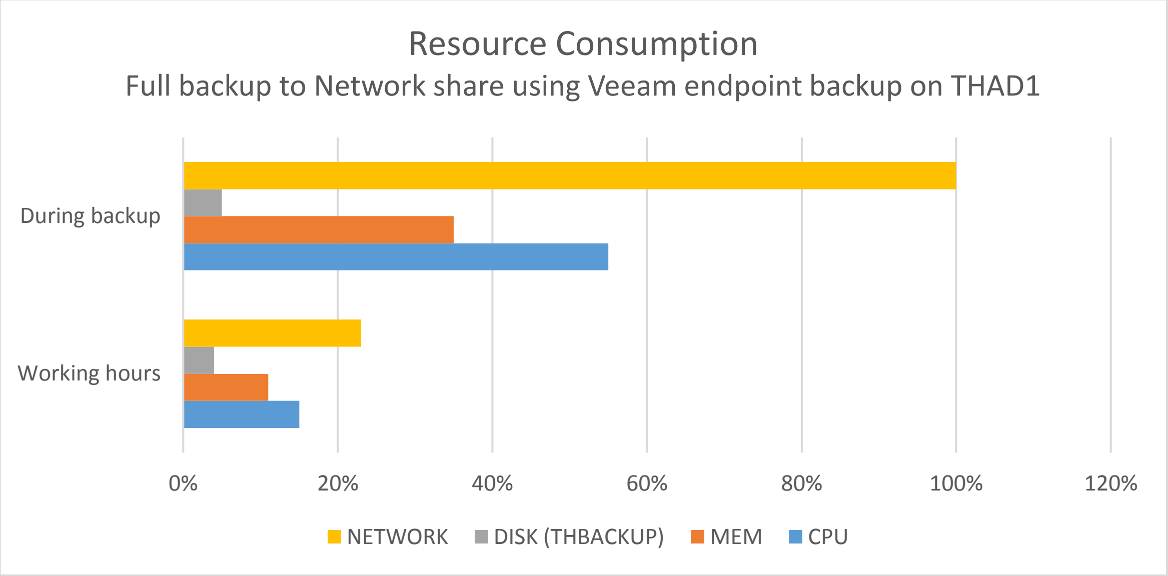
Picture 25. Resource consumption while using method three to run a full backup on THAD1 server. (Picture: Lassi Latva-Nirva).

In conclusion, there was no harm to the server, and it is safe to say that with this setup there are no problems to backup up during office hours. Of course, the best practice is to backup after office hours and during weekends if something was to go wrong.

7.2.6 Full Backup with Veeam Endpoint Backup to a Network Share

The final test method was to take a full backup with the Veeam Endpoint backup and back up data on a network file share.

As Picture 26 below shows, the network was occupied entirely during the backup transfer to THBACKUP server. The bottleneck can be seen as the disk usage on THBACKUP is only at 5%, and the network is at 100%. Network being at 100 resulted that, all other operations were hard to complete due to the lag.



Picture 26. Resource consumption while using method four to run a full backup on THAD1 server. (Picture Lassi Latva-Nirva).

In conclusion, if the network link was faster or the file transfer was to happen on another network, there would be no problem to backup during the office hours. With this setup, it is not recommended.

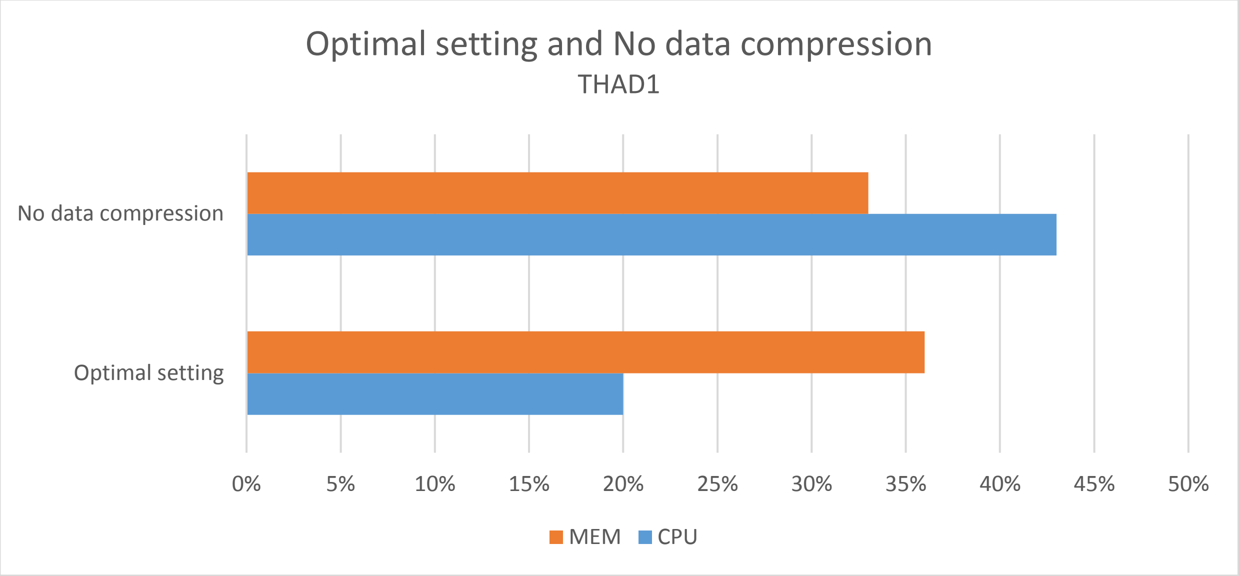
7.3 Full Backup with Different Settings of Veeam Agent on THAD1

Veeam Agent has an option to change performance settings. The following tests run on THAD1 Active Directory server using the full backup with the different options.

7.3.1 No Data Compression

The first option is to choose not to compress data. Disabling compression reduces performance due to an increased amount of data transferred to the target storage.

As Picture 27 shows, using the optimal setting performance on THAD is the memory in average usage of 36% and CPU average at 20%. During the full uncompressed backup to the external hard drive, the average CPU and Memory consumption was 43% and 33% in the range for CPU 14-73% and memory in a variety of 33%-34%



Picture 27. Resource consumption while using no data compression setting to run a full backup on THAD1 server. (Picture: Lassi Latva-Nirva).

The backup took 5:35min, which is longer than the average of four minutes using the "Optimal" setting. In conclusion, there is no slowness noticed while taking the full backup without compressing it, but it takes a longer time, and there is nothing to gain from it.

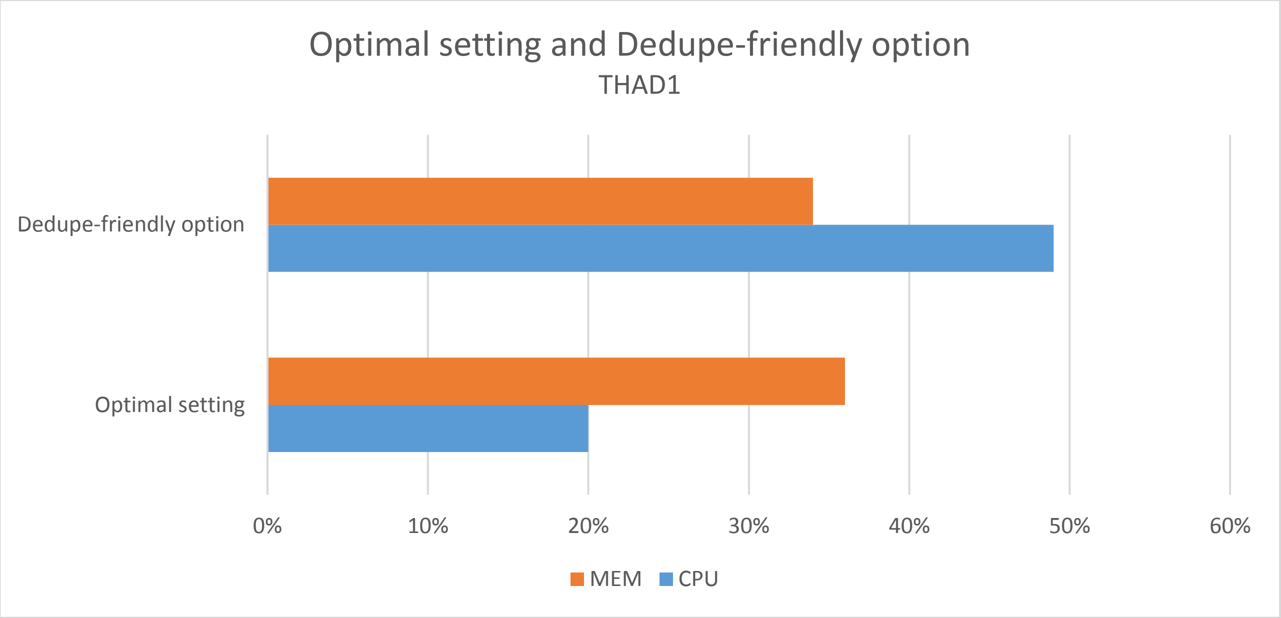
The test was also made with encryption and without it. No difference was noticed in any values measured.

7.3.2 Dedupe-Friendly

Using the dedupe-friendly option is an recommended compression level for deduplicating storage appliances and external WAN accelerators.

Like presented in Picture 28, while using this option, the backup was using an average of 49% of the CPU power in the range of 18-63% and using an average of 34% of the memory in the field of 33-35%.

The backup was faster than the uncompressed option with the time of 5:23min. Also, the restore point size was 2,9GBs smaller.



Picture 28. Resource consumption while using dedupe-friendly setting to run a full backup on THAD1 server. (Picture: Lassi Latva-Nirva).

In conclusion, there is no slowness noticed while taking the full backup using the dedupe-friendly option, it is also faster and smaller than the uncompressed option, but it is still slower than the optimal setting in average.

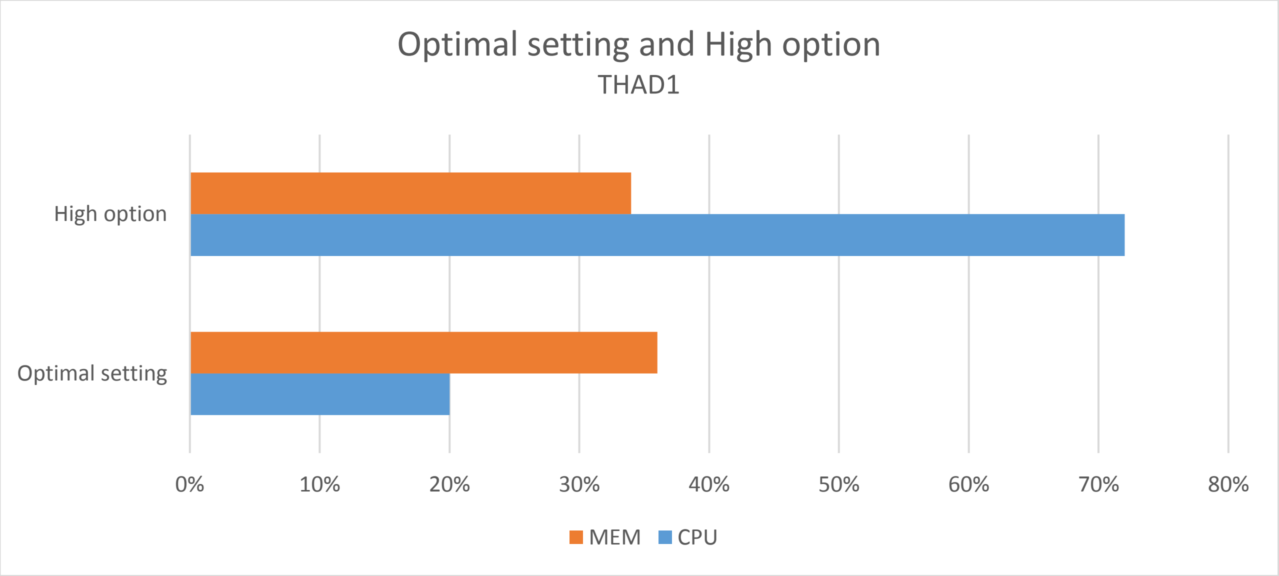
The test was also made with encryption and without it. No difference was noticed in any values measured.

7.3.3 High Option

Setting compression level to high, it provides an additional 10% compression ratio over Optimal, at the cost of 10x higher CPU usage.

While using this option, the CPU usage skyrocketed, and the average was 72% in the range of 28-97%. There was no effect on the memory consumption which stayed at an average of 34% in the field of 33-35% as can be seen in Picture 29.

The restore time was not too impressive setting the finishing time at 5:35 minutes but the restore point size was a lot smaller. It had come down from the 13,2GBs to only 6,17GBs.



Picture 29. Resource consumption while using High setting to run a full backup on THAD1 server. (Picture: Lassi Latva-Nirva).

In conclusion, there was noticeable freezing on the server. Users were unable to change the password or log in on to a new machine. It is undoubtedly a bad idea to do a full backup with compression set on high during the office hours. Using the high compression setting can save a lot of storage space at the price of the server going down for the time of the backup.

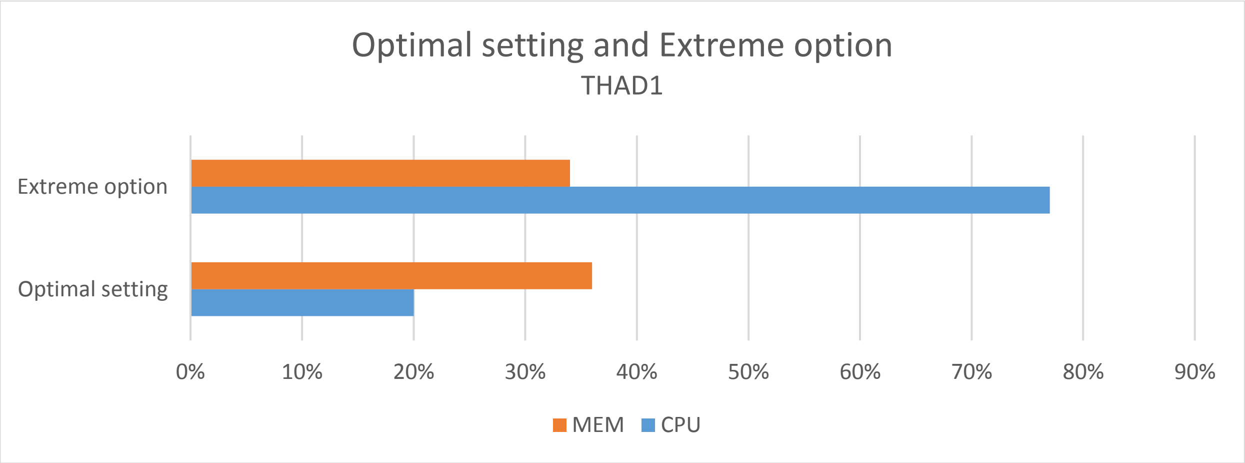
The test was also made with encryption and without it. No difference was noticed in any values measured.

7.3.4 Extreme Option

Extreme compression provides an additional 3% compression ratio over high, at the cost of 2x higher CPU usage.

While using this option the CPU usage was very high with an average of 77% and in the range of 22-100%. There was no effect on the memory consumption which stayed at an average of 34% in the field of 33-35% as can be seen in Picture 30.

The restore time was not too impressive setting the finishing time at 6:45 minutes but the restore point size was even smaller than with the previous option. It had come down from the 6,17GBs to 5,93GBs.



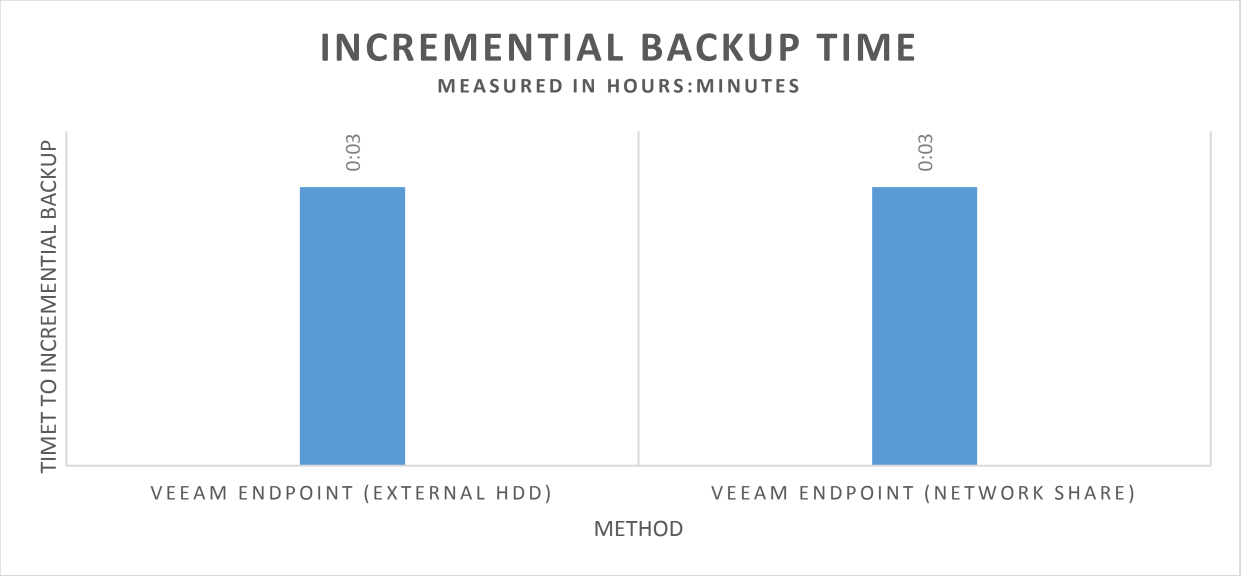
Picture 30. Resource consumption while using Extreme setting to run a full backup on THAD1 server. (Picture: Lassi Latva-Nirva).

In conclusion, there was the same kind of freezing on the server that was noticed with the high setting also. The users were unable to change the password or log in on to a new machine. It is undoubtedly a bad idea to do a full backup with compression set too high or extreme during the office hours. Using these compression settings can save some more storage space compared to the high setting option, but the server will be on very high load during the backup.

The test was also made with encryption and without it. No difference was noticed in any values measured.

7.4 Incremental Backup on THAD1

When taking the incremental backup, only Veeam Agent was capable of performing the task. The average time to make a backup was two minutes and there was no significant difference between the two options, using HDD or network share as can be seen in Picture 31.

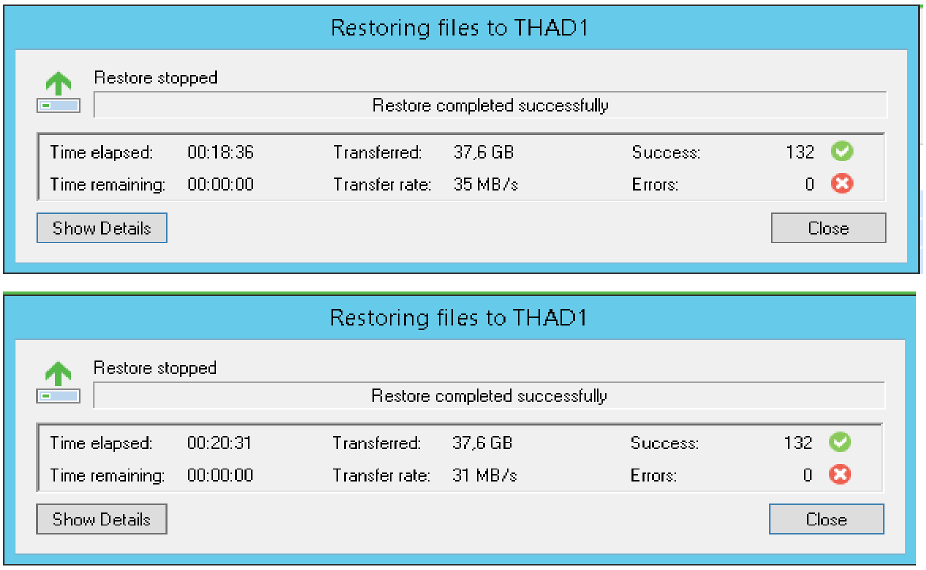


Picture 31. Incremental backup time on THAD1. (Picture: Lassi Latva-Nirva).

7.5 File-level Backup on THAD1

This test type was made using the File level backup option in the Veeam Agent. The test was made a total of 20 times using two different options in Veeam Agent. With the “Optimal” option and the “Depute friendly” option, it took about 20 minutes to a backup a 38GB folder full of files.

When recovering files, a difference was noticed. Using the Optimal option the transfer rate was faster than using the “Dedupe Friendly” option that had 4 MB/s slower transfer rate at the speed of 31 MB/s. Both restores were completed successfully, optimal in time of 18 minutes 36 seconds and dedupe friendly in 20 minutes 31 seconds. The difference can be noticed in Picture 32 below.



Restoring files to THAD1

Restore stopped

Restore completed successfully

Time elapsed: 00:18:36 Transferred: 37,6 GB Success: 132 ✓
Time remaining: 00:00:00 Transfer rate: 35 MB/s Errors: 0 ✖

Restoring files to THAD1

Restore stopped

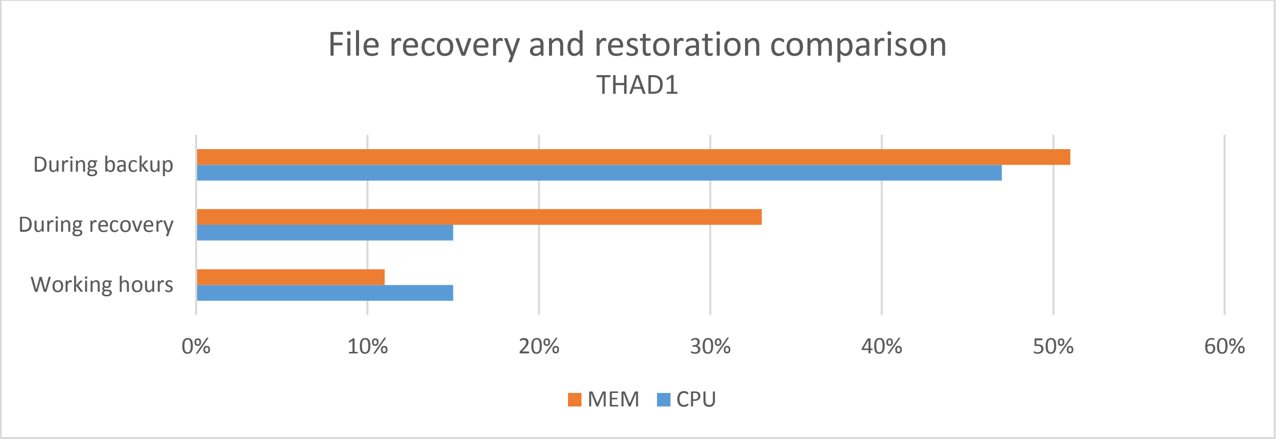
Restore completed successfully

Time elapsed: 00:20:31 Transferred: 37,6 GB Success: 132 ✓
Time remaining: 00:00:00 Transfer rate: 31 MB/s Errors: 0 ✖

Picture 32. File restore on THAD1. (Picture: Veeam agent)

The regular working performance on THAD is the memory in average usage of 11% and CPU average 15% during business hours. When running the File level backup on Veeam Agent using the “Optimal” setting the utilization of resources is at 51% on memory and 47% on CPU usage on average. During the test’s RAM was consumed at 48-51% and CPU at 37-58% usage.

When running the File level restore on Veeam Agent using the same “Optimal” setting the usage of resources is much lower. Memory consumption at an average of 33% and placed in a steady range of 32-33%. CPU consumption was also lighter with an average of 15% at 1-19%. All the values can be seen in Picture 33 below.



Picture 33. File recovery and restoration comparison on THAD1. (Picture: Lassi Latva-Nirva).

In conclusion, there is no harm to the Active Directory server if a file level backup or restore runs during the office hours. There was no delay or slowness reported during the test.

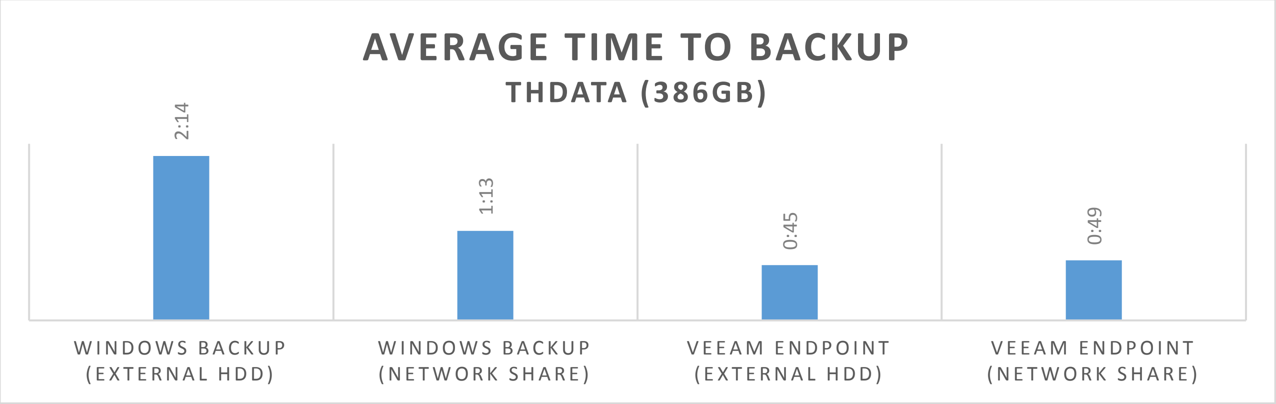
7.6 THDATA

A full backup was carried out 264 times, and the average values of each 50 of these tests were taken, and the 14 values that did not fit the 50 value batch were used as checksums. This experiment was performed for six months. It simulated the backup schedule mentioned in chapter 6.3.4. Windows backup role does not support incremental backups, so it is deployed as a full backup.

Backup is fully automated using any of the methods. Backups are not encrypted. Encryption is possible when changing the setting.

7.6.1 Average Backup on THDATA Server

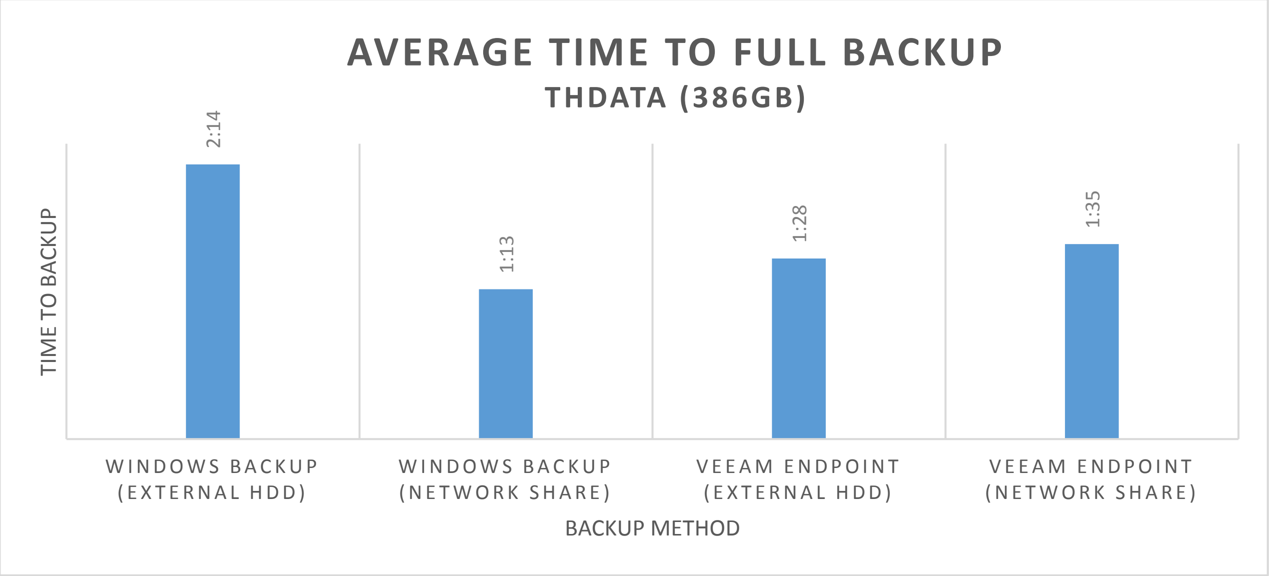
As initial value, Veeam agent that stored the backup on an external hard drive was quick when compared to Windows backup to external HDD. Veeam backed up almost as equally to both network and external hard drive. Windows backup role to network share procedure was slower when compared to Veeam agent. The differences are shown in Picture 34.



Picture 34. Time to backup THDATA server on average. (Picture: Lassi Latva-Nirva).

7.6.2 Full Backup on THDATA Server in Average

Results show that when taking a full backup on THDATA file server, the fastest way is to make a backup with Windows backup role and network share, in this case, our THBACKUP server. As Picture 35 shows, the fastest backup was made in one hour and 13 minutes as the slowest was the Windows Backup role to the external hard drive with the completion time of two hours and 14 minutes.

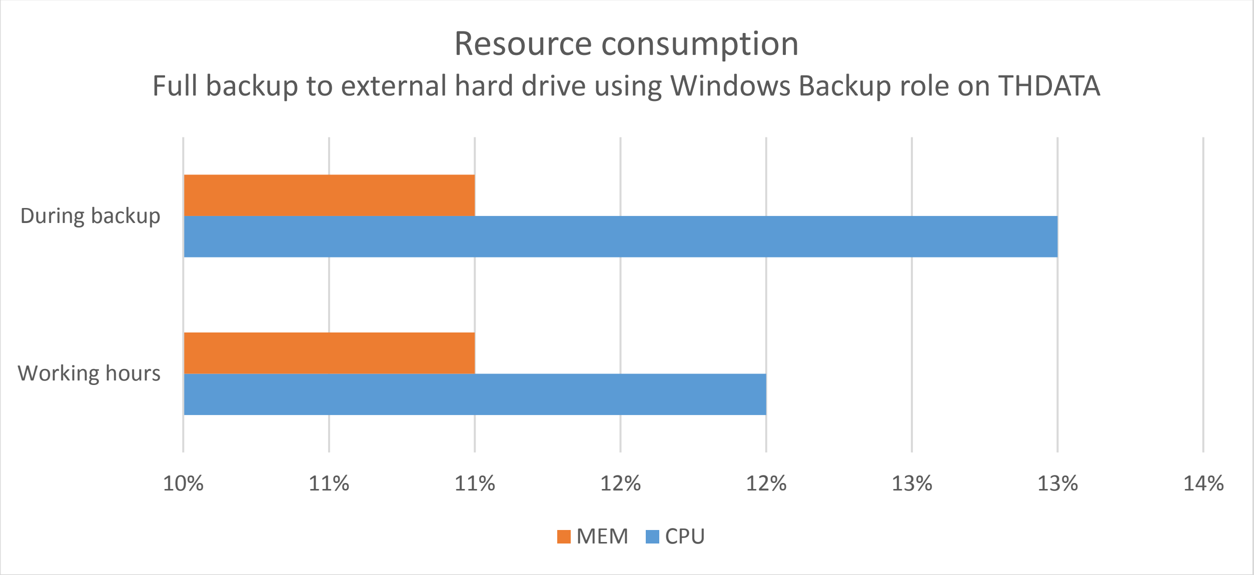


Picture 35. Time to backup THDATA server on average. (Picture: Lassi Latva-Nirva).

7.6.3 Full Backup on THDATA with Windows Backup to External HDD

The first test method was to take a full backup with the Windows backup role and backing up data on an external hard drive.

In Picture 36, resource consumption is described. It can be seen that there is no change in memory consumption compared to the working hour's usage. The CPU usage is just slightly higher.



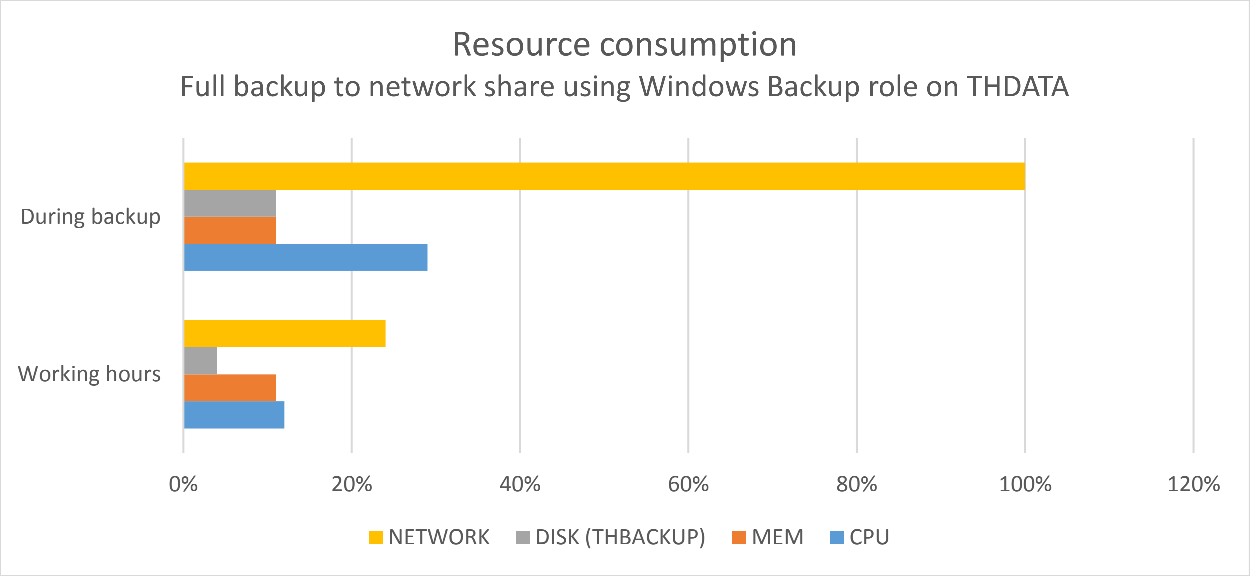
Picture 36. Resource consumption while using method one to run a full backup on THDATA server. (Picture: Lassi Latva-Nirva).

In conclusion, there was no effect on the server performance, and the test users did not report anything during the backup time of two hours and 14 minutes. With this setup, it seems that it is entirely safe to take a backup during the office hours.

7.6.4 Full Backup on THDATA with Windows Backup Role to a Network Share

The second test method was to take a full backup with the Windows backup role and backing up data on the network share. The network share was on THBACKUP which had a one-gigabyte connection.

In conclusion, CPU performance was increased. There was no change in memory consumption. The same as with every other server, the one-gigabyte link is not enough. Logging In took serval minutes, and transferring files was impossible. It is not recommended to use this backup method during the office hours if the network link is only one gigabyte. The resource consumption while using method two is defined as shown in Picture 37.

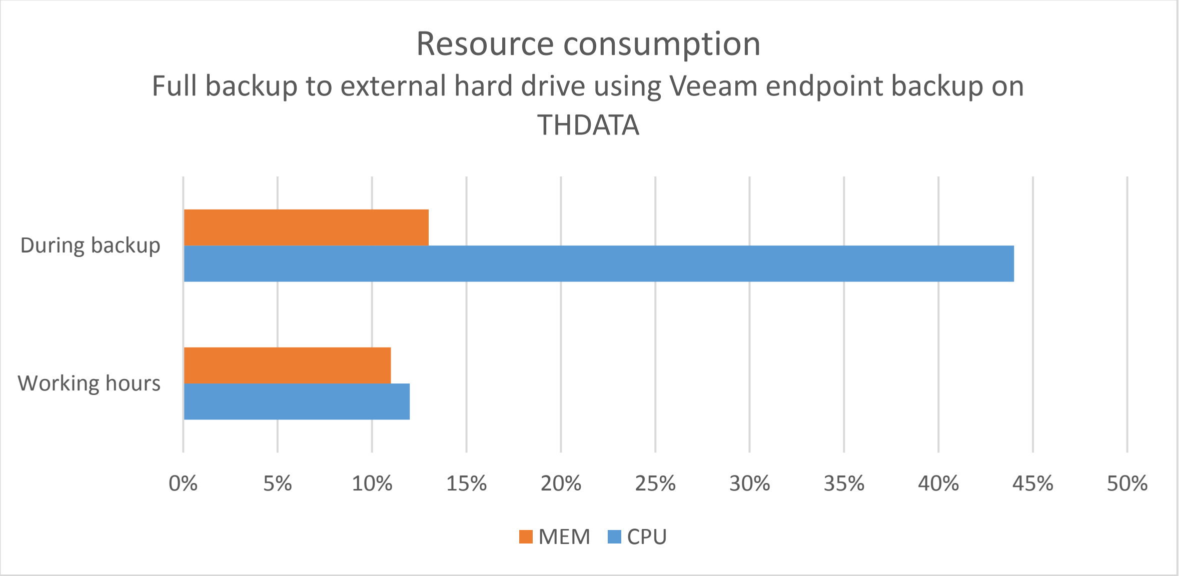


Picture 37. Network traffic is high on THDATA during backup. (Picture: Lassi Latva-Nirva).

7.6.5 Full Backup with Veeam Endpoint Backup to External Hard Drive

The third test method was to take a full backup with the Veeam Endpoint backup and back up data on an external hard drive.

In Picture 38, resource consumption for method three is described. The CPU usage increased during the backup. Memory usage did not change much.



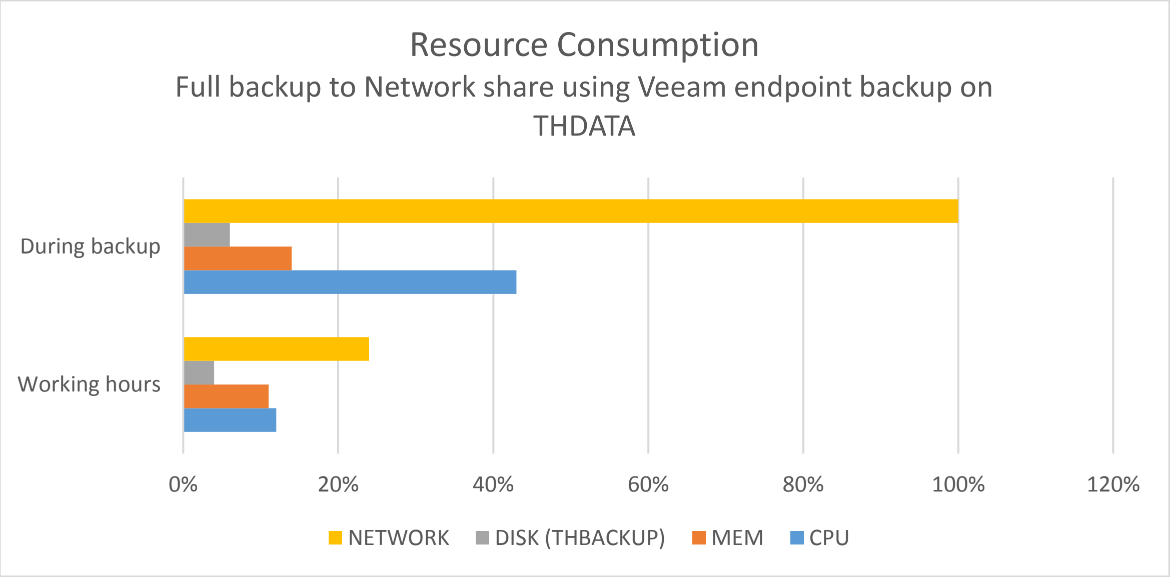
Picture 38. Resource consumption while using method three to run a full backup on THDATA server. (Picture: Lassi Latva-Nirva).

In conclusion, there was no harm to the server, and it is safe to say that with this setup there are no problems to backup up during office hours.

7.6.6 Full Backup with Veeam Endpoint Backup to a Network Share

The final test method was to take a full backup with the Veeam Endpoint backup and back up data on a network file share.

As Picture 39 below shows, and we already know network was at 100% during the backup transfer to THBACKUP server. The same problems occurred as in the tests before.



Picture 39. Resource consumption while using method four to run a full backup on THDATA server.

To conclude this final test, memory is stable, and CPU noticeably increased but has no effect on the performance. The discs could handle more data, but the network slows down the file transfer.

8 Results of Recovery Testing

In this chapter, the results of recovery testing are presented. Also, an experiment of the real-life simulation was performed and is presented in this chapter.

8.1 Recovery of THBACKUP

The first server that the recovery test was performed was THBACKUP server. The backup files were stored in the THDATA server.

8.1.1 Methods One and Two

Recovering THBACKUP with Windows backup was simple enough. Some problems may arise when, for some unknown reason, the restoration files are not found on THDATA server. However with the external hard drive backup, everything should go smoothly if the recovery files are named right and in the rightful place on the external hard drive.

The time it takes to recover With Windows backup role and the external hard drive was seven hours and eight minutes. When using a network share, it was only four hours.

8.1.2 Methods Three and Four

With Veeam the recovery is somewhat more complicated. With a backup role, the server installation media can be used, for example, but with Veeam a recovery media has to be created on USB drive or DVD. It is worth noticing that the media has to be generated before the disaster occurs.

When the server needs to be recovered. It is booted from the recovery media, the hard drives must be wiped clean before Veeam can recover any partitions on them. Time to recover using external hard drive was four hours and six minutes, and with the network share, it takes three hours and 30 minutes.

8.2 Recovery of THAD1

When a domain controller is corrupted or has failed, there are serval options for the system recovery. The possibilities are authoritative restore, nonauthoritative restore, or installing the server as new and promoting it to a domain controller.

8.2.1 A Real-Life Simulation

For the recovery of THAD1, a test among two test groups of two students was arranged. The test was made to simulate a real-life incident happening and how an untrained IT personnel with basic IT-skills (2-4 years of education, some working background) would perform. The test students were given all the necessary information about the network environment including Visio graph of the servers containing server names, IP-addresses, and account information. The students were not given any information about the nature of the disaster about to occur. The test was timed from the start of the failure to the successful recovery. The test began with everything being as usual.

8.2.2 Test Group One

The first test group had a background of two years of education and some working experience.

0:00 Test begins
The timer has not been started as everything is normal.

0:01 Hard drive fails in THAD1
Hard drive fails in THAD1 and the timer starts.

0:05 The incident has been noticed
Five minutes after the failure it has been reported.

0:09 A new hard drive has been installed on THAD1
A new hard drive is now in use, and the server installation media is ready.

0:10 The recovery media loads
The server has been booted on the recovery media.

0:11 The recovery settings are set

The recovery wizard has been completed.

0:12 A problem occurs

A problem that prevents the server from starting the recovery has occurred.

0:18 Problem is under investigation

The problem is being investigated, and it seems like an authentication issue.

0:28 The recovery has failed using method two

Secondary Active directory server does not work as it should.

0:33 Decision is made

A decision is made not to try to fix the THAD2 server, but to get the recovery media for VEEAM which is stored offsite.

0:55 Backup media arrives

Backup media has been retrieved from the storage location.

0:57 Recovery media loads

The recovery media for Veeam recovery loads.

1:00 One hour since the incident occurred

The settings are input to the recovery wizard.

1:01 A problem occurs

Group one realizes that they have picked a wrong size disk when replacing the old one.

1:10 The disc is changed

The drive is replaced and the recovery media loads.

1:12 Entering settings

Inputting settings in the recovery wizard.

1:16 A problem occurs

The disc was used, Veeam cannot partition a drive with previous partitions.

1:17 Boot N Nuke is used

Boot N Nuke is to erase the partitions.

1:24h Recovery media loads

Recovery media loads once again.

1:28h Entering settings

The settings are entered.

1:29h Recovery starts

The recovery finally starts.

1:39h Recovery is made

The recovery is made and server boots.

1:41h A problem occurs

The server seems unstable.

1:44h Bluescreen

The server crashes.

1:48h A decision is made

The backup method one is now in action.

1:49h The recovery media loads

Loading the recovery media from server install USB drive.

1:50h Entering settings

Entering settings to the recovery wizard.

1:51h Recovery starts

Recovery starts on THAD1.

2:13h Recovery is complete

Recovery is complete and the server boots.

2:15h Done

The server has been tested and is in working condition.

8.2.3 Test group two

The second test group had a background of two to four years of education and some working experience. This group was also given the disaster recovery documentation.

0:00h Test begins

The timer has not been started as everything is normal.

0:01h Hard drive fails in THAD1

Hard drive fails in THAD1 and the timer starts.

0:05h The incident has been noticed

Five minutes after the failure it has been reported.

0:09h A new hard drive has been installed on THAD1

A new hard drive is put in its place, and the server installation media is ready.

0:10h The recovery media loads

The server has been booted on the recovery media.

0:11h The recovery settings are set

The recovery wizard has been completed.

0:12h A problem occurs

A problem that prevents the server from starting the recovery has occurred.

0:20h Problem is under investigation

The problem is being investigated, and it seems like an authentication issue.

0:35h The recovery has failed using trying to fix the server

Secondary Active directory server does not work as it should. The group seeks to fix it, but the attempts are useless without the authentication of the THAD1 server.

0:50h Still trying to fix the server

The group two is still trying to get the THAD2 to work. At the same time, one student is getting the recovery media from offsite.

1:18h A decision is made

Now using backup method one.

1:19h The recovery media loads

Loading the recovery media from server install USB drive.

1:20h Entering settings

Entering settings to the recovery wizard.

1:21h Recovery starts

Recovery starts on THAD1.

1:33h Recovery is complete

Recovery is complete and the server boots.

1:35h Done

The server has been tested and is in working condition.

8.2.4 The Conclusion of the Testing

As the test results show, if there is not a proper plan in place it can take hours to perform a recovery. When carried out correctly the restore would only have taken 10-20 minutes in total.

The test was set up so that different kind of problems could occur. The secondary Active Directory server was not promoted to be a domain controller that it could not be used to authenticate the backup.

Then the backup media that were not on the backup server were stored offsite in a different location which took time to fetch.

Lastly, there were three replacement hard drives, one that was new but with capacity too small, one used one with old server partitions inside and one brand new that was the right capacity. The purpose was to measure the accuracy of groups during the disaster.

8.2.5 Group One

The first group had less experience and was not given the backup documentation. They made some mistakes that hopefully they will not repeat in the future again. What caused time was trying to investigate the problem together instead of sending somebody to get the recovery media offsite or copying the required files from the file server.

Next, they tried to use the Veeam software for recovery, which they had no experience in using which caused the recovery to finish partially, which resulted in the server crashing.

Group one had to change the disk two times because they did not take a closer look at the possible hard drives and chose the one with less capacity that was required. Moreover, they also changed in used one as the next option and had to use third-party tools to empty it instead for going with the new one with the correct size. In the end, the server was recovered successfully.

8.2.6 Group Two

The more experienced group two was given the backup and disaster recovery plan. Sadly it was mostly ignored. Group two could have recovered the server much faster, but instead, they tried and tried to fix the secondary Active Directory server. That cost them time, and after trying, they gave up and went with the recovery plan and recover the server.

8.3 Recovery of THDATA

The last server to be recovered was THDATA server. The primary role of this server was to act as a file server.

8.3.1 Methods One and Two

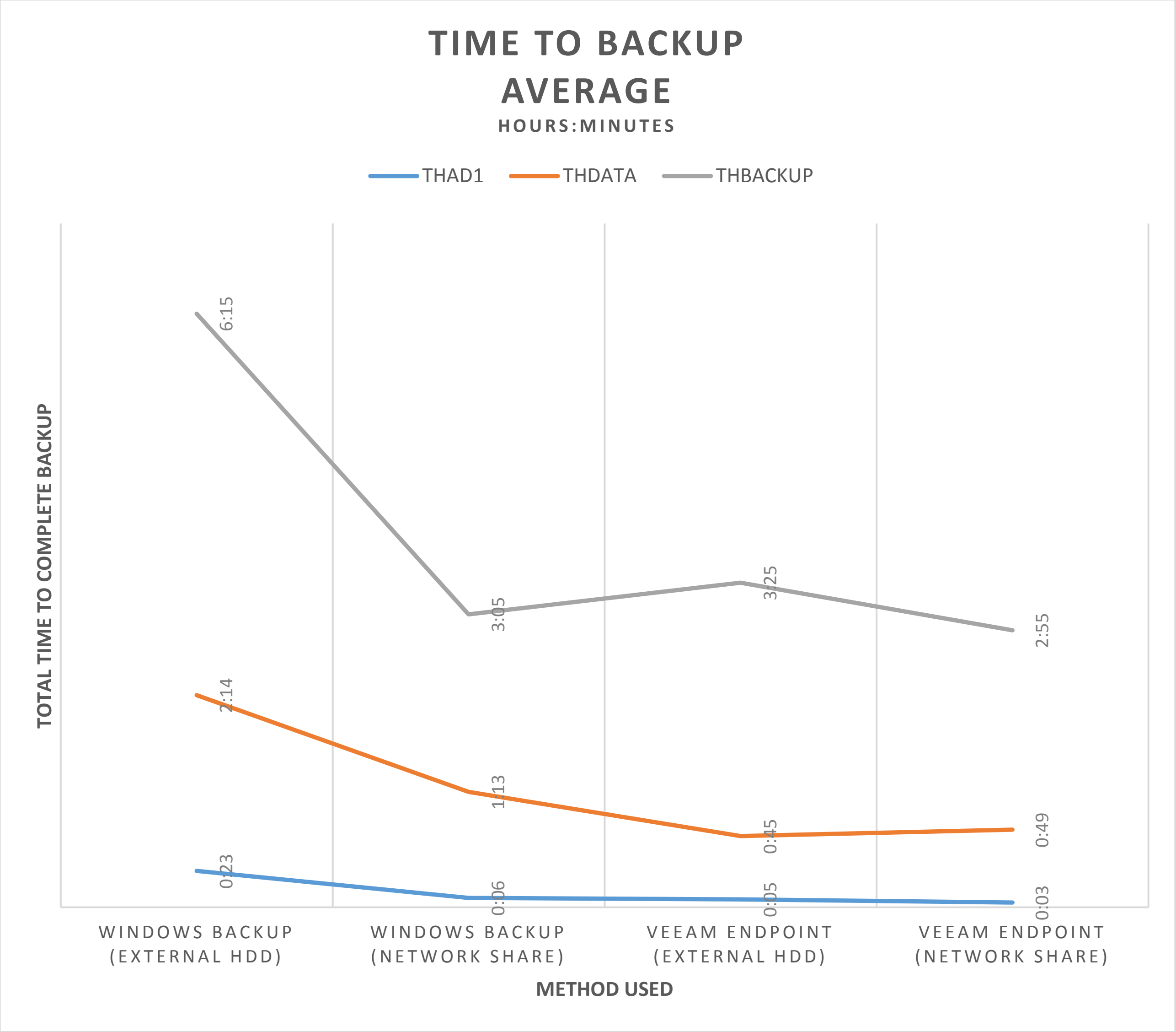
Recovering THDATA with Windows backup was successful without problems. The time it takes to recover with Windows backup role, and the external hard drive was one hour and 44 minutes. When using a network share, it was only one hour.

8.3.2 Methods Three and Four

Time to recover using external hard drive was one hour and 15 minutes, and with the network share, it takes about 45 minutes.

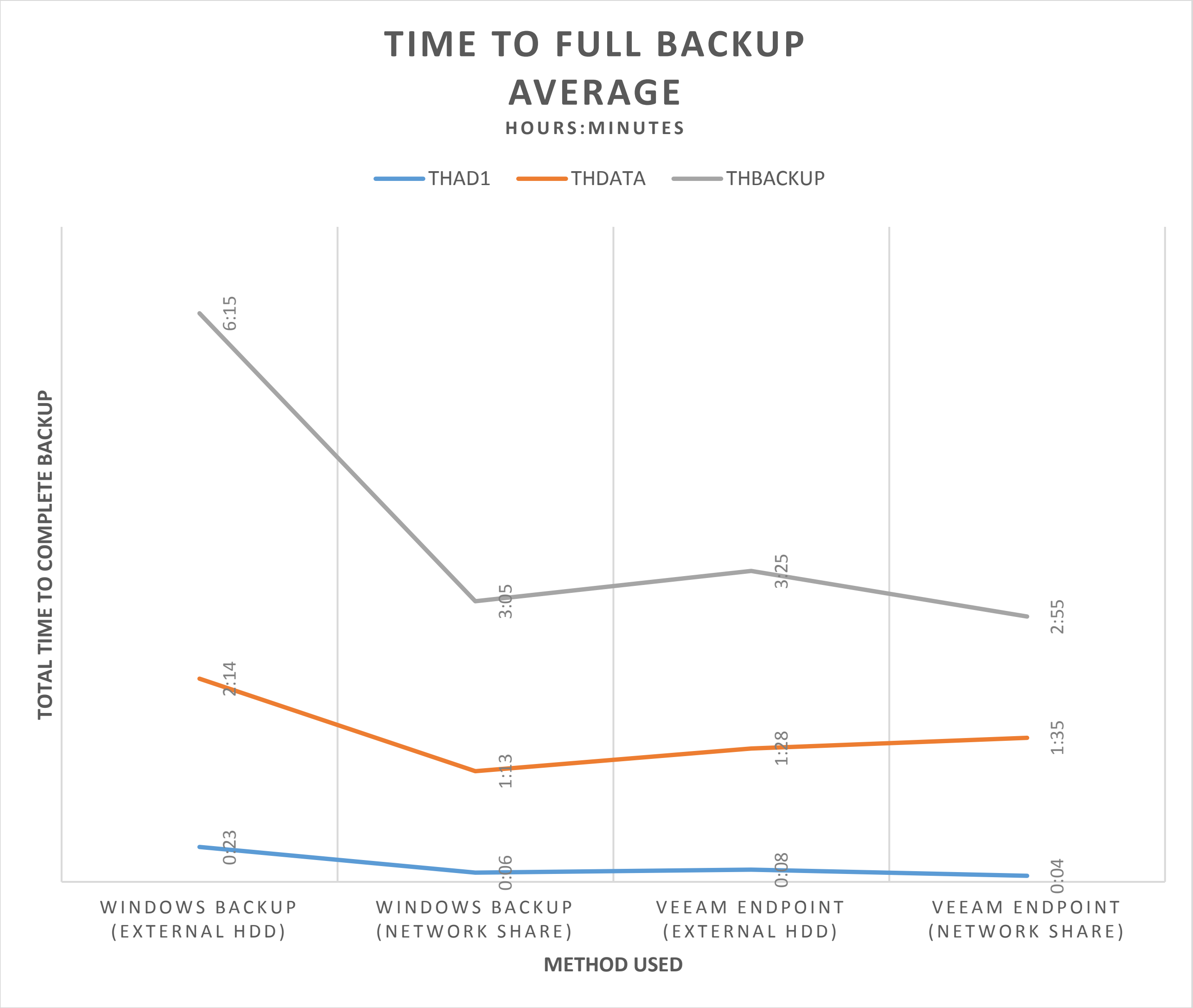
9 Analysis

In the earlier chapters, different backup solutions were explored. From these results, it is noticeable that method one using Windows Backup role to take a backup on an external hard drive is the slowest option on every server. In Picture 40 can be seen how the time consumed is lower when backing up to network shares. Also, Veeam seems to be faster; Veeam does have an edge here because of the incremental backups. The difference in the orange line between methods three and four is worth noticing. On THDATA server the backup time was four minutes longer on network share than on the external hard drive.



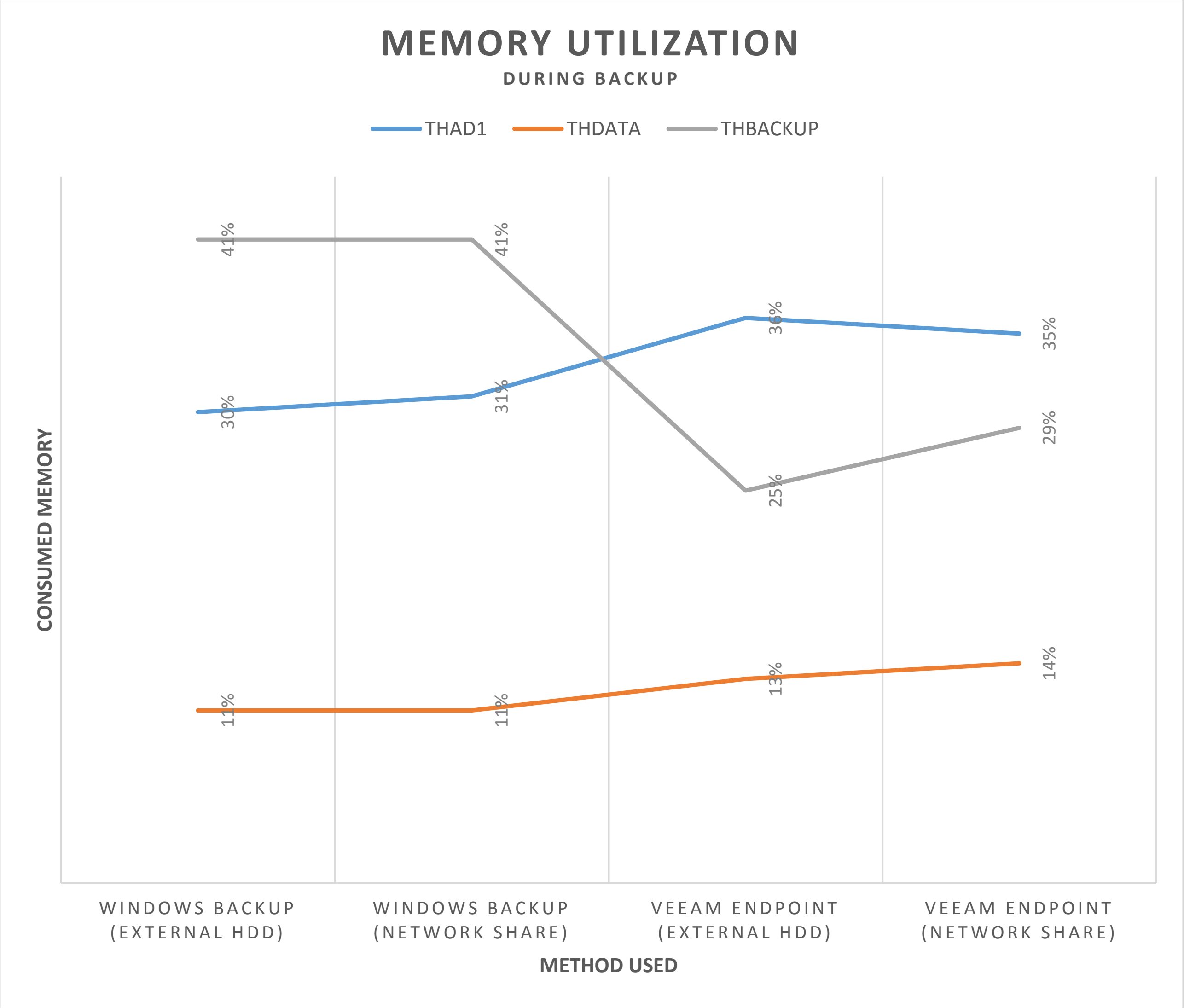
Picture 40. Time to backup the servers on average. (Picture: Lassi Latva-Nirva)

Taking a closer look and removing the incremental backup results from the backup average in Picture 41. The backup times are still mainly faster on the network share, which is explained with the slowness of USB transfer. Even when taking Veeam's advantage away from the results, the results show that Veeam is a faster method. THDATAs testing results again show an anomaly.



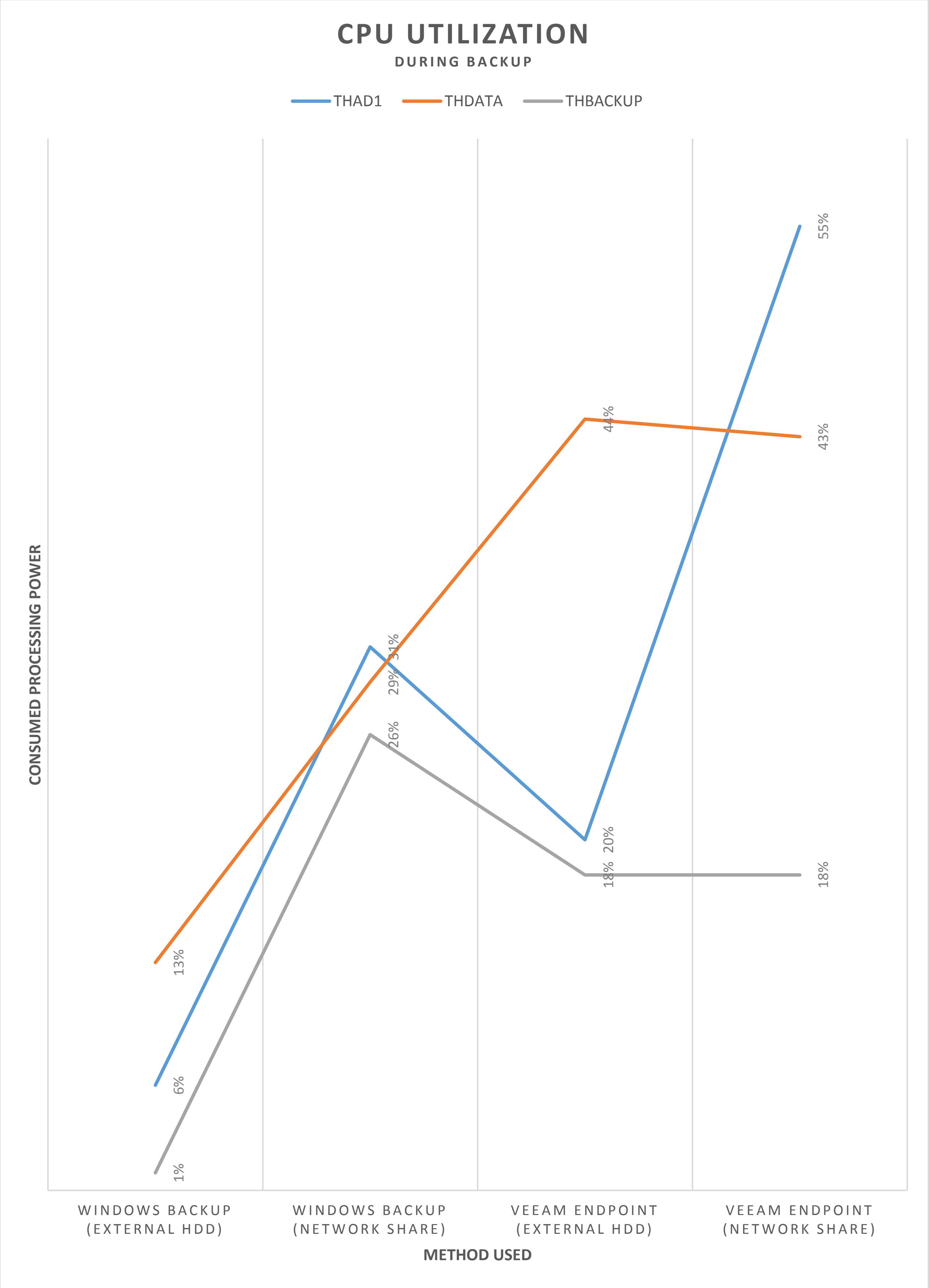
Picture 41. Time with only full backup average times. (Picture: Lassi Latva-Nirva)

Method three and four had an additional memory usage on all the servers but on THBACKUP where it decreased, as can be seen in Picture 42 below.



Picture 42. Consumed memory on the tested servers during backup. (Picture: Lassi Latva-Nirva)

On every server, the second method increased CPU usage. On every server methods, one and two used less CPU than with the methods three and four. When backing up to the network share with Windows Backup Role, Veeam agent to an external hard drive and to the network share with Veeam agent every server had increased CPU usage compared to working hours load. Using method one the CPU usage was lower than during working times comparison on every server but THDATA where it grew. Picture 43 shows the CPU utilization during backup.



Picture 43. CPU Utilization in average on the servers tested. (Picture: Lassi Latva-Nirva)

The resource utilization was highest on the third and fourth method, but the test results are inconclusive and depend highly on the specifications of the server used. On the other hand, all the servers had additional or same memory usage when using method one and looking at the results of working hours.

The most disturbing fact was that when using the backup on the network share, regardless of the server, the network was always jammed. This problem requires attention before any other measures are taken.

10 Closing Words

In this thesis, backup and recovery solutions were investigated. Also, performance testing was a major part of this thesis. The results depend heavily on the hardware used, roles on the server and the number of users online at the time of backups run. Also other variables can cause a change in the results. These results in this thesis are the average values of many tests performed. The accuracy of these tests is left for the reader to decide. In these tests, multiple backup solutions were used on the same server. The backups were run in separate times, so no issues were caused because of that. The author hopes that this research has inspired the reader to do some own research and to think the importance of disaster plans and to test them to see if they would work if a real disaster was to occur.

If a company was to ask for advice, the author would give the following advice:

- create a plan for Risk assessment and perform Business Impact Analysis if not yet created
- create a program for disaster recovery to ensure business continuity
- train employees and help them understand the importance of backup solutions
- if not skilled enough, hire a consultant to help choose a backup solution for the company.

The best practice is that only solutions from one vendor are used. Using multiple backup systems costs companies millions downtime and data loss is written in R1soft blog. The blog author interviewed 3000 IT decision makers, and the results were that 65% of those who answered use multiple vendors at their company. It is not only that it can cause trouble trough disruptions, but the downtime cost can also quickly rise over 1,66 million dollars depending on the company, of course. Based on the blog authors research it would be best to use one vendor and not try to mix many [16].

Dependability and reliability always play a crucial role in enterprises, and that means all the necessary plans and solutions have to be up to date in the IT department as well. Many take a look at the clouds. Hosting storage services, such as backup, in the Azure, for example, has become very attractive due to the advantages offered by the cloud computing model.

Clouds might be the future, but even such big names like Microsoft has unusual solutions put in place when it comes to availability. A lightning strike that hit an Azure data center in San Antonio, Texas terminated their cooling systems, and as a result, the servers overheated and went into automatic shutdown. The shutdown caused outages on almost 40 Azure services hosted in the South Central US region. In addition, a few Azure services and Office 365 services were affected outside the US region. The outage could have been avoided if disaster recovery plans were given more thought and instead of sites relying on each other, they were divided into zones as the competition has already done for some years now [17].

References

1. Techopedia, What is Data loss? https://www.techopedia.com/definition/29863/data-loss. 10.5.2018
2. Dundaslawyers, Legal issues for data loss. https://www.dundaslawyers.com.au/legal-issues-for-data-loss/. 10.5.2018
3. Cisco, Disaster Recovery: Best Practices. https://www.cisco.com/c/en/us/products/collateral/services/high-availability/white_paper_c11-453495.html. 10.5.2018
4. Douglas W. Jones, Punched Cards. http://homepage.divms.uiowa.edu/~jones/cards/. 10.5.2018
5. Maxim Yurin, The history of backup. http://www.backuphistory.com/. 10.5.2018
6. Bernard Marr, How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read. https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#7dfb830260ba. 10.5.2018
7. Overblog, The Advantages of Disk-based Backup. http://ciscorouterswitch.over-blog.com/2018/02/the-advantages-of-disk-based-backup.html. 11.6.2018
8. Techwalla, The Advantages of Portable Hard Drives. https://www.techwalla.com/articles/the-advantages-of-portable-hard-drives. 12.6.2018
9. Liquid Web, Quick Guide to Best Practice for Data Backup. https://www.liquidweb.com/blog/top-six-best-practices-for-data-backup/. 13.6.2018
10. WhatIs, Definition of incremental backup. https://searchdatabackup.techtarget.com/definition/incremental-backup. 14.6.2018
11. WhatIs, What is differential backup? https://searchdatabackup.techtarget.com/definition/differential-backup. 10.5.2018
12. EnterpriseFeatures, Backup Types: Full,Incremental, Differential. http://www.enterprisefeatures.com/backup-types-full-incremental-differential/. 12.5.2018
13. WhatIs, Full, incremental or differential: How tochoose the correct backup type. https://searchdatabackup.techtarget.com/feature/Full-incremental-or-differential-How-to-choose-the-correct-backup-type. 13.5.2018
14. Techworld, What are synthetic backups? https://www.techworld.com/data/what-are-synthetic-backups-1149/. 10.5.2018.
15. Tech Pro Research, Research: 68% report cost is biggest data storage pain point. http://www.techproresearch.com/article/research-68-report-cost-is-biggest-data-storage-pain-point/ 10.5.2018
16. R1soft, Using Multiple Backup Systems Costs Companies Millions in Downtime and Data Loss. https://www.r1soft.com/blog/using-multiple-backup-systems-costs-companies-millions-in-downtime-and-data-loss. 13.4.2019
17. DataCenter Knowledge, Azure Outage Proves the Hard Way that Availability Zones are a Good Idea. https://www.datacenterknowledge.com/microsoft/azure-outage-proves-hard-way-availability-zones-are-good-idea. 13.4.2019