УНИВЕРСИТЕТ ПО БИБЛИОТЕКОЗНАНИЕ И ИНФОРМАЦИОННИ ТЕХНОЛОГИИ

КАТЕДРА ”ФИН”
МАГИСТЪРСКА ПРОГРАМА
”ИНФОРМАЦИОННИ ТЕХНОЛОГИИ”

МАГИСТЪРСКА ТЕЗА

на тема:

Съхранение, архивиране и възстановяване на информация. Технологии, техники и устройства.

Дипломант:

Милен Руменов Палавров

Дистанционнно обучението

Ф.№ 0076-имд

Научен ръководител:.....

(Доц. Д-р Иван Гарванов)

София

2015

РЕЗЮМЕ

на

Магистърска теза на Милен Палавров

на тема

Съхранение, архивиране и възстановяване на информация. Технологии, техники и устройства.

с научен ръководител Доц. Д-р Иван Гарванов

град София, 2015 година

Катедра „ФИН“, факултет „Информационни технологии“ в университет „УНИВЕРСИТЕТ ПО БИБЛИОТЕКОЗНАНИЕ И ИНФОРМАЦИОННИ ТЕХНОЛОГИИ„

Брой страници: 80

Брой цитирани и използвани източници: 20

Брой приложения и графики: 42

В настоящата магистърска теза ще се разгледат ползите от съхранението на данни, наречен Backup или архивиране. Ще бъдат разгледани различни начини, от такива за нормалните потребители, до използваните от големите компании. Устройствата, които са нужни за направата му ще бъдат разгледани, така че да може всеки да се насочи към това, което на него ще му бъде най-удобно и целесъобразно. Също така различите софтуери за Backup ще бъдат разгледани в отделна тема. За всички устройства и софтуери ще бъдат приложени също така приложения и графики, на които ще бъде разяснено начина им на използване, приложението и всичко, което е нужно на нормалните потребители и дори и хората подържащи големи компании. Ще се наблегне също така на проблемите на нормалните потребители на компютри, мобилни устройства, таблети, и общо взето всякакви устройства, използващи и съхраняващи данни. Това е важно, тъй като в днешно време шанса да загубиш важна информация или тя да бъде повредена е много голям, като всеки е зависим дори от най-малките данни, съхранявани на тези устройства, като пример са контактите на телефона, документи на компютъра, снимки, песни, клипчета. Важно е всеки да знае как да направи

така, че изгубвайки важен документ, да може да го възвърне от най-скорошната дата, че и дори по-стара ако е необходимо. След разглеждането на магистърската теза, читателя трябва да бъде запознат с процеса на съхранение на данни, с проблемите, свързани със процеса, с различните софтуери, устройства и методи. Трябва също така да може да прави разлика между Backup и архив. Най-важното е да се види, колко е важно това да се прави бекъп и да се направи схема, която да го устройва.

С Ъ Д Ъ Р Ж А Н И Е

УВОД

Темата, която съм избрал в днешно време е много актуална, и хората трябва да все повече и повече да се интересуват как да се предпазят от безвъзмездното изтриване и загубване на важната за тях информация, било то снимки, документи, че дори и песни.
Примера, който ще дам ми се случи днес. Докато разчиствах ненужни файлове, без да искам си изтрих всички файлове от десктоп-а, а там всичко ми беше важно. За мой късмет на 95% от файловете си имах копиране информацията на Flash drive, но имаше пресни файлове, които не бях копирал никъде, нямах достатъчно актуален бекъп. Хубавото е, че и в такива случаи има решение. Има програми, които възстановяват файловете дори изтрити от компютъра, тъй като дори изтрити и да не ги виждаме, те стоят на хард диска под някакъв номер и препратка. Така и така надявам се да успея да възстановя всички файлове, които изтрих днес по погрешка, но важното и хубавото е, че имам бекъп на Флаш памет, от който ще възстановя 95% от изтритите файлове.

Вместо хората да разчитат на това, че са си копирали ръчно важните файлове на какъвто и да е носител на информация, е хубаво всеки да разбере, кой точно софтуер може да използва за backup на важните му файлове и внимателно и целесъобразно да избере схемата, която да използва.

В първа глава „*СЪХРАНЕНИЕ (BACKUP), АРХИВИРАНЕ И ВЪЗСТАНОВЯВАНЕ НА ИНФОРМАЦИЯ*„ , от темата „*Съхранение, архивиране и възстановяване на информация. Технологии, техники и устройства*„ ще разгледаме разликите между Архив и Бекъп, видовете Backup. Предимствата и недостатъците на всеки от тях. Ще бъдат разгледани също така начини за възстановяване на данни от бекъп, както и без да е бил направен такъв. Също така в тази глава ще може да се види, как точно работи твърдия диск, когато се записва информация на него и какво се случва с изтритите данни.

Във втора глава „*ТЕХНИКИ И ТЕХНОЛОГИИ СЪПРОВОЖДАЩИ ПРОЦЕСА НА СЪХРАНЕНИЕ НА ИНФОРМАЦИЯ И НЕЙНОТО ВЪЗВРЪЩАНЕ. СОФТУЕР И ХАРДУЕР***.**„ ще разгледаме устройствата, които се използват за направата на бекъп, както и видовете софтуер, които може да се използват, като разбира се в домашни условия, за

обикновените потребители, не са нужни такива специализирани устройства, но е хубаво да се знае кое какво представлява. За да може да се придобие по-добра представа, има множество фигури и приложения, които да покажат как изглежда дадено устройство или какви са главните менюта на използваните софтуери. Дадени са и среди и видове устройства, които може да се използват от нормалните потребители. В главата за разглеждане на видовете софтуери, по-добре ще бъде обхванат софтуер-а Data Protector на HP, като един от най-стабилните на пазара.

В трета глава „*ЧЕСТО СРЕЩАНИ ПРОБЛЕМИ,,* ще бъдат разгледани проблемите, свързани с хардуера и софтуера, който се използва за направата на бекъп.

Цялостно, след разглеждането на тази тема, трябва да може да се ориентирате, какво точно да използвате за направата на бекъп в домашни условия или в бизнес среда, какво представлява бекъп-а и каква е разликата между архив и бекъп. Трябва да може да различавате различните видове устройства, били те с касетки или със твърди дискове. Трябва също потребителите да могат да се насочат към избрания от тях софтуер за бекъп след запознаването с главните менюта на по-известните такива, както и някои от най-основните и важни неща за тях.

Използваните източници са предимно публикации и сайтове свързани със технологията Backup, както и различни наръчници за използването на дадените софтуери и хардуери. Също така са използвани и средите за работа, които се използват във компанията Hewlett-Packard.

I. СЪХРАНЕНИЕ (BACKUP), АРХИВИРАНЕ И ВЪЗСТАНОВЯВАНЕ НА ИНФОРМАЦИЯ.

Компании с всякакви размери имат едно нещо което ги свързва: Те създават данни и губят много от тях, включително информация за клиентите, спецификации на продуктите, счетоводителски файлове и други. Всъщност, много кооперации увеличават размера на вътрешните данни всяка година. Със това ниво на растеж идва и предизвикателството на предпазване на данните от инцидентно изтриване и бедствия както и спазване на изискването от регулаторните органи за запазване на данните голям период от време.

В миналото предпазването и съхранението се е извършвало чрез копиране или преместване на данните на касета. Подобряването на икономичността на дисковите масиви и появяването на решения за архивиране създават нови възможности.

1. Какво е Backup

Backup е процеса на копиране на файлове или бази от данни, така че те да се съхранят в случай на повреждане на оборудването или други злополуки. Backup-а обикновено е рутинна част от операциите на големите кооперации със големи сървърни зали, но също така и от администрираните от по-малките компании компютри. За потребителите на персонални компютри, бекъп-а е също необходим, но често пренебрегнат. Възвръщането на файловете от backup се нарича restore, но това ще се наблегне във точки 4.

Глаголната форма на бекъп на английски се състои от две думи „to back up”.

За персоналните компютри, потребителите може да избират между локален backup и Интернет backup.

Backup технологиите ни осигуряват за дълго време възможност ефективно възстановяване на системите от повреди като човешки грешки, повреди във хардуера на системата както и големи природни бедствия. Те са подходящи за бързо възстановяване на големи размери изгубена информация и също така може да възстановят цялостна система към

напълно работен вид във кратък период от време. Бекъпа също представлява и голямо затруднение за storage администраторите. Голямо количество от данни може да направи така, че backup инфраструктурата да не може да смогне. Според компания **Gartner** един нормален дейта център има успех на бекъпите само около 87%. Много също биха казали, че способността успешно да се възвърнат загубени данни е дори по-нисък.

Времето, което се изисква за направата на резервно копие на данни намялава и способността бързо да се възстанови информация значително се подобрява. Чрез ефективно прилагане на backup както върху касети и върху диск, компаниите могат да увеличат производителността и надеждността на тяхната disaster recovery (пълно възстановяване системата в случай на бедствия или изгаряне на хардуер и др.) инфраструктура на разумна цена. Последващо увеличаване на традиционния backup със способности за репликация ще помогне да се разреши най-строгото изискване за предпазванена данните. Но както и да е, тези технологии ще бъдат само временни мерки, ако неконтролируемия растеж на размера на данните изискващи backup не се намали. Това се превръща със истинска опасност, когато компаниите използват бекъпа като единствено решение и за предпазването на данните (protection) и за задържането му във времето (retention), като това е резултат на много неефективно и неефикасно управление а данните.

За пример може да се гледа следното. Повечето организации правят всяка нощ incremental и всяка седмица full бекъп и защитават данните на бекъп-а за 3 месеца, з да защитят информацията в случай на инциденти изтриване (*типовете бекъп ще се разгледат във точка 6*). Второ копие на данните може да бъде репликирано (или изпратено на растояние с касетка) на отдалечена локация, за да се защити в случай на бедствие. Ако се добави и изискване да се запазват бекъпнатите данни в период на години, за да се удоволетворят изискванията за съхраняване на данни, то значително ще се увеличи надхвърлянето на бекъпа. Увеличаването на данните се равнява на увеличаване на цената, специално от към време, пари и персонал.

- **Локален backup**

Опциите за локален backup са няколко, като в зависимост от нуждите зависи и цената им.
Може да се съхраняват критичните файлове на дискети. Този подход главно е използван от хора, които държат техните данни за финанси на персоналните компютри. Много програми, свързани със управление на парите постоянно напомнят на потребителите, когато излизат да съхраняват данните. Ако твърдия диск се развали, вие ще можете да възвърнете вашия файл. Този подход е много остарял, като дискети може би се използват много рядко, но вместо тях може да се използват флашки или преносими твърди дискове.
Друг вариант за бекъп е съхранението на данните от целия ви твърд диск на външен носител, примерно преносим твърд диск.

- **Интернет Backup**

Друга опция за съхранение на важната ви информация е като я изпратите на друго място за съхранение. Така във случай, че диска ви се развали вие ще може да я изтеглите. Повече за видовете бекъп ще се разгледа във точка 6.

2. Какво е архивиране

Архив е колеция от компютърни файлове, които са пакетирани заедно за бекъп, за прехвърляне на друго място, за запазване далече от компютъра, за да може да се освободи място на твърдия диск на компютъра или за други цели. Архивър може да съдържа прост списък от файлове или файлове организирани под директории или каталожна структура.

Защо обаче ни е нужен архив-а при положение, че имаме бекъп ?

Архив е колекция от данни подробно избрано за съхранение за дълго време (long-term retention) и бъдеща справка с тях или използването им. Това са данни, които няма да се променят активно, и дори може да не се използват изобщо. Архивът съдържа непроменящо се копие на данните. Нещо подобно на годишните документи за таксите, документи за правомощия, документи на пациенти, исторически записи и други. Също

така има органи, които ви нареждат да пазите дадена информаиция за дълъг период от време.

Чрез въвеждане на архивирането, компаниите могат да подобрят тяхното ниво на услугите за съхранение и възстановяване, като същевременно редуцират цената за съхранението на данните. Архивирането на файловете също така може да отговаря на изискванията на регулаторните органи за съхранение на данните във времето, като се управляват файловете със пълното познание на файловета система и метадатата на документите, както също и като знаеме съдържанието на файловете. Системата на архивиране на файл премества или копира файла според стойността на действителното съдържание. Също така се намират и възвръщат индивидуални файлове базирани на тяхното съдържание, което може да съдържа всякакъв брой параметри, включително автор, дата, както и някои специфични параметри.

За да може ефективно да се управляват данните, файловите системи за архивиране откриват всички файлове в мрежата и ни осигуряват описване на неструктурирани данни. По време на процеса на откриване, системата събира метадати на файловата система и извлича файлови съдържания, изгражда основа за класифициране на данните. Системата за архивиране на файлове трябва да осигури следните възможности:

- Да бъде осведомена за съдържанието. Примерно трябва да индексира съдържанието на документа, не само метадатата на файловата система.
- Да попълни допълнителните метадата тагове като извлече информация от съдържанието.
- Да се архивира избирателно подмножество от данни, така че да е съгласно регулатора и корпоративно-държавните правила.
- Да осигурява бърз достъп до архивираните данни.

- **Нужно ли ни е архивирането?**

Има строго регулирани индустрии, със правила, които ги задължават архивите да се съхраняват и подържат за определен период от време. Някои от тези индустрии са банкирането, сигурността, здравеопазването и легализиращите институции. Типовете информация, които трябва да се архивира се различава от типа на индустрията, затова няма строго

определени типове данни, които се архивират. Дори да не сте организация от горе изброените, а сте просто нормален потребител, тогава пак има случаи във, които архива би ви бил полезен. Примерно снимки или филми от сватба, или други важни съботия, важни документи, или други неща, които бихте желали да съхраните за дълъг период от време и няма да изискват промени.

3. Разлики между Backup и архивиране

Архивирането и бекъпа имат две напълно различни, но и допълващи се функции, във кооперациите:

- **backup** за високо-скоростно копиране и възвръщане на данни, за да минимизира въздействието от повреда в системата, човешка грешка или бедствие;
- **архивиране** за ефективно управление на данните за съхранение и достъп и възвръщане за дълъг период от време.

Тези две опции за съхранение могат да бъдат приложени заедно, за да оптимизират цената и да подобрят цялостната ефективност на всяка storage инфраструктура. Бъкепа е по-ефективен във среда, която има ефективни решения за архивиране, а и архивите все още превъзхождат бекъп инфраструктурите за техните, заради неговите нужди от защита на данните. И двете решения са важни за ефективна стратегия за управление а данните.

Като цяло бекъпа и архива имат много рзлични цели. Също така главния проблем около разликите между бекъпа и архива всъщност са заради правителството и сигурността. Казани по друг начин, легалните и съответстващите изисквания диктуват на всяка организация, че трябва да имат архиви. От друга страна backup-а е изцяло насочен към достъпността на информацията, най-вече във днешно време, където разчитаме изцяло на IT технологиите и информацията да помагат на бизнеса. Трябва много да се внимава, защото една организация объркa ли това, че бекъп = архив, то ще избере грешна стратегия и среда за съхраняването на информация, което може да доведе до много бавно възстановяване на информация, а и дори до загубена данни.

- **Кратко сравнение между Архив и Бекъп:**

Бекъп	Архив
Малък капацитет	*Голям капацитет*
Много различни версии	*Само една версия*
Скоростта е критично важна	*Скоростта е второстепенна*

4. Видове Backup

Има много на брой видове бекъп и условия, когато става въпрос за съхраняване на вашата дигитална информация. Долупосочените, са най-често използваните видове бекъп, като също така и е дадено кратко описание за предимства и недостатъци на всеки един от тях.

- **Full Backup** (Цялостен бекъп)

Full backup е вид бекъп, при който всички файлове и папки избрани за съхранение ще бъдат бекъпнати. Когато последващ бекъп е пуснат, целия списък от файлове ще бъде бекъпнат оново, може да се види на *фигура 1*.

- **Предимства**

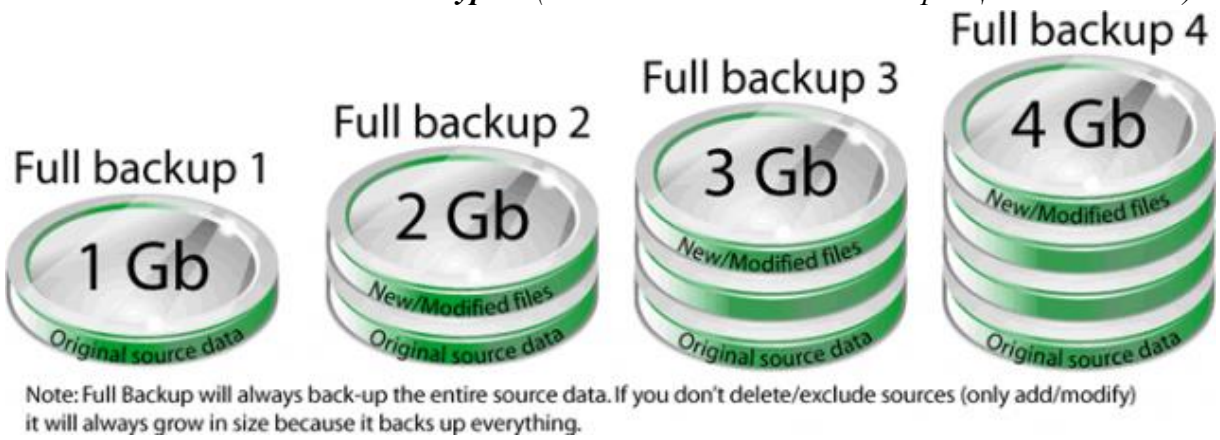
- Възстановяването на файлове е бързо и лесно за управление, имайки впредвид, че целия списък със файлове и папки е във един бекъп файл.
- Лесно за поддържане и възстановяване от различни версии (дати).

- **Недостатъци**

- Бекъпа може да отнеме много време, защото всички файлове и папки се съхраняват всеки път, когато той се стартира.

- Използва много дисково пространство, в сравнение със другите типове бекъп (incremental и differential). Едни и същи файлове се съхраняват всеки път, като резултата от това е недостиг във дисковото място.

Фигура 1 *(Как се бекъпват данните при Цялостен бекъп)*



- **Incremental Backup** (Нарастващ бекъп)

Incremental бекъпа съхранява всички промени, които са извършени от както е бил извършен последния full или incremental бекъп. При него един full бекъп е стартиран в началото и последващите бекъпи стартират само съхранявайки само промените направени от последния бекъп. Резултата от това е много по-бърз бекъп и по-малко дисково пространство, заето от него, примерна бекъп схема за него може да се види на *фигура 2*.

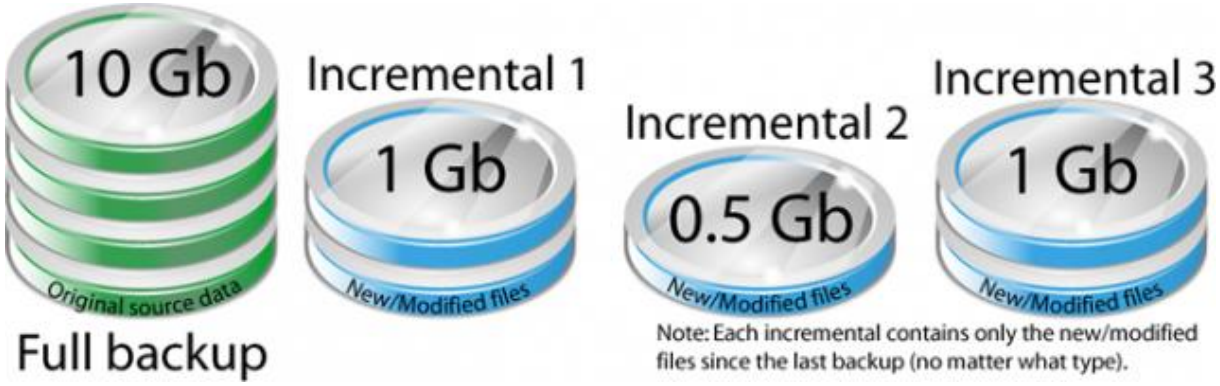
- **Предимства**

- Много по-бързи бекъпи
- Ефективно използване на дисковото пространство отделено за тях, като файловете, които са съхранени не се дублират. Много по-малко заето място, в сравнение със цялостния бекъп и също така със differential бекъпа.

- **Недостатъци**

- Restore операциите са по-бавни в сравниение със full и differential бекъпите.
- Restore операциите също така са и по-сложни, тъй като е нужен целия набор от бекъпи, а именно първия full бекъп и всички последващи incremental бекъпи, за да се извърши възстановяването.

Фигура 2 *(Примерна бекъп схема при нарастващ бекъп)*



- **Differential backup**

Differential backup съхранява всички промени направени от последния full бекъп. При него един цялостен бекъп се прави в началото и последващите бекъпи се стартират съхранявайки промените направени от последния full бекъп, примерна схема може да се види на *фигура 3*.

- **Предимства**

- Много по-бързи бекъпи в сравнение със цялостния.
- По-ефективно използване на дисковото пространство отделено за бекъп в сравнение със цялостния, тъй като само променените файлове от последния цялостен бекъп се копират със всеки стартиран differential.
- По-бързо възстановяване на файловете в сравнение със incremental вида.

- **Недостатъци**

- Изискват повече време в сравниене със Incremental бекъпа.
- Използването на дисковото пространство не е толкова ефективно, колкото при incremental бекъпа. Всички файлове добавени или редактирани след като е бил стартиран поледния цялостен бекъп ще се дублират отново със всеки последващ стартиран differential бекъп.
- Възстановяването на файловете е по-бавно от колкото при цялостния бекъп.
- Restore операциите са малко по-сложни от колкото при full бекъпа, но са по-лесни от колкото при incremental. Набор от цялостния бекъп и нужния differential бекъп е нужен за да се изпълни възстановяването.

Фигура 3 *(Бекъп схема при Differential бекъп схема.)*

- **Mirror Backup** (Огледален бекъп)

  Както наименуването "Mirror backup" предполага, „отражение" на източника се съхранява. Със огледалния бекъп, когато файл при източника бива изтрит, то този файл в скоро време се изтрива и от огледалното копие. Точно поради тази причина, mirror бекъпа трябва да се използва със предпазливост, като се има впредид, че ако се изтрие един файл по невнимание или от вирус, то се изтрива и от mirror бекъпа, примерна схема може да се види на *фигура 4*.

- **Предимства**

- Бекъпа е чист и не съдържа стари или вече ненужни файлове.

- **Недостатъци**

- Има вероятност файла на източника да се изтрие по невнимание, чрез саботаж или чрез вирус, като той също щъ бъде изтрит и от mirror бекъпа.

Фигура 4 *(Примерна схема за Огледален бекъп)*

- **Full Computer Backup** (Бекъп на целия компютър)

  При този тип бекъп, не само индивидуални файлове се бекъпват, а цялостното състояние на хард диск-а на компютъра, който се бекъпва. Със цялостния бекъп на компютъра, може да се възстанови хард диска до абсолютно същото състояние, във което е бил, когато бекъпа е бил направен. При него не само документи, снимки, видео и аудио файлове ще бъдат възстановени, но и операционната система, driver-ите за хардуера, системните файлове, регистрите, програмите, е-мейлите и т.н.

- **Предимства**

- Развален компютър може да бъде възстановен за минути със всички програми, бази данни, е-мейли и др. Няма нужда да се инсталира наново операционна система, програми и да се настройва.
- Идеално решение при евентуално разваляне на хард диска.

- **Недостатъци**

- Може да не е възможно да се възстанови на напълно нов компютър със различно дъно, процесор, видео карта, звукова карта и др.
- Всякакви проблеми, които са съществували на компютъра (като вируси, грешни драйвери излишни програми и др.), които е имало по време на бекъпа, ще ги има и след цялостното възстановяването.

- **Local Backup** (Локален бекъп)

Локален бекъп е всеки вид, при който носителя се държи да е в близост до източника, или в една и съща сграда. Бекъпа може да бъде извършен на втори вътрешен хард диск, закачен външен хард диск, CD/DVD, закачен в мрежата дисков масив (NAS), касетка и други. Локалния бекъп защитава дигиталното съдържание на хард диска от грешки и вируси. Той също така осигурява защита от внезапни грешки или изтривания. Тъй като бекъпите са винаги под ръка, то възстановяването е бързо и удобно.

- **Предимства**

- Предлага добра защита от евентуално разваляне на хард диска, вирусни атаки, внезапно изтриване, саботажи и др.
- Много бърз бекъп и много бързо възстановяване.
- Цената на мястото за съхранение може да е много евтина, когато правилния тип носители се използва, като примерно външни хард дискове.
- Цената за трансфера на данните към носителите може да е незначителна или много ниска.
- Тъй като бекъпите се съхраняват на близо, то те са много удобно за използване при нужда от бекъп или възстановяване.
- Има пълен вътрешен контрол на носителите на бекъпа и на сигурността на данните на тях. Няма нужда да се поверяват носителите на външна компания.

- **Недостатъци**

- Тъй като бекъпите се съхраняват близо до източника, то това не предлага добра защита от кражби, пожар, наводнения, земетресения, и други природни бедствия. Когато източника е повреден от, което и да е от тези обстоятелства, то има голяма вероятност и бекъпа също да бъде повреден.

- **Offsite Backup** (Външен бекъп)

  Offsite backup се нарича когато бекъп носителя се съхранява на различно географско положение от източника. Бекъпа може да бъде извършен локално, но изпрати ли се един път носителя към друга локация, до бекъпа става външен. Пример за външен бекъп е направата на бекъп във офиса и след това касетката да се занесе във друга офис сграда или във депозит във банката. Освен защитата, която локалния бекъп предлага, външния бекъп предлага допълнителна защита от кражба, пожар, наводнения и други природния бедствия. Поставянето на носителя във съседната стая не се счита за външен бекъп, като няма защитите от природния бедствия и от кражба.

- **Предимства**

- Предлага допълнителна защита в сравнение със локалния бекъп, като защита от природния бедствия и кражба.

- **Недостатъци**

- Освен при онлайн бекъпа, то външния бекъп изисква повече усърдие да се занесе носителя до външната локация.
- Може да струва повече, тъй като хората обикновено обслужват няколко бекъп устройства. Примерно, когато носителите се държат във банков депозит, хората обикновено използват 2-3 хард диска и ги въртят. Така поне един хард диск ще бъде във устройството, докато другите се премахват за да се извърши бекъпа.
- Поради увеличеното пренасяне на носителите, рискът от нараняване деликатните части на хард диска или касетата се увеличава, като това не се отнася за онлайн бекъпа.

- **Online Backup**

Това са бекъпи, които са постоянно прехвърлящи данни или извършвани продължително или много често на носител, които е постоянно свързан с източника, който се бекъпва. Обикновено носителя се намира offsite и е свързан със бекъп източника по мрежата или по интернет. Няма включени човешки интервенции за включване на драйвове или носители за да може бекъпа да върви. Много дейта центрове предлагат на клиентите си тези услуги, примерно Google. Тези дейта центрове се намират далече от източника, който се бекъпва, и данните се изпращат подсигурени през интернет.

- **Предимства**

- Предлага най-добрата защита срещу природни бедствия и кражби.
- Тъй като данните са репликирани между няколко носителя, рискът от загуба на данни заради разваляне на хардуера е много нисък.
- Тъй като бекъпите са чести или постоянни, загубата на данни е минимална в сравнение със другите видове бекъп, които вървят по-рядко.
- Тъй като е онлайн, то той изисква малко човешки интервенции след като се настрои един път.

- **Недостатъци**

- По-скъп е от локалния бекъп.
- Инициирането на бекъп, или най-вече първия бекъп може да бъде много бавен процес, продължаващ няколко дена или седмици, в зависимост от скоростта на интернет връзката и количеството данни, които ще се бекъпват.
- Възстановяването също може да е бавно.

- **Remote Backup** (Бекъп от растояние)

Бекъпите от растояние са вид външен бекъп, като разликата е, че вие може да достъпвате, възстановявате или администрирате бекъпите, докато се намирате във локацията на източника или друга локация. Не е задължително физически да се намирате във мястото на бекъп устройството, за да го достъпите. Примерно, поставянето на хард диска във банков депозит не се счита за remote бекъп. Няма как да го администрирате, без да отидете до банката. Онлайн бекъпите също се считат за бекъпи от растояние.

- **Предимства**

- Много по-добра защита от колкото локалните бекъпи.
- По-лесно администриране, тъй като не е нужно да се ходи до външната локация.

- **Недостатъци**

- По-скъпи са от локалните бекъпи.
- Може да изискват повече време за съхранение и възстановяване в сравнение със локалните.

- **Cloud Backup**

Този термин, често се използва заменимо със Online and Remote backups. Този вид бекъп е, когато данните се бекъпват към услуга или съоръжение със дискови масиви през интернет. Със правилните акредитиви за вписване, този бекъп може в последствие да се достъпи или възстанови от, който и да е компютър със достъп до интернет.

- **Предимства**

- Предлага същите предимства като offsite бекъпа.
- Предоставя възможност лесно да се свързваме и достъпваме бекъпа само със връзка към интернет.

- Информацията е репликирана през няколко устройства за съхранение и обикновено използващи няколко интернет конекции, така, че системата не е със една единствена възможност за грешки във връзката.
- Когато услугата е предлагана от добър комерсиален дейта център, услугата е управлявана и защитата не е паралелна.

- **Недостатъци**

- Отново по-скъпи от локалните бекъпи.
- Може да изисква повече време за съхраняване и възстановяване.

- **FTP Backup**

  Това е вид бекъп, който се извършва през FTP (File Transfer Protocol) протокола през интернет към FTP сървър. Типичния FTP сървър се намира във комерсиален дейта център на растояние от източника, който се бекъпва. Тъй като FTP сървъра се намира на различна локация, то това е друг вид offsite backup.

- **Предимства**

- Предлага предимствата на външния бекъп.
- Предлага лесна връзка и достъп до бекъпа, само със интернет връзка

- **Недостатъци**

- По-скъпи са от локалния бекъп, както и другите типове външни бекъпи.
- Както при другите, така и при него трябва повече време за бекъп и възстановяване, като скоростта зависи от скоростта на интернет връзката.

5. Какво е Restore (възстановяване). Видове.

При управлението на данните, restore е процес, който включва копиране на данните, които са били съхранени (backuped или archived), от външно устройство (касетка, zip файл, външен хард диск и др.) на локалния ви хард диск. Resore-а се използва за да се възстановят данните във оригиналното им състояние, при положение, че се е бил повредил, или за да се копира премести на ново място.

Възстановяването на файлове съответно от архив или от бекъп си имат своите различия, които са свързани със начина на извършването на двете, както и различията в естеството им. Възстановяване от бекъп се налага да се извършва много по-често, поради простата причина, че бекъп се прави на файлове, които се използват от компанията във настоящия период, докато възстановяване от архив, не се налага, освен ако не се изиска. При архива, както съм споменал по-горе, се съхраняват файлове за дълъг период, файлове, които се пазят до поискване и са от изминал период във повечето случаи.

Видовете restore зависят отново от видовете бекъп, дали ще бъде на файлова система или на база данни или на exchange база данни (outlook и др.), на виртуален сървър и др. Също така може да се възстановява по файлове, папки, също така може и цял сървър със настройките му (примерно disaster recovery), може от възстановена exchange база данни, да се извлече информация за даден потребител от нея и др.

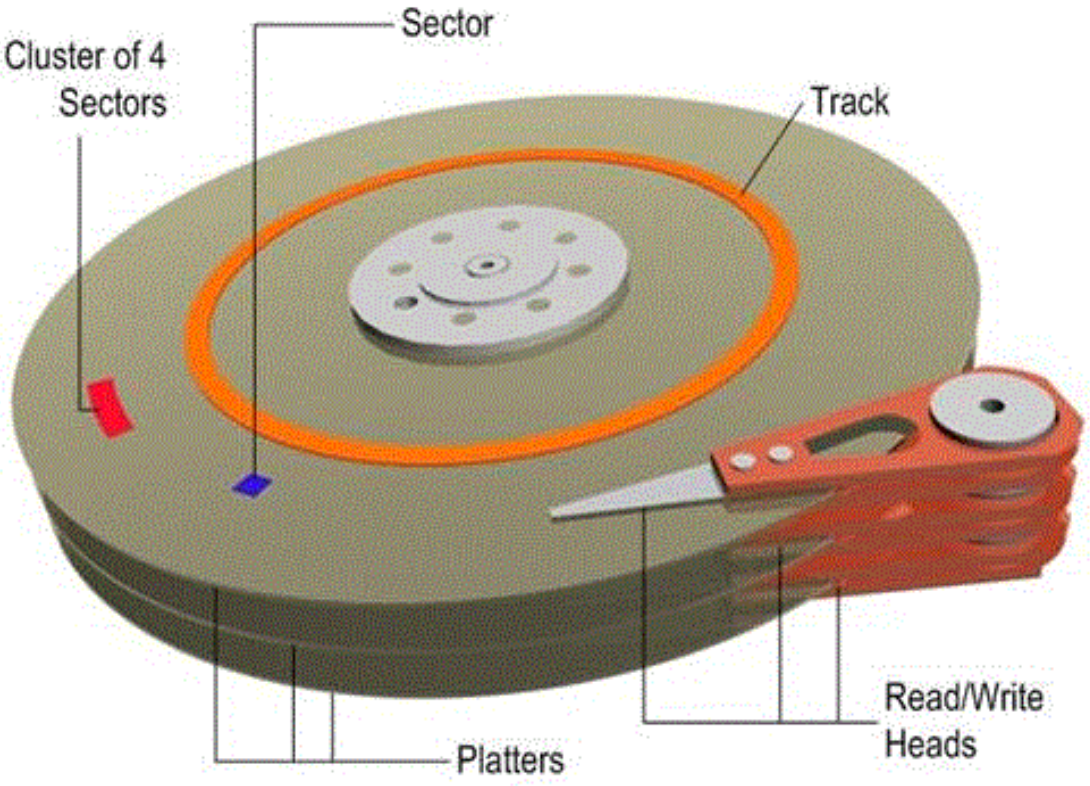
5.1. Възстановяване на файл от хард диска след изтриването му и при липсата на Backup.

На всеки му се е случвало да изтрие важен файл, папка или множество от файлове без преди това да си е подсигурил тяхно копие на външен носител или друг тип бекъп. Може би всеки се е запитвал, възможно ли е възстановяването на този изтрит файл ? Ако е възможно, как ?

За да може да се обясни, как и дали може да се възстанови този файл, може би е по-добре първо да се обясни как точно работи хард диск-а и как се записва, презаписва и изтрива информация от него, тъй като това

което ние виждаме на операционната система, било Linux или Windows, не е това, което отива на твърдия диск.

Фигура 5 *(Устройство на твърд диск)*



Hard Disk Drive 3D Image - Sourced From TechNet, Microsoft Website

- На *Фигура 5* са показани главните характеристики, с които може да се опише един твърд диск.

    - **Sector** – В един сектор се съхранява определен обем от данни, за HDD 512 байта, като по-новите хард дискове е 4096 байта.
    - **Cluster of Sectors** – Няколко сектора обединени в клъстер от сектори се прави, за да може един файл да не заема разхвърляни сектори из целия хард диск, а да са събрани в един пакет от сектори.
    - **Platter** – Това е диска, на който се съхраняват данните. Всички сектори се намират на него. Хард дисковете съдържат по няколко такива магнетични диска.
    - **Read/Write Heads** – Това е главата, която чете по диска, това е причината постоянно да върти и шуми. За да може да намери някой файл на диска, то тази глава превърта всичко и търси по

секторите, като предварително знае разбира се къде се намират точно.
    - **Track** – По този кръг върви четящо/пишещата глава.

- Как файловете в Windows-а се асоцират със секторите на хард диска.

Всеки файл, в зависимост от размера заема или един сектор или един клъстър от сектори. При сектор на хард диска с размер 512 байта и размер на сектора 4096 байта ще бъдат алокирани различен брой сектори. И при двата варианта има и плюсове и минуси. **Пример 1:**

100 файла с размер 100 байта. На хард диск със сектори 512 байта ще заемат 51200байта, а на хард диск със размер на секторите 4096 байта ще заемат 409600 байта. Причината за това е, че на един сектор не може да се запишат два файла. В случая предимство има твърдия диск с по-малък размер на секторите

Пример 2*: 5 файла по 50 Гигабайта. При сектори с размер 512 байта ще има повече заети сектори, и съответно ще трябва повече време на главата да ги обходи всички и да прочете файла или съответно да го запише. В случая предимство имат твърдия диск с по-голям размер на секторите.*

И сега да си дойдем на въпросът. Как се асоцират файловете от Windows-а със секторите на твърдия диск.

Всеки файл има връзка към секторите, **Пример**:

Два файла, на хард диск с размер на секторите 4096 байта. Единия файл е с размер 40 KB с име „Файл 1“ другия е с размер 14 KB с име „Файл 2“

	Име файл	
	Файл 1	*Файл 2*
Сектори	*1, 12, 44, 55, 1234, 5525, 52525, 95952, 996*	*2, 665, 7777, 99999*

В тази табличка, може да се види как хаотично са разхърляните секторите по твърдия диск за двата файла. Това е така, защото диска е фрагментиран и му трябва дефрагментация, тоест да се подредят секторите по хард диска, които се асоцират с дадени файлове. Когато хард диска е дефрагментиран трябва да изглежда дето така.

	Име файл	
	Файл 1	*Файл 2*
Сектори	*1, 2, 3, 4, 5, 6, 7, 8, 9, 10*	*11, 12, 13, 14*

И сега, ако се изтрие файла, какво се случва със секторите, на които се е запазила информацията за него ? Тези сектори, остават с неговата информация, докато не се презапишат или не се зачистят изрично.

Файловете могат да се възвръщат със специализирани програми за възстановяване като “Recover My Files Data Recovery”, “Recuva” и други. Възвръщането на файловете, може да става докато не са се презаписали секторите, затова важно е да не се записват нови неща на твърдия диск, които могат да доведат до презаписването им. Повечето от програмите са платени, но нужно ли е, ще се плати. Процеса на сканиране за изтрити файлове трае много време, в зависимост от големината на твърдия диск.

II. ТЕХНИКИ И ТЕХНОЛОГИИ СЪПРОВОЖДАЩИ ПРОЦЕСА НА СЪХРАНЕНИЕ НА ИНФОРМАЦИЯ И НЕЙНОТО ВЪЗВРЪЩАНЕ. СОФТУЕР И ХАРДУЕР.

Тъй като бекъп системите съдържат поне едно копие на всичката информация, която си струва да бъде запазена, то изискванията към дисковите масиви за данни може да бъдат значителни. Организацията на тези това място със дискови масиви и управлението на бекъп процеса може да бъде сложена задача. Модела за съхранение на данните може да осигури структуриране на дисковия масив (storage). В днешно време има много различни типове устройства за съхранение на данните, които са полезни за направата на бекъп. Има също така много различни начини тези устройства да бъдат подредени, така че да осигуряват обезпечаване на информацията, сигурност на данните и преносимост.

Преди данните да бъдат изпратени към локациите на техните дискови масиви, те са избрани, извлечени и манипулирани. Изработени са много

техники за оптимизиране на бекъп процедурите. Това включва оптимизации за работата със отворени файлове и източниците на данни, които се използват в момента, така както компресиите, криптирането и дедупликирането, както и други. Всяка бекъп схема трябва да включва тестови пускания, които валидират надеждността на данните, които ще се съхраняват чрез бекъпа. Важно е да се знаят ограниченията на

1. Видове техники за съхранение на информацията.

1.1. Видове среди за съхранение.

В зависимост от модела за съхраняване, който е избран, данните трябва да бъдат съхранени на някакви носители за съхранение на данни (storage medium).

- **Magnetic tape** (Магнитно-лентови носители)

Магнитно-лентовите носители от много време на са най-често използваните носители за големи хранилища за данни (storage), бекъп, архиви и обмен. Касетите обикновено са имали значително по-добро съотношение на капацитет/цена, когато се сравняват във хард дисковете, но от скоро това съотношение на цена/капацитет на хард дисковете и касетите се доближи, на *фигура 6* може да се види как изглеждат самите касети.

Има много формати, много от които са собственост на специфичен или точно определен пазар като големи компютърни системи (mainframes) или точно определена марка персонални компютри. Касетата е със последователно достъпване, така че дори времето за достъпване може да е бавно. Степента на цялостно записване или четене на данни може да бъде много бързо. Някои нови устройства за касети са дори по-бързи от модерните хард дискове.

Фигура 6 *(Магнитно лентова касета LTO5, капацитет 1,6 TB, цена около 80лв.)*

- **Hard disk** (HDD, Твърд диск)

Съотношението на цена/капацитет на хард диска се подобрява със много бързо темпо от много години насам. Това го прави по-конкурентен със магнитно-лентовите касети като носител на голям обем информация. Главните предимства на хранилищата от хард дискове са малкото време за достъп, достъпност, капацитета им и, че са лесни за работа. Външните дискове могат да бъдат свързани чрез локални интерфейси като SCSI, USB, FireWire или eSATA или от по-голяма дистанция технологии като Ethernet, iSCSI или Fibre Channel. Някои бекъп системи базирани на дискове, като Virtual Tape Libraries (VTL-виртуални библиотеки), подържат дедупликиране на данните, което може много сериозно да редуцира обема на дисковото пространство във хранилището, което се консумира дневно и седмично от бекъпнати данни. Главните недостатъци

на бекъпа на хард дискове, са че те се повреждат лесно, най-вече когато се транспортират (примерно към външна локация), както и че стабилността им във определен период години е относително неизвестна, на *фигура 7* може да се види как изглежда HDD.

Фигура 7 *(Примерна снимка на твърд диск)*

- **Optical storage** (Оптични носители)

Записваеми CD-та, DVD-та и Blu-ray дискове са обикновено използвани от потребители на персонални компютри и главно имат ниска цена за брой, може да се види на *фигура 8*. Обаче все пак, капацитета и скоростта на тези и други оптични дискове е обикновено в пъти по-ниска от тази на хард дисковете и касетите. Много оптични дискове са от типа WORM (Write Once, Read Many), или иначе казано записва се един път,

чете се многократно. Това ги прави подходящи за архиви, тъй като информацията във тях не може да бъде променяна. Използването на авто-чейнджър или джубокс може да направи оптичните дискове приложим вариант за по-големи бекъп системи. Някои оптични системи за съхранение на данни позволява каталогизиране на бекъпнатите данни без нуждата от човешки контакт със дисковете, което позволява по-дълга цялостност на данните.

Фигура 8 *(CD – Компакт диск)*

- **Solid state storage** (SSD)

Също така са познати като флаш памети, флашки, USB флаш устройства, карта памет и др. Тези устройства са значително скъпи за капацитета им, но са много удобни за бекъпване на системи за малък обем на данните. SSD дисковете не съдържа никакви движещи се части, за разлика от магнитно-лентовите касети и HDD дисковете и може да има огромен обмен на данни, нещо от сорта на 500Mbit/s до 6Gbit/s. Solid state дисковете сега са налични във размери над TBs. На *фигура 9* може да се види пример за Solid-state drive устройство.

Фигура 9 *(Solid state disk)*

- **Remote backup service** (Отдалечени бекъп услуги)

От много години, от както интернет достъпа стана широко разпространен, отдалечените бекъп услуги придобиха популярност. Съхранението на данни чрез интернет към външна локация може да защити вашите данни срещи някои много неприятни неща като пожари, наводнения и др., които биха унищожили всичките бекъпи. Все пак обаче има и много спънки във тези услуги. Първо, интернет връзките обикновено са по-бавни от скоростта на локално вързаните устройства. Основно скоростта е проблемна, като се има в предвид, че рутинните бекъпи трябва да се качват към външен домейн, който обикновено е по-бавен от локалния, който се използва много рядко за възвръщане на файл от бекъп. Това прави така, че да се постави ограничение да се използват тези услуги само за малко количество данни със висока стойност. Друго нещо е, че потребителите трябва да се доверят на външна компания да управлява сигурността на лична информация и целостта на техните данни, въпреки че поверителността може да бъде подсигурена чрез

криптиране на данните преди изпращане за към тези бекъп услуги със криптиран ключ, който само потребителя знае. В края на краищата предлагащите тази услуга трябва да използват един от горе-изброените методи за бекъп, като цялото това нещо може да се гледа като малко по-сложен начин за традиционен бекъп.

- **Floppy disk** (Дискета)

По време на 1980-та и ранната 1990-та много потребители на персонални/домашни компютри асоциирали бекъпа главно със копирането на дискетки. Както и да е, капацитета от данни, който може да побере дискетата не е успял да догони изискването за постоянно растящия размер на данните, като това ги направи непопулярни и излязоха от употреба. Може да се види на *Фигура 10*.

Фигура 10 *(Дискета)*

1.2. Типове съхранение.

Без да се интересуваме от модела на хранилището на данни, или мястото за съхранение използвано за бекъп, трябва да бъде постигнат баланс между достъпността, сигурността и цената. Тези методи за управление на носителите не са взаимно изключващи се и са често комбинирани за да се постигнат нуждите на потребителя. Използването на онлайн дискове за първоначален запис на данните, преди да бъдат изпратено към библиотека със касети, която е наблизо е често срещан случай.

- **On-line**

Онлайн бекъп съхранение обикновено е най-достъпния тип съхранение на данни, при който може да се започне възстановяване на файлове за много кратък период от време, секунди. Добър пример е вграден хард диск или дисков масив (примерно вързана машина към SAN). Този тип съхранение е много удобен и бърз, но е и относително скъп. Онлайн съхранението е сравнително уязвимо към изтривания или презаписвания на файлове, както от невнимание, инцидентно, така и саботаж или вирус.

- **Near-line**

Near-line устройствата за съхранение са обикновено по-малко достъпни и по-евтини в сравнение със онлайн, но все пак са удобни и полезни за бекъм хранилищата на данни. Добър пример е библиотека със касети използвана за прехвърляне на носители на данни от дисков масив към едно от устройствата на библиотеката, където датата може да бъде прочетена или изписана. Общо взето има предпазни свойства близки до тези на онлайн.

- **Off-line**

Офлайн съхранението изисква от части директни човешки действия, за да се осигури достъп до хранилището: Примерно да се вкара касетка във лентовото устройство или включване на кабела. Поради причината, че данните не са достъпни от компютъра, освен във лимитиран период от време, във който те пишат или четат, те са защитени от цял клас грешки, които може да се случат във онлайн модела. Времето за достъп варира, в зависимост от това дали касетките се намират на същата локация или на външна (on-site или off-site).

- **Off-site data protection**

За да защитим срещу природни бедствия или други специфични за дадена локация проблеми, много хора избират да изпратят носителите на бекъпа към различна локация. Мястото за съхранение може да е примерно домът на администратора или някое място със специални условия, устойчиво на бедствия, със контролирана температура, висока сигурност, бункер и други. Също важно е да се знае, че копие на носителя може да е офсайт и да има и един онсайт (Примерно офсайт RAID mirror). Подобно копие не може да бъде наречено бекъп, и не трябва да се бърка със офлайн такъв.

- **Backup site or disaster recovery center (DR center)**

При случай на бедствие, данните на бекъп носителите няма да бъдат задоволително за възстановяване. Компютърните системи, на които данните трябва да бъдат възстановени за restore и правилно конфигуриране на мрежата също са нужни. Някои организации имат техни центрове за възстановяване на данните, които са оборудвани за тези случаи. Други организации имат договори за това със външни фирми със възстановяващи центрове. Поради причината, че Disaster Recovery центровете са голяма инвестиция, бекъпа рядко е считан за предпочитан метод за местене на данните към DR център. По-подходящ метод би бил mirroring на дисковете, което прави така, че DR данните да са със възможно най-новите им версии.

2. Библиотеки. Видове библиотеки.

В хранилищата на данни, библиотека с касети е комбинация от магнитно-лентови касети и устройства. Автоматизирана библиотека е хардуерно устройство, което съдържа във себе си множество лентови устройства за четене и писане на данни, места за достъп, предвидени за вкарване и изкарване на касети, както и роботизирано устройство за въвеждане на касетките в лентовото устройство без човешка намеса.

Във компютърните хранилища, библиотека с касети, понякога наричана „tape silo", „tape jukebox", "tape robot", съхраняващо устройство, което съдържа едно или повече лентови устройства, не малък брой слотове за държане на касетите, баркод четец, служещ за идентифициране на касетите, и автоматизирана система за въвеждане на касетите, робот.

Един от първите примерно за такава библиотека е IBM 3850 Mass Storage System (MSS), обявена през 1974 година, може да се види на *фигура 11*.

Фигура 11 *(Библиотека IBM 3850 MSS)*

За големи хранилища на данни, те са много добро решение като се има в предвид цената, със до скоро цена на гигабайт (GB) около 15 стотинки, или казано по друг начин, поне с 60% по-евтино от цената на GB на повечето хард дискове, също така касетите предоставят систематизиран достъп до много голямо количество данни. Минуса, който те имат в замяна на плюсовете придобити от големия капацитет е това, че имат по-бавно време за достъпване, което обикновено включва механично манипулиране на касетите. Достъпването на данните във библиотеките отнема от няколко секунди до няколко минути.

Заради бавното им последователно достъпване и огромния им капацитет, библиотеките със касети са главно използвани за бекъп и са като последна стъпка от дигиталното архивиране. Типично приложения накрая би било обширни транзакционни записи на организацията с цел направата правна проверка. Друго приложение на библиотеките е

Hierarchical storage management (HSM), при което библиотеката съхранява рядко използвани файлове от файловата система.

- **Autoloaders**

Това са по-малки библиотеки със само едно лентово устройство. Терминът аутолоадер по някой път е заменен със чейнджър (stacker), устройство при което касетата се поставя задължително във даден ред. Има и други видове аутолоадери, които могат да работят със оптични дискове, дискети или компакт дискове, пример за такъв аутолоадер е посочения на *фигура 12*.

Фигура 12 *(Аутолоадер StorageTek SL24)*

3. Устройства за съхранение от диск към диск (D2D – disk to disk). Видове D2D VLS устройствата.

D2D е съкратено от диск към диск (Disk-to-disk), вид бекъп хранилище за данни, във което данните са копирани от диск – обикновено хард диск – към друг диск – примерно друг хард диск или друг вид дисков носител. Във D2D системите, дискът, от който е копирана информацията обикновено се нарича основен диск, а дискът на който информацията се записва се нарича вторичен или бекъп диск.

Едно от предимствата на D2D-тата пред D2T (Disk-to-tape) системите е, че бекъпнатите файлове могат да бъдат достъпени директно, точно както на локалния диск. Касетите, от друга страна, трябва да бъдат претърсвани от началото до като се намери нужния файл, и така не е толкова бързо възвръщането на данни.

- **Предимства на диск към диск системите.**

- По-голяма скорост и по-голям капацитет, отнася се до касетките и дискетите, като в резултат получаваме по-кратък период на бекъпа и на възстановяването.
- Не-линейно възстановяване на данните, позволяващо ни файла, който ни трябва да бъде възстановен да се restore-не по-бърз о и по-лесно, за разлика от при касетите.
- По-ниска крайна цена на притежавания хардуер, заради това, че е повишено автоматизирането и цената на хардуера е по-ниска.

D2D или диск към диск е ефективна и качествена бекъп стратегия, която утилизира хард дисковете като хранилища, по-добре от системите със касетки.

Със падащите цени на хард дисковете и повишаващите се скорост и капацитет, използването на допълнителни хард дискове за D2D бекъпи е станало пословично без много мислене за индивидуални и фирмени интереси във подсигуряване на техните компютърни системи. Със развитието на RAID (Redundant Array of Independent Disks) също допринася за развитието на D2D бекъп стратегиите. Дъната, които подържат разнообразие от RAID, утилизира множество дискове по различни начини, за да увеличи скоростта, да осигури подсигуряване и поправка при грешки за дисковете. И със RAID и без RAID, D2D-тата бекъп устройствата предлагат множество предимства пред тези със касетките или оптичните дискове. Пример за D2D устройство са тези показано на *фигура 13 и фигура 14* като по-долу ще бъде казано повече за тях.

Фигура 13 *(VTL устройство Quantum DXi8500)*

Фигура 14 *(StoreOnce D2D backup device B6200)*

- **Видове D2D**

Съществуват два типа D2D-та: Истински Disk-to-disk устройства и виртуални библиотеки (VTL D2D). Втория вид устройство не е истинско D2D защото то подържа индексиране на файловете подобно на това при касетките. Въпреки че е по-бързо от тях и, все пак включва и неговите си ограничения.

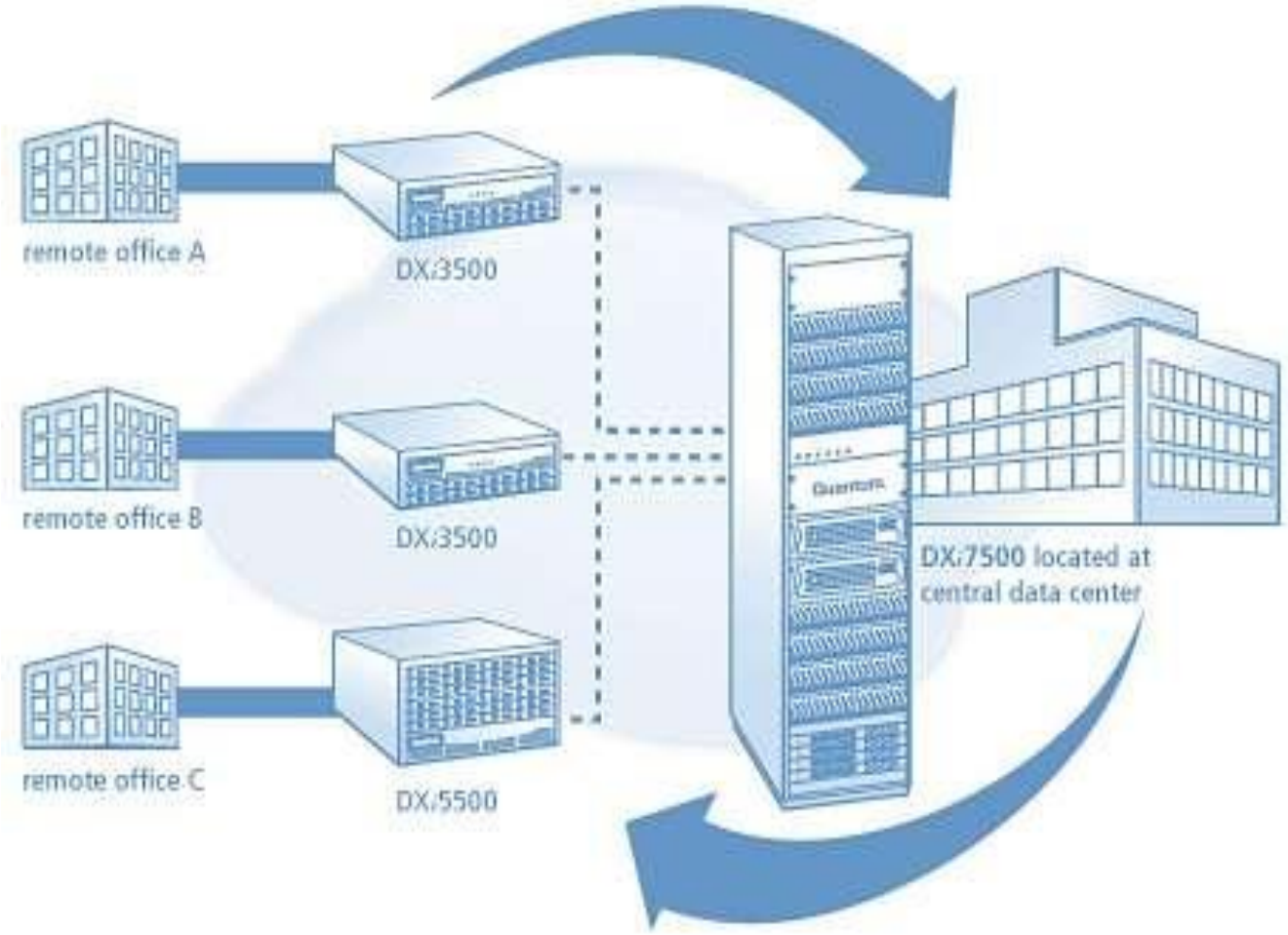
Докато служат за своята цел, хранилищата със касетки имат много слабости и неща, за които да се безпокоим. Примерно ако за файла, който трябва да бъде възстановен, първата задача е да се намери точната касета, която съдържа този файл. След това касетата трябва да бъде прочетена от лентовото устройство, процеса може да отнеме няколко минути. Чак след като файла е намерен, той може да се прехвърли, но дори и този процес по някога е бавен. Други проблем е това, че понякога има „лоши“ касети, износване на лентата и неизправности на лентовото устройство.

Сложността на тези притеснения, операционна система, програми, мултимедийни файлове и постоянно растящите мрежи, правят идеята за възстановяване на системата още по-немислима. Бавния процес на бекъп и рестор на касети става все по-недостатъчен.

Благодарение на достъпните, високо капацитетни хард дискове, D2Dтата са перфектния избор за бекъп. Без значение дали се използва RAID масив за голяма корпоративна мрежа или допълнителен хард диск като скрит такъв, Диск към диск може да засенчи други бекъп стратегии многократно. D2D предлага „моментален“ бекъп и възстановяване, защото системата разпознава бекъп файловете като оригинални. Няма нужда от касета за набавяне, поставяне и сканиране, и няма допълнителни устройства, които да се развалят. Файловете са винаги под ръка, възвръщаеми само със „един клик, без нужда от поддържане на допълнителни архиви, като при касетките. D2D-то се използва с SATA RAID, както също предлага “гореща смяна“(Hot-swapping), когато вградената мониторинг система предупреди, че диск във масива е станал „лош“. Още повече D2D-то има пълната скала за капацитета, където капацитета на дисковия масив може да достигне до терабайти. Общо взето няма много „живото застрашаващи“ минуси при използването на Disk-to-Disk, докато има не малко предимства.

3.1. Replication – Това представлява копиране на инфорамцията от едно място на друго, от едно D2D устройство на друго, в случай на злополука, пожар, природно бедствие, кражба, или каквото и да е, което може да застраши информацията намираща се на това устройство. Принципно второто устройство, на което се прави репликация, се намира в близост между 2 до 30 километра от основното. Чрез нея се постига по-голяма сигурност на съхранената на дадени устройства информация.
Репликация може да се прави както и на две еднакви устройства, така и от малки D2D устройства към едно голямо D2D устройство, както може да се види на *фигура 15*.

Фигура 15 *(Репликация от няколко малки D2D устройства към едно голямо)*



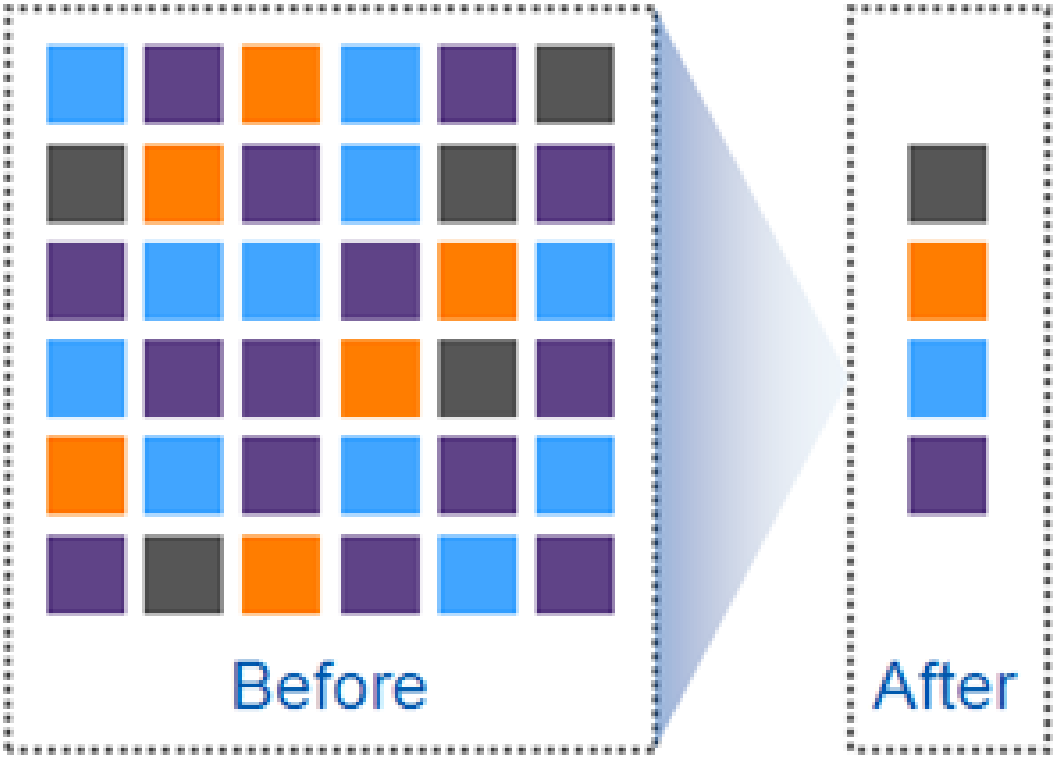
- Дори за домашните потребители, е хубаво да имат вариант за репликация. Представете си, че сте си направили бекъп на важните файлове на флаш памет, и знаете, че са там, но тази флаш памет се развали, то тогава вие няма да имате тези данни ако изтриете оригиналните. Хубаво е винаги да има вариант за допълнително предпазване на данните.

- Репликацията в големите компании служи също така, в случай че главното устройство се развали, да може да се продължи работата на второто, във втората локация, без да спира процеса, без да има загубени данни и без да има недоволни потребители.

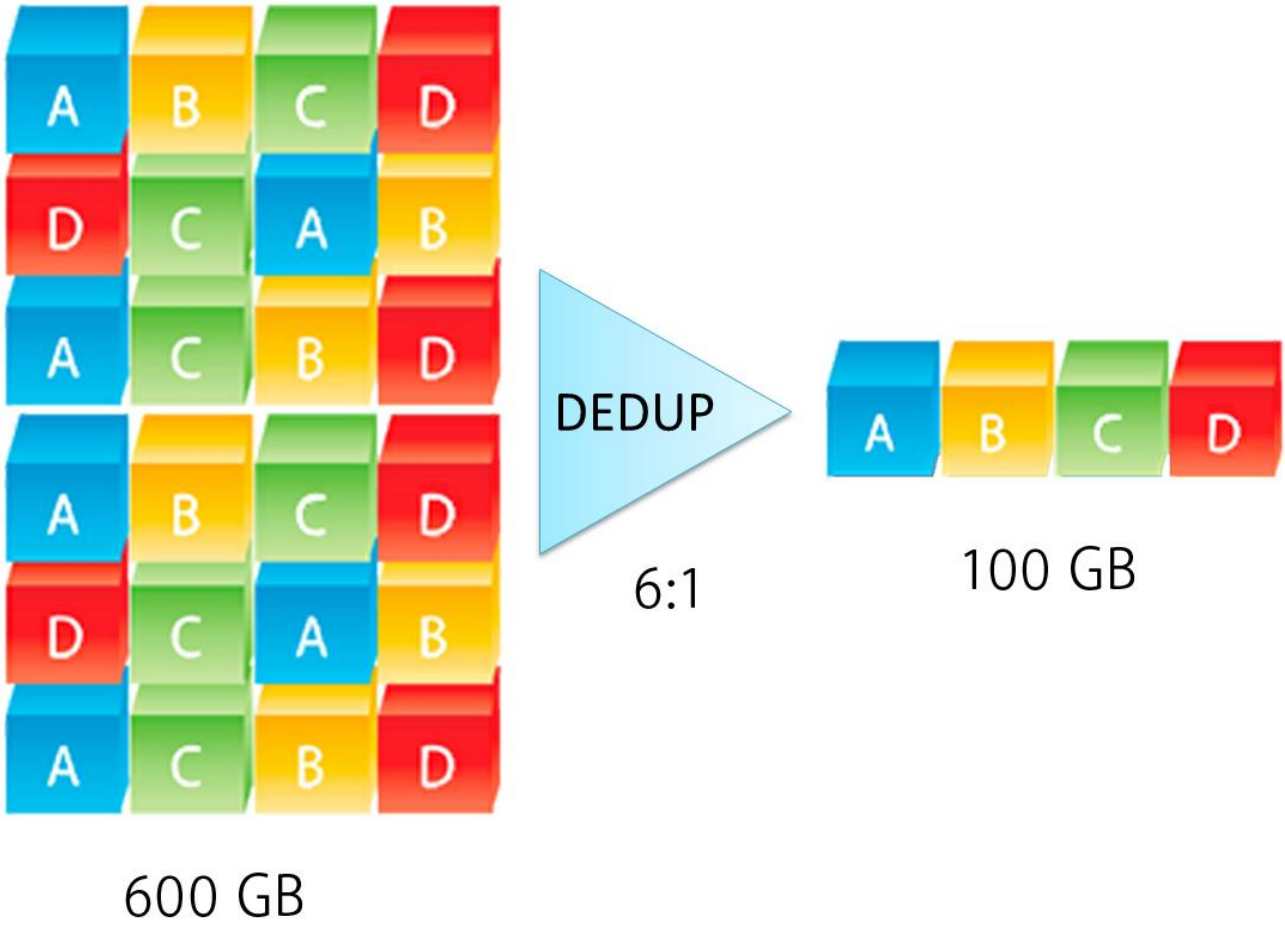
- Репликацията при по-натоварените от бекъп устройства се прави през деня, тъй като бекъп операциите по принцип вървят нощем. Идеята е да не се товари устройството от нея, и да може да си мине самостоятелно през деня.

3.2. Deduplication – В средата на информационните технологии, дедупликация е специализирана техника за компресиране на данните, която служи за елиминиране на повтарящите се копия на файловете. Тази техника се използва, за да се подобри вместимостта и използваемостта на устройствата за съхранение на данни като D2D и VLS. Също така може да се използва при трансфера на данни в мрежата, като намалява броя на байтовете, които трябва да бъдат изпратено. В процеса на дедупликацията, онукални парчета от данни или байтова, се сравняват и съхраняват в специално място за копирането им, и когато има съвпадение, излишните парчета се заместват със малка като размер връзка към уникалното парче, което е запаметено в специалното място за това. Това парченце може да бъде намерено стотици, дори хиляди пъти, като съвпадението зависи от размера на парчето. По този начин трансфера на информацията може да стане много по-бързо и много по-малко данни да бъдат изпратени. На *фигури 16 и 17* може да се види нагледно какво представлява и как работи дедупликацията.

Фигура 16 *(Deduplication Пример 1)*



Фигура 17 *(Deduplication пример 2)*



- От *фигура 16 и 17* би трябвало да е станало ясно какво представлява процеса на дедупликация. При бекъп на D2D и VLS устройства това е най-важното и печелившото решение, тъй като голяма част от информацията е повтаряща се. Системни файлове на Windows, някои програми, както и други неща. Също при всекидневен бекъп снимките, музики, както и други големи файлове се повтарят и чрез дедупликацията съответно не заемат реалното място, а само се създава линк към оригиналния файл

3.3.Предимства и недостатъци на D2D, VLS и TL устройствата.

Предназначението на трите устройства е предимно и само за бекъп. Tape Library устройствата се използват само за бекъп, те са най-сигурните за

сметка на скоростта и цената на GigaByte. Касетките са най-издръжливи във времето, след Solid state drive-овете, които са много скъпи. D2D и VLS устройствата си приличат по това, че използват RAID 5 или 6, повечето от тях, поне по-големите, използват deduplication, една от разликите им е, че софтуера е различен.

4. SAN и NAS устройства

4.1. Какво е SAN

SAN, представлява отдадена мрежа, която предоставя достъп до консолидирани данни в хранилище, използващи блоково ниво на разцепване на информацията. SAN-ът се използва главно за да подсили устройствана съхранение на информация, като дискови масиви, библиотеки с касетки, оптически устройства, които са достъпни до сървъри, на които тези устройства излизат като локално закачени към операционната система. SAN-ът по принцип си има негова мрежа от логални устройства за съхранение на информация, които по принцип не са достъпни през нормалната LAN мрежа, от други устройства. Цената и сложноста на SAN са паднали значително от 2000-ната година насам, като става достъпно както за големи, така и за по-малко компани. Той не осигурява опериране с файлове на файлово ниво, а само операции на блок ниво. Хубавото е, че файлови системи базирани на SAN осигуряват достъп на файловете на файлово ниво. Те са познати като SAN файлови системи или споделени дискови файлови системи.Историческите дейта центрове първо са създадени от директно закачени дискове, създаващи дискови масиви, като всеки е отдаден само на 1 програма, която го използва, и е видим като брой от виртуални хард дискове (LUN).Операционните системи управляват техни файлови системи, със не споделени LUN-ове, като те са локални за тях самите. Ако няколко системи се опитат да споделят един и същ LUN, то те ще взаимодействат една друга и данните на тези дискове ще бъдат заличени. Всички планирания за споделяне на данни на различни компютри със 1 LUN изисква по-напреднали решения на този проблем, подобни на SAN файлова система или клъстериран компютър. Въпреки тези проблеми, SAN-ът помага за увеличаването на дисковия капацитет и ютилизирането му, като множество сървърни компютри консолидират техния storage на дисковия масив.

Главните ползи от това включват осигуряване на споделяне на данните, които изискват бърз достъп. Пример за това са малки е-майл сървъри, база данни, и многоизползвани файлови сървъри.

4.2. Какво е NAS

NAS е сървър за споделяне на данни на файлово ниво, свързан в компютърна мрежа и даващ достъп до данните, които са на него, на подбрана група от клиенти. НАС-ът не само работи като файлов сървър, но е и специализиран в тази си негова задача чрез хардуера, софтуера и конфигурирането на тези му елементи. Той е често направен като компютър, специализиран и направен за съхранение и предоствяне на данни.

От 2010 година, NAS устройствата започнаха да добиват популярност, като удобен начин за споделяне на файлове сред множество от компютри. Потенциалните ползи от предназначен за използване NAS, в сравнение със сървър за общо ползване и за споделяне на файлове, включва по-бързия достъп до данни, по-лесната администрация и лесното конфигуриране.

NAS системите са мрежови устройства, които съдържат един или повече от един твърди дискове, често наредени в логичестки, масив с излишък, RAID. Мрежови вързания масив от дискове, премахва отговорността на файлов сървър да бъде някоя машина в мрежата. Обикновенно осигуряват достъп до файловете използвайки споделянето на файлове в мрежата с протоколи като NFS, SMB/CIFS или AFP

Трябва да се има предвид, че хард дискове съдържащи NAS в тяхното име функционират подобно на другите хард дискове, но може да имат различен firmware, толеранс на вибрациите или да изискват различна сила на тока, за да може това да ги направи подходящи за използване в RAID масиви, които са използвани често в NAS имплементациите. В един RAID масив, когато някой от дисковете се развали, то информацията се взима от другите дискове за да да възобнови, за да може това да се случи, то трябва да се изключена дадена опция на диск-а.

NAS устройство е компютър вързан в мрежата, който предоставя само базирано на файлово ниво споделяне на файлове до други устройства в мрежата.Въпреки, че технически може да подкарва различен софтуер, то той не е проектиран да бъде в някаква главна роля, а е предназначен само за споделяне на файлове. Примерно, NAS-а обикновено няма клавиатура или дисплей, и се управлява и конфигурира през мрежата, често използвайки WEB броузер.

За тези устройства няма нужда от пълна оперцаионна система. Често се използват урязани такива, пример са FreeNAS или NAS4Free, като и двете за безплатно дистрибутирани и са урязани версии на FreeBSD. Тези устройства съдържат един или повече хард дискове, често обединени логически във RAID.

Главната разлика между директно закачените хранилища и закачените хранилища в мрежата (DAS vs NAS) е, че DAS е просто разширение на вече съществуващ сървър и не е задължително да е видим в мрежата. NAS-ът е проектиран за лесно съхранение на данни на него и за споделяне на файлове в мрежата. Както DAS така и NAS може да увеличи свободното пространство на даден сървър, използвайки RAID или клъстеринг. Когато и NAS и DAS са вързани през мрежата, тогава NAS-а ще има по-добър перформанс, защото НАС устройството е направено за споделяне на файлове, което е по-малко вероятно за направа на сървър, на който не е единствената работа споделянето на файлове. И двете устройства може да имат голямо количество памет, което подпомага за доброто представяне. NAS устройствата не може да се преправят от към Процесор, рам, , софтуери и други, те биват фиксирани.

4.3.NAS и SAN – различия, прилики и взаимосвързващи ги неща

NAS устройствата предоставят и хранилище за данни и файлова система. Това често контрастира със SAN устройствата, които предлагат само предоставяне на място в хранилища на блок ниво и оставят грижата за файлова система на клиента. SAN протоколите включват Fibre Channel, iSCSI, ATA over Etherner и HyperSCSI. Един от начините за разграничаването на значенията на NAS и SAN е, че NAS

устройствата излизат на операционните системи като файлов сървър, докато SAN устройствата излизат като физически диск.

Въпреки техните разлики, те не са чак толкова независими един от друг и може да се комбинират до направата на SAN-NAS хибрид, който предлага и файловата система на NAS устройствата и протоколите за достъп на блоково ниво на SAN-а от същата система. Пример за това е софтуера Openfiler, безплатен софтуер, вървящ на Линукс базирани системи. Споделена дискова файлова система също така може да бъда подкарана на основата на CAH, за да предостави услогите на файловата система.

NAS е разработен преди да се е била появила нуждата от SAN, като решение за ограниченията на традиционно използвания директно закачен диск, в който индивидуалните устройства за съхранение на данни, като хард дискове, са свързани директно за васеки индивидуален компютър и не се споделят. И при NAS и при SAN различни компютри в мрежата, може да споделят централизирана информация, през LAN, която се намира на SAN или NAS устройство.

4.4. Използването на SAN и NAS в и за Backup

Backup-а и SAN-а вървят ръка за ръка. Със постоянно растящия обем от информация, голямата скорост при копирането на информацията на D2D, VTL, или то било TL устройства, е изключително важно. За това се включва SAN. Първото хубаво при използването му е, че за Backup-а не се използва LAN мрежата, която се използва и от потребителите на дадена машина, а се използва отделна мрежа, отдадена само за Backup, мрежа, която е на базата на SAN. При бекъп мрежата скоростта е много по-голяма, благодарение на Fiber channel окабеляването, което позволява от 1GB/s до 16GB/s, като масово за момента се използва със 4GB/s. Качественото изграждане на CAH мрежата е от голямо значение, и за това трябва да отговарят специалисти, които да изградят една качествена инфраструктура, без проблеми и ограничения от която и да е страна.

NAS устройствата също могат да се използват за направата на бекъп върху тях, тъй като са споделени във цялата мрежа и са достъпни от всички компютри/сървъри. Копирането на информацията ще става по-

бавно от колкото през SAN, тъй като NAS устройствата са споделени в мрежата през LAN, а там скоростта е по-малка и се използва също така от другите устройства в мрежата и е ограничена.

От друга страна, тъй като NAS устройствата се използват за хранилища на данни, и съдържат голям обем от информация, то и те трябва да се backup-ват. Това е по-сложно от нормален бекъп на една машина. Големината на един NAS дял може да достига над 10TB, което има своите недостатъци. За да може да се копира информацията по-бързо било то на библиотека с касетки, дисков масив, D2D, VLS, то е хубаво да е през SAN, заради по-голямата скорост. За да може да се прави бекъп на NAS, то трябва да бъде конфигуриран по различен начин устройството на което се бекъпва.

5. Различни видове софтуер използвани при backup, restore и архив

При архивирането разнообразието на софтуер, който може да се използва, не е толкова голям колкото при бекъп-а.
Главните софтуерни програми, които може да се използват за направата на backup и restore са:

5.1. Data Protector (DP) – Софтуер на Hewlett Packard, който се използва предимно от големи компании. В приложените изображения под точка 5.1. може да се видят основните менюта на Data Protector софтуера, както и съответните обяснения към тях:

- Главен екран на Data protector, *Фигура 18* (Main menu DP) може да бъде намерена в *Приложение 1*. На него се вижда специално Monitor таб-а. На този таб може да се видят всички текущо вървящи бекъп задачи.

- 1 – File– От него може да се избират опции за настройки на изгледа на софтуера, както и много други настойки.

- 2 – Edit – От тука може да се използват нормалните опции за копиране, както и други настройки, специално създадени за софтуера DP.

- 3 – View – Настройки на изгледа на менюто.

- 4 – Actions – От тука може да се правят различни операции свързани със backup задачите.

- 5 – Help – От тука може да се види информация относно версията на софтуера, наличните пакети, които са добавени, различните добавки към него, както о помощни гайдове.

- 6 – Бутон за връзка към други медиа сървъри. Може да се избира между различни сървъри в мрежата, които са с инсталиран DP.

- 7 – Падащо меню за избор между различните Data Protector менюта.

- 8 – Current Sessions – Под тази лента, както и в дясно на нея, се показват настоящо вървящите бекъп задачи. Тя е налична само във Monitor таб-а.

- 9 – Status – Това показва текущия статус на бекъп задачата. Те биват:

    - In progress – В момента върви, пише/чете, *фигура 16.*

Фигура 16 *(In progress status)*

    - Pending – В момента не върви. Изчаква за свободно устройство за писане/четене.

    - In progress/failures – В момента върви, но има грешки, които ще попречат на backup задачата да завърши изцяло. Най-вероятно ще трябва да се направи проучване за причината и да се стартира наново

- In progress/warnings – В момента върви, но има грешки, които най-вероятно няма да навредят на целостта на backup задачата.

- Completed – Бекъп задачата е цялостно завършена, *фигура 17*.

***Фигура 17** (Completed status)*

- Completed/failures – Бекъп задачата е завършила с грешки, които са навредилина целостта и. Ще трябва да се стартира отново след като се отстрани причината, *фигура 18*.

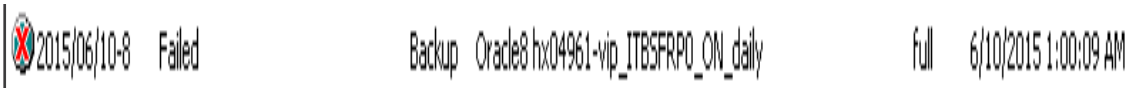
***Фигура 18** (Completed\Failures status)*

- Completed/errors – Бекъп задачата е завършила с грешки, които по-често не вредят на целостта, *фигура 19*.

***Фигура 19** (Completed/Errors status)*

- Failed – Бекъп задачата не е завършила. Била е прекъсната автоматично, поради това, че машината, която се бекъпва е била изключена, нямало е връзка към нея, или друга причина, *фигура 20.*

***Фигура 20** (Failed status)*



- Aborted – Бекъп задачата е прекъсната от потребителя или е прекъсната от променлива зададена по конфигурационните настройки на софтуера, *фигура 21*.

***Фигура 21** (Aborted status)*

- 10 – Type – Тип на бекъп задачата. Те биват:

    - Backup job – Те могат да бъдат различни типове, дали ще са File system, Oracle, MSSQL, Exchange и т.н.
    - Copy – Това са задачи, които имат за цел да прехвърлят информацията от едно място на друго, по принцип се прави от D2D библиотека, VTL, към физическа библиотека, TL.
    - Restore – Това е операция на възстановяване на данни от вече направен Backup.
    - Media – Това е операция, която има за цел да провери ID-то на дадена касетка или да я форматира, както може и друг тип операция със касетка, било то физическа или логическа.

- 11 – Owner – Притежателя на дадена операция. В повечето случаи, това е настроение притежател в конфигурационните файлове на DP софтуера, като ако се пусне от някой потребител, то се изписва неговия акаунт.

- 12 – Session ID – Това е ID-то на сесията, с която е стартирала дадена операция. То е уникално и не се повтаря. От типа 2015/01/01-1 е, като първата цифра е годината, втората цифра е месеца, третата е деня и четвъртата цифра е поредния номер на операцията за дена.
- 13 – Start Time – Това е часът и датата, в която е започнала дадена операция.

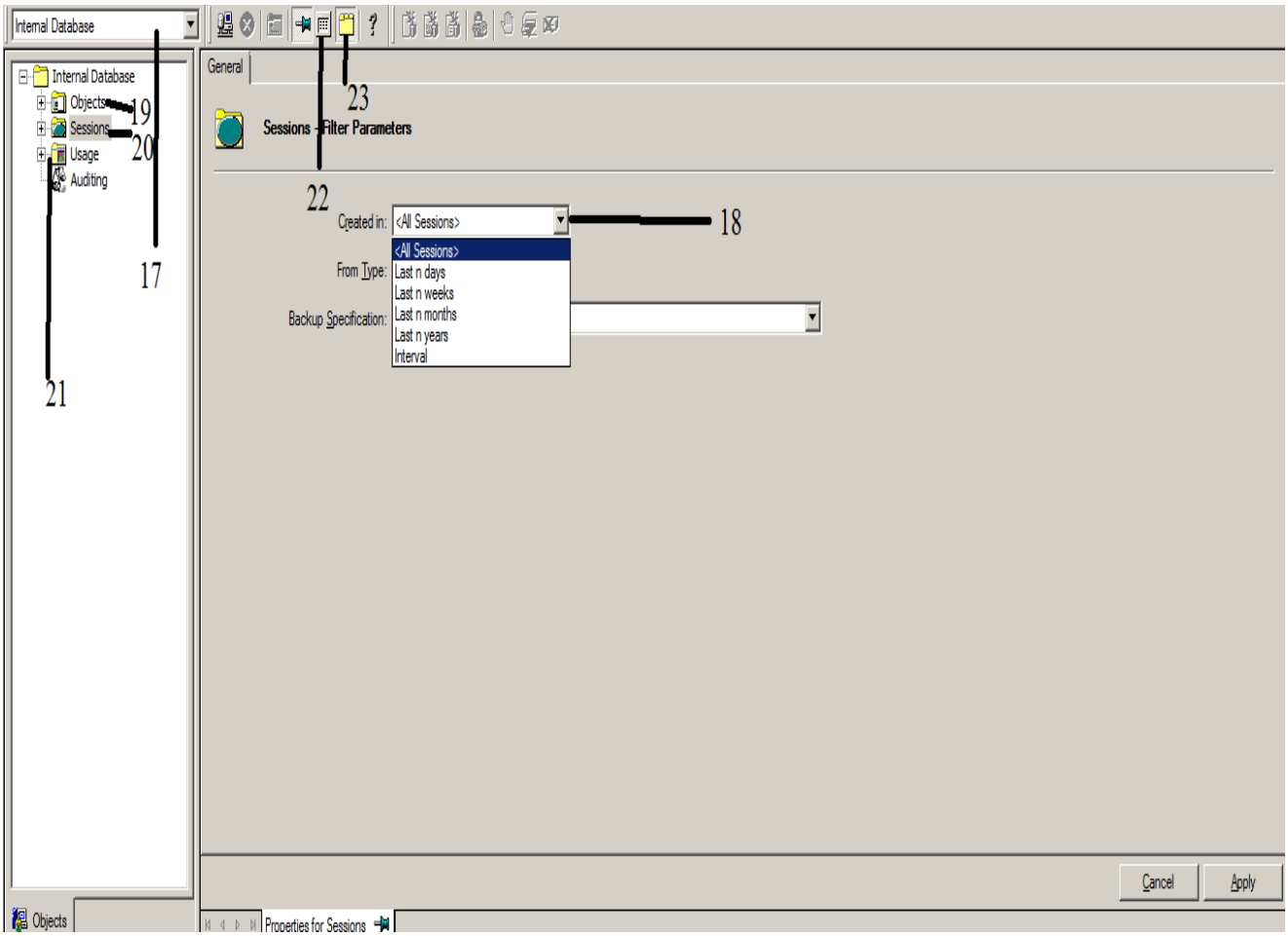
- 14 – Specification – Това е името не спецификацията, която в момента върви.

- 15 – Abort session – С натискане на ръчичката може да се прекрати дадена операция, нарича се Abort.

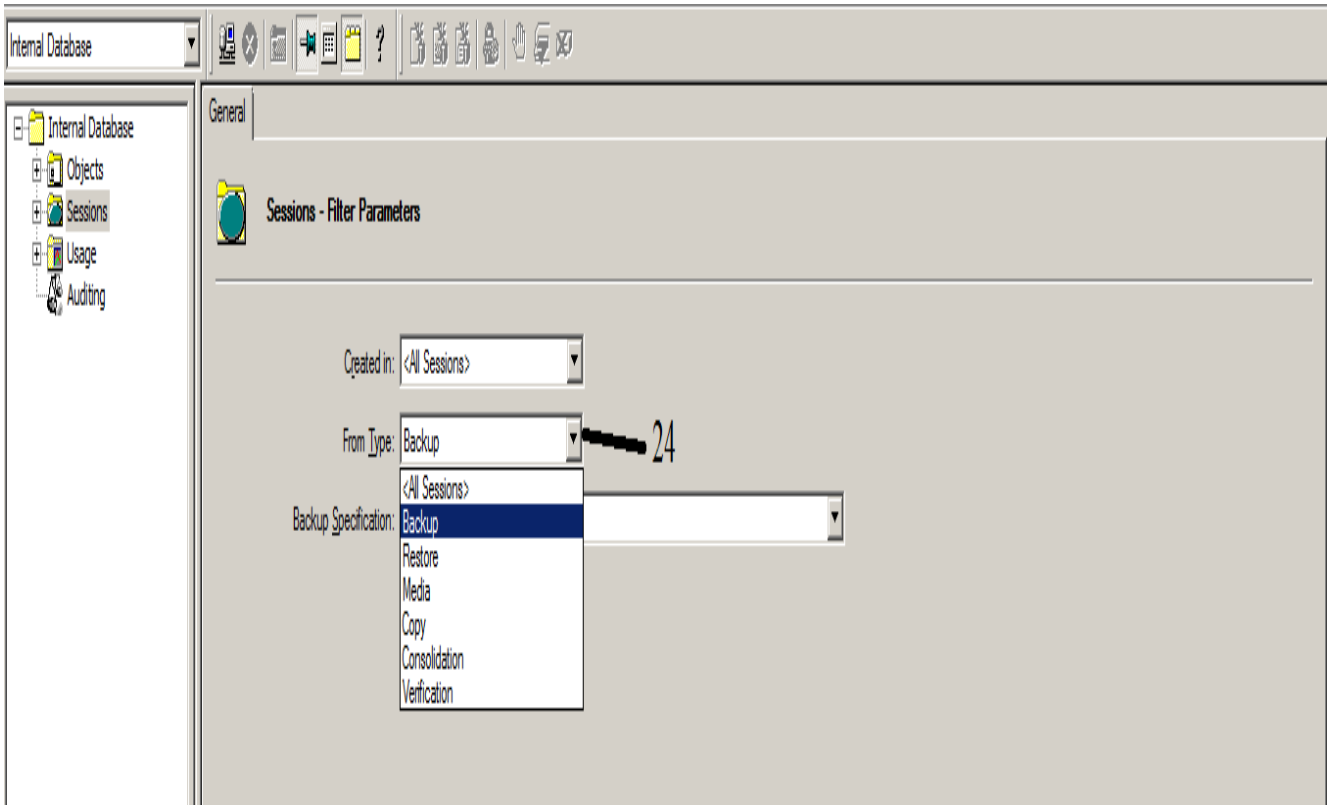
- 16 – Там се намира името на машината, на която в момента сме се закачили към Data Protector софтуера.

- Менюто Internal Database. В него могат да се видят всички операции, които са минали, независимо дали Backup, Copy Job и т.н. Във *фигури 22, 23, 24 и 25* може да се види изгледа от Internal Database менюто.

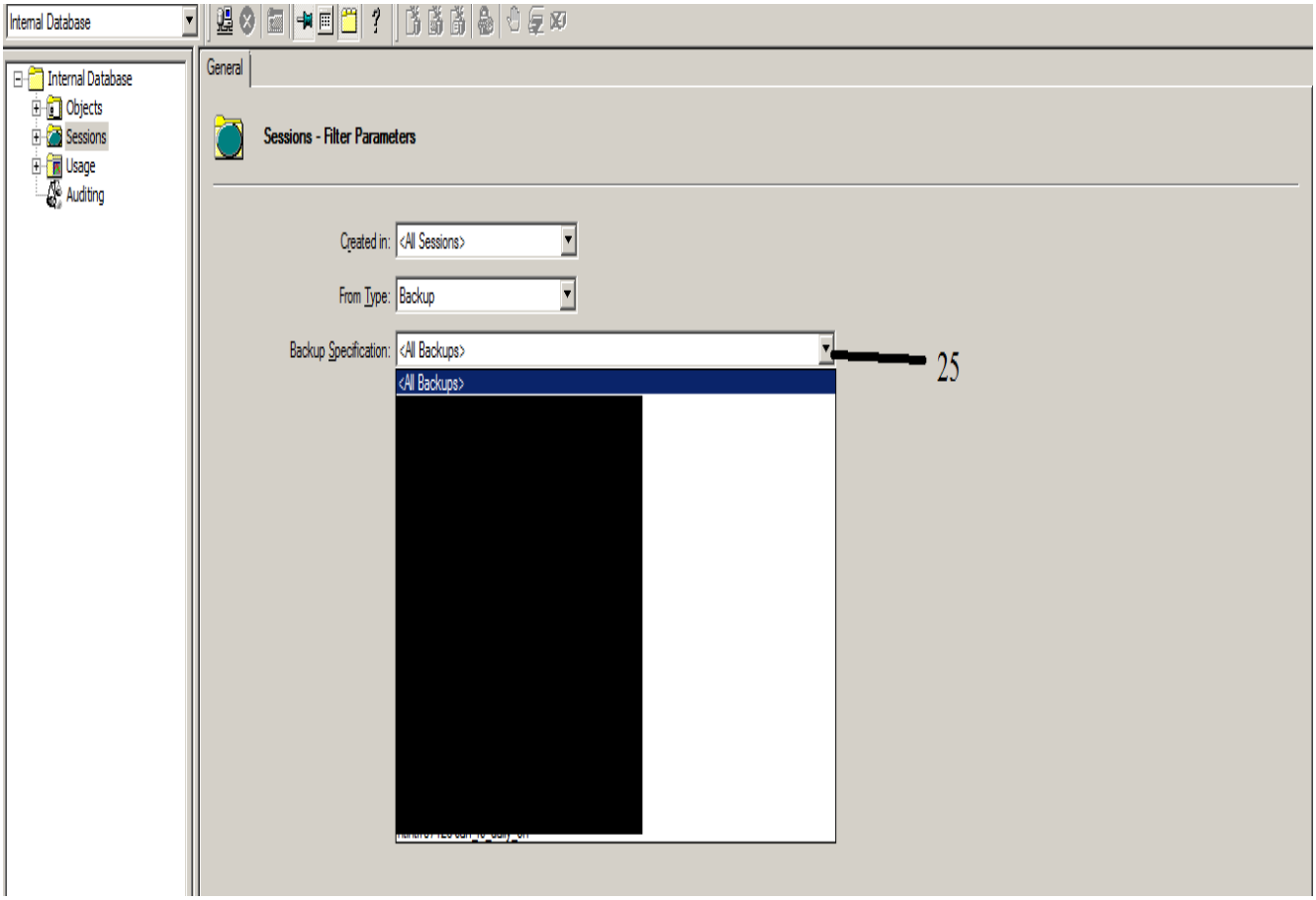
Фигура 22 *(Internal database menu – Created In)*



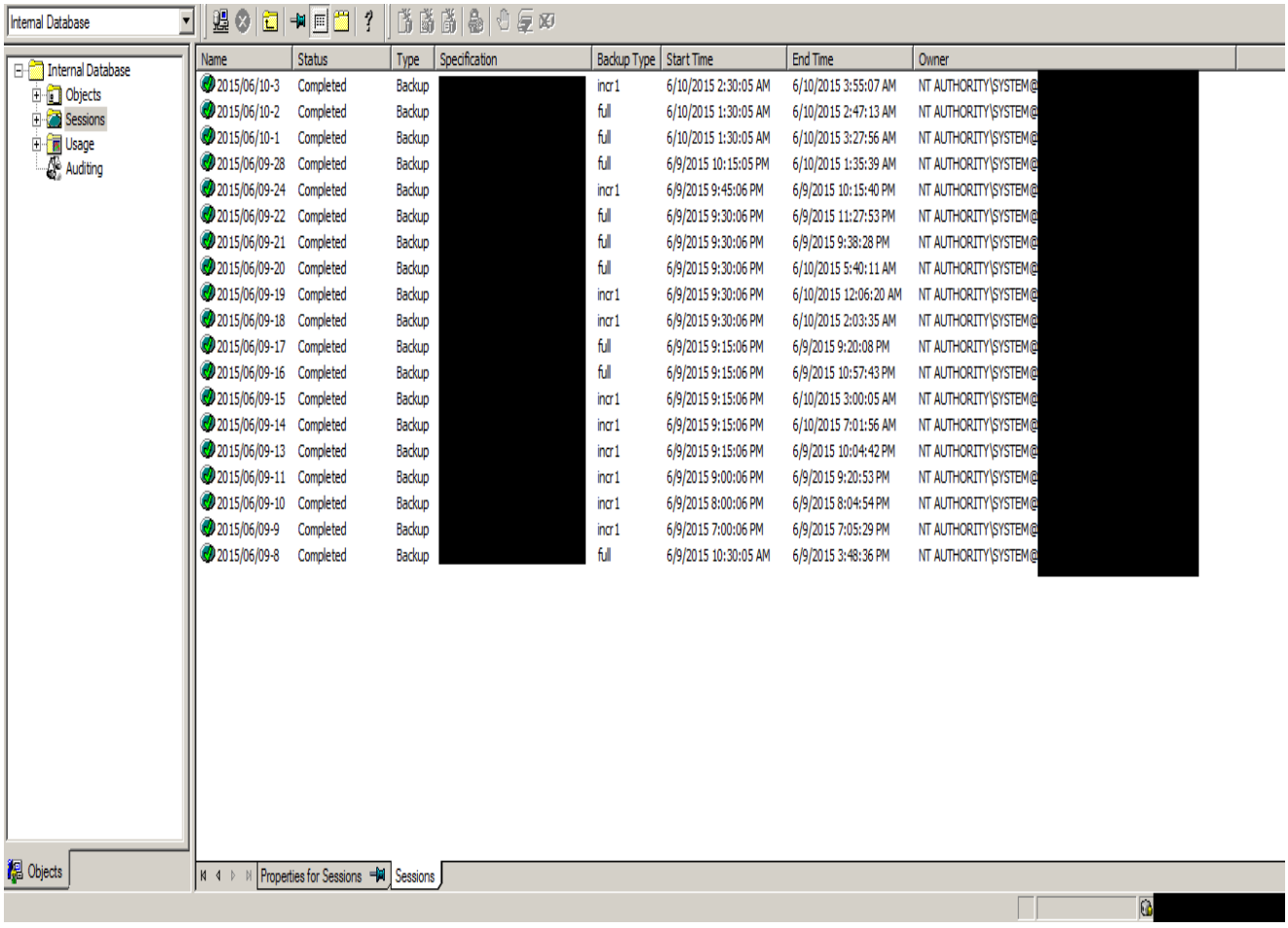
Фигура 23 *(Internal database menu – Избор на вида на показаните сесии в IDB)*



Фигура 24 *(Internal database menu – Избор на Backup спецификацията за показване)*



Фигура 25 *(Internal database menu – Главен изглед)*



- 17 – Падащо меню – От него може да се преминава през всички менюта, които са:
    - Internal Database
    - Monitor
    - Backup
    - Restore
    - Users
    - Objects
    - Reports

- 18 - Created In – От тука може да се избира интервала, за който да показва изминалите операции.

- 19 – Objects – Всички сървъри, които се намират на този cell server.

- 20 – Sessions – Може да се видят всички сесии, които са изминали в зададения период от време от потребителя.

- 21 – Usage - Тъй като Internal Database (IDB) на DP се запълва, от това меню може да се види, колко точно е изразходвано.

- 22 – List view – Преминаване от един изглед на друг. В зависимост от нуждитена потребителя

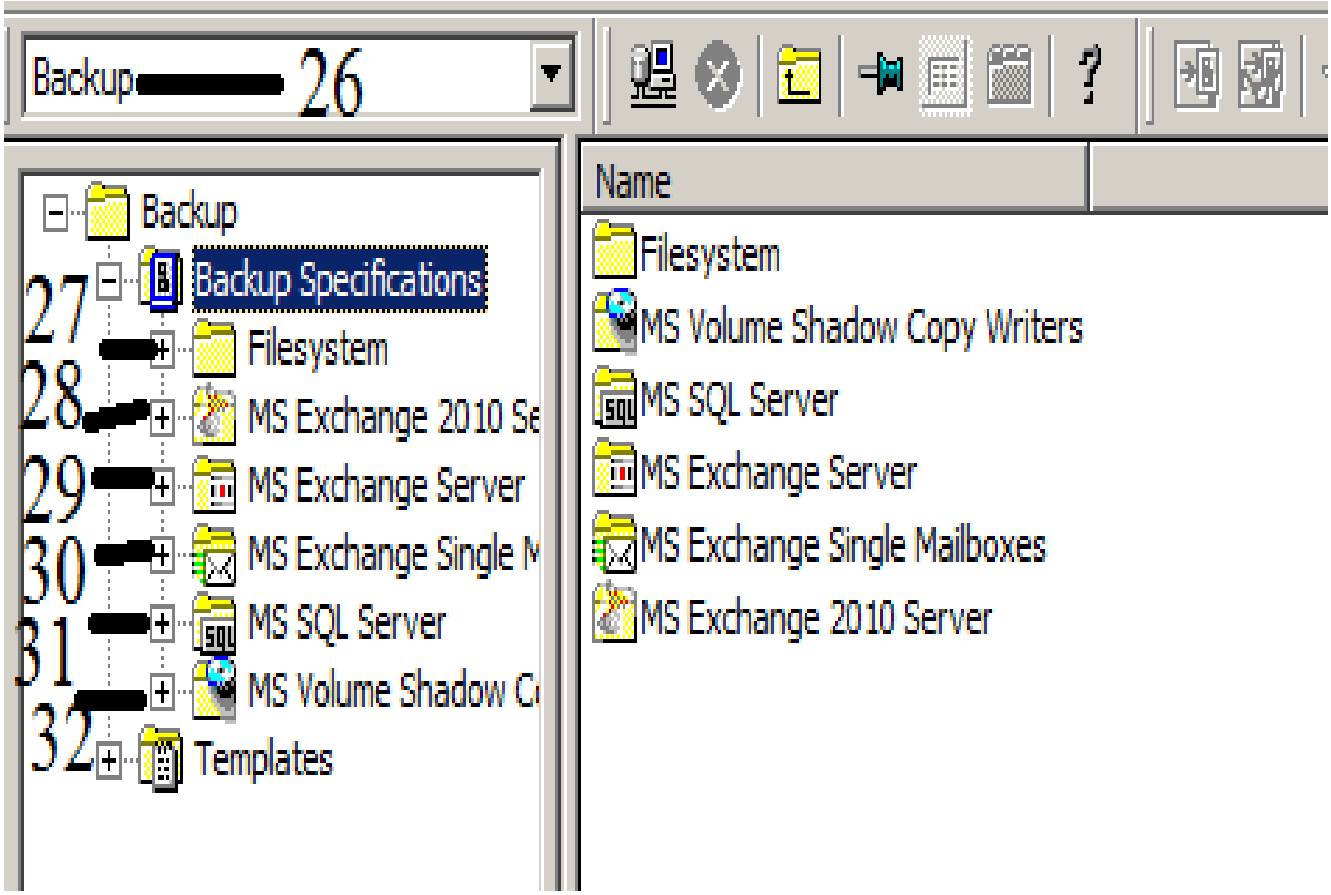
- 23 – Folder View

- 24 – File Type – От тука се избира файловия тип на задачата, Backup, Copy Job или друга.

- 25 – Specification – От тука се избира точна спецификация, която ви трябва да проследите за даден период от време в IDB менюто.

- Менюто Backup. От него може да се гледат вече конфигурирани бекъп задачи, или да се създават нови, *фигура 26*.

***Фигура 26** (Backup tab в DP)*



- 26 – Backup menu – Може да се превключо от падащото меню на друго при жуда.

- 27 – Filesystem – Това е нормалния тип бекъп. Прави се backup на цяла сървър, на даден файл, на зададен дял от операционната система или при избор.

- 28 – MS Exchange 2010 Server – Това е най-новата версия на Exchange backup. При него се прави бекъп на определени файлове, съобразено със Exchange базата.

- 29 – MS Exchange Server – Това е по-старата версия на Exchange беркъп.

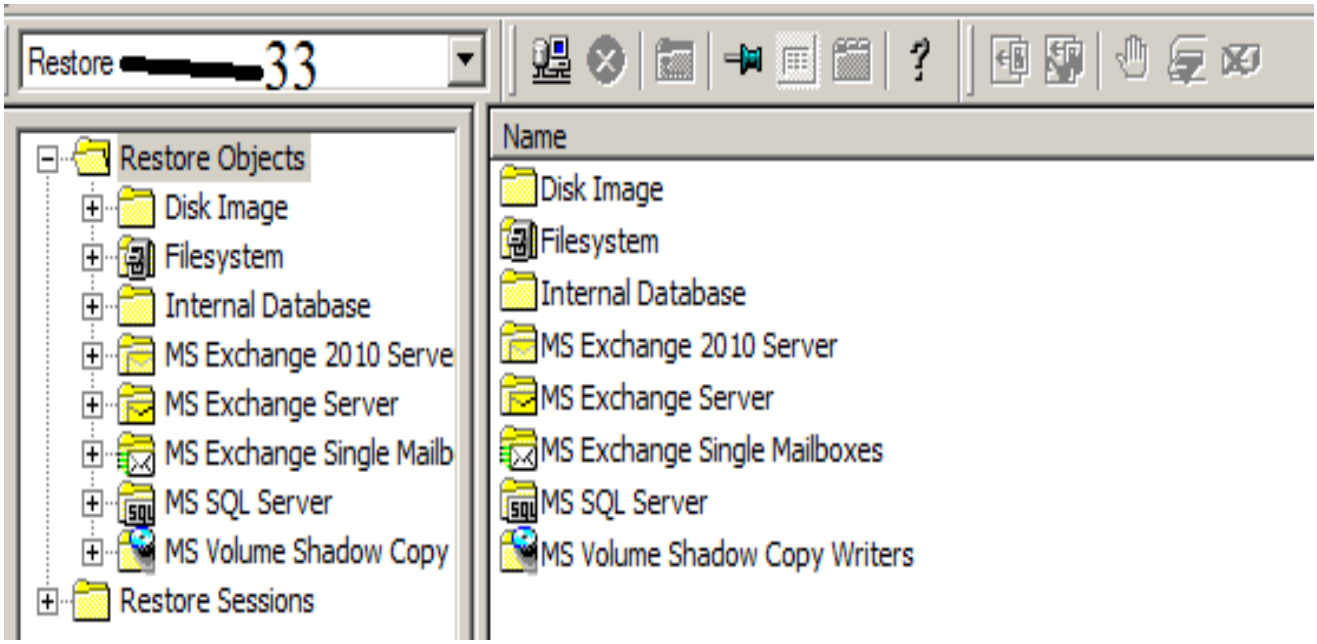
- 30 – MS Exchange Single Mailbox – При този бекъп се прави само на една пощенска кутия, за разлика от другите 2.

- 31 – MS SQL server – Този тип бекъп е на SQL база. Настройките се различават от Filesystem и Exchange.

- 32- MS Volume Shadow Copy – Backup със VSS-и.

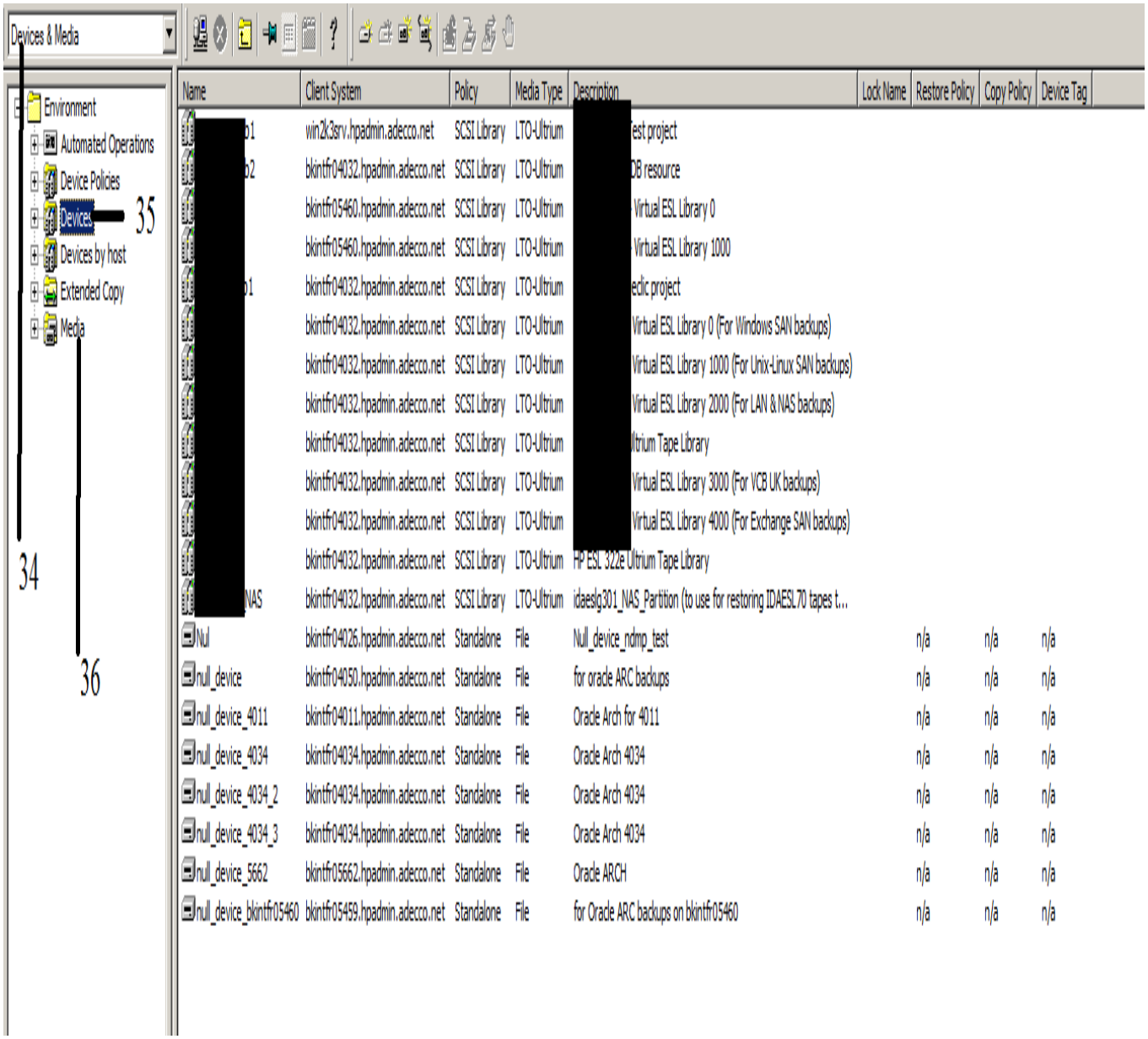
- 33 – Restore меню – От него може да се избира Restore операция от вече направен Backup. Може да се избира по бекъп сесия, по име на сървъра и т.н., *фигура 27*.

Фигура 27 *(Restore tab в DP)*

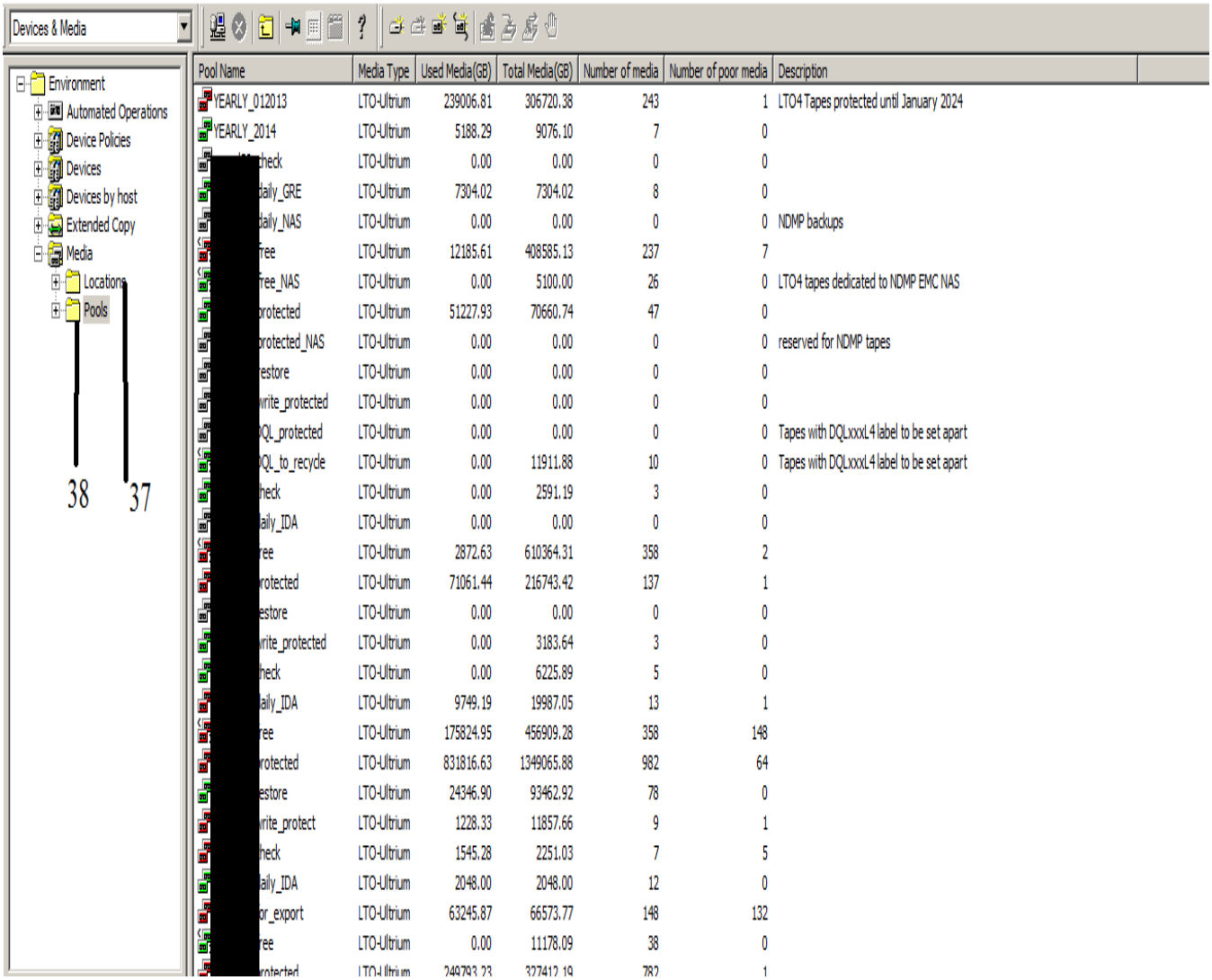


- Меню Devices – Тука може да се видят всички налични устройства, конфигурирани към даден cell server, изглед от меню Devices може да се види на *фигури 28 и 29*.

Фигура 28 *(Главен изглед от меню Devices & Media)*



***Фигура 29** (Изглед от Devices & Media – Media Pools)*



- 34 – Меню Devices & Media – От него може да се конфигурират устройства и да се правят различни операции с касетки.

- 35 – Devices – От това меню се конфигурират всички библиотеки, които се виждат на даден cell server.

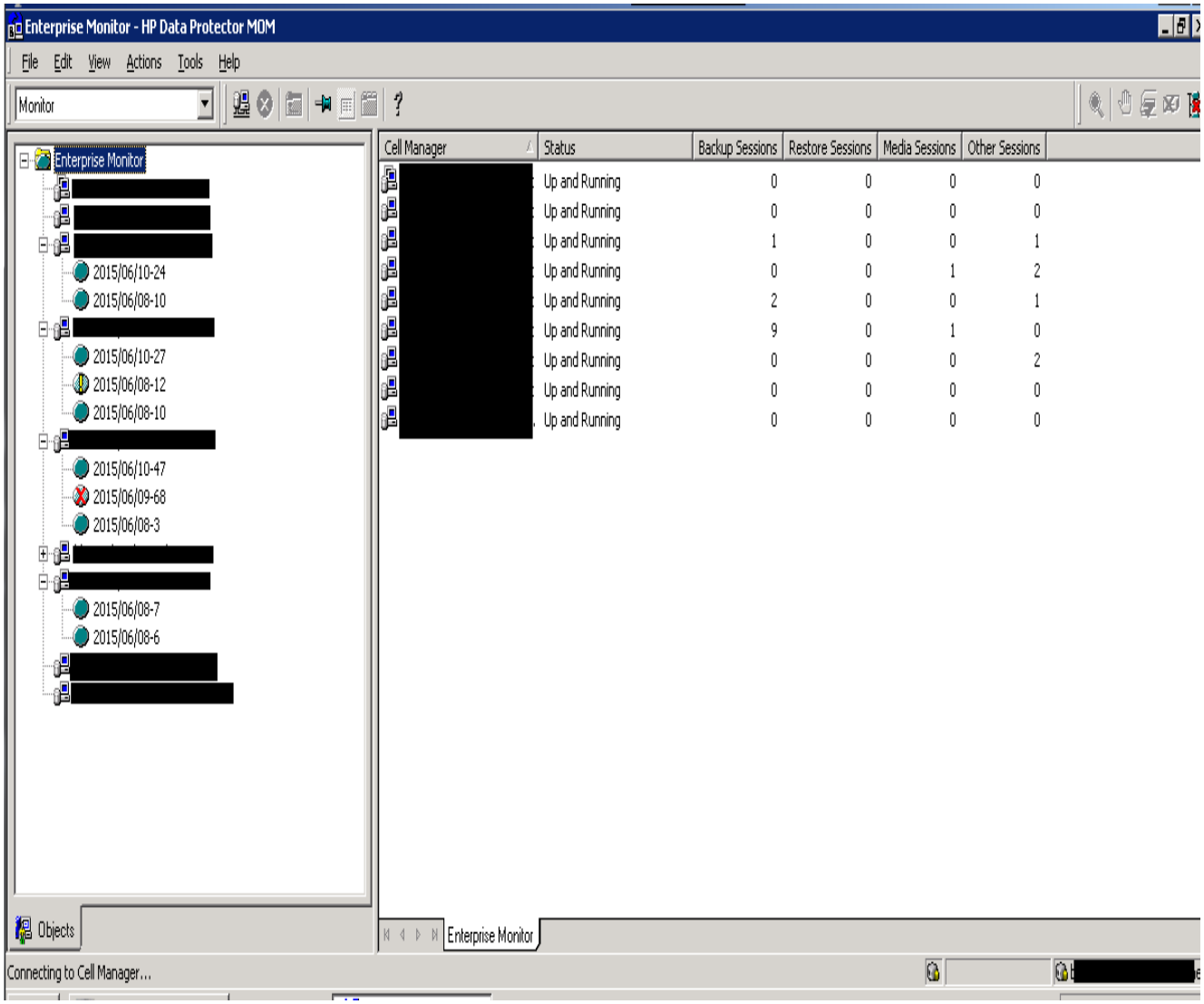
- 36 – Media – От този таб може да се видят всички касетки в избрана от потребителя библиотека. Може да се правят различни операции

- 37 – Location – Това са логически зададени дестинации на касетката. Дали ще бъде с името на някой, за да знае, че е касетка използвана от него. Също location може да е дадена библиотека.

- 38 – Pool – Това представлява логическо обединение на касетките. Може да е в зависимост от предназначението им, дали за File System backup, дали за SQL и т.н. Може да е свързано разпределението с loacation-а им или със състоянието им.

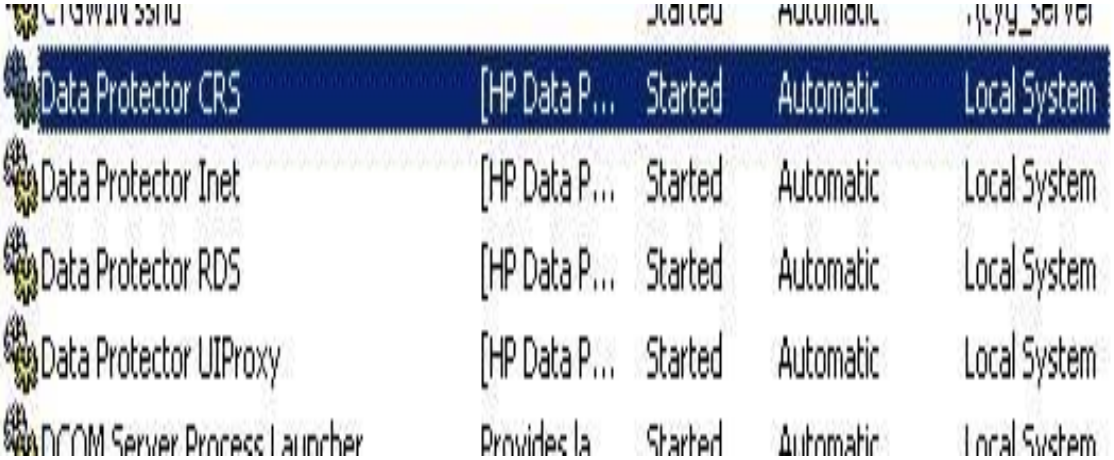
- MOM интерфейс на Data Protector – За да може да се използва MOM GUI, то трябва да бъде допълнително инсталирано. Чрез него може на едно място да се виждат всички вървящи операции на всички cell server-и, които са добавени към него. На *фигура 30* може да се види главния изгледана едно MOM GUI.

Фигура 30 *(Manager of Managers GUI of DP)*

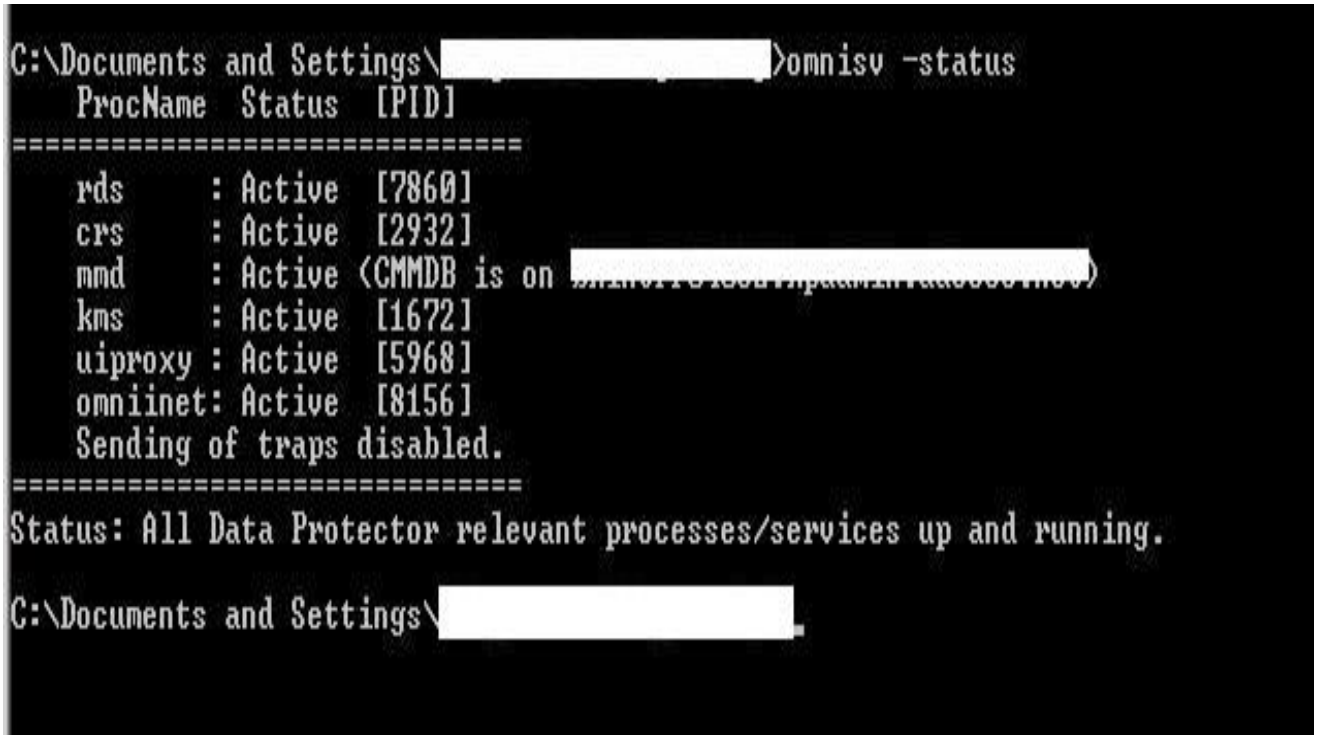


- Data protector services. За да може DP софтуера да върви, то има определени сервизи, които трябва да бъдат стартирани. На *фигури 31 и 32* ще бъдат показани основните DP сервизи, които трябва да бъдат стартирани, за да може да протича процеса на backup.

Фигура 31 *(Data Protector сервизи в Services.msc на Windows)*



Фигура 32 *(Data Protector сервизи в CMD чрез Omnisv –status)*



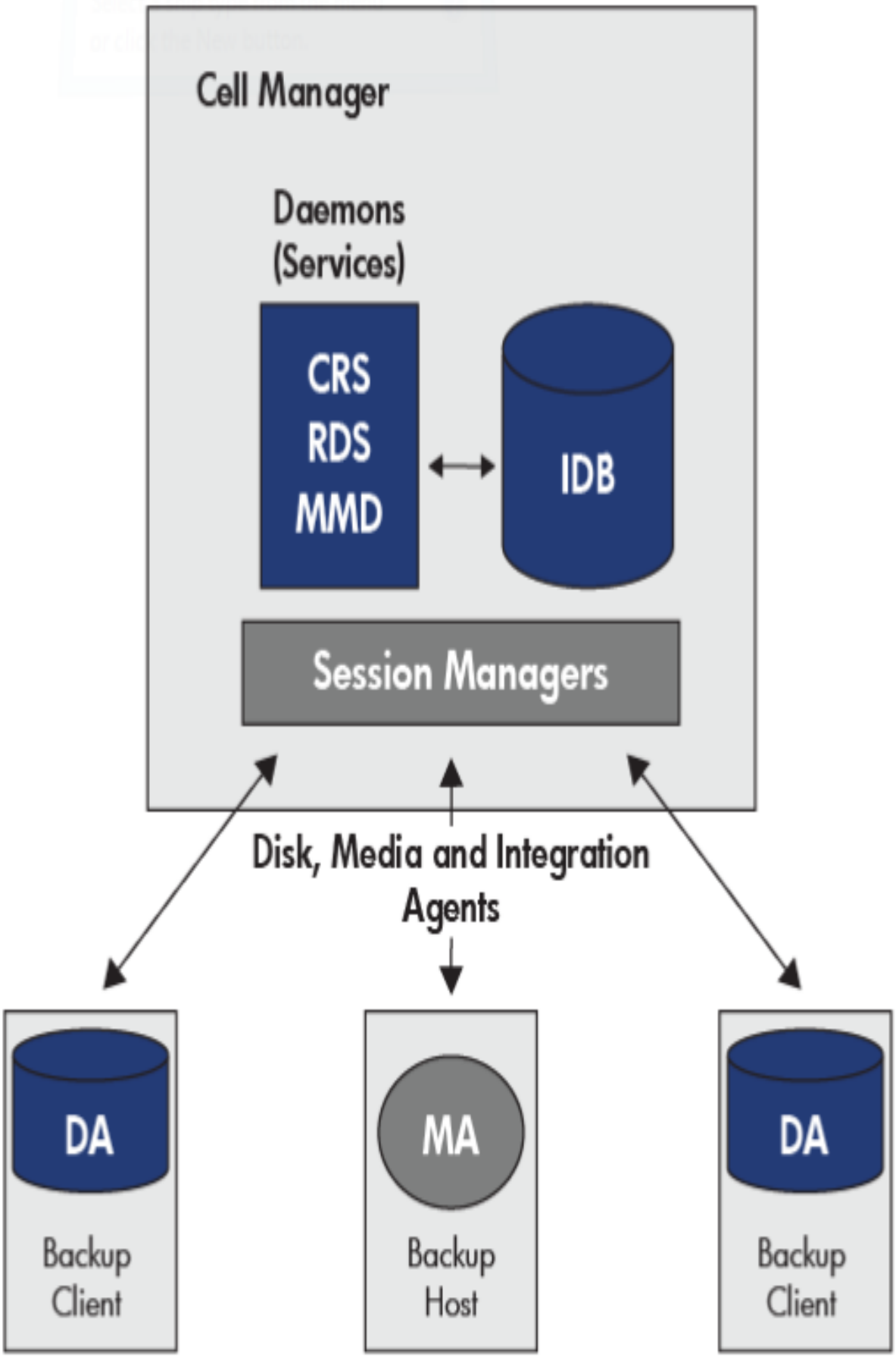
  - IDB – Internal Database – Вътрешната база данни на Data Protector софтуер-а е вградена база данни, която се намира на cell server-а и съхранява информация относно, кои данни къде са бекъпнати, на кои касетки са бекъпнати, как са бекъпнати

и за restore сесиите, на кои устройства са конфигурирани и т.н.

- CRS – Cell Request Service – Този сервиз е притежателя на всички бекъп операции в Data Protector софтуер-а, като изключение правят, някои SQL или ORACLE бекъпи на бази.
- RDS – Raima Database Server service – Това е сервиз, който върви на DP cell server-а, и отговаря за Internal Database IDB.
- MMD - The Media Management Database – Този сервиз е част от IDB-то и съдържа информация относно, касетките, пуловете от касетки, библиотеките, устройствата и др.
- KMS – Key Management Server процеса върви на Cell server-а и усигорява мениджмънт на сигурноста на Data protector. Този процес се стартира, когато Data Protector софтуер-а е инсталиран.
- uiproxy – То служи за комуникацията между Java GUI клиента и Cell server-а, а още прави и бизнес логически операции, и изпраща важна информация до клиентите.
- Omniinet – Този сервис работи на всяка една Windows система в Data protector cell-а и стартира други процеси, които са нужни за backup и restore. На Unix машини се нарича InetD

- Има процеси, които трябва задължително да вървят на cell server-а, както и на сървърите, които са в мрежата и конфигурирани на този cell server. Процесите са следните, като може да се види част от тяхната връзка на *фигура 33*:

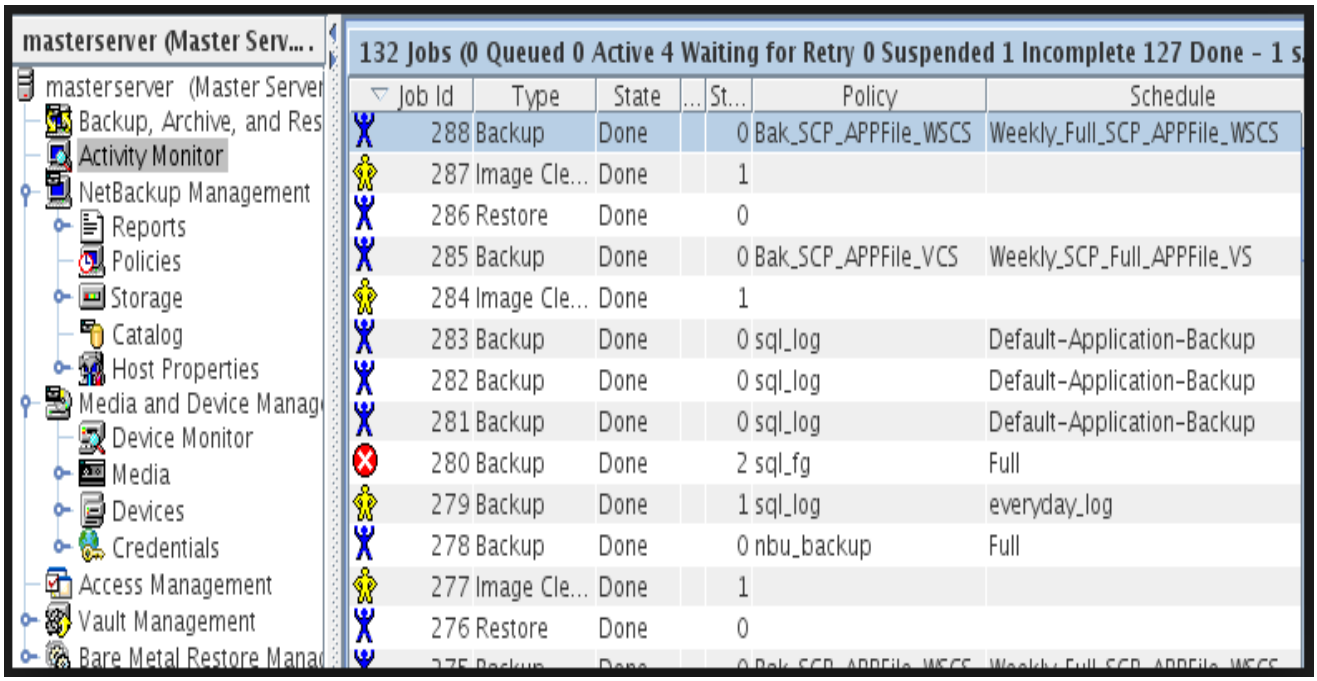
Фигура 33 *(Data Protector процеси – връзка)*



- BSM – Backup Session Manager – Отговаря за стартирането на бекъп операциите.
- BMA – Backup Media Aganet – Отговаря за четенето и писането на бекъп върху медиа (касетка, диск)
- RSM – Restore Session Manager – Стартира при пускането на Restore операция
- CSM – Copy Session Manager – Стартира, когато Copy операция бъде зададена да започне.
- RMA – Restore Media Agent – Стартира се, когато е стартирана Рестор операция.
- UMA - Utility Media Agent – Този процес отговаря за операциите с касетката, вкарване в устройството и изкарване.
- VBDA – Volume Backup Disk Agent – Това е процеса, който се вдига на клиента, когато се стартира File System restore.

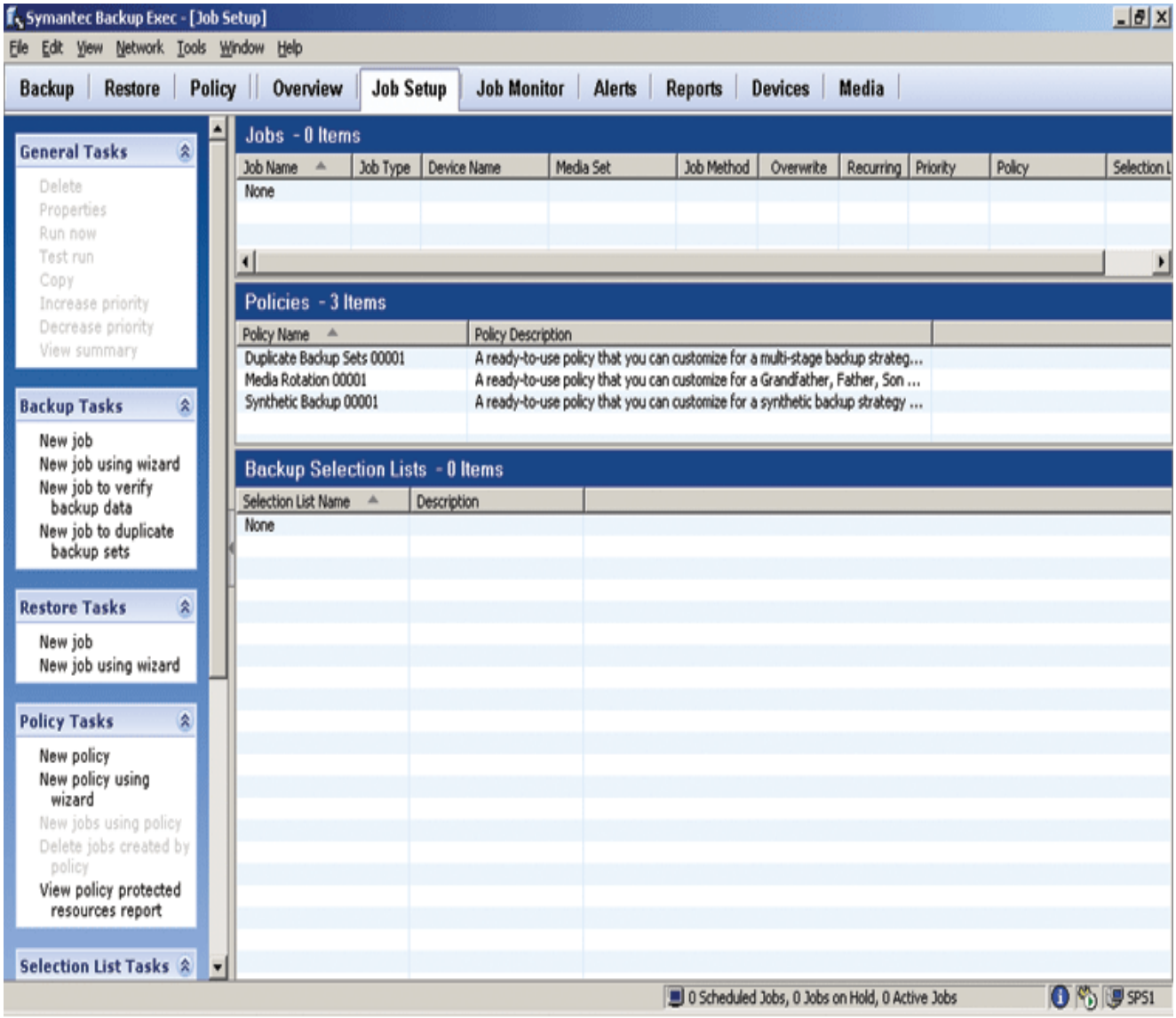
5.2. Net Backup – Софтуер на Symantec, който също като DP се използва при по-големи компании. При този софтуер за разлика от Data Protector, бекъп задачите се конфигурират посредством Job Policies. Също така cell server-а е заменен със Master server, чиято функция е подобна, като там разликата е, че като при MOM GUI-то се виждат всички server-а в мрежата, които са добавени. На *фигура 34* може да се види изгледа в Monitor таб-а на Netbackup, както и някои от основните менюта.

Фигура 34 *(Главно меню, монитор таб на Netbackup)*



5.3. Backup Exec – Софтуер на Symantec, използван при по-малки клиенти, може да се прилага и за 1 компютър/сървър. Тъй този софтуер, за разлика от Data Protector и Net Backup на Symantec, е за по-малки компании, със не голям брой компютри, при него нещата са по-лесни за конфигуриране. Главния изглед плюс Monitor таб-а при него може да се види на *фигура 35*.

Фигура 35 *(Data Protector сервизи в CMD чрез Omnisv –status)*

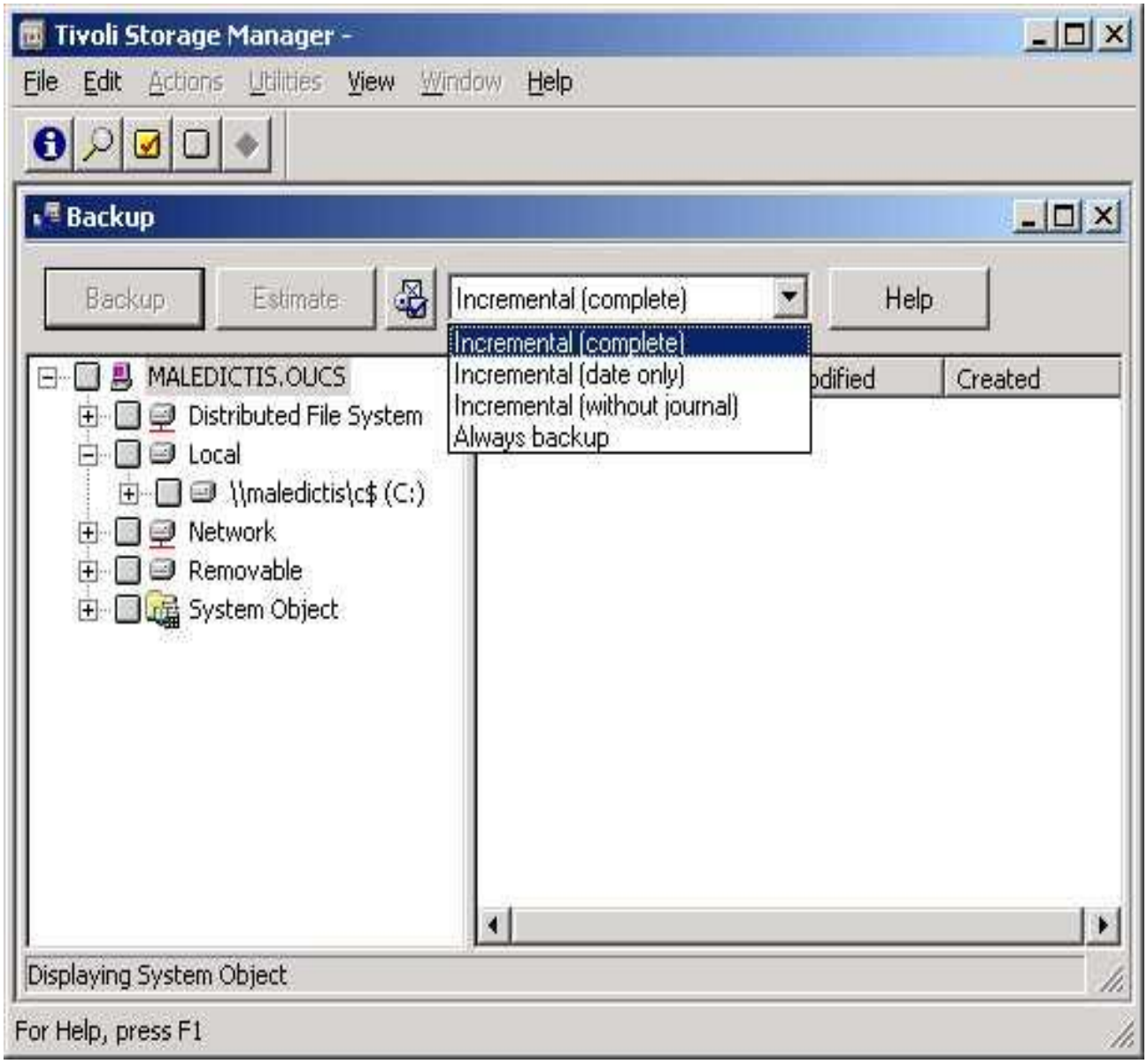


5.4. Tivoli Storage Manager (TSM) – Софтуер на IBM, използва се както за големи така и за малки кооперации. При него специфичното е, че няма един централизиран сървър, на който се управляват бекъп операциите, а трябва на всяка една клиентска машина да се настройва и при проблем да се качваме на нея и да се инвестигира посредством преглеждането на група от ".txt" файлове с логове. Главния изглед на GUI менюто на TSM може да се види на *фигура 36.*

***Фигура 36** (Главен изглед на TSM бекъп софтуер-а на IBM)*

- На *фигура 36* може да се види първоначалния екран от GUI на TSM. От тук може да се избере дали да се пусне бекъп или да се направи рестор от вече направен бекъп. При TSM специфичното е, че има две опции, дали да се направи Backup или Архив. Архив в случая е еденична версия на даден файл, която няма да се извиква скоро, за разлика от бекъп-а при която има няколко версии и е за скорошно извикване.

***Фигура 37** (TSM изглед за стартиране на бекъп операция през GUI)*



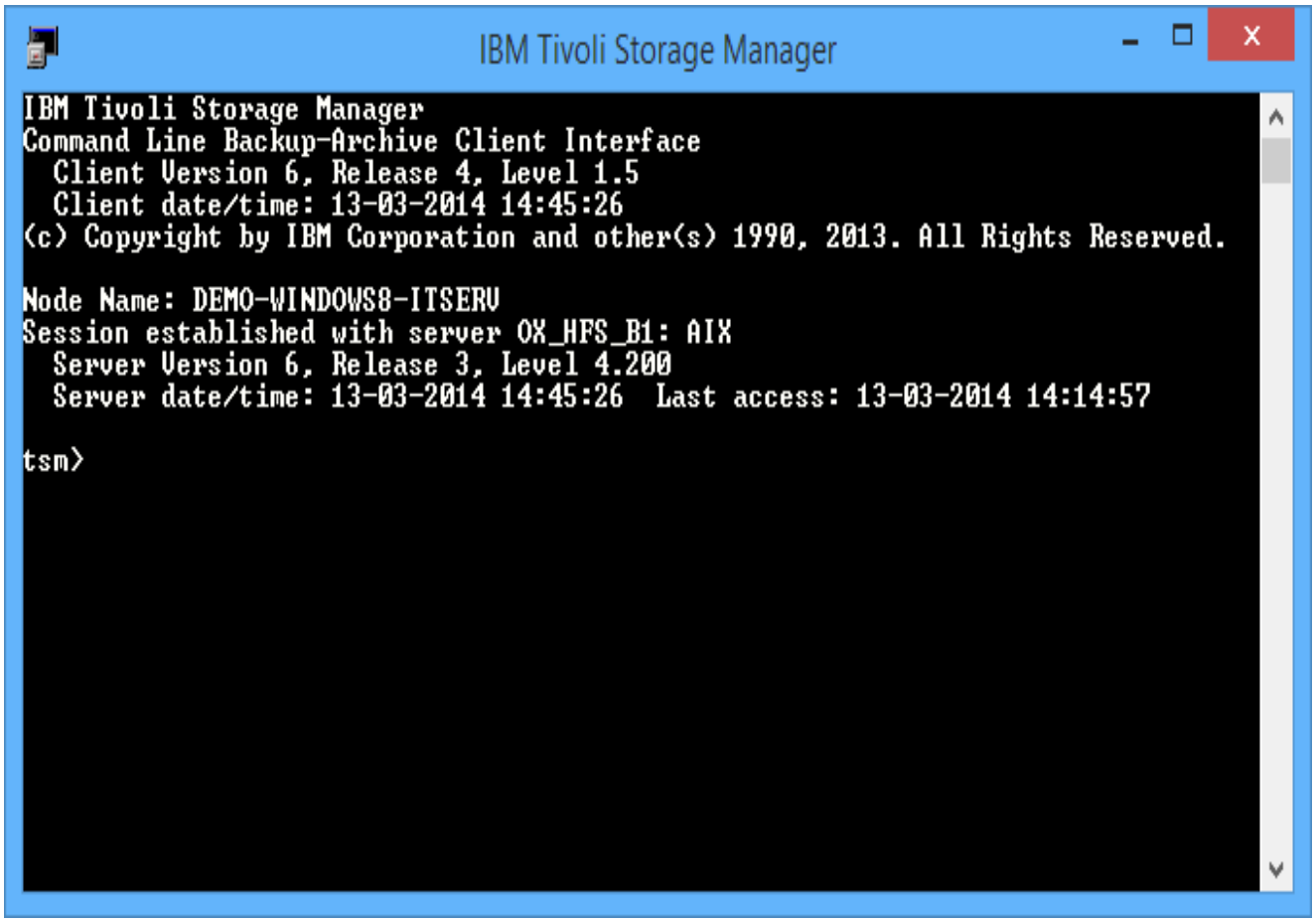
- На *фигура 37* може да се видят типовете backup, които могат да се прваят от TSM софтуера.

    - Incremental (complete) – Представлява нормалния incremental бекъп, като при TSM е incremental forever, след направата на първия Full backup, следват само incremental.
    - Incremental (date only) – Представлява бекъп само на зададена от TSM администратора дата.
    - Incremental (without journal) – Backup без използването на допълнително добавения journal на базите които се бкъпват.

- Always backup – или Selective backup. Това е аналога на Full backup при другите софтуери. При TSM това се прави само един път и следва само incremental forever след това.

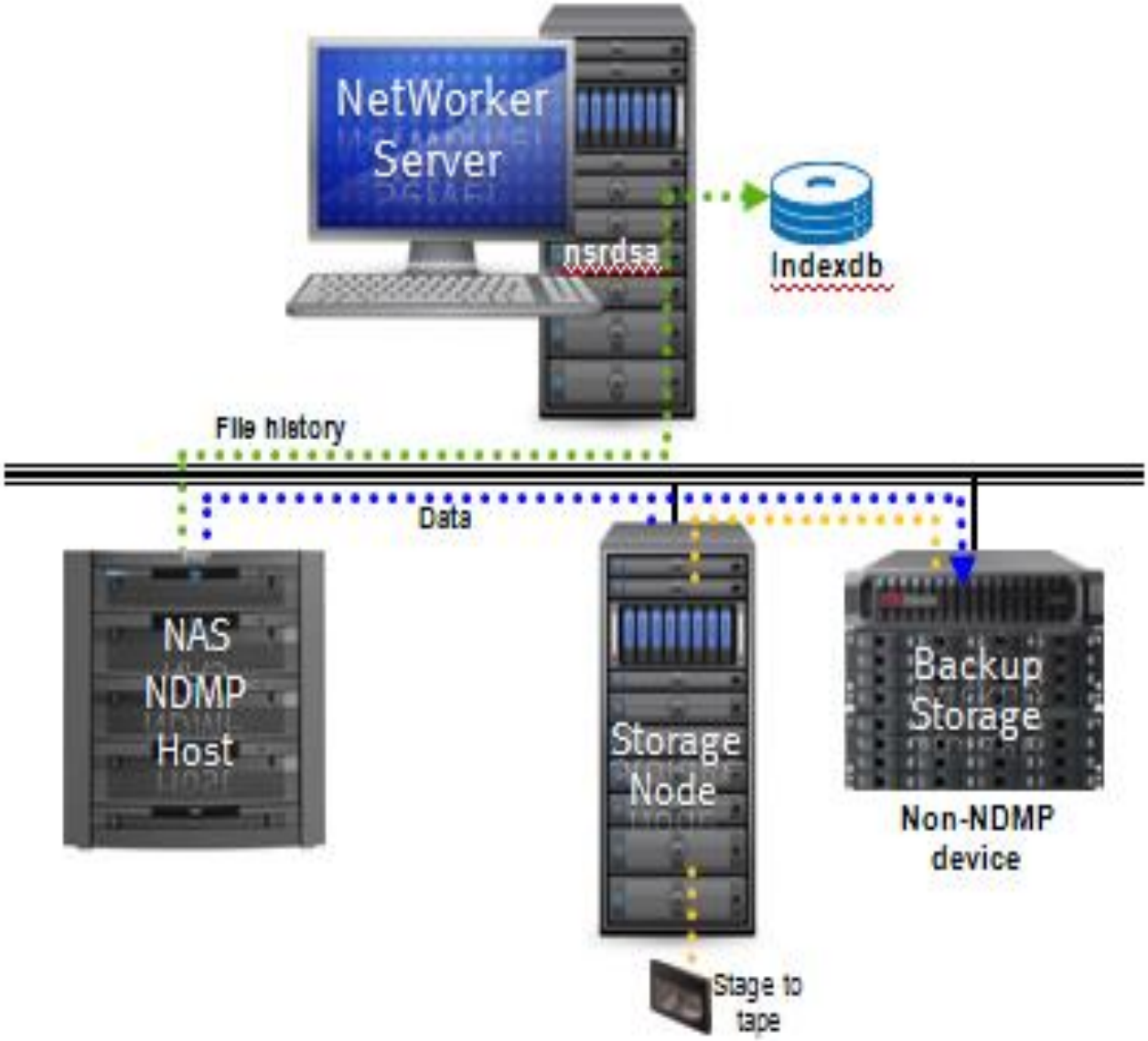
- На *фигура 38* може да се види CLI конзолата на TSM Клиента, която се използва не по-малко от GUI, дори се използва повече. Всички команди могат да бъдат намерени в сайта на IBM за TSM.

Фигура 38 *(CLI интерфейс на TSM)*



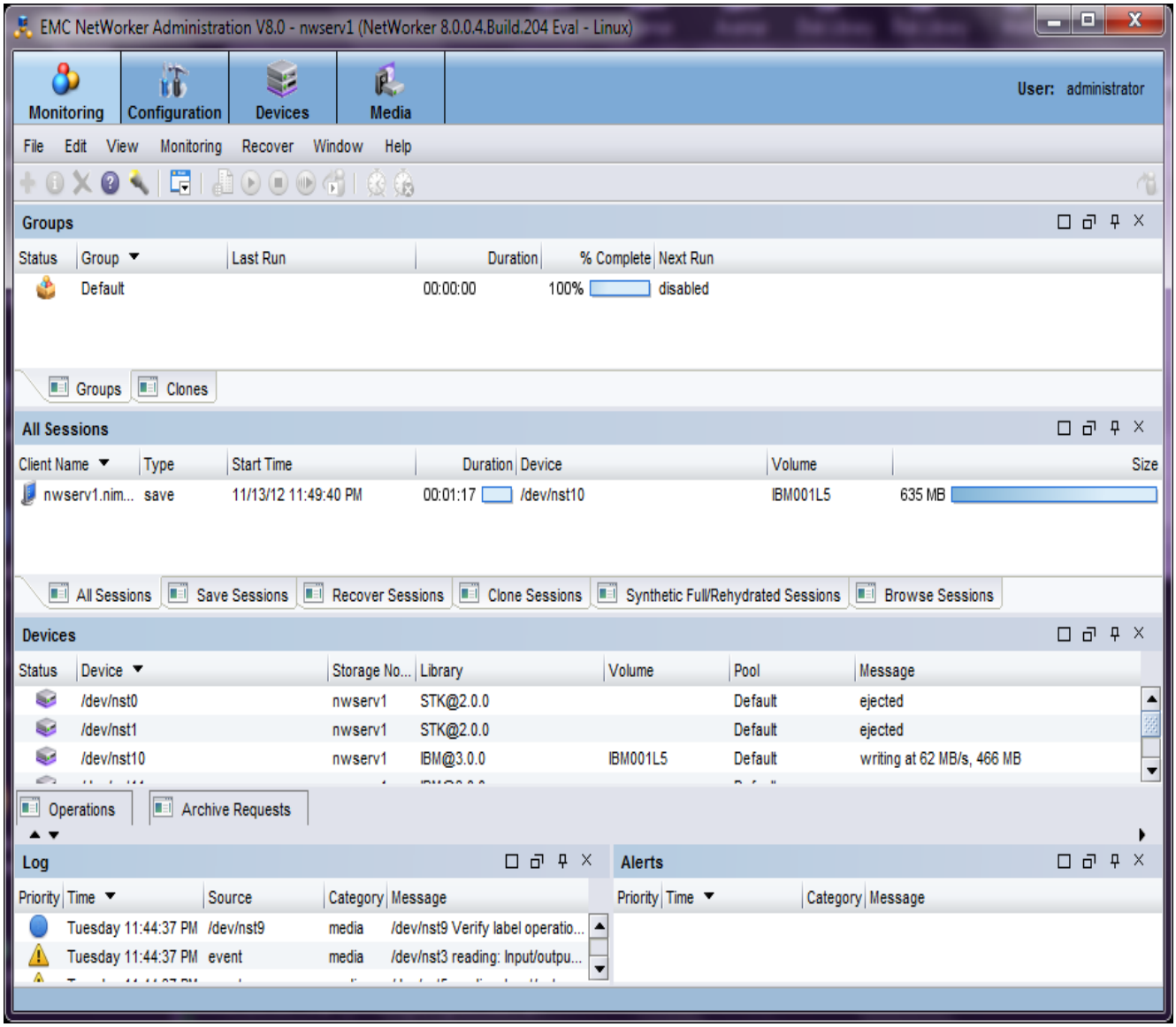
5.5. EMC Networker – Бързо набираща скорост компания на пазара при предлагащите бекъп фирми.

- На *фигура 39* може да се види общата схема на използваните устройства на софтуерана EMC, Networker.
    - ***Фигура 39*** *(Използвани устройства при EMC Networker софтуера)*



- *На фигура 40* може да се видиобщ план на **Monitor** меню-то като горе се виждат и другите 3 главни менюта, **Configuration**, **Devices**, **Media**

- ***Фигура 40*** *(Главен изглед на Монитор таб EMC Networker софтуера)*



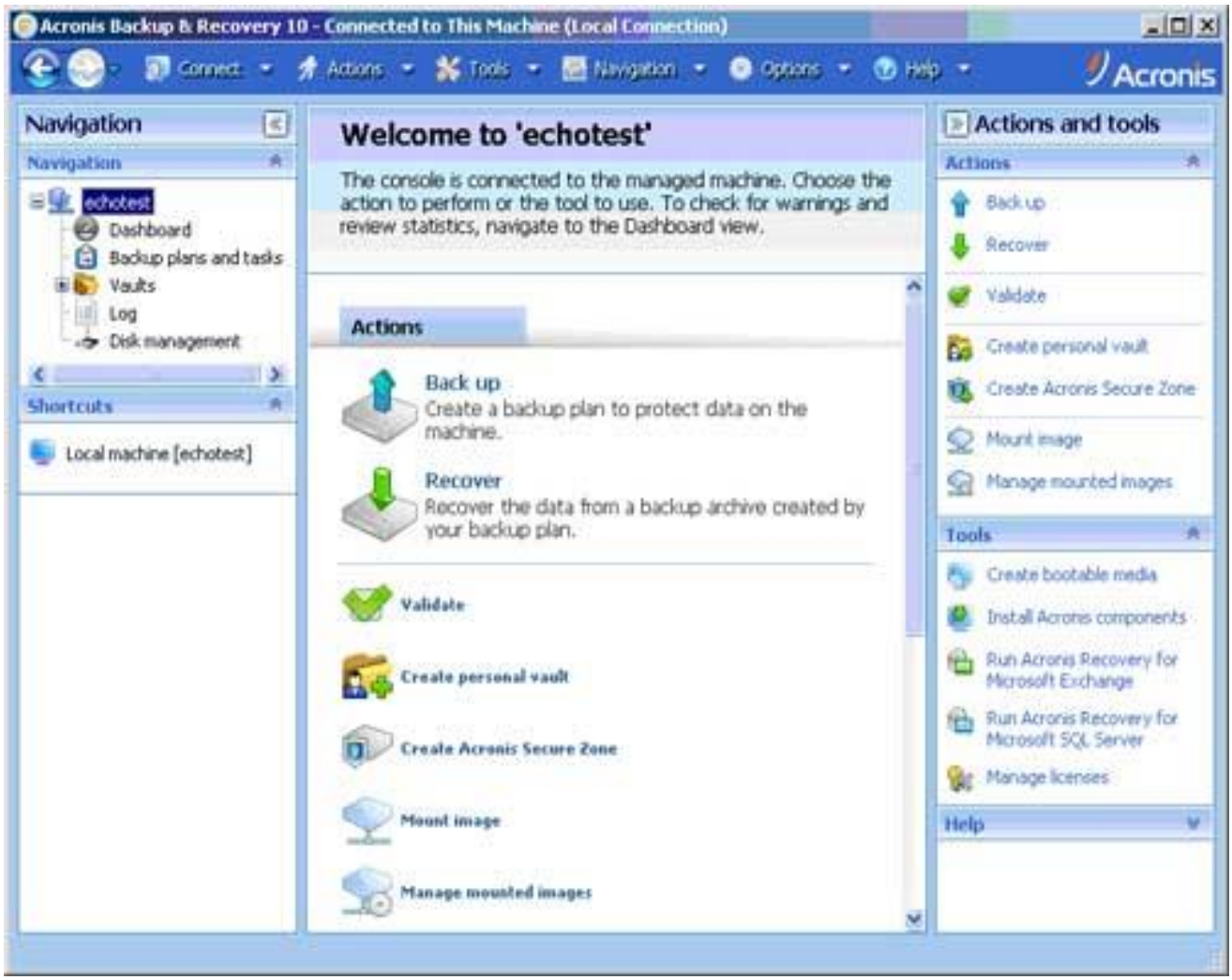
5.6. Acronis – Backup софтуер, който е както за обикновнните потребители, така и за малки, средни и големи компании. Главно преди популяризирането му се е използвал в Америка.

- На *фигура 41* може да се види главния изглед на софтуер-а за бекъп, Акронис. Интерфейса е направен така, че да се върже напълно с Windows XP, което говори, че е малко поостарял, но има и други версии, които са съобразени с новите интерфейси.

Фигура 41 *(Главен изглед ACRONIS)*

- На *фигура 42* може да се види другия изглед на софтуера Acronis за Backup и Restore.

Фигура 42 *(Изглед на меню за стартиране на backup/restore на ACRONIS)*



5.7. Други – Съществуват множество софтуери за Backup, като голям брой от тях са за онлайн бекъп и са предимно предназначени за нормалните потребители, като мен. Малка извадка от такива сайтове са:

- Backblaze
- CrashPlan
- Carbonite
- SOS Online Backup

III. ЧЕСТО СРЕЩАНИ ПРОБЛЕМИ.

1. Софтуерни

Повечето софтуерни проблеми си имат описание на самата грешка, която се генерира при евентуален проблем със бекъп или restore операциите. За тези проблеми при самата фирма, предлагаща услугите си има ръководство от какво е причината и какви са начините за отстраняването и. Ако даден софтуерен проблем не може да се оправи може да се наложи да се чака pach на бекъп софтуера или да се иска помощ от производителя.

Всеки от гореизброените софтуери си има своите недостатъци, повече ще бъде казано специално за Data Protector и малко повече за продуктите на Symantec и IBM в продължението на тази курсова работа.

При онлайн бекъп решенията, главен проблем е скоростта. При този вид съхранение на важната информация, самото копиране може да става изключително бавно. Това зависи от скоростта на интернета на потребителя, както и сайта на който се качва информацията, в зависимост от държавата е по-бързо или по-бавно. Друг проблем е, че не са толкова популярни и няма много информация все още за тях.

При Data Protector софтуера, главен проблем е, това че с всяка нова версия се оправят бъгове, които са били известни при старата версия, но се появяват нови такива, които трябва да бъдат докладвани от потребителите и да започнат да бъдат оправяни от разработчиците. Главните проблеми са по интеграциите на бекъпите различни от файл система, както и с Internal database на Data Protector.
Проблемите при TSM, са сравнително малко, тъй като IBM разбработват този софтуер от много време и е един от най-стабилните на пазара за сметанка на софтуер. При евентуални проблеми с този софтуер, може да се гледа червената книга на IBM (RedBook)< където са написани всички възможни проблеми, които може да имате със програмата и техните решения.

2. Хардуерни

Един от главните хардуерни проблеми при библиотеките с касетки е повредата на лентовите устройства, по-рядко повредата на касети, зависването на касета във устройството и др.

По-често срещаните проблеми при D2D устройствата са свързани със капацитета и дисковете. Тъй като може би всички D2D устройства са със RAID, бил той 5 или 6, има опция да изгорят максимум 2-3 хард диска. Един от проблемите е свързан със развалянето на хард дисковете. При RAID 5 евентуално изгаряне на 3 диска води до загуба на цялата информация във RAID масива, като при RAID 6 при 4. Другия проблема е, че мястото разбира се свършва. За набавянето на ново място трябва да се трият виртуални касетки със стара информация на тях, което не винаги помага на време. При по-големите D2D устройства също така може да бъде проблем и времето за репликация, тъй като през деня е ограничена скоростта, с която се прехвърля информацията, и така може да не смогне да се репликира между двете (или повече) устройства.

3. Други

Проблеми различни от хардуерни и софтуерни, могат да бъдат проблеми с възприятето на различните термини при бекъп, както и правенето на грешна стратегия. При големите компании, занимаващи се със бекъп, проблем е и липсата на специалисти, които да конфигурират една стабилна среда, на даден софтуер, било то TSM или Data Protector или NetBackup.

Проблема с комуникацията съществува и тук, както навсякъде. При големите компании, различни екипи отговарят за различни части на бекъп поддръжката, било то SAN, LAN, Windows, и така нататък. За да може всичко да върви нормално, трябва комуникацията да бъде на ниво, в противен случай услугата ще бъде некачествена и може да няма бекъп на данни, които са важни и изтрити в момента, когато няма да имат актуален бекъп.

ЗАКЛЮЧЕНИЕ

Бекъп-а и архива-а са операции, не само наложени като задължителни от регулаторните органи за големите организации, но също така и като препоръчителни, както за тях, така и за обикновените потребители. Важна информация може да загуби всеки по един или друг начин, като е важно да може да си я възвърнем от някъде. За да можем да направим това, то трябва да мислим на време за последствията от едно грешно натискане на мишката или клавиш на клавиатурата или от евентуален грабеж, токов удар или природно бедствие.

Главното различие между двете, както съм споменал по-горе, е това че архив-а служи за съхранение на данни, които са предвидени да се съхраняват дълго време и не изискват промени, както и такива, които няма да се изисква да се възстановяват скоро и редовно. Бекъпа от друга страна се прави с различни срокове за съхранение и се прави на файлове, които се използват по настоящем от потребителите на компютрите/сървърите. Бекъпа може да служи и за пълно въстановяване на система.

Видовете бекъп, зависят от нуждите на потребителя/компанията. Може да се съхранява във външна локация, може да се прави по мрежата, може да се държи на локалното място. Може да се прави всеки ден пълен бекъп (което не е препоръчително), като може и да се прави един пълен бекъп и след него постоянно да се правят бекъп само на новите/променените файлове (incremental), има много бекъп схеми.

За тези бекъпи при нормалните потребители за носители се използват предимно локалния или външен хард диск, флаш памети, дискове и други, докато при големите организации се използват библиотеки със касетки (Tape Libraries, TL), виртуални библиотеки (VTL), Disk-to-disk устройства (D2D) и друго, като има много модели на горепосочените устройства. Всяко от тях си има своите плюсове и минуси, като D2D устройствата, се използват когато се желае по-бърз бекъп и рестор, докато библиотеките се използват когато се желае малко по-евтино на GB място, а също така и касетите са по-здрави от колкото са хард дисковете.

Тенденциите при използването на Backup се увеличават с всеки изминал ден, както се увеличава и размера на информацията в мрежата. Търсенето на по ефективни начини за съхраняването на важната

информация е голяма част от този растеж. Потребителите трябва да са информирани за това, как и къде се съхранява тяхната информация и в случай, че тя изчезне, какво точно могат да направят те.

След разглеждането на тази тема, потребителите на персонални и служебни компютри трябва да може по-лесно да изберат из между всички видове софтуер и между устройствата, които го подпомагат.

.

Списък на използваните източници

http://en.wikipedia.org/wiki/Backup

http://searchstorage.techtarget.com/definition/backup

http://www.computerworld.com/s/article/103645/Archive_and_backup_What_s_the_difference_

http://www.computerweekly.com/news/1369092/Data-backup-vs-archiving-Whats-the-difference

http://searchdatabackup.techtarget.com/tip/Backup-vs-archive

http://www.bestbackups.com/blog/2447/backup-vs-archive-differences/

http://searchstorage.techtarget.com/definition/archive

http://searchstorage.techtarget.com/definition/restore

http://en.wikipedia.org/wiki/Backup_and_Restore

http://documentation.commvault.com/hds/release_7_0_0/books_online_1/english_us/features/express_recovery/express_recovery.htm

http://typesofbackup.com/

http://www.wisegeek.com/what-is-d2d.htm#didyouknowout

http://www.backup4all.com/kb/full-backup-116.html

http://www.thewindowsclub.com/hard-drive-failure-recovery

http://h20565.www2.hp.com/hpsc/doc/public/display?docId=emr_na-c01698903

http://h20565.www2.hp.com/hpsc/doc/public/display?docId=emr_na-c01704747

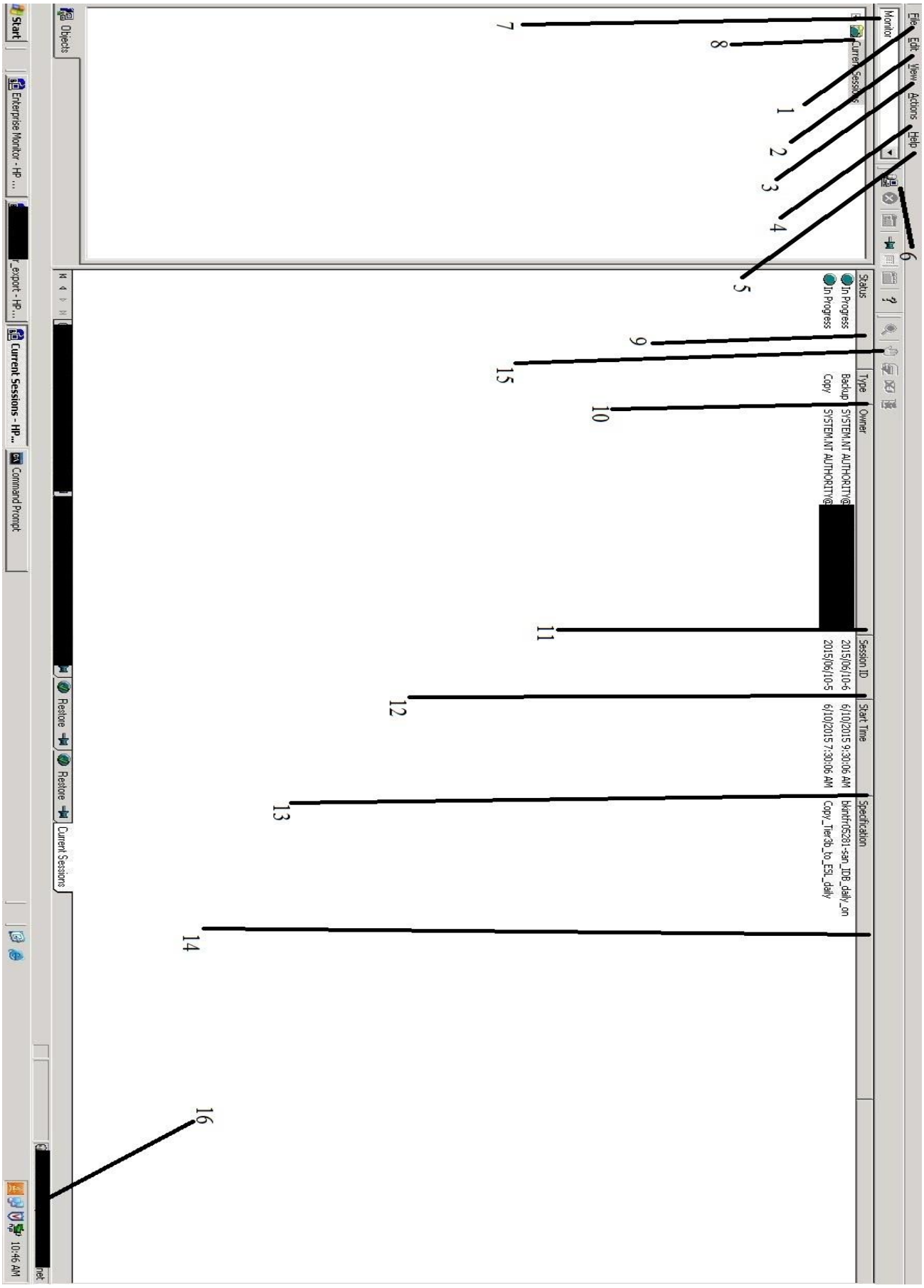
http://www.storagenewsletter.com/rubriques/systems-raid-nas-san/quantum-enhances-dxi7500-d2d-system/

https://en.wikipedia.org/wiki/Data_deduplication

http://www.system-center.fr/?p=3783

Приложение 1

Фигура 18 *(главен изгледна Data Protector backup софтуер)*



СПИСЪК НА ИЗПОЛЗВАНИТЕ СЪКРАЩЕНИЯ

TL - Tape Library - Библиотека използваща лентови касетки

D2D - Disk to disk device - Устройство използващо твърди дискове в RAID, използвано за виртуална TL.

RAID - Redundant array of independent disks - Дискове вързани един със друг, софтуерно или хардуерно, правейки така, че да има излишък от дискове (за по-голяма сигурност) или по-бързо четене/писане от тях.

VLS - Virtual Library System - Виртуализирано устройство за съхраняване на информация, използвано предимно за бекъп.

VTL - Virtual Tape Library - Това е логически създаена библиотека, която се използва за бекъп. Може да е част от D2D или VLS.

MSL - Midrange Storage Libraries - Физически библиотеки, използвани за бекъп. Среден капацитет.

ESL - Enterprise Systems Library - Физически библиотеки, използвани за бекъп. Висок капацитет, използвани от големи компании за голям обем от данни.

SAN - Storage Arrea Network - Мрежа, която предоставя достъп до дисково пространство на базата на блок ниво.

NAS - Network Attached Storage - Устройство, което предоставя пространство в хранилище на компютрите вързани в неговата мрежа. Използва файлово ниво.

SCSI - Small Computer System Interface - Начин за прехвърляне на данни.

FC - Fiber Channel - Високоскоростна мрежова технология за прехвърляне на данни. Може да е 2-4-8-16 Гигабит-а в секунда.

HDD - Hard Disk Drive - Твърд диск

DR - Disaster Recovery - В случай на бедствие, има резервен вариант на оригиналните устройства, като може да започнат да се използват веднага при спирането на функциониране на основните.

LUN - logical unit number. Това представлява ID-то, което се свързва с логическия диск, намиращ се на дадено SAN хранилище.

NFS - Network File System е протокол за предаването на файловете по мрежата, първоначално изработен от Sun Майкрософт през 1984 година, който позволява на потребителите да достъпват файловете през мрежата, като се достъпва до хранилище примерно от тип NAS.

SMB/CIFS – Оперират в Application слоя и служат за споделяне на файлове, принтер и серийни портове.

TB, GB, MB – TeraByte, GigaByte и MegaByte са производни на мерната еденица байт. Главната за измерване е Megabyte.

GUI – Graphic User Interface – Графичен потребителски интерфейс.

CLI – Command line interface – Интерфейс посредством черно-бялата конзола на windows-linux операционни системи.

VSS – Volume Shadow Copy Service – Прави се временен изглед на системата, от който може да се възвърне след време.

DP – Data Protector, Софтуер за бекъп на HP.

Cell server – Това е машина, през която минават всички операции свързани с бекъп и рестор при Data Protector софтуер-а.

Media server – Това е сървърът, през който минава целия поток от данни.

MOM – Manager of Managers – Използва се при DP Софтуер-а, за да може да се виждат в едно DP GUI, Monitor таб-овете на няколко cell server-а