Backup
Past, present and future

Matt Edwards
matt.edwards@rm.com

Past, present and future
Agenda

- Introduction
- The past
- The present
- The future
Introduction

Backup is something we all need to do. Backing up your data is more important now than ever. As physical components are getting smaller in a lot of cases, software files are getting much larger. It is estimated that data growth is around 25% per year. This means that the demands on your backup solution and the importance of the strategy you implement is greater than ever.

In this session we are going to be looking at the past, present and future of backup solutions, covering software and hardware. Of course we will be only taking a brief look at the past section, just to reaffirm ourselves with what came before, some of our customers in smaller establishments may still be using some of these older solutions which is why it will be covered briefly in this session.

Then we will move into the present. Our main focus here will be Disk To Disk To Tape (D2D2T) and Symantec BackupExec. We are going to hopefully demystify some of the terminology relating to D2D2T as well as giving you some best practise advice relating to your hardware. BackupExec can be a complex application to configure and there are some common mistakes made, I will be talking you through what these common mistakes are and why they happen and hopefully give you some idea how you may be able to configure your backup strategy to suit your needs better.

Towards the end of the session we are going to have a look at the future. Not literally but we will be able to see where data backup is going next, some of these solutions may be already available but they are fairly new technologies that you may not have seen or used so I thought I would highlight the options you have available when considering data backup in your establishment.
Backup – the past

There have been many different hardware and software backup solutions used in the past for data backup. I am not going to go through every single one but I wanted to pick out a couple of the ones most commonly used. Some of these will still be used in many establishments today which is why I wanted to talk briefly about them.

**Single tape drive (installed at the server)**

In recent times the most common type of data backup solution used is the single tape drive solution. This will consist of each server on the network having a local tape based backup drive installed. Each server will back up its own data to a tape or a set of tapes depending on how large the server’s backup data is.

The tape drive reads and writes data to and from a magnetic tape. These tapes provide sequential access storage, which works differently from a disk drive which provides random access storage. So what do I mean by that; a disk drive can move its read/write head(s) to any part of the disk in a very short
space of time where a tape must wind the tape between reels to access any one particular piece of data. This of course takes a considerable amount of time in comparison with a disk drive (seek time). However one misconception of the tape drive/tape solution is that although the seek time is much greater than disk drives, the stream of data to and from the tape is actually very comparable with some disk drives. For example modern LTO tape drives can manage continuous transfer rates of up to 80MB/s, which is as fast as most 10,000rpm hard disk drives.

It is advised that the tapes which contain your backup data should always be kept away from the server and the server room in case of fire or water damage for example. The guidance has changed a bit over the last few years as it used to be recommended that you take the tapes offsite every night; however there have been some questions about data protection relating to this practise. I would advise contacting your local authority to ask what the recommended working practise for storing backup tapes is.

A locally installed tape drive installed at the server is a very efficient system for any single server establishments.

A tape based backup solution is still very useful in today’s market and is still used as a vital cog in our more complicated backup solutions which we will be looking at later on.

Let’s have a look at the advantages and disadvantages of using a locally installed tape drive solution –

**Advantages**

- Very useful for data security after backup has taken place. Keep tapes offsite away from the server.
- Easy to set up backup scheduling.
- Less expensive per GB than other solutions.
- Virtually unlimited media capacity for backups via Libraries.
- Useful for small establishments or single server establishments.

**Disadvantages**

- Slower to backup than disk.
- Much slower to restore data from tape than from disk.
- Requires thorough tape management (knowing and managing your library).
- You will also get cost as a disadvantage. Lots of advice will tell you to replace your tapes every year, certainly if you do not clean your tape drives regularly you will be buying new tapes often, possibly even needing to replace the drive.
- Reliability. Tapes and drives are prone to failure or degradation by the environment (heat, sunlight, humidity etc)
- Complicated for multi-server establishments.
Below are the most common tape drive solutions seen in the market –

- **AIT** – Designed by Sony. Ranging from AIT1 (25GB native capacity) though to AIT5 (400GB native capacity) Sony have now discontinued supplying AIT tape drives.

- **LTO** – (Linear Tape Open) Is an open standard alternative to AIT. This is now the current magnetic tape based solution. Ranging from LTO-1 (100GB native capacity) through to LTO-5 (1.5TB native capacity) LTO drives offer great advantages over AIT drives. Firstly the failure rate of AIT drives is much higher than LTO due to the technology LTO uses. Also AIT drives and tapes were only made by one manufacturer (Sony) so it was not competitive on price or quality and tied end users into one manufacturer.

**Compression**

It is always advised that schools should base their usage on the tapes native capacity rather than their advertised compressed capacity, as many applications use some form of compression already or use file formats which are not easily compressed. You will see quotes relating to a 2:1 data compression, this implies that you can compress 200GB worth of data onto a 100GB tape. This just shows you what is possible with the hardware. Your data is unique and therefore when your data is compressed your compression ratio will also be unique also.

**Hardware vs software compression**

When compression is available in the tape drive hardware/firmware, the compression feature of any software package should be turned off. This reduces the processing burden on your computer. Also, hardware based compression is typically much more effective. Do not double compress.

**Common mistakes with AIT/LTO tape drives**

1. **Don’t overwork your drive** - Check the duty cycle of the drive, a drive with a 100% duty cycle should be able to run continuously without error; however a drive with only a 50% duty cycle should not be operated for more than 12 hours a day.

2. **Supply the data fast enough** - If the data transfer rate from the server to the drive is significantly slower than the drives transfer rate the drive will suffer from a start/stop motion as it waits for more data. This is known as ‘shoe shining’. This puts a lot of strain on the tape itself and can affect the integrity of the data on the tape.

3. **Handle and store tapes properly** - Poor handling can reduce the lifespan of a tape. When you clean a tape drive, use a good quality drive cartridge cleaner and follow the manufacturer’s cleaning
recommendations. Fortunately, in most modern systems the cleaning is handled automatically by the specially configured cartridge, minimizing the skill and dedication needed on the part of staff. The days of cleaning around the old reel-to-reel tapes with a Q-tip and isopropyl alcohol are in the past.

4. **Clean your drives** - This is the most common misdiagnosis of failing drives. The drive itself will let you know when it needs cleaning. This means a light will display on the front of the drive indicating the cleaning tape should be used before attempting backup. However we recommend not waiting for this as it may report it needs cleaning in the middle of a backup, which is not what you want. We always advise setting a weekly schedule for running your cleaning tape. It only takes a few minutes to run and will help to keep your drive healthy.

   I have seen many “faulty” tape drives which I then install to test what has failed and the first thing I see is the amber light on the front of the drive signalling that a clean is required.

---

**RDX removable disk storage**

RDX backup drives work in a very similar way to tape drives apart from one key difference; there are no tapes. The RDX drive uses removable cartridges, within these cartridges is a standard 2.5-inch laptop hard drive, the disk drive is surrounded by a protective shell for improving the quality of hard disk drive backup. RM’s RDX backup drive is manufactured by Tandberg.

Using disk drives over tapes offers a few benefits - higher storage capacity, random access read (enabling much faster retrieval of single file data than tape), more cost efficient.

   I must mention that in a lot of cases LTO tape drives are seen as faster to run a backup, due to the sequential way that read and write data. But RDX cartridges are faster to recover a single file due to their ability to use random access read and write.

   The RDX system is an ideal solution for smaller schools.

RM RDX solutions works with RM Server Backup software which is based on NTbackup. However for RDX backup to work correctly this software must be configured correctly. The technical article on how to do this is referenced below.

Another key piece of information which you should be aware of with RDX cartridges is that they are not overwriteable due to limitations within NTbackup. If a cartridge becomes full you need to manually delete old backups from the cartridge, if you attempt to use a tape which is full your backup will fail. We have documentation which talks through how to automate the deletion/format process which is highlighted below in the common issues section.
Common issues

RM Server Backup does not work

- If your backup software is the standard RM Server Backup solution, then a specific software setup is required. This is installed by the factory, however, there could be instances following a 'Server Migration' (also called a 'Server Swap' process) where this might not be updated. Please check the following article to ensure your software setup is correct.
  - Technical article - TEC1284343

RDX cartridge will not eject

- Firstly you should attempt an emergency eject unless the server is turned off.
- If your RDX cartridge will not eject when the eject button on the fascia is pressed, please make sure that your server is not accessing the drive.
- Next, open My Computer and right-click on the RDX drive that is listed as a 'removable device'. Select eject from this context menu and check that the cartridge now ejects.
- If the cartridge ejects, please check that the RDX service is running. From Start, Run type services.msc to open the services dialog. Scroll down to find the 'RDX mon 1.12' service. If this is absent, please install the RDX utility from the TEC article below. If the service is present but stopped, please change the properties to 'Automatic' and start the service.
- If none of the above suggestions work, please use the emergency eject button. Insert a thin screwdriver into the small hole in the front of the drive. You will need to depress the button using a thin screwdriver by about 5mm until the cartridge is fully released. Once ejected, please restart the server by shutting down, pausing for 30 seconds and then powering back on. If the RDX cartridge will still not eject through any means other than the emergency eject button, please log a call with RM Support.
  - RDX Backup drive utility - DWN1173813

Data backup appears to be slow

- The backup speed to an RDX drive varies but is normally in the range of 25 to 45 MB/s.
- If backups to the RDX drive appear to be excessively slow, it is possible that the RDX drive might be set to PIO mode. Please follow the TEC article that explains how to change the drive into DMA mode. Please note that this action requires a restart before the changes are effective.
  - Technical article - TEC446288

Backups fail on an RDX drive due to insufficient space
• Backups using RM Server Backup do not automatically overwrite or delete previous backups. The system administrator will need to periodically delete older backups from the cartridge though My Computer. Please refer to the TEC article for further instruction.
• Technical article - TEC1332734

These are some common issues you may see if you are running an RDX backup solution. For further details or to search for other symptoms please visit –

http://www.rm.com/support/knowledgelibrary.asp

**USB hard drive**

This isn’t often regarded as a backup solution but I would recommend every establishment has a 500GB-1TB USB hard drive tucked away in a drawer somewhere.

If your backups are failing and require diagnostics to work out why, this may take some time. While this is being done I would suggest using your USB hard drive to get at least your user data backed up from the server, while you diagnose the fault on your network backup solution.

You can pick up a good quality 500GB USB hard drive for around £60. It is an investment well worth making if you do not currently have one.
Backup – the present

A lot of what we’ve looked at already is still being used in establishments today and in most cases these are probably the correct solution for the size of the establishment. However some of these backup devices are no longer available to buy new, so next we are going to look at the current range of backup solutions.

So, launching into the present day. In this module we will see what backup solutions are available on the market today and which solutions are being used by different education establishments. We are also going to look at some common misconceptions with some of these, and provide you with some tips and tricks to help you support these backup solutions. But first we’re going to start at the top....
Planning is everything!

Probably the most important change in present day data backup in education is the need for a written strategy. This is known as a “Disaster Recovery Strategy”. Put simply it is a written guide for what to do if the worst case scenario happens; fire or flood in the server room. However much you feel you know what you would do if this happened, you never know how your brain will work under the pressure of that becoming a reality. A lot of local authorities now have their own guidelines for school’s Disaster Recovery Strategy but there are definitely schools that do not have a written procedure in place.

I cannot state the importance enough of having a written procedure for disaster recovery. If you do not currently have a recovery strategy in place then the below information will be of use to you. This was taken from an RM whitepaper on backup.

Develop a Disaster recovery plan

In the unlikely event that you have a complete disaster, you must ensure that you are in the best possible position to recover your network.

A disaster recovery plan may not just be a sequence of technical tasks performed by IT staff to resolve a short-term problem, but it should also consider the following:

- Communicating with the school at large, keeping people informed of progress and expected time for return to service. This might include the times for the different categories of data that you have to restore. For instance, this might mean the return of basic system functionality within four hours and the restoration of large multimedia files within two days.

- Long-term network unavailability. This is often termed ‘business continuity’, and concerns what happens to critical services if you cannot quickly return a system to full use.

Practical elements that should be considered as part of a disaster recovery plan are:

- Hardware maintenance contacts – a full list of the various agents responsible for maintaining your equipment, together with any requirements they may have for logging a call. This might include serial numbers, for instance.
• Operating system and server driver media – a full selection of the required operating installation system media and any required drivers for the server hardware should be duplicated.

• Operating system installation process – the process required to install the server’s operating system and backup software should be copied and stored.

• Server information manifest – make a copy of the server configuration information. This should include:

  server name
  server IP information
  server disk partition sizes
  server SAN connection information (if a SAN is installed)

All of the above should be duplicated at least twice and combined together in a ‘kit’. This would minimise time required to locate the required information.

Review your strategy

Having successfully implemented all of the above, a yearly review should be conducted. As part of the review, you may well consider:

• Testing the SLA is being met. If not, changes to the backup process or to the SLA should be agreed.
• Reviewing hardware and software maintenance required for your backup equipment.
• Reviewing that the processes are still relevant, and updating them if required.
• Formulating a purchasing plan for any new backup media requirements in the coming year.
• Reviewing any process problem or failures during the year and if any necessary action is required.

There have been lots of schools I’ve come across who run backups every night without ever really thinking about why they are doing them. As obvious as it sounds, the only reason to take a backup is to be able to restore. That may mean creating an apparently difficult, convoluted or time consuming backup process in order to improve the likelihood of a successful restore. Restores are not just needed for a user who has deleted a file by accident but also it’s important to ask yourself how do I restore my network if the server room was destroyed?
It sounds melodramatic and you may think it won’t happen to you but you have a responsibility to make sure that loss of data won’t happen at your school, in any situation. To do this you need an appropriate backup solution and you also need a Disaster Recovery Strategy.

Michael Oakes is running a Server Recovery session at this seminar which is looking more at the specifics of recovering the server. However if you do not currently have a written disaster recovery strategy at your school I would recommend attending his session.

**System state**

While I am talking about disaster recovery and creating a backup strategy it is important that I mention System State. There are some common misconceptions on what System State is and why it needs backing up. In short it is not the same as just backing up the C: drive. Below we look at why:

The system state can contain a number of items:

- System registry
- COM + Database
- Certificate Services
- Active Directory
- SysVol
- IIS Metabase

Some of these items are only included if the specified service is installed (AD, IIS, Certificates).

If you need to restore a server, you will need this state to recover the registry, or your AD Domain, or IIS sites.

Let me pass on an analogy I read –

*If you wrote a book, would you only make a copy of the table of contents for safekeeping? Or would you want to copy the actual data itself?*

*The System State contains registry info, AD structure, etc., but it does not contain the actual volume data.*

System State data contains most elements of a system’s configuration, but it might not include all of the information that you require to recover your system from a failure. Therefore, it is recommended that you back up all boot and system volumes, including the System State, when you back up your system.

System State is the last thing to be backed up; it is needed to be able to restore the AD. We have seen more than one establishment that didn’t realize
their backup needed a second tape (because they hadn’t been checking the logs), therefore their backup was incomplete. When the server did die we could not recover the Active Directory, both sites had to be re-commissioned.

**Current backup solutions**

**Internal server backup**

An internal backup device installed at the server (cartridge/tape drive). For multiple server sites you would require a backup device installed at each server. AIT is no longer available from Sony. The current single drive solutions available from RM are either an LTO tape drive or an RDX cartridge drive. Tape or cartridge backups are still highly recommended in education establishments due to removable nature of the media. Your backed up data should never be kept in the same location as your servers. Tape/cartridge gives you the ability to store your backed up data offsite. The software generally used to manage a locally installed backup device is RM Backup (based on NTbackup).

**D2D2T (Disk To Disk To Tape)**

A separate backup server with a tape autoloader attached via SCSI. Data is backed up to the backup server’s (DiskBox) hard disk drives across the network and then transferred to tape using the autoloader. This provides extra security and duplication of your backup data. D2D2T is the most popular backup solution for the education environment. This is because it centralises all of your network backups, provides duplication of backups and makes restores much faster as they can be done from hard disk rather than tape. You do not need a backup device installed at each server on your network as data is transferred to your specific backup server (Diskbox). We will be looking at D2D2T in more detail later and the software used to configure your backups – Symantec Backup Exec.

**NAS (Network Attached Storage)**

RM’s NAS solution is the ‘RM NasBox’. NAS systems are network systems which contain one of more hard disk drives often set up as a RAID array. NAS devices are gaining popularity, as a convenient method of sharing files between multiple computers. Potential benefits of network-attached storage include fast data access, easier administration, and simple configuration. However they do not offer the security of using removable media.
Remote backup –

Remote backup is a service that lets your school back up its important data over the Internet to a secure storage platform. RM’s remote backup solution is called ‘RM Remote Safe’. All you need to use RM Remote backup is an Internet connection and the client software installed at the server. Security is handled by a username, password and encryption key policy, which is set up when the client software is installed. Unless you provide it to us, even RM do not know your encryption key, meaning only the network manager who set up the client software will have access to the data.

Of course the first question about remote backup is how fast does it backup and restore data. This comes down to one thing: your Internet connection. To give you a rough example though, If you are backing up or retrieving a large quantity of data, a simple calculation of the time taken to transmit 10 GB of data over an otherwise unused 8 Mbps broadband connection, gives about 3 hours to transmit 10 GB. For a 2 Mbps broadband connection (the government target for all primary schools by the end of 2006), it would take about 12 hours to transmit 10 GB.

Moving on from this let’s have a look at some of the commonly asked questions and answers about remote backup –

Q. What sort of data should I back up?
A. For your peace of mind, we recommend that you back up your critical data such as reports, management systems data, etc.

Q. How safe is the data I back up?
A. Very - it can only be accessed using a username, password and encryption key. Unless you tell us your encryption key, not even RM can access your stored data.

Q. Can I use RM RemoteSafe Server Edition as part of a disaster recovery strategy?
A. If you are considering using RM RemoteSafe Server Edition as an aspect of your disaster recovery strategy, you should consider the following points:
   • During recovery you will need to arrange to have the hardware and operating system rebuilt. After the server has been rebuilt, the RM RemoteSafe Server Edition client can be re-installed and you will be able to start downloading your data.
     Note: You will also need to restore System State information on your rebuilt server.
   • If you are considering RM RemoteSafe for use on a Community Connect network, be aware that the full disaster recovery of a Community Connect server using just RM RemoteSafe is not supported.
     Note: For this reason we do not recommend that RM RemoteSafe be used as the only backup method on a Community Connect server.

Q. How will I know that my backup was successful?
A. The RM RemoteSafe Server Edition client includes an email notification tool, which you can set to email you with a report about every backup that is carried out. You can set this up if you have access to an unauthenticated SMTP server.
Q. If I need to restore an old file, how many days back can I go? 
A. Up to two months (60 days) worth of daily backups are held for you to access online, available 24 hours a day. In case you need to go even further back, data from two previous month ends is also available.

The key information is that for RM Connect networks we do not support using RM Remote Safe as the only backup solution. You should have a full disaster recovery strategy (which I’ll be talking more about in the next module) and remote backup can play a part in that. It offers very fast retrieval of data and the assurance that files are stored securely offsite. However System State restores will fail if you have only backed up with RM Remote Safe, also it is reliant on your Internet connection and we would always recommend having a local backup solution to work alongside any remote backup. Consider it as an additional offsite data store.

Virtual backups – The future is already here

The use of virtual servers is becoming more popular in the IT industry. I found this description of a virtual server and thought this covered it well –

Server virtualization is the masking of server resources, including the number and identity of individual physical servers, processors, and operating systems, from server users. The server administrator uses a software application to divide one physical server into multiple isolated virtual environments. The virtual environments are sometimes called virtual private servers, but they are also known as guests, instances, containers or emulations.

So how does backup work if my servers are virtualised I hear you cry? Well there is a very simple answer – In exactly the same way as a physical server. The server operating system is no different, the backup software used is the same and it is not configured any differently from a physical server.

There is a lot of discussion about this practise in the industry at the moment and there are conflicting ideas on the best way to configure your virtual backups. Until these conflicting theories can be cleared up, we advise you to keep it simple; handle your virtual server backups in exactly the same way as you always have your physical backups. Symantec Backup Exec does not care if your server is physical or virtual; it will back up the data in just the same way.
Small site vs large site

Finding the correct backup solution for your establishment is one of the most important decisions you will make regarding the IT within your school. Most of you will have a stable backup solution installed at the school and hopefully will have a disaster recovery strategy. However I thought it may be useful for some of you to see what else is being used and where.

Internal server backup
In most cases local backup devices like single tape/cartridge drives are used by small establishments with a single server or maybe two servers each with their own backup device.

D2D2T

D2D2T is recommended for larger sites with multiple servers, now of course you could have a local backup drive installed at each server but for that you would need a different set of backup tapes for each server. This can be extremely expensive and time consuming managing these tape libraries. D2D2T will centralise your backups, meaning it will backup all of your servers on your network to one purpose built backup server (RM DiskBox) and then will backup that data to tape via the tape autoloader. This means only one set of tapes is required and it will provide you with duplication of your backed up data (on disk and tape).
The management of the backup schedule is much easier for large sites with D2D2T as it is all configured centrally via the Symantec Backup Exec software which is installed on the RM DiskBox. If the correct software agent is installed you can also use Symantec Backup Exec to back up your SIMS and Exchange servers. This is a very thorough solution for large educational establishments. We will be looking into D2D2T and Symantec Backup Exec in some more detail shortly.

**RM RemoteSafe**

A good recommendation for any establishment. RM RemoteSafe offers secure encrypted offsite data storage and fast data retrieval (depending on your Internet connection speed). However, as previously mentioned RM RemoteSafe does not replace a full network backup and therefore cannot be recommended as a disaster recovery solution but as a data backup solution.

**What if I’m not big or small?**

We’ve looked at solutions suited to small sites and very large sites. But there is a middle ground where D2D2T might be overkill and where simpler options may not give the security needed or be too difficult to manage. If you are a medium sized establishment you may want to consider an RDX library. This is an autoloader for RDX cartridges. RM is currently looking at some new options for our medium sized sites, so watch this space.

**New backup solution?**

If you are considering reviewing your backup solution soon, you need to consider the following –

The size of your network – how many servers?
What data do you intend backing up?
The cost – is the solution cost effective in the long run?

If you are a small school with one server and 12 workstations and less than 100 users, you probably do not need a D2D2T solution. For that example I would suggest a single RDX drive and RM RemoteSafe would give you a thorough backup solution.
D2D2T (Disk To Disk To Tape)

Disk To Disk To Tape is our current recommended backup solution for RM Connect networks. In this module we are going to have a quick overview of what it is and how it works, for those that may not have or seen a D2D2T backup solution. I will also highlight some good working practises and some common misconceptions with this solution.

What does D2D2T involve?

There are four main components of a D2D2T solution –

The network server (requiring the backup)
The staging server
The tape autoloader
Symantec Backup Exec

The network server –
This is any server on your network which requires backing up. D2D2T can backup any RM Connect server as well as other servers on the domain such as SIMS or Exchange servers.
The staging server –
At the core of D2D2T is the staging server. This is a generic term, usually referring to a dedicated network server containing massive hard disk storage which receives backup data from the individual servers prior to duplication (writing to tape).

A staging server can back up multiple servers in parallel, although as the number of concurrent server connections increases, the staging server’s disk write speed may become a bottleneck.

The backup software installed at the staging server (Symantec Backup Exec) limits the maximum number of concurrent disk backups to 16. If a network contains 17 servers or more, the 17th server will not start its disk backup until the first server has finished.

Data is not copied to the staging server ‘as is’. It is repackaged, uncompressed, into discrete files whose contents can only be read by applications which are ‘BKF compatible’. The files all have the suffix .BKF and are uniquely and sequentially numbered – the Symantec Backup Exec default is B2D000001.BKF to B2D999999.BKF.

The RM staging server is the ‘RM DiskBox D’. Three versions of the RM DiskBox have been released at the time of writing, roughly offering 1800GB (b*), 3600GB (C & D) and 7200GB (D - option) of staging storage.

The tape autoloader -
Connected to the staging server via a SCSI cable is the tape autoloader. In order that backed up data can be secured in a physical location away from the RM DiskBox (staging server backup data is not secure), the backup sets are then duplicated to removable media, by a separate ‘duplicate’ job. The autoloader is our media device; an autoloading tape drive.

The autoloader is a tape drive which can hold multiple magnetic tapes and will automatically load them into the drive when the previous tape becomes full.

The autoloader is not connected to the network directly. This means that your network backup should take place overnight from your network server to your RM DiskBox. Once this backup is complete then the transfer to your autoloader can take place. The transfer of data from your RM DiskBox to your autoloader does not use any network resource as it is connected via a SCSI cable. This means you could run your backup to tape during the school day while users are on the network as this process requires no network resource.

There are some common misconceptions about the best way to use the autoloader within a D2D2T environment; I will be going through these in the common Issues section next in this module.
Symantec Backup Exec

When using single drive backup installed at the server, the software you may be using to configure your backups would be something like RM Server Backup, which is based on NTbackup. This is very easy to use software and offers basic backup options. However if you have multiple servers and a D2D2T solution, the software required to manage the backup schedules and processes needs to be a bit more intelligent. That’s where Symantec Backup Exec comes in.

Symantec Backup Exec is the software used to manage your D2D2T backups. In the next module we will be looking at Symantec Backup Exec in more detail and what the common issues can be when configuring and managing your backups.

Common issues with D2D2T

Your D2D2T solution will have been configured by RM so you should not have any configuration issues with your hardware. But there are a few key bits of information you should know about this solution and some common issues and misconceptions we’ve found while supporting this product.

Don’t make your backups easy, make your restores easy!

There is a very common trend with a lot of network managers and IT professionals in general when it comes to backup processes. They spend a lot of time working out the fastest and most economical way of backing up their data. That seems sensible enough but in actual fact it’s completely back to front.

You should always be thinking about creating the fastest and most economical ‘restore’ process. Sometimes this may mean creating a slightly more long winded or tedious backup procedure in order to make any restores or disaster recovery faster.

An example of this is the choices you make with regards to the backup schedule and the type of backups used. Below is a description of the backup types that Symantec Backup Exec offers in D2D2T, afterwards we will look at how this relates to making your restores easier.
Going back to what I was saying before, an incremental backup seems very useful. Your backups will be much smaller and therefore will complete quicker. However, in the unfortunate event of a disaster you will find your restore process is much more complicated, as you will need the last set of full backup tapes and every incremental backup tape since the last full backup. Our advice is the following –

- Daily differential backups
- A weekly full backup
- A monthly full backup

There is some feeling that monthly backups are being replaced by termly backups. This is a decision you should make yourself. Whichever you use this backup should be locked away somewhere safe.
The backups themselves will take a little longer than other configurations you could use. But if you ever have to do a full server recovery you will get your network up and running again much faster using the above methods.

The autoloader – only put one tape in it!

Well not quite but this is by far the most common misconception with D2D2T. You should only be putting in enough tapes for the next backup. Although your autoloader can hold seven backup tapes/cartridges and then be left for the week to do all your backups automatically, we have seen some establishments get in a mess by doing this. It is easy to get confused regarding which tape in the autoloader contains which night’s backup. Also we have seen establishments where they fill the autoloader full of tapes and leave the tapes in the autoloader all week, even after they have completed backup. This completely defies the point of having a removable media backup at the end of the backup solution.

The reason we have a tape solution is so that once the last backup has completed, you can remove the backup tape and store it offsite away from the server. If you leave the daily backup tapes in the autoloader you lose the offsite security that removable media offers. All you have done is duplicated the backup data, and because the autoloader is generally sat next to the RM DiskBox that won’t help you much if the server room catches fire.

For example, if your daily differential backup fits onto one tape then I would recommend putting two backup tapes in the autoloader, one for the backup and one for contingency (in case the first tape fails). Once that backup is complete you need to remove the backup tape and store it offsite from the server room. The ‘auto’ part of the autoloader comes in when doing full backups which span across more than one tape; you can load up the autoloader on a Friday with the amount of tapes required without having to manually change tapes. Remember contingency, it is worthwhile adding an extra spare tape into the autoloader in case one of the tapes cannot be written to.

To summarise – It is your choice how best to use the autoloader in your establishment and how you manage your own tape library. My own recommendation would be to only put enough tapes in your autoloader to complete the next backup (plus one more for contingency). The key thing to remember is: it’s not about making the backup process easy, it’s about making the restore process easy.
Hardware shutdowns/restarts –

If at any point you feel you need to restart or shut down any of the hardware devices involved in your D2D2T solution, you must do this in a specific order to avoid causing a hardware malfunction. Of course this is not to be done while a backup is running.

Off –

• Power down the autoloader
• Power down the RM DiskBox

On –

• Switch on the autoloader
• Switch on the RM DiskBox
Symantec Backup Exec

• What is Symantec Backup Exec?

• Symantec Backup Exec within D2D2T

• Which version?

• Symantec Backup Exec common issues

Symantec Backup Exec

As we’ve briefly looked at earlier, Symantec Backup Exec is the software which manages the backup of your network servers. In this module we will have a quick look at how it works and what it can do, a look at the different versions of Symantec Backup Exec and a few common Symantec Backup Exec issues.

What Is Symantec Backup Exec?

Symantec Backup Exec is the software which enables you to make a full or partial backup of your server(s). This can be either a local backup within the central Media Server (staging server) or a network backup from a Remote Server (network server).

A Symantec Backup Exec Media Server is the server which you use to back up to. The Media Server may have a local tape drive or an attached tape library or autoloader. On larger, multi-server networks using a Disk-to-Disk-to-Tape solution, initially backups might be made to a backup to disk folder. The other servers on your network will also be backed up to your Media Server. These servers are referred to as Backup Exec Remote Servers. A Remote Server would not usually have a tape or hard disk cartridge drive installed.
You need to install Symantec Backup Exec onto your Media Server first. The Media Server is then used to install the Backup Exec Remote Agent onto any Remote Servers.

Appropriate licences must be purchased for all servers that will run Symantec Backup Exec.

In addition, you can purchase optional Symantec Backup Exec Agents to allow the local or network backup of Microsoft® SQL® Server databases and Microsoft® Exchange® servers.

**Symantec Backup Exec within D2D2T**

The Symantec Backup Exec media software must be installed on your staging server (media server). As mentioned above you can install the Backup Exec Remote Agent onto any of your network servers you intend backing up, via your media server console.

Below are some key components of how Symantec Backup Exec works –

**Selection List**

The collection of resources that you want to include in your backup are defined by you in a Selection List. (For example, volumes or drives, folders, files, Exchange Stores, SQL databases). You can define multiple Selection Lists. A resource may exist in more than one Selection List, for example, C: drive on Server 1 can exist in the **Server 1 Complete** Selection List and in the **Server 1 C Drive only** Selection List.

The RM-recommended backup strategy sets up one Selection List for each server that you want to back up.

**Template**

A template defines how your Selection Lists are backed up. It includes information about the backup, such as which Media Set will be used, which device will store the backed up information, and scheduling. However, the Selection List items themselves are not included.

**Policy**

A Policy collects a set of Templates together, and can also contain rules to define which Template takes precedence over another if both are scheduled to run at the same time. Rules also define how Duplicate Jobs run in a Disk-to-Disk-to-Tape environment.
Jobs

Policies and Selection Lists are linked to form several Jobs. You can also define a one-off backup task as a custom job.

You will receive documentation on how to configure all of the above when you receive your D2D2T install. This documentation is also available on our support page – http://www.rm.com/support/knowledgelibrary.asp

It is always worth consulting the RM recommended advice on the support website if you intend changing the default configuration.

Symantec Backup Exec – which version?

There are many different versions of Symantec Backup Exec, however as we are in the present section of our session I will be concentrating on two versions –

Symantec Backup Exec 12.5
Symantec Backup Exec 2010

Symantec Backup Exec 12.5

Symantec Backup Exec 12.5 was released in October 2008 and is common with most establishments using RM’s D2D2T backup solution. Version 12.5 was not a wholesale change to previous versions but did introduce some new features to the Symantec Backup Exec components, I have a listed a few of the key ones below –

Agent for Microsoft SQL Server

Agent for Microsoft Virtual Server
Lets you do the following:

• Back up and restore the configuration settings for the virtual server host, which is the physical computer that runs the virtual server software.
• Back up and restore all virtual machines, which are the virtual computers that reside on the virtual server host.
• Back up and restore selected online and offline virtual machines.
• Redirect restores of the virtual machines to a different virtual server host or virtual machine.
Agent for VMware Virtual Infrastructure
Lets you back up and restore the online virtual machines that use VMware ESX or VirtualCenter. You can restore a virtual machine to its original location, or redirect it to another virtual server.

Remote Media Agent for Linux servers
Lets you back up data to and restore data from the following devices:
- Storage devices that are directly attached to a Linux server.
- A folder on a hard disk on the Linux server.

MySupport Link in the Backup Exec Assistant
Lets you access MySupport, the Symantec Online case submission tool.

Diagnostic support tools
Lets you run the Gather Utility and Debug Monitor directly from Symantec Backup Exec’s Tools menu.

Knowledge Base search integration
Provides a direct link from Symantec Backup Exec to Symantec’s Knowledge Base, which makes it easier to find solutions for problems.

Symantec Backup Exec 2010
Symantec Backup Exec 2010 is the current version of the software, released only a couple of months ago.
I would like to talk briefly about some of the new features of 2010 as it does offer some real benefits.

First let’s have a look at some of the key updates in Symantec Backup Exec 2010 –

Support for Microsoft Windows Server 2008 R2
Lets you do the following:
- Back up and restore data using the new Express (system state) writers.
- Back up and restore operating system boot files from unnamed partitions.
- Back up and restore Cluster Shared Volumes (CSV).
- Back up from and restore to native VHD files.
Support for Microsoft Windows 7

- Lets you install the Backup Exec Remote Agent for Microsoft Windows 7 computers for backup and restore operations.
- The Backup Exec Desktop and Laptop Option provides automated file protection for Windows 7 computers.
- Symantec Backup Exec also supports BitLocker drive encryption.

Integrated deduplication

- Save time and storage costs.
- Minimize backup windows.
- Operational simplicity fully integrated into Symantec Backup Exec.
- Easily adaptable to your environment.

VMware vSphere 4.0 and Microsoft Hyper-V R2 support and new virtual server application support

- First-to-market granular recovery for applications.
- Rapid Exchange, SQL, and Active Directory backup and recovery.
- Eliminate redundant backups and recover data in minutes.
- Protect the latest VMware vSphere and Hyper-V environments.
- Deduplicate virtual server backups
- Reduce and consolidate storage.

Deduplication

What is deduplication and how can it help me?

Data deduplication is a method of reducing the storage needs by eliminating duplicate data.

I have mentioned it here in our ‘present’ section as it is new functionality that comes with Symantec Backup Exec 2010, however I will be talking to you more about deduplication in our ‘future’ section. This is because RM is still running field trials and tests to find how best it can work within an RM network. I would certainly not advise you go back to school and try and configure deduplication tomorrow. However the theory behind what it can do is worth looking at, so we will revisit this later.
Symantec Backup Exec common issues

I’ve collated a couple of the common issues found when using Symantec Backup Exec. I thought these were worth mentioning as these are common queries or misconceptions made when configuring or using Symantec Backup Exec.

The overwrite protection period –

The overwrite protection period specifies the number of weeks, days, hours or minutes that a tape cannot be overwritten by Symantec Backup Exec. We have come across issues in the past with customers customising the overwrite protection period. The most common mistake made is by setting the overwrite protection period to 0. This implies that it will not protect the overwrite and tapes can always be overwritten, this is not the case. In fact the opposite happens and the writing to tape will fail completely. Our advice would always be to leave the overwrite protection period as the RM default setting.

Backups are failing –

There are of course many reasons which can cause backups to fail. One of the first places to start is to see if Symantec Backup Exec has reported the fail. For this you are searching for a V Code error. A V Code is an error reported by a failing component or configuration of Symantec Backup Exec. To check for V Code errors you need to do the following –

• Click on Job Monitor
• Select Job History
• Double-click the job in question
• Now search for any V Code errors/alerts.
• Within the V Code is very often a link to a Symantec technical article which will explain the error and often will provide solution information.

If you cannot find a V Code error some other things I would suggest looking into would be –

Check Event Viewer on the server for errors, under both Application and System events.

Services – Symantec Backup Exec installs specific services within the server environment when the software is installed. Sometimes as a diagnostics step it is a good idea to stop and start the Symantec Backup Exec services.
To start or stop Symantec Backup Exec services –

2. Select the appropriate options as per below.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Indicates the name of a server for which you want to start, stop, or restart services. You can type the name of a server or import a list of servers.</td>
</tr>
<tr>
<td>Add</td>
<td>Enables you to add the name of a server for which you want to start, stop, or restart services.</td>
</tr>
<tr>
<td>Import List</td>
<td>Enables you to import a list of servers for which you want to start, stop, or restart services.</td>
</tr>
<tr>
<td>Start all services</td>
<td>Starts all Backup Exec services for the selected server.</td>
</tr>
<tr>
<td>Stop all services</td>
<td>Stops all Backup Exec services for the selected server.</td>
</tr>
<tr>
<td>Restart all services</td>
<td>Stops all Backup Exec services and then restart the services for the selected server.</td>
</tr>
<tr>
<td>Services credentials</td>
<td>Changes service account information or changes startup options.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Refreshes this dialog box.</td>
</tr>
<tr>
<td>Remove Servers</td>
<td>Removes a selected server or servers from the server list.</td>
</tr>
</tbody>
</table>

**Selection Lists –**

One common mistake made by customers is when adding a new server into Symantec Backup Exec. It is often forgotten to add a Selection List for the new server.

We strongly recommend you create one Selection List for each server you want to back up. Although this makes more Selection Lists (and thus many more Backup Jobs), it is easier to manage (and troubleshoot, if required) in this way.

1. On the Job Setup tab, in the Backup Selection Lists section, right-click and choose New Backup Selection List.

2. In the ‘Selection list name’ box, type the name `[ServerName] Full` (for example, `RMS-SR-002 Full`).

3. Type the same name in the ‘Selection list description’ box.
4. In the Selection window, choose the local items you want backed up as part of your backup strategy by selecting (ticking) the corresponding boxes.

5. For a typical Windows 2003 server, under [ServerName], Local Selections, select:
   - All fixed drives
   - System State
   - Shadow Copy Components

Note that for the RM Disk to Disk to Tape backup solution, you need to select only: —

The C: drive
The folders on the D: drive where the catalogs and logs are stored (ensure that no other folders on the D: drive are selected).
The System State and Shadow Copy Components for the RM DiskBox.
For this Selection List, type the name ‘DiskBox C drive only’.

Further information on adding different types of servers into Symantec Backup Exec can be found in the RM Knowledge Library - http://www.rm.com/support/knowledgelibrary.asp or in your Symantec Backup Exec Administrators guide supplied with the software.

**Symantec updates**

If Symantec Backup Exec has pulled down software updates from Live Update it is important to check if these updates are for the server media or the agent software.
If the agent software has been updated it is important to push out the updates to all servers using that agent.
It is also worth noting that many of the updates require a reboot of the Media Server but this reboot is not prompted for, you have to go and find it in the Alerts tab or in the Event Viewer Application Log.
The future

Now we move into the future. We’re going to have a quick overview of the future of backup. What are the brand new technologies you might not know of and what is around the corner? Some of these technologies might already be used in some of your establishments, so why am I covering them in the future section you ask? To answer this briefly, I am showing you what I believe will be the future of backup over the next five years.

Diskbox XL

Soon to be released by RM is the ‘RM DiskBox XL’. This offers a few benefits over the current RM DiskBox. It will run on a 64bit operating system, utilising the 64bit hardware. There will be many configuration options in terms of CPU’s and memory. Also worth mentioning is we are introducing LTO5 libraries with the RM DiskBox XL, which is connected via SAS rather than SCSI. This offers a lot of benefits, the main one being transfer speed is increased with SAS.

D2D2D

RM is currently investigating a D2D2D (Disk To Disk To Disk) solution, and some third party D2D2D solutions are already available on the market. The concept works in a similar way to D2D2T but the tape drive autoloader is replaced by an RDX cartridge Library.
As we looked at in our past section an RDX cartridge is basically a laptop hard disk drive encased in a plastic cartridge. The media is still removable so nothing really changes, apart from the time it all takes. Reading and writing data from hard disk drives is much faster than from tape; using D2D2D will shorten your backup window, lower costs of removable media and will make disaster recovery much faster. All while still offering the same offsite security that comes from using tapes.

The cloud

As we looked at earlier in the session cloud backups involve backing up your data to an offsite data storage centre via your Internet connection. As Internet connection speeds rise and establishments have to manage their costs, I can see this method of backup is going to become used more and more.

Current cloud based backups do have some disadvantages such as –

- Dependence on the speed and reliability of the Internet connection in question.
- Size limitations - Depending on bandwidth availability, every organisation will have a threshold for the most reasonable capacity of data that can be transferred daily to the cloud.

However I can see these limitations being overcome in the next few years and therefore I see cloud backups as a strong part of your backup strategy. In my opinion it will never become an all in one backup solution as it relies solely on your Internet connection. I see local backups as an absolute requirement for any network and for now I do not see that changing.

Snapshot backups

The difference between a snapshot and a copy is that one is virtual and one is physical. A snapshot is a virtual copy; it’s a photo or a static view of your data. I found this description online which explains it well –

Snapshots imitate the way a file or device looked at the precise time the snapshot was taken. It is not a copy of the data, only a picture in time of how the data was organized. Snapshots can be taken according to a scheduled time and provide a consistent view of a file system or device for a backup and recovery program to work from.

To give you an example, snapshots are currently used in VMware. You can use them as system restore points for virtual machines. It will record the file system, the VMware configuration and the BIOS configuration. This is very useful when testing if a new application is going to break the file system, if it does you can restore back to your snapshot image very quickly.
This is a very basic example of where snapshots are currently used but as virtualized networks become more and more common in the future, I can see snapshot technology becoming a key part of your backup strategy. It is key to remember I am talking about this technology in a ‘future’ context; there are some problems we have seen with snapshots currently. Mainly when rolling back to a snapshot on a domain controller, there is a potential you may break the Active Directory. Snapshots are not a replacement for backups as we stand but as I stated I can see them becoming more useful in the overall backup strategy.

**Deduplication**

If during a backup there are found to be multiple instances of the same file, with deduplication it will retain one instance of the file and will replace every other instance of the file with a pointer to the unique copy saved. For example; you have an email server being backed up. There are 100 instances of the same 1MB email attachment within the email data. Previously all 100 copies of the file would be backed up, requiring 100MB of storage space on the backup media. With data deduplication only one instance of the email attachment will be saved and all others will be referenced back to the one saved copy. In this example we have reduced a 100MB storage requirement down to 1MB.

Major advantages of deduplication include hardware costs. Of course as your backed up data is smaller, you may not require as much disk storage or backup tapes. There is evidence to suggest that the average data held in a school is growing between 15%-30% per year. Deduplication can play a major role in lowering the costs of your backup media, even as the data itself grows. One other advantage worth mentioning is the backup time itself, if less files are being transferred and your backups are smaller, of course your backup window will be smaller. This also plays a very important role in disaster recovery; restoring deduplicated data across the network will also be much faster. The use of deduplication also makes remote backups much more effective due to the time a backup and restore will take compared to non duplicated data.

Used with hardware compression, data deduplication offers huge advantages in optimizing the use of your storage space.

Deduplication will only work on the new RM DiskBox XL with Symantec Backup Exec 2010. It is not supported by the current RM DiskBox Range.
Summary

Whether you are using a backup solution from the past, present or future there is one fairly new component of data backup that I can never see changing; the backup strategy.

The need for a written backup, or should I say ‘restore’ strategy will always be the most important aspect of any backup solution. Review this strategy on an annual basis, as your data will grow each year your backup requirements may change or your restore process may require changes.

When thinking about your own backup strategy, the key statement to remember is –

Don’t create a strategy to make your backups easy, create a strategy to make your restores easy!

Of course there is a lot more information available on all of the topics I have spoken about in this session. Backup is a very wide subject and I have tried to pull out the key information relating to some of the past, present and future backup technologies.