Server recovery: revisited

Introduction

Server recovery is the final answer to problems, it’s a stage in network management you don’t want to get to and it’s certainly not a step you should take without actually needing to. I’ve spoken to many people around various levels of support and there are some scary stories of servers being rebuilt without any full troubleshooting process. I’m saying it at the start, to make sure it’s not lost in any other text. Server recovery should not be carried out unless you have fully identified that it is required, in fact the only option.

In this session we will be looking at the process of server recovery, but not in huge detail. It would be a waste of time re-writing what has already been written, the process is in documents which are available on request. I will be covering parts of the process which aren’t written down. This is the planning, organising and foreseeing, if you like, of a disaster.

We will also be looking at some things that have changed since our last visit to the last resort. Since then more and more establishments have installed virtual networks, SAN’s and CC4. These three developments change the planning and execution of a server recovery, here I’ll show you the things we need to consider.
Backing up

As I mentioned in the introduction, the purpose of this session is to prepare you for complete server failure, as the likelihood of you needing to recover a server directly after reading this or attending the presentation at the seminar are slim, very slim. So we have to start at the first thing you need to do, and that is to make sure you have a successful backup.

It may seem an obvious statement but you may be surprised at the amount of times we hear of backups not being run daily or checked on networks. When backups haven’t happened and the server fails, you will feel like crawling under the nearest rock. This is not a situation we want you to be in, or we want to try to pull you out of.

The process of backing up has changed during the last few years too, we have disk to disk to tape (D2D2T), remote backups, tape loaders and other such things that were only used in a handful of sites when I was managing networks. There is a backup session running this round so to go into detail on these solutions would be to steal Matt’s thunder.

Backups are 100% your responsibility. If you are running a network you must make sure you are backing up on a daily basis. Just because you bought the server, the tape drive, the tapes, the software, the warranty and the installation from us, it’s still your network!
Your DR Plan

- 1 in 3 Schools don't have a DR plan!

- If you do, have you looked over it recently?

- Re-assess your DR pack and plan every 12 months

Your DR plan

During the process of planning the seminars I will spend some time checking that all the subjects we talk about have the information available to talk about. I spent some time looking at some recent market research we have been doing over the last year, this was for a presentation that isn’t related to this, however, there was some information that frightened me.

One third of schools don’t have a disaster recovery (DR) plan! I had to re-read this and check that the figure was right. Surely there can’t be that many networks with absolutely no plan should catastrophe fall upon them? Our chap who had done the research said that was correct. The more I think about this the more worrying it is, this isn’t measured on it being the perfect DR pack. It is referring to having no plan whatsoever. This doesn’t include packs and plans that are not complete, out of date or simply wouldn’t hold together in a strong wind. Of course there is some speculation there, but I’m confident in my assumption that at least some of those networks which have DR packs and plans aren’t as prepared as they could be.

The first thing a network needs once it’s set up is a disaster recovery pack and plan, what happens if this all goes wrong. Once this created, it needs to be reviewed once a year (at least). This is to ensure that anything that changes is incorporated.
You may notice that I keep referring to the DR pack and plan, quite often all we talk about is the pack, the physical information required to restore a network, which we will cover next. However there is also the need to have a plan, what actually happens on D-Day? This will be covered later on in the presentation but to put it into your mind now, there also needs to be a plan of action. What will each member of your team do and who else will be involved should the worst happen.

First we’ll go back over what is needed in your pack, as a minimum.
Creating your DR pack

The first thing and probably easiest thing to get together is the DR pack, as it doesn't involve people who need to be negotiated with. It is a simple collection of information and software. This needs to be completed for each physical server (we will cover differences with virtual networks later).

Backup

Ok, I know I’m already starting to sound like a broken record here but the backup is important. All the other bits in this pack can be sourced from somewhere if you don’t have them or guessed and botched together if the information isn’t there (not that I am advocating such behaviour), the backup is the only copy of your information that exists, anywhere. If you don’t have this there is a possibility you won’t be asked to come back into work should the unthinkable happen. No-one wants that to happen.

The backup tape needs to be recent (we’ll cover how recent in the next section). There’s no point having a backup from three years ago, I don’t intend on validating that point as it should be self explanatory. Validation is something that needs to be carried out on any tape which will be used for a disaster recovery. It would be a disaster in itself to get as far as sitting down to recover...
your server to find that the backup you are working from doesn’t actually work. For this reason, finding some time at least once a week to check that each server’s backup is restorable. My advice is to make sure you can restore something low down in the tree. This helps ensure that the backup has run through to the end without error. It is possible to check the logs, but don’t trust them. Logs are there to check when something is wrong, there is always the possibility that the log isn’t telling you something. Once a week book some time to go through these test restores. Book it so you will not be disturbed during this period, perhaps pick a time when generally you’re not overwhelmed with urgent requests – as an aside, if you are regularly overwhelmed with urgent requests it may be worth popping along to the FITS session this round (or at least reading my notes on it).

Server recovery CD

The server recovery CD will be required to recover your server operating system. This is very straightforward, so this sub section is not going to be huge. There are a couple of things you will need to check. If you have RM hardware, you’ll need to check which CD you need, you should still have the recovery CD that came with the server. If you don’t have that CD or you have a CD for each server but you’re not sure which is which check article NWS640565 which will help you identify the CD you require.

If you have other hardware a Windows® Server 2003 recovery CD is required.

Service packs

Service packs that have been applied since the install will need to be re-applied; make sure you have these stored on an external hard drive somewhere. Don’t forget, while recovering the server you will not be connected to the Internet (you’ll need to disconnect the server from the outside world to avoid virus attacks). Don’t forget to update your pack each time you install a service pack to the server.

You will need Windows 2000 Server SP4 and/or Windows Server 2003 SP2 depending on your OS

SCSI/RAID drivers

You’ll need your drivers stored on an external hard drive. If you are updating these drivers they also require updating in your DR pack. Don’t rely on downloading these on the day. The key to recovering your network is getting things up and running as soon as possible, fiddling around trying to find the right drivers is going to slow the process down. The server recovery process must be slick and efficient; the only way to ensure this is to have everything to hand when it does happen. If you have the correct RM Server Recovery CD the RAID drivers are included. You only need RAID drivers if you haven’t got the RM Server Recovery CD.
Disk configuration

The configuration of disks should be noted down. Even if you are running a single server network and can proudly recite each aspect of your disk configuration while standing on your head, write them down. The day the network dies will be stressful (hopefully less so having followed these steps), stress can do funny things. Don’t rely on your memory. Also don’t discount the possibility you’re not going to be there if something happens, and if that happens you will need to make sure someone who doesn’t have your knowledge can find this out easily.

First thing to note is how many disks you have in the server, and don’t forget to update the pack if you install a new disk.
Secondly what size are the disks? It’s no good replacing a 300GB disk with a 40GB disk.
Finally how have those disks been partitioned? It’s important that the disks end up in exactly the same format as they were before as when the restore starts, it will be looking to put those files back in exactly the same places.

Server name and TCP\IP configuration

Considering when the server comes back up we will need to connect it to the network, the computers and other servers will need to see this as exactly the same server as before. As far as other network components are concerned this server has been offline for a while and is now back, even if you have to replace the whole server other network components should be unaware of it.

Backup application

I would suggest having a copy of the backup application you use as well. It’s easy to overlook this small point. If the server you are about to restore doesn’t have the software to restore that could add time onto the schedule. It seems obvious stating it, but the point of the pack is that the obvious stuff is contained there too. An example of this is if you are using Symantec Backup Exec 11d, if you do not have an installation agent for this it’s not easily available to download, searching the Internet for this kind of information is not going to help you or a colleague on the day.

We’ve got the pack together and we’re confident that if anything goes wrong we have all the software and information that is needed to get the network back up and running. Many DR plans stop there, because surely when the network goes down everyone in the school will know not to bother you and you can just get on with it. Experience tells us this isn’t the case, so we need a plan of action too.
Setting a DR plan

This is the bit that takes a bit more effort. Here we need to negotiate with a number of people to get the plan together. From speaking with ex-network managers at RM, people who currently manage networks and working from my own experience in these situations things don’t always run smoothly. To make sure they run as smoothly as possible, work out how the day will pan out.

Let’s actually look at a scenario. You get to school in the morning and find the system is down. Through a course of diagnostics and troubleshooting you recognise there is a hardware fault in one of the servers. You ring RM Support to double-check with them and confirm the server needs to be restored.

What else?

• What is expected of you?

• Who does what?

• Don’t panic
Having acquired the new hardware required you now need to get on and restore the network. You grab your disaster recovery pack and...

There is some more preparation that needs to be done before you get on with the restore. Don’t forget teachers will be looking to get onto email, marking systems, pick up files off the network or get on Facebook. Students will be having lessons in the IT suite cancelled, therefore they see a chance to bunk off and muck about while the teacher tries to sort out what to do for the lesson.

The senior leadership team will be seeing this and asking some big questions of you. How long? What is broken? How did it happen? What is the extent of the damage? How much have we lost? When can you fix it?

While your head is spinning, as you are nowhere near ready for this sort of action this early in the morning before your morning tea or coffee, you want to be able to answer those questions but you just want to get on with it.

With all this going on, the system restore is not going to be easy. In actual fact, it should be. This is why you need a DR plan, so that you can mobilise while everyone else is flapping.

**What is expected of you?**

First things first, you need to speak with the senior leadership management team and agree some key points.

- What needs to be restored first
- How much data can be lost
- Restore timescales

When having this conversation have some figures already planned out, this is what you are trying to steer towards. It may be that things don’t end up exactly as you like them, but you are likely to get closer to what you want by giving them an idea of what you believe is realistic.

Checking what needs to be restored first is looking at the most business critical applications that need to be checked and up and running. That is your priority once the server is up, this is key to keeping a calm head (both your head and the head teacher). If you can make sure you have the most critical systems up and running first, you alleviate the pressure. Of course everyone thinks their system is the most business critical in the school, that’s why you get agreement from those in charge of the school. Anyone who says they have a more important system can be directed to the head.

How much data can be lost? Well everyone will say nothing can be lost, this step is more about getting agreement and understanding that if a failure happens during last night’s backup you’ll have lost all of yesterday’s work. If there is a risk with your current backup solution that more than a day’s work may be lost, this meeting will help put that across.

Restore timescales is the tricky part. You have to work out how long, in the event of a complete failure it should take to restore the network to working
order. This is not straightforward and I would urge you to do some rough calculations for a single server and then work on the full network and add half again of contingency on the end. This is the figure you want to reach during these negotiations.

Now you have agreements from the senior leadership team and you know what is expected of you. We now need to look at the actual plan of action.

**Who does what?**

Here is another part of the plan that can get overlooked. No matter how big a catastrophe it appears to be or how busy you look people will pester you as the network manager, they won’t see that you need calm. So you have to fill three key roles to stop this.

- **Engineer**
- **Guard**
- **Messenger**

The engineer gets locked in with the DR pack and the server, yes locked in. The person who takes this role cannot afford any distractions. Therefore that server room door is locked behind them.

The guard stands on the other side of the door stopping people from getting to knock on it. This role is important, the guard can help redirect queries or relay any up to the minute information.

The messenger is the person who relays messages to the school about the status of the restore. This cannot be the guard but could be a member of the SLT.

With these roles in place the restore should be able to happen with the least disruption possible. The less disruption the quicker the restore and the faster everyone gets back to the systems they require.

**Don’t panic**

With the DR pack built and the DR plan in place, there should be no need to panic. The engineer will read through the DR instructions and hey presto, before you know it everything will be back up and running. It may sound optimistic but most recoveries that fail are down to the instructions not being followed – that is normally due to distractions that are not needed.
What’s the problem?

Anything that goes wrong on the network should evoke this question from you, just because this is a complete failure of ‘something’ in the server does by no stretch of the imagination mean you should just shrug and get on with the restore. After asking this question you may find you don’t actually need to carry out a full server recovery at all. There are plenty of scenarios where server recovery is not required, even though you are face to face with a blue screen.

As mentioned in the introduction, the last thing you want to do is carry out a server recovery, full stop. The Blue Screen of Death can be caused by a number of different issues. Driver conflicts and recently installed software can...
cause this, it’s always better to try the last known good configuration before charging head on into hours of work.

If the server simply won’t boot you may start thinking this has to be a hardware failure. Not necessarily (Matt is covering hardware diagnostics this round so I’d recommend at least reading his notes for help with this), servers can fail to boot due to boot file corruption these can be replaced rather than restoring the whole system.

Active Directory corruption or having deleted some objects in Active Directory can be restored without needing the full server recovery process. These situations will either require an authoritative or non-authoritative restore.

**Non-authoritative restore**

A non-authoritative restore is where the Active Directory is restored, the server is brought back on line and any Active Directory objects that have changed will be updated via replication. The server which is being restored has no authority over the others in regards to the current state of Active Directory. This method would be used where there is corruption in the Active Directory but not from human error.

**Non-authoritative restore SYSVOL**

When you non-authoritatively restore the SYSVOL, the local copy of SYSVOL on the restored domain controller is compared with that of its replication partners. After the domain controller restarts, it contacts its replication partners, compares SYSVOL information, and replicates any necessary changes, bringing it up-to-date with the other domain controllers within the domain.

Perform a non-authoritative restore of SYSVOL if at least one other functioning domain controller exists in the domain. This is the default method for restoring SYSVOL and occurs automatically if you perform a non-authoritative restore of the Active Directory.

If no other functioning domain controller exists in the domain, then perform a primary restore of the SYSVOL. A primary restore builds a new File Replication service (FRS) database by loading the data present under SYSVOL on the local domain controller. This method is the same as a non-authoritative restore, except that the SYSVOL is marked primary.

**Authoritative restore**

An authoritative restore is an extension of the non-authoritative restore process. You must perform the steps of a non-authoritative restore before you can perform an authoritative restore. The main difference is that an authoritative restore has the ability to increment the version number of the attributes of all objects in an entire directory, all objects in a sub tree, or an individual object to make it authoritative in the directory.
As with a non-authoritative restore, after a domain controller is back online, it will contact its replication partners to determine any changes since the time of the last backup. However, because the version number of the object attributes that you want to be authoritative will be higher than the existing version numbers of the attribute held on replication partners, the object on the restored domain controller will appear to be more recent and therefore will be replicated out to the rest of the domain controllers within the environment. Unlike a non-authoritative restore, an authoritative restore requires the use of a separate tool, Ntdsutil.exe. No backup utilities including the Windows Server 2003 system tools can perform an authoritative restore.

An authoritative restore will not overwrite new objects that have been created after the backup was taken. You can authoritatively restore only objects from the configuration and domain-naming contexts. Authoritative restores of schema-naming contexts are not supported. Perform an authoritative restore when human error is involved, such as when an administrator accidentally deletes a number of objects and that change replicates to the other domain controllers and you cannot easily recreate the objects.

NB. To perform an authoritative or non-authoritative restore, you must start the domain controller in Directory Services Restore Mode.

**Server hardware failure**

If, having run through full troubleshooting with RM Support, you confirm that the RAID array has died, master hard drive has died or other such catastrophic failure has happened then it is time to start proceedings on the server recovery. Don’t forget RM Support is there for a reason and you don’t have to go through this by yourself.

Once the hardware replacements are available my best advice is to follow the documentation. Computers are not unpredictable; they are totally logical and predictable provided you know what’s happening with them. The server recovery process we supply is very detailed and will give you everything you need to restore your server to working order. If anything out of the ordinary happens ring us and we’ll be able to assist. Don’t forget, you have to be an unlucky network manager to have to do this once in your career. To put this into perspective, I was speaking to a colleague who used to manage networks before joining RM. He used to manage 100 servers for seven different customers, over five years he only ever had to recover one member server. We do server recoveries on a regular basis in comparison, don’t feel calling us is shying away from your job.
What if...

There are a number of changes that have happened to many networks since we last visited the server recovery process. It has only been a couple of years but at that time there was a lot going on. While we spent time looking at the CC3 process (which varies very little from the industry standard methods), virtualisation started to be utilised more heavily in educational establishments, this changes the way we need to approach server recovery. Storage Area Networks have been installed in more and more sites; these huge storage centres hold data from all over the school and are also used in virtual networks, what happens if one of these fails somehow. Also CC4 uses its PostgreSQL database rather than relying on Active Directory for everything. How do we ensure that this can be restored, and how do we go about restoring it.

Here I am potentially opening a can of worms in terms of information that I could give. I’m sure I could present for two hours and write a small book about any of the above, but the purpose of this session is to give you the tools to follow the documentation. Make sure you are prepared for anything that may happen in the future, giving you a process to follow would be reinventing the wheel and frankly muddying the water should you ever need to recover a server.
Virtual network restore

So you have a disaster on your hands, you’ve checked everything and it’s server recovery time. Where do you start? Where has it gone wrong? Where is this actually different from the standard process?

Ok, let’s start at the very beginning; before we start worrying about each individual complexity, how about we just look at the basic information. Once we can identify the top level stuff, we can then start to scratch a level deeper.

What is a virtual network?

This may seem like a silly question to be asking someone who is already managing a virtual network, but we have to be clear that in any plan the basics are the best place to start. Then we can start asking questions of those basics and build the bigger picture. We can also quickly discount parts that don’t vary from the norm.
What are the differences?

Let’s begin by making sure we are all reading from the same page as such. Excuse me for labouring this point somewhat, but I know our experts, some of you and other companies sometimes confuse things by referring to parts of a virtual network differently. I found this while speaking to a few people and studying VM documentation. This is not to say anyone is wrong, but for the purpose of making server recovery simple and understandable I must define the definitions so everyone is clear on what we are talking about at each stage.

Starting from the bottom with the least ambiguous section of the network.

**SAN** (Storage Area Network), typically a stack of storage devices that act as extra storage on physical machines.

**Host**, these are the physical boxes that have you virtualisation software on. These are servers that have moving parts in them.

**Virtualisation software**, although we sell VMWare ESXi I’m purposely avoiding just talking about that particular software. This is due to the fact in this instance the software which is hosting your servers is not relevant. Where I can only vouch for ESXi being able to carry out a particular action I have mentioned it.

**Physical server**, this is a physical tin box server with working parts that you can remove then smash, set fire to and pour water on. Don’t do any of those things by the way. This term is simply to distinguish between virtual and physical.

**Server**, these are the virtual servers. I’ve referred to them as images before but for the sake of clarity these are servers. This also serves the purpose of clarifying that virtual servers are just servers and should be viewed no differently.

Have a look at the desktop; this is merely to illustrate a point. Look at two Windows Server 2003 desktops, everything software, configuration, shortcuts and desktop background are the same. Except one is virtualised the other is not. Which is which? In the System Tray there is an icon to show that VMware Tools is installed’. That is your difference. Everything else is the same.

The whole point of a virtual server is that it is an exact replica of a physical server just without being tied to a single box. That’s a good start, we now know that anything that happens to that server can be restored in the same way a standard physical server can.

That’s at least the server covered, now what about hardware? It’s the same question, what is a virtual network when it comes to hardware. It may be that you have a different setup to this but the basic theory is the same. What physical hardware do you have that can fail? I am using the standard RM implementation of a virtualised network.
What is there that can fail in this diagram? Your SAN will be covered in a moment. The hosts may have hardware failures if you are unlucky. So what happens if a host fails? We go back to the question before.

**What is the problem?**

And so the loop is complete. If a host fails we have to start by asking what the problem is. How has it failed? I won’t go through this again.

In the meantime, your network users have barely noticed a problem as virtual networks are designed to be robust enough that when a host stops running either you can balance the servers yourself or ESXi will do it for you. So what do we actually need to be worried about?

If the host fails all you need to do is identify the problem, get the replacement kit, re-install virtualisation software again. Once it’s reconnected to the network just spread the load on the hosts again.

It’s worth re-iterating the point that the software you’ve chosen to virtualise with doesn’t make a difference in this process. It’s as irrelevant as the hardware in a physical server.
SAN Failure

- Recording cabling
- Recording server configurations
- Mirroring

SAN failure

As identified in the virtual network section this biggest problem you may have if there is a SAN failure. Depending on what exactly goes wrong, we’ve already covered this being the first thing to work out, this could take the network down in one. Much of the documentation and information that is out there points towards a SAN never failing due to mirroring and built in failover solutions. As we’ve already covered the likelihood of you having a SAN or network (virtual or standard) actually fail on you are very slim. We all hope this will never happen and manufacturers of hardware, developers of software and supporters of all of the above do as much as they can to make sure it doesn’t happen.

This presentation is of course about making sure you are prepared for the unthinkable and giving you the best opportunity to turn it around quickly. In this section we will look at what happens if the SAN has a failure, whether it is affecting one server or a number of servers (regardless of whether they are virtual or not) and most importantly what information you can have available to make sure there are no problems getting those back up and running.

Recording cabling

SAN cabling is something you’ll want to record, if you don’t have anything to work from this can cause difficulties and add time onto the overall process of a recovery. The last thing you want to is to think you’ve recovered the SAN to find there are issues and have to unpick and re-cable the SAN and switches.
Because SANs come with two switches (one of which is a failover) it’s easy to have a look and think this is simple to put back together.

I discovered this in a similar situation during my work at this year’s BETT. I was tasked with supporting the Learning Spaces in O2, one of the hundreds of pieces of kit we were responsible for was the Chroma Key kit (green screen technology). This isn’t a SAN but does need a set of cabling that I’m not privy to nor did I have the time to learn it with all the other kit. Before dismantling it in the REAL Centre we took photos with my phone and made sure all the different connections were noted and labelled. We got it to BETT, spent the week using it and then on the Friday night packed it down.

The packing down of BETT is manic, there a lot of false walls to come down, kit to be removed and contractors doing their various bits and bobs. So while all the partners we had there unplugged and removed the kit they were taking back as quickly as possible we worked into the early evening palletising and loading the lorry.

Once we returned to Milton Park we decanted all the kit and sent it back to the relevant places. The Chroma Key kit had been sent directly back to the REAL Centre where another technician took over the role of setting it back up (having never done more than look at it before). We had a tour going on at 12 that day (this is the Monday). We got a phone call asking to come up and set it back up.

We arrived I got my phone out and looked at the photos, checked the labels and re-arranged a couple of the cables. Once reconfigured, we checked the cabling and turned it on.

The Chroma Key kit was not working fully. We re-checked the cabling referencing the photos and couldn’t find a problem, until we looked at one of the photos and realised that one of the cables actually hadn’t returned with the kit. We identified who had packed this down and contacted them, they sent the cable back and we got the kit up and running. This was just before the REAL Centre tour started.

The point of this story is threefold:

1. Good records of the cabling can save lots of time (Photos are a quick way of doing this).
2. Make sure you make this available to anyone who may need to reconfigure the cabling.
3. Labelling is also very useful.

NB. Yes labels on cabling is useful, two extra tips here though. Make sure it is very clear and there can be no mistaking what should be plugged into where. Secondly make sure the photos are done after the labels. This will help avoid any confusion.

In the case of a SAN recovery, it can be manic even if planned. If for any reason you draw a blank on how it was cabled up ten minutes ago there is a
reference. We cable and uncable various hardware all the time, a SAN is not one of those things, unless you are running military style drills, so don’t take it as read you’ll be able to reconfigure this in a couple of minutes without any issues.

**Recording server configuration**

What a SAN does is ‘pretend’ to be physical storage in a server whether a physical or virtual server is unimportant (as covered in the virtual network section there is little difference), so when preparing for any failure you need to make sure you’re aware of where the SAN connects to other servers.

Here I’m going to refer to failures in a ‘disk’ or ‘disks’, this again is simple terminology to remove the ambiguous nature of technical detail that does not need to be covered in information regarding server recovery preparation. A ‘disk’ refers to part of the SAN which is a storage device – whatever it is you refer to that as I don’t intend on contradicting or arguing with it.

If you have a failure in ‘disk1’ on the SAN, which servers are going to lose which drives? This is vital to the recovery process, it may be that you can restore those partitions from backup without issue but it’s worth recording from two points of view.

My first example is that a ‘disk’ fails in the SAN and you need to identify which ‘disk’ in the SAN has failed. By a simple and quick process of elimination, by asking what is and isn’t available, you should be able to tell where the SAN has failed, having taken note of the configuration of course.

The other side of this is where servers need to be recovered and require restoring; it’s always useful to know where the data will be connected to. Backup’s actually record the SAN configuration and when restoring they should restore back to the correct ‘disk’. This said, take note of the configuration and how it’s being held together, never rely on the technology alone.
Recovering the CC4 Database

- Back it up – how to
- Check it’s backed up – how to
- Restoring

Recovering the CC4 database

One of the major changes over the last two years to the process of server recovery is the addition of the CC4 database. It’s an integral part of CC4 and as important as Active Directory is. So it would be bad practice to have not planned for the case of a failure.

Should you lose the CC4 database there will be all sorts of problems. So the first steps are making sure that there is a backup of the database. As with any backup, you’ll need to check the backup is actually working and regularly test the backup. Then we can look at restoring.

Backing up the CC4 database

As with all databases (Printer Credits and other SQL databases) they cannot be backed up while running. You need to stop the database so it can be backed up as a flat file. What we aren’t suggesting by any shape or form is to manually every evening stop the services and manually back it up.

CC4UPD028 made sure that backups of the database work on all backup solutions. What this update did was create a scheduled task to ensure the database is stopped before the backup takes place, thus enabling it to be backed up as one flat file. Most backup solutions will tell you that the database has been backed up successfully as the files are not locked. However when the database is restored may error due to an inconsistent database state.
Instead of just mentioning this is the process and pointing to a technical document I feel it would be beneficial to see how we go about setting a scheduled task to enable the CC4 Database to be backed up. This will help you double-check that the scheduled task is configured correctly.

To create a scheduled task on your Forest Root domain controller which will back up the Postgres database to the local hard drive:

1. Log onto the server as a system administrator.
2. From the Start menu, open Control Panel. Select ‘Performance and Maintenance’, Scheduled Tasks. The Scheduled Tasks window opens (if you are not using the Container View, select Start Menu, Control Panel, Scheduled Tasks).
3. Double-click Add Scheduled Task to run the scheduled task creation wizard.
4. When asked to pick the program that you want to run, click the Browse button and browse to C:\Program Files\RM\Connect\DB Maintenance\RM.Networks.Comms.DBMaintenance.PGDBBackup.exe.
5. At the next window, give the task a meaningful name such as Postgres Database Backup.
6. Configure the task to run Daily.
7. Set the time as appropriate, depending on when your server backup runs. The database backup is not a lengthy process, so a gap of 15 minutes between the two should be enough. For example, if your server backup runs at 11:00pm, set the Postgres Database Backup to run at 10:45pm.
8. When asked for the username and password of the user who should be used to run this task, type the username SYSTEM and do not enter any password details.
9. Click OK to finish creating the scheduled task. You should now see your new task in the list.

Note: This task only needs to be created on the Forest Root domain controller. Other servers do not host the database and do not need to back it up.

Testing the scheduled task

To test that the scheduled task runs correctly, right-click the task created above and select Run. You should then see a folder named with a date and time stamp in D:\RMNetwork\RMManage\RMDatabases\backup (for example, a backup taken on 24 July 2008 at 9:21am will be created in a folder 24072008_092100).

Within that folder should be two files, both with the same date/timestamp format name; one is a .log file (which contains details of what database tables the backup has copied) and the other a .backup file (which contains the database backup).
If those files and folders do not exist, the database backup has not succeeded and you will need to remedy this situation in order to be confident that your server can be completely recovered in case of failure.

**Restoring the database**

It’s all very well backing the database up, but if you don’t know how to restore it you’ll still be stuck. As mentioned all through this presentation the idea of the session is to be prepared for a failure rather than acting directly on a failure. Of course if there is a failure you need to act on it and use the documents provided.

This process is documented but as it is new, as far as seminar sessions go, it’s worth going through the process of restoring it.

1. Copy the folder “D:\RMNetwork\RMManage\RMDatabases\Backup” to a temporary location, i.e. d:\temp\backup.

2. Reset the password of DATABASESERVICE user. The DATABASESERVICE user password is set to Change_Me at installation and must be set to this for the restore to be successful. This can be verified by logging on to the server using DATABASESERVICE user with the password Change_Me.

3. Log off the server if logged on. Log on as an administrator.


5. Expand the Domain node and select the Users node.

6. Click on the user DATABASESERVICE from the right pane.

7. Right-click on the user and select Reset Password from the drop-down menu.

8. Enter the new password **Change_Me**. Click OK to reset the password.


10. Stop the RM Service Host service if it is started, stop the Connection Pool Services if it exists and it is started and stop the RMConnect PostgreSQL service if it is started.

11. Uninstall the ‘PostgreSQL 8.3’ from Add/Remove programs in the Control Panel.

12. Completely delete (including from the recycling bin) the folder “D:\RMNetwork\RMManage\RMDatabases” from the server.

13. Install the CC4 database by clicking on the executable RMDatabaseServer.exe. This is located in D:\RMNetwork\Server\Utilities\RMDatabaseServer\vn.nn.n.n (where vn.nn.n.n represents the version of the installer – Choose the highest version).
14. Verify the database installation by checking under task manager that there are no entries for RMdatabaseServer.exe in the processes tab. The installation of this database will take about five minutes.

15. Start the RM PostgresSS component.

16. Start the executable present in the location
   D:\RMNetwork\Server\Utilities\RM PostgresSS\<version>\ssService.exe.

17. Please wait for the service RMConnectPostgreSQL to start (this normally takes about two minutes).

18. Verify the database installation by checking under task manager that there are no entries for the ssService.exe in the processes tab.

19. Restoration of the previous backup.

20. Open a command prompt.

21. Invoke the executable C:\Program Files\RM\Connect\DB Maintenance\RM.Networks.Comms.DBMaintenance.PGDBRestore.exe with the path of backup as the only parameter (e.g. : C:\Program Files\RM\Connect\DB Maintenance\RM.Networks.Comms.DBMaintenance.PGDBRestore.exe “G:\Backup\31122007_221015\31122007_221015.backup” ) . A return status of 0 and 1 indicates success and failure respectively.

22. Check the need for a database upgrade by checking if there is a folder D:\RMNetwork\Server\Utilities\RM DatabaseServerUpgrade.

   If the folder exists then go to step 23

   If the folder does not exist go to step 25

23. Invoke the executable D:\RMNetwork\Server\Utilities\RM DatabaseServerUpgrade\vn.n.n.n\RMDatabaseServerUpgrade.exe. If more than one folder exists with vn.n.n format, choose the highest version folder.

24. Check if the database upgrade is complete by verifying the entry for RMDatabaseServerUpgrade.exe under the task manager processes tab. If there are no entries in the task manager then the database installation is completed.

25. Reset the DATABASESERVICE user password to a strong one that is agreed with the site administrator: Click on Start, Control Panel, Administrative Tools, ‘Active Directory Users and Computers’

26. Expand the Domain’ node and select the Users node.

27. Click on the user DATABASESERVICE from the right pane.

28. Right-click on the user and select Reset Password from the drop down menu.
29. Enter the new strong password. Click OK to reset the password.


31. Update the “log on” information for RMConnect PostgreSQL database Service service:
   Click on Start, Control Panel, Administrative Tools, Services.

32. Click on Properties for the RMConnect PostgreSQL Server service.

33. Click on the Log On tab and update password for the DATABASESERVICE user. Click Apply.

34. If the DATABASESERVICE user password was reset, the Service Host user password within the database must also be reset – contact TSG.

35. Restart the following services
   - RM Service Host
   - RM Connection pool
   - RMConnect PostSQL

36. After the server recovery has been completed, restart all computers and servers in the CC4 network. The restore log files are saved at:
    D:\RMNetwork\RMManage\LogFiles\DBMaintenanceJobTOC.html
Virtual networks and power outage

While a network failure is relatively unlikely there is always the possibility of a power outage. If you are unlucky enough to have your virtual network drop off due to the power going then it’s important to know what to do.

Starting everything up and hoping for the best is not the best way to approach the situation. If everything stays off when the power comes back then it’s a simple case of making sure everything is started up in the right order. If the power fails and the some of the network switches on, other parts don’t then you’ll need to do some checks. Here are the processes we suggest you follow.

**Manual startup**

Assuming the power has been restored and all your devices are still powered off, you should turn devices back on in this order:

1. SAN switches and core network switches.
   Wait five minutes for initialization.
2. SAN (and any additional disk shelves if they have separate power).
   Wait five minutes for initialization.
3. VMware hosts
   Wait five minutes for initialization.
VMware virtual machine check

Your VMware environment should be configured so that your virtual Domain Controllers will come on automatically when the host is brought back online. You can check this by pinging their IP address from any network computer. If the DCs respond to pings then continue to power on any other physical servers. Once you have confirmed that all servers are up and their services have started successfully, you can instruct users to power on their computers and resume as normal.

If your virtual DCs do not respond to pings even though the VMware hosts have been powered on, run through the following steps:

1. From a network computer, run the vSphere Client and connect to one of the VMware hosts by IP address using the username root and its password. If you don’t have a computer available with the vSphere Client installed, run Internet Explorer, browse to the IP address of the VMware Host and install the vSphere Client from the link on the page.
2. Find the virtual DC, right-click it and choose Power On. Check progress of its boot using the Console tab.
3. Once it has booted to a CTRL+ALT+DEL screen, power on your virtual VCenter server in the same way.
4. Once this is up you can terminal to the vCenter server and run the vSphere Client in your usual way, connecting to the vCenter Server.
5. From vCenter you can then power on the other DCs and CC3/4 servers.
6. Then power on your other virtual and physical servers.

Automatic startup

If some or all of your devices have powered back on automatically, from a network computer, check you can ping the following:

1. Each VMware Host IP address.
   If they do not respond, check they have booted correctly at the console and reboot if required
2. Your vCenter Server.
   If it does not respond, use the process above (if virtual) or check it is powered on (if physical).
3. Your primary Domain Controller (CC3 FRDC, CC4 FRDC or, in a CC4 Matrix network, Windows 2008 DC).
   If it does not respond, use the process above to connect to your vCenter Server and power it on.
4. In a CC4 Matrix network, your CC4 First Server.
   If it does not respond, connect to the vCenter Server as above and power it on or reboot.
5. Other servers.

Then connect to your vCenter Server and check all your devices and datastores are available. If any virtual machines are shown offline and/or in italics, their host may be offline and/or their target SAN may be offline or not detected. Try the following steps as appropriate until the issue is resolved:
1. If a host is shown offline and/or in italics, right-click it and choose Connect. It will take a minute or two to reconnect at which point the VMs on it should come back online too.
2. With the Host selected, choose the Configuration tab, click Storage Adapters and click Rescan. In under a minute the ‘missing’ volumes should be detected and the relevant ‘unavailable’ VMs should become available again and can be started.
3. If that doesn’t work, check the SAN & SAN switches are up and retry step 2.
4. If necessary, power everything down and start again using the Manual Startup approach above.
Things to add to the DR pack

- Photos of switch cabling – labelled
- Location of switch backup – and how to restore
- Information of server \ SAN configuration
- Power outage procedure
- USB Floppy drive
- Pack of floppy disks
- Complete change log

Things to add to the DR pack

We have covered areas where new developments been made in educational networks these days. And while much of the message is, we try to keep processes as similar as possible therefore you shouldn’t have to worry too much; the truth is there are some extras that need to be taken into consideration.

We talked about taking photographs of the switches on the SAN, this should include your core switches too. All switches might be excessive. I ran a presentation a few rounds ago called Ultimate Ninja talking about network monitoring, network mapping and logging issues. One of the concepts I used there was the big red bus theory. Where if on the way to work a big red bus were to put you out of action, how would the network be looked after? It is your responsibility to make sure that the network can be run, and recovered by someone else without your help.

Backing up switch configuration is fairly straight forward and we covered it during David’s ‘Switching Continued’ session last round. Using HP Procurve Manager is one way (where you can find the procedure in David’s notes on the Knowledge Library). If you don’t have this software the manufacturer’s website should have documentation on how to back it up and restore it. Don’t forget to leave a clear document on how to restore this information as well.
Information showing the server\SAN configuration can be found on vSphere under the mapping tab. This is good to have printed off (don’t forget if there is a failure you may not have access to the same information) and add it to the DR pack.

The power outage procedure, as written in these notes, outlines things to check and do if the power has gone causing everything or some things to power down. This should be printed and stored with the DR pack.

Add if USB floppy drive and a set of floppy disks, some VM machines don’t like the server recovery CDs, in this case you’ll need to create a floppy disk to get the virtual servers recovered. The drives aren’t hard to come by but disks can be so it’s worth having a pack of these for emergencies. Many manufacturers have stopped making them these days.

Keep a change log with the DR pack too. If anything has been changed with the network since initial installation, make sure you have that noted down. Once the network is restored someone can go through and make each change without having to guess or deal with issues related to changes not being made.
Three things

We’ve looked at what you need to update in your DR pack and plan, how to plan for a server recovery. As ever there are lots of details within the presentation and notes, therefore I have picked three things I hope for you to glean from this presentation.

Review your plan and pack

Having been through the backup plan and looked at the pack as well, it’s easy to see when 12 months have rolled by it would be worth revisiting this to make sure you have everything you need and all is up to date. Once every 12 months is the longest you should leave it. If you can find the time to do it more regularly then do so.

Virtual servers = normal servers

Something I know our technical leads are trying to get across to everyone is to think of the virtual servers as normal servers. Essentially they are no different so the process of bringing a virtual server back to life is no different from bringing a normal server back to life. Making sure you know what’s wrong will help considerably but keep your thinking clear, just remember the virtual server is the same as a normal server.
Be prepared

Being prepared is more than just saying you know how stuff goes together and having a decent backup. It’s about knowing exactly how that day will pan out. What needs to be restored first, and in order for that to work what needs to be up and running before that? Who is going to do which job? Do they have the information they need to do it? How does the school continue without certain systems?
If you can run a drill and test the plan out every now and then it will certainly help should anything untoward ever happen.

Hopefully this will never happen to you, but whether it does or doesn’t you should be implementing these safety measures. We don’t think twice about fire doors and fire extinguishers these days, they’re everywhere. It wasn’t always like that. As a school shouldn’t be allowed to be open without proper fire safety precautions a network should not be allowed to run without a proper disaster and server recovery plan.