Disaster Prevention and Recovery Plan

for Windows Based Networks

by Jeff Kendrick, Personal Computer Support

1. Prevention

A. Daily tape backups
B. Monthly Automated System Restore (ASR) or Windows 2008 backups and updates
C. Alternate computer ready to take the place of the server
D. Data recovery and server replacement plans in place
E: Anti-virus software

2. Implementation

A. Data recovery plan
    1. Procedure for tape restore
    2. Procedure for Shadow backup restore
B. Server replacement plan
    1. Procedure for stand-in server installation
    2. Procedure for software installation ranked by importance
    3. Procedure for internet connectivity and email restoration
    4. ASR or Windows 2008 backup restore and deployment of normal server
    5. Synchronization of data created / modified during server down time

Daily Tape Backups

The most common and basic tape backup routine involves rotating nine tapes according to the following schedule:

Monday, Tuesday, Wednesday, Thursday tapes are used week after week in order.
Friday tapes are rotated in a five week schedule: Friday-1 through Friday-5

This schedule allows the company to restore files created up to five weeks before by using the Friday tapes and any day of the preceding four weekdays by using the Monday - Thursday tapes.

Companies may choose to include month-end and year-end backups and keep these tapes separate in order to restore data not accessed very recently. It is important to keep a recent backup off site in case of a fire that destroys the computing equipment AND the backups.

The restore procedure is significantly enhanced by keeping a log that tells the status of each nightly backup. By referring to a log, the most recent "good" backup can be determined quickly. Without a log, the restore process can take a good deal more time as individual tapes may have to be examined to see what they contain.

The cost of tape cartridges is often the deciding factor in the decision not to use a tape rotation schedule. This cost can be significant depending on the type of cartridge. SDLT type cartridges are much more expensive than

DAT type cartridges. SDLT devices can backup large amounts of data fairly quickly. However you may not need to backup more than 80 GB a DAT drive will do well then. A complete solution of a DAT 160 drive, tapes and software can be done for as little as $1700.00. SDLT drive can cost over $2500 by themselves.

The cost of quality backup software is also often a factor in decisions made not to purchase this type of software and use a less expensive, "workstation" rather than "server" software. The difference is in the dependability of the backup and restore process. Server based software will cost up to $500 more than workstation based software which will cost around $50. The decision to use workstation based software will result in backups that are hard to restore and that don't include key components like SQL databases or Microsoft Exchange data. If the Microsoft Exchange data is not backed up and the drives have crashed, there may be no restoring.

Automated System Restore (ASR) in Windows 2003 and XP

ASR was a new feature that appeared in Windows XP and is also in Windows 2003 based server operating systems. This software application makes a complete backup of the computer it is run on and makes a floppy diskette that is used to start it in the event that an automated system restoration is necessary.

This is different than a tape backup of the entire system because to be able to restore the tape backup, the system has to exist first. The ASR process is meant to be used to restore an image of the system from the point of installation of the operating system in the event of a hard drive crash or Windows corruption. After the ASR is accomplished, a restore from the most recent tape backup will bring the system data back to the point of the backup.

An ASR can only restore the image of the system back to the state the system was in when the ASR image was created. Therefore an ASR backup has to be run from time to time to include elements that have changed since the last ASR backup. Examples of this are new software that has been installed, users that have been added, shared drives, operating system updates, etc.

The ASR backup image should be made and kept on a drive separate from the normal drives on the workstation or server. This is because a hard drive crash or corruption will take the ASR image down with it and an ASR will not be possible. A portable USB hard drive can do the job a reasonable price. In addition, it must be kept in mind that an ASR image is as large as the system it is made of. Therefore if you have 30 GB of system files and data, the ASR image will be at least 30 GB.

Windows 2008 Backup and restore

The ASR backup and restore feature in Windows 2003 Servers has been replaced with a general system backup and restore in Windows 2008 servers. The same principal of keeping a current backup done applies so that when it comes time for a system recovery, the data used for the recovery will recreate your server as it was recently rather than two years ago. Keep in mind that the backup includes all the user information for your entire network, all the email data, and all the network shares that hold your everyday data.

Alternate computer to take the place of the Server

In the event of a server crash that will take a significant time to replace the failed components, it may be important to

have a computer that can stand in for the failed server until that system can be brought back on line. An example of this is if you use SQL based software that is server based, the data from that software will not be available from a tape restore to another system. The server based software would have to be reinstalled and then the restore made to the system and then the data would be back on-line.

Therefore, it is necessary to decide in advance of the crisis which computer would be designated the server stand in and appropriate software should be preloaded on this machine to speed up the process of getting the data back on line. It may be wise to provide an extra computer in your system for this purpose. The system would also be available to replace failed workstations temporarily.

Anti-virus Software

Without anti-virus software on your server and workstations, there is no data security and the task of repairing damage of any kind is complicated by the element of possible active viruses.

Data recovery and server replacement plans

While agreement in principal with these concepts will promote a better understanding about what needs to be done in a crisis, actual step by step procedures need to be in place so that everyone knows what is expected and when to expect the next step to occur.

Recovery from a failed server is a stressful experience and having a detailed plan can relieve some of this stress and make the process happen faster.

Data Recovery Plan

Procedure for Tape restore

This procedure varies among software types, but the essential elements are the same.

1. The correct tape containing the most recent version of the files to be restored is determined.
2. The tape is inserted into the backup device and the tape backup software is started, the restore function is selected.
3. The user typically sees two columns of data. On the left is a drive and folder selection and on the right, a description of the contents of the left side selected folder or file.
4. The user opens drives and folders on the left side by clicking on the plus sign in front of a folder or drive. This displays the contents on the right side.
5. The appropriate folder or file is selected by placing a check mark in the box next to it by clicking once on the box.

6. When the selections are made, the user must check to determine if the options are set to overwrite the existing files on the drive. Often the default is to not overwrite, resulting in no files being restored.
7. Click the appropriate start function to begin the restore. When the restore is finished, remove the tape to avoid having the nightly backup overwrite the data on this tape.

Procedure for Shadow Copy Restore

For Shadow Copy Restore to work the workstation must be running Windows 7, Vista, XP, 2000, or 98 (not NT 4 or ME) and the Windows server must be at least version 2003. In addition, the services for shadow copy must be enabled on the Server and the workstation client for Shadow Restore be installed.

In the event that these requirements are met, the network users are able to restore previous copies of files by using the Windows Explorer to find the file in question and by right clicking on it and viewing the Properties, the Previous versions tab identifies the versions of the file that are available to be restored. These versions can either be restored or copied and pasted elsewhere.

Server Replacement Plan

Stand-in Server installation

In order to speed up the process of restoring access to important data and services, when a file server is out of service, an alternate computer can be utilized to stand in for the server until the server is ready to be put back on line. The alternate server computer designate should be of similar technology as the original server. It should have the ability to have extra drives added to it by having a case large enough (not a small footprint desktop computer). It should be able to support the type of removable storage that the restored data is available on. We recommend USB v.2 ports. In addition, the operating system should be able to support the drives used on the server (NTFS, SATA or SCSI) in case the actual server drives are directly installed.

This computer should have the necessary server side software pre-installed if possible to accelerate the process of getting it up and running.

Software installation by importance.

It is important to recognize that the IT support team you are working with may be familiar with your computers and network and perhaps your software, but they probably do not know how much you rely on certain pieces of software to get your work done. For that reason, a list of software ranked by importance to your company should be created so that in the recovery from a disaster or server crash, the support team can focus on the software and data that need to be accessed the most.

Internet and email connectivity

In the disaster recovery, the ability for the company employees to access their email may be high on the list of important software. If so, it may be that the email itself is being stored on the downed server in Microsoft Exchange email databases. To enable users that rely on Outlook and Exchange to have access to their email folders while the server is down, folder synchronization must be implemented prior to the crisis. Having this enabled means the users computers will have a copy of their email folders and will only perhaps need an internet service for email access to be installed to continue their communications. It is important to note that Outlook users may be without their contacts list and other email folders until the server itself is put back on-line. Outlook Express users will not be affected in the same way. The problem with Outlook Express is that the email database is almost NEVER backed up because it is kept in a hard to find location on the users workstation rather than on the server so it can be included in the daily tape backup.

The internet connection itself may need some attention, but if the system utilizes a router to provide internet connectivity to the network users, then the system may continue to function without the server.

ASR or Server 2008 system restore of the downed server requires that the failed components be replaced and the server be in condition to have the operating system reinstalled if necessary. It can take up to eight hours for the ASR or Server 2008 system backup to restore the system and data files, perhaps longer if the system is large. If there is no ASR or Windows 2008 backup, then the server software must be reinstalled and the backup software reinstalled and then the latest backup can be restored to get the data recovered. At this point, the users and other system configured functions must be redone. This can take up to16 hours.

Finally, when the server is back on-line and the users are reconnected to it, there is the issue of synchronizing the data that was either created or modified in the time the server was off-line. Generally, this can be accomplished by copying the files to the server using the date stamp as criteria. This identifies all the files that were created or modified recently. The other option is to simply copy the data from the stand-in server back to the server itself. This is the same as a data restore from tape backup and may be considered as an alternative. It can take up to four hours or longer, but can be faster than tape restore.

The general recommendations are:

* Have an external hard drive that contains the ASR or Windows 2008 backup
  1 TB hard external hard drives cost about $185 installed
* Have a server based backup software like Symantec Backup Exec for Windows Servers.
  Backup Exec for Windows Servers costs about $650.00 installed, however, SQL and Exhange agents can drive the cost up to double that.
* Have a high speed, high capacity tape backup device with inexpensive data cartridges like a Quantum LTO3 device and have a tape rotation schedule that is adhered to religiously. Keep a log.
  Quantum LTO3 400GB internal SQSI tape drive is $2500 installed. Tapes are $45 each.
  Quantum DAT 160 drives only hold 80 GB of compressed data, but the cost is about half the LTO3 drive
* Have an alternate computer designated to be used as a stand-in server.
  This has to be a good computer - no use trying to use an old one that has been sitting around.
* Do an ASR or Windows 2008 server backup for disaster recovery on a monthly basis.
  This isn't intended to replace daily backups . Takes about an hour to do it.
* Make sure the Outlook email clients are synchronizing their folders with the server.
  Versions of Outlook have different settings, but look for the Offline status in properties of the folders. Outlook Express does not syncronize and by default keeps the folders on the local computer.
* Keep predefined procedures on hand for disaster recovery.
  This is not hard.
* Keep recent backups off site.
  What if your building burned down? Just take one home with you on Fridays at least.
* Keep a current list of network users and their passwords and email accounts and passwords.
  A password list should be kept confidential until needed by an administrator.
* Make sure you have the Server administrative password.
  You should know this in case a Microsoft or other support technician gets involved.
* Make sure your anti-virus software is made by a well known vendor and is up-to-date.
  McAfee and Symantec are good sources. The corporate versions can be estimated to cost up between $25 and $45 per workstation depending on the licensing version.