

How good are your DR backups?

Contributed by Gareth Eagar
Tuesday, 08 August 2006
Last Updated Friday, 01 December 2006

Here are some questions to ask yourself regarding your backups to see if you really are prepared to use them for disaster recovery.

When preparing your IT systems for disaster recovery, your backups are obviously a central and critical component (unless of course you have replicated disk off-site, but even then you should probably still be taking local backups). Here are some questions to ask yourself regarding your backups to see if you really are prepared to use them for disaster recovery.

What is being backed up?

In Disaster Recovery testing I've come across more customers than you'd think that have only found out during their recovery testing that they are not backing up some critical directory or file. One customer found that the backup of an important database had been deselected around 4 months ago, yet nobody knew who had done it or why - all they knew was that they needed that database for the application they were recovering.

Another customer backed up most of the system but not their Anti-Virus software installation directory. When performing recovery of their Exchange server, they started getting a lot of strange error messages when trying to start Exchange. After a lot of searching, we found that a registry setting was telling Exchange to interface with their Anti-Virus software and yet the Anti-Virus software had not been restored so Exchange was failing.

I strongly recommend that the full system gets backed-up, rather than selecting a sub-set of directories and files. Firstly, if you have a disk failure that requires you to restore the system (hopefully you'd have mirrored or RAID disks and not need to restore just because of a single disk failure) then you'll want a full backup. Also, once you start selecting only certain directories or files, you can easily get into the situation where new software is installed and nobody gets around to adding it to the backup software selection.

If you go for the option of selecting only specific directories for backup, then ensure that your change control process has a section for reviewing potential requirements to change what is backed up and do a review of what gets backed up every 4 - 6 weeks. IE, when a new application is installed, the change control process should pick up that directories related to the new application need to be added to the backup list.

Are you backing up the backup software catalogs/database?

The catalog/database of your backup software keeps track of what data is backed up and on what tape the data resides. Depending on what backup software you use, there may be an easy way to backup and restore the catalog or database of your backup application.

When you go off-site to recover, you will reinstall the backup software and will then either need to scan your tapes so the backup software can rebuild its catalog or you will need to restore the catalog from tape.

The enterprise products (such as IBM's Tivoli Storage Manager or the Symantec/Veritas NetBackup products) generally enable you to make a backup of the catalog/database. When you go off-site, it's quick and easy to restore this database and then start doing your data restores.

Some of the more entry-level products don't provide an easy way to backup and restore the catalogs (such as the Symantec/Veritas BackupExec application). In this case, you need to get the software to scan all of the tapes that you need to use off-site. Most products need to read through the entire tape to build the catalog for that tape and this can be a long and time consuming process, depending on how many tapes you are using, how many tape drives you have available off-site and what tape technology you are using.

If your product supports backup and restore of the catalog/database, make sure that you are backing up the catalog/db on a regular basis, that the tape with the catalog is sent off-site with the data tapes and that you can easily identify which tape has the catalog backup. And then make sure that you know how to restore the catalog. Take a system in your test lab, install the backup software on it and then attempt to restore the catalog.

HINT / TIP: Once you have restored the catalog/database, you may find that this will have also restored the device configuration that your backup software uses to interface with your backup media. If you are recovering off-site to a different model/size library, you may need to delete the device definitions and then reconfigure your backup software for the off-site recovery equipment. On some software (such as IBM's TSM) for certain types of libraries, even if you recover to the same model you will still need to delete and reconfigure the library in TSM as there is some very device specific information in the configuration.

If you are using a product that does not make backing up and restoring the catalogs easy via default functionality, you need to be aware of the time that it may take to scan all the tapes when performing off-site recovery. If you only have a few tapes with modern tape technology, this may take well less than an hour. If you have a relatively large number of tapes and older technology (such as some of the old DLT drives) then this could take you quite a long time.

I recently had a customer that took nearly 8 hours to scan all their tapes. However they only had a single drive on the recovery site and they were using old tape technology. They have now found a way to backup the Backup Exec catalog files to tape and are able to restore the catalog rather than rebuild it at the recovery site. Your application may not provide an automatic way to backup the catalogs, but with a bit of research you may find that it can be done.

Are you using an open-file plugin and other necessary plugins?

If you need to recover the full system (and not just portions of data) you need to ensure that your backup software supports backup of open files. Most applications have a plugin that you need to purchase/license in order to enable backup of files that are in use while the system is backed up.

If you have Windows 2003 and your backup software interfaces with Microsoft's VSS (Volume Shadow Copy Service) then open files can be backed up. Even the backup software included with the Windows 2003 OS can backup open files using VSS (see this TechNet article).

Most "on-line" applications such as databases, e-mail servers, etc will also require a special plug-in specific to your backup software to enable these applications to be backed up and restored cleanly (this is required on both UNIX and Windows servers).

Make sure you are using the correct plug-ins in production and ensure that you are able to reinstall (and license) these plugins at your recovery site.

Who is checking the backup logs?

You may think this is obvious, but too often the backup logs are not checked properly and problems causing backups to fail are not corrected.

Ideally the backup log should be emailed to a group email address every morning and one person should have the responsibility of checking the log for errors. A good idea is to have a roster so that a different person checks the logs each week, although a full team gets the logs via the group email address. Once the person on duty has checked the logs, they should send an email to the rest of the group confirming that there are no problems.

Often a single person is tasked with checking the logs and when they are off sick or on leave, nobody else bothers to check the logs. If the logs get automatically emailed to a group of people and the group knows to expect a confirmation email that the logs have been reviewed with no problems found, then there is a better chance that someone else will check the logs if the person on duty is away for some reason.

Are you backing up the install CD's?

Depending on your recovery method, you may need to reinstall software when doing off-site recovery (this includes installation of patches and service packs).

I have seen a lot of companies go to their DR site with a "battle box" filled with installation CD's, but they are still not able to find the correct version or all the disks for the application they need. It is very difficult to manage the process of copying the installation CD and sending it off-site every time a new application or version is installed on a system.

It is therefore highly recommended that you have a process that copies the installation CD of any software installed on your servers to a share / NFS mount on your network. This must then be backed up regularly and you need to ensure you have sufficient disk space to restore this share during an off-site recovery event.

It is much easier to restore the share and then install over the network rather than looking for copies of install CD's and hoping they aren't scratched or in some other way corrupt.

For this to work though, you need to ensure that the policy/process for copying any new software or version to a network point is strictly enforced. Your change control process should identify anything that is to be installed on your systems and as part of the change control approval, the installer must be instructed to copy the install files to the network share.

The Obvious

In conclusion, the following are some of the more obvious things that you should also keep in mind with regards to your backups.

- Recycle tapes according to the manufactures instructions
- Keep the backups off-site
- Keep a copy of the backup software (and patches) off-site
- Do regular system backups such as a mksysb or creation of an Ignite image [for UNIX systems]