JDEtips Journal November/December 2007 Volume VIII Issue 6

JDEtips On Data Archiving and Disaster Recovery

Backup Considerations for Your JDE® System i Data

By Jeff Babcock

Editor's Note: *Lost data. Just say the phrase and thoughts of hours, days, even years of invaluable work just vanishing are conjured up. It's enough to want to scream: GET ME SOME BACKUP! Fortunately, there is a multitude of options out there, all at varying costs and prices. But Jeff Babcock has a few tricks up his sleeve that will help you keep data safe and secure by just using what you already have available in your current system—and all it costs is a little time and space—disk space that is!*

As IT professionals, we are tasked with safeguarding the company's information from harm. Threats to the integrity of our company's data can come from many different sources. In addition to mechanical problems, environmental issues, or software bugs, your data is most at risk to accidental or intentional deletion and modification. The purpose of this article is to provide you with some tools to better protect your data proactively, as well as enable you to launch speed recovery when things go bad. You have thought about things going bad, haven't you?

My examples are written in IBM's CL programming language, which is used extensively in JD Edwards® World® to run its programs and reports, as well as to perform numerous housekeeping functions. CL language is much like Microsoft's DOS Batch or Window's scripting language because it can perform basic logic decisions and automate essential, but tedious, tasks such as running backup commands or initializing tapes. And as we all know, the more tedious a task is, the more likely it is to be put off till later or not performed at all. The techniques discussed in this article were developed for JDE World A7.3. The CL programs should work for any files on a System i platform running operating system V4R3 or higher.

Risk Assessment

The first thing you must do is to perform a risk assessment. This sounds complex, but it really just means figuring out what is most important to you and how likely is it to get messed up. This is the basis for disaster plans, insurance planning, and many other activities. This risk assessment is essential because we all have limited resources (time, money, personnel) to protect our information systems. We are called to perform many different activities in IT such as training, purchasing hardware and software, application development, and pulling little bits of paper out of printers when they jam up. All of these activities are important; however we must not neglect our most important responsibilities: the backup and the successful recovery of our company's information.

Backup

With our new or fresh look at what data is important to our company, we can begin to plan how to protect it. I know we all perform backups; you could not face yourself in the mirror each morning if you did not have some kind of backup system in place. But look at your backup procedures in light of your current risk assessment and ask yourself the following questions:

- Am I backing up everything that is important?
- Have I recently tested my data restore?
- Are the backups of my data being taken off-site in case of fire, flood, etc.?
- Is the recovery time required to bring my data back onto the system acceptable?
- Is the loss of data between the times of my last backup and now OK?
- How difficult would it be (and is it even possible) to reconstruct data that is lost?

The answers to these questions and the resources at your disposal will help determine your backup procedures. For example, I run a daily backup of my production libraries using a revolving set of 21 tapes. They are labeled with the day of the week (SUN, MON, TUE, etc.) and the set A, B or C. This gives me a three week window of opportunity to restore data if required. I also pull and replace the tape used on the last day of the month and move it to long term storage. This allows me to restore back to any previous month in a test environment, if required. Remember: Tapes are cheap

compared to the cost of recreating lost data. There are many options to safeguard your data. Here are some of the choices available:

- Tape backup
- Virtual Tape Libraries
- Disk-based backup
- High Availability Systems
- Journaling
- FTP

The choices vary in cost and complexity. Your options include everything from high availability solutions (these mirror every change on one system to a secondary off-site system that can take over should something happen to the primary—and cost a pretty penny, too) to the use of built-in operating system utilities that will make backup copies of your critical files. At a minimum, I would suggest the following requirements of whatever option you choose:

- The level of data protection provided must agree with your business requirements.
- The time it takes to restore lost data should be known and approved by management.
- Make sure that all qualified staff in the IT department know how to perform the recovery procedures.
- The window of time required to perform your backups when all users are off the system must be made available.

This article is not going to focus on expensive high availability solutions which work really well (and make me envious at trade shows). Nor will I discuss the merits of a tape-based system as compared to a disk-to-disk solution. Instead I will focus on the "cheaper chicken" solutions of using built-in operating system utilities. Let me further clarify that nothing beats a good "GO SAVE" option 21 to back up everything on your system. It is, however, a real inconvenient truth that users don't want to get off the system to allow you to make a backup.

An IT professional who has a high availability system in place may smile at those of us who do not have one, but consider this: if a user deletes a record or file and decides to go to lunch or have a coffee break before telling you (if they tell you), will not the same change be cheerfully carried out by the HA software on the backup system?

Yes, I know we have journaling and can roll back some changes if the file is set up to do so. Still, are all of your data files protected? Allow me to show you some simple procedures that can be put in place to protect information that is most vulnerable to accidental destruction. And, the best part? It will not cost you anything besides a little time and disk space.

Example

Let's begin with how I created a CL program to copy an Accounts Payable work file that is used for ACH transfers. The work file is cleared each time a payment group is created. The steps the A/P clerk takes when processing ACH payments are:

1. Enter vouchers
2. Create a payment group
3. Print checks or create ACH file
4. Transfer ACH file to PC for processing
5. Post transactions to G/L

If the transfer ACH file step was skipped and the clerk moved on to process other payment groups, the ACH data is lost. To protect the ACH data, I included a menu option to back up the data as one of the processing steps. An example of how to call a CL program from a JDE menu is shown in Figure 1. The corresponding CL program to back up the ACH file is shown in Figure 2. This CL program needed to meet certain goals: I wanted to keep a history of ACH files for six months should we ever need them, and I did not want to have to manually delete the old files after their retention date. The CL begins by finding the current system date and creates names for the files it will be copying in the format of A2MMDDHHMM and A3MMDDHHMM. For example, if today is 11/28/07 at 10:07am, then the file names would be A211281007 and A311281007. By imbedding the date into the filenames, I can perform the housekeeping later to delete the files older then six months. The IF statements in the program perform a rolling deletion of the older files. For example, if the current month is 01, then delete any backup files created in month 07; if it is month 12, delete backup files from month 06, etc. You could modify this CL to handle other files by changing the hard coded filenames.