



Choosing a Backup Approach when using Unisys ClearPath

Baseline Data Services works with individual customers to identify best course of action

With the increasing complexity of technology, companies find it challenging to choose a specific disaster recovery (DR) backup approach. However, for companies using Unisys ClearPath, Baseline Data Services makes it simple.

A company with critical IT operations should use modern technology to rebuild its DR plan, because it allows for data protection of the entire system; elimination/reduction of human interaction; backup of .ASD, .PCD and encryption keys; data replication; offsite data storage; and strong encryption and testing plans.

ClearPath is a virtual machine that runs on top of a qualified Windows server. The ClearPath portion of this system is essentially a virtual machine, very similar in characteristics to a VMware machine. Windows hosts the .ASD files, which are virtual hard drive partitions for the MCP portion of the ClearPath to run. Because of the duality of the ClearPath, companies are presented with multiple paths to building a backup plan.

A client must first consider the following questions. "Where will you be restoring the data in the event of a disaster? Will you be restoring to a pre-built ClearPath that is already running ITI application programs, or will you be restoring a bare metal ClearPath?" Depending on the answers, the approach a company must take to achieve a reliable backup solution will vary.

Generally, companies do not run or manage their own secondary ClearPath. This is usually due to the size and expense of running a secondary mainframe. In the event of a disaster, a company will likely be restoring to a ClearPath that doesn't have their information preloaded. In this instance, it's important that the bank's backup solution capture all needed data files to allow for a successful DR process.

For years now, the main method of data backup for ClearPath companies has been tape based solutions. The theory taken by the core processing provider has been a modular backup approach. However, as time has gone on, many companies have grown in complexity of core processing and have begun to realize the need for more advanced and robust backup solutions. These solutions include broader tape based backup and disk-to-disk backups.

With the modular backup approach, a bank will perform application specific backups throughout a processing day, followed by "pre" and "post" backups before and after the nightly update. What many companies fail to see is that this is not a complete backup. This backup method doesn't include critically important files such as tape encryption keys, company data files, ITI application programs and COM files. Unfortunately, this method

has been half-heartedly supported by other DR technology-based companies. It's safe to say, that ClearPath customers haven't been properly informed in the operation of the system to properly identify these critically important files.

Another method of tape based solutions that companies are starting to adopt is a "pack" backup approach. This approach focuses on capturing the entire contents of each pack rather than narrowly focusing on application specific data. This method is a broad tape based solution which usually captures most of the missing critical files that the modular based approach misses. However, without a proper backup solution for the tape encryption keys, these tapes would be impossible to read on another system.

Tapes are fragile items. Tapes can be easily lost, stolen and/or damaged. Furthermore, without proper physical rotation and offsite storage, tapes could be part of a disaster, and leave the company reverting to a restore point that is days old. On top of physical concerns regarding tape recovery, another concern is time performance. Tapes are restricted in speed, size and I/O performance. To put it simply, tape recovery can be a time consuming process at a time when time is a very precious commodity.

The biggest potential downfall of any of the tape based solutions is the need for a second mainframe to load these tapes to. In the event that a production mainframe is no longer operational, a bank must be able to take its backup tapes to a secondary mainframe and load those tapes. If a bank is using a modular approach, certain questions need to be asked: Will the secondary mainframe have ITI programs? Will those programs be on the same release level? Will the mainframe have the appropriate tape encryption keys preloaded? How long will the user have to wait for that mainframe? If a bank is using a pack based tape approach, some of these questions are eliminated, but other important questions still remain.

Another popular backup approach is a disk-to-disk solution. This solution helps mitigate the impact of tape based solutions by performing electronic backups. These backups are generally achieved by either capturing the .ASD operating files, or by collecting all of the pack data through UNC shares. This data is then replicated to a secondary storage device. This approach reduces tape dependency, adding several layers of security, all while removing layers of human interaction. The down side to this approach can be a poor "point in time" window. If a ClearPath were to suffer a disaster in the middle of a processing day, and didn't utilize a modular tape approach, the bank would be forced to revert back to their last electronic backup, which is generally after update the night before. Essentially, the bank would be losing an entire day's worth of work.

Baseline Data Services identifies the best backup approach to three practices † use tape encryption, perform entire pack backups with EVault online data protection, and clearly define the goals and objective of the test.

For more information about a backup approach for your organization, or to implement a DR plan, contact Baseline Data Services at 317-707-3941, or visit www.baseline-data.com.