

THE NEW HIGH AVAILABILITY - A NON STOP CONTINUOUS PROCESSING ARCHITECTURE [CPA]

"Trust no future. . . act in the living present!"
-Longfellow

OVERVIEW

Business Continuity Planning, more often called Disaster Recovery Planning, is the number one issue facing corporate management today; yet most organizations are doing little to combat the threat to on-going operations - with only 3% of the organizations showing an increase in their disaster tolerance planning, from 2001 to 2002. This fact, according to our latest focus group findings, begins to show the progress, or lack thereof, since September 11th. At the same time, pressure is mounting from all sides to resolve this issue. Funding for better disaster recovery solutions is being done through off-budget allocation and the cancellation of lower priority projects.

CIOs are getting pressure from company Presidents, CEOs, CFOs and other corporate executives. The item is on the agenda for board meetings, and auditors, trade groups and government watchdog agencies are carefully looking at corporate disaster tolerance plans.

There are three problems with a "Disaster Recovery Plan." First being the word "Disaster." This implies that the only time it is needed is after something very bad happens. Most people do not like to think about, or invest in, the assumption of something bad occurring. Most of us like to invest in growth and improvements. The second problem is the word "Recovery." This implies that whatever you had is gone and you need to get it back. It is very unlikely that you can get your systems back to the same state they were before the disaster. The third problem is the word "Plan." No matter

how much is planned, there are always things that are forgotten. Plans can never replace action.

Top 10 Challenges

1. Disaster Management
2. Security Management
3. Money Management
4. Personnel Management
5. Project Management
6. Network/Internet Management
7. Modernization Management
8. Integration Management
9. Goals Management
10. Vendor Management

The Top Ten Challenges are compiled from the Spring 2002 IT Executive Groups. These groups were held across the United States in five cities during June 2002.

Figure 1.0

Mission Critical Applications: Any application that must be up all the time, and downtime will have an adverse effect on the business. The average length of downtime is 5 minutes, or 99.999% uptime per year.

WHAT IS CPA?

CPA is a new, different, and complete approach to addressing the high-availability and disaster tolerance needs of major organizations. The solution, when fully implemented, covers all systems, people, processes, applications, and data. This contrasts with individual system solutions offered today. While implementing and maintaining a CPA solution takes effort, in comparison to maintaining a disaster recovery or business continuity plan it is fairly straightforward and simple. CPA offers two major features: no failure recovery and up-to-date back-up storage. It also can be less expensive than normal disaster recovery solutions. There are four types of CPA: Application Segmentation, Database Segmentation, Functional Segmentation and Live-Live. All four CPA types work on an event-based theory.

Application Segmentation - Applications are split over multiple resources and databases are linked to the application. For example, the order processing applications and the order database are on System A, while the backup database is on System B. The inventory application is on System B with the primary database. The backup database is on System A. When a user updates the order database, it is done through System A. System A then sends a duplicate transaction to System B, to update its order database. When a user updates the inventory, it is done on System B. System B then sends a duplicate record to System A.

Database Segmentation - Using this approach, the database is split along logical lines. For example, the

order database may be divided in two by customer names A to L on System A and M to Z on System B. When a user updates the order on an A-to-L database, it is done through System A. System A then sends a duplicate transaction to System B, to update its A-to-L segment of the order database. The reverse is true for M to Z. With these methods, the order database is kept up-to-date. In case of disaster on either System A or B, the other takes over.

Functional Segmentation - This is the most popular of the CPA techniques and the easiest to implement. System A is the primary system and acts as the database of record. System A does all the write or update functions. When a user updates the order database, it is done through System A. System A then sends a duplicate transaction to System B. In this method the order database is kept up-to-date. In the case of a disaster on System A, System B takes over the update functions. In the normal course of operations, System B will handle the read function or may act as a Business Intelligence Server.

Live-Live - All applications and data are synchronized. When an update occurs on any available resource, it is automatically propagated to all other resources that back up that type of event in real time. For example, an order is entered on System A, which has a database for orders, inventory, and accounts receivable. System A updates its database and sends a duplicate transac-

tion to System B, which has the orders and inventory database, and to System C, which has the database for accounts receivable. Systems A, B, and C are updated almost simultaneously.

CURRENT ARCHITECTURE

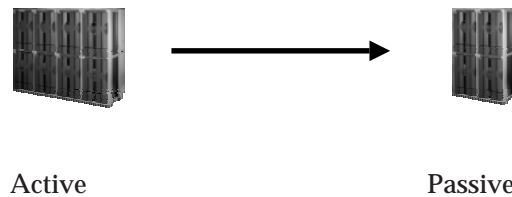


Figure 2.0 Before CPA

The before CPA shows a primary system that is active all the time except during a disaster. The idle secondary system is maintained in case of a disaster and is only active if a disaster occurs.

CPA ARCHITECTURE

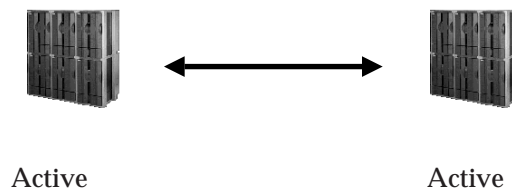


Figure 3.0 After CPA

The after CPA shows two primary systems that are active all the time. They share the processing load. In case of a disaster one of the systems will take over the entire workload.

SURVEY RESULTS

In the spring 2002, The Standish Group conducted a series of interviews with a cross section of HP NonStop Enterprise Server users to gain their impression of the disaster tolerance concept: Continuous Processing Architecture (CPA). A team of interviewers executed 32 sessions, with each session lasting approximately one hour. The average HP NonStop user has 55 mission-critical applications. Fourteen percent (14%) of the HP NonStop user's mission-critical applications are covered under the disaster tolerance umbrella. This is about 40% greater than the non-HP NonStop user. This shows that HP NonStop users have a significantly higher regard for disaster recovery than other users.

This is proven again by the fact that fifty percent (50%) of HP NonStop users tested their disaster recovery solution four or more times a year, compared to only 6% of other users. Sixty-two percent (62%) internally audit their disaster recovery tests and fifty percent (50%) of these use an outside firm.

HP NonStop users rated customer commitment and satisfaction as the top two reasons for implementing both a high availability and disaster recovery solution.

On a scale of 1-to-5, with 5 being the highest level, HP NonStop users rated customer commitment to high availability solutions a 4.8. This is followed by a 4.1 ranking for lost revenue. It could be inferred that companies believe that without availability there would not be as many customers.

In general, HP NonStop users think that this new and different approach, CPA, is in their future. Their consensus is that the current disaster protection plan and service is a limited model, and that CPA is their goal. HP NonStop users gave Live-Live CPA a 4.5 rank, out of a possible 5; compared to an Application Segmentation rank of 3.6, a Database Segmentation rank of 2.7, and a Functional Segmentation rank of 2.3. Eighty-one percent (81%) of HP NonStop users

gave Live-Live CPA a 5 ranking.

HP NonStop users consider money the largest barrier to implementing a CPA. They gave money a high to medium rank of 3.7 out of a possible 5, as a problem in getting CPA introduced into their environment.

Other medium barriers to implementation are people and their skill sets, at a 3.4 ranking. Processes, products, application and data, as barriers, were not major factors. That being said, money and people are the major issues. Here there are trade-offs. Let's look at people first. Most of the effort is in the set-up. Once the CPA is implemented it comes down to system

management to insure that the CPA process is always up-to-date. This is not so in the current thinking of disaster recovery. Every time there is a change in a process, application and/or the IT infrastructure, these changes need to be put into the disaster recovery plan. This takes well-trained and skilled people to manage and, if disaster strikes, to execute properly.

SUMMARY

The vast majority of disaster recovery drills fail because a process was forgotten, files misplaced or an update improperly installed.

Therefore, it takes greater skill and effort to keep a disaster recovery plan up-to-date than to do a one-time CPA implementation. This not only requires trained people, but it also costs money to perform the tasks and test them as well. To do it right is a, forever, on going process. In a CPA environment there are no disaster recovery tests because testing is continuous. Other financial trade-offs are disaster recovery

CPA HUB

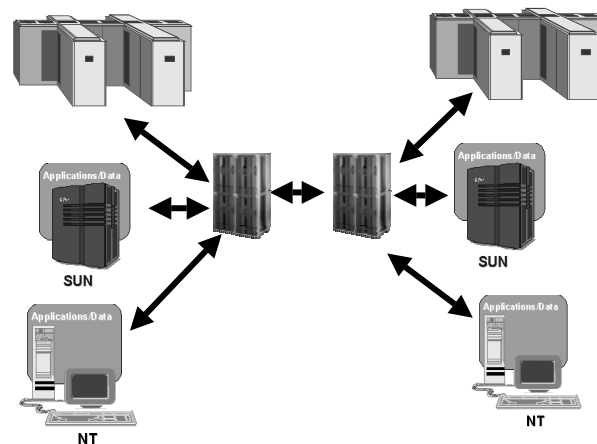


Figure 4.0 - HP NonStop CPA Hub

Create a CPA Hub by using HP NonStop servers with a message system, such as MQSeries. Here other systems can be integrated and replicated to form a real-time solution.

High Availability (HA): For the purpose of this study HA is considered any technology that offers a minimum of three 9s, or better, availability. These technologies include hot or cold standby, fault-resilient, fault-tolerant, or cluster systems.

services, duplicate systems, higher business interruption insurance, and media storage vaulting. CPA is constant action.

Unlike hot or cold standby systems, CPA uses all the resources except for contingent headroom. In fact, CPA can also reduce the unused contingent headroom. Another way it can reduce cost is through reduction in expensive rent, and lower labor costs. Having two active sites in the areas of lower building and labor can significantly reduce expenses. Our research has also shown that breaking up clusters increases availability. Therefore the cost of downtime decreases. Using HP NonStop as a CPA hub, in conjunction with real-time business integration, can add a whole new dimension to the IT infrastructure.

A CPA hub is two systems, one in one site and one in another; each transferring messages back and forth for back up purposes. Each site has resources for the applications being backed up. Using a HP NonStop CPA hub allows other applications, systems and databases to link together through a queuing system. Once in the queuing system one side can send a message to the other side of the hub. The other side then sends it to the back-up system. Each side of the

DISASTER RECOVERY PLANS

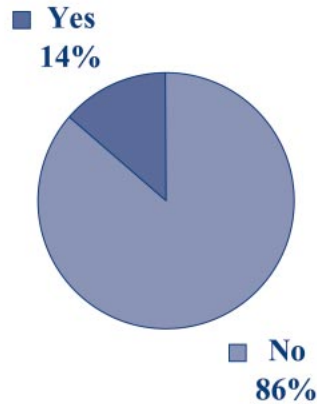


Figure 5.0

HP NonStop system users reported that only 14% of their mission-critical applications are part of a business or disaster recovery plan.

hub can have an Operation Data Store (ODS). The ODS can be used for many purposes, such as CRM, billing, data mining, and other analytic work.

In summary, eighty-eight percent (88%) of mission-critical applications are not on a disaster recovery plan; fifty percent (50%) of mission-critical applications do not operate on a high availability solution. The reason is, planning for disaster recovery is difficult, time consuming, requiring constant management involvement and is only recognized during a disaster. In this

case it could be good or bad exposure. CPA allows for both availability and disaster recovery. Using the CPA approach is a one-time set-up with upgrades including new applications and environmental changes as they occur. It is always up-to-date and always working. CPA is never having to say you are sorry.

Disaster Recovery (DR): For the purpose of this study, DR is considered any technology that provides back-up processing capability in cases of a catastrophic event. These technologies include disaster recovery services and back-up remote sites.



The Standish Group International, Inc. produces research advice based on extensive primary research in the area of mission-critical applications. The Standish Group provides this advice through our continuous information service. This research service studies the requirements for developing, implementing and maintaining mission-critical applications.

**THE
STANDISH
GROUP**