Business Continuity for E-Services : S1 Case Study

Ian Bowdidge MBCI

Hewlett –Packard Limited
Business Recovery Services
HP Services
Nine Mile Ride
Wokingham
Berkshire RG40 3LL
United Kingdom

Telephone +44 (0) 1344 365088

Fax +44 (0) 1344 763753

ian_bowdidge@hp.com

You have just lost your entire IT capability, your business critical processes have stopped. The clock is ticking, your customers are growing frustrated and your down-time costs are mounting – what do you do? How sure are you that you can recover? By when? And what about the data?

Background

Traditionally, companies developed Disaster Recovery Plans to support the recovery of their IT systems in the event of a disaster. Such recoveries involved duplicate hardware and restoring the data from the last "backup" tape, and typically involved downtime of hours or maybe days.

This is no longer acceptable in the "e-services" world where business can only afford downtimes measured in minutes rather than hours or days. Data loss is unacceptable and, with tightly interlinked applications, trying to unravel complex transactions is almost impossible.

So yesterday's Disaster Recovery concept has today evolved via Business Recovery into Business Continuity, which includes all the factors that are critical to a business. Through necessity, recovery timescales of minutes with no data loss have become the norm rather than the exception. A Business Continuity Plan has to exist, be rehearsed and be part of normal business operations.

S1

As a pioneer of Internet banking, and one of today's leading global providers of innovative Internet-based financial services solutions, S1 strongly believes in these business continuity principles. S1 offers a broad range of products and services that empower financial organizations to increase revenue, strengthen customer relationships and gain competitive advantage by meeting the evolving needs of their customers.

In 1999 S1 took the decision to build a European Hosting Services centre in the UK building upon their experience gained from their Hosting businesses in Atlanta, USA and Singapore. The operation was designed with resilience and high availability of systems and infrastructure. However, they wanted to perform a full Business Recovery Rehearsal before the first customer went live.

Early in 2000, S1 chose Hewlett-Packard’s Business Recovery Services as their Business Continuity partner and HP and S1 immediately began working towards that full rehearsal. Hewlett-Packard’s Business Recovery Services have been providing Business Recovery services since 1986 and their global services offering range from traditional fixed and mobile computer and office recovery service’s to virtually non-stop dark site continuity solutions. They also offer a range of consultancy services to support all businesses in their Business Continuity needs.

Both S1 and HP agreed at the outset that the Rehearsal would be videoed in real time, warts and all, both to demonstrate the process and to act as a reference for future improvements. It was also agreed that there would be two primary objectives, namely:

1) Recovery in less than 1 hour
2) Zero data loss

Subsequently, a further objective was added: to ensure that the rehearsal demonstrated a recovery for a real “end user” , the test had to have live users accessing the systems via the Internet.

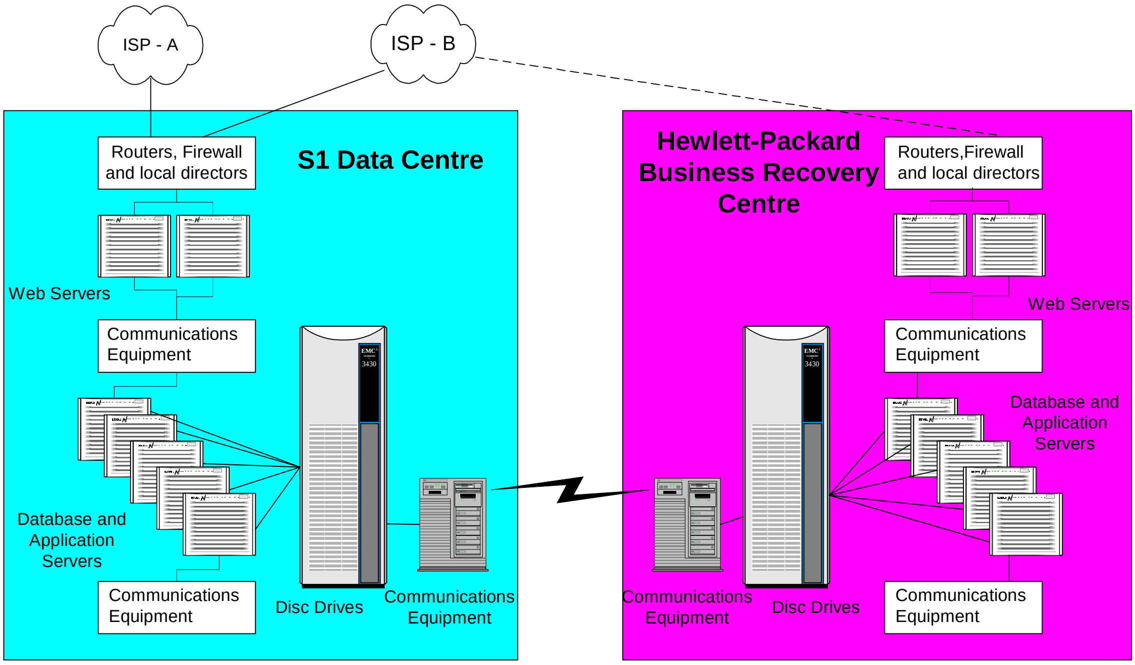
Architecture and design

The optimum architecture to make these objectives achievable consisted of production data being replicated in real time at the remote recovery site, and the recovery computers being available immediately a disaster occurs. However, keeping both sets of computers consistent with web page layout, application software versions and operating system parameter changes could be a lengthy part of the change control process. Being Internet-based, web pages were likely to change frequently, with hopefully infrequent disasters. It was decided, therefore, to maintain all the web pages, application software and operating system on the production disc drives, which are replicated to the recovery site. This would guarantee that the web pages, software and parameters are the same as the production environment in a disaster.

Before the production Hosting Centre was completed, the replication method and recovery process was tested at the recovery centre, initially with the discs side by side, then with the discs at the same site separated by the communication equipment. Return to normality was also tested.

The systems and infrastructure had to be resilient to ensure high availability of S1's service. Accordingly, duplicate servers and routers were built into the design to cater for individual component failure and to ensure, as far as possible, that the Recovery Service would not need to be invoked. In addition, the Hosting Centre has been designed and built to handle a total power failure using UPS (Uninterruptible Power Supply) and a generator.

The chosen infrastructure design that emerged is shown in the following diagram.



Once the S1 production Hosting Centre was completed, the production systems were installed in S1's data hall, with the communications and networking equipment installed on a mezzanine floor. Links between the two disc systems were established, and the internet links for both the production and recovery centres were installed and tested. The production and recovery systems were ready for the Rehearsal.

Rehearsal strategy

The agreed disaster scenario was to be a total power failure to the production data hall, to be effected by hitting the Emergency Power Off (EPO). When the EPO button is pushed, both the UPS and the generator are bypassed. Success would be measured against the stated objectives (recovery in less than 1 hour with no data loss). Additionally, it was necessary to ensure that power to the data hall was available once the Rehearsal was declared complete.

The proof of no data loss was to be achieved by two methods. One was by a user at the recovery site connecting to the S1 suite over the internet, updating values until the power fails and then comparing the last value with the result after recovery. The other was by a script of transactions being run against the S1 suite at the time of the power fail with values being compared after the recovery.

The Rehearsal

Watches were synchronized and the Rehearsal began at 11.40 a.m. on Friday December 1st 2000. Transaction processing started, the internet user logged onto the S1 Suite and began changing values and updating records.

The EPO button was pressed and S1's data hall fell silent as all the computers discs and communications equipment slowed to a halt. The inbuilt batteries in the disc units ensured that the discs performed a graceful shutdown to avoid data corruption.

S1 made the telephone call to invoke the Hewlett-Packard Business Recovery Service. The internet user at the recovery site had received a message saying that there had been a server error. The BRS Specialist returned the call to confirm the alert and then began the agreed procedure. Running a script the disc units were converted from Read Only state to Read/Write. Then the HP-UX computers were booted from the disc unit in the prearranged sequence.

Having collected their Business Continuity Plans, the S1 team drove to the recovery site. By the time the S1 team arrived at the recovery site, all the computers were fully functional. The internet link had switched successfully to the recovery site, and the database was intact and available to the applications.

On returning to his PC, the internet user found that the error message was still up on the screen. He refreshed the screen and was asked to relog into the application. On re-entering the application, the user's data was exactly as it was just prior to the failure, i.e. zero data loss.

Rehearsal results

All of the objectives were achieved:

- Recovery was completed within 1 hour. Actual timing was 34 minutes.

- The transaction script had identical entries in both the production and recovery database, so there had been zero data loss.

- The disruption to the user had been kept to a minimum. He saw a short interruption to service, and was not made aware that he was now accessing a different web and application server on a different site across a different network.

- There were no issues with the infrastructure in the data hall following the Rehearsal; power was successfully restored.

Conclusion

The Rehearsal was a resounding success.

In today's "Always On" environment customers expect access anytime, anywhere. It is not just an advantage to be able to recover quickly from a disaster, it is a business necessity. S1 and Hewlett-Packard's Business Recovery Service have flawlessly recovered an Internet Banking application from a major disaster and have done it in 34 minutes.

This year's rehearsal is going to test other scenarios and develop on the good foundations already rehearsed. The more we rehearse the better prepared we will be for the event that we hope will never occur.