Annual Disaster Recovery Test Report and Gap Analysis for 2011

Prepared by the 2011 Disaster Recovery Test Team

6/8/2011
Prepared Date

Contents

1.0 Test Summary

The annual disaster recovery test was conducted 5/17-5/19, 2011 at the IBM Sterling Forest, New York, BCRS facility. The test incorporated recovery of our Production computer, client MPLS network, various third parties including credit card and national shared branching, recovery of encrypted data, proxy credit union verification, ACH proxy and secure FTP transmissions, and DNS services and ItsMe247.com core proxy test using the Muskegon, MI high availability location.

The test team consisted of seven CU*Answers staff members who traveled to the recovery facility in Sterling Forest, NY to perform the recovery operations. It was also the first time a third shift Operator participated in the event, validating Operations recovery expertise across shifts.

Our thanks for participating in this year's very successful disaster recovery test go to Ohio Catholic Federal CU and Vacationland Federal CU (CU*BASE proxies), as well as Honor CU (ACH testing) and Sage Direct (statements, secure FTP).

This year's test incorporated many firsts, among them it was our first ever test at an IBM Business Continuity and Resiliency Services (BCRS) facility other than our typical Chicago/Schaumberg location and represents a validation of IBM's assertions that recovery can be made at any of their numerous BCRS national facilities that support System-I recovery operations. While the test did stretch IBM a bit and was not without hiccups, it does provide assurances that our data can be recovered at alternate locations.

This was our first recovery and load of a Power 6 system with OS/400 v6r1 and validates our recovery procedures and operations on this latest platform and software version.

The test included the first recovery of two third parties on the new ISO software interface platform. Both ISO FIS and ISO COOP were recovered successfully inclusive of card transaction, and encryption/decryption events (ISO FIS).

FSCC Acquirer national shared branching was successfully tested for the first time, as was CUSC/COOP issuer and acquirer.

For the first time we tested the newly deployed backup 400FTP secure file transfer (FTP) server housed at our high availability site in Muskegon, MI. Secure files were exchanged with Sage Direct, a statement services provider, and relayed to the Disaster Recovery host in Sterling Forest, NY. This server is a step forward for file operations redundancy for CU*Answers and can stand in for the production system in Grand Rapids if necessary.

This was the first test of extending our MPLS client network to a facility other than IBM BCRS/Schaumberg. While it is more of a certification of IBM's ability to extend our network across their footprint, we can report it will work as advertised, though with the consequence of increasing dependencies on proper operations at other IBM facilities through which the traffic is routed to the DR host. Those consequences came to light as two different IBM network events caused some unexpected downtime for the team.

ItsMe247.com has a new logon function called OBC for Online Banking Community. OBC servers are not currently recovered at our High Availability site so a “kill switch” function was constructed to present an alternate logon screen to the member. This function was tested at the disaster recovery site for the first time using the ItsMe247.com standby systems in Muskegon, MI connected to the recovered host in Sterling Forest, NY. ItsMe247.com was tested using the Western Districts Members Credit Union library from three different individuals at three different network locations (one internal to the network, two external disparate Internet connections).

CU*Answers maintains a robust events calendar filled with actual events related to disaster recovery and business continuity readiness. We test the disaster recovery plan for core services annually, in addition to regularly scheduled production roll over events to our Muskegon high availability facility. This year we successfully tested eight “firsts” and as we look to the future we will continue to push our testing envelope. In the second half of 2011 we will add a new Disaster Recovery Coordinator position to ensure corporate recovery posture and recovery planning/testing relevancy remain at the forefront of the financial services data processing industry. If your credit union would like to participate in future disaster recovery test events, please contact a member of our CSR team.

2.0 Gap Analysis

1. The System-I was not configured as requested. We requested four controllers minimum but the machine was only configured with two. Therefore application performance was compromised, although reload times were minimally affected.
    a. The machine was approximately 5 times slower than our Production machine during End of Day/Beginning of Day (EOD/BOD) activities (32 minutes for Production vs. 2 hours 45 minutes at the DR site). This time difference was a result of the lack of the additional disk controllers and the highly disk intensive processing off EOD/BOD.
    b. The system was not configured as requested, but we do not currently contract IBM for a Power 6 system. In a contract renegotiation or addendum for a Power 6, an exact configuration would be specified and expected. This test was a validation of the recovery operations on Power 6 technology to validate the move from Power 5 to Power 6 in a contracted DR environment.
2. Multiple network issues created nearly an hour and a half of unscheduled downtime at the recovery center that resulted in delays to the test schedule and missing or delaying test windows with vendors. The CUSC/COOP test window was missed and had to be rescheduled for 5/19. The test window had to be extended from Thursday morning 8 AM to Thursday afternoon 4 PM.
    a. A test PC from the "mini-comm." test conducted prior to the full event (to validate the network) was left turned on at Schaumberg creating an IP addressing conflict and subsequently occasional interruptions until the source was discovered and the PC shut down. This issue resulted from lack of communication and verification between the test team and the IBM BCRS team in Schaumberg.
    b. IBM's BCRS core network switch at Sterling Forest experienced a "flapping" issue that caused approximately 30 minutes of unplanned network downtime, interrupting nearly all test activities. This was caused by another customer in the facility performing changes to their network which created a "broadcast storm" condition which flooded the network with traffic.
        i. IBM BCRS will implement a procedural change to prevent future recurrences of this issue. When installing customer owned equipment, they will ensure all LAN ports are disabled until the customer is ready to test, and then bring up the equipment one port at a time to ensure everything is operating as expected.
    c. A network switch at Schaumberg crashed causing approximately 50 minutes of unplanned downtime, interrupting nearly all test activities. The switch was our uplink between Sterling Forest and Schaumberg, where our head-end (and default) router is housed. IBM BCRS staff moved our connection to alternate hardware to recover the connection.

        i. IBM BCRS continues to investigate the issue with Cisco, their core switch hardware provider. This was an unexpected hardware failure of a processor card in a high-end Cisco 6509 switch.

3. IBM BCRS did not have the latest version of our agreed upon network diagram. This caused confusion during initial setup of the network though IBM BCRS was able to accommodate the changes we required in a timely fashion.
4. Support and communication with IBM BCRS staff was not to normal standards. Our Project Manager was based out of Schaumberg which made it difficult to coordinate and communicate with the recovery team. Communications were often interrupted as phones and staff were tied up in test events and coordination with Third Parties and proxy credit unions. On site BCRS staff rarely checked in to assess the test or offer assistance. This is in stark contrast to what the team has grown accustom to at Schaumberg. Whether due to culture differences or that the Sterling Forest staff simply left it up to the remote PM, the lack of overt staff and communications was a source of concern and sometimes frustration. If we are to test again at a facility alternate to Schaumberg, on site project management should be required.
5. ACH with Honor Credit Union
    a. Honor could not initially connect to the recovery site. The disaster recovery network subnets are not in the standard routing list (this only affects testing activities and would not be a factor in a real disaster). Our thanks to Kip Kulich of Honor for quickly responding and adding the correct routing to his network.
    b. The FDF (File Description Format) sent to Honor by Operations was not in the correct format. This prevented the file from being sent to the System-I (sanity checks prevented file acceptance). A corrected FDF had to be built and sent to Honor before the file could be successfully uploaded.
6. An automated Robot task configured to send files to client eDOC servers was not stopped on the DR host. This resulted in maintenance files being sent to two client eDOC servers (Sarasota and River Valley) which required manual correction. While this resulted in an unexpected test and validation of communications with client eDOC servers from the recovery center (another first), the recovery run sheets need to be adjusted to ensure disablement of Robot jobs on the recovered host.
7. Some firewall rule changes were necessary to support test activities at the recovery network. While these changes may not have been required in a true disaster, access to the management server at 44th was required. A management server should be configured at Muskegon to ensure firewall changes there can be made with the loss of 44th Street.
8. Our 400FTP secure file transfer system was tested with an upgraded version of the software and operating system used in production. An issue with file transfer to the System-I was discovered, caused by unexpected behavior of one of the upgraded components. The component was downgraded and the transfers were successful.
    a. With current MPLS bandwidth, the transfer of the test EOM April statement file to Sage would have taken over 5 hours. The transmission was cut short to save time and the partially transferred file was verified.

9. The CUBASEFILE restored from PROD backup was subsequently cleared and then overwritten in restore of the CUBASE* libraries from the DEV backup. This is by design; however an edit needs to be put in place not to restore the CUBASEFILE library from the DEV backup.
10. CUSC/COOP had the incorrect gateway configured on their VPN appliance which had to be corrected by their network group, TNS. Additionally, we had to power off the appliance at 28th Street to prevent possible IP address conflicts (would not have been an issue in a real disaster).
11. The FIS VPN device (which we configured) had an incorrect gateway and reversed crypto setup. These were corrected by the CU*Answers team during the test.
12. FSCC and CUSC/COOP software had hard coded production ports and IP addresses in numerous areas of the programs, which caused delays while Programming searched through and updated the software to have the test ports and IP addresses in them for the DR test. This would not have been an issue in a real disaster.
13. There was some confusion with the FSCC test as the test engineer had an incorrect internal form submitted to him (new client vs. DR test).
14. The CUSC/COOP test program had an incorrect IP address for test servers, which created delays as we worked to adjust configurations to correct IP addresses. This would not have been an issue in a real disaster.
15. Crypto Complete master encryption key materials were stored in a 2009 dated envelope, which led to confusion whether or not they were current. In fact, they were current keys which were applied in 2010. It is believed this resulted from the fact these keys, which were generated in 2009, were not properly applied that year, which created confusion at the last DR test. The keys were finally applied in 2010. Policy dictates the key material should be updated every 12 months and while these keys may not actually be in violation of that policy, they should be updated no later than 6/30/2011.

3.0 Future Recommendations

1. This distributed test event underscored the importance of improving communications and coordination between the test team and IBM BCRS for recovery events. As our network has grown and become more complicated, and we extend our test by testing at alternate recovery sites, having a central coordination point of the Disaster Recovery Coordinator will be necessary.
2. The agreement with the recovery services provider should be amended to include recovery to a Power 6 system along with provisions for VPN client recovery in 2013-2014.
3. A firewall management server should be installed in Muskegon to allow core firewall changes to be made if 44th Street is lost. This is already on the roadmap and in the 2011 budget annual.
4. Modify DR TEST Operations run sheets to disable Robot jobs on DR test host.
5. We recommend a strategy change for testing Third Parties. Third Parties almost universally have problems understanding our three center (Production, HA, DR) strategy and this leads to ample confusion and difficulty coordinating test events. There are risks to our production networks during test events, our lack of control and visibility over network configurations, and the fact most Third Parties consider such testing to be Certification events, not Recovery events.
    a. Our recommendation is to install redundant Third Party communications at Muskegon and test them during HA roll swaps. Any recovery at a DR site would be manual and include devices shipped from the vendors (if we can't recover at Muskegon, then all equipment has been destroyed anyway).
    b. Third Parties would be tested out of Muskegon during scheduled high availability roll events.
    c. The DR processes should be documented and coordinated by the DR coordinator, but not typically tested. By having both the HA host and Third Party communications at Muskegon, the network should be amply covered for nearly all perceived events short of super-scale or "Silver Bullet" events that would require relocation out of the Mid-West.
6. We recommend increasing MPLS bandwidth to support client and file transfer requirements. This is already on the roadmap and will be a FY 2012 budget item.
7. Insert an edit for CUBASEFILE library coming from the restore process, and exclude it.
8. We will require a larger public IP address space at the recovery site: space is filling up. We require a minimum of a /26 (currently a /28).
9. The standard routing configuration should to be updated to include disaster recovery site networks (for testing activities only).
10. Incorporate encryption key material auditing function and procedures in Internal Auditing's Master Audit Plan and verify that key materials are being generated and applied per policy.
11. Investigate development of ItsMe247.com disaster recovery splash page on OBC's dead man's switch to include language of functionality unavailable in a disaster event (i.e. CU*SPY, CU*CHECKS, etc.)

12. “Mini-comm.” events should include tear-down checklists that ensure all test equipment is properly removed from the recovery networks.