CU*ANSWERS 2021 DISASTER RECOVERY TEST REVIEW

EVENT DATE(S): 6/14/2021 – 7/01/2021

SUMMARY

The focal point of the CU*Answers Business Continuity strategy is traditionally seen as the High Availability (HA) program, replicating data in real-time between geographically dispersed data centers, and conducting live production rollovers every six months. During these HA rollover events, CU*BASE core processing is provided for all online CU*Answers credit unions from systems at the secondary data center, located more than 750 miles from the primary site.

Although not as frequent as the HA rollovers, CU*Answers has a history of performing disaster recovery tests to restore the CU*BASE production environment from data on backup tape media. Up until 2015, these DR tests were conducted on an annual basis at a fully-equipped hot-site provided by IBM. In 2016, a shift occurred that put the emphasis on recovering systems from data replicated in real-time (High Availability) over data archived on tape media to meet today's strict recovery time objectives. As a result, conducting DR exercises was reserved for specific non-core systems and applications. Daily backup to tape media is still performed as a tertiary recovery strategy and for restoring files on request from a specific point in time.

In the spring of 2021, a project was completed at CU*Answers to change vendors for encrypting data on tape to keep up with advancements in security and to improve performance. The final stage of that project included a "bare metal" restoration of CUAPROD from backup tape to ensure capabilities after the vendor change as well as update/validate recovery procedures. In a catastrophic disaster scenario where both the primary and secondary systems are not available, the ability to restore from backup media is required.

To conduct the bare-metal recovery test, a hosted IBM i Power System was acquired from a local vendor (iInthecloud.com) to allow recovery teams to test the restoration process completely independently from the live production environment. The testing period was scheduled for **June 14 – July 1, 2021**. The scope of this test was focused on the ability to restore data following the change in encryption vendors and to validate procedures for recovering the CU*BASE production server. This recovery test did not include integration with third-party vendors or access from external users or systems.

Since the last test to restore CUAPROD from backup tape (performed in 2015), many significant changes have occurred in the production environment. These changes included not only technology upgrades but also operational changes such as time-zone processing. Knowing this, the recovery test was scheduled over multiple weeks to allow for an initial "practice" test, time for adjustments to process and procedures, and a "final" test to validate those changes.

The effort was very successful. Teams were able to confirm that the change in encryption vendors did not impact the ability to restore data. In addition, the knowledge gained about how changes in production impact the process

for restoring the system in a timely and effective manner, has provided insight that has resulted in changes in the overall recovery strategy.

The following sections of this report identify the details, challenges observed, lessons learned, and recommendations for consideration related to this event.

EVENT DETAILS AND CHALLENGES OBSERVED

As noted earlier, hardware was acquired by a local vendor (iIntheCloud.com), hosted in a tier-one data center with applicable security and environmental controls. Recovery participants were split between on-site and remote, with the bulk of the process performed remotely once the backup tapes were loaded. The duration of the event was scheduled over a four-week period from June 14 to July 1, 2021.

First Recovery Test – Week of June 14

On **Monday, June 14**, recovery team members delivered and loaded the (8) LTO tapes required for the restoration test. During the initial load to restore the IBM Operating System and licensed programs, it was discovered that the syntax for performing the “save system” (SAVSYS) command had changed with a recent OS version upgrade, resulting in missing IBM libraries on the backup tape. These libraries included select licensed programs and system drivers required for the restoration of the server.

As a workaround measure, teams installed the missing libraries from an IBM operating system ISO image. In an actual disaster scenario, installing the operating system from an IBM ISO on DVD may actually reduce the amount of time required for the restoration. Based on what was learned, changes to the script in production for archiving PROD using the SAVSYS command were made to include the IBM libraries required for restoration. This change was validated during the final test the week of June 28. Depending on the additional amount of time required to back up these libraries, teams will determine the optimal solution (tape vs. DVD) for future backups and recovery tests.

On **Tuesday, June 15**, CU*BASE applications and member data libraries were loaded on to the restored server. During this process, it was discovered that the shift to processing by time zone had altered the sequence in which data is stored on each tape. As a result, scripts for restoring the data were reading each tape multiple times to load all of the files separated by time zones. This increased the amount of time required to load each set of libraries. Once discovered, teams modified the scripts to align with the process used to archive the data on the tape. This change was also validated during the final test during the week of June 28.

On **Wednesday, June 16**, CU*BASE application testing was performed by recovery teams to validate the integrity of the data between production and test systems.

The **total time** for restoring the CU*BASE production server from tape for the first test was approximately **35¾ hours**. This was performed with a single tape drive. In an actual disaster, multiple tape drives would likely be utilized (if available) and will be included in future bare-metal recovery tests to reduce the amount of time required. To stay within the scope of the objectives for this test, a single tape drive was used.

The initial operating system load and configuration took approx. 3½ hours as follows:

- Installation of license internal code and O/S (1 hour 52 minutes) – from ISO image

Restoring user profiles	(4 minutes)
Restore configuration	(28 minutes)
Restore objects	(11 minutes)
Restore SMZ* libraries	(29 minutes)
Restore ITE* libraries	(24 minutes)

From there, CU*BASE and member libraries took approx. 32¼ hours as follows:

Create Misc. Libraries (BKPDATA, ARC*, etc.)	(1 minute)
Create Save files in BKPDATA	(2 minutes)
Restore PROJ* Libraries	(25 minutes)
Restore /FILETRANS IFS folder	(20 minutes)
Restore OPERATOR Library	(2 hours 14 minutes)
Restore FILExx Libraries	(12 hours 36 minutes)
Restore FILExxE Libraries	(4 hours 49 minutes)
Restore FILExxNB Libraries	(1 hour 28 minutes)
Restore CUSTOMxx Libraries	(10 minutes)
Restore QUERYxx Libraries	(4 hours 3 minutes)
Restore EMPxxx Libraries	(6 hours 6 minutes)

In comparison, the previous CU*BASE production recovery test performed in 2015 (also with a single tape drive) took approximately 24 hours to restore. The additional amount of data and applications on the system in 2021 requires approximately 48% more time to restore. This is one of the determining factors for why high availability is preferred as the primary strategy for recovering the CU*BASE core processing environment.

During the **week of June 21**, changes to the scripts for archiving data to tape were implemented on the production systems. At the end of the week, fresh data tapes were retrieved to conduct the "final" recovery test.

Second Recovery Test – Week of June 28

On **Monday, June 28**, the second and final recovery test was launched after the changes implemented from challenges observed during the first test were identified. The same process was followed but with modified procedures. Prior to the second test, the existing restore was wiped so that teams would begin with a "bare-metal" system. It was discovered that after the wiping process, the partition was not activated by the vendor, creating a slight delay before recovery teams could begin. The operating system was restored completely from tape, unlike during the initial test. Time to restore from tape was 5¾ hours, versus 3½ hours from the ISO image during the initial test. It was noted, however, that additional changes could be implemented to further enhance the performance of the restore. These changes will be included in future recovery tests.

The initial system load and configuration took approx. 5¾ hours as follows:

Installation of license internal code and O/S	(4 hours 11 minutes) – from tape
Restoring user profiles	(4 minutes)
Restore Configuration	(28 minutes)
Restore objects	(11 minutes)
Restore SMZ* libraries	(29 minutes)
Restore ITE* libraries	(24 minutes)

On **Tuesday, June 29**, during the FILExx library restore tape job, a tape drive hardware failure was experienced. This process was running during the overnight hours and had to be restarted the next morning after identifying which files had completed. In addition, remote recovery testers were experiencing connectivity issues requiring multiple IPLs of the system to resolve. Future recovery tests will likely include more on-site participants.

On **Wednesday, June 30**, another tape drive hardware failure was experienced while restoring files from the most recent EOD tape, ending the job prematurely. Working with the vendor, teams were able to restart the job and continue with the test.

On **Thursday, July 1**, teams concluded application testing and purged the data from the test host. Accounting for the lost time due to tape drive hardware failures, the actual restore times for the second test were within ten (10) minutes of the initial test. **Total time to restore CUAPROD from tape was approximately 38 hours.** This total does not include idle time by the system. In an actual disaster, teams would function in shifts until the restoration was complete. For the purpose of this recovery test, participants were scheduled for normal working shifts.

CONTINUING EFFORTS AND CLOSING REMARKS

What started out as a test to confirm that teams can recover the CU*BASE production server from backup tape after the change in encryption vendors, turned into an opportunity to dive deeper and learn more about the systems and applications that make up the core processing environment. Much like reverse-engineering a manufactured product, understanding how the individual pieces fit and function together helps us to design more resilient applications and respond more effectively when disruptive events occur.

Changes have already been implemented into the production environment as a result of the findings in the 2021 Disaster Recovery Test. Prior to the next recovery test (date to be announced), teams will be meeting to determine methods of reducing the amount of time required for restoring data by looking at technology alternatives (such as multiple tape drives or virtual tape libraries) and reprioritizing the sequence of the data restored so that users can access the system more quickly while non-essential applications are recovered.

Given the existing robust High Availability program at CU*Answers with data replicated in real-time, a scenario where restoring CU*BASE from backup tapes would require that both the primary and secondary systems were not available for a significant period of time. While restoring from backup tapes requires 35-38 hours to complete, HA rollovers are performed in 1-2 hours, even during emergency incidents. This has been validated during more than one unexpected disruption.

Whether planned or unexpected, every rollover and recovery exercise provides the opportunity to continually improve the process. The value and significance of these exercises is multiplied when we consider the ever-changing threat landscape from hardware component failures, dependency on third-party vendors and supply chains, and the frequency and scope of today’s natural disasters, including global pandemics.

Report submitted by Jim Lawrence, CBCP - CISSP | CU*Answers | Vice President of Business Continuity and Operations

Unless otherwise noted, all times noted in this report are Eastern Time.