CU*ANSWERS HIGH AVAILABILITY PROGRAM REVIEW

EVENT DATE(S): 2/06/2022 – 2/13/2022

SUMMARY

As part of an ongoing business continuity program, CU*Answers actively maintains a high-availability (HA) core processing environment with near real-time data replication between identical hosts located at two geographically dispersed, state-of-the-art data centers. Twice each year, live HA rollover events are scheduled to redirect CU*BASE production and operations to the secondary data center (located in Yankton, SD) for a period of one full business week or longer. At the conclusion of the rollover event, core processing is redirected back, and operations resumed at the primary data center (located in Kentwood, MI). These live production HA rollover events are invaluable to validate procedures and ensure the ability to recover CU*BASE GOLD core processing in an effective and timely manner when incidents occur that threaten to disrupt business operations.

As mentioned in previous reports, these rollover events provide the opportunity for performing regular system maintenance to update or replace hardware and software components on production equipment with minimal impact or downtime. During the Fall 2021 HA rollover, an eight-hour maintenance window was scheduled to update the firmware for all core backbone network switches at the production data center. This required a network connectivity disruption at the Kentwood, MI data center. As a precautionary measure, all virtual servers were powered down to minimize the risk of problems mounting data volumes on the SAN once network connectivity is restored. Prior to the fall 2021 maintenance project, core processing and online/mobile banking environments were redirected to systems at the secondary data center to minimize impact to members.

The February 2022 HA rollover also contained a maintenance window. This one included a complete power interruption at the production data center. As part of a remodel project in the Operations Command Center, the Emergency Power Off (EPO) safety system required an update and relocation of one of the activation switches. To complete this step, the server room UPS and transfer switch (utility/generator power) was inactivated. This also required that not only all servers but also all network devices be powered down.

Once again, recovery teams performed a rollover for both CU*BASE core processing and online/mobile banking to redirect traffic to the secondary data center. This allowed the safe completion of the EPO system upgrade with minimal impact to members.

On Sunday, February 6, beginning at 12:01 AM ET, recovery teams initiated the process to redirect online and mobile banking traffic to systems at the Grand Rapids, MI, data center. At 2:00 AM ET, the HA rollover was performed to bring core processing online at the Yankton, SD, data center. The EPO system upgrade project began at 5:00 AM with power interruption occurring from 6:00 AM – 7:00 AM. Once completed, teams began powering up network devices and servers. By 9:00 AM, internal systems were online with a few exceptions, detailed later in this report.

As with most planned maintenance events, the amount of time invested in planning far exceeds the amount of time required to execute the plan. "Measure twice, cut once." The last scheduled power interruption at the production data center occurred in 2012 as part of a project to double the utility power capacity to allow for future growth. Ten years later, we are still reaping the benefits of that added capacity and the knowledge gained, which enabled us to successfully power down/up more than 300 servers and devices in an effective and efficient manner, with minimal impact.

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

All times noted in this report are Eastern Standard Time.

EVENT DETAILS AND TIMELINE

Careful consideration and strategic planning are applied in the design of the data center and the IT infrastructure to allow for flexibility and scalability when planned maintenance is required. This helps to provide an environment where most system and network maintenance projects can be completed during non-peak hours with minimal impact or downtime to users. The scope and complexity of this planned event put that strategy to the test once again, pushing up against the boundaries of the available maintenance window.

Multiple teams worked together to prepare in advance a playbook detailing the steps required to isolate and prioritize the technology supporting the most critical components so that they are the last to power down and the first to power up. While systems are often rebooted during updates and security patch applications, actually powering down to the point where all moving components come to a stop, is a rare event in the data center. Once the plan was approved, the date was scheduled and announced.

The event described below was divided into three phases on Sunday morning, February 6th:

1. **Online and Mobile Banking Rollover** (12:01 AM – 2:00 AM)
   o   To provide online and mobile banking from the secondary data center in Grand Rapids, MI.
2. **CU*BASE HA Rollover** (2:00 AM – 4:30 AM)
   o   To provide CU*BASE/GOLD from the HA data center in Yankton, SD.
3. **Network Maintenance Project** (5:00 AM – 9:00 AM)
   o   Power down all network servers and infrastructure devices (firewalls, switches, routers, etc.).
   o   Rewire and upgrade EPO safety system including power interruption from 6:00 – 7:00.
   o   Power up all infrastructure devices and network servers.

To minimize downtime for members accessing their accounts through online and mobile banking platforms during the maintenance period, a rollover was performed to bring **It's Me 247** and **CU*Publisher** applications online at the secondary data center in Grand Rapids, MI.

On **Sunday, February 6th**, beginning at **12:00 AM ET**, teams initiated the changes to redirect traffic for online and mobile banking. The process primarily involves making necessary domain name server (DNS) record changes for the web sites involved. A small number of issues were observed (as detailed later in this report) but overall traffic redirection was completed by 12:20 AM. Teams continued to monitor the applications until the next phase of the event.

At **2:00 AM**, recovery teams began the HA rollover process to bring CU*BASE core processing online at the secondary data center in Yankton, SD. The rollover event completed by **4:00 AM** with connectivity to all third-party EFT vendor networks confirmed. During each rollover process, all third-party EFT vendors function in "stand-in" mode adhering to predefined settings on transaction types and amounts (set by the credit union).

With the planned power interruption at the production data center, Operators were relocated to workspace at the Grand Rapids, MI, data center for the duration of the event. Once all post-roll application testing was completed, the Operations Team performed normal EOD/BOD processing to prepare for the new business day.

During the HA rollover period, networking teams began to power down non-essential servers to minimize the duration of the EPO system maintenance. Once the HA rollover had completed and all tests confirmed, all remaining servers and network infrastructure devices were powered down, following a strategically created playbook, complete with workaround procedures and contingency plans. The final phase involved powering down the server room UPS, placing the generator in bypass mode, and disabling the transfer switch.

At **6:00 AM**, teams were ready to shut off utility power to the server room and complete the process of upgrading and relocating the EPO safety system. At 6:40 AM, the project was completed, and EPO switch functionality tested. At **7:00** AM, power was restored to the server room and teams began powering up network infrastructure devices and servers.

By **8:05 AM**, most internal servers were back online with a few exceptions. One notable challenge included a hardware error on the production online banking SQL server. With the online banking environment functioning at the secondary data center, the hardware error did not impact members accessing the site. The support vendor was contacted, and replacement parts ordered under a warranty agreement.

Originally scheduled for **10:00 AM**, the decision was made to postpone the online and mobile banking rollback process until after the SQL server was repaired and validated as ready for production. The replacement part was received and installed that evening. After monitoring for several hours, teams completed the online and mobile banking rollback on **Monday, February 7th, at 2:30 PM.**

On the morning of **Sunday, February 13th**, beginning at 2:00 AM, recovery teams started the process to roll-back CU*BASE production to the primary data center. This was completed by 3:50 AM with all services back online.

CHALLENGES AND CONTINUING EFFORTS

Every rollover event, planned or unplanned, provides an opportunity for a valuable learning experience. Even those that appear relatively smooth on the surface often require decisions to be made and resolutions to apply behind the scenes. Every recovery team member gives their all to minimize the impact to clients and members, while performing their job with an intense focus. Challenges observed during this rollover event include the following, grouped by the three phases as noted earlier:

CU*BASE HA Rollover

1. After the HA rollover on Feb. 6th, the HMC (Hardware Management Console) units on both PROD and Hosts were unable to communicate to exchange hardware licensing information.

- Although both servers are equipped with identical hardware, the number of CPUs licensed on the production host is higher than the stand-by host. During a rollover (or failover) event, licenses are swapped to ensure equal capacities for system performance.
- In the months since the last HA rollover, the IP address of the HMC in the HA environment had been changed as part of a network topology upgrade project. Communications had worked fine until the role-swap process was performed, making the server at the Yankton, SD, data center the primary.
- Although the HMC configuration console displayed the correct settings, through network packet captures, teams were able to determine that the HMC was attempting to communicate using the old IP address. An HMC reboot (to clear potentially cached information) did not clear this up.
- The HA rollover itself was performed with minimal issues. A support call was placed with the hardware support vendor (IBM). Based on the circumstances, teams made the decision to continue to the next phase of the project (EPO system upgrade with data center power interruption). The HMC issue would be resolved working with the vendor after power was restored.

2. Future HA rollovers may become less like a mirror of production (for lower priority features).
- This challenge was also included in the previous HA rollover report. As new features and services are added to the core processing platform, it is becoming necessary to prioritize those that will be available during a disaster recovery scenario (high priority), and those that will be restored later (low priority).
- The purpose of performing the HA rollover exercise is to validate procedures and confirm our capabilities to recover should an unplanned disruptive event occur. To properly balance the effort required to minimize downtime and recover less critical features and services, prioritization must occur. That may mean that some services are not available during the brief rollover windows conducted twice each year.
- Teams will continue discussing methods to optimize this process and find the balance that best meets the corporate goals and objectives.

Online and Mobile Banking Rollover

3. A number of changes were implemented since the last online/mobile banking rollover. Some of the changes did not replicate to the secondary systems and required manual configuration changes.
- Select API keys required updating to match those in the production environment.
- Certificates required updating on load balancing appliances after the conversion from **It's My Biz** to **BizLink 247**.

4. Mobile banking code to detect when biometrics is not available (MACO/DAON).
- The network maintenance event on 2/6 involved a power interruption to the server room requiring powering down servers that host the MACO biometric authentication capabilities for the mobile banking platform. The software was updated to include the ability to detect when the MACO servers were offline and prompt the member for the username and password for authentication. While confirmed in a test environment, during the rollover for mobile banking this code modification did not function properly, presenting an error message for users on Android devices.
- Teams were able to remedy the error during the rollover period and will confirm functionality during the next rollover for online and mobile banking.

5. Servers that store optics log data for online/mobile banking applications are not replicated at the secondary data center.
    o This historical information is not available for the maintenance window during the power interruption.
6. Member profile images while on HA (one-way replication).
    o A feature of the latest version of online and mobile banking platforms is the ability to upload profile images as part of the member experience. Replication of these images is a one-way transfer (primary to secondary). When functioning on the secondary servers, profile images are not replicated back to the primary server.
    o Teams are reviewing options for profile images prior to the next OLB rollover. One option is to disable the feature to upload a new image while on secondary servers. Another is to manually synchronize profile images prior to the rollback process.

Network Maintenance Project (EPO system upgrade with power interruption to production data center)

7. Remote access authentication not available during power interruption.
    o The servers that provide the One Time Password (OTP) were not available during the power interruption. Recovery teams were required to authenticate remotely prior to the interruption, for access to the servers at the secondary data center. Remote Access appliances are load-balanced between sites; however, the communications channel for providing the OTP is not replicated.
    o In a true disaster scenario, the servers that provide the OTP would be restored from backup.
8. Application servers that are not part of the current high availability strategy were offline during the power interruption. Multiple announcements were sent to credit unions prior to the event.
    o This included services such as:
        ▪ CU*SPY (reports and statements)GoAnywhere
        ▪ Snapshot libraries
        ▪ Hosted email and web sites
        ▪ CU*Answers corporate email and web sites
        ▪ Hosted credit union equipment (facilities management)
        ▪ CheckLogic (check images)
        ▪ And more.
9. Data center humidifier drain purge process was in the middle of a cycle when the power interruption occurred. This allowed a small amount of water to leak on the server room floor (under the raised tiles).
    o Environmental detectors quickly alerted teams for a prompt response.
    o The unit was tested after power was restored and found to be working properly.
10. A firewall pair as part of the hosted facilities management network failed to boot up properly requiring a restoration of the operating system and configuration files to return to normal operations.
11. A hardware error was detected on the production SQL server for online/mobile banking during boot up.
    o With the application running properly on servers at the secondary data center, rollback to the production site was postponed until replacement parts were acquired under the support agreement.
    o Replacement components were received that evening and installed by 9:30 PM. Teams monitored the server and burn-in process overnight. The OLB rollback was performed at 2:30 PM on 2/7 to bring online and mobile banking back to the production servers.

CLOSING REMARKS

Whether planned or unexpected, each recovery test and high-availability rollover exercise provides the opportunity to continually improve the process. The value and significance of these exercises are 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.

Just as significant is the ever-changing technology environment that makes up the CU*BASE core-processing platform. Increased complexity in application development, vendor integration, and network infrastructure requires more frequent reviews and assessments of the business continuity strategies in place to meet recovery time objectives and a shrinking tolerance for downtime. Regular rollover exercises help us measure our progress and adjust accordingly.

The investment made over the past two decades in building and testing its Business Continuity Program has positioned the CUSO to navigate the storms on the horizon and enables it to reach for new opportunities and serve its owners and client credit unions in innovative ways.

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

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