CU*ANSWERS HIGH AVAILABILITY PROGRAM REVIEW - ONLINE AND MOBILE BANKING ENVIRONMENT EVENT DATE(S): 5/29, 7/17, 8/13-14/2019

EVENT SUMMARY

Following the successful pattern of the HA rollover program for CU*BASE core-processing, the first public rollover for the online and mobile banking environment was performed by recovery teams at CU*Answers. This initial rollover was scheduled, in part, as a result of the recovery effort initiated on February 8, 2019, due to an extreme winter storm causing a loss of utility power and generator failure at the primary production data center. During the winter storm, teams were able to restore the generator before recovery of the **It's Me 247** environment was necessary. However, it left a number of questions unanswered for an effort that had yet to be tested. This became an important goal in 2019 for the organization.

The online/mobile banking environment consists of a pool of load-balanced, redundant servers at the primary production facility in a secure DMZ environment. A clone of this environment is installed on servers at the secondary data center. Application updates are applied to servers at both the primary and secondary data centers to ensure synchronization.

Prior to this scheduled rollover event, testing of the **It's Me 247** online and mobile application on servers at the secondary data centers was limited to internal staff on a private network. Live testing involving credit union members on the public Internet was not part of the program.

The rollover process consists primarily of making DNS changes to the applications that operate in the server environment (including **It's Me 247**, **It's My Biz 247**, APIs, PIB, Mobile, etc.). Once DNS changes are applied (allowing for propagation throughout the public Internet), network traffic is redirected to the secondary data center. The complex portion of the rollover consists in the integration with 60+ third-party vendor interfaces for services such as bill pay, account transfers, and check image retrieval.

Given that this would be the first time servers at the secondary data center deliver the **It's Me 247** application in a live environment, an initial "partial-rollover" was scheduled and performed on July 29 involving only the PIB function of the application. This allowed teams to confirm communications between data centers and gauge the length of time DNS changes required for propagation.

Following the PIB rollover, recovery teams prepared for the initial full application test, scheduled for July 17, 2019. At 6:00 AM ET, the rollover was initiated. Although access to online and mobile applications was successful for most credit unions, it became apparent that credit unions hosted on the partner network at Site-Four were not able to access the servers at the secondary data center. A line was drawn at 7:00 AM to resolve the connectivity issues or rollback to the production servers. Unable to meet the deadline, teams collected information for troubleshooting the issue and initiated the rollback procedures.

During the days that followed, the solution was discovered and implemented, and a follow-up rollover scheduled for August 13. At 6:00 AM ET, recovery teams again initiated the rollover, confirmed that the solutions applied did resolve the known issues, and began working through the list of tests for online and mobile applications. New issues began to surface, mostly resolved through the addition or modification of routes at the secondary data center.

Once credit union branches started to open, support teams received calls from three credit unions indicating that staff were unable to access either the online or mobile applications. Once again, these were mostly due to firewall and/or routing changes, this time on the credit union branch network. The complete list of issues and challenges observed and their resolutions are detailed later in this report.

On the following morning, at 6:00 AM ET, teams initiated the rollback to complete the first successful public rollover of the online and mobile banking environments. A post-event briefing was conducted to discuss and collect all of the relevant information for the event. The following sections identify the timeline of events as they unfolded, as well as challenges observed, lessons learned, and recommendations for consideration.

All times included in this report are Eastern Daylight Time.

EVENT TIMELINE

Prior to the rollover event, communications were sent to all CU*BASE credit unions informing them of the scheduled rollover with a request that they participate by providing prompt feedback of any issues that are reported by their staff and members.

Prior to the initial rollover in July, internal testing detected a potential issue with API applications. The decision was made not to rollover the API services, instead back-hauling them through the production datacenter.

Wednesday, July 17, 2019

- 6:00 AM – Recovery teams initiate the rollover by changing DNS entries for sites that comprise the online and mobile banking environments. Within the first few minutes, traffic is detected on servers at the secondary data center.
- 6:10 AM – A connectivity issue is detected between the application servers at the secondary data center and the CU*BASE host at Site-Four for credit unions on the CU*NorthWest and CU*South networks. Access from all other self-processing credit unions is confirmed.
- 6:15 AM – Teams recycle services on each web server in the pool at the secondary data center. This does not resolve the connectivity issues or intermittent errors observed. Symptoms indicate a potential routing issue between networks.
- 6:30 AM – Testing identifies issues with iPay integration. Recovery teams troubleshoot connectivity with the Fiserv network. Errors are also reported during testing of the **It's My Biz 247** application.
- 6:45 AM – Connectivity issues with Site-Four credit unions are tracked to the routing configuration on the EBN-VPN network. A maintenance deadline is set for 7:00 AM to resolve the connectivity issues or initiate the rollback plan.
- 7:00 AM – Teams gather information for diagnosing observed issues and initiate the rollback to servers at the production data center.
- 7:05 AM – The rollback is completed and application access confirmed.

For the next two weeks, teams parse the log files and information gathered to diagnose issues and apply the resolution. The next rollover attempt is scheduled for Tuesday, August 13 at 6:00 AM.

Prior to the second rollover attempt, a resolution was implemented (reinstallation of DB2 connections on each server) to allow the inclusion of API applications at the secondary data center.

Tuesday, August 13, 2019

- 6:00 AM – Recovery teams initiate the second rollover by changing DNS entries for sites that comprise the online and mobile banking environments. Within the first few minutes, traffic is detected on servers at the secondary data center.
- 6:05 AM – Initial testing uncovered a problem with API applications (after applying the resolution from the previous rollover). An attempt was made to rollback only the API services, which did not resolve the issues.
- 6:15 AM – Test participants report experiencing intermittent connectivity issues for both online and mobile banking. Application services on the web hosts are recycled in an attempt to stabilize the connections.
- 6:35 AM - A source NAT rule for APIs was found to be missing on the web application firewalls at the secondary data center. Adding this rule corrected the issues noted above.
- 6:40 AM – Connection errors are detected from the MAP/MOP hosts (at the primary data center) to the web server pool at the secondary data center. Routes are added to resolve the issue.
- 7:00 AM – Online and mobile banking applications have stabilized at the secondary data center.
- 7:05 AM – Potential issue is detected with the Fiserv Bill Pay link. Endpoint connectors are updated on secondary servers to resolve the issue.
- 7:15 AM – Errors are detected in the log files pertaining to the third-party vendor certificate for Savvy Money. A configuration change is made to the certificate chain on the secondary load balancers to correct the errors.
- 8:25 AM – As credit unions open for business, reports are received from two locations indicating a failure to connect to the **It's Me 247** web servers at the secondary data center. The impact is limited to employees on the credit union's internal network. Members were not affected. Technical teams were engaged to work with IT support teams at each credit union to diagnose and correct the issues by making the necessary firewall and routing changes.
- 9:25 AM – An issue was reported by one credit union indicating that the link to **It's Me 247** was detecting the site as offline. Support teams discovered that a custom legacy login widget was being used on the credit union's web site to direct members to the online banking site. Although the widget was incorrectly detecting the site as offline, clicking through on the link did take the member to the appropriate login page. The Web Services Team was engaged to modify the code on the credit union web site to remove the legacy portion (and its dependence on the go.itsme247.com service).
- 9:45 AM – An issue was discovered by test participants indicating a failed attempt to perform an iPay enrollment. Teams were able to diagnose the problem through the information contained in the log files. A resolution was implemented later that day; however, teams were unable to coordinate a live member test through the credit union. No additional iPay enrollment errors were noted in the log files through the remainder of the rollover event.
- 11:00 AM – One credit union hosted from the Site-Four data center reported not being able to retrieve check images through online banking. A firewall change was made at the Site-Four data center to correct the issue. While troubleshooting this issue, teams discovered that the configured outbound NAT IP

address from the web server pool at the secondary data center did not match the inbound NAT of the same pool. Due to the potential impact of the change, the decision was made to postpone the NAT address correction until the next after-hours maintenance window.

- 11:25 AM – Although not reported, recovery teams discovered an error in the log from a member attempting to retrieve a check image from Associated Bank. An attempt was made to contact the vendor to determine if access was open to servers at the secondary data centers. It is possible that the NAT IP address mismatch identified earlier might have impacted connectivity to select third-party vendors.

Support teams monitored calls for the remainder of the day. No additional issues were reported. The rollback was scheduled for the following morning at 6:00 AM.

Wednesday, August 14, 2019

- 6:00 AM – Recovery teams initiate the rollback by changing DNS entries for sites that comprise the online and mobile banking environments. Within the first few minutes, traffic is detected on servers at the primary production data center.
- 6:10 AM – All post-roll checks are completed. No new issues were reported. Teams gathered notes from the event for debriefing and reporting.

CHALLENGES OBSERVED

Being the first scheduled live rollover event for online and mobile applications at the secondary data center, teams expected issues and challenges to surface. While systems at both data centers are similar, they each require unique host and network configurations. Simply copying the configuration from one to the other will not function properly in a high availability environment. Both must be designed and constructed independently to meet the availability and security demands of the applications they host.

Several issues were detected and resolved during internal pre-roll testing. Other issues (as identified in this report) are only detected in a live environment with end user (staff and member) participation. The experience gained during this initial rollover event gives us the confidence and expectations for responding to incidents where unplanned emergency rollovers are necessary.

Many of the issues observed are noted earlier in this report in the Event Timeline section. Additional issues and challenges as we move forward and prepare for future rollovers are noted below.

- Internal communications
    - During the initial rollover test on July 17th, the impact of issues observed during the first hour led to the decision to rollback and reschedule. The information gathered allowed recovery teams to prioritize and diagnose each problem and apply necessary corrections.
        - When support staff arrived later that morning to receive calls from client credit unions, the fact that teams had rolled back to servers at the production data center was not communicated properly, leading to some confusion among internal teams.
        - A debriefing meeting was held and internal communications improved prior to the August 13-14 rollover event.

- Partner and third-party vendor integration
    - As noted earlier in this report, the integration with multiple CU*BASE partners and self-processors, in addition to the more than 60 upstream and downstream third-party vendor interfaces, creates an application environment that is complex and dynamic. Change is constant and the discipline of implementing, testing, and maintaining those changes throughout each data center is required. Design and support teams must understand how each change impacts the ability to operate from both the primary and secondary sites. Future rollovers will dictate our success in this.
    - One of the challenges, as a core-processor working with third-party vendors, is that developers often do not have (member) user accounts to test functionality. While a credit union can assist in testing the changes in the production environment, it is only during rollover events can we validate the changes at the secondary data center. The nature and frequency of application changes will in part dictate how often future rollover events will be scheduled.

- Internet bandwidth limitations
    - Internet access to the secondary data center is available from redundant gigabit ethernet circuits to the primary production data center and a separate 100 MB ISP circuit. For the purpose of this test, all public online and mobile banking traffic was routed through the 100 MB ISP circuit. While significantly smaller than the production data center, the bandwidth peaked at 55% during the 24-hour rollover test.
        - While capacity was plentiful for this rollover test, in the event of an actual disaster at the primary production data center, this circuit could present a bottleneck. Already in the 2020 budget is a project to upgrade this circuit to 1 GB, matching that of production.

- Client credit union branch connectivity
    - Not only is change constant in the data center, it is also a regular occurrence at the credit union branch network. It is important to communicate the networking firewall and routing requirements prior to and in between rollover events to minimize the risk of having to troubleshoot connectivity issues.
        - Teams will discuss publishing a test page on web servers at the secondary data center that credit unions can test access to periodically from each branch in-between rollover events.

EVENT SCOPE AND RECOMMENDATIONS

As with many web-based applications, there are ancillary products and services that comprise the end-to-end member experience. Many of these functions and features are provided by an external source or alternate hosts that do not share the same redundant components and high-availability strategy as the core I**t's Me 247** application. For the purpose of this rollover event, those ancillary functions include the following:

- Hosted credit union web sites (entry to online banking for the member)
- OBC (Online Banking Community – customized for each credit union)
- MACO (Multiple Authentication Convenience Options)
- MAP/MOP (Membership Application/Opening Process)
- CU*Publisher (Mobile app controls)

- CU*Spy (Digital receipts, statements, reports, eSignatures, etc.)
- CheckLogic (check images through eDOC)
- RDC (Remote Deposit Capture through eDOC)

In the event of an actual disaster scenario, the applications listed above (hosted by a combination of physical and virtual servers) would be restored from backup data in order of priority on available hardware at the secondary data center. While application rollovers are typically performed in minutes, recoveries are often measured in hours.

The cost of implementing a high-availability rollover strategy for each application environment can be significantly more expensive than that of a recovery strategy. Having validated the ability to quickly rollover the online and mobile banking environment through testing, teams will seek to enhance the capabilities for additional applications, where it is cost-effective to do so and aligns with business objectives. These will be included in discussions and budget considerations throughout the 2020 fiscal year. Changes implemented will be included in the scope of future rollover events.

CLOSING REMARKS

This initial public rollover of the **It's Me 247** online/mobile banking environment is a significant accomplishment for the organization and the network. It marks a shift from a strategy of recovery (restore from backup) to rollover (synchronize servers and redirect network traffic). It reduces the amount of time required to bring applications back online in the event of an unplanned disruption at the primary production facility. **It's Me 247** now joins CU*BASE/GOLD in our high-availability rollover program.

Performing these rollover and recovery exercises on a regular basis helps us to improve our processes, sharpen our skills, and design and deliver better products in the 24x7 world we live in. CU*Answers is committed to that goal as demonstrated in this report.

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