opentext™

Root Cause Analysis

Tracking number: 231115-001643
Incident window: November 16, 2023, from 02:30 CST to November 30, 2023, at 09:00 CST
Services affected: Zix Email Encryption, Email Threat Protection and Archiving

Overview

On November 16, 2023, at 02:30 PM CST, Zix detected a Severity 1 failure of a large SAN storage infrastructure (SAN pool) in the Dallas Data Center. Multiple services were impacted as a result: ZixPort, Secure Cloud Email Encryption, Legacy Email Threat Protection, Legacy ZixArchive, and ZixEncrypt, among others.

Impact

Customer experienced several issues including inability to send and receive secure messages and using features of the Zix services.

Response

The SAN storage provider was immediately contacted for support and assistance with the SAN recovery, which was resolved on November 21. Internal teams worked to restore services starting with the most critical services in parallel with the SAN recovery effort.

Root Cause

Firmware Defect

A large SAN storage group stopped responding, rendering several Zix services inaccessible. The database software vendor was contacted immediately to assist. Their investigation revealed that the issue stemmed from an unreported firmware defect.

Redundancy Impact

High availability disaster recovery systems responded and initiated redirects to secondary storage locations. Due to the scope of the issue, the recovery system was unable to transition to secondary storage locations seamlessly, and intermittent outages occurred. Additionally, repeated attempts by the service to connect with the impaired data storage group caused other issues. Subsystems were also affected because they were redirected to secondary devices that were part of the impacted storage group.

On November 16, 2023, Zix experienced a failure in the Dallas data center SAN pool due to a firmware defect in the SAN pool, which resulted in failed or degraded services.

Primary high availability systems, owned and operated by Zix, automatically responded by way of failovers and sound disaster recovery mechanisms. ZixPort (Zix Secure Messaging Portal) exhibited some brief outage symptoms as the service seamlessly switched to secondary storage instances. Sporadic symptoms persisted for ZixPort due to interactions with the still connected failed SAN pool. Many other subsystems were impacted, with some doing full failovers to secondary infrastructure and materially restoring capability, along with some non-mission critical capabilities failing due to secondary instance not being present or on the impacted SAN pool.

The SAN storage provider was immediately contacted and assigned the failure with high priority by assigning skilled personnel. Our combined teams were able to quickly identify that the event was the result of firmware defect, which to our best knowledge was not known to the SAN storage provider prior to this incident. It was determined that SAN data had not been lost but would need to be migrated to alternate functioning physical equipment to be accessed and used. The team proceeded along that recovery path while also building in parallel alternative/replacement primary database infrastructure (for ZixPort) on the contingency that rebuild might be faster than SAN recovery. During the morning of Saturday November 20, Zix attempted to deploy the replacement ZixPort primary database design and did not succeed. The attempt caused another brief availability event for the ZixPort service which caused us to abort that initiative and continue to focus on SAN recovery.

After the initial outage of the SAN storage through Thursday, November 16, there was evidence that SAN recovery might be enabled in a matter of hours, but as various service outages continued through Friday, November 17, it became increasingly evident that the SAN recovery process was going to continue for an extended period. At that point, software developers were engaged to design a workaround to restore outbound mail flow through the Multitenant Encryption Service (used in Secure Cloud and other encryption service contexts). By mid-day Saturday, November 18, it was determined that the most efficacious solution to restoring all other affected capabilities required disabling the email archiving for our legacy ZixArchive customers (without effecting already archived data). However, Zix's priority is to maintain service for its customers so alternative solutions were investigated to avoid this trade off. Unfortunately, no viable alternative was discovered, and the solution was deployed at approximately 3PM (Central) Sunday, November 19. At that point, the Multitenant Encryption functionality was fully restored. Immediately following the restoration of mail flow for the encryption services, software developers started designing a solution to restore the impacted Legacy Archive service. The solution was placed into production Monday, November 20.

On Wednesday, November 22, and after multiple difficult failed attempts, the teams achieved full recovery of the SAN data. On Friday, November 24, the Software Development team selectively marshaled deployment of selective server-enabling data from the recovered SAN pool to mitigate multiple secondary service impediments and materially improved the performance of still-existing temporary service solutions.

During the evening of Sunday, November 26, redeployment of major primary systems, enabled by the recovered SAN pool, successfully began. IBM DB2 HADR (High Availability Disaster Recovery) systems, which had been out-of-service for many days, required extensive activity data storage redundancy re-alignment and complex, sequenced recovery procedures. A two-step process (executed Tuesday, November 28 and Wednesday, November 29 evenings) for ZixPort primary instance recovery resulted in recovery of full resiliency for that service by 9PM (CST) on Wednesday, November 29.

Timeline in GMT

- 11/16/2023 02:30:00: Event Start.
- 11/16/2023 03:16: Sev1 raised for ZixPort outage. DBAs, Integration, and NetEng teams begin investigating.
- 11/16/2023 02:30: Issue Identified.
- 11/16/2023 13:01: SM9 Incident Open.

- 11/16/2023 13:16: A request to escalate this ticket to a Major Incident has been submitted.
- 11/16/2023 03:23: ZixPort is reported to be currently stable on secondary db2. NetEng team are in process of rolling back router upgrade.
- 11/16/2023 04:32: ZixPort is intermittently available. Internal teams are still investigating.
- 11/16/2023 05:44: ZixPort is believed to be up and stable and Severity status is lowered to SEV2. Teams continue investigating.
- 11/16/2023 07:55: Issues are observed with the reporting database and INT team is working to restore the reporting database.
- 11/16/2023 09:00: INT team is working to restore impacted services.
- 11/16/2023 11:30: INT/NetEng/DBA teams are investigating new and recurring ZixPort intermittency reports.
- 11/16/2023 13:22: The service is degraded. Zix SAN Storage issue in Zix Dallas Data Center. This is impacting ZixPort, Hosted Enterprise and Hosted SMB services. Teams are engaged and investigating further.
- 11/16/2023 13:31: ZixPort status remains intermittent. In addition, Zix Hosted Enterprise and ZixSMB services are impacted, and internal resources are unavailable or delayed. Additional escalation is requested, and all required resources are investigating.
- 11/16/2023 16:09: The service remains degraded. Team identified storage ports connecting to the network switch is flapping. Team has opened a high priority case with Vendor (SR 3-34891245838) and waiting for further instructions. All the teams remain engaged on the call. It was determined that the following services were impacted: ZixPort, Hosted Enterprise, Hosted SMB services, Secure Cloud encryption (multi-tenant).
- 11/16/2023 18:46: Service is degraded. Vendor's engineer is engaged. SMEs are working with Vendor to determine the root cause on a separate call.
- 11/16/2023 19:51: As ongoing issues persist for the SAN storage array, per CloudOPS Engineer; we are going to switch mail flow for both SMB and MT to Atlanta DC only.
- 11/16/2023 19:55: Per CloudOPS Engineer: pool5 (all SSD) may be part of the issue. It is degraded but one disk needs to be replaced. The log drives will have to be replaced. The drives may need to be reset 20 minutes apart in pool5 to prevent a re-silver of a lot of drives at once.
- 11/16/2023 21:06: Service remains degraded. SMEs are engaged on a call with the vendor. Team switched mail flow for SMB and MT to Atlanta Data Center as there were hardware issues identified. Teams are reviewing required changes to the impacted storage to recover the service.
- 11/16/2023 21:54: Per NOC Technician: Update - Mail flow for our encryption services is being redirected to our second data center to assist with the slowdown of mail in our primary. ZixPort access is still being affected and we believe is related to the SAN issue that is currently ongoing. Our engineers are working with the 3rd party vendor of the SAN to rectify the situation. Information will be updated as it becomes available. Adding Secure Cloud Encryption Services (AEE/ZEE) to the affected systems. The configuring of new domains added to the domains is impacted.
- 11/16/2023 22:20: Per Support Staff: Our Engineers and Vendor appear to have isolated the issue to a pool of drives within a SAN that require a reseating to reset them. Our engineers are in a meeting with OT leadership to decide the best course of action to minimize the impact to the customer even further.
- 11/16/2023 23:07: Service is degraded. SMEs with Vendor have isolated the issue to be with a pool of

drives within SAN. Teams are engaged to decide the best course of action to minimize the impact to the customer even further.

- 11/17/2023 00:53: Per NOC Technician: Vendor is shipping (5) - 3.2 TB drives to be here tomorrow by 10:30 am CST (16:30 GMT 11/17)
- 11/17/2023 01:22: Service remains degraded. Drives have been reseated, and SMEs are actively working with the vendor to address the issue.
- 11/17/2023 03:58: Service remains degraded. SMEs removed Pool5 from the storage controllers to isolate the issue with that storage pool and exported the bundle logs to be sent to the Vendor team for analysis. The team is currently working on bringing some services back up and plans to reconvene with Vendor support at 12:00 AM EST (17:00 GMT) to review the initial results of the log reviews.
- 11/17/2023 04:03: Update from CloudOPS Manager:- Team have removed pool5 from the storage controllers to isolate the problem with that storage pool and are exporting the bundle logs to be send to the Vendor team for analysis. SME's currently bringing some services up and will reconvene with Vendor support at 12:00 AM EST to go over the initial results of the log reviews.
- 11/17/2023 12:24: The call with Vendor support reconvened at 11:00 GMT on 11/17. Teams continue to work with Vendor support to recover from this issue.
- 11/17/2023 12:24: Update from CloudOPS Manager: New Update, the team got together today at 6:00 AM EST with Vendor and are attempting to restore the data out from the pool5.
- 11/17/2023 14:03: Indications from Enterprise ZixPort customer base that ZixPort operation has materially improved.
- 11/17/2023 16:55: Many non-ZixPort services still degraded. The copying of data to another pool is in progress The replacement drives have been received at the office and are being brought to the datacenter. Teams remain engaged on the call and continue to troubleshoot.
- 11/17/2023 23:37: Services and resources remain degraded. Replacement hardware continues to be utilized for data copying and will be reintroduced when complete. The Zix engineering team continues to work in conjunction with the Vendor’s, engineering team, directly on a support call. Updates to be provided as we are made aware.
- 11/17/2023 23:41: Per Zix Support: Our engineers continue to work on the issue with vendor engineers. They currently are in a crucial part of the data copy to a new pool from the old pool of drives. Once this has been completed, the engineers will swap out damaged drives and finally start the copy back once the drives are tested. There is no ETA for this action.
- 11/18/2023 00:19: Per CloudOPS VP: The Zixport DB is still copying. It is 640gb in size, but looks like it needs to copy the full LUN which is 2 TB - we are at about 45%. At least 2-3 hours of data copy for that. The good part is; it's moving - it is a critical piece. The Rsyncs are being worked while the DB is being copied. VM files are being re-pointed we are making progress, but I think we need to expect to be here for at least another 6-9 hours – best case. Once we get the DB copied then we can put full attention to getting the VM's up. I don't believe they need to be copied back to new disk.
- At this time, Secure Cloud ETP is considered fully restored.
- 11/18/2023 02:21: Services remain degraded. Team is in the process of completing the copy of the Data (5th LUN). Although the progress is slow, it is advancing. Teams continue to work with Vendor’s engineering team to recover from this issue.
- 11/18/2023 04:26: Services remain degraded. Team is actively working to complete the copy of the largest LUNs, nearing completion at 94% and the synchronization of images for the 20VMs is ongoing, with

increased concurrency to enhance overall throughput. Teams continue to work with Vendor's, engineering team to recover from this issue.

- 11/18/2023 05:43: Service remains degraded. LUN copy successfully completed. Team is working at running parallel Rsync of critical NFS mounts/VM images at the moment. Call continues with Vendor and Engineering.
- 11/18/2023 06:36: Service remains degraded. All remaining rsync processes are currently underway, and the team expects them to run for a couple of hours. CloudOps Eng will monitor the progress and provide status updates while the rest of the team plans to take a few hours of rest until the copying is completed. They will notify the team if the processes conclude earlier than expected; the target completion time for the team is approximately 4 hours.
- 11/18/2023 10:53: Service remains degraded. Rsync process is still underway. Vendor being re-engaged by the team to provide additional guidance.
- 11/18/2023 12:25: Service remains degraded. Rsync process is still underway and progressing. Some teams remain engaged on Zoom call with Vendor as extended teams perform integrity checks and other required VM functions.
- 11/18/2023 15:33: Service remains degraded. Rsync process still underway (approx. 60% complete). The team is working through booting up one of the VMs now. The goal is to get the rsync part of the recovery process completed by early afternoon. Teams continue to work with Vendor resources.
- 11/18/2023 19:51: Service remains degraded. Rsync process is still underway. QA team has successfully run sanity and feature testing on Enterprise ZixPort portals with no defects being identified. ZixPort is now considered fully restored pending customer validation. The recovery team continues working with Vendor resources.
- 11/18/2023 23:38: RSync process is still underway. One key Enterprise ZixPort customer has fully validated following our sanity and feature testing. The team also reports that the majority of services have been restored for customers. The recovery team continues work on infrastructure stabilization. At 23:43 ZixPort service is reported to be stable based on functional tests.
- 11/19/2023 04:14: Another round of data replication is being initiated while also cloning the database server. As these efforts progress overnight, the call is being adjourned until 13:00g on 11/19, providing an opportunity for rest. There will be no further updates until the call is reconvened unless there is a significant event.
- 11/19/2023 14:58: It is indicated that a majority of the services have been restored. Zix engineers are working to restore remaining services.
- 11/19/2023 17:21: Cloning of the database server is progressing and is now 79% complete. The team is in the process of rebuilding the Cuckoo server utilizing a clone from the staging environment which is 45% complete. Work continues on restoration of VMs that had their VMDK files Rsync'ed to from the failed pool. Rsync of the filesystems are still progressing.
- 11/19/2023 22:31: A rebuild of the second DB2 server is progressing (new ZixPort primary). The cloned server is up and running and the database dump/restore is in process. ETA for completion has been extended to 9gmt on 11/20. ETP workaround is in place however outbound mail flow for MSP is held because the new process does not inject a header required by subsequent systems. Engineering is working on a hotfix, ETA not yet available. Legacy Cuckoo is now up and we continue to work on ST Cuckoo.
- 11/20/2023 03:41: The rebuild of the second DB2 server is progressing. The server is up and running and the database backup/restore is in progress. ETA for completion has been extended to 17:00 on 11/20. The ETP workaround is in place and outbound mail flow for MSP is now also working. The team is continuing to work all avenues to restore service. The call is adjourned and will reconvene at 12:00 on 11/20. There will

be no further updates until the call is reconvened unless there is a significant event.

- 11/21/2023 01:00: At this time, Legacy Archiving feed and Legacy Email Thread Link Protection services are fully restored.
- 11/22/2023 15:00: Internal tools and VMs for Legacy Threat and Legacy Archive Search are restored.
- 11/22/2023 16:00: SAN data recovered but kept offline to avoid conflicts with multiple replacement workaround services that have been necessarily deployed.
- 11/24/2023 18:00: QA reports significant removal of remaining customer-facing service weaknesses after selective deployment of recovered SAN data and related services. At this time, services were restored for ZixSMB, ZHE, Legacy Email Threat, and Legacy Archiving.
- 11/25/2023 16:00: Legacy Email Threat and Legacy Archiving are fully restored.
- 11/27/2023 (Sunday Evening) 02:00: CloudOPS/DBA team start recovery operations for IBM DB2 redundancy-enabling subsystems.
- 11/30/2023 (Wednesday Evening) 03:00: ZixPort IBM DB2 redundancy/resiliency subsystems are restored per CloudOPS/DBA team.
- 12/01/2023 05:30: DB2 resiliency is restored on all subsystems.

Resolution

Recovery and Replacement Efforts
A decision was made to migrate the data located on the affected device to an alternate location for access and use. It was also determined that rebuilding the primary database on new equipment instead of repairing existing equipment could expedite recovery. Restoration efforts for the impacted storage devices began in tandem with the build of replacement devices.

Replacement Device Implementation Unsuccessful
The deployment of replacement devices on November 20, 2023, was unsuccessful and resulted in a brief service disruption. This initiative was abandoned, and recovery of the impacted devices continued.

Recovery of Encryption Functionality and Legacy Archive Service
Teams investigated workarounds to restore outbound mail flows. On November 18, 2023, a workaround was deployed, and encryption functionality was restored. A solution to restore the impacted Legacy Archive service was implemented on November 20, 2023, at 03:00 PM CST.

Data from Impacted Storage Device Restored
Full data recovery from the storage device was achieved on November 21, 2023. On Friday November 24, 2023, data from the recovered device was selectively enabled to improve the performance of existing temporary service solutions and mitigate further service impact.

Redeployment of Disaster Recovery Systems
On November 26, 2023, redeployment efforts began, and were successfully completed. Restoration of high availability disaster recovery systems required extensive realignment and sequenced recovery procedures. Recovery of full resiliency for the ZixPort primary service instance was completed on at 09:00 PM CST, on November 29, 2023.

Recovery of all remaining databases and internal systems were completed at 11:30 PM CST on December 1, 2023.

Action Plan

No.	Task	Status
1	Improved email data management by implementing subsystems which couple Legacy Archive and Outbound Filtering in outbound email encryption service paths.	**Complete**
2	Replaced the previous outbound filtering subsystem for email encryption with a more redundant/resilient functional alternative.	**Complete**
3	Restore all impacted services to original state of readiness and resiliency.	**Complete**
4	Conduct an infrastructure audit and a review of issue disaster recovery procedures. Develop an implementation plan for the identified enhancements/improvements.	**In progress** **Target complete December 2023**

About OpenText

OpenText enables the digital world, creating a better way for organizations to work with information, on-premises or in the cloud. For more information about OpenText (NASDAQ/TSX: OTEX), visit opentext.com.

Connect with us:

OpenText CEO Mark Barrenechea's blog

Twitter | LinkedIn