中國銀行澳門分行災備建設簡介

龔存
中國銀行澳門分行
資訊科技部
系統運維團隊
Email: gong_cun@bocmacau.com

Abstract—銀行信息系統的安全運行是金融業穩定運行和長遠發展的基礎，并關係到民生和社會穩定，做好災難備份體系建設是銀行業信息安全的重要保障和關鍵環節。本文主要介紹了中國銀行澳門分行在金融業務多元化發展、IT 應用環境日趨複雜的情況下，如何通過技術和架構的演進，將災備建設從業務種類單一的災備外包服務，發展成涵蓋本地所有重要系統的云數據中心，並對未來的進一步發展提出了建議。

1 背景

中國銀行澳門分行（以下簡稱澳門分行）是澳門特區的發鈔行、政府公庫代理行、人民幣業務清算行，主流業務約占本地市場份額的 40%，因此澳門分行的災備建設不僅保障了本行業務的可持續性，對特區經濟的穩定和信息化建設都有重要的參考意義。

澳門分行自 2009 年開始啟動開放平台災備建設，其中歷經了 2009 ~ 2016 年災難恢復外包，2016 ~ 2017 年災備機房自建和部分災備系統遷移，以及 2017 ~ 2018 年大規模災備系統建設等三個階段，每個階段均得到了澳門分行行領導及各部門的大力支持，以下將詳細介紹這三個階段的災備架構和技術演進。

2 技術演進

在災備恢復方面，RTO 和 RPO 是業界公認的衡量災備系統的兩個重要指標 [1]：

- RTO（Recovery Time Objective）即恢復時間目標，指災難發生后，信息系統從停頓到必須恢復的時間要求。
- RPO（Recovery Point Objective）即恢復點目標，指災難發生后，數據必須恢復到的時間點要求。

RTO 和 RPO 實際反映的是業務連續性目標和數據一致性目標，澳門分行各個階段的災備架構和技術演進，都圍繞著這兩個目標展開。

2.1 災備外包服務（2009~2016）

澳門分行 2009 年 7 月開始啟動開放平台災備建設，與 IBM 簽署災備外包服務，由 IBM 提供災備場所、硬件設施、通訊線路等資源及服務（Business Continuance Recovery Service, BCRS）。災備中心位於澳門氹仔的澳門電訊（以下簡稱 CTM）機房（由 IBM 向 CTM 租用）。災備中心成立之初只覆蓋櫃員終端、網上銀行等基本交易系統，之後又陸續增加了人民幣清算系統、證券系統等重要業務系統。

由於澳門分行主中心和備份中心之間的專線帶寬只有 100 Mbit/s，因此主中心和備份中心之間的存儲複製採用了 Global Mirror with Change Volumes (GM/CV) 技術，GM/CV 是一種異步存儲複製技術，源存儲通過 CV 週期性地複製增量數據，而目標存儲通過 CV 為上一個週期保留完整增量數據。假如災難發生導致存儲複製中斷，且數據不一致，目標存儲將可以通過 CV 回滾到最後一次檢查點，以保證數據一致性。因此理論上 GM/CV 的 RPO $\leq 2 \times$ Cycle，由於帶寬受限，週期 Cycle（默認為 10 分鐘）實際是一個變值，假如數據量較大（如夜晚批處理作業時段），一次 Cycle 可能需要數小時，這樣 RPO 就有可能達不到業務及監管要求。

這個時期的切換演練難度很大，主要體現為：

1) 系統切換后有大量手工配置要進行。為了縮短 RTO 時間，我們盡量將所有數據包括操作系統都通過 GM/CV 遠程複製到災備中心，但要讓操作系統在不同型號和配置的硬件上啟動，需要做很多適配，甚至有一些老版本操作系統不支持在不同設備上直接啟動，需要做一些特殊處理。
2) 完成系統啟動后，由於 RPO $\neq 0$，應用還要進行數據和交易一致性檢查，修復應用啟動中的種種問題。
3) 由於主中心和 CTM 機房的網絡獨立，生產系統切換到災備中心后，網絡需要做大量調整，如地址轉換、防火墻開通等。

由於切換難度大，不僅造成了 RTO 較長，而且在演練回退時也帶來一定的風險，如存儲複製的方向，路由和防火墻要重新調整等。

2.2 災備機房自建（2016~2017）

隨著加入災備的重要系統不斷增加，IBM 所提供的災備場所無論服務器還是實際操作的空間都已經不能滿足要求，澳門中銀于 2016 年啟動了北安災備機房自建工程，將位於氹仔的北安倉庫改建為災備機房（以下簡稱北安災備中心）。是次自建的目標是：

1) 為業務系統進行可用性分級，將本地重要災備系統新建或遷移到北安災備中心。通過業務恢復需求評估，對於缺失 DR 能力的系統，到底多大程度地影響本地重要業

務的連續性，并在北安災備中心建設過程中彌補缺失的環節。

2) 重新進行架構設計，簡化災備操作步驟，縮小 RPO、RTO 時間。在滿足災備需求的基礎上，盡量複用資源，提高投資回報率。

2.2.1 業務影響分析

業務影響分析（Business Impact Analysis, BIA），包括：

1) 業務可用性分級
澳門分行通過合規部牽頭，統籌各業務部門評定業務系統可用性等級，科技部對於分級過程及結果給予技術評估和反饋意見。
2) 業務關聯分析
根據業務可用性分級，櫃員終端、網上銀行、證券投資、支付清算、移動應用等系統具有較高的優先級，但實際上，有些系統可能會在業務可用性分級中遺漏，但卻和重要業務系統之間有很大的依賴關係，從而影響到重要業務系統的可用性。這就需要通過業務關聯分析進行補充。

澳門分行由業務和科技部門共同參與，針對典型場景和重要交易，分析清楚每一筆交易從業務發起到結束所經過的所有環節，梳理出重要業務系統及其支撐系統共 24 個。由於這些復合系統間交互多且複雜，必須進行災備架構的重新設計。

2.2.2 架構設計

如前所述，新架構的目標是減少災備方案複雜度，縮小 RPO、RTO 時間，同時在滿足災備的基礎上，盡量複用資源，提高投資回報率。為實現這個目標，最自然的方案就是通過在數據鏈路層打通網絡，將生產中心的網絡直接延伸到災備中心，這樣網絡架構的簡化不僅將減少 RTO 時間，同時對應用架構和交互關係的影響也會減至最低。同時，並且利用兩中心之間的高帶寬線路，做同步存儲複製將 RPO 減至最低。

我們通過以下步驟來實施以上方案：

1) 租用多條寬頻專線，通過光纖通訊技術，提高帶寬傳輸率。目前主中心機房和北安機房之間承載 2 條帶寬為 10gib/s 的網絡光纖和 4 條帶寬為 8gib/s 的存儲光纖：

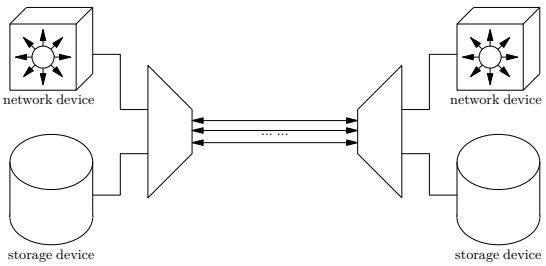

圖 1: 通訊架構

生產和北安災備中心的地理距離約 3km，線路距離約 10km，兩端的往返延遲（round-trip times, RTT）≤ 0.1ms。

2) 實時存儲複製：當生產和災備中心實現高帶寬低損耗傳輸后，對於重要系統，使用實施存儲複製（Metro Mirror, MM）代替異步存儲複製，使得 RPO 降為 0。由於同步存儲複製的寫操作（Write）需要異地存儲的 Ack 同步確認，因此同步存儲複製對性能會產生一定的延遲影響（在“效能”章節將分析影響）：

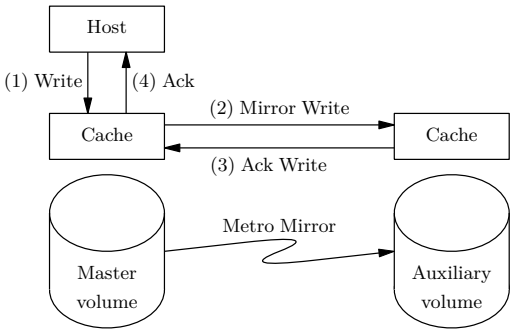

圖 2: 實時存儲複製

3) 通過 Cisco 疊加傳輸虛擬化（Overlay Transport Virtualization, OTV）技術在數據鏈路層（Data Link）打通生產和災備中心網絡連接。OTV 是一項“MAC in IP”技術，通過使用 MAC 地址路由規則，提供一種疊加（overlay）網絡，能夠在 IP 層建立二層連接的虛擬隧道：

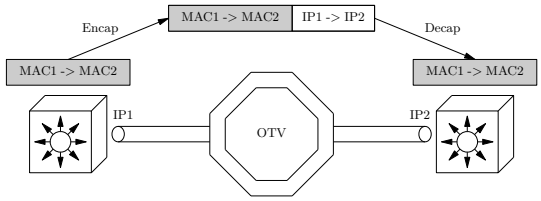

圖 3: OTV 架構

實現網絡二層打通之後，針對災備的網絡配置如 IP 路由等大大簡化，也為種種依賴于二層網絡連接的集群應用或虛擬化技術等打下了基礎。

4) 通過二層和三層網絡連接組合實現部分組件的雙活。並不是任何類型的網絡都必須打通二層連接，比如面向互聯網服務請求的 Web 服務器。由於前期應用系統已經將處理互聯網請求的 Web 服務器、處理業務邏輯的應用服務器以及進行數據處理的數據庫服務器等進行了合理分層，因此我們通過在災備中心新增面向互聯網的 Web 服務器，并和生產中心的應用服務器進行三層連接，通過全局負載均衡器派發請求，就已經在 Web 層達到了生產和災備多活。全局負載均衡器（Global Traffic Manager, GTM）通過向已知頁面發送 HTTP/HTTPS 請求來監控是否正常工作，并動態派發 DNS 和 Web 請求。如下圖所示，當正常運行時，位於災備中心的 Web 服務器也能處理應用請求：

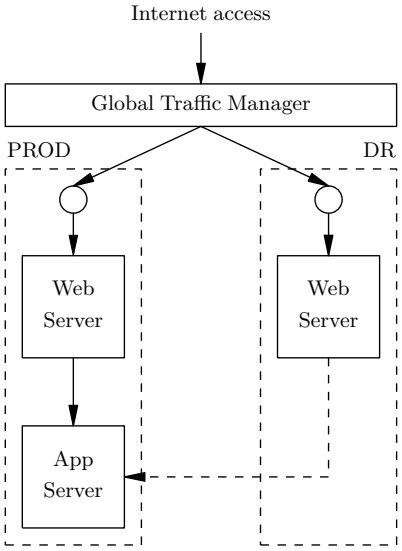

圖 4: GTM(Normal)

當啟動災備時，應用服務器將通過存儲複製在災備中心運行，全部應用交易將發生在災備中心。

2.2.3 效能

根據以上架構，效能的考量主要在於生產中心和災備中心之間存儲複製或網絡傳輸對應用造成的延遲影響。圖 5 是通過不同的塊大小（block size）寫 2GB 文件，遠程同步複製下的磁盤 I/O 和本地磁盤 I/O 的對比。可以發現，隨著 block size 的增大，傳輸速率也隨著增大，雖然兩者的差距也隨之增大（遠程複製要比本地慢），但並不是一個嚴重的問題，因為當文件大小固定（2GB）時，block size 越大，傳輸的次數越少，網絡傳輸的序列發送時延就越明顯 [2]。實際數據傳輸並不是固定大小的數據塊，而應視為沒有起始也沒有結束的數據流，對於 TCP 或光纖傳輸而言，只需要一個足夠大的滑動窗口來提供最大的吞吐量，就可以抵消滯後效應。這就類似於實況足球轉播，雖然電視轉播和現場觀看有一定的延遲，但電視觀眾看到的比賽仍然是流暢的。

針對主機房和北安機房之間的長肥網絡（Long Fat Network，LFN），我們從以下幾個方面來提高效能：

1) 通過調大 TCP 的 *receive buffer* 及光纖通道的 *buffer credits* 來擴大滑動窗口。只要在滑動窗口內接收到對方的確認報文（Ack），就可以將滑動窗口不斷向右推進，從而形成一條不間斷流水線，避免停等帶來的時延，從而提升吞吐量：

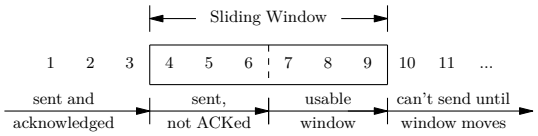

圖 6: 滑動窗口

2) 由於長肥網絡 LFN 內的分組丟失會使吞吐量急劇減少，數據接收和發送方應盡量開啟有選擇的確認（Selective Acknowledgment，SACK），有利於提高重傳效率，提高傳輸性能。
3) 對於關鍵應用，適當調大主機 CPU 以減少處理時延。

2.3 云數據中心（2017~2018）

當實現了網絡二層打通之後，就可以在生產和災備中心之間使用各種依賴于二層網絡連通的虛擬化技術，比如 IBM Live Partition Mobility (LPM) 技術或 VMware VMotion 技術，這兩種技術都允許在共享二層網絡和存儲的物理服務器之間，動態遷移其上運行的虛擬服務器，并保持進程、內存及網絡狀態的一致。因此如果將遠程同步複製的存儲合併為一個虛擬的共享存儲，并同時掛載在生產和災備服務器上，就可以實現生產和災備中心之間應用系統的動態遷移。通過 IBM SAN Volume Controller Stretched Cluster (SVC-SC) 技術，可以達到這一目的：

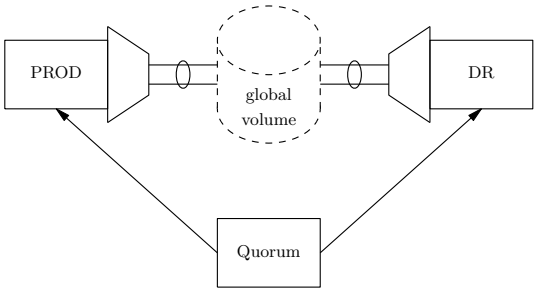

圖 7: SVC Stretched Cluster

如上圖所示，SVC-SC 將圖 4 所示的顯式複製的生產和災備磁盤，變為隱式複製的鏡像卷（Mirrored Volume），一對鏡像卷作為一個虛擬磁盤同時掛載給生產和災備服務器，這種冗餘性保證了無論生產還是災備任何一個位置丟失了磁盤，另一邊仍能訪問磁盤。但是，仍然要注意防範當中間線路中斷可能引起的“裂腦”（split-brain）風險 — 如果中間線路中斷，而兩邊均能訪問本地磁盤，就會造成數據不一致。因此，除了為中間線路租用多條不同的 ISP 專線之外，原 CTM 機房改造為仲裁節點，當發生中間線路中斷時，仲裁節點將決定在哪個場所能夠訪問磁盤，并阻斷另一個場所對磁盤的訪問。

SVC-SC 的實現意味著虛擬化的進一步提升，在原有網絡打通的基礎上，生產的某一服務器集群，可以動態遷移其中一部或幾部到災備中心運行，而不會對業務有任何影響，並且在任何時候，生產和災備中心的硬件資源都可以動態調動，真正實現了“災備 = 多活 + 高可用”的云數據中心。

3 展望與總結

從以上的技術演進可以看出，澳門分行在基礎設施架構上做了大量工作，在應用開發基本無需改造的情況下，實現了多活的虛擬數據中心，但仍存在一些問題有待解決。

3.1 通過自動化簡化災備流程

由於 24 個災備系統數量多，系統間依賴關係複雜，大量系統的切換不僅需要手工操作，在組織流程上也有很大難度。多活災備中心在 2018 年底建設實施完成，當年 11 月份進行了完成建設后的第一次災備演練，為了能夠順利實施切換驗證，我們將整體工作步驟分解，并成立多級調度進行指揮協調，其中一級調度負責總體指揮，二級調度負責統籌各團隊的具體實施內容、并對切換中可能遇到的問題進行組織決策。

通過實際演練，證明了多級調度和問題管理機制，對於大規模場景下的的災備演練是非常有效的，但是大量的手工操作，特別

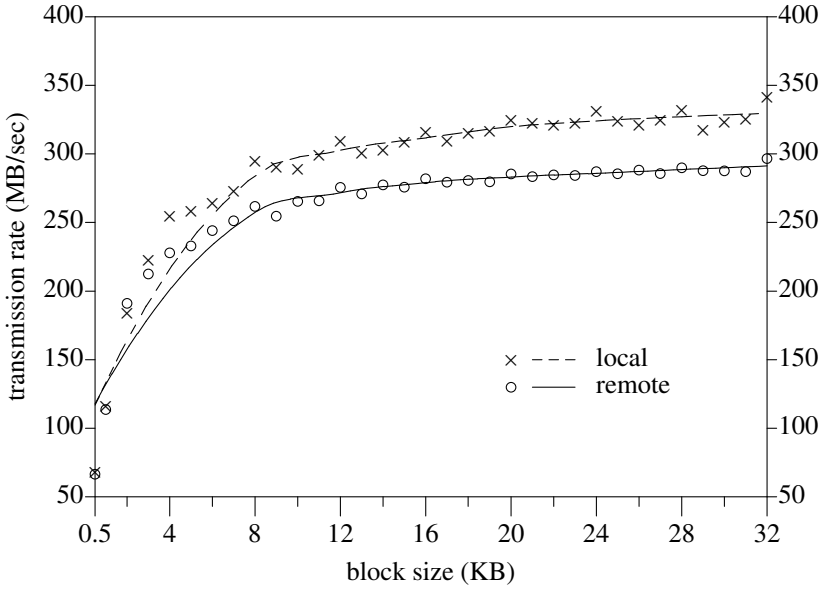

圖 5: 遠程複製下的磁盤寫速率和本地磁盤對比

是應用啟停和對依賴關係的判斷，都非常依靠特定技術人員，不僅影響了 RTO 指標，也影響實際切換的可操作性。因此，未來應該將應用間的關聯關係抽象為以下有限自動機：

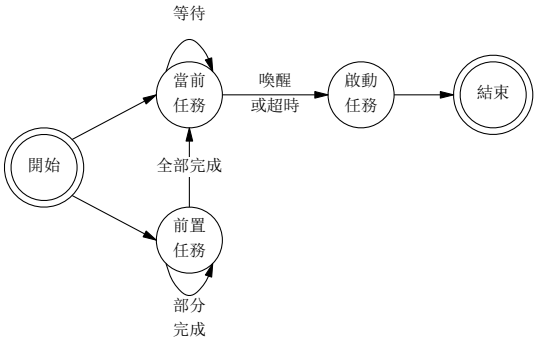

圖 8: 應用啟動狀態圖

藉助腳本或工具，我們可以將有限自動機變為可執行的自動化流程，甚至達到一鍵切換，從而大大較少操作時間和操作風險。

3.2 增強災備監控和應急

由於新架構下的災備中心實際成為了生產中心的延伸，因此在災備中心的監控上需要在未來做進一步的加強，包括對跨中心的網絡和存儲狀態的監控、對災備中心的互聯網入口的入侵防範等，并準備好相應的應急預案。值得注意的是，雖然 SVC-SC 跨域存儲允許任何一個節點丟失對磁盤的訪問，但是一旦丟失了任一節點，意味著圖 2 中的緩存（Cache）缺失，對磁盤的寫訪問將變為 write-through mode，從而影響到磁盤 I/O 效能，因此未來應該考慮通過增加多個 I/O group，當其中某一 I/O group 的單節點失效時，可以動態將磁盤遷移到另一 I/O group。

3.3 向分佈式架構發展

目前的災備架構，雖然虛擬化程度已經達到了云數據中心的要求，但災備切換方案還是基於傳統的主備切換方案。事實上我們應該在圖 4 的基礎上，向全雙活架構發展，特別是數據庫的設計上可以向 Facebook 學習，將數據庫做主副拷貝，生產中心部署主數據庫，災備中心則是只讀副本，發生災備切換時賦予災備中心寫數據庫權限 [3]：

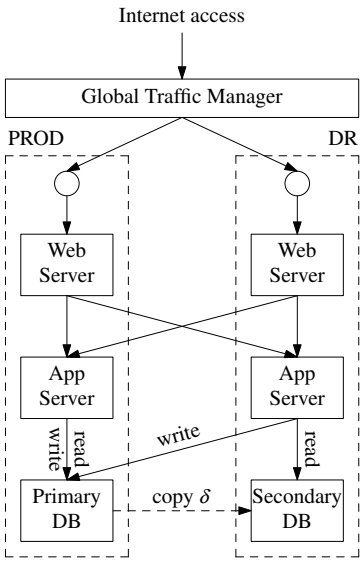

圖 9: 全雙活架構

除了典型的分層架構，云數據中心、基礎設施自動化、虛擬化、容器化的發展，將反哺業務向更細粒度的微服務架構擴展：每種服務都圍繞著具體的業務進行構建，并能夠被獨立開發和部署在不同的數據中心，不僅能夠更好地體現業務邏輯，而且可以充分利用分佈式架構在容災方面的天然優勢，具有更好的反脆弱性。可以預見，未來從災備中心真正轉型到云平台的過程中，架構設計和工程實踐的華爾茲將一直跳下去。

3.4 總結

經過多年努力，澳門分行的災備建設工作已取得長足進步，但仍有提升空間。一是分行內部各部門對災備建設的認識還有待加強，特別是還存在兩個誤區：

1) 對 RTO 和 RPO 這兩個反映業務連續性和數據一致性的基本指標缺乏概念，反映在業務可用性分級上就是要麼沒有任何災備需求，要麼一哄而上，全部定為最高等級，沒有從災難發生場景下用戶面臨的或運營需要的問題來驅動和統籌考慮。這一點科技部在和各部門做業務關聯分析時，逐漸引導各部門建立起了基本認識，但仍然任重而道遠。
2) 認為災備建設的推行是科技部門的事，應該由科技部門獨立承擔。實際上，災備建設不僅是全行上下都應參與的系統工程，而且業務和科技應該圍繞系統的服務級別管理，在成本分析的基礎上，對系統災難恢復的可用性進行評估、實施與管理，並且形成一種服務計費方式，從而更好地保障服務質量。

二是澳門各金融機構間的聯繫越來越緊密，跨機構業務增多，對關係到金融機構自身運行的其他外聯機構的災備建設也提出了很高要求，這些系統的災備建設及災備演練等工作可以由監管部門進行統籌安排。

總之，災備項目建設投資巨大，沒有盡善盡美的方案，只有認真分析實際需求、制定符合自身需求的方案，才能在項目建設費用和效率中獲得平衡并取得預期效果。

References

[1] 中國人民銀行 (PBC), 銀行業信息系統災難恢復管理規範, 中國人民銀行發佈, JR/T 0044—2008, 2008。
[2] W.Richard Stevens, *TCP/IP Illustrated, Volume 3*, 1st Edition, Addison-Wesley, 1996: 附錄 A.3 詳細講述了遲延和帶寬的關係。
[3] Rajesh Nishtala *et al.*, *Scaling Memcache at Facebook*, 10th USENIX NSDI'13, 2013: 介紹了 Facebook 分佈式系統的工程實踐，其中第 5 部分講述了多數據中心部署的主副拷貝，以及如何縮短副本數據庫滯後主數據庫的時間。