私立東海大學資訊工程與科學研究所

碩士論文

指導教授：蔡清檥 博士(Dr. Ching Tsorng Tsai)

以災難復原 RTO/RPO 概念建置校園儲存高可用度(HA)架構

Base on RTO/RPO concept, implemented a campus storage HA architecture

研究生：馬廣智 (Kuang-Chih Ma)

中 華 民 國 九 十 七 年 一 月

摘要

現今，資訊服務必需提供七天二十四小時的服務，即使是計劃性的停機對於資訊人員及使用者都將是負面的衝擊。企業為了停供不中斷的客戶服務便訂立企業永續經營(BC)及災難復原(DR)的計劃，大學校園目前也是提供校內師生全年無休的服務，建置高可用度的目的主要維持資訊系統的正常運作，一旦發生天災、人禍等不可抗拒因素時，能夠迅速恢復系統的有效運作，將有形、無形的災害損失降至最低。

建置等級越高的可用度系統需要的成本愈高，但什麼樣的高可用度等級符合現有資訊系統儲存環境的使用呢？考量到總持有成本(TCO)及投資報酬率(ROI)，並導入衡量災難復原指標的復原點目標 (RPO)/復原時間目標(RTO)，建置高可用度容錯系統，可降低風險、減少管理的人力、以及當障礙發生時導入其它可用的冗餘設備，並且可以避免因災害發生時間拉長，復原資料及系統的成本會愈來愈高。

災難復原是我們最常聽到的衡量標準，建立容許服務恢復正常運作的時間，以及就時間上而論資料損失可容許的數量，而要維持服務不中斷的目標，需投入愈來愈多的成本。以企業為例，為了保護資料達成服務不中斷的目的，投入了大量的成本去建置大型的資料儲存系統與設備來達成此一目標，並且為了預防災難事件的發生，避免將所有的資料集中於特定的儲存設備會因為毀損而無法提供服務，所以發展出階層式儲存架構，讓資

料保存多份副本於各儲存層中，透過此種多層級儲存層的保護，以降低資料無法復原的風險，另外為了避免因資料集中於某地，當區域型的災難事件發生導致所有的儲存設備皆受此災害影響，故發展出備份磁帶異地存放、異地備援，甚至最近討論充份利用資源的異地互援方案，簡而言之，儲存系統欲達成的目標有四項：1.風險最小化；2.投資報酬最大化；3.改善性能；4.增加靈活性。

Abstract

Information offers people whole day service. Even the routine server shut down, it will be negative impacts to IT group and user. Enterprises provide the nonstop service for customer with the disaster recovers Plan to making Enterprises forever. Also the campus built the High Availability server system to offer the stable info service for teachers and students. The expenditure to keep the normal operation of the information system mainly, when such irresistible factors such as the natural disaster, man-made calamity, it can resume effective operation of the system rapidly for the lowest that tangible.

This research passes technology for two directions about storage technology and operation flows improve. We want to do two things on management for improve storage designing and technique improve the performance from the storage SAN network and storage management service center. It improving to store service of the system for more stability and can be recovery easily. Through the method of service level agreement to provide the campus administrator system more effective serve. Through new storage architecture design base on the user requirement and experience of the storage system administrator to define the new service agreements, follow the SOP (Standard Operation Procedure) steps to input the existing storage layers. Through the continuities measuring of Quality index and user department requirements and negotiating to build the most matched for user requirement and resource management solution.

Key word: Business Continuity, disaster recovery, service level agreement, High Availability

目　次

圖示列表

第一章

第二章

第三章

第四章

表格列表

第二章

第四章

第一章 導論

隨著資訊科技的發展，應用的服務愈來愈多，維持服務的穩定及資料的正確性一直以來皆是資訊服務提供的單位所努力的目標。現今，資訊服務必需提供七天二十四小時的服務，即使是計劃性的停機對於資訊人員及使用者都將是負面的衝擊，建置高可用度的目的主要維持資訊系統的正常運作，一旦發生天災、人禍等不可抗拒因素時，能夠迅速恢復系統的有效運作，將有形、無形的災害損失降至最低。

企業要提供不停機的服務分會擬定災難復原(DR)或企業永續經營(BC)計劃[1]，實施營運衝擊分析(BIA) [2] 評估，針對整個企業及 IT 所面臨的弱點再做詳細的檢查，什麼是可能的威脅、以及引發的後果(損失)。災難復原是我們最常聽到的衡量標準[3]，建立容許服務完全恢復正常運作的時間, 以及就時間上而論訂定資料損失可容許的時間間隔，而要維持服務不中斷的目標，需投入愈來愈多的成本。以企業為例，為了保護資料達成服務不中斷的目的，投入了大量的購置成本去建置大型的資料儲存系統與設備來達成此一目標。並且為了預防災難事件的發生，因所有的資料可能集中於特定的儲存設備會因毀損而無法提供服務，所以發展出來階層式儲存架構，讓資料保存多份副本於各儲存層中。透過此種多層級儲存層的保護，以減少資料無法復原的風險。另為避免因資料集中於某地，當區域型的災難事件發生導致所有的儲存設備皆受此災害影響，故發展出來備份磁帶異地存放、異地備援，甚至最近討論的充份利用資源的異地互援方案[4]。簡而言之，儲存系統欲達成的目標有四項：1.風險最小化；2.投資報酬最大化；3.改善性能；4.增加靈活性。

目前儲存技術的趨勢焦點在於降低成本及提高傳輸速度[5]，儲存容量

的增加以及大量的使用磁碟，直接導致了付出的成本愈來愈高，傳統無限制地添置硬體設備的管理辦法，已無法滿足目前的儲存需求。隨著企業重要服務價值的資料不斷的累積，資料損毀帶來的影響日益擴大，企業已無法承受資料損失所帶來的衝擊及客戶服務的中斷，除了加速系統還原的機制以外，還需要更密集的備份還原點來減少資料損失的衝擊。

現今的儲存技術都是以虛擬化(Virtualization)為核心，強化管理，以往儲存或備份的工作都是利用前端伺服器的資源來進行相關工作，目前則逐漸演變為將所有備份的工作整合至後端的儲存設備，透過這樣簡化管理的方式來讓前端的應用伺服器更專職於提供應用服務的品質及穩定度。

1.1 研究動機

當資訊人員在規劃資料保護服務的時候，會引用二項衡量的指標：復原時間目標(RTO, recovery time objective)—容許服務回復正常運作最長之時間；復原點目標(RPO, recovery point objective)—容許資料損失最長之時間。此二項目標是以時間為單位，有周、天、時、分、秒，對於資料的保護當然是以 RTO 及 RPO 愈短愈好，因 RTO 及 RPO 時間愈長代表資料的損失及服務復原時間愈長，需要花費更多的成本於災難復原上面，但相反的若需達到最好的 RTO 及 RPO 標準，需要投入的建置成本極高，如何找出適合現有儲存環境的需求，並循序階段性的強化基礎架構，是比較務實的作法。

上面所提的幾個儲存應用的方式異地存放、異地備援、異地互援等儲存應用，點出現成企業及組織單位所面臨的問題是儲存資料成長的速度，尤其企業要面對競爭、增加營收，絕對無法以現有的資訊服務與架構達成企業所訂立的營運目標，必需持續提供創新的服務，才能吸引使用者持續的消費，挹注營收，在此狀況之下，後端的資料勢必同步持續的成長。儲存

技術也由早期的 DAS、NAS、SAN 等儲存技術進展到階層式儲存架構再往後延伸，一直擴展需求，以階層式儲存為例，當資料量成長需擴充儲存設備時，各個儲存層的設備皆需要擴充。而異地備援的方式，會需要建設主機房及備援機房一比一的複製(Replication)，所以當儲存設備擴充時二地的建置成本也非常驚人。故近年來儲存技術相關的議題也一直環繞在儲存資源管理(SRM, Storage Resource Management)[6]及資訊生命周期管理(ILM)[7][8]等這類強化管理的應用上。

本篇論文主要是以某大學的校園資料儲存中心為研究對象，因學校機關並不像大型的企業能夠提供大量的預算來採購大量的儲存設備，必需要以有限的預算來達成最大的使用效益，學校單位的使用者有數萬人以上，有許多的前端應用程式如 mail 系統、校務公文系統、師生資訊系統(考試、選課、註冊、學生成績、學位申請等)、差假考勤系統、帳號認證系統(SSO)、FTP、BBS…等，在有限的資源下一旦遭遇到系統障礙、駭客攻擊、超出系統負荷(儲存容量、系統效能)等問題，導致無法提供服務給使用者，在重要的時刻如考試、選課等重大影響學生權益的活動時，可能影響到數千人至數萬人的權益，另外以實際遭遇的問題為例，因資料量的成長及儲存系統負荷過大，導致儲存系統暫時性的無法再存入資料。基於此需求，思考調整現有的儲存架構，兼顧系統穩定及最佳化的成本效益，將儲存系統資源調整至最好。

本篇論文研究有二個層面的改進，一個是在技術面如何在目前的架構下建置一個高可用性自動容錯的系統，依照 RPO/RTO 規範的目標，以最少的成本達成最高的投資報酬率，透過現儲存管理架構導入高可用度的容錯系統與網路備援，提升整體的儲存基礎架構的品質，另一個層面是在執行面，透過新的儲存改善架構，依照校務系統服務使用單位的需求以及儲存系統管理人員的經驗來訂立儲存服務的層級協議，依照標準化的流程導入至現

有儲存架構最符合效益的儲存階層，經過不斷的服務品質量測以及使用單位對現有使用環境的持續協調，建構出最符合目前需求的解決方案，另外可以針對各別服務訂定出位於不同階層式儲存的位置所適合的 RTO、RPO 目標值，當有持續狀況發生時所有的風險都能夠在掌握之中，並達到資料中心營運持續計劃中所要求的障礙時間目標值。

1.2 論文章節架構

本篇論文的架構第一章主要在探討本研究對象校園資料中心儲存的需求及目標、儲存的趨勢、災難復原的相關討論與作法，第二章介紹有關儲存技術及災難復原指標與高可用度的探討，第三章則是現有儲存系統改善的評估及相關運作的設計，第四章則依據儲存改善計劃進行實作，並針對建置前與建置後提升效益與優點的比較，第五章則是結論與未來研究方向。

1.3 研究步驟與流程

本篇論文的研究步驟由技術面與執行面來進行儲存架構改進的實作，技術方面由儲存技術的改善如儲存技術的提升、儲存空間使用率與效能的提升、災難復原設計、階層式儲存架構、服務可用度與可復原性的強化來進行儲存服務的提升，研究對象資料中心儲存架構目前不足的部分為服務可用度與可復原性的提升，所以依此需求建置高可用度架構。

執行面的部分，由使用單位的儲存需求、系統管理者的維運經驗來建構出適合的儲存服務品質模式，並依校務系統服務的屬性訂立各別服務的 RTO/RPO 目標值，最後再依現有儲存服務的階層式儲存架構進行規劃與導入，並透過使用單位的客訴與相關回饋、持續性的服務品質量測指標，分別訂立各階層的 RTO/RPO 目標值，改善至現有儲存環境的最佳架構。

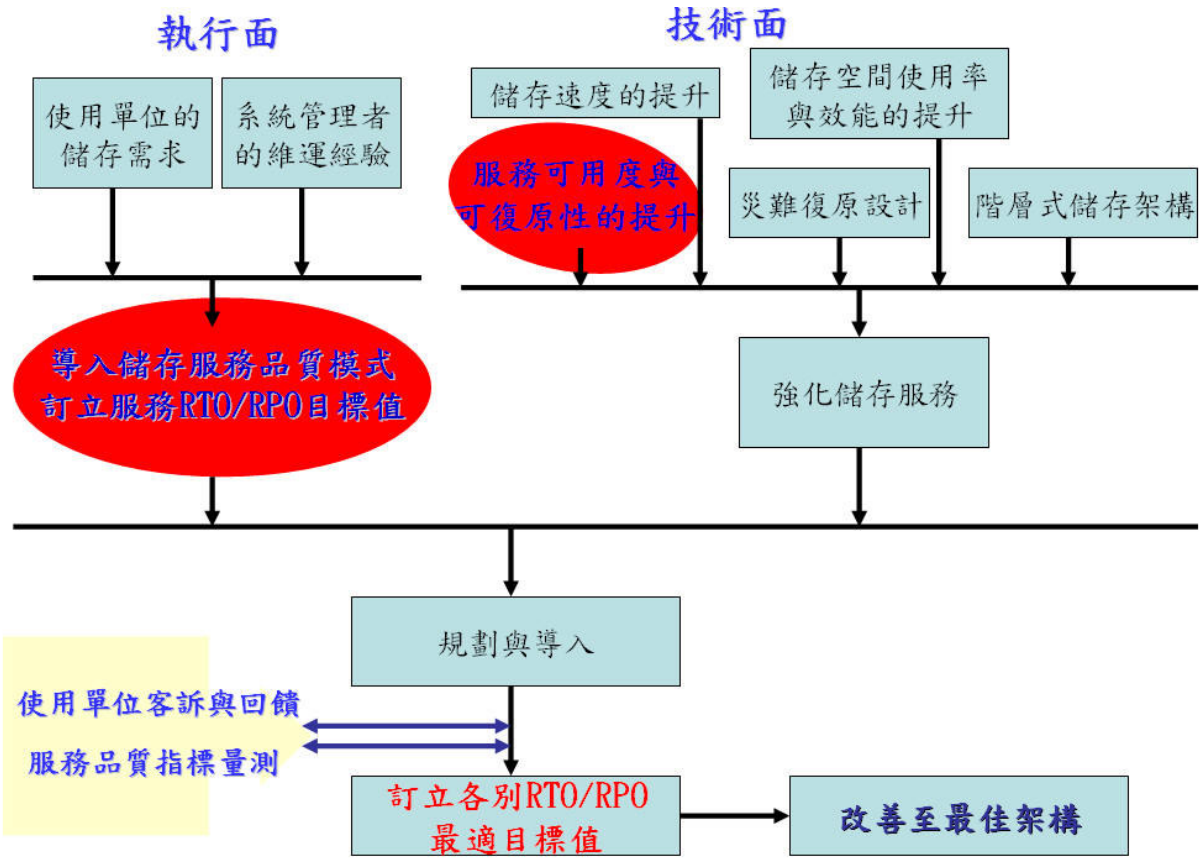

圖 1-1 研究步驟與流程

第二章 相關研究

2.1 儲存技術與指標

儲存的技術的演進由早期的直接連接儲存(DAS, Direct Attached Storage)到網路附加儲存(NAS, Network Attached Storage)、儲存區域網路(SAN, Storage Area Network)及以乙太網路為基礎的 IP-SAN。DAS 儲存成本最低，但難以管理，NAS 的優點是容易建置，在現有網路下即可運作，價格性能比佳，但缺點是速度及資料分享皆不及 SAN 優良，也無法處理需要運算的資料，SAN 的優點是速度快、分享性佳，目前大部份的企業皆採用 SAN 架構，缺點是建置成本高，而 IP-SAN 則是建置在乙太網路下，採用與 SAN 相同的

通訊協定，技術目前仍在發展當中，建置在以上這幾種儲存技術的基礎之下，儲存技術也應用了以下幾種相關的方法，來改善實際環境中所遭遇的問題。

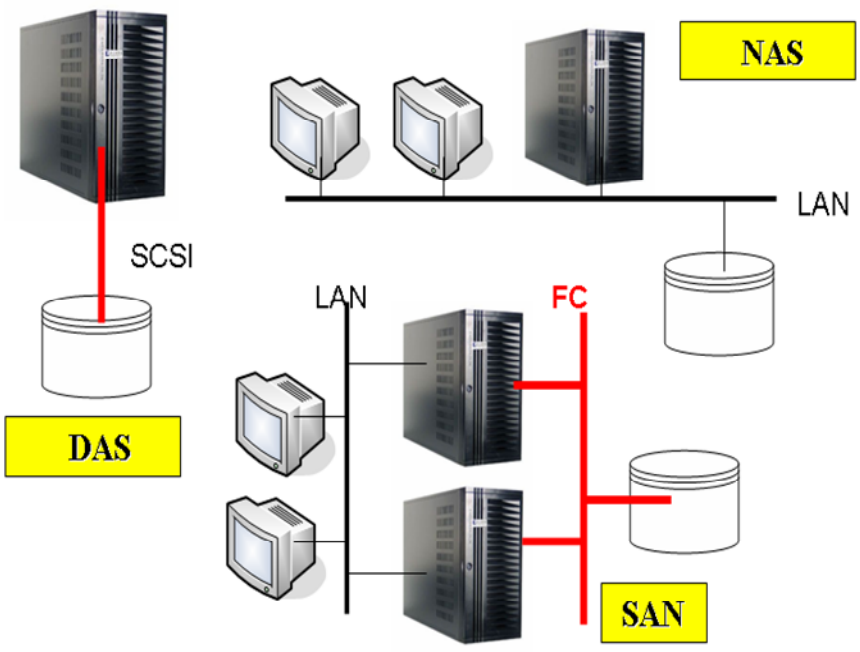

圖 2-1　儲存架構圖示

2.1.1 儲域網路（SAN, Storage Area Network）

儲存區域網路（Storage Area Network，SAN），是指採用光纖通道（Fiber Channel）技術，通過光纖通道交換機連接伺服器主機和儲存陣列，建立專用於數據儲存的區域網路，其優點為將儲存空間統一管理，增加儲存架構的可用性與表現，以大型的儲存需求來看，一般以 SAN 儲存架構為首選。

SAN 是專門連接儲存外圍設備和伺服器的網路，它通常包括伺服器、外部儲存設備、伺服器連接介面、集線器以及網路、儲存管理工具等。SAN 除了綜合了網路的靈活性、可管理性及可擴展性的同時，更提高了網路的頻寬和儲存 I/O 的可靠性，它降低了儲存的管理費用，並平衡了開放式系統伺服器的儲存能力和性能，為企業級儲存應用提出了解決方案。SAN 獨立於應用伺服器網路系統之外，擁有幾乎無限的儲存能力，它採用高速的光

纖通道作為傳輸媒介，FC（光纖通道）+SCSI 的應用協議作為儲存的傳輸協議，將儲存系統網路化，實現了真正高速的共享儲存，同時附帶提到 LAN-free 和 Server-less 的備份原理。

傳統透過 LAN 進行備份還原的儲存架構，備份資料皆是透過 LAN 傳送至備份伺服器後再存入儲存設備，因為這樣的備份方式會增加網路資料的傳輸量同時增加網路負載，而後來也發展出改良式的 LAN 架構，透過另一條 LAN 的儲存網路路徑來進行備份及還原的動作，但是隨著光纖通道技術的發展，傳輸的速度增快，在 SAN 架構下每個儲存設備皆可當作各主機的本地設備使用，每個實體儲存設備透過適當的軟體管理和設定，就可以將儲存設備動態分配給前端各個主機使用，無需再透過 LAN 傳輸，故稱為 LAN-free 備份。

而進行 LAN-free 備份時，資料還是需要通過 FC 讀回到每個應用程式主機，這需要佔據部分的主機資源，而另一種備份的方式則是假設是由備份伺服器發出啟動備份命令傳送給各應用伺服器主機，同時也可以指定後端儲存設備的容量及位置，應用伺服器收到命令後即向 SAN 交換機發出一個稱為擴展拷貝的命令，透過此指令可直接將資料送入儲存設備，因此大量備份資料可以避掉應用伺服器主機的資源，而透過 FC 寫入儲存設備，實現了 server-less 備份。

2.1.2 系統建置與災難復原相關指標

2.1.2.1 儲存服務品質模式(Quality of Storage Service Model)

IT 主管已逐漸體會到管理儲存資料，以及讓各種關鍵商務應用系統持續運用資料所引發的設備購置的高額成本，為了降低大量儲存資料與複雜系統的持有成本，資料中心主管正建置許多新技術，例如像儲存區域網路(SAN)以及虛擬化儲存(Storage Virtualization)，並尋找其它理想工具，讓 IT 員工能有效率地管理持續擴充的環境。儲存服務品質模式 (Quality of Storage

Service Model) ，利用虛擬化的技術建置高度集中化的儲存管理策略可確定資料中心團隊的權責範圍，以滿足不同單位的多元化儲存需求，這種權責規劃，可形諸於正式的服務協議，亦可視為 Quality of Storage Service (QoSS) 儲存服務品質，儲存服務品質模式涵蓋四個考量重點：1.資料的存活能力（Survivability）: 資料的存活能力指的是一種類似“保險”的觀念，保證應用系統的儲存資料在經歷各種錯誤或管理疏失後，仍能回復至可運作狀態；2.回復時間（Time-to-Recovery）: 管理應用系統從錯誤發生後到回復正常所需要的時間；3.儲存容量上線時間（Time-to-Capacity）: 指新增的儲存設備可開始“供應”或指派至特定系統並上線使用所需的時間；4.應用系統效能保證（Application Performance Guarantees）: 確保儲存基礎設備能針對應用系統的需要提供所需的效能。

每項 QoSS 標準皆應配合各單位的應用系統，這些系統我們稱之為”Storage Accounts”，例如入口網站首頁是使用者進入相關系統的進入點，因此需要極快的系統回復時間；財務及會計部門希望確保資料的完整性以及資料可以在遭遇災害後依然能保存，因此需要將資料複本存放在遠端的災難回復備援地點，提供 Storage Account 所建置的 QoSS 愈高，供應這些服務的相關成本亦更高，管理這些 Storage Account 的重要元素明確定義出各種權責範圍與處理方法，規範儲存資料的安全性以及每個 Account 儲存資源的總持有成本。

2.1.2.2 復原時間目標(RTO)與復原時間點目標(RPO)

資訊或服務復原的時間點(RPO, Recovery Point Objective) 或是資訊或服務復原的最長的時間(RTO, Recovery Time Objective)，也就是重新啟動服務所需要的時間，簡而言之，此二項指標皆是以時間單位的長短為衡量標準，目標時間愈短代表可用度愈高，RPO 取決於現有系統的備份周期，備份周期愈頻繁 RPO 需時愈短，RTO 取決於系統處理障礙回復的時間，系統能夠

自行恢復或切換至其它可用系統或人員介入處理愈快，則 RTO 需時愈短。企業會以這二種指標，參考並訂立資料保護的政策，參考 SNIA 這個組織以 RTO 及 RPO 為基準對可用度的量測方式[9]，一般來說 RPO/RTO 所訂定的等級愈低，所需復原的時間愈長且浪費的成本就愈高，而建議的災難復原指標如以 RTO 為基準，若以天為單位，系統復原的指標以現有的全量備份，在系統回復服務後進行重建資料；若以小時層級為例當系統環境回復後以增量備份的資料來進行回復；分鐘級的指標則以重啟服務及依現有系統記錄(log)回復至系統最後可用狀態同時並重建與各個端點的連結；而秒級則是需要能夠主動藉由錯誤偵測並將服務引導至其它可用的備援系統，同時能夠不中斷服務。而 RPO 的備份機制則是與 PTO 的還原機制相對應的，依實際可用的預算及資料儲存的需求資料量來導入符合的儲存技術，若訂定回復的時間要求愈短，所需建置的成本愈高。

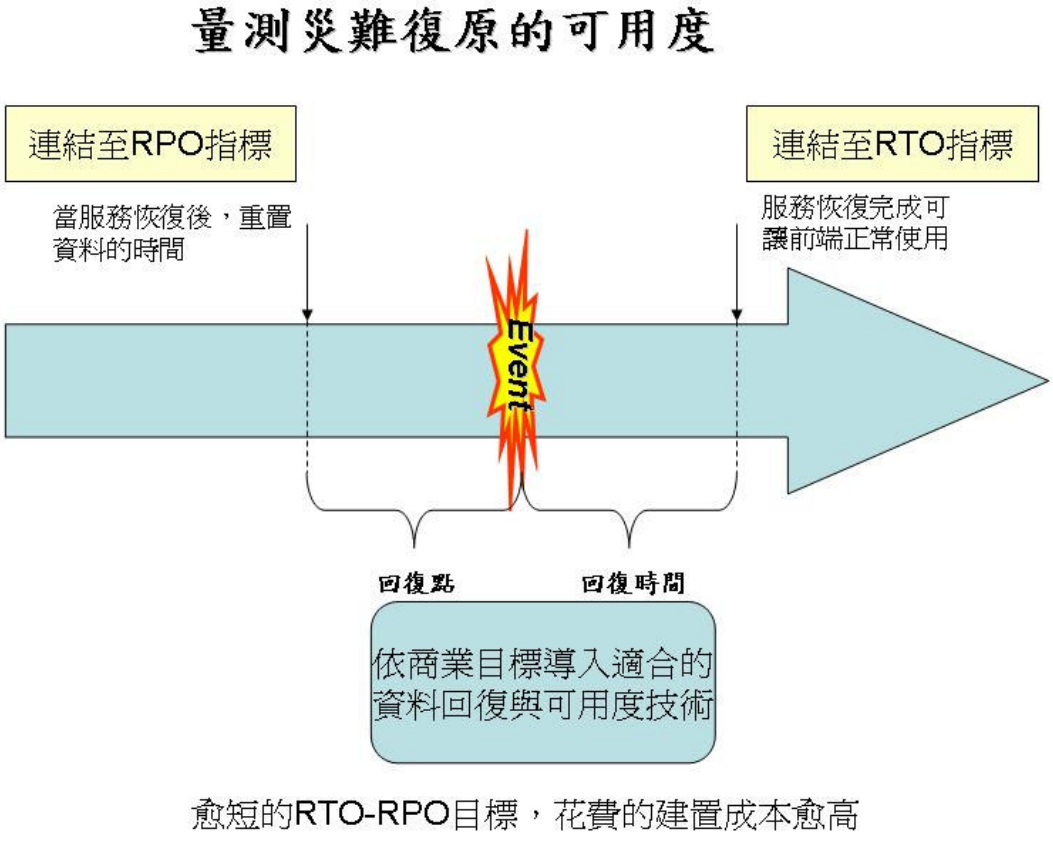

圖 2-2 RPO 與 RTO 示意圖

- 其它儲存系統建置指標：

ROI（Return on Investment）投資報酬率、總持有成本(TCO, Total cost of ownership)這二項指標是企業對於成本及投質報酬率的基本衡量指標。

企業提供愈來愈多的服務，資料的成長是以倍數的方式向上成長，當初資料儲存容量的規劃可能過了幾年之後即將面臨到又需要採購大型的儲存設備，對於企業想要達成降低資產總持有成本的目標而言是背道而馳的。隨著企業資料的快速成長，如何做好資料管理、分享、重複使用、快速復原，以及做好儲存的成本控管這些目標是愈來愈重要，依照資料儲存的四大步驟：捉取、管理、保存、傳遞，保存是需要強化儲存的硬體及軟體設備，一直以來企業都是以此目標進行建置，而強化管理則是目前熱烈討論的議題，相關的議題有儲存資源管理(SRM, Storage Resource Management)、資訊生命周期管理(ILM)…等，參考 HP 對於 ILM 的解讀 ，HP 的 ILM 注重的是企業經營的 4 個階段，從抓取開始、還有管理、保存及最後的傳遞，強化管理將是未來儲存技術的走向。

2.2 備援機制與階層式架構

企業為了分擔經營的風險發展出許多相關的備份應用方式如異地儲存、異地備援、遠端儲存，甚至最近討論的充份利用資源的異地互援機制，另外還有發展出階層式的儲存架構(Hierarchical Storage Management)，以即時性需求，進行資料同步的儲存，此儲存層的成本最高稱為在線(On-line)層；資料的處理為非即時性的需求、進行非同步的資料儲存，可以使用儲存成本較低的儲存媒體進行複製(Replication)、隨機存取、或作所有資料的第二線備份，以達成分散風險，此儲存層的成本次高，稱為近線(Near-line)層；第三層儲存成本最低，可進行完全備份，但缺點是儲存及還原速度最慢，且還原資料的正確性及可用度最低，僅是備份還原的最後一道防線，稱之為離線(Off-line)層。

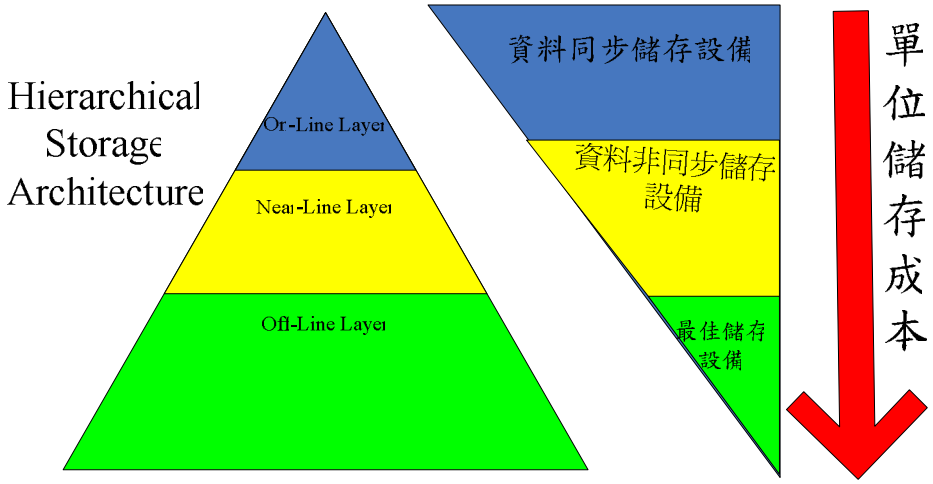

圖 2-3 階層式的儲存架構

階層式備份架構(HSM)的速度是傳統檔案備份及還原速度的數倍，所以對於客戶而言，整個過程不需要管理、不需要參與，完全自動化，而用戶的儲存空間可以由原伺服器上的空間加上二級儲存空間同時構成，當數個應用程式同時在階層式備份架構下使用時，如同每個人都擁有了如此大的空間，對於關鍵的計劃而言，當使用階層式備份架構後，一旦有效空間不足時，階層式備份系統可以將最不常用的檔案移到二級儲存上，保證了應用系統的連續性。

會有 HSM 架構的產生，主要是因為需要分散風險，因儲存架構每一個點(NODE, DISK, NIC, ARRAY…etc)都有可能毀損，對於用戶而言最重要的資料不能毀損。故透過不同成本、不同時間的儲存特性，將資料的副本能多筆的保留下來，當有發生資料毀損，才能一層一層的還原回去，以確保資料的完整及可用性。

2.3 虛擬化技術(Virtualization)

虛擬化(virtualization)[10]是近年來應用程式及儲存設備的熱門話題，大意指企業不需要親臨檢視個別應用程式及儲存設備的運作情形，只要利用軟體就可以將內部與外接式儲存資源匯整成單一虛擬應用或儲存資源。為

了讓應用服務及備份儲存的使用及管理上更方便，所有的服務架構都傾向於虛擬化，透過虛擬化的方式，以應用程式為例，可讓使用者在使用服務時，不需要知道知道目前的工作在那一台伺服器上執行，讓所有提供服務的伺服器能夠有效的整合資源，提高效率及節省成本。而儲存設備的虛擬化則可以簡化前端伺服器的設定，伺服器不需要知道要備份儲存的資料要丟到那一個儲存媒體，這樣可以有效的簡化管理的複雜度，儲存虛擬化讓實體硬碟裝置變成虛擬硬碟裝置，因為虛擬硬碟透過軟體 (OS 上的虛擬化軟體套件或儲存硬體/儲存交換器裡的虛擬化firmware)處理而產生，它比硬體裝置容易操作，使用者可以動態地改變硬碟大小(online disk resizing)、做檔案系統快照(snapshot)、硬碟遠端複寫(replication)等，Virtualization 的運作原則不難，它把實體的硬碟以虛擬化儲存目標 (virtual storage target) 匯出給伺服器，虛擬硬碟的大小、數量，甚至QoS (Quality of Service) 都不必跟實體硬碟的一樣，Client (伺服器、工作站、桌上電腦、等) 可以用不同方式存取這個虛擬硬碟，虛擬化的好處可顯著提升存取效能、提升資料可用性、節省儲存空間成本及降低管理的複雜度。這樣的技術讓前端可以方便的存取，而後端可以更有效的來管理，透過虛擬化的技術應用於儲存系統上，對使用者而言當有檔案搬移的需求時，整個檔案的遷移對於使用者與應用程式而言是透明的(transparent)，當應用程式需要使用到已被遷移到二級伺服器上的檔案時，階層式備份系統會自動將檔案取回放在Cache中，加速使用者的使用，以下為一個儲存虛擬化應用模式的示意圖{圖2-4}。儲存可經由底層的區塊(block)、Tape、檔案、Record等這些型態的虛擬化，透過主機、伺服務、網路、儲存設備的虛擬化來傳遞資料，並透過in-bound及out-bound的轉換讓使用者不會察覺到虛擬化與實體的不同。

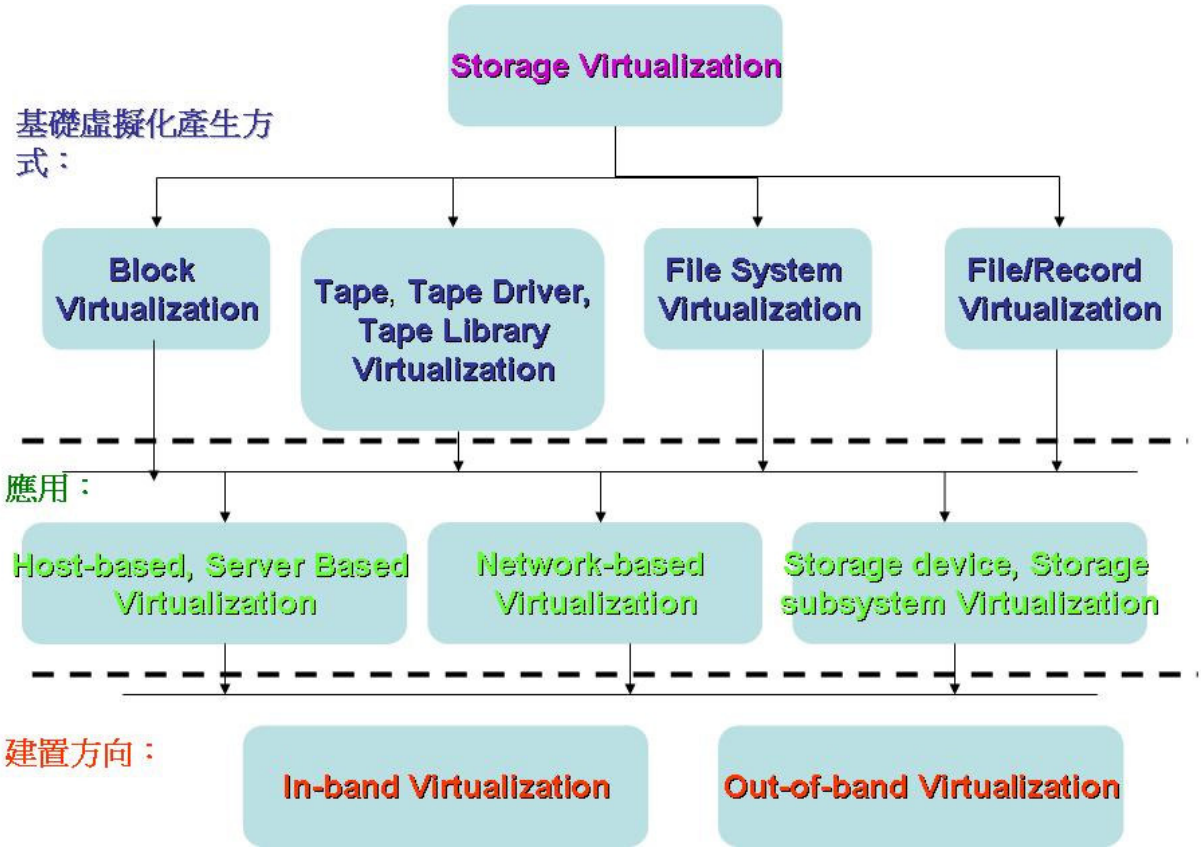

圖 2-4 儲存虛擬化的應用

虛擬化的目的都是對使用者隱藏複雜性，在磁碟陣列中，其目的是對儲存管理員隱藏複雜性，並為應用開發提供標準環境，提高效能/價格比。

儲存陣列適用於完成複雜工作的複雜裝置，與只有 1 個磁碟機的磁碟陣列相比，管理擁有 50 個磁碟機的磁碟陣列更加複雜，這正是虛擬化方法得以大顯身手的場合，藉助虛擬化技術，使用者可以像管理單一大型磁碟機或大型 Storage Pool 般地處理及管理數十個磁碟機，虛擬化的威力就在於簡化。

現在我們討論一下虛擬化的定義，儲存陣列中的虛擬化主要是指建立和管理虛擬儲存裝置，其宗旨是以 LUN (Logic Unit Number) 的形式表現磁碟機上的多磁碟儲存，如此一來系統管理員看到的不再是實體磁碟機，而是簡化過的實體儲存虛擬對應，如 LUN。

2.4 高可用度(HA)

高可用度的設計可以讓系統容許錯誤的產生，並且根據其設計繼續提供服務，利用多餘硬體 (Hardware Redundancy)、多餘軟體 (Software Redundancy)、多餘時間 (Time Redundancy) 或是多餘資訊 (Information Redundancy) 設計出來的容錯系統，可稱之為高可用度系統。高可用度(HA)的基本應用在於當系統於計畫性或非計畫性停機或暫停服務時，仍希望可以提供服務讓使用者使用，計劃性的停機包括重建系統、更新程式、執行軟體升級、硬體升級、系統維護、完整系統備份…等，非計劃性的停機包括硬體故障、系統障礙、應用程式發生錯誤、人為疏失、軟體瑕疵、發生意外災害…等，圖 2-5 為一般發生停機的原因統計，有 40%的比率因應用程式的錯誤所導致，另有 40%是因人為的操作錯誤，而 20%原因才是因為硬體故障。

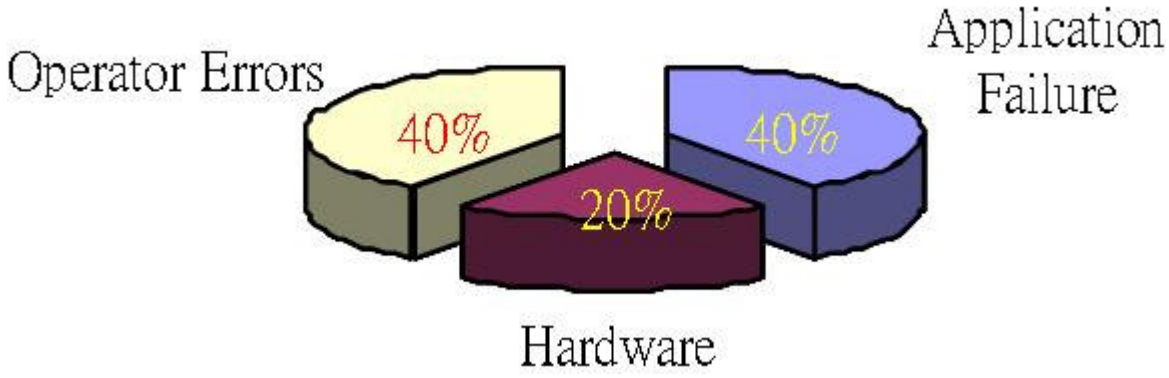

圖 2-5 系統停機的簡易原因統計

如何規劃建置高可用度(HA)呢？[11]1.首先考慮什麼樣的狀況會需要使用 HA 來改善現有狀況;2.列出所有可能遭遇的風險,特別是單點失效(SPOF, Single-Points-Of-Failures)所引發的狀況，(單點失效的定義很簡單：一旦失效就有可能導致系統無法穩定的運作的元件。) 之後提出對應的處置方式來降低風險；3.規劃出磁碟及網路的 HA 環境。

但是高可用度需要如何被衡量呢？可以透過系統持續運作存活的時間(UP-TIME)，並以一年的時間為分母來計算存活時間的比例，依達成 99%以上的幾個小數點位數，有以下簡略的 HA 分級方式，UP TIME 比率為 99%，為第 2 級，可容忍的年度停機(DOWN TIME)時間總計為 3 天 15 小時 36 分鐘，這樣的等級適合應用於個人或辦公室的桌上型 PC，比率為 99.9%為第三級，適合一般 IT 設備使用，第四級 99.99%，適合網路設備使用，第五級為 99.999%，可停機時間年度僅有 5 分 15 秒，適合重大服務(Mission Critical)的電信設備或是金融交易的企業伺服器等級。

除了一般利用叢集(Cluster)架置建立高可用度方式之外，也可透過其它的方式增加可用度，例如透過軟體的熱機切換，或是運作中的服務備用多組的硬體設備，像是硬碟、網路、電源、風扇等…，例如圖 2-6 就是一個高可用度可執行的層級簡表。

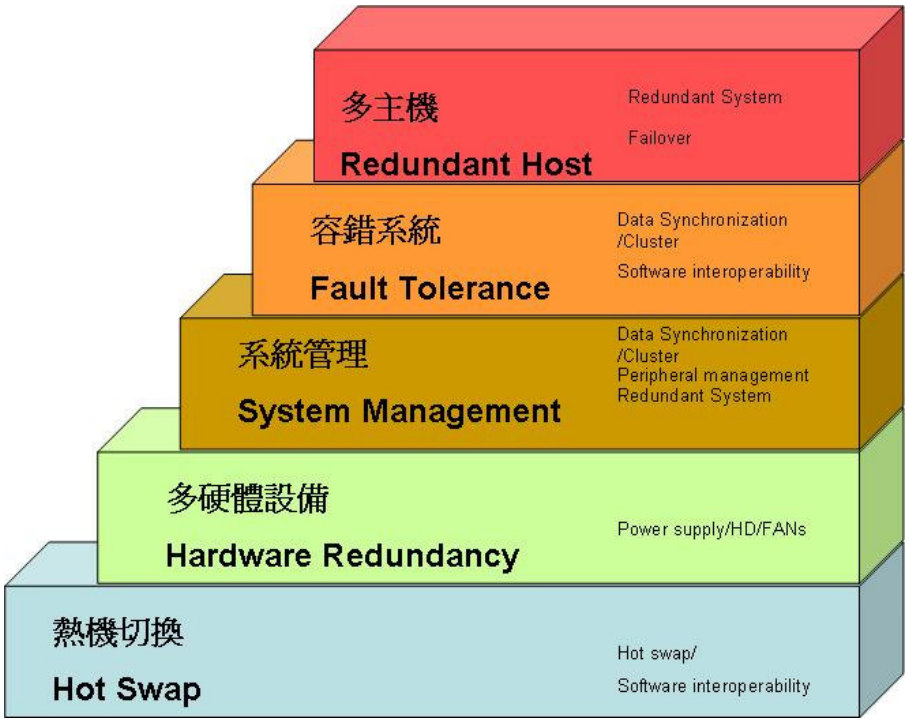

圖 2-6 HA 簡易層級簡表

表 2-1 HA 等級劃分

層級	可用頻率	停機時間/每年	應用範例
2	99%	3天15小時36分	一般用戶使用等級
3	99.9%	8小時45分	一般IT設備
4	99.99%	52分33秒	網路應用設備
5	99.999%	5分15秒	電信設備等級或交易型的企業伺服器

高可用度的應用一般都會規劃於 Cluster 的技術。大致上應用可以分為 1. 雙主機 Active-Standby 架構；2. 雙主機 Active-Active 架構；3. N+1 叢集系統 Active-Active 架構；4. 階級式的多主機備援(Cascading Fail-Over)；5. 多方向性相互備援(Multi-directional Fail-Over)。

- **雙主機 Active-Standby 架構：**

架構為由兩部主機透過 SCSI 或 Fiber Channel 連接到共享磁碟機(Share Disk, 通常是採用磁碟陣列系統 Disk Array)而構成一叢集系統，應用程式的資料庫儲存於 Disk Array 上，同一時間內應用程式只在其中一部主機上工作(Active)並只允許該主機能讀寫資料庫，當此主機任何元件發生當機或應用程式服務無法正常工作時，另一部主機(Standby)可立即接管儲存設備的存取權並重新啟動應用程式，維持系統服務正常運作而不停擺，提供系統容錯及更高的系統可用性，此種 Active/Standby 模式最為一般客戶所採用，原因是架構簡單，容易維護及管理，若兩台主機配備相同，系統服務不會因為錯誤移轉 Fail Over 到另一台之後產生效能降低情形，這將可維持穩定的服務效能，但另一方面，由於 Standby 主機的閒置也使得價格效益比降低。

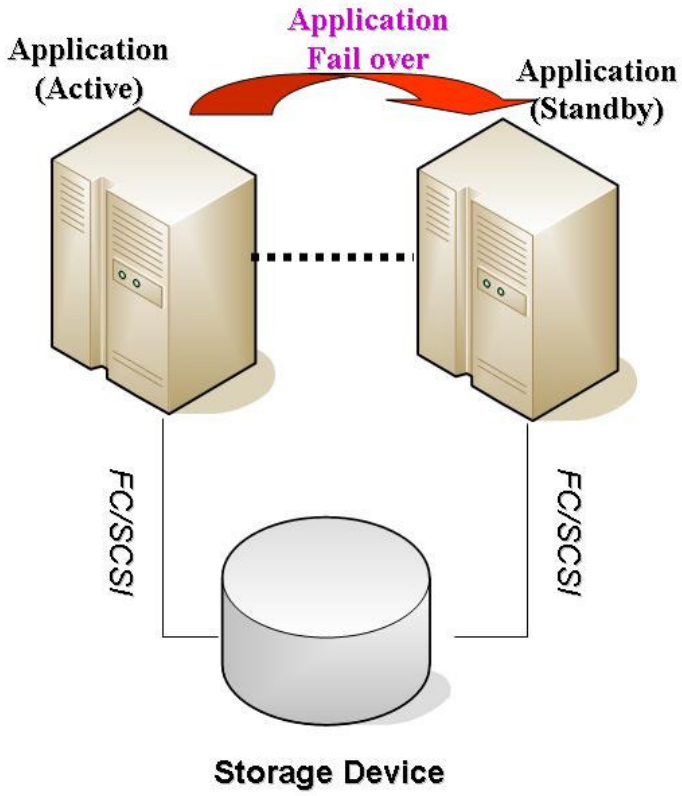

圖 2-7 雙主機 Active-Standby 架構

- **雙主機 Active-Active 架構：**

基本架構如同 Active/Standby 一樣，但兩部主機各有執行獨立的應用程式服務，同時亦相互做備援(Standby)，當任何一部主機發生故障或應用程式服務無法正常工作時，另一部主機除了本身的應用程式服務持續運作外並自動接管故障主機之應用程式服務，維持整體系統運作，此種 Active/Active 可有效避免 Standby 主機閒置的情形，提高價格效益比，但此模式容易因錯誤移轉 Fail Over 發生後造成接管主機負載比原本的架構來得重而無法維持一定的服務效能。

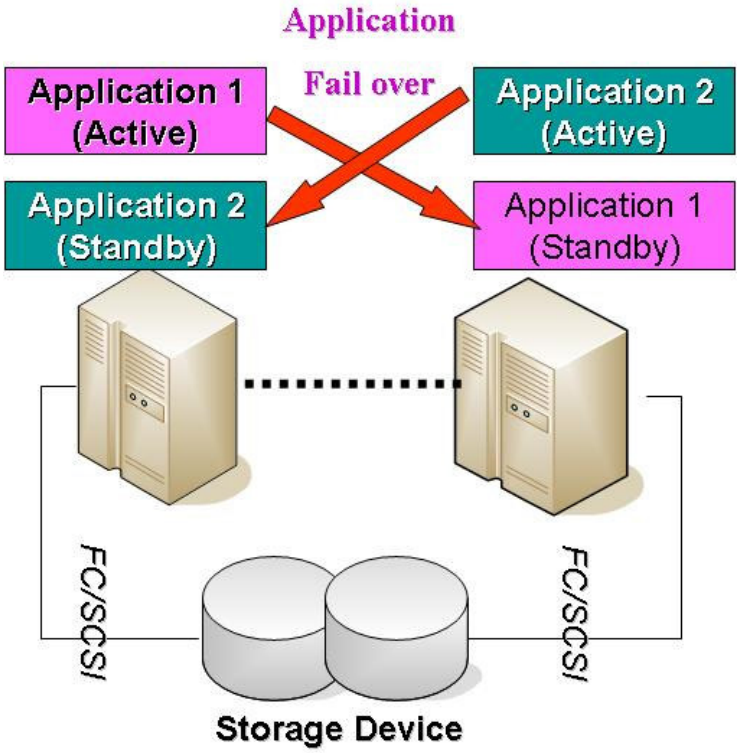

圖 2-8 雙主機 Active-Active 架構

- **N+1 叢集系統 Active-Active 架構：**

此種架構採用多部主機透過 SCSI 或 Fiber Channel 連接到共享磁碟機(Share Disk, 通常是採用磁碟陣列系統 Disk Array)而構成一個叢集系統，如同 Active/Active 一樣，其中每部主機各有執行獨立的應用程式服務，被指定的最後一台主機作為各主機的備援(Standby)，當任何一部主機發生故障或應用程式服務無法正常工作時，Standby 主機將自動接管故障主機之應用程式服務，維持整體系統運作。此種多對一 Active/Active 方式除了可有效避免 Standby 主機閒置的情形，提高價格效益比之外，也不會因為錯誤移轉 Fail Over 發生後造成接管主機負載比原本的架構來得重而無法維持一定的服務效能，更可允許各自執行獨立的應用程式服務的多部主機同時損壞，大幅提高了系統可用度。在 N+1 的多主機備援的模式下，搭配 SAN(Fiber)的系統架構解決方案，管理者可依實際需求隨時可以新增或移除主機(Node)到原有的叢集系統內，不需中斷服務，提高了擴充性(Scalability)，主機及

儲存設備將可更有效率的被運用。

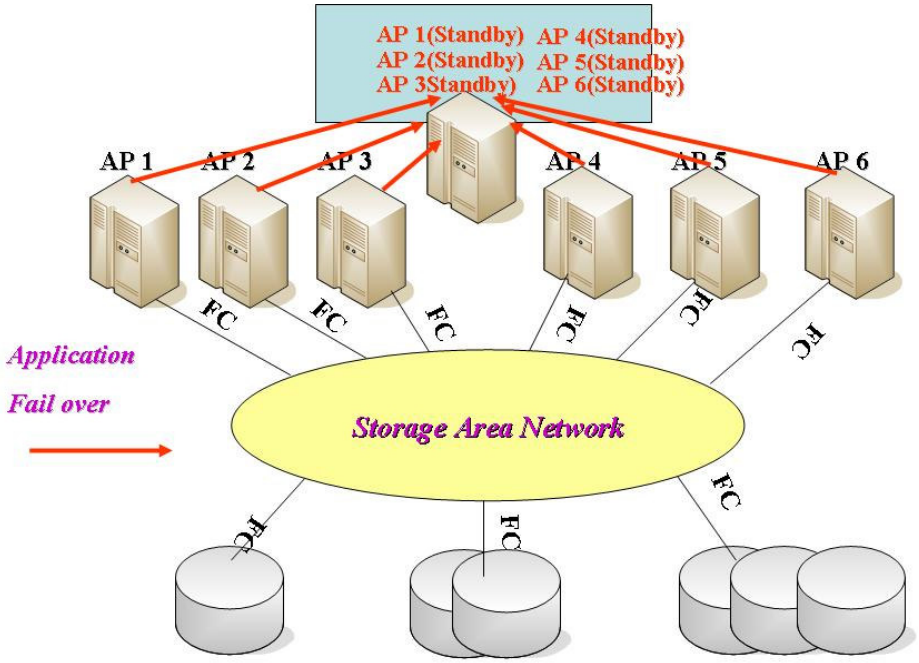

圖 2-9 N+1 叢集系統 Active-Active 架構

- **階級式的多主機備援(Cascading Fail-Over)**

此種架構係針對當錯誤移轉 Fail-Over 發生時，應用程式服務會被正確的移轉到 Standby 主機 Node 上來運作，倘若該 Standby Node 又發生問題時，此時第二備援主機將被指定為下一個接管者，如此類推。一對多個 Node 的叢集系統確保了應用程式在叢集系統下可被依階級方式(Cascade)指定多個 Node 來執行備援服務，完全提高了應用程式的可信賴度。對於應用程式服務及資料儲存環境較為複雜的中大型企業而言，提供了相當完整的解決方案。在階級式的多主機備援(Cascading Fail-Over)的模式下，搭配 SAN(Fiber)的系統架構解決方案，管理者可依實際需求隨時可以新增或移除主機(Node)到原有的叢集系統內，不需中斷服務，提高了擴充性(Scalability)，主機及儲存設備將可更有效率的被運用。

- **多方向性相互備援(Multi-directional Fail-Over)**

此種架構綜合了 Active-Active 與 Active-Standby 以及多主機模式。在多方向性相互備援的模式下，搭配 SAN(Fiber)的系統架構解決方案，管理者

可依實際需求隨時可以新增或移除主機(Node)到原有的叢集系統內，不需中斷服務，提高了擴充性(Scalability)，主機及儲存設備將可更有效率的被運用。

第三章 儲存整合方案改善計劃

目前儲存技術的趨勢焦點在於降低成本及提高傳輸速度[12]，儲存容量的增加以及大量的使用磁碟，直接導致了付出的成本愈來愈高，傳統無限制地添置硬體設備的管理辦法，已無法滿足目前的儲存需求。隨著校園經驗傳承的資料的不斷累積，資料損毀帶來的影響已不能慢慢重建資料來回復，除了加速系統還原的機制之外，還需要更密集的備份還原點來減少資料損失的衝擊。

要提高傳輸速度首先需要改善儲存的架構，提供更快速的網路儲存速度，引用一些方法來降低整體儲存設備的成本，例如分層儲存的架構，並可以利用分層儲存資料不同時間複製備份的特性導入災難復原異地備援的機制，更進階的可以處理重復資料的刪除及依資料的重要性及符合保存法規的原則進行資料生命周期的管理，以達成更完美的儲存架構。

本章我們設計一個儲存環境的改善計劃，將現有資料中心資料儲存的方式由現有的階層式異地備援儲存架構，再進一步的升級為 SAN 網路的高可用度建置與儲存管理服務的高可用度系統的建置，透過此設計的變更可以有效的提升傳輸的速度及儲存服務的可用性，同時提升 RTO 縮短了系統及服務恢復的時間。

3.1 改善方向

資料中心的資訊服務系統主要提供的服務有對外部的入口網站主機、

郵件伺服器、FTP 主機、BBS 主機…等；內部有校務系統的入口網站主機、學生及教職員的認證資料伺服器與校務電子公文會計差勤系統資料庫的主機…等，內部與外部的網路透過防火牆來阻擋駭客及病毒的入侵。校務系統一般而言其作法為資料的備份方式透過各主機系統個別管理系統及檔案備份機制,例如對外入口網站及內部入口網站伺服器,本機使用延伸的 SCSI 硬碟儲存每日工作備份的資料，郵件伺服器系統也是如此，可能因為資料量較大而連結至較大的磁碟陣列進行儲存。而資料中心的儲存架構如圖 3-1 為三層式的儲存架構，第一層為上線層(On-line)負責同步複製的備份工作，第二層為近線層(Near-line)，建置於與主機房不同棟的建築物，做為異地備援的災難復原點及進行非同步複製的工作,第三層為離線層(Off-line)負責前端伺服器定期的備份作業，因考量實體磁帶存取速度較實體磁碟存取速度較慢，所以導入虛擬磁帶櫃(VTL)的機制，將價格低廉的實體磁碟模擬成磁帶的方式，在現有架構不需要異動的狀況下，加速備份工作的執行。

儲存技術逐漸的進步，在實務上儲存是每日必須進行的工作且以成本的導向來看不可能僅以設備上新增採購或是提升至最新儲存技術這樣的方案就可以解決日常儲存管理的問題，以實際可行的改善方法有以下幾個方向：**儲存速度的提升**，包含儲存基礎架構的改善，每個儲存路徑的節點與網路使用率、存取介面的速度與規格及相容性，另外就是**空間使用率及使用效能的提升**，即使是現在虛擬化的技術將所有異質的儲存設備虛擬成一個龐大的儲存池，但是使用者的需求是變化快速的，而且對於使用量的期望值很高，這樣的結果同時也造成了很多儲存的資源掌握在幾個關鍵的使用者或單位身上，其過度要求與不佳的使用率可能就拖累了整體儲存空間有效的利用率，這部份可以透過儲存服務系統的監控及與使用單位建立儲存服務層級協議(Service Level Agreement, SLA)及定期的量測與報告來調整，還有另外一個方向就是**儲存服務可用度及可復原能力的提升**，這部份

可以透過災難復原的規劃及建置高可用度架構來達成。

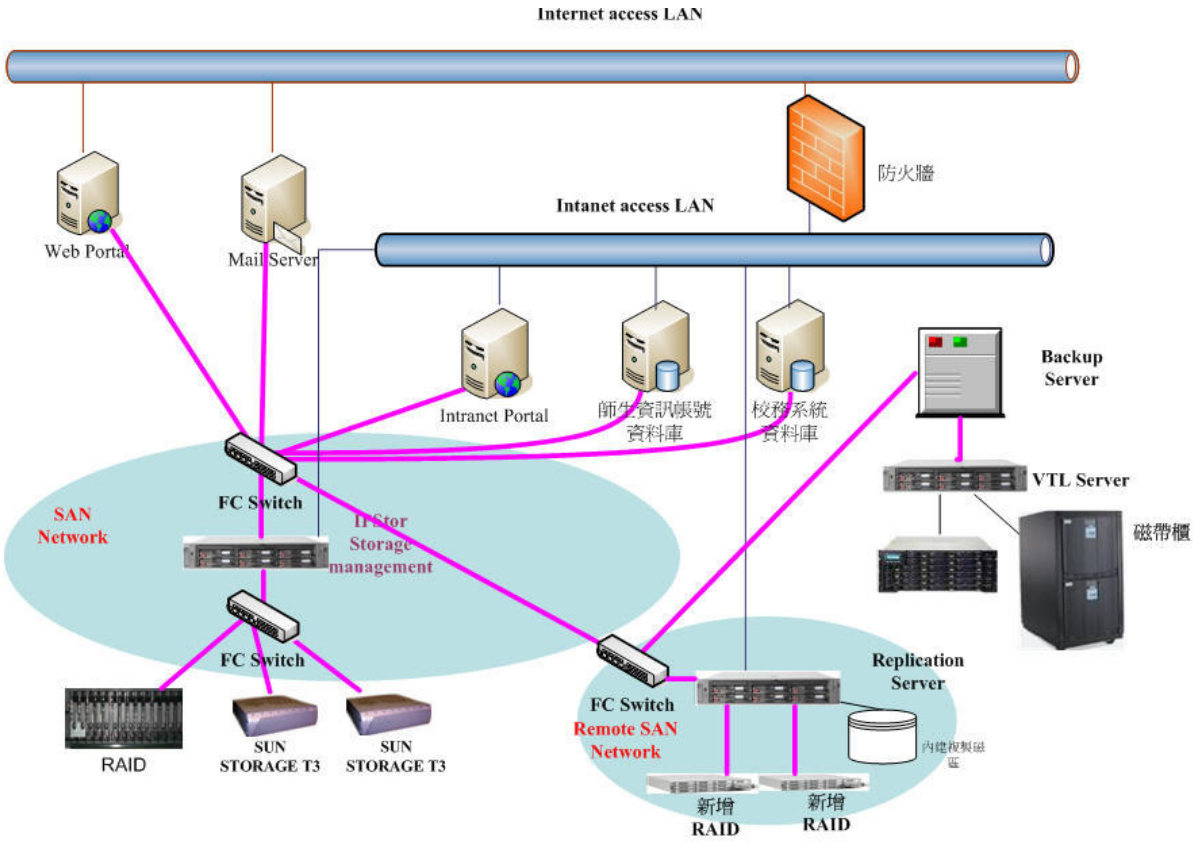

圖 3-1 校園目前儲存系統架構

3.1.1 儲存速度的提升

2006 儲存論壇有提到二種儲存技術的趨勢，其中一種是加速儲存備份的速度，而現有的儲存技術大致以二種儲存網路技術來做區分，一種是以乙太網路(Ethernet)為基礎的 IP 儲存網路，另一種則是以光纖通道(Fiber Channel)為基礎的儲存區域網路，IP 儲存網路的速度有 10M、100M、Gigabit(1G)的速度，FC 的速度有 1G、2G 及 4G，下一個世代的速度理論可以到達 10G，IP 儲存網路本身是利用 TCP/IP 的協議，TCP/IP 本身經常會發生封包碰撞(Collection)及隨著距離的增加導致傳輸品質降低，且資料的承載量(Throughput)較差。資料中心儲存網路目前已全面改為 SAN 儲存網路，採用 2G 的主流速度，較高速及超高速乙太網路有更好的傳輸速率、效能及承

載量，其延伸的連線距離可以透過不同的光纖線路延伸的更長，擴充性較佳，也有更好及更穩定的傳輸品質。

但是除了 SAN 網路儲存速度與服務的穩定外，要維持傳輸不中斷及分散流量以提升整個儲存網路的承載量，我們可以規劃利用建置多個平行的 FC 路徑，有效分散前端主機的資料順利分流至後端的實體儲存設備，增加同一時間點內有效的傳輸流量，此種方式可以列為有效改善傳輸速度的一種選擇。

3.1.2 空間使用率及使用效能的提升

儲存的另一種改善方法在於管理，強化儲存的管理讓儲存資源能夠更有效的應用，資料中心目前是引進 FalconStor 的 IPStor 儲存管理服務軟體，透過虛擬化的技術將異質的儲存設備整合為一個儲存空間聚合在一起的儲存池，這樣可以更便利的對現有儲存設備做管理，前端有儲存需求變更，需要更彈性的對儲存設備重新做設定，透過軟體及虛擬化的方式會更為便利。

3.1.3 儲存服務可用度及可復原能力的提升

服務可用度的能力可以透過技術面的改善例如多路由設計以及系統 HA 的建置來達到容錯及自行切換至可用備份系統的機制，一般系統建置高可用度多使用叢集的方式來達成高可用度的架構，當建置完成之後，系統的可用度會較原有的架構提升，風險也會相對的降低，而透過整個架構的完整性，當遭遇災害發生時，其所供應服務的節點並非單一，所以也可讓災害復原的時間及耗費的人力、物力相對的減少。

3.1.4 災難復原的設計

資訊的最底層是資料，有了資訊的累積才能夠突顯服務的價值，而且隨著資訊及電子化的普及，數位化多媒體資料成為現今最重要的資產之

一，因此當數位資料一旦無法正常存取或是毀損時將會造成單位組織原有的工作會無法進行同時也可能導致前人努力的心血付之一炬，因此對於資料存取及保護的重要性是可想而知。

傳統的資料保護計劃往往是將資料透過例行性的工作將資料備份至延伸的磁碟或磁帶及磁帶櫃，然而由重大的災害事件如 921 地震、911 恐怖攻擊等天災人禍的發生，造成了不可抗拒的因素的影響導致服務停擺，目前的備份機制根本無法保障資料的安全，所以需要有解決方案來改善現有儲存方案太過單一化的問題，目前有關災難復原的解決方案在企業內常被應用的有磁帶的異地儲存、磁碟的異地備援方式甚至最近討論到多儲存站台平時獨立運作，災害發生時透過網路設備自行切換的異地互援機制，因此如何透過異地備援以確保災難發生時能快速復原，成為目前所急需解決的問題。

一般我們在評估災難復原的架構時最常引用災難復原指標 RTO 及 RPO 這二項衡量標準，這二個指標皆是以時間的長短為單位，隨著時間的拉長對系統的傷害及服務的損失成本會愈來愈大。針對 RPO 與 RTO 的指標儲存技術有如圖 3-2 對應的處理方式，RPO 是取決於備份資料的頻率，最快的備份機制是同步複製再來依序是非同步複製、周期性複製，最後才是磁帶備份，RTO 是取決於服務復原的時間，最快的回復機制為叢集容錯處理，然後是人工介入處理搬移資料，最後才是磁帶回復系統資料的機制。

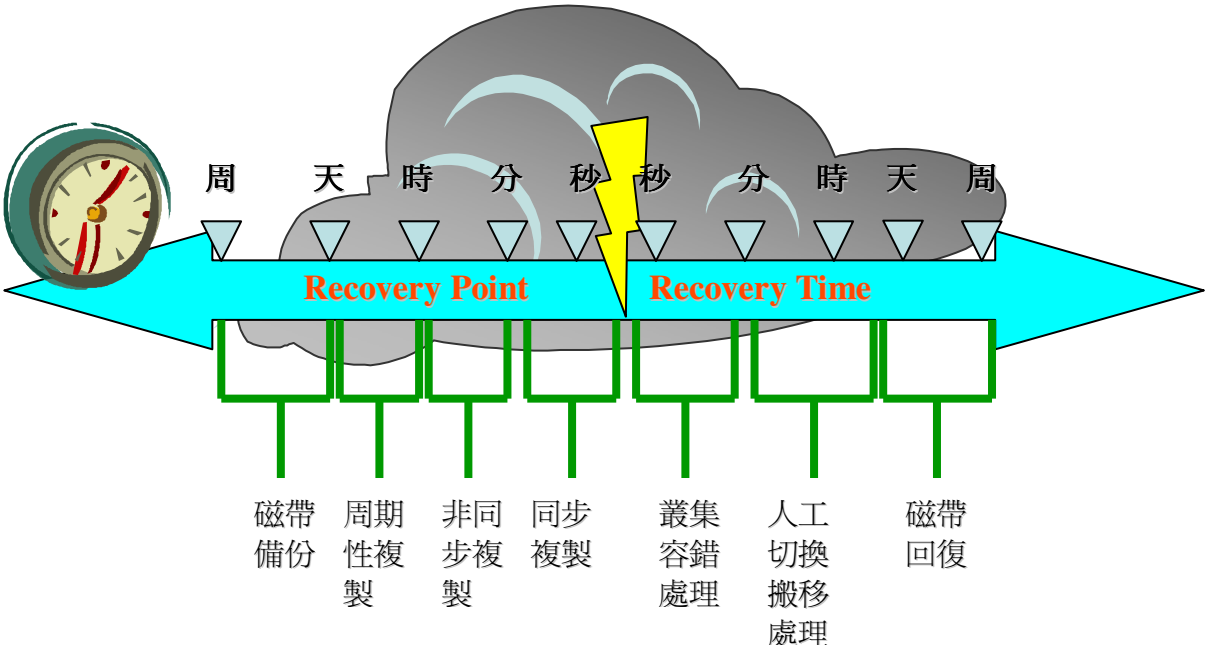

圖 3-2 RTO/RPO 指標對應資料複製與系統復原方式

由以上災難復原的處理方式，我們可以將建置於 SAN 架構的儲存服務軟體導入到同步複製的 RPO 層級，另也可透過不同 RPO 要求的備份方式建立階層式的儲存架構，以防止當只有單一備份點但遇到災害時，沒有其它備援的處理方式而造成資料無法復原，所以我們規劃以非同步複製的機制來達成異地備援的功能，因所在校園其它縣市並無分校，故以不同建築物來建置異地備援機制的儲存點。而周期性複製與磁帶備份這部分可以規劃轉換為虛擬磁帶櫃與實體的磁帶備份來達成，所以風險得以分散。另針對 RTO 的復原需求，目前僅能夠達到人工介入處理的目前，所以在下一節會討論高可用度的設計，以達到叢集容錯處理的目標。

3.2 高可用度規劃設計

為達成 RTO 目標遭遇障礙時能夠迅速的復原系統與服務，所以建置高可用度的架構，由網路及儲存服務系統此二部分來提高儲存服務的穩定度，在網路的部分我們建置了更多的傳輸路徑可供分散單點傳輸中斷的風險，在系統的部份選用雙主機 Active/Standby 的叢集架構。本章節是在介紹

依照上面所述的規劃下，日常的備份工作與高可用度的切換及回復機制。

3.2.1 系統備份

系統備份維持現有架構，應用程式的資料每周六、日進行全量備份，各系統每日進行增量備份，重要性高的系統除了本機磁碟保留外並於儲存於線上(Online)層進行同步或更密集的資料備份。導入高可用度架構之後，對於前端系統備份的方式不會有影響，後端的儲存設備會有多一套網路設備的連結，前面所設計的備份機制是由儲存服務主機來控制，也不會有異動，加入高可用度的機制後，當主要儲存服務軟體主機發生問題時，整個備份的工作會切換至次要儲存服務軟體主機，當切換時原安裝於應用伺服器端的 snapshot agent 會先行釋放備份的工作權給伺服器，當切換後需要執行備份工作時 snapshot agent 會取得控制權再進行備份的工作。所以主機端的工作能夠持續延續下去。

而儲存資源例如新增磁碟陣列或者是設定新的 LUN 給特定服務，在虛擬磁碟重新設定後，需要進行 Active-Standby 主機設定檔的同步作業。這可以透過儲存服務主機本身 HA 的軟體定時的來進行同步作業。視系統設定的頻繁度，及二部主機資料的差異性周期設定資料同步作業的時間，例如設定每一小時資料同步一次。若密集的同步作業會影響主機的效能，則拉長資料同步的作業頻率。也可於每次執行完成異動設定之後，手動執行同步的作業。以避免因資料未同步導致系統切換 Fail over 後找不到對應的資料或虛擬磁碟區，發生備份錯誤。

3.2.2 系統障礙切換（Fail over）

建立高可用度的目的主要是當儲存作業發生障礙時，能夠切換到可以替代的系統或路由，目前以現有資料中心的儲存容量及效能來評估，並符合 RTO 能快速的讓服務恢復正常及現有經費的考量，決定採用雙主機

Active-Standby 的高可用度架構。目前此架構規劃故障切換的方式是以系統自動偵測到異常，自動切換由 Standby 主機提升為 Active 主機，原異常的 Active 主機再自行排除或是需要再由資訊管理人員介入檢修。故障切換 Fail over 主要參考的因素有儲存服務主機軟體的異常、硬體的異常、IP 網路的異常、儲存服務主機 HA 溝通機制的異常、光纖通道(FC)的異常、前端應用伺服器的異常、後端磁碟陣列的異常…等，而切換的方式主要以自行監測到異常自動 Fail over 為主，若遇到雙主機同時發生障礙或是軟體切換的問題需要人員手動介入時，方進行手動切換。

3.2.2.1 路徑的切換

參考對於 SAN 網路架構高可用度的支援，FalconStor 公司的技術白皮書[13]內有提到一項 DynaPath 的機制，是透過 DynaPath ®Agent 這個 IPStor 儲存系統提供的常駐應用程式，主要的功能為透 SAN 架構，達成最大的可用度。它的運作方式是在 SAN 網路上建立平行可用的儲存路徑，當發生儲存網路的問題事件時能夠將應用程式資料複製的 Traffic 導向至其它可用的冗餘(redundant)儲存路徑，以確保儲存網路中的工作不會被中斷。更進階的它可以支援負載平衡(Load Balance)，可以自動化的分散伺服器資料傳輸量至多儲存路徑，支援多重路由(Multi-Path)可以提高每個傳輸路徑的使用率及避掉瓶頸(bottlenecks)，基本運作的方式如圖 3-3，而整體網路介面的規劃如圖 3-4。因為此套軟體是安裝於應用伺服器上，於伺服器上新增額外的 I/O 路徑以提供自動的故障切換及保護。DynaPath ®機制的好處簡而言之有：1.透過延伸可復原的多重 I/O 路徑，提升儲存網路的高可用性；2.增加頻寬同時可提升傳輸的 throughput；3.網路負載平衡(Load Balance)的機制能夠最佳化 I/O 的存取效能。

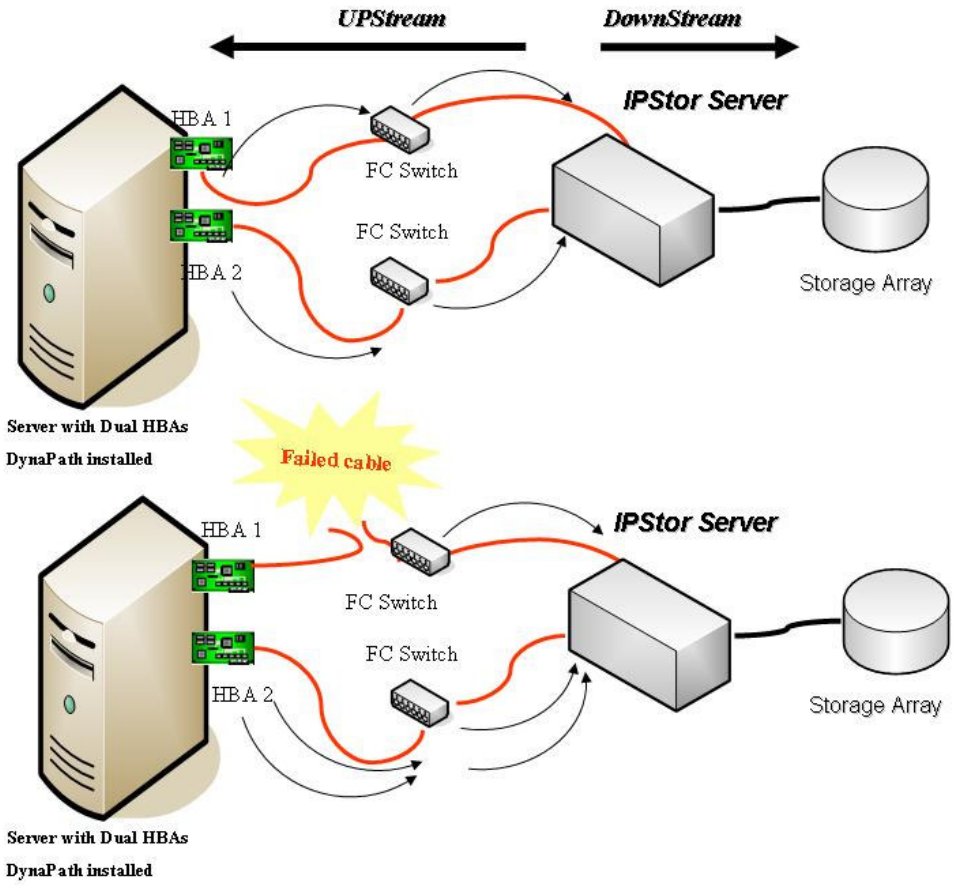

圖 3-3 DynaPath®多路徑路由運作方式

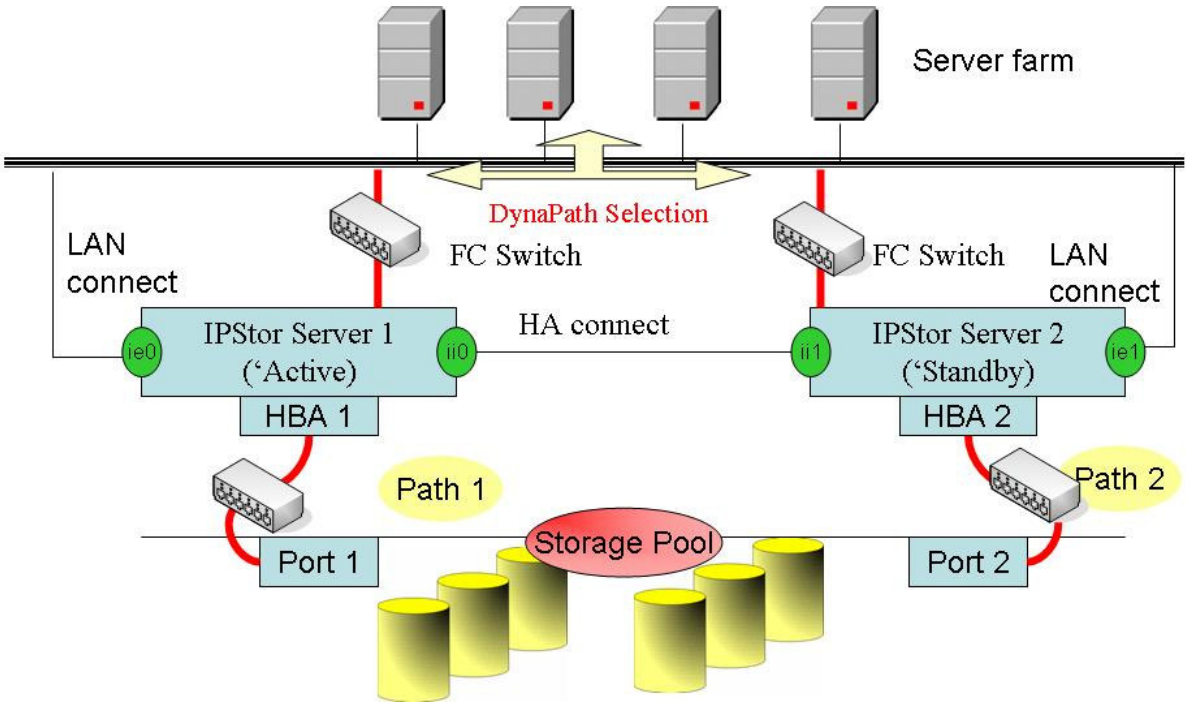

圖 3-4 HA 架構的 Interface 及 DynaPath 運作

3.2.2.2 自動切換 Fail over

3.2.2.2.1 軟體仲裁

可依照儲存服務主機既有的高可用度軟體功能的網路偵測對 IP、SCSI port 進行存活 alive 測試回應，及儲存服務主機服務的效能及處理狀態是否正常，若有上述的節點(node)、服務異常，則卸載 Active 儲存服務主機的服務並呼叫 Standby Server 接手。一般 HA ACTIVE-STANDBY 的架構可以透過 Cluster 的機制 mapping 成為主機(HOST)或服務(Service)的群組，透過 Heart Beat 的方式透過私有區域網路(Private LAN)或 RS-232 序列埠來監控服務，並於異常時強制切換。

3.2.2.2.2 ACTIVE 主機自行偵測無法排除後切換

Active Server 可自行檢測與前端應用伺服器 snapshot agent 的連結是否正常，儲存服務於本機的運作是否正常，同時本機也可以檢測 OS 控制的 SCSI Driver 及 HBA Driver 是否有正常運作，或有其它錯誤訊息。以及測試連結後端儲存設備透過 FC 連結的 SCSI Port 是否可以正常連接。若有以上狀況，OS level 的部分本機會嘗試排除。此類問題若無法排除再進行 Fail over 至 Standby Server 的動作。而儲存服務主機的軟體部分，Active 依照儲存應用程式 I/O 軟體堆疊的方式，先確認 File System 與 Database manger 的功能是否正常運作，再來確認虛擬化 Virtualization 磁碟是否運作正常，然後再檢測後端對應的實體路徑是否有存在或異常狀況。若上述有異常發生，則進行切換至 Standby Server 的動作，或自行執行重啟服務或重啟機器的動作並將控制權釋出。

3.2.2.2.3 STANDBY 主機偵測對方異常

當 Active Server 系統太過繁忙無法再回應任何需求，以及主機或系統異常也無法重啟服務或機器時，Standby 主機需主動偵測此狀況，同時並主導成為 Active Server 提供服務，Standby 主機的偵測行為如下：首先需確認

自身主機狀況正常可以提供服務，各網路節結點皆可順利連結。第二步驟定時的去嘗試 ping Active 主機各個存取 interface 的介面，是否可以順利回應，第三可以模擬一般備份存取的行為，至後端的虛擬磁碟區檢測 Active 主機備份的資料是否皆有正常的存入，當發現第二及第三項有異常狀況時，自行啟動儲存服務軟體高可用度的服務成為 Active 主機。

3.2.2.3 手動切換

當系統管理人員收到系統異常的告警，或是服務出現異常時，需要人力介入查詢異常原因，雖然這是在時間反應上比較慢的機制，但卻是最後一道保險的防線，因即使是再穩定、再高技術等級的系統，隨著運轉時間的增長、設備的老舊都有可能在各個環節發生狀況。備份機制皆是希望備而不用，透過監控機制的規劃，讓系統設備異常時能夠將訊息發送至系統管理人員，此部分會列在未來的規劃改善方向，目前傾向不建置此功能。

當系統人員發現 HA 無法正常順利切換時，首先進行服務的檢測，確認出可用機器重新啟動服務，後續再針對無法排除的部分進行處理以維持服務的持續性，若二部主機同時間皆無法正常運作，則需啟用後續的緊急應變方案，儘速排除問題。

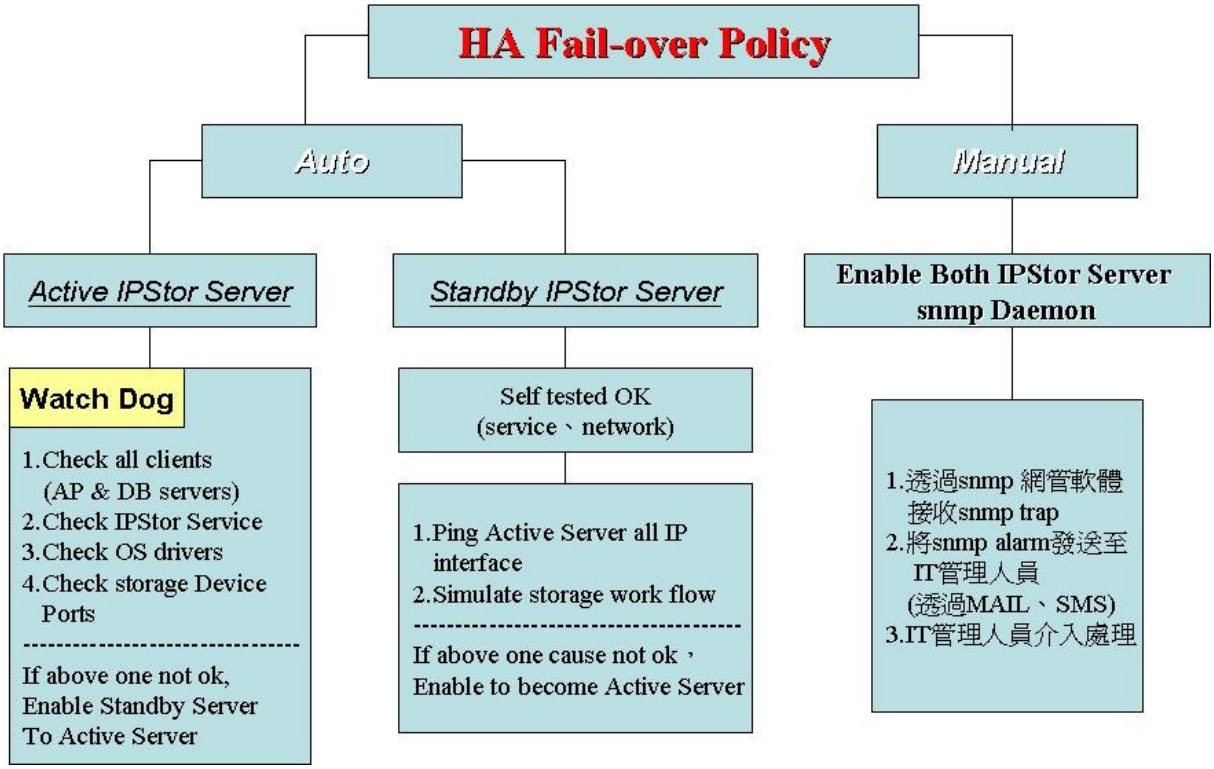

圖 3-5 HA Fail-over Policy

3.2.3 系統還原

ACTIVE/STANDBY 的雙主機架構，經常處理單機待機的動作，所以主要的系統執行的負載落在經常提供服務 Active 的主機上面，基於以上特性及精簡成本的考量，Active-Standby 的主機可以選用不同規格的主機來配置，Standby 主機用規格較 Active 主機規格等級為低的設備來建置，所以 Standby 主機的性質可設定為不長時間 Active 的主機，當系統 Fail over 之後，需讓原來效能較好的主機自動回復到 HA ACTIVE 的狀態，這樣的好處有二項：1.讓效能較佳的機器來執行服務資源會有較好的效能；2.透過這樣 HA 自行 Recovery 的動作，可以避免當 Standby 主機 Active 之後因系統或其它問題造成二次 Fail over 時，因無法清除原 Active 主機的故障問題而導致系統服務中斷，而 HA 回復(Recovery)的機制，可參考下圖 3-6 區分為自動還原及手動還原。

3.2.3.1 自動還原

一般若是軟體的問題，例如 IPStor 的相關應用程式故障經重啟服務排除

之後，透過主機軟體自動監測的機制，如網路、服務已正常運作後，可設定一個時間點或於服務存取的離峰時間進行切換至 Active 的狀態。

3.2.3.2 手動還原

若是系統異常、硬體設備故障需人力介入的狀態，在進行維護時會先進行 HA 服務卸載的動作，當問題排除之後，也需手動的再加入 HA 的 Group，加入之後再檢視二部主機的狀況及現 Active 主機的負載量，確認切換影響度較低時，手動重啟 Active 的主機。

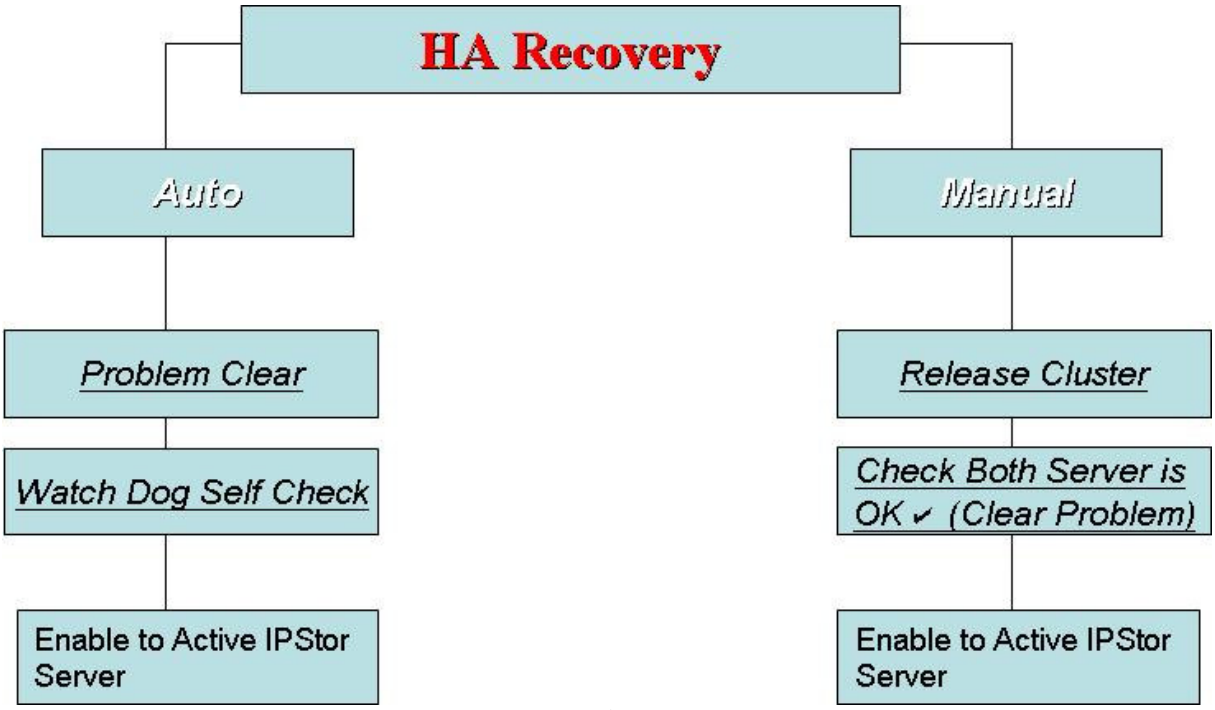

圖 3-6 HA 系統復原的機制

3.3 以服務層級協議(SLA)的規劃將服務導入改進儲存架構

一般在業界會以契約約定的方式，讓服務提供者及顧客雙方同意的約定去定義了服務的目標及雙方的預期結果及責任，同時因為每項服務的重要性不一，服務中斷時對客戶及對營收的影響也不相同，所以可以依照不同的服務、重要性及期望值來要求服務提供者對不同的服務提供相對的服務保證，而這份約定一般就稱為服務層級協議(SLA，Service Level Agreement)[14][15][16]。

導入 SLA 的概念，主要是利用現在校務系統內有各種不同的服務，而不同的服務其重要性有所不同，服務受到影響所造成的損失也不同，不同的使用者及使用單位對障礙發生時的感受與反應也有所不同，利用上述的不同點來對服務進行分類及管理，以 SLA 的精神來達成系統儲存資源與使用者期望的服務效果取得平衡及雙贏的局面。

但是要建立真正實用的 SLA 層級是需要循序漸進的，透過使用者需求的調查，來定義出使用單位真實的需求，一般資料中心針對使用單位儲存的需求有制式的儲存空間需求表單，表單內一些參考的欄位可以做為參考的價值，例如服務定位為重要性與否、服務提供的作業時間、整體儲存容量的需求、允許系統障礙的容忍度及一些使用單位的特殊要求，此類表單可以描繪出使用單位對資料中心儲存服務的期望值。而資料中心的儲存系統管理人員會參考使用單位的需求單並依照標準作業流程(SOP)於現有的儲存資源做適合的分配，但使用單位的期望值經常是與系統管理人員的儲存資源分配有落差，所以使用單位會再將欲達到的服務期望值與資料中心的負責人員進行協調，而管理者經過系統維運經驗的累積與使用單位的協商經驗這樣反覆的流程，對於現有服務儲存的資源做協調後的調整，可以滿足使用單位的需求及系統資源的有效運用，最後可以針對各別服務定出可提供的儲存資源，並對應至各別服務的 RTO/RPO 目標，建立了規則之後便可以達到現階段最有效益的儲存分配，整個應用改善的流程如圖 3-7。

有了 SLA 的規則之後，也必須來驗證現有的 SLA 是否有效？一般可以透過一些服務品質量測的標準，例如在儲存管理系統方面可量測儲存服務的效能、後端實體儲存設備的反應時間、單位時間內資料流的承載量、監測各別服務儲存空間的平均使用量、變更異動的頻率；在儲存網路部份可以量測 IP 效能、FC 效能、延遲的量測、封包流失的量測、多路徑延遲的量測，以上這些量測值的追蹤可以再連結至儲存系統的變更管理及意外管理。

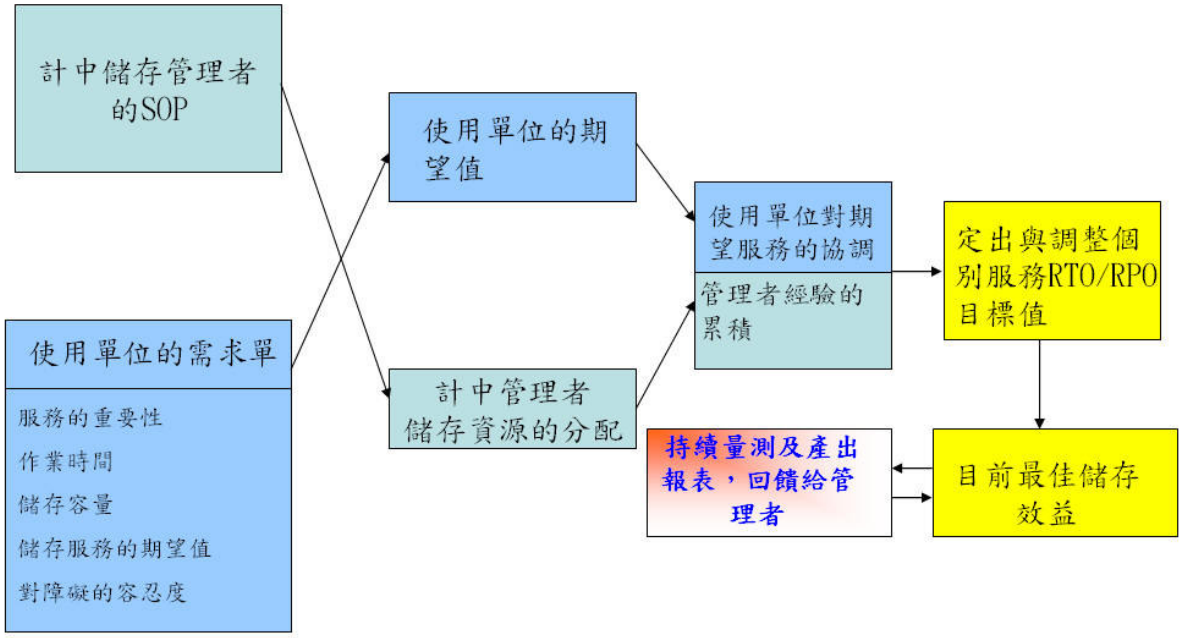

圖 3-7 使用單位的需求與管理 SOP 的改善流程

SLA 的管理可分為幾個項目，首先需要做的就是定義 SLA 的參數，這部份主要可以由使用者的需求如期望值、作業時間、容忍度、其它需求、例外清單…等，系統端的設定如空間的設定、服務應用於階層式儲存架構的定位、RTO/RPO 的目標…等等。再來就是上面所提到的 SLA 針對一些服務品質、網路品質的量測，並由持續的量測來產生服務品質報告，以達成後續的服務品質(QoS)管理，再來則是建立 SLA 的客訴回饋機制，可以透過提供給使用單位的技術支援窗口來收集相關的資訊，也可以數據化 SLA 的客訴統計，例如各別服務的每月處理件數、障礙時間…等等，來追蹤現有的 SLA 是否需要調整。

第四章 系統架構實作

由前一章所規劃的儲存改善計劃，圖 4-1 來表示一般要執行儲存系統架構改善的流程圖，因目前資料中心的儲存方式已經是導入了虛擬磁帶櫃的

技術，儲存網路也已經是 2Gbit/S 主流的儲存速度，也已透過儲存管理將異質的儲存設備整合為一個主要的儲存池，也已建置了異地備援的機制，所以需要改善的部分為建置高可用度架構，可以分為二個方向來建置，一個是儲存管理系統主機的高可用度建置，另外一部分是建置 SAN 儲存網路的 FC 高可用度架構，當高可用度建置完成後預期的效果為系統可以自動容錯，並於系統故障時自動切換至可用的主機及儲存路徑。

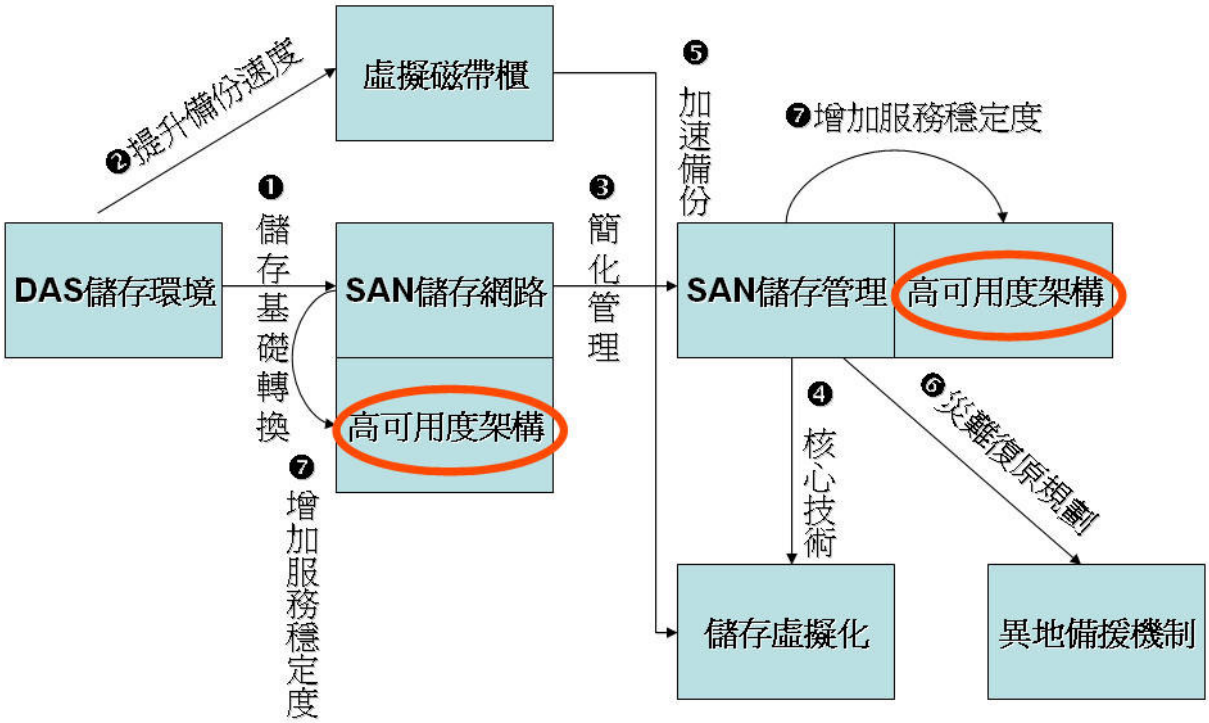

圖 4 - 1 儲存改善計劃執行流程圖

4.1 高可用度的建置

依第三章所提及的 HA 設計概念，新增一套 IPStor 的軟體及標準伺服器及一組 FC Switch 來建置 HA 的架構，首先建置軟體系統的高可用度架構，主機先要安裝 FalconStor 公司所提供的 IPStor 軟體，安裝完成後再來進行叢集 Cluster 架構加安裝與加入。

高可用度架構雙主機的建置方式主要是以叢集的方式來建置，我們選用的方式是雙主機 Active/Standby 的方式，透過 Heartbeat 這個傳輸協定來

建置叢集架構同時監控主機的狀態及目前的組態設定。

二部主機提供的 HA 的架構是以 IP 為基本的服務控制介面，HA 架構有二個主要的 IP 介面，一個是提供 IPStor 的主要 IP 介面，另一個則是提供給 Heartbeat 使用的 IP 介面。IPStor 第一部主機有獨立的 IP 為 IP A，第二部主機的對應介面的 IP 為 IP B，這二部主機的介面上再虛擬出一個 IP 為 IP C，這個 IP 就成為擁有 IPStor 服務主控權的 IP，一般也稱之為 Cluster IP 或 Virtual IP。

另一個 Heartbeat 使用的介面第一部主機是設定為 IP 1，第二部主機設為 IP 2，二個介面是透過網路線以交錯式(Cross over)的方式連結，互相偵測 Heartbeat HA 的機制是否存活，以及透過 Heartbeat 來同步彼此組態設定變更及新的工作進行(Provision)的最新狀態，另外比較特別的是為了避免因為單一 IPStor Server 當機導致另一部 Standby 的主機無法同步到最新工作執行的資料，切換為 Active 主機後原有的工作會產生錯誤而無法執行，所以於儲存池內切了一塊稱為 Quorum 的 LUN 儲存區給二部主機的同步資料及組態設定檔存放，讓二部主機皆可以保持及取得最新的儲存工作資料。

再來進行 FC 網路多重路徑高可用度的建置，前端應用伺服器添購新的 HBA 卡連接至新的 FC Switch，後端的實體儲存設備也連接新的 FC Switch，舊的 IPStor 服務主機也建立新的 FC Switch 的連結，而新的 IPStor 服務主機除了建立新的 FC 連結路徑外，同時也連結至舊的 FC Switch，因考量系統服務中斷時間要儘量縮短的因素，所以 FC 連結順序為新的 IPStor 服務主機首先與前後端的新增的 FC Switch 做連結，此時不會有服務的中斷，第二步為新的 IPStor 主機連結至舊有的 FC Switch，FC Switch 僅有連接時極短的影響時間，服務中斷幾乎不會被查覺，第三步為原有的 IPStor 主機連結至新置的 FC Switch，第四步為前端應用伺服器各別進行連結至新增的 FC Switch，因此動作前端伺服器需要停機，故需要應用程式主機各別

依排定切換時間進行停機及通知前端的使用者，整個執行 HA 建置的過程如圖 4-2。

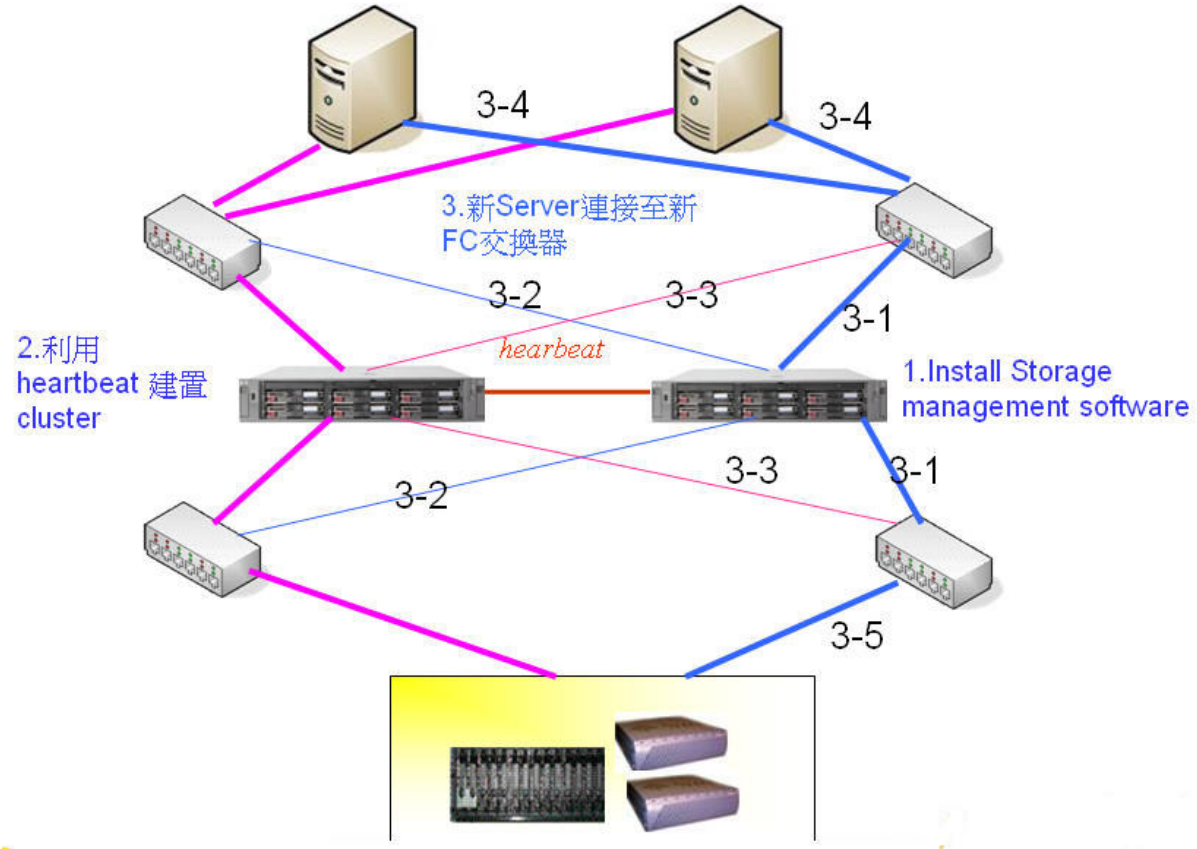

圖 4 - 2 HA 實作歷程

新的 SAN FC 架構透過 FC Switch 將前、後端的設備與 IPStor 儲存主機連接起來，當單一 FC 節點遭遇線路障礙的時候，不需要 IPStor 的 Fail over 即可透過 DynaPath®的多重路徑選擇達到資料持續傳輸不中斷的效果，可能當線路進行選擇切換時原來的傳輸 FC 路徑會有數秒鐘將傳輸暫時停止住，再選擇可用路徑繼續傳送。

現在導入的高可用度架構可以設定系統自行偵測 IPStor 自我檢測服務的頻率，及 Heartbeat 偵測的頻率，目前設定為每 2 秒自行偵測 IPStor 的服務是否正常運作，每 5 秒檢測 Heartbeat 的溝通是否正常，HA 相關的設定資訊如下圖 4-3。

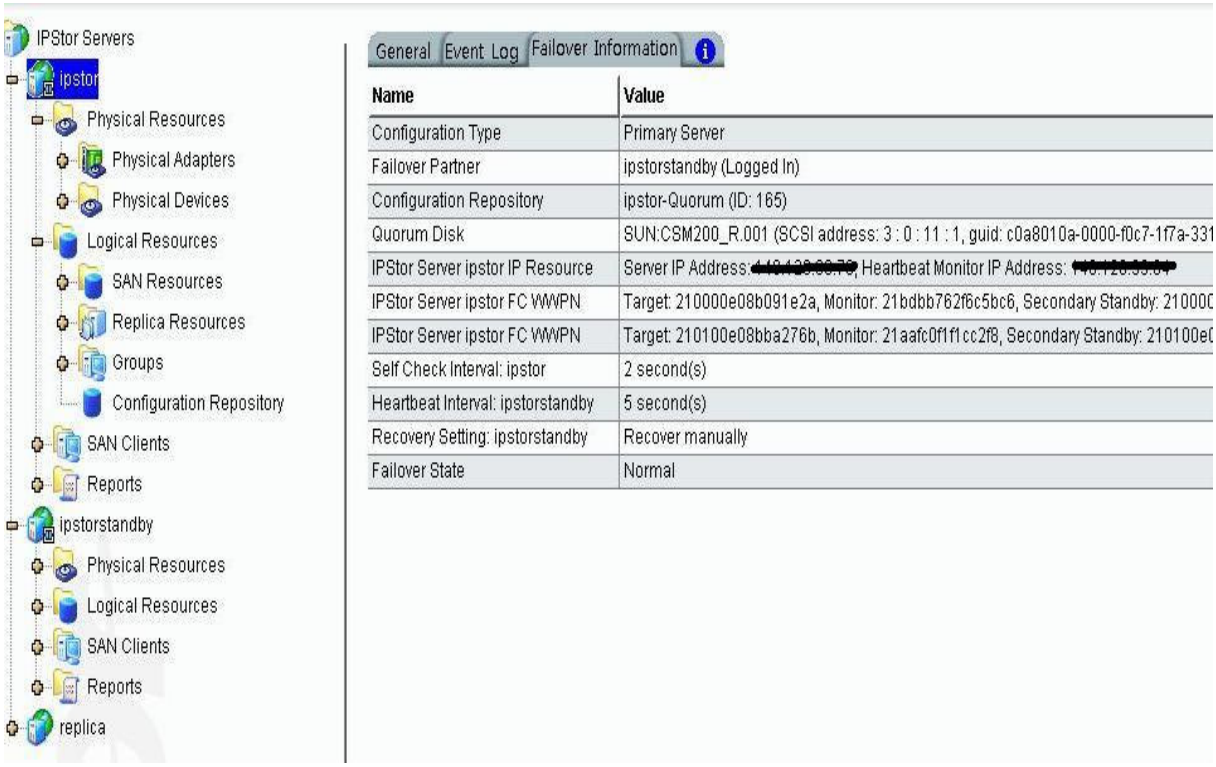

圖 4 - 3 HA Fail over Information

整個 HA 建置 FC 多重路徑及建置雙主機叢集 Active/Standby 的架構圖如圖 4-4，圖中粗線粉紅色的部份為 Active 主機 FC 可選擇路徑，而粗線藍色部份則為第二部主機 FC 的可選擇路徑，實作的結果較原先規劃的設計在 FC Switch 上多了更多路徑的連接，而圖 4-5 則為整套系統建置完成後的完整架構圖。

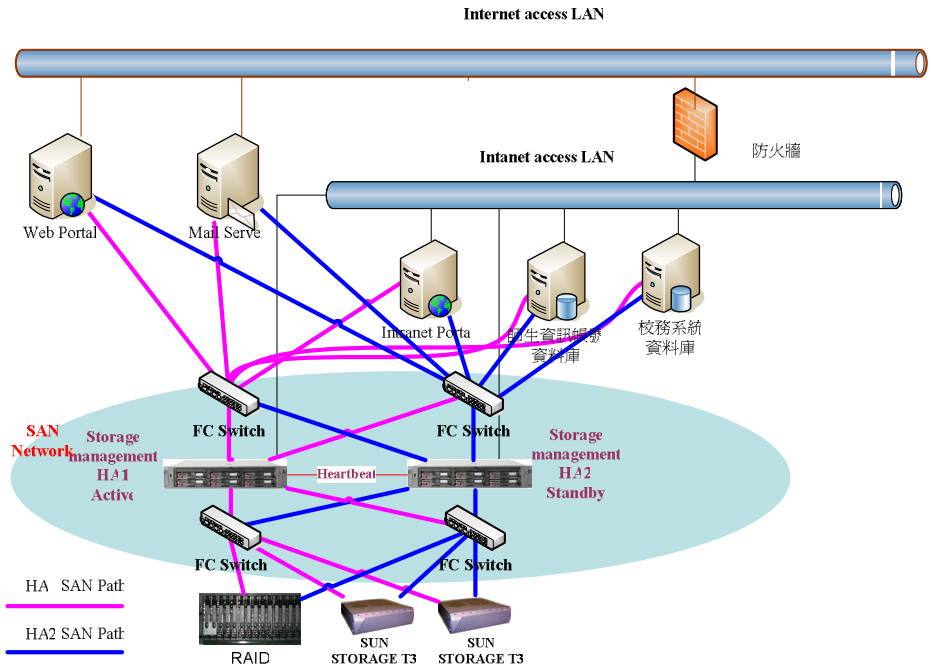

圖 4 - 4 建置高可用度架構

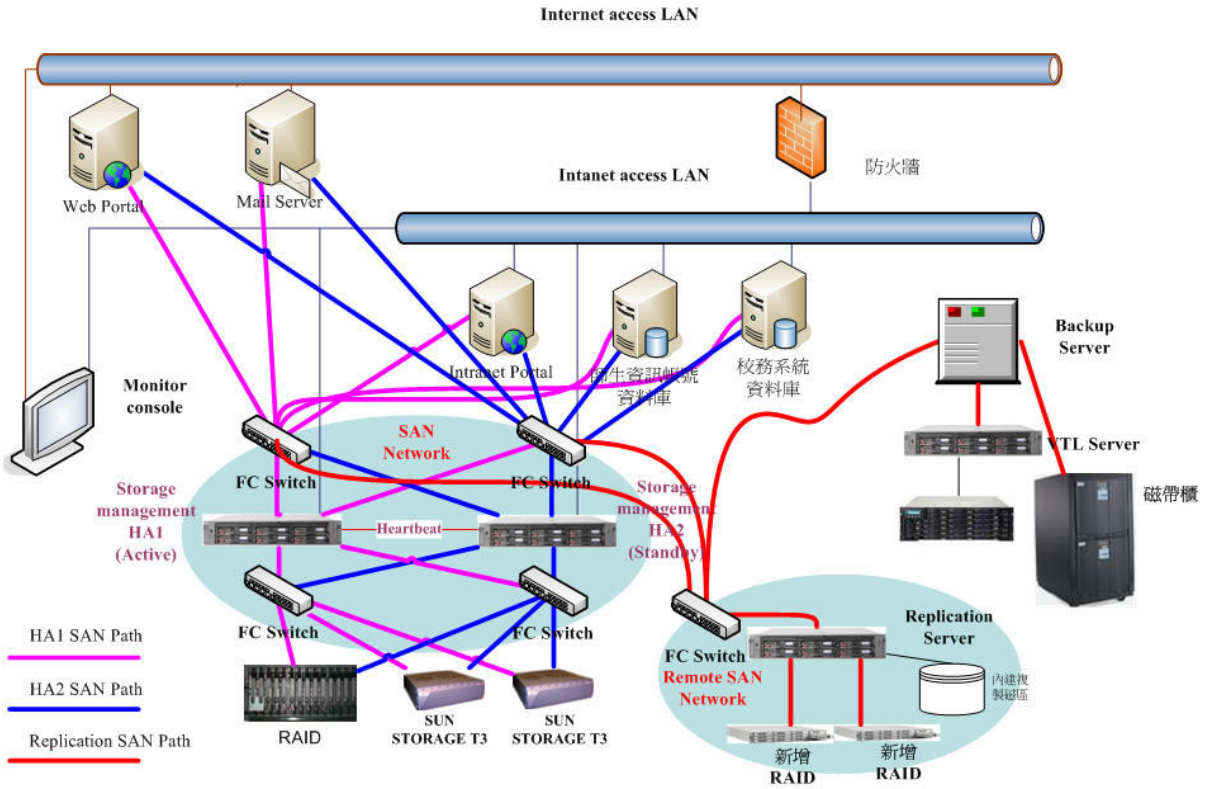

圖 4 - 5 實作後的完整架構圖

4.2 高可用度建置前與建置後的比較

4.2.1 多重 FC 路徑建置後的資料承載量及可用性比較

前端的應用程式伺服器安裝 FalconStor 的 DynaPath®Agent 之後，及新的 FC 與 FC Switch 新路徑建置完成後，儲存路徑的選擇變成不是單一路徑的選擇，而在實際儲存工作進行時資料流的承載量會由原先的單一 FC 路徑有效分散至新增的 FC 路徑，當單一 FC 障礙點發生時，原始的架構備份的選擇只有等待 FC 路徑被修復後路徑重新建立起來再繼續傳輸，新的架構則是 DynaPath 自行偵測到問題會先 Hold 住現有路徑數秒後再轉由其它可用 FC 路徑。

4.2.2 災難復原機制的比較，RPO 與 RTO 目標的達成

RPO 是取決於備份周期的頻率，若以一般儲存備份的機制來看僅有例行的磁帶備份機制，其 RPO 依備份的頻率大多僅達天至周的等級，資料中心先前導入的架構已將 RPO 進化為天至小時的等級，而重要的服務系統導入同步儲存架構 On-line 層後，RPO 甚至可進化為秒至分鐘的等級，所以以 RPO 的等級而言目前資料中心的現有架構已足以應付絕大部分的需求。而 RTO 的部份原先的系統還原機制是以人力介入處理，搭配 RPO 備份的周期於服務復原後再將相關用戶及系統資料復原，這樣的服務等級對應到的 RTO 目標值僅達到小時至天的層級，而加入高可用度的改善之後，因有叢集容錯的機制，系統可以自動容錯及多重路徑的選擇，若 Active 的主機無法自動復原則將服務的控制權透過主機本身、儲存管理服務的軟體、備用主機進行切換，使系統可以繼續提供服務，而這樣子的改善也使 RTO 的目標值進化至秒至分的等級。

圖 4-12 為依照 RTO 與 RPO 的建置技術，改善後的作法與目前及一般

的備份作法對應至 RTO 與 RPO 的目標差異，一般的備份作法僅進行周期性的備份，而資料中心目前的儲存管理系統則可達到同步 RPO 的標準，但是 RTO 的目前則是停留在人工處理的流程，導入 HA 架構之後，RTO 的目標提提升至叢集自動容錯處理及自動障礙切換。

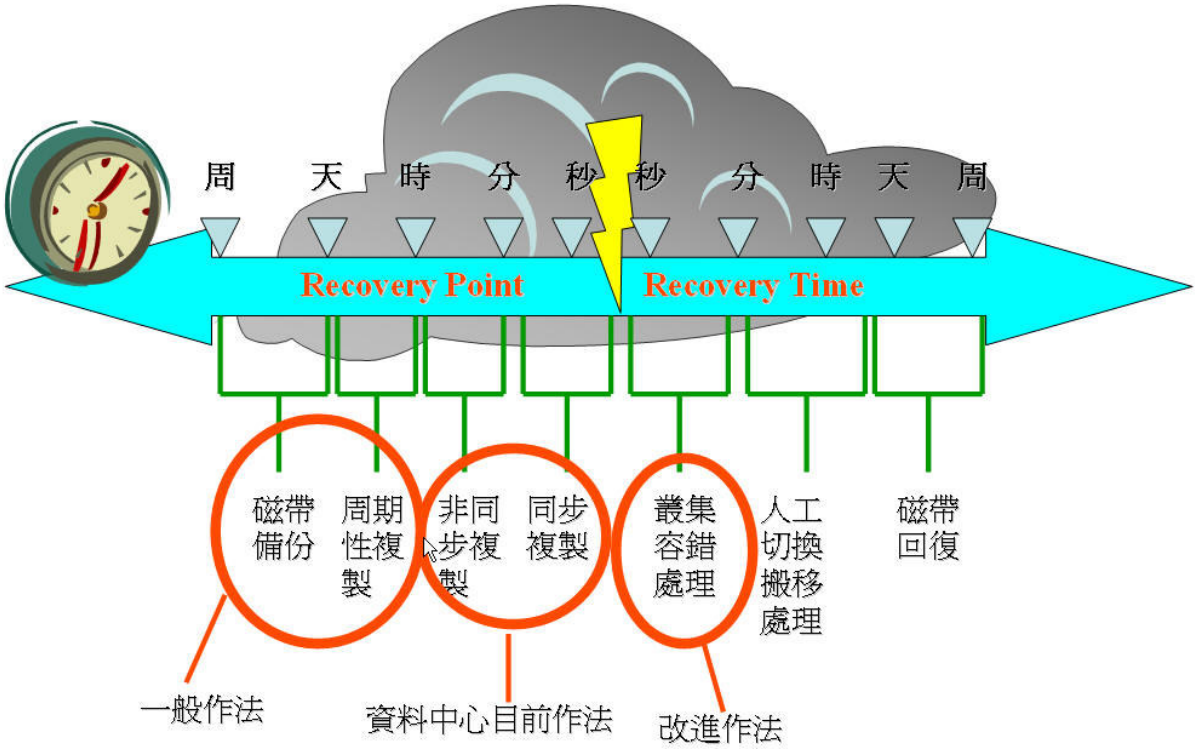

圖 4–6 建置 HA 改善的作法與先前作法及一般作法的 RPO/RTO 比較

4.2.3 高可用度建置後與先前及一般儲存作法的比較

加入高可用度(HA)架構後，當有障礙狀況發生時，雖然應用程式皆有中斷的時間。但是原架構假設發生軟體障礙時，需自行發現並手動排除；而硬體障礙發生時需待料及維護廠商的處理需時數小時至數天(此需依賴資料中心所簽訂的維護合約等級)；而高可用度架構，假設障礙無法排除，因有多餘的設備可將服務導致可用的機器，雖 Active-Standby 機制切換時服務會中斷，但卻能馬上提供給使用者持續性的服務。建置高可用度架構之後，面對障礙發生的風險會降低，儲存服務受到影響的時間會縮短，可以有更多的籌碼可以面對未知的狀況，由路由的多重選擇，系統容錯的自動切換，

可以持續的維持服務的運作，逐步改善達成不停機的目標，如同前面一直強調的增加可用度及可復原性。

綜合以上的優點，匯總了一個列表如表 4-1 用以比較建置前後的差異。

表 4-1 儲存整合改善方案建置後的比較

	一般儲存作法	東海計中作法	本研究改善作法
儲存方法	*DAS+磁帶*	*包含DR的階層式架構*	*高可用度架構*
技術組成	*DAS* *+Tape*	*Management* *+Virtualization* *+VTL* *+3 Tier HSM*	*Management* *+Virtualization* *+VTL* *+3 Tier HSM* *+HA*
檔案共享性	*不可*	*可，方便*	*可，方便*
RPO	磁帶備份	同步複製	同步複製
RTO	磁帶回復	人工介入	系統叢集容錯
服務是否中斷	*是*	*是*	*是*
影響時間	*最長*	*次短*	*最短*
風險	*最大*	*小*	*更小*
備份最小速度	12.5MB/s	250MB/s	250MB/s
效益	1倍	>20倍	>>20倍
說明	磁帶備份速度為15 MB/s，Ethernet存取進度為100 Mb/s=12.5MB/s， SCSI磁碟介面速度實際約80MB/s，FC-SAN介面為2Gbps=250MB/s		

4.2.4 降低管理成本

當只有一套系統維持所有的服務時，若這是屬於非常重要性的服務。系統管理人員需要安排密集的時間來監控系統是否正常，服務是否穩定，深怕這個重大服務如果出問題，需要更多的人力及資源來進行災害復原的動作。建置自動回復的 HA 架構，可於異常的關鍵時刻自動執行切換至可用備援系統的動作，對於後者而言，系統自動切換表示服務可以正常，對於異常的狀態，可以關心並從容的找出原因來處理，但前者需要面對使用者對回復系統要求的壓力，只能以最迅速治本的方式來恢復服務，若相同的障礙原因無法排除，這樣的障礙會持續發生影響性會持續擴大，而所需投入的人力、時間、管理成本也相對的會拉大。

4.2.5 復原成本比較

此架構縮短了系統障礙復原的平均時間，也減少了因服務中斷而導致的損失成本，損失的成本在企業方面是可以用金額來表示障礙的時間逐漸減少了公司的營收，而隨著時間增加而損失成本以倍數計，而校園的損失包含了許多無形的成本，如損失成本包含時間、校譽、行政效率、師生的權益、各校競爭的評鑑等等…。

4.3 校務系統導入改進儲存架構並建立最適的 RTO/RPO 目標

校務系統提供了許多大大小小不同的服務，而這些服務有共同點也有相異點，而資料中心現有的儲存的資源不可能將所有的服務皆導入最好的儲存架構內，所以必需要依照使用單位的需求、服務的重要性及一些相關問題發生時的服務可接受度來進行有效的儲存資源的分配，利用不同服務訂立不同的 RTO、RPO 標準，來規劃出更好的災難復原應變計劃及資源調整。

為了讓儲存資源有效的被利用，首先需針對各別的服務進行分類，我們先由使用者的角色來分類，資料中心使用者的角色主要有學校職員、教師及學生，還有其它的如校友、協助廠商…等等，使用的服務有共用的部分如 USSC 個人帳號服務、會計帳務管理系統、全球資訊網、學務系統、郵件服務、個人網站/網路硬碟、BBS 等；校務系統的運作主要是以學校職員日常行政工作為主，所以有總務系統、差勤系統、公文系統、人事系統、校務評鑑、職員資訊系統等等，教師部份則有教師資訊系統及學術研究成果管理系統，學生則有學生資訊系統，再加上其它的使用者提供如校友系統、校牧系統等，如表 4-2 所列。

圖 4–7 校務系統介紹

表 4-2 校務系統依使用者與共用性分類

共用服務	非共用服務	使用者
USSC 個人帳號服務 會計帳務管理系統 全球資訊網 學務系統 郵件服務 BBS 個人網頁/網路硬碟	總務系統 差勤系統 公文系統 人事系統 校務評鑑系統 職員資訊系統	校務職員
	學術研究成果 教師資訊系統	教師
	學生資訊系統	學生
	校友系統 校牧系統	其它

這一章我們實作的目標在於實際儲存架構的執行面，首先我們需要彙集系統服務使用者的需求資料，例如各別服務的作業時間、對於儲存系統效能、速度、空間等的要求，系統障礙最大的容忍度，是否需要技術窗口及對應技術層級的提供，計劃性停機與維護的要求條件，對儲存服務可用性與復原能力的期望值，以及此項服務的重要性。

再則資料中心這邊需要依使用者一般的需求及系統管理者的經驗先定

義出儲存管理服務層級的類別，依 SLA 的層級對應現有儲存架構中適合的儲存方式，一步一步的導入到儲存系統中，然後再建立針對服務品質量測的機制，持續的進行效能的量測並產出統計報表，依報表呈現的結果持續進行服務儲存層級的調整，依此循環調整至最好的儲存架構，整體的改善流程如下圖。

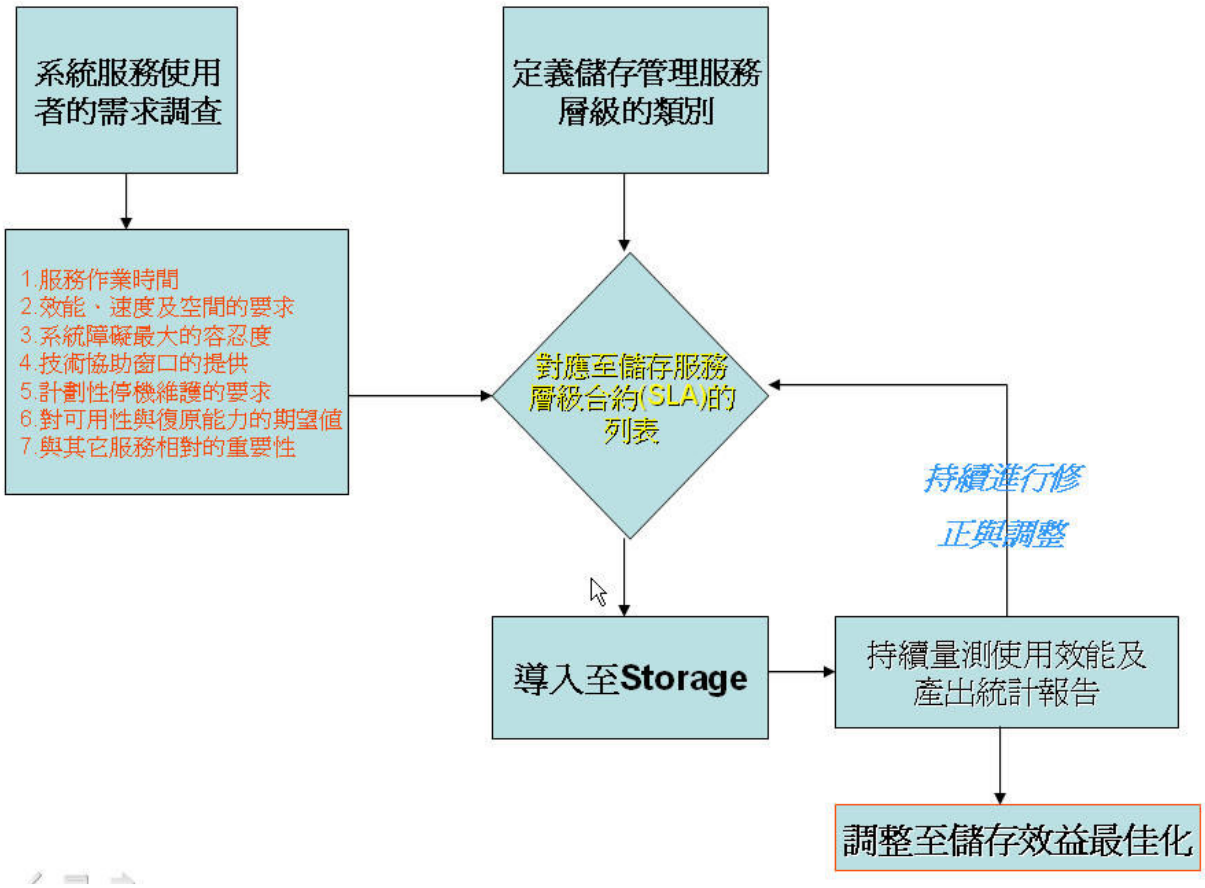

圖 4–8 服務需求與 SLA 的導入改善流程

前一章我們有提到要依照 SLA 的規劃將校務系統的服務導入至改善後的儲存架構，依照 SLA 管理的流程，首先我們需要定義一些需用到的 SLA 參數，定義的參數說明如下：

- 使用者類別

以目前建置的校務系統的使用者來區分，因校務系統主要在執行校務行政流程上電子化的運作，所以使用的比重以校務行政的教職員為主，另外會有一般的教師與學生及其它如校友、協助廠商等可歸類於其它使用

者，其中因為學生與教師的使用層級相同，故使用者類別分為三類，教職員、教師與學生、其它使用者。

- 系統共用類別

因相關的校務服務系統可能提供的對象為單一類別的使用者或是同時提供二種以上甚至是全部的使用者類別來使用，依此可以定義出服務是否提供給不同使用者共用，以突顯其重要性，此類別定義為二類，共用與非共用。

- 讀寫存取性質類別

此類別區分為三個等級，分別是讀寫、僅讀取及僅備份，校務系統後端的資料可能經過複製或直接存入儲存系統，儲存之後的功用也不盡相同，有的資料會被重新讀取寫入後更新，例如一些表單系統的資料、有的資料則不會再異動僅提供讀取使用，例如郵件服務系統，而更有一些是僅作為日後備份存檔配合法規保存的時限，或僅進行備份但使用率極低。

- 異動頻率類別

依據資料於一段時間資料存取的異動率做為評估的要點，資料的取得由原先使用者的預估值至導入儲存系統後，系統管理者持續的量測平均值，這邊分為三種異動頻率，高異動頻率為每小時內有進行資料異動，中等異動頻率為平均一天之內會進行資料異動，低異動頻率為一周之內有進行資料異動。

- 障礙容忍度要求類別

此類別分為四種層級，第一級為四小時內，因一般障礙若系統管理人員無法自行排除，依照與廠商的維護合約最緊急的處理方式為廠商接獲通報處理需要四小時之內處理完成，第二級為一天內，此為一般廠商為當日工作日能夠處理完成的保證，第三級為三天內，此狀況為配合廠商當日無法處理完成需要更換硬體設備等待料件，或尋求上一層的廠商支援，而第

四級為一周內，此等級一般為無維護合約，系統障礙時需要依個案狀況自行研判問題，連絡配合廠商叫修處理(By Call)，所以處理時效較無法保證。

依照以上的 SLA 參數，我們定義了五個 SLA 的層級，判斷的標準如下圖所示，第一級的 SLA 為教職員、教師、學生的共用系統，且存取功能為讀寫，每一小時內皆有資料存取的活動產生，而障礙的容忍度為四個小時以內，可以導入 SLA 1 對應的儲存階層；而第二級的 SLA 則是延伸第一級的架構，當以下三種條件如服務為非共用或是異動頻率為中等及服務的障礙容忍度為一天內，只要其中一項條件成立就歸類為 SLA 2，而當使用者為使用類別第 3 級的其它使用者時，則歸類為 SLA 3，第四級 SLA 為存取類別為僅供讀取以及障礙容忍度為三天內，當其中一項條件成立就歸類為 SLA4，第五級則為讀取類別僅供備份、異動頻率低、障礙容忍度為一周，則可歸類為 SLA 5。

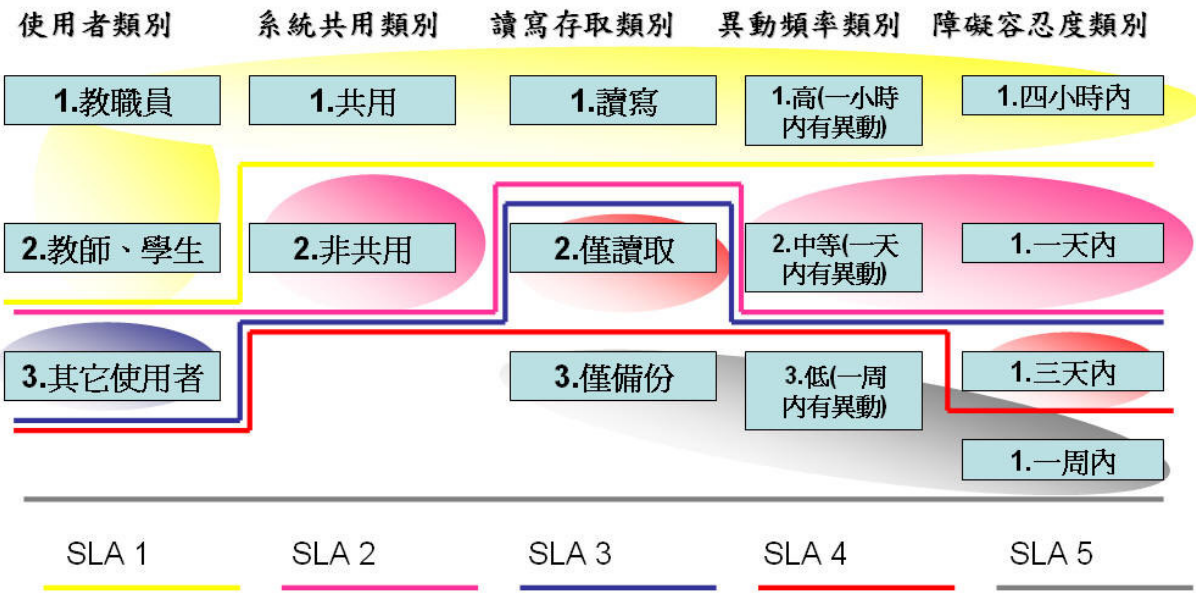

圖 4-9 SLA 的參數定義流程

由系統服務使用者的需求單的資料彙整後，配合 SLA 的設定檔，目前校務系統的 SLA 層級可對應如下表，USSC 個人帳號服務的 SLA 層級為 1，主要判別為此服務為教職員及師生使用的共用系統，儲存資料的存取要求高且異動頻率也高，而障礙的容忍時間為一小時內，故設定至最高級的 SLA

1，而大部分的校務系統皆歸類至 SLA 2 的層級，因校務系統每日皆在持續使用，異動頻率為每日，障礙時間的容忍度為一天，所以依照 SLA 的分配規則設定在第二層，而個人網頁/網路硬碟及學術研究成果，因障礙容忍度時間為三日，故歸類至 SLA 4 的層級，郵件系統的備份資料因存取性質多為讀取，且用戶可自行下載至 PC 端儲存，故也歸類至 SL4，而校園的 BBS 服務及校友、校牧系統因障礙可容許時間為一周，故歸類為 SL 5。

表 4-3 校務系統 SLA 等級

校務系統服務名稱	使用者	共用系統	資料結構化	導入SAN儲存系統	儲存檔案存取性質(讀或寫)	異動頻率	儲存容量	障礙時間容忍度	異動資料保存周期	SLA
USSC 個人帳號服務	校務職員 教師 學生	是	是	Y	讀寫	高	XXX	一小時內	2天	1
會計帳務管理系統	校務職員 教師 學生	是	是	Y	讀寫	中等	XXX	一天	6天	2
全球資訊網	校務職員 教師 學生	是	是	Y	讀寫	中等	XXX	一天	3天	2
BBS	校務職員 教師 學生	是	否	Y	讀	低	XXX	一周	無	5
個人網頁/網路硬碟	校務職員 教師 學生	是	否	Y	讀寫	中等	XXX	三天	3天	4
學務系統	校務職員	否	是	Y	讀寫	中等	XXX	一天	6天	2
郵件服務	校務職員	否	是	Y	讀	中等	XXX	一天	1.5天	4
總務系統	校務職員	否	是	Y	讀寫	中等	XXX	一天	6天	2
差勤系統	校務職員	否	是	Y	讀寫	中等	XXX	一天	6天	2
公文系統	校務職員	否	是	Y	讀寫	中等	XXX	一天	6天	2
人事系統	校務職員	否	是	Y	讀寫	中等	XXX	一天	6天	2
校務評鑑系統	校務職員	否	是	Y	讀寫	中等	XXX	三天	6天	4
職員資訊系統	校務職員	否	是	Y	讀寫	中等	XXX	一天	6天	2
學術研究成果	教師	否	是	Y	讀寫	中等	XXX	三天	24天	4
教師資訊系統	教師	否	是	Y	讀寫	中等	XXX	一天	6天	2
學生資訊系統	學生	否	是	Y	讀寫	中等	XXX	一天	6天	2
校友系統 校牧系統	其它		是	N	讀	低	XXX	一周	無	5

依據現有儲存架構可以定出 5 個層級的儲存資源可以提供給校務系統的服務導入使用，分別是 On-line 層使用 mirror 技術、On-line 層 snapshot 技術、On-line 層 TimeMark 技術，及 Near-line 層與 Off-line 層，這 5 個層級剛好可以對應至目前歸類的 5 項 SLA 的層級，依此對應方式導入至階層式儲存架構。

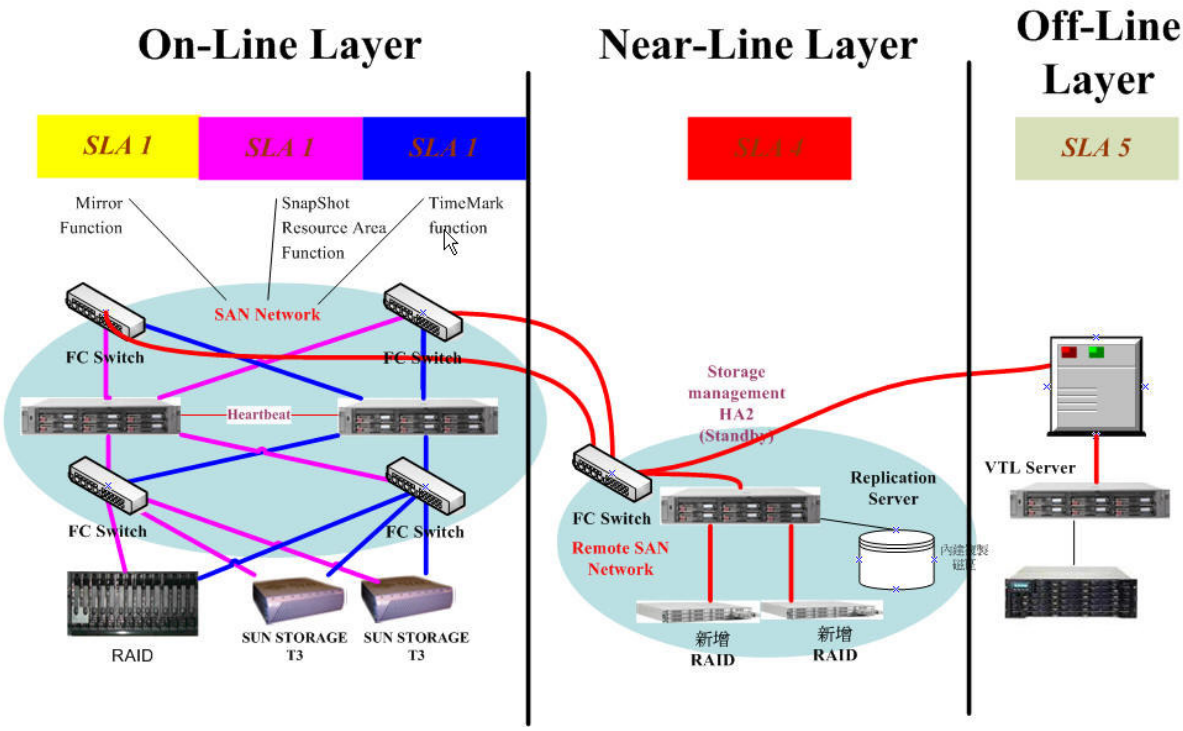

圖 4-10 SLA 層級導入現有儲存階層

而 SLA 1 至 3 儲存位置目前位於資料中心的 On-line 層，依照分散風險的原則，我們可以於 Near-line 層再複製一份副本，並同時可以執行例行備份作業至 Off-line 層，便可以依照此不同層次的差異性來各別訂定符合服務需求的 RTO、RPO 目標。

關於 On-Line 層的 RTO 與 RPO 目標，因此層 RTO 取決於系統自動回復的時間，因改善後的架構當障礙發生可以選用的 FC 路徑及切換至儲存管理系統的備援主機，在沒有遭受到雙主系統皆發生重大障礙或後端實體儲存設備二部以上的失效的狀況下仍然可以維持服務的可用度，但由於是 Active-Standby 的架構，所以仍會有停機時間，所以 RTO 的目標可以訂在一個小時以內，而 RPO 的標準則以差異性的備份映像檔 TimeMark 為依據，例如像會計、差勤、人事、公文等系統目前資料中心以每一小時做一次 TimeMark 資料的複製，而總務、學務、教務則以每三小時做一次複製，重要的認證異動資料 USSC 則以每三十分鐘複製一次，依此複製頻率成為各項服務的 RPO 標準。

表 4-4 校務系統於 On-line layer 的 RTO/RPO 目標

服務名稱	HA(Online)-SLA 1~3				
	IPStor support tech			RTO (服務回覆時	RPO (資料損失時
	data mirror	data snapshot	data TimeMark		
個人網站/網路硬碟	X	X	X	NA	NA
bbs站台	X	X	X	NA	NA
總務系統	X	✓	3hrs	1hrs	3hrs
學務系統	X	✓	3hrs	1hrs	3hrs
教務系統	X	✓	3hrs	1hrs	3hrs
會計出納系統	X	✓	1hr	1hrs	1hr
差勤系統	X	✓	1hr	1hrs	1hr
人事系統	X	✓	1hr	1hrs	1hr
公文系統	X	✓	1hr	1hrs	1hr
學術研究成果系統	X	X	X	X	X
webmail(tmail)	X	X	6hrs	1hrs	6hrs
個人帳號服務中心(USSC	✓	✓	30 mins	1hrs	30 mins
電子郵件	X	X	X	X	X

關於 Near-Line 層的 RTO 與 RPO 目標，本儲存階層的 RTO 系統回復目標值為四個小時，當 On-line 層發生障礙無法於 RTO 回復目標一小時內完成，此時 Near-Line 層將接手系統障礙及服務復原的工作，可將第二層的儲存設備直接改接至原第一層同步復製的工作，若是有硬體上的故障也可依照與廠商契約約定最短四小時內進行障礙排除的工作，Near-line 層的功能主要是提供異地備援的功能，可以定義副本資料保存的天數，由 Replica 的複製周期乘上 TimeMark 的次數即可設定好要儲存資料的天數，依服務的需求性可以提供使用者所需的保留天數，而 RPO 的目標值則是取決於各別服務設定的 Replica 複製周期。

表 4-5 校務系統於 Near-line layer 的 RTO/RPO 目標

服務名稱	Replication（NearLine，DR Site)-SLA 4			
	Replica (同步週期)	TimeMark (for Replica)	RTO (服務回覆時間)	RPO (資料損失時間)
個人網站/網路硬碟	6 hrs	12 times	4 hrs	6 hrs
bbs站台	X	X	X	X
總務系統	6 hrs	24 times	4 hrs	6 hrs
學務系統	6 hrs	24 times	4 hrs	6 hrs
教務系統	6 hrs	24 times	4 hrs	6 hrs
會計出納系統	6 hrs	24 times	4 hrs	6 hrs
差勤系統	6 hrs	24 times	4 hrs	6 hrs
人事系統	6 hrs	24 times	4 hrs	6 hrs
公文系統	6 hrs	24 times	4 hrs	6 hrs
學術研究成果系統	24 hrs	24 times	4 hrs	6 hrs
webmail(tmail)	12hrs	3 times	4 hrs	12 hrs
個人帳號服務中心(USSC	3 hrs	16 times	4 hrs	3 hrs
電子郵件	12hrs	3 times	4 hrs	12 hrs

關於 Off-line 層的 RTO 與 RPO 目標，此層為原有的例行備份作業，系統服務復原的時間需要搭配資料中心的營運持續計劃規範的障礙時間二十

四小時，RPO 的目標為各校務系統服務的備份週期。

表 4-6 校務系統於 Off-line layer 的 RTO/RPO 目標

服務名稱	Backup（Offline）-SLA5			
	VTL			
	備份週期	全備份份數	RTO	RPO
個人網站/網路硬碟	3 day	2	24 hrs	3 day
bbs站台	1week	2	24 hrs	1week
總務系統	1 day	3	24 hrs	1 day
學務系統	1 day	3	24 hrs	1 day
教務系統	1 day	3	24 hrs	1 day
會計出納系統	1 day	3	24 hrs	1 day
差勤系統	1 day	3	24 hrs	1 day
人事系統	1 day	3	24 hrs	1 day
公文系統	1 day	3	24 hrs	1 day
學術研究成果系統	1 day	3	24 hrs	1 day
webmail(tmail)	1 day	2	24 hrs	1 day
個人帳號服務中心(USSC	1 day	7	24 hrs	1 day
電子郵件	1 day	2	24 hrs	1 day

依以上的 SLA 定義流程及 RTO、RPO 的目標值，可以讓實際的儲存服務系統維運的目標及量測的指標更為明顯，在未來也將會持續進行服務品質的監測，由監測產生的數據來檢視是否都在 RTO、RPO 的目標值之內，並進行持續的改進計劃。

第五章 結論

本論文提出的系統架構，由技術面來看其貢獻在於提高校園資料中心儲存系統的可用度及可復原性，能夠在有效的預算及資源下，評估現有儲存環境適合的高可用度架構，透過多方向如網路、系統的高可用度來達成更好的投資報酬率及更佳的儲存效益，藉由儲存網路架構的變更，提升儲存網路資料流的速度與穩定度，較建置前為佳的容錯及自動 Fail over 機制，減少需人員介入的管理人力及停機風險，更完整的災難復原架構，更好的系統儲存還原效能。

由日後維運管理的技術面來看透過 SLA 定義出現有校務系統服務需求的標準流程，能夠更有效的定義出儲存服務提供給前端應用服務的目標值

在那裏，能夠持續的量測及調整現有的儲存架構至最有效益的方式，並能夠符合資料中心所規範的持續營運計劃。

問題發生的時間，通常要快速的解決問題需要找到對的人、對的需求部門，而儲存服務需要找到對的儲存方法，在本文中就是要找到對的儲存層，同時符合成本效益與使用者需求滿足。

資料儲存的目的是在保護資料，並確認資料可以提供使用，但在面臨火災、地震、颱風等天災；病毒、駭客、人員操作不當等人禍，及系統、設備及日常維運發生的損害等意外，資訊人員需要不斷的強化資料保護及保存的基本作業。但這樣的處理作業是需要持續性的進行，並不是一蹴可及的，只能透過一階段一階段來進行改善，持續縮短 RTO/RPO 的時間目標值，並以降低總持有成本(TCO)及達成最佳投資報酬率(ROI)為目標，好的應用系統需要資訊維運人員的實作經驗來動態的判斷與調整，未來的研究方向朝向實作系統導入 ILM 的政策，依實際的維運經驗增加需要的屬性值及判斷式，以符合日益複雜的應用程式及網路架構，並精算實際改善後效能的提升、成本的降低，並推廣於更複雜的企業環境中，以上為本篇論文所提出的宗旨。

參考文獻

[1] 李俊隆，論災難備援計畫在資訊安全的重要性－以美商 CTS Corporation 為例，國立中山大學資訊管理學系研究所碩士論文，2003 年 7 月。

[2] 蒲樹盛(2006),風險控制策絡概論，2006 年 7 月取自 http://risk.rdec.gov.tw/Upload/A15/SmrFile/43.pdf

[3] HITACHI(2006)，業務永續服務解決方案簡介，2006 年 1 月，取自

http://events.ap.seeuthere.com/hds/tw/2006/09/newsletter/file/01BC_Solution_Brief.pdf

[4] IT home(2007)，異地互援，2007 年 2 月，取自 http://www.ithome.com.tw/itadm/article.php?c=41951

[5] Bulent Abali, Dan Poff, Mohammad Banikazemi, Storage-Based Intrusion Detection for Storage Area Networks(SANs), Proceedings of the 22nd IEEE/13th NASA Goddard Conference on Mass Storage Systems and Technologies(MSST'05)

[6] Edward K. Lee, Highly-Available,Scalable Network Storage, 1995 IEEE

[7] IT home(2006), 2006 儲存技術趨勢：降低成本、提高傳輸率, 2006 年 5 月 3 日，取自 http://www.ithome.com.tw/itadm/article.php?c=36992&s=1

[8] http://sdm.lbl.gov/srm-wg/papers/SRM.book.chapter.pdf ,Arie Shoshani, Alexander Sim, and Junmin Gu, Storage Resource Managers: Essential Component for the Grid, Lawrence Berkeley Naitonal Laboratory.

[9] Ying Chen, Information valuation for Information Lifecycle Management. Proceedings of the Second International Conference on Autonomic Computing (ICAC'05)

[10] Katarzyna Keahey, 1st IEEE/ACM international workshop on virtualizaion technologies in distributed computing, Proceedings of the 2006 ACM/IEEE conference on Supercomputing, 2006

[11] Michael Peterson, Edgar st. Pierre , SNIA's vision for ILM, http://www.snia.org/forums/dmf/knowledge/archives/SNIAs_Vision_for_ILM-SNWOct04.pdf, October 2004.

[12] Kembel, Robert W. The Fiber Channel Consultant: Fiber Channel Switched Fabric. Tucson, AZ: Northwest Learning Associates, 2001.

[13] http://www.falconstor.com/en/library/?pg=WhitePapers, FalconStor Software, Inc.,IPStor_Dynapath,White Papers.

[14]皮世明，許通安，范金爭強，影響資訊系統服務品質的因素研究，資訊管理研究第三卷第一期，2001 年 1 月

[15]Jong-Tae Park, Jong-Wook Baek, Management of Service Level Agreements for Multimedia Internet Service Using a Utility Model,IEEE Communications Magazine, May 2001..

[16]Eric Bouillet,　Debasis Mitra, Fellow, IEEE, and K.G.Ramakrishnan, The Structure and Management of Service Level Agreements in NetworkS.

[17]R. Baird, Virtual Storage Architecture Guide (VSAG), Hewlett-Packard Corporation.

[18]Edward K.Lee, Highly-Available, Scalable Network Storage, Digital Equipment Corporation.

[19]Toigo, Jon William. Disaster Recovery Planning. Upper Saddle River, NJ: Prentice Hall, 2002.

[20]http://www.itri.org.tw/chi/southern_branch/ccl_01c.jsp，儲存網路 iSCSI 介面技術，財團法人工業技術研究院，南部分院，研發，網路與通訊技術。

[21]http://storage.ithome.com.tw/，技術智庫，微軟儲存百科網。

[22]. http://www.falconstor.com/en/library/?pg=WhitePapers, FalconStor Software, Inc., Accelerating Backup/Restore with the Virtual Tape Library Configuration That Fits Your Environment, White Papers.

[23]http://www.falconstor.com/en/library/?pg=WhitePapers, FalconStor Software, Inc., Heterogeneous Midrange Storage with Local Mirroring and Remote IP Replication, White Papers.

[24]http://www.falconstor.com/en/library/?pg=WhitePapers, FalconStor Software, Inc., Strategies for Accelerated Backup and Immediate Recovery: Going Beyond Traditional Backup Methods, White Papers.

[25]Jiwu Shu, Bigang Li, and Weimin Zheng, Design and Implementation of an SAN System Based on the Fiber Channel Protocol., IEEE Transactions on

Computers, VOL54, NO4, APRL 2005

[26]經濟部標準檢驗局，ISO 27001:2005 資訊安全管理系統要求,http://www.bsmi.gov.tw/upload/b05/b0503/cns17800/ISO27001.pps

[27]P. Lyman, H. R. Varian, K. Swearingen, P. Charles, N. Good, L. L. Jordan, J. Pal. How much information?2003 , http://www2.sims.berkeley.edu/research/projects/how-much-info-2003/printable_report.pdf