向內憂外患 Say No!
ASUSTOR NAS 由內而外的資安攻略

以往人們習慣將重要資料、文件儲存在外接儲存裝置分別收藏，認為這是一種安全的儲存方式。然而隨著時代的變遷，資料文件大量e化後，許多人逐漸棄外接儲存而轉往存取便利的雲端儲存，一是疲於對記憶力的挑戰，二是免於裝置未隨身攜帶時面臨開天窗的窘況。公有雲的興起衍然成為網路世代的生活型態之一，然而隨之而來的資安問題卻也層出不窮，因此選擇NAS來打造私有雲端的使用族群逐漸增加，除了能自主掌握資料外，NAS所具備的安全設置彈性能降低儲存世界中「內憂外患」的威脅，進一步保障資料的安全。

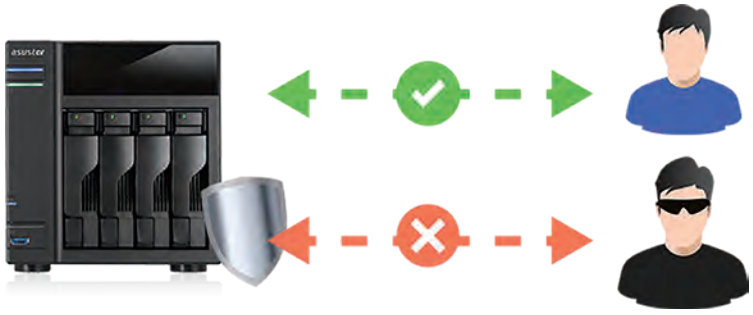
由內而外的防護罩

將資料存放在公有雲的確便利存取，使用者不需要煩惱硬碟是否會產生壞軌，也無需更換硬碟，在管理上看似省事，但實際上卻有著帳號被盜、資料遺失或外流的風險；而利用NAS如ASUSTOR來打造私有雲，不僅能提供完善的備份方案，於系統、網路及資料等安全選項上也不遑多讓，可藉由簡易的操作介面完成由內而外的安全設置，形成堅不可摧的防護罩，層層保障資料及網路的安全。

系統網路安全

為了保障使用者的連線安全，ASUSTOR NAS除了可設定登入錯誤的容許次數，以及二步驟驗証的登入外，在網路連線防護上甚至提供多重機制來阻絕惡意連線。例如，在不需要存取的時間區段中設置定時休眠及開關機時間，當需要存取時再利用網路喚醒機制回復系統運作；此外，如同電腦設置一般提供了ADM Defender選項，使用者可利用內建的防火牆及黑白名單的管理，針對各別的通訊埠來決定允許或封鎖特定用戶端的IP位址，或將特定IP設定為信任清單，因此即使登入時的錯誤次數超過限制，也不會被鎖入黑名單中。啟用黑名單後，也能依IP位址、區段、甚至來源國家、地區來定義，而列入黑名單的IP將無法使用SAMBA、AFP、FTP、HTTP、SSH等服務，來提高網路連線上的安全性。

富彈性定時系統休眠及開關機。



黑白名單的設置可提高網路連線安全性。

資料安全

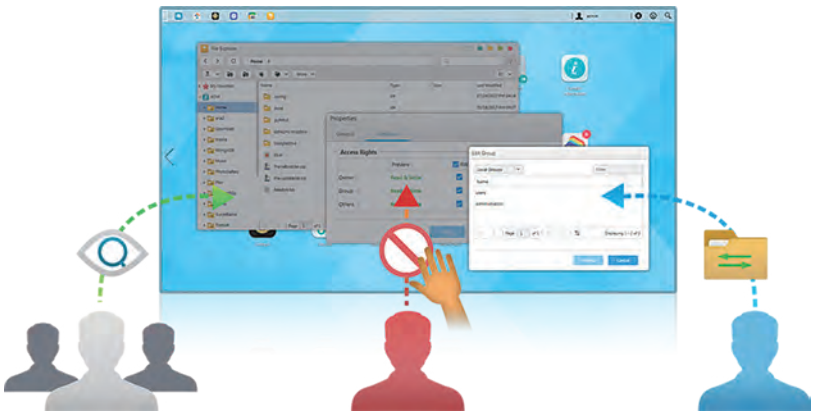
備份在保障資料安全中有著不可撼動的一席之地，如同前期所提及的備份3-2-1原則，基於風險分散的概念，使用者若能掌握此原則，即能在不同的裝置及空間中擁有多份相同的資料。而有別於備份，將NAS硬碟設置為磁碟陣列，即能在資料存入NAS的那一刻起受到保護。磁碟陣列是依硬碟的使用數而有不同的設置，倘若使用2 bay的NAS，那麼最佳的硬碟保護設置則為RAID 1，此設置能將資料在儲存時同時寫入二顆硬碟中，萬一其中一顆硬碟出現壞軌，資料還是存在另一顆硬碟中而不影響讀取，此時，只需更換一顆新的硬碟，系統即會自動重建磁碟陣列保持運作。

ASUSTOR NAS提供磁碟陣列設置以保護資料。

另一個保護資料的功能莫過於快照（Snapshot）了，華芸快照是基於儲存空間的快照技術，能將存放在NAS上的資料完整建立複本，建立快照時可依單次、每日、或每週的頻率，每五分鐘至十二個小時不等來建立快照，最多可建立256個快照檔案，倘若資料意外遭破壞或刪除，則可回溯日期，倒帶回到特定日期時的資料狀態。

華芸ADM 3.0以上即支援快照，保護資料無時差。

除了上述二種保護資料的方法外，存取權限的設置則是依人來管理存取保護資料，例如在華芸NAS上可設定如Windows般的存取權限，嚴格管控資料存取角色，讓NAS可以是個人專用的設備，也適合多人共享；在實務上甚至可將機密資料夾進行加密後，搭配密碼來存取資料，此功能提高了商務人士或是多人共用裝置時對NAS的信任度與安全感。



Windows存取權限設定。

華芸採用AES 256位元資料夾加密技術，更嚴密的來保障用戶的機密資料。

結語

在前一期中筆者向大家闡述了NAS的備份及防駭對策，例如登入時的雙重身份認証、資料夾加密以保障高機密文件的存取安全。事實上NAS在資安上能做的還不僅於此，其中更包含了許多安全性上的設置細節，來提升系統及資料的安全性。ASUSTOR NAS挾容量自主的優勢，提供了有如防護罩般的安全措施，只要充份運用這些相關的安全設置，就能使系統、網路以及資料，由內而外得到多層級的安全守護，輕鬆打造一個安全無虞的雲端儲存空間你我都可以！