

Power Admin File Sight Ultra

提供您使用者檔案存取監控、完整的檔案存取軌跡稽核記錄及報告



請告訴我！今天誰存取過公司的機敏檔案？

這件事情看來似乎簡單！但是，事實上呢？

為何需要機敏檔案存取軌跡稽核

何人？在何時？做了何事？

IT 管理標準程序需要它！

法規遵循服務稽核需要它！

您，該如何提供相關的檔案存取軌跡稽核紀錄呢？

需要哪些存取軌跡稽核資料

檔案及目錄 建立、刪除

檔案及目錄 讀取、寫入

檔案及目錄 移動、重新命名

擁有者變更、存取權限變更、稽核設定變更

用戶端檔案複製追蹤 *

用戶端電腦名稱及來源 IP 位置 ***

概觀

PA File Sight Ultra 是您在沙賓法案以及 PCI DSS 支付卡產業資料安全標準法規遵循中，協助您執行軌跡稽核的重要工具的一部分，甚至更多；PA File Sight Ultra 可以提供您在先前所無法獲得的伺服器檔案存取軌跡稽核紀錄。

PA File Sight Ultra 提供詳盡的 Windows 伺服器檔案稽核、報表及警示，它可以幫助管理者瞭解何人(帳號、電腦名稱、IP)於何時對伺服器上之重要文件(檔案及目錄)，正在進行新增、修改、刪除、移動或更改名稱！除此之外，您還能瞭解是哪一個程式做了這個動作！

PA File Sight Ultra 也提供使用者檔案存取軌跡監控，並提供完整的檔案存取稽核記錄及報告。透過報表系統更可以協助您瞭解過去發生了哪些事件！（譬如說：誰在何時存取了哪些檔案？）。甚至於可以封鎖惡意存取行為的使用者以杜絕惡意存取或勒索病毒入侵。 **

* 用戶端電腦需安裝 File Sight Endpoint Agent

** 可依據存取條件自訂使用者封鎖機制 Block User

*** 被稽核之主機作業系統為 Windows 2008R2 (含)以後方支援此功能

功能及優點

- ✓ 安裝簡單，程式安裝及設定僅需 1~2 分鐘
- ✓ 僅需指定欲監看之檔案類型及路徑，即可立即進行檔案稽核監看
- ✓ 以服務的方式啟動，因此當您的系統啟動後就可以立即進行稽核監看 - 無須登入系統或手動啟動程式
- ✓ 提供檔案存取稽核：Reads (讀取)、Writes (寫入、修改)、Creates (新增)、Deletes (刪除)、Moves (移動)、Renames (變更名稱)、Permission Changed (存取權限變更)、Owner Changed (擁有者變更)、Audit Setting Changed(稽核設定變更)，並可以稽核出用戶端電腦名稱及來源 IP 位置、以及用戶端複製檔案(Remote Files Written) *
- ✓ 提供監看白名單功能：File Types (檔案類型)、Files (特定檔案)、Subdirectories (特定目錄)、Users (使用者帳號)、Processes (程序)
- ✓ 提供檔案存取、使用者登入帳號及存取程式之紀錄，可依存取使用者、類型或時間類別產生稽核報表
- ✓ 可自訂依據特定存取行為即封鎖使用者存取能力 **
- ✓ 稽核記錄資料存放於資料庫 (MS SQL、Express)，增加稽核紀錄資料之穩定度及安全性
- ✓ 提供不同條件之報表產生：日期 / 時間、伺服器、使用者帳號、存取事件型態、檔案路徑、處理程序
- ✓ 提供 HTTP 網頁化基礎之稽核報表方式，可直接經由瀏覽器查看稽核報表，並提供瀏覽權限控管
- ✓ 可排程自動產生稽核報表，並經由電子郵件將報表連結(URL)傳送給管理者，無需繁複的固定產生報表工作
- ✓ 可依管理需求，提供管理者依照稽核需求條件設定警示/警訊通知：email、SMS、SNMP、SNPP pager 等；或是啟動指定動作（執行 Script、重啟服務、重新開機、寫入記錄檔或 Event Log... 等）



機敏檔案存取軌跡稽核 Power Admin File Sight Ultra

提供您使用者檔案存取監控、完整的檔案存取軌跡稽核記錄及報告

稽核類別

- ✓ File Types (檔案類型)
- ✓ File Activities (檔案活動)
- ✓ Directory Activities (目錄活動)
- ✓ User Activities (使用者活動)
- ✓ Streams and Behaviors (串流及行為)

檔案及目錄活動(存取軌跡)稽核

- ✓ Creates (建立)、Deletes (刪除)
- ✓ Reads (讀取)、Writes (寫入)
- ✓ Moves (移動)、Renames (重新命名)
- ✓ Owner Changes (擁有者變更)
- ✓ Permission Changes (存取權限變更)
- ✓ Audit Setting Changes (稽核設定變更)
- ✓ User Computer, Address (用戶端電腦名稱、IP) ***
- ✓ Remote Process (遠端程序) *
- ✓ Remote Files Written (遠端檔案寫入) *
- ✓ Remote User (遠端使用者) *

稽核排除

- ✓ File Types (檔案類型)
- ✓ Files (特定檔案)
- ✓ Subdirectories (特定目錄)
- ✓ Users (使用者帳號)
- ✓ Processes (程序)

稽核報表

- ✓ 日期 / 時間
- ✓ 伺服器
- ✓ 使用者帳號
- ✓ 存取事件型態
- ✓ 檔案路徑
- ✓ 處理程序
- ✓ 用戶端電腦名稱 / 用戶端 IP 位置 ***

存取控制

- ✓ 提供中央控管及遠端衛星管理機制
- ✓ 中控服務主機提供容錯轉移機制(Automatic Fail Over)
- ✓ 以角色為基礎的存取控制
- ✓ 以群組為基礎的可視範圍

系統需求

- ✓ 記憶體：50 ~ 300 MB
- ✓ 磁碟空間：50MB ~ 10GB (程式使用約 15MB · 報表檔約 10MB · 其餘空間決定在稽核記錄之保留時程)
- ✓ Internet Explorer 9 or later
- ✓ Microsoft .NET Framework 2.0 or later (檢視狀態報表時)

資料庫需求

- ✓ Microsoft SQL Server 2008 / 2008 R2 / Express
- ✓ Microsoft SQL Server 2012 / Express
- ✓ Microsoft SQL Server 2014 / Express
- ✓ Microsoft SQL Server 2016 / Express
- ✓ Microsoft SQL Server 2017 / Express

支援作業系統

- ✓ Windows 7 / 8 / 8.1 / 10
- ✓ Windows Server 2008 / 2008 R2
- ✓ Windows Server 2012 / 2012 R2
- ✓ Windows Server 2016
- ✓ 32 位元、64 位元作業系統皆支援

* 用戶端電腦需安裝 File Sight Endpoint Agent

** 可依據存取條件自訂使用者封鎖機制 Block User

*** 被稽核之主機作業系統為 Windows 2008R2 (含)以後方支援此功能

Power Admin 授權代理商

京祺科技股份有限公司

www.vbuster.com.tw

高雄

高雄市 80457 鼓山區中華一路 336 號 10 樓之 2

電話：07-550-2699

傳真：07-553-5291

台北

台北市 11070 信義區基隆路一段 141 號 4 樓之 10

電話：02-2747-8659

傳真：02-2747-8929

Power Admin LLC Headquarters

12710 South Pflumm Road

Suite #206

Olathe, KS 66062

USA

www.poweradmin.com

