Windows Embedded

Windows XP Embedded嵌入式功能介紹

- Enhanced Write Filter

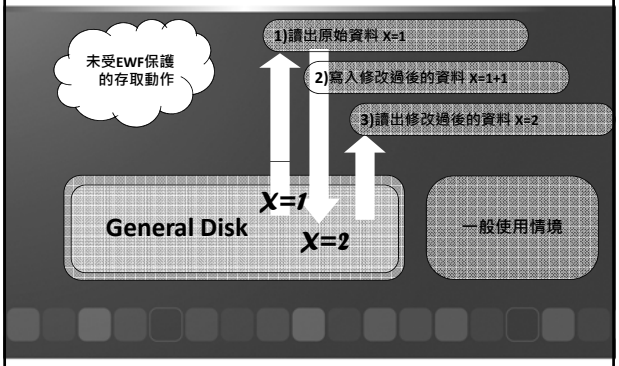
Stone Lee
FAE
Microsoft OEM Embedded Distributor

引言...

- 常見DVR系統的問題
  - 過熱、當機
  - 中毒、植入木馬
  - 磁碟寫入頻繁 (CF Card, DOM)
  - 系統設定檔遭篡改
- 解決方案 - EWF
  - EWF概念
  - EWF overlay三種模式介紹
  - EWF環境下更新檔案
  - EWF命令列
  - 常見問題

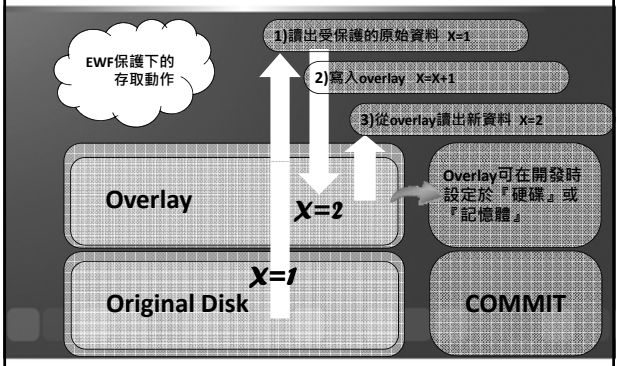
Windows Embedded

一般磁碟存取方式



Windows Embedded

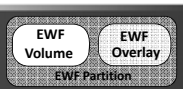
EWF存取方式



Windows Embedded

Enhanced Write Filter (EWF)

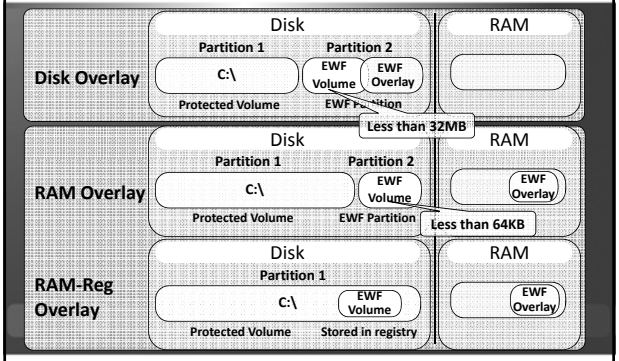
- EWF組成要件：



  - EWF Volume：會從預留的未分割磁碟空間(unpartitioned)被建立，存放所有EWF組態資料：包含被包護的磁碟數量、尺寸及Overlay層數
  - EWF Overlay：EWF暫存資料的位置，可存在於記憶體或磁碟分割
- EWF三種模式：
  - DISK mode, RAM mode, RAM-Reg mode

Windows Embedded

Enhanced Write Filter Overlay三種模式



Windows Embedded

EWF 維護及管理

- EWF Manager Console Application
  - EWF命令列管理工具
- Enhanced Write Filter API
  - EWF API support library : EWFAPI.H and EWFAPI.LIB
    - EWF API
      http://msdn.microsoft.com/en-us/library/ms933204.aspx
    - EWF API Code Sample
      http://msdn.microsoft.com/en-us/library/ms912855.aspx
    - Controlling EWF by Using the EWF APIs
      http://msdn.microsoft.com/en-us/library/ms838476.aspx

Windows Embedded

EWF命令列管理

	EWF Commands
Both mode	ALL ENABLE , DISABLE COMMIT , COMMITANDDISABLE DESCRIPTION , NOCMD
Disk mode	GAUGE SETLEVEL=[overlay level] CHECKPOINT (same as SETLEVEL =[current overlay +1]) RESTORE (same as SETLEVEL =[current overlay -1])
	以上與Overlay相關的指令需重開機後才會生效
RAM mode	EWFMGR C: -COMMITANDDISABLE -live

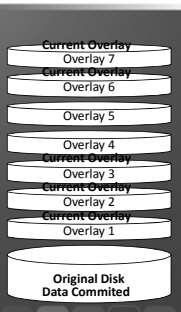
Windows Embedded

如何在EWF保護下安裝更新檔

Disk-based Overlay	RAM-based Overlay
	重新啟動以清空RAM overlay上暫存資料
使用EWF命令列 - 關閉EWF overlay >>ewfmgr c: -disable	使用EWF命令列 - 關閉EWF overlay 及 將overlay資料寫入被保護的磁區 >>ewfmgr c: -commitanddisable
重新啟動，使關閉EWF overlay生效	重新啟動，使關閉EWF overlay生效
安裝更新檔或應用程式	安裝更新檔或應用程式
使用EWF命令列 - 重新啟動EWF overlay >>ewfmgr c: -enable	使用EWF命令列 - 重新啟動EWF overlay >>ewfmgr c: -enable
重新啟動，使啟動EWF overlay生效	重新啟動，使啟動EWF overlay生效

Windows Embedded

EWF 命令列管理指令 (Disk overlay)



In this case of EWF function Definition:

The maximum supported overlay level is 7

Initial overlay level set in overlay 1 (after FBA)

>>EWFMGR C: -CHECKPOINT

Same as : >>EWFMGR C: -SETLEVEL=[current overlay +1]

>>EWFMGR C: -RESTORE

Same as : >>EWFMGR C: -SETLEVEL=[current overlay -1]

>>EWFMGR C: -SETLEVEL=3

>>EWFMGR C: -COMMIT

Windows Embedded

變更系統分頁檔位置

系統啟動分頁檔(pagefile) 將影響EWF效能，為了解除此問題，我們可以把分頁檔配置於未受EWF保護的磁區。那麼你至少需要兩個磁碟分割：受EWF保護的磁碟及非受EWF保護、可寫入的磁碟

使用登錄檔更改分頁檔位置的

- 在EWF disable的狀態下利用以下登錄檔，更改分頁檔位置：
  - Key Name: HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\
  - Value Name: PagingFiles
  - Type: REG_MULT_SZ
  - Data: D:\pagefile.sys 150 500
- 在"數值資料"欄位，可修改分頁檔存放的位置及配置的"起始大小"和"最大值" (單位MB)

Windows Embedded

EWF常見問題

- EWF磁碟環境中包含動態磁碟
- 磁碟已存在四個主要磁碟分割，使EWF partitions建立失敗
- 沒有未分割磁區或足夠的空間以建立EWF partitions
- FBA前已存在的EWF Volume未被刪除

Windows Embedded