ERA v6 防毒管理系統問題分析工具

https://www.seekinfo.com.tw/
更新日期：2017/1/1

以前席克資訊設計了一個程式 AVLog 來分析 ESET Remote Administrator (ERA) v5 (或更舊版本) 及 Avira Management Console (AMC) v2 的資料，如果有異常，會通知指定的人。因為新的 ERA v6 的架構與過去完全不同，所以 AVLog 完全無法使用。但為了讓 ERA v6 的管理工作更加輕鬆且有效率，席克資訊再設計了一個新的工具程式 - EraAdvice.exe 來取代 AVLog 的功能。**使用 EraAdvice，不必花費大量的時間在 ESET Web Console 眾多的資訊中逐一檢查，輕鬆就能掌握全公司電腦防毒系統的運作狀況。**

此程式主要功能如下：

- 分析未正常更新病毒碼的用戶端電腦
- 分析有病毒狀況的電腦，可能是病毒狀況無法自動排除，或者警示其他病毒問題
- 電腦有安裝 ESET 以外的其他防毒軟體 (需開啟回報非安裝 ESET 的應用程式)
- ESET 防毒軟體異常警示通知
- 電腦是否使用舊版 ESET 防毒軟體
- 授權到期提示
- 未安裝 ESET 防毒軟體的電腦清單
- 超過 7 天未連線的電腦清單

適用對象

- 購買 ESET 企業版的席克資訊 Premium 客戶 (如果您不確定是否為 Premium 客戶，請詢問您接洽的業務專員)
- ESET 授權數量 50u 或更多
- ERA v6.3 (Windows 版本) 或更新版本
- ERA 資料庫使用 Microsoft SQL Express

費用

符合適用對象條件者，可免費使用。

使用方法

在 ERA Server 的 C:\ESET\EraDbBackup 資料夾中，直接執行 EraAdvice.exe 即可。如果沒有 EraAdvice.exe，下載 https://download.seekinfo.com.tw/EraDbBackup.7z 並解壓縮到 `C:\ESET\EraDbBackup`。

EraAdvice 執行完畢就結束，並不會常駐在記憶體，所以建議使用 Windows 本身的工作排程來定期執行 EraAdvice.exe，**每天至少執行一次**，也可以執行多次，高興就好。**請注意，EraAdvice 只看當天發生的記錄，所以何時執行是重要關鍵。最佳的執行時間是下班後或者當日結束之前，例如：23:00 ~ 23:30 這段時間，需確保 EraAdvice.exe 在 24:00 之前執行完畢。**

分析報告

執行 EraAdvice.exe 之後，程式如果有發現異常，會建立報告在 C:\ESET\EraDbBackup\Report 裡面，保留最新的 90 個檔案。檢視分析報告，請連到下列網址。也可以在偵測到問題時，直接寄電子郵件通知，需設定，請參閱後面 **設定** 的小節。

`http://<ERA Server IP Address>:3128/EraDbBackup/Report.htm`
(例如：http://192.168.11.3:3128/EraDbBackup/Report.htm)

設定

如果要讓 EraAdvice.exe 寄送電子郵件通知，需要設定 SMTP 相關的值。設定檔案名稱是 EraAdvice.ini (檔案請置於 EraAdvice.exe 相同的資料夾)，可以直接將 EraAdvice.ini.sample 改名為 EraAdvice.ini 再修改內容。

EraAdvice.ini 的內容說明如下：

```
[Setting]
Email = Yes     # 是否使用電子郵件寄送通知

[SMTP]
Server =        # SMTP 伺服器的 FQDN 或 IP Address
Port =          # SMTP 伺服器的 Port
Username =      # 如果 SMTP 需要驗證，登入的帳號
Password =      # 登入的密碼
Sender =        # 寄件者的電子郵件
Recipient =     # 收信者的電子郵件，如果要寄給多個電子郵件，以 , 區隔不同的電子郵件地址
```

設定完畢之後，建議先測試一下，確認寄信的功能是正常的。測試方法，執行：

`EraAdvice.exe emailtest`

如果有收到一封測試的電子郵件表示設定無誤。

請注意：如果是使用 Google 的 SMTP 寄信，需要到 `https://www.google.com/settings/security/lesssecureapps` 將帳號的安全性設定，開啟 **“安全性較低的應用程式存取權限 “**。

報告範本

EraAdvice 產生的報告範本請參見 https://www.seekinfo.com.tw/support/eraadvicesample.htm。

常見問題

- 新版 ERA Web Console 上面病毒資料庫欄位不是很明確顯示 **已更新**，為什麼還需要執行 EraAdvice 去分析？

  > 這是 ERA v6 改善的功能，不像以前是顯示病毒碼的版本及日期。表面上很貼心的功能，但實際上我們已經多次發現這個判斷的機制並不精準。上面顯示已更新，實際上並沒有更新。如果不用 EraAdvice，建議至少手動建立一個報表，可以看到病毒碼版本的清單，從中去判斷是否每一部電腦的病毒碼真的都有更新成功。

- 執行 EraAdvice 多久可以收到通知的信件？

  > 視情況而定，也有可能沒有通知。套句老外說的：No news is good news。如果沒有偵測到問題，怎麼會有通知？

- EraAdvice 和 ERA Web Console 本身的報告功能有何差異？

  > EraAdvice 的精神在於**過濾掉不必要的資訊，只呈現真正需要人為關注的問題，不必將寶貴的時間浪費在無意義的地方**。

- 明明 ERA Web Console 上有一台電腦沒有更新，或者有偵測到一個病毒，為什麼 EraAdvice 沒有寄出通知？

  > EraAdvice 不是這麼笨的程式，它有一些邏輯判斷，如果那麼簡單在 ERA Web Console 看到一個訊息就認定是有問題，那有必要浪費時間寫這個程式嗎？很簡單談一下 EraAdvice 運作的邏輯，首先電腦必須要有開機 (有連線到 ERA Web Console 的意思)，然後 EraAdvice 才會去解讀這部電腦的資料。您可以想想看，沒有連線的電腦病毒碼肯定是舊的，這樣豈不是每次執行 EraAdvice 就會收到一些垃圾訊息？話說回來，也不是看到一筆訊息就認定有問題，還要符合某些條件。

- EraAdvice 可以幫我找出 ESET 偵測不到的病毒嗎？

  > 假設某個病毒 ESET 防毒軟體完全偵測不到，這樣 ERA Web Console 上完全不會收到任何記錄，如果 EraAdvice 能在這種狀況下找出病毒，那我們應該有機會獲得圖靈獎。這是不可能的事情，OK？不過席克資訊另外提供了一項服務，可以檢測電腦裡面是否有潛伏的病毒，如果擔心電腦裡面有 ESET 未知的病毒，可以使用我們的這項服務。
  > 另外有一種狀況，某個病毒同時有幾個檔案在電腦裡，雖然 ESET 無法完全偵測到所有的病毒，可是其中某幾個檔案被偵測到，這樣就會在 ERA Web Console 看到記錄，EraAdvice 就會警示這部電腦，提醒您該去關心它。

- EraAdvice 如果有新版本，會主動通知嗎？

  > 每次執行 EraAdvice，它會先檢查是否有新版本，如果有的話，程式會自動升級，無需人工更新。

如果對本文有不了解的地方，請聯絡**席克資訊 TEL: 04-22132276**