# Red Hat Linux 伺服器導入組態基準與更新管理工具 Satellite 經驗分享

文／黃裕欽　臺灣證券交易所電腦作業部專員

**SUMMARY**

Red Hat Enterprise Linux（以下簡稱RHEL）伺服器已受到GCB及FCB之規範，資安有保障。本文從RHEL相關組態基準說明及其參考指引，介紹導入流程和檢核方式，針對特殊組態項目分享，再到伺服器的更新，一併建置管理工具——Red Hat Satellite，可整合系統至一臺主機，更有效管理伺服器運作。

## 壹、前言

因應資安與駭客攻擊事件頻傳，我國對資訊安全的要求也越來越高。本公司Windows伺服器已參照政府組態基準（Government Configuration Baseline，以下簡稱GCB），設定了一致性的系統安全規範，以降低資安事件之風險。

Red Hat Enterprise Linux（以下簡稱RHEL）伺服器部份，「國家資通安全研究院」（前身為行政院國家資通安全會報技術服務中心，以下簡稱資安院）於110年9月針對RHEL 8版本發佈GCB設定規範。同年「金融資安資訊分享與分析中心」（Financial Information Sharing and Analysis Center，以下簡稱F-ISAC）亦於110年底完成「金融業電腦系統組態基準（Financial Configuration Baseline，以下簡稱FCB）參考指引」。故本公司參考上述二項指引，以及Red Hat專業顧問之建議，於111年底將部分RHEL伺服器導入GCB及FCB之規範，以確保RHEL伺服器之安全性。

在RHEL伺服器的管理上，除了導入GCB外，本公司還建置了RHEL伺服器的更新管理工具Red Hat Satellite，以掌握RHEL伺服器的更新情況。以下就本公司的導入過程，提出一些經驗與大家分享。

## 貳、RHEL相關組態基準說明

### 一、政府組態基準（GCB）

GCB目的在於規範資通訊終端設備（如個人電腦等）之一致性安全設定（如密碼長度、更新期限等），以降低成為駭客入侵管道，進而引發資安事件之風險。

資安院自102年起逐步發展與推廣使用者電腦Windows作業系統與IE瀏覽器之GCB。109年針對機關環境常用之RHEL 8著手發展組態基準設定，並於110年9月進行發佈。其目的在於規範RHEL 8一致性安全組態設定，以及提升作業系統使用安全性。

RHEL 8之GCB項目包括「基本項目」9項類別共計 243 項設定項目，項目統計如下表：

| 項次 | 項目 | 類別 | 項數 | 合計 |
|---|---|---|---|---|
| 1 | 基本項目 | 磁碟與檔案系統 | 31 | 243 |
| | | 系統設定與維護 | 60 | |
| | | 系統服務 | 10 | |
| | | 安裝與維護軟體 | 6 | |
| | | 網路設定 | 24 | |
| | | 日誌與稽核 | 53 | |
| | | SELinux | 7 | |
| | | cron 設定 | 16 | |
| | | 帳號與存取控制 | 36 | |

基本項目部署完成後，再依系統所選擇使用之防火牆（如 Firewalld、Nftables 或 Iptables 等）與 SSH 伺服器，額外部署相對應之組態基準項目，Firewalld、Nftables、Iptables 及 SSH 伺服器組態基準項目分別有 5、7、6 及 31 項設定項目，項目統計如下表：

| 項次 | 項目 | 類別 | 項數 |
|---|---|---|---|
| 1 | Firewalld 防火牆組態基準 | Firewalld 配置 | 5 |
| 2 | Nftables 防火牆組態基準 | Nftables 配置 | 7 |
| 3 | Iptables 防火牆組態基準 | Iptables 配置 | 6 |
| 4 | SSH 伺服器組態基準 | SSH 設定 | 31 |

## 二、金融業電腦系統組態基準參考指引（FCB）

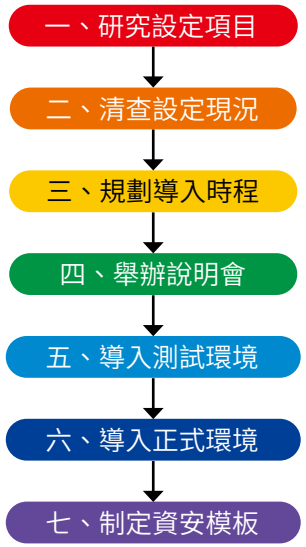
F-ISAC 依據金融監督管理委員會「金融資安行動方案」執行項目，辦理「金融業電腦系統安全組態基準參考指引研究案—Windows 及 Red Hat 伺服器作業系統」，以規範金融業系統之安全性設定，降低駭客入侵管道。

F-ISAC 於 110 年底完成 FCB，其中包括 RHEL 8 之參考指引。FCB 是以資安院所制定之 GCB 為基礎，並參考國際相關資安組織規範及金融資安實務，以規範金融領域資通訊系統之一致性安全設定，降低可能造成之資安漏洞與風險。FCB 與 GCB 的差異說明如下：

| Red Hat 8 | 高 | 中 | 低 | NRV 或未定義 | FCB |
|---|---|---|---|---|---|
| (1) 補充原有 TWGCB 沒有項目 | 3 | 25 | 3 | 6 | 37 |
| (2) 原有 TWGCB 加強度 | 0 | 5 | 0 | 0 | 5 |
| (3) 原有 TWGCB 加說明 | 12 | 134 | 10 | 129 | 285 |
| 總計 | 15 | 164 | 13 | 135 | 327 |

## 參、組態基準導入流程

圖 1：組態基準導入流程圖




組態基準導入流程共分成七個階段，分別說明如下：

### 一、研究組態基準之設定項目

本次組態基準導入作業同時參考 GCB 與 FCB 之參考指引，以及 Red Hat 專業顧問的導入經驗及建議，確認其各項設定值之可行性後，制定出最適合本公司的版本，以確保不會影響本公司系統正常之運作。

## 二、清查各 RHEL 伺服器組態設定現況

由於每一台 RHEL 伺服器所安裝的軟體及組態設定都不太一樣，故須於導入作業前先清查各台伺服器的現況，以釐清現行設定值與規範建議值之間的差異。

## 三、規劃系統導入時程及順序

依照系統等級「普」、「中」及「高」三種等級順序規劃導入時程，重要性較低的系統先行導入以降低風險。

## 四、舉辦導入前說明會

與顧問制定出最適合的規範版本後，接著舉辦導入前說明會，向應用系統負責單位說明導入時程、要改變的設定項目及配合事項，並確認這些項目是否會影響應用系統之運作，以及應用系統負責單位該如何因應等。

## 五、導入測試環境

應用系統負責單位確認規範導入可行後，便先針對測試環境之系統進行資安合規

導入作業，導入過程中可驗證各項設定之適用性，若有與原應用系統不適用或不相容的資安規範，將視情況予以例外管理。

## 六、導入正式環境

確認測試環境導入組態基準一段時間沒有問題後，便可於正式環境進行導入作業，並依據系統特性選擇是否於假日進行作業，導入過程可能仍須進行系統調整及評估例外管理項目。

## 七、制定資安合規模板

待所有系統皆完成組態基準導入作業後，將依據導入過程中所得到的經驗，歸納出一套適合本公司 RHEL 的組態基準模版，未來新建 RHEL 系統時，都能直接套用該模板以利統一管理。

# 肆、組態基準檢核方式

GCB 加上 FCB 的組態基準共有 329 項設定項目，由於數量龐大且繁雜，無法用人工方式一一檢查各個設定項目。因此在檢查每一台伺服器的組態設定時，是使用預先撰寫好的 Script 程式去自動檢核，並將檢核結果以報表方式產出。程式執行畫面如下：

## 一、執行程式時可選擇檢核 GCB 或 FCB，並選擇是否將結果產出至報表。

圖 2：檢核程式執行畫面

```
[root@wbeer-fcb 20221101_GCB_BIN_V1]# sh gcb-initial.sh
Please input job :
Checking GCB    [ 1 ]
Checking FCB    [ 2 ]
Enter your choice :
1
Save report to file???
YES  [ 1 ]
NO   [ 2 ]
```

## 二、報表內容包括的欄位如下：

1.Target：執行受檢核的標的伺服器

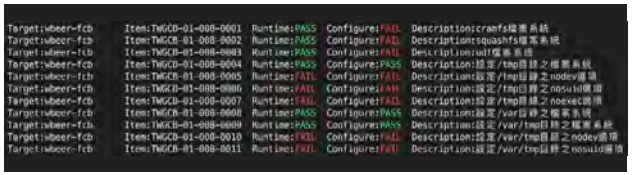
2.GCB Item：檢核的 GCB 組態設定 ID

3.Runtime status：實際執行的檢核結果

4.Configure status：設定檔的檢核結果

5.GCB Item description：組態設定項目的說明描述

圖 3：報表顯示畫面



檢核結果分為 Runtime status 及 Configure status 兩種，因為有時候在設定檔中雖然已設定完成，但不一定會立即生效，所以還須另外檢查實際的執行狀況是否已生效。報表除了可看出哪些 GCB 項目不合格外，還可以更進一步查看該項目不合格的原因。

圖 4：不合格項目之報表畫面


## 三、執行單項組態檢核

若想針對某一項組態設定進行檢核時，也可以直接執行該項的檢核程式，不必全部的檢核再跑一次。

圖 5：單項組態檢核結果畫面

# 伍、特殊組態項目分享

在執行導入組態設定的過程會遇到一些需特別注意或不適用的項目，以下就本公司的經驗分享如下：

## 一、GCB 部分

| TWGCB-ID | 原則設定名稱 | GCB 設定值 | 執行狀況 |
|---|---|---|---|
| TWGCB-01-008-0028 | 設定 NFS 檔案系統之 noexec 選項 | 啟用 | 因部分系統之 NFS 上之檔案需要執行權限，故須列為例外處理。 |
| TWGCB-01-008-0044 | 設定全系統加密原則 | FUTURE 或 FIPS | 設定全系統加密後，部分系統之應用程式須配合修改才可順利執行。 |
| TWGCB-01-008-0140 | 稽核日誌目錄權限 | 600 或更低權限 | auditd 將無法啟動。 |
| TWGCB-01-008-0147 | 稽核日誌達到其檔案大小上限之行為 | keep_logs | 因為本公司有將 log 導至其他 log server，故不保留全部的舊 log。 |
| TWGCB-01-008-0189 | 未受限程序 | 無未受限程序 | 因部分系統有安裝未支援 SELinux 之第三方軟體，故先暫時列為例外處理。 |
| TWGCB-01-008-0267 | SSH 主機私鑰檔案所有權 | root:root | Red Hat 顧問不建議修改 RHEL 之預設值。 |
| TWGCB-01-008-0268 | SSH 主機私鑰檔案權限 | 600 或更低權限 | Red Hat 顧問不建議修改 RHEL 之預設值。 |

## 二、FCB 部分

| TWFCB-ID | 原則設定名稱 | FCB 設定值 | 執行狀況 |
|---|---|---|---|
| TWFCB-01-008-0327 | PAM 模組設定檔預設存取原則需為拒絕存取 | pam_deny.so | 因 pam_deny.so 未定義清楚順序性，及正確語法，極易導致設定不正確狀況下，會導致無法登入作業系統。 |
| TWFCB-01-008-0329 | 網路檔案系統 (NFS)，無需高強度身份驗證即可匯出機密資料的程序。 | 不可使用 no_root_squash | 因本公司的 NFS 環境需要使用 root 權限進行資料存取，故需要保留 no_root_squash 設定值。 |

## 陸、RHEL 伺服器更新方式

RHEL 的更新伺服器稱作 YUM(Yellow dog Update, Modified)。在 YUM 伺服器上放置最新的軟體套件，RHEL client 端便可透過內部網路連至該 YUM 伺服器進行軟體更新。透過這樣的方式雖然可以讓 RHEL 伺服器進行更新套件，但是卻無法即時掌握每一台 RHEL 伺服器的更新狀況，必須一台一台登入檢查才行。有鑑於此，本公司在導入 GCB 的案子中一併建置了一套更新管理工具——Red Hat Satellite。

Red Hat Satellite 為 Red Hat 公司之更新管理工具，與 YUM 功能類似，差別在於 Satellite 可整合所有 RHEL 伺服器之組態設定及系統更新狀態至一台主機上，不僅讓系統管理者可透過單一介面掌握所有 RHEL 伺服器的更新狀況，並能遠端執行系統更新作業。當有重大漏洞需要進行修補時，可透過該平台進行清查每一台 RHEL 伺服器的更新現況，有效提升更新漏洞的效率。

## 柒、Red Hat Satellite 建置流程

### 一、建置各區更新主機

本公司 RHEL 伺服器分散於四個網段，分別是台北的 OA、INT、SUV 及台中。由於每個網段之間有防火牆隔開，所以必須在每一區建置一台更新主機供該區的 RHEL 伺服器進行更新。並設定由 OA 區的更新主機作為主控台，由該主控台對外向 Red Hat 網站下載更新套件，其他各區之更新主機再與該主控台進行更新。

### 二、確認各更新主機資料同步

開通 OA 區更新主機對外更新的防火牆設定，以及各區更新主機對 OA 區更新主機間的防火牆設定，並確認可正常對外進行更新，各更新主機間的資料也都有同步。

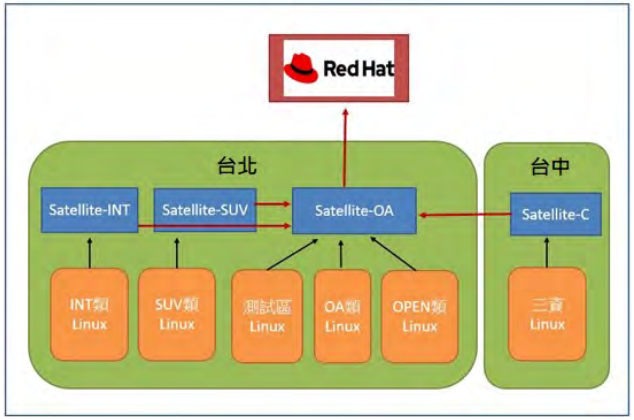
### 三、將測試區 RHEL 伺服器納入管理平台

將測試區的 RHEL 伺服器加入 Satellite 管理平台進行測試，驗證主控台管理功能及 client 端更新功能是否正常。

### 四、將正式區 RHEL 伺服器納入管理平台

將正式區各區的 RHEL 伺服器透過該區的更新主機納入 Satellite 管理平台，並驗證主控台與各 client 主機雙向功能是否正常。完成後架構圖如下：

圖 6：Satellite 架構圖



## 捌、Red Hat Satellite 功能介紹

以下就本公司目前所使用的功能做一個簡單的介紹：

### 一、透過 Script 進行註冊

RHEL 伺服器須與更新主機進行註冊後才可以成為 Satellite 的納管主機，但註冊時必須輸入繁複的指令以及使用 Activation Key 進行驗證。為簡化註冊流程，本公司開發一支 Script 程式，讓系統管理人員可以透過這支程式直接選擇所對應區域的更新主機即可完成註冊程序。

圖 7：Satellite 註冊程式畫面


### 二、顯示與查詢納管主機資訊

在主控台可看到所有已註冊 RHEL 伺服器的資訊，包括作業系統版本、待更新套件之數量以及上次與主控台報到的時間等。在畫面中的 Filter 欄位中可針對主機每個欄位資訊進行查詢。

圖 8：Satellite 納管主機畫面

### 三、顯示與查詢 Errata 資訊

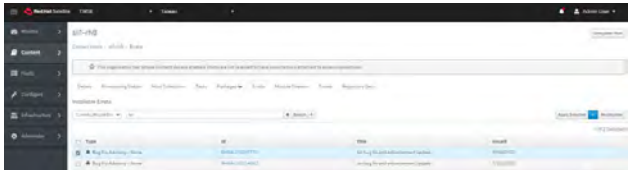
Satellite 主控台可根據 ID 查詢 Errata 的詳細資訊，包括所對應的 CVE、嚴重等級與發佈時間等。每一條 Errata 點進去還可以看到目前受影響的伺服器有哪些，方便管理者了解各條 Errata 的處理情形。

圖 9：Satellite Errata 畫面

### 四、遠端安裝套件及修補漏洞

除了靜態瀏覽及查詢外，主控台還可以直接選擇某一台 RHEL 伺服器進行套件安裝或 Errata 的修補。

圖 10：遠端修補 Errata 畫面




## 玖、結論

RHEL 伺服器導入組態基準後，將可降低資安事件之風險，並符合未來資安法規之要求。只是因為 GCB 才發佈初版，FCB 也還在試運行的階段，有許多組態設定還有待驗證。因此在導入這些組態基準時，需要仔細評估每一項設定的可行性與適用性，才不會為了增加安全性而影響了系統既有的功能。

Satellite 更新管理工具不僅有助於 RHEL 系統之更新管理，更有效提升系統的更新效率。未來可結合 Ansible 自動化工具，讓整個更新流程更為完善。

資料參考：行政院國家資通安全會報技術服務中心網站 https://www.nics.nat.gov.tw/GCB