|  |  |  |
| --- | --- | --- |
|  | | |
| **政府組態基準**  **Red Hat Enterprise Linux 9**  **TWGCB-01-013**  **(工作站)**  **(預告版V1.0)** | | |
|  |  |  |
|  | | |
| 國家資通安全研究院  中華民國112年3月 | | |

**修訂歷史紀錄表**

|  |  |  |  |
| --- | --- | --- | --- |
| 項次 | 版次 | 修訂日期 | 說明 |
| 1 | 1.0 | 112/3/28 | 新編 |
| 2 |  |  |  |
| 3 |  |  |  |
| 4 |  |  |  |
| 5 |  |  |  |
|  | | | |

**目　次**

[1. 前言 1](#_Toc119944798)

[1.1 適用環境 1](#_Toc119944799)

[1.2 項數統計 1](#_Toc119944800)

[1.3 文件發行 2](#_Toc119944801)

[2. Red Hat Enterprise Linux 9政府組態基準列表 3](#_Toc119944802)

[3. 參考文獻 217](#_Toc119944803)

**表 目 次**

[表1 Red Hat Enterprise Linux 9組態基準項目統計 1](#_Toc119944804)

[表2 Red Hat Enterprise Linux 9政府組態基準列表(基本項目) 3](#_Toc119944805)

[表3 Red Hat Enterprise Linux 9 Firewalld防火牆政府組態基準列表 206](#_Toc119944806)

[表4 Red Hat Enterprise Linux 9 Nftables防火牆政府組態基準列表 210](#_Toc119944807)

# 前言

政府組態基準(Government Configuration Baseline，以下簡稱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(如通行碼長度、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。

## 適用環境

本文件適用於紅帽公司(Red Hat)所發行之Red Hat Enterprise Linux 9作業系統，且該系統扮演工作站(Workstation)角色。

## 項數統計

政府組態基準針對電腦作業環境提供一致性資安防護基準與實作指引，供政府機關透過建立安全組態，提升資安防護能力。項目統計詳見表1，其中Red Hat Enterprise Linux 9組態基準須部署之基本項目共計229項(詳見表2)，包含磁碟與檔案系統、系統設定與維護、系統服務、安裝與維護軟體、網路設定、日誌與稽核、SELinux、cron設定及帳號與存取控制等9類別設定項目，接著再依系統所選擇使用之防火牆(如Firewalld或Nftables)，額外部署相對應之組態基準設定，包含Firewalld防火牆組態基準5項設定項目(詳見表3)與Nftables防火牆組態基準7項設定項目(詳見表4)。

1. Red Hat Enterprise Linux 9組態基準項目統計

| 項次 | 項目 | 類別 | 項數 | 合計 |
| --- | --- | --- | --- | --- |
| 1 | 基本項目 | 磁碟與檔案系統 | 20 | 241 |
| 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 | 23 |
| 日誌與稽核 | 52 |
| SELinux | 6 |
| cron設定 | 16 |
| 帳號與存取控制 | 36 |
| 2 | Firewalld防火牆組態基準 | Firewalld配置 | 5 |
| 3 | Nftables防火牆組態基準 | Nftables配置 | 7 |
| 本院整理 | | | | | |

## 文件發行

本文件最新版本公布於本院網站之「政府組態基準」專區，網址為<https://www.nics.nat.gov.tw/GCB>。

# Red Hat Enterprise Linux 9政府組態基準列表

1. Red Hat Enterprise Linux 9政府組態基準列表(基本項目)

| 項次 | TWGCB-ID | 類別 | 原則設定名稱 | 說明 | 設定方法 | GCB 設定值 |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | TWGCB-01-013-0001 | 磁碟與檔案系統 | cramfs檔案系統 | * 這項原則設定決定是否支援cramfs檔案系統 * cramfs (compressed ROM file system，壓縮唯讀閃存檔案系統)檔案系統是一開放式之Linux檔案系統，目的是更簡單更有效率 * cramfs檔案系統以zlib壓縮資料，不需載入到記憶體中，因此可節省許多記憶體空間，可直接使用cramfs映像檔案無須先解壓，使用於某些舊系統或對記憶體有限制之地方 * 停止支援cramfs檔案系統，以降低系統被攻擊面 | * 開啟終端機，執行vim指令，在/etc/modprobe.d目錄新增或編輯「cramfs.conf」檔案，範例如下：   #vim /etc/modprobe.d/cramfs.conf  並在檔案中加入以下內容：  install cramfs /bin/true  blacklist cramfs   * 開啟終端機，執行下列指令，移除cramfs模組：   #rmmod cramfs   * 完成後，請重新開機 | 停用 |
| 2 | TWGCB-01-013-0002 | 磁碟與檔案系統 | squashfs檔案系統 | * 這項原則設定決定是否支援squashfs檔案系統 * squashfs是一個即時解壓縮之檔案系統，專門為唯讀壓縮檔案系統之使用而設計，常見於各Linux發行版之LiveCD * 停止支援squashfs檔案系統，以降低系統被攻擊面 | * 開啟終端機，執行vim指令，在/etc/modprobe.d目錄，新增或編輯「squashfs.conf」檔案，範例如下：   #vim /etc/modprobe.d/squashfs.conf  並在檔案中加入以下內容：  install squashfs /bin/true  blacklist squashfs   * 開啟終端機，執行下列指令，移除squashfs模組：   #rmmod squashfs   * 完成後，請重新開機 | 停用 |
| 3 | TWGCB-01-013-0003 | 磁碟與檔案系統 | udf檔案系統 | * 這項原則設定決定是否支援udf檔案系統 * udf(Universal disk format，通用磁碟格式)是根據ISO/IEC 13346與ECMA-167標準所實做之檔案系統，由光學儲存技術協會(OSTA)開發與維護，廣泛應用在如CD-R/RW與DVD-R/RW等可寫光學儲存媒體 * 停止支援udf檔案系統，以降低系統被攻擊面 | * 開啟終端機，執行vim指令，在/etc/modprobe.d目錄，新增或編輯「udf.conf」檔案，範例如下：   #vim /etc/modprobe.d/udf.conf  並在檔案中加入以下內容：  install udf /bin/true  blacklist udf   * 開啟終端機，執行下列指令，移除udf模組：   #rmmod udf   * 完成後，請重新開機 | 停用 |
| 4 | TWGCB-01-013-0004 | 磁碟與檔案系統 | 設定/tmp目錄之檔案系統 | * 這項原則設定決定/tmp目錄是否使用tmpfs檔案系統 * /tmp是具有全域寫入權限之目錄，所有使用者與某些應用程式都將其用於暫存檔案 * tmpfs是一個不存在於實體硬碟上，而是駐存在記憶體之特殊檔案系統，可提供優於傳統機械硬碟之存取速度 * 將/tmp目錄掛載到tmpfs，可於掛載選項上使用noexec選項，指定/tmp目錄不能啟動可執行二進制檔案，使攻擊者不能安裝執行惡意程式以降低風險 | 執行以下任一操作以設定/tmp目錄之檔案系統：   1. 開啟終端機，執行下列指令，編輯/etc/fstab   #vim /etc/fstab  /tmp之掛載設定範例如下：  tmpfs /tmp tmpfs defaults,rw,nosuid,nodev,noexec,relatime 0 0   1. 開啟終端機，執行下列指令，運用systemd掛載/tmp：   #systemctl unmask tmp.mount  #systemctl enable tmp.mount  編輯/etc/systemd/system/local-fs.target.wants/tmp.mount以掛載/tmp：  [Mount]  What=tmpfs  Where=/tmp  Type=tmpfs  Options=mode=1777,strictatime,noexec,nodev,nosuid | tmpfs |
| 5 | TWGCB-01-013-0005 | 磁碟與檔案系統 | 設定/tmp目錄之nodev選項 | * 這項原則設定決定/tmp目錄是否啟用nodev選項，以禁止在/tmp目錄中建立裝置檔案 * 由於/tmp目錄用途不在於支援裝置，設定nodev選項以確保使用者無法在/tmp目錄建立裝置檔案或存取隨機硬體裝置，降低惡意程式感染風險 * 可設定之參數如下：  1. dev：允許建立裝置檔案 2. nodev：禁止建立裝置檔案 | 執行以下任一操作以設定/tmp目錄之nodev選項：   1. 編輯/etc/fstab檔案，在掛載點為/tmp列，於第4欄加入「,nodev」   開啟終端機，執行下列指令，重新掛載/tmp：  #mount -o remount,nodev /tmp   1. 編輯/etc/systemd/system/local-fs.target.wants/tmp.mount，將nodev添加到/tmp掛載選項：   [Mount]  Options=mode=1777,strictatime,noexec,nodev,nosuid  開啟終端機，執行下列指令，重新掛載/tmp：  #mount -o remount,nodev /tmp | 啟用 |
| 6 | TWGCB-01-013-0006 | 磁碟與檔案系統 | 設定/tmp目錄之nosuid選項 | * 這項原則設定決定/tmp目錄是否啟用nosuid選項，以禁止/tmp目錄存在具有SUID屬性之檔案 * SUID(Set User ID)是針對可執行二進制檔案(Binary file)設計之一項功能，任何使用者執行該程式時，會以該程式之擁有者身分執行，藉由短暫提權讓一般使用者存取未被授權之檔案 * 可設定之參數如下：  1. suid：允許存在具有SUID屬性之檔案 2. nosuid：禁止存在具有SUID屬性之檔案 | 執行以下任一操作以設定/tmp目錄之nosuid選項：   1. 編輯/etc/fstab檔案，在掛載點為/tmp列，於第4欄加入「,nosuid」   開啟終端機，執行下列指令，重新掛載/tmp：  #mount -o remount,nosuid /tmp   1. 編輯/etc/systemd/system/local-fs.target.wants/tmp.mount，將nosuid添加到/tmp掛載選項：   [Mount]  Options=mode=1777,strictatime,noexec,nodev,nosuid  開啟終端機，執行下列指令，重新掛載/tmp：  # mount -o remount,nosuid /tmp | 啟用 |
| 7 | TWGCB-01-013-0007 | 磁碟與檔案系統 | 設定/tmp目錄之noexec選項 | * 這項原則設定決定/tmp目錄是否啟用noexec選項，以禁止在/tmp目錄中啟動可執行二進制檔案 * /tmp目錄主要做為暫時存放檔案之用，禁止使用者啟動可執行二進制檔案，以避免感染惡意程式 * 可設定之參數如下：  1. exec：允許啟動可執行二進制檔案 2. noexec：禁止啟動可執行二進制檔案 | 執行以下任一操作以設定/tmp目錄之noexec選項：   1. 編輯/etc/fstab檔案，在掛載點為/tmp列，於第4欄加入「,noexec」   開啟終端機，執行下列指令，重新掛載/tmp：  #mount -o remount,noexec /tmp   1. 編輯/etc/systemd/system/local-fs.target.wants/tmp.mount將noexec添加到/tmp掛載選項：   [Mount]  Options=mode=1777,strictatime,noexec,nodev,nosuid  開啟終端機，執行下列指令，重新掛載/tmp：  # mount -o remount,noexec /tmp | 啟用 |
| 8 | TWGCB-01-013-0008 | 磁碟與檔案系統 | 設定/dev/shm目錄之nodev選項 | * 這項原則設定決定/dev/shm目錄是否啟用nodev選項，以禁止在/dev/shm目錄中建立裝置檔案 * /dev/shm目錄是系統利用記憶體建立之虛擬磁碟空間，用以存放暫存檔案，一方面存取速度比硬碟快，另一方面可依實際檔案大小動態分配空間 * 由於/dev/shm目錄用途不在於支援裝置，設定nodev選項以確保使用者無法在/dev/shm目錄建立裝置檔案或存取隨機硬體裝置，降低惡意程式感染風險 * 可設定之參數如下：  1. dev：允許建立裝置檔案 2. nodev：禁止建立裝置檔案 | * 編輯/etc/fstab檔案，在掛載點為/dev/shm列，於第4欄加入「,nodev」 * 開啟終端機，執行下列指令，重新掛載/dev/shm：   #mount -o remount,nodev /dev/shm | 啟用 |
| 9 | TWGCB-01-013-0009 | 磁碟與檔案系統 | 設定/dev/shm目錄之nosuid選項 | * 這項原則設定決定/dev/shm目錄是否啟用nosuid選項，以禁止/dev/shm目錄存在具有SUID屬性之檔案 * /dev/shm目錄是系統利用記憶體建立之虛擬磁碟空間，用以存放暫存檔案，一方面存取速度比硬碟快，另一方面可依實際檔案大小動態分配空間 * SUID(Set User ID)是針對可執行二進制檔案(Binary file)設計之一項功能，任何使用者執行該程式時，會以該程式之擁有者身分執行，藉由短暫提權讓一般使用者存取未被授權之檔案 * 可設定之參數如下：  1. suid：允許存在具有SUID屬性之檔案 2. nosuid：禁止存在具有SUID屬性之檔案 | * 編輯/etc/fstab檔案，在掛載點為/dev/shm列，於第4欄加入「,nosuid」 * 開啟終端機，執行下列指令，重新掛載/dev/shm：   #mount -o remount,nosuid /dev/shm | 啟用 |
| 10 | TWGCB-01-013-0010 | 磁碟與檔案系統 | 設定/dev/shm目錄之noexec選項 | * 這項原則設定決定/dev/shm目錄是否啟用noexec選項，以禁止在/dev/shm目錄中啟動可執行二進制檔案 * /dev/shm目錄是系統利用記憶體建立之虛擬磁碟空間，用以存放暫存檔案，一方面存取速度比硬碟快，另一方面可依實際檔案大小動態分配空間 * 設定noexec選項，禁止使用者啟動可執行二進制檔案，以避免感染惡意程式 * 可設定之參數如下：  1. exec：允許啟動可執行二進制檔案 2. noexec：禁止啟動可執行二進制檔案 | * 編輯/etc/fstab檔案，在掛載點為/dev/shm列，於第4欄加入「,noexec」 * 開啟終端機，執行下列指令，重新掛載/dev/shm：   #mount -o remount,noexec /dev/shm | 啟用 |
| 11 | TWGCB-01-013-0011 | 磁碟與檔案系統 | 設定可攜式儲存裝置之nodev選項 | * 這項原則設定決定可攜式儲存裝置是否啟用nodev選項，以禁止在可攜式儲存裝置中建立裝置檔案 * 設定nodev選項以確保使用者無法在可攜式儲存裝置建立裝置檔案或存取隨機硬體裝置，降低惡意程式感染風險 * 可設定之參數如下：  1. dev：允許建立裝置檔案 2. nodev：禁止建立裝置檔案 | * 開啟終端機，執行以下指令，檢查是否有掛載可攜式儲存裝置：   #mount   * 若發現有掛載可攜式儲存裝置，則編輯/etc/fstab檔案，在掛載點為「可攜式儲存裝置」列，於第4欄加入「,nodev」 | 啟用 |
| 12 | TWGCB-01-013-0012 | 磁碟與檔案系統 | 設定可攜式儲存裝置之nosuid選項 | * 這項原則設定決定可攜式儲存裝置是否啟用nosuid選項，以禁止可攜式儲存裝置存在具有SUID屬性之檔案 * SUID(Set User ID)是針對可執行二進制檔案(Binary file)設計之一項功能，任何使用者執行該程式時，會以該程式之擁有者身分執行，藉由短暫提權讓一般使用者存取未被授權之檔案 * 可設定之參數如下：  1. suid：允許存在具有SUID屬性之檔案 2. nosuid：禁止存在具有SUID屬性之檔案 | * 開啟終端機，執行以下指令，檢查是否有掛載可攜式儲存裝置：   #mount   * 若發現有掛載可攜式儲存裝置，則編輯/etc/fstab檔案，在掛載點為「可攜式儲存裝置」列，於第4欄加入「,nosuid」 | 啟用 |
| 13 | TWGCB-01-013-0013 | 磁碟與檔案系統 | 設定可攜式儲存裝置之noexec選項 | * 這項原則設定決定可攜式儲存裝置是否啟用noexec選項，以禁止在可攜式儲存裝置中啟動可執行二進制檔案 * 設定noexec選項，禁止使用者啟動可執行二進制檔案，以避免感染惡意程式 * 可設定之參數如下：  1. exec：允許啟動可執行二進制檔案 2. noexec：禁止啟動可執行二進制檔案 | * 開啟終端機，執行以下指令，檢查是否有掛載可攜式儲存裝置：   #mount   * 若發現有掛載可攜式儲存裝置，則編輯/etc/fstab檔案，在掛載點為「可攜式儲存裝置」列，於第4欄加入「,noexec」 | 啟用 |
| 14 | TWGCB-01-013-0014 | 磁碟與檔案系統 | 設定使用者家目錄之nodev選項 | * 這項原則設定決定使用者家目錄是否啟用nodev選項，以禁止在使用者家目錄中建立裝置檔案 * 使用者家目錄是系統預設之使用者主目錄，目錄下存放使用者之環境設定與個人檔案 * 由於使用者家目錄用途不在於支援裝置，設定nodev選項以確保使用者無法在/home目錄建立裝置檔案或存取隨機硬體裝置，降低惡意程式感染風險 * 可設定之參數如下：  1. dev：允許建立裝置檔案 2. nodev：禁止建立裝置檔案 | * 開啟終端機，執行下列指令，尋找使用者家目錄(/home/使用者帳號)：   #awk -F: '($3>=1000)&&($1!="nobody"){print $1,$3,$6}' /etc/passwd   * 執行下列指令，檢查/etc/fstab檔案，確認系統開機時掛載之檔案系統：   #more /etc/fstab   * 若發現使用者家目錄掛載在獨立檔案系統，則編輯/etc/fstab檔案，在掛載點為「使用者家目錄」列，於第4欄加入「,nodev」 | 啟用 |
| 15 | TWGCB-01-013-0015 | 磁碟與檔案系統 | 設定使用者家目錄之nosuid選項 | * 這項原則設定決定使用者家目錄是否啟用nosuid選項，以禁止使用者家目錄存在具有SUID屬性之檔案 * 使用者家目錄是系統預設之使用者主目錄，目錄下存放使用者之環境設定與個人檔案 * SUID(Set User ID)是針對可執行二進制檔案(Binary file)設計之一項功能，任何使用者執行該程式時，會以該程式之擁有者身分執行，藉由短暫提權讓一般使用者存取未被授權之檔案 * 可設定之參數如下：  1. suid：允許存在具有SUID屬性之檔案 2. nosuid：禁止存在具有SUID屬性之檔案 | * 開啟終端機，執行下列指令，尋找使用者家目錄(/home/使用者帳號)：   #awk -F: '($3>=1000)&&($1!="nobody"){print $1,$3,$6}' /etc/passwd   * 執行下列指令，檢查/etc/fstab檔案，確認系統開機時掛載之檔案系統：   #more /etc/fstab   * 若發現使用者家目錄掛載在獨立檔案系統，則編輯/etc/fstab檔案，在掛載點為「使用者家目錄」列，於第4欄加入「,nosuid」 | 啟用 |
| 16 | TWGCB-01-013-0016 | 磁碟與檔案系統 | 設定使用者家目錄之noexec選項 | * 這項原則設定決定使用者家目錄是否啟用noexec選項，以禁止在使用者家目錄中啟動可執行二進制檔案 * 使用者家目錄是系統預設之使用者主目錄，目錄下存放使用者之環境設定與個人檔案 * 設定noexec選項，禁止使用者啟動可執行二進制檔案，以避免感染惡意程式 * 可設定之參數如下：  1. exec：允許啟動可執行二進制檔案 2. noexec：禁止啟動可執行二進制檔案 | * 開啟終端機，執行下列指令，尋找使用者家目錄(/home/使用者帳號)：   #awk -F: '($3>=1000)&&($1!="nobody"){print $1,$3,$6}' /etc/passwd   * 執行下列指令，檢查/etc/fstab檔案，確認系統開機時掛載之檔案系統：   #more /etc/fstab   * 若發現使用者家目錄掛載在獨立檔案系統，則編輯/etc/fstab檔案，在掛載點為「使用者家目錄」列，於第4欄加入「,noexec」 | 啟用 |
| 17 | TWGCB-01-013-0017 | 磁碟與檔案系統 | 設定NFS檔案系統之nodev選項 | * 這項原則設定決定NFS檔案系統是否啟用nodev選項，以禁止在NFS檔案系統中建立裝置檔案 * 設定nodev選項以確保使用者無法在NFS檔案系統中建立裝置檔案或存取隨機硬體裝置，降低惡意程式感染風險 * 可設定之參數如下：  1. dev：允許建立裝置檔案 2. nodev：禁止建立裝置檔案 | * 開啟終端機，執行下列指令，檢查/etc/fstab檔案，確認系統開機時是否有掛載NFS檔案系統：   #grep nfs /etc/fstab   * 若發現有掛載NFS檔案系統，則編輯/etc/fstab檔案，在掛載點為「NFS檔案系統」列，於第4欄加入「,nodev」 | 啟用 |
| 18 | TWGCB-01-013-0018 | 磁碟與檔案系統 | 設定NFS檔案系統之nosuid選項 | * 這項原則設定決定NFS檔案系統是否啟用nosuid選項，以禁止NFS檔案系統存在具有SUID屬性之檔案 * SUID(Set User ID)是針對可執行二進制檔案(Binary file)設計之一項功能，任何使用者執行該程式時，會以該程式之擁有者身分執行，藉由短暫提權讓一般使用者存取未被授權之檔案 * 可設定之參數如下：  1. suid：允許存在具有SUID屬性之檔案 2. nosuid：禁止存在具有SUID屬性之檔案 | * 開啟終端機，執行下列指令，檢查/etc/fstab檔案，確認系統開機時是否有掛載NFS檔案系統：   #grep nfs /etc/fstab   * 若發現有掛載NFS檔案系統，則編輯/etc/fstab檔案，在掛載點為「NFS檔案系統」列，於第4欄加入「,nosuid」 | 啟用 |
| 19 | TWGCB-01-013-0019 | 磁碟與檔案系統 | 設定NFS檔案系統之noexec選項 | * 這項原則設定決定NFS檔案系統是否啟用noexec選項，以禁止在NFS檔案系統中啟動可執行二進制檔案 * 設定noexec選項，禁止使用者啟動可執行二進制檔案，以避免感染惡意程式 * 可設定之參數如下：  1. exec：允許啟動可執行二進制檔案 2. noexec：禁止啟動可執行二進制檔案 | * 開啟終端機，執行下列指令，檢查/etc/fstab檔案，確認系統開機時是否有掛載NFS檔案系統：   #grep nfs /etc/fstab   * 若發現有掛載NFS檔案系統，則編輯/etc/fstab檔案，在掛載點為「NFS檔案系統」列，於第4欄加入「,noexec」 | 啟用 |
| 20 | TWGCB-01-013-0020 | 磁碟與檔案系統 | 設定全域寫入權限目錄之粘滯位 | * 這項原則設定決定所有具有全域寫入(World-writable)權限之目錄是否設定粘滯位(Sticky bit) * 設定粘滯位(Sticky bit)確保只有擁有者才能刪除或更名自己建立之檔案，以防止使用者任意刪除或更名其他使用者所建立之檔案 | 開啟終端機，執行下列指令，在所有具有全域寫入(World-writable)權限之目錄設定粘滯位：  #df --local -P | awk '{if (NR!=1) print $6}' | xargs -I '{}' find '{}' -xdev -type d \( -perm -0002 -a ! -perm -1000 \) 2>/dev/null | xargs -I '{}' chmod o+t '{}' | 設定粘滯位 |
| 21 | TWGCB-01-013-0021 | 系統設定與維護 | GPG簽章驗證 | * 這項原則設定決定是否啟用GPG簽章驗證功能 * gpgcheck決定在安裝套件前，是否先進行RPM套件簽章檢查，可用以確保欲安裝之RPM套件來自可信賴來源，避免安裝已被竄改之檔案 * gpgcheck選項存在於/etc/yum.conf、/etc/dnf/dnf.conf設定檔及/etc/yum/repos.d/目錄下所有設定檔 * gpgcheck選項可設定參數如下：  1. 1：啟用，先進行RPM套件簽章檢查，通過後才能安裝套件 2. 0：停用，安裝前不進行RPM套件簽章檢查 | * 編輯/etc/yum.conf與/etc/dnf/dnf.conf檔案，在「main」段落新增或修改成以下內容：   gpgcheck=1   * 編輯/etc/yum.repos.d目錄下所有檔案，將全部之「gpgcheck」設定，修改成以下內容：   gpgcheck=1 | 1 |
| 22 | TWGCB-01-013-0022 | 系統設定與維護 | sudo套件 | * 這項原則設定決定是否安裝sudo套件，sudo允許合法使用者按照所授予之帳號權限，以管理員身分(superuser)或其他使用者身分執行指令 * sudo預設設定檔為/etc/sudoers，將一般使用者帳號與所授予之權限設定在/etc/sudoers設定檔，一般使用者在需要取得特殊權限時，則可於指令前加上「sudo」並輸入使用者自己之通行碼，即可用管理員身分執行指令 * 注意：建議可依系統維運與管理需求，適當賦予使用者執行sudo之權限，並可考量將各使用者之設定存放於不同設定檔中 | 開啟終端機，執行下列指令安裝sudo套件：  #dnf install sudo | 安裝 |
| 23 | TWGCB-01-013-0023 | 系統設定與維護 | 設定sudo指令使用pty | * 這項原則設定決定sudo指令是否使用pty(pseudo terminal，虛擬終端) * pty是一對提供雙向通訊之虛擬終端設備，分別為主要(master)與從屬(slave)設備，從屬設備提供模擬硬體終端機設備，主要設備提供模擬終端機程序以操作控制從屬設備 * 攻擊者在使用sudo執行惡意程序時，在主程序完成後可能會衍生另一個背景程序保留在終端設備上，sudo設定為使用pty時可避免此情況 | 開啟終端機，執行「visudo -f」指令編輯/etc/sudoers檔案或 /etc/sudoers.d/目錄下檔案，新增以下內容：  Defaults use\_pty | Defaults use\_pty |
| 24 | TWGCB-01-013-0024 | 系統設定與維護 | sudo自定義日誌檔案 | * 這項原則設定決定是否設定sudo自定義日誌檔案 * 預設情況下sudo藉由syslog記錄日誌，但sudo可在設定檔(預設為/etc/sudoers)中自定義日誌檔案，有助於簡化sudo指令之稽核工作 | * 開啟終端機，執行「visudo -f」指令編輯/etc/sudoers檔案或 /etc/sudoers.d/目錄下檔案，新增以下內容：   Defaults logfile="(日誌檔案路徑)"   * 日誌檔案路徑使用「/var/log/sudo.log」之範例如下：   Defaults logfile="/var/log/sudo.log" | 啟用 |
| 25 | TWGCB-01-013-0025 | 系統設定與維護 | AIDE套件 | * 這項原則設定決定是否安裝AIDE(Advanced Intrusion Detection Environment，先進入侵偵測環境)套件 * AIDE截取檔案系統狀態之快照，包括修改時間、權限及檔案雜湊，藉由將快照與檔案系統之當前狀態進行比較，以檢測系統變更情況，找出被修改或損毀之檔案 * AIDE可藉由檔案完整性檢查，協助系統管理者早期發現系統入侵跡象 * 注意：建議可依系統維運與管理需求新增或調整AIDE規則 | * 開啟終端機，執行以下指令安裝AIDE套件：   #dnf install aide   * 執行以下指令初始化AIDE：   #aide --init  #mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz | 安裝 |
| 26 | TWGCB-01-013-0026 | 系統設定與維護 | 定期檢查檔案系統完整性 | * 這項原則設定決定是否使用AIDE工具定期檢查檔案系統完整性 * AIDE截取檔案系統狀態之快照，包括修改時間、權限及檔案雜湊，藉由將快照與檔案系統之當前狀態進行比較，以檢測系統變更情況，找出被修改或損毀之檔案 * 定期檢查檔案系統完整性，可協助系統管理者定期確認是否有重要檔案在未經授權之情況下被修改 | * 開啟終端機，執行以下指令，編輯crontab：   #crontab -u root -e   * 在crontab新增以下內容，設定每天5點進行檔案系統完整性檢查：   0 5 \* \* \* /usr/sbin/aide --check | 每天 |
| 27 | TWGCB-01-013-0027 | 系統設定與維護 | 開機載入程式設定檔之所有權 | * 這項原則設定決定開機載入程式(GRUB)設定檔之擁有者與群組 * GRUB設定檔主要功能是用來記錄載入作業系統核心所使用之參數 * 將GRUB設定檔之擁有者與擁有群組設為root，以防止非root使用者變更檔案內容 * 備註：如果使用其他開機載入程式(如LILO或EFI GRUB)，請比照上述原則進行設定 | 開啟終端機，執行以下指令，設定GRUB設定檔之擁有者與群組：  #chown root:root /boot/grub2/grub.cfg  #chown root:root /boot/grub2/grubenv | root:root |
| 28 | TWGCB-01-013-0028 | 系統設定與維護 | 開機載入程式設定檔之權限 | * 這項原則設定決定是否設定開機載入程式(GRUB)設定檔之權限 * GRUB設定檔主要功能是用來記錄載入作業系統核心所使用之參數 * 禁止群組與其他身分讀取、寫入及執行GRUB設定檔，以防止非root使用者取得或修改開機參數，進而危及系統安全 * 備註：如果使用其他開機載入程式(如LILO或EFI GRUB)，請比照上述原則進行設定 | 開啟終端機，執行以下指令，設定GRUB設定檔之權限為600或更低權限：  #chmod 600 /boot/grub2/grub.cfg  #chmod 600 /boot/grub2/grubenv | 600或更低權限 |
| 29 | TWGCB-01-013-0029 | 系統設定與維護 | 開機載入程式之通行碼 | * 這項原則設定決定是否設定開機載入程式之通行碼，以限制需通過通行碼鑑別後，才能設定開機載入程式之參數 * 設定通行碼保護開機載入程式，可避免攻擊者開機進入單一使用者或維護模式，不需鑑別root身分，即可取得系統上所有檔案之存取權限 | * 開啟終端機，執行以下指令，使用grub2-setpassword建立一組通行碼：   #grub2-setpassword  Enter password: (輸入通行碼)  Confirm password: (再次輸入通行碼)   * 執行以下指令更新grub2設定檔：   #grub2-mkconfig -o /boot/grub2/grub.cfg | 設定通行碼 |
| 30 | TWGCB-01-013-0030 | 系統設定與維護 | 單一使用者模式身分鑑別 | * 這項原則設定決定單一使用者模式(Single user mode)是否啟用身分鑑別功能 * 當系統在開機載入過程發生問題時，將使用單一使用者模式(或稱為救援模式)進行還原 * 設定單一使用者模式需使用身分鑑別，可防止攻擊者將系統重新開機後，不需身分鑑別即可進入單一使用者模式，進而危害系統安全 | * 編輯/usr/lib/systemd/system/rescue.service檔案，新增或修改成以下內容：   ExecStart=-/usr/lib/systemd/systemd-sulogin-shell rescue   * 編輯/usr/lib/systemd/system/emergency.service檔案，新增或修改成以下內容：   ExecStart=-/usr/lib/systemd/systemd-sulogin-shell emergency | 啟用 |
| 31 | TWGCB-01-013-0031 | 系統設定與維護 | 核心傾印功能 | * 這項原則設定決定是否啟用核心傾印(Core dump)功能 * 核心傾印檔案是程式異常終止時，系統將當時記憶體內容以檔案方式記錄下來所產生之記憶體映像檔案，可供程式除錯之用 * 禁止使用者與SUID程式產生核心傾印檔案，避免核心傾印檔案洩露如記憶體位址或空間配置等敏感資訊 | * 編輯/etc/security/limits.conf檔案或/etc/security/limits.d/目錄下檔案，新增以下內容：   \* hard core 0   * 編輯/etc/sysctl.conf或/etc/sysctl.d/目錄下檔案，設定參數如下：   fs.suid\_dumpable = 0   * 開啟終端機，執行以下指令，設定核心參數：   #sysctl -w fs.suid\_dumpable=0   * 如果已安裝coredump服務，編輯/etc/systemd/coredump.conf檔案，新增或修改成以下內容：   Storage=none  ProcessSizeMax=0   * 開啟終端機，執行以下指令重新載入systemd：   #systemctl daemon-reload | 停用 |
| 32 | TWGCB-01-013-0032 | 系統設定與維護 | 記憶體位址空間配置隨機載入 | * 這項原則設定決定系統開機時是否立即啟用記憶體位址空間配置隨機載入(Address space layout randomization, ASLR)功能 * ASLR利用隨機方式配置資料位址，使得敏感資料(例如作業系統核心程式)能配置到一個惡意程式未能事先得知之位址 * 啟用記憶體位址空間配置隨機載入，提高攻擊難度，以降低緩衝區溢位攻擊之威脅 * 可設定參數如下：  1. 0：停用ASLR功能 2. 1：隨機配置堆疊(Stack)、記憶體映射函數(mmap)及vDSO(Virtual Dynamically-linked Shared Object，虛擬動態連結共享物件)頁面 3. 2：隨機配置堆疊(Stack)、記憶體映射函數(mmap)、vDSO頁面及堆積(Heap) | * 編輯/etc/sysctl.conf檔案或/etc/sysctl.d/目錄下檔案，設定參數如下：   kernel.randomize\_va\_space = 2   * 開啟終端機，執行以下指令，設定核心參數：   #sysctl -w kernel.randomize\_va\_space=2 | 2 |
| 33 | TWGCB-01-013-0033 | 系統設定與維護 | 設定全系統加密原則 | * 這項原則設定決定採取何種全系統加密原則 * 全系統加密原則(System-wide crypto-policies)與加密核心元件，允許在全系統範圍使用一致性之加密原則 * 可設定原則如下：  1. DEFAULT：預設全系統加密原則。允許使用TLSv1.2與1.3協定，以及IKEv2與SSH2協定，要求RSA密鑰與Diffie-Hellman金鑰至少為2,048位元 2. LEGACY：此原則可確保與Red Hat Enterprise Linux 5與更舊版本之最大兼容性，比DEFAULT原則多支援TLSv1.0與1.1協定，並允許使用DSA、3DES及RC4演算法，要求RSA密鑰與Diffie-Hellman金鑰至少為1,024位元 3. FUTURE：採取保守之安全原則，可承受近期相關攻擊，不允許使用SHA-1演算法，要求RSA密鑰與Diffie-Hellman金鑰至少為3,072位元 4. FIPS：符合FIPS140-2要求原則，使用內建之fips-mode-setup工具，將作業系統切換到FIPS模式  * 設定全系統加密原則使用FUTURE或FIPS原則，避免使用較舊且易被攻擊之加密演算法 | * 開啟終端機，執行以下指令，確認全系統加密原則是否為FUTURE或FIPS：   #grep -E -i '^\s\*(FUTURE|FIPS)\s\*(\s+#.\*)?$' /etc/crypto-policies/config   * 若不是使用FUTURE或FIPS原則，請執行以下任一操作，變更全系統加密原則：  1. 執行以下指令，將系統設定為「FUTURE」原則：   #update-crypto-policies --set FUTURE  接續執行以下指令，以套用更新後之全系統加密原則：  #update-crypto-policies   1. 執行以下指令，將系統設定為「FIPS」原則，並重新開機，以使生效：   #fips-mode-setup --enable | FUTURE或FIPS |
| 34 | TWGCB-01-013-0034 | 系統設定與維護 | /etc/passwd檔案所有權 | * 這項原則設定決定/etc/passwd檔案擁有者與群組 * /etc/passwd記錄每位使用者之名稱、通行碼、使用者ID、群組ID及家目錄等資訊 * 設定/etc/passwd檔案擁有者與群組為root，避免/etc/passwd檔案遭未授權使用者修改，降低檔案被竄改後進一步利用於其他惡意攻擊之風險 | 開啟終端機，執行以下指令，設定/etc/passwd檔案所有權：  #chown root:root /etc/passwd | root:root |
| 35 | TWGCB-01-013-0035 | 系統設定與維護 | /etc/passwd檔案權限 | * 這項原則設定決定/etc/passwd檔案權限 * /etc/passwd記錄每位使用者之名稱、通行碼、使用者ID、群組ID及家目錄等資訊 * 將/etc/passwd檔案權限設為僅root擁有讀取與寫入權限，其餘所有使用者僅可讀取，避免/etc/passwd檔案遭未授權使用者修改，降低檔案被竄改後進一步利用於其他惡意攻擊之風險 | 開啟終端機，執行以下指令，設定/etc/passwd檔案權限為644或更低權限：  #chmod 644 /etc/passwd | 644或更低權限 |
| 36 | TWGCB-01-013-0036 | 系統設定與維護 | /etc/shadow檔案所有權 | * 這項原則設定決定/etc/shadow檔案擁有者與群組 * /etc/shadow記錄每個使用者帳號加密過後之通行碼、最後變更通行碼之日期及下次可變更通行碼前之經過天數等資訊 * 若攻擊者取得/etc/shadow檔案後，可嘗試透過通行碼破解程式取得通行碼後進行攻擊 * 設定/etc/shadow檔案擁有者與群組，以保護帳號通行碼資訊，降低檔案被竄改後進一步利用於其他惡意攻擊之風險 | 開啟終端機，執行以下任一指令，設定/etc/shadow檔案之所有權：  #chown root:root /etc/shadow  或  #chown root:shadow /etc/shadow | root:root或root:shadow |
| 37 | TWGCB-01-013-0037 | 系統設定與維護 | /etc/shadow檔案權限 | * 這項原則設定決定/etc/shadow檔案權限 * /etc/shadow記錄每個使用者帳號加密過後之通行碼、最後變更通行碼之日期及下次可變更通行碼前之經過天數等資訊 * 若攻擊者取得/etc/shadow檔案後，可嘗試透過通行碼破解程式取得通行碼後進行攻擊 * 將/etc/shadow檔案權限設為000(所有使用者不具有讀取、寫入及執行權限)，以保護帳號通行碼資訊，降低檔案被竄改後進一步利用於其他惡意攻擊之風險 | 開啟終端機，執行以下指令，設定/etc/shadow檔案之權限為000：  #chmod 000 /etc/shadow | 000 |
| 38 | TWGCB-01-013-0038 | 系統設定與維護 | /etc/group檔案所有權 | * 這項原則設定決定/etc/group檔案擁有者與群組 * /etc/group記錄每個群組之名稱、通行碼、ID及屬於該群組之使用者清單 * 設定/etc/group檔案擁有者與群組為root，避免/etc/group檔案遭未授權使用者修改 | 開啟終端機，執行以下指令，設定/etc/group檔案所有權：  #chown root:root /etc/group | root:root |
| 39 | TWGCB-01-013-0039 | 系統設定與維護 | /etc/group檔案權限 | * 這項原則設定決定/etc/group檔案權限 * /etc/group記錄每個群組之名稱、通行碼、ID及屬於該群組之使用者清單 * 設定/etc/group檔案權限，僅root擁有讀寫權限，其餘所有使用者僅可讀取，避免/etc/group檔案遭未授權使用者修改 | 開啟終端機，執行以下指令，設定/etc/group檔案權限為644或更低權限：  #chmod 644 /etc/group | 644或更低權限 |
| 40 | TWGCB-01-013-0040 | 系統設定與維護 | /etc/gshadow檔案所有權 | * 這項原則設定決定/etc/gshadow檔案擁有者與群組 * /etc/gshadow記錄每個群組加密過後之通行碼，以及使用者與管理者資訊，攻擊者讀取/etc/gshadow檔案後，可嘗試透過通行碼破解程式取得通行碼後進行攻擊 * 設定/etc/gshadow檔案擁有者與群組，以保護群組帳號通行碼資訊，降低檔案被竄改後進一步利用於其他惡意攻擊之風險 | 開啟終端機，執行以下任一指令，設定/etc/gshadow檔案所有權：  #chown root:root /etc/gshadow  或  #chown root:shadow /etc/gshadow | root:root或root:shadow |
| 41 | TWGCB-01-013-0041 | 系統設定與維護 | /etc/gshadow檔案權限 | * 這項原則設定決定/etc/gshadow檔案權限 * /etc/gshadow記錄每個群組加密過後之通行碼，以及使用者與管理者資訊，攻擊者讀取/etc/gshadow檔案後，可嘗試透過通行碼破解程式取得通行碼後進行攻擊 * 設定/etc/gshadow檔案權限為000(所有使用者不具有讀取、寫入及執行權限)，以保護群組帳號通行碼資訊，降低檔案被竄改後進一步利用於其他惡意攻擊之風險 | 開啟終端機，執行以下指令，設定/etc/gshadow檔案權限為000：  #chmod 000 /etc/gshadow | 000 |
| 42 | TWGCB-01-013-0042 | 系統設定與維護 | /etc/passwd-檔案所有權 | * 這項原則設定決定/etc/passwd-檔案擁有者與群組 * /etc/passwd-備份每位使用者之名稱、通行碼、使用者ID、群組ID及家目錄等資訊 * 設定/etc/passwd-檔案擁有者與群組為root，避免/etc/passwd-檔案遭未授權使用者修改，降低檔案被竄改後進一步利用於其他惡意攻擊之風險 | 開啟終端機，執行以下指令，設定/etc/passwd-檔案之所有權：  #chown root:root /etc/passwd- | root:root |
| 43 | TWGCB-01-013-0043 | 系統設定與維護 | /etc/passwd-檔案權限 | * 這項原則設定決定/etc/passwd-檔案權限 * /etc/passwd-備份每位使用者之名稱、通行碼、使用者ID、群組ID及家目錄等資訊 * 設定/etc/passwd-檔案權限，僅root擁有讀取與寫入權限，其餘所有使用者僅可讀取，避免/etc/passwd-檔案遭未授權使用者修改，降低檔案被竄改後進一步利用於其他惡意攻擊之風險 | 開啟終端機，執行以下指令，設定/etc/passwd-檔案之權限為644或更低權限：  #chmod 644 /etc/passwd- | 644或更低權限 |
| 44 | TWGCB-01-013-0044 | 系統設定與維護 | /etc/shadow-檔案所有權 | * 這項原則設定決定/etc/shadow-檔案擁有者與群組 * /etc/shadow-備份每個使用者帳號加密過後之通行碼、最後變更通行碼之日期及下次可變更通行碼前之經過天數等資訊 * 若攻擊者取得/etc/shadow-檔案，可嘗試透過通行碼破解程式取得通行碼後進行攻擊 * 設定/etc/shadow-檔案所有權，以保護帳號通行碼資訊，降低檔案被竄改後進一步利用於其他惡意攻擊之風險 | 開啟終端機，執行以下任一指令，設定/etc/shadow-檔案之所有權：  #chown root:root /etc/shadow-  或  #chown root:shadow /etc/shadow- | root:root或root:shadow |
| 45 | TWGCB-01-013-0045 | 系統設定與維護 | /etc/shadow-檔案權限 | * 這項原則設定決定/etc/shadow-檔案權限 * /etc/shadow-備份每個使用者帳號加密過後之通行碼、最後變更通行碼之日期及下次可變更通行碼前之經過天數等資訊 * 若攻擊者取得/etc/shadow-檔案，可嘗試透過通行碼破解程式取得通行碼後進行攻擊 * 設定/etc/shadow-檔案權限為000(所有使用者不具有讀取、寫入及執行權限)，以保護帳號通行碼資訊，降低檔案被竄改後進一步利用於其他惡意攻擊之風險 | 開啟終端機，執行以下指令，設定/etc/shadow-檔案之權限為000：  # chmod 000 /etc/shadow- | 000 |
| 46 | TWGCB-01-013-0046 | 系統設定與維護 | /etc/group-檔案所有權 | * 這項原則設定決定/etc/group-檔案擁有者與群組 * /etc/group-備份每個群組之名稱、通行碼、ID及屬於該群組之使用者清單 * 設定/etc/group-檔案擁有者與群組為root，避免/etc/group-檔案遭未授權使用者修改 | 開啟終端機，執行以下指令，設定/etc/group-檔案所有權：  #chown root:root /etc/group- | root:root |
| 47 | TWGCB-01-013-0047 | 系統設定與維護 | /etc/group-檔案權限 | * 這項原則設定決定/etc/group-檔案權限 * /etc/group-備份每個群組之名稱、通行碼、ID及屬於該群組之使用者清單 * 設定/etc/group-檔案權限，僅root擁有讀取與寫入權限，其餘所有使用者僅可讀取，避免/etc/group-檔案遭未授權使用者修改 | 開啟終端機，執行以下指令，設定/etc/group-檔案權限為644或更低權限：  #chmod 644 /etc/group- | 644或更低權限 |
| 48 | TWGCB-01-013-0048 | 系統設定與維護 | /etc/gshadow-檔案所有權 | * 這項原則設定決定/etc/gshadow-檔案擁有者與群組 * /etc/gshadow-備份每個群組加密過後之通行碼，以及使用者與管理者資訊，攻擊者讀取/etc/gshadow-檔案後，可嘗試透過通行碼破解程式取得通行碼後進行攻擊 * 設定/etc/gshadow-檔案所有權，以保護群組帳號通行碼資訊，降低檔案被竄改後進一步利用於其他惡意攻擊之風險 | 開啟終端機，執行以下任一指令，設定/etc/gshadow-檔案之所有權：  #chown root:root /etc/gshadow-  或  #chown root:shadow /etc/gshadow- | root:root或root:shadow |
| 49 | TWGCB-01-013-0049 | 系統設定與維護 | /etc/gshadow-檔案權限 | * 這項原則設定決定/etc/gshadow-檔案權限 * /etc/gshadow-備份每個群組加密過後之通行碼，以及使用者與管理者資訊，若攻擊者讀取/etc/gshadow-檔案後，可嘗試透過通行碼破解程式取得通行碼後進行攻擊 * 設定/etc/gshadow-檔案權限為000(所有使用者不具有讀取、寫入及執行權限)，以保護群組帳號通行碼資訊，降低檔案被竄改後進一步利用於其他惡意攻擊之風險 | 開啟終端機，執行以下指令，設定/etc/gshadow-檔案之權限為000：  #chmod 000 /etc/gshadow- | 000 |
| 50 | TWGCB-01-013-0050 | 系統設定與維護 | 其他使用者寫入具有全域寫入權限之檔案 | * 這項原則設定決定其他使用者是否允許寫入具有全域寫入(World-writable)權限之檔案 * 具有全域寫入權限之檔案可被任何使用者修改，錯誤或不完整之程式碼將可能影響系統運作或危害系統安全 * 設定其他使用者不能寫入具有全域寫入權限之檔案，以避免系統重要檔案被未經授權竄改 | * 開啟終端機，執行以下指令，在系統上所有磁區(partition)，逐一檢查磁區所掛載之檔案目錄(如根目錄)，找出具有全域寫入權限(World-writable)之檔案：   #find (partition) -xdev -type f -perm -0002   * 針對所找到之檔案，執行下列指令，以移除其他身分寫入權限：   #chmod o-w (檔案名稱) | 禁止寫入 |
| 51 | TWGCB-01-013-0051 | 系統設定與維護 | 檢查所有檔案與目錄之擁有者 | * 這項原則設定決定是否所有檔案與目錄擁有者皆為合法使用者 * 不屬於合法使用者之檔案可能是由入侵者植入、不正確之軟體安裝、不完整之軟體移除或已遭刪除使用者所遺留之檔案 * 確認所有檔案與目錄擁有者皆為合法使用者，以避免新使用者帳號與已被刪除使用者帳號相同時，可以存取前任使用者所建立之檔案，將可能存取未被授權之檔案 | * 開啟終端機，執行以下指令，在系統上所有磁區(partition)，逐一檢查磁區所掛載之檔案目錄(如根目錄)，找出擁有者不是合法使用者之檔案或目錄：   #find (partition) -xdev -nouser   * 針對所找到之檔案與目錄指定合法使用者或移除：   #chown (使用者) (檔案名稱或目錄名稱)  或  #rm (檔案名稱或目錄名稱) | 所有檔案與目錄擁有者皆為合法使用者 |
| 52 | TWGCB-01-013-0052 | 系統設定與維護 | 檢查所有檔案與目錄之擁有群組 | * 這項原則設定決定是否所有檔案與目錄擁有群組皆為合法群組 * 不屬於合法群組之檔案可能是由入侵者植入、不正確之軟體安裝、不完整之軟體移除或已遭刪除使用者所遺留之檔案 * 確認所有檔案與目錄擁有群組皆為合法群組，以避免新使用者帳號與已被刪除使用者帳號相同時，可以存取前任使用者所屬群組之檔案，將可能存取未被授權之檔案 | * 開啟終端機，執行以下指令，在系統上所有磁區(partition)，逐一檢查磁區所掛載之檔案目錄(如根目錄)，找出擁有群組不是合法群組之檔案或目錄：   #find (partition) -xdev -nogroup   * 針對所找到之檔案與目錄指定合法群組或移除：   #chgrp (群組) (檔案名稱或目錄名稱)  或  #rm (檔案名稱或目錄名稱) | 所有檔案與目錄擁有群組皆為合法群組 |
| 53 | TWGCB-01-013-0053 | 系統設定與維護 | 所有具有全域寫入權限目錄之擁有者 | * 這項原則設定決定是否所有具有全域寫入權限之目錄擁有者為root或其他系統帳號 * 若具有全域寫入權限之目錄之擁有者為一般使用者，該使用者將可刪除或置換其他使用者所建立之檔案 * 設定所有具有全域寫入權限之目錄擁有者為root或其他系統帳號，避免系統資源遭未經授權存取 | * 開啟終端機，執行以下指令，在系統上所有磁區(partition)，逐一檢查磁區所掛載之檔案目錄(如根目錄)，找出一般使用者(UID大於999)具有全域寫入(World-writable)權限之目錄   #find (partition) -xdev -type d -perm -0002 -uid +999 -print   * 針對所找到之目錄，執行以下指令，設定目錄擁有者為root或其他系統帳號   #chown root (目錄名稱) | root或其他系統帳號 |
| 54 | TWGCB-01-013-0054 | 系統設定與維護 | 所有具有全域寫入權限目錄之擁有群組 | * 這項原則設定決定是否所有具有全域寫入權限之目錄擁有群組為root或其他系統群組(sys、bin或應用程式群組) * 若具有全域寫入權限之目錄之擁有群組為一般使用者群組，該群組使用者將可刪除或置換其他使用者所建立之檔案 | * 開啟終端機，執行以下指令，在系統上所有磁區(partition)，逐一檢查磁區所掛載之檔案目錄(如根目錄)，找出一般使用者群組(GID大於999)具有全域寫入(World-writable)權限之目錄   #find (partition) -xdev -type d -perm -0002 -gid +999 -print   * 針對所找到之目錄，執行以下指令，設定目錄擁有群組為root或其他系統群組(sys、bin或應用程式群組)：   #chgrp root (目錄名稱) | root或其他系統群組 |
| 55 | TWGCB-01-013-0055 | 系統設定與維護 | 系統命令檔案權限 | * 這項原則決定是否設定系統命令檔案權限，使系統命令檔案具有755或更低權限 * 系統命令檔案包含儲存在作業系統預設可執行檔案目錄之檔案，以及存在於系統預設可執行檔案搜索路徑目錄之檔案 * 限制權限以保護系統命令檔案，避免被未經授權竄改，使管理者與系統服務可正常執行指令 | * 開啟終端機，執行以下指令，檢查系統命令檔案之權限：   #find -L /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin -perm /0022 | xargs ls -al   * 若找到系統命令檔案權限高於755，執行以下指令，設定系統命令檔案之權限為755或更低權限：   #chmod 755 (系統命令檔案名稱) | 755或更低權限 |
| 56 | TWGCB-01-013-0056 | 系統設定與維護 | 系統命令檔案擁有者 | * 這項原則決定是否設定系統命令檔案擁有者 * 系統命令檔案包含儲存在作業系統預設可執行檔案目錄之檔案，以及存在於系統預設可執行檔案搜索路徑目錄之檔案 * 設定root擁有，以保護系統命令檔案，避免被未經授權竄改，使管理者與系統服務可正常執行指令 | * 開啟終端機，執行以下指令，檢查系統命令檔案擁有者：   #find -L /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin ! -user root | xargs ls -al   * 若找到系統命令檔案擁有者非root，執行以下指令，設定系統命令檔案擁有者為root：   #chown root (系統命令檔案名稱) | root |
| 57 | TWGCB-01-013-0057 | 系統設定與維護 | 系統命令檔案擁有群組 | * 這項原則決定是否設定系統命令檔案擁有群組 * 系統命令檔案包含儲存在作業系統預設可執行檔案目錄之檔案，以及存在於系統預設可執行檔案搜索路徑目錄之檔案 * 設定root群組擁有，以保護系統命令檔案，避免被未經授權竄改，使管理者與系統服務可正常執行指令 | * 開啟終端機，執行以下指令，檢查系統命令檔案擁有群組：   #find -L /bin /sbin /usr/bin /usr/sbin /usr/local/bin /usr/local/sbin ! -group root | xargs ls -al   * 若找到系統命令檔案擁有群組非root，執行以下指令，設定系統命令檔案擁有群組為root：   #chgrp root (系統命令檔案名稱) | root |
| 58 | TWGCB-01-013-0058 | 系統設定與維護 | 程式庫檔案權限 | * 這項原則決定是否設定程式庫檔案權限，使程式庫檔案具有755或更低權限 * 系統程序在啟動或運行時會連結到程式庫檔案，將程式庫檔案載入到系統核心之記憶體空間，程式庫檔案還包含用以升級特權執行之特權程序 * 限制權限以保護程式庫檔案，避免被未經授權竄改，維持系統完整性 | * 開啟終端機，執行以下指令，檢查程式庫檔案之權限：   #find -L /lib /lib64 /usr/lib /usr/lib64 -perm /0022 -type f | xargs ls -al   * 若找到程式庫檔案權限高於755，執行以下指令，設定程式庫檔案之權限為755或更低權限：   #chmod 755 (程式庫檔案名稱) | 755或更低權限 |
| 59 | TWGCB-01-013-0059 | 系統設定與維護 | 程式庫檔案擁有者 | * 這項原則決定是否設定程式庫檔案擁有者 * 系統程序在啟動或運行時會連結到程式庫檔案，將程式庫檔案載入到系統核心之記憶體空間，程式庫檔案還包含用以升級特權執行之特權程序 * 設定root擁有，以保護程式庫檔案，避免被未經授權竄改，維持系統完整性 | * 開啟終端機，執行以下指令，檢查程式庫檔案擁有者：   #find -L /lib /lib64 /usr/lib /usr/lib64 ! -user root | xargs ls -al   * 若找到程式庫檔案擁有者非root，執行以下指令，設定程式庫檔案擁有者為root：   #chown root (程式庫檔案名稱) | root |
| 60 | TWGCB-01-013-0060 | 系統設定與維護 | 程式庫檔案擁有群組 | * 這項原則決定是否設定程式庫檔案擁有群組 * 系統程序在啟動或運行時會連結到程式庫檔案，將程式庫檔案載入到系統核心之記憶體空間，程式庫檔案還包含用以升級特權執行之特權程序 * 設定root群組擁有，以保護程式庫檔案避免被未經授權竄改，維持系統完整性 | * 開啟終端機，執行以下指令，檢查程式庫檔案擁有群組：   #find -L /lib /lib64 /usr/lib /usr/lib64 ! -group root | xargs ls -al   * 若找到程式庫檔案擁有群組非root，執行以下指令，設定程式庫檔案擁有群組為root：   #chgrp root (程式庫檔案名稱) | root |
| 61 | TWGCB-01-013-0061 | 系統設定與維護 | 帳號不使用空白通行碼 | * 這項原則設定決定是否允許存在使用空白通行碼之帳號 * 使用空白通行碼意謂著任何人皆可以此帳號登入系統，並以該帳號之權限執行相關指令，將可能危害系統安全 * 設定帳號都必須具有通行碼或被鎖定，以防止未經授權之使用者登入該帳號 | * 開啟終端機，執行以下指令，列出使用空白通行碼之帳號：   #awk -F: '($2 == "" ) { print $1 " does not have a password "}' /etc/shadow   * 若有使用空白通行碼之帳號，則執行下列指令以設定通行碼：   #passwd (帳號名稱)  或執行下列指令以鎖定帳號：  #passwd -l (帳號名稱) | 帳號必須具有通行碼或被鎖定 |
| 62 | TWGCB-01-013-0062 | 系統設定與維護 | root帳號之路徑變數 | * 這項原則設定決定是否允許root帳號之路徑(PATH)變數存在相對路徑或空目錄(例如：「.」、「..」、路徑開頭不是「/」及空元素) * root帳號可以執行系統上所有指令，若PATH設定錯誤，root將可能執行到偽裝之程式檔案，危害系統安全   .：目前目錄  ..：上一層目錄 | * 開啟終端機，執行以下指令，顯示PATH變數內容：   #echo $PATH   * 如出現「.」、「..」、路徑開頭不是「/」及空元素等內容，請編輯/etc/profile檔案進行修改 | 不允許「.」、「..」、路徑開頭不是「/」及空元素 |
| 63 | TWGCB-01-013-0063 | 系統設定與維護 | root帳號之路徑變數不包含world-writable或group-writable目錄 | * 這項原則設定決定是否允許root帳號之路徑(PATH)變數存在具有world-writable權限或group-writable權限之目錄 * root可以執行系統上所有指令，若PATH變數包含world-writable(全域寫入)權限或group-writable(群組身分寫入)權限之目錄，將可能導致root執行到惡意程式，危害系統安全 | * 開啟終端機，執行以下指令，顯示PATH變數內容：   #echo $PATH   * 如出現具有world-writable權限或group-writable權限之目錄，請編輯/etc/profile檔案進行修改，或執行下列指令變更目錄權限：   #chmod o-w (目錄名稱)  或  #chmod g-w (目錄名稱) | 不包含world-writable或group-writable目錄 |
| 64 | TWGCB-01-013-0064 | 系統設定與維護 | /etc/passwd檔案行首之「+」符號 | * 這項原則設定決定/etc/passwd檔案行首是否允許存在「+」符號 * 「+」符號代表不需輸入通行碼即可從網路資訊服務(NIS)主機取得帳號、通行碼、主機名稱或群組等資訊 * 當NIS沒有啟動或NIS設定錯誤時，/etc/passwd檔案行首若存在「+」符號，攻擊者可使用帳號「+」與空白通行碼登入，提供攻擊者一個獲得系統權限之途徑 | * 開啟終端機，執行以下指令，確認/etc/passwd檔案行首是否存在「+」符號：   #grep '^\+:' /etc/passwd   * 如果有，則編輯/etc/passwd檔案，將行首為「+」符號之列移除 | 禁止 |
| 65 | TWGCB-01-013-0065 | 系統設定與維護 | /etc/shadow檔案行首之「+」符號 | * 這項原則設定決定/etc/shadow檔案行首是否允許存在「+」符號 * 「+」符號代表不需輸入通行碼即可從網路資訊服務(NIS)主機取得帳號、通行碼、主機名稱或群組等資訊 * 當NIS沒有啟動或NIS設定錯誤時，/etc/shadow檔案行首若存在「+」符號，攻擊者可使用帳號「+」與空白通行碼登入，提供攻擊者一個獲得系統權限之途徑 | * 開啟終端機，執行以下指令，確認/etc/shadow檔案行首是否存在「+」符號：   #grep '^\+:' /etc/shadow   * 如果有，則編輯/etc/shadow檔案，將行首為「+」符號之列移除 | 禁止 |
| 66 | TWGCB-01-013-0066 | 系統設定與維護 | /etc/group檔案行首之「+」符號 | * 這項原則設定決定/etc/group檔案行首是否允許存在「+」符號 * 「+」符號代表不需輸入通行碼即可從網路資訊服務(NIS)主機取得帳號、通行碼、主機名稱或群組等資訊 * 當NIS沒有啟動或NIS設定錯誤時，/etc/group檔案行首若存在「+」符號，攻擊者可使用帳號「+」與空白通行碼登入，提供攻擊者一個獲得系統權限之途徑 | * 開啟終端機，執行以下指令，確認/etc/group檔案行首是否存在「+」符號：   #grep '^\+:' /etc/group   * 如果有，則編輯/etc/group檔案，將行首為「+」符號之列移除 | 禁止 |
| 67 | TWGCB-01-013-0067 | 系統設定與維護 | UID=0之帳號 | * 這項原則設定決定系統除了root帳號外，其他帳號之UID是否允許設為0 * UID=0之帳號具有系統管理權限 | * 開啟終端機，執行以下指令，列出UID=0之帳號：   #awk -F: '($3 == 0) { print $1 }' /etc/passwd   * 若存在非root帳號，則執行以下指令，移除帳號或重新設定UID：   #userdel (帳號名稱)  或  #usermod -u (UID) (帳號名稱) | 僅root帳號之UID為0 |
| 68 | TWGCB-01-013-0068 | 系統設定與維護 | 使用者家目錄權限 | * 這項原則設定決定使用者家目錄權限 * 使用者家目錄是系統預設之使用者主目錄，目錄下存放使用者之環境設定與個人檔案，因此任何使用者皆不應具有可寫入其他使用者家目錄之權限 * 使用者家目錄應限制群組不具寫入(g-w)權限，其他使用者不具讀取、寫入及執行(o-rwx)權限，避免遭未經授權存取與竊取資料 | * 開啟終端機，執行以下腳本，檢查每個使用者家目錄權限：   #!/bin/bash  grep -E -v '^(halt|sync|shutdown)' /etc/passwd | awk -F: '($7 != "'"$(which nologin)"'" && $7 != "/bin/false") { print $1 " " $6 }' | while read user dir; do  if [ ! -d "$dir" ]; then  echo "The home directory ($dir) of user $user does not exist."  else  dirperm=$(ls -ld $dir | cut -f1 -d" ")  if [ $(echo $dirperm | cut -c6) != "-" ]; then  echo "Group Write permission set on the home directory ($dir) of user  $user"  fi  if [ $(echo $dirperm | cut -c8) != "-" ]; then  echo "Other Read permission set on the home directory ($dir) of user  $user"  fi  if [ $(echo $dirperm | cut -c9) != "-" ]; then  echo "Other Write permission set on the home directory ($dir) of user  $user"  fi  if [ $(echo $dirperm | cut -c10) != "-" ]; then  echo "Other Execute permission set on the home directory ($dir) of user  $user"  fi  fi  done   * 若出現群組具寫入權限，其他使用者具讀取、寫入及執行權限之家目錄，則可執行以下指令，變更目錄權限為700或更低權限：   #chmod 700 /home/(使用者帳號名稱)   * 注意：請先通知使用者再變更家目錄相關設定，以避免影響使用者作業 | 700或更低權限 |
| 69 | TWGCB-01-013-0069 | 系統設定與維護 | 使用者家目錄擁有者 | * 這項原則設定決定使用者家目錄擁有者是否為使用者 * 使用者家目錄是系統預設之使用者主目錄，目錄下存放使用者之環境設定與個人檔案 * 設定使用者家目錄為使用者擁有，以確保使用者個人資料安全 | * 開啟終端機，執行以下腳本，檢查每個使用者家目錄擁有者：   #!/bin/bash  grep -E -v '^(halt|sync|shutdown)' /etc/passwd | awk -F: '($7 != "'"$(which nologin)"'" && $7 != "/bin/false") { print $1 " " $6 }' | while read user dir; do  if [ ! -d "$dir" ]; then  echo "The home directory ($dir) of user $user does not exist."  else  owner=$(stat -L -c "%U" "$dir")  if [ "$owner" != "$user" ]; then  echo "The home directory ($dir) of user $user is owned by $owner."  fi  fi  done   * 若出現使用者之家目錄非使用者擁有，則可執行以下指令，變更家目錄擁有者為使用者： * #chown (使用者帳號名稱) /home/(使用者帳號名稱) * 注意：請先通知使用者再變更家目錄相關設定，以避免影響使用者作業 | 使用者擁有 |
| 70 | TWGCB-01-013-0070 | 系統設定與維護 | 使用者家目錄擁有群組 | * 這項原則設定決定使用者家目錄擁有群組是否為使用者群組 * 使用者家目錄是系統預設之使用者主目錄，目錄下存放使用者之環境設定與個人檔案 * 若使用者家目錄擁有群組GID與使用者群組GID不同，將導致其他使用者可存取該使用者之檔案 * 設定使用者家目錄為使用者群組擁有，以確保使用者個人資料安全 | * 開啟終端機，執行以下腳本，檢查每個使用者家目錄之擁有群組GID：   #!/bin/bash  grep -E -v '^(halt|sync|shutdown)' /etc/passwd | awk -F: '($7 != "'"$(which nologin)"'" && $7 != "/bin/false") { print $1 " " $4 " " $6 }' | while read user gid dir; do  if [ ! -d "$dir" ]; then  echo "The home directory ($dir) of user $user does not exist."  else  owner=$(stat -L -c "%g" "$dir")  if [ "$owner" != "$gid" ]; then  echo "The home directory ($dir) of group $gid is owned by group $owner."  fi  fi  done   * 若出現使用者家目錄非使用者群組所擁有，則可執行以下指令，變更家目錄擁有者為使用者群組：   #chgrp (使用者群組名稱或GID) /home/(使用者帳號名稱)   * 注意：請先通知使用者再變更家目錄相關設定，以避免影響使用者作業 | 使用者群組擁有 |
| 71 | TWGCB-01-013-0071 | 系統設定與維護 | 使用者家目錄之「.」檔案權限 | * 這項原則設定決定是否設定使用者家目錄之「.」檔案權限，使用者家目錄之「.」檔案包含使用者之初始化檔案與其他設定檔 * 限制使用者家目錄之「.」檔案寫入權限，以避免惡意人士藉由竊取或修改使用者資料，進而取得該使用者之系統權限 | * 開啟終端機，執行以下腳本，檢查每個使用者家目錄之「.」檔案權限：   #!/bin/bash  grep -E -v '^(halt|sync|shutdown)' /etc/passwd | awk -F: '($7 != "'"$(which nologin)"'" && $7 != "/bin/false") { print $1 " " $6 }' | while read user dir; do  if [ ! -d "$dir" ]; then  echo "The home directory ($dir) of user $user does not exist."  else  for file in $dir/.[A-Za-z0-9]\*; do  if [ ! -h "$file" -a -f "$file" ]; then  fileperm=$(ls -ld $file | cut -f1 -d" ")  if [ $(echo $fileperm | cut -c6) != "-" ]; then  echo "Group Write permission set on file $file"  fi  if [ $(echo $fileperm | cut -c9) != "-" ]; then  echo "Other Write permission set on file $file"  fi  fi  done  fi  done   * 若出現具有world-writable或group-writable權限之「.」檔案，則可執行以下指令，移除群組與其他身分之寫入權限或更低權限：   #chmod go-w (檔案名稱)   * 注意：請先通知使用者再變更家目錄相關設定，以避免影響使用者作業 | go-w或更低權限 |
| 72 | TWGCB-01-013-0072 | 系統設定與維護 | 使用者家目錄之「.forward」檔案 | * 這項原則設定決定是否移除使用者家目錄之「.forward」檔案 * 「.forward」檔案用於設定將使用者郵件轉發到指定之電子郵件信箱 * 移除「.forward」檔案以停用郵件轉發功能，避免機敏資料洩漏 | * 開啟終端機，執行以下腳本，檢查每個使用者家目錄是否存在「.forward」檔案：   #!/bin/bash  grep -E -v '^(root|halt|sync|shutdown)' /etc/passwd | awk -F: '($7 != "'"$(which nologin)"'" && $7 != "/bin/false") { print $1 " " $6 }' | while read user dir; do  if [ ! -d "$dir" ]; then  echo "The home directory ($dir) of user $user does not exist."  else  if [ ! -h "$dir/.forward" -a -f "$dir/.forward" ]; then  echo ".forward file $dir/.forward exists"  fi  fi  done   * 若存在「.forward」檔案，則可執行以下指令移除檔案：   #rm (檔案名稱)   * 注意：請先通知使用者再變更家目錄相關設定，以避免影響使用者作業 | 移除 |
| 73 | TWGCB-01-013-0073 | 系統設定與維護 | 使用者家目錄之「.netrc」檔案 | * 這項原則設定決定是否移除使用者家目錄之「.netrc」檔案 * 「.netrc」檔案包含用於登入遠端FTP主機進行檔案傳輸之帳號與明文通行碼，移除「.netrc」檔案以避免對遠端FTP主機造成之風險 | * 開啟終端機，執行以下腳本，檢查每個使用者家目錄是否存在「.netrc」檔案：   #!/bin/bash  grep -E -v '^(root|halt|sync|shutdown)' /etc/passwd | awk -F: '($7 != "'"$(which nologin)"'" && $7 != "/bin/false") { print $1 " " $6 }' | while read user dir; do  if [ ! -d "$dir" ]; then  echo "The home directory ($dir) of user $user does not exist."  else  if [ ! -h "$dir/.netrc" -a -f "$dir/.netrc" ]; then  echo ".netrc file $dir/.netrc exists"  fi  fi  done   * 若存在「.netrc」檔案，則可執行以下指令移除檔案：   #rm (檔案名稱)   * 注意：請先通知使用者再變更家目錄相關設定，以避免影響使用者作業 | 移除 |
| 74 | TWGCB-01-013-0074 | 系統設定與維護 | 使用者家目錄之「.rhosts」檔案 | * 這項原則設定決定是否移除使用者家目錄之「.rhosts」檔案 * 「.rhosts」檔案用於指定那個使用者可以不需要輸入通行碼即可執行rsh遠端連線，移除「.rhosts」檔案以避免遭惡意人士取得可攻擊其他遠端主機之資訊 | * 開啟終端機，執行以下腳本，檢查每個使用者家目錄是否存在「.rhosts」檔案：   #!/bin/bash  grep -E -v '^(root|halt|sync|shutdown)' /etc/passwd | awk -F: '($7 != "'"$(which nologin)"'" && $7 != "/bin/false") { print $1 " " $6 }' | while read user dir; do  if [ ! -d "$dir" ]; then  echo "The home directory ($dir) of user $user does not exist."  else  for file in $dir/.rhosts; do  if [ ! -h "$file" -a -f "$file" ]; then  echo ".rhosts file in $dir"  fi  done  fi  done   * 若存在「.rhosts」檔案，則可執行以下指令移除檔案：   #rm (檔案名稱)   * 注意：請先通知使用者再變更家目錄相關設定，以避免影響使用者作業 | 移除 |
| 75 | TWGCB-01-013-0075 | 系統設定與維護 | 檢查/etc/passwd檔案設定之群組 | * 這項原則設定決定是否檢查/etc/passwd檔案設定之群組，是否都存在於/etc/group檔案中 * 在/etc/passwd檔案中，使用者帳號設定之群組，若不存在於/etc/group檔案中，代表群組權限管理不恰當，將可能對系統安全構成威脅 | * 開啟終端機，執行以下腳本，檢查/etc/passwd檔案中帳號之群組是否都存在於/etc/group檔案中：   #!/bin/bash  for i in $(cut -s -d: -f4 /etc/passwd | sort -u ); do  grep -q -P "^.\*?:[^:]\*:$i:" /etc/group  if [ $? -ne 0 ]; then  echo "Group $i is referenced by /etc/passwd but does not exist in /etc/group"  fi  done   * 若有帳號之群組不存在於/etc/group檔案中，則編輯/etc/passwd檔案，或執行以下指令，修改帳號之群組(GID)：   #usermod -g (群組名稱或GID) (帳號名稱) | /etc/passwd檔案中帳號之群組皆須存在於/etc/group檔案中 |
| 76 | TWGCB-01-013-0076 | 系統設定與維護 | 唯一之UID | * 這項原則設定決定是否檢查/etc/passwd檔案之使用者帳號UID(User Identifier，使用者識別碼)皆不相同 * 儘管透過useradd指令新增使用者帳號時，不允許建立重複之UID，但系統管理者可手動編輯/etc/passwd檔案並更改UID，造成UID重複之情形 * 為每個使用者帳號設定唯一之UID，以提供適當之存取防護 | * 開啟終端機，執行以下腳本，尋找是否有不同帳號使用相同之UID：   #!/bin/bash  cut -f3 -d":" /etc/passwd | sort -n | uniq -c | while read x ; do  [ -z "$x" ] && break  set - $x  if [ $1 -gt 1 ]; then  users=$(awk -F: '($3 == n) { print $1 }' n=$2 /etc/passwd | xargs)  echo "Duplicate UID ($2): $users"  fi  done   * 若有不同帳號使用相同之UID，則編輯/etc/passwd檔案，或執行以下指令，為帳號設定唯一之UID：   #usermod -u (UID) (帳號名稱) | 為每個帳號設定唯一之UID |
| 77 | TWGCB-01-013-0077 | 系統設定與維護 | 唯一之GID | * 這項原則設定決定是否檢查/etc/group檔案之群組GID(Group Identifier，群組識別碼)皆不相同 * 儘管透過groupadd指令新增群組時，不允許建立重複之GID，但系統管理者可手動編輯/etc/group檔案並更改GID，造成GID重複之情形 * 為每個群組設定唯一之GID，以提供適當之存取防護 | * 開啟終端機，執行以下腳本，尋找是否有群組使用相同之GID：   #!/bin/bash  cut -d: -f3 /etc/group | sort | uniq -d | while read x ; do  echo "Duplicate GID ($x) in /etc/group"  done   * 若有不同群組使用相同GID，則編輯/etc/group檔案，或執行以下指令，為群組設定唯一之GID：   #groupmod -g (GID) (群組名稱) | 為每個群組設定唯一之GID |
| 78 | TWGCB-01-013-0078 | 系統設定與維護 | 唯一之使用者帳號名稱 | * 這項原則設定決定是否檢查/etc/passwd檔案之使用者帳號名稱，並確認每個使用者帳號名稱皆不相同 * 儘管透過useradd指令新增使用者帳號時，不允許建立重複之帳號名稱，但系統管理者可手動編輯/etc/passwd檔案並更改帳號名稱，造成帳號名稱重複之情形 * 為每個使用者帳號設定唯一之名稱，以提供適當之存取防護 | * 開啟終端機，執行以下腳本，尋找是否有帳號使用重複之帳號名稱：   #!/bin/bash  cut -d: -f1 /etc/passwd | sort | uniq -d | while read x  do echo "Duplicate login name ${x} in /etc/passwd"  done   * 若有帳號使用重複之帳號名稱，則編輯/etc/passwd檔案，為帳號設定唯一不重複之帳號名稱 | 為每個使用者帳號設定唯一之名稱 |
| 79 | TWGCB-01-013-0079 | 系統設定與維護 | 唯一之群組名稱 | * 這項原則設定決定是否檢查/etc/group檔案之群組名稱，並確認每個群組名稱皆不相同 * 儘管透過groupadd指令新增群組時，不允許建立重複之群組名稱，但系統管理者可手動編輯/etc/group檔案並更改群組名稱，造成群組名稱重複之情形 * 為每個群組設定唯一之群組名稱，以提供適當之存取防護 | * 開啟終端機，執行以下腳本，尋找是否有不同群組使用相同之群組名稱：   #!/bin/bash  cut -d: -f1 /etc/group | sort | uniq -d | while read x  do echo "Duplicate group name ${x} in /etc/group"  done   * 若有群組使用相同之群組名稱，則編輯/etc/group檔案，為每個群組設定唯一之群組名稱 | 為每個群組設定唯一之群組名稱 |
| 80 | TWGCB-01-013-0080 | 系統設定與維護 | shadow群組成員 | * 這項原則設定決定shadow群組成員是否無使用者 * 隸屬於shadow群組之使用者具有可讀取/etc/shadow檔案之權限，若攻擊者可讀取/etc/shadow檔案，使用者通行碼與其他安全資訊將可能被攻擊者破解並執行進一步攻擊 * 設定shadow群組不包含任何使用者，以降低系統風險 | * 開啟終端機，執行以下指令，列舉shadow群組中之使用者帳號：   #awk -F: '($1=="shadow") {print $NF}' /etc/group   * 如shadow群組有使用者帳號，請針對每個帳號執行下列步驟：  1. 執行以下指令，從shadow群組移除使用者帳號：   #sed -ri 's/(^shadow:[^:]\*:[^:]\*:)([^:]+$)/\1/' /etc/group   1. 執行以下指令，將使用者帳號之主要群組，從shadow修改為預設群組：   #usermod -g (預設群組名稱) (帳號名稱) | shadow群組不包含任何使用者 |
| 81 | TWGCB-01-013-0081 | 系統服務 | xinetd套件 | * 這項原則設定決定是否移除xinetd套件 * xinetd(Extended Internet daemon)套件取代原有之inetd守護程序，負責管理網路相關服務 * xinetd監聽來自網路之請求，進而啟動相應服務，可以用來啟動使用特權埠與非特權埠之服務 * 移除xinetd套件可降低系統被攻擊面 | 開啟終端機，執行以下指令移除xinetd套件：  #dnf remove xinetd | 移除 |
| 82 | TWGCB-01-013-0082 | 系統服務 | chrony校時設定 | * 這項原則設定決定是否設定chrony守護程序之校時來源 * chrony是一個守護程序，藉由實做網路時間協定(NTP)，以於各系統之間同步系統時間，並可使用高準確之校時來源 * 設定chrony校時來源，以確保系統時間正確 | 編輯/etc/chrony.conf檔案，新增或修改NTP伺服器設定，範例如下：  server (NTP伺服器名稱)  或  pool (NTP池名稱) | 設定1個以上校時來源 |
| 83 | TWGCB-01-013-0083 | 系統服務 | rsyncd服務 | * 這項原則設定決定是否啟用rsyncd服務 * rsyncd服務用於透過網路連接在兩台電腦之間同步檔案與目錄，並可利用差分編碼以減少資料傳輸量 * 由於rsyncd服務使用未加密協議進行資料傳輸，停用rsyncd服務可降低資安風險 | 開啟終端機，執行以下指令停用rsyncd服務：  #systemctl --now disable rsyncd | 停用 |
| 84 | TWGCB-01-013-0084 | 系統服務 | sshd守護程序 | * 這項原則設定決定是否啟用sshd守護程序 * sshd(Openssh Server程式)實做SSH(Secure Shell)協定，可在兩個主機之間提供安全加密通訊 * 啟用sshd守護程序，以加密方式保護傳輸資訊，以防攻擊者藉由封包攔截取得明文機敏資訊 | 執行以下指令，停用sshd守護程序：  #systemctl --now disable sshd.service | 停用 |
| 85 | TWGCB-01-013-0085 | 系統服務 | SNMP服務 | * 這項原則設定決定是否啟用SNMP服務 * SNMP(Simple Network Management Protocol，簡單網路管理協定)服務用於監聽來自SNMP管理系統之SNMP命令，執行命令或蒐集資訊，然後將結果送回請求系統 * SNMP伺服器可以使用SNMPv1與SNMPv2進行通訊，因SNMPv1與SNMPv2使用不安全之明文傳輸設計，停用SNMP服務可降低系統被攻擊面 | 執行以下任一操作設定SNMP服務：   1. 停用SNMP服務   開啟終端機，執行以下指令停用SNMP服務：  #systemctl --now disable snmpd   1. 僅啟用SNMPv3功能   使用「net-snmp-create-v3-user」工具設定啟用SNMPv3功能之範例如下：   * 開啟終端機，執行以下指令停止SNMP服務：   #systemctl stop snmpd   * 執行以下指令設定SNMPv3並建立SNMPv3使用者，設定為僅允許讀取、身分鑑別使用SHA及傳輸加密使用AES：   #net-snmp-create-v3-user -ro -A (使用者通行碼) -a SHA -X (傳輸加密用金鑰) -x AES (使用者名稱)   * 執行以下指令編輯/etc/snmp/snmpd.conf檔案：   #vim /etc/snmp/snmpd.conf   * 將包含com2sec、group、view及access參數之行內容註解(新增#符號於行首)，以停用SNMPv1與SNMPv2，範例如下：   #com2sec notConfigUser default public  #group notConfigGroup v1 notConfigUser  #group notConfigGroup v2c notConfigUser  #view systemview included .1.3.6.1.2.1.1  #view systemview included .1.3.6.1.2.1.25.1.1  #access notConfigGroup "" any noauth exact systemview none none   * 執行以下指令重新啟動SNMP服務，令設定生效僅啟用SNMPv3：   #systemctl start snmpd | 停用SNMP服務或僅啟用SNMPv3功能 |
| 86 | TWGCB-01-013-0086 | 系統服務 | Squid服務 | * 這項原則設定決定是否啟用squid服務，以運行代理伺服器功能 * 攻擊者透過代理伺服器攻擊其他伺服器時，可以藉此隱匿身分，甚至進而進入到其他受保護之網段中 * 停用Squid服務可降低系統被攻擊面 | 開啟終端機，執行以下指令停用Squid服務：  #systemctl --now disable squid | 停用 |
| 87 | TWGCB-01-013-0087 | 系統服務 | Samba服務 | * 這項原則設定決定是否啟用Samba服務 * Samba運用SMB ( Server message block)協定分享目錄與檔案予微軟Windows作業系統 * 停用Samba服務可降低系統被攻擊面 | 開啟終端機，執行以下指令停用Samba服務：  #systemctl --now disable smb | 停用 |
| 88 | TWGCB-01-013-0088 | 系統服務 | FTP伺服器 | * 這項原則設定決定是否啟用FTP伺服器服務 * FTP(File Transfer Protocol，檔案傳輸協定)可透過網路連接在兩台電腦之間傳輸檔案，因使用明文傳輸方式，故有資料洩露風險 * 停用FTP伺服器服務可降低系統被攻擊面 * 如有FTP使用需求，建議改採SFTP，以保護資料傳輸安全 | 開啟終端機，執行以下指令停用FTP伺服器服務(vsftpd)：  #systemctl --now disable vsftpd | 停用 |
| 89 | TWGCB-01-013-0089 | 系統服務 | NIS伺服器 | * 這項原則設定決定是否啟用NIS伺服器服務 * NIS(Network Information System，網路資訊服務)可提供帳號、通行碼、主機名稱或群組等資訊進行登入鑑別，NIS使用較不嚴謹之身分鑑別機制，易受到服務阻斷攻擊 * 停用NIS伺服器服務可降低系統被攻擊面 | 開啟終端機，執行以下指令停用NIS伺服器服務(ypserv)：  #systemctl --now disable ypserv | 停用 |
| 90 | TWGCB-01-013-0090 | 系統服務 | kdump服務 | * 這項原則設定決定是否啟用kdump(核心當機時之傾印機制)服務 * kdump是Linux核心其中一項功能，當系統當機時，kdump會被觸發並匯出一個記憶體映像檔案，該映像檔可用於除錯以找出導致當機之原因 * 啟用kdump服務保留作業系統狀態資訊，以提供系統管理者修復系統所需相關資訊 | 開啟終端機，執行以下指令啟用kdump服務：  #systemctl --now enable kdump.service | 啟用 |
| 91 | TWGCB-01-013-0091 | 安裝與維護軟體 | NIS用戶端套件 | * 這項原則設定決定是否安裝NIS用戶端套件(ypbind) * NIS(Network Information System，網路資訊服務)可提供帳號、通行碼、主機名稱或群組等資訊進行登入鑑別，NIS使用較不嚴謹之身分鑑別機制，易受到服務阻斷攻擊 * 移除NIS用戶端套件，以避免使用較不安全之NIS服務 | 開啟終端機，執行以下指令移除ypbind套件：  #dnf remove ypbind | 移除 |
| 92 | TWGCB-01-013-0092 | 安裝與維護軟體 | telnet用戶端套件 | * 這項原則設定決定是否安裝telnet用戶端套件 * telnet協定不安全且未加密傳輸，將可能導致機敏資料外洩 * 移除telnet用戶端套件，以避免使用不安全之telnet服務 | 開啟終端機，執行以下指令移除telnet套件：  #dnf remove telnet | 移除 |
| 93 | TWGCB-01-013-0093 | 安裝與維護軟體 | telnet伺服器套件 | * 這項原則設定決定是否安裝telnet伺服器套件(telnet-server) * telnet協定不安全且未加密傳輸，將可能導致機敏資料外洩 * 移除telnet伺服器套件，以避免使用不安全之telnet服務 | 開啟終端機，執行以下指令移除telnet-server套件：  #dnf remove telnet-server | 移除 |
| 94 | TWGCB-01-013-0094 | 安裝與維護軟體 | rsh伺服器套件 | * 這項原則設定決定是否安裝rsh伺服器套件(rsh-server) * rsh伺服器提供未加密之遠端存取服務，將可能導致機敏資料外洩 * 移除rsh伺服器套件，以避免使用不安全之rsh服務 | 開啟終端機，執行以下指令移除rsh-server套件：  #dnf remove rsh-server | 移除 |
| 95 | TWGCB-01-013-0095 | 安裝與維護軟體 | tftp伺服器套件 | * 這項原則設定決定是否安裝tftp伺服器套件(tftp-server) * tftp(Trivial File Transfer Protocol，簡單檔案傳輸協定)可 讓使用者在用戶端與伺服器之間使用tftp通訊協定來傳輸檔案。tftp通訊協定不支援任何身分鑑別或加密機制，將可能導致資料外洩 * 移除tftp伺服器套件，以降低系統被攻擊面 | 開啟終端機，執行以下指令移除tftp-server套件：  #dnf remove tftp-server | 移除 |
| 96 | TWGCB-01-013-0096 | 安裝與維護軟體 | 更新套件後移除舊版本元件 | * 這項原則設定決定系統更新套件後是否移除舊版本元件 * 安裝更新後，若未從系統中移除舊版本元件，可能遭攻擊者利用舊版本元件漏洞進行攻擊 | 編輯/etc/yum.conf與/etc/dnf/dnf.conf檔案，新增或修改成以下內容：  clean\_requirements\_on\_remove=True | True |
| 97 | TWGCB-01-013-0097 | 網路設定 | IP轉送 | * 這項原則設定決定是否啟用IP轉送(Forwarding)功能 * IP轉送功能可在不同網卡之間傳遞封包，讓兩個網域可以互相溝通 * IP轉送功能一般實做在路由器上，擁有多網路介面之主機也可以實做 * 系統並非做為路由器，停用IP轉送功能，以提升網路安全性 * 可設定之參數如下：  1. 0：表示停用IP轉送功能 2. 1：表示啟用IP轉送功能 | 開啟終端機，執行以下指令，將net.ipv4.ip\_forward與net.ipv6.conf.all.forwarding皆設為0，以停用IP轉送功能，並使變動立即生效：  #grep -Els "^\s\*net\.ipv4\.ip\_forward\s\*=\s\*1" /etc/sysctl.conf /etc/sysctl.d/\*.conf /usr/lib/sysctl.d/\*.conf /run/sysctl.d/\*.conf | while read filename; do sed -ri "s/^\s\*(net\.ipv4\.ip\_forward\s\*)(=)(\s\*\S+\b).\*$/# \*REMOVED\* \1/" $filename; done; sysctl -w net.ipv4.ip\_forward=0; sysctl -w net.ipv4.route.flush=1  #grep -Els "^\s\*net\.ipv6\.conf\.all\.forwarding\s\*=\s\*1" /etc/sysctl.conf /etc/sysctl.d/\*.conf /usr/lib/sysctl.d/\*.conf /run/sysctl.d/\*.conf | while read filename; do sed -ri "s/^\s\*(net\.ipv6\.conf\.all\.forwarding\s\*)(=)(\s\*\S+\b).\*$/# \*REMOVED\* \1/" $filename; done; sysctl -w net.ipv6.conf.all.forwarding=0; sysctl -w net.ipv6.route.flush=1 | 0 |
| 98 | TWGCB-01-013-0098 | 網路設定 | 所有網路介面禁止傳送ICMP重新導向封包 | * 這項原則設定決定所有網路介面是否允許傳送ICMP重新導向(Redirect)封包 * 當路由器發現主機所選之路徑並非最佳路徑時，會送出ICMP重新導向封包，通知主機較佳之路徑 * 系統並非做為路由器，停用ICMP重新導向功能，以提升網路安全性 * 若啟用ICMP重新導向功能，攻擊者可利用已被入侵之主機發送惡意之ICMP重新導向封包給其他路由器，誘使其他主機連線至攻擊者所架設之假系統 * sysctl設定ICMP重新導向封包時，網路介面包含all與default兩種類型，all包含default，但設定時建議all與default都要進行設定 * 可設定之參數如下：  1. 0：表示禁止傳送ICMP重新導向封包 2. 1：表示允許傳送ICMP重新導向封包 | * 編輯/etc/sysctl.conf檔案或/etc/sysctl.d/目錄下之檔案，新增或修改參數如下：   net.ipv4.conf.all.send\_redirects = 0   * 開啟終端機，執行以下指令設定核心參數：   #sysctl -w net.ipv4.conf.all.send\_redirects=0   * 開啟終端機，執行以下指令使變動立即生效：   #sysctl -w net.ipv4.route.flush=1 | 0 |
| 99 | TWGCB-01-013-0099 | 網路設定 | 預設網路介面禁止傳送ICMP重新導向封包 | * 這項原則設定決定預設網路介面是否允許傳送ICMP重新導向(Redirect)封包 * 當路由器發現主機所選之路徑並非最佳路徑時，會送出ICMP重新導向封包，通知主機較佳之路徑 * 系統並非做為路由器，停用ICMP重新導向功能，以提升網路安全性 * 若啟用ICMP重新導向功能，攻擊者可利用已被入侵之主機發送惡意之ICMP重新導向封包給其他路由器，誘使其他主機連線至攻擊者所架設之假系統 * sysctl設定ICMP重新導向封包時，網路介面包含all與default兩種類型，all包含default，但設定時建議all與default都要進行設定 * 可設定之參數如下：  1. 0：表示禁止傳送ICMP重新導向封包 2. 1：表示允許傳送ICMP重新導向封包 | * 編輯/etc/sysctl.conf檔案或/etc/sysctl.d/目錄下之檔案，新增或修改參數如下：   net.ipv4.conf.default.send\_redirects = 0   * 開啟終端機，執行以下指令設定核心參數：   #sysctl -w net.ipv4.conf.default.send\_redirects=0   * 開啟終端機，執行以下指令使變動立即生效：   #sysctl -w net.ipv4.route.flush=1 | 0 |
| 100 | TWGCB-01-013-0100 | 網路設定 | 所有網路介面阻擋來源路由封包 | * 這項原則設定決定所有網路介面是否接受來源路由封包 * 來源路由(Source routing)可以用來指定一條從來源位址到目之位址之間之資料傳送路徑，阻擋來源路由封包，以防止封包偽裝(Packet Spoofing)攻擊 * 可設定之參數如下：  1. 0：表示阻擋來源路由封包 2. 1：表示接受來源路由封包 | * 編輯/etc/sysctl.conf檔案或/etc/sysctl.d/目錄下之檔案，新增或修改參數如下：   net.ipv4.conf.all.accept\_source\_route = 0  net.ipv6.conf.all.accept\_source\_route = 0   * 開啟終端機，執行以下指令設定核心參數：   #sysctl -w net.ipv4.conf.all.accept\_source\_route=0  #sysctl -w net.ipv6.conf.all.accept\_source\_route=0   * 開啟終端機，執行以下指令使變動立即生效：   #sysctl -w net.ipv4.route.flush=1  #sysctl -w net.ipv6.route.flush=1 | 0 |
| 101 | TWGCB-01-013-0101 | 網路設定 | 預設網路介面阻擋來源路由封包 | * 這項原則設定決定預設網路介面是否接受來源路由封包 * 來源路由(Source routing)可以用來指定一條從來源位址到目之位址之間之資料傳送路徑，阻擋來源路由封包，以防止封包偽裝(Packet Spoofing)攻擊 * 可設定之參數如下：  1. 0：表示阻擋來源路由封包 2. 1：表示接受來源路由封包 | * 編輯/etc/sysctl.conf檔案或/etc/sysctl.d/目錄下之檔案，新增或修改參數如下：   net.ipv4.conf.default.accept\_source\_route = 0  net.ipv6.conf.default.accept\_source\_route = 0   * 開啟終端機，執行以下指令設定核心參數：   #sysctl -w net.ipv4.conf.default.accept\_source\_route=0  #sysctl -w net.ipv6.conf.default.accept\_source\_route=0   * 開啟終端機，執行以下指令使變動立即生效：   #sysctl -w net.ipv4.route.flush=1  #sysctl -w net.ipv6.route.flush=1 | 0 |
| 102 | TWGCB-01-013-0102 | 網路設定 | 所有網路介面阻擋ICMP重新導向封包 | * 這項原則設定決定所有網路介面是否接受ICMP重新導向封包 * ICMP重新導向封包是路由器用來通知主機更改路由表之工具，因此，攻擊者可透過此功能修改主機之路由表 * 可設定之參數如下：  1. 0：表示阻擋ICMP重新導向封包 2. 1：表示接受ICMP重新導向封包 | * 編輯/etc/sysctl.conf檔案或/etc/sysctl.d/目錄下之檔案，新增或修改參數如下：   net.ipv4.conf.all.accept\_redirects = 0  net.ipv6.conf.all.accept\_redirects = 0   * 開啟終端機，執行以下指令設定核心參數：   #sysctl -w net.ipv4.conf.all.accept\_redirects=0  #sysctl -w net.ipv6.conf.all.accept\_redirects=0   * 開啟終端機，執行以下指令使變動立即生效：   #sysctl -w net.ipv4.route.flush=1  #sysctl -w net.ipv6.route.flush=1 | 0 |
| 103 | TWGCB-01-013-0103 | 網路設定 | 預設網路介面阻擋ICMP重新導向封包 | * 這項原則設定決定預設網路介面是否接受ICMP重新導向封包 * ICMP重新導向封包是路由器用來通知主機更改路由表之工具，因此，攻擊者可透過此功能修改主機之路由表 * 可設定之參數如下：  1. 0：表示阻擋ICMP重新導向封包 2. 1：表示接受ICMP重新導向封包 | * 編輯/etc/sysctl.conf檔案或/etc/sysctl.d/目錄下之檔案，新增或修改參數如下：   net.ipv4.conf.default.accept\_redirects = 0  net.ipv6.conf.default.accept\_redirects = 0   * 開啟終端機，執行以下指令設定核心參數：   #sysctl -w net.ipv4.conf.default.accept\_redirects=0  #sysctl -w net.ipv6.conf.default.accept\_redirects=0   * 開啟終端機，執行以下指令使變動立即生效：   #sysctl -w net.ipv4.route.flush=1  #sysctl -w net.ipv6.route.flush=1 | 0 |
| 104 | TWGCB-01-013-0104 | 網路設定 | 所有網路介面阻擋安全之ICMP重新導向封包 | * 這項原則設定決定所有網路介面是否接受安全之ICMP重新導向封包 * 安全ICMP重新導向僅接受已被列入受信任列表之閘道器所傳送之封包，但若在受信任列表中之閘道器被入侵變成惡意閘道器，將可能影響系統安全性 * 可設定之參數如下：  1. 0：表示阻擋安全之ICMP重新導向封包 2. 1：表示接受安全之ICMP重新導向封包 | * 編輯/etc/sysctl.conf檔案或/etc/sysctl.d/目錄下檔案，新增或修改參數如下：   net.ipv4.conf.all.secure\_redirects = 0   * 開啟終端機，執行以下指令設定核心參數：   #sysctl -w net.ipv4.conf.all.secure\_redirects=0   * 開啟終端機，執行以下指令使變動立即生效：   #sysctl -w net.ipv4.route.flush=1 | 0 |
| 105 | TWGCB-01-013-0105 | 網路設定 | 預設網路介面阻擋安全之ICMP重新導向封包 | * 這項原則設定決定預設網路介面是否接受安全之ICMP重新導向封包 * 安全ICMP重新導向僅接受已被列入受信任列表之閘道器所傳送之封包，但若在受信任列表中之閘道器被入侵變成惡意閘道器，將可能影響系統安全性 * 可設定之參數如下：  1. 0：表示阻擋安全之ICMP重新導向封包 2. 1：表示接受安全之ICMP重新導向封包 | * 編輯/etc/sysctl.conf檔案或/etc/sysctl.d/目錄下檔案，新增或修改參數如下：   net.ipv4.conf.default.secure\_redirects = 0   * 開啟終端機，執行以下指令設定核心參數：   #sysctl -w net.ipv4.conf.default.secure\_redirects=0   * 開啟終端機，執行以下指令使變動立即生效：   #sysctl -w net.ipv4.route.flush=1 | 0 |
| 106 | TWGCB-01-013-0106 | 網路設定 | 所有網路介面記錄可疑封包 | * 這項原則設定決定所有網路介面是否記錄如偽造封包、來源路由封包或重新導向等可疑封包，以協助系統管理者早期發現系統遭受攻擊跡象 * 可設定之參數如下：  1. 0：表示停用記錄可疑封包功能 2. 1：表示啟用記錄可疑封包功能 | * 編輯/etc/sysctl.conf檔案或/etc/sysctl.d/目錄下檔案，新增或修改參數如下：   net.ipv4.conf.all.log\_martians = 1   * 開啟終端機，執行以下指令設定核心參數：   #sysctl -w net.ipv4.conf.all.log\_martians=1   * 開啟終端機，執行以下指令使變動立即生效：   #sysctl -w net.ipv4.route.flush=1 | 1 |
| 107 | TWGCB-01-013-0107 | 網路設定 | 預設網路介面記錄可疑封包 | * 這項原則設定決定預設網路介面是否記錄如偽造封包、來源路由封包或重新導向等可疑封包，以協助系統管理者早期發現系統遭受攻擊跡象 * 可設定之參數如下：  1. 0：表示停用記錄可疑封包功能 2. 1：表示啟用記錄可疑封包功能 | * 編輯/etc/sysctl.conf檔案或/etc/sysctl.d/目錄下檔案，新增或修改參數如下：   net.ipv4.conf.default.log\_martians = 1   * 開啟終端機，執行以下指令設定核心參數：   #sysctl -w net.ipv4.conf.default.log\_martians=1   * 開啟終端機，執行以下指令使變動立即生效：   #sysctl -w net.ipv4.route.flush=1 | 1 |
| 108 | TWGCB-01-013-0108 | 網路設定 | 不回應ICMP廣播要求 | * 這項原則設定決定是否不回應ICMP廣播要求，以防遭受ICMP攻擊 * 當主機接收到ICMP echo-request封包時，若願意回應，則會送出echo-reply封包，攻擊者可利用此特性於ICMP封包假造來源為受害主機IP，並使用廣播傳送至網域，當網域內主機收到惡意之ICMP廣播封包後，送出echo-reply封包至受害主機，將導致受害主機可能無法提供服務 * 可設定之參數如下：  1. 0：表示回應ICMP廣播要求 2. 1：表示不回應ICMP廣播要求 | 開啟終端機，執行以下指令，將net.ipv4.icmp\_echo\_ignore\_broadcasts設為1，以不回應ICMP廣播要求，並使變動立即生效：  #grep -Els "^\s\*net\.ipv4\.icmp\_echo\_ignore\_broadcasts\s\*=\s\*0" /etc/sysctl.conf /etc/sysctl.d/\*.conf /usr/lib/sysctl.d/\*.conf /run/sysctl.d/\*.conf | while read filename; do sed -ri "s/^\s\*(net\.ipv4\.icmp\_echo\_ignore\_broadcasts\s\*)(=)(\s\*\S+\b).\*$/# \*REMOVED\* \1/" $filename; done; sysctl -w net.ipv4.icmp\_echo\_ignore\_broadcasts=1; sysctl -w net.ipv4.route.flush=1 | 1 |
| 109 | TWGCB-01-013-0109 | 網路設定 | 忽略偽造之ICMP錯誤訊息 | * 這項原則設定決定是否忽略偽造之ICMP錯誤訊息，以避免系統遭受ICMP攻擊 * 惡意者在ICMP封包使用假來源位置，並使用廣播送出給網域內所有主機。當網域內主機沒有將此ICMP封包過濾，網域內主機將會傳送ICMP回應封包到受害主機，導致受害主機服務受到影響 * 可設定之參數如下：  1. 0：表示回應偽造之ICMP錯誤訊息 2. 1：表示忽略偽造之ICMP錯誤訊息 | 開啟終端機，執行以下指令，將net.ipv4.icmp\_ignore\_bogus\_error\_responses設為1，以忽略偽造之ICMP錯誤訊息，並使變動立即生效：  #grep -Els "^\s\*net\.ipv4\.icmp\_ignore\_bogus\_error\_responses\s\*=\s\*0" /etc/sysctl.conf /etc/sysctl.d/\*.conf /usr/lib/sysctl.d/\*.conf /run/sysctl.d/\*.conf | while read filename; do sed -ri "s/^\s\*(net\.ipv4\.icmp\_ignore\_bogus\_error\_responses\s\*)(=)(\s\*\S+\b).\*$/# \*REMOVED\* \1/" $filename; done; sysctl -w net.ipv4.icmp\_ignore\_bogus\_error\_responses=1; sysctl -w net.ipv4.route.flush=1 | 1 |
| 110 | TWGCB-01-013-0110 | 網路設定 | 所有網路介面啟用逆向路徑過濾功能 | * 這項原則設定決定所有網路介面是否啟用逆向路徑過濾(Reverse path filtering)功能 * 逆向路徑過濾功能可針對所收到之封包，利用逆向路徑確認來源IP與所進入之網路介面設定是否相符，以判斷是否為合法封包，若不是合法封包將自動丟棄，以防止IP偽造(IP spoofing)攻擊 * 可設定之參數如下：  1. 0：表示停用逆向路徑過濾功能 2. 1：表示啟用逆向路徑過濾功能 | 開啟終端機，執行以下指令，將net.ipv4.conf.all.rp\_filter設為1，以啟用逆向路徑過濾功能，並使變動立即生效：  #grep -Els "^\s\*net\.ipv4\.conf\.all\.rp\_filter\s\*=\s\*0" /etc/sysctl.conf /etc/sysctl.d/\*.conf /usr/lib/sysctl.d/\*.conf /run/sysctl.d/\*.conf | while read filename; do sed -ri "s/^\s\*(net\.ipv4\.net.ipv4.conf\.all\.rp\_filter\s\*)(=)(\s\*\S+\b).\*$/# \*REMOVED\* \1/" $filename; done; sysctl -w net.ipv4.conf.all.rp\_filter=1; sysctl -w net.ipv4.route.flush=1 | 1 |
| 111 | TWGCB-01-013-0111 | 網路設定 | 預設網路介面啟用逆向路徑過濾功能 | * 這項原則設定決定預設網路介面是否啟用逆向路徑過濾(Reverse path filtering)功能 * 逆向路徑過濾功能可針對所收到之封包，利用逆向路徑確認來源IP與所進入之網路介面設定是否相符，以判斷是否為合法封包，若不是合法封包將自動丟棄，以防止IP偽造(IP spoofing)攻擊 * 可設定之參數如下：  1. 0：表示停用逆向路徑過濾功能 2. 1：表示啟用逆向路徑過濾功能 | * 編輯/etc/sysctl.conf檔案或/etc/sysctl.d/目錄下檔案，新增或修改參數如下：   net.ipv4.conf.default.rp\_filter=1   * 開啟終端機，執行以下指令設定核心參數：   #sysctl -w net.ipv4.conf.default.rp\_filter=1   * 開啟終端機，執行以下指令使變動立即生效：   #sysctl -w net.ipv4.route.flush=1 | 1 |
| 112 | TWGCB-01-013-0112 | 網路設定 | TCP SYN cookies | * 這項原則設定決定是否啟用TCP SYN cookies功能 * 啟用SYN Cookie 時，主機於發送SYN/ACK確認封包前，會要求Client端在短時間內回覆一個序號，此序號包含IP、port 等許多原本SYN封包內之資訊。若Client端可以回覆正確之序號，主機確定該封包可信任，則會發送SYN/ACK封包，否則不理會此一封包。透過此機制可避免SYN flood攻擊 * 可設定之參數如下：  1. 0：表示停用TCP SYN cookies功能 2. 1：表示啟用TCP SYN cookies功能 | 開啟終端機，執行以下指令，將net.ipv4.tcp\_syncookies設為1，以啟用TCP SYN cookies功能，並使變動立即生效：  #grep -Els "^\s\*net\.ipv4\.tcp\_syncookies\s\*=\s\*[02]\*" /etc/sysctl.conf /etc/sysctl.d/\*.conf /usr/lib/sysctl.d/\*.conf /run/sysctl.d/\*.conf | while read filename; do sed -ri "s/^\s\*(net\.ipv4\.tcp\_syncookies\s\*)(=)(\s\*\S+\b).\*$/# \*REMOVED\* \1/" $filename; done; sysctl -w net.ipv4.tcp\_syncookies=1; sysctl -w net.ipv4.route.flush=1 | 1 |
| 113 | TWGCB-01-013-0113 | 網路設定 | 所有網路介面阻擋IPv6路由器公告訊息 | * 這項原則設定決定所有網路介面是否接受IPv6路由器公告訊息 * IPv6路由器會定期在網路上傳送路由器公告訊息(Router Advertisement，RA)封包，RA封包透過ICMPv6進行傳送，系統接收到IPv6路由器發出之RA封包，即可得到IPv6位址 * 接受IPv6路由器公告訊息，可能被誘騙將流量路由到已受害之電腦 * 可設定之參數如下：  1. 0：表示阻擋IPv6路由器公告訊息 2. 1：表示接受IPv6路由器公告訊息 | * 編輯/etc/sysctl.conf檔案或/etc/sysctl.d/目錄下檔案，新增或修改參數如下：   net.ipv6.conf.all.accept\_ra = 0   * 開啟終端機，執行以下指令設定核心參數：   #sysctl -w net.ipv6.conf.all.accept\_ra=0   * 開啟終端機，執行以下指令使變動立即生效：   #sysctl -w net.ipv6.route.flush=1 | 0 |
| 114 | TWGCB-01-013-0114 | 網路設定 | 預設網路介面阻擋IPv6路由器公告訊息 | * 這項原則設定決定預設網路介面是否接受IPv6路由器公告訊息 * IPv6路由器會定期在網路上傳送路由器公告訊息(Router Advertisement，RA)封包，RA封包透過ICMPv6進行傳送，系統接收到IPv6路由器發出之RA封包，即可得到IPv6位址 * 接受IPv6路由器公告訊息，可能被誘騙將流量路由到已受害之電腦 * 可設定之參數如下：  1. 0：表示阻擋IPv6路由器公告訊息 2. 1：表示接受IPv6路由器公告訊息 | * 編輯/etc/sysctl.conf檔案或/etc/sysctl.d/目錄下檔案，新增或修改參數如下：   net.ipv6.conf.default.accept\_ra = 0   * 開啟終端機，執行以下指令設定核心參數：   #sysctl -w net.ipv6.conf.default.accept\_ra=0   * 開啟終端機，執行以下指令使變動立即生效：   #sysctl -w net.ipv6.route.flush=1 | 0 |
| 115 | TWGCB-01-013-0115 | 網路設定 | DCCP協定 | * 這項原則設定決定是否啟用DCCP協定 * DCCP協定(Datagram Congestion Control Protocol，封包壅塞控制協定)是一個擁有壅塞控制機制之非可靠式傳輸層網路通訊協定，其特性適合用於多媒體資料串流 * 停用DCCP協定可降低系統被攻擊面 | * 開啟終端機，執行vim指令，在/etc/modprobe.d目錄，新增或編輯「dccp.conf」檔案，範例如下：   #vim /etc/modprobe.d/dccp.conf  並在檔案中加入以下內容：  install dccp /bin/true  blacklist dccp   * 完成後，請重新開機 | 停用 |
| 116 | TWGCB-01-013-0116 | 網路設定 | SCTP協定 | * 這項原則設定決定是否啟用SCTP協定 * SCTP協定(Stream Control Transmission Protocol，資料流控制傳輸協定)屬於傳輸層通訊協定，支援訊息導向通訊，並結合了TCP與UDP之特點，提高資料傳輸可靠性與效率 * 停用此協定可降低系統被攻擊面 | * 開啟終端機，執行vim指令，在/etc/modprobe.d目錄，新增或編輯「sctp.conf」檔案，範例如下：   #vim /etc/modprobe.d/sctp.conf  並在檔案中加入以下內容：  install sctp /bin/true  blacklist sctp   * 完成後，請重新開機 | 停用 |
| 117 | TWGCB-01-013-0117 | 網路設定 | RDS協定 | * 這項原則設定決定是否啟用RDS協定 * RDS(Reliable Datagram Sockets)協定是由甲骨文(Oracle)發展之協定，提供節點與叢集間可靠之高效能與低延遲通訊，應用在VoIP網路電話 * 停用此協定可降低系統被攻擊面 | * 開啟終端機，執行vim指令，在/etc/modprobe.d目錄，新增或編輯「rds.conf」檔案，範例如下：   #vim /etc/modprobe.d/rds.conf  並在檔案中加入以下內容：  install rds /bin/true  blacklist rds   * 完成後，請重新開機 | 停用 |
| 118 | TWGCB-01-013-0118 | 網路設定 | TIPC協定 | * 這項原則設定決定是否啟用TIPC協定 * TIPC(Transparent Inter-Process Communication，透通處理程序間通訊)協定提供一個有效率之叢集式通訊協定，提高系統效能、可用性及擴展性 * 停用此協定可降低系統被攻擊面 | * 開啟終端機，執行vim指令，在/etc/modprobe.d目錄，新增或編輯「tipc.conf」檔案，範例如下：   #vim /etc/modprobe.d/tipc.conf  並在檔案中加入以下內容：  install tipc /bin/true  blacklist tipc   * 完成後，請重新開機 | 停用 |
| 119 | TWGCB-01-013-0119 | 網路設定 | 網路介面混雜模式 | * 這項原則設定決定是否啟用網路介面混雜模式 * 網路介面若處於混雜模式(promiscuous mode)，即可接收所有經過該網路介面之網路封包 * 停用網路介面混雜模式，以避免被攻擊者用於蒐集網路流量數據資料，其中可能包含登入帳號、通行碼及金鑰等機敏資訊 | * 開啟終端機，執行以下指令，檢查網路介面是否處於混雜模式：   #ip link | grep -i promisc   * 若發現網路介面處於混雜模式，則執行以下指令，關閉網路介面混雜模式：   #ip link set dev (網路介面裝置名稱) multicast off promisc off | 停用 |
| 120 | TWGCB-01-013-0120 | 日誌與稽核 | auditd套件 | * 這項原則設定決定是否安裝auditd套件 * auditd為Linux系統使用之稽核工具套件，負責將稽核紀錄寫入磁碟予以保存 * 運用稽核工具記錄系統事件，可供系統管理者判斷系統是否發生未經授權存取等異常行為 | 開啟終端機，執行以下指令安裝auditd套件  #dnf install audit audit-libs | 安裝 |
| 121 | TWGCB-01-013-0121 | 日誌與稽核 | auditd服務 | * 這項原則設定決定是否使用auditd服務 * 啟用auditd服務記錄系統事件，可供系統管理者判斷系統是否發生未經授權存取等異常行為 | 開啟終端機，執行以下指令啟用auditd服務：  #systemctl --now enable auditd | 啟用 |
| 122 | TWGCB-01-013-0122 | 日誌與稽核 | 稽核auditd服務啟動前之程序 | * 這項原則設定決定是否針對auditd服務啟動前之程序(Process)進行稽核 * 記錄auditd服務啟動前之程序(Process)所產生之事件，有助於發現潛在惡意行為 | * 編輯/etc/default/grub檔案，在GRUB\_CMDLINE\_LINUX參數設定加入「audit=1」，範例如下：   GRUB\_CMDLINE\_LINUX="audit=1"   * 開啟終端機，執行以下指令更新grub2設定檔：   #grub2-mkconfig -o /boot/grub2/grub.cfg | 啟用 |
| 123 | TWGCB-01-013-0123 | 日誌與稽核 | 稽核待辦事項數量限制 | * 這項原則設定決定是否設定稽核待辦事項數量限制 * 稽核待辦事項數量限制(audit\_backlog\_limit)為設定開機過程中所建立稽核紀錄之保留數量限制，預設值為64 * 設定audit\_backlog\_limit為8,192以上，以完整保留開機過程中所建立稽核紀錄，避免因稽核紀錄遺失導致無法發現潛在惡意行為 | * 編輯/etc/default/grub檔案，在GRUB\_CMDLINE\_LINUX參數設定加入「audit\_backlog\_limit=(BACKLOG SIZE)」，將BACKLOG SIZE設定為8,192以上，範例如下：   GRUB\_CMDLINE\_LINUX="audit\_backlog\_limit=8192"   * 開啟終端機，執行以下指令更新grub2設定檔：   #grub2-mkconfig -o /boot/grub2/grub.cfg | 8,192以上 |
| 124 | TWGCB-01-013-0124 | 日誌與稽核 | 稽核處理失敗時通知系統管理者 | * 這項原則設定決定稽核處理失敗時是否通知系統管理者 * 對於系統管理者而言，了解系統是否依設定處理稽核日誌至關重要，稽核處理失敗原因包含軟體或硬體出錯，以及稽核日誌儲存磁碟空間異常等情況 * 啟用此通知讓系統管理者得知系統稽核功能異常並儘速處理，避免因稽核功能異常導致無法發現潛在惡意行為 | 編輯/etc/aliases檔案，新增或修改成以下內容，設定在稽核失敗時通知系統管理者：  postmaster: root | 啟用 |
| 125 | TWGCB-01-013-0125 | 日誌與稽核 | 稽核日誌檔案所有權 | * 這項原則設定決定是否設定稽核日誌檔案之所有權 * 稽核日誌檔案包含系統之稽核紀錄、稽核設定及稽核結果等資訊 * 設定稽核日誌檔案所有權，避免因未經授權存取而洩露稽核記錄，讓攻擊者取得系統與組態設定等機敏資訊 | * 開啟終端機，執行以下指令，尋找稽核日誌檔案：   #grep -iw log\_file /etc/audit/auditd.conf   * 執行以下指令，設定稽核日誌檔案擁有者與群組：   #chown root:root (稽核日誌檔案名稱)   * 設定稽核日誌檔案「/var/log/audit/audit.log」之指令範例如下：   #chown root:root /var/log/audit/audit.log | root:root |
| 126 | TWGCB-01-013-0126 | 日誌與稽核 | 稽核日誌檔案權限 | * 這項原則設定決定是否設定稽核日誌檔案之權限 * 稽核日誌檔案包含系統之稽核紀錄、稽核設定及稽核結果等資訊 * 設定稽核日誌檔案權限，避免因未經授權存取而洩露稽核記錄，讓攻擊者取得系統與組態設定等機敏資訊 | * 開啟終端機，執行以下指令，尋找稽核日誌檔案： * #grep -iw log\_file /etc/audit/auditd.conf * 執行以下指令，設定稽核日誌檔案權限為600或更低權限： * #chmod 600 (稽核日誌檔案名稱) * 設定稽核日誌檔案「/var/log/audit/audit.log」之指令範例如下： * #chmod 600 /var/log/audit/audit.log | 600或更低權限 |
| 127 | TWGCB-01-013-0127 | 日誌與稽核 | 稽核日誌目錄所有權 | * 這項原則設定決定是否設定稽核日誌目錄所有權 * 稽核日誌目錄存有稽核日誌檔案，該檔案包含系統之稽核紀錄、稽核設定及稽核結果等資訊 * 設定稽核日誌目錄所有權，避免因未經授權存取而洩露稽核紀錄，遭攻擊者取得系統與組態設定等機敏資訊 | * 開啟終端機，執行以下指令，尋找稽核日誌目錄：   #grep -iw log\_file /etc/audit/auditd.conf   * 執行以下指令，設定稽核日誌目錄擁有者與群組：   #chown root:root (稽核日誌目錄名稱)   * 設定稽核日誌目錄「/var/log/audit」之指令範例如下：   #chown root:root /var/log/audit | root:root |
| 128 | TWGCB-01-013-0128 | 日誌與稽核 | 稽核日誌目錄權限 | * 這項原則設定決定是否設定稽核日誌目錄之權限 * 稽核日誌目錄存有稽核日誌檔案，該檔案包含系統之稽核紀錄、稽核設定及稽核結果等資訊 * 設定稽核日誌目錄權限，避免因未經授權存取而洩露稽核紀錄，遭攻擊者取得系統與組態設定等機敏資訊 | * 開啟終端機，執行以下指令，尋找稽核日誌目錄：   #grep -iw log\_file /etc/audit/auditd.conf   * 執行以下指令，設定稽核日誌目錄權限為700或更低權限：   #chmod 700 (稽核日誌目錄名稱)   * 設定稽核日誌目錄「/var/log/audit」之指令範例如下：   #chmod 700 /var/log/audit | 700或更低權限 |
| 129 | TWGCB-01-013-0129 | 日誌與稽核 | 稽核規則檔案權限 | * 這項原則設定決定是否設定稽核規則檔案權限 * 系統管理者應設定要稽核之事件，因錯誤之稽核設定會導致稽核系統負擔過重，進而降低系統效能，並使負責調查與分析資安事件之人員作業更加困難 * 設定稽核規則檔案權限，避免未經授權人員修改稽核規則，導致遺失重要稽核紀錄 | 開啟終端機，執行以下指令，設定/etc/audit/rules.d/audit.rules檔案權限為600或更低權限：  #chmod 600 /etc/audit/rules.d/audit.rules | 600或更低權限 |
| 130 | TWGCB-01-013-0130 | 日誌與稽核 | 稽核設定檔案權限 | * 這項原則設定決定是否設定稽核設定檔案權限 * 系統管理者應設定要稽核之事件，因錯誤之稽核設定會導致稽核系統負擔過重，進而降低系統效能，並使負責調查與分析資安事件之人員作業更加困難 * 設定稽核設定檔案權限，避免未經授權人員修改稽核設定，導致遺失重要稽核紀錄 | 開啟終端機，執行以下指令，設定/etc/audit/auditd.conf檔案權限為640或更低權限：  #chmod 640 /etc/audit/auditd.conf | 640或更低權限 |
| 131 | TWGCB-01-013-0131 | 日誌與稽核 | 稽核工具權限 | * 這項原則設定決定是否設定稽核工具權限 * 稽核工具可用以查看日誌資料、操作稽核系統及記錄稽核資訊，以及自訂查詢與產生報告 * 設定稽核工具權限，避免稽核紀錄遭未經授權修改 | * 開啟終端機，執行以下指令，檢查稽核工具權限：   #stat -c "%a %n" /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace /sbin/auditd /sbin/audisp-remote /sbin/audisp-syslog /sbin/augenrules   * 若有稽核工具權限高於750，則執行以下指令，設定稽核工具權限為750或更低權限：   #chmod 750 (稽核工具名稱) | 750或更低權限 |
| 132 | TWGCB-01-013-0132 | 日誌與稽核 | 稽核工具所有權 | * 這項原則設定決定是否設定稽核工具所有權 * 稽核工具可用以查看日誌資料、操作稽核系統及記錄稽核資訊，以及自訂查詢與產生報告 * 設定稽核工具所有權，避免稽核紀錄遭未經授權修改 | * 開啟終端機，執行以下指令，檢查稽核工具擁有者與群組：   #ls -al /sbin/auditctl /sbin/aureport /sbin/ausearch /sbin/autrace /sbin/auditd /sbin/audisp-remote /sbin/audisp-syslog /sbin/augenrules   * 若有稽核工具擁有者與群組非root，則執行以下指令，設定稽核工具擁有者與群組為root：   #chown root:root (稽核工具名稱) | root:root |
| 133 | TWGCB-01-013-0133 | 日誌與稽核 | 保護稽核工具 | * 這項原則設定決定是否啟用稽核工具保護功能，以保護稽核工具之完整性 * 稽核工具可用以查看日誌資料、操作稽核系統及記錄稽核資訊，以及自訂查詢與產生報告 * 保護稽核工具之完整性，避免稽核工具被攻擊者替換或竄改，以降低稽核紀錄被竄改之風險 | 編輯/etc/aide.conf檔案，新增或修改為以下內容，以保護稽核工具之完整性：  #Audit Tools  /usr/sbin/auditctl p+i+n+u+g+s+b+acl+xattrs+sha512  /usr/sbin/auditd p+i+n+u+g+s+b+acl+xattrs+sha512  /usr/sbin/ausearch p+i+n+u+g+s+b+acl+xattrs+sha512  /usr/sbin/aureport p+i+n+u+g+s+b+acl+xattrs+sha512  /usr/sbin/autrace p+i+n+u+g+s+b+acl+xattrs+sha512  /usr/sbin/audisp-remote p+i+n+u+g+s+b+acl+xattrs+sha512  /usr/sbin/audisp-syslog p+i+n+u+g+s+b+acl+xattrs+sha512  /usr/sbin/augenrules p+i+n+u+g+s+b+acl+xattrs+sha512 | 啟用 |
| 134 | TWGCB-01-013-0134 | 日誌與稽核 | 稽核日誌檔案大小上限 | * 這項原則設定決定是否設定稽核日誌檔案大小上限 * max\_log\_file參數可設定稽核日誌檔案大小上限值(MB)，以避免影響系統運作與遺失稽核紀錄 | 編輯/etc/audit/auditd.conf檔案，設定以下參數，將稽核日誌檔案大小上限值設為32(MB)：  max\_log\_file = 32 | 32以上 |
| 135 | TWGCB-01-013-0135 | 日誌與稽核 | 稽核日誌達到其檔案大小上限之行為 | * 這項原則設定決定是否設定稽核日誌達到其檔案大小上限之行為 * max\_log\_file\_action參數可設定稽核日誌檔案達到檔案大小上限時，系統要如何處理稽核日誌檔案，將參數設為keep\_logs，則系統將輪替日誌，且不會刪除舊日誌 * 注意：請定期備份日誌檔案，以及清理與維護系統磁碟空間，以確保有足夠空間可保存稽核日誌檔案 | 編輯/etc/audit/auditd.conf檔案，設定參數如下：  max\_log\_file\_action = keep\_logs | keep\_logs |
| 136 | TWGCB-01-013-0136 | 日誌與稽核 | 記錄系統管理者活動 | * 這項原則設定決定是否記錄系統管理者活動 * /etc/sudoers檔案為sudo套件之預設設定檔，可設定授予使用者帳號之權限，當使用者執行sudo時，系統會自動根據/etc/sudoers檔案，判斷該使用者是否具有執行sudo之權限 * 當/etc/sudoers檔案變更或檔案屬性變更時，將記錄至稽核紀錄中，並標記為「scope」，以及早發現未經授權之行為 | * 開啟終端機，執行vim指令，在/etc/audit/rules.d/目錄，新增或編輯「audit.rules」檔案，範例如下：   #vim /etc/audit/rules.d/audit.rules   * 在檔案中加入以下內容：   -w /etc/sudoers -p wa -k scope  -w /etc/sudoers.d/ -p wa -k scope | 啟用 |
| 137 | TWGCB-01-013-0137 | 日誌與稽核 | 記錄變更登入與登出資訊事件 | * 這項原則設定決定是否記錄變更登入與登出資訊之事件 * 下列為登入與登出資訊相關檔案，若遭非預期變更代表系統可能已被入侵、入侵者想要隱藏蹤跡或入侵其他使用者帳號：  1. /var/run/faillock/：此目錄保存登入失敗紀錄 2. /var/log/lastlog：記錄使用者最近一次成功登入  * 建議系統記錄變更登入與登出資訊之事件於/var/log/audit/audit.log，並標記為「logins」，以監控登入與登出行為 | * 開啟終端機，執行vim指令，在/etc/audit/rules.d/目錄，新增或編輯「audit.rules」檔案，範例如下：   #vim /etc/audit/rules.d/audit.rules   * 在檔案中加入以下內容：   -w /var/run/faillock/ -p wa -k logins  -w /var/log/lastlog -p wa -k logins | 啟用 |
| 138 | TWGCB-01-013-0138 | 日誌與稽核 | 記錄會談啟始資訊 | * 這項原則設定決定是否記錄變更會談(Session)啟始資訊之事件 * 下列為會談啟始資訊相關檔案，包含所有使用者登入、登出、重新開機或關機等資訊  1. /var/run/utmp：記錄目前登入到系統之使用者訊息 2. /var/log/wtmp：記錄登入、登出、重新開機及關機等資訊 3. /var/log/btmp：記錄錯誤之登入嘗試  * 建議系統記錄變更所有使用者登入、登出、重新開機或關機等資訊之事件，並標記為「session」或「logins」，以監控會談啟始資訊相關檔案之變更 | * 開啟終端機，執行vim指令，在/etc/audit/rules.d/目錄，新增或編輯「audit.rules」檔案，範例如下：   #vim /etc/audit/rules.d/audit.rules   * 在檔案中加入以下內容：   -w /var/run/utmp -p wa -k session  -w /var/log/wtmp -p wa -k logins  -w /var/log/btmp -p wa -k logins | 啟用 |
| 139 | TWGCB-01-013-0139 | 日誌與稽核 | 記錄變更日期與時間事件 | * 這項原則設定決定是否記錄變更日期或時間資訊之事件 * 下列為系統日期與時間相關參數：  1. adjtimex：調整系統核心時間 2. settimeofday：以時區方式設定系統時間 3. stime：以秒為單位設定系統時間(從1970年1月1日到現在之秒數) 4. clock\_settime：設定內部時鐘與計時器  * 建議系統記錄包含adjtimex、settimeofday、stime及clock\_settime等系統呼叫(System calls)進行日期與時間變更之事件於/var/log/audit.log檔案中，並標記為「time-change」 * 非預期之系統日期與時間變更，可能為惡意活動跡象，有助於發現異常行為 | * 開啟終端機，執行vim指令，在/etc/audit/rules.d/目錄，新增或編輯「audit.rules」檔案，範例如下：   #vim /etc/audit/rules.d/audit.rules   * 在檔案中加入以下內容：   -a always,exit -F arch=b64 -S adjtimex -S settimeofday -k time-change  -a always,exit -F arch=b32 -S adjtimex -S settimeofday -S stime -k time-change  -a always,exit -F arch=b64 -S clock\_settime -k time-change  -a always,exit -F arch=b32 -S clock\_settime -k time-change  -w /etc/localtime -p wa -k time-change | 啟用 |
| 140 | TWGCB-01-013-0140 | 日誌與稽核 | 記錄變更系統強制存取控制事件 | * 這項原則設定決定是否記錄變更系統強制存取控制(Mandatory access controls)事件，包含/etc/selinux與/usr/share/selinux/目錄屬性變更，以及在目錄內新增、刪除或修改檔案之事件 * 當/etc/selinux與/usr/share/selinux/目錄屬性或檔案遭非預期變更，代表未授權使用者嘗試變更存取控制或改變安全設定，將可能導致系統被入侵，應進行記錄，並標記為「MAC-policy」 | * 開啟終端機，執行vim指令，在/etc/audit/rules.d/目錄，新增或編輯「audit.rules」檔案，範例如下：   #vim /etc/audit/rules.d/audit.rules   * 在檔案中加入以下內容：   -w /etc/selinux/ -p wa -k MAC-policy  -w /usr/share/selinux/ -p wa -k MAC-policy | 啟用 |
| 141 | TWGCB-01-013-0141 | 日誌與稽核 | 記錄變更系統網路環境事件 | * 這項原則設定決定是否記錄變更系統網路環境之事件 * 當主機名稱與網域名稱變更時，將可能破壞以這2個參數為基礎之安全設定 * /etc/hosts定義主機名稱與IP位置對應檔案，入侵者可變更此檔案將連線導至其他主機 * 入侵者可利用/etc/issue與/etc/issue.net放置錯誤訊息登入畫面，誘騙使用者提供資訊給入侵者 * /etc/sysconfig/network-scripts/目錄包含網路介面腳本與設定檔，當入侵者變更目錄內之檔案，可能導至服務中斷或系統資訊洩漏 * 當/etc/issue、/etc/issue.net、 /etc/hosts及/etc/sysconfig/network-scripts/等檔案被變更時，以及使用sethostname與setdomainname可變更名稱之系統呼叫，應進行記錄並標記為「system-locale」 | * 開啟終端機，執行vim指令，在/etc/audit/rules.d/目錄，新增或編輯「audit.rules」檔案，範例如下：   #vim /etc/audit/rules.d/audit.rules   * 在檔案中加入以下內容：   -a always,exit -F arch=b64 -S sethostname -S setdomainname -k system-locale  -a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale  -w /etc/issue -p wa -k system-locale  -w /etc/issue.net -p wa -k system-locale  -w /etc/hosts -p wa -k system-locale  -w /etc/sysconfig/network-scripts/ -p wa -k system-locale | 啟用 |
| 142 | TWGCB-01-013-0142 | 日誌與稽核 | 記錄變更自主存取控制權限事件 | * 這項原則設定決定是否記錄變更自主存取控制(Discretionary access control)權限之事件 * 記錄變更檔案權限(例如：chmod、fchmod及fchmodat)、檔案延伸屬性(例如：setxattr、lsetxattr、fsetxattr、removexattr、lremovexattr及fremovexattr)、擁有者及擁有群組(例如：chown、fchown、fchownat及lchown)之事件 * 稽核紀錄僅記錄系統使用者(auid>=1000，並忽略守護程序auid=4294967295)所產生之事件，並標記為「perm\_mod」 * 監控檔案屬性之變更，可為系統管理者提供入侵者跡象或違反原則行為 * 設定時，如系統曾變更UID\_MIN參數，請執行下列指令取得UID\_MIN數值，並將auid>=1000調整為auid>=UID\_MIN數值：   awk '/^\s\*UID\_MIN/{print $2}' /etc/login.defs | * 開啟終端機，執行vim指令，在/etc/audit/rules.d/目錄，新增或編輯「audit.rules」檔案，範例如下：   #vim /etc/audit/rules.d/audit.rules   * 在檔案中加入以下內容：   -a always,exit -F arch=b64 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm\_mod  -a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm\_mod  -a always,exit -F arch=b64 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm\_mod  -a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm\_mod  -a always,exit -F arch=b64 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm\_mod  -a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm\_mod | 啟用 |
| 143 | TWGCB-01-013-0143 | 日誌與稽核 | 記錄不成功之未經授權檔案存取 | * 這項原則設定決定是否記錄所有使用者未經授權存取檔案之行為 * 建議設定系統監控包含控制建立(creat)、開啟(open、openat)及截斷(truncate、ftruncate)等系統呼叫存取檔案之行為，並針對系統使用者(auid>=1000，並忽略守護程序auid=4294967295)，且顯示對此檔案無權限(EACCES)或系統呼叫參數錯誤(EPERM)等事件進行記錄，並標記為「access」 * 開啟、建立或截斷檔案之失敗嘗試，代表可能有使用者或程序試圖對系統進行未授權存取 * 設定時，如系統曾變更UID\_MIN參數，請執行下列指令取得UID\_MIN數值，並將auid>=1000調整為auid>=UID\_MIN數值：   awk '/^\s\*UID\_MIN/{print $2}' /etc/login.defs | * 開啟終端機，執行vim指令，在/etc/audit/rules.d/目錄，新增或編輯「audit.rules」檔案，範例如下：   #vim /etc/audit/rules.d/audit.rules   * 在檔案中加入以下內容：   -a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access  -a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access  -a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access  -a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access | 啟用 |
| 144 | TWGCB-01-013-0144 | 日誌與稽核 | 記錄變更使用者或群組資訊事件 | * 這項原則設定決定是否記錄變更使用者或群組資訊之事件 * 當/etc目錄下group、passwd、gshadow、shadow及opasswd等檔案被修改或變更檔案屬性(例如權限)時，應進行記錄並標記為「identity」 * 此類檔案遭非預期變更，代表系統可能已被入侵，或入侵者想要隱藏蹤跡，或入侵其他使用者帳號 | * 開啟終端機，執行vim指令，在/etc/audit/rules.d/目錄，新增或編輯「audit.rules」檔案，範例如下：   #vim /etc/audit/rules.d/audit.rules   * 在檔案中加入以下內容：   -w /etc/group -p wa -k identity  -w /etc/passwd -p wa -k identity  -w /etc/gshadow -p wa -k identity  -w /etc/shadow -p wa -k identity  -w /etc/security/opasswd -p wa -k identity | 啟用 |
| 145 | TWGCB-01-013-0145 | 日誌與稽核 | 記錄變更檔案系統掛載事件 | * 這項原則設定決定是否記錄檔案系統掛載之事件 * 對於非系統管理者而言，將檔案系統掛載到系統為異常行為，潛在有資料未經授權匯出至外部儲存裝置之風險 * 建議設定系統監控mount與umount系統呼叫檔案系統掛載之行為，針對系統使用者(auid>=1000，並忽略守護程序auid=4294967295)所產生之事件，並標記為「mounts」 * 設定時，如系統曾變更UID\_MIN參數，請執行下列指令取得UID\_MIN數值，並將auid>=1000調整為auid>=UID\_MIN數值：   awk '/^\s\*UID\_MIN/{print $2}' /etc/login.defs | * 開啟終端機，執行vim指令，在/etc/audit/rules.d/目錄，新增或編輯「audit.rules」檔案，範例如下：   #vim /etc/audit/rules.d/audit.rules   * 在檔案中加入以下內容：   -a always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts  -a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts | 啟用 |
| 146 | TWGCB-01-013-0146 | 日誌與稽核 | 記錄特權指令使用情形 | * 這項原則設定決定是否記錄特權指令使用情形 * 特權指令是指具有setuid或setgid特權之程式，任何人執行該程式時，會以該程式之擁有者身分執行，藉由短暫提權讓一般使用者存取未被授權之檔案。因此須監控特權指令使用狀況，以及早發現使用者非法存取未授權資源之情形 * 建議系統監控與記錄系統使用者(auid>=1000，並忽略守護程序auid=4294967295)使用特權指令所產生之事件，並標記為「privileged」 * 設定時，如系統曾變更UID\_MIN參數，請執行下列指令取得UID\_MIN數值，並將auid>=1000調整為auid>=UID\_MIN數值：   awk '/^\s\*UID\_MIN/{print $2}' /etc/login.defs | * 開啟終端機，執行以下指令，在系統上所有磁區(partition)，逐一檢查磁區所掛載之檔案目錄(如根目錄)中的特權程式，並為每個特權程序之執行，建立稽核規則：   #find (partition) -xdev \( -perm -4000 -o -perm -2000 \) -type f | awk '{print "-a always,exit -F path=" $1 " -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged" }'   * 在/etc/audit/rules.d/目錄，新增或編輯「privileged.rules」檔案，將根磁區(root partition)之特權程式稽核規則加入到該檔案，指令範例如下：   #find / -xdev \( -perm -4000 -o -perm -2000 \) -type f | awk '{print "-a always,exit -F path=" $1 " -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged" }' >> /etc/audit/rules.d/privileged.rules | 啟用 |
| 147 | TWGCB-01-013-0147 | 日誌與稽核 | 記錄檔案刪除事件 | * 這項原則設定決定是否蒐集使用者利用unlink、unlinkat、rename或renameat等系統呼叫進行刪除檔案、移除檔案屬性、更換檔名或路徑等事件   + unlink：刪除檔案   + unlinkat：刪除檔案或目錄   + rename：變更檔名   + renameat：變更檔名或路徑 * 建議系統監控並記錄系統使用者(auid>=1000，並忽略守護程序auid=4294967295)所產生之事件，並標記為「delete」 * 設定時，如系統曾變更UID\_MIN參數，請執行下列指令取得UID\_MIN數值，並將auid>=1000調整為auid>=UID\_MIN數值：   awk '/^\s\*UID\_MIN/{print $2}' /etc/login.defs | * 開啟終端機，執行vim指令，在/etc/audit/rules.d/目錄，新增或編輯「audit.rules」檔案，範例如下：   #vim /etc/audit/rules.d/audit.rules   * 在檔案中加入以下內容：   -a always,exit -F arch=b64 -S unlink -S unlinkat -S rename -S renameat -F auid>=1000 -F auid!=4294967295 -k delete  -a always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F auid>=1000 -F auid!=4294967295 -k delete | 啟用 |
| 148 | TWGCB-01-013-0148 | 日誌與稽核 | 記錄核心模組掛載與卸載事件 | * 這項原則設定決定是否記錄核心模組掛載與卸載事件 * 核心模組掛載與卸載事件包含安裝核心模組(insmod)、移除核心模組(rmmod)、控制載入與卸載核心模組(modprobe)、掛載模組(init\_module)及刪除模組( delete\_module)，以及init\_module與delete\_module系統呼叫可用於起其他程序掛載與卸載核心模組 * 建議系統監控與記錄核心模組掛載與卸載事件，並標記為「modules」 * 核心模組掛載與卸載事件紀錄反映系統有未經授權之使用者掛載與卸載核心模組，可能損害系統安全性 | * 開啟終端機，執行vim指令，在/etc/audit/rules.d/目錄，新增或編輯「audit.rules」檔案，範例如下：   #vim /etc/audit/rules.d/audit.rules   * 在檔案中加入以下內容：   -w /sbin/insmod -p x -k modules  -w /sbin/rmmod -p x -k modules  -w /sbin/modprobe -p x -k modules  -a always,exit -F arch=b64 -S init\_module -S delete\_module -k modules | 啟用 |
| 149 | TWGCB-01-013-0149 | 日誌與稽核 | 記錄系統管理者活動日誌變更 | * 這項原則設定決定是否記錄系統管理者活動日誌(sudo.log)變更之事件 * 當使用者以sudo執行特權指令，系統會自動根據/etc/sudoers檔案，判斷該使用者是否具有執行sudo之權限，並將所有管理者指令都記錄到/var/log/sudo.log * 建議系統監控與記錄/var/log/sudo.log檔案寫入狀況或屬性變更情形，並標記為「actions」 * /var/log/sudo.log檔案若遭修改，代表系統管理員已執行sudo指令，或是檔案遭未經授權竄改 * 系統管理者可將稽核事件與/var/log/sudo.log紀錄內容進行比對，以驗證是否有未經授權指令被執行 | * 開啟終端機，執行指令如下，尋找sudo日誌檔案路徑   #grep -r logfile /etc/sudoers\* | sed -e 's/.\*logfile=//;s/,? .\*//'   * 執行vim指令，在/etc/audit/rules.d/目錄，新增或編輯「actions.rules」檔案，範例如下：   #vim /etc/audit/rules.d/actions.rules   * 在檔案中加入以下內容：   -w (sudo日誌檔案路徑) -p wa -k actions   * 以系統預設路徑「/var/log/sudo.log」為例，在「actions.rules」檔案中加入以下內容：   -w /var/log/sudo.log -p wa -k actions | 啟用 |
| 150 | TWGCB-01-013-0150 | 日誌與稽核 | 記錄chcon指令使用情形 | * 這項原則設定決定是否記錄chcon指令使用情形 * chcon指令用於更改檔案之SELinux安全性本文(security context)，建立使用系統重要指令、程序或系統呼叫之稽核紀錄，可提供系統管理者用於調查與分析資安事件 * 建議系統監控與記錄系統使用者(auid>=1000，並忽略守護程序auid=4294967295)使用chcon指令所產生之事件，並標記為「perm\_chng」 * 設定時，如系統曾變更UID\_MIN參數，請執行下列指令取得UID\_MIN數值，並將auid>=1000調整為auid>=UID\_MIN數值：   awk '/^\s\*UID\_MIN/{print $2}' /etc/login.defs | * 開啟終端機，執行vim指令，在/etc/audit/rules.d/目錄，新增或編輯「audit.rules」檔案，範例如下：   #vim /etc/audit/rules.d/audit.rules   * 在檔案中加入以下內容：   -a always,exit -F path=/usr/bin/chcon -F perm=x -F auid>=1000 -F auid!=4294967295 -k perm\_chng | 啟用 |
| 151 | TWGCB-01-013-0151 | 日誌與稽核 | 記錄ssh-agent程序使用情形 | * 這項原則設定決定是否記錄ssh-agent程序使用情形 * ssh-agent程序用於保存驗證公鑰所使用之私鑰，建立使用系統重要指令、程序或系統呼叫之稽核紀錄，可提供系統管理者用於調查與分析資安事件 * 建議系統監控與記錄系統使用者(auid>=1000，並忽略守護程序auid=4294967295)使用ssh-agent程序所產生之事件，並標記為「privileged-ssh」 * 設定時，如系統曾變更UID\_MIN參數，請執行下列指令取得UID\_MIN數值，並將auid>=1000調整為auid>=UID\_MIN數值：   awk '/^\s\*UID\_MIN/{print $2}' /etc/login.defs | * 開啟終端機，執行vim指令，在/etc/audit/rules.d/目錄，新增或編輯「audit.rules」檔案，範例如下：   #vim /etc/audit/rules.d/audit.rules   * 在檔案中加入以下內容：   -a always,exit -F path=/usr/bin/ssh-agent -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-ssh | 啟用 |
| 152 | TWGCB-01-013-0152 | 日誌與稽核 | 記錄unix\_update程序使用情形 | * 這項原則設定決定是否記錄unix\_update程序使用情形 * unix\_update程序是pam\_unix模組之輔助程序，用於更新使用者通行碼，建立使用系統重要指令、程序或系統呼叫之稽核紀錄，可提供系統管理者用於調查與分析資安事件 * 建議系統監控與記錄系統使用者(auid>=1000，並忽略守護程序auid=4294967295)使用unix\_update程序所產生之事件，並標記為「privileged-unix-update」 * 設定時，如系統曾變更UID\_MIN參數，請執行下列指令取得UID\_MIN數值，並將auid>=1000調整為auid>=UID\_MIN數值：   awk '/^\s\*UID\_MIN/{print $2}' /etc/login.defs | * 開啟終端機，執行vim指令，在/etc/audit/rules.d/目錄，新增或編輯「audit.rules」檔案，範例如下：   #vim /etc/audit/rules.d/audit.rules   * 在檔案中加入以下內容：   -a always,exit -F path=/sbin/unix\_update -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-unix-update | 啟用 |
| 153 | TWGCB-01-013-0153 | 日誌與稽核 | 記錄setfacl指令使用情形 | * 這項原則設定決定是否記錄setfacl指令使用情形 * setfacl指令用於設定檔案之存取控制表(ACL)，建立使用系統重要指令、程序或系統呼叫之稽核紀錄，可提供系統管理者用於調查與分析資安事件 * 建議系統監控與記錄系統使用者(auid>=1000，並忽略守護程序auid=4294967295)使用setfacl指令所產生之事件，並標記為「perm\_chng」 * 設定時，如系統曾變更UID\_MIN參數，請執行下列指令取得UID\_MIN數值，並將auid>=1000調整為auid>=UID\_MIN數值：   awk '/^\s\*UID\_MIN/{print $2}' /etc/login.defs | * 開啟終端機，執行vim指令，在/etc/audit/rules.d/目錄，新增或編輯「audit.rules」檔案，範例如下：   #vim /etc/audit/rules.d/audit.rules   * 在檔案中加入以下內容：   -a always,exit -F path=/usr/bin/setfacl -F perm=x -F auid>=1000 -F auid!=4294967295 -k perm\_chng | 啟用 |
| 154 | TWGCB-01-013-0154 | 日誌與稽核 | 記錄finit\_module指令使用情形 | * 這項原則設定決定是否記錄finit\_module指令使用情形 * finit\_module指令用於載入核心模組，建立使用系統重要指令、程序或系統呼叫之稽核紀錄，可提供系統管理者用於調查與分析資安事件 * 建議系統監控與記錄系統使用者(auid>=1000，並忽略守護程序auid=4294967295)使用finit\_module指令所產生之事件，並標記為「module\_chng」 * 設定時，如系統曾變更UID\_MIN參數，請執行下列指令取得UID\_MIN數值，並將auid>=1000調整為auid>=UID\_MIN數值：   awk '/^\s\*UID\_MIN/{print $2}' /etc/login.defs | * 開啟終端機，執行vim指令，在/etc/audit/rules.d/目錄，新增或編輯「audit.rules」檔案，範例如下：   #vim /etc/audit/rules.d/audit.rules   * 在檔案中加入以下內容：   -a always,exit -F arch=b32 -S finit\_module -F auid>=1000 -F auid!=4294967295 -k module\_chng  -a always,exit -F arch=b64 -S finit\_module -F auid>=1000 -F auid!=4294967295 -k module\_chng | 啟用 |
| 155 | TWGCB-01-013-0155 | 日誌與稽核 | 記錄open\_by\_handle\_at系統呼叫使用情形 | * 這項原則設定決定是否記錄open\_by\_handle\_at系統呼叫使用情形 * open\_by\_handle\_at系統呼叫可透過檔案描述符(File descriptor)開啟所指定之檔案，建立使用系統重要指令、程序或系統呼叫之稽核紀錄，可提供系統管理者用於調查與分析資安事件 * 建議系統監控與記錄系統使用者(auid>=1000，並忽略守護程序auid=4294967295)使用open\_by\_handle\_at系統呼叫所產生之事件，並標記為「perm\_access」 * 設定時，如系統曾變更UID\_MIN參數，請執行下列指令取得UID\_MIN數值，並將auid>=1000調整為auid>=UID\_MIN數值：   awk '/^\s\*UID\_MIN/{print $2}' /etc/login.defs | * 開啟終端機，執行vim指令，在/etc/audit/rules.d/目錄，新增或編輯「audit.rules」檔案，範例如下：   #vim /etc/audit/rules.d/audit.rules   * 在檔案中加入以下內容：   -a always,exit -F arch=b32 -S open\_by\_handle\_at -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k perm\_access  -a always,exit -F arch=b64 -S open\_by\_handle\_at -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k perm\_access  -a always,exit -F arch=b32 -S open\_by\_handle\_at -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k perm\_access  -a always,exit -F arch=b64 -S open\_by\_handle\_at -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k perm\_access | 啟用 |
| 156 | TWGCB-01-013-0156 | 日誌與稽核 | 記錄usermod指令使用情形 | * 這項原則設定決定是否記錄usermod指令使用情形 * usermod指令可用於修改使用者帳號設定，建立使用系統重要指令、程序或系統呼叫之稽核紀錄，可提供系統管理者用於調查與分析資安事件 * 建議系統監控與記錄系統使用者(auid>=1000，並忽略守護程序auid=4294967295)使用usermod指令所產生之事件，並標記為「privileged-usermod」 * 設定時，如系統曾變更UID\_MIN參數，請執行下列指令取得UID\_MIN數值，並將auid>=1000調整為auid>=UID\_MIN數值：   awk '/^\s\*UID\_MIN/{print $2}' /etc/login.defs | * 開啟終端機，執行vim指令，在/etc/audit/rules.d/目錄，新增或編輯「audit.rules」檔案，範例如下：   #vim /etc/audit/rules.d/audit.rules   * 在檔案中加入以下內容：   -a always,exit -F path=/usr/sbin/usermod -F perm=x -F auid>=1000 -F auid!=4294967295 -k privileged-usermod | 啟用 |
| 157 | TWGCB-01-013-0157 | 日誌與稽核 | 記錄chacl指令使用情形 | * 這項原則設定決定是否記錄chacl指令使用情形 * chacl指令用於更改檔案或目錄之存取控制表(ACL)，建立使用系統重要指令、程序或系統呼叫之稽核紀錄，可提供系統管理者用於調查與分析資安事件 * 建議系統監控與記錄系統使用者(auid>=1000，並忽略守護程序auid=4294967295)使用chacl指令指令所產生之事件，並標記為「perm\_chng」 * 設定時，如系統曾變更UID\_MIN參數，請執行下列指令取得UID\_MIN數值，並將auid>=1000調整為auid>=UID\_MIN數值：   awk '/^\s\*UID\_MIN/{print $2}' /etc/login.defs | * 開啟終端機，執行vim指令，在/etc/audit/rules.d/目錄，新增或編輯「audit.rules」檔案，範例如下：   #vim /etc/audit/rules.d/audit.rules   * 在檔案中加入以下內容：   -a always,exit -F path=/usr/bin/chacl -F perm=x -F auid>=1000 -F auid!=4294967295 -k perm\_chng | 啟用 |
| 158 | TWGCB-01-013-0158 | 日誌與稽核 | 記錄kmod指令使用情形 | * 這項原則設定決定是否記錄kmod指令使用情形 * kmod指令用於控制Linux核心模組，建立使用系統重要指令、程序或系統呼叫之稽核紀錄，可提供系統管理者用於調查與分析資安事件 * 建議系統監控與記錄使用kmod指令所產生之事件，並標記為「modules」 | * 開啟終端機，執行vim指令，在/etc/audit/rules.d/目錄，新增或編輯「audit.rules」檔案，範例如下：   #vim /etc/audit/rules.d/audit.rules   * 在檔案中加入以下內容：   -w /bin/kmod -p x -k modules | 啟用 |
| 159 | TWGCB-01-013-0159 | 日誌與稽核 | 記錄Pam\_Faillock日誌檔案 | * 這項原則設定決定是否記錄Pam\_Faillock日誌檔案 * Pam\_Faillock用於指定之時間間隔內對帳號認證失敗進行計數與鎖定，並將登入嘗試失敗之資料儲存在日誌檔案，建立使用系統重要指令、程序或系統呼叫之稽核紀錄，可提供系統管理者用於調查與分析資安事件 * 建議系統監控與記錄Pam\_Faillock日誌檔案，並標記為「logins」 | * 開啟終端機，執行vim指令，在/etc/audit/rules.d/目錄，新增或編輯「audit.rules」檔案，範例如下：   #vim /etc/audit/rules.d/audit.rules   * 在檔案中加入以下內容：   -w /var/log/faillock -p wa -k logins | 啟用 |
| 160 | TWGCB-01-013-0160 | 日誌與稽核 | 記錄execve系統呼叫使用情形 | * 這項原則設定決定是否記錄execve系統呼叫使用情形 * execve系統呼叫可建立新程序取代執行中之程序並保持相同PID(Process ID)，建立使用系統重要指令、程序或系統呼叫之稽核紀錄，可提供系統管理者用於調查與分析資安事件 * 建議系統監控與記錄execve系統呼叫使用情形，以避免程序使用比使用者更高權限執行而產生安全漏洞 | * 開啟終端機，執行vim指令，在/etc/audit/rules.d/目錄，新增或編輯「audit.rules」檔案，範例如下：   #vim /etc/audit/rules.d/audit.rules   * 在檔案中加入以下內容：   -a always,exit -F arch=b32 -S execve -C uid!=euid -F key=execpriv  -a always,exit -F arch=b64 -S execve -C uid!=euid -F key=execpriv  -a always,exit -F arch=b32 -S execve -C gid!=egid -F key=execpriv  -a always,exit -F arch=b64 -S execve -C gid!=egid -F key=execpriv | 啟用 |
| 161 | TWGCB-01-013-0161 | 日誌與稽核 | auditd設定不變模式 | * 這項原則設定決定是否啟用auditd設定不變模式(Immutable mode) * 如果設為不變模式，使用者即使使用auditctl指令變更稽核規則，新稽核規則不會立即作用，必須重新開機後才能生效 * 設為不變模式後，任何稽核規則變更必須重新開機後才會生效，藉此可防止惡意使用者利用變更稽核規則來隱藏惡意活動，亦可協助系統管理者藉由觀察非預期之重新開機，研判系統是否存在惡意活動 * 可設定參數如下；  1. 設為0：停用稽核 2. 設為1：啟用稽核 3. 設為2：稽核設定不變模式 | * 在/etc/audit/rules.d/目錄，新增或編輯稽核規則中最後被執行之「.rules」檔案： * 在該檔案最後一行加入以下內容：   -e 2   * 執行以下終端機指令，若輸出結果出現「-e 2」，代表設定完成：   #grep "^\s\*[^#]" /etc/audit/rules.d/\*.rules | tail -1 | 2 |
| 162 | TWGCB-01-013-0162 | 日誌與稽核 | rsyslog套件 | * 這項原則設定決定是否安裝rsyslog套件 * rsyslog為系統公用程式，提供系統資訊記錄功能，支援本機端日誌紀錄，並以加密傳輸方式發送日誌紀錄至遠端伺服器，以及可用資料庫儲存日誌紀錄 * 安裝rsyslog套件，為系統日誌管理提供更完備之功能 | 開啟終端機，執行以下指令，安裝rsyslog套件：  #dnf install rsyslog | 安裝 |
| 163 | TWGCB-01-013-0163 | 日誌與稽核 | rsyslog服務 | * 這項原則設定決定是否啟用rsyslog服務 * rsyslog為系統公用程式，提供系統資訊記錄功能，支援本機端日誌紀錄，並以加密傳輸方式發送日誌紀錄至遠端伺服器，以及可用資料庫儲存日誌紀錄 * 啟用rsyslog服務，為系統日誌管理提供更完備之功能 | 開啟終端機，執行以下指令，啟用rsyslog服務：  #systemctl --now enable rsyslog | 啟用 |
| 164 | TWGCB-01-013-0164 | 日誌與稽核 | 設定rsyslog日誌檔案預設權限 | * 這項原則決定是否設定rsyslog日誌檔案預設權限 * rsyslog在有需求時會為系統建立新日誌檔案，「$FileCreateMode」參數用於控制新增日誌檔案之預設權限 * 為日誌檔案設定預設權限，以保護系統機敏資料 | 編輯/etc/rsyslog.conf檔案與 /etc/rsyslog.d/目錄下之「.conf」檔案，設定參數「$FileCreateMode」為0640或更低權限，範例如下：  $FileCreateMode 0640 | 0640或更低權限 |
| 165 | TWGCB-01-013-0165 | 日誌與稽核 | 設定rsyslog日誌記錄規則 | * 這項原則決定是否設定rsyslog日誌記錄規則，以記錄認證、授權及系統服務等重要系統資訊 * /etc/rsyslog.conf與/etc/rsyslog.d/\*.conf檔案可設定日誌記錄規則，以及將指定之類別資訊儲存至日誌檔案 * 啟用rsyslog保存認證、授權及系統服務日誌，以供系統管理者監控是否有未經授權存取行為 | * 編輯/etc/rsyslog.conf檔案與 /etc/rsyslog.d/目錄下之「.conf」檔案，新增或修改成以下內容：   auth.\*,authpriv.\* /var/log/secure  daemon.\* /var/log/messages   * 開啟終端機，執行以下指令重新啟動rsyslog服務：   #systemctl restart rsyslog.service | auth、authpriv及daemon |
| 166 | TWGCB-01-013-0166 | 日誌與稽核 | /var/log/messages檔案所有權 | * 這項原則設定決定是否設定/var/log/messages檔案所有權 * 當系統出現錯誤，例如系統資源耗盡與核心活動發生錯誤等事件發生，將會記錄到/var/log/messages檔案 * 設定/var/log/messages檔案所有權為系統管理者，避免因未經授權存取而洩露機敏資訊 | 開啟終端機，執行以下指令，設定/var/log/messages檔案擁有者與群組：  #chown root:root /var/log/messages | root:root |
| 167 | TWGCB-01-013-0167 | 日誌與稽核 | /var/log目錄所有權 | * 這項原則設定決定是否設定/var/log目錄所有權 * 當系統出現錯誤，例如系統資源耗盡與核心活動發生錯誤等事件發生，將會記錄到/var/log/messages檔案 * 設定/var/log目錄所有權為系統管理者，避免因未經授權存取而洩露機敏資訊 | 開啟終端機，執行以下指令，設定/var/log目錄擁有者與群組：  #chown root:root /var/log | root:root |
| 168 | TWGCB-01-013-0168 | 日誌與稽核 | 設定journald將日誌發送到rsyslog | * 這項原則設定決定是否設定journald將日誌發送到rsyslog * systemd是Linux系統設定管理程式，並提供journald做為自身之日誌系統，journald之資料可以暫存於記憶體或永久保存在伺服器上，並允許將日誌從journald匯出至rsyslog * 啟用journald將日誌發送到rsyslog，以透過rsyslog服務提供一致性之日誌保存方式 | 編輯/etc/systemd/journald.conf檔案，新增以下內容：  ForwardToSyslog=yes | yes |
| 169 | TWGCB-01-013-0169 | 日誌與稽核 | 設定journald壓縮日誌檔案 | * 這項原則設定決定是否設定journald壓縮日誌檔案 * systemd是Linux系統設定管理程式，並提供journald做為自身之日誌系統，journald之資料可以暫存於記憶體或永久保存在伺服器上，並允許將日誌從journald匯出至rsyslog * journald可壓縮過大日誌檔案，啟用此功能可避免日誌檔案占用空間與資源，導致系統異常 | 編輯/etc/systemd/journald.conf檔案，新增以下內容：  Compress=yes | yes |
| 170 | TWGCB-01-013-0170 | 日誌與稽核 | 設定journald將日誌檔案永久保存於磁碟 | * 這項原則設定決定是否設定journald將日誌檔案永久保存於磁碟 * systemd是Linux系統設定管理程式，並提供journald做為自身之日誌系統，journald之資料可以暫存於記憶體或永久保存在伺服器上，並允許將日誌從journald匯出至rsyslog * 設定將日誌檔案永久保存於磁諜中，可提供系統管理者分析資安事件發生原因 | 編輯/etc/systemd/journald.conf檔案，新增以下內容：  Storage=persistent | persistent |
| 171 | TWGCB-01-013-0171 | 日誌與稽核 | 設定/var/log目錄下所有日誌檔案權限 | * 這項原則設定決定是否設定/var/log目錄下所有日誌檔案之權限 * /var/log目錄所儲存之日誌檔案，包含系統上許多服務之日誌紀錄，為日誌檔案設定權限，以保護系統機敏資料 | 開啟終端機，執行以下指令，設定var/log目錄下所有日誌檔案之權限為g-wx,o-rwx或更低權限：  find /var/log -type f -exec chmod g-wx,o-rwx "{}" + | g-wx,o-rwx或更低權限 |
| 172 | TWGCB-01-013-0172 | SELinux | SELinux套件 | * 這項原則設定決定是否安裝SELinux(Security-Enhanced Linux，安全增強Linux)套件 * SELinux是一個Linux核心安全模組，提供強制存取控制(MAC)安全性原則，可強制Linux系統中的檔案與程序依據定義的原則限制存取行為，啟用SELinux有助於提升伺服器安全性 | 開啟終端機，執行以下指令安裝SELinux：  #dnf install libselinux | 安裝 |
| 173 | TWGCB-01-013-0173 | SELinux | 開機載入程式啟用SELinux | * 這項原則設定決定是否在開機載入程式中啟用SELinux * 在開機載入程式中啟用SELinux，確保SELinux正常運作，以提升伺服器安全性 | * 編輯/etc/default/grub檔案，檢查所有CMDLINE\_LINUX參數設定，並移除所有「selinux=0」與「enforcing=0」內容，範例如下：   GRUB\_CMDLINE\_LINUX\_DEFAULT="quiet"  GRUB\_CMDLINE\_LINUX=""   * 開啟終端機，執行以下指令更新grub2設定檔：   #grub2-mkconfig -o /boot/grub2/grub.cfg | 啟用 |
| 174 | TWGCB-01-013-0174 | SELinux | SELinux政策 | * 這項原則設定決定SELinux運作時所採用之政策 * 設定SELinux使用預設之targeted政策，針對守護程序與系統軟體加以管制 * 可設定政策如下：  1. targeted：預設使用的政策，對大部分網路服務程序進行管制 2. minimum：以targeted政策為基礎，僅對選定的網路服務程序進行管制 3. mls：多層級安全保護，對所有程序進行管制，是最嚴格的政策 | 編輯/etc/selinux/config檔案，設定SELINUXTYPE參數如下：  SELINUXTYPE=targeted | targeted或更嚴格之政策 |
| 175 | TWGCB-01-013-0175 | SELinux | SELinux啟用狀態 | * 這項原則設定決定系統開機時是否啟用SELinux，以及啟用的模式 * 模式選項如下：  1. enforcing：強制模式，依據設定來限制檔案資源存取 2. permissive：寬容模式，不限制檔案資源存取，但仍會依據設定檢查並記錄相關訊息 3. disabled：停用模式，停用SELinux  * 注意：建議先進行測試再啟用SELinux，並於啟用後確認各項系統服務可正常運作 | 編輯/etc/selinux/config檔案，設定SELINUX參數如下：  SELINUX=enforcing | enforcing |
| 176 | TWGCB-01-013-0176 | SELinux | 未受限程序 | * 這項原則設定決定是否允許存在未受限程序 * 未受限程序在SELinux的「unconfined\_service\_t」區域中執行，幾乎擁有全部的存取權限 * 若未受限程序被攻陷，SELinux將無法阻止攻擊者取得系統資源與資料 * 注意：建議先進行測試再變更程序類型，並於啟用後確認各項系統服務可正常運作 | * 開啟終端機，執行以下指令，檢查是否有未受限程序在執行：   #ps -eZf | grep unconfined\_service\_t   * 檢視上一步驟的輸出結果，若有未受限程序在執行，須執行chcon指令，將該程序設定至非「unconfined\_service\_t」之區域。以將「/usr/sbin/httpd」程序設定至「httpd\_exec\_t」區域為例，chcon指令範例如下：   #chcon -t httpd\_exec\_t /usr/sbin/httpd | 無未受限程序 |
| 177 | TWGCB-01-013-0177 | SELinux | mcstrans套件 | * 這項原則設定決定是否使用mcstrans套件 * mcstrans(Multi category security translation service)套件主要用於將SELinux的多重類別安全性(MCS)標籤轉換為人類可讀的格式 * 此套件非經常使用，移除mcstrans套件可降低系統被攻擊面 | 開啟終端機，執行以下指令移除mcstrans套件：  #dnf remove mcstrans | 移除 |
| 178 | TWGCB-01-013-0178 | cron設定 | cron守護程序 | * 這項原則設定決定是否啟用cron守護程序 * cron守護程序是Linux系統上基於時間的任務管理系統，可透過cron以排程方式於固定時間、日期及間隔執行任務 * 啟用cron守護程序，以執行包含安全監控等系統維護作業 | 開啟終端機，執行以下指令，啟用cron守護程序：  #systemctl --now enable crond | 啟用 |
| 179 | TWGCB-01-013-0179 | cron設定 | /etc/crontab檔案所有權 | * 這項原則設定決定/etc/crontab檔案擁有者與群組 * cron使用/etc/crontab檔案來控制自身的作業，檔案中包含cron所運行的系統作業資訊 * 為/etc/crontab檔案設定擁有者與群組，以保護檔案避免遭未經授權存取，進而嘗試提升權限 | 開啟終端機，執行以下指令，設定/etc/crontab檔案擁有者與群組：  #chown root:root /etc/crontab | root:root |
| 180 | TWGCB-01-013-0180 | cron設定 | /etc/crontab檔案權限 | * 這項原則設定決定是否設定/etc/crontab檔案權限 * cron使用/etc/crontab檔案來控制自身的作業，檔案中包含cron所運行的系統作業資訊 * 為/etc/crontab檔案設定權限，以保護檔案避免遭未經授權存取，進而嘗試提升權限 | 開啟終端機，執行以下指令，設定/etc/crontab權限為600或更低權限：  #chmod 600 /etc/crontab | 600或更低權限 |
| 181 | TWGCB-01-013-0181 | cron設定 | /etc/cron.hourly目錄所有權 | * 這項原則設定決定/etc/cron.hourly目錄擁有者與群組 * /etc/cron.hourly目錄包含cron每小時需要執行的作業資訊，此目錄下的檔案無法使用crontab命令進行操作，而是由系統管理者使用編輯器進行編輯 * 為/etc/cron.hourly目錄設定擁有者與群組，限制一般使用者存取權限，以避免藉此進而提升權限 | 開啟終端機，執行以下指令，設定/etc/cron.hourly目錄擁有者與群組：  #chown root:root /etc/cron.hourly | root:root |
| 182 | TWGCB-01-013-0182 | cron設定 | /etc/cron.hourly目錄權限 | * 這項原則設定決定是否設定/etc/cron.hourly目錄權限 * /etc/cron.hourly目錄包含cron每小時需要執行的作業資訊，此目錄下的檔案無法使用crontab命令進行操作，而是由系統管理者使用編輯器進行編輯 * 為/etc/cron.hourly目錄設定權限，限制一般使用者存取權限，以避免藉此進而提升權限 | 開啟終端機，執行以下指令，設定/etc/cron.hourly目錄權限為700或更低權限：  #chmod 700 /etc/cron.hourly | 700或更低權限 |
| 183 | TWGCB-01-013-0183 | cron設定 | /etc/cron.daily目錄所有權 | * 這項原則設定決定/etc/cron.daily目錄擁有者與群組 * /etc/cron.daily目錄包含cron每日需要執行的作業資訊，此目錄下的檔案無法使用crontab命令進行操作，而是由系統管理者使用編輯器進行編輯 * 為/etc/cron.daily目錄設定擁有者與群組，限制一般使用者存取權限，以避免藉此進而提升權限 | 開啟終端機，執行以下指令，設定/etc/cron.daily目錄擁有者與群組：  #chown root:root /etc/cron.daily | root:root |
| 184 | TWGCB-01-013-0184 | cron設定 | /etc/cron.daily目錄權限 | * 這項原則設定決定是否設定/etc/cron.daily目錄權限 * /etc/cron.daily目錄包含cron每日需要執行的作業資訊，此目錄下的檔案無法使用crontab命令進行操作，而是由系統管理者使用編輯器進行編輯 * 為/etc/cron.daily目錄設定權限，限制一般使用者存取權限，以避免藉此進而提升權限 | 開啟終端機，執行以下指令，設定/etc/cron.daily目錄權限為700或更低權限：  #chmod 700 /etc/cron.daily | 700或更低權限 |
| 185 | TWGCB-01-013-0185 | cron設定 | /etc/cron.weekly目錄所有權 | * 這項原則設定決定/etc/cron.weekly目錄擁有者與群組 * /etc/cron.weekly目錄包含cron每週需要執行的作業資訊，此目錄下的檔案無法使用crontab命令進行操作，而是由系統管理者使用編輯器進行編輯 * 為/etc/cron.weekly目錄設定擁有者與群組，限制一般使用者存取權限，以避免藉此進而提升權限 | 開啟終端機，執行以下指令，設定/etc/cron.weekly目錄擁有者與群組：  #chown root:root /etc/cron.weekly | root:root |
| 186 | TWGCB-01-013-0186 | cron設定 | /etc/cron.weekly目錄權限 | * 這項原則設定決定是否設定/etc/cron.weekly目錄權限 * /etc/cron.weekly目錄包含cron每週需要執行的作業資訊，此目錄下的檔案無法使用crontab命令進行操作，而是由系統管理者使用編輯器進行編輯 * 為/etc/cron.weekly目錄設定權限，限制一般使用者存取權限，以避免藉此進而提升權限 | 開啟終端機，執行以下指令，設定/etc/cron.weekly目錄權限為700或更低權限：  #chmod 700 /etc/cron.weekly | 700或更低權限 |
| 187 | TWGCB-01-013-0187 | cron設定 | /etc/cron.monthly目錄所有權 | * 這項原則設定決定/etc/cron.monthly目錄擁有者與群組 * /etc/cron.monthly目錄包含cron每月需要執行的作業資訊，此目錄下的檔案無法使用crontab命令進行操作，而是由系統管理者使用編輯器進行編輯 * 為/etc/cron.monthly目錄設定擁有者與群組，限制一般使用者存取權限，以避免藉此進而提升權限 | 開啟終端機，執行以下指令，設定/etc/cron.monthly目錄擁有者與群組：  #chown root:root /etc/cron.monthly | root:root |
| 188 | TWGCB-01-013-0188 | cron設定 | /etc/cron.monthly目錄權限 | * 這項原則設定決定是否設定/etc/cron.monthly目錄權限 * /etc/cron.monthly目錄包含cron每月需要執行的作業資訊，此目錄下的檔案無法使用crontab命令進行操作，而是由系統管理者使用編輯器進行編輯 * 為/etc/cron.monthly目錄設定權限，限制一般使用者存取權限，以避免藉此進而提升權限 | 開啟終端機，執行以下指令，設定/etc/cron.monthly權限為700或更低權限：  #chmod 700 /etc/cron.monthly | 700或更低權限 |
| 189 | TWGCB-01-013-0189 | cron設定 | /etc/cron.d目錄所有權 | * 這項原則設定決定/etc/cron.d目錄擁有者與群組 * /etc/cron.d目錄包含cron作業資訊，其執行方式與/etc/crontab中的每小時、每日、每週及每月的作業相似，主要使用於需要對執行時間做更精細控制之場合。此目錄下的檔案無法使用crontab命令進行操作，而是由系統管理者使用編輯器進行編輯 * 為/etc/cron.d目錄設定擁有者與群組，限制一般使用者存取權限，以避免藉此進而提升權限 | 開啟終端機，執行以下指令，設定/etc/cron.d目錄擁有者與群組：  #chown root:root /etc/cron.d | root:root |
| 190 | TWGCB-01-013-0190 | cron設定 | /etc/cron.d目錄權限 | * 這項原則設定決定是否設定/etc/cron.d目錄權限 * /etc/cron.d目錄包含cron作業資訊，其執行方式與/etc/crontab中的每小時、每日、每週及每月的作業相似，主要使用於需要對執行時間做更精細控制之場合。此目錄下的檔案無法使用crontab命令進行操作，而是由系統管理者使用編輯器進行編輯 * 為/etc/cron.d目錄設定權限，限制一般使用者存取權限，以避免藉此進而提升權限 | 開啟終端機，執行以下指令，設定/etc/cron.d目錄權限為700或更低權限：  #chmod 700 /etc/cron.d | 700或更低權限 |
| 191 | TWGCB-01-013-0191 | cron設定 | at.allow與cron.allow檔案所有權 | * 這項原則設定決定at.allow與cron.allow檔案所有權 * 刪除/etc/at.deny與/etc/cron.deny檔案的拒絕清單，並設定/etc/cron.allow與/etc/at.allow檔案所有權，限制僅系統管理者可授權誰可以使用at與cron建立排程工作 | 開啟終端機，執行以下指令，移除/etc/cron.deny與/etc/at.deny，並建立/etc/cron.allow與/etc/at.allow後，設定其所有權：  #rm /etc/cron.deny  #rm /etc/at.deny  #touch /etc/cron.allow  #touch /etc/at.allow  #chown root:root /etc/cron.allow  #chown root:root /etc/at.allow | root:root |
| 192 | TWGCB-01-013-0192 | cron設定 | at.allow與cron.allow檔案權限 | * 這項原則設定決定是否設定at.allow與cron.allow檔案權限 * 刪除/etc/at.deny與/etc/cron.deny檔案的拒絕清單，並設定/etc/cron.allow與/etc/at.allow檔案權限，限制僅系統管理者可授權誰可以使用at與cron建立排程工作 | 開啟終端機，執行以下指令，移除/etc/cron.deny與/etc/at.deny，並建立/etc/cron.allow與/etc/at.allow後，設定其權限為600或更低權限：  #rm /etc/cron.deny  #rm /etc/at.deny  #touch /etc/cron.allow  #touch /etc/at.allow  #chmod 600 /etc/cron.allow  #chmod 600 /etc/at.allow | 600或更低權限 |
| 193 | TWGCB-01-013-0193 | cron設定 | cron日誌記錄功能 | * 這項原則設定決定是否啟用cron日誌記錄功能 * 啟用cron日誌記錄功能時，可查看cron作業之成功或失敗執行紀錄，供系統管理者及早發現未經授權存取與惡意使用cron工具之行為 | * 開啟終端機，執行以下指令，檢查cron日誌記錄功能設定：   #grep cron /etc/rsyslog.conf /etc/rsyslog.d/\*.conf   * 若無發現cron日誌記錄功能設定，請編輯/etc/rsyslog.conf檔案或/etc/rsyslog.d/目錄下的檔案，新增或修改成以下內容，以記錄所有cron訊息：   cron.\* /var/log/cron.log | 啟用 |
| 194 | TWGCB-01-013-0194 | 帳號與存取控制 | 可設定通行碼次數 | * 這項原則設定決定重新設定通行碼時，若通行碼強度未達到系統要求，可以連續輸入通行碼之次數 * 若使用PAM模組管理通行碼，pam\_pwquality.so將會檢驗通行碼相關規則，例如通行碼長度、通行碼使用字元及通行碼複雜度等，高強度通行碼可降低系統遭攻擊者進行字典檔查詢或暴力破解等通行碼攻擊之影響 * retry=3：使用者有3次機會設定符合規定之通行碼，若超過3次無法變更成功，則會回應錯誤 | 開啟終端機，執行以下腳本，更新system-auth與password-auth檔案：  #!/bin/bash  CP=$(authselect current | awk 'NR == 1 {print $3}' | grep custom/)  for FN in system-auth password-auth; do  [[ -n $CP ]] && PTF=/etc/authselect/$CP/$FN || PTF=/etc/authselect/$FN  [[ -n $(grep -E '^\s\*password\s+requisite\s+pam\_pwquality.so\s+.\*\s+retry=\S+\s\*.\*$' $PTF) ]] && sed -ri '/pwquality/s/retry=\S+/retry=3/' $PTF || sed -ri 's/^\s\*(password\s+requisite\s+pam\_pwquality.so\s+)(.\*)$/\1\2 retry=3/' $PTF  done  authselect apply-changes | 3以下，但須大於0 |
| 195 | TWGCB-01-013-0195 | 帳號與存取控制 | 強制root通行碼須符合通行碼規則 | * 這項原則設定決定是否強制root帳號之通行碼須符合通行碼規則 * 若使用PAM模組管理通行碼，pam\_pwquality.so將會檢驗通行碼相關規則，例如通行碼長度、通行碼使用字元及通行碼複雜度等，高強度通行碼可降低系統遭攻擊者進行字典檔查詢或暴力破解等通行碼攻擊之影響 * 啟用root帳號通行碼檢查功能，以確保即使重新設定通行碼者為root帳號，亦須符合通行碼規則，以提高通行碼強度 * Enforce\_for\_root：強制root帳號之通行碼須符合通行碼規則 | 開啟終端機，執行以下腳本，更新system-auth與password-auth檔案：  #!/bin/bash  CP=$(authselect current | awk 'NR == 1 {print $3}' | grep custom/)  for FN in system-auth password-auth; do  [[ -n $CP ]] && PTF=/etc/authselect/$CP/$FN || PTF=/etc/authselect/$FN  [[ -z $(grep -E '^\s\*password\s+requisite\s+pam\_pwquality.so\s+.\*enforce\_for\_root\s\*.\*$' $PTF) ]] && sed -ri 's/^\s\*(password\s+requisite\s+pam\_pwquality.so\s+)(.\*)$/\1\2 enforce\_for\_root/' $PTF  done  authselect apply-changes | 啟用 |
| 196 | TWGCB-01-013-0196 | 帳號與存取控制 | 通行碼最小長度 | * 這項原則設定決定使用者帳號之通行碼可包含之最少字元數 * 若使用PAM模組管理通行碼，pam\_pwquality.so將會檢驗通行碼相關規則，例如通行碼長度、通行碼使用字元及通行碼複雜度等，高強度通行碼可降低系統遭攻擊者進行字典檔查詢或暴力破解等通行碼攻擊之影響 * minlen = 12：表示通行碼至少包含12個字元 | 編輯/etc/security/pwquality.conf檔案，新增或修改成以下內容：  minlen = 12 | 12個字元以上 |
| 197 | TWGCB-01-013-0197 | 帳號與存取控制 | 通行碼必須至少包含字元類別數量 | * 這項原則設定決定使用者帳號之通行碼至少包含幾種類別之字元 * 設定使用者帳號之通行碼至少包含4種類別字元(數字、大寫、小寫及特殊字元)，以提高通行碼複雜度與強度，降低系統遭攻擊者進行字典檔查詢或暴力破解等通行碼攻擊之影響 * minclass = 4：表示通行碼至少要有4種類別字元 | 編輯/etc/security/pwquality.conf檔案，新增或修改成以下內容：  minclass = 4 | 4 |
| 198 | TWGCB-01-013-0198 | 帳號與存取控制 | 通行碼必須至少包含數字個數 | * 這項原則設定決定使用者帳號之通行碼至少包含幾個數字 * 當dcredit大於或等於0時，代表通行碼每出現1個數字時，Length credit加1(最多加到與dcredit相同) * 當dcredit小於0時，代表通行碼必須至少包含之「數字」個數 * dcredit=-1：表示通行碼至少包含1個數字 | 編輯/etc/security/pwquality.conf檔案，新增或修改成以下內容：  dcredit = -1 | 1個以上 |
| 199 | TWGCB-01-013-0199 | 帳號與存取控制 | 通行碼必須至少包含大寫字母個數 | * 這項原則設定決定使用者帳號之通行碼至少包含幾個大寫字母 * 當ucredit大於或等於0時，代表通行碼每出現1個大寫字母時，Length credit加1(最多加到與ucredit相同) * 當ucredit小於0時，代表通行碼必須至少包含之「大寫字母」個數 * ucredit=-1：表示通行碼至少包含1個大寫字母 | 編輯/etc/security/pwquality.conf檔案，新增或修改成以下內容：  ucredit = -1 | 1個以上 |
| 200 | TWGCB-01-013-0200 | 帳號與存取控制 | 通行碼必須至少包含小寫字母個數 | * 這項原則設定決定使用者帳號之通行碼至少包含幾個小寫字母 * 當lcredit大於或等於0時，代表通行碼每出現1個小寫字母時，Length credit加1(最多加到與lcredit相同) * 當lcredit小於0時，代表通行碼必須至少包含之「小寫字母」個數 * lcredit=-1：表示通行碼至少包含1個小寫字母 | 編輯/etc/security/pwquality.conf檔案，新增或修改成以下內容：  lcredit = -1 | 1個以上 |
| 201 | TWGCB-01-013-0201 | 帳號與存取控制 | 通行碼必須至少包含特殊字元個數 | * 這項原則設定決定使用者帳號之通行碼至少包含幾個特殊字元 * 當ocredit大於或等於0時，代表通行碼每出現1個小寫字母時，Length credit加1(最多加到與ocredit相同) * 當ocredit小於0時，代表通行碼必須至少包含之「特殊字元」個數 * ocredit=-1：表示通行碼至少包含1個特殊字元 | 編輯/etc/security/pwquality.conf檔案，新增或修改成以下內容：  ocredit = -1 | 1個以上 |
| 202 | TWGCB-01-013-0202 | 帳號與存取控制 | 新通行碼與舊通行碼最少相異字元數 | * 這項原則設定決定使用者帳號之新通行碼內必須有幾個字元與舊通行碼不同 * 設定新通行碼與舊通行碼之相異字元數，以避免使用者長期使用相同或相似之通行碼 * difok =3：表示新通行碼必須有3個字元與舊通行碼不同 | 編輯/etc/security/pwquality.conf檔案，新增或修改成以下內容：  difok = 3 | 3以上 |
| 203 | TWGCB-01-013-0203 | 帳號與存取控制 | 同一類別字元可連續使用個數 | * 這項原則設定決定使用者帳號之通行碼最多允許同一類別字元可連續使用個數 * 若使用PAM模組管理通行碼，pam\_pwquality.so將會檢驗通行碼相關規則，例如通行碼長度、通行碼使用字元及通行碼複雜度等，高強度通行碼可降低系統遭攻擊者進行字典檔查詢或暴力破解等通行碼攻擊之影響 * maxclassrepeat = 4：表示通行碼最多允許連續4個同一類別之字元 | 編輯/etc/security/pwquality.conf檔案，新增或修改成以下內容：  maxclassrepeat = 4 | 4以下，但須大於0 |
| 204 | TWGCB-01-013-0204 | 帳號與存取控制 | 相同字元可連續使用個數 | * 這項原則設定決定使用者帳號之通行碼最多允許可連續使用幾個相同字元 * 若使用PAM模組管理通行碼，pam\_pwquality.so將會檢驗通行碼相關規則，例如通行碼長度、通行碼使用字元及通行碼複雜度等，高強度通行碼可降低系統遭攻擊者進行字典檔查詢或暴力破解等通行碼攻擊之影響 * maxrepeat = 3：表示通行碼最多允許3個連續相同字元 | 編輯/etc/security/pwquality.conf檔案，新增或修改成以下內容：  maxrepeat = 3 | 3以下，但須大於0 |
| 205 | TWGCB-01-013-0205 | 帳號與存取控制 | 必須禁止使用字典檔單字做為通行碼 | * 這項原則設定決定是否禁止使用字典檔單字做為使用者帳號之通行碼 * 若使用PAM模組管理通行碼，pam\_pwquality.so將會檢驗通行碼相關規則，例如通行碼長度、通行碼使用字元及通行碼複雜度等，高強度通行碼可降低系統遭攻擊者進行字典檔查詢或暴力破解等通行碼攻擊之影響 * dictcheck=1：表示通行碼不可為字典檔單字 | 編輯/etc/security/pwquality.conf檔案，新增或修改成以下內容：  dictcheck=1 | 1 |
| 206 | TWGCB-01-013-0206 | 帳號與存取控制 | 帳戶鎖定閾值 | * 這項原則設定決定使用者帳號被鎖定之嘗試登入失敗次數，以降低通行碼暴力攻擊之影響 * deny=5：使用者帳號被鎖定嘗試登入失敗最多5次 | 編輯/etc/security/faillock.conf檔案，新增或修改成以下內容：  deny = 5 | 5次以下，但須大於0 |
| 207 | TWGCB-01-013-0207 | 帳號與存取控制 | 帳戶鎖定時間 | * 這項原則設定決定使用者帳號被鎖定後之帳號解鎖時間，以降低通行碼暴力攻擊之影響 * unlock\_time=900：決定鎖定帳號後，必須經過900秒才能解除鎖定 * 若解除鎖定之時間未到，可由系統管理者執行下列指令逕行解除鎖定：   #faillock --user (使用者帳號名稱) --reset | 編輯/etc/security/faillock.conf檔案，新增或修改成以下內容：  unlock\_time = 900 | 900秒以上 |
| 208 | TWGCB-01-013-0208 | 帳號與存取控制 | 強制執行通行碼歷程記錄 | * 這項原則設定決定記錄幾個使用者最近使用之舊通行碼，並限制新通行碼不能與此類舊通行碼重複 * 藉由限制使用者不能持續重複使用舊通行碼，令攻擊者難以猜測通行碼以提升安全性 | 開啟終端機，執行以下腳本，新增或修改設定為「remember=3」，更新system-auth檔案：  #!/bin/bash  CP=$(authselect current | awk 'NR == 1 {print $3}' | grep custom/)  [[ -n $CP ]] && PTF=/etc/authselect/$CP/system-auth || PTF=/etc/authselect/system-auth  [[ -n $(grep -E '^\s\*password\s+(sufficient\s+pam\_unix|requi(red|site)\s+pam\_pwhistory).so\s+([^#]+\s+)\*remember=\S+\s\*.\*$' $PTF) ]] && sed -ri 's/^\s\*(password\s+(requisite|sufficient)\s+(pam\_pwquality\.so|pam\_unix\.so)\s+)(.\*)(remember=\S+\s\*)(.\*)$/\1\4 remember=3 \6/' $PTF || sed -ri 's/^\s\*(password\s+(requisite|sufficient)\s+(pam\_pwquality\.so|pam\_unix\.so)\s+)(.\*)$/\1\4 remember=3/' $PTF  authselect apply-changes | 3以上 |
| 209 | TWGCB-01-013-0209 | 帳號與存取控制 | 顯示登入失敗次數與日期 | * 這項原則設定決定是否在使用者登入時顯示登入失敗次數，以及最近一次登入失敗之日期 * 顯示使用者登入失敗與日期，有助於使用者及早發現帳號遭冒用之情形 | 編輯/etc/pam.d/postlogin檔案，新增或修改以下內容至檔案最上方：  session required pam\_lastlog.so showfailed | 啟用 |
| 210 | TWGCB-01-013-0210 | 帳號與存取控制 | 通行碼雜湊演算法 | * 這項原則設定決定系統所採用之通行碼雜湊演算法 * SHA512相對於MD5提供更強之雜湊演算法，可提高攻擊者破解通行碼難度，為系統提供多一層安全防護 | * 編輯/etc/login.defs檔案，新增或修改成以下內容：   ENCRYPT\_METHOD SHA512   * 開啟終端機，執行以下腳本，新增或修改設定為「sha512」，更新system-auth與password-auth檔案：   #!/bin/bash  CP=$(authselect current | awk 'NR == 1 {print $3}' | grep custom/)  for FN in system-auth password-auth; do  [[ -n $CP ]] && PTF=/etc/authselect/$CP/$FN || PTF=/etc/authselect/$FN  [[ -z $(grep -E '^\s\*password\s+sufficient\s+pam\_unix.so\s+.\*sha512\s\*.\*$' $PTF) ]] && sed -ri 's/^\s\*(password\s+sufficient\s+pam\_unix.so\s+)(.\*)$/\1\2 sha512/' $PTF  done  authselect apply-changes | SHA512 |
| 211 | TWGCB-01-013-0211 | 帳號與存取控制 | 通行碼最短使用期限 | * 這項原則設定決定在使用者變更通行碼之前，通行碼必須使用之期限(天數)。設為0代表可隨時變更通行碼，設為-1代表停用此原則 * 設定通行碼最短使用期限為1天，以避免使用者重複使用相同通行碼 | * 編輯/etc/login.defs檔案，設定PASS\_MIN\_DAYS參數如下：   PASS\_MIN\_DAYS 1   * 針對進行上述設定前已存在之使用者帳號，須再執行下列指令，使該帳號之通行碼最短使用期限變更為1天：   #chage --mindays 1 (使用者帳號名稱) | 1天以上 |
| 212 | TWGCB-01-013-0212 | 帳號與存取控制 | 通行碼到期前提醒使用者變更通行碼 | * 這項原則設定決定在使用者通行碼即將到期時，要提前多久(天數)提醒使用者進行通行碼變更 * 設定通行碼到期前14天提醒使用者，預先提供通行碼即將到期之警告，讓使用者有時間思考安全通行碼 | * 編輯/etc/login.defs檔案，設定PASS\_WARN\_AGE參數如下：   PASS\_WARN\_AGE 14   * 針對進行上述設定前已存在之使用者帳號，須再執行下列指令，才能使通行碼到期前14天提醒使用者變更通行碼：   #chage --warndays 14 (使用者帳號名稱) | 14天以上 |
| 213 | TWGCB-01-013-0213 | 帳號與存取控制 | 通行碼最長使用期限 | * 這項原則設定決定系統要求使用者變更通行碼之前，通行碼可以使用之期限(天數)。設為-1代表停用此原則 * 設定通行碼最長使用期限為90天，提高通行碼更換頻率，提高攻擊者破解通行碼難度 | * 編輯/etc/login.defs檔案，設定PASS\_MAX\_DAYS參數如下：   PASS\_MAX\_DAYS 90   * 針對進行上述設定前已存在之使用者帳號，須再執行下列指令，才能使通行碼最長使用期限變更為90天：   #chage --maxdays 90 (使用者帳號名稱) | 90天以下，但須大於0 |
| 214 | TWGCB-01-013-0214 | 帳號與存取控制 | 通行碼到期後，帳號停用前之天數 | * 這項原則設定決定使用者帳號於通行碼到期後，若超過設定天數則停用帳號 * 設定通行碼到期後，超過30天即停用帳號，避免未使用帳號對系統構成威脅 | * 開啟終端機，執行以下指令，設定通行碼到期後之帳號停用天數：   #useradd -D -f 30   * 針對進行上述設定前已存在之使用者帳號，須再執行下列指令，才能使通行碼到期後，超過30天即停用帳號：   #chage --inactive 30 (使用者帳號名稱) | 30天以下，但須大於0 |
| 215 | TWGCB-01-013-0215 | 帳號與存取控制 | 登入嘗試失敗之延遲時間 | * 這項原則設定決定在使用者登入嘗試失敗後須延遲多久時間(秒)，才允許再次嘗試登入系統 * 設定登入嘗試失敗之延遲時間，可減緩自動猜測通行碼攻擊速度，提高通行碼猜測難度 | 編輯/etc/login.defs檔案，將FAIL\_DELAY參數值設為4以上，範例如下：  FAIL\_DELAY 4 | 4秒以上 |
| 216 | TWGCB-01-013-0216 | 帳號與存取控制 | 新使用者帳號預設建立使用者家目錄 | * 這項原則設定決定當系統新增新使用者帳號時，是否為該帳號建立使用者家目錄 * 為新增使用者帳號預設建立使用者家目錄，供使用者存放環境設定與個人檔案 | 編輯/etc/login.defs檔案，設定CREATE\_HOME參數如下：  CREATE\_HOME yes | yes |
| 217 | TWGCB-01-013-0217 | 帳號與存取控制 | 要求使用者必須經過身分鑑別才能提升權限 | * 這項原則設定決定是否要求使用者必須經過身分鑑別，才能使用sudo提升權限或更換角色 * 設定使用sudo提權時必須經過身分鑑別，以避免遭使用者存取未被授權之檔案或服務 | * 開啟終端機，執行以下指令，尋找「NOPASSWD」或「!authenticate」：   #egrep -i '(nopasswd|!authenticate)' /etc/sudoers /etc/sudoers.d/\*   * 執行「visudo -f」指令編輯/etc/sudoers檔案或 /etc/sudoers.d/目錄下檔案，針對包含「NOPASSWD」或「!authenticate」之指令行，予以註解(#)或刪除 | 要求身分鑑別 |
| 218 | TWGCB-01-013-0218 | 帳號與存取控制 | 限制每個帳號可同時登入之數量 | * 這項原則設定決定是否限制每個帳號可同時登入之數量 * 限制系統上每個帳號可同時登入之數量，有助於降低阻斷服務攻擊之風險 * 注意：這項原則設定可能會影響系統服務之同時登入上限，啟用此項設定後，請確認各項系統服務正常運作 | 編輯/etc/security/limits.conf檔案或/etc/security/limits.d/目錄下之「.conf」檔案，新增或修改成以下內容：  \* hard maxlogins 10 | 10以下，但須大於0 |
| 219 | TWGCB-01-013-0219 | 帳號與存取控制 | kbd套件 | * 這項原則設定決定是否安裝kbd套件，套件提供vlock工具可用於鎖定使用者終端機螢幕 * 安裝kbd套件後，即可使用vlock工具在終端機介面啟動螢幕鎖定機制，以防止資訊外洩或遭人惡意終止目前正在執行之作業 * 輸入啟動終端機螢幕鎖定之使用者通行碼可解除鎖定狀態 | 開啟終端機，執行以下指令，安裝kbd套件：  #dnf install kbd.x86\_64 | 安裝 |
| 220 | TWGCB-01-013-0220 | 帳號與存取控制 | 使用者會談鎖定 | * 這項原則設定決定是否設定使用者會談鎖定，以啟用螢幕保護裝置 * 設定使用者會談鎖定，提供使用者需暫時離開系統之防護措施，必須重新進行身分鑑別才能解除鎖定登入系統 | * 開啟終端機，執行以下指令，建立或編輯資料庫，設定螢幕保護裝置：   #vim /etc/dconf/db/local.d/00-screensaver   * 編輯資料庫之「org/gnome/desktop/screensaver」段落，新增或修改成以下內容：   [org/gnome/desktop/screensaver]  ##Set this to true to lock the screen when the screensaver activates  lock-enabled=true   * 執行以下指令更新系統資料庫：   #dconf update | 啟用 |
| 221 | TWGCB-01-013-0221 | 帳號與存取控制 | GNOME使用者會談逾時時間 | * 這項原則設定決定是否設定GNOME使用者會談逾時時間，超過逾時時間系統將鎖定該會談 * 設定使用者會談逾時時間，提供使用者離開系統而未登出之防護措施，必須重新進行身分鑑別才能解除鎖定登入系統 | * 開啟終端機，執行以下指令，建立或編輯資料庫，設定螢幕保護裝置：   #vim /etc/dconf/db/local.d/00-screensaver   * 編輯資料庫之「org/gnome/desktop/session」段落，新增或修改成以下內容：   [org/gnome/desktop/session]  ##Set the lock time out to 900 seconds before the session is considered idle  idle-delay=uint32 900   * 執行以下指令更新系統資料庫：   #dconf update | 900秒以下，但須大於0 |
| 222 | TWGCB-01-013-0222 | 帳號與存取控制 | 禁止GNOME使用者自動登入 | * 這項原則設定決定是否禁止GNOME使用者在圖形使用者介面下自動登入 * 禁止GNOME使用者自動登入，以避免使用者無需身分鑑別即可存取系統資料，導致資料外洩或遭竄改設定 | 編輯/etc/gdm/custom.conf檔案，在「daemon]」段落，新增或修改成以下內容：  [daemon]  AutomaticLoginEnable=false | false |
| 223 | TWGCB-01-013-0223 | 帳號與存取控制 | 系統帳號登入方式 | * 這項原則設定決定是否藉由設定nologin參數，以禁止系統帳號登入 * 系統帳號是除了root外，UID小於1000之帳號，與一般使用者無關，是為了執行相關管理功能而存在於系統中 * 針對系統帳號進行通行碼鎖定與設定無法登入之合法 shell(/sbin/nologin)，以提高攻擊者使用此類帳號進行攻擊之難度 * 系統帳號雖無法使用bash或其他shell登入系統，但仍可使用系統資源提供服務 | * 開啟終端機，執行以下指令，設定系統帳號(sync、shutdown及halt帳號除外)不可使用殼層(Shell)登入：   #awk -F: '($1!="root" && $1!="sync" && $1!="shutdown" && $1!="halt" && $1!~/^\+/ && $3<'"$(awk '/^\s\*UID\_MIN/{print $2}' /etc/login.defs)"' && $7!="'"$(which nologin)"'" && $7!="/bin/false") {print $1}' /etc/passwd | while read user; do usermod -s $(which nologin) $user; done   * 執行以下指令，鎖定所有非root之系統帳號：   #awk -F: '($1!="root" && $1!~/^\+/ && $3<'"$(awk '/^\s\*UID\_MIN/{print $2}' /etc/login.defs)"') {print $1}' /etc/passwd | xargs -I '{}' passwd -S '{}' | awk '($2!="L" && $2!="LK") {print $1}' | while read user; do usermod -L $user; done | nologin |
| 224 | TWGCB-01-013-0224 | 帳號與存取控制 | Bash shell閒置時登出時間 | * 這項原則設定決定Bash shell閒置超過多少秒後自動登出 * Bash目前是Linux之標準shell，Bash主要相容於sh，並且依據一些使用者需求而加強之shell版本 * 當shell屬於前景程序時，才能自動從shell登出，例如使用vim編輯檔案並已閒置15分鐘，自動登出將不會發生 * 設定Bash shell閒置逾時時間，可提供使用者離開系統而未鎖定螢幕之防護措施，避免其他使用者未經授權使用shell | * 編輯/etc/bashrc檔案，新增或修改參數如下：   readonly TMOUT=900 ; export TMOUT   * 編輯/etc/profile檔案或/etc/profile.d/目錄下之「.sh」檔案，新增或修改參數如下：   readonly TMOUT=900 ; export TMOUT | 900秒以下，但須大於0 |
| 225 | TWGCB-01-013-0225 | 帳號與存取控制 | 防止修改圖形使用者介面(GUI)設定 | * 這項原則設定決定是否防止修改圖形使用者介面(GUI)設定 * 使用者會談鎖定(Session Lock)機制，提供使用者需暫時離開系統之防護措施，必須重新進行身分鑑別才能解除鎖定登入系統 * 防止使用者修改GUI介面設定，避免使用者變更系統之鎖定機制以保護系統安全 | * 開啟終端機，執行以下指令，建立或編輯資料庫，設定防止修改圖形使用者介面(GUI)設定：   #vim /etc/dconf/db/local.d/locks/session   * 編輯資料庫，新增或修改成以下內容：   /org/gnome/desktop/session/idle-delay  /org/gnome/desktop/screensaver/lock-enabled  /org/gnome/desktop/screensaver/lock-delay  /org/gnome/desktop/lockdown/disable-lock-screen | 啟用 |
| 226 | TWGCB-01-013-0226 | 帳號與存取控制 | root帳號所屬群組 | * 這項原則設定決定是否檢查root帳號所屬群組 * usermod指令可用於指定root帳號所屬群組，這會影響root管理者所建立檔案之權限 * root帳號所屬群組使用GID 0，有助於防止一般使用者意外存取root帳號所擁有之檔案 | 開啟終端機，執行以下指令，設定root帳號所屬群組：  #usermod -g 0 root | GID 0 |
| 227 | TWGCB-01-013-0227 | 帳號與存取控制 | 所有使用者帳號之預設umask | * 這項原則設定決定是否在/etc/profile中設定所有使用者帳號之預設umask，用以指定新建立檔案之預設權限 * umask設為027，表示使用者所建立之檔案，其他使用者與群組無讀取、寫入及執行權限 * umask第1個位元代表擁有者，第2個位元代表群組，第3個位元代表其他使用者，設定值說明如下：  1. 0：可讀取、寫入及執行 2. 1：不可執行 3. 2：不可寫入 4. 3：不可寫入與執行 5. 4：不可讀取 6. 5：不可讀取與執行 7. 6：不可讀取與寫入 8. 7：不可讀取、寫入及執行 | 編輯/etc/profile檔案、/etc/profile.d/目錄下之「.sh」檔案及/etc/bashrc檔案，新增或修改參數如下：  umask 027 | 027或更低權限 |
| 228 | TWGCB-01-013-0228 | 帳號與存取控制 | 在/etc/login.defs設定所有使用者之預設umask | * 這項原則設定決定在/etc/login.defs設定所有使用者之預設umask，umask用以指定新建立之檔案或目錄之預設權限 * 設定umask為077表示使用者所建立之檔案與目錄，系統內之其他使用者與群組無讀、寫及執行權限 * umask第1個位元代表擁有者，第2個位元代表群組，第3個位元代表其他使用者，設定值說明如下：  1. 0：可讀、寫及執行 2. 1：不可執行 3. 2：不可寫 4. 3：不可寫與執行 5. 4：不可讀 6. 5：不可讀與執行 7. 6：不可讀與寫 8. 7：不可讀、寫及執行 | 編輯/etc/login.defs檔案，設定UMASK參數值如下：  UMASK 027 | 027或更低權限 |
| 229 | TWGCB-01-013-0229 | 帳號與存取控制 | 可使用su指令之群組 | * 這項原則設定決定是否設定wheel群組(所有系統管理者所屬群組)，並限制僅wheel群組內之使用者才能使用su指令 * su指令允許使用者以其他使用者身分執行指令或shell，預設情況下任何使用者皆可執行su指令，透過啟用/etc/pam.d/su檔案之pam\_wheel.so設定，將僅允許wheel群組中之用戶執行su指令，有利於系統管理者控管使用者提升特權行為 | * 編輯/etc/pam.d/su檔案，新增或修改成以下內容：   auth required pam\_wheel.so use\_uid   * 編輯/etc/group檔案之wheel群組設定，建立允許使用su指令之使用者帳號清單，如下所示：   wheel:x:GID:root,(使用者帳號清單)   * 範例：如欲在wheel群組(GID為10)建立允許root、user1及user2帳號使用su指令，內容如下：   wheel:x:10:root,user1,user2 | 僅限wheel群組才能使用su指令 |
| 本院整理 | | | | | | |

1. Red Hat Enterprise Linux 9 Firewalld防火牆政府組態基準列表

| 項次 | TWGCB-ID | 類別 | 原則設定名稱 | 說明 | 設定方法 | GCB 設定值 |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | TWGCB-01-013-0230 | Firewalld配置 | firewalld防火牆套件 | * 這項原則設定決定是否安裝firewalld防火牆套件 * 藉由防火牆管理與設定，以保護系統安全 | 開啟終端機，執行以下指令，安裝firewalld防火牆套件：  #dnf install firewalld | 安裝 |
| 2 | TWGCB-01-013-0231 | Firewalld配置 | firewalld服務 | * 這項原則設定決定是否啟用firewalld服務 * firewalld為一款動態防火牆管理工具，加入了區域(zone)概念，且同時支援IPv4與IPv6環境，並提供介面讓服務程序或應用程式依需求直接新增防火牆規則 * 建議啟用防火牆服務，以保護系統安全 | 開啟終端機，執行以下指令，啟用firewalld服務：  #systemctl --now enable firewalld | 啟用 |
| 3 | TWGCB-01-013-0232 | Firewalld配置 | iptables服務 | * 這項原則設定決定是否啟用iptables服務 * iptables為Linux作業系統本機端防火牆，藉由控制Linux核心之netfilter模組，進行封包過濾與處理 * 同時運行firewalld與iptables服務，可能因彼此間之規則衝突，導致系統運作異常或產生資安風險，因此在使用firewalld時，建議停用並遮蔽iptables服務 | 開啟終端機，執行以下指令，停用並遮蔽iptables服務：  #systemctl --now mask iptables | 停用 |
| 4 | TWGCB-01-013-0233 | Firewalld配置 | nftables服務 | * 這項原則設定決定是否啟用nftables服務 * nftables為iptables後繼產品，屬於Linux核心子系統，提供對網路封包(Packets)、資料包(Datagram)及訊框(Frame)進行過濾與分類功能 * 安裝firewalld套件時，具有相依性之nftables套件會一起安裝 * 同時運行firewalld與nftables服務，可能因彼此間之規則衝突，導致系統運作異常或產生資安風險，因此在使用firewalld時，建議停用並遮蔽nftables服務 | 開啟終端機，執行以下指令，停用並遮蔽nftables服務：  #systemctl --now mask nftables | 停用 |
| 5 | TWGCB-01-013-0234 | Firewalld配置 | firewalld防火牆預設區域 | * 這項原則設定決定是否設定防火牆預設區域 * 防火牆區域定義了網路連線、介面或來源位址綁定之信任等級，這是一對多關係，意謂著網路連線、介面或來源位址只是區域中的一部分，但一個區域可包含多個網路連線、介面或來源位址 * 所有未明確分配給特定區域之網路連線、介面或來源位址，都將被歸至預設區域 * 設定預設區域，可確保所有網路連線、介面或來源位址皆被納管，以保護系統安全 | * 開啟終端機，執行以下指令設定預設區域：   #firewall-cmd --set-default-zone=(區域名稱)   * 設定預設區域為public之範例如下:   #firewall-cmd --set-default-zone=public | 須設定預設區域 |
| 本院整理 | | | | | | |

1. Red Hat Enterprise Linux 9 Nftables防火牆政府組態基準列表

| 項次 | TWGCB-ID | 類別 | 原則設定名稱 | 說明 | 設定方法 | GCB 設定值 |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | TWGCB-01-013-0235 | Nftables配置 | nftables服務 | * 這項原則設定決定是否啟用nftables服務 * nftables為iptables後繼產品，屬於Linux核心子系統，提供對網路封包(Packets)、資料包(Datagram)及訊框(Frame)進行過濾與分類功能 * 建議啟用防火牆服務，以保護系統安全 | 開啟終端機，執行以下指令，啟用nftables服務：  #systemctl --now enable nftables | 啟用 |
| 2 | TWGCB-01-013-0236 | Nftables配置 | firewalld服務 | * 這項原則設定決定是否啟用firewalld服務 * firewalld(Dynamic Firewall Manager)為一款動態防火牆管理工具，加入了區域(zone)概念，且同時支援IPv4與IPv6環境，並提供介面讓服務程序或應用程式依需求直接新增防火牆規則 * 同時運行firewalld與nftables服務，可能因彼此間之規則衝突，導致系統運作異常或產生資安風險，因此在使用nftables時，建議停用並遮蔽firewalld服務 | 開啟終端機，執行以下指令，停用並遮蔽firewalld服務：  #systemctl --now mask firewalld | 停用 |
| 3 | TWGCB-01-013-0237 | Nftables配置 | 在nftables中建立表 | * 這項原則設定決定是否在nftables中建立至少1個表(Tables) * nftables預設不存在表，表為鏈(Chains)的容器，必須建立表，後續才能建立與保存鏈 * 每個表必須定義一個位址族(Address family)，位址族選項如下：  1. ip：IPv4位址族，處理IPv4封包 2. ip6：IPv6位址族，處理IPv6封包 3. inet：IPv4/IPv6位址族，可同時處理IPv4/IPv6封包 4. arp：ARP位址族，處理IPv4 ARP封包 5. bridge：Bridge位址族，處理橋接封包 6. netdev：Netdev位址族，處理入口封包 | * 開啟終端機，執行以下指令，在nftables建立表：   #nft create table inet (表名稱)   * 建立一個使用「inet」位址族且表名稱為「 filter」之範例如下：   #nft create table inet filter | 1個以上 |
| 4 | TWGCB-01-013-0238 | Nftables配置 | 在nftables建立基本鏈 | * 這項原則設定決定是否在nftables建立至少1個基本鏈(Base chains) * nftables預設不存在表，在nftables建立表後才能建立鏈，鏈為規則(Rules)的容器，必須建立鏈，後續才能建立與保存規則 * 建立輸入(input)、轉發(forward)及輸出(output)之基本鏈，以使用nftables進行網路封包過濾 | * 開啟終端機，執行以下指令，在nftables建立基本鏈：   #nft create chain inet (表名稱) (鏈名稱) { type filter hook (input|forward|output) priority 0 \; }   * 在「 filter」表中建立基本鏈之範例如下：   #nft create chain inet filter input { type filter hook input priority 0 \; }  #nft create chain inet filter forward { type filter hook forward priority 0 \; }  #nft create chain inet filter output { type filter hook output priority 0 \; } | 1個以上 |
| 5 | TWGCB-01-013-0239 | Nftables配置 | 在nftables設定回送流量規則 | * 這項原則設定決定是否在nftables設定回送流量(loopback traffic)規則 * 設定回送介面接受回送網路流量，並設定其他介面拒絕回送網路(127.0.0.0/8與::1)的流量 * 回送網路流量是同一台電腦中程序彼此之間通訊所產生之流量，對於系統的運作至關重要 * 設定僅回送介面可接受回送網路流量，且所有其他介面都應忽略回送網路流量，以協助防止偽冒攻擊 | 開啟終端機，執行以下指令，在「filter」表中設定「iif」介面之回送流量規則：  #nft add rule inet filter input iif lo accept  #nft add rule inet filter input ip saddr 127.0.0.0/8 counter drop  #nft add rule inet filter input ip6 saddr ::1 counter drop | 建立回送流量規則 |
| 6 | TWGCB-01-013-0240 | Nftables配置 | 在nftables建立預設拒絕規則 | * 這項原則設定決定是否在nftables建立預設拒絕規則 * 所建立之預設規則，會套用在已通過其他規則並到達鏈尾端之封包，該規則可設為接受(accept)或丟棄(drop) * 將預設拒絕規則設為丟棄，將到達鏈尾端之封包丟棄，以防止惡意封包通過防火牆，進而影響系統安全 | * 開啟終端機，執行以下指令，針對輸入、轉發及輸出的基本鏈，建立預設拒絕規則：   #nft chain (位址族) (表名稱) (鏈名稱) { policy drop \; }   * 在位址族「inet」與表「 filter」下，建立input、forward及output基本鏈預設拒絕規則，範例如下：   #nft chain inet filter input { policy drop \; }  #nft chain inet filter forward { policy drop \; }  #nft chain inet filter output { policy drop \; } | Drop |
| 7 | TWGCB-01-013-0241 | Nftables配置 | 載入nftables規則 | * 這項原則設定決定是否設定開機即載入nftables規則，使得系統運作期間，所設定之規則皆發揮作用，以保護系統安全 * nftables服務藉由讀取/etc/sysconfig/nftables.conf設定檔所引入之路徑，以載入nftables規則集，nftables規則集包含輸入、轉發及輸出之基本鏈，以執行網路封包過濾 | * 開啟終端機，執行vim指令，編輯/etc/sysconfig/nftables.conf檔案，範例如下：   #vim /etc/sysconfig/nftables.conf   * 將檔案中包含include參數的行內容取消註解(刪除行首的#符號)，以設定在服務啟動時載入nftables規則集，範例如下：   include "/etc/nftables/main.nft" | 開機時自動載入nftables規則集 |
| 本院整理 | | | | | | |

# 參考文獻

1. TWGCB-01-009\_Red Hat Enterprise Linux 8政府組態基準說明文件(V1.0)

<https://www.nics.nat.gov.tw/GCB>

1. Center for Internet Security, CIS Red Hat Enterprise Linux 8 Benchmark v2.0.0.

<https://www.cisecurity.org/cis-benchmarks/>

1. Center for Internet Security, CIS Red Hat Enterprise Linux 9 Benchmark v1.0.0.

<https://www.cisecurity.org/cis-benchmarks/>

1. Defense Information Systems Agency (DISA), Red Hat Enterprise Linux 8 STIG Version 1, Release 7.

<https://public.cyber.mil/stigs/downloads/>