政府組態基準(GCB)實作研習活動 (Red Hat Enterprise Linux 5)

行政院國家資通安全會報 技術服務中心

大綱

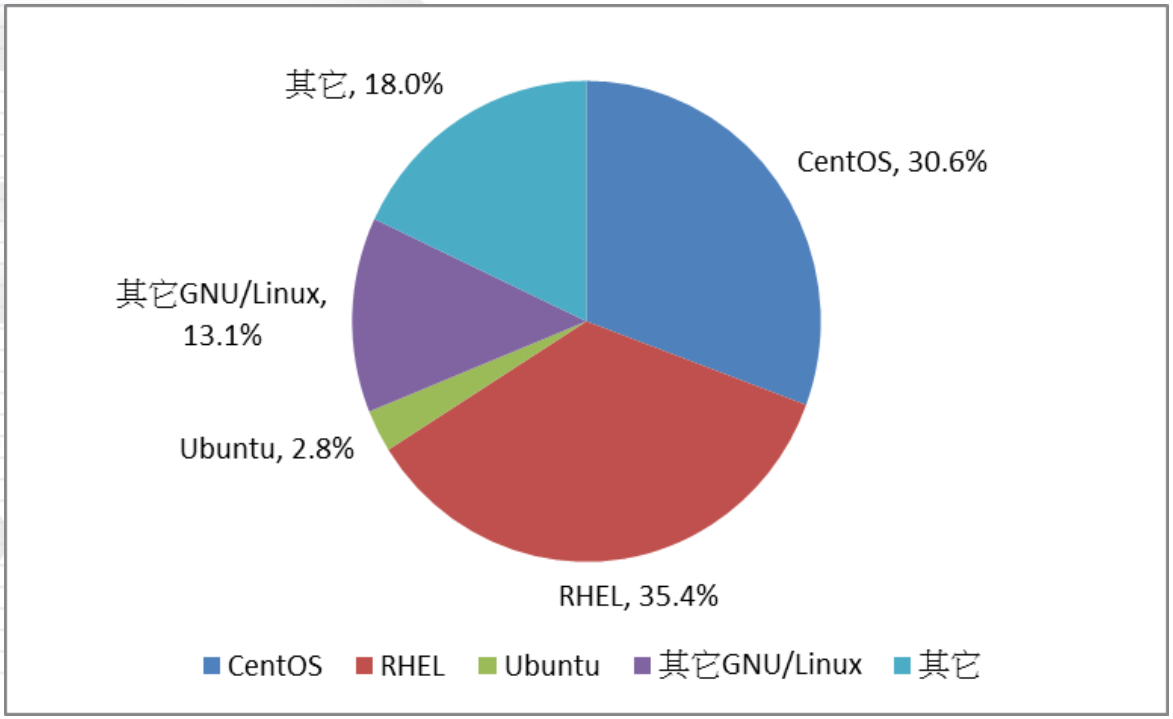
- 前言
- RHEL 5政府組態基準組態設定分類說明
- RHEL 5政府組態基準設定項目說明
- 問題與討論

前言(1/2)

- Red Hat Enterprise Linux是Red Hat公司所發行的Linux版本
- 目前最新版本
  - RHEL 5.11：發行日期 2014-09-16
  - RHEL 6.7：發行日期 2015-07-22
  - RHEL 7.1：發行日期 2015-03-05

前言(2/2)

- 根據102年技服中心調查40家政府機關所使用非Windows作業系統發現，以RHEL約佔35.4%為最多，其中又以RHEL 5佔所有RHEL版本超過50%



RHEL 5組態設定分類說明(1/2)

- 安裝與軟體維護
- 檔案權限與遮罩
- 帳號與存取控制
- SELinux
- 網路配置與防火牆
- 日誌與稽核
- 過時服務
- 基礎服務

RHEL 5組態設定分類說明(2/2)

RHEL 5系統安全性基準分類	組態設定數量
安裝與軟體維護	12
檔案權限與遮罩	46
帳號與存取控制	54
SELinux	8
網路配置與防火牆	24
日誌與稽核	18
過時服務	9
基礎服務	20
總和	191

安裝與軟體維護

RedHat GPG 金鑰(1/2)

- 建議值
  - 安裝
- 說明
  - 這項原則設定決定是否安裝Red Hat GPG金鑰
  - 所有的Red Hat Enterprise Linux套件都透過Red Hat, Inc. GPG金鑰進行簽證
  - GPG(GNU Privacy Guard或GnuPG)可用來確保套件中檔案的完整性。Red Hat利用私密金鑰對套件進行簽章，使用者則用公開金鑰以驗證套件的完整性，如果驗證不通過，即表示該套件可能已被竄改過
  - 透過此機制可確保所安裝的原廠檔案未遭竄改，以避免安裝到惡意程式

RedHat GPG 金鑰(2/2)

- 設定方式
  - 從Red Hat網頁(https://access.redhat.com/security/team/key)下載公鑰檔案，更名為「RPM-GPG-KEY-redhat-release」，並將檔案存放在/etc/pki/rpm-gpg/目錄下
  - 執行下列指令匯入GPG金鑰：
    - #rpm --import /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release

全系統套件簽章驗證

- 建議值
  - 啟用
- 說明
  - 這項原則設定決定系統是否全面啟用GPG簽章驗證功能
  - gpgcheck決定yum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，避免安裝已被篡改之檔案
- 設定方式
  - 編輯/etc/yum.conf檔案，在「main」段落新增或修改成以下內容：
    - gpgcheck=1

rhnsd服務

- 建議值
  - 停用
- 說明
  - 這項原則設定決定是否啟用rhnsd (Red Hat Network Deamon)服務
  - rhnsd服務會在背景定期檢查Red Hat是否有更新通知
  - 新的更新程式應經過測試後再部署至已上線運作之伺服器，以避免因更新問題導致系統服務異常
- 設定方式
  - 執行下列指令以停用rhnsd服務：
    - #chkconfig rhnsd off

AIDE套件

- 建議值
  - 安裝
- 說明
  - 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
- 設定方式
  - 執行下列指令以安裝AIDE套件：
    - #yum install aide

檔案權限與遮罩

非root分割區啟用nodev選項

- 建議值
  - 啟用
- 說明
  - 這項原則設定決定非root分割區是否啟用nodev選項，禁止解析系統中的裝置檔案，以防止掛載未經授權裝置，降低惡意程式感染風險
  - root分割區基本上包含/dev目錄，該目錄為已授權裝置檔案之主要存放位置，因此不能對root分割區啟用nodev選項
- 設定方式
  - 編輯/etc/fstab檔案，在掛載點不是「/」且檔案系統為ext2或ext3之列，於第4欄加入「,nodev」

可攜式儲存裝置啟用nodev, noexec及nosuid選項

- 建議值
  - 啟用
- 說明
  - 此三項原則設定決定可攜式儲存裝置是否啟用nodev、noexec及nosuid選項，以禁止掛載、執行及提權使用未經授權裝置，降低惡意程式感染風險
- 設定方式
  - 編輯/etc/fstab檔案，在掛載點為可攜式儲存裝置之列(例如：floppy, cdrom)，於第4欄加入「,nodev」、「,noexec」、「, nosuid」

/tmp目錄啟用nodev,noexec及nosuid選項

- 建議值
  - 啟用
- 說明
  - 此三項原則設定決定/tmp目錄是否啟用nodev、noexec及nosuid選項，以禁止掛載、執行及提權使用未經授權裝置，降低惡意程式感染風險
- 設定方式
  - 編輯/etc/fstab檔案，在掛載點為/tmp列，於第4欄加入「,nodev」、「,noexec」、「, nosuid」

在/dev/shm增加nodev, noexec, nosuid

- 建議值
  - 啟用
- 說明
  - 此三項原則設定決定/dev/shm目錄是否啟用nodev、noexec及nosuid選項，以禁止掛載、執行及提權使用未經授權裝置，降低惡意程式感染風險
- 設定方式
  - 編輯/etc/fstab檔案，在掛載點為/dev/shm列，於第4欄加入「,nodev」、「,noexec」、「, nosuid」

cramfs, freevxfs, hfs, hfsplus, jffs2, squashfs, udf檔案系統(1/2)

- 建議值
  - 停用
- 說明
  - 這項原則設定決定系統是否支援以下檔案系統
    - cramfs(compressed ROM file system，壓縮唯讀閃存檔案系統)
    - Vxfs(Veritas File System)檔案系統
    - hfs(Hierarchical File System，階層式檔案系統)
    - hfsplus是hfs檔案系統的改進版本
    - jffs2(Journalling Flash File System version 2)
    - squashfs是一個即時解壓縮的檔案系統
    - udf(Universal disk format，通用磁碟格式)
  - 移除不需要的檔案系統格式，以降低被攻擊面

停用掛載cramfs, freevxfs, hfs, hfsplus, jffs2, squashfs, udf檔案格式(2/2)

- 設定方式
  - 在/etc/modprobe.d目錄，新增gcb-blacklist檔案，並在檔案中加入以下內容：
    - install cramfs /bin/true
    - install freevxfs /bin/true
    - install hfs /bin/true
    - install hfsplus /bin/true
    - install jffs2 /bin/true
    - install squashfs /bin/true
    - install udf /bin/true
  - 建立完成後，請重新開機

/etc/group檔案權限、擁有者及擁有群組(1/2)

- 建議值
  - 檔案權限：644
  - 擁有者：root
  - 擁有群組：root
- 說明
  - 這項原則設定決定/etc/group檔案權限
  - /etc/group記錄每個群組的名稱、密碼、ID及屬於該群組的使用者清單

/etc/group檔案權限、擁有者及擁有群組(2/2)

- 設定方式
  - 執行下列指令，設定為僅root擁有讀寫權限，其餘所有使用者僅可讀取：
    - #chmod 644 /etc/group
  - 執行下列指令，將/etc/group擁有者與擁有群組皆設為root：
    - #chown root:root /etc/group

/etc/passwd檔案權限、擁有者及擁有群組(1/2)

- 建議值
  - 檔案權限：644
  - 擁有者：root
  - 擁有群組：root
- 說明
  - 這項原則設定決定/etc/passwd檔案權限
  - /etc/passwd記錄每位使用者的名稱、密碼、使用者ID、群組ID及家目錄等資訊

/etc/passwd檔案權限、擁有者及擁有群組(2/2)

- 設定方式
  - 執行下列指令，設定為僅root擁有讀寫權限，其餘所有使用者僅可讀取：
    - #chmod 644 /etc/passwd
  - 執行下列指令，將/etc/passwd擁有者與擁有群組皆設為root：
    - #chown root:root /etc/passwd

/etc/shadow檔案權限、擁有者及擁有群組(1/2)

- 建議值
  - 檔案權限：400
  - 擁有者：root
  - 擁有群組：root
- 說明
  - 這項原則設定決定/etc/shadow檔案權限、擁有者及擁有群組
  - /etc/shadow記錄每個使用者帳號加密過後的密碼、最後變更密碼的日期及下次可變更密碼前的經過天數等資訊

/etc/shadow檔案權限、擁有者及擁有群組(2/2)

- 設定方式
  - 執行下列指令，設定/etc/shadow僅root可讀取：
    - #chmod 400 /etc/shadow
  - 執行下列指令，將/etc/shadow擁有者與擁有群組皆設為root：
    - #chown root:root /etc/shadow

/etc/gshadow檔案權限、擁有者及擁有群組(1/2)

- 建議值
  - 檔案權限：400
  - 擁有者：root
  - 擁有群組：root
- 說明
  - 這三項原則設定決定/etc/gshadow檔案權限擁有者及擁有群組
  - /etc/gshadow記錄每個群組加密過後的密碼，以及使用者與管理者資訊，若攻擊者讀取/etc/gshadow檔案後，可嘗試透過密碼破解程式取得密碼後進行攻擊

/etc/gshadow檔案權限、擁有者及擁有群組(2/2)

- 設定方式
  - 執行下列指令，設定/etc/gshadow僅root可讀取：
    - #chmod 400 /etc/gshadow
  - 執行下列指令，將/etc/gshadow擁有者與擁有群組皆設為root：
    - #chown root:root /etc/gshadow

ExecShield(1/2)

- 建議值
  - 1
- 說明
  - 這項原則設定決定系統開機時是否立即啟用ExecShield功能
  - ExecShield是一種記憶體分區與保護技術，能大大降低緩衝區溢位攻擊的威脅。ExecShield把虛擬記憶體分成可執行與不可執行兩種區段，任何試圖在可執行區段外執行的程式(例如藉由緩衝區溢位弱點植入的惡意程式)會因為分區錯誤而自動結束，藉以降低緩衝區溢位的風險

ExecShield(2/2)

- 設定方式
  - 編輯/etc/sysctl.conf檔案，新增或修改成以下內容：
    - kernel.exec-shield = 1

記憶體位址空間配置隨機載入(1/2)

- 建議值
  - 1
- 說明
  - 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的位址，提高攻擊的難度，以降低緩衝區溢位攻擊的威脅

記憶體位址空間配置隨機載入(2/2)

- 設定方式
  - 編輯/etc/sysctl.conf檔案，新增或修改成以下內容：
    - kernel.randomize_va_space = 1

帳號與存取控制

非root系統帳號登入方式(1/2)

- 建議值
  - 停用
- 說明
  - 這項原則設定決定非root系統帳號登入方式與shell設定
  - 非root系統帳號是除了root外，UID小於500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

非root系統帳號登入方式(2/2)

- 設定方式
  - 執行下列指令，列出所有使用者、UID及shell：
    - #awk -F： '{print $1 " : " $3 " : " $7}' /etc/passwd
  - 針對UID小於500之非root系統帳號，執行下列指令進行帳號鎖定與shell設定：
    - # usermod -L (系統帳號)
    - # usermod -s /sbin/nologin (系統帳號)

使用空白密碼之帳號登入方式

- 建議值
  - 停用
- 說明
  - 此原則設定決定系統是否允許存在使用空白密碼之帳號
  - 使用空白密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
- 設定方式
  - 執行下列指令列出使用空白密碼之帳號：
    - # awk -F: '($2 == "") {print}' /etc/shadow
  - 若有使用空白密碼之帳號，則執行下列指令以設定密碼：
    - #passwd (帳號)

UID=0之帳號(1/2)

- 建議值
  - root
- 說明
  - 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

UID=0之帳號(2/2)

- 設定方式
  - 執行下列指令，列出UID=0之帳號：
  - # awk -F: '($3 == "0") {print}' /etc/passwd
  - 若存在非root帳號，可執行下列指令移除帳號或重新設定UID：
    - #userdel (帳號)
    - 或
    - #usermod -u (UID) (帳號)

密碼最短使用期限(1/2)

- 建議值
  - 1天
- 說明
  - 這項原則設定決定在使用者變更密碼之前，密碼必須使用的期限(天數)。設為0代表可隨時變更密碼，設為-1代表停用此原則
  - 設定密碼最短使用期限為1天，以避免使用者重複使用相同密碼

密碼最短使用期限(2/2)

- 設定方式
  - 編輯/etc/login.defs檔案，新增或修改成以下內容：
    - PASS_MIN_DAYS 1
  - 針對進行上述設定前就已存在之使用者帳號，須再執行下列指令，使該帳號之密碼最短使用期限變更為1天：
    - #chage –m 1 (使用者帳號)

密碼最長使用期限(1/2)

- 建議值
  - 60天
- 說明
  - 這項原則設定決定系統要求使用者變更密碼之前，密碼可以使用的期限(天數)。設為-1代表停用此原則

密碼最長使用期限(2/2)

- 設定方式
  - 編輯/etc/login.defs檔案，新增或修改成以下內容：
    - PASS_MAX_DAYS 60
  - 針對進行上述設定前就已存在之使用者帳號，須再執行下列指令，才能使密碼最長使用期限變更為60天
    - #chage –M 60 (使用者帳號)

密碼到期前提醒使用者變更密碼(1/2)

- 建議值
  - 14天
- 說明
  - 這項原則設定決定在使用者密碼即將到期時，要提前多久(天數)提醒使用者進行密碼變更。設為-1代表停用此原則

密碼到期前提醒使用者變更密碼(1/2)

- 設定方式
  - 編輯/etc/login.defs檔案，新增或修改成以下內容
    - PASS_WARN_AGE 14
  - 針對進行上述設定前就已存在之使用者帳號，須再執行下列指令，才能使密碼到期前14天提醒使用者變更密碼
    - #chage -W 14 (使用者帳號)

密碼最小長度

- 建議值
  - 12個字元
- 說明
  - 這項原則設定決定使用者帳號的密碼可包含的最少字元數，預設值為8個字元
- 設定方式
  - 編輯/etc/login.defs檔案，新增或修改成以下內容：
    - PASS_MIN_LEN 12

密碼規則設定方式

- 設定方式
  - 編輯/etc/pam.d/system-auth檔案，新增或修改成以下內容：
    - password requisite pam_cracklib.so try_first_pass retry=3 minlen=12 dcredit=-1 ucredit=-1 ocredit=-1 lcredit=-1 difok=3

可設定密碼次數

- 建議值
  - 3
- 說明
  - 這項原則設定決定重新設定密碼時，若密碼強度不符系統要求，在設定密碼狀態，可以連續輸入密碼之次數
- 設定方式
  - password requisite pam_cracklib.so try_first_pass retry=3 minlen=12 dcredit=-1 ucredit=-1 ocredit=-1 lcredit=-1 difok=3

```
[ian@localhost ~]$ passwd
Changing password for user ian.
Changing password for ian
(current) UNIX password:
New UNIX password:
BAD PASSWORD: it is too short
New UNIX password:
BAD PASSWORD: it is too short
New UNIX password:
BAD PASSWORD: it is too short
passwd: Authentication token manipulation error
[ian@localhost ~]$
```

密碼必須至少包含數字個數

- 建議值
  - –1
- 說明
  - –這項原則設定決定使用者帳號的密碼至少包含幾個數字
- 設定方式
  - –編輯/etc/pam.d/system-auth檔案，新增或修改成以下內容：
    - password requisite pam_cracklib.so try_first_pass retry=3 minlen=12 dcredit=-1 ucredit=-1 ocredit=-1 lcredit=-1 difok=3

密碼必須至少包含大寫字母個數

- 建議值
  - 1
- 說明
  - 這項原則設定決定使用者帳號的密碼至少包含幾個大寫字母
- 設定方式
  - 編輯/etc/pam.d/system-auth檔案，新增或修改成以下內容：
    - password requisite pam_cracklib.so try_first_pass retry=3 minlen=12 dcredit=-1 ucredit=-1 ocredit=-1 lcredit=-1 difok=3

密碼必須至少包含特殊字元個數

- 建議值
  - 1
- 說明
  - 這項原則設定決定使用者帳號的密碼至少包含幾個特殊字元
- 設定方式
  - 編輯/etc/pam.d/system-auth檔案，新增或修改成以下內容：
    - password requisite pam_cracklib.so try_first_pass retry=3 minlen=12 dcredit=-1 ucredit=-1 ocredit=-1 lcredit=-1 difok=3

密碼必須至少包含小寫字母個數

- 建議值
  - 1
- 說明
  - 這項原則設定決定使用者帳號的密碼至少包含幾個小寫字母
- 設定方式
  - 編輯/etc/pam.d/system-auth檔案，新增或修改成以下內容：
    - password requisite pam_cracklib.so try_first_pass retry=3 minlen=12 dcredit=-1 ucredit=-1 ocredit=-1 lcredit=-1 difok=3

新密碼與舊密碼最少相異字元數

- 建議值
  - 3
- 說明
  - 這項原則設定決定使用者帳號的新密碼內必須有幾個字元與舊的密碼不同
- 設定方式
  - 編輯/etc/pam.d/system-auth檔案，新增或修改成以下內容：
    - password requisite pam_cracklib.so try_first_pass retry=3 minlen=12 dcredit=-1 ucredit=-1 ocredit=-1 lcredit=-1 difok=3

帳戶鎖定閾值

- 建議值
  - 5
- 說明
  - 這項原則設定決定使用者帳號被鎖定的嘗試登入失敗次數，以降低密碼暴力攻擊之影響
- 設定方式
  - 編輯/etc/pam.d/system-auth檔案，在「pam_unix」前，新增或修改成以下內容：
    - auth required pam_tally2.so deny=5 onerr=fail

強制執行密碼歷程記錄

- 建議值
  - 24
- 說明
  - 這項原則設定決定重複使用舊密碼前，必須與使用者帳號相關的唯一新密碼數目
  - 這項原則可讓系統管理員藉由確定不再繼續重複使用舊密碼，以增加安全性
- 設定方式
  - 編輯/etc/pam.d/system-auth檔案，新增或修改成以下內容：
    - password sufficient pam_unix.so existing_options remember=24

密碼到期後，帳號停用前的天數(1/2)

- 建議值
  - 30天
- 說明
  - 這項原則設定決定使用者帳號在密碼到期後，超過幾天就進行帳號停用

密碼到期後，帳號停用前的天數(2/2)

- 設定方式
  - 編輯/etc/default/useradd檔案，新增或修改成以下內容：
    - INACTIVE=30
  - 針對進行上述設定前就已存在之使用者帳號，須再執行下列指令，才能使密碼到期後，超過30天就進行帳號停用：
    - #chage -I 30 (使用者帳號)

/etc/grub.conf檔案權限、擁有者及擁有群組(1/2)

- 建議值
  - 檔案權限：600
  - 擁有者：root
  - 擁有群組：root
- 說明
  - 這項原則設定決定/etc/grub.conf檔案權限
  - GRUB (GRand Unified Boot loader)是開機載入程式，主要功能是用來載入作業系統的核心
  - 設定只有root可以讀取或寫入/etc/grub.conf，其他使用者不具有讀取、寫入及執行權，以防止非root使用者取得或修改開機參數危及系統安全

/etc/grub.conf檔案權限、擁有者及擁有群組(1/2)

- 設定方式
  - 執行下列指令，設定為「僅root擁有讀寫權限，其餘使用者不具有讀取、寫入及執行權」：
    - #chmod 600 /etc/grub.conf
  - 執行下列指令，將/etc/grub.conf擁有者與擁有群組皆設為root：
    - #chown root:root /etc/grub.conf

GNOME螢幕保護裝置(1/2)

- 建議值
  - 啟用
- 說明
  - 這項原則設定決定是否啟用GNOME螢幕保護裝置
  - 啟用螢幕保護裝置可降低使用者忘記鎖定螢幕而造成資訊外洩之影響
  - 如果停用這個設定，螢幕保護裝置不會執行

GNOME螢幕保護裝置(2/2)

- 設定方式
  - 執行下列指令以啟用螢幕保護裝置：
    - # gconftool-2 --direct --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory --type bool --set /apps/gnome-screensaver/idle_activation_enabled true

GNOME螢幕保護裝置逾時(1/2)

- 建議值
  - 15分鐘
- 說明
  - 這項原則設定決定螢幕保護裝置必須在使用者閒置時間經過多久之後才啟動
  - 預設安裝GNOME圖形界面操作桌面環境，gnome-screensaver套件負責執行螢幕保護功能

GNOME螢幕保護裝置逾時(2/2)

- 設定方式
  - 執行下列指令，設定螢幕保護裝置逾時為15分鐘：
    - # gconftool-2 --direct --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory --type int --set /apps/gnome-screensaver/idle_delay 15

以密碼保護GNOME螢幕保護裝置(1/2)

- 建議值
  - 啟用
- 說明
  - 這項原則設定決定是否要以密碼保護GNOME螢幕保護裝置
  - 如果啟用這項原則設定，螢幕保護裝置會受到密碼保護

以密碼保護GNOME螢幕保護裝置(2/2)

- 設定方式
  - 執行下列指令，以密碼保護GNOME螢幕保護裝置：
    - # gconftool-2 --direct --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory --type bool --set /apps/gnome-screensaver/lock_enabled true

特定GNOME螢幕保護裝置(1/2)

- 建議值
  - blank-only
- 說明
  - 這項原則設定決定是否指定特定GNOME螢幕保護裝置
  - 螢幕保護裝置設定為空白，以避免資訊透過螢幕顯示而外洩
  - 設定為blank-only：代表不顯示任何螢幕保護裝置主題

特定GNOME螢幕保護裝置(2/2)

- 設定方式
  - 執行下列指令，指定GNOME螢幕保護裝置為blank-only：
    - # gconftool-2 --direct --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory --type string --set /apps/gnome-screensaver/mode blank-only

終端機介面螢幕鎖定

- 建議值
  - 安裝
- 說明
  - 這項原則設定決定系統是否安裝vlock套件
  - 系統預設不安裝vlock套件，因此須進行手動安裝，才能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密碼可解除鎖定狀態
- 設定方式
  - 執行下列指令以安裝vlock套件：
    - #yum install vlock

Bash shell閒置時登出時間(1/2)

- 建議值
  - 900秒
- 說明
  - 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的標準shell。Bash主要相容於sh，並且依據一些使用者需求而加強的shell版本
  - 當shell屬於前景程序時，才能自動從shell登出，例如使用vi編輯檔案並已經閒置15分鐘，自動登出將不會發生

Bash shell閒置時登出時間(2/2)

- 設定方式
  - 在/etc/profile.d目錄下新增tmout.sh檔案，並在檔案增加以下內容：
    - TMOUT=900
    - readonly TMOUT
    - export TMOUT

SELinux

SELinux啟用狀態

- 建議值
  - enforcing
- 說明
  - 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
  - 設定為enforcing：表示系統強制執行SELinux，會阻擋有可能危害伺服器安全的操作
- 設定方式
  - 編輯/etc/selinux/config檔案，新增或修改成以下內容：
    - SELINUX=enforcing

SELinux政策

- 建議值
  - targeted
- 說明
  - 這項原則設定決定SELinux運作時所採用之政策
  - 設定為targeted：此為預設設定，針對網路服務限制較多，針對本機限制較少
- 設定方式
  - 編輯/etc/selinux/config檔案，新增或修改成以下內容：
    - SELINUXTYPE=targeted

開機載入程式啟用SELinux

- 建議值
  - 啟用
- 說明
  - 這項原則設定決定是否在開機載入程式中啟用SELinux
  - SELinux設定檔(/etc/selinux/config)內容可被開機載入程式覆蓋，因此，須確認開機載入程式未停用SELinux，以確保SELinux正常運作
- 設定方式
  - 編輯/etc/grub.conf檔案，移除selinux=0或enforcing=0內容

網路配置與防火牆

iptables服務

- 建議值
  - 啟用
- 說明
  - 這項原則設定決定系統是否啟用iptables服務
  - iptables服務為Linux作業系統本機端防火牆，專門用來過濾網路封包，正確的設定iptables規則可有效提升網路安全
- 設定方式
  - 執行下列指令以啟用iptables服務：
    - #chkconfig iptables on

INPUT與FORWARD防火牆規則鏈的預設規則(1/2)

- 建議值
  - DROP
- 說明
  - 這項原則設定決定是否變更iptables內建之INPUT與FORWARD防火牆規則鏈的預設規則
  - INPUT與FORWARD防火牆規則鏈的預設規則由ACCEPT變更為DROP，以提升網路安全

INPUT與FORWARD防火牆規則鏈的預設規則(2/2)

- 設定方式
  - 編輯/etc/sysconfig/iptables檔案，變更成下列內容：
  - *filter
  - :INPUT DROP [0:0]
  - :FORWARD DROP [0:0]

所有網路介面傳送ICMP重新導向封包(1/2)

- 建議值
  - 停用
- 說明
  - 這項原則設定決定是否允許所有網路介面傳送ICMP重新導向(Redirect)封包
  - 如果上線運作之系統並非做為路由器，應停用ICMP重新導向功能
  - 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的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的假系統

所有網路介面傳送ICMP重新導向封包(2/2)

- 設定方式
  - 編輯/etc/sysctl.conf檔案，新增或修改成以下內容：
    - net.ipv4.conf.all.send_redirects=0

無線網路介面卡(1/2)

- 建議值
  - 停用
- 說明
  - 這項原則設定決定系統是否停用無線網路介面卡
  - 若系統不透過無線網路進行連線與提供服務，應將無線網路介面卡設為停用，確保系統無法透過無線網路卡進行連線，以降低被攻擊面

無線網路介面卡(2/2)

- 設定方式
  - 首先執行下列指令，取得網路介面卡資訊，從中找出無線網路介面卡(***interface***可能為wlan0、eth0或wifi0)：
    - #ifconfig –a
  - 執行下列指令，立即關閉無線網路介面卡：
    - #ifdown ***interface***
  - 上述設定可立即關閉無線網路介面卡，但重新開機後，仍可使用無線網路介面卡。若要以後開機時皆關閉無線網路介面卡，請執行下列指令移除相關設定檔：
    - #rm /etc/sysconfig/network-scripts/ifcfg-***interface***

日誌與稽核

稽核服務

- 建議值
  - 啟用
- 說明
  - 這項原則設定決定是否啟用auditd服務
  - 啟用auditd服務可記錄系統事件，供系統管理者判斷系統是否發生未經授權存取之行為
- 設定方式
  - 執行下列指令以啟用auditd稽核服務：
    - # chkconfig auditd on

稽核auditd服務啟動前之程序(1/2)

- 建議值
  - 啟用
- 說明
  - 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

稽核auditd服務啟動前之程序(2/2)

- 設定方式
  - 編輯/etc/grub.conf檔案，在kernel行新增audit=1
  - 範例如下：
    - kernel /vmlinuz-version ro vga=ext root=/dev/VolGroup00/LogVol00 rhgb quiet audit=1

記錄變更日期與時間事件(1/2)

- 建議值
  - 啟用
- 說明
  - 這項原則設定決定系統是否記錄變更日期或時間資訊之事件針對調整系統核心時間(adjtimex)、以時區方式設定系統時間(settimeofday)、以秒為單位設定系統時間(stime)、設定內部時鐘與計時器(clock_settime)等系統呼叫行為做紀錄
  - 非預期的系統日期與時間變更，可能是惡意活動的跡象，有助於發現異常行為

記錄變更日期與時間事件(2/2)

- 設定方式
  - 先使用uname -m，查詢作業系統是32位元(b32)或64位元(b64)
  - 編輯/etc/audit/audit.rules檔案，新增或修改成以下內容(32位元系統請將***ARCH***改為b32，64位元系統請將***ARCH***改為b64)：
    - -a always,exit -F arch=***ARCH*** -S adjtimex -S settimeofday -S stime -k time-change
    - -a always,exit -F arch=***ARCH*** -S clock_settime -k time-change
    - -w /etc/localtime -p wa -k time-change

記錄使用者或群組變更資訊事件 (1/2)

- 建議值
  - 啟用
- 說明
  - 這項原則設定決定系統是否記錄變更使用者或群組資訊之事件
  - 這些檔案遭非預期變更，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

記錄使用者或群組變更資訊事件(2/2)

- 設定方式
  - 編輯/etc/audit/audit.rules檔案，新增或修改成以下內容：
    - -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

記錄不成功的未經授權檔案存取(1/2)

- 建議值
  - 啟用
- 說明
  - 這項原則設定決定系統是否記錄所有使用者未經授權存取檔案之行為
  - 若啟用這項原則設定，系統將會監控包含控制建立(creat)、開啟(open、openat)及截斷(truncate、ftruncate)等系統呼叫存取檔案之行為，並針對非系統管理者(auid大於500)、非服務事件(auid等於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」

記錄不成功的未經授權檔案存取(2/2)

- 設定方式
  - 先使用uname -m，查詢作業系統是32位元(b32)或64位元(b64)
  - 編輯/etc/audit/audit.rules檔案，新增或修改成以下內容(32位元系統請將***ARCH***改為b32，64位元系統請將***ARCH***改為b64)：
    - -a always,exit -F arch=***ARCH*** -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=500 -F auid!=4294967295 -k access
    - -a always,exit -F arch=***ARCH*** -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=500 -F auid!=4294967295 -k access

記錄變更登入與登出資訊事件(1/2)

- 建議值
  - 啟用
- 說明
  - 這項原則設定決定系統是否記錄嘗試變更登入與登出資訊之事件
  - 這些檔案遭非預期變更，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

記錄變更登入與登出資訊事件(2/2)

- 設定方式
  - 編輯/etc/audit/audit.rules檔案，新增或修改成以下內容：
    - -w /var/log/faillog -p wa -k logins
    - -w /var/log/lastlog -p wa -k logins

過時服務

telnet-server套件

- 建議值
  - 移除
- 說明
  - 這項原則設定決定是否安裝telnet-server套件
  - 安裝telnet-server套件後，系統可透過telnetd服務成為telnet伺服器
  - Telnet協定以明文方式傳輸資訊，建議改安裝ssh套件，以加密方式進行傳輸，以保護資料安全
- 設定方式
  - 執行下列指令，移除telnet-server套件
    - #yum erase telnet-server

rsh-server套件

- 建議值
  - 移除
- 說明
  - 這項原則設定決定是否安裝rsh-server套件
  - rsh-server套件提供指令進行遠端操作
- 設定方式
  - 執行下列指令，移除rsh-server套件
    - #yum erase rsh-server

tftp-server套件

- 建議值
  - 移除
- 說明
  - 這項原則設定決定系統是否安裝tftp-server套件
  - 簡單檔案傳輸協定(Trivial File Transfer Protocol, tftp)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驗證或加密機制，將可能導致資料外洩
- 設定方式
  - 執行下列指令，移除tftp-server套件：
    - #yum erase tftp-server

基礎服務

藍芽服務

- 建議值
  - 停用
- 說明
  - 這項原則設定決定是否啟用預設安裝的藍芽服務，若系統不需要此服務，建議停用以降低系統安全威脅
- 設定方式
  - 執行下列指令，停用藍芽服務：
    - #chkconfig bluetooth off

microcode_ctl服務

- 建議值
  - 停用
- 說明
  - 這項原則設定決定是否啟用microcode_ctl服務
  - Intel IA32處理器(Pentium Pro, PII, Celeron, PIII, Xeon,Pentium 4等)會提供一個外掛的微指令集提供系統運作，以支援Intel IA32處理器功能
  - 系統非使用IA32處理器，不會影響系統運作
- 設定方式
  - 執行下列指令，停用microcode_ctl服務：
    - #chkconfig microcode_ctl off

apmd服務

- 建議值
  - 停用
- 說明
  - 這項原則設定決定是否啟用apmd服務
  - APM(Advanced Power Management，進階電源管理)服務提供前一代電源管理機制，現已被acpid取代
  - APM在BIOS層級上提供 CPU 及週邊設備的電源管理
- 設定方式
  - 執行下列指令，停用apmd服務：
    - #chkconfig apmd off

acpid服務

- 建議值
  - 啟用
- 說明
  - 這項原則設定決定是否啟用acpid服務
  - ACPI(Advanced Configuration and Power Interface，進階組態與電源介面)提供新一代電源管理機制，由作業系統直接統一控制所有硬體的電源操作，取代由BIOS管理的APM
- 設定方式
  - 執行下列指令，啟用acpid服務：
    - #chkconfig acpid on

報告完畢
敬請指教