



# SELinux 管理配置

*Kenduest Lee*

*kenduest@info.sayya.org*

最近更新時間：2008/5/14

# 章節大綱



- 章節大綱
  - SELinux 簡介
  - SELinux 規則
  - SELinux 程式
  - SELinux 測試
  - SELinux 文件

# SELinux 簡介



- **SELinux** 簡介
  - **SELinux** 全名為 **Security-Enhanced Linux**，為美國國家安全局 (**National Security Agency, NSA**) 所開發的安全功能
  - **SELinux** 提供別於傳統 UNIX 系統以使用者權限控管的作法，可提供更詳盡逐一的授權控管
  - 目前 **SELinux** 開發由 NSA 與 RedHat 投入整合，最開始預先納入到 **Fedora** 與 **RHEL** 等版本，後續 Ubuntu/Debian 與 SuSE Linux 相關版本都納入支援

# 權限控管機制



- 權限控管機制
  - 項目說明
    - **DAC** (Discretionary Access Control, 自主存取控制)
      - 依據當時候運作的身份決定存取權限
    - **MAC** (Mandatory Access Control, 強制存取控制)
      - 依據指定條件決定是否具備可存取權限

# 權限控管機制



- 權限控管機制
  - **DAC (Discretionary Access Control)**
    - 自主存取控制，為大部份作業系統的權限存取控管方式
    - 對於一般檔案系統來說
      - 依據檔案的 owner/group/other 的 r,w,x 等權限規範
    - 一般的規範特性限制
      - root 身份執行程式有最高身份權限，無法限制
      - 檔案目錄的 r,w,x 權限太單純，無詳細的權限規範
      - 無法針對不同的行程本身進行限制

# 權限控管機制

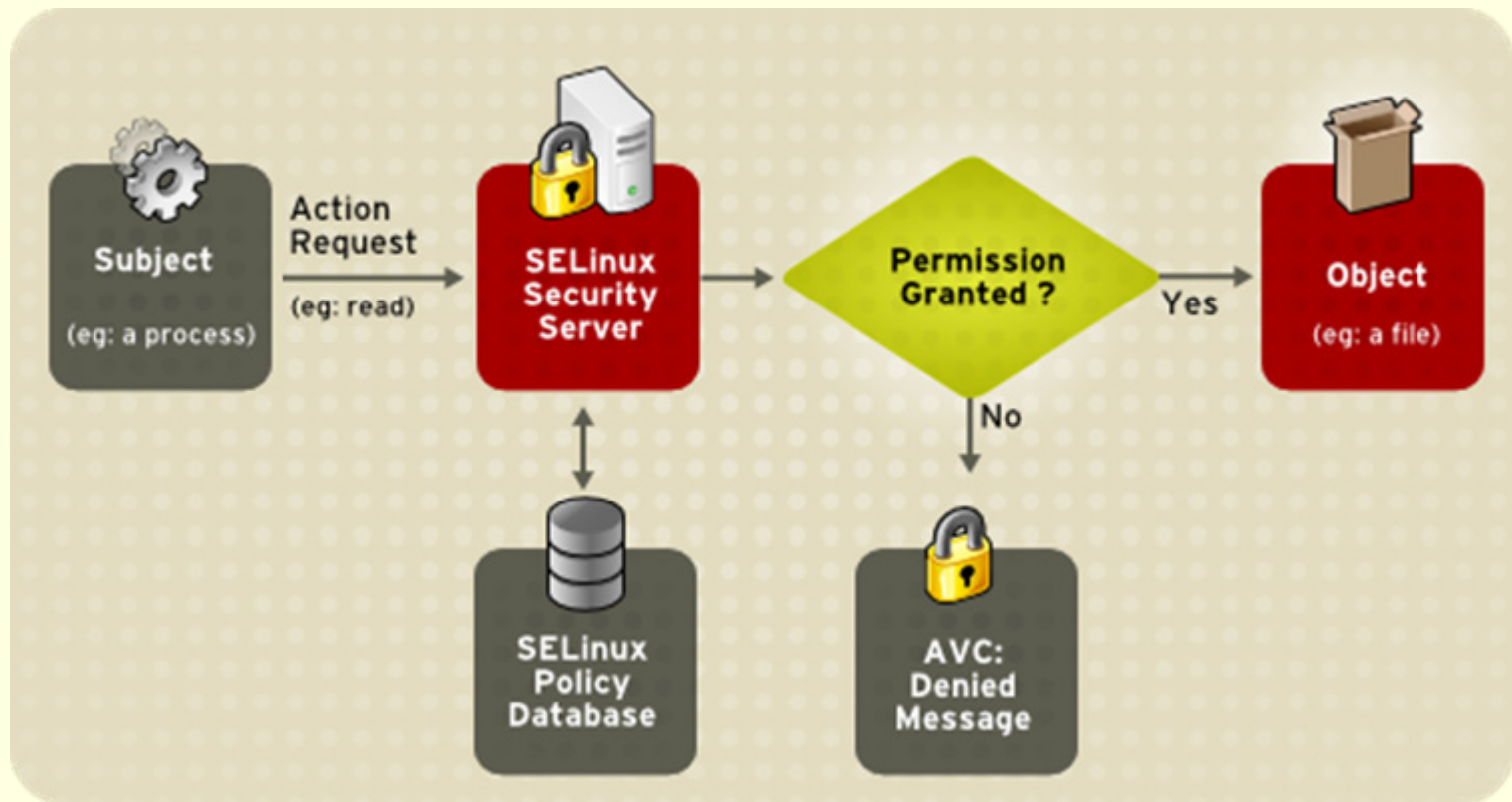


- 權限控管機制
  - **MAC (Mandatory Access Control)**
    - 強制存取控制
    - 可以規範個別細部項目進行限制存取
      - 可針對檔案目錄、行程、網路連線取等項目進行規範
    - 實際行程需要先符合 DAC 限制規範後，並通過 MAC 限制規範後才能夠存取所需要的項目

# SELinux 運作示意



## SELinux 運作示意圖



# SELinux 控管機制



- **SELinux** 運作示意圖
  - 組成項目說明
    - **Subject**
      - 一般表示系統的行程項目，欲進行操作存取的行程
    - **Object**
      - 一般表示被存取的項目
        - File, Directory, IP , Socket, Pipe 等項目

# SELinux 控管機制



- **SELinux 控管機制**
  - 組成特點項目
    - **Mandatory Access Control ( MAC )**
    - **Role Based Access Control ( RBAC )**
    - **Type Enforcement ( TE )**
    - **Domain Translation**

# SELinux 控管機制



- **SELinux 控管機制**
  - 組成特點項目
    - **Mandatory Access Control ( MAC )**
      - 提供明確完整的徹底化規範限制
        - **Object Classes and Permissions** 逐一規範
      - **Object Classes and Permissions** 組成項目
        - 檔案系統面， read, write, unlink, rename, mount 等項目
        - 網路通訊面， listen, accept, bind 等項目
        - 行程管理面， fork, signal 等項目
        - ...

# SELinux 控管機制



- **SELinux 控管機制**
  - 組成特點項目
    - **Role Based Access Control ( RBAC )**
      - 制定許多 Role 指定不同權限規範
        - 可以規範不同使用者有不同的角色項目
        - 切換到特定角色才賦予特定存取權限

# SELinux 控管機制



- **SELinux 控管機制**
  - 組成特點項目
    - **Type Enforcement ( TE )**
      - 提供給行程最低所需的權限環境
      - 使用 Type 與 Domain 規範
        - 所有檔案目錄、網路連結項目使用 Type 貼上標籤
        - Process 給予一個 Domain 標籤
        - 規範該 Domain 本身對於 Type 項目的存取規則
      - SELinux 本身的 TE 源自於 RBAC 規範

# SELinux 控管機制



- SELinux 控管機制

- 組成特點項目

- Type Enforcement ( TE ) 範例說明

- 制定項目

- 設定 httpd 行程使用 **httpd\_t** 這個 domain 運作
        - 將 httpd 所使用的 port 列入 **httpd\_port\_t** 規範內
        - 將網頁目錄 type 標示為 **httpd\_sys\_content\_t**
      - 限制以 **httpd\_t** 該 domain 運作的 web 服務程式，只能夠聆聽標示為 **httpd\_port\_t** 的 port ，並且限制存取標示為 **httpd\_sys\_content\_t** 的網頁檔案

# SELinux 控管機制



- **SELinux 控管機制**

- 組成特點項目

- **Domain Translation**

- 規範是否進行 Domain 轉移 (權限擴展或縮減規範)
        - A Process 規範使用 A-Domain 環境執行
        - B Process 規範使用 B-Domain 環境執行
        - 於 A-Domain 執行 B 程式時，可以規範 B 本身是否要沿用 A-Domain 環境，或使用 B-Domain 該自己專屬 Domain 環境來執行

# SELinux 支援設定



- **SELinux 支援檢視**
  - 設定檔案
    - `/etc/sysconfig/selinux` 或者是 `/etc/selinux/config`
      - `/etc/sysconfig/selinux` 為 symlink 檔案，連結到 `/etc/selinux/config` 檔案
  - 設定項目
    - **SELINUX=[ enforcing | permissive | disabled ]**
      - 指定 SELinux 啓用的模式
    - **SELINUXTYPE=[ targeted | strict | mls ]**
      - 指定 SELinux 使用的 Policy 項目

# SELinux 支援設定



- **SELinux** 支援檢視

- 設定項目說明

- **SELINUX**=[ **enforcing** | **permissive** | **disabled** ]

- **enforcing** ) 強制模式，並提供限制存取機制

- **permissive** ) 開啓功能，但是提供警告模式代替限制機制

- **disabled** ) 關閉

- **SELINUXTYPE**=[ **targeted** | **strict** | **mls** ]

- **targeted** ) 只有限制有規範的網路程式加以保護限制

- **strict** ) 完整保護受限模式

- **mls** ) mls 保護受限模式

# SELinux 支援設定



- **SELinux** 支援檢視
  - **GRUB** 參數設定
    - 於 kernel 敘述內傳入參數指定 selinux 功能
    - 設定項目
      - **selinux=[ 0 | 1 ]**
        - 設定核心是否要支援 SELinux
        - 若是由 0 要改成 1 時，需要搭配檔案系統 relabel 設定
      - **enforcing=[ 0 | 1 ]**
        - 設定指定預用用 permissive 或 enforcing 模式

# SELinux Policy



- **SELinux Policy**

- 說明

- SELinux 制定許多 Policy 項目提供使用
    - 目前一般可選擇項目有 **targeted**, **strict** 與 **mls**

- 放置目錄

- **/etc/selinux/<POLICYNAME>/policy/**

- 資訊檢視與檢索

- **seinfo**
    - **sesearch -a**
    - **sesearch -a -t ftpd\_t**

# SELinux Relabel



## ■ SELinux Filesystem Relabel

### ■ 說明

- 將檔案系統重新標上 selinux security context 資訊項目

### ■ 用途

- SELinux 將檔案目錄本身的標籤資訊紀錄於檔案系統的延伸屬性 (**Extended Attribute**) 項目內
- 當初 selinux 選擇關閉，或者是切換 policy 成爲 targeted 與 strict 時，可以透過該功能將檔案系統應有的 selinux 資訊恢復

### ■ 作法

- **touch /.autorelabel ; reboot**

# SELinux label



## ■ SELinux Filesystem label

### ■ 說明

- SELinux 將檔案目錄本身的標籤資訊紀錄於檔案系統的延伸屬性 (**Extended Attribute**) 項目內
- 可以使用 **getfattr/setfattr** 檢視與修改 **selinux** 項目 (不建議)

### ■ 作法

- **getfattr -m . -d /etc/passwd**

### ■ 附註

- 若是要使用 **getfattr/setfattr** 工具，**/etc/fstab** 檔案額外設定 **user\_xattr** 參數

# 相關程式



- 程式項目
  - **sestatus** - 查詢系統的 selinux 目前的狀態
  - **selinuxenabled** - 查詢系統的 selinux 支援是否有啓用
  - **setenforce** - 設定 selinux 運作狀態
  - **getsebool** - 列出所有 selinux bool 數值清單列表與內容
  - **setsebool** - 設定 selinux bool 數值內容

# 相關程式



## ■ 程式項目

- **chcon** - 變更檔案目錄 security context
- **restorecon** - 恢復檔案目錄的預設的 security context
- **fixfiles** - 修正檔案目錄的預設的 security context
- **semanage** - SELinux policy 管理程式
- **secon** - 檢視行程、檔案等等項目的 SELinux context
- **audit2why** - 檢視 SELinux audit 訊息內容
- **sealert** - SELinux 訊息診斷用戶端程式

# SELinux 程式



- SELinux 相關程式

- **sestatus**

- 說明：查詢系統的 selinux 目前的狀態

- 輸出項目

- **SELinux status:** **enabled**
      - **SELinuxfs mount:** **/selinux**
      - **Current mode:** **enforcing**
      - **Mode from config file:** **permissive**
      - **Policy version:** **21**
      - **Policy from config file:** **targeted**

# SELinux 程式



- SELinux 相關程式
  - **selinuxenabled**
    - 說明：檢查系統 `selinux` 是否開啓
    - 傳回項目
      - 回傳結束代碼為 **0**，表示系統有開 `selinux` 功能
      - 回傳結束代碼為 **1**，表示系統關閉 `selinux` 功能
      - `shell` 環境可以使用 `?` 變數取得結果
        - **echo \$?**

# SELinux 程式



- SELinux 相關程式
  - **setenforce**
    - 說明：設定 selinux 運作狀態
    - 使用方式：**setenforce [ Enforcing | Permissive | 1 | 0 ]**
    - 設定項目
      - **Enforcing** 與 **1**，表示開啓強制模式
      - **Permissive** 與 **0**，表示開啓警告但是無限制模式

# SELinux Boolean 值

- **SELinux boolean value**

- 說明

- SELinux 規範了許多 boolean 數值清單檔案，提供開啓或者關閉個功能存取項目

- 目錄位置

- **/selinux/booleans/** 目錄內相關檔案

- 程式項目

- **getsebool**
    - **setsebool**

# SELinux Boolean 值

- SELinux boolean value 程式
  - **getsebool**
    - 說明：列出所有 selinux bool 數值清單列表與內容
    - 使用方式：**getsebool [ -a ]**
    - 使用範例
      - **getsebool ftpd\_disable\_trans**
      - **getsebool -a**

# SELinux 程式



## ■ SELinux boolean value 程式

### ■ setsebool

- 說明：設定 selinux bool 數值清單列表與內容
- 使用方式：**setsebool [ -P ] boolean value | bool1=val1 .....**
- 參數配置
  - **-P** ) 設定該項目永久套用
- 使用範例
  - **setsebool ftpd\_disable\_trans=on** ( on 亦可用 1 )
  - **setsebool -P ftpd\_disable\_trans=off** ( off 亦可用 0 )

# Security Context



## ■ SELinux - Security Context

### ■ 說明

- SELinux 依據 Security Context 規範來決定行為是否可存取

### ■ 內容組成

#### ■ Subject 與 Object

- 特定的“身份”所執行的“行程”組成 **Subject**
- 特定的“檔案目錄”, ”網路連結埠”等項目組成 **Object**

### ■ 規範方式

- 每個 Subject 與 Object 都具備一個 **Security Context** 項目
- SELinux 規範了上面這兩者本身的關係存取限制關係

# SELinux 檢視



- 檢視檔案目錄與行程 SELinux Security Context
  - 說明
    - 提供檢視使用者、檔案目錄、行程的 Security Context 資訊
  - 檢視方式
    - **id -Z**
    - **ls -Z , ls --scontext**
    - **ps Z , ps -Z , ps auxZ**
    - **netstat -Z**

# SELinux 檢視



- 檢視 SELinux security context
  - **id -Z**
    - 訊息輸出
      - **root:system\_r:unconfined\_t:SystemLow-SystemHigh**
      - **user\_u:system\_r:unconfined\_t**
    - 描述
      - 上面為 root 帳號與一般使用者帳號登入時的執行結果

# SELinux 檢視



- 檢視 SELinux Security Context

- `ls -Z` , `ls --scontext`

- 訊息輸出

- `drwxr-xr-x root root system_u:object_r:bin_t bin`

- 描述

- 為執行 `ls -Zd /bin` 的執行結果

# SELinux 檢視



- 檢視 SELinux Security Context

- `ps Z` , `ps -Z` , `ps auxZ`

- 訊息輸出

- | LABEL                    | PID | TTY | STAT | TIME | CMD      |
|--------------------------|-----|-----|------|------|----------|
| system_u:system_r:init_t | 1   | ?   | Ss   | 0:00 | init [5] |

- 描述

- 為執行 `ps axZ | head` 的執行結果

# Security Context



- **SELinux - Security Context**
  - 格式組成
    - 一般基礎格式組成
      - **identity:role:type**
    - 其他擴增項目
      - **MLS ( Multi Level System )**
        - **user:role:type:sensitivity:compartments**
      - **MCS ( Multi Category System )**
        - **user:role:type:sensitivity:category**
        - 其中 **sensitivity** 固定為 s0

# Security Context



- **SELinux** 資訊組成與識別
  - **identity**
    - 近似於 Linux 系統的使用者帳號名稱，提供身份識別
      - **root** 表示 root 帳號身份
      - **system\_u** 表示系統行程
      - **user\_u** 表示一般使用者帳號
    - 透過 **identity** 項目可以確認身份類型，切換到其他帳號身份時該項目皆不會變動。一般搭配 **role** 使用
      - 有不同的 **role** 具備不同的權限規範
    - 在 **targeted** 的 **selinux** 環境下，該項目沒實質功能

# Security Context



- **SELinux** 資訊組成與識別
  - **role**
    - 所屬角色類型
      - 檔案目錄，一般為 **object\_r**
      - 行程資訊，一般為 **system\_r**
      - 使用者
        - **targeted policy** 下為 **system\_r**
        - **strict policy** 下細分 **sysadm\_r**, **staff\_r** , **user\_r**

# Security Context



- **SELinux** 資訊組成與識別
  - **role**
    - 使用者的 **role** 類似於群組，不同角色可以具備不同身份權限
      - 可以具備多個，但是同一時間內只能夠使用一個 **role**
    - 在 **targeted** 的 **selinux** 環境下，該項目沒實質功能

# Security Context



- **SELinux** 資訊組成與識別
  - **role**
    - 於 **targeted policy** 環境
      - 所有使用者、行程 role 皆為 **system\_r**
    - 於 **strict policy** 環境
      - 一般使用者登入時，role 為 **user\_r**
      - root 帳號登入時預設 role 為 **staff\_r**，但是沒有實質特權
      - 切換到 **sysadm\_r** 該 role 的使用者才具備實際最高身份權限
        - 屬於 **staff\_r** 該 role 帳號才允許切換到 **sysadm\_r**

# Security Context



- **SELinux** 資訊組成與識別
  - **targeted policy** 使用者 **identity** 與 **Role** 應對

SELinux Identify	Roles	Description
root	system_r	供 root 帳號登入特殊使用
system_u	system_r	系統非交談模式運作行程
user_u	system_r	一般無特權使用者

# Security Context



- SELinux 資訊組成與識別
  - strict policy 使用者 identity 與 Role 應對

SELinux Identify	Roles	Description
root	staff_r, sysadm_r	供 root 帳號登入特殊使用
system_u	system_r	系統非交談模式運作行程
user_u	user_r	一般無特權使用者
staff_u	staff_r, sysadm_r	系統管理者 (一般身份權限)
sysadm_u	sysadm_r	系統管理者 (管理特權)

# Security Context



- **SELinux** 資訊組成與識別
  - **type**
    - SELinux 內的 **type** 又可以稱呼為 **domain**
    - 檔案目錄, 行程皆有一個 **type** 標示規範項目
      - 一般檔案目錄主要稱呼為 **type**
      - 執行中的行程主要稱呼為 **domain**
    - 可以依據 **type** 相關組合來限制可以存取資源項目

# Security Context



- SELinux 資訊組成與識別
  - type
    - 產生名稱爲 **foo\_t** 的 domain
      - 制定 **foo\_conf\_t** 與 **foo\_exec\_t** 存取規則限制
        - **foo\_conf\_t** 爲設定檔案的 type
        - **foo\_exec\_t** 爲程式檔案的 type
    - 使用 **foo\_t** 的 domain
      - 執行標示爲 **foo\_exec\_t** 的 foo 程式表示進入 **foo\_t** 該 domain 環境，該 domain 環境限制可規範存取標示爲 **foo\_conf\_t** 設定檔

# SELinux 程式



- SELinux 相關程式

- **chcon**

- 說明：變更檔案目錄的 security context

- 使用方式

- **chcon [OPTION]... CONTEXT FILE...**

- **chcon [OPTION]... --reference=RFILE FILE...**

- 參數

- **-u USER** set user USER in the target security context

- **-r ROLE** set role ROLE in the target security context

- **-t TYPE** set type TYPE in the target security context

# SELinux 程式



- SELinux 相關程式
  - chcon
    - 範例
      - `chcon -t var_t /etc/vsftpd/vsftpd.conf`
      - `chcon --reference=/var/www/html index.html`
    - 其他事宜
      - 若是變更於目錄上，後續於該目錄內建立的檔案目錄會套用目錄本身 type 設定

# SELinux 程式



- SELinux 相關程式

- restorecon

- 說明

- 恢復檔案目錄的預設的 security Context

- 規格來源

- /etc/selinux/<POLICY>/contexts/files/ 目錄內的  
**file\_contexts** 與 **file\_contexts.local**

- 使用方式

- **restorecon [FRrv] [-e excludedir ] pathname... ]**

# SELinux 程式



- SELinux 相關程式

- restorecon

- 參數

- **-r | -R** 包含子目錄與其下檔案目錄
      - **-F** 恢復使用預設的項目 (就算是檔案符合存取規範)
      - **-v** 顯示執行過程

# SELinux 程式



- SELinux 相關程式
  - restorecon
    - 使用範例
      - `restorecon /etc/ntp.conf`
      - `restorecon -v /etc/ntp.conf`
      - `restorecon -v -F /etc/ntp.conf`

# SELinux 程式



- SELinux 相關程式

- restorecon

- 手動配置新增恢復規則

- 檔案名稱

- `/etc/selinux/<POLICYTYPE>/contexts/files/`

- file\_contexts.local**

- 新增配置範例

- `/var/ftp(/.*)? system_u:object_r:public_content_t`

- 附註

- 可以使用 **semanage** 程式來維護會比較方便

# SELinux 程式



- SELinux 相關程式
  - **fixfiles**
    - 說明
      - 修正檔案目錄的預設的 security Context
      - 依據 `/etc/selinux/<POLICY>/contexts/files/` 內相關檔案修正
    - 使用方式
      - **fixfiles { check | restore[[-F] relabel } [[dir] ... ]**
      - **fixfiles -R rpmpackage[,rpmpackage...] { check | restore }**

# SELinux 程式



- SELinux 相關程式
  - **fixfiles**
    - 參數
      - **-R** ) 使用指定的 rpm 套件所提供的檔案清單
    - 使用範例
      - **fixfiles check /etc**
      - **fixfiles restore /etc**
      - **fixfiles -F relabel /**
      - **fixfiles -R setup check**

# SELinux 測試



- **SELinux** 限制測試

- 測試項目

- ① 設定 `vsftpd` 是否可以支援一般使用者帳號登入時，是否可以存取家目錄

- ② 設定 `vsftpd` 是否可以支援匿名登入後，是否可以在指定目錄內來上傳檔案

# SELinux 測試



- SELinux 限制測試
  - vsftpd 服務限制 (1)
    - 說明
      - selinux 組態內預設限制 vsftpd 一般帳號帳號登入 ftp 服務時無法存取家目錄與其下檔案
    - 測試方式
      - 執行 **ftp localhost** 登入，使用一般使用者帳號登入
      - 是否得到無法切換到使用者家目錄的錯誤訊息

# SELinux 測試



- **SELinux 限制測試**
  - **vsftpd 服務限制 (1)**
    - 設定是否開放一般帳號登入存取家目錄功能
      - **setsebool -P ftp\_home\_dir=on** ( Allow )
      - **setsebool -P ftp\_home\_dir=off** ( Deny )
  - 附註
    - **-P** 表示永久套用，沒使用表示暫時性下次開機就恢復預設

# SELinux 測試



- SELinux 限制測試
  - vsftpd 服務限制 (2)
    - 說明
      - selinux 限制 vsftpd 服務程式使用匿名身份登入後，若是要能夠有寫入的權限，該檔案目錄的 context 需要為 **public\_content\_rw\_t**
    - 設定檔案
      - **/etc/vsftpd/vsftpd.conf**

# SELinux 測試



- SELinux 限制測試
  - vsftpd 服務限制 (2)
    - 修改 `/etc/vsftpd/vsftpd.conf` 配置
      - `anon_upload_enable=YES`
    - 建立提供上傳的目錄與設定好可以存取權限
      - `cd /var/ftp ; mkdir upload ; chmod 777 upload`
    - 測試方式
      - 修改 upload 目錄的 type 分別為 `public_content_t` 與 `public_content_rw_t` 時，是否可以上傳檔案

# SELinux 問題診斷



- SELinux 問題診斷
  - 診斷方式
    - 確認 **setroubleshoot** 服務有啓動提供診斷
      - 檢視 **/var/log/messages** 於 **setroubleshoot** 顯示訊息
      - 使用 **sealert -l xxxxx-xxxxx-xxxx** 檢視問題點與建議
      - RHEL 於 GUI 環境提供警示圖示與程式檢視功能
    - 若是有啓動 **auditd** 服務，可以檢視 **auditd** 本身的紀錄檔案
      - **/var/log/audit/audit.log**
      - **audit2why < /var/log/audit/audit.log**

# SELinux 問題診斷



- SELinux 相關程式
  - **audit2why**
    - 說明
      - 檢視 SELinux audit 訊息內容
      - 提供檢視 `/var/log/audit/audit.log` 內的紀錄資訊說明
    - 使用範例
      - `audit2why < /var/log/audit/audit.log`

# SELinux 問題診斷



- SELinux 相關程式
  - **audit2why**
    - 附註
      - 需要搭配啓動 **auditd** 服務程式一起使用

# SELinux 問題診斷



- SELinux 相關程式

- **sealert**

- 說明：SELinux 訊息診斷用戶端程式

- 參數

- **-H, --html\_output** ) 使用網頁格式輸出 (搭配 **-a** or **-l** 使用)

- **-l, --lookupid ID** ) 檢視指定 ID 的警示訊息

- 範例

- **sealert -l xxxxx-xxxxx-xxxx**

- **sealert -H -l xxxxx-xxxxx-xxxx > output.html**

# SELinux 問題診斷



- SELinux 相關程式
  - **sealert**
    - 附註
      - 需要搭配 **setroubleshoot** 服務一起使用
      - **setroubleshoot** 服務啓動後，會依據 **audit** 服務提供的資訊給予適當問題診斷，然後輸出於 **/var/log/messages**，該檔案內會有相關輸出資訊提供除錯檢視

# SELinux 規則維護



- SELinux 規則維護

- **semanage**

- 說明：selinux policy 維護工具

- 使用方式

- **semanage { login | user | port | interface |  
fcontext | translation} -l [-n]**

# SELinux 規則維護



- SELinux 規則維護

- semanage

- 使用方式

- `semanage login -{a|d|m} [-sr] login_name`
      - `semanage user -{a|d|m} [-LrRP] selinux_name`
      - `semanage port -{a|d|m} [-tr] [ -p protocol ] port | port_range`
      - `semanage interface -{a|d|m} [-tr] interface_spec`
      - `semanage fcontext -{a|d|m} [-fst] file_spec`
      - `semanage translation -{a|d|m} [-T] level`

# SELinux 規則維護



- SELinux 規則維護

- **semanage**

- 使用範例

- **semanage login -l**
      - **semanage user -l**
      - **semanage port -l**
      - **semanage port -a -t http\_port\_t -P tcp 81**
      - **semanage fcontext -a -t httpd\_sys\_Context\_t \**  
**"/home/users/(.+)/public\_html(/.\*)?"**

# SELinux 規則維護



- SELinux 規則維護

- secon

- 說明

- 檢視程式、檔案與使用者等相關 SELinux Context

- 使用方式

- **secon [-hVurtscmPRfLp] [CONTEXT]**
      - **secon [--file] FILE | [--link] FILE | [--pid] PID**

# SELinux 規則維護



- SELinux 規則維護

- secon

- 參數

- **-u, --user** ) show the user of the security context
      - **-r, --role** ) show the role of the security context
      - **-t, --type** ) show the type of the security context
      - **-f, --file FILE** ) gets the context from the specified file FILE
      - **-p, --pid PID** ) gets the context from the specified process PID

# SELinux 規則維護



- SELinux 規則維護
  - secon
    - 使用範例
      - `secon -u`
      - `secon -r`
      - `secon -t`
      - `secon --file /etc/passwd`
      - `secon --pid <pid>`

# SELinux Domain



## ■ SELinux Domain transition

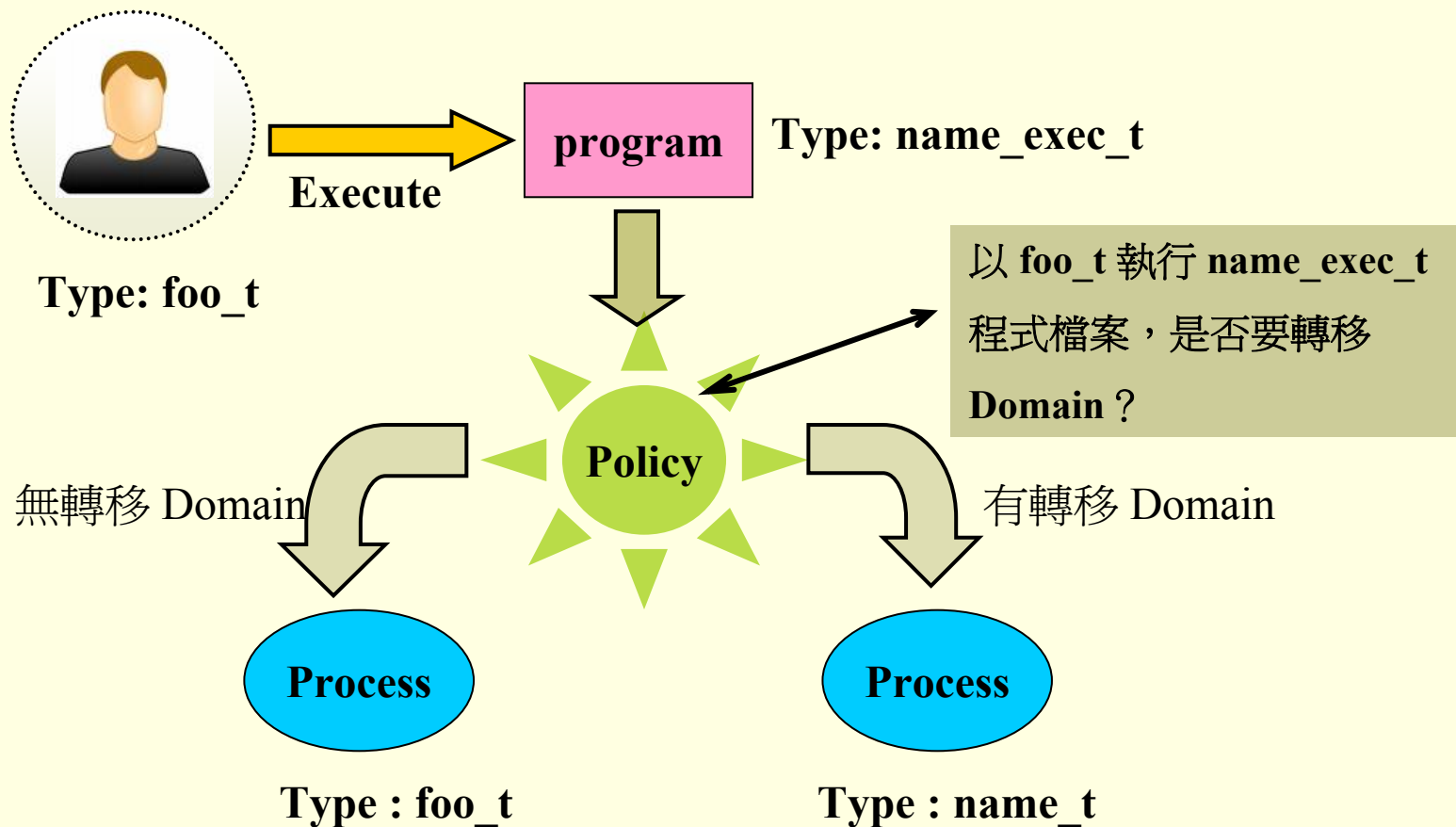
### ■ 說明

- 決定目前在 A Domain 環境執行 B 程式時，是否要進入 B 程式運作的 Domain 環境
- 可提供是否要繼續使用原本 Domain 環境，還是進入另外一個 Domain 環境進行運作

# SELinux Domain



## SELinux Domain transition



# SELinux Domain



- **SELinux Domain transition**
  - 環境說明
    - 目前執行身份的 security context
      - **root:system\_r:unconfined\_t**
    - 檔案 security content
      - **/etc/init.d/vsftpd**
        - **system\_u:object\_r:initrc\_exec\_t**
      - **/usr/sbin/vsftpd**
        - **system\_u:object\_r:ftpd\_exec\_t**

# SELinux Domain



- **SELinux Domain transition**

- 環境說明

- selinux policy 設定

- **type\_transition unconfined\_t initrc\_exec\_t : process initrc\_t**

- 以 type 爲 **unconfined\_t** 的身份執行 type 爲 **initrc\_exec\_t** 的檔案，行程的 type 轉移到 **initrc\_t**

- **type\_transition initrc\_t ftpd\_exec\_t : process ftpd\_t**

- 以 type 爲 **initrc\_t** 的身份執行 type 爲 **ftpd\_exec\_t** 的檔案，行程的 type 轉移到 **ftpd\_t**

# SELinux Domain



## ■ SELinux Domain transition

### ■ 運作流程說明

- 目前執行身份的 type 如下
  - **root:system\_r:unconfined\_t**
- 執行了 `/etc/init.d/vsftpd` 命令，該 `vsftpd` 檔案的 type 如下
  - **system\_u:object\_r:initrc\_exec\_t**
- 因為如下 policy 規範，所以會進行 domain 轉移
  - **type\_transition unconfined\_t initrc\_exec\_t : process initrc\_t**
- 執行中 domain 為 **initrc\_t** 的行程，會執行 `/usr/sbin/vsftpd`

# SELinux Domain



## ■ SELinux Domain transition

### ■ 運作流程說明

- 要執行的 `/usr/sbin/vsftpd` 檔案 type 如下
  - `system_u:object_r:ftpd_exec_t`
- 因為有如下 policy 設定，所以 domain 會轉移
  - `type_transition initrc_t ftpd_exec_t : process ftpd_t`
- 轉移後 `/usr/sbin/vsftpd` 以 `ftpd_t` 的 domain 運作
- 後續可以以 `ftpd_t` 這個 domain 來繼續規範可以存取哪些 type

# SELinux Domain



- **SELinux Domain transition**

- 結論

- `/etc/init.d/` 目錄內的啓動腳本 type 皆爲 `initrc_exec_t`
    - 於 **targeted policy** 的規範下，只有使用 `/etc/init.d/` 目錄內的啓動腳本來啓動服務，該啓動的服務會進行 Domain 轉移進而受到 SELinux 規範的環境規範

# 相關計畫



- 相關計畫
  - **Smack**
    - <http://www.schaufler-ca.com/>
  - **AppArmor**
    - <http://forge.novell.com/modules/xfmod/project/?apparmor>
  - **TOMOYO Linux**
    - <http://tomoyo.sourceforge.jp/>

# 相關文件



- 相關文件
  - **NSA SeLinux Official**
    - <http://www.nsa.gov/selinux>
  - **Fedora SELinux FAQ**
    - <http://docs.fedoraproject.org/selinux-faq/>
    - <http://fedoraproject.org/wiki/SELinux>
  - **Managing RedHat Linux Enterprise 5**
    - <http://people.redhat.com/dwalsh/SELinux/Presentations/ManageRHEL5.pdf>

# 相關文件



- 相關文件
  - **Paranoid Penguin - Introduction to SELinux**
    - <http://www.linuxjournal.com/article/9500>
  - **Access Control With SELinux**
    - [http://www.linux-magazine.com/w3/issue/69/Access\\_Control\\_with\\_SELinux.pdf](http://www.linux-magazine.com/w3/issue/69/Access_Control_with_SELinux.pdf)
  - **HOWTO Understand SELinux**
    - [http://gentoo-wiki.com/HOWTO\\_Understand\\_SELinux](http://gentoo-wiki.com/HOWTO_Understand_SELinux)

# 相關文件



- 相關文件
  - **SELinux Quick Start Guide**
    - <http://www.engardelinux.org/doc/guides/selinux-quick-start-guide/selinux-quick-start-guide.pdf>
  - **Red Hat Enterprise Linux Deployment Guide - SELinux**
    - [http://www.centos.org/docs/5/html/Deployment\\_Guide-en-US/selg-overview.html](http://www.centos.org/docs/5/html/Deployment_Guide-en-US/selg-overview.html)
  - **Gentoo SELinux Handbook**
    - <http://www.gentoo.org/proj/en/hardened/selinux/selinux-handbook.xml>

# 相關文件



- 相關文件
  - **A Brief Introduction to Multi-Category Security (MCS)**
    - <http://james-morris.livejournal.com/5583.html>
  - **Getting Started with Multi-Category Security (MCS)**
    - <http://james-morris.livejournal.com/8228.html>
  - **SELinux Conditional Policy Language Extensions**
    - [http://www.crypt.gen.nz/selinux/conditional\\_policy.html](http://www.crypt.gen.nz/selinux/conditional_policy.html)
  - **Write SELinux Policy HowTO**
    - <http://www.lurking-grue.org/writinglinuxpolicyHOWTO.html>