Red Hat Enterprise Linux 7
虛擬化安全性指南

保護您的虛擬環境

Scott Radvan Tahlia Richardson
Thanks go to the following people for enabling the creation of this guide:
Paul Moore Kurt Seifried David Jorm

Red Hat Enterprise Linux 7 虛擬化安全性指南

保護您的虛擬環境

Scott Radvan
Red Hat 客戶服務部出版中心
sradvan@redhat.com

Tahlia Richardson
Red Hat 客戶服務部出版中心
trichard@redhat.com

Paul Moore
Red Hat 工程部

Kurt Seifried
Red Hat 工程部

David Jorm
Red Hat 工程部

Thanks go to the following people for enabling the creation of this guide:

法律聲明

摘要

本指南提供了 Red Hat 所提供的虛擬化安全技術總覽，同時亦包含了虛擬化環境中，安全性主機、客座端、共享架構與資源的建議。

內容目錄

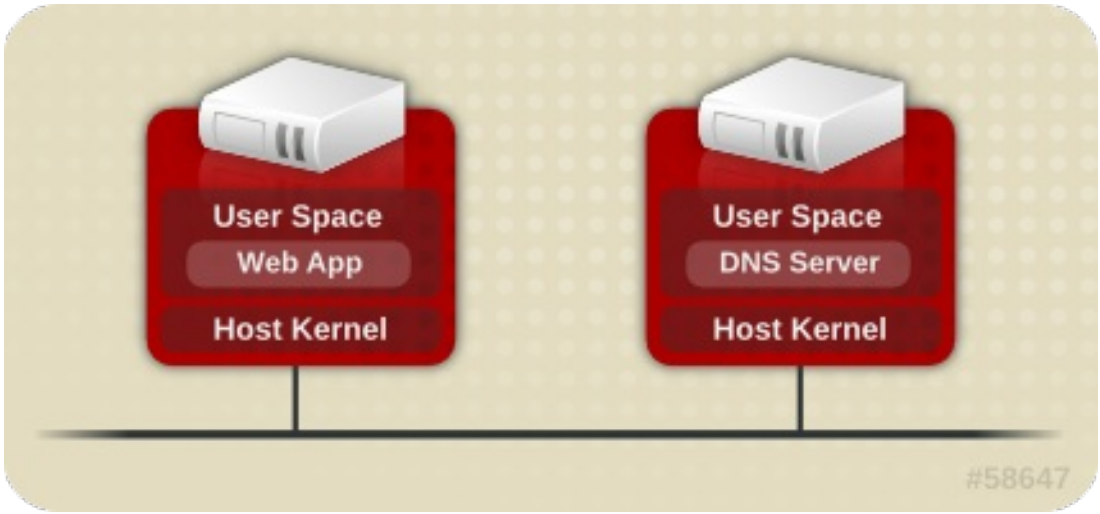
章 1. 簡介

1.1. 虛擬化與非虛擬化環境

對於尋找攻擊的切入點、或修補尚未被廣為人知的漏洞時，虛擬環境非常有用。因此，很重要的是採取行動，確保實體主機與其上的虛擬機器在建立、維護時，都是安全的。

非虛擬環境

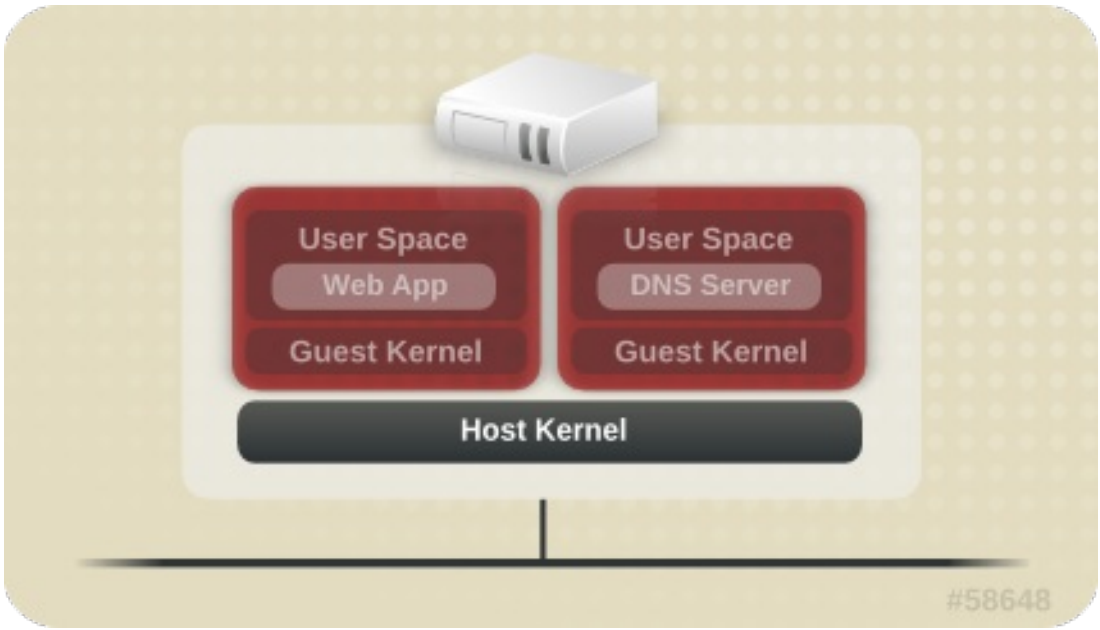
在非虛擬環境中，主機與其它實體主機是分離開來的，而且每台主機都有自己的空間、包含多種服務（例如網站伺服器或 DNS 伺服器）。這些服務會與自己的使用者空間、主機的 kernel 與實體主機通訊，直接向網路提供服務。以下圖片顯示了非虛擬環境：



圖形 1.1. 非虛擬環境

虛擬化環境

在虛擬環境中，使用者可以在單一主機 kernel 與實體主機上建置多種作業系統（亦即「客座端」——guest）。以下圖片顯示了虛擬化環境：



圖形 1.2. 虛擬化環境

當服務並未虛擬化時，每台機器在實體上都是分開的。因此一般來說，任何弱點都只受限於受影響的機器，自外於網路攻擊之外。當服務在虛擬化環境中集結成群時，更多的弱點就會集合在系統上。如果 hypervisor 中有安全性弱點、且會感染虛擬機器時，那麼受感染的虛擬機器不但會攻擊主機，還會攻擊位於同一台主機上的其它虛擬機器。這並不是理論上的假設；攻擊已經存在於 hypervisor 上了。這些攻擊可以延伸到虛擬機器之外，讓其它客座端也暴露在攻擊之下。

1.2. 為何虛擬化的安全性至關重要

在基礎建設中建置虛擬化方案，可提供多項好處，但也可能導致新的風險。虛擬化資源與服務應考量以下安全性問題，才加以建置：

- 主機與 hypervisor 會成為主要目標；對於客座端與資料來說，主機與 hypervisor 多半是單點失效之處。
- 虛擬機器會在意想不到的情況下互相干擾。假設沒有存取控制來避免互相干擾，惡意的客座端就有可能繞過有弱點的 hypervisor，直接存取主機系統上的其它資源，例如其它客座端的儲存裝置。
- 資源與服務會變得難以追蹤、維護；隨著虛擬化系統的快速建置，管理資源的需求也隨之增加，包括足夠的升級、監控與維護。
- 技術人員可能缺乏相關知識，與新技術有鴻溝，且缺乏管理虛擬環境的經驗。這通常會導致弱點發生。
- 例如儲存裝置等資源散佈各處，且仰賴多台機器。這可能導致過於複雜的環境，並讓系統難以管理及維護。
- 虛擬化並不會移除現有環境中的任何傳統安全性風險；整個解決方案都必須受到防護，而不是只有虛擬層。

本指南旨在建議多項 Red Hat Enterprise Linux（以下簡稱 RHEL）與 Red Hat Enterprise Linux（以下簡稱 RHEV）實務，幫助使用者降低安全性風險，保護虛擬化架構。

1.3. 在 sVirt 上善用 SELinux

sVirt 會將虛擬化與 SELinux 所提供的既有安全性架構相整合，並將「*強制存取控制*」（MAC，Mandatory Access Control）套用至虛擬機器上。sVirt 的主要目的是保護主機與客座端免於遭受到 hypervisor 的安全性漏洞所導致的攻擊。SELinux 透過在不同的程序上套用存取政策，進而防護系統。透過將每個客座端視為程序，sVirt 會將此能力延伸到主機與客座端，允許管理者套用類似的政策，避免惡意客座端存取受限制的資源。欲取得更多 sVirt 的相關資訊，請參閱〈章 4, *sVirt*〉。

章 2. 主機安全性

2.1. 為何主機的安全性至關重要

建置虛擬化技術時，主機安全性是至關重要的。RHEL 主機系統會負責管理、控制對實體主機裝置、儲存裝置、網路的存取，當然這也及於虛擬客座端本身。如果主機系統被攻陷，不僅主機會遭受侵害，客座端及其資料也無法倖免。

只有主機系統安全時，虛擬客座端才安全；保障 RHEL 主機系統的安全是建立安全的虛擬化平台之第一要務。

2.2. 建議的 RHEL 主機安全性實務

鑑於主機安全性在虛擬化架構扮演了如此重要的角色，以下乃架構安全的 RHEL 主機系統的建議實務，作為起始的第一步：

- 只在系統上執行使用、管理客座端所需的服務。如果您需要提供額外服務，例如檔案或列印服務，請考慮在 RHEL 客座端中執行。
- 僅限於需要管理系統的人存取系統。也請考慮停用他人共享 root 的存取，若要使用這項功能，請使用諸如 **sudo** 的工具，根據管理角色將管理權限授與使用者。
- 請確定 SELinux 已配置完善，並以「強制」模式執行。除了安全性實務以外，還有 sVirt 所提供的更先進的虛擬化安全功能，其基礎也建構於 SELinux 之上。欲取得更多有關於 SELinux 與 sVirt 的詳情，請參閱〈章 4, *sVirt*〉。
- 請確定主機系統上啓用了稽核功能，且 libvirt 已設置會發出稽核記錄。稽核啓用時，libvirt 會產生關於客座端配置變化的紀錄、以及啓動 / 停止事件，這能幫助您追蹤客座端的狀態。除了標準稽核的日誌檢查工具外，libvirt 稽核事件也可以透過特有的 auvirt 工具來檢視。
- 請確定系統上的所有遠端管理工具，皆使用了安全的網路頻道。SSH 之類的工具與 TLS 或 SSL 之類的網路通訊協定，都提供了身分認證與資料加密的安全性，確保只有正確的管理者能從遠端管理系統。
- 請確認防火牆已正確配置，且在開機時就會啓動。只開放需要使用、需要用以管理功能的網路連接埠。
- 請不要賦予客座帳號直接存取整個磁碟或區塊裝置（例如 **/dev/sdb**）的權限；反之，請使用分割區（例如 **/dev/sdb1**）或 LVM 卷冊做為客座帳號的儲存裝置。
- 請確認員工接受了虛擬環境的相關訓練與知識。

警告

在虛擬機器沒有 SR-IOV 的情況下連接 USB 裝置、實體功能、或實體裝置時，能提供對裝置的存取，但卻不足以覆寫裝置的韌體。這會導致潛在的安全性問題，駭客可以覆寫裝置的韌體，加入惡意程式碼，以致在虛擬機器間切換、或主機開機時，覆寫裝置的韌體。建議您在可能的情況下，使用 SR-IOV 虛擬功能裝置的指定功能。

注意

本指南的目標是解釋關於安全性的獨特挑戰、弱點、與解決方案，這些問題存在於大部分虛擬環境中；也列出解決這些問題的建議。然而，要讓 RHEL 系統（不管是獨立主機、虛擬主機、或虛擬機器）變得安全，有許多建議上需採行的實務。這些建議上的實務包含了例如系統更新、密碼安全、加密、以及配置防火牆這些步驟。相關資訊在位於〈https://access.redhat.com/site/documentation/〉的《*Red Hat Enterprise Linux 安全性指南*》中有進一步的描述。

2.2.1. 公開雲端營運者的特別考量

跟傳統的虛擬化用戶比起來，公開雲端營運者會暴露在更多安全性風險中。虛擬客座端隔離（介於主機與客座端、還有客座端與客座端之間）是非常重要的，因為有些威脅來自惡意客座端，同時虛擬化架構中需要保護客戶資料的機密性與完整性。

除了上述建議關於 RHEL的實務以外，公開雲端營運者還需要考量以下項目：

- 停用來自客座端任何對硬體的存取。PCI、USB、FireWire、Thunderbolt、eSata 及其它裝置的穿越機制不但會造成管理上的難題，也常常會仰賴底層的硬體來強制分離客座端。
- 將雲端供應者的私有管理網路與客戶的客座端網路隔開，也將不同客戶的網路隔開，這樣一來：
  - 客座端就無法透過網路存取主機系統。
  - 客戶無法透過雲端供應者的內部網路，直接存取另一位客戶的客座端系統。

2.3. 建議的 RHEV 主機安全性實務

2.3.1. RHEV 網路連接埠

RHEV 使用了多個網路連接埠進行管理，並支援其它虛擬化特性。做為主機的 RHEL 連接埠必須開啓，才能支援 RHEV 的這些功能。以下清單涵蓋了 RHEV 所使用的連接埠及用法：

- 必須允許向內的 ICMP echo 請求，以及向外的 ICMP 回覆。
- 必須開啓連接埠 22（TCP）讓 SSH 存取、並啓始安裝。
- SNMP 需要連接埠 161（UDP）。
- 連接埠 5900 到 65535（TCP）是給客座端主控台透過 SPICE/VNC session 存取用。
- 連接埠 80 或 443（TCP），端視管理程式的安全性設定而定，這是給 *vdsm-reg* 服務交換主機資訊用。
- 連接埠 16514（TLS）或 16509（TCP）是用來支援 libvirt 所產生的遷移通訊用。
- 連接埠 49152 到 49215（TCP）是用來遷移用。根據同時遷移發生的數量，會使用這範圍中的任何連接埠。
- 預設上，*VDSM* 會使用連接埠 54321（TCP）進行管理、儲存與主機之間的通訊用。使用者可以修改這個值。

警告

請特別注意，除非真的需要透過外部來管理裝置，否則請在網路邊界上關閉連接埠 161（UDP）上的 SNMP 通訊。

章 3. 客座端的安全性

3.1. 為何客座端的安全性至關重要

主機系統的安全性極其重要，方能確保其上客座端的安全性；但這並不表示就可以不必注重每台虛擬機器的安全性。任何與傳統、非虛擬化系統有關的安全性風險，同樣存在於虛擬化客座端上。任何存取客座端的資源，例如重要的企業資料或敏感的客戶資訊，都可能因為客座端被攻破而遭到侵害。

3.2. 建議的客座端安全性實務

所有《*Red Hat Enterprise Linux 安全指南*》針對 Red Hat Enterprise Linux 系統所推薦的安全性實務都適用於傳統、非虛擬化的系統，也及於虛擬化客座端上的系統。然而，要在虛擬化環境中執行客座端，有幾個非常重要的安全性實務。

- 客座端的管理工作就如同由遠端進行，請確保管理系統時只透過安全的網路頻道進行。SSH 之類的工具與 TLS 或 SSL 之類的網路通訊協定，皆提供身分認證與資料加密的安全性，確保只有正確的管理者能從遠端管理系統。
- 有些虛擬化技術使用特別的客座端代理程式或驅動程式，以啓用一些虛擬化的特定功能。請確保這些代理程式與應用程式皆使用了標準的 RHEL 安全功能，例如 SELinux。
- 在虛擬化環境中，會有敏感資料被客座端以外存取的風險。請使用 **dm-crypt** 與 **GnuPG** 之類的加密工具來保護敏感性資料；雖然您必須要多花點心思確保加密金鑰的機密性。

注意

使用例如 Kernel Same-page Merging（KSM）的「page deduplication」技術可能會開啓側通道，並造成客座端之間的資訊流出並遭盜取。當有這項問題上的考量時，您可全域停用 KSM，或將特定客座端上的 KSM 停用。有關於 KSM 的詳情請參閱《Red Hat Enterprise Linux 7 虛擬化微調與優化指南》。

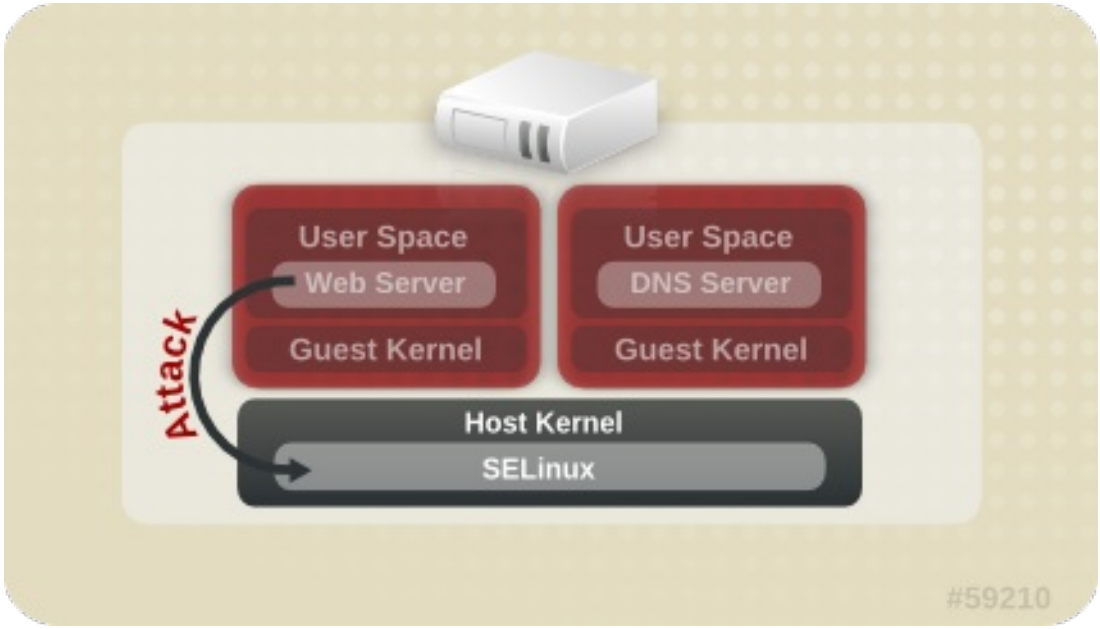
章 4. sVirt

4.1. 簡介

因為 KVM 下的虛擬機器會以 Linux 的程序來運行，因此 KVM 善用了標準 Linux 的安全性模式，以提供隔離與資源控制等功能。Linux kernel 包含了 SELinux（加強安全性的 Linux，Security-Enhanced Linux）－ 由美國國家安全局所開發，透過彈性、可客製化的安全性政策，加入了 MAC（強制性存取控制，Mandatory Access Control）功能、MLS（多層次安全性，multi-level security）與 MCS（多類別安全性，multi-category security）。針對執行於 Linux kernel 上方的程序（包括虛擬機器程序），SELinux 提供了嚴謹的資源隔離與限制。sVirt 專案構築於 SELinux 上，更進一步善用虛擬機器的隔離功能、與受控制的分享功能。舉例來說，使用分類細緻的存取權限，可以將虛擬機器分門別類以存取資源。

從安全性角度來看，hypervisor 對攻擊者來說是極具誘惑力的目標，因為入侵 hyvervisor 之後，便有可能存取主機系統上的所有虛擬機器。整合 SELinux 與虛擬技術之後，有助於加強 hypervisor 的安全性，以避免惡意的虛擬機器試圖存取主機系統、或其它虛擬機器。

請參閱以下圖片，圖片顯示了隔離的客座端，限制了已被入侵的 hypervisor（或客座端）進行更進一步的攻擊，或延展到另一個 instance：



圖形 4.1. 攻擊路徑已被 SELinux 隔離

注意

欲取得更多有關於 SELinux 的相關資訊，請參閱位於〈https://access.redhat.com/site/documentation/〉的《*Red Hat Enterprise Linux SELinux 使用者與管理者指南*》。

4.2. SELinux 與 MAC

SELinux 將 MAC 實作於 Linux kernel 中，它會在檢查了標準的 DAC（無條件存取控制，Discretionary Access Control）之後檢查允許進行的作業。SELinux 可以強制使用使用者自訂的安全性政策，用於執行中的程序及其動作，包括試圖存取檔案系統物件。RHEL 會預設啓用 SELinux，限制住應用程式與系統服務（例如 hypervisor）的弱點所造成的潛在損害範圍。

sVirt 與 libvirt（虛擬管理的萃取層）整合後，可以為虛擬機器提供 MAC 架構。這架構能讓 libvirt 支援的所有虛擬化平台與 sVirt 支援的所有 MAC 實作相互溝通。

4.3. sVirt 配置

SELinux 的布林值是個能切換開或關的變數，可快速啓用或停用一些功能或特殊條件。布林值能透過執行 **setsebool *boolean_name* {on|off}** 進行暫時性的改變，或執行 **setsebool -P *boolean_name* {on|off}** 進行永久性的變更，這項變更在開機之後仍會持續作用。

以下表格顯示了 libvirt 執行 KVM 時，會影響 KVM 的 SELinux 布林值。這些布林值的現有狀況（開或關）可以透過執行 **getsebool -a|grep virt** 找到。

表格 4.1. KVM SELinux 布林值

SELinux 布林值	描述
staff_use_svirt	允許 staff 使用者建立、轉移到 sVirt 網域。
unprivuser_use_svirt	允許沒有特權的使用者建立、轉移到 sVirt 網域。
virt_sandbox_use_audit	允許 sandbox（沙箱）container 發送稽核訊息。
virt_sandbox_use_netlink	允許 sandbox container 使用 netlink 系統呼叫。
virt_sandbox_use_sys_admin	允許 sandbox container 使用 sys_admin 系統呼叫，例如 mount。
virt_transition_userdomain	允許虛擬程序以 userdomain 執行。
virt_use_comm	允許 virt 使用序列埠與平行埠。
virt_use_execmem	允許受限的虛擬客座端使用可執行記憶體與可執行堆疊。
virt_use_fusefs	允許 virt 讀取 FUSE 的掛載檔案。
virt_use_nfs	允許 virt 管理 NFS 所掛載的檔案。
virt_use_rawip	允許 virt 與 rawip 插槽互動。
virt_use_samba	允許 virt 管理 CIFS 所掛載的檔案。
virt_use_sanlock	允許受限的虛擬客座端與 sanlock 互動。
virt_use_usb	允許 virt 使用 USB 裝置。
virt_use_xserver	允許虛擬機器與 X Windows 系統互動。

注意

欲知 SELinux 布林值的更多資訊，請參閱《*Red Hat Enterprise Linux SELinux 使用者與管理者指南*》。

4.4. sVirt 標籤

和其它受 SELinux 保護的服務一樣，sVirt 使用以程序為主的機制、標籤與限制，為客座端提供額外的安全性與控制。根據現有執行中的虛擬機器（動態），標籤會自動套用到系統的資源上；但也可以由系統管理者手動指定（靜態），以符合任何可能存在的特定需求。

4.4.1. sVirt 的標籤類型

以下表格顯示了各種能夠指定給資源的不同 sVirt 標籤（例如虛擬機器程序、映像檔、與共享內容）：

表格 4.2. sVirt 標籤

類型	SELinux Context	描述 / 效用
虛擬機器程序	system_u:system_r:svirt_t:*MCS1*	*MCS1* 是隨機選取的欄位。目前大約支援 500,000 種標籤。
虛擬機器映像檔	system_u:object_r:svirt_image_t:*MCS1*	只有擁有同樣 *MCS1* 欄位的 *svirt_t* 程序可以讀 / 寫這些映像檔與裝置。
虛擬機器共享讀 / 寫內容	system_u:object_r:svirt_image_t:s0	所有 *svirt_t* 程序都可以寫入 *svirt_image_t:s0* 檔案與裝置。
虛擬機器共享的唯讀內容	system_u:object_r:svirt_content_t:s0	透過這個標籤，所有 *svirt_t* 程序都可以讀取檔案與裝置。
虛擬機器映像檔	system_u:object_r:virt_content_t:s0	映像檔存在時所使用的系統預設標籤。若使用此標籤，*svirt_t* 虛擬程序將不允許讀取檔案與裝置。

4.4.2. 動態配置

sVirt 搭配 SELinux 時，動態標籤配置是預設的標籤選項。請參見以下動態標籤的範例：

```
# ps -eZ | grep qemu-kvm

system_u:system_r:svirt_t:s0:c87,c520 27950 ?  00:00:17 qemu-kvm
```

在這範例中，**qemu-kvm** 程序的基礎標籤是 **system_u:system_r:svirt_t:s0**。libvirt 系統已經為這程序產生獨特的 MCS 標籤 **c87,c520**。這基礎標籤與 MCS 標籤合在一起，形成該程序的完整安全標籤。同樣地，libvirt 會以同樣的 MCS 標籤與基礎標籤來形成映像檔標籤。接下來這映像檔標籤會自動套用到所有虛擬機器所需要存取的所有主機檔案，例如磁碟映像檔、磁碟裝置、PCI 裝置、USB 裝置、以及 kernel/initrd 檔案。透過不同的標籤，每個程序皆會與其它虛擬機器隔離開來。

以下範例顯示了虛擬機器的特有安全標籤（此處加上相對應的 MCS 標籤 **c87,c520**），套用到 **/var/lib/libvirt/images** 中的客座端磁碟映像檔：

```
# ls -lZ /var/lib/libvirt/images/*

  system_u:object_r:svirt_image_t:s0:c87,c520   image1
```

以下範例顯示了客座端 XML 配置的動態標籤：

```
<seclabel type='dynamic' model='selinux' relabel='yes'>
  <label>system_u:system_r:svirt_t:s0:c87,c520</label>
  <imagelabel>system_u:object_r:svirt_image_t:s0:c87,c520</imagelabel>
</seclabel>
```

4.4.3. 使用基礎標籤進行動態配置

要在動態模式中覆寫預設的基礎安全標籤，可以手動配置 XML 客座端配置項目中的 **<baselabel>** 選項，如以下範例所示：

```
<seclabel type='dynamic' model='selinux' relabel='yes'>
  <baselabel>system_u:system_r:svirt_custom_t:s0</baselabel>
  <label>system_u:system_r:svirt_custom_t:s0:c87,c520</label>
  <imagelabel>system_u:object_r:svirt_image_t:s0:c87,c520</imagelabel>
</seclabel>
```

4.4.4. 靜態配置搭配動態資源標籤

有些應用程式需要對產生安全標籤進行完整的控制，但仍需要 libvirt 負責資源的標籤。以下客座端 XML 配置示範了靜態配置搭配動態資源標籤：

```
<seclabel type='static' model='selinux' relabel='yes'>
  <label>system_u:system_r:svirt_custom_t:s0:c87,c520</label>
</seclabel>
```

4.4.5. 無資源標籤的靜態配置

無資源標籤的靜態配置是允許的，主要用於 MLS 或受到嚴密控制的環境中。靜態標籤允許管理者選擇特定的標籤，包括 MCS/MLS 欄位，供虛擬機器使用。執行靜態標籤的虛擬機器之管理者需負責設定用於映像檔的正確標籤。虛擬機器皆會以該標籤啓始，sVirt 系統永遠不會修改靜態標籤的虛擬機器之內容。以下客座端的 XML 配置展示了這種情況的範例：

```
<seclabel type='static' model='selinux' relabel='no'>
  <label>system_u:system_r:svirt_custom_t:s0:c87,c520</label>
</seclabel>
```

章 5. 虛擬化環境的網路安全性

5.1. 網路安全性總覽

在大部分情況下，網路是存取系統、應用程式與管理介面的唯一途徑。有鑑於網路在管理虛擬系統、取用虛擬系統的應用程式上扮演如此重要的角色，確保虛擬系統的網路雙向頻道安全，是至關重要的事情。

防護網路能讓管理者控制、保護機密資料不至於外洩或遭到竄改。

5.2. 網路安全性的建議事項

網路安全性乃安全虛擬架構的重要部分。請參閱以下建議事項，以確保網路安全：

- 確保系統上的任何遠端管理工具，皆使用了安全的網路頻道。SSH 之類的工具與 TLS 或 SSL 之類的網路通訊協定，皆提供身分認證與資料加密的安全性，確保對系統的存取是安全、受控制的。
- 確保客座端的應用程式傳送機密資料時，只會透過安全性網路頻道進行。如果無法使用例如 TLS 或 SSL 等通訊協定，請考慮使用 IPsec 之類的通訊協定。
- 配置防火牆，並確保防火牆在開機時會啓動。請只允許系統需要使用、進行管理工作的連接埠連線。請定時測試、檢視防火牆規則。

5.2.1. 連至 Spice 的安全性連線

Spice 遠端桌面通訊協定支援 SSL/TLS，所有 Spice 通訊頻道（主頻道、顯示、輸入、游標、播放、錄影）都應該予以啓用。

5.2.2. 連至儲存裝置的安全性連線

您可以透過多種不同方式將虛擬化系統連上網路的儲存裝置。每種方法都有不同的安全性益處與考量；然而，同樣的安全性原則可以套用在每一種方式上：使用儲存集區前需先經過授權，在傳輸資料前保護資料的機密性與完整性。

儲存資料時也必須確保其安全性。Red Hat 建議在儲存資料之前，先予以加密並（或）賦予數位簽章。

注意

欲取得更多有關於網路儲存的詳細資訊，請參閱《*Red Hat Enterprise Linux 虛擬化建置與管理指南*・*儲存集區*》一章。

附錄 A. 更進一步的資訊

A.1. SELinux 與 sVirt

SELinux 與 sVirt 的更進一步資訊：

- SELinux 的主網站：http://www.nsa.gov/research/selinux/index.shtml。
- SELinux 文件：http://www.nsa.gov/research/selinux/docs.shtml。
- sVirt 主網站：http://selinuxproject.org/page/SVirt。
- Dan Walsh 的部落格：http://danwalsh.livejournal.com/。
- 非官方 SELinux FAQ：http://www.crypt.gen.nz/selinux/faq.html。

A.2. 虛擬化的安全性

虛擬化安全性的更進一步資訊：

- NIST（國家安全暨標準局，National Institute of Standards and Technology）的完整虛擬化安全準則：http://www.nist.gov/itl/csd/virtual-020111.cfm。

附錄 B. 修訂記錄

修訂 1.0-13.2 **Mon Feb 8 2016** **Terry Chuang**
翻譯、校閱完成

修訂 1.0-13.1 **Mon Feb 8 2016** **Terry Chuang**
讓翻譯檔案與 XML 來源 1.0-13 同步

修訂 1.0-13 **Thu Nov 12 2015** **作者：Laura Novich**
準備文件，出版 7.2 GA。

修訂 1.0-12 **Thu Nov 12 2015** **作者：Laura Novich**
準備文件，出版 7.2 GA。

修訂 1.0-11 **Thu Nov 12 2015** **作者：Laura Novich**
準備文件，出版 7.2 GA。

修訂 1.0-10 **Thu Nov 12 2015** **作者：Laura Novich**
準備文件，出版 7.2 GA。

修訂 1.0-9 **Thu Oct 08 2015** **Jiri Herrmann**
已修整修訂紀錄

修訂 1.0-8 **Wed Feb 18 2015** **Scott Radvan**
7.1 GA 發行版本。