Fedora 13

SELinux FAQ

Respuestas a preguntas frecuentes sobre Seguridad Mejorada de Linux

Karsten Wade
Paul W. Frields
Scott Radvan

Resumen

Este FAQ responde a muchas preguntas acerca de Seguridad Mejorada de Linux. La información de este FAQ es valiosa para aquellos que son nuevos en SELinux. Este FAQ, sin embargo, no

está diseñado para proporcionar una cobertura completa de SELinux. Para guías e instrucciones detalladas sobre la comprensión y el uso de SELinux, consulte primero la Guía del Usuario de SELinux y la Guía de Administración de Servicios Confinados. Están disponibles en *http://docs.fedoraproject.org*

Recursos Externos

- Sitio principal de SELinux dela NSA — *http://www.nsa.gov/research/selinux/index.shtml*
- FAQ de SELinux FAQ de la NSA — *http://www.nsa.gov/research/selinux/faqs.shtml*
- Wiki del Proyecto SELinux — *http://selinuxproject.org/*
- Página Wikipedia de SELinux — *http://en.wikipedia.org/wiki/Security-Enhanced_Linux*
- Página de la comunidad SELinux — *http://selinux.sourceforge.net*
- FAQ no oficial de SELinux — *http://www.crypt.gen.nz/selinux/faq.html*
- Política de Referencia — *http://oss.tresys.com/*
- Curso de entrentamiento en el desarrollo de políticas de SELinux — *https://www.redhat.com/training/security/courses/rhs429.html*
- Iniciándose en SELinux — *http://www.linuxtopia.org/online_books/getting_started_with_SELinux/index.html*
- Lista de las clases de objetos de SELinux y los permisos — *http://tresys.com/selinux/obj_perms_help.shtml*
- Lista de correo de Fedora — *mailto:fedora-selinux-list@redhat.com*; lea los archivos o suscríbase en *https://admin.fedoraproject.org/mailman/listinfo/selinux*
- La Guía del Usuario de SELinux y la Guía de Administración de Servicios Confinados en SELinux en *http://docs.fedoraproject.org*
- En IRC - irc.freenode.net, #fedora-selinux y #selinux

1. SELinux

P: ¿Qué es SELinux?

R: SELinux (*Linux de Seguridad Mejorada*, o Security-Enhanced Linux) en Fedora es una implementación del *control de acceso obligatorio* en el kernel de Linux usando el marco de trabajo de los *Módulos de Seguridad de Linux* (MSL). La seguridad estándar de Linux es un modelo de *control de acceso discrecional*.

Control de acceso discrecional (DAC)

DAC es la seguridad estándar de Linux y provee una protección mínima para la ejecución de software dañado o malware a un usuario normal o a root. Los usuarios pueden permitir niveles riesgosos de acceso a sus propios archivos.

Control de Acceso Obligatorio (MAC)
: El MAC provee control total sobre todas las interacciones del software. La política definida administrativamente controla las interacciones del usuario y los procesos con el sistema, y pueden proveer protección de software dañado o malware que se esté ejecutando como de cualquier usuario.

En un modelo DAC, las decisiones de archivo y recursos están basados solamente en la identidad del usuario y la propiedad de los objetos. Cada usuario y cada programa que éste ejecuta tiene discreción completa sobre los objetos del usuario. El software malicioso o inseguro puede hacer cualquier cosa con los archivos y recursos que controla mediante el usuario que inició el proceso. Si el usuario es el superusuario o si la aplicación es **`setuid`** o **`setgid`** a root, el proceso puede tener control a nivel de superusuario de todo el sistema.

Un sistema MAC no sufre de estos problemas. Primero, se puede definir administrativamente una política de seguridad sobre todos los procesos y objetos. Segundo, se puede controlar todos los procesos y objetos, en el caso de SELinux a través del kernel. Tercero, las decisiones se basan en toda la información de seguridad relevante disponible y no sólo en la identidad del usuario autenticado.

MAC bajo SELinux le permite proveer de permisos granulares para todos los *sujetos* (usuarios, programas, procesos) y *objetos* (archivos, dispositivos). En la práctica, imagínese a los sujetos como los procesos, y a los objetos como el destino de una operación hecha por el proceso. Se puede dar en forma segura a un proceso solamente los permisos que necesita para su funcionamiento y nada más.

La implementación de SELinux usa el *control de acceso basado en roles* (RBAC en inglés), que provee control a nivel de usuario abstracto basado en roles, y la *Obligación de Tipos*® (TE en inglés). TE usa una tabla o *matriz* para manejar los controles de acceso, obligando a cumplir reglas de política basándose en los tipos de procesos y objetos. Los tipos de proceso se llaman *dominios* y una referencia cruzada en la matriz del dominio del proceso y los tipos de objeto definen su interacción. Este sistema provee un nivel granular muy detallado en un sistema Linux.

P: ¿Qué es la política de SELinux?

R: La política de SELinux describe los permisos de acceso para todos los sujetos y objetos, es decir, el sistema completo de usuarios, programas y procesos, y los archivos y dispositivos sobre los que estos actúan. La política de Fedora viene en un paquete, con un paquete fuente asociado. Los paquetes actuales de política son:

`selinux-policy-<`*`version`*`>.noarch.rpm`
: Este paquete es común a todos los tipos de política y contiene los archivos de configuración y páginas man. Esto incluye los archivos de interface para el entorno de desarrollo. Esto reemplaza los paquetes -sources del pasado. Este paquete contiene los archivos de interface de la Política de Referencia, junto con un archivo Makefile y una herramienta llamada **`sepolgen`** que se usa para generar un archivo template de política. Los archivos de la interface residen en el directorio **`/usr/share/selinux/devel/include`**. Si quiere ver todos los archivos de política que se usan para construir la Política de Referencia, necesita instalar el .src.rpm.

P: ¿Qué pasó con la política estricta?

R: La política estricta que había en el Linux para Empresas de Red Hat v 5 y en Fedora Core 5 evolucionó a la política destinada en donde los dominios no confinados son eliminados. Esto significa que todos los usuarios deben tener un tipo definido para ellos tales como staff_t o user_t. También, todos los procesos iniciados desde init necesitarían tener una política escrita para ellos. Hasta Fedora Core 9, la política estricta fue eliminada y mezclada con la política destinada.

P: ¿Qué programas son protegidos por la política de SELinux?

R: El número de programas que tienen una política de SELinux definida para ellos está cambiando y evolucionando constantemente. Las versiones distintas de la política tienen más o menos ejecutables cubiertos. Por convención, todos los ejecutables confinados tienen una etiqueta que termina con exec_t. El paquete de herramientas de SELinux (setools) incluye la aplicación seinfo que le permite examinar la política instalada.

```
# seinfo -t | grep exec_t | wc -l
620
```

P: ¿Qué es la Política de Referencia?

R: La *Política de Referencia* es un proyecto mantenido por Tresys Technology (*http://www.tresys.com/*) diseñado para rescribir toda la política de SELinux en una forma que sea más fácil de usar y de entender. Para hacerlo, usa los conceptos de modularidad, abstracción e interfaces bien definida. Vea en *http://oss.tresys.com/* más información sobre la Política de Referencia.

Note que la Política de Referencia no es un tipo nuevo de política. Sino es una nueva base sobre la que se pueden construir las políticas.

P: ¿Qué son los contextos de archivo?

R: Los *contextos de archivo* son usados por el comando **`setfiles`** para generar etiquetas persistentes que describen el contexto de seguridad de un archivo o directorio.

Fedora viene con el script **`fixfiles`**, que da soporte a cuatro opciones: **`check`**, **`relabel`**, **`relabel`** y **`verify`**. Este script permite a los usuarios reetiquetar el sistema de archivo completo sin tener el paquete **`selinux-policy-targeted-sources`** instalado. El uso de lína de comando es más amigable que el comando estándar **`setfiles`**.

P: ¿Cómo veo el contexto de seguridad de un archivo, usuario o proceso?

R: La opción nueva **`-Z`** es el método resumido para mostrar el contexto de un sujeto u objeto:

```
ls -Z archivo.txt
id -Z
ps -eZ
```

P: ¿Qué diferencia hay entre un *dominio* y un *tipo*?

R: No hay diferencia entre dominio y tipo, aunque el dominio se usa a veces para referirse al tipo de un proceso. El uso de dominio de esta forma choca con los modelos de Obligación de Dominio y de Tipo (DTE), donde los dominios y tipos son separados.

P: ¿Qué son los módulos de política?

R: Las políticas de SELinux son modular, lo que significa que hacer un cambio no requiere la fuente de toda la política, modificarla, compilarla y reemplazar la política actual con el compilado nuevo. Esto significa que los desarrolladores externos pueden incluir los módulos de política con sus aplicaciones, y pueden agregarse a la política sin tener que cambiarla entera. El nuevo módulo se agrega entonces al almacén de módulos, dando como resutado un nuevo binario de política que combina la política previa y el nuevo módulo.

Esto sehace separando los pasos compilación y encadenamiento en el procedimiento de construcción de política. Los módulos de política se compilan desde código fuente, y se encadenan cuando se instalan en el almacén de módulos (vea *Managed Policy*). Esta política encadenada se carga luego en el kernel para obligar a cumplirla.

El comando principal para manejar módulos es **`semodule`**, que le permite realizar las funciones básicas tales como la instalación, actualización o eliminación de módulos. Otros comandos útiles incluyen a **`checkmodule`**, que es el compilador de módulos y se instala con el rpm checkpolicy, y **`semodule_package`**, que crea un archivo de paquete de política (.pp) de un módulo de política compilado.

Los módulos son almacenados usualmente en un archivo de paquete de política (extensión .pp) en **`/usr/share/selinux/`*`policyname`*`/`**. En ese lugar, al menos debe encontrar base.pp, que es el módulo base.

Para ver cómo escribir un módulo de política simple, vea en *Local Policy Customizations*.

P: ¿Qué es la política administrada?

R: Hay una biblioteca, **`libsemanage`**, para facilitarle a las herramientas en el espacio del usuario la administración de políticas. Toda la administración de políticas debe usar esta biblioteca para acceder al almacén de políticas. El almacén de políticas guarda toda la información de políticas, y está en **`/etc/selinux/`*`policyname`*`/modules/`**.

Nunca tiene que editar el almacén directamente, debe usar las herramientas que se encadenaron con libsemanage. Una herramienta ejemplo es **`semanage`**, que es una herramienta en modo texto para administrar la mayor parte de la política tales como el mapeo de usuarios de SELinux, los mapeos de puertos de SELinux y las entradas de contextos de archivo. Otros ejemplos de herramientas que usan libsemanage incluyen a **`semodule`** que se usa para administrar los módlos de políticas de SELinux instalados en el almacén de políticas y **`setsebool`** que se usa para administrar los booleanos de la política de SELinux. Además, se están desarrollando herramientas gráficas para usar la funcionalidad provista por libsemanage.

1.2. Control de SELinux

P: ¿Cómo instalo/desinstalo SELinux?

R: El instalador sigue la elección que realiza en la pantalla de **Configuración del Cortafuego**. La política que se ejecuta por defecto es la destinada.

P: Como administrador, ¿qué necesito hacer para configurar SELinux en mi sistema?

R: La respuesta puede ser ¡nada! Hay muchos usuarios de Fedora que ni siquiera se dan cuenta de que están usando SELinux. SELinux le provee protección para sus sistemas con una configuración ya hecha. Dicho esto, hay algunas cosas que un administrador podría querer hacer para configurar sus sistemas. Estas incluyen a:

booleanos
: Los booleanos son configuración del tiempo de ejecución que se pueden cambiar para alterar el comportamiento de la política de SELinux sin tenerque escribir una política nueva. Hay muchos booleanos que se pueden configurar en Fedora, y le permiten configurar SELinux en un detalle muy fino dependiendo de los requerimientos. Para ver los booleanos disponibles y modificar sus valores, use **`system-config-selinux`** o los comandos modo texto **`getsebool`** y **`setsebool`**.

configuración de contextos de archivo personalizables
: Los archivos en un sistema SELinux tienen un contexto de seguridad que se guarda en el atributo extendido del archivo (el comportamiento puede variar en distintos sistemas de archivo, pero así es como funciona en ext3). Estos atributos son puestos por **`rpm`** automáticamente, pero a veces el usuario puede querer tener algún contexto en particular en un archivo. Un ejemplo sería el contexto en un directorio **`html_publico`** para que **`apache`** lo pueda acceder, como se ilustra en *How do I make a user public_html directory work under SELinux*.

  Para una lista de los tipos que se puede asignar a los archivos, vea **`/etc/selinux/targeted/contexts/customizable_types`**. Estos son los tipos comúnmente asignados a archivos de los usuarios y administradores. Para ponerlos, use el comando **`chcon`**. Note que los tipos en **`customizable_types`** también son preservados después de un reetiquetado, por lo que el reetiquetado del sistema no deshará los cambios.

hacer que las bibliotecas que muestran un comportamiento incorrecto funcionen
: Hay muchas bibliotecas por ahí que funcionan mal e intentan romper con las protecciones de memoria que provee SELinux. Estas bibliotecas realmente se deben corregir, por lo que debe informar un error al mantenedor de la biblioteca. Dicho esto, se puede hacer que funcionen. Más información y soluciones para hacer funcionar las bibliotecas se puede encontrar en *I have a process running as unconfined_t, and SELinux is still preventing my application from running*.

P: ¿Como activo/desactivo la protección de SELinux en demonios específicos bajo la política destinada?

R: Use **`system-config-selinux`**, conocido también como la herramienta gráfica de **Administración de SELinux**, para controlar los valores de los booleanos específicos para los demonios servidores. Por ejemplo, si necesita deshabilitar SELinux para Apache, para que funcione correctamente en su entorno, puede deshabilitar el valor en **`system-config-selinux`**. Este cambio desactiva la transición a la política definida en **`apache.te`**, permitiendo a **`httpd`** que quede bajo la seguridad normal del DAC de Linux.

Los comandos **`getsebool`** y **`setsebool`** también se pueden usar, incluso en sistemas quen o tienen la herramienta **`system-config-selinux`**. Por favor, vea en las páginas man de estos comandos: **`getsebool(8)`** y **`setsebool(8)`** más detalles sobre su funcionamiento.

P: En el pasado escribíun archivo fuente de política local.te para mi propia personalización de política, ¿Cómo hago esto ahora?

R: Desde Fedora Core 5, se usa la política modular, por lo que ya no tiene que escribir el fuente completo de la política. Ahora, se puede crear un módulo de política local para su personalización de política. Para esto, siga estos pasos.

1. Cree un directorio temporal y vaya a él.

```
$ mkdir temp
$ cd temp
```

2. Cree archivos vacíos te, if y fc.

```
$ touch local.te local.if local.fc
```

3. Edite el archivo local.te, agregando el contenido apropiado. Por ejemplo:

```
policy_module(local, 1.0)

require {
 attribute httpdcontent;
 type smbd_t;
}

allow smbd_t httpdcontent:dir create_dir_perms;
allow smbd_t httpdcontent:{ file lnk_file } create_file_perms;
```

   Hay 3 partes para este archivo.

   - La llamada al **`policy_module`** inserta sentencias para hacer que funcione el módulo, incluyendo la declaración del módulo y los roles de sistema, clases y permisos requeridos. Asegúrese de que el nombre esté aquí (local en este caso) y que coincida con el nombre que Ud. le dio al archivo (local.te).
   - El bloque **`require`** lista los símbolos que este módulo usa y que se deben declarar en otros módulos. En este caso, se necesita el atributo **`httpdcontent`** y el tipo **`smbd_t`**. Note que todos los tipos y atributos que se usan en roles son necesarios aquí a menos que Ud. los declare más abajo.
   - El resto del archivo es la política, en este caso consta sólo de un par de reglas para permitir acceso. También se pueden poner declaraciones de tipos, sentencias no-auditar, llamadas de interface, o la mayoría de las cosas que pueden ir en un archivo te normal pueden ir aquí.

4. Construir el módulo de política.

```
$ make -f /usr/share/selinux/devel/Makefile
Compliling targeted local module
/usr/bin/checkmodule:  loading policy configuration from tmp/local.tmp
```

```
/usr/bin/checkmodule:  policy configuration loaded
/usr/bin/checkmodule:  writing binary representation (version 5) to tmp/local.mod
Creating targeted local.pp policy package
rm tmp/local.mod.fc tmp/local.mod
```

Note que se usa **checkmodule**, que es parte del rpm checkpolicy. Así que asegúrese de instalar este rpm antes de hacer esto.

5. Vuélvase root e instale el módulo de política con **semodule**.

```
$ su -
Password:
# semodule -i local.pp
```

El módulo está identificado unívocamente por su nombre

Esto significa que si después inserta otro **local.pp**, éste reemplazará al anterior. Por lo que debe debe mantener su archivo **local.te** y agregarle lo que necesite para hacer personalizaciones posteriores a la política. Si lo pierde, pero quiere mantener la política previa, simplemente use un nombre de módulo de política distinto(digamos local2.te).

P: Tengo algunas negaciones avc que me gustaría permitir, ¿cómo hago esto?

R: Si tiene mensajes AVC específicos, se puede usar**audit2allow** para generar un archivo de Obligación de Tipo listo para cargarlo como módulo de política.

```
audit2allow -M local < /tmp/avcs
```

Esto crea un archivo **local.pp** que se puede cargar en el kernel usando **semodule -i local.pp**. Se puede también editar **local.te** para agregar personalizaciones adicionales. Para crear un módulo permitiendo todas las negaciones desde la última reiniciada que podrá luego personalizar,ejecute lo siguiente:to make additional customizations. To create a module allowing all the denials since the last reboot that you can then customize, execute the following:

```
audit2allow -m local -l -i /var/log/messages > local.te
```

Note que para lo anterior se asume que no está usando el demonio audit. Si estuviera usando el demonio audit, entonces debeusar el archivo **/var/log/audit/audit.log** en vez de **/var/log/messages** como el archivo log. Esto genera un archivo **local.te**, que se parece al siguiente:

```
module local 1.0;

require {
        class file { append execute execute_no_trans getattr ioctl read write };
        type httpd_t;
        type httpd_w3c_script_exec_t;
```

```
};


allow httpd_t httpd_w3c_script_exec_t:file { execute execute_no_trans getattr ioctl
 read };
```

Se puede editar a mano este archivo, eliminando las sentencias allow (permitir) indeseadas y luego recompilarlo y recargarlo usando

- **`checkmodule -M -m -o local.mod local.te`** para compilar el archivo.Note que **`checkmodule`** es parte del rpm checkpolicy, por lo que necesita tenerlo instalado.
- **`semodule_package -o local.pp -m local.mod`** para crear un paquete de política.
- **`semodule -i local.pp`** para agregarlo a la política actualmente en ejecución de la máquina. Esto instala un módulo nuevo llamado local con estas reglas en el almacén de módulos.

Importante

Para cargar este paquetede política recién creado al kernel, se necesita que ejecute **`semodule -i local.pp`**

Note que si después instala otro módulo con el nombre local, el nuevo reemplazará el anterior. Si quiere mantener estas reglas, tiene que agregar las personalizaciones futuras a local.te o bien crear un archivo nuevo con un nombre distinto.

P: ¿Cómo puedo ayudar a escribir políticas?

R: Su ayuda es definitivamente apreciada.

- Puede comenzar uniéndose a la lista de correo Fedora SELinux. Puede suscribir y leer los archivos en *https://admin.fedoraproject.org/mailman/listinfo/selinux*.
- El FAQ no oficial tiene alguna información genérica en COMO (HOWTO) sobre cómo escribir políticas genéricas. Vaya a *http://www.crypt.gen.nz/selinux/faq.html* para más información.
- Otro recurso es el COMO sobre Escritura de políticas de SE Linux, ubicado en *http://www.lurking-grue.org/writingselinuxpolicyHOWTO.html*.

También, dado a que la política de Fedora está basada en *Reference Policy*, debe ver también la documentación en la páginadel proyecto. Otra excelente fuente de información son los archivos de políticas ejemplo en **`/usr/share/selinux/devel`**.

Si quiere crear un nuevo dominio de política, puede mirar a los archivos de interface en los subdirectorios de **`/usr/share/selinux/devel`**.

`Facilitando las cosas con sepolgen`

La herramienta **`sepolgen`** es na forma fácil de crear una política de SELinux. El procedimiento siguiente es un ejemplo de cómo usar **`sepolgen`** para crear la política necesaria para un demonio llamado `midemonio`:

```
sepolgen /usr/sbin/midemonio
```

sepolgen hace luego lo siguiente:

1. Busca los templates apropiados en las direcciones /var/lib, /var/run, /etc/init.d/rc.d/ midemonio:

   ```
   rpm -qlf /usr/sbin/midemonio
   ```

2. Busca a syslog, setuid, setgid, etc. y agrega los accesos apropiados:

   ```
   nm -D /usr/sbin/midemonio
   ```

Luego se generan cuatro archivos:

```
midemonio.te - Contiene todos los tipos y reglas para permitir descubiertas para este
 demonio.
midemonio.if - Contiene las interfaces a ser usadas con los tipos generados para este
 demonio.
midemonio.fc - Contiene los mapeos de contextos de archivo entre tipos y direcciones en
 el disco.
midemonio.sh - Es un script de ayuda para compilar/instalar la política y etiquetar los
 directorios correctamente.
```

El escritor de política luego sólo necesita ejecutar **mydaemon.sh** y la política será compilada e instalada - el demonio estará luego listo para probarlo.

El siguiente procedimiento puede ayudarle a entender el proceso de prueba:

```
begin:
        service midemonio start
        run tests against midemonio
        check for AVC messages
        if None
            Break;
        audit2allow -R >> midemonio.te
        Verify the policy is good or fix it.
        ./midemonio.sh
        goto begin
```

P: ¿Cómo cambio la política que estoy usando actualmente?

R:

Tenga cuidado al cambiar la política

A no ser que esté probando una política nueva en una máquina de prueba por razones de investigación, debe considerar seriamente su situación antes de cambiar a una política diferente en un sistema usado en producción. El acto del cambio es simple. El método es seguro, pero debe probarlo primero en un sistema de prueba.

Para usar el método automatizado, ejecute la herramienta **Configuración del Nivel de Seguridad**. Desde el menú del entorno gráfico elija **Escritorio** → **Configuración del Sistema** → **Nivel de Seguridad**, o desde una terminal, ejecute **`system-config-selinux`**. Cambie la política como lo desee y asegúrese de marcar la opción **Reetiquetar en la próxima reiniciada**.

También se pueden hacer estos pasos manualmente con el siguiente procedimiento:

1. Edite el archivo **`/etc/selinux/config`** y cambie el tipo y el modo de la política:

   ```
   SELINUXTYPE=policyname SELINUX=permissive
   ```

   Este paso no asegura que quede bloqueado después de reiniciar. SELinux ejecutará la política correcta, pero no le permitirá ingresar si hay un problema de etiquetado de archivo incorrecto.

2. Ponga al sistema para que se reetiquete todo el sistema de archivo al reiniciar:

   ```
   touch /.autorelabel
   ```

3. Reinicie el sistema. Un reinicio limpio bajo la nueva política permite a todos los procesos del sistema que se inicien en el contexto apropiado, y muestra cualquier problema en el cambio de política.

4. Confirme que sus cambios fueron tomados con el siguiente comando:

   ```
   sestatus -v
   ```

   Con el nuevo sistema ejecutándose en modo **`permisivo`**, busque en **`/var/log/messages`** la cadena **`avc: denied`** en los mensajes. Estos pueden indicar un problema que se necesita resolver para que se ejecute sin problemas bajo la nueva política.

5. Cuando esté satisfecho de que el sistema está funcionando estable bajo la nueva política, ponga en modo obediente cambiando **`SELINUX=enforcing`**. Puede reiniciar o ejecutar **`setenforce 1`** para ponerlo en modo obediente en tiempo real.

P: ¿Cómo se puede respaldar archivos desde un sistema de archivo con SELinux?

R: Ahora se puede usar normalmente **`tar`**, ya no es necesario usar **`star`**. El programa *Bacula*[1] también tiene soporte para las extensiones xattr cuando se usa SELinux, y puede sacar respaldos de sistemas de archivo SELinux.

P: ¿Cómo hago que el directorio del usuario **public_html** funcione bajo SELinux?

R: Este proceso asume que tiene habilitado los directorios HTML públicos de los usuarios en su archivo de configuración de apache, **/etc/httpd/conf/httpd.conf**. Este proceso sólo cubre el servicio de contenido Web estático. Para más información sobre Apache y SELinux, vea la Guía de Administración de Servicios Confinados de SELinux en *http://docs.fedoraproject.org*.

1. Si todavía no tiene un directorio **~/public_html**, créelo y ponga algunos archivos y carpetas en él.

```
cd ~
mkdir public_html
cp /directorio/del/contenido ~/public_html
```

2. En este punto, **httpd** está configuradco para servir los contenidos, pero todavía se recibe el error **403 forbidden**. Esto es porque **httpd** no tiene permitido leer el tipo de seguridad de los archivos dado que está creado en el directorio de inicio del usuario. Cambie el contexto de seguridad de la carpeta y sus contenido con la opción **-R**:

```
ls -Z -d public_html/
drwxrwxr-x unusuario unusuario user_u:object_r:user_home_t public_html
chcon -R -t httpd_user_content_t public_html/ ls -Z -d public_html/
drwxrwxr-x unusuario unusuario user_u:object_r:httpd_user_content_t public_html/
ls -Z public_html/
-rw-rw-r-- unusuario unusuario user_u:object_r:httpd_user_content_t bar.html
-rw-rw-r-- unusuario unusuario user_u:object_r:httpd_user_content_t baz.html
-rw-rw-r-- unusuario unusuario user_u:object_r:httpd_user_content_t foo.html
```

   En un momento posterior se puede ver que el campo de usuario, que ahí aparece como **user_u**, se cambia a **system_u**. Esto no afecta la forma en que funciona la política destinada. El campo que importa es el del tipo.

3. Sus páginas estáticas ahora deben ser servidas correctamente. Si todavía tiene errores, asegúrese de que el booleano que activa los directorios de los usuarios esté activado. Puede activarlo desde **system-config-selinux**. Seleccione la pestaña **SELinux**, y luego seleccione el área **Modificar la Política de SELinux**. Elija **Permitir a HTTPD que lea los directorios de los usuarios**. Los cambios se activan inmediatamente.

P: ¿Cómo desactivo SELinux en el arranque?

R: Ponga **SELINUX=disabled** en **/etc/selinux/config**.

Alternativamente, se puede agregar el parámetro de arranque del kernel **selinux=0**. Sin embargo, esta opción no es recomendada.

Tenga cuidado al deshabilitar SELinux

Si arranca con **`selinux=0`**, cualquier archivo que se crea cuando SELinux está deshabilitado no tiene la información del contexto de SELinux. El sistema de archivo se marca para reetiquetar en la siguiente iniciada. Si un problema inesperado hace que no pueda iniciar normalmente, puede necesitar iniciar en modo rescate monousuario.

P: ¿Cómo activo/desactivo el modo obligatorio en el arranque?

R: Se puede especificar el modo SELinux usando el archivo de configuración **`/etc/sysconfig/selinux`**.

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - No SELinux policy is loaded.
SELINUX=enforcing
# SELINUXTYPE= can take one of these two values:
#       targeted - Only targeted network daemons are protected.
# mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Poniendo el valor a **`enforcing`** es lo mismo que agregar el parámetro de arranque al kernel **`enforcing=1`**. Poniendo el valor **`permissive`** es lo mismo que agregar el parámetro de arranque al kernel **`enforcing=0`**.

Sin embargo, poniendo el valor a **`disabled`** no es lo mismo que la opción de arranque del kernel **`selinux=0`**. En vez de deshabilitar completamente SELinux en el kernel, el valor **`disabled`** desactiva el modo de obediencia y saltea la carga de una política.

Precedencia de la Configuración de SELinux

Los parámetros de la línea de comando del kernel toman precedencia sobre el archivo de configuración.

P: ¿Cómo se desactiva temporalmente el modo de obediencia sin tener que reiniciar?

R: A veces puede necesitar realizar una acción que sería rechazada por la política. Ejecute el comando **`setenforce 0`** para desactivar el modo de obediencia en tiempo real. Cuando termine, ejecute **`setenforce 1`** para volverlo a activar.

P: ¿Cómo se activa/desactiva la auditoría de llamadas al sistema en el arranque?

R: Agurege **`audit=1`** a la línea de comando del kernel para activar la auditoría de llamadas al sistema. Agregue **`audit=0`** a la línea de comando del kernel para desactivar la auditoría de llamadas al sistema.

La auditoría de llamadas al sistema está *activada* por defecto. Cuando está activada, provee información acerca de las llamadas al sistema que se estaban ejecutando cuando se generó un mensaje de **negación** de SELinux. El mensaje de error es útil para depurar la política.

P: ¿Cómo desactivo temporalmente la auditoría de llamadas al sistema sin tener que reiniciar?

R: Ejecute **auditctl -e 0**. Note que este comando no afecta la auditoría de las negaciones AVC de SELinux.

P: ¿Cómo obtengo la información de estado de mi instalación de SELinux?

R: Como root, ejecute el comando **/usr/sbin/sestatus -v**. Para más información, vea en la página de manual de **sestatus(8)**.

P: ¿Cómo escribo la política para permitir a un dominio usar pam_unix.so?

R: Muy pocos dominios en el mundo de SELinux tienen permitido leer el archivo **/etc/shadow**. Hay reglas restrictivas que evitan que los escritores de políticas escriban código como el siguiente

```
allow mydomain_t shadow_t:file read;
```

En el Linux para Empresas de Red Hat 4 se puede usar el comando **unix_chkpwd**. La forma más fácil es usar el atributo **unix_chkpwd**. Por lo que si está escribiendo la política para un demonio ftpd debería escribir algo como lo que sigue

```
daemon_domain(vsftpd, `auth_chkpwd')
```

Esto crearía un contexto donde vsftpd_t -> chkpwd_exec_t -> system_chkpwd_t que puede leer a **/etc/shadow**, mientras que vsftpd_t no puede hacerlo.

En Fedora y el Linux para Empresas de Red Hat 5 y posterior, agregue la regla

```
auth_domtrans_chk_passwd(vsftpd_t)
```

P: He creado un nuevo paquete de política, ¿dónde lo pongo para asegurarme de que se cargó en el kernel?

R: Necesita ejecutar el comando **semodule -i mipol.pp**. Esto modifica la política que esté guardada en la máquina. Su módulo de política está ahora cargado con el resto de la política. Se puede incluso eliminar el archivo .pp del sistema.

semodule -l lista los módulos actualmente cargados.

```
#semodule -i mipol 1.2.1
```

Si después quiere eliminar el paquete de política, se puede ejecutar **semodule -r mipol**.

1.3. Resolviendo Problemas

P: ¿Dónde se guardan los mensajes AVC de SELinux (registros de negaciones, etc.)?

R: Los mensajes están en **`/var/log/messages`** a menos que elija instalar y habilitar el demonio `audit`, en cuyo caso los mensajes AVC se guardarán en **`/var/log/audit/audit.log`**.

P: Mi aplicación no está funcionando como se espera y estoy viendo mensajes **`avc: denied`**. ¿Cómo corrijo esto?

R: Este mensaje significa que la política de SELinux actual no está permitiendo a la aplicación hacer algo. Hay un número de razones por la que puede pasar esto.

Primero, uno de los archivos a los que trata de acceder la aplicación está mal etiquetado. Si el mensaje AVC de refiere a un archivo específico, vea su etiqueta actual con **`ls -alZ /direccion/del/archivo`**. Si parece incorrecto, use el comando **`restorecon -v /direccion/del/archivo`** para restaurar el contexto predeterminado del archivo. Si tiene un número muy grande de negaciones referidas a archivos, puede necesitar usar **`fixfiles relabel`**, o **`restorecon -R /direccion`** para reetiquetar el directorio y su contenido.

Las negaciones son aveces debidas a cambios en la configuración del programa que provocó el mensaje de negación. Por ejemplo, si cambia a Apache para que escuche en el puerto 8800, también debe cambiar la política de seguridad, **`apache.te`**.

Si está teniendo problema en hacer que alguna aplicación específica como Apache funcione, vea en *How to use system-config-selinux* más información sobre cómo deshabilitar el modo de obediencia sólo para esa aplicación.

P: ¿Por qué SELinux no da la dirección completa en un mensaje de error?

R: Para responder esto, primero examine la estructura de un mensaje de error AVC típico de SELinux. Los items a observar en este ejemplo están en **`negrita`**:

```
node=equipo.ejemplo.com.ar type=AVC msg=audit(12/13/2006 11:28:14.395:952) : avc:
 denied { getattr } for pid=7236 comm=vsftpd name=public_html dev=dm-0 ino=9601649
 scontext=system_u:system_r:ftpd_t:s0 tcontext=system_u:object_r:httpd_sys_content_t:s0
 tclass=dir

node=equipo.ejemplo.com.ar type=SYSCALL msg=audit(12/13/2006 11:28:14.395:952) :
 arch=i386 syscall=lstat64 success=no exit=0
a0=8495230 a1=849c830 a2=874ff4 a3=328d28 items=0 ppid=7234 pid=7236 auid=dwalsh
 uid=dwalsh gid=dwalsh euid=dwalsh suid=dwalsh fsuid=dwalsh egid=dwalsh
 sgid=dwalsh fsgid=dwalsh tty=(none) comm=vsftpd exe=/usr/sbin/vsftpd
 subj=system_u:system_r:ftpd_t:s0 key=(null)
```

Este mensaje AVC consta de dos registros, el registro de **`AVC`** actual y el registro de **`SYSCALL`** o llamada a sistema actual. El kernel genera estos dos registros cuando el sistema SELinux niega el acceso. Este mensaje AVC indica que SELinux negó a **`/usr/sbin/vsftpd`** hacer **`getattr`** en un **`dir`** llamado **`public_html`**.

`Pero, ¿qué directorio public_html es el que tiene el problema?`

Los registros AVC por si mismo no muestran la dirección completa del directorio public_html con problema. Esto fue hecho así por razones de performance. Dado a que los mensajes AVC pueden ocurrir infrecuentemente, haciendo que el kernel informe la dirección completa no se considera que valga la pena por la sobrecarga que implica. Los registros AVC sin embargo, sí incluyen el dispositivo (**dm-0**) y el nodoi en cuestión (**9601649**). Puede usar esta información de nodo i y de dispositivo para encontrar la información de la dirección correcta y si el archivo o directorio todavía existe.

La forma lenta:

```
# find / -inum 9601649
```

Una forma mejor:

Las herramientas de *setroubleshoot* pueden usar el comando the **locate** para intentar reconstruir la dirección en cuestión:

```
# locate -r /public_html$

/home/dwalsh/public_html
/home/obama/public_html
...(continúa)
```

luego *setroubleshoot* usa **stat** para sacar el nodo i de cada archivo devuelto y lo compara con los valores del mensaje AVC; si coinciden, analiza la dirección completa. Por supuesto, necesita tener el paquete *mlocate* para obtener estas direcciones.

Vea en *http://danwalsh.livejournal.com/34903.html* más detalles sobre este tema.

P: He instalado un sistema con una partición **/home** preexistente, y ahora no puedo ingresar. ¿Qué puedo hacer?

R: Su partición **/home** no está etiquetada correctamente. Puede corregirlo fácilmente de dos maneras diferentes.

Si solamente quiere reetiquetar recursivamente **/home**:

```
/sbin/restorecon -v -R /home
```

Si solamente quiere asegurarse que no hay otros archivos incorrectamente etiquetados, puede reetiquetar todo el sistema de archivo:

```
/sbin/fixfiles relabel
```

Debe tener instalado el paquete **policycoreutils** para usar **fixfiles**.

P: Después de reetiquetar mi directorio **/home** usando **setfiles** o **fixfiles**, ¿Todavía puedo leer **/home** con un sistema sin SELinux habilitado?

R: Puede leer los archivos desde una distribución que no tenga SELinux, o que tenga SELinux deshabilitada. Sin embargo, los archivos creados por esos sistemas no tendrán el contexto de seguridad, ni los archivos que elimine y que vuelva a crear. Esto puede ser un desafío con los archivos como los de **~/.bashrc**. Puede tener que reetiquetar **/home** cuando reinicie con Fedora con SELinux habilitado.

P: ¿Cómo comparto directorios usando NFS entre Fedora y otros sistemas que no tienen SELinux?

R: Dado a que NFS soporta transparentemente muchos tipos de sistemas de archivo, se puede usar para compartir directorios entre sistemas con y sin SELinux.

Cuando monte un sistema de archivo que no tiene SELinux vía NFS, por defecto SELinux trata todos los archivos en ese lugar compartido como que tienen el contexto **nfs_t**. Puede cambiar este contexto predeterminado manualmente, usando la opción **context=**. El siguiente comando hace que los archivos en el directorio NFS montado aparezcan como que tienen el contexto **system_u:object_r:tmp_t** en SELinux:

```
mount -t nfs -o context=system_u:object_r:tmp_t servidor:/compartido/eldir /mnt/eldir
```

Cuando SELinux exporta un archivo vía NFS, los archivos recién creados tienen el contexto del directorio donde fueron creados. En otras palabras, la presencia de SELinux en la máquina remota no tiene efecto en los contextos de seguridad local.

P: ¿Cómo puedo crear una cuenta nueva de usuario Linux con directorio de inicio del usuario?

R: Se puede crear su usuario nuevo con el comando estándar **useradd**. Primero debe convertirse en `root`.

Para la política destinada:

```
su - root
id -Z
root:system_r:unconfined_t
useradd unusuario
ls -Z /home
drwx------ unusuario unusuario root:object_r:user_home_dir_t /home/unusuario
```

El contexto inicial para un directorio de usuario nuevo tiene la identidad de **root**. El reetiquetado subsiguiente del sistema de archivo cambia la identidad a **system_u**. Estos son funcionalmente iguales, dado que el rol y el tipo son idénticos (**object_r:user_home_dir_t**.)

P: El comando **su** cambia mi identidad y rol SELinux?

R: El comando **su** realiza una transición completa del dominio y cambia su rol. Esto es más fácil que usar el comando **newrole** dado a que éste último requiere que iongrese dos contraseñas - una par identificar al usuario, y otra para identificarse como root.

Otras formas de cambios de identidad de Linux/UNIX®, por ejemplo **`setuid(2)`**, no provocan un cambio de identidad de SELinux.

P: Tengo problemas con errores **`avc`** que están llenando mis registros para un programa en particular. ¿Cómo eligo no auditar esos accesos?

R: Si lo que quiere es no auditar mensajes **`dmesg`**, por ejemplo, póngalo en su archivo **`dmesg.te`**:

```
dontaudit dmesg_t userdomain:fd { use };
```

Esto elimina la salida de error a la terminal para todos los dominios de usuarios, incluyendo `user`, `staff` y `sysadm`.

P: Aún en modo permisivo, Todavía obtengo una cantidad muy grande de mensajes **`avc denied`**.

R: En modo no obediente, debe igualmente recibir *más* mensajes que en modo obediente. El kernel registra cada acceso negado como si estuviera en modo obediente. Dado a que no está restricto por la obligación de la política, puede realizar más acciones, lo que resulta en más errores de negación registrados.

Si una aplicación que estaba corriendo en modo obediente tiene el acceso denegado para un número de archivos en un directorio, se detiene una sola vez al comienzo de la acción. En modo no obediente, la aplicación no es detenida al leer todo el árbol del directorio, y eso genera un mensaje de negación por cada archivo leído en el directorio.

P: Obtengo una negación de permiso específico sólo cuando SELinux está en modo obediente, pero no veo ningún mensaje en **`/var/log/messages`** (o **`/var/log/audit/audit.log`** si estoy usando el demonio audit). ¿Cómo puedo identificar la causa de estas negaciones silenciosas?

R: La razón más común de una negación silenciosa es cuando la política contiene una regla explícita **`dontaudit`** que suprime los mensajes de auditoría. La regla **`dontaudit`** se usa a menudo de esta forma cuando un mensaje benigno está llenando los registros de auditoría.

Para ver una negación en particular, habilite la auditoría de todas las reglas **`dontaudit`**:

```
semodule -b /usr/share/selinux/targeted/enableaudit.pp
```

La salida cuando `dontaudit` está habilitado es muy larga

La habilitación de la auditoría de todas las reglas **`dontaudit`** producirá una cantidad muy grande de información de auditoría, la mayor parte será irrelevante para su negación.

Use esta técnica sólo si está buscando específicamente un mensaje de auditoría para una negación que parece ocurrir sileciosamente. Debería reactivar las reglas **`dontaudit`** lo más pronto posible.

Una vez que ha encontrado el problema, puede resetear al modo predeterminado ejecutando

```
semodule -b /usr/share/selinux/targeted/base.pp
```

P: ¿Por qué no veo la salida cuando ejecuto ciertos demonios en modo depuración o interactivo?

R: SELinux deshabilita intencionalmente el acceso a los dispositivos tty para evitar que los demonios se comuniquen con la terminal que los controla. Esta comunicación es potencialmente un agujero de seguridad debido a que esos demonios podrían insertar comandos en la terminal controlante. Un programa roto o comprometido podría usar este agujero para causar serios problemas.

Hay algunas formas por las cuales se puede capturar la salida desde los demonios. Un método es entubar la salida al comando cat.

```
snmpd -v | cat
```

Cuando se depura un demonio, puede desear deshabilitar la transición del demonio a su dominio específico. Puede hacerlo con **`system-config-selinux`** o con **`setsebool`** en la línea de comando.

Una opción final es deshabilitar el modo obediente mientras depura. Emita el comando **`setenforce 0`** para desactivar el modo obediente y use el comando **`setenforce 1`** para reactivar SELinux cuando termine de depurarlo.

P: Cuando actualizo el paquete de política (por ejemplo, usando **`yum`**), ¿qué pasa con la política? ¿Se actualiza automáticamente?

R: La política se recarga a si mismo cuando el paquete es actualizado. Este compartamiento reemplaza el trabajo manual **`make load`**.

En ciertas situaciones, puede necesitar reetiquetar todo el sistema de archivo. Esto puede ocurrir debido a una corrección de error en SELinux en donde los contextos de archivo se volvieron inválidos, o cuando la actualización de la política realiza cambios al archivo **`/etc/selinux/targeted/contexts/files/file_contexts`**.

Después que el sistema de archivo es reetiquetado, no se necesita reiniciar con **`reboot`**, pero es útil para asegurar que todos los procesos y programas se ejecuten en el dominio apropiado. Esto depende mucho de los cambios en la política actualizada.

Para reetiquetar tiene varias opciones. Puede usar el comando **`fixfiles`**:

```
fixfiles relabel && reboot
```

O puede usar el mecanismo **`/.autorelabel`**:

```
touch /.autorelabel && reboot
```

P: Si la política que viene con el paquete de una aplicación cambia de una forma que necesita reetiquetar, ¿RPM reetiquetará los archivos que pertenecen al paquete?

R: Si. Los contextos de seguridad de los archivos que corresponden al paquete se almacenan en los datos cabecera del paquete. Los contextos de archivo se ponen directamente después de la copia **cpio**, como si fuera que se estuvieran poniendo en los archivos en el disco.

P: ¿Por qué los binarios de las políticas distribuidas con Fedora, como por ejemplo **/etc/selinux/<*policyname*>/policy/policy.<*version*>**, y aquellos que compilo yo tienen distintos tamaños y chequeos de suma MD5?

R: Cuando instala un paquete de política, los archivos binarios precompilados de la política se ponen directamente en **/etc/selinux**. Los entornos de construcción diferentes harán que los archivos destino tengan tamaños diferentes y chequeos de suma MD5 distintos.

P: ¿Los paquetes de política nuevos deshabilitarán mi sistema?

R: Hay una posibilidad de que lso cambios en el paquete de política o en la política que viene en el paquete de una aplicación pueda causar errores, más negaciones u otros comportamientos desconocidos. Puede descubrir qué paquete causó la ruptura revirtiendo la política y los paquetes de la aplicación de una vez. Si no quiere volver al paquete previo, la versión más vieja de los archivos de configuración se guardarán con la extensión **.rpmsave**. Use las listas de correo, bugzilla y el IRC para obtener ayuda sobre el problema. Si e anima, escriba o corrija la política para resolver su problema.

P: Mi consola se está llenando de mensajes. ¿Cómo los desactivo?

R: Para volver a tener el control, desactive los mensajes del kernel a la consola con este comando:

```
dmesg -n 1
```

P: ¿Puedo probar la política por defecto sin instalar los fuentes de la política?

R: Se puede probar la política predeterminada de SELinux instalando los paquetes **selinux-policy-*policyname*** y **policycoreutils**. Sin los fuentes de la política instalado, el comando **fixfiles** automatiza el reetiquetado del sistema de archivo.

El comando **fixfiles relabel** es equivalente a **make relabel**. Durante el reetiquetado, se borrarán todos los archivos de **/tmp**, para limpiar los archivos que pudieran tener las etiquetas de contexto de archivo viejas.

Otros comandos son **fixfiles check**, que verifica los archivos mal etiquetados y **fixfiles restore**, que corrige los archivos mal etiquetados, pero no borra los archivos de **/tmp**. El comando **fixfiles** command no toma una lista de directorios como argumento, porque reetiqueta todo el sistema de archivo. Si necesita reetiquetar un directorio específico, use **restorecon**.

P: ¿Por qué algunas de mis aplicaciones KDE tienen problema en SELinux?

R: Los ejecutables de KDE siempre aparecen como **kdeinit**, que limita lo que puede hacerse mediante la política de SELinux. Esto es debido a que todas las aplicaciones de KDE se ejecutan en el dominio de **kdeinit**.

Los problemas pueden surgir cuando se instala SELinux debido a que no es posible reetiquetar **/tmp** y **/var/tmp**. No hay un buen método de determinar qué archivo debe tener qué contexto.

La solución es salir de KDE y borrar todos los archivos temporales de KDE:

```
rm -rf /var/tmp/kdecache-<usuario> rm -rf /var/tmp/<other_kde_files>
```

En el siguiente ingreso, su problema debería estar resuelto.

P: ¿Por qué **SELINUX=disabled** no funciona para mí?

R: Tenga cuidado de los espacios en blanco en el archivo **/etc/sysconfig/selinux**. El código es muy sensible a los espacios en blanco, incluso al final de la línea.

P: Tengo un proceso que se ejecuta como **unconfined_t**, y SELinux todavía evita que se ejecute.

R: Se ha comenzado a confinar el dominio **unconfined_t** de alguna forma. SELinux restringe ciertas operaciones de protección de memoria. La siguiente es una lista de esas negaciones, así como las posibles causas y soluciones a las mismas. Para más información sobre estas restricciones, vea *http://people.redhat.com/drepper/selinux-mem.html*.

Estas se muestran en **/var/log/messages** (o **/var/log/audit/audit.log** si usa el demonio audit) como negaciones avc. Estos también pueden aparecer cuando se ejecutan programas con errores como

```
error while loading shared libraries: /usr/lib/libavutil.so.49:
cannot restore segment prot after reloc: Permission denied
```

Lo que indica que la biblioteca está tratando de realizar una reubicación del programa y ha fallado. Las reubicaciones de programa son malos, y se pueden permitir con el primer consejo de abajo. Más abajo están los permisos de memoria que SELinux niega, así como consejos sobre cómo tratarlos.

execmod

Este es normalmente basado en una etiqueta de la biblioteca. Puede cambiar el contexto de la biblioteca de forma permanente con los siguientes comandos

```
# /usr/sbin/semanage fcontext -a -t textrel_shlib_t '/usr/lib/libavutil.so.49.0.0'
# /sbin/restorecon -v /usr/lib/libavutil.so.49.0.0
```

con la biblioteca en particular que falla en lugar de **/usr/lib/libavutil.so.49.0.0**. Ahora, su aplicación se debería poder ejecutar. Por favor, informe este error en *http://bugzilla.redhat.com*.

execstack

Intente **execstack -c *BIBLIOTECA***. Ahora pruebe su aplicación de nuevo. Si la aplicación funciona ahora, la biblioteca fue marcada incorrectamente como que necesita **execstack**. Por favor, informe este error en *http://bugzilla.redhat.com*.

execmem, execheap

Se provee un booleano para cada uno de estos errores de chequeos de memoria. Por lo que si necesita ejecutar una aplicación que necesita alguno de estos permisos, puede poner el booleano allow_exec* en 1 para corregir el problema. Por ejemplo, si intenta ejecutar una aplicación y recibe un mensaje AVC que contenga una falla **execstack**. Puede activar el Booleano con:

```
setsebool -P allow_execstack=1
```

P: ¿Qué significan estos errores de rpm?

R:

```
restorecon reset /etc/modprobe.conf context system_u:object_r:etc_runtime_t-
>system_u:object_r:modules_conf_t
restorecon reset /etc/cups/ppd/homehp.ppd context user_u:object_r:cupsd_etc_t-
>system_u:object_r:cupsd_rw_etc_t
```

Durante el proceso de actualización, el paquete de selinux ejecuta restorecon con la diferencia entre los contextos de archivos de la política instalada y los nuevos contextos de la política a instalar. Esto mantiene los contextos de archivos correctos en el disco.

```
libsepol.sepol_genbools_array: boolean hidd_disable_trans no longer in policy
```

Esto indica que la política actualizada ha eliminado el booleano de la política.

P: Si quiere ejecutar un demonio en un puerto no estándar, pero SELinux no lo permite. ¿Cómo se hace funcionar esto?

R: Puede usar el comando **semanage** para definir los puertos adicionales. Digamos que desea que httpd escuche en el puerto 8082. Podría ingresar el comando.

```
semanage port -a -p tcp -t http_port_t 8082
```

P: ¿Se está escribiendo un script PHP que necesita crear archivos y posiblemente ejecutarlos. La política de SELinux está negando esto. ¿Qué se debe hacer?

R: Primero, nunca debería permitir que un servicio del sistema ejecute algo que pueda ser escrito por él. Esto dá al atacante la posibilidad de subir código malicioso y luego ejecutarlo, lo que realmente se quiere evitar.

Si solamente necesita permitir a su script crear archivos (no ejecutables), esto es posible.
Se debería evitar que las aplicaciones del sistema escriban al directorio **/tmp**, dado que los

usuarios tienden también a usar el directorio **/tmp**. Sería mejor crear un directorio en otro lugar que pueda pertenecer solamente al proceso apache y permitir al script escribir en el. Debe etiquetar el directorio con **httpd_sys_script_rw_t**, lo que permitirá a apache leer y escribir archivos en ese directorio. Este directorio debería ubicarse en algún lugar al que apache pueda acceder (even **$HOME/public_html/**).

P: Estoy configurando el intercambio a un archivo, pero veo mensajes AVC en mis archivos log.

R: Necesita identificar el archivo de intercambio con SELinux poniendo su contexto de archivo a **swapfile_t**.

```
chcon -t swapfile_t ARCHSWAP
```

P: Por favor, explique los permisos **relabelto**/**relabelfrom**.

R: Para archivos, **relabelfrom** significa "¿puede el dominio D reetiquetar un archivo de (i.e. actualmente con el) tipo T1?" y **relabelto** significa "¿Puede el dominio D reetiquetar un archivo con el tipo T2?", por lo que ambos chequeos se aplican cuando se reetiqueta un archivo, donde T1 es el tipo original y T2 es el tipo nuevo especificado por el programa.

Documentos útiles a consultar:

- Resumen de clases de objetos y permisos por Tresys *http://tresys.com/selinux/obj_perms_help.shtml*
- Implementación de SELinux como un informe técnico LSM (describe los chequeos de permisos sobre la base de los enlaces) *http://www.nsa.gov/selinux/papers/module-abs.cfm*. Este está también disponible en el paquete selinux-doc (y más actualizado ahí).
- Integración del Soporte Flexible para las Políticas de Seguridad en el Sistema Operativo Linux - informe técnico (describe el diseño original y la implementación, incluyendo tablas resumen de las clases, permisos y qué chequeos de permisos se aplican a qué llamadas del sistema. No está totalmente actualizado con la implementación actual, sin embargo es un buen recurso). *http://www.nsa.gov/selinux/papers/slinux-abs.cfm*

1.4. Despliegue de SELinux

P: ¿Qué sistemas de archivo se puede usar para SELinux?

R: El sistema de archivo debe dar soporte a las etiquetas **xattr** en el espacio de nombre *security.** apropiado. Además de ext2/ext3/ext4, XFS agregó recientemente el soporte para las etiquetas necesarias.

Note que el soporte SELinux de XFS se rompió en las versiones de kernel de Linux en desarrollo 2.6.14 y 2.6.15, pero se corrigió (con un atajo) en la versión 2.6.16. Su kernel debe ser de esta versión o posterior para poder usar XFS con SELinux.

P: ¿Cómo impacta SELinux en la performance del sistema?

R: Esto es algo difícil de medir, y es muy dependiente de la configuración personalizada y uso del sistema que está usando SELinux. La última vez que se midió, el impacto en la performance fue

del 7% para código completamente genérico. Los cambios siguientes en los componentes del sistema tales como la red seguramente empeorarán el impacto en algunos casos. La mejora en la performance de SELinux continúa siendo una prioridad del equipo de desarrollo.

P: ¿Qué tipos de despliegues, aplicaciones y sistemas se puede mejorar con SELinux?

R: Inicialmente, SELinux se usó en servidores con salida a Internet que estén realizando unas pocas funciones especializadas, donde es crítico mantener una seguridad máxima. Los administradores típicamente eliminan de ese equipo todo el software y servicios extra, y corren unos cuantos servicios. Un servidor web o de correo es un buen ejemplo.

En estos servidores, se puede bloquear la política al máximo. El menor número de interacciones con otros componentes hace que este bloqueo sea más fácil. Un sistema dedicado corriendo una aplicación de tercero especializada es también un buen candidato.

En el futuro, SELinux será destinado a todos los entornos. Para conseguir esto, la comunidad y *los fabricantes de software independientes* (FSIs) deberán trabajar con los desarrolladores de SELinux para producir las políticas necesarias.

P: ¿Cómo afecta SELinux a las aplicaciones de terceros?

R: Un objetivo de la implementación de la política destinada de SELinux en Fedora es para permitir a las aplicaciones de terceros funcionar sin modificaciones. La política destinada es transparente para las aplicaciones no contempladas y termina funcionando como la seguridad DAC estándar de Linux. Estas aplicaciones, sin embargo, no se ejecutarán de una manera extrasegura. Ud. o algún otro proveedor deberá escribir una política para proteger estas aplicaciones son seguridad MAC.

Es imposible predecir cómo funcionarán las aplicaciones de terceros con SELinux, aún cuando se ejecuta con la política destinada. Quizás pueda resolver algunos problemas cambiando la política. Podrá observar que SELinux saca a la luz cuestiones de seguridad desconocidas de su aplicación. Puede ser que tenga que modificarla para que funcione bajo SELinux.

Note que con el agregado de *Policy Modules*, ahora es posible que desarrolladores externos incluyan módulos de políticas con su aplicación. Si Ud. es un desarrollador externo o mantenedor de paquete, por favor, considere incluir un módulo de política en su paquete. Esto le permitirá asegurar el comportamiento de su aplicación con el poder de SELinux para cualquier usuario que instale su paquete.

Un valor importante que introducen los testeadores y usuarios de Fedora a la comunidad es la prueba extensiva de aplicaciones de terceros. Con esto en mente, por favor, acérquenos sus experiencias a la lista de correo apropiada, tal como la lista fedora-selinux, para discutirla. Para más información sobre esta lista, vaya a *https://admin.fedoraproject.org/mailman/listinfo/selinux*.