Monitorización de Configuraciones con RANCID

Carlos Vicente/José A. Domínguez
Servicios de Red
Universidad de Oregón

Necesidad

- Problemas causados por cambios de configuración
  - ¿Qué cambio exactamente?
    - Deja ver si todavía lo tengo en el buffer de mi xterm
    - “Nadie cambió nada”. -- Ya, seguro...
  - ¿En qué momento exacto cambió?
- Historial de cambios
  - ¿Cómo recupero la configuración que tenía hace dos meses?
  - Diferencias incrementales

Necesidad

- Recuperación de desastres
  - Después de un problema de hardware
  - Al hacer una actualización
  - En general, tan fácil como copiar y restaurar
- Notificación de cambios
  - Por e-mail
  - Al grupo más interesado, preferiblemente
  - Mientras más frecuentemente, mejor.

RANCID: *Really Awesome New Cisco Config Differ*

- Disponible en http://www.shrubbery.net/rancid/
- Diseñado inicialmente para enrutadores Cisco, pero ahora soporta muchos otros tipos y fabricantes:
  - Juniper, Foundry, Extreme, Redback, Alteon, HP Procurve, Force10, etc.
- Operación básica
  - Descarga la configuración del equipo (comandos show)
  - *Reajusta* la información
    - Quita información sensible (passwords)
    - Quita las partes móviles e incrementales
  - Compara la información con la última copia guardada
  - Notifica los cambios
  - Guarda la nueva versión en un sistema de control de versiones
    - CVS o Subversion

Rancid: Grupos

- Rancid organiza los dispositivos en grupos administrativos. Esto permite distribuir las notificaciones al grupo apropiado solamente.
  - Frecuentemente, las organizaciones tienen distintos equipos humanos gestionando las distintas tecnologías:
    - Enrutadores (capa 3)
    - Switches, Access Points, etc. (capa 2)
  - Si es un departamento pequeño, puede bastar con un solo grupo

Ejemplo

En este caso, se quitó una tarjeta Gigabit Ethernet.

```
From: rancid <rancid@example.com>
To: rancid-example@example.com
Subject: example router config diffs
Precedence: bulk

Index: configs/dfw.example.com
===================================================================
===
retrieving revision 1.144
diff -u -4 -r1.144 dfw.example.com
@@ -57,14 +57,8 @@
  !Slot 2/MBUS: hvers 1.1
  !Slot 2/MBUS: software 01.36 (RAM) (ROM version is 01.33)
  !Slot 2/MBUS: 128 Mbytes DRAM, 16384 Kbytes SDRAM
  !
- !Slot 6: 1 Port Gigabit Ethernet
- !Slot 6/PCA: part 73-3302-03 rev C0 ver 3, serial CAB031216OL
- !Slot 6/PCA: hvers 1.1
- !Slot 6/MBUS: part 73-2146-07 rev B0 dev 0, serial CAB031112SB
- !Slot 6/MBUS: hvers 1.2
- !Slot 6/MBUS: software 01.36 (RAM) (ROM version is 01.33)
  !Slot 7: Route Processor
  !Slot 7/PCA: part 73-2170-03 rev B0 ver 3, serial CAB024901SI
  !Slot 7/PCA: hvers 1.4
  !Slot 7/MBUS: part 73-2146-06 rev A0 dev 0, serial CAB02060044
@@ -136,11 +130,8 @@
  boot system flash slot0:
  logging buffered 32768 debugging
  no logging console
  enable secret 5 $1$73Y1$grXuRjuZxfSiLYv1sBRUz0
```

Requisitos

- Lenguaje Expect
  - http://expect.nist.gov/
- Subversion
  - Reemplaza a CVS
  - http://subversion.tigris.org/
  - Libro http://svnbook.red-bean.com/
- Apache
  - Para acceder a los repositorios via web
- ViewVC
  - Provee una interfaz web, con posibilidad de acceder a distintas versiones
  - Sitio web http://www.viewvc.org/

Instalación

- Descargar el paquete

```
apt-get install rancid-core rancid-cgi rancid-util
```

- Directorios

```
Binarios: /usr/lib/rancid/bin

Configuración: /etc/rancid

Trabajo: /var/lib/rancid

Logs: /var/log/rancid
```

- Usuario

```
rancid
```

Configuración

- Editar el archivo de configuración

```
# vi /etc/rancid/rancid.conf
```

- Agregar los grupos necesarios y especificar que queremos usar *Subversion (SVN)* y *no CVS*

```
LIST_OF_GROUPS="routers switches"

RCSSYS=svn
```

- Crear un archivo .cloginrc en el directorio del usuario que va a ejecutar Rancid `(/var/lib/rancid)`
  - `Editar este archivo con los datos necesarios para que Rancid pueda conectarse a los equipos`
  - `Ver ejemplos en /usr/share/doc/rancid-core/examples/cloginrc.sample`

Parametros de Configuración

add password <nombre_router|expresión> <clave_acceso> <clave_enable>

add user <nombre_router|expresión> <usuario>

El usuario por defecto es $USER (e.g.: el usuario que corre clogin).

add userprompt <nombre_router|expresioó> <mensaje_usuario>

Lo que el enrutador imprime para preguntar por el nombre de usuario.

Por defecto: {"(Username|login|user name):"}

add userpassword <nombre_router|expresión> <clave_usuario>

La clave para el usuario si es diferente del password que se configuró

con 'add password'.

Parametros de Configuración

add passprompt <nombre_router|expresión> <mensaje_password>

Lo que el enrutador imprime para preguntar por la clave de acceso.

Por defecto: {"(\[Pp]assword|passwd):"}

add method <nombre_router|expresión> {ssh} [...]

Define en que orden y cuales métodos de acceso se utilizarán para conectarse

a un dispositivo, seleccionado de las opciones {ssh,telnet,rsh}.

eg: add method * {ssh} {telnet} {rsh}

intentará una conexión ssh primero. Si ssh falla con conexión negada (no

debido a una clave equivocada), entonces trata telnet y despues rsh.

Por defecto: {telnet} {ssh}

Parametros de Configuración

add noenable <nombre_router|expresion>

Equivalente a usar -noenable en la linea de comandos. No habilita enable

cuando accesa el dispositivo.

add enableprompt <nombre_router|expresion> <mensaje_enable>

Lo que el router despliega cuando pregunta por el password de enable.

Por defecto: {"\[Pp]assword:"}

add enauser <nombre_router|expresioó> <nombre_usuaurio>

Esto es solo necesarion si el dispositivo requiere un nombre de usuario cuando se quiere cambiar a modo enable y el nombre es diferente del usuario que se uso para accesar al dispositivo.

add autoenable <nombre_router|expresión> <1/0>

Utilizado si el proceso de accesar automaticamente te pone en modo enable.

Parametros de Configuración

add cyphertype <nombre_router|expresión> <tipo_encripción_ssh>

Por defecto: 3des.

add identity <nombre_router|expresion> <camino_a_archivo_identidad>

Por defecto: es el archivo de identidad de ssh.

include <nombre_archivo>

incluye un archivo .cloginrc secundario

Nuestra Configuración

- Como root hacer

  su - rancid

- Crear .cloginrc con:

  # todos los enrutadores

  add password * {”walc08"} {walc08}

  add method * telnet

- Cambiar el acceso para .cloginrc

  chmod 700 .cloginrc

Configuración

- Como root, agregar los aliases correspondientes para recibir las notificaciones

```
# vi /etc/aliases
    rancid-routers: walc
    rancid-admin-routers: walc
    rancid-switches: walc
    rancid-admin-switches: walc
# newaliases
```

Configuración

- Crear los directorios y archivos de configuración que estarán bajo control de versiones

```
# su - rancid
# /usr/lib/rancid/bin/rancid-cvs
```

- Agregar los nombres de los equipos en el archivo *router.db* de cada grupo

```
# vim routers/router.db
# vim switches/router.db
El formato es <router>:<fabricante>:<up|down>
Ejemplo: router.domain.com:cisco:up
```

Pruebas

- Probar que las credenciales son correctas

  `bin/clogin <nombre del router>`

- Probar todos los dispositivos configurados, manualmente

  - `bin/rancid-run`

- Revisar si hay errores en los logs (logs/*)

  - FAQ de Rancid: http://www.shrubbery.net/rancid/FAQ
  - FAQ de Subversion: http://subversion.tigris.org/faq.html

- Repetir hasta que no haya errores

- La última configuración debe econtrarse bajo:

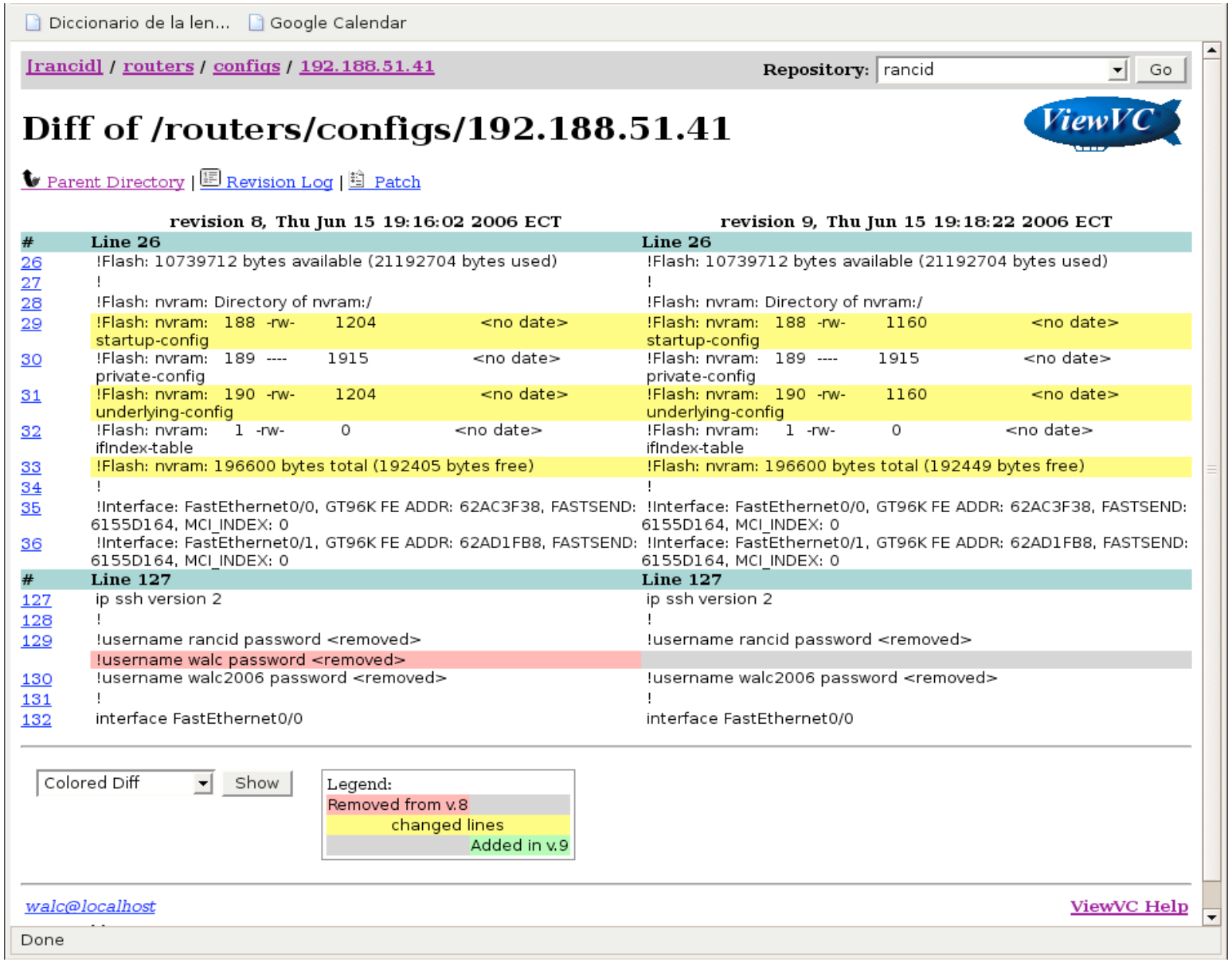
  `/var/lib/rancid/<grupo>/configs/`

Automatización

- Crear una entrada en *cron* para hacer las revisiones periódicamente
  - Dependiendo de la cantidad de dispositivos, Rancid necesitará más o menos tiempo para revisar todas las configuraciones (este ejemplo chequea cada 10 minutos

```
# su – rancid
# crontab -e
0,10,20,30,40,50 * * * * /usr/lib/rancid/bin/rancid-run routers
0,10,20,30,40,50 * * * * /usr/lib/rancid/bin/rancid-run switches
50 23 * * * /usr/bin/find /var/lib/rancid/logs -type f -mtime +2 -exec rm {} \;
```

ViewVC


Diccionario de la len...
Google Calendar
[rancid] / routers / configs / 192.188.51.41
Repository: rancid
Go
Diff of /routers/configs/192.188.51.41
ViewVC
Parent Directory | Revision Log | Patch
revision 8, Thu Jun 15 19:16:02 2006 ECT
revision 9, Thu Jun 15 19:18:22 2006 ECT
Line 26
Line 26
26 !Flash: 10739712 bytes available (21192704 bytes used)
27 !
28 !Flash: nvram: Directory of nvram:/
29 !Flash: nvram: 188 -rw- 1204 <no date> startup-config
30 !Flash: nvram: 189 ---- 1915 <no date> private-config
31 !Flash: nvram: 190 -rw- 1204 <no date> underlying-config
32 !Flash: nvram: 1 -rw- 0 <no date> ifIndex-table
33 !Flash: nvram: 196600 bytes total (192405 bytes free)
34 !
35 !Interface: FastEthernet0/0, GT96K FE ADDR: 62AC3F38, FASTSEND: 6155D164, MCI_INDEX: 0
36 !Interface: FastEthernet0/1, GT96K FE ADDR: 62AD1FB8, FASTSEND: 6155D164, MCI_INDEX: 0
!Flash: 10739712 bytes available (21192704 bytes used)
!
!Flash: nvram: Directory of nvram:/
!Flash: nvram: 188 -rw- 1160 <no date> startup-config
!Flash: nvram: 189 ---- 1915 <no date> private-config
!Flash: nvram: 190 -rw- 1160 <no date> underlying-config
!Flash: nvram: 1 -rw- 0 <no date> ifIndex-table
!Flash: nvram: 196600 bytes total (192449 bytes free)
!
!Interface: FastEthernet0/0, GT96K FE ADDR: 62AC3F38, FASTSEND: 6155D164, MCI_INDEX: 0
!Interface: FastEthernet0/1, GT96K FE ADDR: 62AD1FB8, FASTSEND: 6155D164, MCI_INDEX: 0
Line 127
Line 127
127 ip ssh version 2
128 !
129 !username rancid password <removed>
!username walc password <removed>
130 !username walc2006 password <removed>
131 !
132 interface FastEthernet0/0
ip ssh version 2
!
!username rancid password <removed>
!username walc2006 password <removed>
!
interface FastEthernet0/0
Colored Diff
Show
Legend:
Removed from v.8
changed lines
Added in v.9
walc@localhost
ViewVC Help
Done

Instalación de ViewVC

- Requisitos:
  - Languaje Python: http://www.python.org/
  - enscript: http://www.codento.com/people/mtr/genscript
- Instalación:

```
# apt-get install viewvc
```

- Configuración

```
# vi /etc/viewvc/viewvc.conf
    svn_roots = rancid: /var/lib/rancid/CVS
    default_root = rancid
    address = <a href="mailto:walc@localhost.localdomain">walc@localhost</a>
```

- Cambiar permisos

```
# chown -R rancid:www-data /var/lib/rancid/CVS
```

Apache y ViewVC

- Crear los siguientes enlaces

```
# vi /etc/apache2h/httpd.conf
ScriptAlias /rancid /usr/lib/cgi-bin/viewvc.cgi
```

- Reiniciar el servidor web

```
# /etc/init.d/apache2 reload
```

- Probar el acceso

  http://localhost.localdomain/rancid