

# Seguridad y Hardening en Servidores Linux

Alex Callejas  
Technical Account Manager  
Noviembre 2014

# Agenda

- Qué queremos proteger?
- Instalación endurecida
- Post instalación
- Administración segura del sistema
- Control de acceso
- Servicios seguros
- Preparándonos para el desastre

# Qué queremos proteger?

Disponibilidad

Confidencialidad

Integridad

# Instalación Endurecida

donde todo comienza!

# Seguridad física y control de acceso

- Si existe acceso físico al equipo, tenemos un punto crítico de falla
- Acceso al servidor
  - ✓ Rack
  - ✓ Acceso físico y control de acceso
- Proteger el BIOS/UEFI
  - ✓ Prevención de modificaciones
  - ✓ Evita el boot no autorizado
- Deshabilitar periféricos no utilizados
- Fuentes redundantes
- RAID

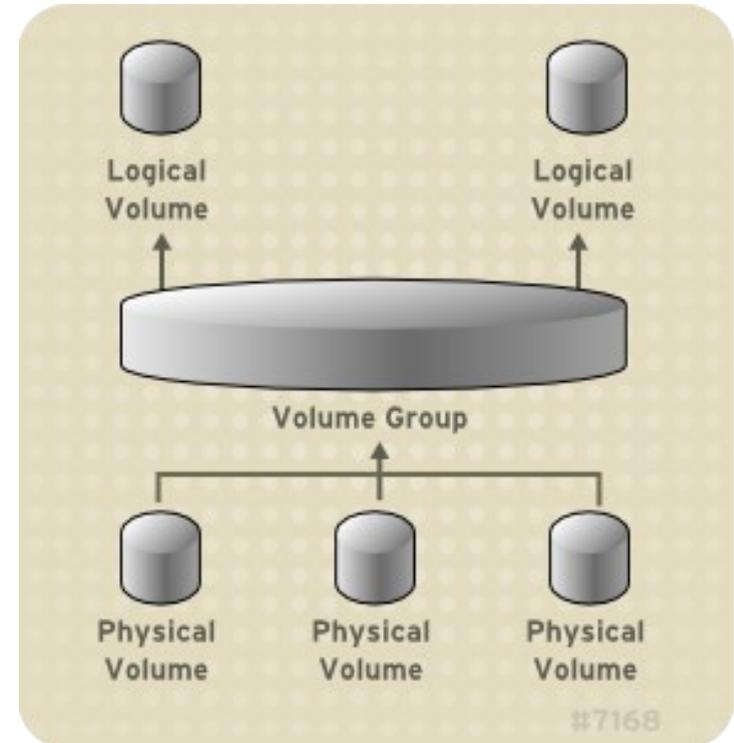


# Instalación: Mejores prácticas

- Tipo de instalación
  - ✓ Minimal/Basic
- Particionamiento
  - ✓ Planeación
    - Reduce el tiempo de acceso a datos
    - Facilita la recuperación ante desastres
    - Minimiza los problemas por disponibilidad de espacio en disco
- Swap
  - ✓ Analizar el caso de uso

# Instalación: Mejores prácticas

- **Use LVM!**
  - ✓ A demanda
- /boot
  - ✓ kernel, GRUB
  - ✓ Sin encriptación
  - ✓ Contraseña en GRUB
- /home
  - ✓ Sólo datos de usuario
- /var/tmp y /tmp
  - ✓ Archivos temporales
  - ✓ No se almacenan durante un largo periodo



# Post Instalación

Ya puedo entrar en producción?

# Actualización del Sistema

- Actualización completa del sistema
  - ✓ `yum update`
- Revisión de erratas
  - ✓ `yum check-update --security`
- Instalación de erratas
  - ✓ `yum update --security`

# Prevenir combinación de reinicio

```
[root@server ~]# cp /etc/init/control-alt-delete.conf  
/etc/init/control-alt-delete.override
```

```
[root@server ~]# vi /etc/init/control-alt-  
delete.override
```

...

```
exec /bin/true
```

```
[root@server ~]#
```

# Limitar información sobre el equipo

- Modificar `/etc/banner` y `/etc/banner.issue`

Este sistema es para el uso exclusivo de usuarios autorizados, por lo que las personas que lo utilicen estarán sujetos al monitoreo de todas sus actividades en el mismo. Cualquier persona que utilice este sistema permite expresamente tal monitoreo y debe estar consciente de que si este revelara una posible actividad ilícita, el personal de sistemas proporcionara la evidencia del monitoreo al personal de seguridad, con el fin de emprender las acciones civiles y/o legales que correspondan.

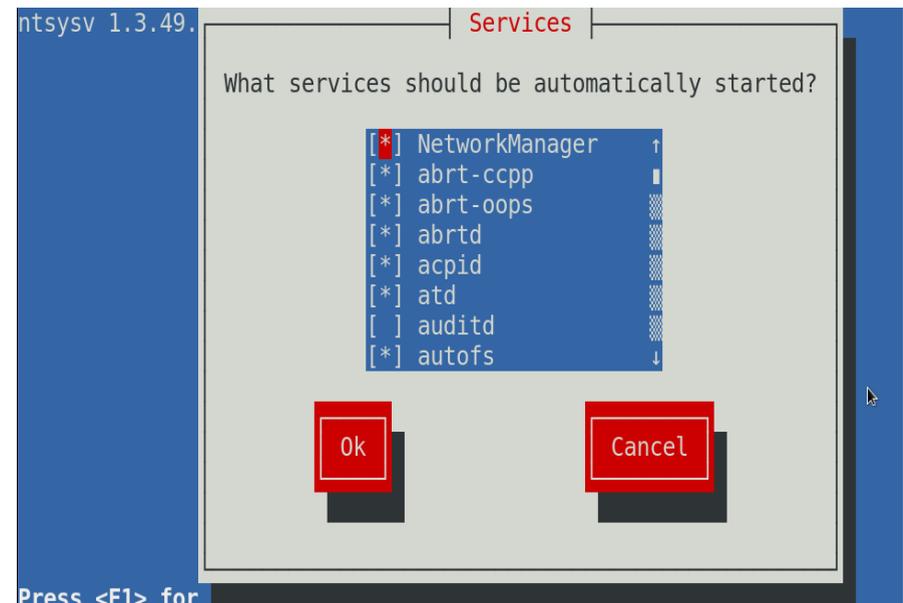
- `/etc/motd`

- ✓ Política de uso de información y del sistema

# Servicios: Cuáles deben estar activos?

- Sólo los necesarios!

- ✓ ntsysv
- ✓ chkconfig
- ✓ systemctl



```
# systemctl list-unit-files
```

```
# systemctl disable httpd
```

```
root@server:~ 72x3
[root@server ~]# chkconfig sshd --list
sshd          0:off  1:off  2:on   3:on   4:on   5:on   6:off
[root@server ~]#
```

# Servicios: performance y seguridad

- ✓ ps, netstat
- ✓ top, htop, nmon
- ✓ lsof, pgrep
- ✓ systemtap

```
root@server:~ 94x33
nmon-14g Hostname=server Refresh= 2secs 00:37.42
CPU Utilisation
-----+-----+-----+-----+-----+
CPU  User%  Sys%  Wait%  Idle|0          |25          |50          |75          |100|
 1   0.0   0.0   0.0 100.0|          >          |          |          |          |
-----+-----+-----+-----+-----+
Memory Stats
-----+-----+-----+-----+-----+
Total MB      RAM      High      Low      Swap      Page Size=4 KB
Free MB       3517.5   -0.0     -0.0   3968.0
Free Percent  91.8%   100.0%  100.0%  100.0%
MB           MB           MB           MB
Buffers=     7.7 Swapcached= 0.0 Inactive =  87.2
Dirty  =     0.0 Writeback = 0.0 Mapped  =   7.0
Slab   =    67.1 Commit_AS = 77.6 PageTables= 1.6
-----+-----+-----+-----+-----+
Network I/O
-----+-----+-----+-----+-----+
I/F Name Recv=KB/s Trans=KB/s packin packout insize  outside Peak->Recv Trans
  lo      0.0     0.0     0.0     0.0     0.0     0.0     0.0     0.0     0.0
 eth0    0.1     0.1     1.0     0.5    59.0    242.0    24.3    307.1
-----+-----+-----+-----+-----+
Disk I/O ---/proc/diskstats--- mostly in KB/s---Warning:contains duplicates---
DiskName Busy  Read WriteKB|0          |25          |50          |75          |100|
vda      0%    0.0   0.0|          >          |          |          |          |
vda1     0%    0.0   0.0|          >          |          |          |          |
vda2     0%    0.0   0.0|          >          |          |          |          |
dm-0     0%    0.0   0.0|          >          |          |          |          |
dm-1     0%    0.0   0.0|          >          |          |          |          |
Totals  Read-MB/s=0.0      Writes-MB/s=0.0      Transfers/sec=0.0
-----+-----+-----+-----+-----+
```

# Limitar recursos

- Limitar el acceso como root a las terminales
  - ✓ `/etc/securetty`
- Forzar el logout de los usuarios
  - ✓ `.bashrc` ó `/etc/profile`
    - `TMOUT=360`
- Limitar el acceso a los recursos
  - ✓ `/etc/security/limits.conf`



# Administración Segura del Sistema

Cómo aplica los parches de seguridad?

# Equipo de Respuesta a Incidentes de Seguridad Infomática

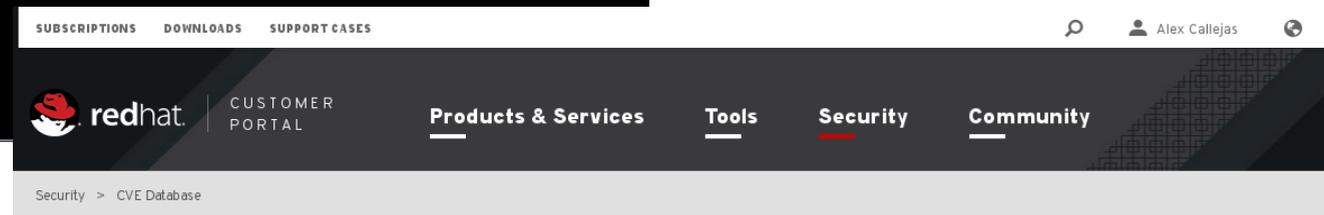
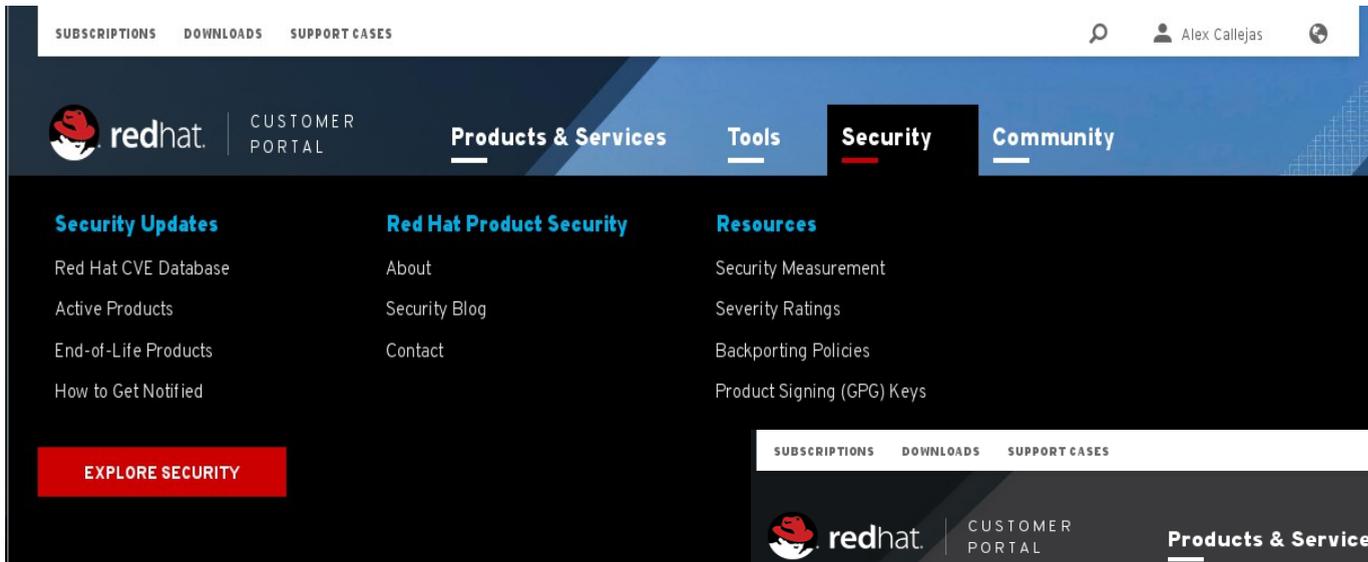


- **CERT**

<http://www.cert.org.mx/index.html>

- Publica información respecto a vulnerabilidades de seguridad y alertas de la misma índole
  - Realiza investigaciones sobre productos afectados y sus contramedidas
- 
- **Publicación de erratas**
    - ✓ Severidades
    - ✓ Impactos
    - ✓ CVE (Common Vulnerabilities and Exposures)

# Red Hat CVE Database



## Impacto:

- ✓ Crítico
- ✓ Importante
- ✓ Moderado
- ✓ Bajo

**CVE DATABASE**

### Red Hat vulnerabilities by CVE name

The Common Vulnerabilities and Exposures (CVE) project, maintained by [The MITRE Corporation](#), is a list of standardized names for vulnerabilities and security exposures.

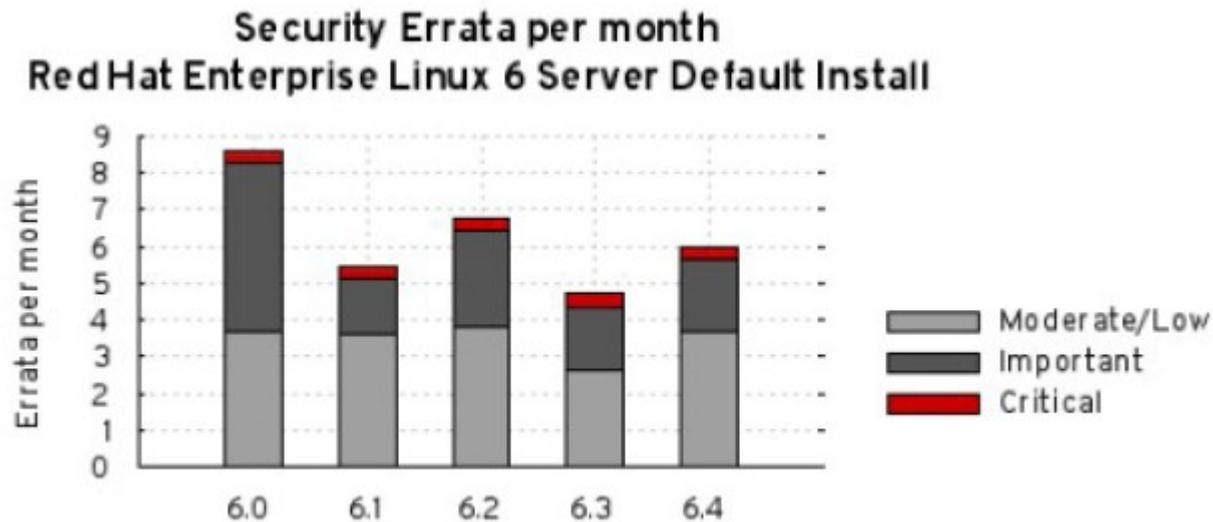
2014 | 2013 | 2012 | 2011 | 2010 | 2009 | 2008 | 2007 | 2006 | 2005 | 2004 | 2003 | 2002 | 2001 | 2000 | 1999

Show 10 entries

CVE	Synopsis	Impact	Public Date
<a href="#">CVE-2014-0001</a>	Buffer overflow in client/mysql.cc in Oracle MySQL and MariaDB before 5.5.35 allows remote database servers to cause a denial of service (crash) and possibly execute arbitrary code via a long server version string.	Moderate	2014-01-30
<a href="#">CVE-2014-0002</a>	The XSLT component in Apache Camel before 2.11.4 and 2.12.x before 2.12.3 allows remote attackers to read arbitrary files and possibly have other unspecified impact via an XML document containing an external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue.	Moderate	2014-02-28
<a href="#">CVE-2014-0003</a>	The XSLT component in Apache Camel 2.11.x before 2.11.4, 2.12.x before 2.12.3, and possibly earlier versions allows remote attackers to execute arbitrary Java methods via a crafted message.	Important	2014-02-28
<a href="#">CVE-2014-0004</a>	Stack-based buffer overflow in udisks before 1.0.5 and 2.x before 2.1.3 allows local users to cause a denial of service (crash) and possibly execute arbitrary code via a long mount point.	Important	2014-03-10

# Erratas

- Red Hat Security Advisory (RHSA)
- Red Hat Bug Fix Advisory (RHBA)
- Red Hat Enhancement Advisory (RHEA)



# YUM Security plugin - instalación

```
[root@server ~]# yum -y install yum-plugin-security
```

```
[root@server ~]# cat /etc/yum/pluginconf.d/security.conf
```

```
[main]
```

```
enabled=1
```

```
[root@server ~]#
```

# YUM Security plugin – verificación de erratas

```
[root@server ~]# yum updateinfo
Updates Information Summary: available
  4 Security notice(s)
    2 Important Security notice(s)
    2 Moderate Security notice(s)
  7 Bugfix notice(s)
  4 Enhancement notice(s)
updateinfo summary done
[root@server ~]#
```

# YUM Security plugin – verificación de erratas

- Lista de paquetes

```
[root@server ~]# yum updateinfo list
```

- Lista de paquetes que solucionan errata

```
[root@server ~]# yum updateinfo list --advisory=RHSA-2014:1843
```

- Detalle de errata

```
[root@server ~]# yum updateinfo RHSA-2014:1843
```

- Verificación de CVE

```
[root@server ~]# yum updateinfo list --cve=CVE-2014-3185
```

# Administración de actualizaciones

- Aplicación actualizaciones
  - × La mayor parte de los ataques ocurren con software no actualizado
- Monitoreo post actualización
- Administración de cambios
- Factibilidad

A screenshot of the Red Hat Satellite web interface showing the "Errata Relevant to Your Systems" page. The page displays a list of errata with columns for Type, Advisory, Synopsis, Systems, and Updated. The interface includes a navigation menu, a search bar, and a filter by synopsis section.

Type	Advisory	Synopsis	Systems	Updated
Security	RHBA-2014:1804	java-1.6.0-openjdk bug fix update	57	11/4/14
Security	RHBA-2014:1799	initscripts bug fix update	82	11/3/14
Security	RHBA-2014:1734	yum-rhn-plugin bug fix update	82	10/29/14
Security	RHSA-2014:1764	Moderate: wget security update	63	10/29/14
Security	RHSA-2014:1767	Important: php security update	8	10/29/14
Security	RHBA-2014:1730	scl-utils bug fix and enhancement update	60	10/28/14
Enhancement	RHEA-2014:1733	tzdata enhancement update	82	10/28/14
Enhancement	RHEA-2014:1718	qemu-kvm enhancement update	15	10/26/14
Security	RHBA-2014:1719	tuned bug fix update	62	10/26/14
Security	RHBA-2014:1720	libvirt bug fix update	49	10/26/14
Security	RHBA-2014:1678	watchdog bug fix update	4	10/21/14
Security	RHBA-2014:1672	libipathverbs bug fix update	1	10/20/14
Security	RHSA-2014:1676	Moderate: wireshark security update	2	10/20/14

# Control de acceso

**Tenga el control de la administración del sistema**

# Firewall

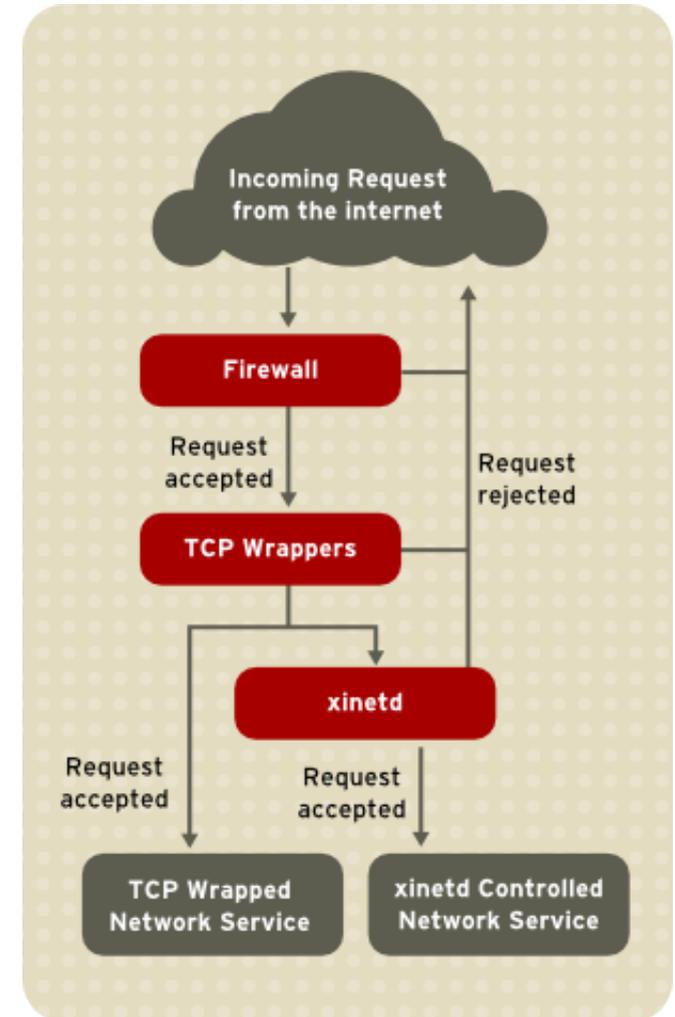
- Sirve como separación entre su red e internet
- Permite el uso legítimo de la red
- Previene el tráfico no autorizado al servidor (malicioso)
- `iptables`
  - ✓ Evaluación
  - ✓ Búsqueda de normas existentes
- Identificar las necesidades de protección
- Definición de estrategia



# TCP Wrappers

- Herramienta que permite o niega el acceso a servicios
  - ✓ Utiliza la librería Libwrap
  - ✓ Archivos de control:
    - `/etc/hosts.allow`
    - `/etc/hosts.deny`
  - Usar en conjunto con firewall

```
sshd: client1.example-rh.com : allow  
sshd: client1.example-rh.com : deny
```



# Control de acceso

- MAC (Mandatory Access Control)
  - ✓ **SELinux** (Security-Enhanced Linux)
  - ✓ Por defecto en RHEL

<http://stopdisablinglinux.com/>

- DAC (Discretionary Access Control)
  - ✓ `chmod`
  - ✓ `chattr`
- ACL
  - ✓ `filesystem`



# Control de acceso

- Permisos especiales
  - SUID, SGID, sticky bit
- Atributos
  - `chattr`, `lsattr`

- Revisar directorios con permisos especiales

```
[root@server ~]# find / -type f -perm 1000 -ls
```

- `sudo`
  - `sudosh`

# Auditoria: Use audit!

- Mecanismo de monitoreo de información relevante para la seguridad, basado en reglas predefinidas
- audit no proporciona ningún nivel de seguridad adicional
- Los eventos se almacenan en logs
- Es útil para la evaluación de violaciones a las políticas de seguridad y las actividades realizadas en el sistema
- Los posibles violaciones se pueden evitar con medidas preventivas conforme al análisis de logs

# Auditoria: Política de login/contraseñas

## chage

```
root@server:~ 73x9
[root@server ~]# chage -l angel
Last password change           : Nov 12, 2014
Password expires               : never
Password inactive              : never
Account expires                : never
Minimum number of days between password change : 0
Maximum number of days between password change : 99999
Number of days of warning before password expires : 7
[root@server ~]#
```

## /etc/login.defs

```
PASS_MAX_DAYS 99999
PASS_MIN_DAYS 0
PASS_MIN_LEN 5
PASS_WARN_AGE 7
LOGIN_RETRIES 5
LOGIN_TIMEOUT 60
```

# Seguridad en el almacenamiento de datos

- **Backup!**

- Estrategia

- ✓ Storage, cinta...
- ✓ Calendarización
- ✓ Software
  - ♦ Bacula
  - ♦ Amanda



# Servicios Seguros

Puntos de atención, riesgos y amenazas

# Servicios – algunos riesgos

- Servicios inseguros
  - x Denial of Service (DoS)
  - x Distributed Denial of Service (DDoS)
  - x Buffer overflow
  - x Remote script execution



# Servicios: SSH

- **Mantenerlo actualizado!**
- Restringir el uso
- **Indispensable** para SysAdmins



```
/etc/ssh/sshd_config
```

```
Port 22
```

```
Protocol 2
```

```
PermitRootLogin no
```

```
LoginGraceTime 60
```

```
PermitEmptyPasswords no
```

```
Allow users tux linus
```

```
Banner /etc/issue
```

- **Use Llaves!**
  - ✓ ssh-keygen
  - ✓ ssh-copy-id

# Servicios: FTP

- VSFTP (Very Secure FTP)
- Alternativas:
  - ProFTP, Pure-ftp, etc...
- **Mantener actualizado!**
- Enjaular (**chroot**)
- Analizar caso de uso
  - Usuarios
  - Cuota
  - Upload/Download



# Servicios: vsftpd

- Configurar banner
  - `ftpd_banner=FTP Server`
- Deshabilitar login anónimo
  - `anonymous_enable=NO`
- Permitir que los usuarios suban archivos
  - `write_enable=YES`
- Delimitar usuarios
  - `userlist_enable=YES`
  - `userlist_file=/etc/vsftpd.allowed_users`
- Enjaular usuarios
  - `chroot_local_user=YES`

# Servicios: vsftpd

- **Control del acceso**

- ✓ `/etc/ftpusers`

- **Prevenir DoS**

- › `ls_recurse_enable=NO`
  - › `max_clients=200`
  - › `max_per_ip=4`

- **FTP con SSL**

- › `ssl_enable=YES`
  - › `allow_anon_ssl=NO`
  - › `force_local_data_ssl=NO`
  - › `force_local_logins_ssl=NO`
  - › `ssl_tlsv1=YES`
  - › `ssl_sslv2=NO`
  - › `ssl_sslv3=NO`
  - › `rsa_cert_file=/etc/vsftpd/vsftpd.pem`



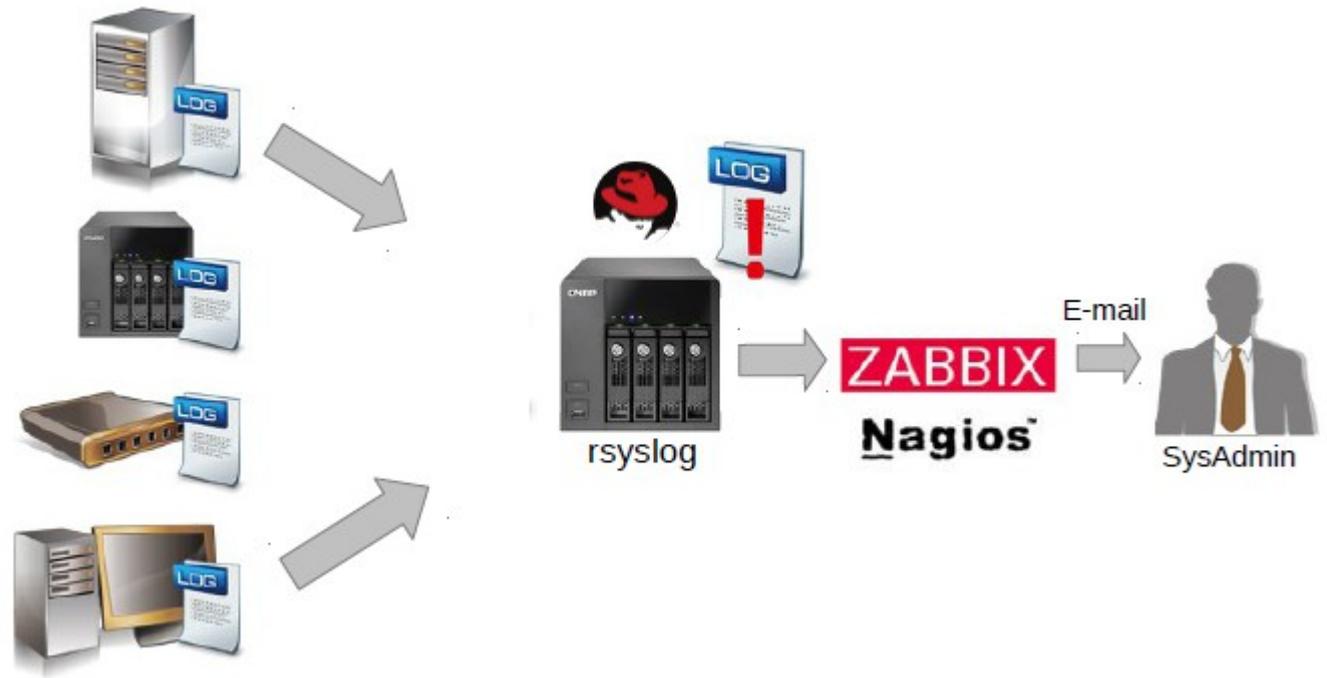
# Servicios: web server

- **Mantenerlo actualizado!**
- Agregar soporte a conexiones encriptadas
- Analizar el uso de modulos de seguridad
  - `mod_security`, `mod_evasive`, `mod_access`, `mod_authz`
- Analizar el caso de uso
- Probar las configuraciones antes de aplicar en producción
  - `apachectl configtest`
  - `apachectl graceful`
- Restringir acceso
  - `.htaccess` y `htpasswd`



# Syslog centralizado

- rsyslog
- rsyslog-gnutls
- logrotate



# Tuneame el kernel

- Evitar SYN ATACK que causa negación de servicio (DoS)
  - ✓ `/proc/sys/net/ipv4/tcp_syncookies`
- Engañar el “OS guessing” en scans
  - ✓ `/proc/sys/net/ipv4/ip_default_ttl`
- Bloquear ICMP (ping)
  - ✓ `/proc/sys/net/ipv4/icmp_echo_ignore_all`
- Ignorar broadcast
  - ✓ `/proc/sys/net/ipv4/icmp_echo_ignore_broadcasts`
- Deshabilitar IPV6
  - ✓ `/proc/sys/net/ipv6/conf/all/disable_ipv6`

# Preparándonos para el desastre

## Planificando contingencias y continuidad

# BIA - Business Impact Analysis

- ¿Cuánto tiempo puede detenerse producción en caso de un incidente?
- ¿Cuál es el impacto del tiempo de inactividad en el negocio?
- ¿Cuáles son los requisitos mínimos para volver a la normalidad?
- ¿Hay contingencia?
- En caso de desastre, ¿cuanto es el tiempo minimo necesario para regresar a la normalidad?

# Plan de Contingencia

- Ciclo de vida PDCA (plan-do-check-act)
- Análisis de riesgo
  - Identificar amenazas
- Plan Contingencia
  - ✓ Plan de respaldo
  - ✓ Plan de emergencia
  - ✓ Plan de recuperación



# DRP – Plan de Recuperación de Desastres



# DRP – BCP

- **Backup!**
- Capacitación
- Monitoreo
- Medios alternos
  - kickstart, snapshot, clonezilla





**Gracias**



redhat.