Seguridad y Hardening

en servidores Linux

Alex Callejas
Senior Technical Support Engineer
December 2019

Red Hat

Alex Callejas

Senior Technical Support Engineer @Red Hat

@dark_axl

/rootzilopochtli

www.rootzilopochtli.com

Geek by nature, Linux by choice, Fedora of course!

Red Hat

Consideraciones Iniciales

- Esta sesión es una plática, no una lectura
- Hablaremos sobre tuercas y tornillos, sin comerciales, a menos que ustedes lo sugieran
- Esta presentación es realizada con fines **estrictamente** educativos
- La mala ejecución puede dar como resultado la pérdida de datos y poner en duda las capacidades mínimas necesarias para el desempeño de la labor asignada
- El presentador se deslinda de cualquier responsabilidad sobre las decisiones tomadas como resultado de esta presentación

Red Hat

¿Qué queremos proteger?

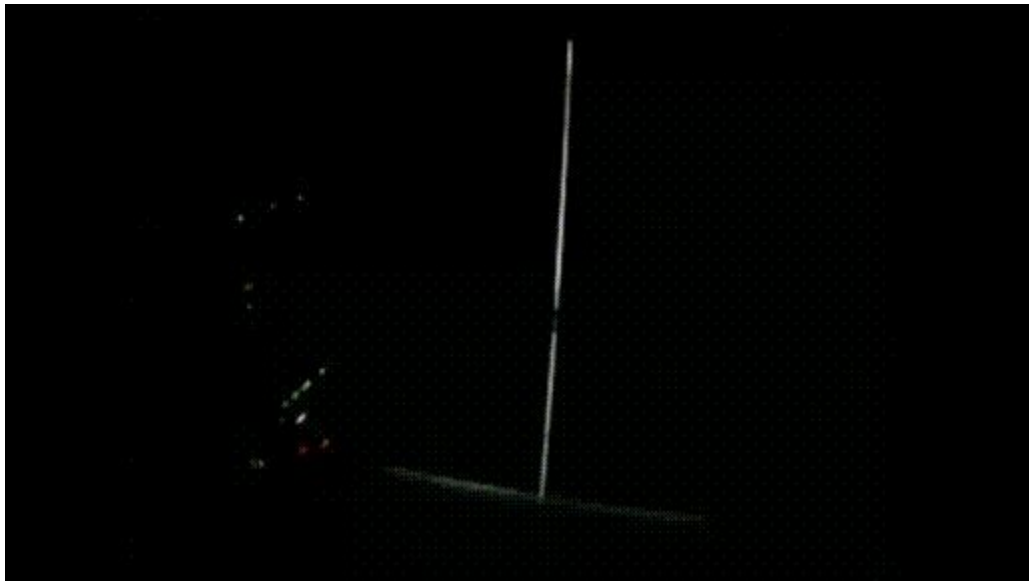
Integridad

Confidencialidad

Disponibilidad

Seguridad física y control de acceso

- Si existe acceso físico al equipo, tenemos un punto crítico de falla



Seguridad física y control de acceso

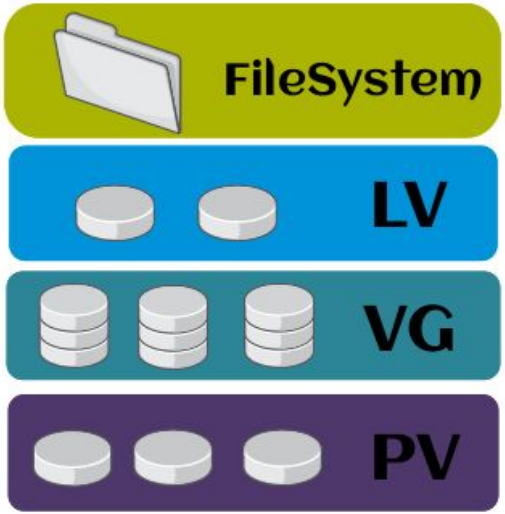
- Acceso al servidor
  - Rack
  - Acceso físico y control de acceso
- Proteger el BIOS/UEFI
  - Prevención de modificaciones
  - Evitar el boot no autorizado
- Deshabilitar periféricos no utilizados
- Fuentes redundantes
- RAID

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

- **Usa LVM!**
  - *A demanda*
- `/boot`
  - kernel, GRUB
    - Sin encripción
    - Contraseña en GRUB
- `/home`
  - Sólo datos de usuario
- `/var/tmp` y `/tmp`
  - Archivos temporales
  - No se almacenan durante un largo período



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

- Para deshabilitar la combinación de teclas **Ctrl+Alt+Supr**, es necesario enmascarar el servicio:

```
# systemctl mask ctrl-alt-del.target
```

- Para desenmascarar el **ctrl-alt-del.target** y dar rollback:

```
# systemctl unmask ctrl-alt-del.target
```

Limitar la información expuesta sobre el equipo

- `/etc/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 ilicita, 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.
```

Limitar la información expuesta sobre el equipo

- /etc/motd

```
With great powers comes great responsibility, be worthy
```

Servicios: ¿Cuáles deben estar activos?

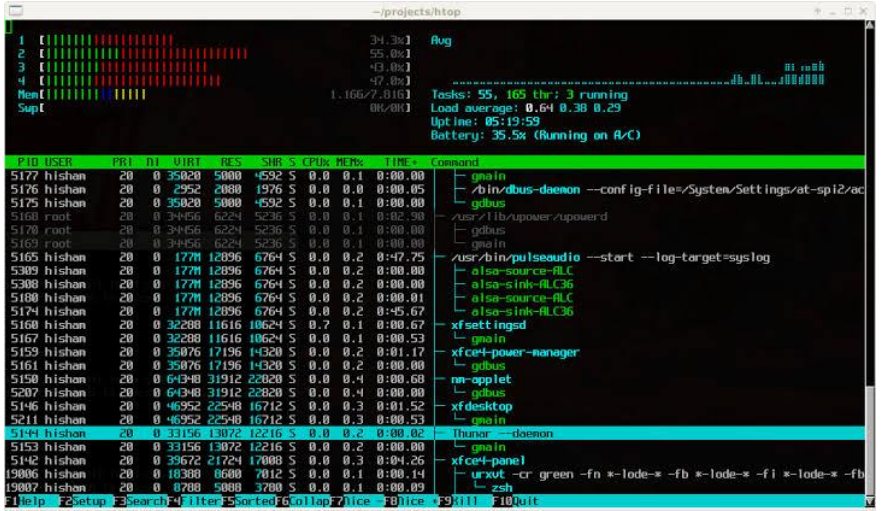
- ¡Sólo los necesarios!

```
# systemctl list-unit-files | grep running
```

```
# systemctl | grep running
```

Servicios: performance y seguridad

- ps, netstat
- top, htp, nmon
- sar
- lsof, pgrep
- systemtap



Red Hat

Limitar recursos

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

Equipo de respuesta a incidentes de seguridad informática

- **CERT**
  - www.cert.org.mx
  - 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)

Errata

Errata style guide

Terminology	Enhancement Advisory	Bug Fix Advisory	Security Advisory / CVE			
Icon						
Icon color	Text color	Text color	Text color if no severity level specified			
Severity			Low  #8b8d8f pf-black-500	Moderate  Text color pf-black	Important  #ec7a08 pf-orange-400	Critical  #cc0000 pf-red-100

Red Hat

yum-plugin-security: Verificación de erratas

- Resumen de actualizaciones de seguridad

```
# yum updateinfo
```

- Lista de actualizaciones disponibles

```
# yum updateinfo list available
```

Control de acceso: **firewalld**

- Status

```
# systemctl status firewalld
```

- Listar reglas

```
# iptables -nL
```

```
# firewall-cmd --list-all
```

Control de acceso: **firewalld**

- Agregar servicio y puerto

```
# firewall-cmd --permanent --add-service={http,https,ssh}
```

```
# firewall-cmd --permanent --add-port={22/tcp,80/tcp,443/tcp,8080/tcp,8443/tcp}
```

- Permitir el tráfico de un puerto o servicio, sólo por un determinado segmento de red

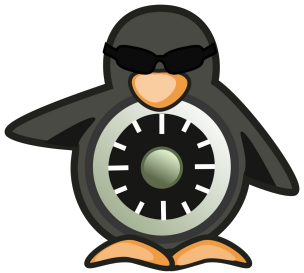
```
# firewall-cmd --permanent --zone=public --add-rich-rule='rule family="ipv4"
source address="172.16.0.0/24" port protocol="tcp" port="22" accept'
```

- Recargar el servicio

```
# firewall-cmd --reload
```

Control de acceso: **SELinux**

- **MAC** (Mandatory Access Control)
  - **SELinux** (Security-Enhanced Linux)
    - `getenforce`
    - `setenforce 0|1`
    - stopdisablingselinux.com
    - setroubleshoot



```
# yum install setroubleshoot setroubleshoot-server
```

Control de acceso: **SELinux**

- Ejemplo práctico

```
[root@vmlab01 ~]# vi ~/index.html
[root@vmlab01 ~]#
[root@vmlab01 ~]# cat ~/index.html
Hola Mundillo!
[root@vmlab01 ~]# mv ~/index.html /var/www/html/
[root@vmlab01 ~]#
[root@vmlab01 ~]# wget localhost
--2019-12-01 20:49:22--  http://localhost/
Resolving localhost (localhost)... ::1, 127.0.0.1
Connecting to localhost (localhost)|::1|:80... connected.
HTTP request sent, awaiting response... 403 Forbidden
2019-12-01 20:49:22 ERROR 403: Forbidden.

[root@vmlab01 ~]#
```

Control de acceso: **SELinux**

- Apache y audit logs

```
[root@vmlab01 ~]# tail /var/log/httpd/error_log
[Sun Dec 01 20:49:22.387701 2019] [core:error] [pid 555:tid 139880684480256]
(13)Permission denied: [client ::1:54922] AH00035: access to /index.html denied
(filesystem path '/var/www/html/index.html') because search permissions are
missing on a component of the path
[root@vmlab01 ~]#
```

```
[root@vmlab01 ~]# ausearch -m avc -ts recent
time->Sun Dec 01 20:49:22 2019
type=AVC msg=audit(1555447762.387:114): avc:  denied  { getattr } for  pid=555
comm="httpd" path="/var/www/html/index.html" dev="vda1" ino=3207
scontext=system_u:system_r:httpd_t:s0
tcontext=unconfined_u:object_r:admin_home_t:s0 tclass=file permissive=0
----
```

Control de acceso: **SELinux**

- journalctl

```
[root@vmlab01 ~]# journalctl -f -t setroubleshoot
-- Logs begin at Sun 2019-12-01 20:49:18 UTC. --
Dec 02 20:49:22 vmlab01.iti.iii.lab setroubleshoot[1539]: failed to retrieve rpm
info for /var/www/html/index.html
Dec 02 20:49:22 vmlab01.iti.iii.lab setroubleshoot[1539]: SELinux is preventing
httpd from getattr access on the file /var/www/html/index.html. For complete
SELinux messages run: sealert -l 4cc11a34-9f9f-49c2-ba0f-0dc9a848ee38
Dec 02 20:49:22 vmlab01.iti.iii.lab setroubleshoot[1539]: failed to retrieve rpm
info for /var/www/html/index.html
Dec 02 20:49:22 vmlab01.iti.iii.lab setroubleshoot[1539]: SELinux is preventing
httpd from getattr access on the file /var/www/html/index.html. For complete
SELinux messages run: sealert -l 4cc11a34-9f9f-49c2-ba0f-0dc9a848ee38
[root@vmlab01 ~]#
```

Control de acceso: **SELinux**

- Ejemplo práctico

```
[root@vmlab01 ~]# ls -Z /var/www/html/index.html
unconfined_u:object_r:admin_home_t:s0 /var/www/html/index.html
[root@vmlab01 ~]#
[root@vmlab01 ~]# restorecon -v /var/www/html/index.html
Relabeled /var/www/html/index.html from unconfined_u:object_r:admin_home_t:s0 to
unconfined_u:object_r:httpd_sys_content_t:s0
[root@vmlab01 ~]#
[root@vmlab01 ~]# ls -Z /var/www/html/index.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/index.html
[root@vmlab01 ~]#
```

Control de acceso: **SELinux**

- Ejemplo práctico

```
[root@vmlab01 ~]# wget localhost
--2019-12-01 21:23:15--  http://localhost/
Resolving localhost (localhost)... ::1, 127.0.0.1
Connecting to localhost (localhost)|::1|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 15 [text/html]
Saving to: ‘index.html’

index.html
100%[=================================================>]  15  --.-KB/s    in 0s


2019-12-01 21:23:15 (2.82 MB/s) - ‘index.html’ saved [15/15]

[root@vmlab01 ~]#
```

Control de acceso

- **DAC** (Discretionary Access Control)
  - `chmod`
  - `chattr`
- **ACL** (Access Control List)
  - filesystem
- Permisos especiales
  - SUID, SGID, sticky bit
- Atributos
  - `chattr`, `lsattr`
- Revisar directorios con permisos especiales

```
# find / -type f -perm 1000 -ls
```

Auditoria: Política de login / contraseñas

- Checar información de expiración de contraseña de usuarios

```
# chage -l <user>
```

- **/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

Auditoria: sesión de super-usuario

- sudo
  - tlog
    - github.com/Scribery/tlog
    - Grabar sesión

```
# tlog-rec --writer=file --file-path=tlogtest.log
```

    - Reproducir sesión

```
# tlog-play --reader=file --file-path=tlogtest.log
```

Servicios: **SSH**

- **¡Mantenerlo actualizado!**
- Restringir el uso
- **Indispensable** para SysAdmins
- ¡Usa llaves de confianza!
  - `ssh-keygen`
  - `ssh-copy-id`

`/etc/ssh/sshd_config`

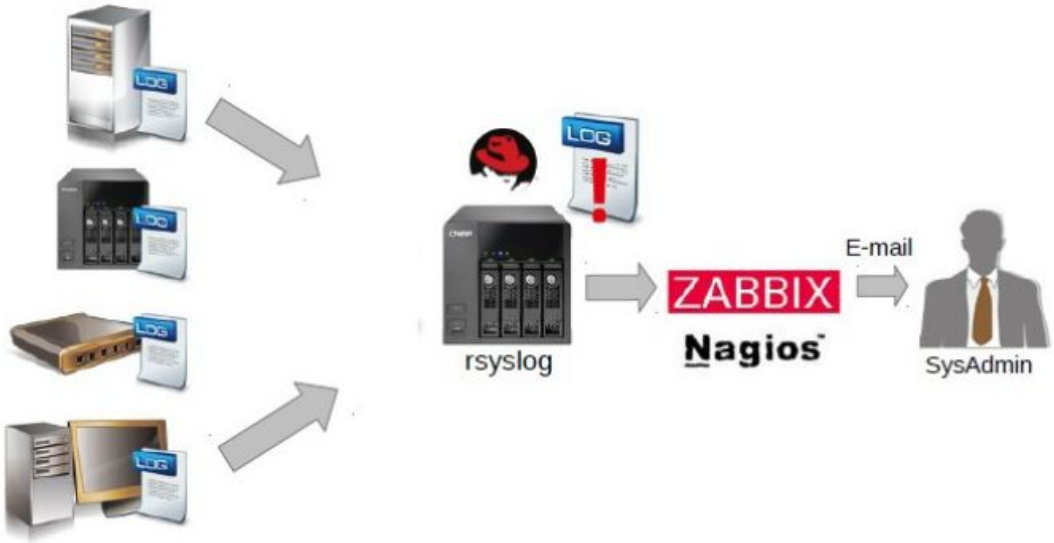
```
Port 22
Protocol 2
PermitRootLogin no
LoginGraceTime 60
PermitEmptyPasswords no
Allow users tux linus
Banner /etc/issue
```

Servicios: **Web Server**

- **¡Mantenerlo actualizado!**
- Agregar soporte a conexiones encriptadas
- Analizar el uso de módulos 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 gracefull`
- Restringir acceso
  - `.htaccess y htpasswd`

syslog centralizado

- rsyslog
- rsyslog-ng
- logrotate



Red Hat

Tuneame el **kernel**

- Evitar SYN ATTACK 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`

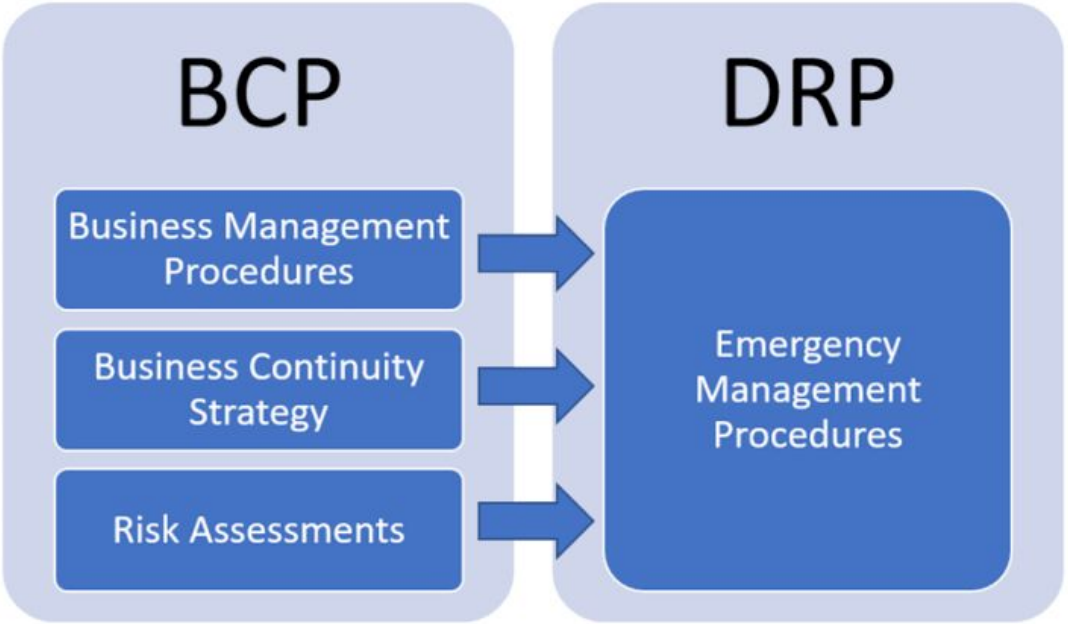
Preparándonos para el Desastre:
Planificando Contingencias y Continuidad

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 mínimo necesario para regresar a la normalidad?

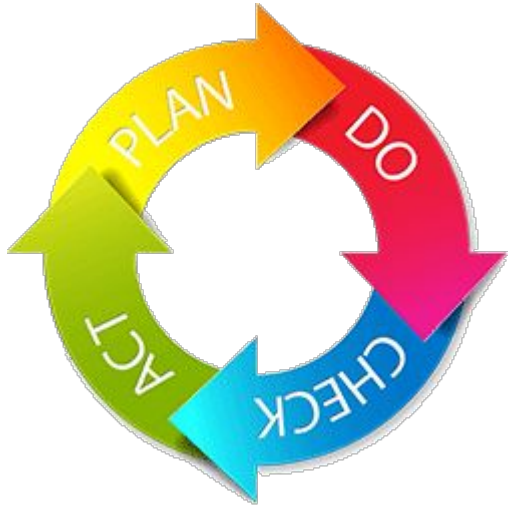
Red Hat

Business Continuity Plan



Plan de Contingencia

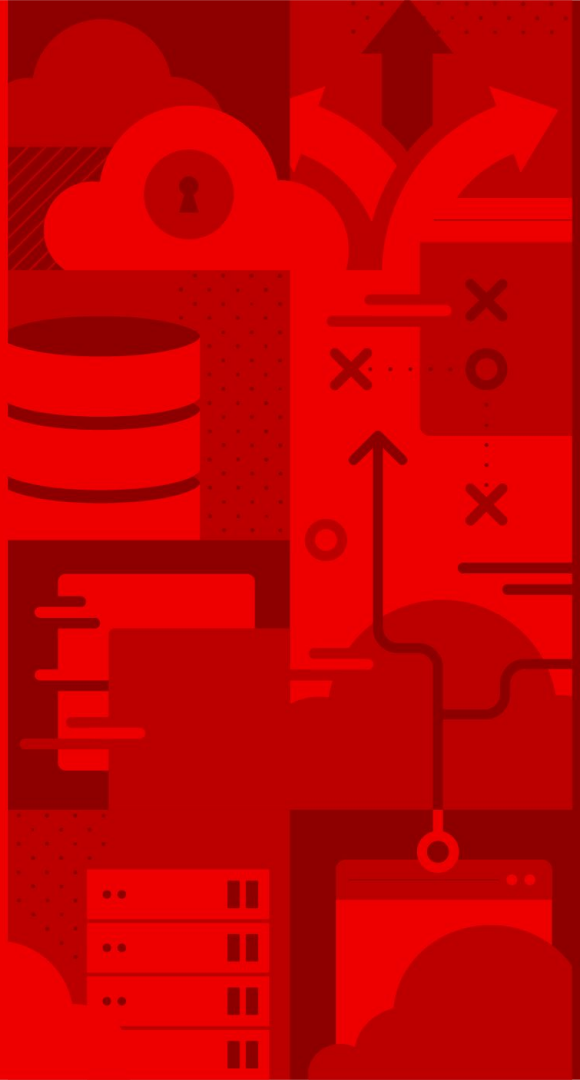
- Ciclo de vida PDCA (**plan-do-check-act**)
- Análisis de riesgo
  - Identificar amenazas
- Plan Contingencia
  - Plan de respaldo
  - Plan de emergencia
  - Plan de recuperación



DRP - Plan de Recuperación de Desastres

https://www.youtube.com/watch?v=r2pqBlv_lUs

Red Hat



¡Únete a nuestra Comunidad!

Red Hat

Learn more. Code more. Share more.

RED HAT® DEVELOPER PROGRAM

Join Us!

Sólo necesitas una cuenta de correo: developers.redhat.com

Red Hat Enterprise Linux 8

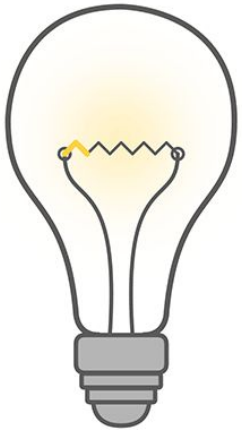
Download

developers.redhat.com/rhel8

Learn

www.edx.org/course/fundamentals-of-red-hat-enterprise-linux

BUILD SOMETHING GREAT



Red Hat

Gracias

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.

linkedin.com/company/red-hat

youtube.com/user/RedHatVideos

facebook.com/redhatinc

twitter.com/RedHat

Red Hat