Servidores y Seguridad

Open Source @ Inacap

2007-11-21

Arturo Hoffstadt Urrutia
Estudiante Ing. Civil Informática
ahoffsta@inf.utfsm.cl
http://arturo.hoffstadt.cl

Temario

- Seguridad
  - ¿Qué es seguridad?
  - Entonces... ¿que veremos?
- Mitos
- Administración de Sistemas y Servidores
  - Instalación
  - Pasos a Seguir
  - Consideraciones Físicas
  - El Proceso de Autenticación
  - Sistemas de Respaldos
- Políticas de Seguridad
- Conceptos de seguridad básicos
  - Modelos de seguridad

¿Qué es seguridad? (1/4)

- *"Es la ciencia que se dedica a manejar **actos y comportamientos maliciosos** que involucran las TIC"*
  - Ejemplos de actos y comportamientos maliciosos:
    - Robo
    - Fraude
    - Terrorismo
    - Espionaje
    - Sabotaje
    - Spam
    - Contenido Ilegal

¿Qué es seguridad? (2/4)

- Aspectos que cubre la Seguridad de Sistemas Computacionales:
  - Disponibilidad
    - Asegurar que los usuarios autorizados tienen acceso a la información cuando sea requerido.
  - Confidencialidad
    - Asegurar que la información es accesible solo a los que poseen autorización para verla.
  - Integridad
    - Salvaguardar la correctitud y completitud de la información y métodos de procesamiento.

¿Qué es seguridad? (3/4)

- ¿Porqué nos interesa la Seguridad de Sistemas Computacionales?
  - Hoy en día casi todos la información es administrada computacionalmente. Entonces, nos interesa para:
    - Mantener privacidad de nuestra información medica
    - Resguardar nuestras cuantas bancarias
    - Autenticar la veracidad de un mensaje
    - Salvaguardar vidas en los hospitales.
    - Etc.
  - Por eso, la aproximación de Seguridad que se requiere hoy en día, es sistémica. Debe aplicarse seguridad en todos las componentes del Sistema, y en sus canales de comunicación.

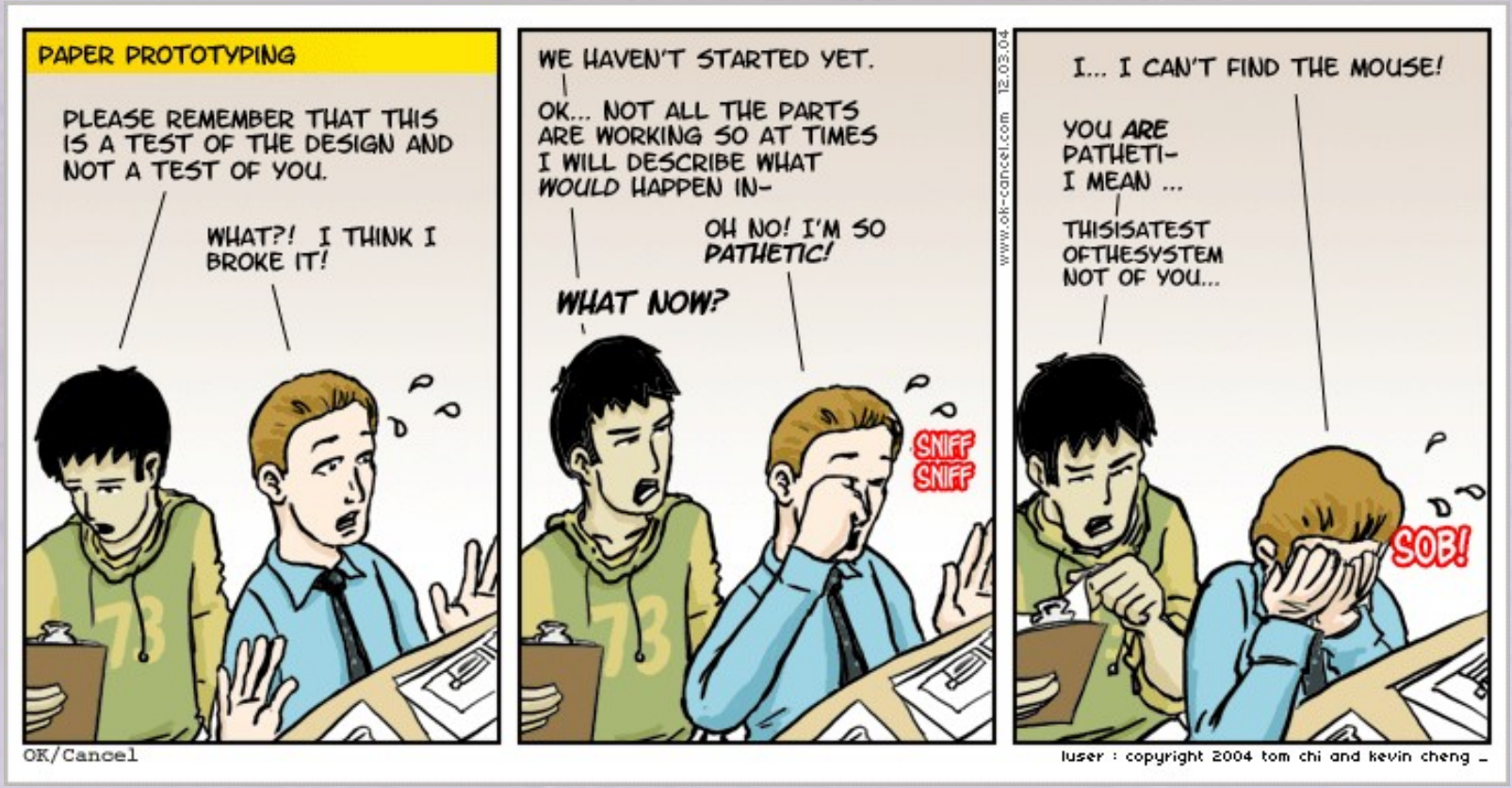
¿Qué es seguridad? (4/4)

Finalmente...

Recordar que la seguridad (de sistemas) envuelve acciones humanas. No solo nos debemos preocupar de los computadores y programas, sino tambien de las USUARIOS.

Entonces... ¿Qué veremos? (1/2)

- Veremos
  - Servidores y proceso de instalación
  - Administración de Sistemas
  - Políticas de Seguridad
  - **Usuario**, Capa 8, e interfaz teclado-silla.

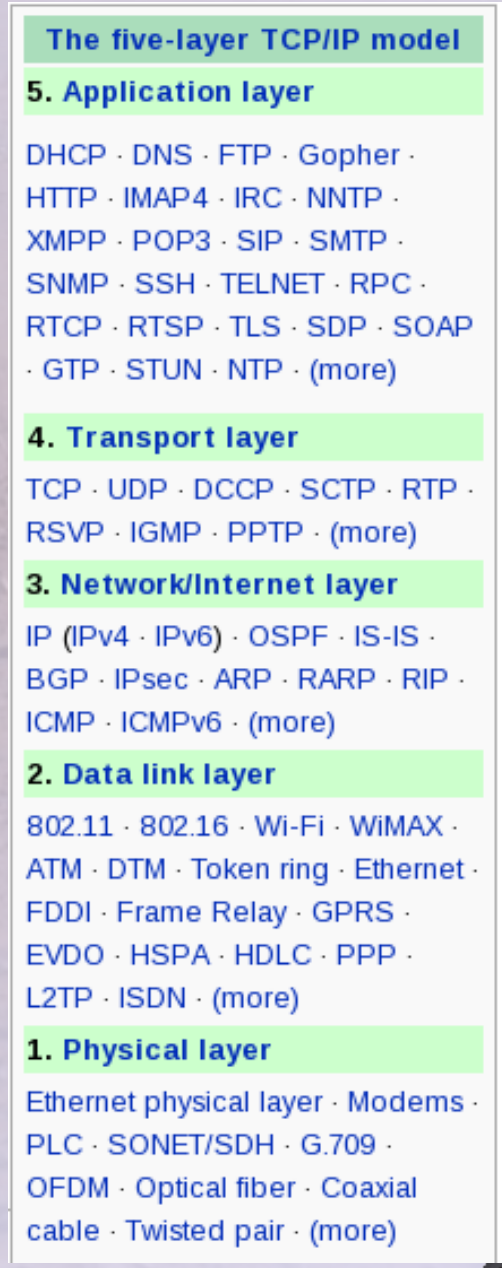


Entonces... ¿Qué veremos? (2/2)

- No veremos
  - Seguridad y programación.
    - Memoria de Rodrigo Riveros, DI, UTFSM.
    - Secure Programming for Linux and Unix HOWTO (http://www.dwheeler.com/secure-programs)
    - La charla “Web: Ataque y Defensa”, por Claudio Salazar.
  - Criptografía.
    - Si necesitan implementar criptografía, no inventen un algoritmo. Existen muchos algoritmos de especificación abierta (e incluso implementación), que son extremadamente seguros y efectivos.
    - Aprender a utilizarlo es mucho mas importante que programar un buen algoritmo. Si la llave de encriptación es administrada debilmente, **el algoritmo no sirve de nada.**

Mitos

- **Un firewall, es lo único que necesito.**
  - El firewall solo restringe puertos, orígenes, destinos, y protocolos (depende, normalmente capa 3 y 4).
  - Varios de los problemas de seguridad, no suelen ser solucionados por un firewall (usuario anoto su contraseña).
- **Si un software que uso esta mal programado, no es mi problema.**
  - El software es un medio de acceso a los datos que resguardo.



Mitos

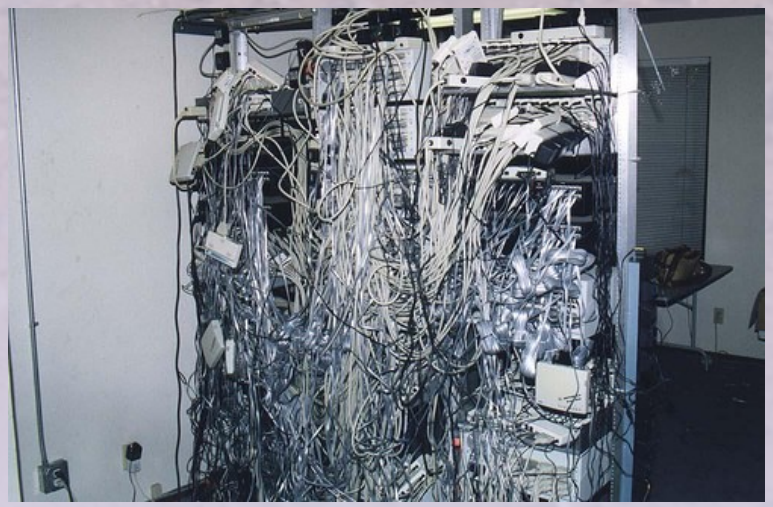
- **Si el software que tengo en mis sistema, usa encriptación, no tengo que preocuparme.**
  - La administración de las contraseña/llave es más delicada que el método de encriptación usado.
- Las jaulas chroot, son impenetrables.
  - Las jaulas chroot tienen que ser creadas por el usuario root, y por ende, el mismo puede salir de ellas.
  - Chroot no fue creado con el fin de contener programas con posibles fallos o exploits de seguridad.

Mitos

- **La seguridad de sistema es un problema/tarea solo de Administración de Sistemas**
  - QUÉEEEEEEEEE!!!!!!!!!!!!!!!!!!!

Administración de Sistemas y Seguridad

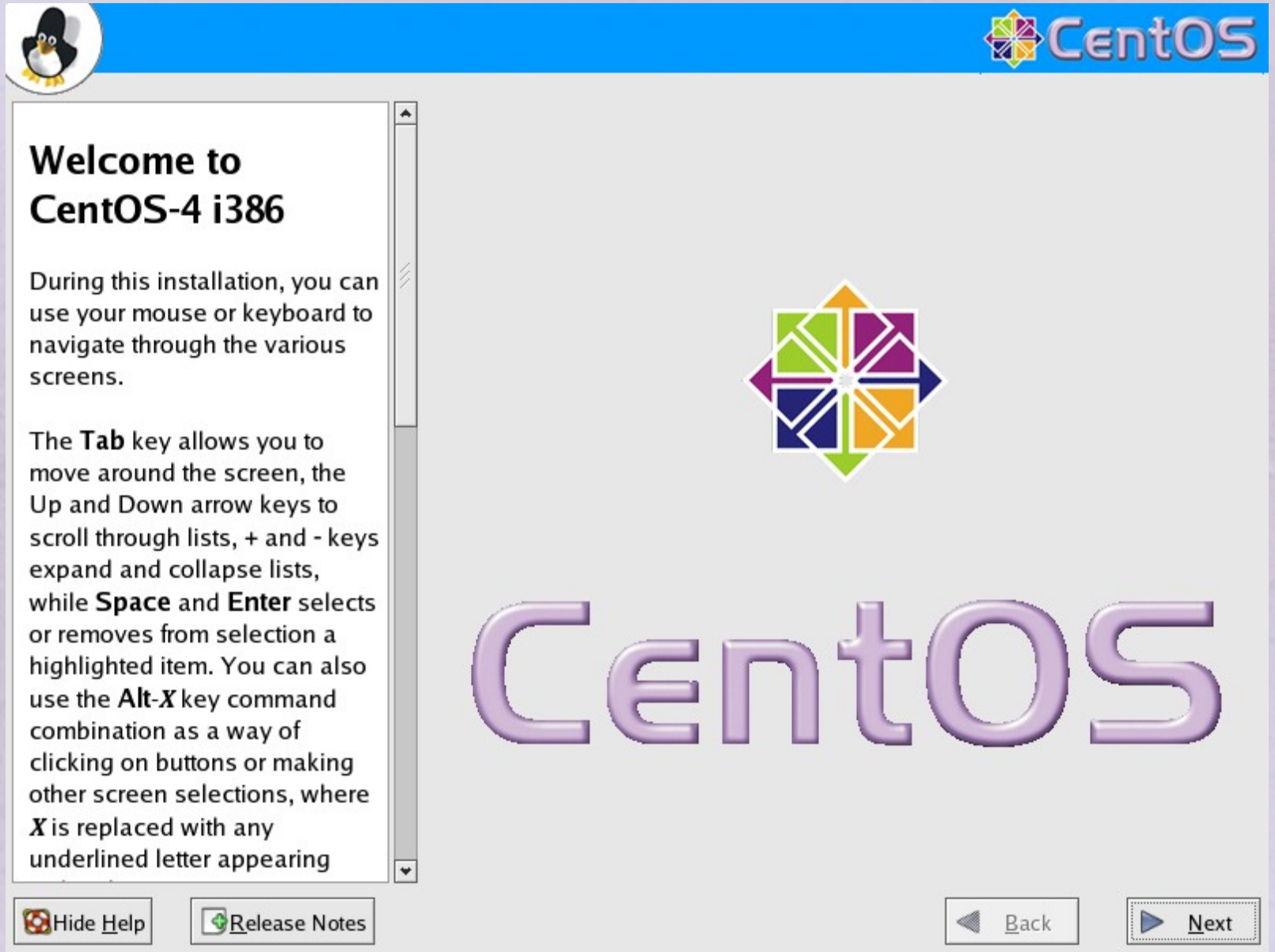
- La Administración de Sistemas, es uno de los trabajos que más se encuentra con Seguridad (después, obviamente, de la Ingeniería de Seguridad).
- Veremos varios puntos de las tareas de un Administrador de Sistemas, partiendo por la instalación de un servidor.



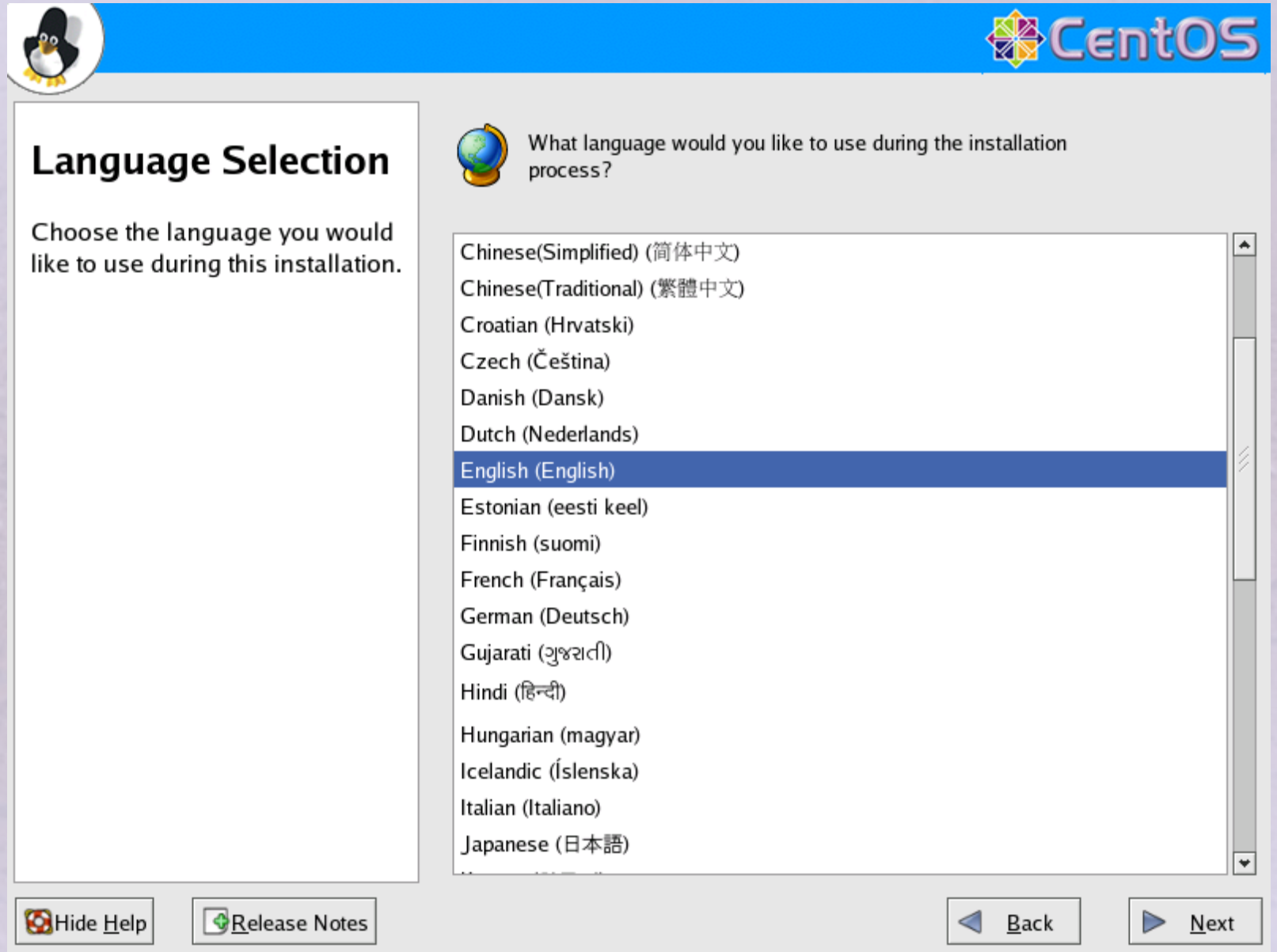
CentOS

O cualquier otro
“Enterprise” o
“Server” Edition

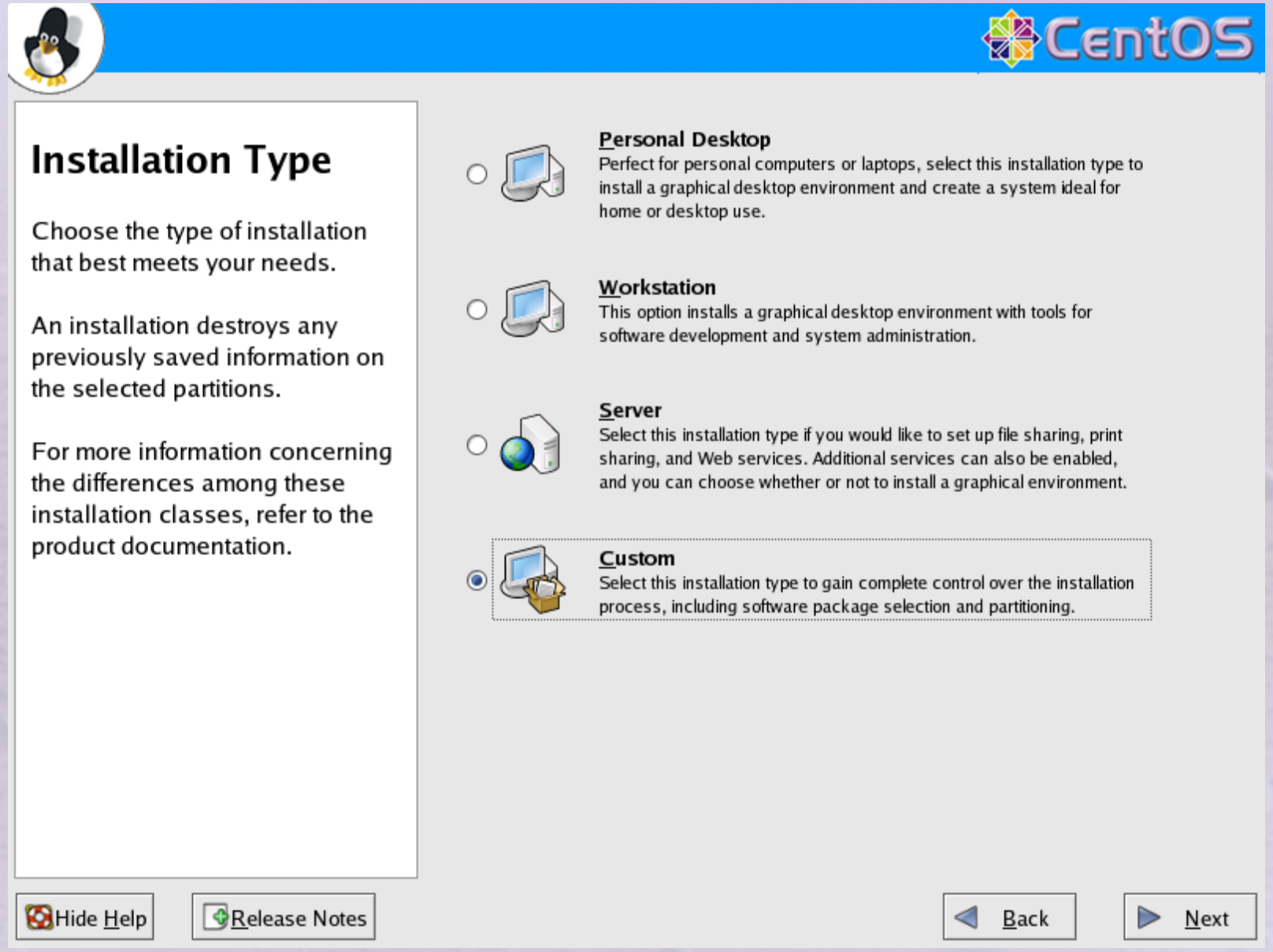
Que ofrece CentOS



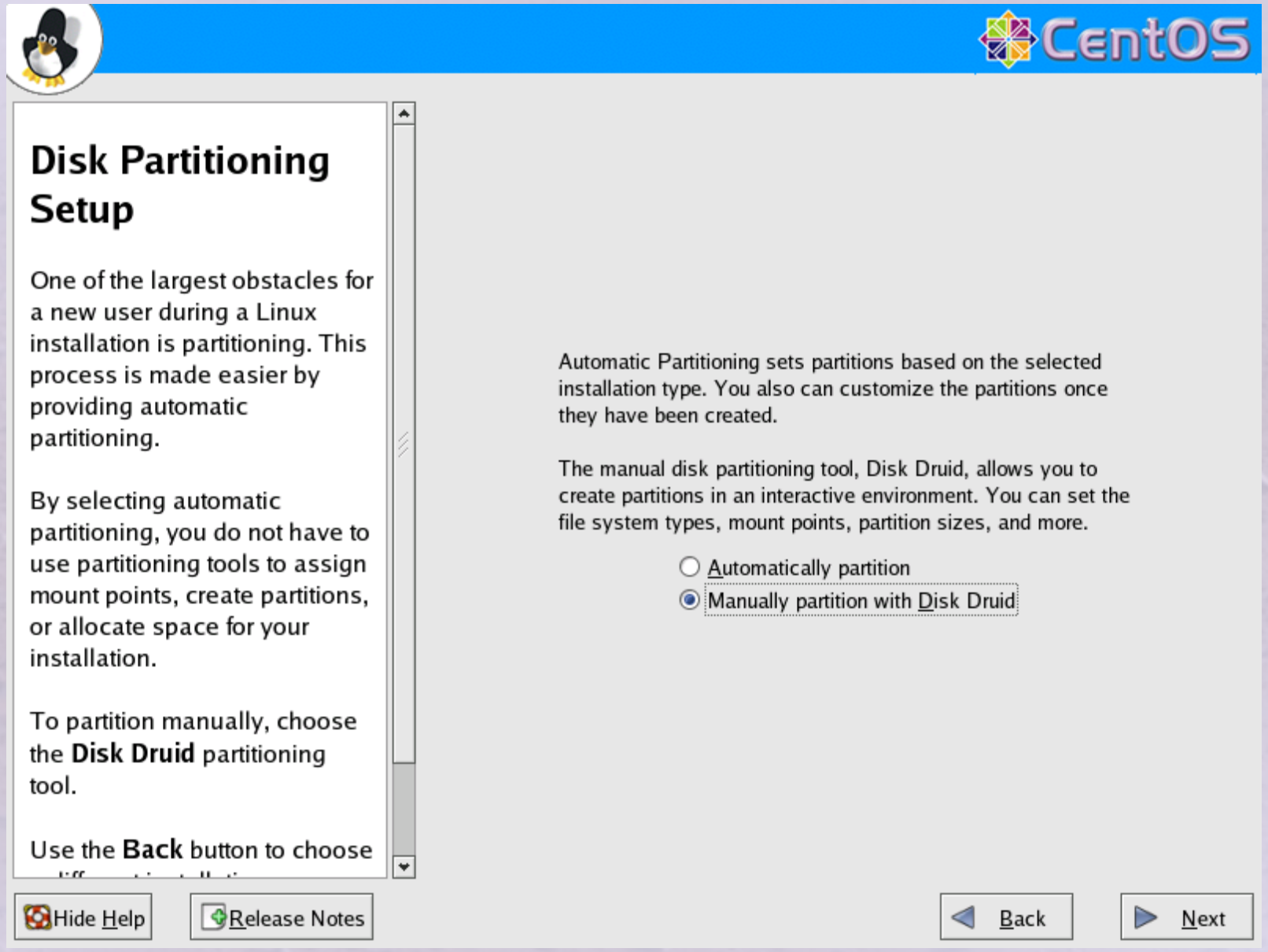
Ingles... ¿porqué?



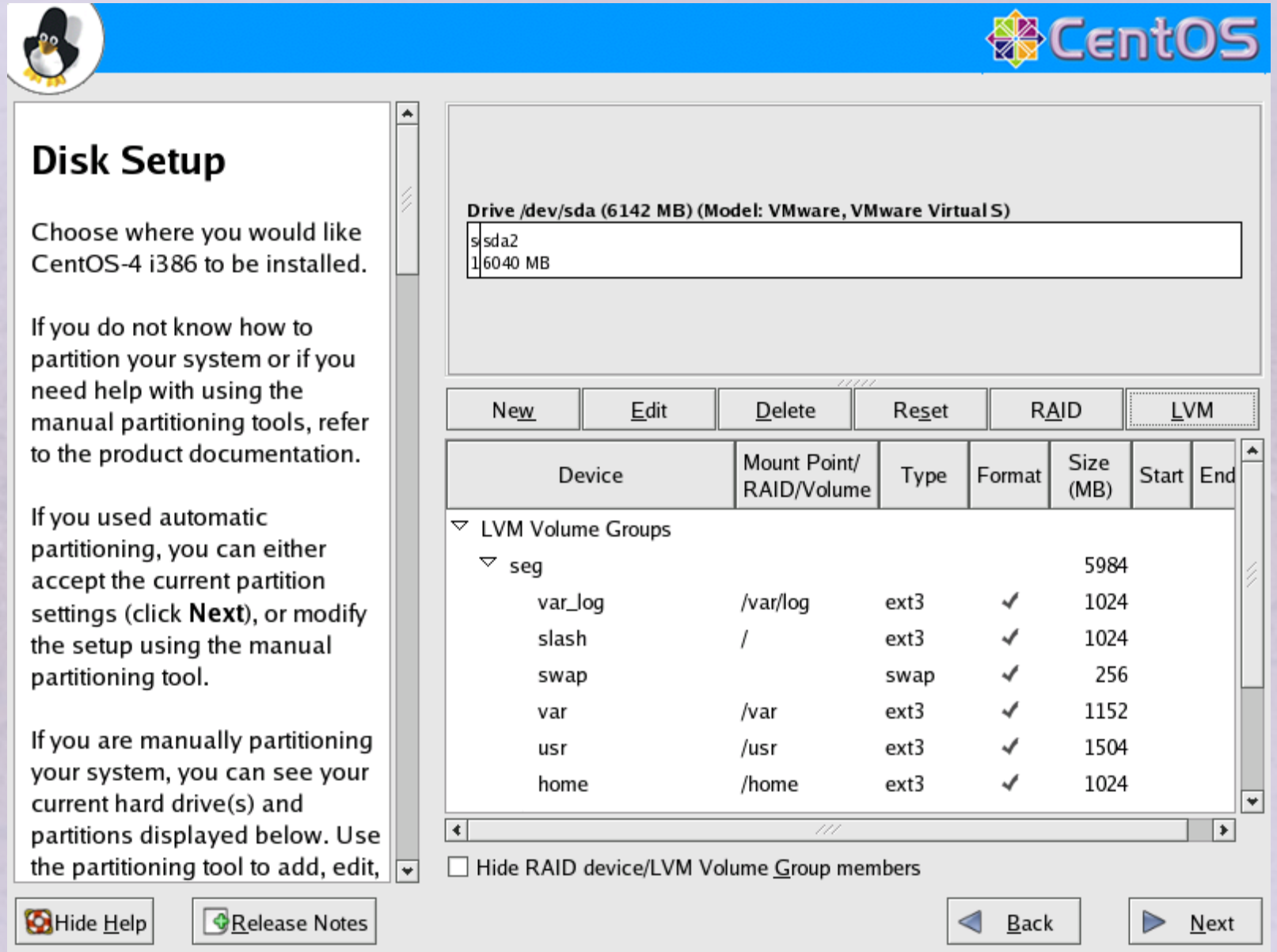
Customizada



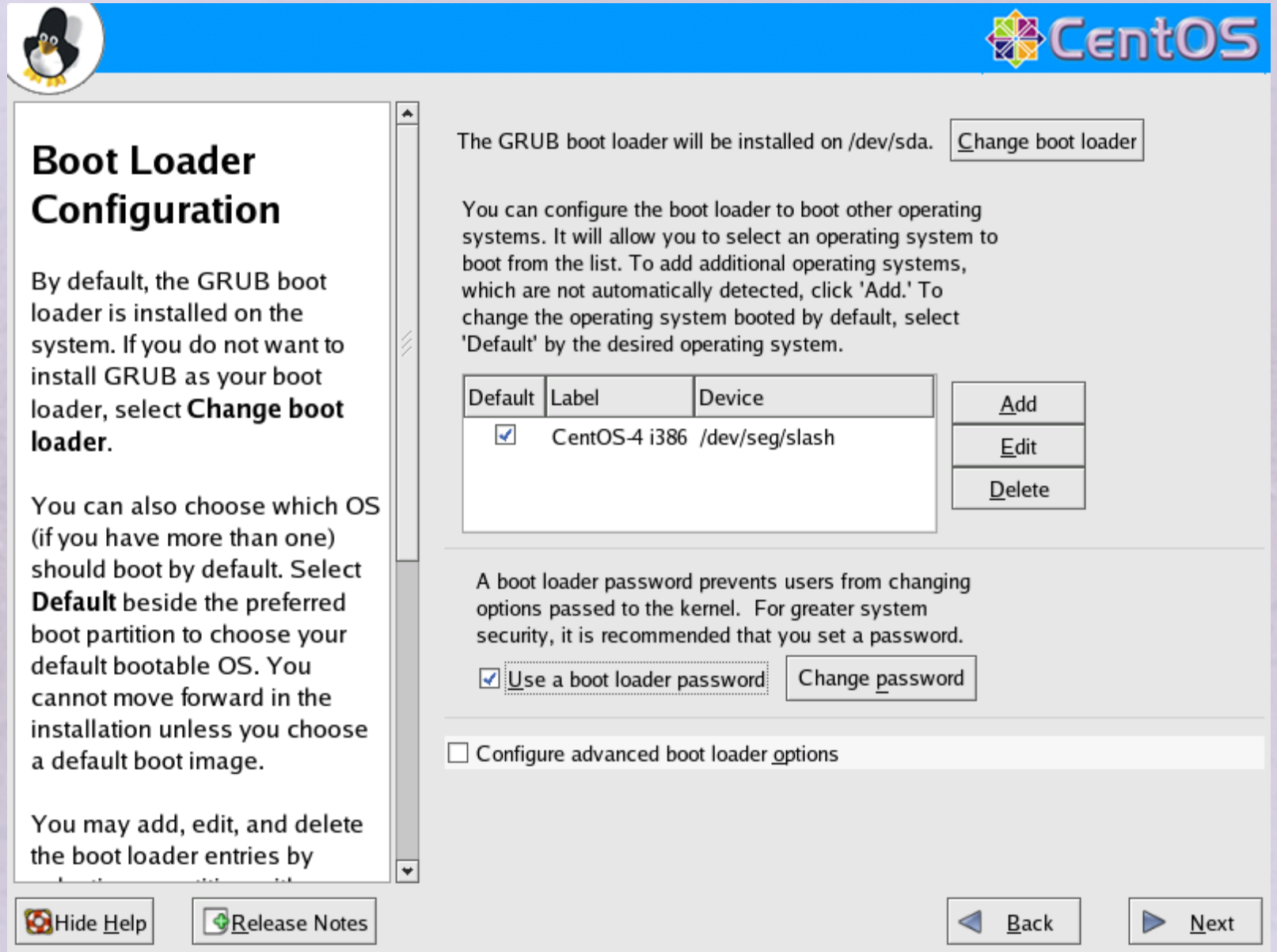
Particiones manuales

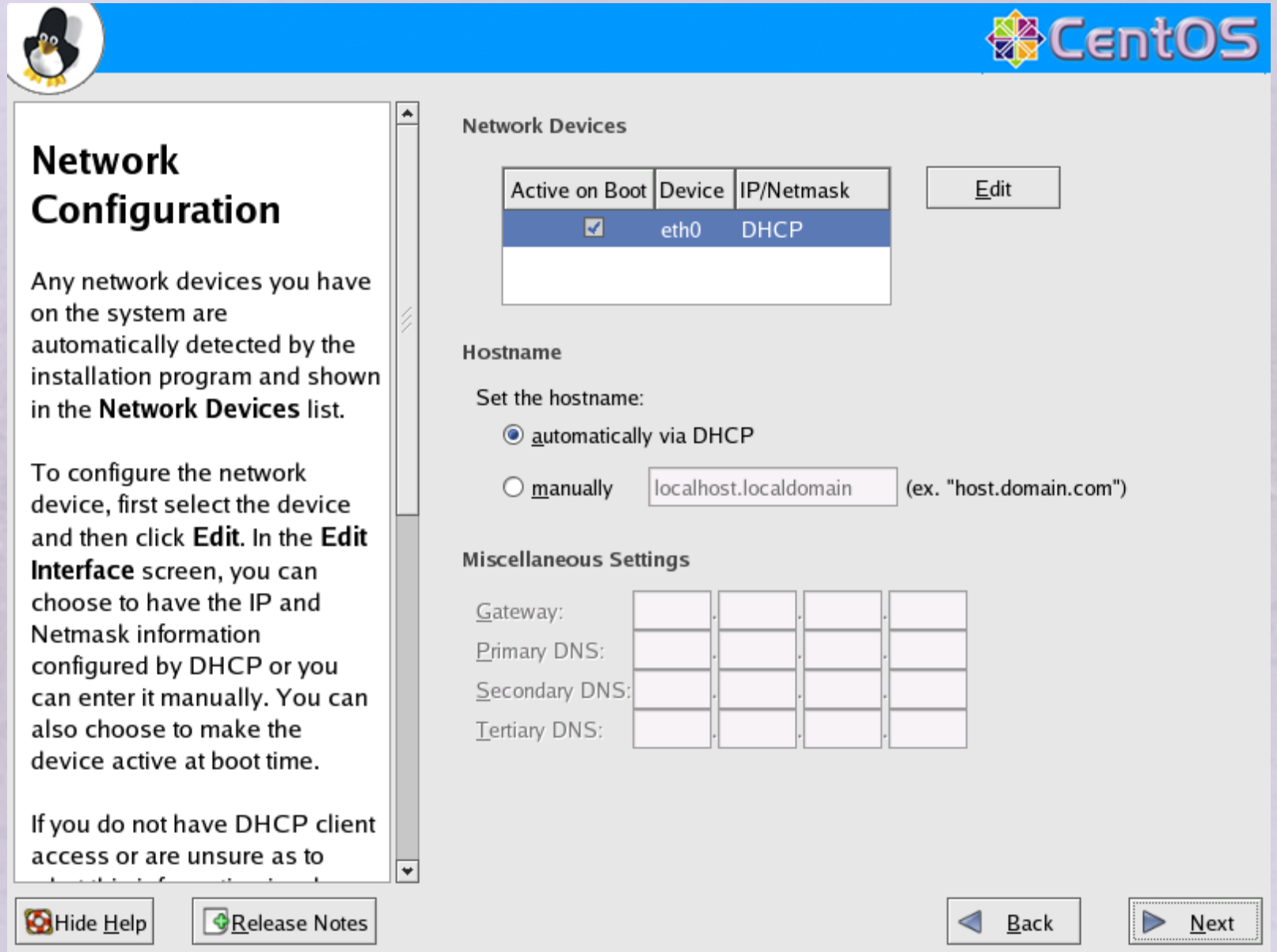


Esquema de partición

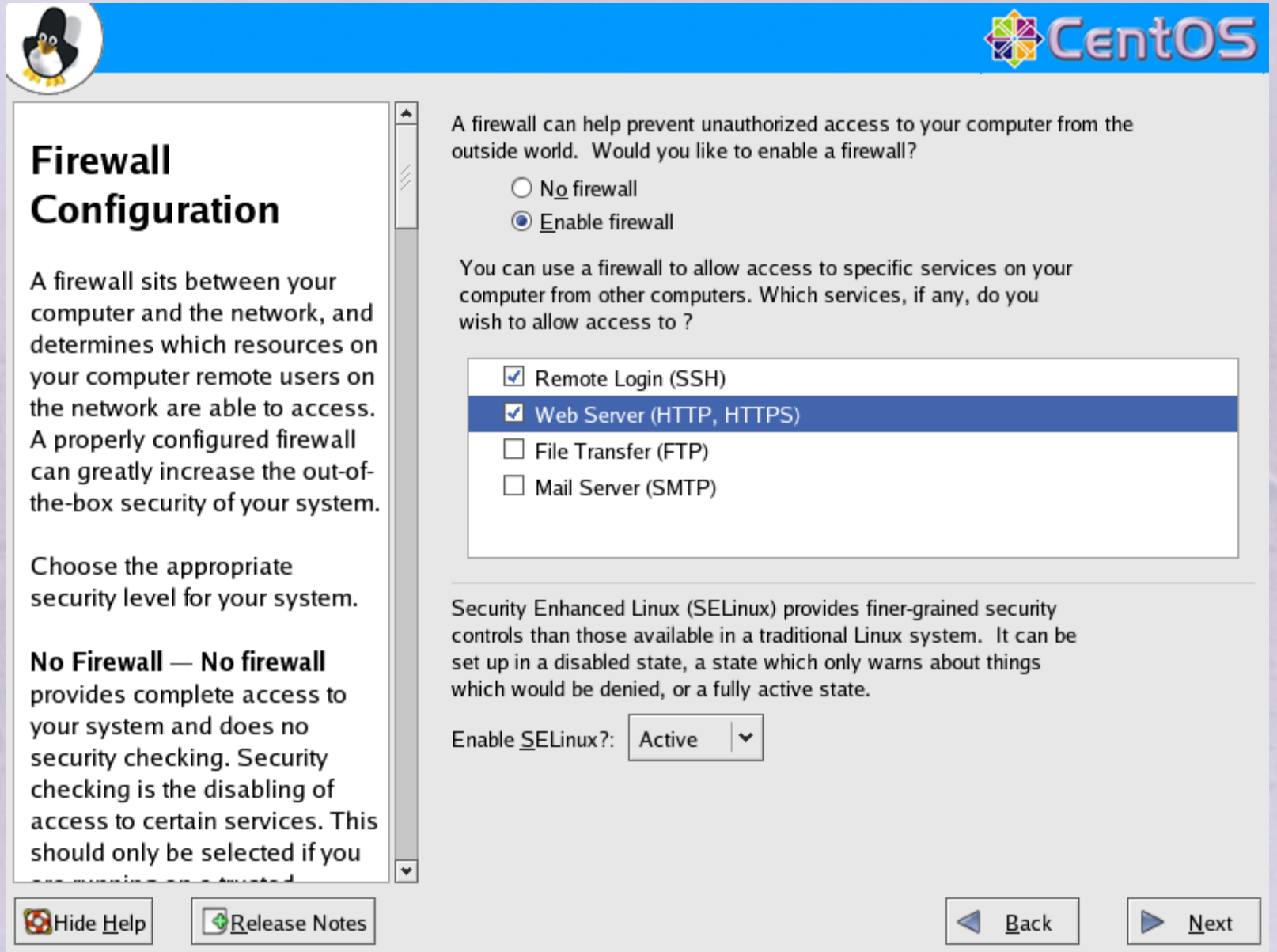


Password en grub... ¿porqué?

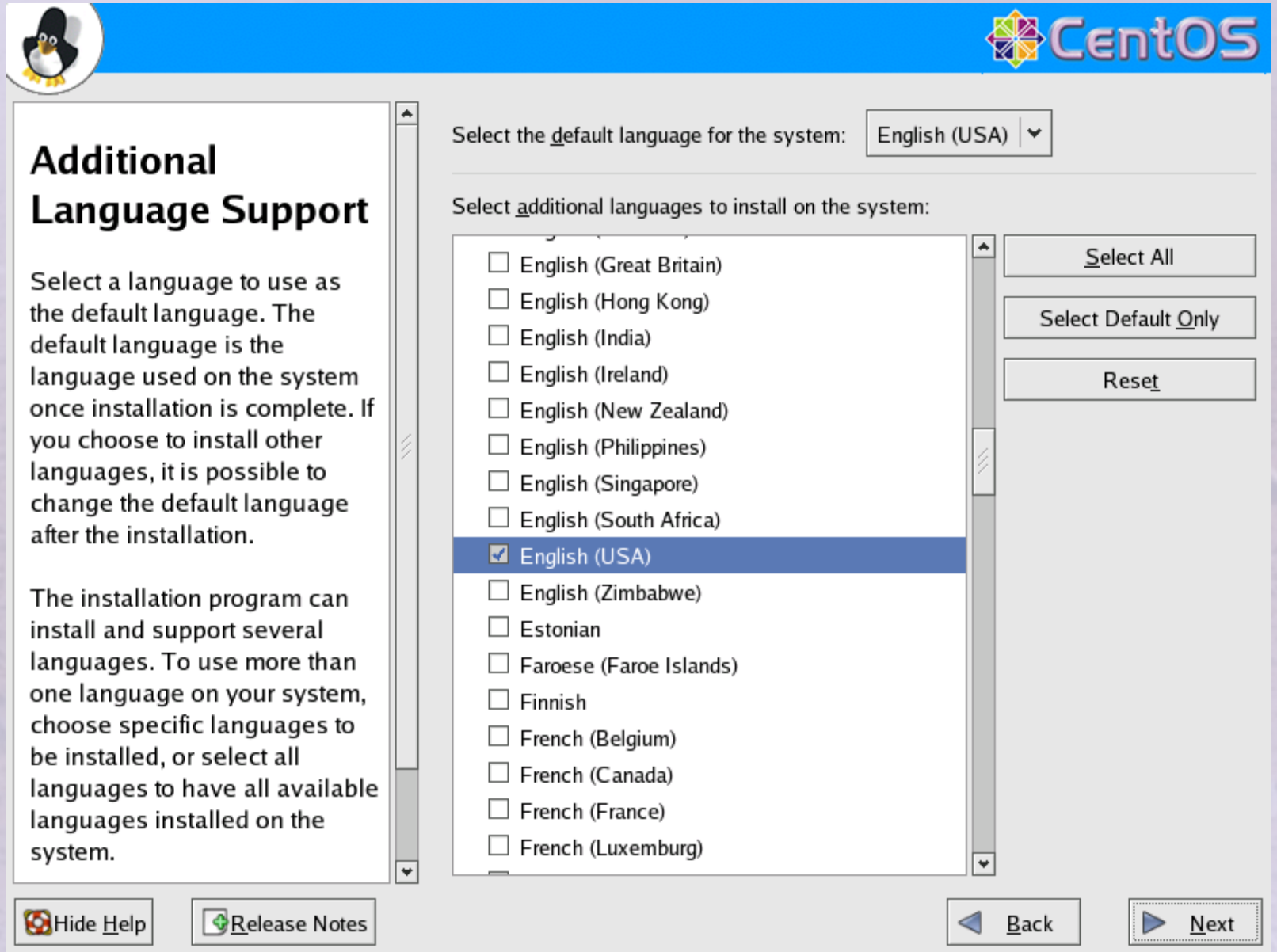



CentOS
Network Configuration
Any network devices you have on the system are automatically detected by the installation program and shown in the Network Devices list.
To configure the network device, first select the device and then click Edit. In the Edit Interface screen, you can choose to have the IP and Netmask information configured by DHCP or you can enter it manually. You can also choose to make the device active at boot time.
If you do not have DHCP client access or are unsure as to
Network Devices
Active on Boot
Device
IP/Netmask
eth0
DHCP
Edit
Hostname
Set the hostname:
automatically via DHCP
manually
localhost.localdomain
(ex. "host.domain.com")
Miscellaneous Settings
Gateway:
Primary DNS:
Secondary DNS:
Tertiary DNS:
Hide Help
Release Notes
Back
Next

Firewall, SELinux

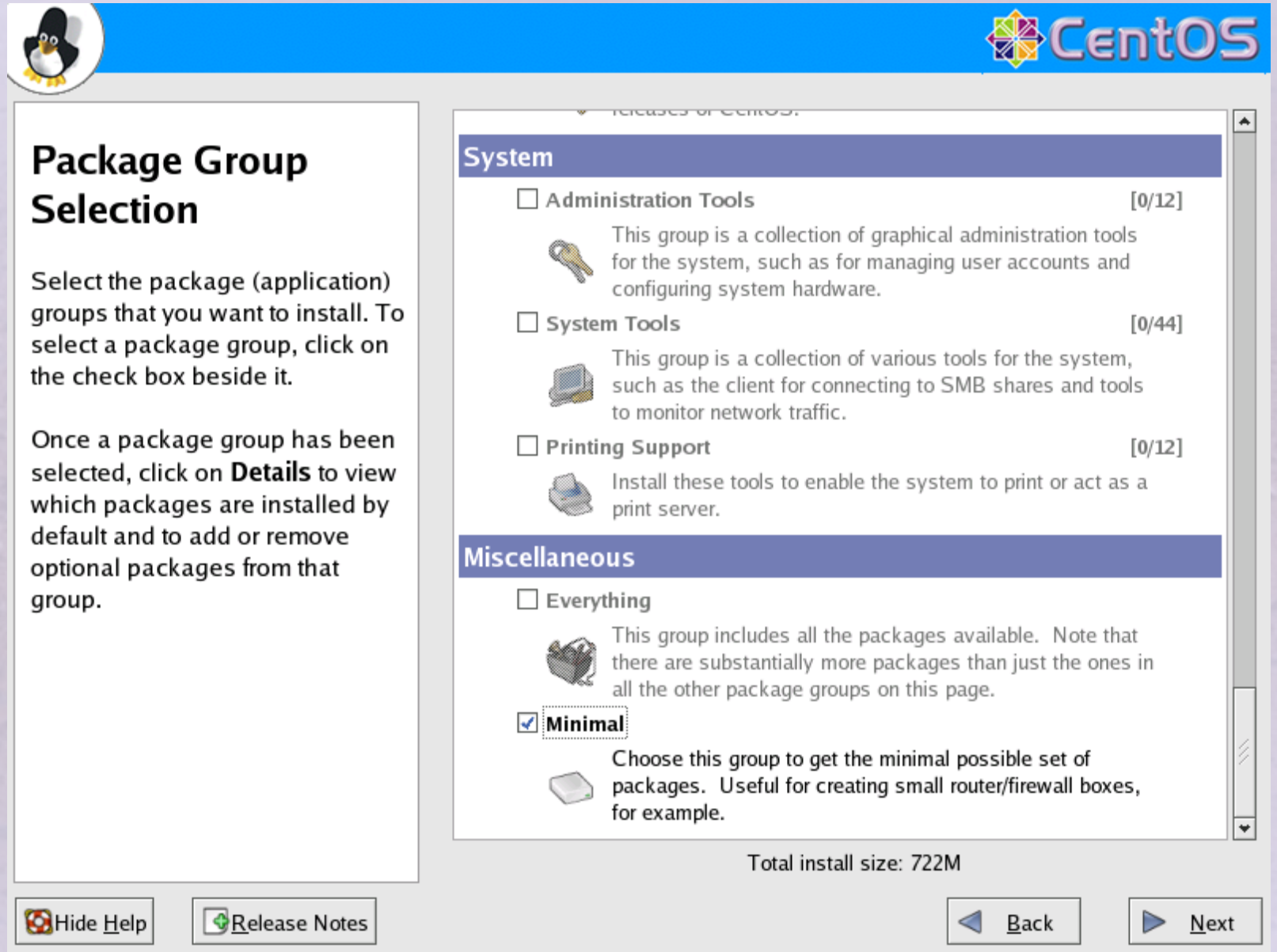


Inglés, ¿nuevamente?



Selección de passwords

Paquetes a instalar... Mínimo



CentOS

About to Install

Caution: Once you click **Next**, the installation program begins writing the operating system to the hard drive(s). This process cannot be undone. If you have decided not to continue with this installation, this is the last point at which you can safely abort the installation process.

To abort this installation, press your computer's Reset button or reset using **Control-Alt-Delete**, and then remove the installation media between the unmounting and reboot screen messages.

Click next to begin installation of CentOS-4 i386.

A complete log of the installation can be found in the file '/root/install.log' after rebooting your system.

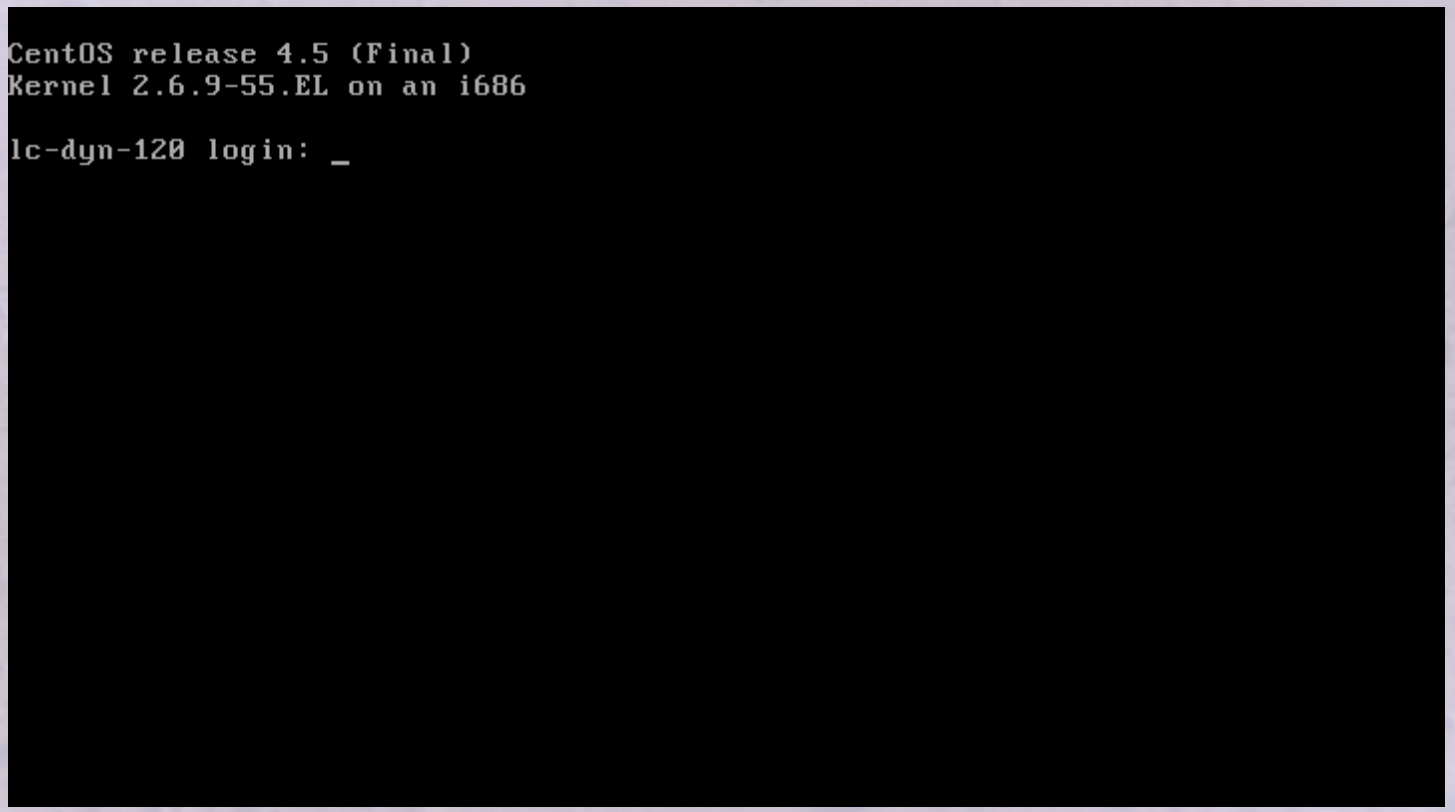
A kickstart file containing the installation options selected can be found in the file '/root/anaconda-ks.cfg' after rebooting the system.

Hide Help | Release Notes | Back | Next

Instalando...


CentOS
Installing Packages
We have gathered all the information needed to install CentOS-4 i386 on the system. It may take a while to install everything, depending on how many packages need to be installed.
Welcome to CentOS 4 !
Thank you for installing CentOS 4.
CentOS is an Enterprise-class Linux Distribution derived from sources freely provided to the public by a prominent North American Enterprise Linux vendor. CentOS conforms fully with the upstream vendors redistribution policy and aims to be 100% binary compatible. (CentOS mainly changes packages to remove upstream vendor branding and artwork.)
More Info: http://www.centos.org/
Installing rootfiles-8-1.noarch (20 KB)
The basic required files for the root user's directory.
Hide Help
Release Notes
Back
Next

Y como recien salido del horno...



Pasos a seguir

- Deshabilitar servicios sin usar
  - Seguir el principio de mínima superficie de exposición
  - Saber que tienes instalado en tu sistema
- Habilitar NTP, y mantenerlo sincronizado.
  - Instalar y levantar el servicio ntpd
- `echo "export HISTFILESIZE=10000" >> /root/.bashrc`

Pasos a seguir

- Control remoto del servidor:
  - Ssh y sus llaves
- Yum
  - Aplicar `yum update`
  - Actualizar a lo menos diariamente
  - Seleccionar cuidadosamente los repositorios a utilizar
- Opciones (nosuid, noexec) a las particiones /tmp /var, /home

Consideraciones Físicas

- Aire acondicionado
- Acceso Físico
  - Limitado
  - Solo en casos que se necesite contacto directo
- Electricidad
  - UPS
    - Energía **continua** en cortes no prolongados
  - Equipos Electrógenos (generadores)
    - Energía en cortes prolongados
- Detectores de Humo
- Sensor de Temperatura
- Instalación eléctrica
- Discos con soporte SMART (y activarlo)

El Proceso de Autenticación

- Entendiendo el sistema de autenticación:
  - Linux guarda la información de los usuarios (por defecto), en /etc/passwd
  - Inclusive la contraseña
    - Lo cual es muy inseguro, dado que a este archivo deben tener acceso muchas aplicaciones.

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
                                              8,1           Comienzo
```

`user:password:uid:gid:comentario:home:shell`

El Proceso de Autenticación

- Se introduce el sistema Shadow.
  - Las password, pasan de /etc/passwd a /etc/shadow, y el root es el único que puede leerlas.

```
root:$1$rs9pdsmT$yd/O.RBJDrPBXtWPh8W/b/:13795:0:99999:7:::
bin:*:13731:0:99999:7:::
daemon:*:13731:0:99999:7:::
adm:*:13731:0:99999:7:::
lp:*:13731:0:99999:7:::
sync:*:13731:0:99999:7:::
shutdown:*:13731:0:99999:7:::
halt:*:13731:0:99999:7:::
"/etc/shadow" [Sólo lectura] 87L, 2303C                    8,1      Comienzo
```

`user:password:lstchg:min:max:warn:inact:expire`

`Contraseña en Shadow:`

`User::`	Indica que no tiene password.
`User:*:`	Indica cuenta lockeada.

El Proceso de Autenticación

- PAM (Pluggable Authentication Modules)
  - Elimina el problema de autenticación y obtención de datos de usuario, de los programas.
  - Proporcionan una interfaz de acceso, y una arquitectura de modulos, lo que permite cambiar la fuente de datos de usuarios.
    - Shadow
    - LDAP
    - Samba
    - NIS
  - Permite restringir acceso a cuentas en base a muchos criterios
  - Permite restringir las password que se asignan.

Sistemas de Respaldos

- **Siempre ponte en el peor caso, porque va a suceder**

  (y si... los edificio arden, muahahaha).

- Si realmente quieres Disponibilidad, vas a necesitar tener Respaldos
  - Incluso a pesar de los múltiples servidores failover, con RAID 1 o 5.
  - Los errores no necesariamente son maliciosos, accidentes o desastres. El mismo software puede corromper datos.

- Una vez definido, probarlo. Siempre puede faltar algo por respaldar.

Sistemas de Respaldos

- Tipos de Respaldos
  - Full: Respaldan todo
  - Incremental: Necesita un fullbackup, y solo respalda los cambios entre si, y el último fullbackup, o incremental.
  - Diferencial: Necesita un fullbackup, y solo respalda los cambios entre si, y el último fullbackup.
- Restaurar:
  - Simplemente restaurar sobre los corruptos
  - Reinstalación y restaurar sobre el sistema nuevo.
  - BareMetal Restore: El respaldo debe ser del sistema completo. Ni siquiera se reinstalar, sino que se “quema” la imagen al disco duro.

Sistemas de Información de Usuarios

- Opciones (algunas)
  - Local
  - LDAP
  - NIS
  - Samba
- Consideraciones
  - Tráfico encriptado (SSL/TLS)
  - La administración debe ser consistente con las políticas de administración de usuarios.
  - Control de la información publica, privada
  - Permitir Replicación -> aumenta disponibilidad

Políticas de Seguridad

- Hasta el momento, nos hemos restringido al ámbito de servidores y estaciones de trabajo.
- Pero no hemos visto el factor mas importante, la interfaz silla-computador.
  - La mayor parte de los problemas de seguridad se generan ahí.
    - Compartir la cuenta
    - Anotar la password
    - Dar la password a cualquier persona
    - Publicar su email en forma plana
- ¿Como solucionar el problema?
  - No hay solución completa. Solo recomendaciones, reglas, y pautas a seguir:
    - Políticas
    - Buenas practicas, etc

Políticas de Seguridad

- Administración de Usuarios
  - Mantener a todos los usuarios registrados
    - Saber quien puede entrar a que sistema, y quien no.
  - No mantener usuarios “fantasmas”
    - Usuarios usados por una aplicación, o como ejemplo o pruebas.
  - Solo tener a los usuarios necesarios en el sistemas
    - Considerar un ciclo de vida establecido que ate un usuario con un(as) cuenta(s).
    - Si un usuarios abandona la organización, borrar su cuenta inmediatamente (tras respaldarla).
  - Por sanidad mental, tener un sistemas de autenticación e información de usuarios centralizado.
    - Evitar tener sistemas que no se integren con la autenticación centralizada, porque requieren MUCHO más trabajo ser mantenidos.

Políticas de Seguridad

- Administración de Usuarios
  - 1 usuario <-> 1 cuenta
    - Permite auditar las acciones de los usuarios.
    - Asigna un responsable identificable.
  - Tener sanciones para las violaciones a las reglas
  - Desconfiar del usuario:
    - El usuario promedio es ignorante en computación e informática, por lo tanto, todo debe hacerse para que el usuario y los sistemas DEBAN estar lo más seguros.

Políticas de Seguridad

- Administración de Contraseñas
  - Explicar al usuario porque una contraseñas debe ser segura.
    - Numero mezclados con letras, (¿y caracteres no alfanuméricos?).
    - Fácil de recordar
    - No formada por palabras
    - **Letras tomadas de una frase, es muy buen generador de contraseñas fáciles de recordar, y complicadas.**
  - Indicarle que no debe entregar la contraseña. Ningún sistema bien hecho, pedirá al administrador de sistemas obtener la contraseña de un usuario.
  - Toda cuenta debe tener una contraseña, y nunca crear las cuentas con contraseñas predeterminadas:
    - Existen programas que generan contraseña. (pwgen)

Políticas de Seguridad

- Administración de Contraseñas
  - Explicar al usuario porque una contraseñas debe ser segura.
    - Numero mezclados con letras, (¿y caracteres no alfanuméricos?).
    - Fácil de recordar
    - No formada por palabras
    - **Letras tomadas de una frase, es muy buen generador de contraseñas fáciles de recordar, y complicadas.**
  - Indicarle que no debe entregar la contraseña. Ningún sistema bien hecho, pedirá al administrador de sistemas obtener la contraseña de un usuario.
  - Toda cuenta debe tener una contraseña, y nunca crear las cuentas con contraseñas predeterminadas:
    - Existen programas que generan contraseña. (pwgen)

Políticas de Seguridad

- Al cotizar equipos:
  - Evaluar soporte y actualizaciones
  - Evaluar historial de seguridad, y de reparación de bugs.
  - Es MUY raro que un equipo no tenga fallos de seguridad.
  - No comprar de empresas que dejar pasar los bugs. (A menos que hayan indicado el fin del soporte del producto (EOL)).
- Al elegir software:
  - Reporte de bugs arreglados.
  - Suscribirse a la lista de anuncios
  - El problema de “Dancing Pigs”
  - Imponer seguridad sobre comodidad

Firewalls

- Regla de Oro:
  - “Denegar todo, permitir según sea absolutamente necesario y **firma de venta del alma del solicitante**”
- Establecer un esquema de red
  - Internet
    - Proveedor de acceso a internet
  - DMZ
    - Segmento de red a la cual se puede tener acceso desde internet
    - Hay salida y entrada de conexiones.
    - DMZ no puede acceder a Intranet.
  - Intranet
    - Segmento de red a la cual ningún computador de internet puede tener acceso.
    - Solo hay salida de conexiones.
    - Intranet puede acceder a Internet e Intranet.

Ataques

- IP Spoofing
  - Se cambia la IP de origen en los mensajes
    - DNS Amplification
- DoS (Denial of Service)
  - A través de algún método (variante), lograr que un servicio no tenga disponibilidad
    - Spam
    - DNS Amplification
    - ICMP Flooding
- Malware
  - Software malicioso, a veces crackeado para portar código malicioso.
  - Virus
  - Adware: No es solicitado

Ataques

- Fuerza Bruta
  - Averiguar la password mediante ataque combinatorial
- Basado en Diccionario
  - Utiliza palabras de un diccionario, modificándolas según reglas usuales.
- Falsificación de Identidad
  - Ataque muy usual, dado que el sistema de email posee la misma seguridad que el correo tradicional.
- Buffer Overflow
  - Se aprovecha fallos en los códigos de programas, para reescribir el mismo programa.
- Cross-site Scripting
- SQL-Injection

Modelos de Seguridad (1/2)

- Existen muchos modelos de seguridad, pero Linux solo implementa 2:
- Recursos: cada recurso, poseen atributos que indican quien puede o no realizar cierta acción sobre el recurso.
  - Normalmente es muy costoso, el indicar todos contra todos, así que se reduce a:
    - A: all
    - U: user
    - G: group
    - O: other

Modelos de Seguridad (2/2)

- ACL (Access Control List)
  - Cada agente del sistema (usuario, programa, kernel), se le indica que es lo que puede realizar.
    - Mucho mas costoso, no fue posible de implementar hasta hace poco en sistemas operativos.
    - SELinux y NSA

¿Te interesa al tema?, donde continuar...

- IDS e IDP
  - Detección y prevención de intrusos
- Temas de Actualidad
  - Worm Storm
  - Explosión de Spam
- Linux
  - SELinux
  - HoneyNET
- Departamento
  - Ramo de “Seguridad de Sistemas Computacionales”
  - News (resucitarlo)