Bisoños Usuarios de GNU/Linux de Mallorca y Alrededores | Bergantells Usuaris de GNU/Linux de Mallorca i Afegitons

Módulo 4.1.2 Servicios RPC: NIS y NFS (32145 lectures)

Per **Daniel Rodriguez**, ***DaniRC*** (http://www.ibiza-beach.com/)

Creado el 12/08/2003 23:09 modificado el 12/08/2003 23:09

Traducción al castellano del Módulo 4.1.2 de MandrakeCampus. Ahora MandrakeCampus es parte del Club Mandrake.

Presentacion de los servicios RPC

Una tecnología de Sun Microsystems

Los servicios de RPC (Remote Procedure Call) son un conjunto de servicios desarrollados por Sun para permitir la interaccion de varias máquinas en una red.

Los protocolos de comunicacion son publicos, lo que permite que la mayoria de los servicios se implementen sobre distintos sistemas operativos. Este un elemento esencial para la interoperabilidad.

Un elemento esencial: el portmapper

Los servicios de RPC tienen un punto en comun: la utilizacion de un portmapper. Se trata de un servicio similar a inetd. Sin embargo, si bien inetd tiene puertos fijos para cada servicio, este no es el caso de RPC. Los servicios RPC son registrados en el portmapper, que les ofrece un puerto cuando lo necesitan. Cuando una maquina necesita un servicio RPC, esta maquina contacta con el portmapper que ejecutara el servicio e informara al cliente de a que puerto debe dirigirse.

Los principales servicios de RPC

La comparticion de ficheros

El servicio RPC que permite la comparticion de fichieros es el NFS. Se trata de un sistema de ficheros compartido en red. Desde el punto de vista del cliente se comporta como un sistema de ficheros local y se integra perfectamente en el arbol de directorios Unix. Como todo sistema de ficheros Unix, el NFS controla el acceso a los ficheros, propietarios y grupos.

La comparticion de "agendas".

La comparticion de Agendas es un medio relativamente sencillo de permitir a los usuarios que se conecten a cualquier maquina de la red con una sola contraseña. Cuando un usuario se conecta, la maquina lanza una consulta al servidor de NIS y este valida la contraseña. El servidor de NIS se encarga de verificar la identidad del usuario e informa a la maquina sobre la que se conecta el usuario del exito o fracaso de dicha autentificacion.

Los otros servicios son obsoletos.

Existen varios otros servicios RPC. Pero hoy en día se considera su utilización algo anecdótico. Sirven principalmente para recopilar informacion sobre las maquinas conectadas a la red, con el objetivo de facilitar la administracion centralizada.

Los servicios RPC se concibieron para funcionar en entornos seguros. Es peligroso usarlos hoy en dia ya que no son demasiado buenos bajo el punto de vista de la seguridad. El principal problema es que no utilizan encriptacion sobre los datos que hacen circular sobre la red.

La comparticion de "Agendas"

Ventajas de la uniformidad

Cuando tenemos que administrar un importante numero de ordenadores es particularmente molesto tener que recordar contraseñas para cada sector de la red. Sobretodo si hablamos de las rebuscadas contraseñas de administracion.

El problema es aun mas grave con los usuarios finales, sobretodo si estos deben usar varias maquinas diferentes con frecuencia. Nos encontramos con contraseñas tales como "12345" repetida varias veces en varias máquinas.

La comparticion de agendas, es decir: la centralizacion de la gestion de usuarios nos va a permitir resolver estos problemas:

Una puesta en marcha algo pesada

Esquematicamente, cuando un usuario se conecta a una maquina, esta consulta un fichero de contraseñas (generalmente /etc/passwd o talvez /etc/shadow) y verifica la identidad proporcionada por el usuario.

Con NIS, la maquina interroga al servidor de NIS para pedirle que haga la comprobación. Todas la maquinas de la red utilizan entonces el mismo fichero de contraseñas, lo que simplifica la vida de los usuarios. Hay por contra un inconveniente y es que cuando un usuario tiene acceso a una maquina obtiene acceso a todas las maquinas de la red. Esto conlleva problemas de seguridad, pero NIS fue concebido donde el nivel de confianza entre usuarios/maquinas es altamente elevado.

Compartir ficheros

Historial de NFS

Los servicios de NIS y NFS son parte de los servicios llamados RPC y son complementarios.

NFS es un protocolo que data de los años 80. En esas fechas los problemas de seguridad eran menores. Todavia podian construirse protocolos basados en la confianza, tanto el servidor como el cliente confiando en la información que intercambian. Internet convierte este principio en algo absurdo y este es sin duda uno de los mayores problemas de NFS. La version 2 del protocolo es la primera version publicada y sigue la siendo la mas extendida en nuestros dias.

Existen implementaciones sobre varias plataformas diferentes y se han descrito pocos problemas de compatibilidad.

La version 3 del protocolo data de 1992 y presenta varias mejoras:
- Mejora del rendimiento debido a la reescritura del codigo de la red, y al uso de paquetes de datos mayores.
- Mejora en la seguridad:
  - Listas de ACL (Listas de control de acceso) que permiten difinir acceso a los recursos por UID y fichero a fichero.
  - Implementacion de un sistema de autentificacion basado en contraseña.

Por desgracia, la version 3 de NFS para Linux esta todavia en pañales. NFS para GNU/Linux es intrinsecamente inseguro y peligroso si se administra mal.

Funcionamiento teórico.

NFS es una interfaz entre el sistema de ficheros fisico, sea el que sea -ext2 por ejemplo- y un sistema remoto. Cuando NFS recibe una peticion via red, opera las modificaciones sobre el sistema local.
NFS dispone de todo lo que podemos esperar de un sistema de ficheros tipo Unix: gestion de permisos, propiedades avanzadas, enlaces, tuberias con nombre ... Pero como indica su nombre ha sido ideado para ser usado de forma transparente a traves de la red.
Desde el punto de vista del cliente, se trata de un sistema de ficheros clasico, se monta con mount, y se integra en la jerarquia de ficheros existente en la maquina. Todas las ordenes de entrada salida son enviadas al servidor que se encarga de procesarlas, controlar acceso concurrente a ficheros, etc.

Algunos problemas comunes

Problemas de seguridad

Lose servicios de RPC tienen en comun grandes agujeros de seguridad. Estos servicios son ya viejos, y en su epoca las redes eran mucho mas cerradas. Los fallos de los servicios de RPC son altamente conocidos y explotados sobre Internet. Una de las reglas basicas cuando utilizamos un servicio RPC es restringir el acceso a la red local y no realizar exports de forma descontrolada.

Incluso en una red local, hay que saber que las contraseñas circulan sin encriptar sobre la red. Cualquier máquina puede "escuchar" los intercambios entre un cliente NIS y el servidor y descubrir un buen numero de contraseñas. Por defecto no se utiliza ningun algoritmo de cifrado.

Una arquitectura envejecida

Utilizacion del protocolo UDP (User Datagran Protocol), en modo no conectado. Hay algunas ventajas, en particular cuando la red esta sobrecargada, pero se trata mas de una herencia que de otra cosa. El protocolo TCP esta mucho mas adaptado, pero no es soportado mas que por las ultimas versiones de NFS, y algunos clientes no lo soportan todavia.

Configuracion de un cliente de NFS

Montaje de las particiones

Para poner en servicio un cliente de NFS, hay que asegurars de que el kernel de Linux que estamos usando tiene compilado el soporte para NFS.

Para montar una particion hay que conocer algunos parametros:

el nombre del servidor
el nombre de la particion a la que se desea acceder
el nombre del directorio donde vamos a montar la particion NFS.

La sintaxis del comando mount es la siguiente:
mount -t nfs maquina:/particion/a/montar /punto/de/montaje

Nota : Se puede facilitar el montaje de una particion si la incluimos en el /etc/fstab para que se monte al iniciarse el sistema.

Podriamos usar algunas opciones de montaje para dotar de mayor segurudad el sistema. La opcion -o nosuid quita el bit SUID sobre los ejecutables montados por NFS. Esto puede resultar molesto si estamos montando /usr pero tiene sentido si estamos montando particiones de datos. La opcion -o noexec es todavia mas radical, ya que imposibilita la ejecucion de programas desde la particion montada por NFS. Si tenemos usuarios que escriben scripts esta opcion puede ser muy molesta.

Ejemplos de uso.

Los ejemplos de uso de una particion NFS son numerosos. Podemos imaginar, entre otros, una particion de lectura/escritura sobre /home. Asi cada usuario puede trabajar sobre cualquier maquina de la red encontrando siempre sus ficheros personales sin esfuerzo.

Nota : Es frecuente que se exporten los buzones de correo de los usuarios. Esta es una mala idea, ya que la gestion de concurrencia de NFS no es muy fiable y exportar /var/spool/mail por ejemplo, puede producir perdidas de mensajes.

Podemos tambien compartir una particion que contencta ejecutables, como /usr/bin para ganar algo de espacio en disco sobre las maquinas locales. Llegando al extremo podriamos tener ordenadores sin disco duro trabajando directamente sobre particiones NFS.

Montar automaticamente las particiones NFS

Utilizaremos a este proposito el /etc/fstab como para cualquier otro sistema de ficheros.
maquina:/partition/distante /punto/montaje nfs defaults 0 0
maquina:/partition/distante /punto/montaje nfs noauto,user 0 0

La primera opcion permite montar la particion automaticamente en el arranque. La seguna opcion permite que cualquier usuario monte la particion con mount, pero no la monta en el arranque.

Particularidades de la particion montada.

Los derechos de propiedad (permisos de acceso)

Cuando navegamos por una particion montada, podemos constatar una serie de cosas. Lo primero es que los propietarios de los ficheros sobre el servidor y sobre la maquina local no concuerdan. Es que Linux no usa los nombres de usuario y grupos sino que utiliza los codigos de usuario y de grupo (UID, GID). Las equivalencias aparecen en /etc/passwd /etc/groups respectivamente. Estos ficheros no son compartidos por NFS.

Ahora imaginemos lo siguiente: el usuario TOTO dispone de una cuenta en el servidor donde tiene asignado el UID 542 y alli tiene algunos ficheros de su posesion. Su particion de trabajo es importada sobre otra maquina donde el UID 542 corresponde al usuario TITI. Esto es un problema porque ahora TITI puede acceder a los documentos de TOTO pero TOTO no puede acceder ni a sus propios documentos! Se trata de uno de los inconvenientes ligado a NFS.

Varias soluciones son posibles, siendo la mas evidente el uso de NIS para tener un control de usuarios uniforme.

Los accesos concurrentes

Las diferentes versiones del protocolo NFS dejan en manos del implementador la solucion de los problemas derivados de la concurrencia. Uno de los problemas mas habituales en una red lenta o subestimada es que las particiones pueden ser desmontadas de forma "violenta" cuando los tiempos de respuestas son excesivamente lentos. Esto conlleva problemas de perdida de datos.

Configuracion de un servidor de NFS

Los diferentes tipos de servidor

Existen dos servidores NFS en GNU/Linux, uno funciona como un servidor tradicional y el otro integrado en el kernel. Este ultimo es frecuentemente llamado knfsd, y ofrece mejores resultados en terminos de rapidez. Se le reprocha en todo caso una falta de estabilidad pero este deberia ser un problema temporal.

Paquetes que instalar

Los paquetes de utilidades suelen ser dos:
nfs-utils-clients
nfs-utils

Las herramientas del cliente: showmount

Estrictamente hablando solo es necesario el programa mount para hacer funcionar un cliente de NFS. Pero las utilidades de cliente son a menudo muy utiles. Showmount en este caso, nos permite ver la lista de particiones NFS montadas por otras maquinas dentro de la red.

Las herramientas del servidor : mountd, nfsd

Si estamos usando el NFS incluido en el kernel, el trabajo lo lleva a cabo directamente el modulo nfsd.o de Linux. El programa rpc.nfsd solo sirve para comunicar el portmapper con el kernel.

El programa rpc.mountd es el programa responsable de la seguridad de los montajes con NFS. Cuando una maquina cliente solicita la exportacion de una particion, mountd verifica si dicha maquina cliente está autorizada.

Configuracion de un servidor de NFS

Definir las particiones y los clientes

El fichero /etc/exports

El fichero /etc/exports contiene la lista de las maquinas y de los repertorios que deben ser exportados. La sintaxis es:
/directorio maquina1(option) maquina2(option) ...
/usr titi(ro) 192.168.2.5(rw)

La mayoria de implementaciones de NFS no autorizan la exportacion de un subdirectorio de un directorio previamente exportado. El servidor de NFS del kernel si que permite esta opcion y esto puede favorecer ciertas configuraciones. Entre las opciones mas corrientes, podemos citar las opciones de seguridad que veremos mas adelante y las opciones de montaje tales como rw o ro que permiten la exportacion en modo lectura/escritura o solo lectura respectivamente.

Por defecto los directorios son exportados en modo rw.
Los nombres de las maquinas pueden ser nombres DNS, direcciones IP, clases de direcciones IP o dominios enteros. Si estamos utilizando NIS podemos tambien precisar el nombre de un grupo de NIS. Veremos esta ultima opcion mas adelante.

Modificar dinamicamente las particiones exportadas.

El servidor NFS no actualiza los cambios realizados en el fichero /etc/exports. Hay que activarlos usando el comando exportfs.

Releer la configuracion: exportfs -r

Este comando permite sincronizar la lista de montajes posibles, conservada en /var/lib/nfs/xtab sobre el fichero /etc/exports

Anular la exportation : exportfs -u directorio

Este comando nos permite interrumpir momentaneamente la exportacion de uno o varios directorios. Este comando no modifica el contenido de /etc/exports y la modificacion no es definitiva. Esta opcion permite prohibir todo nivel de montaje, pero los montajes existentes no son desactivados.

Problemas de seguridad

La restriccion de los permisos de los clientes

Cuando el administrador de una maquina monta una partición NFS, dispone de permisos de acceso de escritura, como sobre cualquier otra particion del disco local. Si la red es administrada por varios usuarios root diferentes en maquinas distintas se sugiere el uso de la opcion root_squash en el fichero de /etc/exports

Esta opcion elimina los privilegios de root sobre la particion montada, lo que asegura la integridad de la misma. En el marco de una exportacion de /home impediria que el usuario root de una maquina cualquiera accediera a los directorios personales de todos los miembros de la red NFS.

Se puede usar tambien la opcion all_squash que otorga a todos los usuarios los privilegios de "nobody".

El problema del UID

Utilizar la opcion all_squash

El problema de propiedad de los ficheros no es particularmente sensible que cuando tratamos con particiones de usuarios. Es posible esquivar el problema usando la opcion all_squash en el montaje.

En primer lugar no montamos directamente /home en el conjunto de maquinas cliente, sino que el servidor debe exportarlas una a una sobre cada cliente. Hecho esto usamos la opcion all_squash para que todas las modificaciones remotas sean consideradas como realizadas por nobody. Las opciones anonuid=UID y anongid=GID nos permiten reemplazar nobody por el UID y el GID del usuario en cuestion para que tenga acceso a su directorio personal sin problemas.

La autentificacion por maquina funciona relativamente bien si los recursos personales son montados desde clientes windows donde solo hay un usuario. Es sin embargo es problematico en entornos multi-usuario.

La comparticion de la "agenda".

El servicio NIS

Metodo de funcionamiento

El protocolo de NIS funciona bajo el modelo cliente/servidor. Los servidores (que pueden cooperar para balancear la carga) disponen de listas de usuarios, de grupos y de contraseñas para uno o varios dominios. Donde dominio es un grupo de maquinas que comparte la misma agenda. Cuando un usuario necesita autentificarse ante la maquina la informacion que proporciona se compara con la que dispone el servidor NIS.

Las diferentes versiones.

Existe NIS y NIS+ con soporte para encriptacion. En estos momentos NIS+ es bastante experimental e inestable, asi que nos centraremos en NIS.

Terminologia.

Los dominios de NIS

Grupos de máquinas.

Un dominio NIS agrupa varias maquinas, que comparten su base de datos de usuarios. En el interior del dominio cohabitan el servidor maestro, algunos servidores de replicas, llamados esclavos, y el conjunto de clientes.

Utilizando los protocolos YP (o NIS)

Antes de llamarse NIS, este servicio se llamaba Yellow Pages, en referencia a su papel de "paginas amarillas". El propietario de la marca (British Telecom) se quejó y el servicio cambió de nombre. En recuerdo, la mayoria de programas relativos a NIS llevan el prefijo yp.

NIS es un servicio RPC

Como todo servicio RPC se necesita un portmapper y tener conciencia de que es un protocolo inseguro salvo en redes aislas del exterior con alto nivel de confianza en los usuarios.

Los shadow passwords son desaconsejados.

La comparticion de contraseñas en red necesita que todas las maquinas utilicen el mismo metodo de cifrado de contraseñas. Es por ello que esta fuertemente desaconsejado usar shadow passwords o MD5 ya que son algoritmos dependientes de la maquina que los ejecuta.

Configuracion de un cliente NIS

Los paquetes yp*

Deberiamos instalar los paquetes

ypserv para herramientas del servidor.
ypbind para herramientas de cliente
yptools para herramientas varias de cliente de NIS

Aqui encontraremos utilidades para cambiar de contraseña frente a un servidor NIS sin tener que conectarnos directamente al servidor, por ejemplo.

Integrar un dominio NIS : el fichero /etc/yp.conf

El fichero /etc/yp.conf indica a ypbind con que servidor debe contactar. Generalmente un cliente NIS envia una peticion a todas las maquinas de la red y cualquier maquina de la red que pueda le responde. El cliente confia en que la respuesta es autentica, sin mas.

Para obetner esta conducta habitual se usa en el fichero /etc/yp.conf la opcion:

domain NOMBRE_DEL_DOMINIO broadcast

Se puede hacer la transaccion algo mas segura pidiendo que se contacte un servidor en particular:
domain NOMBRE_DEL_DOMINIO server NOMBRE_DEL_SERVIDOR

El fichero /etc/nsswitch.conf

El fichero /etc/nsswitch.conf permite configurar un cierto numero de llamadas al sistema de la biblioteca de C, utilizado por la mayoria de ejecutables bajo GNU/Linux. Se trata de funcionalidades y de ficheros de configuracion correspondientes.

En el caso que nos interesa, se trata de configurar este fichero para que el sistema sepa que debe llamar al demonio ypbind para la autentificacion de usuarios y que no debe consultar unicamente los datos locales del /etc/shadow por ejemplo.
Para ello podriamos modificar las entradas para passwd, group, shadow y netgroup de esta forma:
passwd: compat
group: compat
shadow: compat
netgroup: nis

En estas condiciones, el sistema leera el fichero /etc/passwd para la autentificacion. Este debe contener referencias especificas a la autentificacion NIS, que abordaremos mas adelante.

Sobre una maquina que no use en absoluto NIS tendriamos algo como esto:
passwd: files
group: files
shadow: files

Si deseamos usar unicamente informacion proporcionada por NIS podriamos hacer esto:
/etc/nsswitch.conf :
passwd: nis
group: nis
shadow: nis

Esta ultima opcion se desaconseja porque si falla el servidor o si falla ypbind nos quedamos sin acceso a la maquina.

El fichero /etc/passwd

Para hacer que /etc/passwd busque informacion en el servicio de NIS debemos agregar una linea tal que asi:
+::::::

Se trata de una entrada de /etc/passwd totalmente valida. El + indica al sistema que debe interrogar a NIS para completar los datos que le falten (los campos vacios). Esta linea se coloca al final del fichero, lo que nos permite tener usuarios locales que podran identificarse sin pasar por NIS.

Modificacion de los paramentros de la base de datos de NIS.

Podemos prohibir a ciertos usuarios de NIS el acceso a la maquina. Para ello usamos la linea:
-usuario::::::
+::::::

La primera linea invalida el acceso al usario. Si deseamos dar acceso a un numero muy restringido de usuarios, la mejor forma de hacerlo sera:
+autorizado1::::::
+autorizado2::::::
+::::::/bin/false

De esta forma los usuarios autorizados seran aceptados y todos los demas iran a parar a un /bin/false que les cortara el acceso al sistema.

Como esto se indica el en /etc/passwd se superpone a las posibles respuestas que pudiera ofrecer NIS

Los ficheros /etc/group y /etc/shadow

Hay que modificar estos ficheros igual que hemos hecho con el /etc/passwd

Las modificaciones que hacemos no aportan gran cosa, nos podemos contentar con poner en /etc/group una linea tal que asi:
:::
y en /etc/shadow
:::::::

Despues de los cambios hay que relanzar el servicio con un kill -HUP pid-ypbind, o haciendo un /etc/rc.d/init.d/ypbind restart

Configuracion de un servidor de NIS

Generacion de la base de datos con ypinit

Un servidor NIS no exporta directamente ficheros tal como son. Transfiere una serie de bases de datos dbm (una para cada uno de los ficheros compartidos), que hay que generar en el momento de la configuracion.re de générer au moment de la configuration.

Configuracion de /var/yp/Makefile

La generacion de estas bases de datos se hace gracias al fichero /var/yp/Makefile que contiene todas las informaciones necesarias para guiar al programa ypinit.

Este fichero contiene comentarios sobre las opciones que es posible modificar. Destacaremos en particular las opciones MINUID y MINGID que permiten que no se añadan al registro los usuarios creados por el propio sistema tales como bin o mail.

La entrada all permite definir la lista de ficheros que vamos a incluir en la base de datos. La lista por defecto es talvez demasiado grande.
Unicamente passwd, group, y talvez shadow se pueden considerar esenciales. Otras como printcap, son generalmente innecesarias.

Una vez creadas las bases de datos podemos lanzar el demonio ypserv, con el comando /etc/rc.d/init.d/ypserv start

Podemos verificar el correcto funcionamiento del servidor interrogando al portmapper:
rpcinfo -u nombre_de_maquina ypserv

La respuesta deberia ser que el programa se halla correctamente registrado.

ypinit

El programa ypinit es un script que permite inicializar las bases de datos. Permite indicar a ypserv si se debe comportar como maestro, y exportar sus bases de datos sobre servidores secundarios, llamados esclavos, o si por contra debe comportarse como un servidor esclavo. En este ultimo caso tendremos que indicar a que servidor maestro hay que interrogar en busca de una actualizacion de las bases de datos.

ypinit -m

El script solicita cierta informacion a los posibles servidores esclavos. Volveremos sobre este punto mas adelante.

Administracion habitual

Cambiar la informacion de los usuarios.

Sobre un sistema clasico que utiliza el /etc/passwd tenemos varios comandos para cambiar la informacion de los usuarios.
- passwd permite cambiar la contraseña
- chsh permite cambiar el shell por defecto
- chfn permite cambiar el nombre completo del usuario (y otros datos incluidos en /etc/passwd)

En un dominio NIS, solo los cambios efectuados sobre un servidor maestro pueden ser tomados en cuenta. Lo normal es tener que reconstruir las bases de datos despues de cada cambio. Por suerte algunas herramientas nos dejaran realizar estos cambios desde el cliente. Se trata respectivamente de:
- yppasswd, ypchsh y ypchfn.

Estas ordenes estan concebidas para interactuar con otro servicio RPC el yppasswdd. Este recibe las llamadas de modificacion generadas por estas aplicaciones, actualiza el /etc/passwd del servidor y actualiza las bases de datos automaticamente.

Para usar estas funcionalidades es necesairo tener lanzado el servicio con el comando rpc.yppasswdd -e chsh -e chfn
Sin la opcion -e, unicamente se autoriza el cambio de contraseña.

Modificar las bases de datos.

Si realizamos cambios en el fichero de cotraseñas, como por ejemplo agregar usuarios, es necesario regenerar las bases de datos. Para ello basta con hacer make all en el directorio /var/yp

Configuracion de un servidor esclavo.

Un servidor esclavo es ante todo un cliente del servidor maestro.

El servidor esclavo no hace otra cosa que conservar una copia conforme de las bases de datos maestras. Es necesario que el esclavo disponga de un acceso de lectura sobre dichas bases de datos, lo que se hace al configurarlo como cliente.

Configurar el servidor maestro para que exporte sus bases de datos.

El servidor maestro debe ser informado de la existencia de servidores esclavos. Hay que modificar 2 elementos:

La variable NOPUSH del Makefile debe ser FALSE. De este modo el maestro enviara copias de sus datos a los esclavos en caso de modificacion.
Hay que volver a lanzar ypinit -m precisando los nombres de los servidores esclavos.

Configurar el esclavo.

En el servidor esclavo, inicializamos ypserv con la orden ypinit -s nombre_del_maestro

Nota: Recordar que ypinit es un script de shell. Puede que algo salga mal y tengamos que editarlo a mano, como por ejemplo para indicar otro path de busqueda para las bases de datos.

A pesar de que el servidor informa a los clientes de los cambios, pudiera ser que un cliente no quedara avisado de un cambio. Por estar el equipo apagado, por ejemplo.

Podemos forzar la sincronizacion lanzado periodicamente en el esclavo un comando de sincronizacion. Se podria poner algo tal que asi en el crontab:
0 * * * * root /usr/lib/yp/ypxfr_1perhour gt/dev/null 2>&1
0 12 * * * root /usr/lib/yp/ypxfr_1perday gt/dev/null 2>&1
0 6,18 * * * root /usr/lib/yp/ypxfr_2perday gt/dev/null 2>&1

Configurar los clientes

Los servidores esclavos no son utilizados mas que si se configuran los clientes en modo broadcast. En modo broadcast el cliente recibe la respuesta del primer ordenador de la red que le pueda responder y no de un servidor especifico.

Por seguridad lo mejor es configurar todos los clientes para acceder a un unico servidor maestro. El uso de servidores secundarios aporta pocas mejoras de eficiencia en el caso de NIS.

Para seguir aprendiendo ...

Referencias bibliograficas:

La mayoria de informacion que vamos a encontrar corresponde a los propios implementadores de protocolos NFS y NIS

http://sunsite.net.edu.cn/tutorials/NetworkingGuide/BOOKCHAPTER-12.html. Descripcion de NFS.
http://uhp.u-nancy.fr/linux/HOWTOFRENCH/NFS-HOWTO/NFS-HOWTO.html. La FAQ del How-To es muy interesante.
http://uhp.u-nancy.fr/linux/HOWTOFRENCH/NIS-HOWTO/NIS-HOWTO.html. How-to relativo a NIS
http://www.suse.de/~kukuk/nisplus/nis-utils/index.html. Pagina del proyecto dedicado a NIS+

E-mail del autor: dannircJUBILANDOSEbulma.net