Configuración integrada de servicios básicos de información de red: Servicio *install.hosts*

Integrated Configuration of Basic Network Information Services: Install.hosts service

O.Walid, T. de Miguel y D. Fernández

Resumen

Hoy en día tenemos a nuestra disposición un gran número de servicios de red (DNS, DHCP, etc.) que nos permiten ser usuarios de las redes de datos de forma más ergonómica, segura y agradable. Sin embargo, las tareas de configuración de esos servicios siguen siendo en muchos casos manuales, engorrosas y expuestas a errores humanos.

Para solucionar el problema, en el DIT-UPM, venimos desarrollando desde hace años un conjunto de herramientas que permiten la manipulación y configuración conjunta y sincronizada de los diferentes servicios de información de red que usamos para nuestras redes. Así, el DNS, el DHCP o la red WIFI se configuran todos a partir de una base de datos común (centralizada y simple). Además la administración de los servicios es independiente de su operación y resulta fácilmente extensible a otros servicios.

Las ventajas principales de esta integración son la seguridad y facilidad en la manipulación de los datos, la sincronización de los mismos y la posibilidad de realizar comprobaciones cruzadas. Nuestro artículo expondrá brevemente el funcionamiento de la herramienta *install.hosts* y las implicaciones que ha supuesto su utilización.

Palabras clave: Gestión de red, administración de servicios, dns, dhcp, dhcpv6, fwbuilder, iptables, ip6tables.

Summary

Nowadays there are a lot of network services (like DNS, DHCP, etc) that make us capable of using the data networks in an easy way, as well as more secure, ergonomic and pleasant. However, the configuration tasks associated to those services are generally carried out manually, being difficult and exposed to human errors.

To solve this problem in DIT-UPM context, we have developed a set of tools that allow manipulating and configuring in a synchronous way the different network information services we use inside our network. In this way, DNS, DHCP or the WIFI are all configured from a common database (centralized and simple). Besides, these services administration tasks' become independent from their operation and it is easily extensible to other services.

The main advantages of this integration are the security and the easiness when changing configuration data, the synchronization among the different configuration files and the possibility of making cross verifications. Our paper will briefly expose the operation of the install.hosts tool and the implications and experience derived from its use.

Keywords: Network administration, service administration, dns, dhcp, dchpv6, fwbuilder, iptables, ip6tables.

En el DIT-UPM, venimos desarrollando herramientas que permiten la manipulación y configuración conjunta y sincronizada de los diferentes servicios de información de red

La simplificación en la gestión de los sistemas básicos de red es muy productiva

1. Introducción

Uno de los principales problemas a los que se enfrenta hoy en día el administrador de servicios de red es la gran diversidad de los sistemas de información que son utilizados para proporcionar al usuario final la conectividad con el resto de las redes (y por ende a Internet). Estos servicios van desde los más básicos, como la asignación de una dirección IP de forma automática (DHCP), a los más complejos como pueden ser la autenticación del usuario a distintos niveles o incluso la movilidad del terminal de usuario entre múltiples dominios.

Si bien la gestión de cualquier servicio es susceptible de simplificación, en el caso de los sistemas básicos de red esta simplificación es aún más productiva, debido a que las tareas asociadas al mantenimiento de estos sistemas son las que más esfuerzo requieren por parte de los operadores de la red.

Para mejorar el rendimiento de estas tareas no sólo han de ser simples sino en la medida de lo posible, automatizables –tanto en su configuración como en fase de comprobación– y lo menos rutinarias posible para evitar los consabidos "errores humanos" que tanto tiempo hacen perder a operadores y usuarios finales, con la consiguiente degradación de imagen y servicio.

El objetivo de este artículo es mostrar al lector el enfoque que le hemos dado en el Departamento de Ingeniería de Sistemas Telemáticos de la Universidad Politécnica de Madrid al problema de la gestión de los servicios básicos de información de red, o más concretamente, a la configuración del DHCP, del DNS, del filtrado de direcciones IP y de la autenticación WiFi.

La idea de funcionamiento del programa era la utilización de una única tabla central de datos con las asociaciones entre las direcciones IP y los nombres de *host*

2. Evolución de *install.hosts*

Históricamente, allá por el año 1996, el motivo principal de la creación de nuestra herramienta *install.hosts* fue la sincronización de los sistemas de información que utilizábamos para la resolución de nombres y direcciones IP.

La idea de funcionamiento del programa era la utilización de una única tabla central de datos (que llamamos tabla.numeros) en la que aparecieran las asociaciones entre las direcciones IP y los nombres de *host*. El programa *install.hosts* habría de recorrer la tabla desde el primer hasta el último elemento introduciendo de una sola pasada el *host* (su nombre, dominio e IP) en cada uno de los archivos de configuración resultantes, es decir, en el archivo de configuración del servidor de páginas amarillas, en el de configuración del DNS y en la tabla de *hosts*.

A medida que surgían nuevas necesidades, *install.hosts* fue ampliando sus capacidades hasta las que tiene hoy en día y que son principalmente las siguientes:

A medida que surgían nuevas necesidades, *install.hosts* fue ampliando sus capacidades

- generación de bases de datos DNS (en formato ISC bind) para IPv4 e IPv6,
- generación de archivos /etc/hosts por grupos y redes IPv4 e IPv6,
- generación de archivos /etc/ethers,
- generación de archivos netgroup para sistemas NIS,
- generación de la configuración de sistemas de arranque remoto en formato BOOTP e ISC DHCP para IPv4 y en formato DHCPv6 (dhcpv6.sourceforge.net) para IPv6,
- generación de ACLs para la infraestructura Wi-Fi,
- generación de archivos de contabilidad de asignaciones IPv4 e IPv6,
- generación de lista de redes y máscaras de red respectivas,

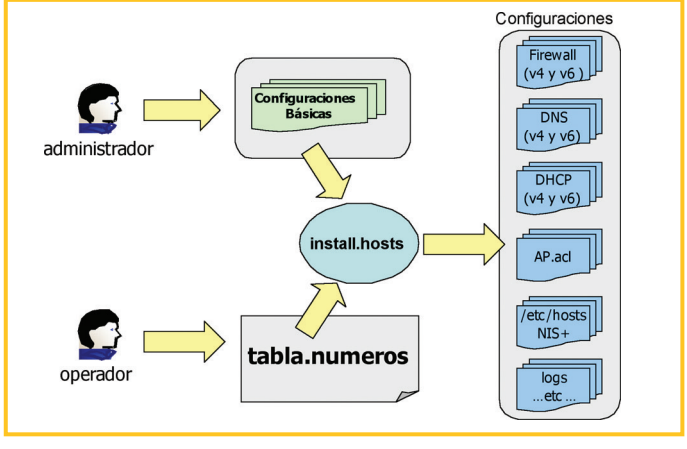
Además, de esto, también se encarga de las tareas de:

- distribución automática de las bases de datos y ficheros de configuración,
- reinicio automático de los servicios,
- comprobación rutinaria del funcionamiento de los mismos,
- comprobación de la definición de los hosts de las reglas de filtrado IPv4 e IPv6.

3. Estructura y subtareas de *install.hosts*

El programa *install.hosts* es un *shell script* que se encarga de enlazar las diferentes tareas necesarias para crear, distribuir y comprobar las diferentes bases de datos y configuraciones mencionadas anteriormente. En muchos de los casos, estas tareas las realizan a su vez otros *scripts* que se encargan de procesar los diferentes archivos de entrada para crear los archivos de configuración de los diferentes servicios, que son las salidas (figura 1).

FIGURA 1.
DIAGRAMA FUNCIONAL DE install.hosts



La tarea de generación de los archivos para el DNS, el DHCP, el BOOTP, las ACLs de Wi-Fi, las tablas de *hosts*, de *ethers*, de redes y de NIS a partir de la base de datos principal, la realiza un *script* escrito en *perl* y que recibe por nombre *mkhosts*. Este programa es el corazón del sistema *install.hosts* y se encarga de generar, partiendo de las cabeceras de los ficheros de configuración, de algunos otros archivos de datos (como el serial_no o el mx.DOM) y de los datos del tabla.numeros, las salidas en todos los formatos necesarios. La extracción de datos se realiza línea a línea, de forma secuencial y recorriendo el archivo tabla.numeros una única vez.

El programa *install.hosts* es un *shell script* que se encarga de enlazar las diferentes tareas

El *mkhosts* está pensado de tal forma que cualquier dato necesario para configurar un host en cualquiera de las bases de datos de servicio (DNS, DHCP, etc.) ha de estar definido antes de procesar la línea de *host*. Por ello, cuando *mkhosts* encuentra en tabla.numeros una línea de parámetros de configuración, actualiza las variables internas con el fin de que éstas apliquen (como máximo) hasta la siguiente subred o hasta que se encuentre otra línea de parámetros de configuración relativa al mismo servicio. Una vez que *mkhosts* ha sido ejecutado, quedan por realizar las tareas de distribución segura de las bases de datos, relanzamiento de los servicios y comprobación del funciona-miento de los mismos —en los casos necesarios—.

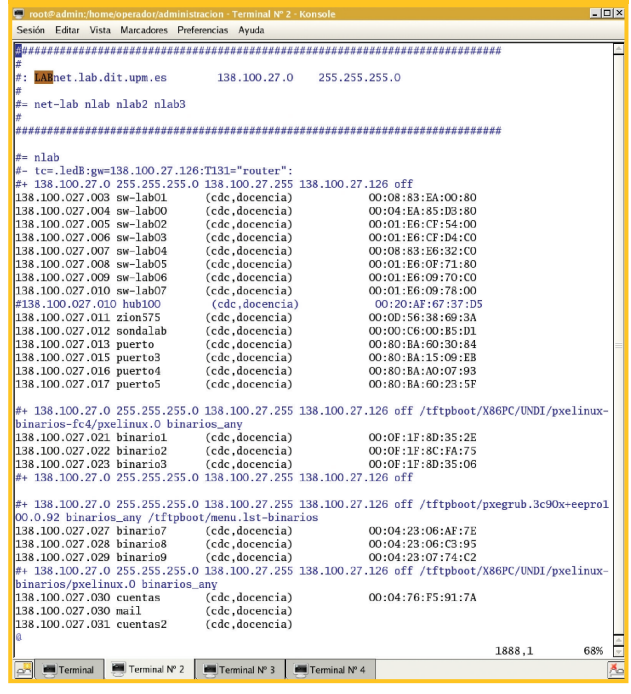
La extracción de datos se realiza línea a línea, de forma secuencial y recorriendo el archivo tabla.numeros una única vez

Para finalizar, en el año 2004 se añadió una nueva funcionalidad (y por lo tanto una nueva tarea): el análisis de las reglas de filtrado IPv4 e IPv6 en función del nuevo conjunto de *hosts*. Este análisis y sus tareas derivadas, permite disponer de un conjunto de reglas de filtrado (en cualquiera de las dos versiones del protocolo IP existentes) actualizadas con respecto a los *hosts* disponibles.

De esta forma se evita que existan reglas relativas a *hosts* antiguos y se automatiza la actualización de las direcciones MAC de los equipos a los que se les han cambiado las interfaces de red, permitiendo que el filtrado no sólo se realice a nivel IP sino también a nivel de trama (*ethernet*). También se borran los hosts que ya no existan, se actualizan en caso de haber cambiado de IP, se deshabilitan automáticamente las reglas que se hayan quedado sin *hosts* a los que ser aplicadas y se recompilan y redistribuyen las reglas de filtrado.

El sistema de filtrado IP soportado es *fwbuilder* (*www.fwbuilder.org*), una herramienta que se ha convertido en un estándar de facto para la gestión gráfica de reglas de filtrado IP ya que soporta múltiples filtros en S.O. tipo Unix (ipchains, iptables, ipfw, ...). *Fwbuilder* utiliza archivos XML para almacenar tanto los *hosts* como los servicios y las reglas de filtrado, y son éstos archivos XML los que se han de procesar para conseguir que estén permanentemente actualizados. El procesamiento se realiza a través de varios *scripts* en *perl* (checker.pl, filtraXML.pl, limpiaXML.pl) que se encargan de gestionar adecuadamente los archivos XML de la herramienta *fwbuilder* y de generar registros de los cambios realizados en ellos.

FIGURA 2.
FRAGMENTO DE tabla.numeros



En el año 2004 se añadió una nueva funcionalidad: el análisis de las reglas de filtrado IPv4 e IPv6 en función del nuevo conjunto de *hosts*

Como en 2004 *fwbuilder* no generaba reglas de filtrado para ip6tables (el equivalente de *iptables* en IPv6), se decidió utilizar el campo de comentario de los hosts en *fwbuilder* para almacenar la información IPv6 de cada *host*. Luego se fabricó un compilador de reglas IPv6 para ip6tables, el fw_ip6t.pl, que interpretaba todos esos comentarios de los archivos XML de fwbuilder. De esta forma, el tratamiento y actualización de las reglas de filtrado se realiza tanto en IPv4 como en IPv6 a través del *frontend* gráfico de *fwbuilder,* permitiendo gestionar ambos conjuntos de reglas de filtrado de una forma uniforme.

La base de datos central en la que se almacenan las configuraciones de red de los diferentes servicios que gestiona el install.hosts es básicamente, un fichero de texto con tres tipos de entradas

4. Formato del tabla.numeros

La base de datos central en la que se almacenan las configuraciones de red de los diferentes servicios que gestiona el *install.hosts* recibe el nombre de tabla.numeros. Es, básicamente, un fichero de texto que tiene tres tipos de entradas:

- líneas de comentarios, que son líneas que comienzan por el carácter almohadilla (#) seguido por un espacio y cualquier cadena de caracteres,
- líneas de parámetros de configuración, que comienzan por el carácter almohadilla (#) y siguen con uno o más caracteres especiales, se utilizan para especificar la configuración de un servicio determinado (por ejemplo, #: para el DHCP) de los que se gestionan, y
- líneas de *host,* que se utilizan para especificar un *host* por línea, y comienzan definiéndose a partir de la dirección (o sufijo) IP del *host.*

La estructura mínima de datos en tabla.numeros es la subred. En ella, un conjunto de líneas de parámetros de configura-ción y otro conjunto de líneas de *host* definen los sistemas IP que conforman la subred, permitiendo configurar para ella todos los servicios soportados (DNS, DHCP, etc). En la figura 2 podemos observar un fragmento del tabla.numeros relativo a la red del laboratorio del DIT.

5. Conclusiones

Las ventajas más importantes que ofrece la utilización de la herramienta *install.hosts* que hemos venido describiendo son las que se detallan a continuación:

A nivel técnico:

- configuración de los principales sistemas a partir de una base de datos central (tabla.numeros), procesándola de una sola pasada,
- base de datos central simple, secuencial, ampliable y basada en texto y marcas,
- utilización de archivos separados (cabeceras) para almacenar la parte fija de cada servicio,
- distribución segura e inmediata de los cambios,
- comprobación básica del funcionamiento de los sistemas más importantes,
- generación total (no incremental) de los archivos de configuración de los servicios cada vez (posibilidad de regenerar los servicios sin necesidad de *backups*),
- correlación automática (tanto en IPv4 como en IPv6) de los datos IP con los utilizados en las tablas de filtrado de los cortafuegos corporativos, corrigiendo así posibles incongruencias.

A nivel de operación:

- disminución notable y simplificación del número de tareas rutinarias a realizar para las configuraciones más habituales,
- homogeneización de las tareas del operador independientemente de la versión del protocolo IP utilizado para la máquina que se quiere configurar,
- concentración en un único archivo de los datos relativos al plan de numeración IP de la organización, permitiendo mostrar de un solo vistazo la información más relevante de cada red, *host* a *host,*
- dos niveles de configuración: por un lado, el operador, que se encarga de gestionar dominios y sistemas previamente preconfigurados a través del tabla.numeros, y por otro, el administrador, que es capaz de añadir nuevas cabeceras y configuraciones para los nuevos servicios y/o servidores.

Una ventaja importante de la herramienta es que facilita la distribución segura e inmediata de los cambios

Install.hosts/tabla.numeros ha demostrado ser una herramienta muy versátil, potente e integradora que permite gestionar de forma automatizada gran cantidad de servicios básicos de información de red y ahorrando una ingente cantidad de tiempo y esfuerzo a la hora de realizar operaciones rutinarias.

install.hosts/tabla.numeros ha demostrado ser una herramienta muy versátil, potente e integradora

Referencias

Para más información sobre la herramienta *install.hosts* (versión extendida de este documento), consultar el siguiente enlace: *www.dit.upm.es/cdc/install.hosts/*

Omar Walid Llorente
(omar@dit.upm.es)
Tomás de Miguel Moro
(tomas@dit.upm.es)
David Fernández Cambronero
(david@dit.upm.es)
Dpto. de Ingeniería de Sistemas Telemáticos
ETSIT - UPM