Network Documentation Tool - Netdot

Manual del Usuario

Contents

1 Copyright

1.1 Propósito

En este manual se documenta todo lo relacionado con la instalación, administración y operación de Netdot.

2 Introducción

Netdot es una herramienta de código abierto diseñada para ayudar a los administradores de red a obtener, organizar y mantener la documentación de la red.

Netdot se desarrolla de manera activa por el grupo de Servicios de Redes y Telecomunicaciones de la Universidad de Oregón.

Las características principales de Netdot son:

- Descubrimiento de dispositivos a través de SNMP
- Descubrimiento y visualización de topología de capa/nivel 2, utilizando las siguientes fuentes de información: CDP+LLDP, Protocolo Spanning Tree, tablas de reenvío de los switches y subredes punto a punto de enrutadores.
- Gestión del espacio de direcciones IPv4 e IPv6 (también conocido como IPAM), incluyendo organizacion jerárquica, visualización de direcciones en bloques y seguimiento de direcciones IP y MAC.
- Información del cableado de planta: edificios, oficinas, tomas de red, closets/armarios, enlaces entre edificios o dentro de los mismos, circuitos dedicados, etc.
- Información de contacto para las diferentes entidades que se documentan: departmentos, proveedores, fabricantes, peers BGP, etc.
- Netdot puede generar ficheros de configuración para un conjunto de herramientas de gestión y administración de redes:
  - Nagios,
  - Sysmon,
  - RANCID
  - Cacti
  - BIND y DHCPD de ISC
  - Smokeping
- Netdot implementa control de acceso por usuarios y roles, lo cual permite que tareas como la gestión de direcciones IP, la documentación de puertos de switches y la actualización de la información de contacto puede ser delegada a grupos específicos con acceso limitado a la interfaz web.

2.1 Estructura

Netdot está compuesto por los siguiente componentes:

1. Base de datos

   El objetivo es que Netdot no sea dependiente de un sistema de bases de datos en la medida de lo posible. En principio se puede usar cualquier base de datos soportada por Perl DBI. Existen, sin embargo, algunas limitaciones, por ejemplo, los scripts para las migraciones de esquemas son específicos de la base de datos pueden no estar disponibles. Actualmente el soporte para MySQL está completamente implementado. Existe un soporte parcial para PostgreSQL.

2. Las librerías

   El código principal está compuesto por clases de Perl orientadas a objeto, lo cual puede funcionar como interfaz de programación (API). Una ventaja de este modelo es que la presentación, captura de datos y base de datos puede distribuirse sin importar las diferentes arquitecturas.

3. Interfaz de Usuario (IU)

   La interfaz de usuarios web esta basada en un sistema de plantillas llamado HTML::Mason

4. Scripts de la interfaz de comandos (CLI)

   Algunas tareas como descubrimiento de dispositivos, mantenimiento de la BD, scripts de exportación de configuraciones, etc., pueden ser ejecutados desde la interfaz de comandos. También estas tareas pueden ser automatizadas ejecutándolas periódicamente a través de CRON.

3 Instalación

3.1 Obtener y desempaquetar el archivo de distribución

Descargar el paquete de Netdot más reciente desde el sitio web

`https://osl.uoregon.edu/redmine/projects/netdot/wiki/DownLoad`

Desempaquetar el archivo en un directorio diferente del aquél en que se desea instalar Netdot, por ejemplo:

```
~# tar xzvf netdot.tar.gz -C /usr/local/src/
```

3.2 Requerimientos

- Perl 5.6.1 o superior
- Apache2 con `mod_perl2`
- MySQL o PostgreSQL
- Servidor de autenticación (opcional). Netdot implementa autenticacion local y también a través de RADIUS y LDAP.
  - Para RADIUS, recomendamos FreeRadius, disponible en: http://www.freeradius.org/
  - Para LDAP, puede optar por OpenLdap, disponible en: http://www.openldap.org/
- El paquete RRDtool, incluyendo sus módulos Perl, disponible en: http://oss.oetiker.ch/rrdtool/
- el paquete GraphViz, disponible en: http://www.graphviz.org/
- La última versión de las MIBs de Netdisco http://sourceforge.net/projects/netdisco/files/netdisco-mibs/
- Varios módulos Perl

3.2.1 Instalación de dependencias

`Existen dos formas de instalar las dependencias: La primera forma (recomendada) es mediante los gestores de paquetes de la distribución que se está utilizando (este método no sólo instalará los módulos Perl, sino también los demás paquetes necesarios).`

- Para sistemas con APT (ej. Debian o sistemas basados en Debian como Ubuntu), ejecutar:

  ```
  ~# make apt-install
  ```

  Uno de los paquetes instalados es 'netdisco-mibs-downloader', el cual requiere que usted descargue e instale manualmente los ficheros MIB:

  ```
  ~# sudo /usr/sbin/netdisco-mibs-download\n";
  ~# sudo /usr/sbin/netdisco-mibs-install\n";
  ```

  Luego, deberá editar el siguiente fichero

  ```
  ~# sudo editor /etc/snmp/snmp.conf
  ```

y comentar esta línea (agregar un '#' al principio):

```
# mibs:
```

- Para sistemas con RPM (ej. Red Hat, Centos, Fedora), ejecute:

  ```
  ~# make rpm-install
  ```

  Pista Si después de ejecutar los pasos anteriores siguen faltando módulos Perl, se puede completar el proceso ejecutando el siguiente paso.

- Si su gestor de paquetes no está soportado, o si le faltan dependencias, puede instalar éstas a mano. Sin embargo, al menos tendrá la asistencia de la herramienta CPAN para instalar los módulos Perl automáticamente.

  Para verificar qué módulos Perl necesita, ejecute lo siguiente:

  ```
  ~% make testdeps
  ```

  Luego, el siguiente comando instalará los módulos necesarios:

  ```
  ~# make installdeps
  ```

  Si necesita instalar los módulos individualmente, puede ejecutar lo siguiente:

  ```
  ~# perl -MCPAN -e shell
  >install Module::Blah
  ```

3.3 Configuración

Netdot tiene un fichero de configuración que se necesita actualizar en función de las necesidades de la instalación. Se necesita crear una copia de `Default.conf` con el nombre `Site.conf`

```
~% cp etc/Default.conf etc/Site.conf
```

Realizado esto, se procede a modificar `Site.conf` en función de la configuración de instalación. En el fichero aparece cada una de las opciones con su descripción correspondiente.

Netdot leerá primero Default.conf y luego Site.conf

La razón para tener dos ficheros de configuración es que cuando se realice una actualización del sistema, el fichero `Default.conf` será modificado (para agregar nuevas variables, etc.) y así no será necesario sobreescribir el fichero `Site.conf` con las definiciones de la instalación anterior.

> **Pista** Tenga en cuenta que cada vez que actualice el fichero etc/Site.conf, es necesario reiniciar Apache para que los cambios surjan efecto en la interfaz web.

3.4 Actualización a nuevas versiones

Busque un fichero llamado doc/UPGRADE y allí encontrará instrucciones detalladas acerca de su distribución particular.

Debe verificar si la versión que está instalando tiene nuevos requerimientos:

```
~# make testdeps
~# make installdeps (or rpm-install, apt-install)
```

El esquema de la base de datos de Netdot **generalmente** sólo tiene cambios entre revisiones mayores. Por ejemplo, si se actualiza de la version 0.8.x a 0.9.x, se necesita ejecutar un script de actualización para adaptar la base de datos actual al nuevo esquema.

Si en su caso fuera necesario efectuar una actualización, puede hacerlo con el siguiente comando:

(haga una copia de respaldo de su base de datos primero!)

```
~# make upgrade
```

Luego instale el nuevo Netdot y reinicie Apache:

```
~# make install
~# /etc/init.d/httpd restart
```

3.5 Instalando Netdot por primera vez

- Prepare la cuenta de administrador de la base de datos (DBA)

  Usuarios de MySQL: La cuenta de DBA de MySQL generalmente se crea durante la instalación del paquete. Asegúrese de proporcionar una clave en este paso.

  Usuarios de Pg: PostgreSQL normalmente viene con una cuenta de DBA llamada 'postgres'. Al terminar la instalación, es posible que necesite configurar la clave para dicha cuenta como sigue:

  ```
  ~% sudo -u postgres psql postgres
  ```

  Configure la clave para el rol 'postgres' así:

  ```
  \password postgres
  ```

  Y escriba la clave cuando se le indique. Use Control+D para salir del diálogo.

- Ajuste la configuración de su base de datos si fuera necesario

  Usuarios de MySQL: Si planea utilizar las funciones de IPAM de Netdot, es posible que necesite incrementar el tamaño máximo del búfer de paquete en el fichero my.conf, por ejemplo:

  ```
  max_allowed_packet = 16M
  ```

- Compruebe que se ha creado el fichero etc/Site.conf, en el paquete de instalación, con las opciones de configuración en función de sus necesidades (Está explicado anteriormente).

- Luego proceda a crear la base de datos.

  ```
  ~% make installdb [parametros]
  ```

  Recuerde que necesita definir `DB_DBA` y `DB_DBA_PASSWORD` con el usuario y contraseña de administración de la base de datos en el fichero etc/Site.conf antes de ejecutar el comando. Alternativamente, se puede especificar `DB_DBA` y `DB_DBA_PASSWORD` como parámetros en la línea de comandos (como estos datos son usados frecuentemente por Netdot, necesita definirlos finalmente en el fichero etc/Site.conf

  ```
  DB_DBA=CUENTA-ADMIN-BASE-DE-DATOS
  DB_DBA_PASSWORD=CONTRASEÑA-CUENTA-ADMIN-BASE-DE-DATOS
  ```

- Ubicándose en el directorio raíz del paquete de instalación de Netdot, ejecute:

  ```
  ~# make install [parámetros]
  ```

  Opcionalmente, incluya los siguientes parámetros:

  ```
  PREFIX=DIRECTORIO-DE-INSTALACION (/usr/local/netdot)
  APACHEUSER=USUARIO-QUE-EJECUTA-APACHE (apache)
  APACHEGROUP=GRUPO-QUE-EJECUTA-APACHE (apache)
  ```

  > **Pista** Usuarios de Debian/Ubuntu: Probablemente tendrá que especificar las variables APACHEUSER y APACHEGROUP con el valor "www-data", el cual es el usuario con el que el servidor Apache se ejecuta.

3.6 Configuración del Servidor Web Apache

Edite el fichero plantilla de Apache que viene con Netdot para establecer la autenticación Local, RADIUS o LDAP. Cópielo en el directorio de configuración de Apache e inclúyalo en el fichero de configuración de Apache (httpd.conf), por ejemplo:

```
Include conf/netdot_apache2_<local|radius|ldap>.conf
```

Algunas configuraciones de Apache definen un directorio desde el cual se incluyen ficheros automáticamente cuando Apache se inicia. En ese caso, puede crear un enlace al fichero de Netdot desde ese directorio:

For example, in Debian or Ubuntu, it's a two-step process:

```
~# cd /etc/apache2
~# sudo ln -s /usr/local/netdot/etc/netdot_apache2_local.conf sites-available/netdot
~# sudo ln -s sites-available/netdot sites-enabled/netdot
```

O en otras distribuciones con sólo un directorio:

```
~# ln -s /usr/local/netdot/etc/netdot_apache2_radius.conf /etc/apache2/conf.d/netdot
```

> **Pista** Asegúrese de utilizar la versión del fichero que se copia en el directorio de instalación al ejecutar make install. No utilice el fichero que está en el directorio fuente del paquete. Al ejecutar el comando de instalación, este fichero de configuración de Apache cambia dinámicamente en función de las rutas de carpetas definidas.

Terminando todo lo anterior, reinicie Apache2. Si utiliza las opciones por defecto, cargue en su navegador la siguiente direccion:

```
http://nombreservidor.midominio/netdot/
```

Se muestra la página de autenticación, inicialmente puede entrar con las siguientes credenciales:

```
username: "admin"
password: "admin"
```

> **Pista** Si está utilizando las opciones de autenticación de RADIUS o LDAP, debe configurar en `/usr/local/netdot/etc/netdot_apache2_<radius|ldap>.conf` * la opción "NetdotRadiusFailToLocal" o "NetdotLDAPFailToLocal" con el valor "yes" según corresponda. Así se garantiza autenticación local mínimamente.

> **Advertencia** Recuerde cambiar la contraseña del usuario "admin" ! Vaya a `Contacts -> People`, busque 'Admin', haga click en [edit] e introduzca una contraseña nueva. Luego haga click en Update.

3.7 Tareas programadas utilizando CRON

Netdot utiliza una serie de *scripts* que deben ser ejecutados periódicamente como tareas programadas utilizando cron.

- Captura de las tablas de reenvío y ARP para seguimiento de las direcciones IP/MAC
- Los dispositivos de la red deben ser redescubiertos utilizando SNMP de forma periódica para mantener una lista de puertos, direcciones ip, etc.
- Descubrimiento de la topología de la Red
- Netdot mantiene un historial de registros para algunos objetos cada vez que son actualizados. Con el tiempo, los registros más antiguos son borrados de la base de datos para ahorrar espacio.
- Netdot genera documentación que es fácil de manejar utilizando comandos de filtrado (grep), por ejemplo: información sobre personas, localidades, asignaciones de puertos en dispositivos, etc. Esta documentación debería actualizarse exportándola frecuentemente.
- Pueden generarse configuraciones para otros programas utilizando la información de Netdot. Ver detalles más adelante.
- El fichero netdot.cron incluido en este paquete es un ejemplo de fichero de tareas programadas de cron para netdot. Se puede actualizar en función de las necesidades de instalación y copiarlo al directorio cron para su ejecución, por ejemplo:

  ```
  ~# cp etc/netdot.cron /etc/cron.d/netdot
  ```

4 Operación

4.1 Gestión de Dispositivos

En Netdot, los dispositivos (devices) representan equipos de infra- estructura de red: switches, enrutadores, cortafuegos, puntos de acceso inalámbrico, servidores, etc. Los nodos finales tales como computadores de sobremesa, laptops o printers no son 'devices'.

Netdot puede descubrir y gestionar un gran número de dispositivos de red. La vía más simple para obtener y almacenar esta información es consultar a los dispositivos utilizando Simple Network Management Protocol (SNMP). También pueden ser descubiertos individualmente, por subred o a través de un fichero texto con una lista de dispositivos.

4.1.1 Descubrimiento de Dispositivos utilizando la interfaz web

Ir a `Management -> Devices`. En las seccion "Device Tasks", se hace click en [new] y se escribe el nombre o la direccián IP del dispositivo que se desea adicionar, además se selecciona la comunidad SNMP y la version, luego se hace click en [discover]. Netdot entonces consulta al dispositivo utilizando SNMP y muestra una ventana donde se puede asignar un entidad propietaria (por ejemplo, la organización) y la entidad que utiliza el dispositivo (por ejemplo, los clientes), tambien la ubicación y la lista de contactos.

Si se está descubriendo un dispositivo de nivel 3 con reenvio IP activado (enrutador o cortafuegos), Netdot preguntará si se desea crear automáticamente las subredes que atiende ese dispositivo, basado en la configuracion IP de sus interfaces. Esta es una via efectiva para adicionar las subredes a Netdot.

Otra opción es definir si Netdot debe asignar a cualquier nueva subred las mismas entidades de propietario y usuario configuradas en el dispositivo.

Una vez que se hace click en el botón [update], Netdot muestra la información del proceso de descubrimiento y un enlace a la página del dispositivo.

Siempre se puede hacer una actualización del dispositivo a través de SNMP manualmente, haciendo click en el botón [snmp-update] en la esquina superior derecha de la página de dispositivos. Por ejemplo, si se ha adicionado un nuevo puerto, o tarjetas de interfaz u otra actualizacion física del dispositivo.

4.1.2 Interfaz de línea de comandos para el descrubrimiento de los

dispositivos

Asumiendo que está ubicado en la carpeta de instalación de Netdot (/usr/local/netdot).

Se puede descubrir un dispositivo específico ejecutando:

```
~# bin/updatedevices.pl -H <nombre> -I -c <comunidad-snmp>
```

Se puede descubrir los dispositivos de toda una subred ejecutando:

```
~# bin/updatedevices.pl -B 192.168.1.0/24 -I -c <comunidad>
```

También se pueden descubrir dispositivos desde una lista en un fichero texto:

```
~# bin/updatedevices.pl -E <fichero-texto> -I
```

El fichero debe contener una lista de dispositivos y sus comunidades SNMP respectivas, separados por espacio y un par dispositivo/comunidad por linea, por ejemplo:

```
dispositivo1 comunidad1
dispositivo2 comunidad2
dispositivo3 comunidad3
...
```

Netdot puede capturar las tablas ARP y de reenvío de los conmutadores. Las tablas ARP se obtienen de los dispositivos de nivel 3 (enrutadores y cortafuegos) y las tablas de reenvio de los dispositivos de nivel 2 (conmutadores). Ejemplo:

```
~# bin/updatedevices.pl -H <router> -A -c <community>
```

```
~# bin/updatedevices.pl -H <switch> -F -c <community>
```

Netdot puede descubrir la topología de la red, ejecutando:

```
~# bin/updatedevices.pl -T
```

Si la opción de configuración `ADD_UNKNOWN_DP_DEVS` está activada, entonces Netdot intentará descubrir nuevos dispositivos adyacentes, si éstos fueren vistos (via CDP/LLDP) en las interfaces de los dispositivos existentes. Con el comando anterior, Netdot sólo intentará descubrir dispositivos directamente conectados. Si se desea que Netdot descubra los dispositivos adyacentes, y los adyacentes a éstos, entonces debe utilizar el siguiente parámetro:

```
~# bin/updatedevices.pl -T --recursive
```

Generalmente, una vez que se han descubierto todos los dispositivos de la red, se pueden actualizar todas estas informaciones ejecutando una tarea programa de forma periódica (e.j. cada hora) utilizando CRON. La línea para el cron sería la siguiente:

```
0 * * * * root /usr/local/netdot/bin/updatedevices.pl -DIFAT
```

Si desea actualizar solamente un subconjunto de los dispositivos existentes en su base de datos, puede utilizar el parámetro "–matching" para especificar un patrón (expresión regular) que servirá para filtrar los dispositivos basado en su nombre completo. Por ejemplo, si todos sus enrutadores tuviesen nombres con el prefijo "-gw", podría hacer algo como:

```
0 * * * * root /usr/local/netdot/bin/updatedevices.pl -DIFAT --matching "-gw"
```

Se pueden encontrar ejemplos de configuraciones para cron en etc/netdot.cron

4.1.3 Documentación de dispositivos

Una vez que se ha adicionado un dispositivo, se puede completar su documentación con más información.

Ir a `Management -> Devices` para realizar un búsqueda del dispositivo por nombre, dirección IP o MAC.

Desde la página del dispositivo, se puede navegar a diferentes sub-secciones o pestañas, en función de la información que se desee editar.

Pestaña Basics: En esta sección puede ver y editar información general sobre el dispositivo, por ejemplo su ubicación, la información de contacto y otros detalles de gestión.

Interfaces: Aquí se pueden editar las descripciones de las interfaces, asignar los conectores de red, etc, haciendo click en el boton [edit]. Se puede editar una interfaz específica haciendo click en su número o nombre. Si se ha ejecutado un descubrimiento de la topología, se puede ver la información de los dispositivos adyacentes. Si por alguna razón el proceso de descubrimiento de la topología no detecta los dispositivos adyacentes, estos se pueden adicionar manualmente haciendo click en el botón [add] de la columna "neighbor".

Cuando se adiciona un vecino de forma manual, se activa el marcador "Neighbor Fixed" en el objeto Interface. Este marcador evita que el proceso de descubrimiento de la topología de la red elimine esa conexión.

> **Pista** Las conexiones entre dispositivos adyacentes tienden a cambiar a medida que se reemplaza el hardware y se cambian las conexiones. Es por eso que las definiciones de conexiones fijas (Neighbor Fixed) pueden quedar obsoletas con facilidad. Es recomandable dejar al proceso de descubrimiento de la topología actualizar la conexiones entre dispositivos.

Pestaña Módulos: Si el dispositivo provee información de módulos de hardware via SNMP, Netdot la mostrará en esta sección. Los módulos se muestran organizados jerárquicamente dependiendo de cómo los módulos están incluidos dentro de otros.

Pestaña IP: Esta sección lista todas las direcciones IP utilizadas por el dispositivo, junto con las subredes a las que pertenecen, las interfaces donde están configuradas, y de manera opcional, su nombre DNS.

Al final de esta sección, encontrará un diálogo para marcar la opción "Auto DNS" en todas las interfaces con direcciones IP. La finalidad de esta opción es

hacer que Netdot genere nombres de DNS para cada dirección IP basándose en el nombre de la interfaz y del dispositivo.

La lógica de esta operación se delega a un módulo "plugin", lo que significa que usted puede escribir su propio plugin para generar nombres DNS basado en su propio esquema (vea el fichero de configuración para más detalles). El plugin incluido con Netdot genera nombres como "ge-0-1.router1.mydomain.com", asumiendo que el nombre del dispositivo fuera 'router1' y la interfaz GigabitEthernet0/1. Esto es súmamente útil para cuando se está utilizando la herramienta 'traceroute'.

Para que este mecanismo funcione, necesita lo siguiente:

- El dispositivo ha de tener la opción 'Auto DNS' activada globalmente (pestaña Basics) de la página de dispositivos.
- Cada interfaz con una IP address debe tener la opción 'Auto DNS' activada
- La dirección IP debe pertenecer a un bloque IP al cual se le haya asignado un dominio (Zone) de DNS (Management -> Address Space)
- Para que se generen también los récords tipo PTR, el bloque IP debe tener una zona inversa asignada (in-addr.arpa o ip6.arpa).

Pestaña BGP: Si el dispositivo es un enrutador con sesiones BGP, y la información se puede capturar con SNMP, Netdot mostrará esta información en esta pestaña. Entre los campos mostrados están la dirección IP del vecino BGP, el ID y el AS. El récord BGPPeering también incluye campos opcionales para indicar el número máximo de prefijos IPv4 o de IPv6 que se han de permitir, o si la sesión se ha de monitorizar (con Nagios), etc.

Para cada AS descubierto, Netdot intenta encontrar más información utilizando la herramienta WHOIS. Si la información existe, se crea un récord tipo "entity" incluyendo el número y nombre del AS. Usted puede completar dicho record con más información de contacto, comentarios, etc.

4.2 Activos de Hardware (Assets):

Un asset en Netdot es un récord que contiene información común acerca del hardware red, por ejemplo, número de serie, dirección MAC, nombre del producto, etc. Además, los récords asset pueden usarse para documentar unidades adquiridas que aún no se han instalado. Una vez que el hardware haya sido instalado y descubierto con Netdot, el récord asset permanece y es referenciado por el nuevo dispositivo.

4.2.1 Importar Assets

Vaya a Management -> Assets -> [import] Este formulario le permite importar múltiples assets. Por ejemplo, puede utilizar un escaneador de códigos de barras para capturar la información desde las cajas de los equipos a medida que los recibe.

Cree un fichero de texto compuesto de número de pieza, número de serie y otros campos opcionales. El número de pieza debe coincidir con un récord tipo "product" en Netdot. El orden de los campos en cada línea debe coincidir con la lista de campos en el menú "Fields for import".

Una vez importados, puede ver un reporte de sus assets en la sección de reportes.

4.3 Gestión del espacio de direcciones IP

Netdot es una herramienta muy útil para la gestión del espacio de direcciones IPv4 e IPv6. Las principales características son:

- El espacio de direciones es organizado jerárquicamente utilizando un algoritmo de árbol binario, la misma técnica utilizada por los enrutadores para realizar búsquedas de prefijos.
- Nuevas subredes pueden ser creadas automáticamente a partir de la información obtenida de los enrutadores y cortafuegos.
- Interfaz muy intuitiva para visualizar el espacio usado y disponible, lo cual permite realizar las asignaciones con mayor claridad
- Gestión de configuraciones de DNS y DHCP

4.3.1 Bloques IP

Los objetos IP son llamados bloques IP. Estos objetos pueden representar direcciones de nodo o grupos de direcciones. La carcterística que los diferencia es el prefijo. Por ejemplo, un bloque IPv4 con un prefijo de 32 bits es una dirección de nodo, mientras que un bloque con un prefijo de 24 bits representa un grupo de 254 direcciones de nodo.

Cada dirección o bloque tiene un estado definido, los cuales se muestran en detalle a continuación.

Estado de los bloques IP Los objetos IP pueden tener un estado en función de su origen. A continuación se muestran los diferentes estados tomando en consideración si es una dirección de nodo o de bloque.

Los estados de una dirección de nodo son los siguientes:

- *Static*: Estas son direcciones que han sido asignadas de forma estática/manual a dispositivos o interfaces.
- *Dynamic*: Direcciones que pertenecen a un rango de direcciones y se distribuyen utilizando DHCP.
- *Discovered*: Direcciones que no han sido asignadas de manera estática o dinámica, pero han sido detectadas en la red, por ejemplo, a partir de registros ARP.
- *Reserved*: Direcciones que no deben ser asignadas.
- *Available*: Direcciones que han sido utilizadas anteriormente pero que están disponibles para ser utilizadas en otra cosa.

Por otro lado, los estados de un bloque IP son los siguientes:

- *Container*: Este tipo de bloque define un grupo o contenedor de otros bloques, como son bloques Subnet (subred) u otros bloques Container. Por ejemplo, el espacio de direcciones IPv4 por gestionar es 192.168.0.0/16. Además, se ha particionado el bloque anterior en dos bloques /17 y a partir de aqui se definen las subredes que se configuran en los enrutadores. En este caso, se define de la siguiente forma:

```
192.168.0.0/16 -> Container
    192.168.0.0/17  -> Container
        192.168.0.1/24 -> Subnet
        192.168.0.2/24 -> Subnet
    192.168.128.0/17 -> Container
        192.168.128.10/24 -> Subnet
        192.168.128.20/24 -> Subnet
```

- *Subnet*: Este tipo de bloque representa las subredes que son configuradas en las interfaces de los dispositivos de nivel/capa 3 (enrutadores y cortafuegos). Las subredes contienen direcciones de nodo que son asignadas a los usuarios finales.
- *Reserved*: De manera similar, los bloques reservados no son asignados bajo ningun concepto.

4.4 DNS

Netdot puede gestionar los datos de zona de DNS. Las zonas son exportadas como ficheros de texto para ser utilizados por el servidor DNS. Actualmente, sólo está implementada la exportación de ficheros de zona para ISC BIND.

Pista El mecanismo por el cual los ficheros de zona son transferidos y cargados al servidor de DNS se deja en manos de los administradores. Una vía para realizar esto es instalar un servidor DNS de forma local en el servidor que ejecuta netdot y guardar los ficheros de zona en un lugar donde el software dns pueda cargarlos periódicamente. Una configuración más compleja implicaría guardar los ficheros en sistemas de control de versiones (CVS, SVN, etc), los cuales pueden ser usados por sistemas de automatizacion de configuraciones como Puppet o CfEngine, que permiten ejecutar chequeos de sintaxis y cargarlos en los servidores DNS apropiados.

Netdot soporta los siguientes registros DNS: A, AAAA, CNAME, DS, HINFO, LOC, MX, NAPTR, SRV, y TXT.

Se pueden importar los ficheros de zona existentes hacia Netdot con la ayuda de la herramienta `import_bind_zones.pl` que está en la carpeta import

```
usage: import/import_bind_zones.pl
 [ -n|domain <name>, -f|file <path> ] (for single zone)
 [ -c|config <path>, -d|dir <path>  ] (for multiple zones)
 [ -g|--debug ] [-h|--help]

 -c  --config <path>   Fichero de configuración de BIND conteniendo definiciones de zona.
 -d, --dir <path>      Directorio donde ubicar los archivos de zona
 -n, --domain <name>   Dominio o nombre de zona
 -f, --zonefile <path> Fichero de zona
 -w, --wipe            Borrar información de zona existente
 -g, --debug           Mostrar información de depuración
 -h, --help            Mostrar ayuda
```

Para adicionar una nueva zona manualmente, vaya a `Management -> DNS Zones`. Opcionalmente puede seleccionar una zona para utilizar como plantilla (template). Esto indicará a Netdot que copie la zona de plantilla, incluyendo todos sus récords, y la guarde con otro nombre. Esto es útil cuando se deben crear múltiples zonas que comparten las mismas propiedades (récords NS, MX, etc.) Haga un click en [add]. Se mostrará una nueva zona creada a partir de la plantilla, o con los valores por defecto extraídos del fichero de configuración.

Una vez que la zona es creada, debe ser asignada a un bloque IP (Subnet o Container). Esto se realiza haciendo click en el boton [add] de la sección de bloques IP en la página de definición de zonas.

La forma más conveniente de crear zonas inversas (in-addr.arpa ó ip6.arpa) es yendo a la página del bloque IP correspondiente, sección DNS Zones, y hacer click en [add]. Si la zona inversa correspondiente no existe, Netdot le presentará el nombre de zona apropiado y la opción de crearla. Esto es especialmente últi con bloques IPv6, los cuales suelen requerir nombres de zona muy largos.

Alcanzado este punto, se pueden adicionar nuevos registros, haciendo click en el boton [add] de la sección *Records*. Los registros puede ser adicionados desde otras páginas de la interfaz web, por ejemplo, la página de direcciones IP o la página de DNS Records.

Los registros pueden ser importados completamente hacia la definición de zona, haciendo click en el botón [import] de la sección *Records* y pegando el texto del fichero de zona BIND en la caja de texto de la interfaz web.

Cada vez que la zona o su contenido es modificado, la operación es adicionada a una lista de cambios pendientes. Esta lista se guarda en una tabla de la base de datos llamada "hostaudit", y sirve para determinar cuándo una zona necesita ser exportada. Las zonas pueden ser exportadas de forma manual a través de la interfaz web en el menú *Export* o utilizando tareas programadas cron. Cuando una zona es exportada, su número de serie es incrementado y los cambios marcados como "pendientes" se cambian a "no pendientes".

Netdot puede generar y gestionar los registros DNS para direcciones IP que pertenecen a interfaces de dispositivos, como enturadores. La operación de cómo estos nombres son generados es manejada por un plugin y configurado *etc/Site.conf*. Para establecer que Netdot realice la generación de nombres para los dispositivos, configure la opción "Auto DNS" con el valor "yes" en la sección de gestión (*Management*) de la página de dispositivos. Después, se debe acceder a la pestaña *IP Info* del dispositivo y para cada interfaz con direccion IP establezca que la opción "Auto DNS" tiene el valor "yes".

4.4.1 El registro '@'

En Netdot, igual que en BIND, el registro '@' representa el dominio en cuestión (también llamado el ápice de la zona). Para adicionar registros que representan al dominio, como NS, MX, A, etc. este récord '@' debe existir. Netdot crea este récord automáticamente al momento de crear la zona. Además, crea dos récords NS (ns1.nombre-zona y ns2.nombre-zona) por defecto.

4.5 DHCP

Netdot puede gestionar la información de DHCP y generar las configuraciones para ISC DHCPD.

La información DHCP está organizada jerárquicamente alrededor del objeto de ámbito DHCP (*DHCP Scope*). Netdot soporta "ámbitos" de los siguientes tipos: global, subnet, shared-subnet, group y host. Cada uno de los "ámbitos" anteriores tienen asignados varios atributos.

4.5.1 Ámbitos Globales/Global Scopes

Un ámbito global representa a un servidor DHCP (o una pareja de servidores redundantes). Los atributos definidos en éste ámbito son los que se heredan en el resto de los ámbitos. Los atributos en ámbitos más específicos tienen preferencia sobre los atributos del ámbito global.

Para crear un ámbito global, haga click en `Management->DHCP`. Luego, haga click en el botón [new]. Se asigna al ámbito un nombre (por ejemplo, el nombre del servidor DHCP) y se seleccion el tipo "global". Los ámbitos globales no son contenidos por ningún otro ámbito, así que se deja el campo "Container" sin seleccionar.

Una vez que el ámbito es creado, se pueden adicionar atributos a él. Por ejemplo, haga click en el botón [attributes] y entonces haga click en el botón [add]. Se mostrará una nueva página donde se pueden crear nuevos atributos. Por ejemplo, se quieren adicionar una lista de servidores DNS. Introduzca "name-servers" en el caja de formulario "Name" y realice click en el botón "List". Seleccione el atributo "domain-name-servers" de la lista y adicione una lista de valores. Finalmente se hace click en Insert.

4.5.2 Ambitos de subredes/Subnet Scopes

Los ámbitos de subredes contienen atributos que se aplican a todos los dispositivos de una subred. Estos ámbitos están contenidos dentro del ámbito global.

La via más fácil para habilitar DHCP para una subred en particular es desde la página de "Subnet". Primero, es necesario asegurarse que la subred existe (se puede crear manualmente o descubriendo al enrutador que maneja esa subred). Se muestra la subred haciendo click en `Management->Address Space` y navegando hasta la subred o realizando una búsqueda de la dirección en cuestión.

Ya ubicados en la página de la subred, vaya a la sección Dhcp Scope y realice click en [enable]. Esto abrirá una sección donde se selecciona el ámbito global adecuado y la definición de enrutadores. Por defecto, Netdot muestra la primera dirección de la subred como valor para la definición del enrutador de la subred. Se puede cambiar este valor si la interfaz del enrutador tiene una dirección diferente. Haga click en "Save". Se mostrará el ámbito de subred en la página de subred. Si se realiza click en el nombre del ámbito, se mostrará la página con los atributos definidos, para realizar actualizaciones.

4.5.3 Ambitos de nodo/Host Scopes

Los ambitos de nodo permiten asignar atributos que se aplican a dispositivos específicos. Este tipo de ámbito tambíen establece un enlace entre la dirección Ethernet y la dirección IP.

Se puede crear un nuevo ámbito de nodo desde la página de récords DNS.

- Primero, se necesita un objeto de dirección IP estática. Se puede definir una dirección IP estática, si se selecciona de la página de Subred
- Cuando la dirección IP estática es creada, se le define un nombre. Se localiza la sección DNS A records y se realiza click en [add].
- Una vez que se ofrece un nombre para el registro A, se realiza una redirección hacia la página de dispositivos. Allí, se localiza la sección `DHCP for <IP address>` y se realiza click en [add]. Se introduce la dirección Ethernet y se guardan los cambios.
- Cuando se realiza click en la dirección Ethernet, se muestra la página de direcciones MAC, la cual tiene una sección "*DHCP Scopes*". Haciendo click en la dirección IP se mostrará la página de ámbitos DHCP, allí se pueden definir atributos para el dispositivo.

4.5.4 Plantillas de Ambitos/Template Scopes

Una plantilla de ámbito no es un ámbito real, sólo una colección de atributos que se pueden aplicar a elementos en grupo. Por ejemplo, el ámbito de dispositivos DHCP para un teléfono IP puede tener varios atributos que definan de dónde puede obtener su configuración. Se puede crear una plantilla que contenga estos atributos y utilizarla cada vez que sea necesario crear un ambito de dispositivos para teléfonos IP.

4.5.5 Ambitos Activos e Inactivos

La opción 'active' en el objeto Scope determina si éste ha de ser incluído cuando se exporta la configuración de DHCP. Por ejemplo, si usted quisiera documentar la asignación de direcciones IP a direcciones MAC en una subred, pero no desea usar DHCP en tal subred, puede definir un ámbito de subred y marcarlo como inactivo.

Similar a como se hace con los registros DNS, los cambios de DHCP se registran en la tabla "hostaudit", la cual Netdot utiliza para determinar si la configuración de DHCP necesita ser exportada. Ona vez exportada, los cambios marcados como "pendientes" se cambian a "no pendientes".

4.6 Información de Contacto

Netdot utiliza el concepto de "Contact Lists" para mostrar la información de contacto para diferentes objetos: dispositivos, localidades, entidades (departamentos, proveedores, etc.).

El objeto persona en Netdot contiene información personal como: domicilio, e-mail, números telefónicos, localizadores, etc.

Como una persona generalmente es el punto de contacto para diferentes elementos, entonces puede tener varios roles, lo cual enlaza a esa persona con un Lista de Contacto/Contact Lists determinada.

Se pueden crear nuevas Personas, Entidades, Localidades y Listas de Contacto en la sección *Contacts*.

4.7 Planta de Cableado

Netdot permite documentar el cableado entre edificios y del interior de los edificios, los armarios, conectores, etc.

4.7.1 Sites

Los Sites son generalmente edificios con uno o más niveles (floors), closets y habitaciones. Los Sites se pueden asociar a otras cosas como gente, departamentos, subredes, etc.

Para crear un Site nuevo, vaya a Cable Plant -> Sites -> [new]. Necesitará asignar al menos un nombre único. También el 'Site ID' es un valor (más corto) que representará a este Site de manera única dentro de su organización. Es posible incluir fotos de los Sites en la base de datos.

4.7.2 Closets

Los closets de comunicaciones alojan equipos de red y terminaciones de cableado. Un closet se ubica en una habitación (room), la cual se ubica en un nivel (floor), el cual se ubica en un edificio (Site).

Para crear un nuevo closet, vaya a Cable Plant -> Closets -> [new]. También es posible incluir fotos de los closets en la base de datos. Esto es útil para cuando los técnicos necesitan verificar las caracte- rísticas físicas del espacio del closet antes de visitarlo.

4.7.3 Cables dorsales (Backbone Cables)

Estos cables conectan dos closets entre sí.

- Si un cable físico atraviesa closets en varios Sites, para fines de representación en Netdot, estas secciones de cable se deberán repre- sentar como cables dorsales separados

- Los cables dorsales pueden interconectar closets dentro del mismo edificio.

Pueden crearse nuevos cables dorsales yendo a Cable Plant -> Backbone Cables -> [new]. Se le pedirá que provea un closet de origen y uno de destino, el tipo de cable (cobre, fibra, etc.) y un identificador único (ID). Netdot puede sugerir un ID, el cual estará compuesto de los IDs de los sitios donde están ubicados los closets, seguido de un número de secuencia, por ejemplo: "123/456-1".

El campo de número de filamento (Number of Strands), indicará a Netdot que deberá crear tal número de filamentos asociados a este cable.

4.7.4 Filamentos de cable (Cable Strands)

Estos tienen varios atributos, incluyendo:

- Número de secuencia
- Estado - No terminado, disponible, dañado o en uso
- Tipo de Fibra - Multi-modo o mono-modo
- Circuito - Un circuito extremo a extremo compuesto de una secuencia de filamentos empalmados (spliced strands)

Puede hacer modificaciones de rangos de filamentos en grupo. Por ejemplo, si tuviese un nuevo cable de fibra híbrido de 24 fibras, de las cuales 12 son mono-modo y 12 son multi-modo, en la página del cable dorsal, al final de la lista de filamentos, escriba "1-12", y luego seleccione el tipo "Single Mode", y el estado "Not Terminated". Y luego haga algo similar con el rango "13-24".

Los filamentos de distintos cables dorsales pueden empalmarse unos con otros para formar una secuencia. Para empalmar un rango de filamentos, vaya al final de la página de Backbone Cable, en la sección "Manually Splice Strand Range", escriba el rango de filamentos que están empalmados con otro dorsal, por ejemplo, "1-12", y los filamentos correspondientes del otro dorsal, por ejemplo "1-12" o "13-24", y entonces seleccione el otro dorsal, y haga click on "Go". Ahora debería ver los filamentos contiguos en la columna "Spliced With", y la secuencia completa en la sección "Part of Sequence".

4.7.5 Circuitos

Luego de haber creado secuencias de filamentos desde un origen A hasta un destino B, puede crear un circuito para agrupar esos filamentos y asignarlos a un par de interfaces de dispositivos.

Para crear un circuito, vaya a Cable Plant -> Circuits -> [new]. Será necesario proporcionar un identificador único, y luego un proveedor. En este caso, el

proveedor podría ser su propia organización. También puede utilizar los circuitos en Netdot para documentar enlaces provistos por otros proveedores. En tales casos, el circuito probablemente no estará asociado a filamentos de cable de su propiedad.

Los circuitos tiene las siguientes propiedades, entre otras:

- Site Link: Registra la asociación entre dos Sites que están conectados por este circuito. El enlace entre dos Sites puede estar conformado por más de un circuito.
- Status: Activo, Inabilitado, Desconectado, Pendiente
- Type: DS3, Ethernet, Frame Relay, etc.
- Loss: Los últimos valores de pérdida medidos en el circuito

Una vez creado un circuito, tendrá la opción de asociarlo a una lista de secuencias de filamentos. Simplemente seleccione los sitios de origen y destino, y luego seleccione un par de secuencias de filamentos que compondrán este circuito (asumiendo que es un circuito de fibra).

También encontrará la opción de asociar un par de interfaces de dispositivos a este circuito.

4.7.6 Cables Horizontales

Un cable horizontal representa cableado que comienza en un closet y termina en una toma de red en alguna oficina o habitación, generalmente cable de par de cobre categoría 5 o similar. Describiremos algunos de sus atributos:

- Jack ID: Un identificador único de la toma en toda la organización. Por ejemplo, una toma ubicada en el sitio #123, terminada en el closet "A", y cuyo número de secuencia es "456" podría identificarse de manera única con algo similar a "123-A-456".
- Faceplate ID: Identificador de placa. Generalmente varias tomas de red se agrupan en una placa única que se encaja en la pared. Este campo aloja la identificación única de la placa, no de la toma de red.
- Type: Cat5, Cat6, etc.
- Closet: El armario o closet the comunicaciones donde se inicia el cable
- Room: La oficina o habitación donde termina el cable.

Una vez creado, puede asignar este cable a una interfaz de dispositivo yendo a la página de dispositivos, seleccionando la pestaña "Interfaces" y luego [edit]. Debería ver una lista de los cables existentes en la columna "Jack(cable)". Note que también existen los campos de texto sin formato opcionales "Room" y "Jack". Estos están disponibles por si usted no tuviera necesidad de documentar los cables horizontales, pero sí las asignaciones de puerto a tomas de red.

4.8 Operaciones avanzadas de BD

La sección *Advanced* del menu principal muestra la operaciones básicas Examinar/Browse, Buscar/Search y Adicionar/Add para las tablas que componen la base de datos. Este tipo de operaciones implica un conocimiento preciso de la estructura de la base de datos.

En este sección se puede realizar consultas personalizadas escritas en SQL, que pueden ser guardadas para uso futuro. El resultado de una consulta SQL query output puede guardarse en el formato de fichero con valores separado por comas (CSV, comma-separated).

4.9 Reportes

La sección *Reportes* ofrece un conjunto de reportes muy útiles.

4.9.1 Reportes de dispositivos

Por Tipo/Modelo Muestra los dispositivos agrupados por tipo (switches, routers, servers, etc) y luego cada uno agrupados por modelo, con los totales por tipo y modelo.

Por Modelo/OS Muestra los dispositivos por fabricante, luego por modelo, mostrando la versión de OS (sistema operativo) recomendada para cada modelo (este atributo debe ser definido anteriormente) y todas las versiones de ese OS que se encuentran en la red, con los totales correspondientes.

Dispositivos con tiempo de inactividad programado Netdot exporta configuraciones para herramientas de monitoreo de redes como Nagios. Algunos dispositivos puede que tengan un tiempo de inactividad planificado, lo cual los excluye del procesion de monitoreo durante el tiempo establecido. Este reporte muestra los dispositivos que tengan un tiempo de inactividad (Downtime) establecido.

Conexiones duplex discordantes (Duplex Mismatches) Este reporte muestra una lista de interfaces adyacentes que tienen configuraciones dúplex de Ethernet incongruentes.

Versiones de sistemas operativos discordantes (OS Mismatches) Este reporte muestra una lista de dispositivos que tienen una versión de sistema operativo que difiere de la recomendada. La lista está agrupada por fabricante, modelo, tipo de dispositivos y version actual del SO.

4.9.2 Reportes de activos (Assets)

Los reportes de assets son principalmente útiles para la identificación de hardware, ya sea instalado o sin instalar.

Por tipo/modelo (Type/Model) Muestra un resumen del hardware por tipo y modelo, y muestra las cantidades de cada uno.

Detallado (Detailed) Muestra una lista de activos incluyendo su tipo, modelo, número de serie, número de inventario, si está instalado o no, comentarios, etc.

4.9.3 Reportes de IP (IP Reports)

Subredes no utilizadas/Unused Subnets Se muestra una lista de subredes que no tienen direcciones IP de nodos asignadas. Sólo se pueden seleccionar subredes IPv4 o IPv6.

Subredes congestionadas/Maxed out Subnets Se muestra una lista de subredes que están ocupadas por encima de un umbral de direcciones definidos. Este umbral se define en la opción `SUBNET_USAGE_MINPERCENT` en el fichero `etc/Site.conf`.

Direcciones estáticas en desuso/Unused Static Addresses Este reporte muestra las direcciones estáticas que no han sido detectadas en la red, por un período de tiempo determinado. Esto permite realizar operaciones de limpiezas del espacio de direcciones de forma más fácil.

4.9.4 Direcciones MAC/MAC Addresses

Este reporte muestra una lista de prefijos de direcciones MAC (OUI), organizadas por número de direcciones. El usuario tiene la opción de incluir todas las direcciones, sólo las direcciones correspondientes a equipos de infraestructura de red, o únicamente direcciones detectadas en tablas de reenvío o de ARP.

5 Exportar configuraciones para programas externos

Se puede utilizar la herramienta de exportación para generar los ficheros texto que serán utilizados por las aplicaciones externas.

La herramienta de exportacion está disponible en la interfaz web, en la opción Export . Se selecciona el programa hacia el cual se desea exportar la configuracion y se hace click en el botón [submit]. Netdot mostrará algunos mensajes de la herramienta de exportación y las rutas donde están los ficheros que fueron creados.

Además, la herramienta de exportación puede ser ejecutada desde la línea de comandos. Por ejemplo, paa generar la configuración de Nagios:

```
~# bin/exporter.pl -t Nagios
```

Para exportar varias configuraciones en una sola ejecución:

```
~# bin/exporter.pl -t Nagios,Sysmon,Rancid,BIND,DHCPD
```

Existen varios parámetros para cada configuración que se pueden definir en el fichero `Site.conf`.

5.1 Integración con herramienta Cacti

La integración de Cacti se hace de manera diferente (es más bien una "importación" que una "exportación"). Existe un script llamado 'netdot_to_cacti.php' dentro del directorio export/cacti del paquete Netdot. Este script debe colocarse, junto con su fichero de configuración, en el directorio "cli" de su instalación Cacti (no es necesario que sea en el mismo servidor que aloja a Netdot, pero sí debe asegurarse de que el script pueda conectarse a la base de datos de Netdot). Deberá ejecutar este script periódicamente, por ejemplo, una vez al día.

6 Autorización

A partir de la version 0.9, netdot soporta autorización basada en roles.

Existen tres tipos de usuarios que definen los niveles de acceso en Netdot:

- Admin: Acceso completo a la interfaz web, operaciones y objetos.
- Operator: Acceso completo a la interfaz web y sólo lectura de los objetos.
- User: Acceso limitado a la interfaz web, con opciones de mostrar, editar y eliminar para objetos específicos.

6.1 Asignar permisos a los usuarios

Los permisos pueden ser asignados a usuarios o grupos. Los usuarios son agrupados en listas de contacto/Contact Lists. Si un usuario es miembro de una lista de contacto, hereda los permisos de esa lista. Sin embargo, el usuario puede tener permisos más específicos (o ninguno) si fuera necesario.

Existe un limitado número de objetos a los cuales pueden acceder usuarios restringidos:

- Registros DNS: Los usuarios pueden crear, modificar y borrar registros de cierta zona. Los permisos puden definirse para la zona completa o partes de ella, basándose en bloques IP. Por ejemplo, si un usuario tiene permisos para ver, editar y borrar registros de mizona.com, entonces puede ver, editar y borrar cualquier registro de esa zona. Por otro lado, si la zona contiene registros de la supered 10.0.0.0/16 y el usuario sólo tiene control sobre registros de una subred específica 10.0.0.0/24, entonces no se asignan permisos de acceso a la zona mizona.com, sino a la subred específicamente.
- Los usuarios con permiso para editar una subred no tienen la opción de asignar direcciones IP específicas. Esto ayuda a mantener las direcciones en rangos contiguos de modo que sea más fácil cambiar el tamaño de las subredes si esto fuera necesario. Si el administrador de Netdot desea otorgar tal permiso a un usuario o grupo, puede utilizar el permiso "Choose IP" para tal motivo.
- Interfaces de dispositivos: Los usuarios pueden ver detalles de los puertos como: número, nombre, VLAN, habitación, toma de red, descripción y dispositivo adyacente. El usuario sólo puede editar los atributos: habitación, toma de red y descripción. Para asignar permisos a varios dispositivos seleccione el tipo de dispositivo y luego aquellos que serán accesibles por el usuario.

- Listas de Contacto: Un usuario puede adicionar, modificar y borrar contactos de una lista de contacto.

Para asignar permisos para usuarios específicos, se realiza lo siguiente:

- Asegurarse de que existe un objeto Person para el usuario. Esto se comprueba realizando una búsqueda en `Contacts -> People` a partir del nombre de la persona. Si el objeto no existe, se puede crear uno nuevo haciendo click en el botón [new] en la esquina superior derecha de la página.
- Asegúrese que la persona tiene los atributos Username y User Type definidos. Si se ha configurado Netdot para utilizar autenticación con RADIUS o LDAP es necesario que el Usuario/Username coincida con el que se ha definido en esos sistema de autenticación. Si está utilizando autenticación local, es necesario que se defina una contraseña local en el atributo Password.
- En la página de Usuario/Person, se pueden adicionar permisos haciendo click en el botón [access_rights]. Se monstrarán los permisos actuales y la posibilidad de adicionar nuevos con el botón [add] a la derecha.
- En la ventana de Permisos/UserRight, seleccione la clase de objeto/Object Class, los objetos específicos y los permisos (ver, editar, borrar). Sólo seleccione el permiso 'none' para revocar todos los permisos heredados de un grupo. Finalmente realice click en 'Insert'.

6.2 Registros de Auditoría

Una vez usted asigne permisos a los usuarios para modificar la base de datos de Netdot, querrá poder saber "quién hizo qué y cuándo". Existe una tabla en la base de datos llamada "audit", la cual registra cada operación de la base de datos hecha por una persona (es decir, que las operaciones automáticas no se registran). Cada registro de auditoría contiene la siguiente información: sello de tiempo, nombre de usuario, tipo de operación (inserción, actualización, borrado), tabla afectada, ID del récord, descripción del récord, campos y valores cambiados.

Podrá acceder a estos registros yendo a "Advanced" -> "Browse" -> "audit", o, si quiere buscar algo en particular, elija "Search" -> "Audit".

Esta tabla puede reciclarse periódicamente por medio del programa bin/prune_db.pl.

7 Interfaz REST

La interfaz REST permite acceso remoto a Netdot mediante el protocolo HTTP/HTTPS. Actualmente, los objectos se formatean en código XML us-

ando el módulo Perl XML::Simple. En el futuro, Netdot podría soportar otros formatos como YAML.

7.1 Recursos tipo REST Genéricos

- La interfaz REST está disponible a través del siguiente URL (o similar, dependiendo de su configuración de Apache):

```
https://myserver.mydomain.com/netdot/rest/
```

Esto debe cargar la clase Netdot::REST y mostrar algo como lo siguiente en su navegador:

```
Netdot/1.0 REST OK.
```

- Los recursos REST a procesar representan objetos Netdot y son parte del URI de la petición HTTP. Por ejemplo, en este URI:

```
http://myserver.mydomain.com/netdot/rest/device/1
```

el recurso es "device/1", el cual, en una petición tipo "GET", retornará el contenido del objeto Device con ID "1".

- Usando el siguiente URI en la petición tipo "GET":

```
http://myserver.mydomain.com/netdot/rest/device
```

esta interfaz devolverá los contenidos de todos los objetos tipo "Device" existentes.

- Es posible especificar ciertos filtros para limitar el alcance de los resultados:

```
http://myserver.mydomain.com/netdot/rest/device?sysname=host1
```

Esto realizará una búsqueda de todos los "devices" cuyo campo "sysname" tenga el valor "host1".

- La palabra clave "meta_data", en lugar de un ID de objeto, proveerá información acerca de la clase de objeto:

```
http://myserver.mydomain.com/netdot/rest/device/meta_data
```

- Un recurso existente podrá actualizarse utilizando el método “POST” con parámetros relevantes. Por ejemplo, una petición tipo “POST” con el siguiente URI:

```
http://netdot.localdomain/rest/device/1?sysname=newhostname
```

actualizará el campo ‘sysname’ del objeto “Device” con ID “1” y le asignará el valor “newhostname”. De manera similar, puede crearse un nuevo objeto con una petición tipo “POST”. Sin embargo, en este caso el ID del objeto no debe incluirse:

```
http://netdot.localdomain/rest/person/?firstname=John&lastname=Doe
```

- Finalmente, un objeto en específico se puede eliminar utilizando el método “DELETE” de HTTP.

7.2 Recursos tipo REST de propósito específico

7.2.1 /rest/host

El recurso especial ‘/rest/host’ provee una interfaz simplificada para manipular los récords DNS y DHCP. Vamos a ilustrar su uso con los siguientes ejemplos:

Obtener datos de hosts (HTTP GET)

- Obtener todos los objetos RR (DNS)

```
http://netdot.localdomain/netdot/rest/host
```

- Obtener todos los objetos DNS de una zona

```
http://netdot.localdomain/netdot/rest/host?zone=localdomain
```

- Recuperar el RR con nombre ‘foo’

```
http://netdot.localdomain/netdot/rest/host?name=foo
```

- Recuperar el RR con id 1

```
http://netdot.localdomain/netdot/rest/host?rrid=1
```

- Obtener todos los objetos IP de una subred

```
http://netdot.localdomain/netdot/rest/host?subnet=192.168.1.0/24
```

Crear nuevos records (HTTP POST).

- Crear un récord tipo A llamado 'host1' y asignar la primera dirección IP disponible (Ojo: No especificar el Id):

```
URL:  http://netdot.localdomain/netdot/rest/host?name=host1
POST: {subnet=>'192.168.1.0/24'}
```

Actualizar récords existentes (HTTP POST).

- Cambiar el nombre al host con RR Id 2. Requiere rrid o ipid:

```
URL:  http://netdot.localdomain/netdot/rest/host?rrid=2
POST: {name=>'nombre-nuevo'}
```

- Actualizar la dirección MAC del host DHCP con Ipblock Id 3

```
URL:  http://netdot.localdomain/netdot/rest/host?ipid=2
POST: {ethernet=>'DEADDEADBEEF'}
```

Borrar records (HTTP DELETE)

- Borrar el nombre de host con RR Id 3 (también libera la IP)

```
http://netdot.localdomain/netdot/rest/host?rrid=3
```

7.3 Autorización en la interfaz REST

Todos los tipos de usuario pueden interactuar con la interfaz REST siempre que se le hayan asignado permisos. Sin embargo, sólo los usuarios tipo Admin pueden editar o borrar objetos utilizando los recursos genéricos REST. Los usuarios tipo 'Operator' y tipo 'User' pueden 'ver' los recursos genéricos pero sólo pueden editar o borrar algunas cosas utilizando los recursos de propósito específico como 'rest/host'.

7.4 Módulo Perl para programas cliente en CPAN

Se provee un módulo conveniente a través de CPAN para ser utilizado en programas que necesiten acceso a la interfaz REST de Netdot. El nombre del módulo es "Netdot::Client::REST". Puede instalarse con algo similar a:

Si está en un sistema basado en Debian (ej. Ubuntu):

```
~# sudo apt-get install libnetdot-client-rest-perl
```

o sino:

```
~# cpan
>install Netdot::Client::REST
```

8 Mantenimiento de la base de datos

La base de datos de Netdot crecerá con el tiempo, por lo que será necesario borrar información caducada. Encontará una utilidad de línea de comandos llamada "prune_db.pl" en el directorio bin/ de la distribución. La sintaxis de dicho comando es como sigue:

```
usage: bin/prune_db.pl
-H, --history | -F, --fwt | -A, --arp |
-M, --macs | -I, --ips | -R, --rr | -a, --audit | -t, --hostaudit
[ -d, --num_days <number> ] [ -n, --num_history <number> ] [ -r, --rotate ]
[ -g, --debug ] [-h, --help]

   -H, --history      Tablas con historia
   -F, --fwt          Tablas de reenvío
   -A, --arp          Cachés de ARP
   -M, --macs         Direcciones MAC
   -I, --ips          Direcciones IP
   -R, --rr           Récords DNS
   -a, --audit        Récords de auditoría
   -t, --hostaudit    Récords de auditoría de DNS y DHCP
   -d, --num_days     Mantener récords por número de días (default: 365);
   -n, --num_history  Número de récords históricos a mantener por cada record
   -r, --rotate       Rotar (en lugar de borrar) las tablas de reenvío y ARP
   -p, --pretend      Mostrar actividad sin realmente borrar nada
   -g, --debug        Información de depuración (mucha)
   -h, --help         Mostrar ayuda
```

El fichero de muestra "netdot.cron" incluído con el paquete muestra ejemplos de uso recomendado de este programa.

> **Nota**: Sea especialmente cuidadoso al utilizar las opciones -I y -M para borrar direcciones IP y MAC. El criterio para su eliminación depende del sello de tiempo "last seen" (visto por última vez) incluído en estos récords. Esto implica que si Netdot no está recopilando las tablas de ARP y de reenvío de los enrutadores, cortafuegos y

switches donde se encontrarían estas direcciones, Netdot asumirá que no están activas, y por tanto las incluirá en la lista de eliminación.