

Entorno de gestión de políticas basado en un directorio LDAP

David Morón Ruano, Antoni Barba Martí
Departamento de Ingeniería Telemática. Universidad Politécnica de Cataluña.
{dmoron, telabm}@mat.upc.es

Abstract. La gestión de red basada en políticas resuelve muchos de los problemas de los sistemas gestión de red actuales como SNMP. Estos sistemas son complejos en cuanto a la utilización y a la gestión. La gestión de red basada en políticas (PBNM) ofrece una solución a este problema. En este artículo se presenta el desarrollo de un entorno de gestión de políticas que utiliza como repositorio una implementación Open Source del protocolo LDAP para acceso a directorios. La herramienta openLDAP[1] junto con el motor también Open Source BerkeleyDB[2] nos ofrece un repositorio estable y con pocos requerimientos de memoria y procesador.

1. Gestión de red basada en políticas.

Los proveedores de servicios de Internet (ISP) y las empresas cada vez gestión más tráfico y cada vez con más demanda de calidad para esos servicios. Actualmente, estos ISP necesitan ofrecer más servicios a sus clientes. Esto incluye la capacidad de control de sus infraestructuras, garantizar el acuerdo de nivel de servicio (SLA) contratado por el usuario, etc.

En las redes tradicionales, los nuevos servicios se añaden de manera lenta, añadiendo nuevo hardware, y reconfigurando la red de manera manual. Los administradores de red han de reconfigurar los elementos e la red de uno en uno. Esto implica que los sistemas actuales sean muy poco flexibles, y no permiten la gestión dinámica de los recursos de los que dispone. Esto es un problema cuando hablamos de redes que han de ofrecer una cierta calidad de servicio ya que se ha de garantizar que se cumple el contrato adquirido con el cliente. Cuando el numero de clientes y de servicios en el sistema es grande es imposible reconfigurar los elementos de red de manera manual para asegurar que en cada instante la red cumple el SLA.

Con la gestión de red basada en políticas (PBNM) es una posible solución a este problema. Ofrece un control dinámico y coordinado de los elementos de la red ya que las decisiones se toman de manera automática basándose en reglas, peticiones de usuarios o de servicios. Esta gestión dinámica de los elementos de la red representa un cambio cualitativo, desde el punto de vista empresarial, ya que permite la gestión de los recursos de la red y de los servicios de manera más eficiente.

2. Vista general del sistema.

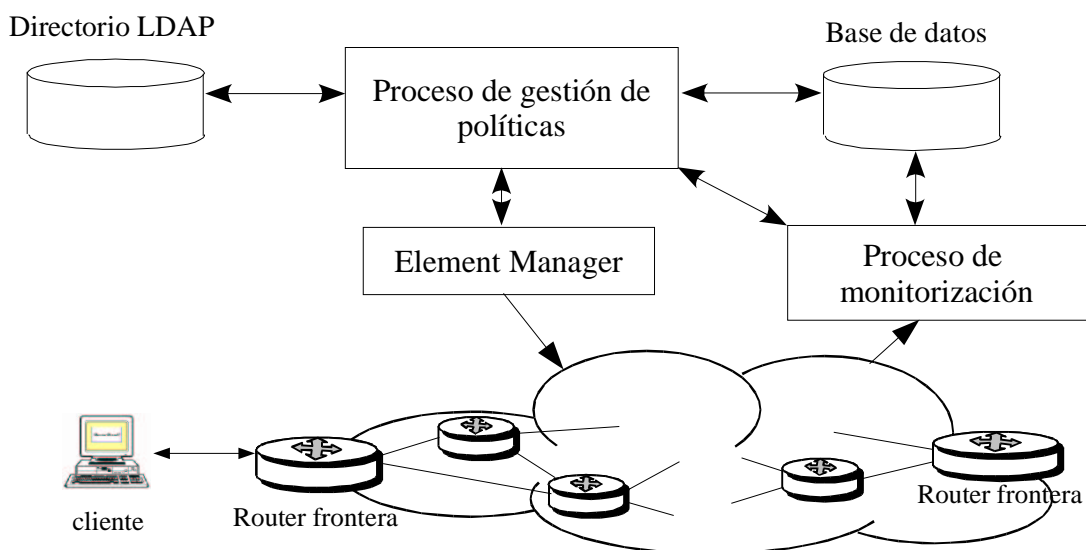


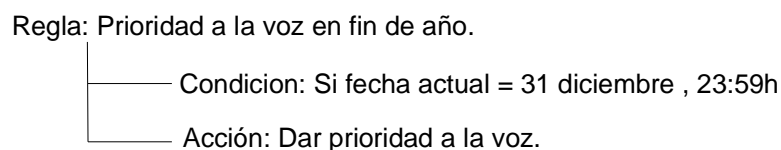
Figura 1. Esquema del sistema.

Se dispone de una red formada por máquinas Linux y Unix que ofrecen calidad de servicio mediante

servicios diferenciados. Dos de estas máquinas hacen la función de routers frontera que son los puntos de ingreso y de egreso de la red. Cada uno de los nodos de la red (core routers) dispone de varios enlaces de salida y es capaz de ofrecer en cada uno de ellos cuatro niveles de calidad de servicio. Tanto los core routers como los edge routers (routers frontera) dispone de un proceso de monitorización que testea el ancho de banda utilizado, el retardo, jitter y pérdidas para cada uno de los servicios. Esta información de monitorización se almacena en una base de datos para que sea accesible para el gestor de políticas.

El objetivo es el de gestionar la red que ofrece servicios diferenciados mediante políticas de manera automática. Para esto es necesario almacenar las políticas adecuadas en el directorio LDAP para que el gestor de políticas, mediante la información de monitorización de la base de datos, la información de usuario y de SLS almacenada en el directorio y la información de las alarmas del sistema sea capaz de tomar decisiones correctas en tiempo de ejecución.

Una política no es más que una regla que sigue la sintaxis *si-entonces*. a modo de ejemplo se muestra una posible política que daría prioridad a la voz el 31 de diciembre a las 23:59 de la noche (su función es la de reasignar recursos para que la gente pueda felicitar el año nuevo por teléfono).



El sistema de gestión de políticas es una aplicación que, basándose en el modelo de políticas del IETF (PCIM)[3] y sus extensiones (PCIM Extensions) [4] lee las políticas que sea oportunas del directorio, evalúa sus condiciones, y si se cumplen, entonces envía las acciones al Element Manager para que sean ejecutadas.

3. Directorio openLDAP.

Un directorio LDAP es una base de datos optimizada para la lectura y búsqueda de información que almacena la información de manera jerárquica. Los directorios soportan opciones avanzadas de filtrado. Generalmente no soportan transacciones complejas que si ofrecen los sistemas de gestión de bases de datos diseñadas para procesar un gran volumen de actualizaciones. Los cambios en la información almacenada en un directorio suelen ser del tipo "o todo o nada", es decir, cambios de las ramas del árbol (DIT - Directory Information Tree) completamente, pero, aunque no estén optimizados para ello, los directorios pueden permitir cambios muy específicos. Los directorios están preparados para dar una respuesta rápida a un gran volumen de búsquedas. Disponen de mecanismos de replicación de la información en varios servidores para de incrementar la disponibilidad y fiabilidad del servicio mientras se reduce el tiempo de respuesta.

LDAP significa Lightweight Directory Access Protocol (Protocolo ligero de acceso a directorios). Como el nombre sugiere, es un protocolo de acceso a servicios de directorio basados en X.500. LDAP funciona sobre TCP/IP u otros servicios de transferencia orientados a conexión. Los detalles del protocolo están definidos en [5] RFC2251 "The Lightweight Directory Access Protocol (v3)".

3.1 Posibilidades que ofrece.

El servidor openLDAP ofrece una serie de posibilidades que han sido explotadas en este proyecto:

- Implementación del protocolo LDAPv3: Este protocolo está definido en [6] y permite el uso de IPv4 e Ipv6.
- Autenticación y nivel de seguridad: Permite servicios de autenticación mediante SASL. El acceso al directorio ha de ser restringido ya que contiene información de usuarios (nombres de usuarios y contraseñas), información de las políticas y parámetros de los SLS. Por esta razón sólo el administrador del directorio tiene acceso a la información.
- Control de acceso: openLDAP permite definir una serie de filtros para el control de acceso a diferentes DITs, entradas, o atributos de estas entradas.
- Distribución de información en varios servidores: openLDAP implementa el método de *referrals* para la distribución de los DITs en diferente servidores.
- Es totalmente gratuito bajo licencia Open Source y está disponible para sistemas operativos Linux y

Unix.

El servidor openLDAP hace una implementación Open Source del protocolo LDAP y requiere un *backend* o motor para almacenar y hacer búsquedas de la información. En el sistema se ha instalado Berkeley DB que es un gestor de bases de datos disponible de forma gratuita y bajo licencia también Open Source en www.sleepycat.com.

3.2 Almacenamiento de información en el directorio LDAP.

El directorio dispone de tres *backends* independientes para almacenar información de los usuarios de la red, los parámetros de calidad para cada una de las clases de servicio y las políticas respectivamente.

1. Información de usuarios: Se almacenan los nombres de usuario, contraseñas, grupo al que pertenecen y que SLS tienen asignado.
2. Información de los SLS: Contiene los parámetros de rendimiento de tráfico y de función de policía para cada una de las clases de servicio.
3. Políticas: Los documentos PCLS [6] y PCELS [7] (en el que estamos contribuyendo en su desarrollo) definen el modo de almacenar estas políticas en el directorio. Actualmente hay almacenadas políticas de control de admisión y políticas de gestión.

4. Gestor de políticas.

4.1 Descripción.

El gestor de políticas es el proceso encargado de tomar las decisiones a tomar sobre la red. Utilizando la terminología de la gestión basada en políticas se denominaría un PDP (Policy Decision Point). Esta aplicación ha sido programada en Java y su esquema funcional es el siguiente:

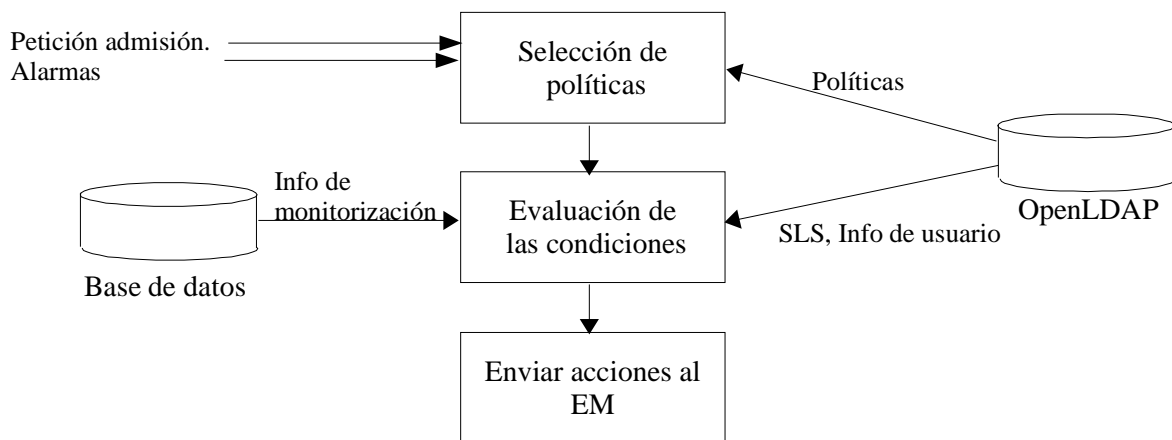


Figura 2. Esquema funcional del gestor de políticas.

4.2 Funcionamiento.

El gestor de políticas espera las llegadas de peticiones de admisión de nuevos usuarios y de alarmas de los diferentes nodos de la red. Cuando se produce uno de estos dos eventos el gestor de políticas decide que políticas se han de aplicar y a continuación accede al directorio LDAP donde están almacenadas. Para cada una de las políticas cargadas del directorio evalúa sus condiciones. Para ello accede a las fuentes de información convenientes para cada caso: la información del contexto en el que se produce el evento a través de las alarmas y de las peticiones, la base de datos para condiciones donde intervengan valores de monitorización de la red y los SLS e información de usuario para políticas de control de admisión.

Para el caso de las condiciones de la políticas sea ciertas, entonces envía las acciones al Element Manager, este traduce la acción en alto nivel a acciones concretas para cada nodo de la red (PEP - Policy Execution Point). Una vez los PEPs han realizado las acciones el nuevo estado de la red se ve reflejado en la base de datos.

5. Capacidad actual del sistema.

El sistema dispone actualmente de una políticas básicas que se pueden dividir en dos grupos:

- Políticas de admisión: Estas políticas hacen un chequeo de los parámetros de las peticiones de admisión de nuevos usuarios, tanto de parámetros de identificación de usuario (nombre de usuario, contraseña, ...) como de los parámetros de rendimiento solicitados (ancho de banda, retardo, jitter, pérdidas).
- Políticas de función de policía: Hacen un reajuste del ancho de banda asignado a cada clase de servicio en el caso de que no se está cumpliendo el SLA de algún usuario.

Actualmente se están haciendo medidas de tiempos de respuesta de los directorios utilizando políticas no-distribuidas. Podemos adelantar que el tiempo de respuesta para la lectura de una política simple que sólo contenga una condición y dos acciones está por debajo de los 50 ms (PentiumII 400MHz , 128MB RAM, Linux RedHat 7.2).

También se están haciendo medidas de los tiempos de toma de decisiones para el gestor de políticas ya que, para los sistemas de gestión de red, este retardo es el parámetro más crítico.

6. Agradecimientos.

Desearíamos mostrar nuestro agradecimiento a Angélica Reyes por toda la ayuda ofrecida durante la realización de este proyecto. También desearíamos agradecer a Carles Bonfill el desarrollo de toda la red y la base de datos en los que se apoya este proyecto. El trabajo de Carles Bonfill está publicado como proyecto final de carrera [8].

7. Conclusiones.

Utilizando herramientas Open Source hemos logrado crear un entorno de pruebas para la gestión basada en políticas. Aunque openLDAP no implementa actualmente algunas extensiones del protocolo LDAPv3, su estado de desarrollo permite implementar el repositorio de políticas definido en [6] y [7].

La utilización de un directorio LDAP en lugar de una base de datos relacional nos permite hacer un preselección de las políticas mediante la selección de las ramas en función de la información de la red antes de hacer una búsqueda (algunas bases de datos permiten hacer algo similar mediante la utilización de índices). Es preciso señalar que actualmente sólo existe un estándar para el almacenamiento de políticas y corresponde al almacenamiento en directorios [6] y [7], y que cualquier almacenamiento de políticas en un repositorio que no sea éste puede ser objetivo de futuros estudios.

8. Referencias.

- [1] openLDAP (www.openldap.org).
- [2] BerkeleyDB (www.sleepycat.com).
- [3] B. Moore, et al. "Policy Core Information Model." RFC 3060. Febrero 2001.
- [4] B. Moore, et al. "Policy Core Information Model (PCIM) Extensions." RFC 3460. Enero 2003.
- [5] M. Wahl, T. Howes, S. "Lightweight Directory Access Protocol (v3)." RFC 2251. Diciembre 1997.
- [6] J. Strassner, et al. "Policy Core LDAP Schema." draft-ietf-policy-core-schema-16.txt.
- [7] A. Reyes, et al. "Policy Core Extensions LDAP Schema." draft-reyes-policy-core-ext-schema-01.txt.
- [8] C. Bonfill, A. Barba. Proyecto de final de carrera: "Implementación de un sistema de gestión basado en políticas: Configuración de red, monitorización y control JDMK." Mayo 2003.