Administración de Redes Basadas en Políticas

Mario Leandro Bertogna, Rodolfo Del Castillo
Departamento de Informática y Estadística, Universidad Nacional del Comahue,
Buenos Aires 1400, Neuquén, Argentina
Email: mlbertog, rolo@uncoma.edu.ar

Resumen En nuestros días la complejidad y el dinamismo de las redes informáticas han vuelto su control y mantenimiento un verdadero dolor de cabeza para los administradores. Nuestro objetivo es simplificar estas labores a través de la implementación y extención de un esquema para administración, basado en políticas, donde de la definición de las políticas con un nivel alto de abstracción se ira transformado de reglas de negocio a reglas de configuración aplicables a los distintos tipos de dispositivos en forma automática. A partir de esto, se define el marco de trabajo del proyecto y se enuncian los distintos aspectos de diseño y dificultades a nivel de implementación que se encuentran al momento de desrrollar una solución de estas caracteristicas.

1. Introducción

En la mayoría de las organizaciones, la red de computadoras, es uno de los puntos críticos para poder ejercer una óptima administración y uso de los recursos de la empresa, pero este medio ha evolucionado y a su vez se ha transformado también en un recurso escaso y complejo. Distintos niveles de usuario, distintos tipos de servicio, control de acceso, heterogeneidad de soluciones a nivel de hardware y software, requieren inversión, personal con distintos perfiles y capacitado en forma permanente para poder satisfacer los requerimientos actuales.

El objetivo es poder fusionar en un solo esquema de administración simple y centralizado, parámetros de calidad de servicio (QOS) como control de admisión, administración de las congestiones, evitación de las congestiones, etc., a través de políticas de alto nivel o reglas de negocios, un ejemplo de estas políticas podría ser implementar una política de trafico de VoIP, este debe tener un comportamiento similar al tráfico sobre las redes de telefonía y a este servicio podrían tener acceso los niveles gerenciales y solo en horario de trabajo.

Esta política, involucra clasificación de usuarios mediante roles, clasificación de servicios y discriminación del servicio en el tiempo, además que indirectamente el comportamiento de VoIP involucra configuraciones de demora mínima, jitter, perdida de paquetes y ancho de banda. Estas políticas deberán ser interpretadas, almacenadas y aplicadas en el punto correcto de la red forma automática, y deberán ser lo suficientemente amplias como para poder abarcar requerimientos y dispositivos futuros.

En este trabajo se expone una arquitectura para poder lograr el esquema de la aplicación y se mencionarán implementaciones para cada punto propuesto. En la primer sección se analizará en detalle el framework de administración basada en políticas definido por la IETF[1] que describe una estructura de control, la segunda sección presentará los puntos a tener en cuenta sobre la definición de políticas de negocio, y en la última sección, se enunciarán los protocolos de comunicación y plantearemos un esquema para lograr una abstracción efectiva en los puntos de aplicación.

2. Modelo de Administración

Como se mencionó anteriormente, la definición de las políticas poseen un alto nivel de abstracción, para que los dispositivos de hardware puedan interpretar y aplicar los requerimientos, las políticas deben ser procesadas y traducidas a reglas de configuración.

Si se toma la definición anterior como en [2] se podría tener tres etapas, la de instanciación que debe conocer la información del entorno, como diagramas de tiempo y usuarios, comprender los eventos recibidos y su impacto en las políticas y la información propia del modelo. La etapa localización que deberá tener conocimiento del alcance de las acciones para cada dispositivo presente en la red, las relaciones del modelo de información o entre sus dispositivos, la topología o flujos de información y la capacidad de transferir el subconjunto de políticas resultantes a las

entidades correctas, y por último la de traducción que deberá poder interpretar las reglas generales en acciones de configuración.
Estas tres etapas de transformación y aplicación se corresponden con dos elementos de la arquitectura propuesta por el IETF [1], un punto de decisión (PDP Policy Decision Point) y uno o varios puntos de aplicación (PEP Policy Enforcement Point).
El PEP es un elemento que se corresponde directamente con un nodo en la red y el PDP es una entidad que puede estar en un servidor de políticas y se vale de otras funcionalidades como por ejemplo autenticación, administración de cuentas, información del almacenamiento, etc.
La interacción entre ellos comienza en el PEP, este recibe notificaciones o formula requerimientos que requieren de decisión de políticas y se los envía al PDP, este retorna una respuesta basada en las políticas al PEP y este las aplica.
Todo este mecanismo debe ser administrado por un interfaz de usuario que permitirá el acceso centralizado, deberá proveer el ingreso sencillo de las políticas, la inserción de nuevos dispositivos y el monitoreo de la evolución de la aplicación de las políticas como lo planteado en vemos en algunas herramientas como el esquema de administración de SUN [3].
Todo esto confluye en un marco de trabajo con un flujo de control y en la definición de una herramienta de administración centralizada, con interfaces claramente definidas y que abstraiga de los parámetros específicos de las empresas que desarrollaron los dispositivos de la red, optimizando a un máximo las tareas de configuración y administración del equipamiento.

3. Politicas

A través de los distintos trabajos existen una gran cantidad de conceptos similares bajo el termino de política, para continuar la presentación es necesario tener una definición más objetiva de los elementos del dominio en el que se trabaja y poder analizar desde allí las diferentes soluciones. Una amplia exposición sobre este tema se ha realizado en el IETF [4]. Este trabajo define que una política es *un objetivo claro o método de acción que guía y determina el presente y futuras decisiones,* y un detalle a tener en cuenta que se plantea muy claramente, es que debe ser implementada o ejecutada sin un contexto particular.
La relación de esta definición de políticas, la red y sus dispositivos surge de la especificación en [5] donde se propone que una forma de poder resolver esta relación es primero modelar a la red como una máquina de estados y luego usar las políticas para controlar en que estado debe estar, o se le permite estar, a un dispositivo controlado por la política en un determinado tiempo. Según este método la política se aplica usando un conjunto de reglas. Cada regla consiste de un conjunto de condiciones y acciones, y el conjunto de condiciones asociadas a una regla específica cuando una regla es aplicable.

3.1 Transformaciones

Si se analiza en detalle las definiciones anteriores, vemos que se esta descendiendo el nivel de abstracción, se paso de reglas de negocio a reglas de aplicación o configuración. En los trabajos del IETF [6][7] existe una propuesta de almacenamiento orientado a objetos y una propuesta de implementación con Lightweight Directory Access Protocol (LDAP) como su protocolo de acceso.
Pero antes de poder realizar la transformación deben realizarse chequeos y validaciones [8] para poder llegar a presentar formalmente las políticas a un nivel inferior, como por ejemplo, validar si los parámetros en la especificación de la política pueden ser aplicados por los dispositivos y la red, que dos políticas no tengan conflictos entre ellas, etc.
En algunas implementaciones ya existen trabajos realizados en este tema de algoritmos de validación y chequeo como en el lenguaje de políticas Ponder [9], que clasifica los tipos de conflictos que pueden ocurrir entre las políticas, menciona los tiempos de chequeo, que son similares a un leguaje de computación, tiempo de compilación y ejecución y propone soluciones

para el primer caso como podría ser prioridad a las políticas para lograr algún esquema de precedencia.

3.2 Presentación

Ya se ha planteado que las políticas deben definirse a un nivel alto deben traducirse y validarse, pero esto debe ser adaptado con la forma de definir la política en una aplicación real, como la que queremos lograr como conclusión del trabajo de investigación, desde el punto de vista del ser humano la opción ideal seria una aplicación con lenguaje natural, pero al estar estos trabajos todavía en etapas preliminares debemos tomar otras opciones y en este punto es donde surgen dos ramas alternativas.

Las ramas de especificación son el modelo procedural o el modelo declarativo, la primera especifica un lenguaje imperativo que explícitamente da la secuencias de pasos y el orden que deben seguir para producir el resultado, la segunda describe las relaciones entre las variables en términos de funciones y reglas de inferencia, que el interprete o el compilador pueden aplicar un algoritmo para producir un resultado y tenemos dos ejemplos de esto, el primero es LaSCO [10] que realiza una conversión al lenguaje JAVA y pueden ser ejecutadas y el segundo en el lenguaje Ponder [11].

5. Aplicación

Por último, se vera la capa de mas bajo nivel, la de aplicación, para lograr una comunicación con los distintos dispositivos generalmente se ha usado el protocolo SNMP o alguna de sus extensiones, pero se ha propuesto el uso del protocolo específico que soporta control de políticas sobre protocolos de QOS COPS (Common Open Policy Service) [12]. COPS se basa en los requerimientos y respuesta del PDP y PEP. Este protocolo fue diseñado para ser extensible, por lo que puede llegar a soportar otras clases de clientes basados en políticas en el futuro.

Existen varias propuestas para el PEP por ejemplo los trabajos [13,14] pero básicamente la mayoría son implementaciones similares en agregar una capa de transformación similar a una máquina virtual como la del lenguaje JAVA, que permite la ejecución de las aplicaciones sobre distintos tipos de sistemas operativos, en estos casos la llaman VCM (Virtual Configuration Manager) o PMA (Policy Management Agents) y estas aplican las configuraciones a los dispositivos usando COPS, SNMP o CLI.

6. Conclusiones y trabajo futuro

Se ha planteado en este trabajo los aspecto a tener en cuenta en el desarrollo de una herramienta de administración basada en políticas, como se ha podido observar, existen decisiones importantes tanto a nivel de diseño, como de implementación, en estos momentos se encuentran muchas RFCs Internet Drafs del IETF para tratar de estandarizar definiciones y conceptos para políticas o factores como modelos de transformación y almacenamiento de reglas. El desafío que nos hemos planteado luego de haber concluido con la definición del framework, que nos permite definir el flujo de control, es poder realizar una aplicación cumpliendo las propuestas del IETF, para poder, en primer termino disponer de una herramienta de dominio público compatible con las nuevas tecnologías y estándares, y en segundo termino, con la experiencia del desarrollo de una aplicación usarla como punto de partida para realizar pruebas concretas en entornos de producción, y así optimizar cada uno de los puntos involucrados.

Referencias

1. R. Yavatkar, D. Pendarakis, R. Guerin, “A Framework for Policy-based Admission Control”, RFC 2753, January 2000.

2. Jean-Christophe Martin," Policy-Based Networks", Sun BluePrints™ OnLine, October 1999.
3. D. Kakadia, "Enterprise QOS Policy Based Systems & Network Mangement", 2001.
4. Westerinen, et al.," Terminology for Policy-Based Management", IETF RFC 3198, November 2001.
5. B. Moore, E. Ellesson, J. Strassner, A. Westerinen., "Policy Core Information Model -- Version 1 Specification", IETF RFC 3060, February 2001.
6. Snir, Ramberg, Strassner, Cohen, Moore, "Policy QoS Information Model", IETF Internet Draft, November 2001.
7. B. Moore, E. Ellesson, J. Strassner , R. Motas, "Policy Core LDAP Schema", IETF Internet-draft, October 2002
8. Dinesh C. Verma,"Simplifying Network Administration using Policy based Management", 2001.
9. Lupu, E. & Sloman, M.,"Conflicts in Policy-Based Distributed Systems Management". IEEE Transactions on Software Engineering, Special Issue on Inconsistency Management, 25(6):852-869, Nov./Dec. 1999.
10. James Hoagland, "Specifying and Implementing Security Policies Using LaSCO, the Language for Security Constraints on Objects". Ph.D.Dissertation, University of California, Davis, March 2000.
11. N. Damianou, N. Dulay, E. Lupu, and M Sloman, "Ponder: A Language for Specifying Security and Management Policies for Distributed Systems", Imperial College, UK, Research Report DoC 2001, Jan. 2000.
12. J. Boyle, R. Cohen, D. Durham, S. Herzog, R. Rajan and A. Sastry, "The COPS(Common Open Policy Service) Protocol", RFC 2748 , January 2000.
13. J. Ogawa, Y. Nomura, "A Simple Resource Management Architecture for Differentiated Services", Inet. Japan, 2000.
14. Leonidas Lymberopoulos, Emil Lupu and Morris Sloman, "An Adaptive Policy Based Management Framework for Differentiated Services Networks", Proc. 3rd IEEE Workshop on Policies for Distributed Systems and Networks, June 2002.