

Unificación de Servicios de Red en Aulas Informáticas

Consolidation of Network Services in Computer Labs

Albert Teixidó (albert.teixido@uab.cat)

SIDLLP

Universitat Autònoma de Barcelona

Jordi Guijarro (jordi.guijarro@uab.cat)

SIDCB

Universitat Autònoma de Barcelona

José A. Lorenzo (joseantonio.lorenzo@uab.cat)

SIEE

Universitat Autònoma de Barcelona

Resumen

Se ha conseguido homogeneizar los servicios ofrecidos por las diferentes aulas de informática de la universidad mediante una plataforma desarrollada con software libre e integrada con la base de datos de usuarios corporativa. El servicio proporciona al personal docente y a los alumnos la posibilidad de acceder a cualquier equipo del campus y a sus recursos de red de manera fácil. Dada la diversidad de necesidades de los distintos centros se ha optado por un modelo de administración delegada.

Palabras clave: Movilidad, Servicio de Directorio, Servicio de Ficheros, Software Libre, Administración delegada

Summary

We have achieved the homogenization of the services offered by the different computer labs of the university building a custom platform developed with free software and integrated with the corporate users database. The platform provides to the teaching staff and the students the possibility of gaining access to any equipment of the campus and its resources in an easy way. Given the diversity of needs of the different centers we opted for a delegated administration model.

Keywords: Roaming, Directory Service, File Server, free software, delegated administration.

1. Introducción

La constante evolución de los sistemas de la información exige que las organizaciones replanteen sus modelos de funcionamiento para poder garantizar necesidades actuales y futuras. En nuestro entorno universitario se hace patente, además, que es necesario homogeneizar las diversas tecnologías usadas por las entidades que lo componen. Al plantearnos la unificación de servicios en el caso de las aulas de informática el carácter distribuido y la diversidad de necesidades docentes en cada facultad del campus nos condicionaron la configuración de la solución implementada.

En el caso de la Universitat Autònoma de Barcelona, y en el ámbito de la docencia, cada centro o facultad ofrecía sus recursos de red y servicio de directorio de forma independiente. Esta situación impedía compartir entre los centros los esfuerzos dedicados a la administración y el desarrollo de los sistemas.

Entre los objetivos principales se tuvo en cuenta, por un lado, facilitar la movilidad de los alumnos en el campus y el uso de un único usuario ligado al directorio corporativo, y, por otro lado, permitir el uso de la forma más distribuida posible y transparente para el usuario de los recursos de red y las aplicaciones.

Además, el entorno nos obliga a integrar sistemas y servicios dependientes de cada facultad, los cuales son administrados por equipos autónomos de técnicos distribuidos por el campus, con capacidades de actuación dentro de su ámbito.

2. Análisis de la viabilidad

Se evaluaron diferentes opciones y se optó por usar software libre. Se trata de un entorno abierto que nos permite la configuración adecuada para nuestras necesidades particulares. Hemos implementado una solución bien conocida y sobre la que ya existía documentación: Debian GNU/Linux[1], Samba[2] y OpenLDAP[3] a la que hemos añadido un conjunto de herramientas y la hemos adecuado a nuestro entorno.

En un inicio, y debido a la falta de casos en producción con soluciones corporativas similares a la planteada, se decidió realizar una prueba piloto. De esta forma, hemos asegurado la viabilidad del proyecto para el número de usuarios y máquinas cliente que está soportando actualmente el sistema. Por otro lado, la instalación del piloto también nos permitió comprobar el funcionamiento del diseño teórico y replantearlo tras varias pruebas de rendimiento.

3. Servicio de directorio

3.1. Conexión entre la base de datos corporativa y el directorio

Con el objetivo de minimizar la administración de usuarios se decidió integrar la base de datos corporativa, que funciona sobre INGRES, con el servicio de directorio. La información sobre usuarios se estructura en la base de datos en función de los colectivos a los que pertenecen: alumnos, profesores, etc. Sin embargo, y de cara a poder delegar la administración de los usuarios a sus respectivos centros o facultades, se hacía necesario transformar esta estructura en otra jerárquica, con ramas que definan a qué centro o facultad pertenece cada usuario.

Para ello se desarrolló una serie de scripts que actúan a modo de pasarela de datos entre la base de datos corporativa y el servidor de directorio. La pasarela toma los datos corporativos y según unas reglas definidas, y la lista de centros donde el sistema está implantado, calcula tres atributos para cada usuario: CA (código de centro donde el usuario es alumno), CP (código de centro donde el usuario es profesor) y CH (código de centro donde el usuario tendrá alojado su *home directory*). Estos atributos permiten a la pasarela decidir:

1. A qué centro va destinado un usuario en el momento del alta
2. A qué centro destinar un usuario existente cuando alguno de sus centros CA o CP cambia
3. Dar de baja el usuario si no pertenece a ningún centro soportado por el sistema

Así se consigue pasar de la estructura organizada en colectivos a la estructura organizada según centro. Los datos procesados a través de la pasarela se guardan para efectuar posteriormente la carga en el directorio.

3.2. Arquitectura

El sistema dispone de un directorio central que se alimenta de la información preparada en la pasarela, y de uno o más servidores de directorio en cada uno de los centros donde el sistema está implantado. Los servidores de directorio de los centros son réplicas completas del servidor de directorio central. En cada centro un servidor Samba usa el directorio replicado como base de datos de usuario para ofrecer servicios de autenticación y recursos de red.

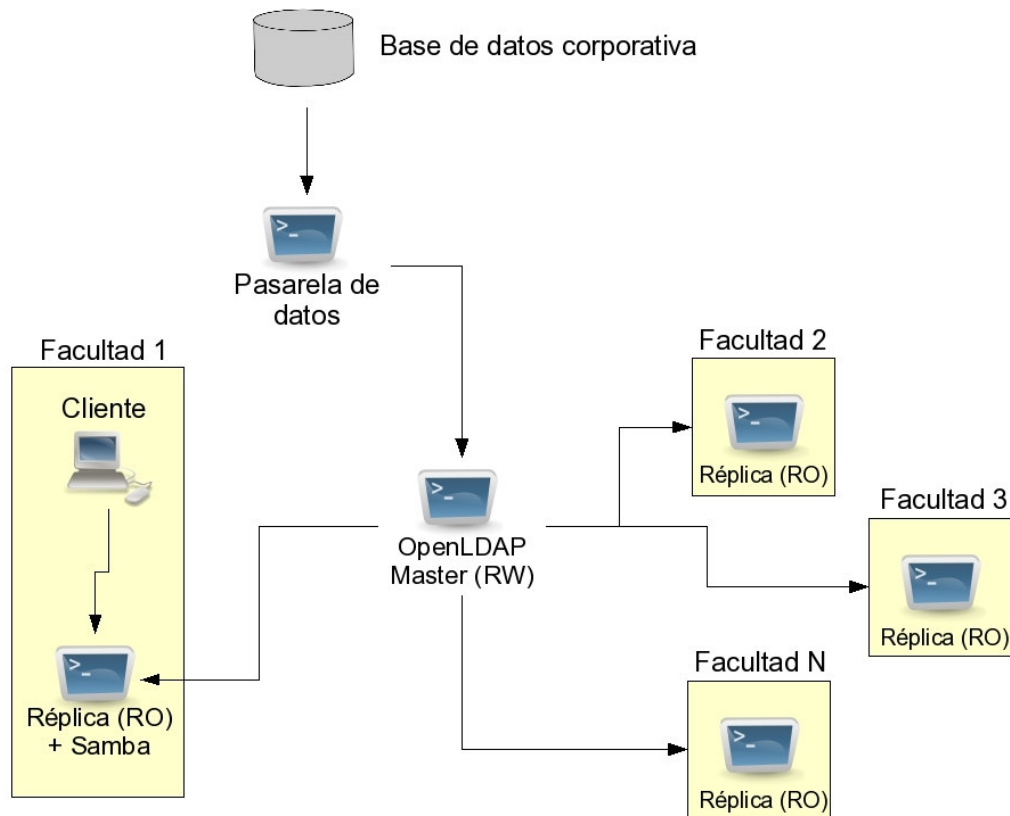


Figura 1: arquitectura de la plataforma

Los directorios replicados de los centros son una copia exacta del contenido del servidor central. En una primera fase del proyecto se optó por que cada centro dispusiera en su directorio sólo de los datos de los usuarios que le corresponden. Si un usuario externo al centro intentaba hacer uso de los ordenadores de las aulas, el servidor de directorio consultaba el servidor central. En la práctica el rendimiento de esta solución no era el deseable debido a la latencia generada por las peticiones entre servidores.

El excelente funcionamiento de OpenLDAP en las réplicas completas permite tener en cada una de ellas todos los datos de usuarios del sistema sin que el rendimiento se vea afectado. De esta manera se obtiene una cierta tolerancia a fallos: si el servidor central deja de estar disponible, los centros no podrán hacer altas o modificaciones de datos, pero podrán seguir sirviendo autenticación y recursos de red sin ningún problema.

La estructura del LDAP consta, básicamente, de una rama de usuarios (OU=USUARIOS) que contiene tantas ramas como centros usan el sistema. Dentro de la rama de cada centro (OU=CENTRO, OU=USUARIOS) se encuentran sus usuarios. Para poder autenticar usuarios de cualquier centro en un centro concreto, Samba los busca a partir de la raíz de todos los centros (OU=USUARIOS).

Por otro lado, y para poder delegar la administración de los usuarios propios a cada centro, se aplican listas de control de acceso (ACL, Access Control Lists) tanto en el LDAP del centro como en el LDAP central.

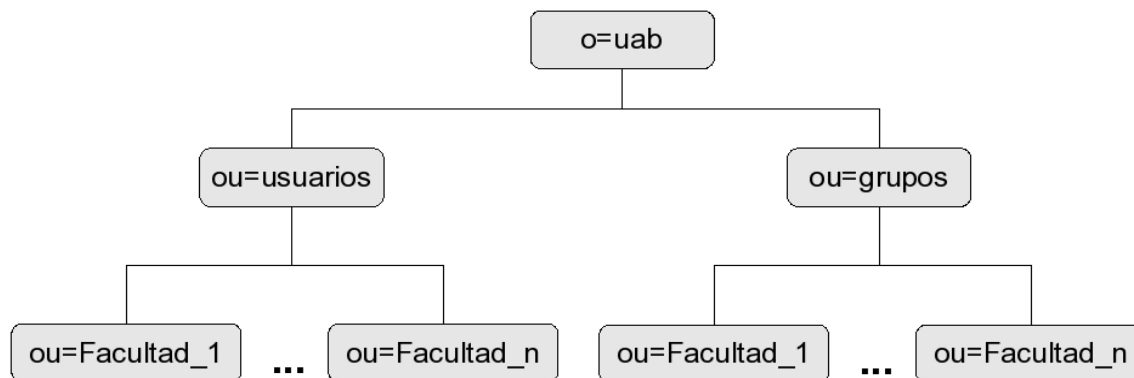


Figura 2: estructura del directorio

4. Despliegue y recuperación ante desastres

Debido a la naturaleza distribuida del sistema y el alto número de componentes a integrar en los diferentes centros, se ha optado por el desarrollo de un paquete de instalación específico para la distribución de Linux utilizada, Debian GNU/Linux 3.1. La utilización del paquete[4] simplifica enormemente el procedimiento de alta de un nuevo centro y permite parametrizar las características del sistema por los propios administradores del centro donde se realiza la instalación.

Dentro de los usos del paquete de instalación y no perdiendo de vista aspectos relacionados con la continuidad del servicio, tenemos que destacar la posibilidad, de utilizarlo para realizar una reinstalación de un centro ya operativo. Esta funcionalidad permite la recuperación de un centro de forma fácil y efectiva. Permitiendo minimizar la parada del servicio en caso de desastres.

El modelo de despliegue utilizado asegura una correcta instalación de los sistemas remotos, configura un parque de servidores homogéneo y facilita la continuidad del servicio.

5. Administración

La ausencia de herramientas completas de administración de sistemas Linux basadas en una solución samba-ldap, acompañado de unas necesidades muy específicas del entorno, facilitó también el desarrollo de una consola a medida. La consola, de carácter modular, utiliza las herramientas desarrolladas por IdealX[5], y ofrece la posibilidad de realizar a los administradores de centro las operaciones cotidianas de administración de una forma fácil y muy intuitiva. Se adapta a nuevas necesidades y es ampliable mediante posibles add-ons asociados a grupos definidos según perfiles.

Las características del producto también incluyen un módulo de monitorización de uso de disco y la categorización mediante listas Top Ten.

6. Monitorización

El sistema de monitorización está dividido según el ámbito de actuación. Por un lado se considera como prioritario y en consecuencia caracterizado de una forma global, todos los componentes que alimentan, mantienen y distribuyen el servicio de directorio. La monitorización de estos componentes se realiza desde el punto más estratégico del sistema, el servidor maestro de ldap, que se encarga de notificar cualquier incidencia a los administradores del centro/s afectado/s.

Por otro lado, la monitorización de los servicios ofrecidos por los servidores de centro recae sobre sus propios administradores. En la mayoría de casos se utilizan productos como Monit[6] o Munin[7] previamente evaluados y documentados por el grupo coordinador del sistema, asegurando así el menor impacto sobre la plataforma en producción y actuando como unidad certificadora.

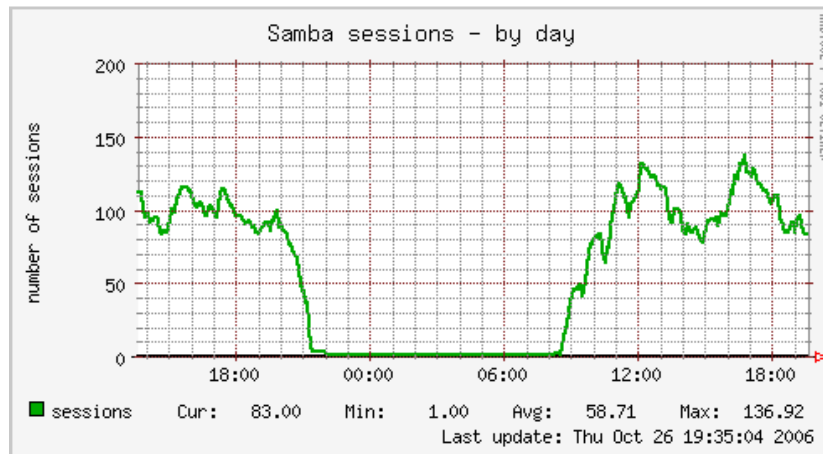


Figura 3: número de sesiones de Samba de un servidor de centro

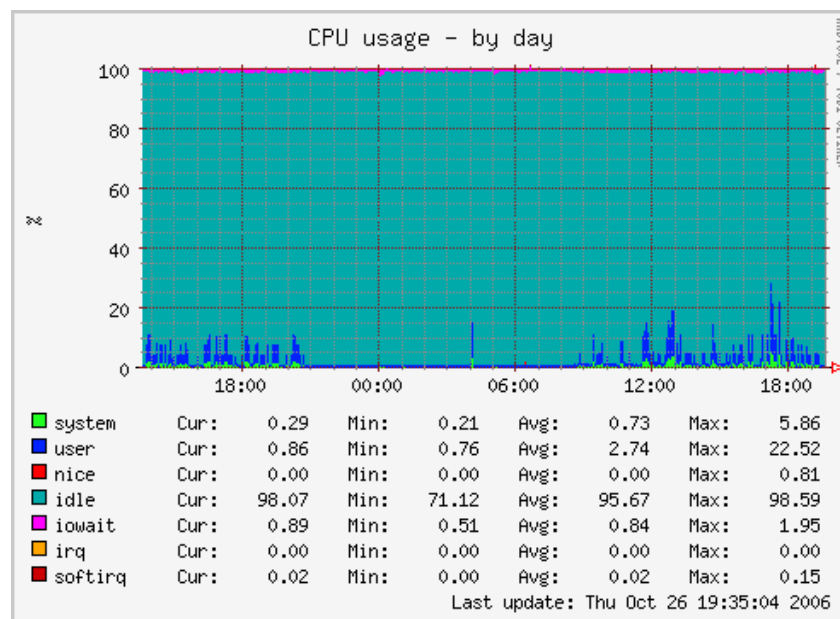


Figura 4: uso de CPU de un servidor de centro

7. Conclusiones

Los costes de administración se han reducido con la automatización y homogeneización de la gestión de usuarios. Todos los administradores disponen de una base homogénea pero a la vez de una gran autonomía para el desarrollo de nuevas funcionalidades. Éstas son añadidas en cada caso según el ámbito de soporte a la docencia que tienen las facultades sin interferir las unas con las otras.

Actualmente se da servicio a más de 35000 usuarios, y a 1300 máquinas cliente repartidas entre 12 centros con un excelente rendimiento.

8. Referencias

- [1] Debian GNU/Linux: <http://debian.org>
 - [2] Samba: <http://www.samba.org>
 - [3] OpenLDAP: <http://www.openldap.org>
 - [4] Debian Policy Manual: <http://www.us.debian.org/doc/debian-policy>
 - [5] IdealX Smbldap-tools: <http://www.idealx.com/content/view/184/169/lang.en>
 - [6] Monit: <http://www.tildeslash.com/monit>
 - [7] Munin: <http://munin.projects.linpro.no>
- The Official Samba-3 HOWTO and Reference Guide: <http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/>
- OpenLDAP 2.2 Administrator's Guide: <http://www.openldap.org/doc/admin22/>