Seguimiento de correos electrónicos

Universidad de Sevilla

Apoyo a la docencia e investigación
Servicio de informática y comunicaciones

Víctor Téllez Lozano
vtellez@us.es

Servicio de Informática
y Comunicaciones

Índice

1. Introducción (I)

- **Contexto**:

En un sistema de correo electrónico encontramos que:

- Los correos electrónicos son tratados por **diferentes procesos** tales como procesos antivirus, antispam, rbls, control de receptores, controles de envíos masivos,etc.
- Cada uno de estos **procesos** suelen estar **repartidos** en distintos servidores y no registran la información de la misma manera.

- Realizar un seguimiento de un correo se convierte en una **tarea tediosa** y **requiere conocimientos** amplios.
- Los usarios finales **no disponen de herramientas**.

1. Introducción (II)

- **Justificación del proyecto**:

Para paliar esta diversidad de información y facilitar el trabajo diario y la labor de trazabilidad, se crea una herramienta:

- **Tratar y unificar** los logs de los diferentes procesos.
- Presentar una aplicación web sencilla e intuitiva tanto para **administradores** como para **usuarios finales**.
- Brindar **funcionalidades extras**:
  - Indicadores de correo.
  - Seguir el correcto despliegue de una lista de distribución.
  - Combatir casos de Phishing.

1. Introducción (y III)

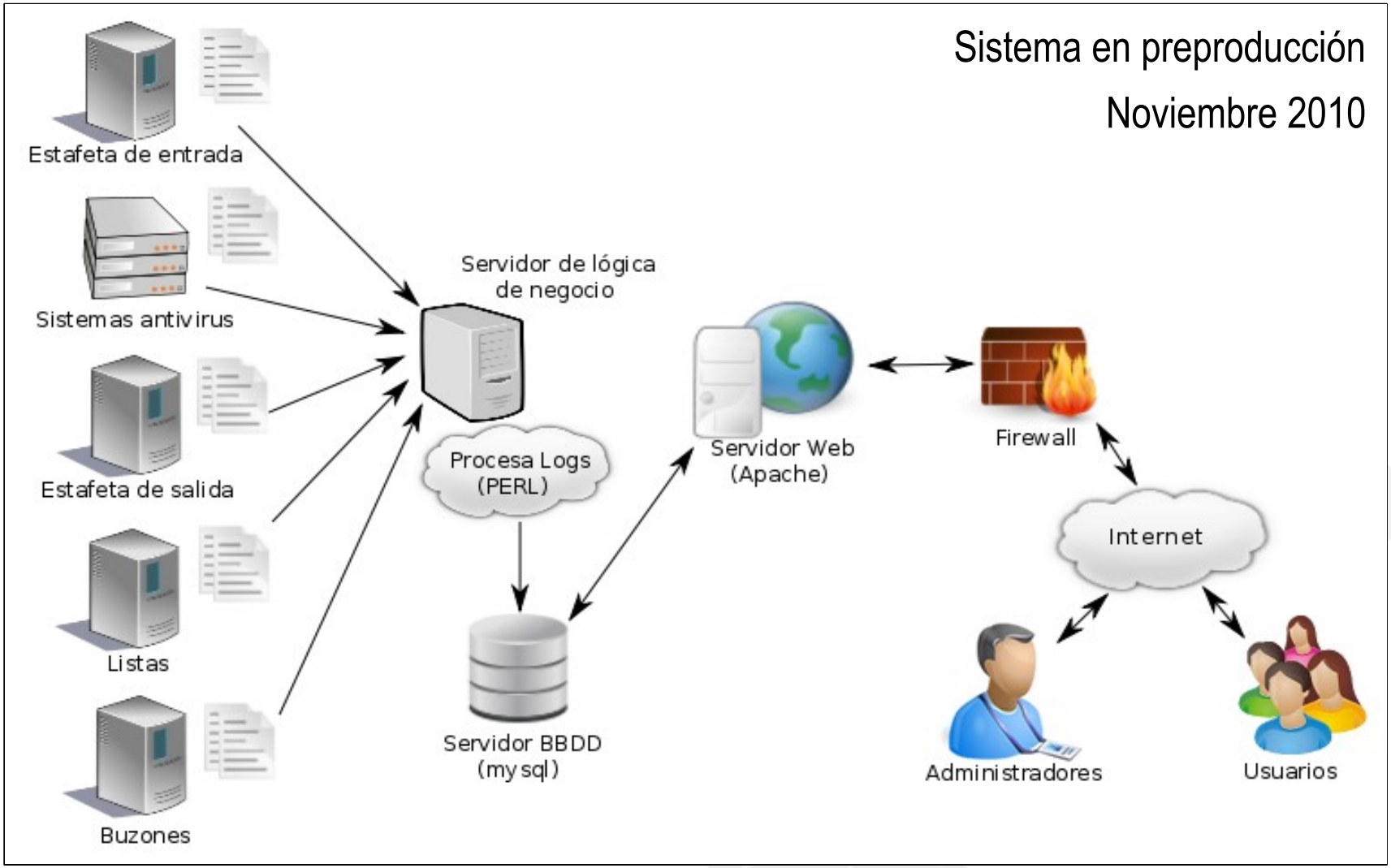
- **Requisitos para su puesta en marcha**:

La herramienta debía de cumplir una serie de requisitos:

- No interferir en los procesos que tratan el correo. Ni ralentizar el tiempo de trabajo de éstos.
- Debe ser únicamente de carácter observatorio sobre las estafetas de producción.
- Ofrecer resultados “en tiempo real” a los usuarios.
- Utilizar el message-id y el destinatario para el seguimiento en los distintos logs.
- Abierto a posibles cambios en las herramientas Software usadas así como a futuros cambios en los logs de éstas.

Índice

2. Esquema principal de funcionamiento (I)



2. Esquema principal de funcionamiento (y II)

Aspectos técnicos:

- Integrado con el Single Sign-On de la Universidad.
- El procesado de logs centralizado se realiza con PERL.
- Capa de presentación desarrollada con el framework de PHP CodeIgniter, usando el patrón MVC.
- Obtención de los logs utilizando un medio de transferencia segura siempre solicitado desde el servidor de lógica de negocio.
- Los correos permanecerán registrados 15 días en el sistema (3 millones de correo aprox.)

Índice

3. Estado actual del proyecto (I)

Actualmente el proyecto está **aún en desarrollo**:

- Entorno de preproducción pero obteniendo información de los sistemas de producción.
- Procesado de logs para las siguientes aplicaciones:
  - Qmail (qmail-send, qmail-smtpd) *
  - SpamAssassin
  - ClamAV
  - Qmail-scanner
  - Mailman
- Importante resaltar que la aplicación puede extenderse a otras aplicaciones típicas en sistemas de correo como postfix, sendmail, etc.

3. Estado actual del proyecto (y II)

Línea de trabajo actual antes de salir a producción:

- Mejora de la implementación de la interfaz web.
- Búsqueda de soluciones a ciertos problemas:
  - Codificaciones distintas en cada log.
  - Adaptaciones complejas en los logs de qmail para poder registrar el message-id.
- Proceso actual de migración:
  - Desarrollo de modulo de procesamiento de logs para **Postfix** y **Dovecot**.

Índice

4. Demo


Inicio
Mis mensajes
Buscador
Ayuda
Administración
vtellez@us.es
Todos
Mensajes recibidos
Mensajes enviados
Vista detallada de mensaje
Volver a la lista de mensajes
vtellez@us.es
Mensaje
grupocorreo@us.es
#Cod 351: El correo se ha sido entreg
Datos del mensaje
Parámetro
Valor
Remitente
vtellez@us.es
Destinatario
grupocorreo@us.es
Asunto
Fwd: Excedido el número de actualizaciones en BBDDCorp
Fecha envío
12/11/2010 - 09:31
Dirección IP de envío
Desconocida
Message-id
2145142337.10469.1289550705867.JavaMail.open-xchange@oxus.us.es
Historial del mensaje

DEMO

Índice

5. Futuro del proyecto y conclusiones

Nuevas ideas para futuras **ampliaciones**:

- Indicadores a demanda en un intervalo de tiempo específico.
- Desbloqueo de IPs bloqueadas, muestra online de logs, etc.

Conclusiones:

- Herramienta sencilla que permite que cualquier persona realice un seguimiento en segundos incluso sin ser un experto ni conocer el sistema de correo.
- Eficacia, comodidad y ahorro de tiempo significativo en el trabajo diario de administradores.
- Extensible y adaptable a cualquier sistema corporativo de correo.

Seguimiento de correos electrónicos

¡Gracias!

¿Alguna pregunta?

vtellez@us.es

Servicio de Informática
y Comunicaciones