Registro, Centralización y Análisis de Eventos en un entorno Corporativo Multiplataforma

DARÍO IVÁN ORTEGA VALIDO
ETIS

IGNASI RIUS FERRER

08 de marzo de 2013

AGRADECIMIENTOS

Mi más sincera gratitud a todos los que han hecho posible este momento
-compañeros, tutores y docentes-.

En especial, a Resu. Sin él, este trabajo jamás hubiera existido.
A él, a Mapi, a Luis y a Victor -recupérate pronto- por su apoyo y empuje indicional durante estos años.
A Susi, Antonio, Moisés y Octavio por esos minutos que siempre pudieron dedicar.

Gracias, Ignasi por tus ánimos y adecuada guía en este trabajo final de carrera.

Índice de Contenidos

Índice de Tablas

Índice de Ilustraciones

1. DESCRIPCIÓN DEL TRABAJO FINAL DE CARRERA

1.1. INTRODUCCIÓN: EVENTOS y LOGS

Durante muchos años la gestión de eventos y el termino anglosajón “log” han sido utilizados casi como sinónimos por la íntima relación existente entre ellos. Sin embargo, desde un punto de vista formal, este último hace solamente referencia a la parte de gestión de eventos que tiene que ver con su registro. Es decir, se refiere a la gestión registral de los eventos. Así, por ejemplo, cuando hablamos de “archivos de logs”, hablamos de los archivos que se utilizan para registrar los sucesos o eventos acaecidos en un sistema o producto.

En este documento, y en los próximos realizados sobre este trabajo, queremos hacer especial hincapié sobre esta diferenciación. Así, cuando hablemos de la gestión de “logs” nos referiremos a la gestión que se hace sobre los archivos o sistemas de registros de eventos. Mientras que al hablar de la gestión de eventos, nos referiremos hacia todos aquellos usos y/o funcionalidades que tienen que ver con los sucesos de un sistema con independencia de cómo la fuente origen los registra y/o almacena.

De igual forma, este trabajo remarca desde su concepción (de hecho es una de las motivaciones esenciales del mismo), la especial importancia que tienen los procesos registrales, la salvaguarda y la no alteración de los ficheros originales que resultan de los mismos.

1.2. ANTECEDENTES

La arquitectura de sistemas de cualquier entorno corporativo suele estar conformada por la conjunción de diferentes tecnologías interrelacionadas. Esta disparidad de tecnologías y plataformas suelen tener un elemento común de vital importancia: la generación de eventos.

La gestión de eventos no solo es una parte esencial de la ingeniería de sistemas como tal, sino que también ha adquirido especial relevancia en ámbitos como el de la seguridad o el legislativo. Así, en la actualidad, se ha provocado un salto cualitativo en como los servicios informáticos conciben la gestión de los eventos. Este ha ido evolucionando, desde un mantenimiento más o menos ordenado de una multiplicidad de LOGS (registros de eventos) dispersos, a la gestión centralizada de sucesos. Esta gestión permite, entre otras funcionalidades, un análisis integral de lo que está pasando en los sistemas mediante la correlación de acontecimientos entre elementos dependientes. Por otro lado, esta gestión centralizada permite una política integral de la salvaguarda de la integridad de los LOGS mediante un repositorio común, estructurado y securizado, de ficheros que se firman y registran para su posterior verificación.

Sin duda, los sistemas GNU/Linux y el software libre sustentado sobre ellos, abanderan este nuevo concepto de gestión de los eventos. Así, bajo esta forma de entender el desarrollo de las tecnologías nos encontramos con múltiples herramientas (Rsyslog, LogAnalizer, webalizer, logsreporters, etc) integrables bajo una misma arquitectura, que proporcionan servicios multi-plataforma y que nos permiten lograr esa visión global de lo que pasa en nuestros sistemas. Y es por ello, por lo que son idóneos para la implementación de una arquitectura de este estilo.

1.3. DESCRIPCIÓN DEL TRABAJO

El presente trabajo final de carrera pretende diseñar e implementar una arquitectura del registro, centralización, y análisis de de eventos multi-servicio y multi-plataforma basado en software libre y en sistemas GNU/Linux.

Para ello, el proyecto pivotará sobre tres elementos esenciales: la sincronización de LOGS en un repositorio centralizado y securizado, el re-envío de eventos a un sistema centralizado de análisis de sucesos y el acceso mediante una única consola unificadora de las principales herramientas de análisis.

Los ejes que vertebraran el desarrollo del proyecto serán:

1. El análisis y categorización de tipología de eventos según los diferentes servicios, productos y plataformas: diseño de una **política** de centralización de eventos y LOGS
2. El diseño e implementación de un sistema de centralización, sincronización y securización de LOGS**:** repositorio centralizado de LOGS firmados y registro de verificación de firmas
3. El diseño y la implementación de un sistema de **correlación y análisis de eventos**: herramienta de análisis de eventos en tiempo real
4. La implementación de herramientas de análisis de ficheros de **LOGS con semántica propia**, para la generación de reportes estadísticos.
5. El desarrollo de un interface web único de acceso a las diferentes herramientas de análisis: **consola unificada de análisis de eventos**.

1.4. ALCANCE

El alcance del proyecto viene definido por dos grandes bloques de actuación:

1. Implementación y configuración de la nueva arquitectura de gestión de eventos y logs. Entendiéndose como tal, la instalación y configuración de los productos específicos (rsync, rsyslo, nfs server, mysql server, etc) para la consecución de los objetivos del proyecto. De igual forma, se explicitaran las políticas adoptadas para la gestión de los eventos y la estructuración de repositorios centralizados.
2. Configuración de productos y servicios consumidores de la nueva arquitectura. Dado el gran número de potenciales servicios y/o productos integrables y el tiempo limitado de realización del proyecto se suscribe el desarrollo del mismo a los siguientes consumidores:
    - Sistemas Operativos: -Linux- Red Hat Enterprise 5 y 6, Centos 6; -Windows- Windows 2003 y 2008 server
    - Electrónica de red: CISCO
    - Bases de Datos: MySQL
    - Gestión de Accesos: SSH, FTP y Proxy
3. El desarrollo de un interface web único de acceso a las diferentes herramientas de análisis

No se entiende como alcance del proyecto la descripción de la instalación y configuración de software base sino para aquellos elementos esenciales para la consecución de los objetivos del mismo

1.5. SISTEMAS GNU/LINUX y SOFTWARE LIBRE a IMPLEMENTAR

A continuación se relacionan el conjunto de sistemas y productos inicialmente detectados como esenciales para la materialización del proyecto:

- Sistemas GNU/Linux: Red Hat Enterprise 5 y 6; Centos 6
- Herramientas de centralización: Rsync, Rsyslog, NTSyslog, Delta Copy
- Herramientas de análisis: LogAnalyzer, Postfix and Amavisd-new Log Reporting, Webalizer y otras herramientas ofrecidas por la comunidad de usuarios de Internet, y que sean susceptibles de ser integradas opcionalmente.
- Servidor de Bases de Datos: MySql
- Servidor Web: Apache
- Lenguaje de programación: PHP, AJAX
- Utilidades: Google Chart Tools y PHP File Tree, JQuery, TinyBox2

1.6. MARCO DE REALIZACIÓN

El marco de realización del proyecto será un entorno corporativo real. Este es un escenario idóneo para testar la integración de los diferentes consumidores en la nueva arquitectura. Además, se encuentra estratificado por entornos (pre-produccción y producción) lo que facilita la integración de la nueva arquitectura sin afectar a la producción real y posibilita la incorporación de funcionalidades que solo tengan fines didácticos o de aplicabilidad en el presente trabajo de fin de carrera.

2. OBJETIVOS

2.1. OBJETIVO GENERAL

El objetivo general de trabajo será el diseño y la implementación de una arquitectura para la gestión centralizada de eventos basada en sistemas GNU/Linux y Software Libre.

2.2. OBJETIVOS ESPECÍFICOS

Como objetivos específicos se fijaran los siguientes:

1. Diseño de una política para el registro de Eventos
2. Diseño de una política para la centralización de LOGS
3. Instalación y configuración sistemas de sincronización de eventos
4. Instalación y configuración sistemas de centralización de LOGS
5. Configuración clientelar de consumidores.
6. Instalación productos análisis de eventos:
    - LogAnalyzer
    - Postfix Log Reporting

- Amavisd-new Log Reporting
- Webalizer

7. Desarrollo e integración de una consola unificada de acceso al sistema de análisis

3. PLANIFICACIÓN

A continuación se relacionan la lista de tareas y su planificación:

Nombre de tarea	Duración	Comienzo	Fin
Propuesta Inicial del TFC y plan de trabajo	**14 días**	**mié 27/02/13**	**mar 12/03/13**
Identificación de TFC	3 días	mié 27/02/13	vie 01/03/13
Identificación posibles tecnologías de la solución	5 días	sáb 02/03/13	mié 06/03/13
Realización propuesta inicial y Plan de Trabajo	5 días	jue 07/03/13	lun 11/03/13
Entrega Propuesta Inicial del Plan de Trabajo	1 día	mar 12/03/13	mar 12/03/13
PAC1: Plan de trabajo	**16 días**	**lun 04/03/13**	**mar 19/03/13**
Correcciones	3 días	mié 13/03/13	vie 15/03/13
Realización Plan Trabajo	3 días	sáb 16/03/13	lun 18/03/13
Entrega: Plan de Trabajo	1 día	mar 19/03/13	mar 19/03/13
PAC2: Descripción de las tecnologías del TFC (20% TFC)	**12 días**	**mié 20/03/13**	**dom 31/03/13**
TFC20: Especificación de requisitos Arquitectura	**1 día**	**mié 20/03/13**	**mié 20/03/13**
Requisitos de Producto	1 día	mié 20/03/13	mié 20/03/13
Requisitos de Integración	1 día	mié 20/03/13	mié 20/03/13
TFC21: Análisis y definición de productos	**7 días**	**jue 21/03/13**	**mié 27/03/13**
Análisis de la tipología de eventos del alcance del proyecto	2 días	jue 21/03/13	vie 22/03/13
Definición de la política de centralización de eventos	1 día	sáb 23/03/13	sáb 23/03/13
Definición de la política de centralización de LOGS	1 día	sáb 23/03/13	sáb 23/03/13
Definición Software Base: SO GNU/Linux	1 día	dom 24/03/13	dom 24/03/13
Definición Software Sincronización de Eventos: syslog/Rsyslog	2 días	lun 25/03/13	mar 26/03/13
Definición Software Centralización de LOGS: rsync	1 día	lun 25/03/13	lun 25/03/13
Definición Software Análisis de Eventos: LogAnalizer, LogReporting, Webalizer	2 días	lun 25/03/13	mar 26/03/13
Definición de lenguajes y Utilidades: PHP, AJAX, Chart, PHP File Tree	1 día	mié 27/03/13	mié 27/03/13
Realización PAC2	3 días	jue 28/03/13	sáb 30/03/13
Entrega PAC2	1 día	dom 31/03/13	dom 31/03/13
PAC3: Diseño e implementación del proyecto (50% TFC)	**21 días**	**lun 01/04/13**	**dom 21/04/13**
TFC30: Diseño Arquitectura	**1 día**	**lun 01/04/13**	**lun 01/04/13**
Definición de Servidores Virtuales	1 día	lun 01/04/13	lun 01/04/13
Definición de Background de BD	1 día	lun 01/04/13	lun 01/04/13
Definición Sistema de Archivos Compartidos	1 día	lun 01/04/13	lun 01/04/13
TFC31: Instalación y Configuración	**10 días**	**mar 02/04/13**	**jue 11/04/13**
Instalación y Configuración Software Base	1 día	mar 02/04/13	mar 02/04/13
Instalación y Configuración BD	1 día	mié 03/04/13	mié 03/04/13
Instalación y Configuración Software Sincronización Eventos	2 días	jue 04/04/13	vie 05/04/13
Instalación y Configuración Software Centralización LOGS	1 día	sáb 06/04/13	sáb 06/04/13
Instalación y Configuración Software Análisis: LogAnalizer, LogReporting, Webalizer	5 días	dom 07/04/13	jue 11/04/13
TFC32: Instalación y Configuración Clientes	**3 días**	**vie 12/04/13**	**dom 14/04/13**
Configuración de clientes: Servidores GNU/Linux	1 día	vie 12/04/13	vie 12/04/13
Configuración de clientes: Electrónica de Red CISCO	1 día	vie 12/04/13	vie 12/04/13
Configuración de clientes: BD MySQL	2 días	sáb 13/04/13	dom 14/04/13
TFC33: Desarrollo Consola Única	**3 días**	**lun 15/04/13**	**mié 17/04/13**
Inteface WEB	1 día	lun 15/04/13	lun 15/04/13
Integración de Productos	2 días	mar 16/04/13	mié 17/04/13

Realización PAC3	3 días	jue 18/04/13	sáb 20/04/13
Entrega PAC3	1 día	dom 21/04/13	dom 21/04/13
PAC4: Resultados y análisis del trabajo (70% TFC)	**28 días**	**lun 22/04/13**	**dom 19/05/13**
TFC40: Pruebas Funcionales	**11 días**	**lun 22/04/13**	**jue 02/05/13**
Pruebas Centralización de Eventos	2 días	lun 22/04/13	mar 23/04/13
Pruebas Centralización de LOGS	2 días	mié 24/04/13	jue 25/04/13
Pruebas Software Análisis	2 días	vie 26/04/13	sáb 27/04/13
Pruebas Consola	2 días	dom 28/04/13	lun 29/04/13
Adecuaciones Finales	3 días	mar 30/04/13	jue 02/05/13
Análisis de Resultados	3 días	vie 03/05/13	dom 05/05/13
Realización PAC4	10 días	lun 06/05/13	mié 15/05/13
Entrega PAC4	1 día	dom 19/05/13	dom 19/05/13
Memoria Final	**20 días**	**lun 20/05/13**	**sáb 08/06/13**
Correcciones Finales	19 días	lun 20/05/13	vie 07/06/13
Entrega Memoria	1 día	sáb 08/06/13	sáb 08/06/13
Video Presentación	**6 días**	**sáb 15/06/13**	**jue 20/06/13**
Realización Video	5 días	sáb 15/06/13	mié 19/06/13
Entrega Video	1 día	jue 20/06/13	jue 20/06/13
Tribunales	**4 días**	**mar 25/06/13**	**vie 28/06/13**

Tabla 1. Planificación de Tareas

3.1. DIAGRAMA DE GANTT. PLANIFICACIÓN INICIAL

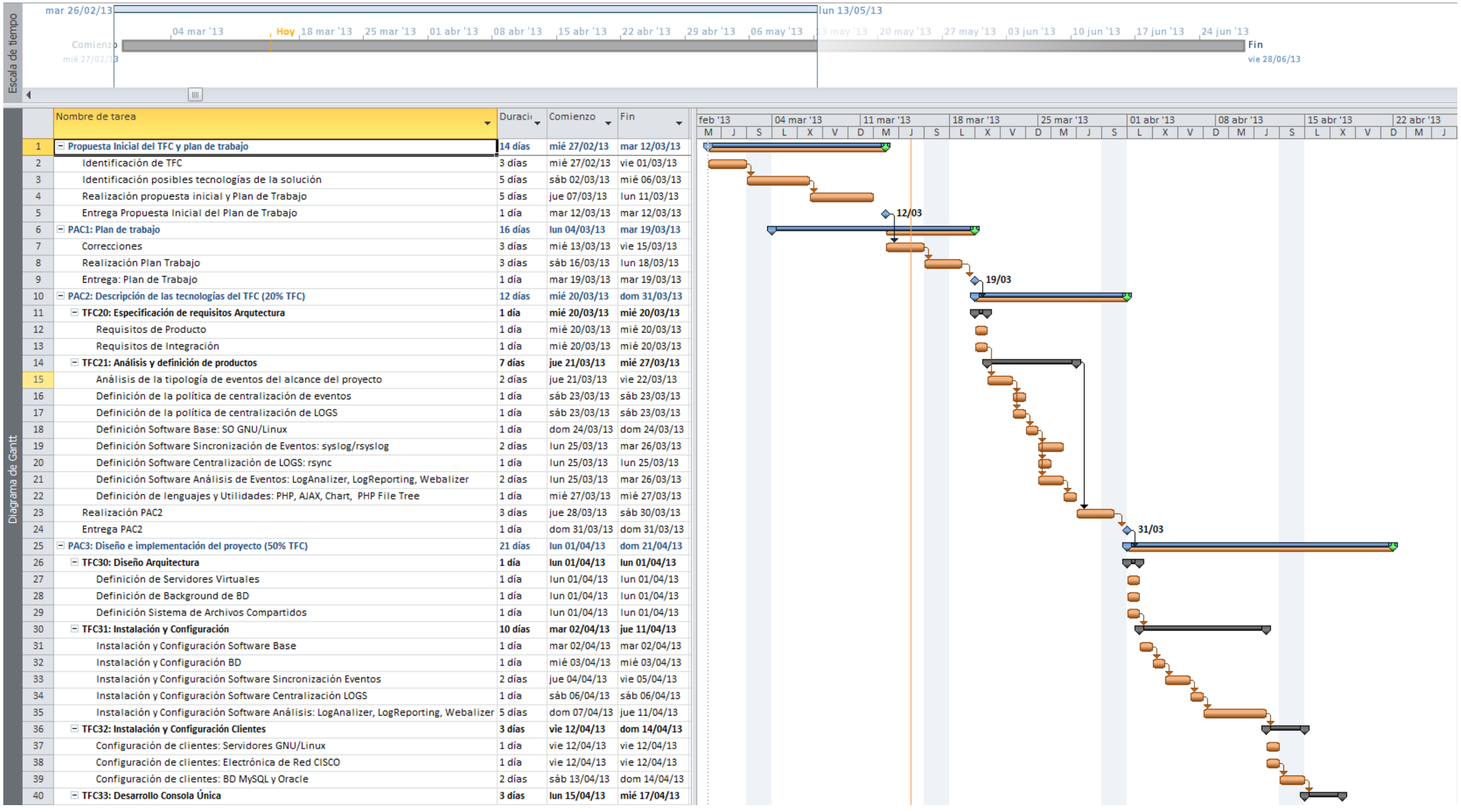


Ilustración 1. Diagrama de GANTT.

Ilustración 2. Diagrama de GANTT -continuación-.

3.2. DIAGRAMA DE GANTT. SEGUIMIENTO PAC2

Escala de tiempo: lun 18/02/13 — mar 14/05/13 — Comienzo mié 27/02/13 — Hoy — Fin vie 28/06/13

		Nombre de tarea	Duraci	Comienzo	Fin	Pag. Memoria
1	✓	**Propuesta Inicial del TFC y plan de trabajo**	**14 días**	**mié 27/02/13**	**mar 12/03/13**	**6**
2	✓	Identificación de TFC	3 días	mié 27/02/13	vie 01/03/13	7
3	✓	Identificación posibles tecnologías de la solución	5 días	sáb 02/03/13	mié 06/03/13	8
4	✓	Realización propuesta inicial y Plan de Trabajo	5 días	jue 07/03/13	lun 11/03/13	8
5	✓	Entrega Propuesta Inicial del Plan de Trabajo	1 día	mar 12/03/13	mar 12/03/13	
6	✓	**PAC1: Plan de trabajo**	**16 días**	**lun 04/03/13**	**mar 19/03/13**	
7	✓	Correcciones	3 días	mié 13/03/13	vie 15/03/13	
8	✓	Realización Plan Trabajo	3 días	sáb 16/03/13	lun 18/03/13	
9	✓	Entrega: Plan de Trabajo	1 día	mar 19/03/13	mar 19/03/13	
10	✓	**PAC2: Descripción de las tecnologías del TFC (20% TFC)**	**12 días**	**mié 20/03/13**	**dom 31/03/13**	
11	✓	**TFC20: Especificación de requisitos Arqutectura**	**1 día**	**mié 20/03/13**	**mié 20/03/13**	**14**
12	✓	Requisitos de Producto	1 día	mié 20/03/13	mié 20/03/13	14
13	✓	Requisitos de Integración	1 día	mié 20/03/13	mié 20/03/13	16
14	✓	**TFC21: Análisis y definición de productos**	**7 días**	**jue 21/03/13**	**mié 27/03/13**	**19**
15	✓	Análisis de la tipología de eventos del alcance del proyecto	2 días	jue 21/03/13	vie 22/03/13	28
16	✓	Definición de la política de centralización de eventos	1 día	sáb 23/03/13	sáb 23/03/13	26
17	✓	Definición de la política de centralización de LOGS	1 día	sáb 23/03/13	sáb 23/03/13	30
18	✓	Definición Software Base: SO GNU/Linux	1 día	dom 24/03/13	dom 24/03/13	33
19	✓	Definición Software Sincronización de Eventos: syslog/rsyslog	2 días	lun 25/03/13	mar 26/03/13	36
20	✓	Definición Software Centralización de LOGS: rsync	1 día	lun 25/03/13	lun 25/03/13	35
21	✓	Definición Software Análisis de Eventos: LogAnalizer, LogReporting, Webalizer	2 días	lun 25/03/13	mar 26/03/13	39
22	✓	Definición de lenguajes y Utilidades: PHP, AJAX, Chart, PHP File Tree	1 día	mié 27/03/13	mié 27/03/13	45
23	✓	Realización PAC2	3 días	jue 28/03/13	sáb 30/03/13	
24	✓	Entrega PAC2	1 día	dom 31/03/13	dom 31/03/13	

Diagrama de Gantt

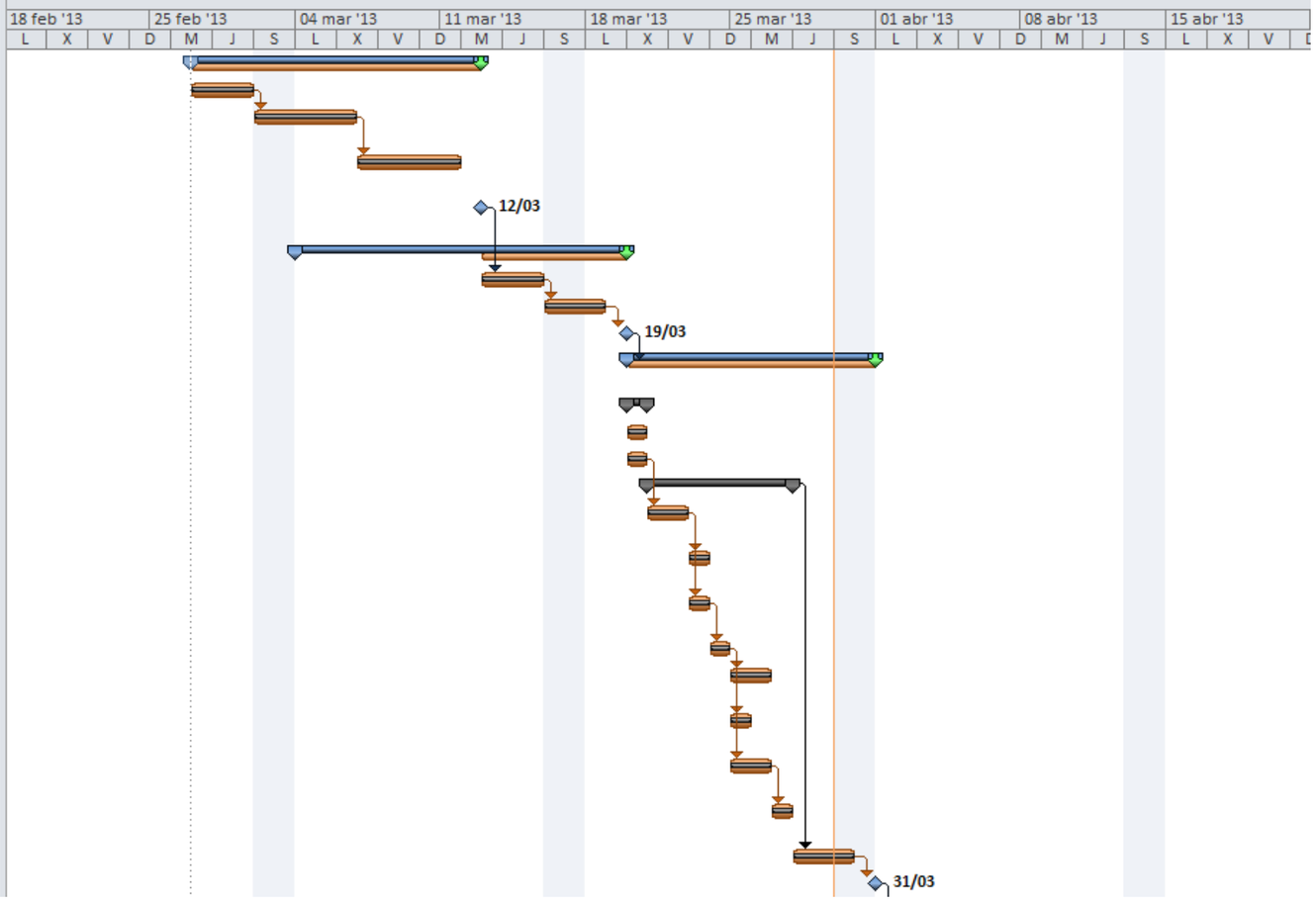


Ilustración 3. Diagrama de GANTT. Seguimiento PAC2.

3.3. DIAGRAMA DE GANTT. SEGUIMIENTO PAC3

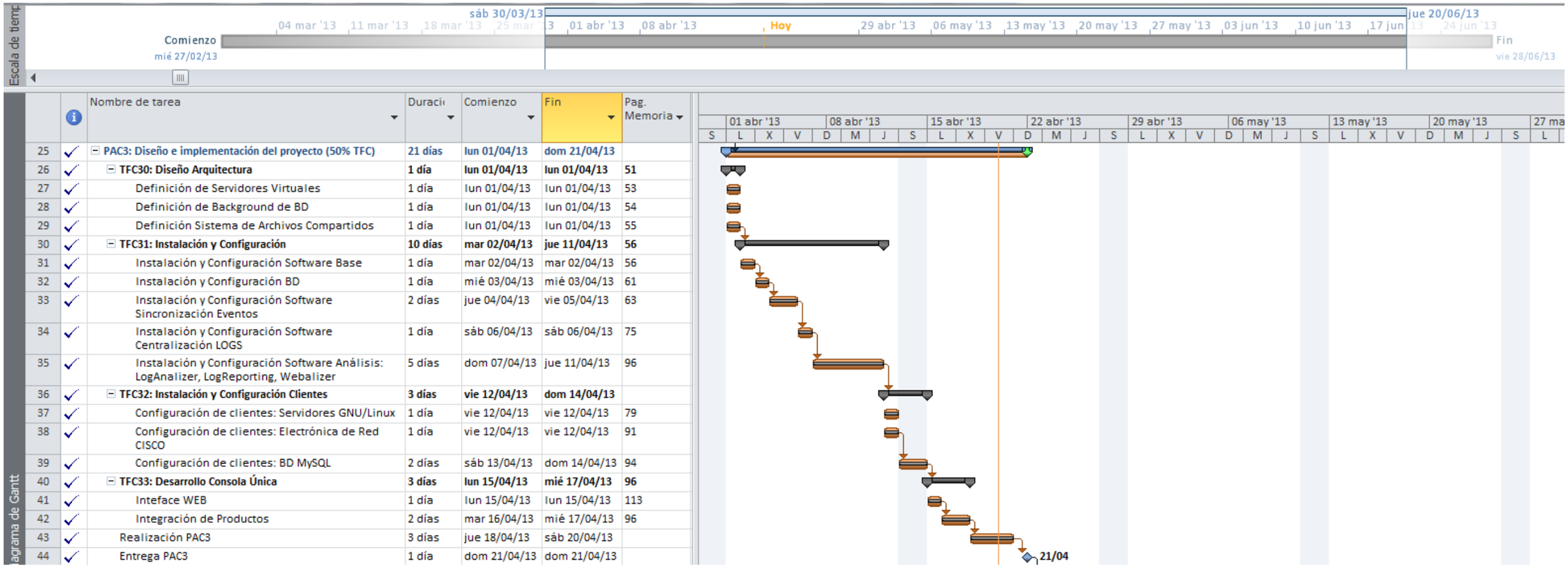


Ilustración 4. Diagrama de GANTT. Seguimiento PAC3.

3.4. DIAGRAMA DE GANTT. SEGUIMIENTO PAC4

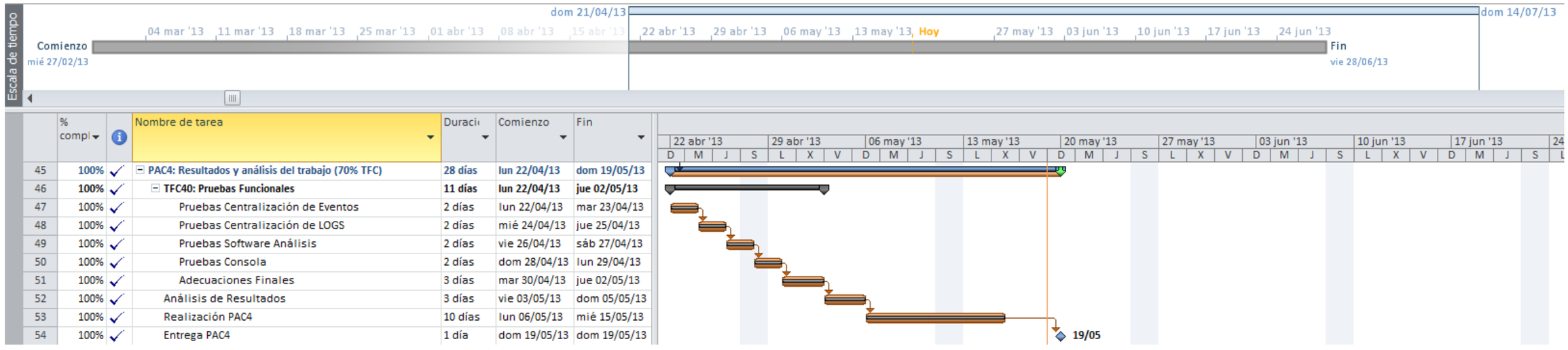


Ilustración 5. Diagrama de GANTT. Seguimiento PAC4.

4. ESPECIFICACIÓN DE REQUISITOS

La especificación inicial de requisitos se ha estratificado en cuatro niveles de profundidad:

1. Requisitos Globales de Funcionalidad: se recogen aquellos aspectos esenciales de necesidades y/o funcionalidades que deben estar disponibles en la plataforma (Nivel 1: Macro-visión de requisitos)
2. Requisitos específicos de los producto: se recogen las capacidades tecnológicas mínimas que deben cumplir los productos vertebradores de la solución (Nivel 2: Adecuación tecnológica de productos)
3. Requisitos de integración: se recogen los aspectos básicos necesarios para la adecuación de la solución al ecosistema tecnológico de la organización -identificación básica de consumidores, integración con productos tecnológicos transversales a toda la organización, flujos de información.- (Nivel 3: Adecuación al entono y política tecnológica corporativa existente)
4. Requisitos de funcionamiento: se recogen las necesidades iniciales detectadas para el correcto funcionamiento de la nueva plataforma (Nivel 4: Necesidades básicas de implementación)

4.1. REQUISITOS FUNCIONALES GLOBALES

Se identifican como requisitos esenciales de la plataforma los siguientes:

- La sincronización de LOGS en un repositorio centralizado: los clientes deben poder sincronizar diariamente los ficheros de LOGS en un sistema de ficheros centralizado. Se debe registrar el nombre del servidor origen, la fecha y hora de centralización, el tamaño y la firma del fichero. La firma debe ser verificable para asegurar la integridad del mismo en el tiempo.
- El re-envío y registro de eventos a un sistema centralizado de análisis de sucesos. El sistema debe permitir la estratificación por entorno (pre-producción y producción), el filtrado y la búsqueda avanzada, así como la generación de estadísticas e informes.
- El acceso mediante una única consola unificadora de las principales herramientas de análisis: Consola Web que identifique y estratifique cada uno de los productos de análisis. Debe ser accesible desde los principales navegadores, con capacidad de auto-refresco, permitir la navegación por el “logstore” centralizado e informar del consumo de espacio del mismo.

4.2. REQUISITOS ESPECÍFICOS DE LOS PRODUCTO A IMPLEMENTAR

4.2.1. HERRAMIENTAS DE CENTRALIZACIÓN

- Centralización de LOGS:
  - Herramienta Open Source, licencia GNU o similar
  - Compatible con hash MD5
  - Transferencia rápida de archivos incrementales
  - Actualización de árboles de directorios y sistemas de archivos completos

  - Conservación de los enlaces simbólicos, enlaces duros, propiedades de los archivos, permisos, dispositivos y "timestamp"
  - Utilización de rsh, ssh o direct socket como transporte
  - Soporte de sincronización anónimo
- Centralización de Eventos:
  - Herramienta Open Source, licencia GNU o similar
  - Gestión de "hostname" del suceso (host gestor de suceso, host origen)
  - Conservación de "hostname" para entornos con NAT
  - Soporte sub-archivos de configuración
  - Estadísticas periódicas sobre los contadores syslog
  - Adaptado Estándar RFC5424, RFC3195
  - Capacidad para crear analizadores de mensajes personalizados
  - Integración con balanceadores de carga para crecimiento horizontal
  - Capacidad de ejecutar múltiples listeners TCP (en puertos diferentes)
  - Soporte para la exportación en formato CSV
  - Soporte syslog-transport-tls
  - Soporte nativo para el envío de mensajes de correo
  - Capacidad de monitorizar archivos de texto.
  - Conversión de txt en mensajes de syslog
  - Capacidad de enviar mensajes de captura SNMP
  - Interfaz API
  - Uso de expresiones regulares en el filtrado
  - Redundancia a fallo
  - Soporte para IPv6
  - Delimitación de remitentes permitidos
  - Soporte syslog comprimido
  - Control de formato de hora según standares ISO 8601/RFC 3339
  - Ejecución de scripts según mensajes recibidos
  - Filtrado de cualquier parte del mensaje
  - Soporte nativo para la escritura a bases de datos MySQL
  - Soporte para ejecución de múltiples instancias
  - Soporte para ficheros de log de más de 2GB
  - Filtrado de mensajes basándose en la secuencia de llegada

4.2.2. HERRAMIENTAS DE ANÁLISIS

- Herramienta genérica de análisis de eventos:
  - Herramienta Open Source, licencia GNU o similar
  - Interfaz Web
  - Selección de origen de análisis
  - Selección de vista
  - Categorización de eventos
  - Búsqueda Avanzada temporalizada por tipología de log, severidad, servicio y/o fuente
  - Búsqueda genérica de mensajes

        - Integración nativa protocolo syslog
        - Exportación en formato CSV y XML
        - Estadísticas de eventos producidos, fuentes de origen, tipología y marco temporal
        - Generación de informes eventos producidos, fuentes de origen, tipología y marco temporal
        - Integración con MySQL
        - Integración Apache Web Server
- Herramientas de análisis de ficheros de LOGS con semántica propia:
    - Herramientas análisis de LOGS de correo:
        - Herramientas Open Source, licencia GNU o similar
        - Postfix MTA y Amavis-new log parser
        - Funcionamiento Standalone o como módulo Logwatch
    - Herramienta de análisis de Web Logs Server:
        - Herramientas Open Source, licencia GNU o similar
        - Interpretación de CLF (Common Log Format)
        - Interpretación de FTP format logs (wu-ftpd/proftpd)
        - Interpretación de Squid proxy server
        - Interpretación de W3C Extended log format

4.3. REQUISITOS DE INTEGRACIÓN

Un resumen ejecutivo del ecosistema tecnológico nos revela que la organización posee un 69% de máquinas con sistema operativo Linux y con un crecimiento de aproximadamente un 4,05% semestral, frente a un 31% con tecnología Microsoft Windows con un crecimiento de un 2,37%. El total de máquinas -físicas y virtuales- supera ampliamente las 800, con más de 40 tipos de tecnologías diferentes (servidores web, servidores aplicaciones, servidores aplicaciones remotas, proxy's, ftp, vpn, antivirus corporativos, servicios de directorios, servicios identidad única, correo, soluciones movilidad, dashboard, servicios telefonía, servicios de voip, servicios videoconferencia, servicios monitorización, administración, nómina, personal, tele-formación, servicios ficheros, servicios impresión, servicios de backup, gestión incidencias, bases de datos, etc.) a lo que hay que sumar todos los elemento de cohesión (electrónica de red, refrigeración, etc.) necesarios para el adecuado funcionamiento de los servicios. Un entorno tan heterogéneo y complejo requiere unas políticas de integración y homogenización de tecnológica que permita su gestionabilidad. De cara al proyecto que nos ocupa podemos resaltar las siguientes:

1. Política de especificación de consumidores del servicio
2. Política de homogenización tecnológica
3. Política de almacenamiento, repositorios de información
4. Política de flujos de interconexión

A continuación se relacionan las especificaciones de dichas políticas que son identificadas como requisitos de integración en el presente proyecto.

4.3.1. ESPECIFICACIÓN DE CONSUMIDORES DEL SERVICIO

La presente política explicita los consumidores naturales de todos los servicios a implementar. El nivel 0 de dicha política explicita la estratificación básica para proyectos en implantación en donde se caracterizan los tipos consumidores básicos, para el presente proyecto serán:

1. Servidores con tecnología Linux.
2. Servidores con tecnología Windows.
3. Electrónica de red.

4.3.2. HOMOGENIZACIÓN TECNOLÓGICA

La motivación básica de esta política es la buscar una línea equilibradora entre la diversidad tecnológica y la gestionabilidad. En ella, actualmente, se establece:

- "Red Hat Enterprise Linux versión 5 como sistema operativo corporativo para servidores con tecnologías Linux."
- "los sistemas auditables deben incorporar como mínimo el protocolo SYSLOG de mensajes para la notificación de eventos."
- "MySQL versión 5.1 como base de datos corporativa para productos OpenSource"

4.3.3. ALMACENAMIENTO Y REPOSITORIOS DE INFORMACIÓN

En esta política se explicitan las acciones para la gestión del almacenado de la información. En ella, actualmente, se establece:

- "Toda información clasificada como relevante o superior debe ser almacenada, al menos, en un repositorio centralizado (vía SAN o NAS) que disponga de redundancia en el acceso, tolerancia a fallos y mecanismos de copia de seguridad."

4.3.4. FLUJOS DE INTERCONEXIÓN

Se establece la normativa básica de intercomunicación de servicios. En ella, actualmente, se establece:

- "Por norma general, los flujos de interacción deben ser iniciados desde el origen con el fin de delimitar las dependencias de seguridad entre los elementos"
- "Esta política en su totalidad o en parte podrá ser sobreseída por la aplicabilidad de la política de seguridad"

4.4. REQUISITOS DE IMPLEMENTACIÓN

Dado el gran número de servidores, eventos y LOGS a tratar se estiman como requisitos básicos para la implantación de la nueva plataforma los siguientes:

- Un servidor de almacenamiento de LOG:
  - Servidor Linux kernel 2.6.18 o superior
  - Doble Procesador multi-núcleo 2,8 Ghz (64-bit)

    - Memoria Ram: 4Gb
    - Almacenamiento local de al menos 250Gb
    - Tarjetas Fiber Channel redundante
    - Dos tarjetas de red ethernet gigabit tolerante a fallos
    - Interfaz de gestión de consola remota
- Un servidor de Base de Datos: El gestor de BBDD deberá garantizar al menos la capacidad de realizar 400 operaciones de INSERT concurrentemente.
    - Servidor Linux kernel 2.6.18 o superior
    - Doble Procesador multi-núcleo 2,8 Ghz (64-bit)
    - Memoria Ram: 6Gb
    - Almacenamiento local de al menos 250Gb
    - Tarjetas Fiber Channel redundante
    - Dos tarjetas de red ethernet gigabit tolerante a fallos
    - Interfaz de gestión de consola remota
- Un servidor de Web Consola Unificada:
    - Servidor Linux kernel 2.6.18 o superior
    - Doble Procesador multi-núcleo 2,8 Ghz (64-bit)
    - Memoria Ram: 4Gb
    - Almacenamiento local de al menos 250Gb
    - Tarjetas Fiber Channel redundante
    - Dos tarjetas de red ethernet gigabit tolerante a fallos
    - Interfaz de gestión de consola remota
- Dos Tera Byte de espacio SAN

Todos estos requisitos son genéricos no ligados a ninguna familia, ni producto. Admitiéndose igualmente características homónimas en sistemas virtualizados.

5. ANÁLISIS DE LA CENTRALIZACIÓN DE LOGS Y EVENTOS.

El proceso de centralización conforma uno de los ejes esenciales dentro del proyecto. En su concepción más simple, en este proceso podemos distinguir dos tareas principales:

- La centralización de LOGS
- La re-colección centralizada de notificaciones de eventos

Ambas, abordan la transferencia de información de servidores remotos a un repositorio común. Sin embargo, en la primera estaríamos hablando de la transferencia de ficheros al repositorio centralizado (transferencia de archivos) mediante una aplicación –rsync- para la transmisión eficiente de datos incrementales. Mientras que en la segunda, hablamos de remisión de notificaciones de eventos (recolección de eventos) utilizando el re-envío de mensajes según especificaciones de un protocolo –syslog- recogido en el RFC5424.

5.1. TRANSFERENCIAS CON RSYNC

Rsync es una utilidad de software libre (GNU General Public License) que proporciona una transferencia rápida y eficiente de datos incrementales. Mediante una técnica de "delta encoding", permite sincronizar archivos y directorios entre dos máquinas de una red. El algoritmo "Delta encoding" tiene como objetivo obtener solamente los bytes que han sido modificados desde la última versión del archivo, permitiendo reducir considerablemente el tamaño de éste y lograr una optimización del uso de la red al momento de realizar un respaldo. Una vez que se tiene comprimido un archivo, se puede obtener el archivo original teniendo la versión de referencia del archivo y el archivo generado por el algoritmo de Delta encoding.

Además de las bondades de la transferencia incremental, rsync presenta otras funcionalidades especialmente interesantes para la centralización de LOGS como: actualización de árboles de directorios y sistemas de archivos completos; conservación de los enlaces simbólicos, enlaces duros, propiedades de los archivos, permisos, dispositivos y "timestamp"; utilización de rsh, ssh o direct socket como transporte.

Rsync es co-natural al mundo Linux, aunque existen utilidades "Windows Friendly" de licenciamiento OpenSource como "DeltaCopy" que realmente son contenedores de Rsync.

Rsync funcionará como un demonio en el servidor de centralización de LOGS

5.2. EL PROTOCOLO SYSLOG. LOS COLECTORES

El protocolo syslog define como transmitir mensajes de notificación de eventos. Syslog está estratificado en capas como muchos otros protocolos. Concretamente, utiliza tres capas que son las siguientes:

- Capa de contenidos: gestiona la información contenida en un mensaje de syslog.
- Capa de aplicación: se encarga de la generación, interpretación, enrutamiento y almacenamiento de los mensajes syslog.
- Capa de Transporte: se encarga del transporte del mensaje

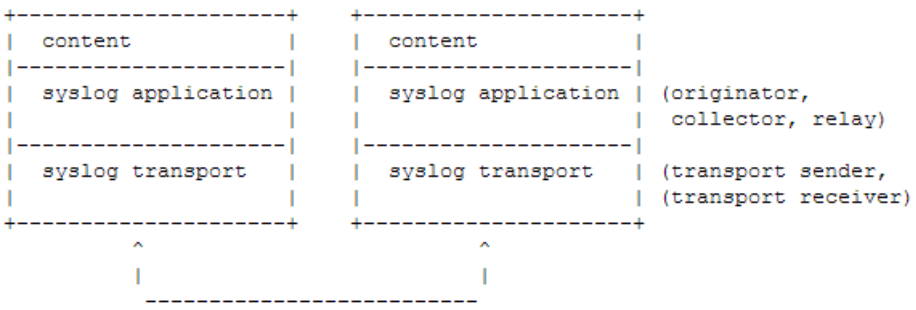


Ilustración 6. Capas del protocolo Syslog

Esta estructuración en capas nos permite múltiples escenarios posibles a la hora de diseñar la arquitectura de recolección. En ellos se distinguen tres actores principales:

- Originator: es la fuente que genera el contenido del mensaje
- Relay: encargado de re-enviar los mensajes hacia otros "relays" o a los "collectors" finales
- Collector: reúne y almacena los mensajes para futuro análisis.

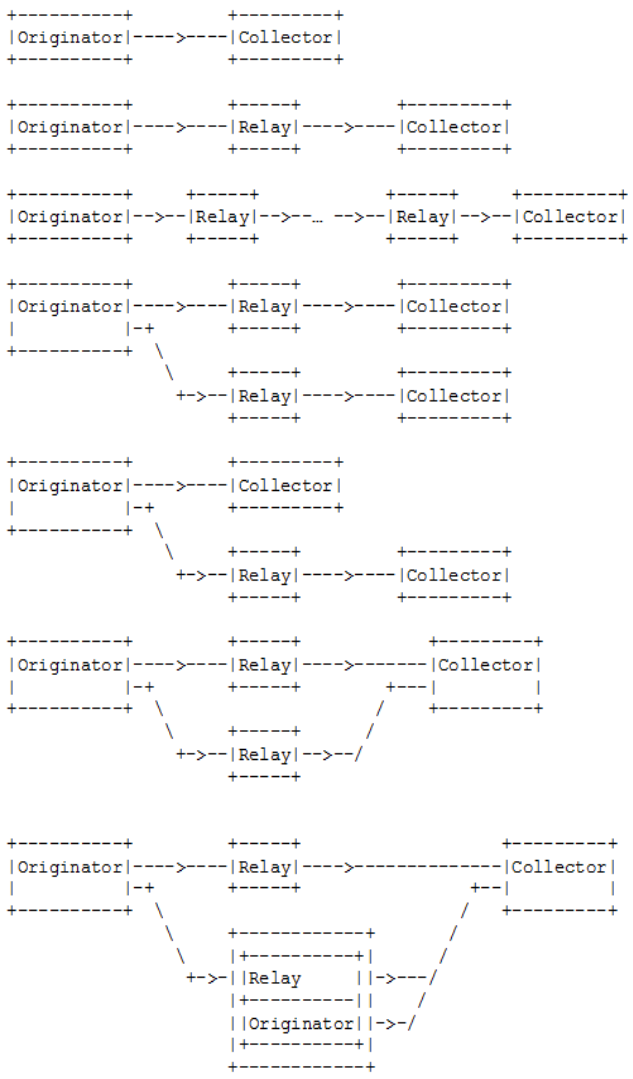


Ilustración 7. Posibles escenarios de arquitectura de Syslog

Este hecho, dota de gran versatilidad al protocolo y será esencial a la hora del diseño de la arquitectura de centralización de eventos.

Es necesario, indicar que la especificación de Syslog no define ningún protocolo de transporte especifico sino que insiste que cualquier protocolo de transporte empleado “NO DEBE alterar deliberadamente” el mensaje de syslog. Como complemento a esta especificación, y para mantener la asociación histórica que tenía syslog con el protocolo UDP, se definió el RFC5426 que si aborda la transmisión de mensajes Syslog sobre UDP.

Con respecto a los mensajes, syslog si describe exhaustivamente como deben ser construidos los mensajes

5.2.1. EL FORMATO DEL MENSAJE

El mensaje de syslog tiene la siguiente ABNF [RFC5234] definición:

```
SYSLOG-MSG      = HEADER SP STRUCTURED-DATA [SP MSG]

HEADER          = PRI VERSION SP TIMESTAMP SP HOSTNAME
                  SP APP-NAME SP PROCID SP MSGID
PRI             = "<" PRIVAL ">"
PRIVAL          = 1*3DIGIT ; range 0 .. 191
VERSION         = NONZERO-DIGIT 0*2DIGIT
HOSTNAME        = NILVALUE / 1*255PRINTUSASCII

APP-NAME        = NILVALUE / 1*48PRINTUSASCII
PROCID          = NILVALUE / 1*128PRINTUSASCII
MSGID           = NILVALUE / 1*32PRINTUSASCII

TIMESTAMP       = NILVALUE / FULL-DATE "T" FULL-TIME
FULL-DATE       = DATE-FULLYEAR "-" DATE-MONTH "-" DATE-MDAY
DATE-FULLYEAR   = 4DIGIT
DATE-MONTH      = 2DIGIT  ; 01-12
DATE-MDAY       = 2DIGIT  ; 01-28, 01-29, 01-30, 01-31 based on
                          ; month/year
FULL-TIME       = PARTIAL-TIME TIME-OFFSET
PARTIAL-TIME    = TIME-HOUR ":" TIME-MINUTE ":" TIME-SECOND
                  [TIME-SECFRAC]
TIME-HOUR       = 2DIGIT  ; 00-23
TIME-MINUTE     = 2DIGIT  ; 00-59
TIME-SECOND     = 2DIGIT  ; 00-59
TIME-SECFRAC    = "." 1*6DIGIT
TIME-OFFSET     = "Z" / TIME-NUMOFFSET
TIME-NUMOFFSET  = ("+" / "-") TIME-HOUR ":" TIME-MINUTE


STRUCTURED-DATA = NILVALUE / 1*SD-ELEMENT
SD-ELEMENT      = "[" SD-ID *(SP SD-PARAM) "]"
SD-PARAM        = PARAM-NAME "=" %d34 PARAM-VALUE %d34
SD-ID           = SD-NAME
PARAM-NAME      = SD-NAME
PARAM-VALUE     = UTF-8-STRING ; characters '"', '\' and
                               ; ']' MUST be escaped.
SD-NAME         = 1*32PRINTUSASCII
                  ; except '=', SP, ']', %d34 (")
```

```
MSG             = MSG-ANY / MSG-UTF8
MSG-ANY         = *OCTET ; not starting with BOM
MSG-UTF8        = BOM UTF-8-STRING
BOM             = %xEF.BB.BF
UTF-8-STRING    = *OCTET ; UTF-8 string as specified
                  ; in RFC 3629
OCTET           = %d00-255
SP              = %d32
PRINTUSASCII    = %d33-126
NONZERO-DIGIT   = %d49-57
DIGIT           = %d48 / NONZERO-DIGIT
NILVALUE        = "-"
```

Como podemos observar el mensaje está compuesto por tres grandes grupos de información separados entre sí por un espacio –SP-:

- HEADER
- STRUCTURED DATA
- MSG

5.2.1.1. LA CABECERA (HEADER)

La cabecera del mensaje está formada de la siguiente manera:

```
HEADER = PRI VERSION SP TIMESTAMP SP HOSTNAME SP APP-NAME
         SP PROCID SP MSGID
```

Donde

- PRI: Hace referencia a la Prioridad. Es calculado basándose en los valores de la "facilidad" y "severidad" del mensaje. Así, la fórmula para calcular la prioridad sería:

  $$PRI = Facility * 8 + Severity$$

  Donde valores más pequeños indican mayor nivel de prioridad. Por ejemplo, un mensaje del kernel (facilidad = 0) con una severidad de emergencia (severidad = 0) tendrá un valor de prioridad 0. Mientras que un mensaje de uso local (facilidad = 20) con una severidad de aviso (severidad =5) generará un valor de prioridad de 165

  $$Mensaje\ del\ Kernel \rightarrow PRI = (Facility = 0) * 8 + (Severit = 0) = 0$$

  $$Mensaje\ local \rightarrow PRI = (Facility = 20) * 8 + (Severit = 5) = 165$$

- VERSION: Especifica la versión de protocolo Syslog. Se compone de dos dígitos, y no puede valer 0. Debe seguir inmediatamente al carácter ">" del campo PRI sin espacios.
- TIMESTAMP: Identifica cuando el mensaje fue creado. Con el siguiente formato: Mmm dd hh:mm:ss,
- HOSTNAME: Cadena de 255 caracteres –máximos- que indica el nombre de la máquina que envío el mensaje. Debe contener el nombre de host o su dirección IP
- APP-NAME: Cadena de 48 caracteres –máximos- que identifica el dispositivo o aplicación que origina el mensaje.

- PROCID: Cadena de 128 caracteres –máximos- que identifica el nombre o ID del proceso asociado.
- MSGID: Cadena de 32 caracteres –máximos- que identifica el tipo de mensaje

Código	Facility (facilidad)
0	Mensajes de kernel
1	Mensajes de nivel de usuario
2	Sistema de correo
3	Demonios del sistema
4	Mensaje de seguridad/autorización[1]
5	Mensaje generado internamente por syslogd
6	Subsistema de impresora en línea
7	Subsistema de noticias de red
8	Subsistema UUCP
9	Demonio de reloj[2]
10	Mensaje de seguridad/autorización[1]
11	Demonio FTP
12	Subsistema NTP
13	Auditoria de eventos[1]
14	Alerta de eventos[1]
15	Demonio de reloj[2]
16	Uso local 0
17	Uso local 1
18	Uso local 2
19	Uso local 3
20	Uso local 4
21	Uso local 5
22	Uso local 6
23	Uso local 7

Tabla 2. Tabla de códigos de facilidad

Código	Severity (gravedad)
0	Mensajes de kernel
1	Mensajes de nivel de usuario
2	Sistema de correo
3	Demonios del sistema
4	Mensaje de seguridad/autorización
5	Mensaje generado internamente por syslogd
6	Subsistema de impresora en línea
7	Subsistema de noticias de red

Tabla 3. Tabla de códigos de severidad

5.2.1.2. LOS DATOS ESTRUCTURADOS (STRUCTURED-DATA)

Provee un mecanismo para estructurar información de una manera bien definida, fácil de interpretar y parsear. En este campo se puede almacenar meta-información sobre el mensaje syslog que sea de interés.

Tiene la siguiente estructura: `STRUCTURED-DATA = NILVALUE / 1*SD-ELEMENT`

[1] Se han encontrado algunos sistemas operativos que utilizan las Facilidades 4, 10, 13 y 14 para seguridad/autorización.

[2] Se han encontrado algunos sistemas operativos que utilizan las Facilidades 9 y 15 para mensajes de reloj

Y contiene un conjunto de SD-ELEMENT en el que cada elemento tiene un SD-ID y un conjunto de pares Nombre-Valor. Por ejemplo: [origin ip="192.1.1.1" ip="192.1.1.115"]

5.2.1.3. EL MENSAJE (MSG)

El campo MSG es una cadena de caracteres libre a disposición de la aplicación que provee información sobre el evento. Debe ser texto UNICODE, UTF-8 [RFC3629].

5.2.2. LOS COLECTORES.

La versatilidad ofertada por el protocolo Syslog no sólo se refiere hacia el modelado de la arquitectura sino que se ha extendido, a través de sus diferentes implementaciones (syslog-ng, Rsyslog), a los repositorios finales de almacenamiento de la información. Así, el repositorio de información puede ser cualquier tipo de almacenamiento estándar (discos) -en sus dos vertientes servidor local o remoto-, como una base de datos (transaccional como MySQL o no orientadas a SQL como MongoDB).

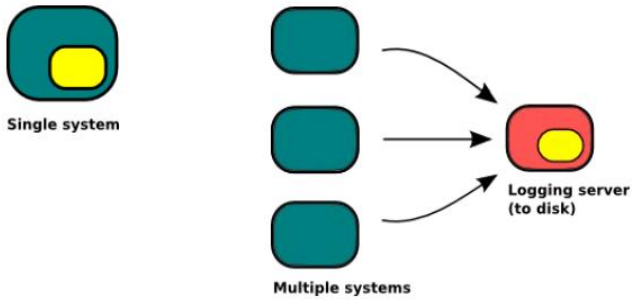


Ilustración 8. Configuración de colector con repositorio en disco.

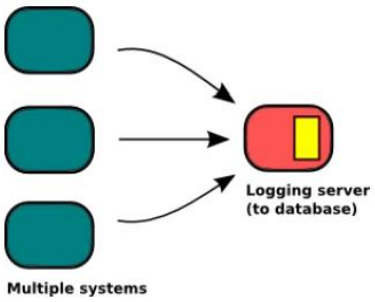


Ilustración 9. Configuración de colector con repositorio en base de datos.

Este hecho, es de vital importancia en plataformas extensas en el que el número de mensajes es tan grande que se requieren elementos activos que garanticen el performance adecuado en el registro de eventos on-line.

De las distintas familias de colectores que aportan esta facilidad nos inclinamos por la implementación RSYSLOG. Que además incorpora un nuevo protocolo –RELP- para el transporte que mejora la fiabilidad sobre TCP evitando duplicación de eventos en caso de error.

5.3. RECOLECCIÓN DE EVENTOS

5.3.1. ESQUEMA BÁSICO DE FUNCIONAMIENTO

El proceso de centralización del registro de eventos tiene por fin último que todos los eventos susceptibles de análisis tengan como repositorio final una base de datos (con independencia de su salvaguarda en otros soportes, tal y como indicará la política de recolección de eventos). Así, dependiendo de las capacidades ofertadas por las distintas implementaciones del protocolo syslog, existirá un flujo de re-envío de eventos que pasamos a describir a continuación.

Los consumidores tipo 1 –granja de servidores Linux- a través de la implementación RSYSLOG volcaran directamente (procedimiento soportado nativamente) los eventos en tiempo real sobre la base de datos (hacer notar que el servidor de base de datos al ser también consumidor de tipo 1 volcará sus eventos sobre el mismo soporte).

Los consumidores tipo 2 y 3 –granja de servidores Windows, electrónica de red y con demonios genéricos de Syslog- realizarán un re-envío de notificaciones de eventos a un servidor tipo 1 (en nuestro caso el de almacenamiento de logstore) que los volcará directamente sobre la base de datos.

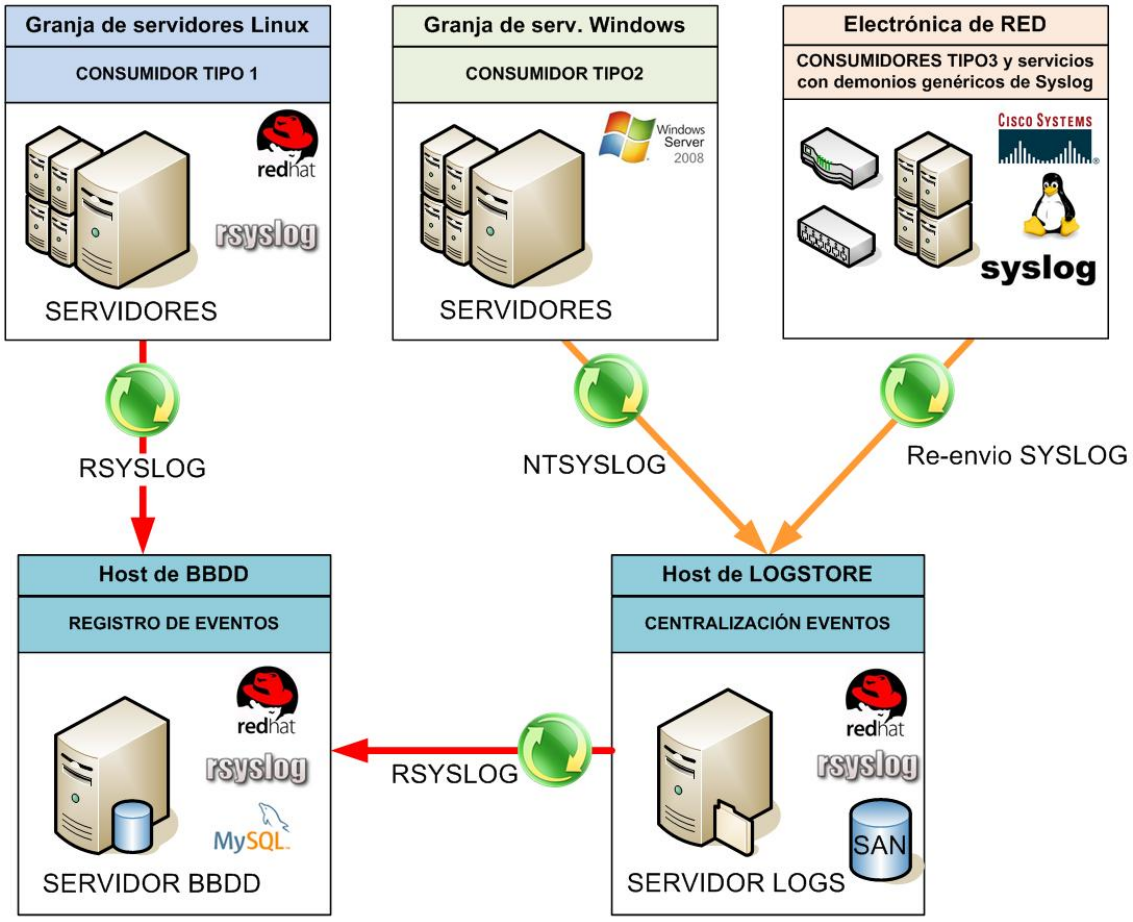


Ilustración 10. Esquema de Centralización y Recolección de Eventos.

5.3.2. POLÍTICA RECOLECCIÓN DE EVENTOS

5.3.2.1. Salvaguarda de los eventos

Los eventos serán salvaguardados en 2 tipos de soporte distintos:

- Sobre sistema de ficheros en repositorios locales que serán agrupados por la centralización de logs.
- Sobre Base de Datos.

5.3.2.2. Organización de los repositorios locales

Ubicación

Para el salvaguardo de los eventos sobre sistema de ficheros, se utilizará un directorio base sobre el que guardar todos los ficheros de eventos que el logger reciba, intentando siempre mantener una estructura plana y sin subdirectorios. No obstante, dependiendo del servicio y para una mejor categorización, excepcionalmente podrá utilizarse un subdirectorio dentro del directorio base.

Por defecto y para los sistemas basados en Linux, el directorio base será /var/log/.

La configuración de la ubicación quedará explicitada por configuración del logger RSYSLOG.

Nomenclatura de ficheros

La sintaxis de cada fichero de eventos deberá tener una nomenclatura específica que servirá para una rápida identificación del origen de los eventos, permitiendo:

- Identificar el host/equipo generador del registro.
- Determinar el entorno en el que se produce el evento.
- Identificar la el servicio específico que lo ha generado.
- Emplazar en un rango de tiempo, la sucesión de eventos.

Así, el formato del nombre del fichero será el siguiente:

<hostname>-<[exp|pre]>-<servicio>-<fecha>.log

Esta quedará delegada en el propio sistema dinámico de RSYSLOG.

Rotación de ficheros

Dado el carácter masivo de eventos susceptibles de ser registrados, se ha determinado que una ventana temporal adecuada de rotación de estos. Esta ventana será de 24 horas, empezando la rotación a las 00:00 de cada día.

Así mismo, cada fichero rotado tendrá que mantenerse en el sistema por lo menos un periodo de 7 días, permitiendo a cualquier administrador el poder utilizarlos para labores de supervisión local de eventos.

La tarea de rotado quedará delegada en el propio sistema dinámico de RSYSLOG.

Limitación por tamaño de los ficheros

No existirá limitación física para el tamaño de los ficheros, dependiendo la dimensión de este únicamente de la cantidad de eventos que se registren en el periodo concebido entre su rotación.

Compresión de ficheros

Los ficheros históricos que hayan sido rotados, serán comprimidos mediante compresión estándar "UNIX gzip", a efectos de:

- No provocar desbordamiento del espacio de disco en el servidor.
- Minimizar el tiempo de movimiento/copia de los ficheros rotados, a cualquier otro sistema que los necesite, como puede ser el de centralización de logs.

Para identificar que los ficheros han sido comprimidos, se los renombrará bajo el mismo formato, con la excepción de que se les añadirá una nueva extensión ".gz":

<hostname>-<[exp|pre]>-<servicio>-<fecha>.log.gz

La tarea de compresión será aplicada mediante mecanismos ajenos a sistemas RSYSLOG, pudiendo estar delegada en tareas de sistemas como shell scripts con ejecución automatizada mediante scheduler crontab.

5.3.2.3. Tipificación para BBDD

Para dotar de mayor fortaleza al análisis de eventos, se incorpora un sistema de almacenamiento en base de datos de aquellos eventos susceptibles a ser auditados con mayor frecuencia, y cuya complejidad pueda implicar un tratamiento complejo en acciones relacionadas con el análisis forense (como localizar patrones de mensaje, acotados por rangos de fecha y hora específicas).

Esquemas basados en servicios

Dado el grado de escritura que el gestor de base de datos puede tener, se utilizarán distintos esquemas de BBDD, para cada tipo de servicio a auditar. Cada esquema de BBDD vendrá definido por uno nombre significativo, tipificado de la siguiente manera: RSYSLOGDB_<SERVICIO>.

Por ejemplo, el esquema RSYSLOGDB_AUTHPRIV almacenará con independencia de su severidad todas las notificaciones de autenticación (authpriv) sobre los programas SSHD, CROND, ANACRON. Para una lista completa de servicios y esquemas consultar la Tabla 4. Tipología de notificaciones de eventos a registrar.

Purga de eventos

Dado el alto volumen de registros, el gestor de base de datos deberá contar con procedimientos almacenados o mecanismos capaces de purgar aquellos eventos susceptibles de considerarse antiguos.

Estructura del esquema

- Tabla EVENTS: es la tabla principal de cada esquema y viene definida por los siguientes campos de información:
  - ID: Campo auto-numerado. Clave primaria de la tabla.
  - TIMESTAMP: Fecha de creación del evento, en el formato: AAAA-MM-DD HH:MM:SS
  - DATE_PARSER: Fecha de generación del evento, en el formato: AAAA-MM-DD
  - TIME_PARSER: Fecha de generación del evento, en el formato: HH:MM:SS
  - HOSTNAME: Nombre del sistema que genera el evento. Convertido automáticamente a mayúsculas.
  - SERVICE: Nombre del servicio que genera el evento.
  - SERVICE_SESSION: ID numérico de la sesión del servicio.
  - MSG: Evento RAW captado por el logger.
- Procedimiento almacenado PURGE_INTERVAL (INPUT days INT): procedimiento almacenado que eliminará los registros cuya fecha sea mayor al número de días indicado por parámetro, desde la fecha actual de ejecución.

5.3.2.4. TIPOLOGÍA DE EVENTOS

En la siguiente tabla se especifican los tipos de registro que se tomarán por servicio, software que lo genera, severidad y esquema de destino:

Servicio	Software	Severity	Service	BBDD
Logs genéricos	-	*.info; authpriv.none; cron.none; mail.none; localX.none	messages	-
Logs críticos	-	*.error	errors	RSYSLOGDB_ERROR
Autenticación	SSHD, CROND, ANACRON	authpriv.*	authpriv	RSYSLOGDB_AUTHPRIV
Correo	POSTFIX, PERDITION, COURIER, AMAVIS	mail.*	mail	RSYSLOGDB_MAIL
FTP	PROFTPD	Local1.*	proftpd	RSYSLOGDB_FTP
Navegación proxy	SQUID	Local2.*	squid-error	RSYSLOGDB_HTTP_ERROR
Eventos web	APACHE		http-error https-error	
Windows Events (PRE)	SO Windows	Local4.*	event	RSYSLOGDB_WINDOWS_EVENTS
Windows Events (EXP)	SO Windows	Local5.*	event	RSYSLOGDB_WINDOWS_EVENTS
Electrónica de red	Cisco	Local6.*	syslog	RSYSLOGDB_NETWORK
log-centralizer	RSYNC	local7.notify	-	RSYSLOGDB-LOG-CENTRALIZER

Tabla 4. Tipología de notificaciones de eventos a registrar.

5.4. CENTRALIZACIÓN DE LOGS

5.4.1. ESQUEMA BÁSICO DE FUNCIONAMIENTO

La idea básica de la centralización de logs es el envío de ficheros de log mediante algoritmo "Delta encodig" (en sus diferentes implementaciones Rsync o DeltaCopy) a un sistema de ficheros en un servidor remoto. Éste, será diario y siguiendo las directrices de la política de centralización de logs. Hacer constar que los consumidores tipo 3, mediante el re-envío de eventos han centralizado en el host de logstore, el cual hará rsync diario sobre el repositorio centralizado.

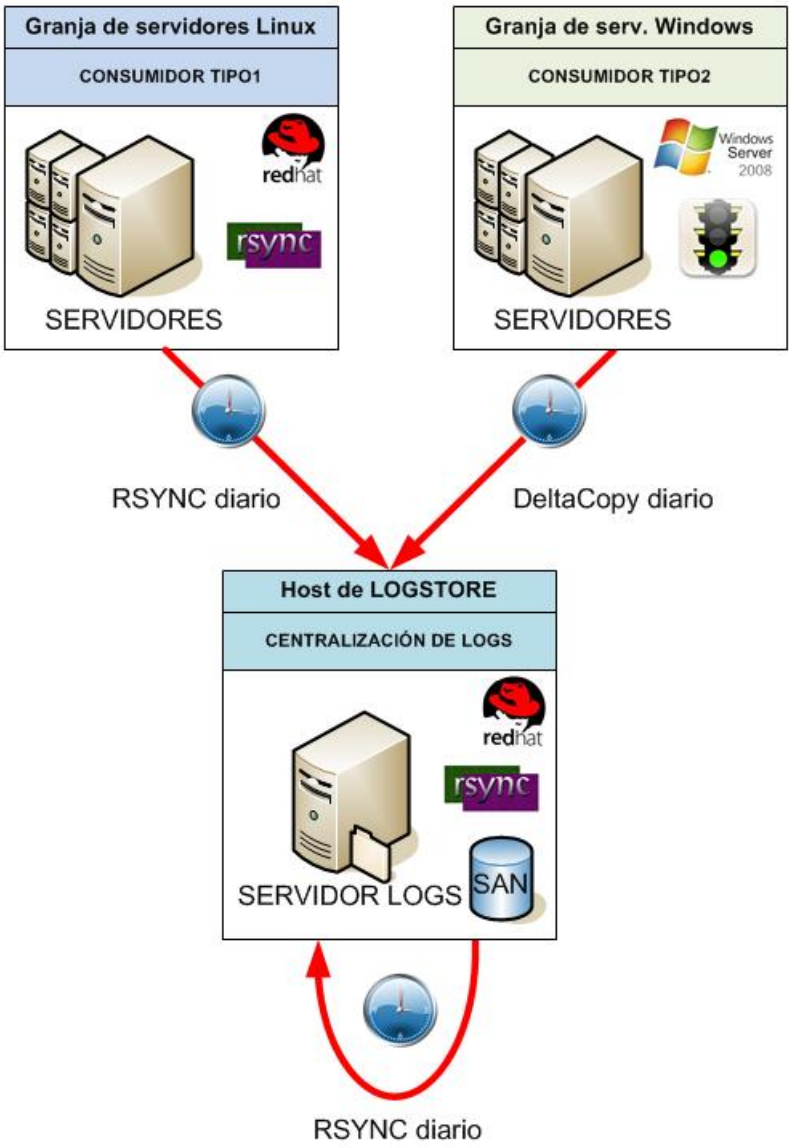


Ilustración 11. Esquema de centralización de LOGS.

5.4.2. POLÍTICA DE CENTRALIZACIÓN DE LOGS

5.4.2.1. Competencias generales del sistema de centralización

Compresión de ficheros

Como norma relativa al proceso de centralización, los ficheros serán alojados en el servidor de manera comprimida, y previo al proceso de comulación, de cara a optimizar el tiempo y ocupación del ancho de banda durante la cesión de los datos. Por lo tanto, La compresión queda delegada en cada uno de los sistemas remotos que utilicen el servicio de centralización. Se exceptúa, el caso de la centralización de los ficheros obtenidos por re-envíos syslog -caso de los servidores Windows y similares- que serán comprimidos de forma automatizada por el propio servidor de centralización.

No obstante, el servidor de centralización de forma periódica (diariamente) hará un chequeo de los ficheros alojados para verificar que todos están correctamente comprimidos.

Transmisión de ficheros

La transmisión de un fichero será la acción, que hace que un fichero de logs (comprimido), localizado en un sistema que genere eventos, sea copiado de forma fiable y sin alteraciones en el sistema de centralización. Esta práctica quedará delega en los sistemas remotos, siendo el servidor de centralización un receptor pasivo de la acción.

Frecuencia

Se establece que la frecuencia de reenvío de ficheros de log será diaria.

Rotación

La de rotación de ficheros del repositorio centralizado hacia un sistema de almacenamiento histórico o su descarte definitivo vendrá especificada por las políticas de seguridad sobre la salvaguarda de información.

5.4.2.2. Organización del repositorio centralizado

Directorio base

De cara a mantener una estructura ordenada de todos los ficheros a centralizar, se dispondrá de un directorio base sobre el que montar cada uno de los volúmenes SAN destinados al almacenaje de fichero de log. Este se define como: /logstore

Sub-directorios de volúmenes

Jerárquicamente dependiendo del directorio base, se definen los sub-directorios sobre los que se montaran los volúmenes de datos. Para una identificación óptima de estos volúmenes se seguirá la siguiente nomenclatura: “logvol-<descripción>”.

Inicialmente, se especifican dos volúmenes que identifican los dos entornos genéricos de pre-explotación y explotación:

- logvol-pre (volumen contenedor de LOGS de pre-explotación)
- logvol-exp (volumen contenedor de LOGS de explotación)

Sub-directorios organizativos basados en fechas

Sobre cada volumen, se desplegará una estructura de directorios basada en fechas del tipo \AAAA\MM\DD, y sobre cada uno de estas estructuras de sub-directorios se recolectaran todos los ficheros obtenidos de cualquiera de los sistemas que centralicen en este servidor, aquellos ficheros susceptibles de ser centralizados.

```
|-- logvol-exp
|   `-- 2013
|       |-- 01
|       |   |-- 29
|       |   |-- 30
|       |   `-- 31
|       `-- 02
|           |-- 01
|           |-- 02
|           |-- 03
|           |-- 04
|-- logvol-pre
|   `-- 2013
|       |-- 01
|       |   |-- 29
|       |   |-- 30
|       |   `-- 31
|       `-- 02
|           |-- 01
|           |-- 02
|           |-- 03
...
```

Ilustración 12. Sub-directorios organizativos basados en fechas.

Formato de ficheros

Los ficheros de datos auditados correspondientes a la fecha indicada, serán normalizados para su inequívoca identificación de acuerdo a la siguiente nomenclatura: “server”-“entorno”-“servicio”-“AAAAMMDD”.

```
|-- logvol-exp
|   `-- 2013
|       |-- 01
|       |   |-- 28
|       |   |   |-- iruela1-exp-authpriv-20130128.log.gz
|       |   |   |-- iruela1-exp-cron-20130128.log.gz
|       |   |   |-- iruela1-exp-mail-20130128.log.gz
|       |   |   `-- iruela1-exp-messages-20130128.log.gz
...
```

Ilustración 13. Formato de los ficheros

6. DEFINICIÓN DE PRODUCTOS

6.1. SOFTWARE BASE: SISTEMAS OPERATIVOS GNU/LINUX

La distribución y el versionado del sistema operativo vienen determinada por la política corporativa de homogenización tecnológica. Ésta, actualmente, indica que se establece "Red Hat Enterprise Linux versión 5 como sistema operativo corporativo para servidores con tecnologías Linux". Destacar que este no es el último versionado de la distribución, que acaba de liberar la 6.4. Sin embargo, la versión 5 tiene como fecha de final de producción marzo de 2017 y como final de ciclo de vida primer trimestre del 2020.

Antes de relacionar el conjunto de características técnicas de la distribución destacaremos aquella que, sin duda, es de mayor relevancia de cara al proyecto. Ésta, tiene que ver con liberación de la versión de mantenimiento Red Hat Enterprise Linux 5.9 el pasado 8 de enero del 2013. En las notas de la versión, se recoge explícitamente, que se incluye el paquete de la nueva versión de rsyslog. De esta forma, se garantiza la integración de natural de rsyslog dentro de la distribución, que ya aplicaba la misma política con otra de las herramientas esenciales del proyecto como es rsync. Sin duda, esto garantiza un sustrato base importante para la extensa plataforma de consumidores tipo 1. Mencionar además, que en la versión 6 se remplaza definitivamente el paquete estándar de syslog por el de rsyslog garantizando la progresión evolutiva.

6.1.1. RESUMEN BÁSICO DE CARACTERÍSTICAS DE LA DISTRIBUCIÓN

Red Hat® Enterprise Linux® 5, inicialmente lanzado en marzo de 2007, contiene más de 1.200 componentes que cubren un amplio rango de funcionalidades, como son:

- Servidor
- Escritorio
- Seguridad
- Redes e interoperabilidad
- Entorno de desarrollo
- Almacenamiento
- Administración
- Virtualización

La distribución está basada en el kernel de Linux 2.6.18, optimizado para procesadores multinúcleo. Presenta, compatibilidad ininterrumpida con una amplia plataforma de hardware; tecnologías avanzadas de rendimiento de E/S y de virtualización, como SRIOV; amplio soporte con SMP para sistemas tanto físicos como virtuales; descarga de fragmentación de IPv4/IPv6 y gestión de buffers; planificadores de E/S por cola conmutables dinámicamente y posibilidad de unir buffers del kernel para mejorar las operaciones de E/S. Además, posee herramientas de desarrollo y rendimiento, incluida SystemTap.

La distribución para servidores se presenta en dos paquetes distintos:

- Red Hat Enterprise Linux Advanced Platform
- Red Hat Enterprise Linux

A continuación, se adjunta cuadro comparativo de versiones:

	Versión 5		Versión 6
	Advanced	Servidor	
Soporte para arquitecturas de categoría Server			
x86, AMD64, Intel64	Sí	Sí	Sí
Itanium2	Sí	Sí	No
IBM POWER	Sí	Sí	Sí
Mainframe IBM	No	Sí	Sí
Límites de soporte para la categoría Server, según suscripción al producto Red Hat Enterprise Linux			
Número máximo de sockets/CPU físicos	Ilimitado	2	Varía según la suscripción
Memoria máxima	Ilimitado	Ilimitado	Ilimitado
Número máximo de guests e instancias virtualizados	Ilimitado	4	1/4/ilimitado (varía según la suscripción)
Virtualización de almacenamiento (con Red Hat GFS y Cluster Suite)	Sí	No	Opcional

Tabla 5. Cuadro comparativo de versiones de Red Hat 5 y 6.

Una relación completa de funcionalidades se puede encontrar en los documentos:

- http://www.redhat.com/f/pdf/rhev/DOC049R4-RHEV-Overall-Datasheet.pdf
- http://i.dell.com/sites/doccontent/business/solutions/operating-systems/en/Documents/red-hat-enterprise-linux-55-datasheet.pdf
- http://www.redhat.com/f/pdf/rhel/RHEL6_datasheet.pdf

6.1.2. ALTERNATIVAS

La alternativa natural si se buscara una distribución Linux sin modelo de subscripción, sería Centos. Ésta, es casi un clon de las distribuciones de Red Hat Enterprise Server incluso en la liberación de versiones. No obstante, el conjunto de paquetes utilizados en el proyecto son tan co-nativos Linux que no debiera existir gran dificultad en su adaptación a cualquier distribución.

6.2. CENTRALIZACIÓN DE LOGS

6.2.1. RSYNC

La herramienta Rsync ya ha sido introducida en el punto "5.1 TRANSFERENCIAS CON RSYNC". En él, destacábamos principalmente las bondades del algoritmo de transferencia así como que la herramienta es co-natural el mundo Linux. Podríamos aventurarnos a decir que no existe una distribución que no la incorpore y son pocos los procedimientos de backup o transferencia de archivos, en el mundo Linux, que no la utilicen.

6.2.1.1. Características.

Las principales características de Rsync son las siguientes:

- Transferencia rápida de archivos incrementales
- Actualización de árboles de directorios y sistemas de archivos completos
- Conservación de los enlaces simbólicos, enlaces duros, propiedades de los archivos, permisos, dispositivos y "timestamp"
- No requiera privilegios especiales para su instalación
- Internal pipelining -canalización interna- para reducir la latencia
- Utilización de rsh, ssh o direct socket como transporte
- Soporte de sincronización anónimo

6.2.1.2. Alternativas

Quizás la alternativa más clara a rsync podrían ser Rdiff-backup. Éste, hace copias de seguridad de un directorio a otro. El directorio de destino tiene una copia del directorio de origen, pero además almacena en un subdirectorio especial las diferencias entre distintas transferencias para recuperar copias anteriores. La idea es combinar las características de un espejo y una copia de seguridad incremental. Rdiff-backup también conserva subdirectorios, enlaces duros, archivos dev, permisos, uid / gid, tiempos de modificación, atributos extendidos, ACLs, etc. También, puede operar con canalización interna, como rsync.

También podemos encontrar herramientas como Zsync especializada en la sincronización de grandes ficheros pero dado el ciclo de rotación de log sugerido no parece la mejor alternativa.

6.2.2. DELTACOPY

DeltaCopy es un contenedor –OpenSource- para Windows de Rsync utilizando las bibliotecas de Cygwin

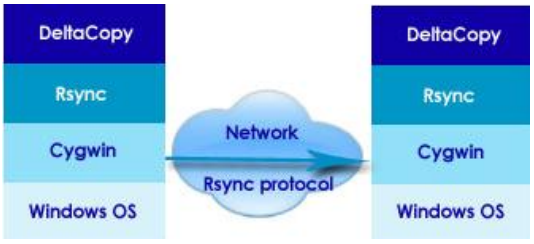


Ilustración 14. Esquema de capas del contenedor DeltaCopy.

DeltaCopy está sólo disponible para Windows y está estrechamente integrado con los servicios de las plataformas de Microsoft (XP, 2000, 2003, Vista, Windows 7 y 2008).

6.2.2.1. Características.

Las principales características de DeltaCopy son las siguientes:

- Copia de seguridad incremental.
- Programador de tareas.
- Notificación por correo electrónico.
- One-Click Restore (restauración fácil de archivo).
- GUI amigable para entorno Windows.

6.2.2.2. Alternativas

Una posible alternativa a DeltaCopy sería cwRsync. CwRsync es otro contenedor de Rsync basado en las librerías Cygwin pero aunque permite especificar las fuentes y el destino (local, remoto ssh y modos de demonio), filtros y un subconjunto de las opciones ligadas al comando rsync adolece de un programador de tareas elemento esencial para el proyecto.

6.3. RECOLECCIÓN DE EVENTOS

6.3.1. RSYSLOG

Rsyslog es una implementación del protocolo de syslog que aparece en 2004, con el ánimo de dotar al demonio de syslog de características avanzadas y mayor fiabilidad sin perder la compatibilidad con este. Con el tiempo se ha convertido en un estándar de facto que incorporan la mayoría de distribuciones Linux como Fedora, openSUSE, Debian GNU/Linux, Ubuntu, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, FreeBSD, OpenBSD, Gentoo, Arch Linux. Además, participa junto a RedHat y Balabit (mantenedores de Syslog-NG) en el proyecto project lumberjack / CEE (proyecto de código abierto para actualizar y mejorar la arquitectura del registro de eventos con la creación y estandarización del contenido de los registros de eventos).

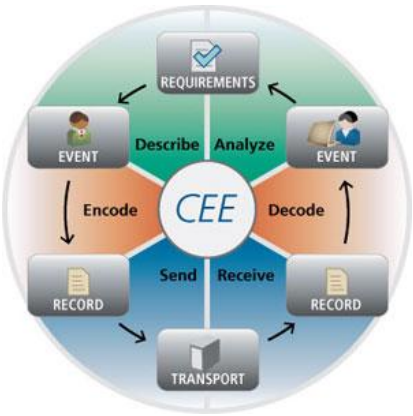


Ilustración 15. Ciclo de vida de unificación de auditorías y eventos propuesto por CEE.

Un resumen de sus principales características es:

- Modularidad en la configuración, que además es casi compatible con la original de sysklogd
- Nuevo protocolo RELP, que mejora la fiabilidad sobre TCP evitando duplicados en caso de error
- Escritura en disco local o remoto, volcado a BBDD nativo o envío de e-mail… con gestión automática de colas (en memoria o disco) en caso de ralentización o error de comunicación y planificación horaria.
- Mejoras como marcas de tiempo con mayor precisión, soporte nativo de cifrado, repetidores intermedios…

6.3.1.1. Características

Las principales características de Rsyslog son las siguientes:

- Soporte nativo de escritura en bases de datos MySQL
- Soporte nativo de escritura en bases de datos Postgres
- Soporte de Firebird / Interbase, OpenTDS (MS SQL, Sybase), SQLLite, Ingres, Oracle y mSQL a través libdbi (capa de abstracción de base de datos)
- Soporte nativo para el envío de mensajes de correo
- Soprte syslog sobre TCP
- Soporte para enviar y recibir mensajes de syslog comprimido
- Permite la gestión de cola de mensajes que no se pueden procesar con suficiente rapidez (esencial en plataformas extensas de syslog)
- Permite el procesamiento selectivo de mensajes preferentes. Envíos priorizados según ventana temporal y encolamiento del resto.
- Permite examinar los archivos de texto y convertir su contenido en mensajes de syslog
- Permite configuraciones activo – pasivo. Si el principal falla, el control se cambia según una lista priorizada de las standby
- Soporta RFC 3195 y RFC5424
- Capacidad para generar nombres de archivos y directorios (objetivos de registro) de forma dinámica.
- Control de formato de registro de salida, incluyendo la capacidad de presentar y canal prioritario como datos de registro visibles
- Control de formato de hora (ISO 8601/RFC 3339 de segunda resolución zona UTC)
- Capacidad para formatear el contenido del mensaje
- Soporte para archivos de registro de más de 2GB
- Soporte para la limitación del tamaño del archivo y la ejecución automática de comandos de rotación
- Soporte para ejecutar múltiples instancias de rsyslogd en una sola máquina
- Soporte para protección TLS (tanto de forma nativa como a través stunnel)
- Capacidad de filtrar en cualquier parte del mensaje, no sólo las instalaciones y severidad
- Capacidad de utilizar expresiones regulares en los filtros

- Soporte para descarte de mensajes basado en filtros
- Capacidad de ejecutar scripts de shell en los mensajes recibidos
- Permite el control del nombre del host de salida (host local o host del origen del mensaje)
- Permite preservar el nombre original del host en entornos con NAT y cadenas de retransmisión
- Permite limitar los remitentes permitidos
- Permite
- Pemite multi-threaded (ideal para alto volumen de registro en máquinas multi-núcleo)
- Plug-in para emulación completa del paquete sysklogd
- Soporte para IPv6
- Permite controlar la reducción de mensajes repetido
- Soporta sub-archivos de configuración
- Soporta múltiples acciones por filtro
- Diseño modular para las entradas y salidas - fácilmente extensible a través de plugins personalizados-
- Interfaz API
- Permite enviar mensajes de captura SNMP
- Permite filtrar mensajes basándose en la secuencia de llegada
- Exporta a formato CSV- RFC 4180.
- Soporta expresiones complejas (lógicas, de cadena y aritmética) en el filtrado de mensajes

6.3.1.2. Alternativas

Sysklogd. Bajo esta denominación realmente se esconden dos demonios separados: syslogd para mensajes de sistema y klogd para los mensajes del kernel. La última versión publicada (1.5) data de 2007 con poca actividad desde entonces

syslog-ng. Es una alternativa al sysklogd aparecida a finales de la década de 1990. Sus innovaciones pasan por añadir filtros más potentes (por ejemplo, filtrando por contenido) y la posibilidad de utilizar como transporte TCP, lo que lo hace teóricamente más fiable. Actualmente, está soportado por una empresa quién ha realizado un fork no libre en el que se realizan las principales innovaciones quedando la versión libre algo relegada a segundo plano.

6.3.2. NTSYSLOG

Seguramente, el encontrar un re-enviador de syslog en el mundo Windows -con licenciamiento libre- es uno de los puntos más oscuros del proyecto. Existen múltiples clientes pero todos ellos están en estado muy incipiente o han parado su evolución. Nosotros, nos decantamos NTSYSLOG que ha demostrado su solvencia aunque creemos que proyectos como eventlog-to-syslog albergado por google recogerán la alternativa en breve.

NTsyslog es una aplicación con licenciamiento GNU que se instala como servicio en los sistemas Windows y que re-envía los eventos a un servidor de syslog remoto. Dispone de un GUI que permite configurar el tipo de mensajes a monitorizar.

6.3.2.1. Características

- Compatible RFC3164 –especificación origen de RFC5424-
- Se instala como servicio
- GUI de configuración
- Permite configuración del mensaje
- Soporta eventos definidos por usuario

6.3.2.2. Alternativas

Existen múltiples alternativas (syslog-win32, winSyslog, snare, winlogd) pero sin duda eventlog-to-syslog albergado por google parece la más plausible, dado el gran número de desarrollo colaborando en el proyecto. En cuanto solvente algunos fix relacionados con el transporte TCP, el re-envío de errores y añada una gestión adecuada de mensajes será un candidato idóneo de uso.

6.4. ANÁLISIS DE EVENTOS

6.4.1. LOGANALYZER

LogAnalyzer es un interfaz web para el análisis de mensajes syslog y eventos de Windows mantenido por Adiscon (también proporciona el mantenimiento de rsyslog). Utiliza como repositorio nativo MySQL.

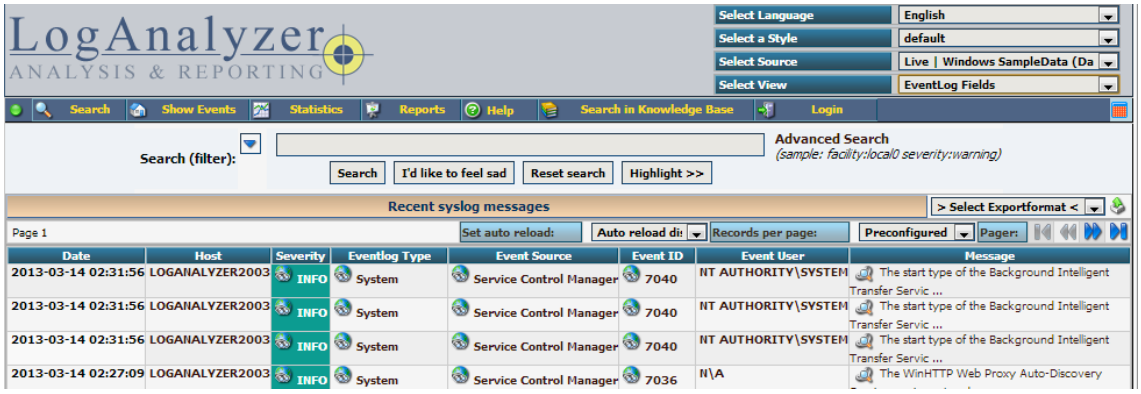


Ilustración 16. Interfaz WEB LogAnalyzer.

Permite la categorización y selección de las diferentes fuentes de origen, así como vistas por tipología de eventos

Ilustración 17. LogAnalyzer, selección de fuente y vista.

Permite la búsqueda y el filtrado avanzado

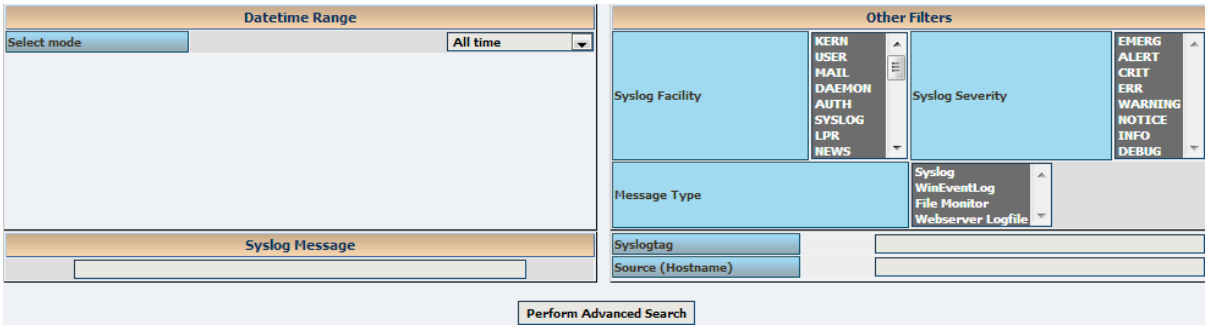


Ilustración 18. LogAnalyzer, búsqueda y filtrado.

Integra nativamente herramientas de estadísticas de actividad de eventos

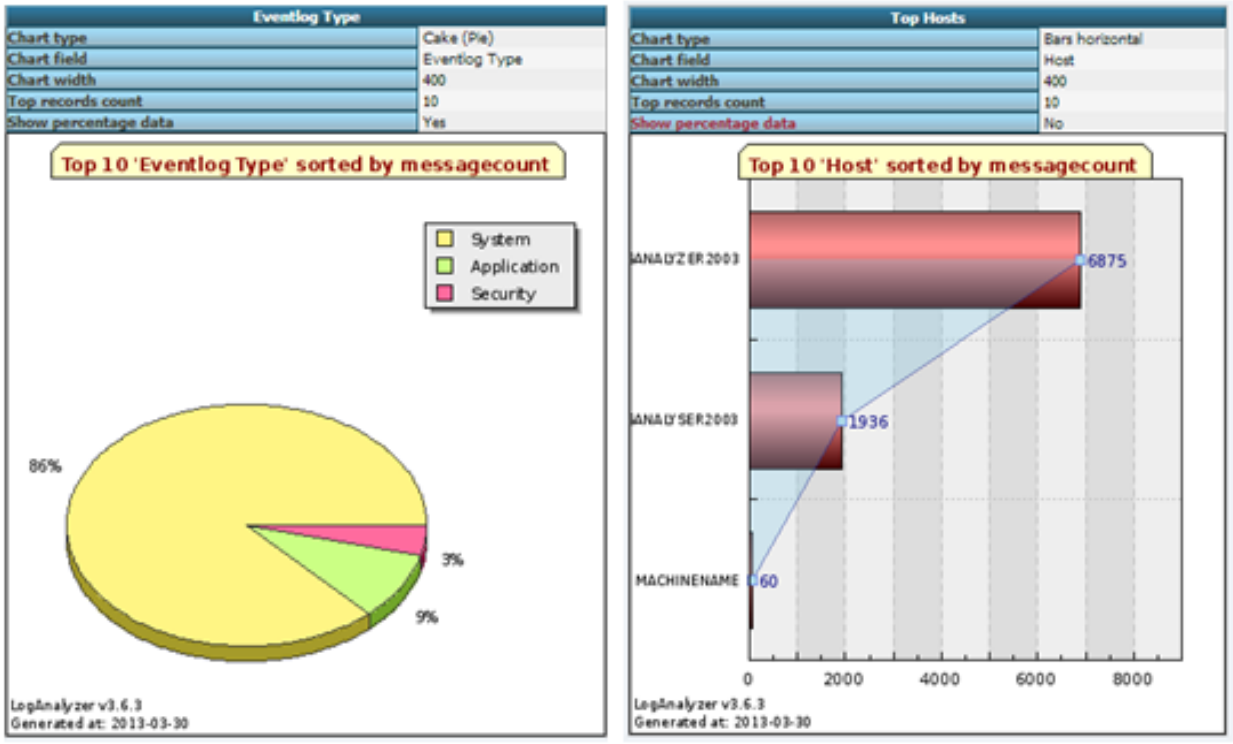


Ilustración 19. LogAnalyzer, estadísticas.

Integra generación de reports y su exportación en varios formatos

Report Summary

Event Summary	
Total Events	2293
INFO	1173
NOTICE	1012
WARNING	79
ERR	29

Computer Summary
XPTEST(1029), W2003R2(980), W2KTESTING(247), MACHINENAME(37),

Events Consolidated per Host

XPTEST

No.	First Event	Last Event	Process	Type	Event ID	Count
1	2008-09-16 15:14:42	2008-09-16 15:17:58	VMTools	INFO	105	29
	Description		The service was started.			
2	2008-09-16 15:14:48	2008-09-16 15:14:49	Windows Update Agent	INFO	18	23
	Description		Installation Ready: The following updates are downloaded and ready for installation. This computer is currently scheduled to install these updates on Mittwoch, 16. August 2006 at 03:00: - Security Update for Windows XP (KB890859) - Security Update for Windows XP (KB914389) - Security Update for Windows XP (KB920683) - Security Update for Windows XP (KB908519) - Update for Windows XP (KB894391) - Cumulative Security Update for Outlook Express for Windows XP (KB911567) - Security Update for Windows XP (KB896428) - Security Update for Windows XP (KB913580) - Security Update for Windows XP (KB905749) - Security Update for Windows XP (KB908531) - Security Update for Windows XP (KB904706) - Update for Windows XP (KB916595) - Security Update for Windows XP (KB912919) - Security Update for Windows XP (KB900725) - Security Update for Windows XP (KB888302) - Security Update for Windows XP (KB917422) - Security Update for Windows XP (KB901214) - Security Update for Windows XP (KB917953) - Security Update for Windows XP (KB905414) - Security Update for Windows XP (KB917344) - Security Update for Windows XP (KB914388) - Security Update for Windows XP (KB899589) - Security Update			

Ilustración 20. LogAnalyzer, generación de reports.

6.4.1.1. Características

Las principales características de LogAnalyzer son las siguientes:

- Selección de origen de análisis
- Selección de vista
- Categorización de eventos
- Búsqueda Avanzada temporalizada por tipología de log, severidad, servicio y/o fuente
- Búsqueda genérica de mensajes

- Integración nativa protocolo syslog
- Exportación en formato CSV y XML
- Estadísticas de eventos producidos, fuentes de origen, tipología y marco temporal
- Generación de informes eventos producidos, fuentes de origen, tipología y marco temporal
- Integración con MySQL
- Integración Apache Web Server

6.4.1.2. Alternativas

Algunas de las alternativas pudieran ser LogStash pero su desarrollo es bastante incipiente (no tiene gestión de log, ni de búsquedas avanzadas, etc) o el proyecto enterprise-log-search-and-archive albergado por google que también parece requerir una mayor evolución.

6.4.2. LOGREPORTERS: POSTFIX Y AMAVISD

Postfix-logwatch es un analizador de registros de log Postfix MTA que genera resúmenes, datos y estadísticas sobre el funcionamiento de Postfix. Esta utilidad se puede utilizar como un programa independiente o como un módulo Logwatch filter. Postfix-logwatch es capaz de producir una amplia gama de informes con datos agrupados y ordenados (informes breves sumarios que proporcionan una visión general rápida de general, como detallados indicando desglose cuantitativo de notificaciones)

```
****** Summary ********************************************

      81   *Warning: Connection rate limit reached (anvil)
     146   Warned

  68.310M  Bytes accepted                        71,628,177
  97.645M  Bytes delivered                      102,388,245
========   ================================================

    3464   Accepted                                  41.44%
    4895   Rejected                                  58.56%
--------   ------------------------------------------------
    8359   Total                                    100.00%
========   ================================================
```

Ilustración 21. Postfix-logwatch, información general.

```
****** Detailed *******************************************

    261   MX errors ------------------------------------
    261      Unable to look up MX host
    222         Host not found
     73            foolishspammer.local
     60            completely.bogus.domain.example
     11            friend.example.com
     39         No address associated with hostname
     23            dummymx.sample.net
     16            pushn.spam.sample.com
```

Ilustración 22. Postfix-logwatch, información detallada.

Amavis-logwatch, al igual que Postfix-logwatch, es un analizador de registros pero esta vez de Amavisd-new (Amavisd-new es un interfaz de código abierto para el servidor de correo que filtra los mensajes en busca de spam y virus). También, genera resúmenes generales y detallados que analizan semánticamente el servicio.

```
****** Summary ********************************************

       9   Miscellaneous warnings

   20313   Total messages scanned ----------------  100.00%
1008.534M  Total bytes scanned               1,057,524,252
========   ================================================

    1190   Blocked -------------------------------    5.86%
      18     Malware blocked                          0.09%
       4     Banned name blocked                      0.02%
     416     Spam blocked                             2.05%
     752     Spam discarded (no quarantine)           3.70%

   19123   Passed --------------------------------   94.14%
      47     Bad header passed                        0.23%
   19076     Clean passed                            93.91%
========   ================================================

      18   Malware -------------------------------    0.09%
      18     Malware blocked                          0.09%

       4   Banned --------------------------------    0.02%
       4     Banned file blocked                      0.02%

    1168   Spam ----------------------------------    5.75%
     416     Spam blocked                             2.05%
     752     Spam discarded (no quarantine)           3.70%

   19123   Ham -----------------------------------   94.14%
      47     Bad header passed                        0.23%
   19076     Clean passed                            93.91%
========   ================================================

    1982   SpamAssassin bypassed
      32   Released from quarantine
       2   DSN notification (debug supplemental)
       2   Bounce unverifiable
    2369   Whitelisted
       2   Blacklisted
      12   MIME error
      58   Bad header (debug supplemental)
      40   Extra code modules loaded at runtime
```

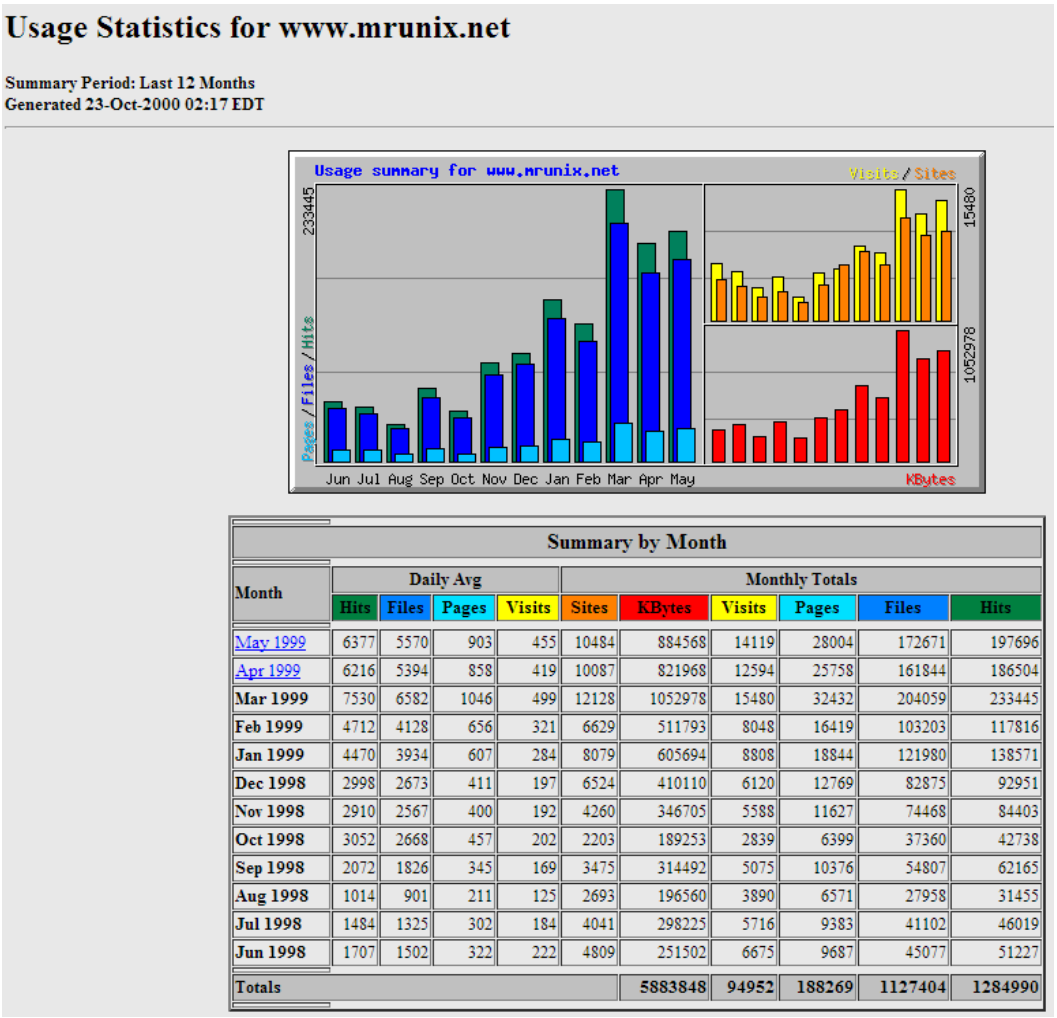
Ilustración 23. Amavis-logwatch, informe general.

```
****** Detailed *******************************************

   19346   Spam blocked ----------------------------------
     756      from@example.com
      12         10.0.0.2
      12            <>
      12         192.168.2.2
      12            <>
       5         192.168.2.1
     ...
```

Ilustración 24. Amavis-logwatch, informe detallado

6.4.3. WEBALIZER

Webalizer es un analizador de log de servidores web distribuido bajo licencia GNU. Este incluye estadísticas de accesos, visitas, países de los visitantes, y la cantidad de datos descargados. Estas estadísticas se pueden ver gráficamente y presentado por diferentes marcos de tiempo, como por día, hora o meses. Está escrito en C y es extremadamente rápido (70.000 registros por segundo). Genera reports que pueden ser configurados desde una línea de comandos.



Usage Statistics for www.mrunix.net

Summary Period: Last 12 Months
Generated 23-Oct-2000 02:17 EDT

Summary by Month

Month	Daily Avg				Monthly Totals					
	Hits	Files	Pages	Visits	Sites	KBytes	Visits	Pages	Files	Hits
May 1999	6377	5570	903	455	10484	884568	14119	28004	172671	197696
Apr 1999	6216	5394	858	419	10087	821968	12594	25758	161844	186504
Mar 1999	7530	6582	1046	499	12128	1052978	15480	32432	204059	233445
Feb 1999	4712	4128	656	321	6629	511793	8048	16419	103203	117816
Jan 1999	4470	3934	607	284	8079	605694	8808	18844	121980	138571
Dec 1998	2998	2673	411	197	6524	410110	6120	12769	82875	92951
Nov 1998	2910	2567	400	192	4260	346705	5588	11627	74468	84403
Oct 1998	3052	2668	457	202	2203	189253	2839	6399	37360	42738
Sep 1998	2072	1826	345	169	3475	314492	5075	10376	54807	62165
Aug 1998	1014	901	211	125	2693	196560	3890	6571	27958	31455
Jul 1998	1484	1325	302	184	4041	298225	5716	9383	41102	46019
Jun 1998	1707	1502	322	222	4809	251502	6675	9687	45077	51227
Totals						5883848	94952	188269	1127404	1284990

Ilustración 25. Estadistcas generadas con WebAlizer

6.4.3.1. Características

Las principales características de WebAlizer son las siguientes

- Gran rapidez de análisis
- Interpretación de CLF (Common Log Format)
- Interpretación de algunas variedades de NCSA logfile
- Interpretación de FTP format logs (wu-ftpd/proftpd)
- Interpretación de Squid proxy server

- Interpretación de W3C Extended log format
- Generación de reports desde línea de comandos
- Soporte para múltiples lenguajes: albanés, árabe, catalán, chino (tradicional y simplificado), croata, checo, danés, holandés, Inglés, estonio, finés, francés, gallego, alemán, griego, húngaro, islandés, indonesio, italiano, japonés, coreano, letón, lituano, malayo, noruego, polaco, portugués (Portugal y Brasil), rumano, ruso, serbio, eslovaco, esloveno, español, sueco, tailandés, turco y ucraniano
- Análisis de archivos de registro de tamaño ilimitado
- Soporte para IPv4 e IPv6. Incluye una función de búsqueda de DNS distribuidos y servicios nativos de geo-localización.

6.4.3.2. Alternativas

Algunas alternativas son:

- AWStats: es una herramienta gratuita de análisis web que funciona como un script CGI en el servidor Web o desde la línea de comandos. Puede ejecutarlo y evalúa sus registros web con muchos informes diferentes. También se puede utilizar para analizar los registros de FTP y correo electrónico, así como archivos de registro Web. Algunas funciones útiles incluyen la posibilidad de exportar los informes a XML, texto y PDF.
- Google Analytics: es una de las mejores herramientas gratuitas de análisis de registros Web disponibles. Hay algunos informes que no están incluidos, pero los gráficos e informes están bien definidos. Sin embargo, hay que permitir el acceso directo a las métricas de los sitios.

Otras alternativas de menor calado podrían ser W3Perl, Power Phlogger, BBClone, etc.

6.5. LENGUAJES Y UTILIDADES

Se ha determinado que el lenguaje a emplear para el desarrollo de la consola unificada sea PHP por su potencia, adaptabilidad web y su integración con algunas herramientas como LogAnalyzer. También, se utilizaran funcionalidades AJAX y algunas utilidades (Google Chart Tools y PHP File Tree, JQuery, TinyBox2) para mejorar el diseño, la funcionalidad y la amigabilidad de la consola.

6.5.1. PHP FILE TREE

Es una función PHP que genera una lista válida, XHTML anidada del directorio especificado. El guión incluye una extensión de JavaScript que hace que toda la lista expandir y contraer de forma dinámica.

Las características principales son:

- Genera XHTML válido, semántico
- Totalmente personalizable con CSS
- Capacidad de personalizar los iconos de archivo de estilo basándose en la extensión
- Fácil de implementación
- Extensión de JavaScript para efectos dinámicos

6.5.1.1. JQuery

Query es una biblioteca de JavaScript, creada inicialmente por John Resig, que permite simplificar la manera de interactuar con los documentos HTML, manipular el árbol DOM, manejar eventos, desarrollar animaciones y agregar interacción con la técnica AJAX a páginas web

Las características principales son:

- Selección de elementos DOM.
- Interactividad y modificaciones del árbol DOM, incluyendo soporte para CSS 1-3 y un plugin básico de XPath.
- Eventos.
- Manipulación de la hoja de estilos CSS.
- Efectos y animaciones.
- Animaciones personalizadas.
- AJAX.
- Soporta extensiones.
- Utilidades varias como obtener información del navegador, operar con objetos y vectores, funciones para rutinas comunes, etc.

6.5.1.2. Google Chart Tools

Google Chart Tools proporcionan una manera para visualizar los datos en su sitio web. Desde gráficos de líneas simples a complejos mapas de árbol jerárquico. Es totalmente customizable, soporta HTML5/SVG y admite múltiples protocolos de enlace a datos dinámicos.

6.5.1.3. TinyBox 2

Es una actualización de la secuencia de comandos TinyBox modal box (gestor de ventanas html) que incluye nuevas características en menos de 5 KB:

- La secuencia de comandos ahora soporta iframes y las imágenes de forma nativa.
- Puede añadir comentarios con Ajax.
- Al hacer clic en ESC es capaz de cerrar la ventana.
- Soporta funciones de devolución de llamadas.
- Soporta encadenamiento de de acontecimientos.
- Puede configurar los ID de CSS para anular el estilo predeterminado.
- La posición de CSS puede cambiar entre fijo y absoluto.
- La opacidad de la máscara puede ser usada.
- Ofrece el control total sobre la ubicación de las ventanas.
- Ofrece un botón de cierre de las ventanas se puede cambiar.

La secuencia de comandos se ejecuta ahora pasando un objeto, debido a la gran cantidad de opciones. No hay nada para inicializar, simplemente se llama a la función con cualquier clic de ratón o mediante eventos del navegador.

7. ARQUITECTURA

7.1. ESQUEMA DE LA ARQUITECTURA

El esquema simplificado de la arquitectura presenta la tradicional segmentación por capas de seguridad. En el que podríamos considerar primer segmento (de fuera hacia dentro), encontramos el firewall externo y la zona DMZ. En este primer segmento hallamos consumidores del tipo 1, 2 y 3 que proporcionan servicios al exterior y cuyo único canal de comunicación con la nueva plataforma pasa por el firewall interno. El segundo segmento, la "LAN de servidores" será la ubicación natural de los elementos de la nueva plataforma. Junto a ellos, encontramos también una gran cantidad de consumidores 1,2 y 3 que prestan servicios internos o que no deben ser expuestos directamente en una zona no confiable. Finalmente, encontramos un tercer segmento en el que residen el conjunto de dispositivos de usuarios internos dela organización.

Como cabe pensar, este es un esquema simplificado y conceptual de la arquitectura que en su implementación real contiene bastante más elementos como segmentaciones, VLANs, zonas securizadas por servicios, etc.

7.1.1. ELEMENTOS DE LA PLATAFORMA DE CENTRALIZACIÓN Y RECOLECCIÓN DE LOG Y EVENTOS

Como ya se ha ido adelantando, tres serán los elementos esenciales de la arquitectura de la nueva plataforma:

1. El servidor de LOGSTORE. Servidor para la centralización de LOGS y la recolección de eventos de consumidores que no tienen implementación RSYSLOG. Este servidor requiere acceso a la SAN para el montaje del repositorio centralizador. Este repositorio será exportado por NFS en acceso de solo lectura por este servidor a la consola unificadora de herramientas de análisis. Montado sobre RHEL 5.9 –Red Hat Enterprise Linux-, implementa servicios de RSYNC, RSYSLOG y NFS por los puertos 873/tcp, 514/tcp, 514/udp y 2049/tcp respectivamente.
2. El servidor de Base de Datos. Recolector en tiempo real de todos los eventos auditados por los demonios RSYSLOG. Este servidor requiere acceso a la SAN para garantizar el crecimiento de la BBDD. Montado sobre RHEL 5.9, implementa servicios de base de datos a través del gestor de base de datos relacional MySQL por el puerto 3006/tcp
3. El servidor de LOGCONSOLE. Servidor para la implementación de todas las herramientas de análisis y la consola unificadora de servicios. Montado sobre RHEL 5.9 implementa servicios de NFS como cliente, RSYNC como cliente, RSYSLOG mediante sockets UNIX y APACHE por los puertos 80-443/tcp.

Los tres servidores serán montados en la "LAN de Servidores" que le otorga libre acceso a la mayoría de los consumidores. La comunicación con los consumidores de la zona DMZ estará securizada por el firewall Interno.

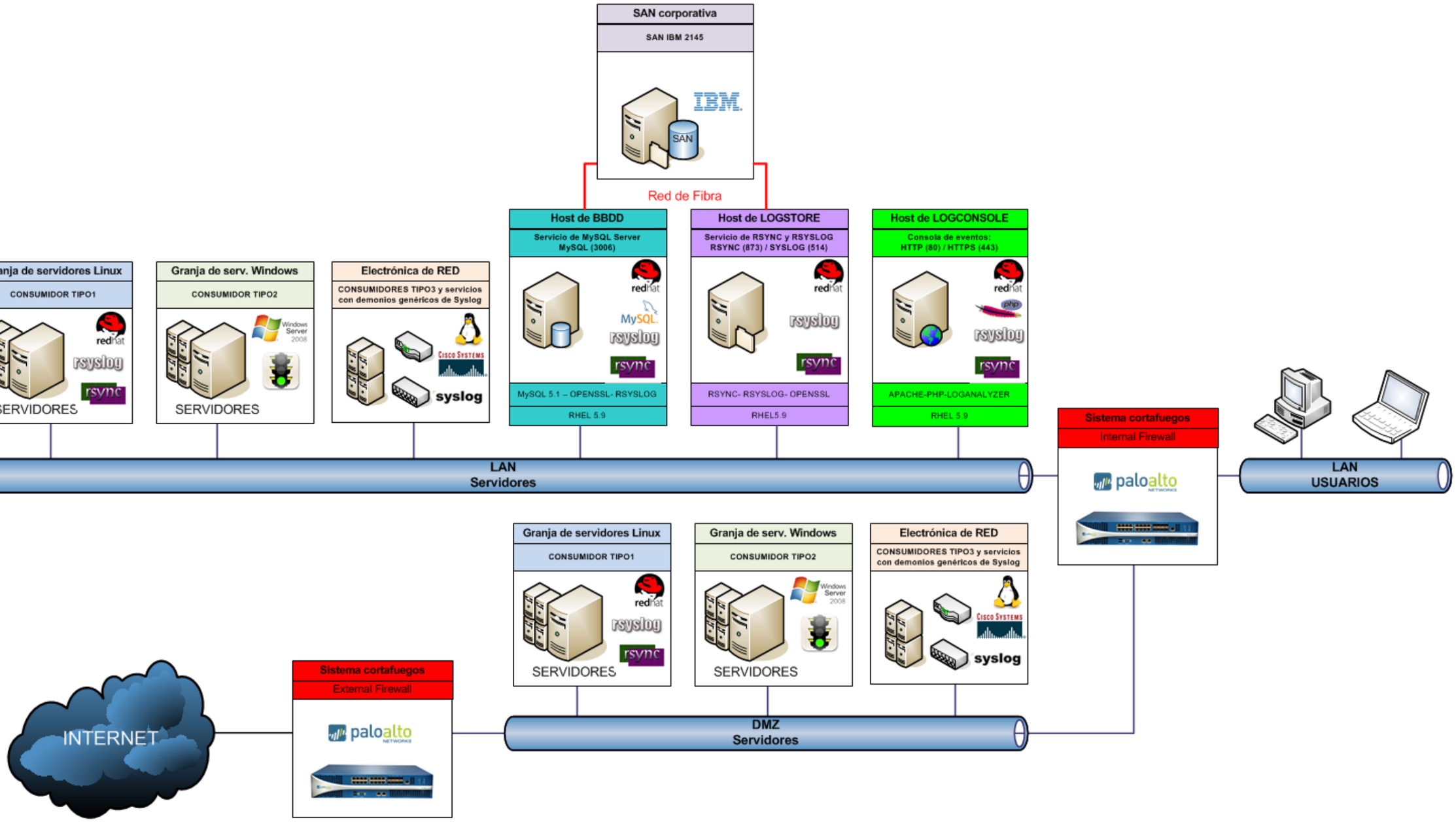


Ilustración 26. Esquema Arquitectura.

7.2. DEFINICIÓN DE SERVIDORES VIRTUALES

La implementación inicial se hará en servidores virtuales cuya especificación básica es la siguiente:

- Servidor de LOGSTORE:
  - CPU: 2 SOCKETS – 1 Core por Socket
  - Memoria definida : 4096 Mb
  - Memoria física garantizada: 3072 Mb
  - Disco: Asignación LUN directa de 500Gb
  - Tarjetas Fiber Channel redundante
  - Tarjeta red ethernet gigabit tolerante a fallos
  - Interfaz de gestión de consola remota

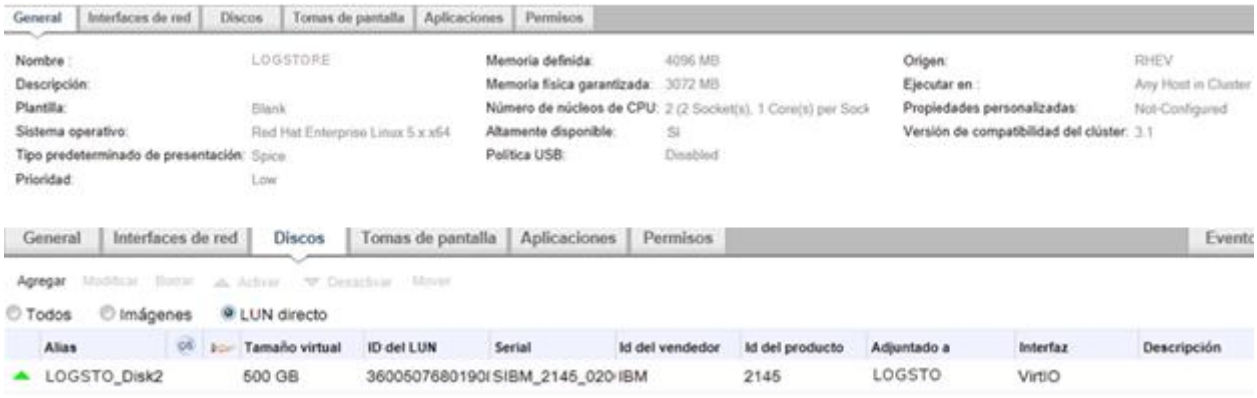


Ilustración 28. Definición de la Máquina Virtual RHEV para LOGSTORE

- Servidor de Base de Datos:
  - CPU: 4 SOCKETS – 1 Core por Socket
  - Memoria definida : 8192 Mb
  - Memoria física garantizada: 6144 Mb
  - Disco: Asignación LUN directa de 850Gb
  - Tarjetas Fiber Channel redundante
  - Tarjeta red ethernet gigabit tolerante a fallos
  - Interfaz de gestión de consola remota

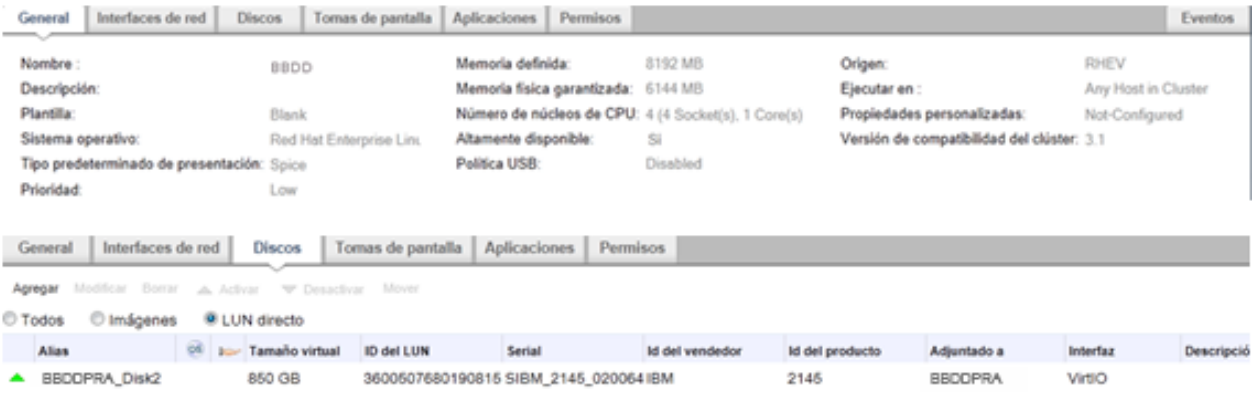


Ilustración 29. Definición de Máquina Virtual RHEV para BBDD.

- Servidor LOGCONSOLE:
  - CPU: 1 SOCKETS – 1 Core por Socket
  - Memoria definida : 3072 Mb
  - Memoria física garantizada: 2304 Mb
  - Imagen de disco de 100Gb
  - Tarjeta red ethernet gigabit tolerante a fallos
  - Interfaz de gestión de consola remota

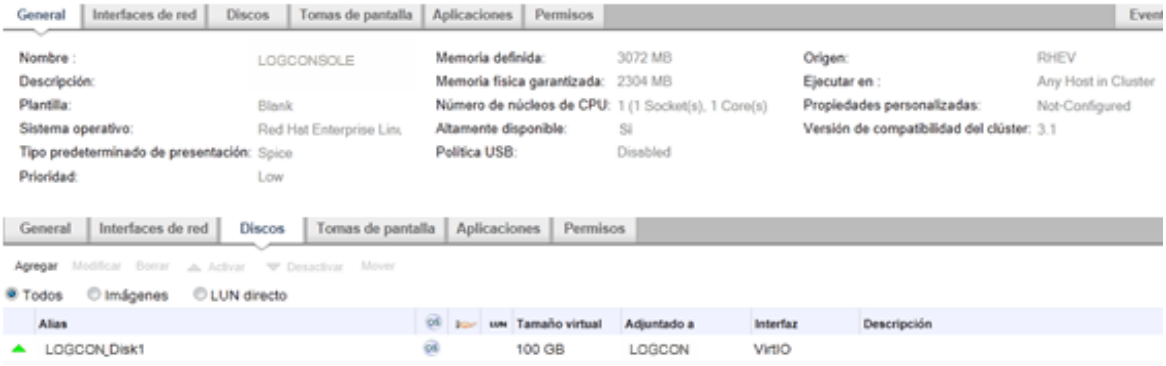


Ilustración 30. Definición de Máquina Virtual RHEV para LOGCONSOLE.

7.3. DEFINICIÓN DE BACKGROUND DE BASE DE DATOS

Para la implementación del sistema se ha optado por la disgregación de los eventos según tipología y/o servicio, de tal modo que se han creado los siguientes esquemas:

- Esquema para el almacenamiento de eventos de seguridad (RSYSLOGDB_AUTHPRIV): acceso a servidores (como por ejemplo vía SSH), escalados de permisos (su), etc.
- Esquema para el almacenamiento de eventos de error (RSYSLOGDB_ERROR): errores reportados por los handlers de eventos de sistemas y servicios.
- Esquema para el almacenamiento de eventos del servicio FTP (RSYSLOGDB_FTP): eventos producidos por el core del servicio FTP.
- Esquema para el almacenamiento de eventos del servicio PROXY (RSYSLOGDB_HTTP_ERROR): eventos producidos por el core del servicio Proxy.
- Esquema para el almacenamiento de eventos del sistema de centralización de logs (RSYSLOGDB_LOG_CENTRALIZER): eventos relativos a las transacciones de los clientes de rsync, así como para el almacenamiento de los informes generados por las herramientas de reporting.
- Esquema para el almacenamiento de eventos del servicio de correo (RSYSLOGDB_MAIL): eventos producidos por el servicio de correo, incluyendo la trazabilidad SMTP de los correos.
- Esquema para el almacenamiento de eventos de la electrónica de red (RSYSLOGDB_NETWORK): eventos de acceso VPN vía Cisco, etc.
- Esquema para el almacenamiento de eventos del parque de servidores Windows (RSYSLOGDB_WINDOWS_EVENTS): eventos registrados en los DC de AD, así como cualquier otro servidor Windows en standalone.

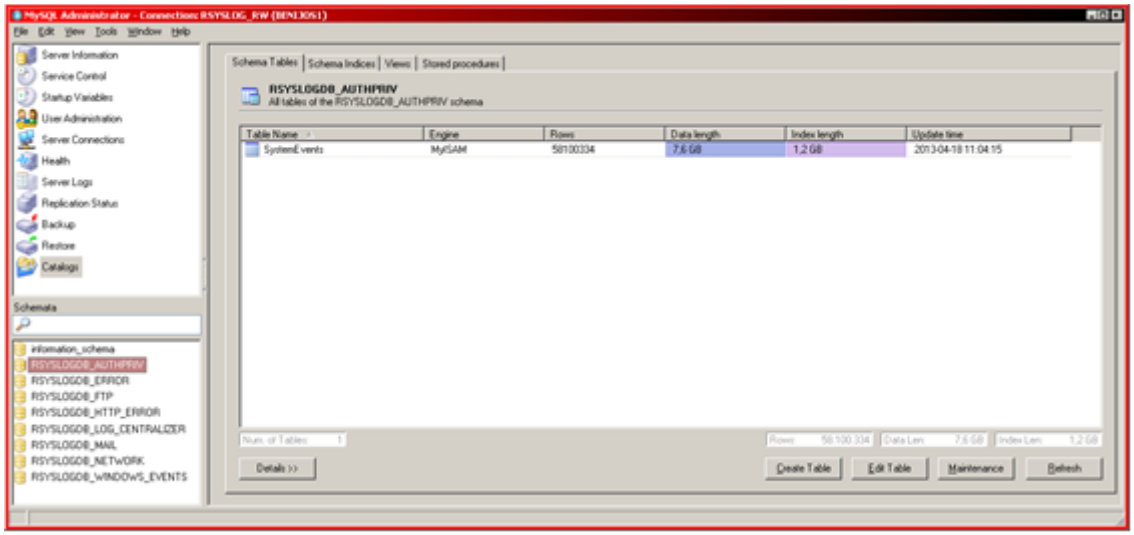


Ilustración 31. Administrador MySQL, esquemas de las BBDD.

Así mismo, y de cara a tener diferenciados los distintos entornos de la corporación, este escenario se mantiene análogo en 2 instancias distintas:

- PRE-EXPLOTACIÓN: alojará los esquemas RSYSLOG relativos al parque de máquinas del entorno de PRE-explotación (desarrollo y pruebas de concepto).
- EXPLOTACIÓN: alojará el esquema RSYSLOG relativos al parque de máquinas del entorno de producción.

7.4. DEFINICIÓN SISTEMA DE ARCHIVOS COMPARTIDOS

Para el almacenamiento tanto de logs como de las BBDD MySQL de eventos se ha utilizado una solución de SAN, confiando en la alta disponibilidad (multi-path) y alto rendimiento (iSCSI) que provee este tipo de solución de almacenamiento, disponiendo de discos SAN tanto para el servidor de centralización y almacenamiento de logs (LOGSTORE), como para el SGBD MySQL Server:

```
Servidor de MySQL Server
[root@BBDDEXP ~]# multipath -ll
mpath5 (360050768019081536000000000000022c) dm-1 IBM,2145
[size=200G][features=1 queue_if_no_path][hwhandler=0][rw]
\_ round-robin 0 [prio=100][active]
 \_ 0:0:0:1 sdb 8:16  [active][ready]
 \_ 1:0:0:1 sdh 8:112 [active][ready]
\_ round-robin 0 [prio=20][enabled]
 \_ 0:0:1:1 sde 8:64  [active][ready]
 \_ 1:0:1:1 sdk 8:160 [active][ready]
mpath3 (360050768019081536000000000000021e) dm-2 IBM,2145

[root@BBDDEXP ~]# mount
/dev/mapper/mpath5p1 on /datos3 type ext3 (rw)
```

```
Servidor de centralización
[root@LOGSTORE ~]# multipath -ll
mpath1 (360050768019081536000000000000021c) dm-2 IBM,2145
[size=2.0T][features=1 queue_if_no_path][hwhandler=0][rw]
\_ round-robin 0 [prio=100][active]
 \_ 1:0:0:1 sdf 8:80  [active][ready]
 \_ 2:0:0:1 sdh 8:112 [active][ready]
\_ round-robin 0 [prio=20][enabled]
 \_ 1:0:1:1 sdg 8:96  [active][ready]
 \_ 2:0:1:1 sdi 8:128 [active][ready]
mpath0 (360050768019081536000000000000200) dm-0 IBM,2145
[size=300G][features=1 queue_if_no_path][hwhandler=0][rw]
\_ round-robin 0 [prio=100][active]
 \_ 1:0:1:0 sdc 8:32  [active][ready]
 \_ 2:0:1:0 sde 8:64  [active][ready]
\_ round-robin 0 [prio=20][enabled]
 \_ 1:0:0:0 sdb 8:16  [active][ready]
         \_ 2:0:0:0 sdd 8:48  [active][ready]

[root@LOGSTORE ~]# mount
/dev/sda6 on /logstore/logvol-local type ext3 (rw)
/dev/mapper/mpath1p1 on /logstore/logvol-exp type ext3 (rw)
```

Para hacer disponible los volúmenes de centralización de logs (sistemas de ficheros donde se almacena los logs), también se ha utilizado un servidor NFS para ofrecerlo mediante seguridad basada en TCP Wrapper, al servidor de LOGCONSOLE, de tal modo que estos sean accesibles en modo de sólo lectura:

```
Servidor NFS en LOGSTORE
[root@LOGSTORE ~]# exportfs -v -a
exporting LOGCONSOLE:/logstore/logvol-pre
exporting LOGCONSOLE:/logstore/logvol-exp
```

```
Servidor de consola LOGCONSOLE
[root@LOGCONSOLE ~]# mount
logstore:/logstore/logvol-pre on /logstore/logvol-pre type nfs (ro,udp,posix,bg,addr=10.140.xxx.xxx)
logstore:/logstore/logvol-exp on /logstore/logvol-exp type nfs (ro,udp,posix,bg,addr=10.140.xxx.xxx)
```

8. INSTALACIÓN Y CONFIGURACIÓN

8.1. INSTALACIÓN Y CONFIGURACIÓN DE SOFTWARE BASE

La instalación del sistema operativo depende en gran medida del hardware existente y las especificaciones del servicio a montar. De forma genérica, la “Guía de Instalación de Red Hat Enterprise Linux”[3] describe exhaustivamente el proceso. A continuación, hacemos un recorrido por los aspectos más genéricos realizados en una instalación.

En primer lugar haremos el arranque del Linux, especificando la opción de arranque “linux text askmethod”, opciones que lanzaran el arranque en modo texto y con la posibilidad de

[3] https://access.redhat.com/site/documentation/es-ES/Red_Hat_Enterprise_Linux/5/html-single/Installation_Guide/index.html

seleccionar el método de instalación (en el caso de tratarse de un servidor con HBA realizaríamos un arranque con “linux text noprobe askmethod” para facilitar la detección de los discos)

Ilustración 32. Instalación de Red Hat Enterprise Linux 5.x. (1).

Dejaremos el idioma por defecto –ingles- (aunque en la fase final de la instalación añadiremos el español como lenguaje adicional), para facilitar la integración de dispositivos nuevos o propietarios y especificaremos el teclado en “Español”

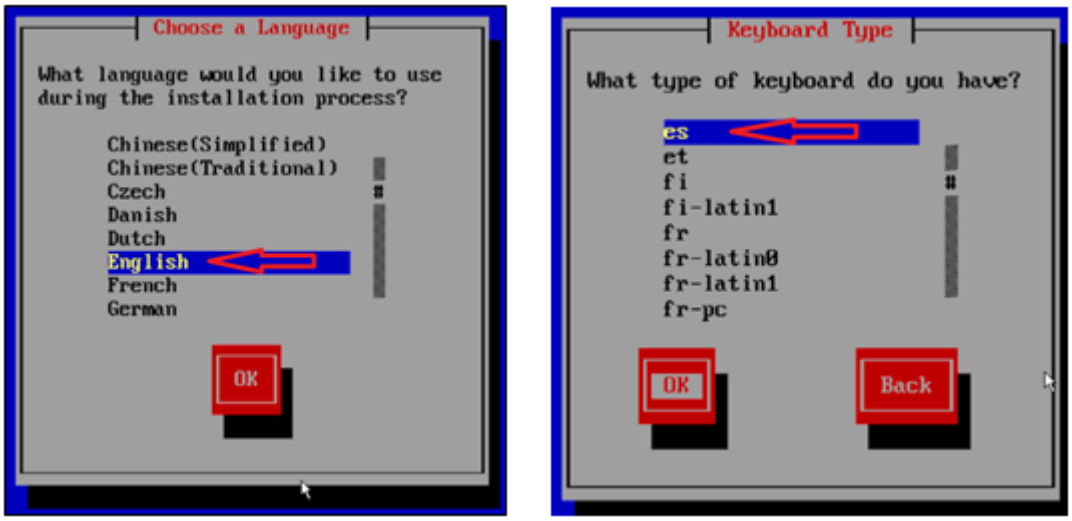


Ilustración 33. Instalación de Red Hat Enterprise Linux 5.x. (2).

Seleccionaremos el método dependiendo donde tengamos la imagen del software de instalación. Nuestro siguiente hito será la especificación del formato y tamaño de los discos

Ilustración 34. Instalación de Red Hat Enterprise Linux 5.x. (3).

Con "Disk Druid" especificaremos las particiones del SO. Crearemos las nuevas particiones del sistema, que por defecto y a no ser serán, a no ser que se indique lo contrario, las siguientes:

- / partición root Partición primaria (mínimo 4 Gb)
- /boot partición boot Partición primaria (500 Mb)
- /var particion var (8 Gb)
- swap partición swap (Para calcular el tamaño de la swap utilizaremos la siguiente fórmula:

  If M < 2
  S = M * 2
  Else
  S = M + 2

  Donde M es la cantidad de RAM en GB y S la cantidad en GB de swap resultante. Usando esta fórmula, un sistema con 2 GB de RAM físico debería tener 4 GB de swap, mientras que un sistema con 3 GB de RAM tendría 5 GB de swap.)

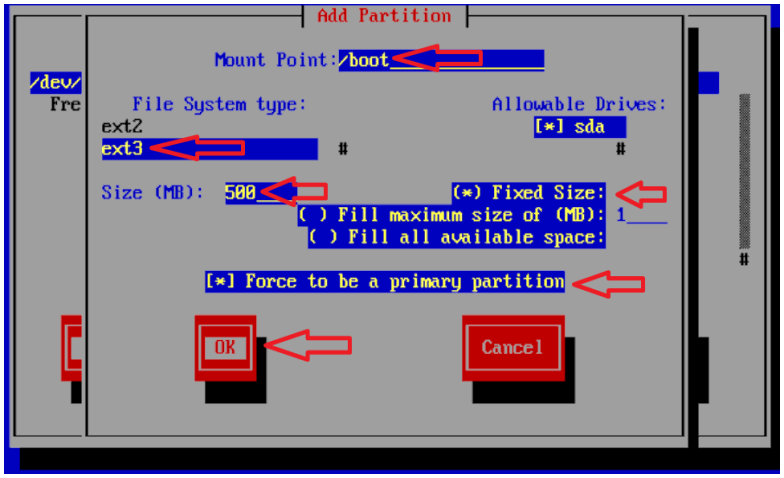


Ilustración 35. Instalación de Red Hat Enterprise Linux 5.x. (4).

Posteriormente, seleccionaremos GRUB como gestor de arranque, la partición de arranque, la configuración de red y el nombre de máquina

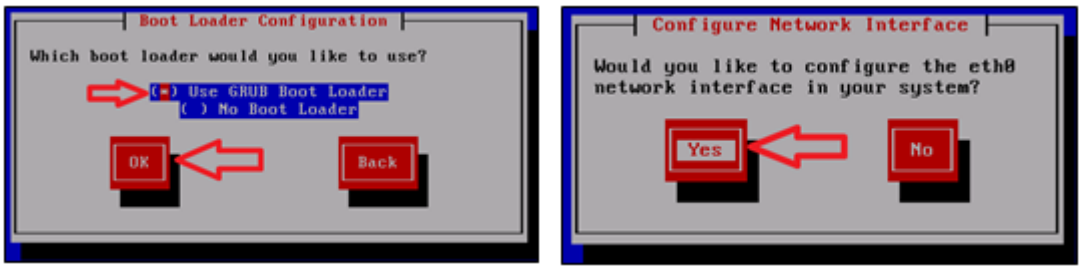


Ilustración 36. Instalación de Red Hat Enterprise Linux 5.x. (5).

En cuanto a la configuración de seguridad, en nuestro caso está definida de forma perimetral así que en principio no es necesaria su especificación en cada uno de los host.

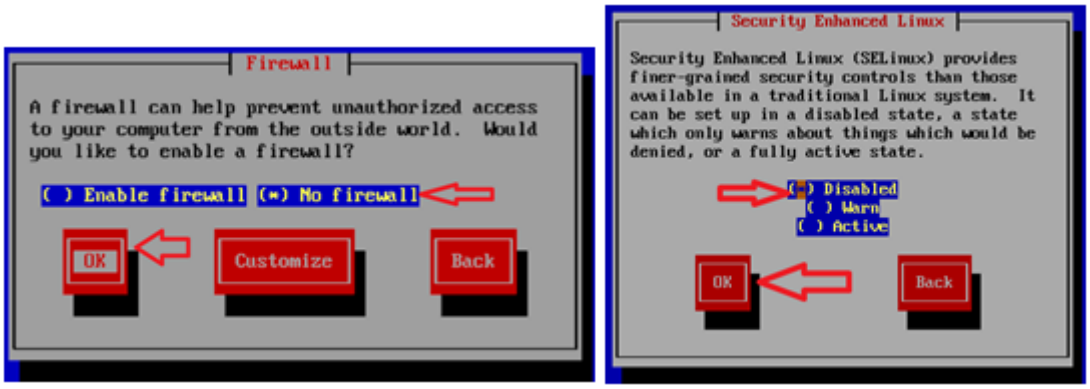


Ilustración 37. Instalación de Red Hat Enterprise Linux 5.x. (6).

Ya en la fase final de recogida de especificaciones de instalación, determinaremos la zona horaria, la password de root y la especificación de paquetes a instalar (en principio los básicos de servidor: Administration Tools, System Tools, Development Tools).

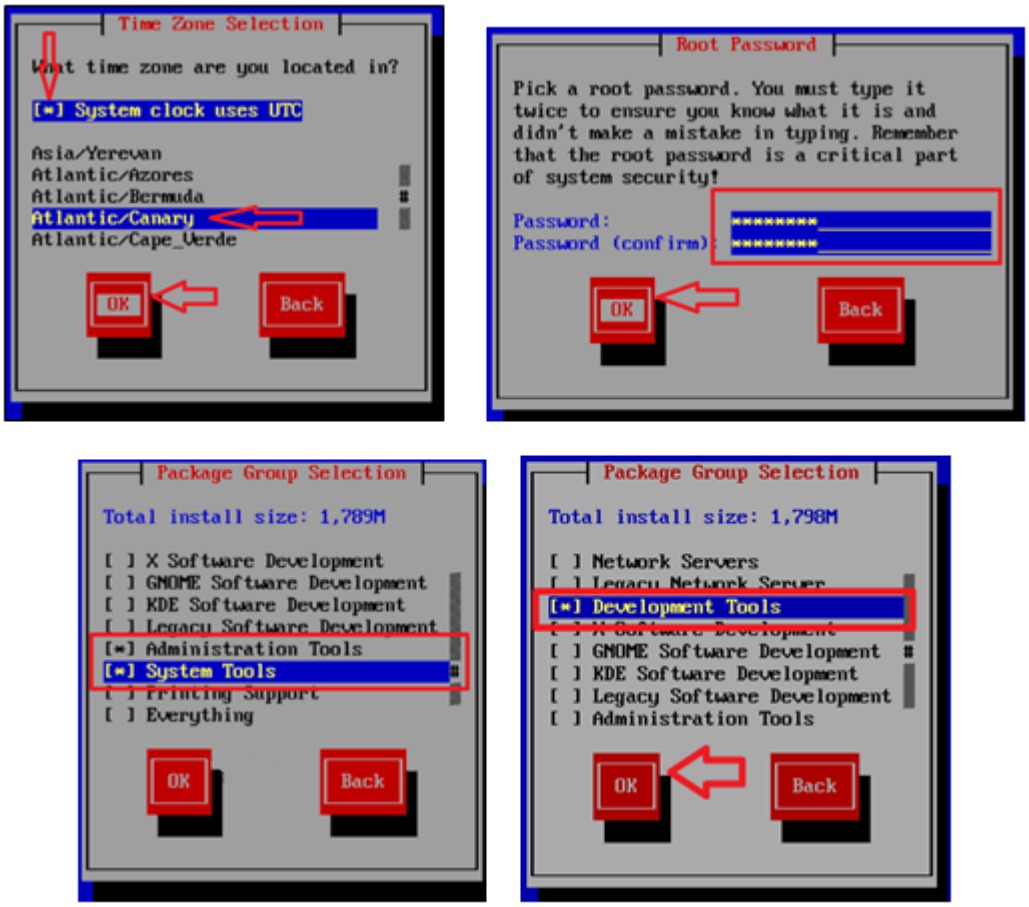


Ilustración 38. Instalación de Red Hat Enterprise Linux 5.x. (7).

Finalmente, comenzará la instalación que terminará con el reinicio del host

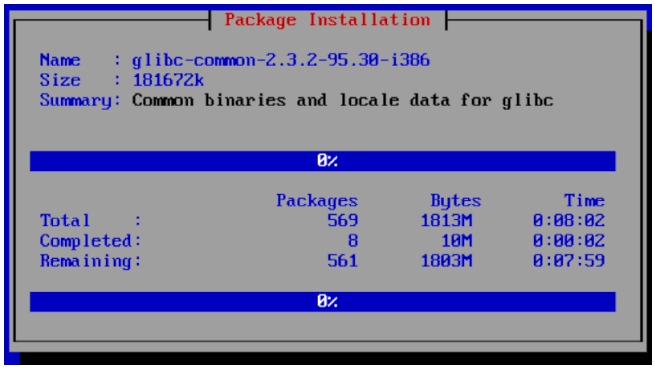


Ilustración 39. Instalación de Red Hat Enterprise Linux 5.x. (8).

8.2. INSTALACIÓN Y CONFIGURACIÓN BASE DE DATOS

La instalación de MySQL en Red Hat Enterprise es relativamente sencilla ya que se encuentra paquetizada. Simplemente, hay que invocar al instalador con el conjunto de paquetes requeridos y después configurar los servicios de arranque:

```
# yum install mysql mysql-server

#  chkconfig --add mysqld
#  chkconfig mysqld on
#  service mysqld start
```

Por defecto, el usuario root de MySQL base de datos está en blanco. Fijaremos la nueva password con el comando siguiente:

```
# mysqladmin -u root password YourNewPassword
```

8.2.1. CREACIÓN DE ESQUEMA MYSQL PARA EVENTOS

Para la utilización de MySQL como repositorio de RSYSLOG es necesario la creación de los diferentes esquemas. Para ello, hemos construido un script sql que permite la creación de cada uno de los esquemas que necesitemos pasándole los siguientes parámetros:

- Usuario de la BBDD con privilegios para la creación de Esquemas
- Password del usuario
- Servidor y Puerto
- Nombre de la Base de Datos a crear.

Ejecución para la creación de los esquemas sería la siguiente:

```
# mysql -u <usuario> -p<password> -h <servidor> -P <puerto> <NombreBBDD> < createSysEventsSchema.sql
```

Y el código del script:

```
DELIMITER $$

DROP TABLE IF EXISTS SystemEvents $$

CREATE TABLE  `SystemEvents` (
  `ID` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `CustomerID` bigint(20) DEFAULT NULL,
  `ReceivedAt` datetime DEFAULT NULL,
  `DeviceReportedTime` datetime DEFAULT NULL,
  `Facility` smallint(6) DEFAULT NULL,
  `Priority` smallint(6) DEFAULT NULL,
  `FromHost` varchar(60) DEFAULT NULL,
  `Message` text,
  `NTSeverity` int(11) DEFAULT NULL,
```

```
  `Importance` int(11) DEFAULT NULL,
  `EventSource` varchar(60) DEFAULT NULL,
  `EventUser` varchar(60) DEFAULT NULL,
  `EventCategory` int(11) DEFAULT NULL,
  `EventID` int(11) DEFAULT NULL,
  `EventBinaryData` text,
  `MaxAvailable` int(11) DEFAULT NULL,
  `CurrUsage` int(11) DEFAULT NULL,
  `MinUsage` int(11) DEFAULT NULL,
  `MaxUsage` int(11) DEFAULT NULL,
  `InfoUnitID` int(11) DEFAULT NULL,
  `SysLogTag` varchar(60) DEFAULT NULL,
  `EventLogType` varchar(60) DEFAULT NULL,
  `GenericFileName` varchar(60) DEFAULT NULL,
  `SystemID` int(11) DEFAULT NULL,
  `processid` varchar(60) NOT NULL DEFAULT '',
  `checksum` int(11) NOT NULL DEFAULT '0',
  PRIMARY KEY (`ID`),
  KEY `IDX_FromHost` (`FromHost`),
  KEY `IDX_SysLogTag` (`SysLogTag`)
) ENGINE=MyISAM AUTO_INCREMENT=100000 DEFAULT CHARSET=latin1 $$

DROP PROCEDURE IF EXISTS DeleteInterval $$

CREATE PROCEDURE DeleteInterval (IN days INT)
BEGIN
  DELETE
  FROM SystemEvents
  WHERE DeviceReportedTime < DATE_SUB(CURDATE(), INTERVAL days DAY);
END $$

DROP PROCEDURE IF EXISTS SearchCountInterval $$

CREATE PROCEDURE SearchCountInterval (IN days INT)
BEGIN
  SELECT COUNT(*)
  FROM SystemEvents
  WHERE DeviceReportedTime < DATE_SUB(CURDATE(), INTERVAL days DAY);
END $$

DROP PROCEDURE IF EXISTS SearchInterval $$

CREATE PROCEDURE SearchInterval (IN days INT)
BEGIN
  SELECT *
  FROM SystemEvents
  WHERE DeviceReportedTime < DATE_SUB(CURDATE(), INTERVAL days DAY);
  OPTIMIZE TABLE SystemEvents;
END $$

DELIMITER ;
```

8.3. INSTALACIÓN Y CONFIGURACIÓN LOGSTORE

8.3.1. INSTALACIÓN Y CONFIGURACIÓN RSYSLOG

Procederemos de forma análoga para la instalación de rsyslog. Así, desde una sesión de consola o shell de root, se invocará al instalador con las siguientes sentencias:

```
[root@LOGSTORE ~]# yum install rsyslog rsyslog-gnutls rsyslog-gssapi rsyslog-mysql
Loaded plugins: fastestmirror, security
Setting up Reinstall Process
Loading mirror speeds from cached hostfile
 * base: ftp.udl.es
 * extras: sunsite.rediris.es
 * updates: sunsite.rediris.es
Resolving Dependencies
--> Running transaction check
---> Package rsyslog.x86_64 0:3.22.1-7.el5 set to be updated
---> Package rsyslog-gnutls.x86_64 0:3.22.1-7.el5 set to be updated
---> Package rsyslog-gssapi.x86_64 0:3.22.1-7.el5 set to be updated
---> Package rsyslog-mysql.x86_64 0:3.22.1-7.el5 set to be updated
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package                Arch           Version               Repository    Size
================================================================================
Reinstalling:
 rsyslog                x86_64         3.22.1-7.el5          base         453 k
 rsyslog-gnutls         x86_64         3.22.1-7.el5          base          20 k
 rsyslog-gssapi         x86_64         3.22.1-7.el5          base          22 k
 rsyslog-mysql          x86_64         3.22.1-7.el5          base          13 k

Transaction Summary
================================================================================
Remove        0 Package(s)
Reinstall     4 Package(s)
Downgrade     0 Package(s)

Total download size: 509 k
Is this ok [y/N]: y
Downloading Packages:
(1/4): rsyslog-mysql-3.22.1-7.el5.x86_64.rpm             |  13 kB     00:00
(2/4): rsyslog-gnutls-3.22.1-7.el5.x86_64.rpm            |  20 kB     00:00
(3/4): rsyslog-gssapi-3.22.1-7.el5.x86_64.rpm            |  22 kB     00:00
(4/4): rsyslog-3.22.1-7.el5.x86_64.rpm                   | 453 kB     00:01
--------------------------------------------------------------------------------
Total                                       232 kB/s | 509 kB     00:02
Running rpm_check_debug
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing     : rsyslog                                                 1/4
  Installing     : rsyslog-gssapi                                          2/4
  Installing     : rsyslog-mysql                                           3/4
  Installing     : rsyslog-gnutls                                          4/4

Installed:
  rsyslog.x86_64 0:3.22.1-7.el5          rsyslog-gnutls.x86_64 0:3.22.1-7.el5
  rsyslog-gssapi.x86_64 0:3.22.1-7.el5   rsyslog-mysql.x86_64 0:3.22.1-7.el5

Complete!
```

Además de la instalación, crearemos un directorio de spool, para cachear los eventos destinados a BBDD:

```
[root@LOGSTORE ~]# mkdir –p /var/spool/rsyslog
```

8.3.1.1. Ejecución del demonio Rsyslog

Para comprobar la correcta instalación se procederá a ejecutar el script de inicio del demonio:

```
[root@LOGSTORE ~]# /etc/init.d/rsyslog start
Shut down sysklogd before you run rsyslog
```

Como se observa en la salida del comando anterior, en el caso de que existiera un demonio de syslogd, será necesario parar este, en re-emplazo del nuevo:

```
[root@LOGSTORE etc]# /etc/init.d/syslog stop
Shutting down kernel logger:                               [  OK  ]
Shutting down system logger:                               [  OK  ]
[root@LOGSTORE etc]# /etc/init.d/rsyslog start
Starting system logger:                                    [  OK  ]
```

Hay que recordar que RSYSLOG es totalmente compatible con las configuraciones previas de sysklogd, que es el demonio instalado por defecto, en varias distribuciones Linux, como Red Hat Enterprise Linux 5, por lo que el sistema seguirá funcionan y tomando eventos syslog, sin pérdida del servicio, por falta de nueva configuración.

8.3.1.2. Test de RSYSLOG

Una vez arrancado el servidor, se comprobará el funcionamiento:

```
[root@LOGSTORE etc]# tail /var/log/messages
LOGSTORE kernel: imklog 3.22.1, log source = /proc/kmsg started.
LOGSTORE     rsyslogd:     [origin     software="rsyslogd"     swVersion="3.22.1"     x-pid="5761"     x-
info="http://www.rsyslog.com"] (re)start
Apr 7 11:24:17 LOGSTORE rsyslogd: WARNING: rsyslogd is running in compatibility mode. Automatically
generated config directives may interfer with your rsyslog.conf settings. We suggest upgrading your config
and adding -c3 as the first rsyslogd option.
Apr 7 11:24:17 LOGSTORE rsyslogd: Warning: backward compatibility layer added to following directive to
rsyslog.conf: ModLoad imuxsock
```

Y que está recibiendo eventos con normalidad:

```
[root@LOGSTORE etc]# echo prueba | logger
[root@LOGSTORE etc]# tail -1 /var/log/messages
Apr 7 11:26:02 LOGSTORE logger: prueba
```

8.3.1.3. Configuración automática de inicio

Será necesario habilitar el nuevo servicio en el arranque de los servidores, remplazando (si lo hubiera) el sistema de syslogd que existiera por el servicio RSYSLOG:

```
[root@LOGSTORE etc]# chkconfig syslog off
[root@LOGSTORE etc]# chkconfig rsyslog on
[root@LOGSTORE etc]# chkconfig --list rsyslog
rsyslog         0:off   1:off   2:on    3:on    4:on    5:on    6:off
[root@LOGSTORE etc]# chkconfig --list syslog
syslog          0:off   1:off   2:off   3:off   4:off   5:off   6:off
```

8.3.1.4. Configuración estándar

Esta será la configuración mínima existente en los servidores estándar, si bien, y dependiendo del sistema, este puede ser modificado o diferir ligeramente:

```
###################
# RSYSLOGD CONFIG #
###################

# Use traditional timestamp format
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat
# Provides kernel logging support (previously done by rklogd)
$ModLoad imklog
# Provides TCP support
$ModLoad imtcp
$InputTCPServerRun 514
# Provides support for local system logging (e.g. via logger command)
$ModLoad imuxsock
# MySQL database logging support
$ModLoad ommysql
$ActionOmmysqlServerPort 3006
# Default location for work (spool) files
$WorkDirectory /var/spool/rsyslog
# Set file name, also enables disk mode
$MainMsgQueueFileName mainq
# The domain part from a name that is within the same domain as the receiving system is stripped
$PreserveFQDN off

#############
# TEMPLATES #
#############

# Dynamic standard file templates
$template DynFileCron,"/var/log/%HOSTNAME%-exp-cron-%$YEAR%%$MONTH%%$DAY%.log"
$template DynFileMessages,"/var/log/%HOSTNAME%-exp-messages-%$YEAR%%$MONTH%%$DAY%.log"
$template DynFileAuthPriv,"/var/log/%HOSTNAME%-exp-authpriv-%$YEAR%%$MONTH%%$DAY%.log"
$template DynFileMail,"/var/log/%HOSTNAME%-exp-mail-%$YEAR%%$MONTH%%$DAY%.log"
$template DynFileDaemon,"/var/log/%HOSTNAME%-exp-daemon-%$YEAR%%$MONTH%%$DAY%.log"
$template DynFileKern,"/var/log/%HOSTNAME%-exp-kernel-%$YEAR%%$MONTH%%$DAY%.log"

# Dynamic specific file templates
$template DynFileProFTPD,"/var/log/proftpd/%HOSTNAME%-exp-proftpd-%$YEAR%%$MONTH%%$DAY%.log"
$template DynFileSquidError,"/var/log/squid/%HOSTNAME%-exp-squid-error-%$YEAR%%$MONTH%%$DAY%.log"
$template DynFileApacheError,"/var/log/apache/%HOSTNAME%-exp-apache-error-%$YEAR%%$MONTH%%$DAY%.log"
$template DynFileCiscoVPN,"/var/log/vpn/%HOSTNAME%-exp-cisco-vpn-%$YEAR%%$MONTH%%$DAY%.log"
$template DynFileLogCentralizer,"/var/log/%HOSTNAME%-exp-logcentralizer-%$YEAR%%$MONTH%%$DAY%.log"
```

```
# Database templantes
$template MonitorWareMySQLInsert,"insert into SystemEvents (ReceivedAt, DeviceReportedTime, Facility,
Priority, FromHost, Message, InfoUnitID, SysLogTag, processid) values ('%timegenerated:::date-mysql%',
'%timereported:::date-mysql%', %syslogfacility%, %syslogpriority%, '%HOSTNAME:::UPPERCASE%', '%msg%',
%iut%, '%programname%', '%PROCID%')",SQL
$template StatsReportsSQLInsert,"insert into StatsReports (ReceivedAt, DeviceReportedTime, Facility,
Priority, FromHost, Message, InfoUnitID, SysLogTag, processid) values ('%timegenerated:::date-mysql%',
'%timereported:::date-mysql%', %syslogfacility%, %syslogpriority%, '%HOSTNAME:::UPPERCASE%', '%msg%',
%iut%, '%programname%', '%PROCID%')",SQL

########################
# LOGGING DESTINATIONS #
########################

# Log anything of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none,local0.none;local1.none;local2.none;local3.none;local4.none;local
5.none;local6.none;local7.none        ?DynFileMessages

# Log cron stuff
cron.*          ?DynFileCron

# Log kern stuff
kern.*          ?DynFileKern

# Log daemon stuff
daemon.*        ?DynFileDaemon
daemon.notice   /dev/console
daemon.notice   root, operator

# Everybody gets emergency messages
*.emerg         *

# Save news errors of level crit and higher in a special file.
uucp,news.crit  /var/log/spooler

# Log ALL errors to DB
# Use asynchronous processing
$ActionQueueType LinkedList
# Det file name, also enables disk mode
$ActionQueueFileName dbq_error
# Infinite retries on insert failure
$ActionResumeRetryCount -1
*.error         :ommysql:<SERVIDOR_MYSQL>,RSYSLOGDB_ERROR,<DB_USER>,<DB_PASS>;MonitorWareMySQLInsert

# The authpriv file has restricted access.
authpriv.*      ?DynFileAuthPriv
# Use asynchronous processing
$ActionQueueType LinkedList
# Det file name, also enables disk mode
$ActionQueueFileName dbq_authpriv
# Infinite retries on insert failure
$ActionResumeRetryCount -1
authpriv.*      :ommysql:<SERVIDOR_MYSQL>,RSYSLOGDB_AUTHPRIV,<DB_USER>,<DB_PASS>;MonitorWareMySQLInsert

# Log all the mail messages in one place.
mail.*          -?DynFileMail
# Use asynchronous processing
$ActionQueueType LinkedList
# Det file name, also enables disk mode
$ActionQueueFileName dbq_mail
# Infinite retries on insert failure
$ActionResumeRetryCount -1
mail.*          :ommysql:<SERVIDOR_MYSQL>,RSYSLOGDB_MAIL,<DB_USER>,<DB_PASS>;MonitorWareMySQLInsert

# Log cron stuff
cron.*          ?DynFileCron
```

```
# Everybody gets emergency messages
*.emerg         *

# Save news errors of level crit and higher in a special file.
uucp,news.crit  /var/log/spooler
```

A partir de esta plantilla inicial, y dependiendo del tipo de servidor del que se trate, se configuran los canales (facilitys) específicos a usar para la recogida de eventos (Tabla 4. Tipología de notificaciones de eventos a registrar)

8.3.1.5. Servidores ProFTPd

```
# Log all from ProFTPD
local1.*        -?DynFileProFTPD
# Use asynchronous processing
$ActionQueueType LinkedList
# Det file name, also enables disk mode
$ActionQueueFileName dbq_local1
# Infinite retries on insert failure
$ActionResumeRetryCount -1
local1.*        :ommysql:<SERVIDOR_MYSQL>,RSYSLOGDB_FTP,<DB_USER>,<DB_PASS>;MonitorWareMySQLInsert
```

8.3.1.6. Servidores Squid

```
# Log all from Squid
local2.*        -?DynFileSquidError
# Use asynchronous processing
$ActionQueueType LinkedList
# Det file name, also enables disk mode
$ActionQueueFileName dbq_local2
# Infinite retries on insert failure
$ActionResumeRetryCount -1
local2.*        :ommysql:<SERVIDOR_MYSQL>,RSYSLOGDB_HTTP_ERROR,<DB_USER>,<DB_PASS>;MonitorWareMySQLInsert
```

8.3.1.7. Servidores Apache

```
# Log all from Apache
local2.*        -?DynFileApacheError
# Use asynchronous processing
$ActionQueueType LinkedList
# Det file name, also enables disk mode
$ActionQueueFileName dbq_local2
# Infinite retries on insert failure
$ActionResumeRetryCount -1
local2.*        :ommysql:<SERVIDOR_MYSQL>,RSYSLOGDB_HTTP_ERROR,<DB_USER>,<DB_PASS>;MonitorWareMySQLInsert
```

8.3.1.8. Servidore de recepción de eventos Windows (LOGSTORE)

```
# Receive Windows messages (Only for logstore) - Win Server (PRE)
Local4.*        -?DynFileWinServerPre
# Use asynchronous processing
$ActionQueueType LinkedList
# Det file name, also enables disk mode
$ActionQueueFileName dbq_local4
# Infinite retries on insert failure
$ActionResumeRetryCount -1
Local4.*
:ommysql:<SERVIDOR_MYSQL>,RSYSLOGDB_WINDOWS_EVENTS,<DB_USER>,<DB_PASS>;MonitorWareMySQLInsert
```

```
# Receive Windows messages (Only for logstore) - Win Server (EXP)
local5.*        -?DynFileWinServerExp
# Use asynchronous processing
$ActionQueueType LinkedList
# Det file name, also enables disk mode
$ActionQueueFileName dbq_local5
# Infinite retries on insert failure
$ActionResumeRetryCount -1
local5.*
:ommysql:<SERVIDOR_MYSQL>,RSYSLOGDB_WINDOWS_EVENTS,<DB_USER>,<DB_PASS>;MonitorWareMySQLInsert
```

8.3.1.9. Servidore de recepción de eventos de electrónica red (LOGSTORE)

```
# Receive networking messages
Local6.*        -? DynFileCiscoVPN
# Use asynchronous processing
$ActionQueueType LinkedList
# Det file name, also enables disk mode
$ActionQueueFileName dbq_local6
# Infinite retries on insert failure
$ActionResumeRetryCount -1
Local6.*        :ommysql:<SERVIDOR_MYSQL>,RSYSLOGDB_NETWORK,<DB_USER>,<DB_PASS>;MonitorWareMySQLInsert
```

8.3.1.10. Logger para eventos de centralizacón (servidores RSYSLOG clientes)

```
# RSYNC log-centralizer
# Use asynchronous processing
$ActionQueueType LinkedList
# Det file name, also enables disk mode
$ActionQueueFileName dbq_local7
# Infinite retries on insert failure
$ActionResumeRetryCount -1
local7.notice
:ommysql:<SERVIDOR_MYSQL>,RSYSLOGDB_LOG_CENTRALIZER,<DB_USER>,<DB_PASS>;MonitorWareMySQLInsert
```

8.3.1.11. Logger para el almacenamiento de reports (LOGCONSOLE)

```
#############
# TEMPLATES #
#############

# Database templantes
$template StatsReportsSQLInsert,"insert into StatsReports (ReceivedAt, DeviceReportedTime, Facility,
Priority, FromHost, Message, InfoUnitID, SysLogTag, processid) values ('%timegenerated:::date-mysql%',
'%timereported:::date-mysql%', %syslogfacility%, %syslogpriority%, '%HOSTNAME:::UPPERCASE%', '%msg%',
%iut%, '%programname%', '%PROCID%')",SQL


########################
# LOGGING DESTINATIONS #
########################

local7.=debug
:ommysql:<SERVIDOR_MYSQL>,RSYSLOGDB_LOG_CENTRALIZER,<DB_USER>,<DB_PASS>;MonitorWareMySQLInsert
```

8.3.1.12. Configuración de nuevos servicios

En el caso de tener que tipificar un nuevo fichero de rotación dinámica, se tipificará en la parte de templates, del fichero de configuración /etc/rsyslog.conf, de la siguiente forma:

```
…
#############
# TEMPLATES #
#############
$template DynFile<Service>,"/var/log/%HOSTNAME%-<env>-<service>-%$YEAR%%$MONTH%%$DAY%.log"
Se añadirá la cláusula de logger:
…
########################
# LOGGING DESTINATIONS #
########################

# Log <service>
# Don't log private authentication messages!
localX.*                                        -?DynFile<Service>
…
```

Y en el caso de querer utilizar envío de eventos a BBDD, se utilizarán las siguientes cláusulas:

```
…
# RSYNC log-centralizer
# Use asynchronous processing
$ActionQueueType LinkedList
# Det file name, also enables disk mode
$ActionQueueFileName dbq_local7
# Infinite retries on insert failure
$ActionResumeRetryCount -1
localX.notice                                           :ommysql:<SERVIDOR_MYSQL>,RSYSLOGDB_LOG_CENTRALIZER,
<DB_USER>,<DB_PASS>;MonitorWareMySQLInsert
…
```

8.3.1.13. Purga de datos espurios

Una vez se haya adaptado la configuración de nuestro sistema, al uso de las plantillas predefinidas para los eventos syslog, tendremos que purgar la información referenciada por la configuración anterior:

```
[root@LOGSTORE etc]# rm –f /var/log/messages* /var/log/secure* /var/log/maillog* /var/log/cron*
```

Además de esto, se eliminarán las referencias al antiguo sistema de rotado “logrotated”:

```
[root@LOGSTORE ~]# vi /etc/logrotate.d/syslog
/var/log/spooler /var/log/boot.log {
    sharedscripts
    postrotate
        /bin/kill -HUP `cat /var/run/syslogd.pid 2> /dev/null` 2> /dev/null || true
        /bin/kill -HUP `cat /var/run/rsyslogd.pid 2> /dev/null` 2> /dev/null || true
    endscript
}
: wq
```

8.3.1.14. Debug

Podrá hacerse debug tanto de parseo de la configuración, como del funcionamiento de demonio.

Activación del debug:

```
[root@LOGSTORE ~]# export RSYSLOG_DEBUG="Debug"
[root@LOGSTORE ~]# /etc/init.d/rsyslog stop
[root@LOGSTORE ~]# /etc/init.d/rsyslog start
...
```

Para parar el debug, se deberá utilizar la secuencia “Ctrl+c”, lo que parará el demonio, y dejará de funcionar el servidor de syslog.

Desactivación del debug

Para desactivar el modo de debug, se deberá ejecutar los siguientes comandos:

```
[root@LOGSTORE ~]# unset RSYSLOG_DEBUG
[root@LOGSTORE ~]# /etc/init.d/rsyslog start
```

El demonio de syslogd seguirá funcionando en modo normal.

8.3.1.15. Pruebas de estrés

Para poder hacer test de estrés, se podrá hacer uso de scripts de shell basados en el uso de la utilidad logger:

```
[root@LOGSTORE ~]# COUNT=0; while true; do ((COUNT=COUNT+1)); logger -p authpriv.info "This is a stress
message [${COUNT}]"; done
```

Esto provocará la inundación del puerto del demonio, que podrá usarse para la evaluación y obtención de estadísticas.

8.3.2. ACTIVAR SYSLOG SOBRE TCP/IP

8.3.2.1. Configurar el Puerto de rsyslog forwarding

Para configurar el forwarding del rsyslog debemos indicarle al demonio rsyslogd que establezca los sockets TCP y UDP:

```
[root@LOGSTORE ~]# vi /etc/sysconfig/rsyslog
...
SYSLOGD_OPTIONS="-m 0 -r514"
...
:wq
[root@LOGSTORE ~]# /etc/init.d/rsyslog restart
Shutting down system logger:                               [  OK  ]
Starting system logger:                                    [  OK  ]

[root@LOGSTORE ~]# netstat –lnp
udp   109392      0 0.0.0.0:514                0.0.0.0:*                                   27903/rsyslogd
tcp        0      0 0.0.0.0:514                0.0.0.0:*                   LISTEN      27903/rsyslogd
```

8.3.2.2. Configurar RSYSLOG para la recepción de eventos remotos (clientes SYSLOG genéricos)

Dado que muchos de los sistemas, de entre los que destacan los servidores de Windows, carecen nativamente de un servicio de logger basado en syslog, el servidor rsyslog formará parte importante del sistema de centralización, centralizando en tiempo real, aquellos mensajes y eventos re-enviados desde esos otros sistemas. Es por ello que la configuración rsyslog del centralizador (/etc/rsyslog.conf) debe disponer de la siguiente configuración adicional a la de la plantilla estándar:

```
[root@LOGSTORE ~]# vi/etc/rsyslog.conf
###################
# RSYSLOGD CONFIG #
###################
# Provides TCP support
$ModLoad imtcp
$InputTCPServerRun 514

#############
# TEMPLATES #
#############

# Windows events receiber
$template          DynFileWinServerPre,"/logstore/logvol-pre/%$YEAR%/%$MONTH%/%$DAY%/%HOSTNAME%-pre-event-
%$YEAR%%$MONTH%%$DAY%.log"
$template          DynFileWinServerExp,"/logstore/logvol-exp/%$YEAR%/%$MONTH%/%$DAY%/%HOSTNAME%-exp-event-
%$YEAR%%$MONTH%%$DAY%.log"


########################
```

```
# LOGGING DESTINATIONS #
########################


# Receive Windows messages (Only for logstore) - Win Server (PRE)
Local4.*        -?DynFileWinServerPre
# Use asynchronous processing
$ActionQueueType LinkedList
# Det file name, also enables disk mode
$ActionQueueFileName dbq_local4
# Infinite retries on insert failure
$ActionResumeRetryCount -1
Local4.*
:ommysql:<SERVIDOR_MYSQL>,RSYSLOGDB_WINDOWS_EVENTS,<DB_USER>,<DB_PASS>;MonitorWareMySQLInsert

# Receive Windows messages (Only for logstore) - Win Server (EXP)
local5.*        -?DynFileWinServerExp
# Use asynchronous processing
$ActionQueueType LinkedList
# Det file name, also enables disk mode
$ActionQueueFileName dbq_local5
# Infinite retries on insert failure
$ActionResumeRetryCount -1
local5.*
:ommysql:<SERVIDOR_MYSQL>,RSYSLOGDB_WINDOWS_EVENTS,<DB_USER>,<DB_PASS>;MonitorWareMySQLInsert

# Receive networking messages
Local6.*        -? DynFileCiscoVPN
# Use asynchronous processing
$ActionQueueType LinkedList
# Det file name, also enables disk mode
$ActionQueueFileName dbq_local6
# Infinite retries on insert failure
$ActionResumeRetryCount -1
Local6.*        :ommysql:<SERVIDOR_MYSQL>,RSYSLOGDB_NETWORK,<DB_USER>,<DB_PASS>;MonitorWareMySQLInsert
```

8.3.2.3. Tareas adicionales del servidor

Adicionalmente a las tareas de centralización de logs y recolección de eventos re-enviados desde otros sistemas, el servidor acomete otras tareas que si bien no son propias de los procesos comentados, sí que guardan estrecha relación con el sistema de logs.

Vaciado de registros de eventos en BBDD

Dado que el espacio de BBDD destina a la recolección de eventos en tiempo real es finito, se han implementado mecanismos de purga de eventos, eliminan los registros más antiguos, lo que implica que la información de eventos en BBDD sea acotada en un tiempo finito equivalente a días o semanas.

Para realizar esta tarea se ha generado un script que vacía los esquemas de eventos RSYSLOGDB, en base al parámetro “AVAIL_DAYS”, que permitirá especificar el número de días de histórico de eventos que se mantendrá en BBDD.

El script se ejecuta diariamente mediante demonio cron.

Para habilitarlo y/o modificarlo:

```
[root@LOGSTORE ~]# vi /etc/cron.daily/flush_rsyslogdbs
#!/bin/bash
#

USER_DB=<USUARIO_DE_ESCRITURA_MYSQL>
USER_DB_PASS=<CONTRASEÑA_MYSQL>
DATA_BASE_SERVER=<SERVIDOR_MYSQL>
DATA_BASE_PORT=3001
DATA_BASES="RSYSLOGDB_AUTHPRIV        RSYSLOGDB_ERROR        RSYSLOGDB_HTTP_LDAP        RSYSLOGDB_HTTP_ERROR
RSYSLOGDB_HTTP_ACCESS     RSYSLOGDB_FTP     RSYSLOGDB_PROXY     RSYSLOGDB_MAIL     RSYSLOGDB_LOG_CENTRALIZER
RSYSLOGDB_WINDOWS_EVENTS <OTRAS_BBDD_MYSQL>"

AVAIL_DAYS=<NÚMERO_DE_DÍAS>
FLUSH_LOG=/var/log/`hostname`-exp-flushdb_exp-240horas-`date +"%Y%m%d"`.log

date > ${FLUSH_LOG}
if [[ -x /usr/bin/mysql ]];
then
        for DATA_BASE in $DATA_BASES;
        do
                echo "Flushing old registers from ${DATA_BASE}" >> ${FLUSH_LOG}
                /usr/bin/mysql -u ${USER_DB} -p${USER_DB_PASS} -h ${DATA_BASE_SERVER} -P ${DATA_BASE_PORT}
${DATA_BASE}      -e      "USE      ${DATA_BASE};      CALL      SearchCountInterval(${AVAIL_DAYS});      CALL
DeleteInterval(${AVAIL_DAYS});" >> ${FLUSH_LOG} 2>> ${FLUSH_LOG}
        done
else
        echo "Error! /usr/bin/mysql is not executable." >> ${FLUSH_LOG}
        exit -1
fi
date >> ${FLUSH_LOG}
```

Como resultado a la ejecución diaria, se generará un fichero de logs diario, con el formato "/var/log/<HOSTNAME>-exp-flushdb-<AAAAMMDD>.log":

```
[root@LOGSTORE ~]# ls -1  /var/log/LOGSTORE-exp-flushdb_*
/var/log/LOGSTORE-exp-flushdb-20130412.log.gz
/var/log/LOGSTORE-exp-flushdb-20130413.log.gz
/var/log/LOGSTORE-exp-flushdb-20130414.log.gz
/var/log/LOGSTORE-exp-flushdb-20130415.log.gz
/var/log/LOGSTORE-exp-flushdb-20130416.log.gz
/var/log/LOGSTORE-exp-flushdb-20130417.log.gz
/var/log/LOGSTORE-exp-flushdb-20130418.log
```

Cuyo contenido indicara el número de registros eliminados, y el estado de las tablas de eventos, tras su compactación MyISAM:

```
[root@LOGSTORE ~]# cat /var/log/LOGSTORE-exp-flushdb_exp-240horas-20130418.log
Thu Apr 18 06:03:01 WEST 2013
Flushing old registers from RSYSLOGDB_AUTHPRIV
COUNT(*)
3959926
Table   Op      Msg_type        Msg_text
RSYSLOGDB_AUTHPRIV.SystemEvents optimize        status  OK
Flushing old registers from RSYSLOGDB_ERROR
COUNT(*)
1471783
Table   Op      Msg_type        Msg_text
RSYSLOGDB_ERROR.SystemEvents    optimize        status  OK
Flushing old registers from RSYSLOGDB_FTP
COUNT(*)
24525
Table   Op      Msg_type        Msg_text
```

```
RSYSLOGDB_FTP.SystemEvents      optimize        status  OK
Flushing old registers from RSYSLOGDB_ERROR
COUNT(*)
0
Table   Op      Msg_type        Msg_text
RSYSLOGDB_ERROR.SystemEvents    optimize        status  OK
Flushing old registers from RSYSLOGDB_WINDOWS_EVENTS
COUNT(*)
0
Table   Op      Msg_type        Msg_text
RSYSLOGDB_WINDOWS_EVENTS.SystemEvents   optimize        status  OK
Flushing old registers from RSYSLOGDB_HTTP_ERROR
COUNT(*)
175906
Table   Op      Msg_type        Msg_text
RSYSLOGDB_HTTP_ERROR.SystemEvents       optimize        status  OK
Flushing old registers from RSYSLOGDB_NETWORK
COUNT(*)
127255
Table   Op      Msg_type        Msg_text
RSYSLOGDB_LDAP.SystemEvents     optimize        status  OK
```

8.3.3. INSTALACIÓN Y CONFIGURACIÓN RSYNC

La instalación de RSYNC también se realiza invocando al instalador de paquetes tal y como mostramos a continuación:

```
[root@LOGSTORE ~]# yum install rsync
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package rsync.i386 0:3.0.6-4.el5 set to be updated
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================ Package                 Arch
Version      Repository            Size
================================================================================Updating:
 rsync            i386             3.0.6-4.el5  rhel-mrepo-updates    338 k
Transaction Summary
================================================================================Install       0 Package(s)
Upgrade       1 Package(s)

Total download size: 338 k
Is this ok [y/N]: y
Downloading Packages:
rsync-3.0.6-4.el5.i386.rpm                                                                          |
338 kB     00:00
Running rpm_check_debug
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
  Updating                                                                                :            rsync
1/2
  Cleanup                                                                                 :           rsync
2/2

Updated:
  rsync.i386 0:3.0.6-4.el5

Complete!
```

Se comprueba la instalación:

```
[root@LOGSTORE ~]# ls /usr/bin/rsync
/usr/bin/rsync
```

8.3.3.1. Configuración

Creación de recursos de sistema

Para cada uno de los entornos habrá que crear los repositorios y montar los volúmenes de la SAN:

```
[root@LOGSTORE ~]# mkdir -p /logstore/logvol-exp/
[root@LOGSTORE ~]# mkdir -p /logstore/logvol-pre/
[root@LOGSTORE ~]# mkdir -p /logstore/logvol-local/
[root@LOGSTORE ~]# mount <device del volmen SAN para PRE> /logstore/logvol-pre
[root@LOGSTORE ~]# mount <device del volmen SAN para EXP> /logstore/logvol-exp
[root@LOGSTORE ~]# mount /dev/sda6 /logstore/logvol-local
[root@LOGSTORE ~]# vi /etc/fstab
…
<device del volmen SAN para EXP>    /logstore/logvol-pre    ext3    defaults        0 0
<device del volmen SAN para PRE>    /logstore/logvol-exp    ext3    defaults        0 0
/dev/sda6               /logstore/logvol-local  ext3    defaults        1 2
…

:wq
```

Fichero de configuración del demonio

El fichero de configuración del demonio será el siguiente:

```
[root@LOGSTORE ~]# mkdir /etc/rsyncd
[root@LOGSTORE ~]# vi /etc/rsyncd/rsyncd.conf
motd file = /etc/rsyncd/rsyncd.motd
use chroot = yes
list = yes
uid = root
gid = root
transfer logging = yes
syslog facility = local7
pid file = /var/run/rsyncd.pid
dont compress = yes
read only = false

[logvol-exp]
comment = LOGSTORE - logvol-exp log centralization
path = /logstore/logvol-exp
uid = root
gid = root
list = yes

[logvol-pre]
comment = LOGSTORE - logvol-pre log centralization
path = /logstore/logvol-pre
uid = root
gid = root
list = yes

[logvol-local]
comment = LOGSTORE - logvol-local log centralization
path = /logstore/logvol-local
uid = root
gid = root
list = yes

:wq

[root@LOGSTORE ~]# ls /etc/rsyncd/rsyncd.conf
/etc/rsyncd/rsyncd.conf
[root@LOGSTORE ~]# echo `date` - `date +"/%Y/%m/%d/"` > /etc/rsyncd/rsyncd.motd
```

Script y configuración de auto-arranque

El script de autoarranque queda defino de la siguiente manera:

```
[root@LOGSTORE ~]# vi /etc/init.d/rsync
#!/bin/sh
# Rsyncd This shell script takes care of starting and stopping the rsync daemon
# description: Rsync is an awesome replication tool.

# Source function library.
. /etc/rc.d/init.d/functions

[ -f /usr/bin/rsync ] || exit 0

case "$1" in
start)
action "Starting rsyncd: " /usr/bin/rsync -v --daemon --config=/etc/rsyncd/rsyncd.conf
;;
stop)
action "Stopping rsyncd: " killall rsync
;;
echo "Not yet implemented! Use: $0 stop; $0 start";
;;
status)
if ! [ "`pidof rsync`" == "" ];
then
        ps -p `pidof rsync`
else
        echo "RSYNC is not running."
fi
;;
*)
echo "Usage: rsyncd {start|stop|status|restart}"
exit 1
esac
exit 0

:wq
[root@LOGSTORE ~]# chmod 770 /etc/init.d/rsync
[root@LOGSTORE ~]# ln -s /etc/init.d/rsyncd /etc/rc3.d/S99rsyncd
```

8.3.3.2. Operaciones básicas

A continuación describimos las operaciones básicas de gestión del servicio

Arranque

```
[root@LOGSTORE ~]# /etc/init.d/rsync start
Starting rsyncd:                                           [  OK  ]
```

Parada

```
[root@LOGSTORE ~]# /etc/init.d/rsyncd stop
Stopping rsyncd:                                           [  OK  ]
```

Verificación desde local

```
[root@LOGSTORE ~]# /etc/init.d/rsyncd status
  PID TTY          TIME CMD
 2165 ?        00:00:00 rsync
```

Verificación desde remoto

```
[root@red1 ~]# rsync logstore::
Fri Apr 19 15:11:39 WEST 2013- /2013/04/19/

logvol-exp      LOGSTORE - logvol-exp log centralization
logvol-pre      LOGSTORE - logvol-pre log centralization
```

8.3.3.3. Comprobación de la centralización

Comprobaciones on-line sobre BBDD

De forma adicional al servidor, se ha elaborado un sistema preventivo de monitorización de centralización de logs, que en tiempo real, permitirá ver el estado diario de las centralizaciones, si estas se han producido, y si correctamente se han recogido en la BBDD de supervisión (RSYSLOGDB_LOG_CENTRALIZER), mediante la URL provista a través del servidor de consola LOGCONSOLE.

Comprobación sobre los sistemas de ficheros

Una manera inequívoca de comprobar los logs centralizados, es la de explorar los ficheros localizados en los repositorios destinados para ello, acorde a la política de centralización:

```
[root@LOGSTORE ~]# tree /logstore/logvol-<ENV>/<AÑO>/<MES>/<DÍA>
```

Así por ejemplo, para mostrar los logs centralizados del día 29 de Marzo de 2013, haríamos:

```
[root@LOGSTORE ~]# tree /logstore/logvol-exp/2013/03/29

/logstore/logvol-exp/2013/03/29
|-- LOGCONSOLE-exp-authpriv-20130329.log.gz
|-- LOGCONSOLE-exp-cron-20130329.log.gz
|-- LOGCONSOLE-exp-mail-20130329.log.gz
|-- LOGSTORE-exp-authpriv-20130329.log.gz
|-- LOGSTORE-exp-cron-20130329.log.gz
|-- LOGSTORE-exp-mail-20130329.log
|-- LOGSTORE-exp-messages-20130329.log.gz
`-- irsas-exp-messages-20130329.log.gz
```

Y para poder ver los ficheros de logs, que se están recibiendo mediante re-envío en tiempo real (servidores Windows y otros clientes syslog compatibles):

```
[root@LOGSTORE ~]# tree /logstore/logvol-exp/`date +"%Y"`/`date +"%m"`/`date +"%d"`
/logstore/logvol-exp/2013/03/30
|-- LOGSTORE-exp-mail-20130330.log
|-- berme5-exp-mail-20130330.log
`-- berme5-exp-mail-20130330.log
```

8.3.4. INSTALACIÓN Y CONFIGURACIÓN OPENSSL

Las librerías OpenSSL utilizadas de forma global en el sistema, vendrán instaladas mediante la paquetería por defectos de la seleccionada durante la instalación del servidor:

```
[root@LOGSTORE ~]# rpm -qa | grep openss
openssl-0.9.8e-22.el5_8.4
openssh-server-4.3p2-82.el5
openssh-4.3p2-82.el5
openssh-askpass-4.3p2-82.el5
openssh-clients-4.3p2-82.el5
```

8.3.5. INSTALACIÓN Y CONFIGURACIÓN NFS

Las librerías de NFS utilizadas de forma global en el sistema, vendrán instaladas mediante la paquetería por defectos de la seleccionada durante la instalación del servidor:

```
[root@LOGSTORE ~]# rpm -qa | grep nfs
nfs-utils-lib-1.0.8-7.9.el5
nfs-utils-1.0.9-60.el5
```

8.4. INSTALACIÓN Y CONFIGURACIÓN CONSUMIDORES

8.4.1. INSTALACIÓN Y CONFIGURACIÓN CONSUMIDORES TIPO 1

8.4.1.1. Instalación y configuración RSYSLOG

A excepción de la configuración, el proceso de instalación es el mismo que en el del servidor LOGSTORE.

La configuración de este servicio se basará en la utilización de la plantilla genérica de partida, y aquellas partes específicas según el tipo de servicio que servirán.

Una vez fijada la plantilla genérica, sólo será necesario hacer un “reload” sobre el servicio:

```
[root@LOGCONSOLE ~]# /etc/init.d/rsyslog reload
Reloading system logger...                                 [  OK  ]
```

Una vez se hay configurado y recargado el logger rsyslog, se puede comprobar el efecto inmediato listando los nuevos logs que se comienzan a generar:

```
[root@LOGCONSOLE ~]# ls -altr /var/log/`hostname`*.log
-rw------- 1 root root   4671 Apr 18 08:11 /var/log/LOGCONSOLE-exp-mail-20130418.log
-rw------- 1 root root   4455 Apr 18 10:46 /var/log/LOGCONSOLE-exp-daemon-20130418.log
-rw------- 1 root root   2488 Apr 18 14:01 /var/log/LOGCONSOLE-exp-cron-20130418.log
-rw------- 1 root root 132059 Apr 18 14:35 /var/log/LOGCONSOLE-exp-messages-20130418.log
-rw------- 1 root root 129283 Apr 18 14:35 /var/log/LOGCONSOLE-exp-kernel-20130418.log
-rw------- 1 root root 316921 Apr 18 14:38 /var/log/LOGCONSOLE-exp-authpriv-20130418.log
```

Si el servidor cliente además posee aplicaciones o servicios específicos (como por ejemplo el servicio proftpd), será necesario haber pre-configurado el sistema de logging del mismo, para hacer uso de la facility asignada según la tabla 4:

```
[root@elge ~]# ls -altr /var/log/proftpd/`hostname`-*.log
-rw------- 1 root root  578002 Apr 18 14:42 /var/log/proftpd/elge-exp-proftpd-20130418.log
```

8.4.1.2. Instalación y configuración RSYNC

A excepción de la configuración, el proceso de instalación es el mismo que en el del servidor LOGSTORE.

Una vez desplegado el software, y mediante la utilización del scheduler propio del sistemas (demonio cron), se utilizará un script shell para llevar a cabo el proceso de centralización diario de logs

Script de ejecución log-centralizer

```
#!/bin/sh
#

LOG_BASE_DIR=/var/log
RSYNC_MODULE=logvol-exp
RSYNC_SERVER=logstore

if ! [ -d ${LOG_BASE_DIR} ];
then
        echo "Error! No existe el directorio base ${LOG_BASE_DIR}" > /root/log_rsync.ERORR
        exit -1
fi

if [ -x /usr/bin/which ];
then
        DATE_CMD=`/usr/bin/which --skip-alias date`
        HOSTNAME_CMD=`/usr/bin/which --skip-alias hostname`
        FIND_CMD=`/usr/bin/which --skip-alias find`
        PERL_CMD=`/usr/bin/which --skip-alias perl`
        GZIP_CMD=`/usr/bin/which --skip-alias gzip`
        LOGGER_CMD=`/usr/bin/which --skip-alias logger`
        SLEEP_CMD=`/usr/bin/which --skip-alias sleep`
        RSYNC_CMD=`/usr/bin/which --skip-alias rsync`
        MD5SUM_CMD=`/usr/bin/which --skip-alias md5sum`
        GREP_CMD=`/usr/bin/which --skip-alias grep`
fi
```

```
if ! [ -x ${DATE_CMD} ];
then
        echo "date cmd not found. Using default /bin/date."
        if ! [ -x /bin/date ];
        then
                echo "Error! date required" > ${LOG_BASE_DIR}/log_rsync.ERORR
                exit -1
        else
                DATE_CMD="/bin/date"
        fi
fi

LOG_RSYNC="${LOG_BASE_DIR}/log_rsync-`${DATE_CMD} +"%A"`.log"
LOCAL_UTC=`${DATE_CMD} +"%s"`
${DATE_CMD} > ${LOG_RSYNC}


if ! [ -x ${HOSTNAME_CMD} ];
then
        echo "hostname cmd not found. Using default /bin/hostname."
        if ! [ -x /bin/hostname ];
        then
                echo "Error! hostname required" >> ${LOG_RSYNC}
                exit -1
        else
                HOSTNAME_CMD="/bin/hostname"
        fi
fi

HOSTNAME=`${HOSTNAME_CMD} -s`


if ! [ -x ${RSYNC_CMD} ];
then
        echo "rsync cmd not found. Using default /usr/bin/rsync."
        if ! [ -x /usr/bin/rsync ];
        then
                echo "Error! rsync required" >> ${LOG_RSYNC}
                exit -1
        else
                RSYNC_CMD="/usr/bin/rsync"
        fi
fi


if ! [ -x ${PERL_CMD} ];
then
        echo "perl cmd not found. Using default /usr/bin/perl."
        if ! [ -x /usr/bin/perl ];
        then
                echo "Error! perl recommended, using date --date='1 days ago'" >> ${LOG_RSYNC}
                DST_DIR=`date --date='1 days ago' +'%Y/%m/%d'`
                LOCAL_DAY_FILTER=`date --date='1 days ago' +'%Y%m%d'`
        else
                PERL_CMD="/usr/bin/perl"
        fi
fi
```

```
if [ -x ${PERL_CMD} ];
then
        DST_DIR=`${PERL_CMD} -e '($sec,$min,$hour,$mday,$mon,$year,$wday,$yday,$isdst) = gmtime((shift) -
86400); printf "%4d/%02d/%02d",$year+1900,$mon+1,$mday,$hour,$min,$sec;' ${LOCAL_UTC}`
        LOCAL_DAY_FILTER=`${PERL_CMD}    -e    '($sec,$min,$hour,$mday,$mon,$year,$wday,$yday,$isdst)    =
gmtime((shift) - 86400); printf "%4d%02d%02d",$year+1900,$mon+1,$mday,$hour,$min,$sec;' ${LOCAL_UTC}`
fi


if ! [ -x ${FIND_CMD} ];
then
        echo "find cmd not found. Using default /usr/bin/find."
        if ! [ -x /usr/bin/find ];
        then
                echo "Error! find required" >> ${LOG_RSYNC}
                exit -1
        else
                FIND_CMD="/usr/bin/find"
        fi
fi
FILE_LIST=`${FIND_CMD} ${LOG_BASE_DIR} -iname "${HOSTNAME}-*${LOCAL_DAY_FILTER}*"`


if ! [ -x ${LOGGER_CMD} ];
then
        echo "logger cmd not found. Using default /bin/logger."
        if ! [ -x /bin/logger ];
        then
                echo "Error! logger recommended" >> ${LOG_RSYNC}
        else
                LOGGER_CMD="/bin/logger"
        fi
fi

if [ -x ${LOGGER_CMD} ];
then
        ${LOGGER_CMD}   -p   local7.notice   -t   ${HOSTNAME}-log-centralizer   -i   "Executing   rsync   log
centralization from ${HOSTNAME} for -${LOCAL_DAY_FILTER} log files"
fi


if ! [ -x ${GZIP_CMD} ];
then
        echo "gzip cmd not found. Using default /bin/gzip."
        if ! [ -x /bin/gzip ];
        then
                echo "Error! /bin/gzip recommended" >> ${LOG_RSYNC}
        else
                GZIP_CMD="/bin/gzip"
        fi
fi

if [ -x ${GZIP_CMD} ];
then
        for FILE in ${FILE_LIST};
        do
                echo "Compressing ${FILE}" >> ${LOG_RSYNC}
                ${GZIP_CMD} ${FILE} >> ${LOG_RSYNC} 2>> ${LOG_RSYNC}
        done
fi
```

```
if ! [ -x ${SLEEP_CMD} ];
then
        echo "sleep cmd not found. Using default /bin/sleep."
        if ! [ -x /bin/sleep ];
        then
                echo "Error! /bin/sleep recommended" >> ${LOG_RSYNC}
        else
                SLEEP_CMD="/bin/sleep"
        fi
fi
if [ -x ${SLEEP_CMD} ];
then
        # Waiting for compression
        ${SLEEP_CMD} 60
fi


FILE_LIST=`${FIND_CMD} ${LOG_BASE_DIR} -iname "${HOSTNAME}-*${LOCAL_DAY_FILTER}*"`


if ! [ -x ${MD5SUM_CMD} ];
then
        echo "md5sum cmd not found. Using default /usr/bin/md5sum."
        if ! [ -x /usr/bin/md5sum ];
        then
                echo "Error! /usr/bin/md5sum recommended"  >> ${LOG_RSYNC}
        else
                MD5SUM_CMD="/usr/bin/md5sum"
        fi
fi
if [ -x ${MD5SUM_CMD} ];
then
        for FILE in ${FILE_LIST};
        do
                if [ -x ${LOGGER_CMD} ];
                then
                        ${MD5SUM_CMD} ${FILE} | ${LOGGER_CMD} -t ${HOSTNAME}-md5sum-daily -p local7.notice
                else
                        ${MD5SUM_CMD} ${FILE} >> ${LOG_RSYNC}
                fi
        done
fi


if [ -x ${RSYNC_CMD} ];
then
        if ! [ -x ${GREP_CMD} ];
        then
                echo "grep cmd not found. Using default /bin/grep."
        else
                GREP_CMD="/bin/grep"
        fi
        if [ -x ${GREP_CMD} ]
        then
                if [ `${RSYNC_CMD} --version | ${GREP_CMD} -c "version 2"` -eq 1 ];
                then
                        ${RSYNC_CMD}        --ignore-existing        --stats        -avc        ${FILE_LIST}
${RSYNC_SERVER}::${RSYNC_MODULE}/${DST_DIR} | ${LOGGER_CMD} -t ${HOSTNAME}-rsync-daily -p local7.notice -s
2>> ${LOG_RSYNC}
                else
                        ${RSYNC_CMD} --ignore-existing --stats --log-file=${LOG_RSYNC} -avch ${FILE_LIST}
${RSYNC_SERVER}::${RSYNC_MODULE}/${DST_DIR} | ${LOGGER_CMD} -t ${HOSTNAME}-rsync-daily -p local7.notice
                fi
        fi
fi
```

Este script se alojará en el directorio de tareas a ejecutar diariamente por el scheduler cron:

```
[root@elge ~]# ls -altr /etc/cron.daily/log-centralizer
-rwxr-x--- 1 root root 2835 Apr 14  2013 /etc/cron.daily/log-centralizer
```

8.4.1.3. Comprobación de la centralización

El proceso de centralización dejará registro tanto en local (en el file system de logs del propio servidor cliente), como en la BBDD de centralización (RSYSLOGDB_LOG_CENTRALYZER). Este registro describe puntos esenciales:

1. Localización de ficheros a centralizar (los correspondientes al día anterior).
2. Compresión de los ficheros.
3. Registro del hash MD5 (firma) de cada fichero.
4. Centralización (copia) de los ficheros hasta el servidor LOGSTORE.

```
[root@elge ~]# cat /var/log/`hostname` -exp-logcentralizer-`date +"%Y%m%d"`.log
Apr 18 04:02:35 elge elge-log-centralizer[10669]: Executing rsync log centralization from elge for -
20130417 log files
Apr 18 04:03:36 elge elge-md5sum-daily: 00221ec599a42443871b6896aa7b9924 /var/log/elge-exp-messages-
20130417.log.gz
Apr 18 04:03:36 elge elge-md5sum-daily: cec2cfe49f0d7d3f7bbc2f963727027f /var/log/elge-exp-daemon-
20130417.log.gz
Apr 18 04:03:36 elge elge-md5sum-daily: 4e5fb692e92210a65e7c0841ae439186 /var/log/proftpd/elge-exp-
proftpd-20130417.log.gz
Apr 18 04:03:36 elge elge-md5sum-daily: 627917e2497e3d3da022dd3e610ad853 /var/log/elge-exp-mail-
20130417.log.gz
Apr 18 04:03:36 elge elge-md5sum-daily: abc5f6b58c4a2592e5915b6d6294409e /var/log/elge-exp-
logcentralizer-20130417.log.gz
Apr 18 04:03:36 elge elge-md5sum-daily: 7b5a30fe9719f22f4de6624057238f1d /var/log/elge-exp-cron-
20130417.log.gz
Apr 18 04:03:36 elge elge-md5sum-daily: 0106398ae5f2b788f77cb819106aa865 /var/log/elge-exp-authpriv-
20130417.log.gz
Apr 18 04:03:36 elge elge-rsync-daily: Wed Apr 17 07:30:49 WEST 2013 - /2013/04/17/
Apr 18 04:03:36 elge elge-rsync-daily:
Apr 18 04:03:36 elge elge-rsync-daily: sending incremental file list
Apr 18 04:03:36 elge elge-rsync-daily: elge-exp-authpriv-20130417.log.gz
Apr 18 04:03:36 elge elge-rsync-daily: elge-exp-cron-20130417.log.gz
Apr 18 04:03:36 elge elge-rsync-daily: elge-exp-daemon-20130417.log.gz
Apr 18 04:03:36 elge elge-rsync-daily: elge-exp-logcentralizer-20130417.log.gz
Apr 18 04:03:36 elge elge-rsync-daily: elge-exp-mail-20130417.log.gz
Apr 18 04:03:36 elge elge-rsync-daily: elge-exp-messages-20130417.log.gz
Apr 18 04:03:36 elge elge-rsync-daily: elge-exp-proftpd-20130417.log.gz
Apr 18 04:03:36 elge elge-rsync-daily:
Apr 18 04:03:36 elge elge-rsync-daily: Number of files: 7
Apr 18 04:03:36 elge elge-rsync-daily: Number of files transferred: 7
Apr 18 04:03:36 elge elge-rsync-daily: Total file size: 372.63K bytes
Apr 18 04:03:36 elge elge-rsync-daily: Total transferred file size: 372.63K bytes
Apr 18 04:03:36 elge elge-rsync-daily: Literal data: 372.63K bytes
Apr 18 04:03:36 elge elge-rsync-daily: Matched data: 0 bytes
Apr 18 04:03:36 elge elge-rsync-daily: File list size: 761
Apr 18 04:03:36 elge elge-rsync-daily: File list generation time: 0.002 seconds
Apr 18 04:03:36 elge elge-rsync-daily: File list transfer time: 0.000 seconds
Apr 18 04:03:36 elge elge-rsync-daily: Total bytes sent: 373.99K
Apr 18 04:03:36 elge elge-rsync-daily: Total bytes received: 255
Apr 18 04:03:36 elge elge-rsync-daily:
Apr 18 04:03:36 elge elge-rsync-daily: sent 373.99K bytes  received 255 bytes  748.49K bytes/sec
Apr 18 04:03:36 elge elge-rsync-daily: total size is 372.63K  speedup is 1.00
```

8.4.1.4. Purga de ficheros antiguos

Dado que el espacio de almacenamiento de los servidores es finito, es altamente recomendable purgar ficheros de logs antiguos, que en su defecto, ya han sido centralizados. Para tal menester se utilizará otra tarea mediante el scheduler cron de los sistemas:

```
Script de ejecución log-centralizer
[root@elge ~]# cat /etc/cron.daily/log-expirer
#!/bin/sh
#

LOG_BASE_DIR=/var/log
COMPRESSION_PERIOD=1440
EXPIRATION_PERIOD=10080

[[ -x /bin/logger  ]] && /bin/logger -t$0 -i `Executing log_expirer`

if [ -x /bin/date ];
then
        LOG_EXPIRER=/var/log/log_expirer-`date +"%A"`.log
        /bin/date > ${LOG_EXPIRER}
else
        echo "Error! No existe /bin/date" > ${LOG_BASE_DIR}/ERROR_log-expirer.log
fi

[[ -x /bin/gzip ]] && /bin/gzip >> ${LOG_EXPIRER} || echo "Error! No existe /bin/gzip" >> ${LOG_EXPIRER}


if [[ -x /usr/bin/find ]];
then
        /usr/bin/find  ${LOG_BASE_DIR}  -name  "`hostname`-*.log"  -mmin  +${COMPRESSION_PERIOD}  -exec
/bin/gzip -v -9 {} \; >> ${LOG_EXPIRER}
        /usr/bin/find ${LOG_BASE_DIR} -name "`hostname`-*.log.gz" -mmin +${EXPIRATION_PERIOD} -exec rm -v
-f {} \; >> ${LOG_EXPIRER}
else
        echo  "No  se  ha  encontrado  /usr/bin/find.  No  se  puede  ejecutar  el  rotado  automatico."  >>
${LOG_EXPIRER}
fi
```

Este script se alojará en el directorio de tareas a ejecutar diariamente por el scheduler cron:

```
[root@elge ~]# ls -altr /etc/cron.daily/log-expirer
-rwxr-x--- 1 root root 874 Apr  18  2013 /etc/cron.daily/log-expirer
```

De cara a poder hacer seguimiento de la purga, también se dejará registro a nivel local:

```
[root@elge ~]# cat /var/log/log_expirer-`date +"%A"`.log
Thu Apr 18 04:03:36 WEST 2013
removed `/var/log/elge-exp-logcentralizer-20130411.log.gz'
removed `/var/log/proftpd/elge-exp-proftpd-20130410.log.gz'
removed `/var/log/elge-exp-messages-20130410.log.gz'
removed `/var/log/elge-exp-authpriv-20130410.log.gz'
removed `/var/log/elge-exp-kernel-20130410.log.gz'
removed `/var/log/elge-exp-mail-20130410.log.gz'
removed `/var/log/elge-exp-daemon-20130410.log.gz'
removed `/var/log/elge-exp-cron-20130410.log.gz'
```

8.4.2. INSTALACIÓN Y CONFIGURACIÓN CONSUMIDORES TIPO 2

8.4.2.1. Instalación y configuración DELTACOPY

DeltaCopy se distribuye en forma de paquete comprimido con los ejecutables de instalación. El proceso lanzado desde el ejecutable presenta el típico wizard de Windows que recopila los datos necesarios para la instalación. Antes de terminar, se mostrará la ventana de DeltaCopy Server Console. Esta consola permite el registro de la aplicación como servicio, el arranque y la parada de este.

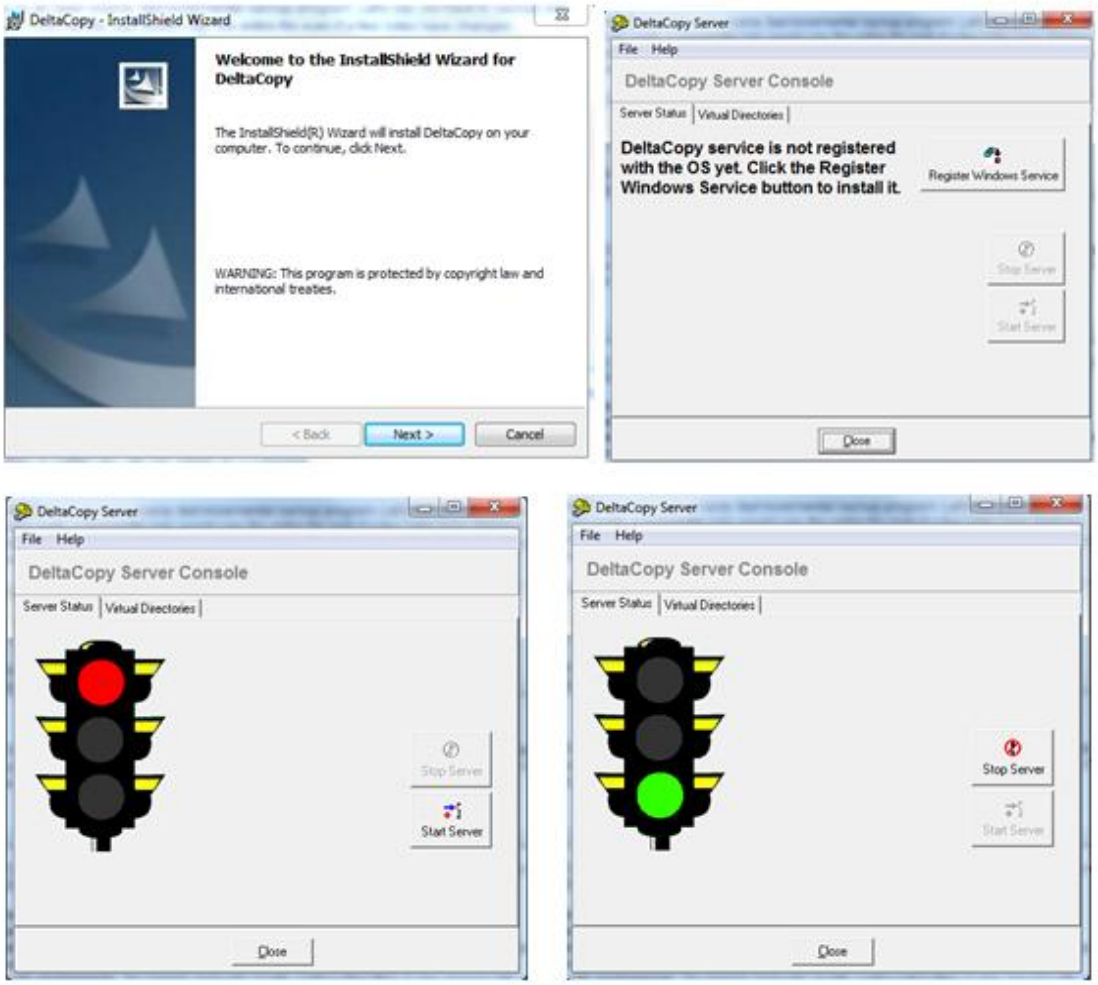


Ilustración 40. Instalación y configuración DELTACOPY (1).

Una vez arrancado el servicio debemos especificar los directorios virtuales de copia si fueran necesarios y crear un nuevo perfil. En la especificación del nuevo perfil le indicaremos el servidor de centralización que nos mostrará los repositorios configurados en este a efectos de elegir el destino correcto de la copia a realizar.

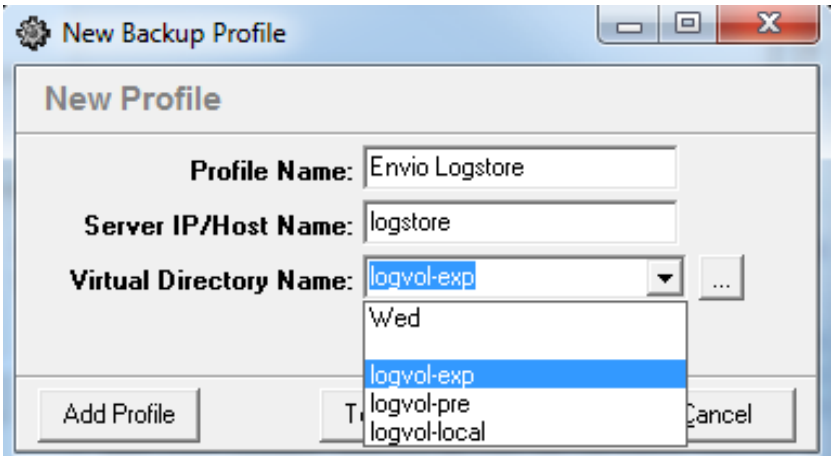


Ilustración 41. Instalación y configuración DELTACOPY (2).

Una vez configurado el perfil habrá que especificar los directorios sobre los que realizar la copia, las opciones, la autenticación y la programación de la tarea de copia a través del schedule.

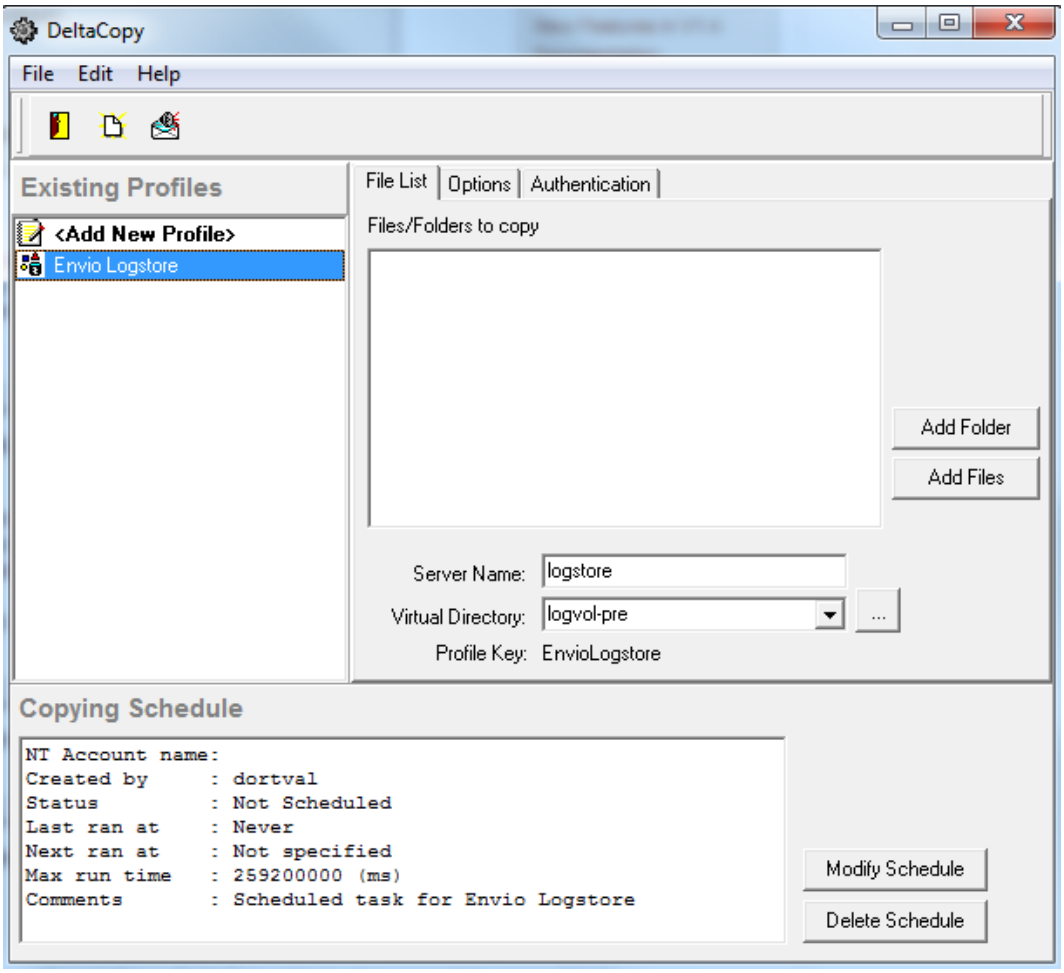


Ilustración 42. Instalación y configuración DELTACOPY (3).

8.4.2.2. Instalación y configuración NTSYSLOG

La instalación de NTSYSLOG se realiza igualmente a través de un ejecutable. Este nos presenta otro wizard que nos guiará a través del proceso de instalación.

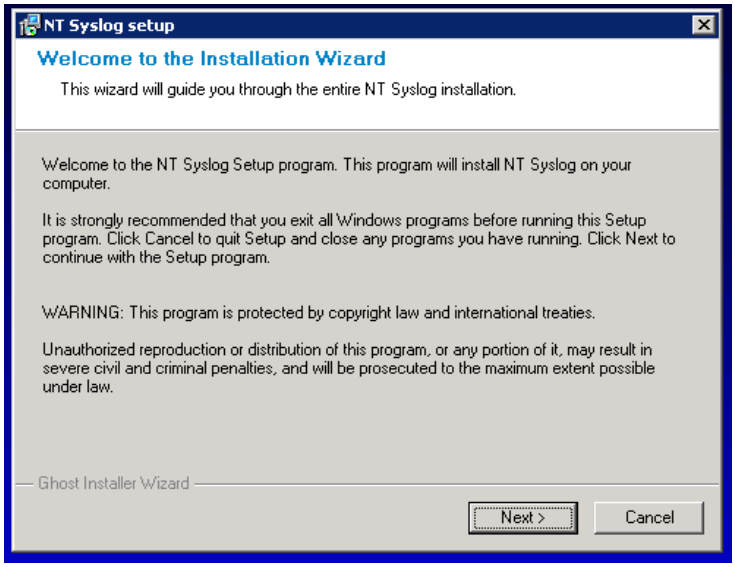


Ilustración 43. Instalación y configuración NTSYSOLOG (1).

Análogamente a DeltaCopy, tendremos que proceder a instalar la aplicación como servicio. Para ello, usamos la utilidad NTSyslog Install (Programas – NTSyslog – NTSyslog Install)

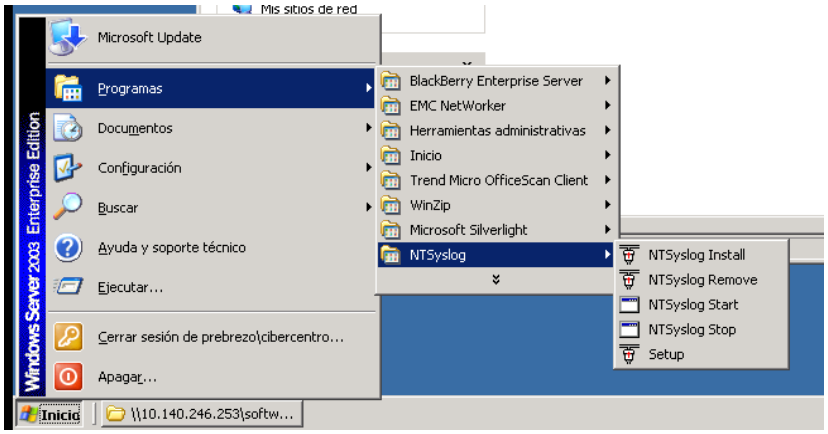


Ilustración 44. Instalación y configuración NTSYSOLOG (2)

Una vez finalizado el proceso, la configuración de opciones se hace a través de especificaciones en el registro de Windows. Así, la configuración para establecer el host de destino se definiría de la siguiente manera

```
HKEY_LOCAL_MACHINE\SOFTWARE\SaberNet]
"Syslog"="loghost.example.com"
```

Para facilitar el proceso se ha creado una serie de archivos *.reg dependiendo del S.O. y rol del servidor que introducen todas las claves de registro necesarias para la configuración.

- DC_ntsyslog_PRE: Controladores de dominio Windows Server 2003
- SR_ntsyslog_PRE: Servidores miembros Windows Server 2003
- SR2k8_ntsyslog_PRE: Servidores miembros Windows Server 2008

En estos archivos se define el Host de destino y los tipos de eventos a recoger.

SR2k8_ntsyslog_PRE

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SaberNet]
@="\"\""
"Syslog"="10.140.xxx.xxx"

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SaberNet\Syslog]
@="\"\""
"LastRun"=dword:4e43bfe9

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SaberNet\Syslog\Application]
@="\"\""
"Information"=dword:00000000
"Warning"=dword:00000001
"Error"=dword:00000001
"Audit Success"=dword:00000000
"Audit Failure"=dword:00000001
"Information Priority"=dword:00000009
"Warning Priority"=dword:000000b1
"Error Priority"=dword:000000b1
"Audit Success Priority"=dword:00000009
"Audit Failure Priority"=dword:000000b1

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SaberNet\Syslog\HardwareEvents]
"Information"=dword:00000000
"Information Priority"=dword:00000009
"Warning"=dword:00000000
"Warning Priority"=dword:00000009
"Error"=dword:00000000
"Error Priority"=dword:00000009
"Audit Success"=dword:00000000
"Audit Success Priority"=dword:00000009
"Audit Failure"=dword:00000000
"Audit Failure Priority"=dword:00000009

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SaberNet\Syslog\Internet Explorer]
"Information"=dword:00000000
"Information Priority"=dword:00000009
"Warning"=dword:00000000
"Warning Priority"=dword:00000009
"Error"=dword:00000000
"Error Priority"=dword:00000009
"Audit Success"=dword:00000000
"Audit Success Priority"=dword:00000009
"Audit Failure"=dword:00000000
"Audit Failure Priority"=dword:00000009
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SaberNet\Syslog\Key Management Service]
"Information"=dword:00000000
"Information Priority"=dword:00000009
"Warning"=dword:00000000
"Warning Priority"=dword:00000009
"Error"=dword:00000000
"Error Priority"=dword:00000009
"Audit Success"=dword:00000000
"Audit Success Priority"=dword:00000009
"Audit Failure"=dword:00000000
"Audit Failure Priority"=dword:00000009

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SaberNet\Syslog\Security]
@="\"\""
"Information"=dword:00000000
"Warning"=dword:00000001
"Error"=dword:00000001
"Audit Success"=dword:00000000
"Audit Failure"=dword:00000001
"Information Priority"=dword:00000009
"Warning Priority"=dword:000000b1
"Error Priority"=dword:000000b1
"Audit Success Priority"=dword:00000009
"Audit Failure Priority"=dword:000000b1

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SaberNet\Syslog\System]
@="\"\""
"Information"=dword:00000000
"Warning"=dword:00000001
"Error"=dword:00000001
"Audit Success"=dword:00000000
"Audit Failure"=dword:00000001
"Information Priority"=dword:00000009
"Warning Priority"=dword:000000b1
"Error Priority"=dword:000000b1
"Audit Success Priority"=dword:00000009
"Audit Failure Priority"=dword:000000b1

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SaberNet\Syslog\Windows PowerShell]
"Information"=dword:00000000
"Information Priority"=dword:00000009
"Warning"=dword:00000000
"Warning Priority"=dword:00000009
"Error"=dword:00000000
"Error Priority"=dword:00000009
"Audit Success"=dword:00000000
"Audit Success Priority"=dword:00000009
"Audit Failure"=dword:00000000
"Audit Failure Priority"=dword:00000009
```

Para finalizar se ha de reiniciar el servicio desde una consola cmd ejecute:

```
C:\>net stop ntsyslog
El servicio de NTsyslog está deteniéndose......
El servicio de NTsyslog fue detenido con éxito.
```

```
C:\>net start ntsyslog
El servicio de NTsyslog está iniciándose.
El servicio de NTsyslog se ha iniciado con éxito.
```

8.4.3. INSTALACIÓN Y CONFIGURACIÓN CONSUMIDORES TIPO 3

8.4.3.1. Configuración de sistemas UNIX / Linux basados en demonios syslog

Bajo este escenario se puede encontrar cualquier distribución Linux o UNIX que use un demonio logger basado en el estándar syslog (nt-syslogd, sysklogd, etc.).

La instrucción básica será la de habilitar el re-envío de todos los eventos syslog al servidor LOGSTORE:

```
[root@berme ~]# cat /etc/redhat-release
Red Hat Enterprise Linux AS release 4 (Nahant Update 6)
[root@berme ~]# vi /etc/rsyslog.conf
…
*.*                                                    @logstore
:wq
[root@berme ~]# /etc/init.d/syslog restart
Desactivando el generador de logs del kernel:              [  OK  ]
Desactivando el generador de logs del sistema:             [  OK  ]
Iniciando logger del sistema:                              [  OK  ]
Iniciando el generador de logs del kernel:                 [  OK  ]
[root@berme ~]#
```

Esta configuración de re-envío permitirá que LOGSTORE almacene los logs de estos clientes, en base a la plantilla genérica RSYSLOG:

```
[root@LOGSTORE ~]# ls -altr /var/log/berme-exp-*.log
-rw------- 1 root root  26154 Apr 18 15:59 /var/log/berm-exp-cron-20130418.log
-rw------- 1 root root 449318 Apr 18 16:02 /var/log/berm-exp-authpriv-20130418.log
-rw------- 1 root root 431644 Apr 18 16:02 /var/log/berm-exp-messages-20130418.log
```

Estos logs serán centralizados desde el propio sistema, mediante la tarea de log-centralizer ejecutada sobre el propio servidor LOGSTORE, en calidad de cliente.

8.4.3.2. Configuración de electrónica de red compatible con syslog (Routers Cisco)

La mayoría de proveedores de electrónica de red implementa en la IOS de estos sistemas, un servicio de re-envío de eventos compatible con el estándar syslog.

Para poder utilizar esta característica en el hardware de electrónica de red como Cisco, sólo será necesario indicar un servidor de syslog (LOGSTORE) y una facility por la que realizar el re-envío de las tramas.

Por ejemplo, para los sistemas ASA de Cisco, y mediante el GUI de administración

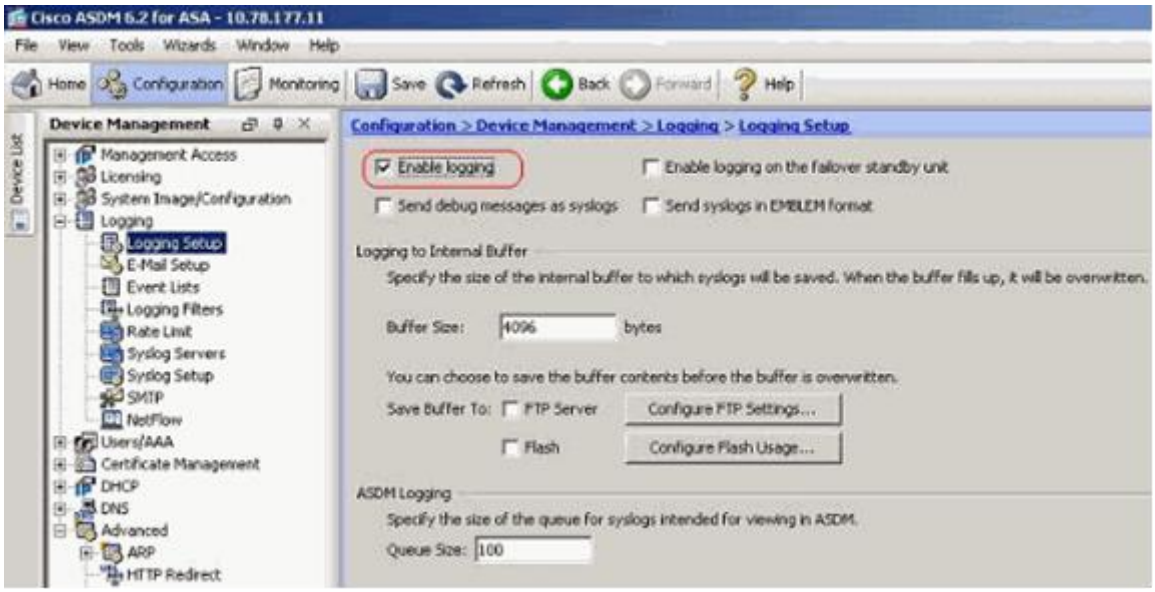


Ilustración 45. Configuración Routers CISCO (1).

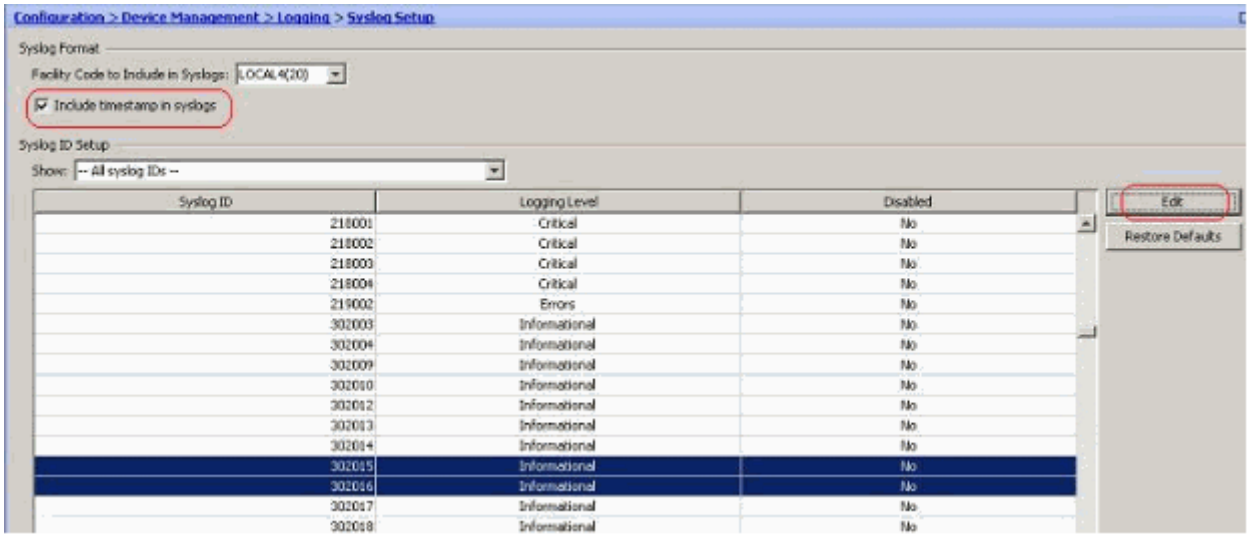


Ilustración 46. Configuración Routers CISCO (2).

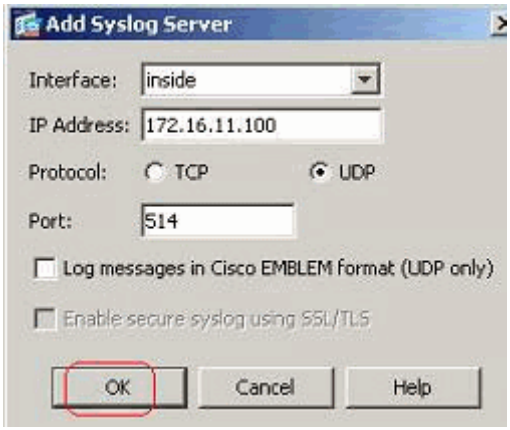


Ilustración 47. Configuración Routers CISCO (3).

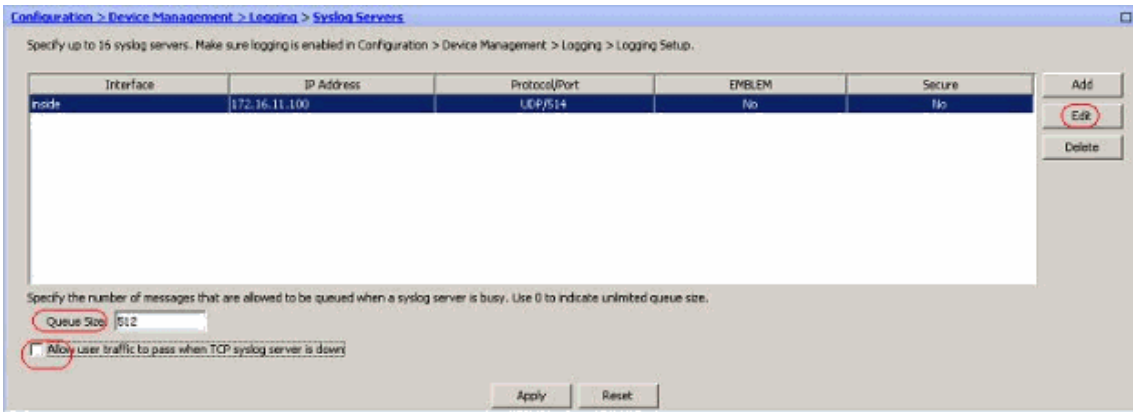


Ilustración 48. Configuración Routers CISCO (4).

Esta configuración también puede realizarse desde CLI:

```
!
logging enable
logging host inside LOGSTORE
logging permit-hostdown
! Local 6 facility has 22 id number
logging facility 22
...
```

Esta configuración de re-envío permitirá que LOGSTORE almacene los logs de estos clientes, en base a la plantilla genérica RSYSLOG:

```
[root@LOGSTORE ~]# ls -altr /var/log/vpn/vpnasa*.log
-rw------- 1 root root 15568947 Apr 18 16:29 /var/log/vpn/vpnasagc-exp-cisco-vpn-20130418.log
-rw------- 1 root root 24624591 Apr 18 16:29 /var/log/vpn/vpnasatf-exp-cisco-vpn-20130418.log
```

Estos logs serán centralizados desde el propio sistema, mediante la tarea de log-centralizer ejecutada sobre el propio servidor LOGSTORE, en calidad de cliente.

8.4.4. CONFIGURACIÓN DE SERVICIOS ESPECÍFICOS

8.4.4.1. Instalación y configuración de recolección de eventos de CORREO

El software de servidor SMTP Postfix utiliza por defecto el logger syslog de los sistemas, por lo que no requiere configuración específica para utilizarlo.

Este servicio utiliza la facility MAIL.

8.4.4.2. Instalación y configuración de recolección de eventos de SSH

El software de servidor OpenSSH utiliza por defecto el logger syslog de los sistemas, por lo que no requiere configuración específica para utilizarlo.

Este servicio utiliza la facility AUTHPRIV

8.4.4.3. Instalación y configuración de recolección de eventos de FTP

El software de servidor ProFTPd es compatible con el logger syslog de los sistemas, y requiere configuración específica para utilizarlo:

```
[proftpd.conf: fichero de configuración principal del servidor]
…
SyslogFacility          local1
…
```

8.4.4.4. Instalación y configuración de recolección de eventos de PROXY

El software de servidor Squid es compatible con el logger syslog de los sistemas, y requiere configuración específica para utilizarlo:

```
[squid.conf: fichero de configuración principal del servidor]
…

logformat       rsyslog %>a "%rm %ru HTTP/%rv" %>Hs %<st %Ss:%Sh
logfile_rotate  0
access_log      syslog:LOG_LOCAL2 rsyslog
…

[/etc/init.d/squid: script de inicio del demonio]
…
               $SQUID -l local2 -z -F 2>/dev/null
…
```

8.4.4.5. Instalación y configuración de recolección de eventos de MYSQL

El software de servidor MySQL Server es compatible con el logger syslog de los sistemas, y requiere configuración específica para utilizarlo:

```
[/etc/my.cnf: fichero de configuración del servidor MySQL Server]
…
[mysqld_safe]
        syslog
…
```

8.4.4.6. Instalación y configuración de recolección de eventos de Apache

El software de servidor Apache es compatible con el logger syslog de los sistemas, y requiere configuración específica para utilizarlo:

```
[/etc/httpd/conf/httpd.conf: fichero de configuración del servidor Apache]
…
ErrorLog syslog:local2
…
```

8.5. INSTALACIÓN Y CONFIGURACIÓN LOGCONSOLE

8.5.1. INSTALACIÓN Y CONFIGURACIÓN APACHE Y PHP

Desde el servicio de instalación de paquetería se instalará el software propio de la distribución Linux:

```
[root@LOGCONSOLE ~]# yum install php-ldap php-cli php php-devel php-common php-mysql php-pear php-pdo php-xml php-gd httpd httpd-devel httpd-manual mod_ssl
```

Una vez instalada la paquetería, se procede a configurar el servidor, prestableciendo el DocumentRoot (directorio raíz desde donde se servirán la consola web), y algunos otros parámetros (forzar la utilización de HTTPS, evitar la navegación por el sistema de ficheros, etc.):

```
[root@LOGCONSOLE ~]# vi /etc/httpd/conf/httpd.conf
…
#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
DocumentRoot "/var/www/html"
…
#
# Each directory to which Apache has access can be configured with respect
# to which services and features are allowed and/or disabled in that
# directory (and its subdirectories).
#
# First, we configure the "default" to be a very restrictive set of
# features.
#
<Directory />
    Options FollowSymLinks -Indexes
    AllowOverride None
        </Directory>
…
#
# HostnameLookups: Log the names of clients or just their IP addresses
# e.g., www.apache.org (on) or 204.62.129.132 (off).
# The default is off because it'd be overall better for the net if people
# had to knowingly turn this feature on, since enabling it means that
# each client request will result in AT LEAST one lookup request to the
# nameserver.
#
        HostnameLookups Off
```

```
#
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If this is not set to valid DNS name for your host, server-generated
# redirections will not work.  See also the UseCanonicalName directive.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
# You will have to access it by its address anyway, and this will make
# redirections work in a sensible way.
#
        ServerName logconsole:80
…
<IfModule mod_rewrite.c>
     RewriteEngine On
     RewriteCond %{HTTPS} off
     RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}
        </IfModule>
…
```

Finalmente se arranca el servidor:

```
[root@LOGCONSOLE ~]# /etc/init.d/httpd start
Starting httpd:                                            [  OK  ]
```

Y se deja habilitado como servicio de arranque por defecto:

```
[root@LOGCONSOLE etc]# chkconfig httpd on
[root@LOGCONSOLE ~]# chkconfig --list | grep httpd
httpd           0:off   1:off   2:on    3:on    4:on    5:on    6:off
```

8.5.1.1. Prueba de acceso

Para verificar el acceso se puede crear el siguiente fichero en el DocumentRoot del servidor:

```
[root@LOGCONSOLE ~]# cat /var/www/html/info.php
<?php
phpinfo();
?>
```

Y acceder a la URL del mismo: https://logconsole/info.php

Ilustración 49. Verificación Instalación PHP.

8.5.2. INSTALACIÓN Y CONFIGURACIÓN LOGANALYZER

Una vez descargado el software, sólo es necesario descomprimirlo y depositar la parte del código de la aplicación, en el DocumentRoot del servidor Apache.

```
[root@LOGCONSOLE ~]# wget http://download.adiscon.com/loganalyzer/loganalyzer-3.6.3.tar.gz
[root@LOGCONSOLE ~]# tar -xzf loganalyzer-3.6.3.tar.gz
[root@LOGCONSOLE ~]# mv loganalyzer-3.6.3/src /var/www/html/LogAnalyzer
```

Una vez depositado el código, se puede comprobar la carga accediendo mediante la URL específica del path: https://logconsole/LogAnalyzer

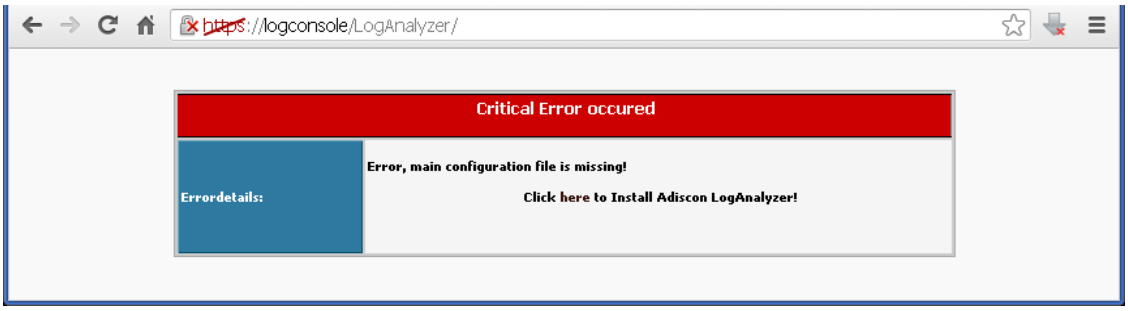


Ilustración 50. Configuración LogAnalyzer (1).

Para configurar el software podemos hacer uso del asistente gráfico disponible desde la URL https://logconsole/LogAnalyzer/install.php

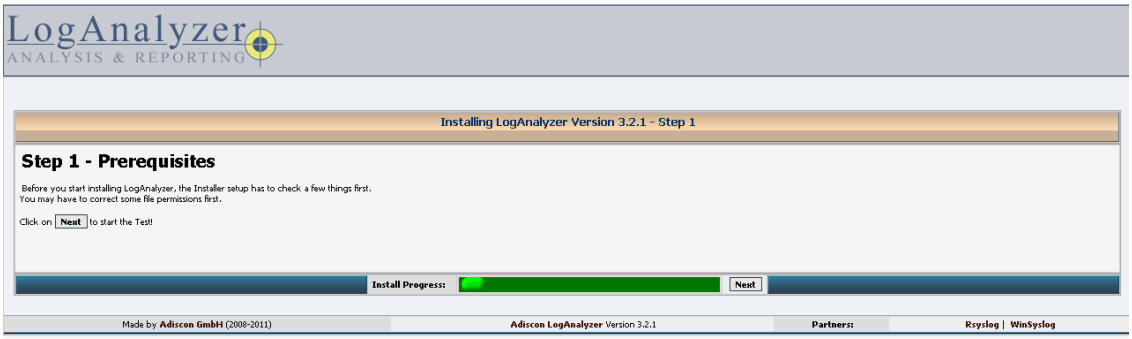


Ilustración 51. Configuración LogAnalyzer (2).

A través de este asistente podremos configurar parámetros básicos de la aplicación:

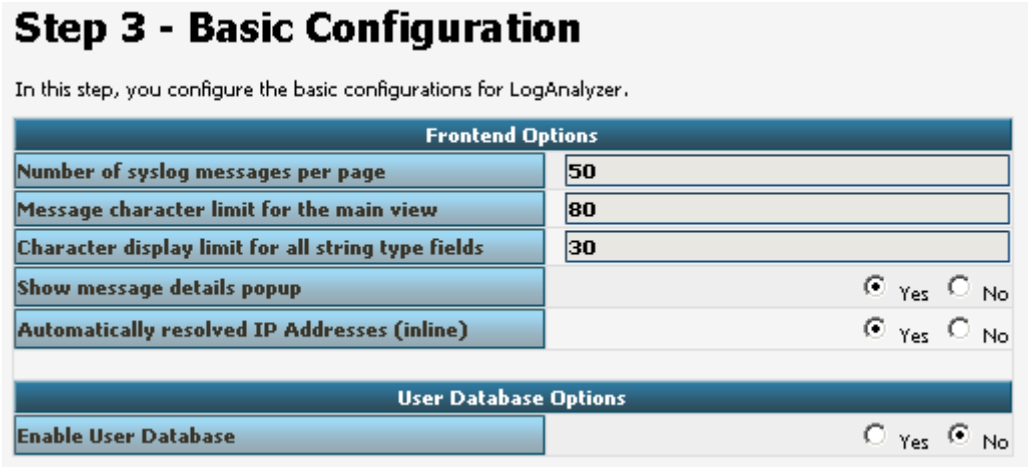


Ilustración 52. Configuración LogAnalyzer (3).

Y agregar un primer data source de acceso a los logs de BBDD:

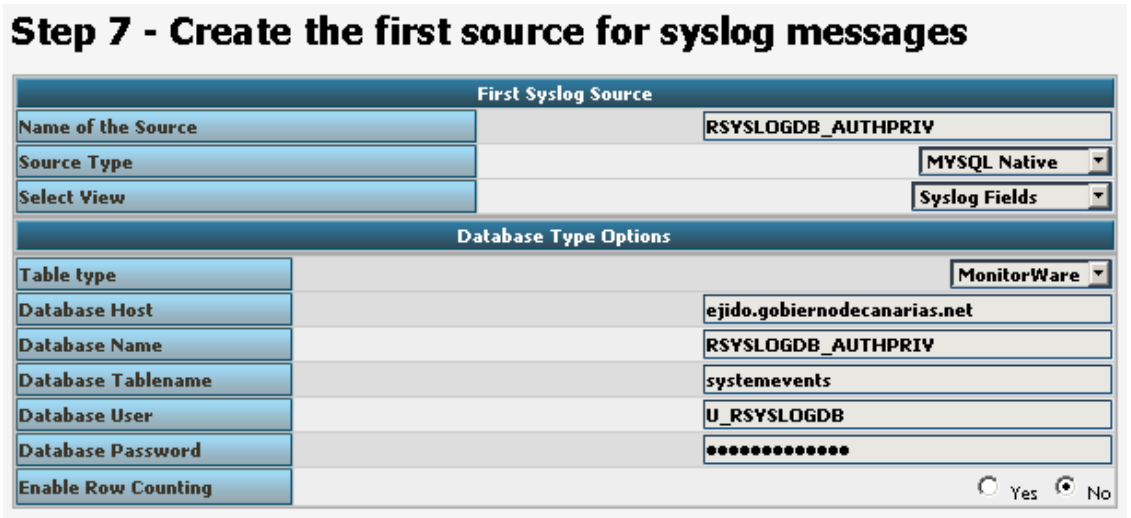


Ilustración 53. Configuración LogAnalyzer (4).

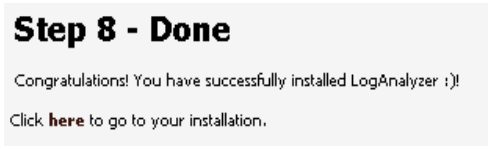


Ilustración 54. Configuración LogAnalyzer (4).

Además de este GUI, es posible y altamente recomendable editar directamente el fichero de configuración principal de la aplicación, de donde podremos utilizar el data source creado para configurar el resto:

```
[root@LOGCONSOLE ~]# vi /var/www/html/LogAnalyzer/config.php
…
$CFG['DefaultSourceID'] = 'Source11';

$CFG['Sources']['Source1']['ID'] = 'Source1';
$CFG['Sources']['Source1']['Name'] = '[PRE] ACCESO';
//$CFG['Sources']['Source1']['ViewID'] = 'SYSLOG';
$CFG['Sources']['Source1']['SourceType'] = SOURCE_DB;
$CFG['Sources']['Source1']['DBTableType'] = 'monitorware';
$CFG['Sources']['Source1']['DBType'] = DB_MYSQL;
$CFG['Sources']['Source1']['DBServer'] = 'ejido:3006';
$CFG['Sources']['Source1']['DBName'] = 'RSYSLOGDB_AUTHPRIV';
$CFG['Sources']['Source1']['DBUser'] = 'U_RSYSLOGDB';
$CFG['Sources']['Source1']['DBPassword'] = 'LOGDB_C_RSYSI';
$CFG['Sources']['Source1']['DBTableName'] = 'SystemEvents';
$CFG['Sources']['Source1']['DBEnableRowCounting'] = false;

$CFG['Sources']['Source11']['ID'] = 'Source11';
$CFG['Sources']['Source11']['Name'] = '[EXP] ACCESO';
$CFG['Sources']['Source11']['SourceType'] = SOURCE_DB;
$CFG['Sources']['Source11']['DBTableType'] = 'monitorware';
$CFG['Sources']['Source11']['DBType'] = DB_MYSQL;
$CFG['Sources']['Source11']['DBServer'] = 'BBDDEXP:3006';
$CFG['Sources']['Source11']['DBName'] = 'RSYSLOGDB_AUTHPRIV';
$CFG['Sources']['Source11']['DBUser'] = 'RSYSLOG_RO';
$CFG['Sources']['Source11']['DBPassword'] = 'CLASOLOLEESYSPRO';
$CFG['Sources']['Source11']['DBTableName'] = 'SystemEvents';
$CFG['Sources']['Source11']['DBEnableRowCounting'] = false;
…
```

En este punto será necesario crear cada uno de los data source disponibles en las BBDD de los entornos de PRE-explotación y producción. Una vez configurados todos los data sources disponibles, será posible acceder a la consola, y hacer uso de la interfaz, seleccionando aquel datasource que queramos auditar:

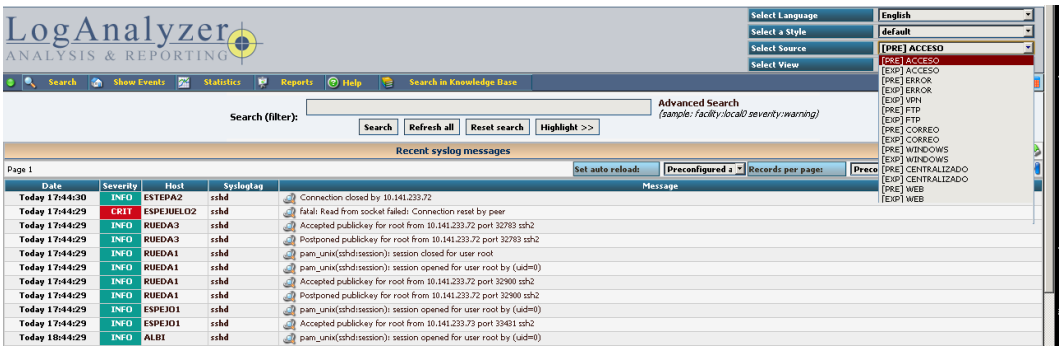


Ilustración 55. Configuración LogAnalyzer (5).

8.5.3. INSTALACIÓN Y CONFIGURACIÓN LOGREPORTERS

Para generar valor añadido a la solución de centralización, se han buscado distintas herramientas GNU y open sorce para crear una base de datos business intelligence sobre los servicios de la organización, para obtener valores como estadísticas de correos, de navegación, etc.

Entre reporters testados se encuentran:

8.5.3.1. postfix-logwatch-1.40.00

Permite obtener un report a través del tratamiento de los logs correo SMTP generado por el demonio Postfix. El software de instalación incluye un "Makefile" con lo que sólo debemos recompilar con:

```
[root@LOGCONSOLE ~]# tar -xzf postfix-logwatch-1.40.00.tgz
[root@LOGCONSOLE ~]# cd postfix-logwatch-1.40.00
[root@LOGCONSOLE postfix-logwatch-1.40.00]# make install-standalone
```

La instalación por defecto quedará ubicada en /usr/local/bin y /usr/local/etc. Para usar como un script de logwatch los ficheros "postfix-logwatch" y "postfix-logwatch.conf" deberán ser instalados en uno de los directorios conocidos del Logwatch. Para evitar sobrescribir los archivos de filtro Logwatch existentes, los archivos se pueden instalar en el directorio global de logwatch que típicamente es "/etc/logwatch". El Makefile incluido se puede utilizar para instalar los archivos, para ello sólo tenemos que recompilar con:

```
[root@LOGCONSOLE amavis-logwatch-1.51.02]# make install-logwatch
```

Para la elaboración periódica de los report, se ha configurado una tarea bajo el scheduler diario del sistema que a partir de los logs Postfix del día en curso:

```
[root@LOGCONSOLE ~]# crontab –l
…
# Generar stats diarias de correo
0 8 * * * [[ -x /root/mail-stats/dispatcher.sh ]] && /root/mail-stats/dispatcher.sh
…
[root@LOGCONSOLE ~]#
```

```
[root/mail-stats/dispatcher.sh]
…
PARSER=/usr/bin/postfix-logwatch
LOG_FILE=${LOGSTORE_BASE_DIR}/${YEAR}/${MONTH}/${DAY}/${FILE_NAME}
TARGET_FILE=/var/log-stats/${YEAR}/${MONTH}/${DAY}/Servidor_${SERVER}_[${YEAR}-${MONTH}-${DAY}].txt
…
cat ${LOG_FILE} | ${PARSER} --nodetail > ${TARGET_FILE}
```

Esto genera un fichero de informe que se almacena en disco:

```
[root@LOGCONSOLE ~]# ls -altr /var/log-stats/2013/04/18/Servidor_correo*
-rw-r--r-- 1 root root 2461 Apr 19 08:00 /var/log-stats/2013/04/18/Servidor_correo1_[2013-04-18].txt
-rw-r--r-- 1 root root 2559 Apr 19 08:00 /var/log-stats/2013/04/18/Servidor_correo2_[2013-04-18].txt
-rw-r--r-- 1 root root 2518 Apr 19 08:00 /var/log-stats/2013/04/18/Servidor_correo3_[2013-04-18].txt
-rw-r--r-- 1 root root 2482 Apr 19 08:00 /var/log-stats/2013/04/18/Servidor_correo4_[2013-04-18].txt
```

Y que también es llevado a BBDD durante la generación, a partir de la herramienta de sistema "logger":

```
[root/mail-stats/dispatcher.sh]
…
cat ${TARGET_FILE} | /bin/logger -t ${HOST}-mail-stats -p local7.debug –i
…
```

Estos reports pueden ser consultados mediante la herramienta de consola diseñada para ello, de tal modo que no sólo se recabe la información propia del report, sino que además se grafican en el tiempo, aquellos parámetros más interesantes, utilizando para ello la API de Google Chart Tools:

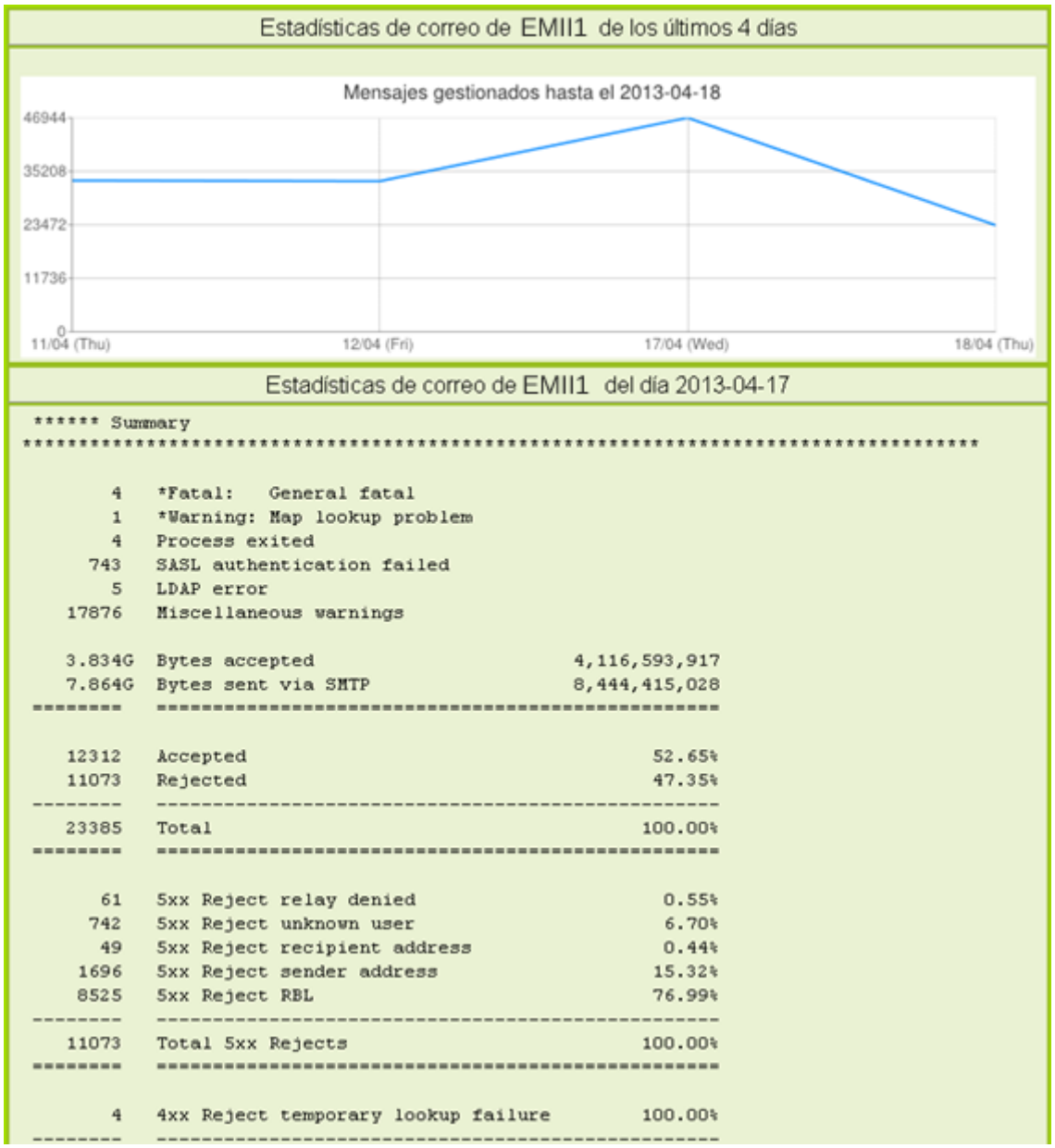


Ilustración 56. Report postfix-logwatch integrado con Google Chart Tools.

8.5.3.2. amavis-logwatch-1.51.02

Permite obtener un report a través del tratamiento de los logs de filtrado antivirus/antispam de correo generado por el demonio AMaViS-new. La instalación es prácticamente idéntica al postfix-logwatch, con la salvedad de que los archivos de logwatch son “amavis-logwatch” y “amavis-logwatch.conf”:

```
[root@LOGCONSOLE ~]# tar –xzf amavis-logwatch-1.51.02.tgz
[root@LOGCONSOLE ~]# cd amavis-logwatch-1.51.02
[root@LOGCONSOLE amavis-logwatch-1.51.02]# make install-standalone
```

Para la elaboración periódica de los report, se ha configurado una tarea bajo el scheduler diario del sistema que a partir de los logs AMaViS del día en curso, genera un fichero de

informe que se almacena en disco y en BBDD, siguiendo el mismo esquema usado con postfix-logwatch y que pueden ser consultados mediante la herramienta de consola diseñada para ello:

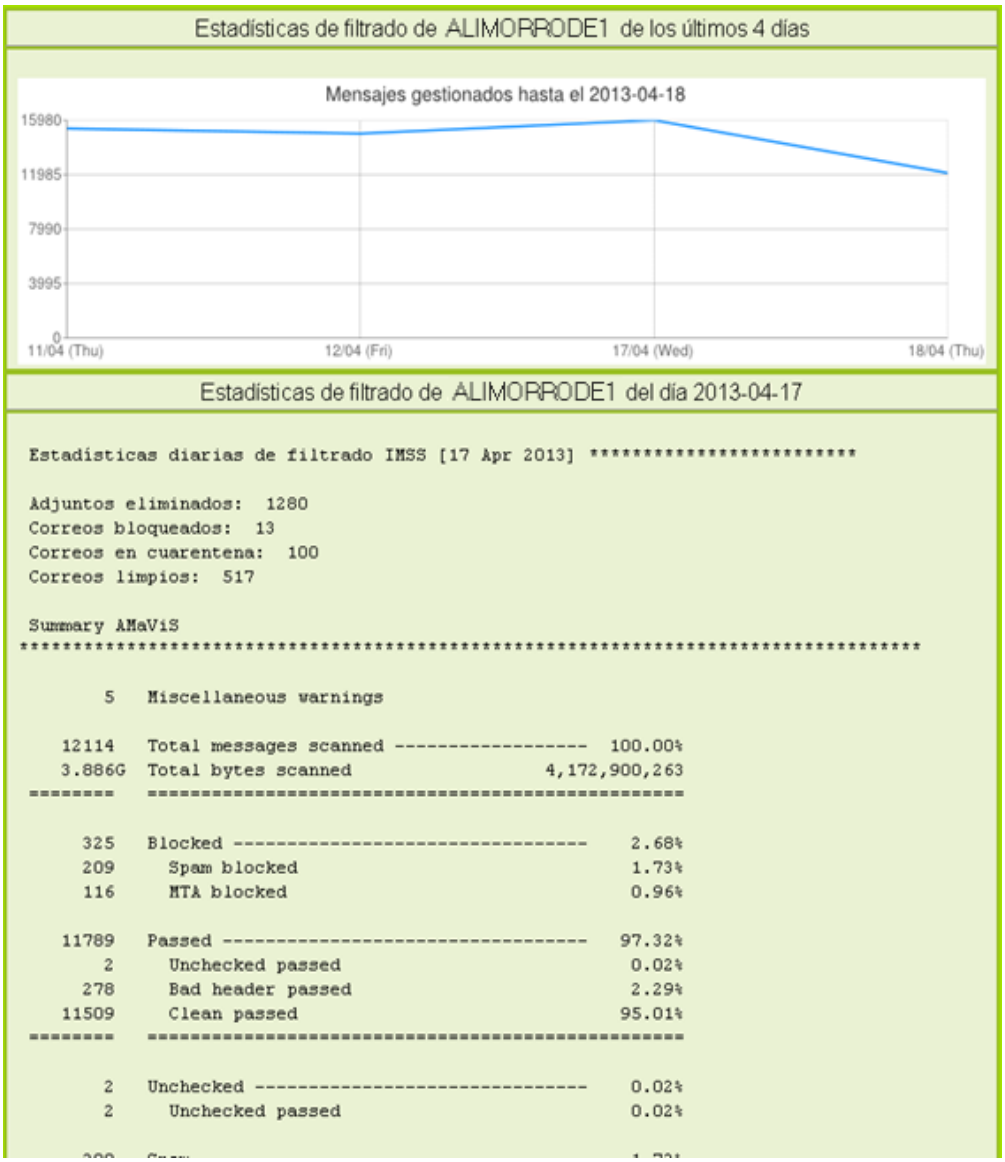


Ilustración 57. Report amavis-logwatch integrado con Google Chart Tools.

8.5.4. INSTALACIÓN Y CONFIGURACIÓN WEBALIZER

La herramienta se instala desde el propio repositorio de la paquetería de la distribución:

```
[root@LOGCONSOLE ~]# yum install webalizer
```

Una vez instalada, la herramienta será capaz de generar un historial estadístico sobre servicios como Squid proxy y ProFTPd, a partir de los logs centralizados en el sistema, y disponibles en LOGCONSOLE.

Para la elaboración periódica de los report, se han configurado tareas bajo el scheduler diario del sistema:

```
[root@LOGCONSOLE ~]# crontab –l
…
# Generar stats diarias e historico de accesos FTP
30 7 * * * [[ -x /root/ftp-stats/dispatcher.sh ]] && /root/ftp-stats/dispatcher.sh
# Generar stats diarias e historico de accesos Proxy
40 7 * * * [[ -x /root/proxy-stats/dispatcher.sh ]] && /root/proxy-stats/dispatcher.sh
…
[root@LOGCONSOLE ~]#
```

Que a partir de los logs de PRoFTPd y Squid del día en curso, añade datos estadísticos de uso y acceso al historial de cada servicio:

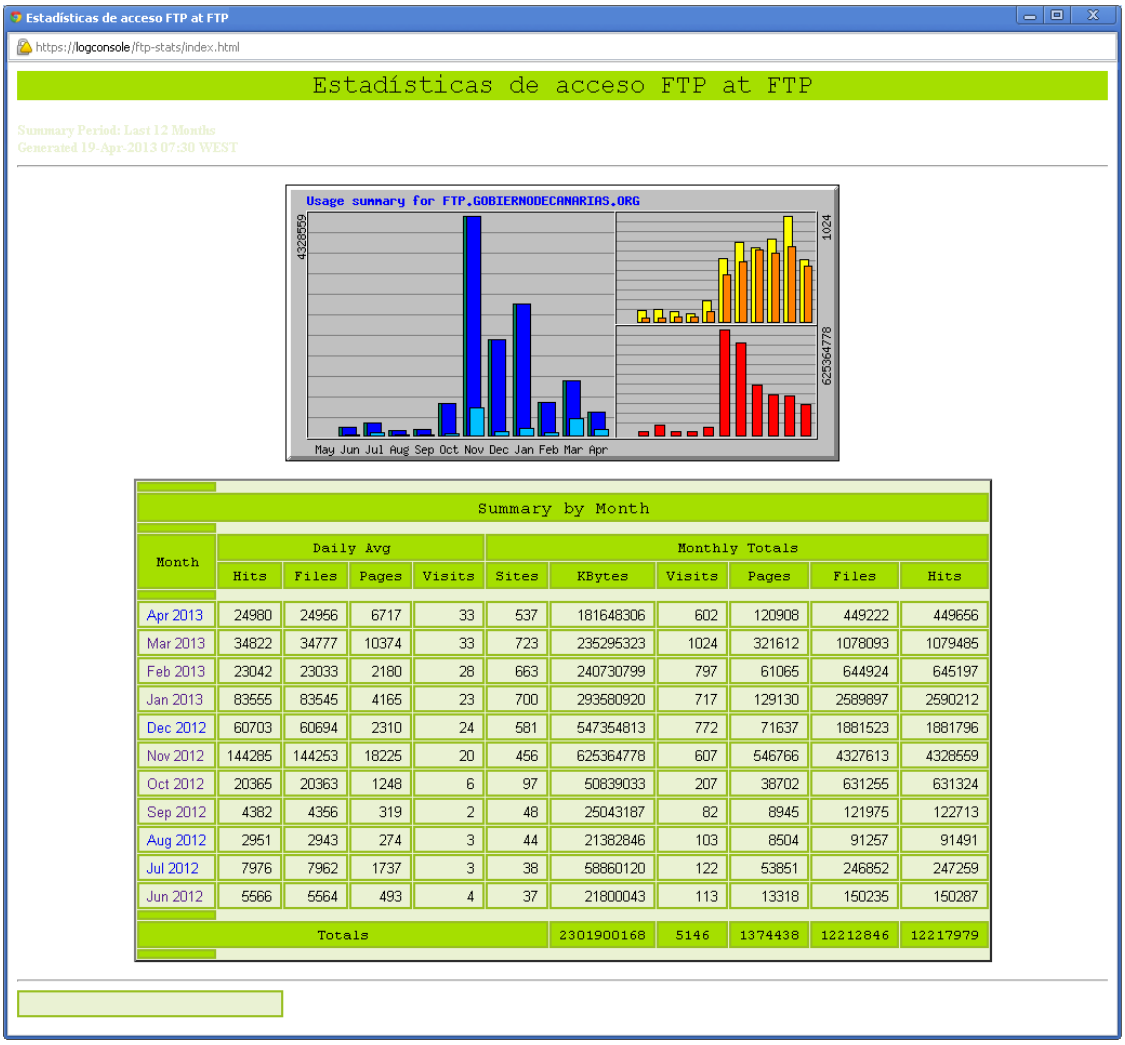
```
[/root/ftp-stats/dispatcher.sh]
…
PARSER=/usr/bin/webalizer
LOG_FILE=${LOGSTORE_BASE_DIR}/${YEAR}/${MONTH}/${DAY}/${FILE_NAME}
TARGET_FILE=/var/log-stats/${YEAR}/${MONTH}/${DAY}/Servidor_${SERVER}_[${YEAR}-${MONTH}-${DAY}].txt
…
cp ${LOGFILE}/root/ftp-stats/tmp/xferlog
${PARSER} -c /root/ftp-stats/webalizer-ftp.conf
```

```
[/root/proxy-stats/dispatcher.sh]
…
PARSER=/usr/bin/webalizer
LOG_FILE=${LOGSTORE_BASE_DIR}/${YEAR}/${MONTH}/${DAY}/${FILE_NAME}
TARGET_FILE=/var/log-stats/${YEAR}/${MONTH}/${DAY}/Servidor_${SERVER}_[${YEAR}-${MONTH}-${DAY}].txt
…
cp ${LOGFILE}/root/proxy-stats/tmp/xferlog
${PARSER} -c /root/proxy-stats/webalizer-proxy.conf
```

```
[/root/ftp-stats/webalizer-ftp.conf: fichero de configuración webalyzer para FTP]
LogFile        /root/ftp-stats/tmp/xferlog
LogType         ftp
OutputDir      /var/www/html/ftp-stats/
HistoryName     /root/ftp-stats/webalizer-ftp.hist
Incremental     yes
IncrementalName /root/ftp-stats/webalizer-ftp.current
ReportTitle Estad&iacute;sticas de acceso FTP at
HostName       FTP
HTMLExtension  html
PageType        htm*
PageType        php
PageType        jsp
PageType        asp
UseHTTPS      yes
DNSCache        /var/lib/webalizer/dns_cache.db
DNSChildren     10
HTMLHead <title>TFC UOC</title>
HTMLHead <link href="/css/webalizer.css" rel="stylesheet" type="text/css">
HTMLBody <BODY BGCOLOR="#FFFFFF">
Quiet           yes
FoldSeqErr      yes
IgnoreHist      no
CountryGraph    no
DailyGraph      yes
DailyStats      yes
HourlyGraph     yes
HourlyStats     yes
GraphLegend     no
GraphLines 10
TopSites        0
TopKSites       0
TopURLs         0
TopKURLs        0
TopReferrers    0
TopAgents       0
TopCountries    0
TopEntry        0
TopExit         0
TopSearch       0
TopUsers        100
AllSites        no
AllURLs no
AllReferrers    no
AllAgents       no
AllSearchStr    no
AllUsers        yes
GroupURL       /home/*          Por usuario
HideAllSites    yes
SearchEngine    yahoo.com       p=
SearchEngine    altavista.com   q=
SearchEngine    google.com      q=
SearchEngine    eureka.com      q=
SearchEngine    lycos.com       query=
SearchEngine    hotbot.com      MT=
SearchEngine    msn.com         MT=
SearchEngine    infoseek.com    qt=
SearchEngine    webcrawler      searchText=
SearchEngine    excite          search=
SearchEngine    netscape.com    search=
SearchEngine    mamma.com       query=
SearchEngine    alltheweb.com   query=
SearchEngine    northernlight.com  qr=
```

```
[/root/proxy-stats/webalizer-proxy.conf: fichero de configuración webalyzer para Squid proxy]
LogFile        /root/proxy-stats/tmp/access_log
LogType         squid
OutputDir      /var/www/html/proxy-stats/
HistoryName     /root/proxy-stats/webalizer-proxy.hist
Incremental     yes
IncrementalName /root/proxy-stats/webalizer-proxy.current
ReportTitle Estad&iacute;sticas de acceso Proxy en
HostName       PROXY
HTMLExtension  html
PageType        htm*
PageType        php
PageType        jsp
PageType        asp
UseHTTPS      yes
DNSCache        /var/lib/webalizer/dns_cache.db
DNSChildren     10
HTMLHead <title>TFC UOC</title>
HTMLHead <link href="/css/webalizer.css" rel="stylesheet" type="text/css">
HTMLBody <BODY BGCOLOR="#FFFFFF">
Quiet           yes
FoldSeqErr      yes
IgnoreHist      no
CountryGraph    no
DailyGraph      yes
DailyStats      yes
HourlyGraph     yes
HourlyStats     yes
GraphLegend     yes
GraphLines 10
TopSites        20
TopKSites       20
TopURLs         10
TopKURLs        10
TopReferrers    5
TopAgents       5
TopCountries    0
TopEntry        0
TopExit         0
TopSearch       0
TopUsers        0
AllSites        yes
AllURLs yes
AllReferrers    yes
AllAgents       yes
AllSearchStr    no
AllUsers        yes
HideAllSites    no
SearchEngine    yahoo.com       p=
SearchEngine    altavista.com   q=
SearchEngine    google.com      q=
SearchEngine    eureka.com      q=
SearchEngine    lycos.com       query=
SearchEngine    hotbot.com      MT=
SearchEngine    msn.com         MT=
SearchEngine    infoseek.com    qt=
SearchEngine    webcrawler      searchText=
SearchEngine    excite          search=
SearchEngine    netscape.com    search=
SearchEngine    mamma.com       query=
SearchEngine    alltheweb.com   query=
SearchEngine    northernlight.com  qr=
```

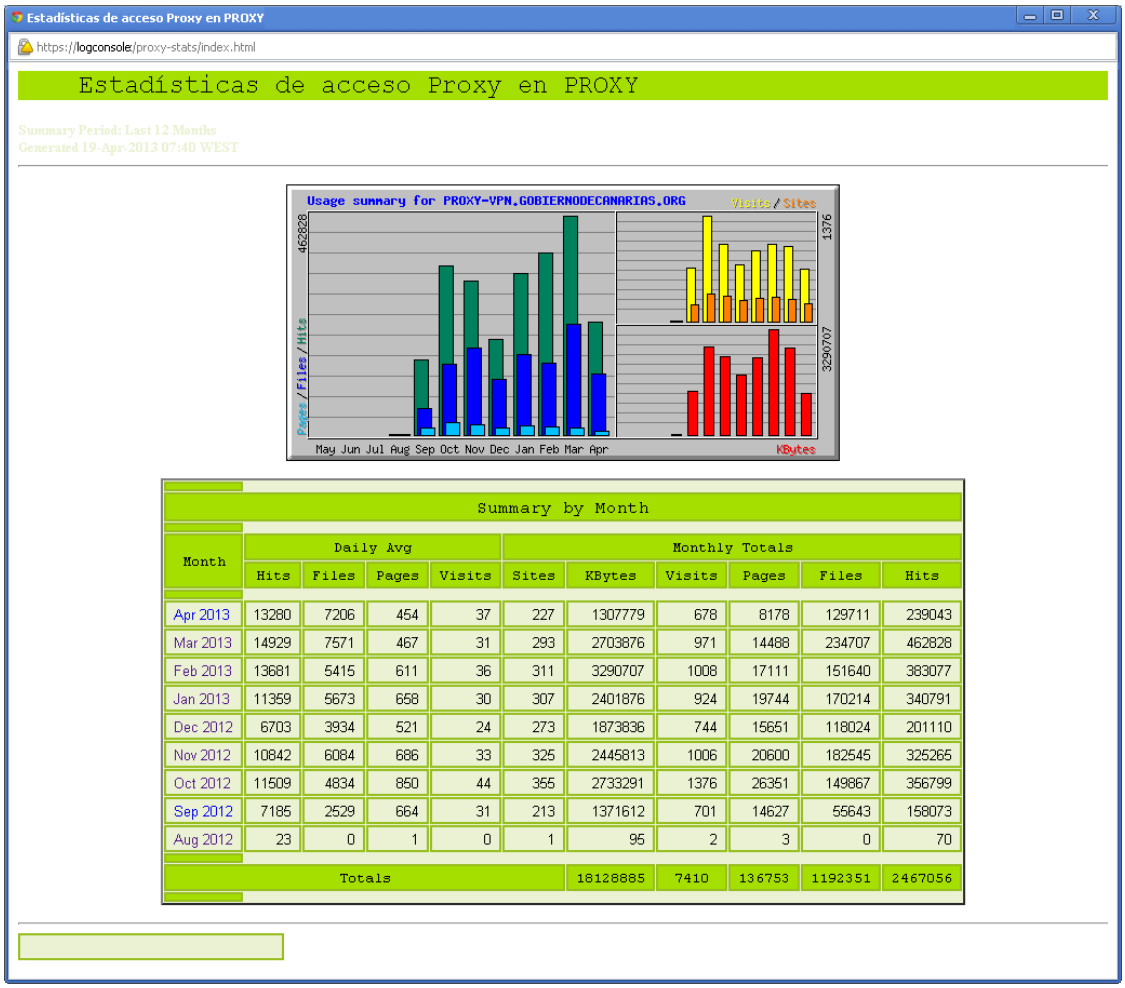
Este histórico de datos estadísticos puede ser consultado mediante la publicación del informe HTML que se genera por cada servicio (FTP y proxy), de tal forma que mediante su depósito en el DocumentRoot del servidor Apache, serán accesibles vía web:



Summary by Month

Month	Daily Avg				Monthly Totals					
	Hits	Files	Pages	Visits	Sites	KBytes	Visits	Pages	Files	Hits
Apr 2013	24980	24956	6717	33	537	181648306	602	120908	449222	449656
Mar 2013	34822	34777	10374	33	723	235295323	1024	321612	1078093	1079485
Feb 2013	23042	23033	2180	28	663	240730799	797	61065	644924	645197
Jan 2013	83555	83545	4165	23	700	293580920	717	129130	2589897	2590212
Dec 2012	60703	60694	2310	24	581	547354813	772	71637	1881523	1881796
Nov 2012	144285	144253	18225	20	456	625364778	607	546766	4327613	4328559
Oct 2012	20365	20363	1248	6	97	50839033	207	38702	631255	631324
Sep 2012	4382	4356	319	2	48	25043187	82	8945	121975	122713
Aug 2012	2951	2943	274	3	44	21382846	103	8504	91257	91491
Jul 2012	7976	7962	1737	3	38	58860120	122	53851	246852	247259
Jun 2012	5566	5564	493	4	37	21800043	113	13318	150235	150287
Totals						2301900168	5146	1374438	12212846	12217979

Ilustración 58. WebAlizer, informe histórico de acceso FTP.



Summary by Month

Month	Daily Avg				Monthly Totals					
	Hits	Files	Pages	Visits	Sites	KBytes	Visits	Pages	Files	Hits
Apr 2013	13280	7206	454	37	227	1307779	678	8178	129711	239043
Mar 2013	14929	7571	467	31	293	2703876	971	14488	234707	462828
Feb 2013	13681	5415	611	36	311	3290707	1008	17111	151640	383077
Jan 2013	11359	5673	658	30	307	2401876	924	19744	170214	340791
Dec 2012	6703	3934	521	24	273	1873836	744	15651	118024	201110
Nov 2012	10842	6084	686	33	325	2445813	1006	20600	182545	325265
Oct 2012	11509	4834	850	44	355	2733291	1376	26351	149867	356799
Sep 2012	7185	2529	664	31	213	1371612	701	14627	55643	158073
Aug 2012	23	0	1	0	1	95	2	3	0	70
Totals						18128885	7410	136753	1192351	2467056

Ilustración 59. WebAlizer, informe histórico de acceso PROXY.

8.5.5. INSTALACIÓN Y CONFIGURACIÓN PHPFILETREE

Una vez descargado el software, sólo es necesario descomprimirlo y depositarlo en el DocumentRoot del servidor Apache.

```
[root@LOGCONSOLE ~]# tar -xzf phpFileTree-1.0.zip
[root@LOGCONSOLE ~]# mv phpFileTree /var/www/html/file-browser
```

Por defecto la aplicación está concebida para realizar barridos recursivos mediante backtracking sobre el sistema de ficheros que se especifique. Esto bajo un sistema de ficheros voluminoso puede resultar excesivo, de cara a que el número de entradas en un sistema de ficheros de almacenamiento de logs puede tener miles de entradas. Para evitar este comportamiento, se modifica la herramienta para hacer podas por nivel de recursividad, para evitar así de esta forma, que el sistema se sature recorriendo todos los niveles de directorio.

Una vez implementada la funcionalidad de poda, se configuran los estilos a utilizar y se indica el directorio base sobre el que ejercer la exploración:

```
[root@LOGCONSOLE file-browser]# vi /var/www/html/file-browser/file-browser.php

<?php
include("./php_file_tree.php");
$logstore_directory = '/logstore/';
echo php_file_tree($logstore_directory, "window.location('#dir=[link]');");
?>

:wq
```

Para poder acceder a la herramienta sólo es necesario ir a la URL de publicación, mediante cualquier browser de navegación web: https://logconsole/file-browser/file-browser.php

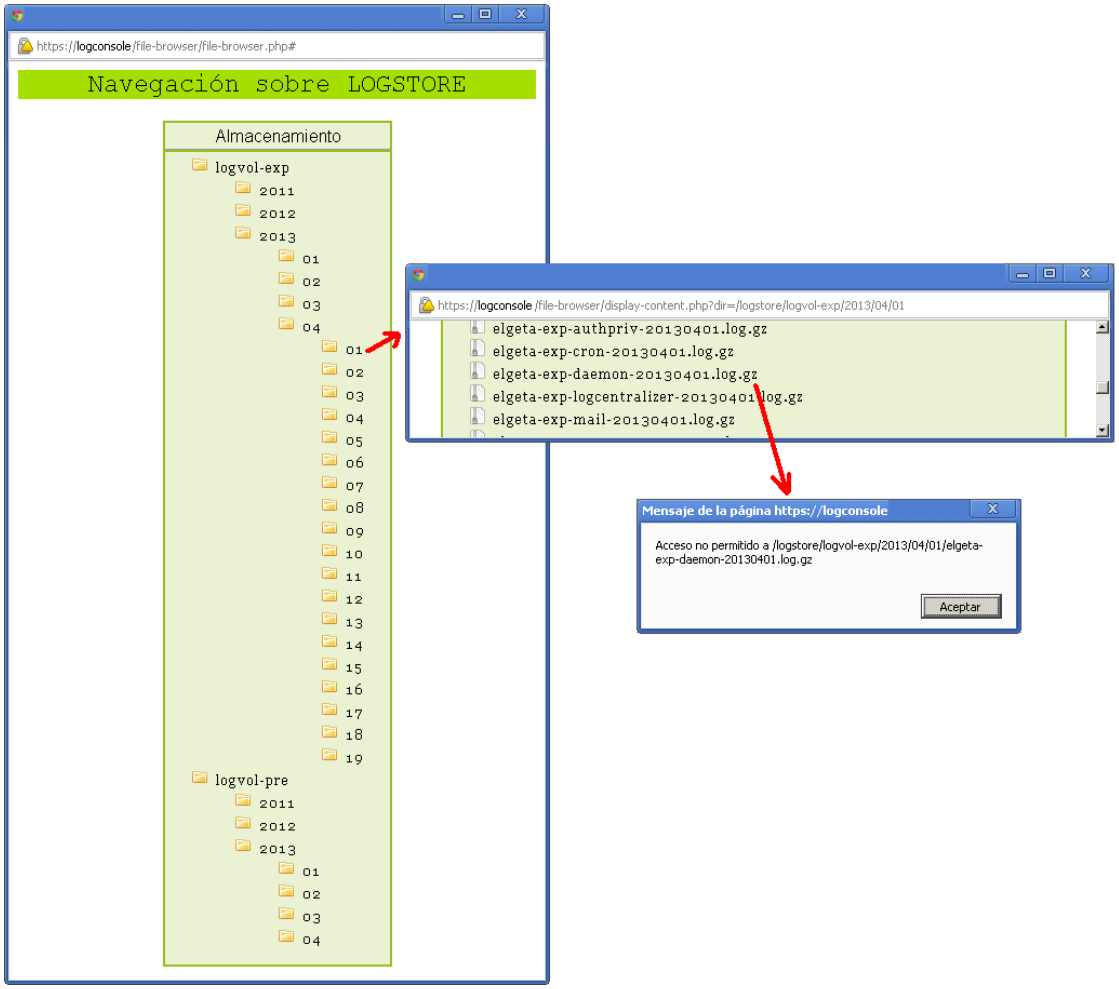


Ilustración 60. Navegación del LOGSTORE con PHPFILETREE.

8.5.6. INSTALACIÓN Y CONFIGURACIÓN JQUERY

Una vez descargado el software, sólo es necesario descomprimirlo y depositarlo en la carpeta común de JavaScript a usar desde DocumentRoot del servidor Apache:

```
[root@LOGCONSOLE ~]# ls -altr /var/www/html/js/jquery*
-rw-r--r-- 1 root root 238159 Apr 12  2013 /var/www/html/js/jquery-1.6.4.js
lrwxrwxrwx 1 root root     32 Apr 12  2013 /var/www/html/js/jquery.js -> /var/www/html/js/jquery-1.6.4.js
```

Desde esta ubicación, y haciedo referencia a ella desde los htmls que se generen, será posible utilizar todas las posibilidades y herramientas que ofrece:

```
[root@LOGCONSOLE ~]# vi /var/www/html/prueba1.php
<?php

echo “
<html>
<head>
<script type='text/javascript' src='/js/jquery.js'></script>
<script type='text/javascript'>
  $(document).ready(function(){
   $('#page_effect').fadeIn(1500);
  });
</script>
</head>

<body bgcolor='#ffffff'>
 <div id='page_effect' style='display: none;'>
  <h1>PRUEBA</h1>
 </div>
</body>
</html>
";

?>

:wq
```

Pudiéndose ver el resultado mediante cualquier navegador web a tarvés de la URL https://logconsole/prueba1.php

8.5.7. INSTALACIÓN Y CONFIGURACIÓN TINTBOX2

Una vez descargado el software, sólo es necesario descomprimirlo y depositar en la carpeta común de JavaScript del DocumentRoot la parte de api, y sobre la carpeta común de estilos CSS del DocumentRoot, su hoja de estilos específica:

```
[root@LOGCONSOLE ~]# ls -altr /var/www/html/js/tinybox.js
-rw-r--r-- 1 root root 5482 Apr 12 12:37 /var/www/html/js/tinybox.js
[root@LOGCONSOLE ~]# ls -altr /var/www/html/css/tinybox.css
-rw-r--r-- 1 root root 1968 Apr 12 11:15 /var/www/html/css/tinybox.css
```

Desde esta ubicación, y haciedo referencia a ella desde los htmls que se generen, será posible utilizar todas las posibilidades y herramientas que ofrece:

```
[root@LOGCONSOLE ~]# vi /var/www/html/prueba2.php
<?php

echo “
<html>
<head>
<link rel='stylesheet' href='/css/tinybox.css' type='text/css'>
<script type='text/javascript' src='/js/tinybox.js'></script>
</head>

<body bgcolor='#ffffff'>
<script>TINY.box.show({html:'Una                                                                                    ventana
emergente',animate:false,close:false,mask:false,boxid:'success',autohide:2,top:0,left:200})</script>
</body>
</html>
";

?>

:wq
```

Pudiéndose ver el resultado mediante cualquier navegador web a tarvés de la URL https://logconsole/prueba2.php

8.5.8. INSTALACIÓN Y CONFIGURACIÓN GOOGLE CHART

Una vez descargado el software, sólo es necesario descomprimirlo y depositarlo en la carpeta común de librerías PHP a usar desde DocumentRoot del servidor Apache:

```
[root@LOGCONSOLE ~]# ls -altr /var/www/html/include/googlecharts.class.php
-rw-r--r-- 1 root root 14214 Apr 11 11:55 /var/www/html/include/googlecharts.class.php
```

Desde esta ubicación, y haciedo referencia a ella desde los htmls que se generen, será posible utilizar la clase googleChart:

```
[root@LOGCONSOLE ~]# vi /var/www/html/prueba3.php
<?php
include_once ('./include/googlecharts.class.php');

$data=array('4,6,21,7,1,6,17,5,2,1,7,9');
$prueba=new googleChart($data);
$prueba->draw();
?>

:wq
```

Pudiéndose ver el resultado mediante cualquier navegador web a tarvés de la URL https://logconsole/prueba3.php

8.6. CONSOLA UNIFICADA

Para el acceso a todas las herramientas se elabora una consola web unificada.

Esta sirve de punto común de acceso a todas las herramientas y utilidades engranadas en el sistema, permitiendo con ello un cómodo acceso a toda la información. La consola se ha desarrollado en su totalidad con PHP y AJAX (vía JQuery y TinyBox2). Para el diseño del interfaz se han seguido dos criterios fundamentales:

- Sensillez: no nos encontramos ante un proyecto de desarrollo web sino que usamos las facilidades web para unificar el acceso a las diferentes herramientas. Así, la definición de la consola web básicamente esta dividia en una cabecera y un frame de integración de aplicaciones. La cabecera acoge todas las llamadas contextuales a las diferentes herramientas que son lanzadas en el frame de aplicación y/o ventanas emergentes.
- Modularidad: para garantizar el crecimiento y la integración de futuras funcionalidades.

Veremos el uso de la consola web unificada con más profundidad en el apartado de pruebas de la plataforma.

9. PRUEBAS FUNCIONALES

Para comprobar la robustez del sistema y con el uso de un servidor de acceso de consola mediante de clave pública RSA (como herramienta de uso trasversal para la organización), se despliegan los distintos clientes de centralización sobre todos los hosts Linux RHEL5 o superior de la organización, lo que permite hacer un despliegue veloz sobre este tipo de servidores:

```
[root@RSYSLOG_DEPLOY]# sh deploy_host_exp.sh
Falta nombre de servidor.

[root@dRSYSLOG_DEPLOY]# sh deploy_host_exp.sh ELGETA
Backing-up rsyslog at server ELA
Copying new configuration to server ${SERVER}
Making spool directory /var/spool/rsyslog
Stoping syslog service at ELA
Reinitializing RSYSLOG in server ELA

Activating log-centralizer at server ELA
Activating log-expirer at server ELA
Disabling syslog rotate.d conf at server ELA
Deleting old messages files at ELA

All tasks completed.

[root@RSYSLOG_DEPLOY]#
```

Para la granja de servidores Windows se crea un paquete MSI que despliega el cliente NTSyslog y que instala en el registro la configuración específica del mismo.

Finalmente para la electrónica de red se pre-configura mediante el gestor de configuraciones centralizado de la organización, todas las directivas necesarias para habilitar el re-envío de eventos syslog al sistema, y se despliega de forma exitosa.

9.1. CONSOLA DE GESTIÓN

La consola de gestión es un desarrollo que aglutina bajo un mismo cuadro de mando, todas aquellos aspectos relativos a la monitorización activa y estadística de las herramientas integradas al sistema de centralización de logs, de tal forma que sirva como factoría de datos business intelligence de la organización.

9.1.1. ACCESO

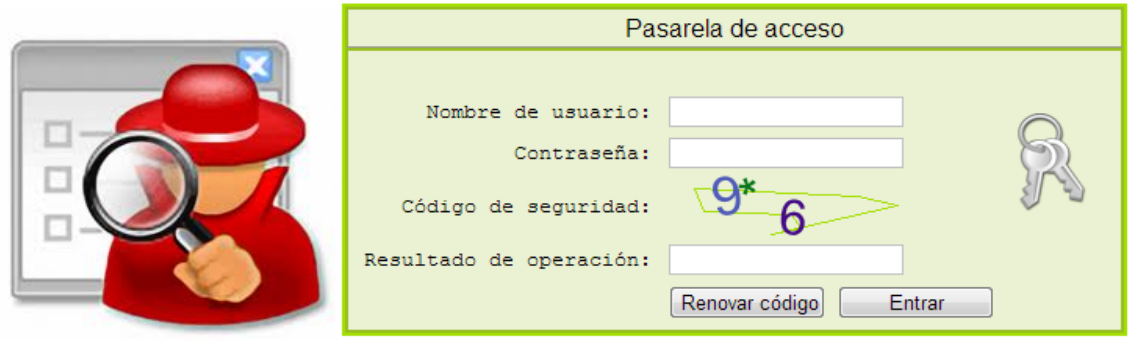


Ilustración 61. Acceso a la Consola.

Como cualquier herramienta que ofrezca información de negocio, el acceso a la consola pasa por un obligatorio inicio de sesión, al que le ha dotado de algunas características importantes para establecer los medios de control necesarios para garantizar que la accesibilidad a esta no sea indebida. Para ello se establece varias medidas de control y seguridad:

- Control de sesión de usuarios basado en PHP Sessions
- Utilización de un directorio LDAP (como por ejemplo OpenLDAP o Active Directory) para autenticar a los usuarios.
- Permisos de acceso por aplicación: para maximizar el sistema de control, también se establece granularmente por aplicación el acceso de los usuarios:

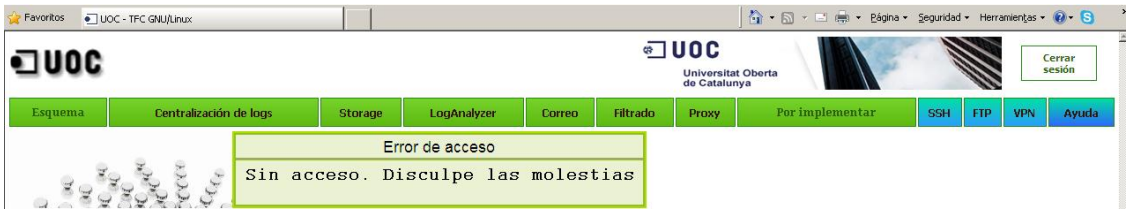


Ilustración 62. Consola, permisos por Aplicación.

- Sistema de autenticación con imagen anti-robot (sistema CAPTCHA).
- Canal de acceso web cifrado vía HTTPS (SSL sobre HTTP).

- Logging completo de sesiones, para la trazabilidad del acceso:

```
…
Tue, 07 May 2013 10:54:18 +0000 Info:   No session initilized from require auth access
Tue, 07 May 2013 10:54:31 +0000 Info:   BIND satisfactorio del usuario ivan
Tue, 07 May 2013 10:54:31 +0000 Info:   [ivan] Comprobando pertenencia a projectmanagement-group [Num of
members: 5]
Tue, 07 May 2013 10:54:31 +0000 Info:   [ivan] Comprobando pertenencia a systems-group [Num of members: 2]
Tue, 07 May 2013 10:54:31 +0000 Info:   [ivan] Comprobando pertenencia a sysapps-group [Num of members: 2]
Tue, 07 May 2013 10:54:31 +0000 Info:   [ivan] Comprobando pertenencia a micro-group [Num of members: 5]
Tue, 07 May 2013 10:54:31 +0000 Info:   [ivan] Asignando grupo de pertenencia micro-group
Tue, 07 May 2013 10:54:31 +0000 Info:   [ivan] Comprobando pertenencia a networks-group [Num of members:
1]
Tue, 07 May 2013 10:54:31 +0000 Info:   Acceso satisfactorio del usuario ivan al sistema
Tue, 07 May 2013 10:55:47 +0000 Info:   [Usuario ivan] - Sin acceso a /tfc/logvol-monitor/logvol-
monitor.php
Tue, 07 May 2013 10:57:40 +0000 Info:   [Usuario ivan] - Acceso a /tfc/log-
centralizer/today_centralization.php
…
```

9.1.2. ORGANIZACIÓN DE LA CONSOLA

Salvado el nivel de acceso a la aplicación y primando la sencillez y modularidad que se ha buscado para la consola, mediante PHP y el uso de hojas de estilos se ha implementa una interfaz distribuida entre los siguientes frames:

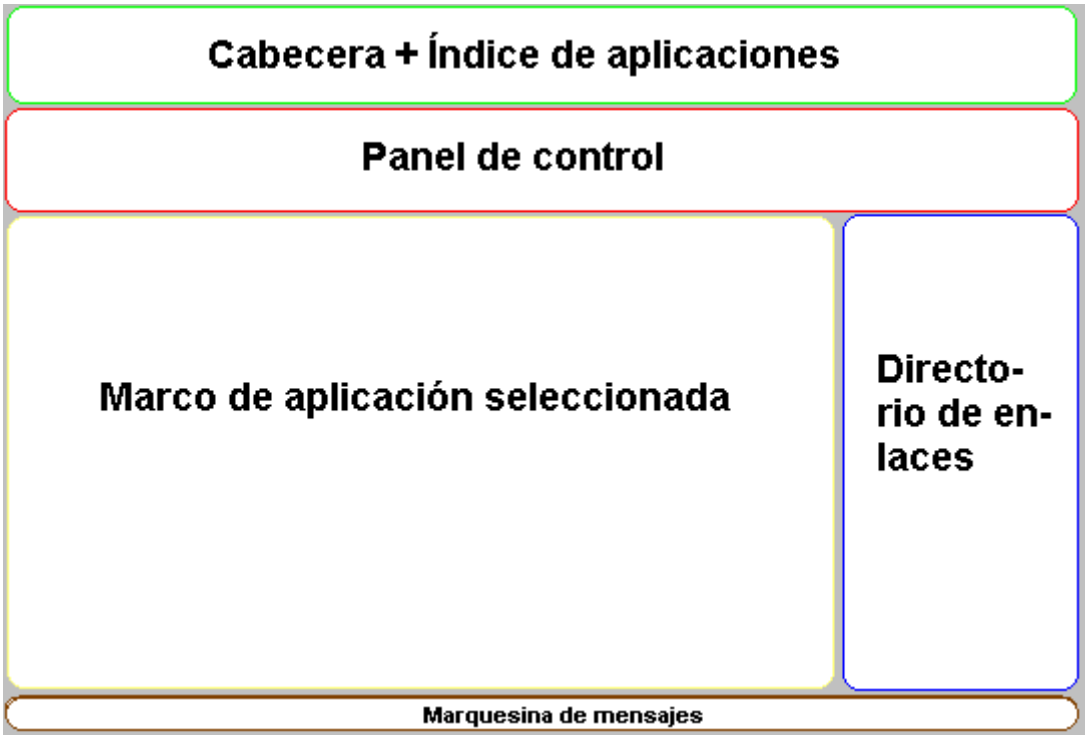


Ilustración 63. Consola, distribución de frames.

Sobre estos frames, distinguimos los dos siguientes como principales:

- Frame de cabecera e índice de aplicaciones: para dar acceso a las distintas aplicaciones a integradas:

Ilustración 64. Consola, cabecera.

A nivel de código, cada enlace de cada aplicación modular se link mediante HTML básico:

```
[root@tfc]# vi header.php
…
     <table width='100%'>
      <tr>
       <td class='header_button'><div
onclick=\"TINY.box.show({image:'../image/MAPA.png',boxid:'frameless',animate:true,openjs:function(){openJS
()}})\">Esquema</div></td>
       <td class='header_button'><a href='". $url_base . "/log-
centralizer/today_centralization.php'>Centralización de logs</a></td>
       <td class='header_button'><a href='". $url_base . "/logvol-monitor/logvol-
monitor.php'>Storage</a></td>
       <td class='header_button'><a href='". $url_base . "/logAnalyzer/index.php'>LogAnalyzer</a></td>
       <td class='header_button'><a href='". $url_base . "/mail-stats-report/today-mail-
stats.php'>Correo</a></td>
       <td class='header_button'><a href='". $url_base . "/filter-stats-report/today-filter-
stats.php'>Filtrado</a></td>
       <td class='header_button'><a href='". $url_base . "/proxy-stats-report/proxy-
stats.php'>Proxy</a></td>
       <td class='header_button'><div onclick=\"TINY.box.show({html:'Sin
implementar',animate:false,close:false,mask:false,boxid:'error',autohide:3,top:400,left:500})\">Por
implementar</a></td>
       <td class='header_button_monitor'><a href='". $url_base . "/ssh-monitor/ssh-
monitor.php'>SSH</a></td>
       <td class='header_button_monitor'><a href='". $url_base . "/ftp-monitor/ftp-
monitor.php'>FTP</a></td>
       <td class='header_button_monitor'><a href='". $url_base . "/vpn-monitor/vpn-
monitor.php'>VPN</a></td>
       <td class='header_button_help'><a href='". $url_base . "/help/help.php'>Ayuda</a></td>
      </tr>
     </table>
…
```

- Frame de integración de aplicaciones: espacio central y más amplio de la consola, en donde se visualizarán las distintas aplicaciones integradas.

Ilustración 65. Consola, frame integración de aplicaciones.

Adicionalmente a estos frames principales, se han incluido tres frames adicionales relativos al control de las aplicaciones, un directorio de enlaces de interés, y una marquesina de información:

- Frame de panel de control: implementa el orquestador de la herramienta, en cuanto a la navegación a través del tiempo, de tal forma que de una forma práctica y sencilla, permite navegar por la información a través del tiempo. Además nos da información útil acerca de la sesión del usuario.

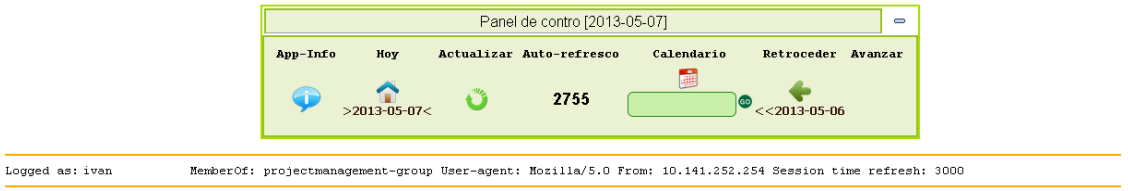


Ilustración 66. Consola, panel de control

Se controlan detalles como el de consulta sobre tiempos futuros.

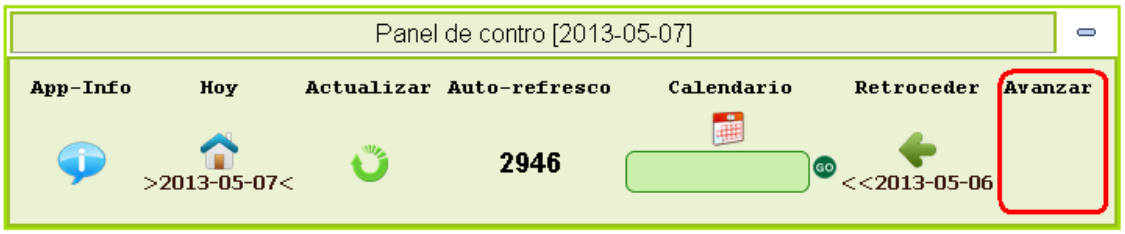


Ilustración 67. Consola, panel de Control -detalles (1)-

Se ha utilizado con efectos JQuery (AJAX) para darle dinamismo a los tiempos de espera.

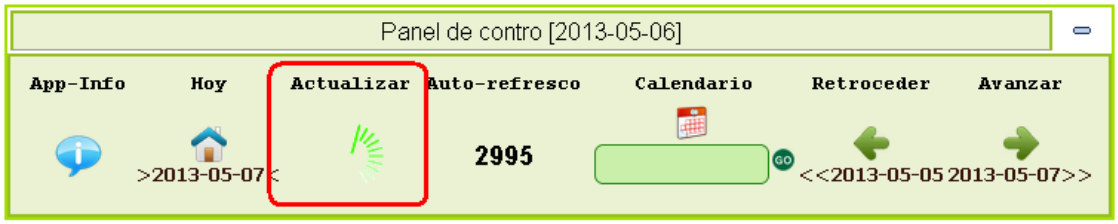


Ilustración 68. Consola, panel de Control -detalles (2)-.

Para maximizar el tamaño de interfaz de aplicaciones, implementa un simple mecanismo de minimización del panel de control.

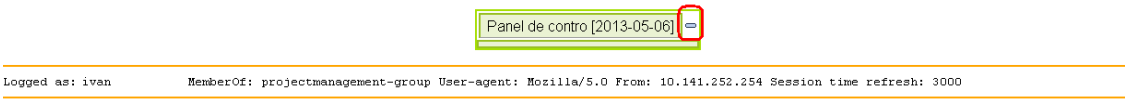


Ilustración 69. Consola, panel de Control -detalles (3)-

Ofrece ayuda contextual según la aplicación residente en el frame principal de aplicación.

Ilustración 70. Consola, panel de Control -detalles (4)-

- Frame de panel de directorio de enlaces: es habitual que determinados informes y visualización de eventos impliquen una rápida actuación sobre los elementos y servicios que los generan. Además es frecuente contar con administración de servicios basadas en http (mediante consolas web). Estas dos características han dado la iniciativa de integrar un director de enlaces de usuario en el frame derecho de la consola:

Ilustración 71. Consola, enlaces.

Permite mantener enlaces clasificados según la naturaleza de los mismo:

- Enlaces de uso habitual de los usuarios.
- Enlaces de gestión y adminitración mediante otras consolas web.

La configuración es totalmente abierta y puede ser aprovisionada desde un array PHP:

```
[root@html]# cat ../private/conf/tfc/right-config.php
<?php

$right_user_links = array (
 array ( "http://www.uoc.edu/portal/ca/index.html", "Acceso a la UOC" ),
 array ( "http://www.google.es", "Buscador Google" ),
 array ( "http://es.wikipedia.org/wiki/Wikipedia:Portada", "Wikipedia" ),
);

$right_gest_links = array (
 array ( "https://servidor_san.domain.net/", "Administraci&oacute;n de la SAN" ),
 array ( "https://vpn_cisco.domain.net/", "Acceso a router Cisco de VPN" ),
);

?>
```

1. Frame de marquesina de información: se añade un pequeño frame rotativo que permite imprimir a pie de página, aquella información que resulte interesante informar:

Ilustración 72. Consola, marquesina de información.

La configuración es totalmente abierta y puede ser aprovisionada desde un string PHP:

```
[root@html]# cat ../private/conf/tfc/bottom-config.php
<?php
$marquesina = "Servicio de gestión, análisis de logs y detección temprana de vulnerabilidades";
?>
[root@html]#
```

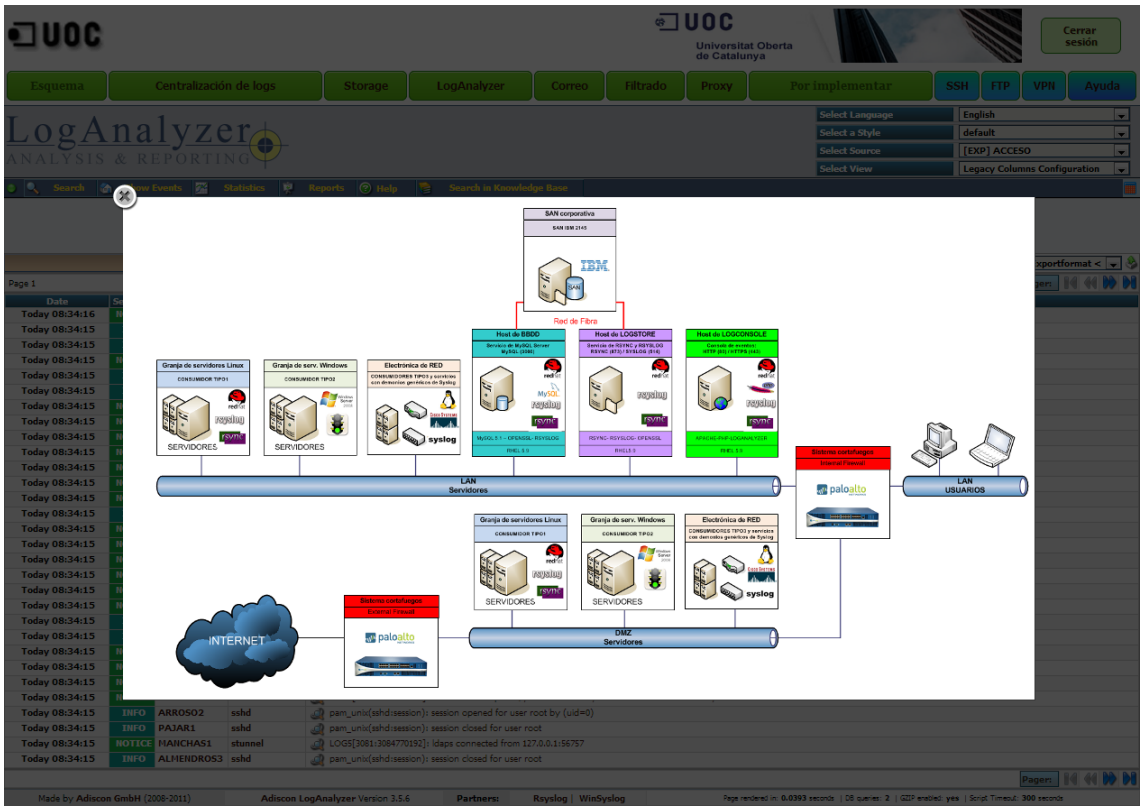
9.1.3. APLICACIONES INTEGRADAS

9.1.3.1. ESQUEMA

Hemos creído adecuado que la primera de las aplicaciones seleccionable de la consola tenga como cometido informar sobre la arquitectura de la plataforma y así dotar a todo administrador que se acerque a la misma de un conocimiento básico de los elementos que la conforman. Esta aplicación, no es más que una llamada al servicio TinyBox para visualizar imágenes en el que se indica la ruta a una imagen del esquema (alojado previamente en el DocumentRoot del servidor Apache), y que hace que se muestre el diagrama de arquitectura a través de efectos AJAX:

```
…
 <link rel='stylesheet' href='/tfc/css/tinybox.css' type='text/css'>
 <script type='text/javascript' src='/tfc/js/jquery.js'></script>
 <script type='text/javascript' src='/tfc/js/tinybox.js'></script>
…
       <td class='header_button'><div
onclick=\"TINY.box.show({image:'../image/MAPA.png',boxid:'frameless',animate:true,openjs:function(){openJS
(){}})\">Esquema</div></td>
…
```

El método de presentación elegido permite una rápida integración en caso de modificación de la arquitectura sin tocar explícitamente el desarrollo.



9.1.3.2. LogAnalyzer

Por su importancia, es la aplicación mostrada por defecto al acceder a la consola. A la hora de presentarla, se opta por mantener solamente la cabecera de la consola (índice de aplicaciones) dedicando el resto de la pantalla a la visualización del LogAnalyzer.

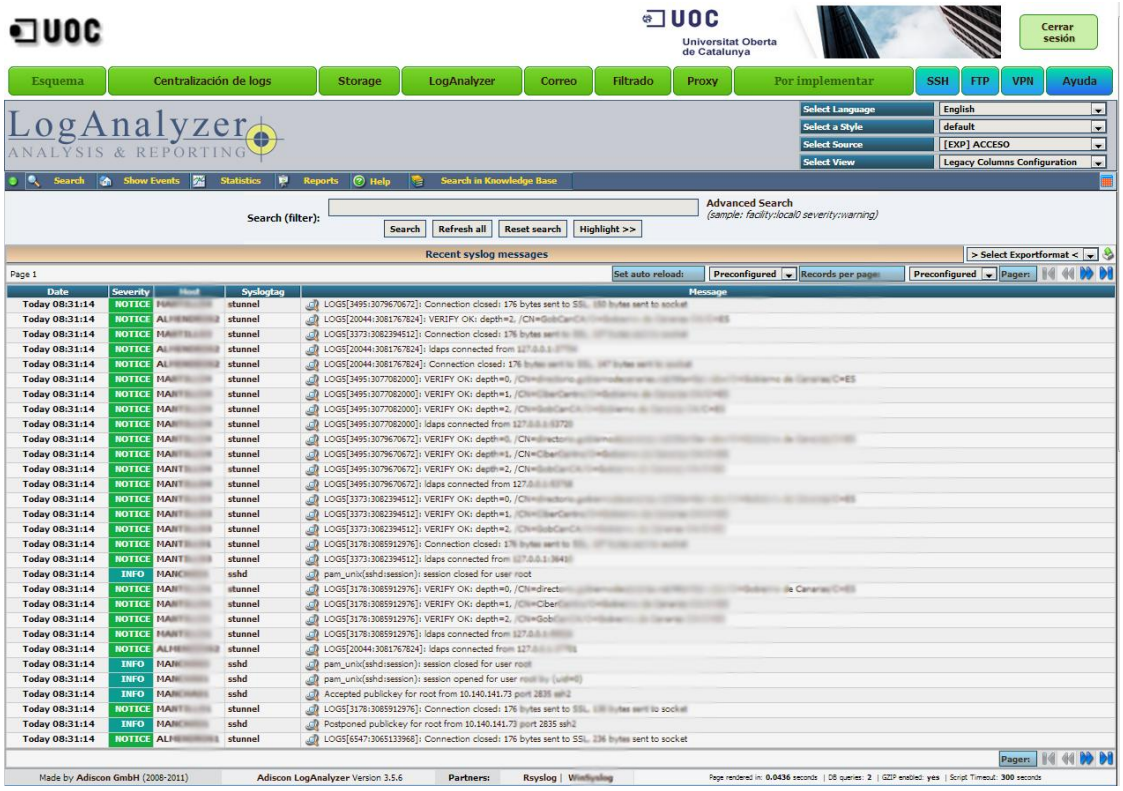


Ilustración 73. Consola. LogAnalyzer.

Para llevar a cabo esto, LogAnalyzer incluye en su fichero de configuración principal, una variable PHP del tipo string, que permite embeber aquel código HTML que queramos en la cabecera. Así, básicamente copiamos el contenido HTML utilizado en el fichero genérico de la configuración del frame de cabecera en el config.php del LogAnalyzer.

```
# vi tfc/logAnalyzer/config.php
…
$CFG['InjectHtmlHeader'] = "
…
     <table width='100%'>
      <tr>
       <td class='header_button'><div
onclick=\"TINY.box.show({image:'../image/046750.png',boxid:'frameless',animate:true,openjs:function(){open
JS()}})\">Esquema</div></td>
       <td class='header_button'><a href='" . $url_base . "/log-
centralizer/today_centralization.php'>Centralización de logs</a></td>
       <td class='header_button'><a href='" . $url_base . "/logvol-monitor/logvol-
monitor.php'>Storage</a></td>
       <td class='header_button'><a href='" . $url_base . "/logAnalyzer/index.php'>LogAnalyzer</a></td>
       <td class='header_button'><a href='" . $url_base . "/mail-stats-report/today-mail-
stats.php'>Correo</a></td>
       <td class='header_button'><a href='" . $url_base . "/filter-stats-report/today-filter-
stats.php'>Filtrado</a></td>
       <td class='header_button'><a href='" . $url_base . "/proxy-stats-report/proxy-
stats.php'>Proxy</a></td>
       <td class='header_button'><div onclick=\"TINY.box.show({html:'Sin
implementar',animate:false,close:false,mask:false,boxid:'error',autohide:3,top:400,left:500})\">Por
implementar</a></td>
       <td class='header_button_monitor'><a href='" . $url_base . "/ssh-monitor/ssh-
monitor.php'>SSH</a></td>
       <td class='header_button_monitor'><a href='" . $url_base . "/ftp-monitor/ftp-
monitor.php'>FTP</a></td>
       <td class='header_button_monitor'><a href='" . $url_base . "/vpn-monitor/vpn-
monitor.php'>VPN</a></td>
       <td class='header_button_help'><a href='" . $url_base . "/help/help.php'>Ayuda</a></td>
      </tr>
     </table>
…
```

Además de esta cabecera de presentación que nos permite tener el LogAnalyzer, este incorpora una sub-cabecera funcional para la gestión de la aplicación. Esta sub-cabecera nos permite la selección del contexto de uso (determinando la BBDD a usar) y la búsqueda rápida.

La aplicación LogAnalyzer permite mostrar en tiempo real cualquier evento centralizado sobre las distintas BBDD creadas, pudiendo seleccionar cada una de estas desde el panel de "Source".

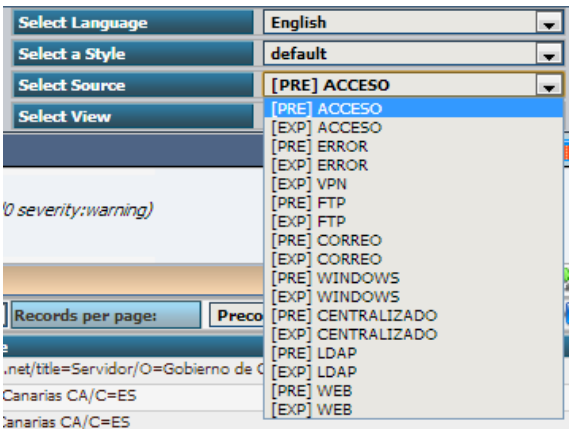


Ilustración 74. Consola, LogAnalyzer selección de Fuente.

En nuestro caso, vemos como las BBDD de eventos registrados (descrita en la "Tipología de eventos a registrar") se concretan en diferentes fuentes estratificadas por entorno:

2. Pre-producción: etiqueta “PRE”
3. Producción: etiqueta “EXP”

y tipología:

- Autenticación: etiqueta “ACCESO” y “LDAP”
- Logs críticos: etiqueta “ERROR”
- Mail: etiqueta “CORREO”
- FTP: etiqueta “FTP”
- Navegación Proxy y eventos WEB: etiqueta “WEB”
- Network: etiqueta “VPN” (primera integración de electrónica de red)
- RSYNC: etiqueta “CENTRALIZADO”

La selección de cualquier “Source” implicará que la aplicación cambie el contexto de uso y trabaje sobre los eventos obtenidos de esa BBDD.

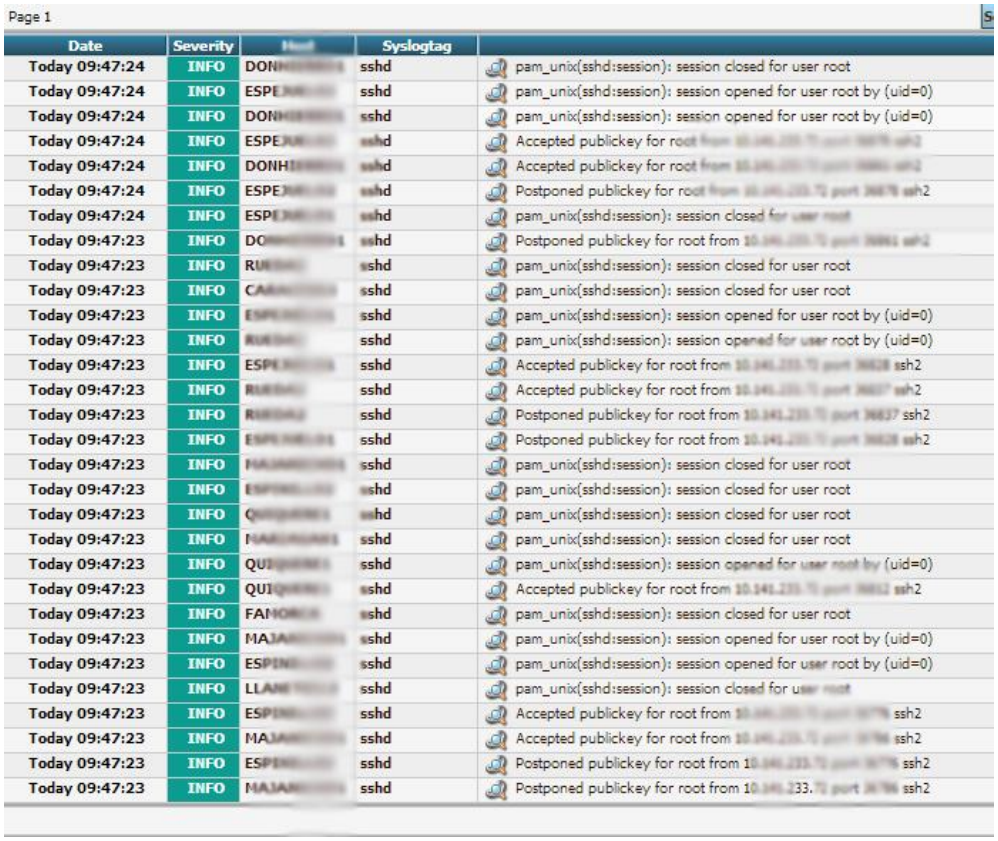


Ilustración 75. Consola. LogAnalyzer, eventos.

La visualización por defecto nos informa de la fecha, la severidad, el host origen, el tag y la descripción del evento.

Junto a esta relación detallada de sucesos acahecidos, la herramienta nos genera gráficas de indicadores esenciales que nos sirven como primer analisis de problemas potenciales. Así, nos facilita una grafica resumen de los 10 host con más sucesos registrados; grafica resumen de los 10 tags mas registrados; grafica resumen de número de sucesos por severidad y grafica resumen de los 10 dias con mayor número de sucesos.

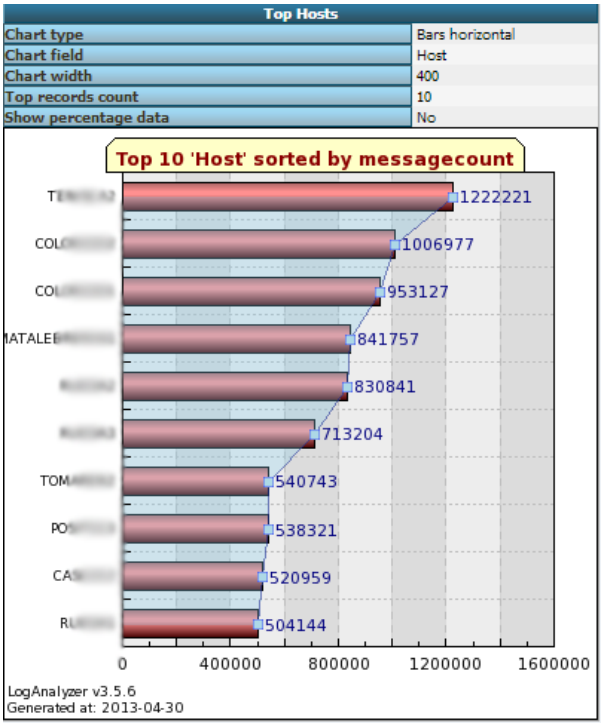


Ilustración 76. Consola. LogAnalyzer, gráfica top ten host con más sucesos registrados.

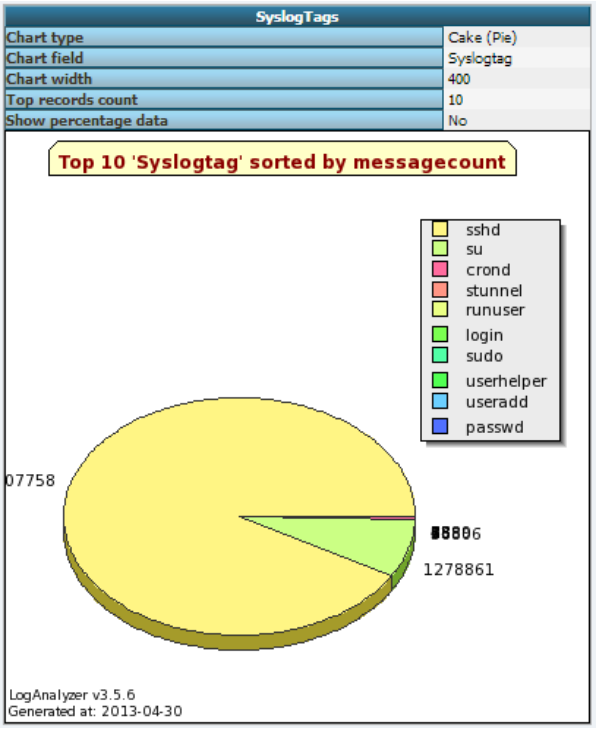


Ilustración 77. Consola. LogAnalyzer, gráfica top ten tag con más sucesos registrados.

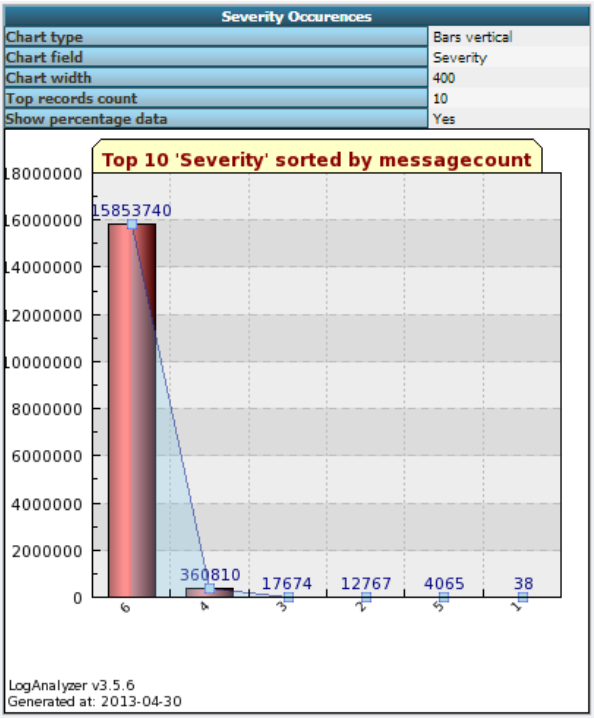


Ilustración 78. Consola. LogAnalyzer, gráfica top ten sucesos por severidad.

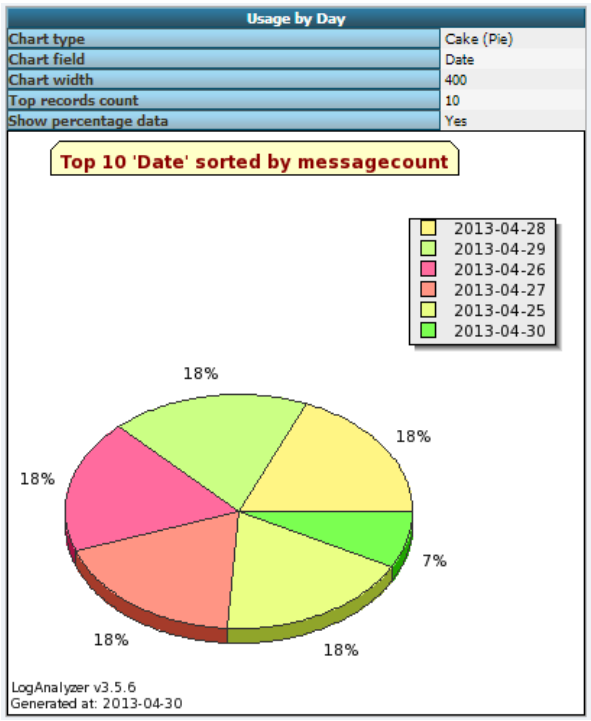


Ilustración 79. Consola. LogAnalyzer, gráfica top ten fechas con más sucesos registrados.

Otra de las opciones esenciales nos permite búsqueda avanzada de eventos, en base a difentes criterios como el tiempo, el origen syslog, patrones de string de los mensajes, etc.:

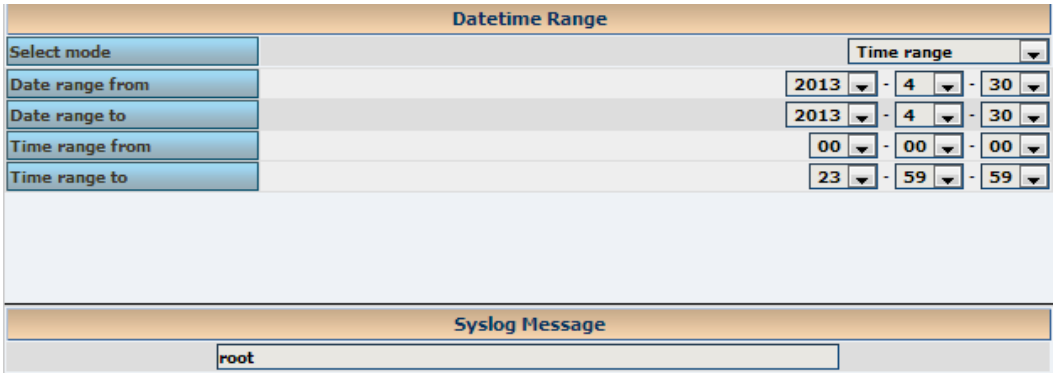


Ilustración 80. Consola. LogAnalyzer, búsqueda Avanzada: especificación fechas y mensaje.

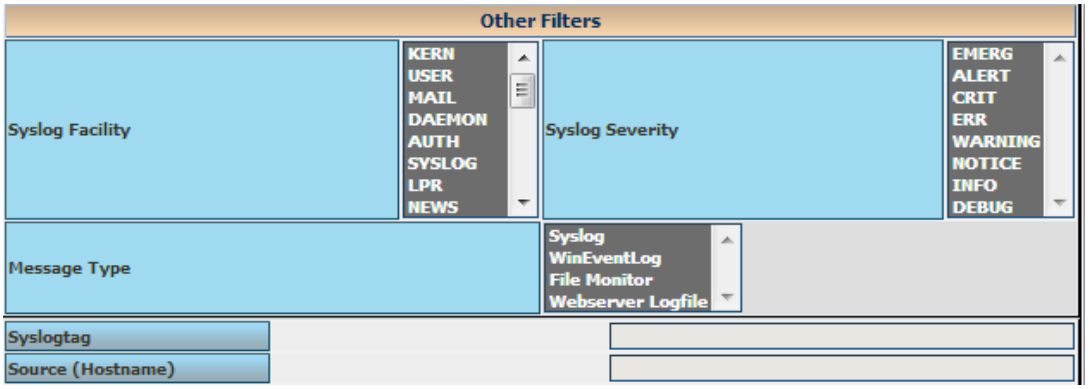


Ilustración 81. Consola. LogAnalyzer, búsqueda Avanzada: especificación criterios.

Se ha de resaltar, que después de construir -con la búsqueda avanzada- nuestra consulta, el LogAnalyzer, nos muestra en el cuadro de búsqueda rápida o filtrado la construcción "sintáctica" de la misma. Lo que nos permite ver la transformación "semántica" de nuestra búsqueda en la instrucción concreta de búsqueda rápida, agilizando el proceso de aprendizaje en este sentido.

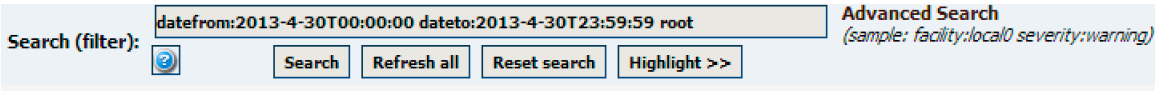


Ilustración 82.Consola. LogAnalyzer, descripción rápida.

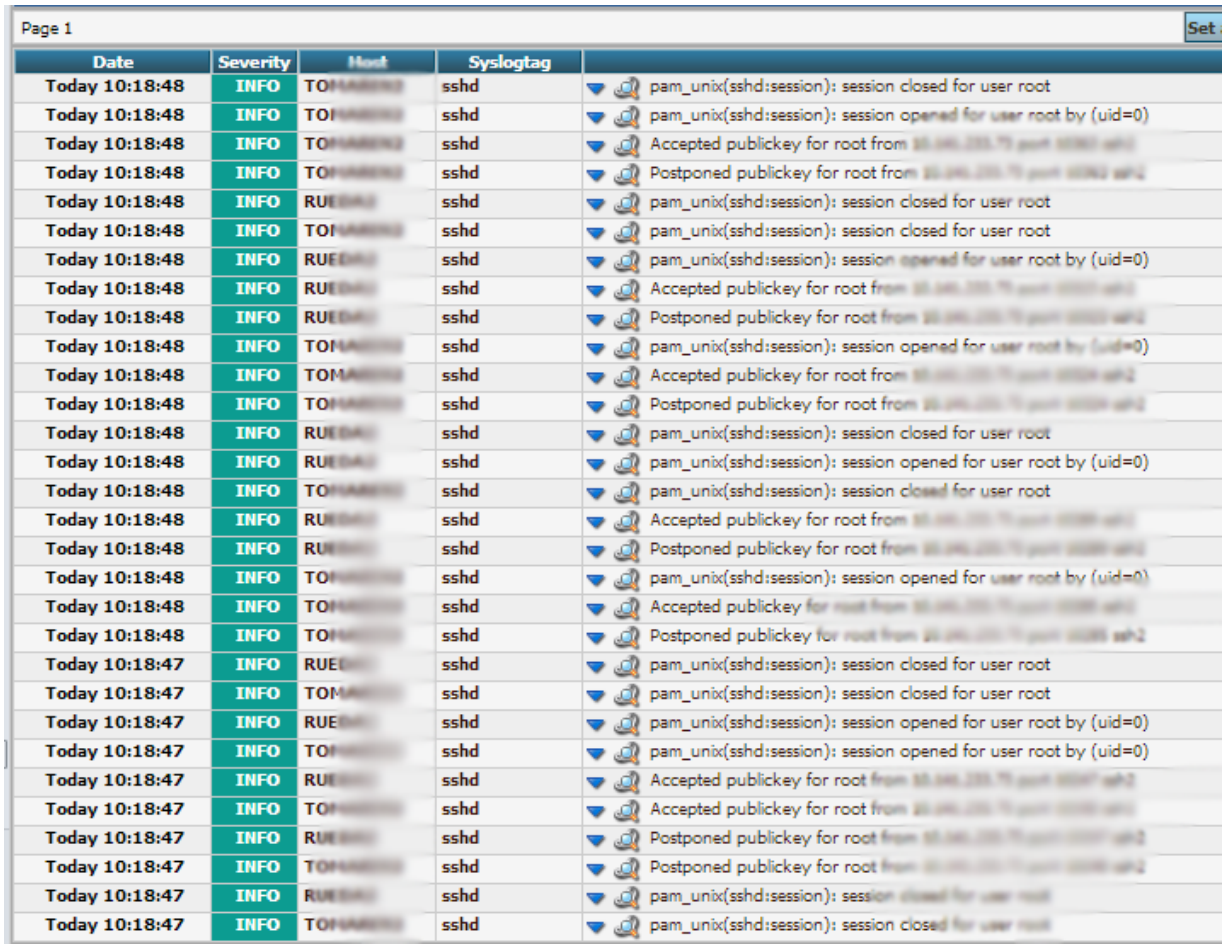


Ilustración 83. Consola. LogAnalyzer, resultado de la búsqueda.

9.1.3.3. CENTRALIZACIÓN DE LOGS

La aplicación es un desarrollo sobre PHP que añade cualidades de reporting al sistema de centralización de logs, de tal forma que de un modo sencillo, los administradores sean capaces de obtener un informe del estado diario de los procesos de centralización de los host integrados en el sistema de centralización.

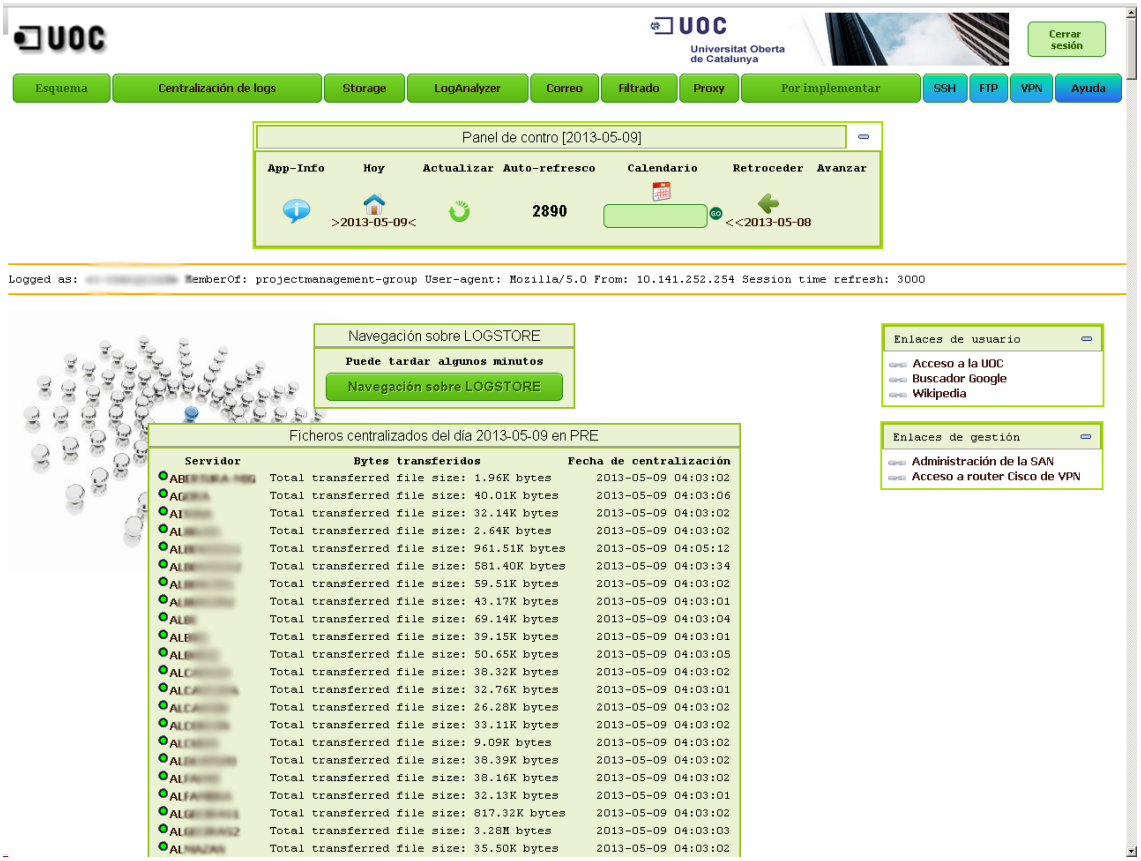


Ilustración 84. Consola. Centralización de LOGS

Sobre esta visión general, se muestran 4 bloques:

1. Un launcher para la aplicación PHPFileTree, que abrirá en una nueva ventana en un explorador que permite navegar sobre los file systems donde residen los logs centralzados

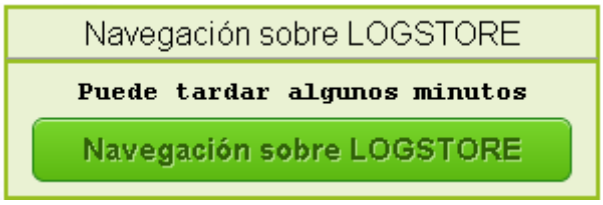


Ilustración 85. Consola. Lanzador de navegación del LOGSTORE

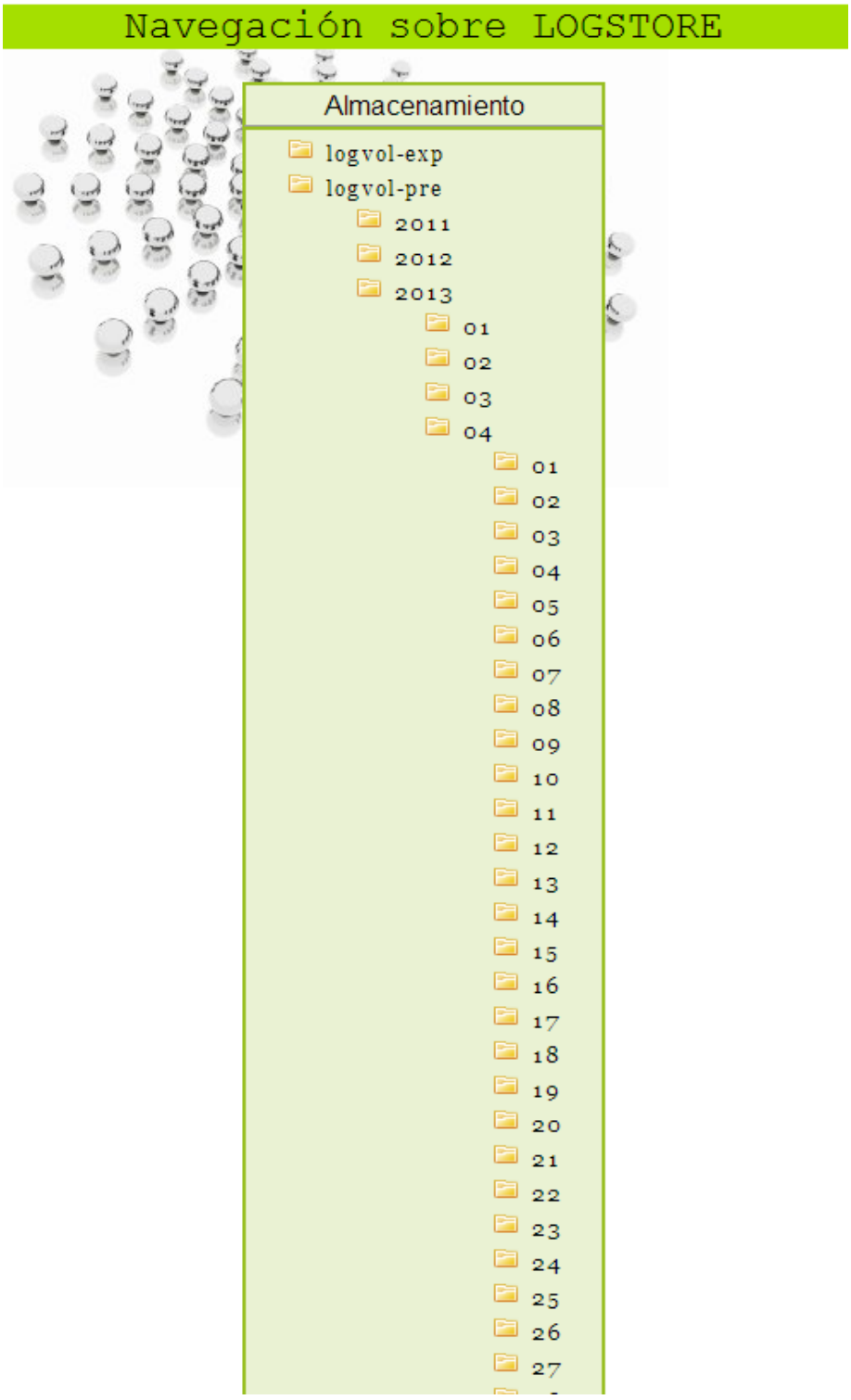


Ilustración 86. Consola. Navegación del LOGSTORE

Ilustración 87. Consola. LOGSTORE, ficheros centralizados en un día concreto.

Para garantizar la integridad y la seguridad de los archivos centralizados, por norma general no se permite ni la edición, ni la descarga a través de la herramienta de Navegación. Para advertir de dicha situación, se ha programado sobre el explorador PHPFileTree para que se ejecute al acceder a cada uno de los logs la Acción de "javascript: alert ()" con un mensaje de acceso no permitido.

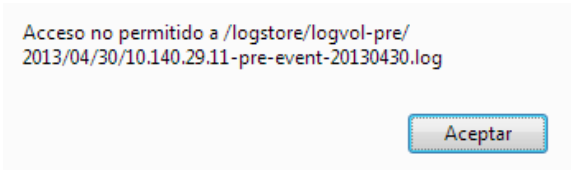


Ilustración 88. Consola. Navegación del LOGSTORE, mensaje de advertencia.

2. Un tabla con la lista de servidores del entorno de pre-explotación que se han centralizado y una sumarización de los mismos.

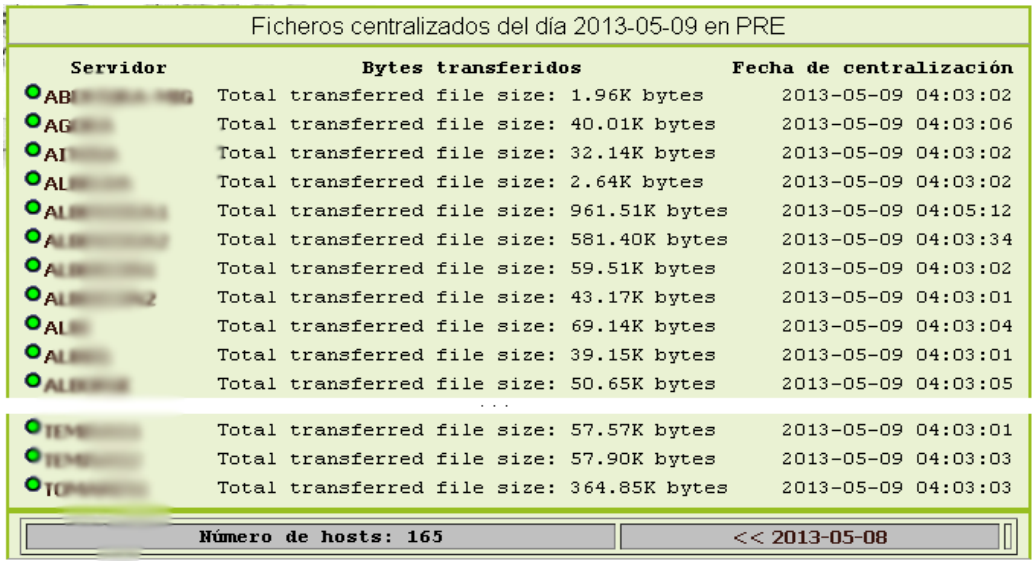


Ilustración 89. Consola, Centraliación de LOGS, entorno de PRE-EXPLOTACIÓN.

3. Un tabla con la lista de servidores del entorno de explotación que se han centralizado y una sumarización de los mismos.

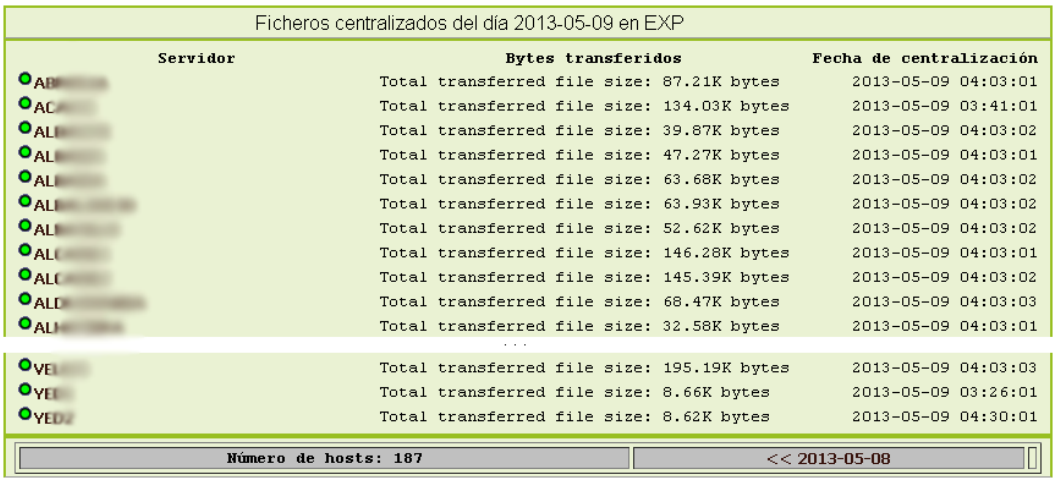


Ilustración 90. Consola. Centraliación de LOGS, entorno de EXPLOTACIÓN.

Sobre estas tablas (puntos 2 y 3) que listan los servidores cuyos ficheros de logs han sido centralizados, al “pinchar” sobre cada uno de ellos, permite acceder a un listado completo de los logs centralizados:

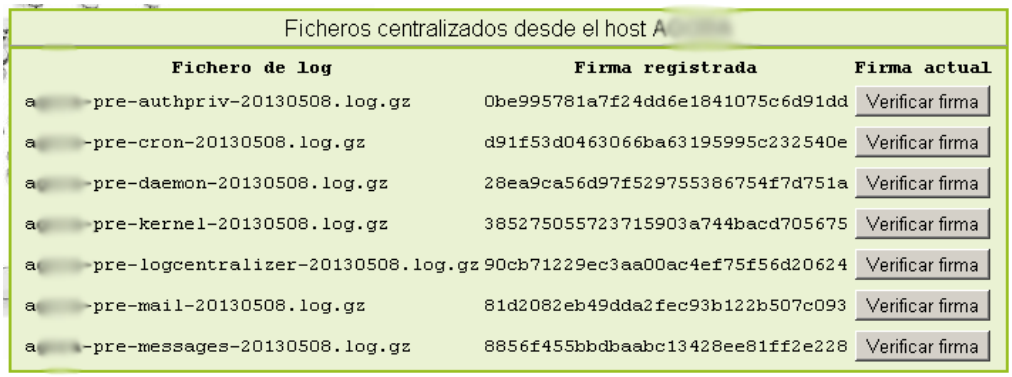


Ilustración 91. Consola. Centralización de LOGS, ficheros centralizados de un host.

Y a su vez, sobre cada fichero centralizado se permite mantener un control de verificación en tiempo real sobre la firma del fichero que se registró durante su centralización, y la que tiene en el momento de consultarlo mediante la consola web. Si por alguna razón se detectara otra firma distinta, o el fichero hubiera desaparecido del almacenamiento, se notificaría el error.

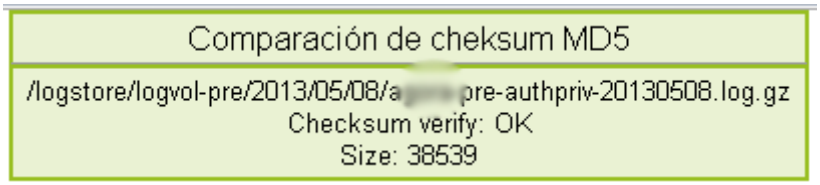


Ilustración 92. Consola. Centralización de LOGS, verificación de firma.

4. Un tabla con la lista de servidores cuyos logs no han sido centralizados en el día en curso, y que habitualmente si se centralizan

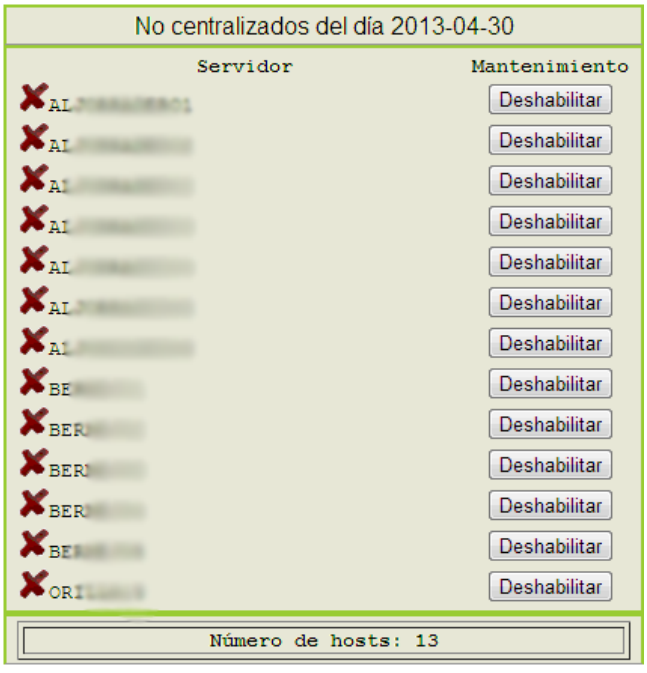


Ilustración 93. Consola. Centralización de LOGS, servidores sin centralizar.

También como valor añadido a la solución, y de cara a que puede ocurrir que cualquier host de la organización se desmantele, sobre la lista de servidores que no han centralizado logs se ha habilitado un botón para eliminar la monitorización de los mismos.

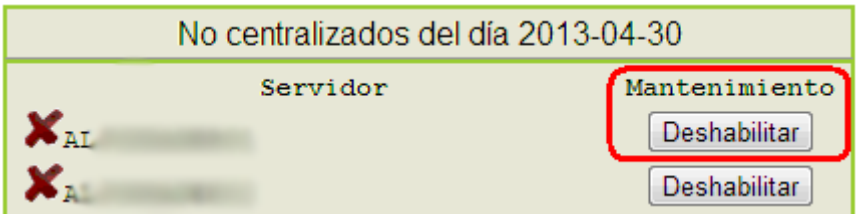


Ilustración 94. Consola. Centralización de LOGS, deshabilitar servidor no operativo.

9.1.3.4. STORAGE

Aplicación destinada a monitorizar el espacio consumido y libre sobre los volúmenes de almacenamiento de logs.

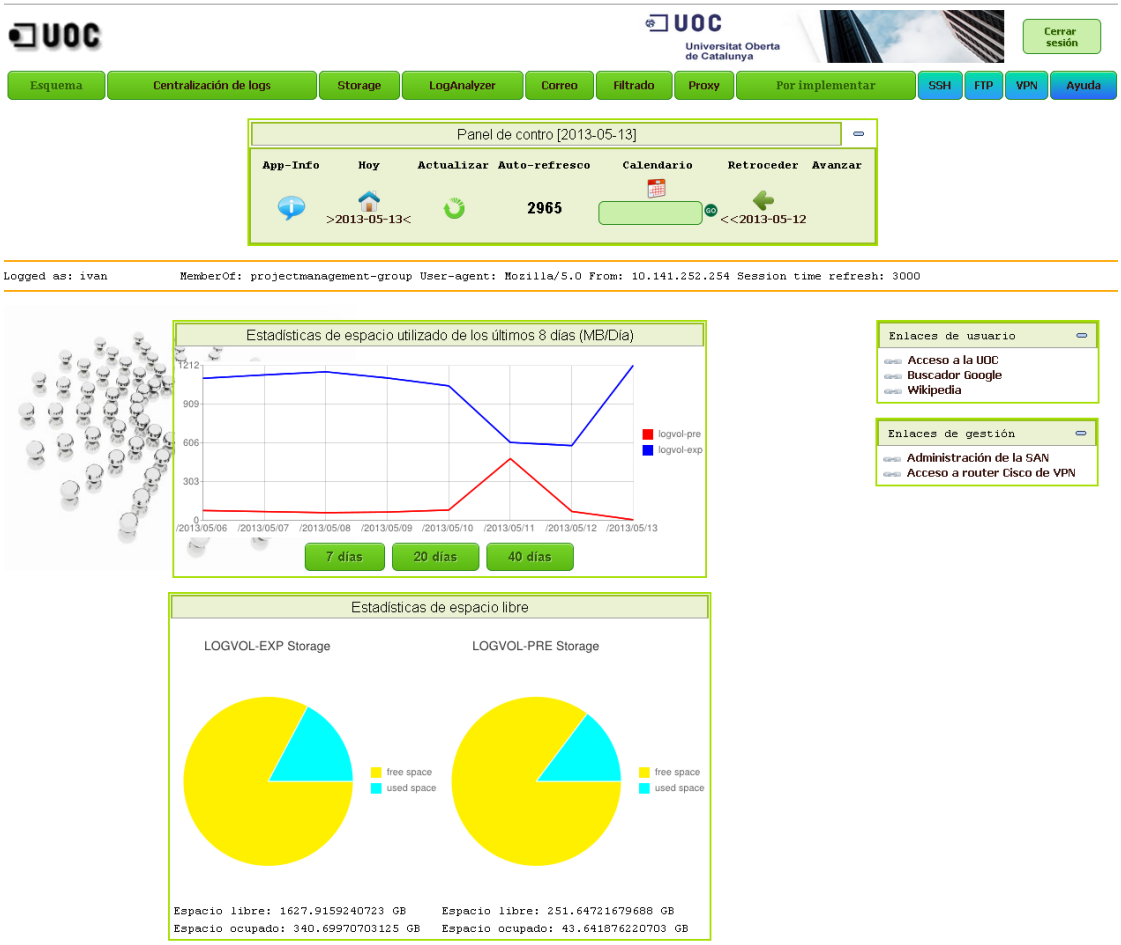


Ilustración 95. Consola, STORAGE.

Además, y como valor añadido a este indicador global de capacidad, muestra gráficas sobre el consumo de espacio utilizado diariamente por los logs, sobre cada uno de los volúmenes (el de logs de pre-explotación y el de producción), en periodos de 1 semana, 20 últimos día y 40 últimos días, permitiendo así a los administradores tener indicadores que puedan advertir de alguna anomalía, ya sea por disminución drástica del espacio utilizado por los logs (que podría derivar de un error en el sistema de centralización o algún error en alguno de los servicios que lo genera), o por el contrario un aumento desmesurado de estos, lo que podría ser un indicador de mal funcionamiento de algún servicio.

Ilustración 96. Consola. STORAGE: estadísticas de espacio utilizado.

9.1.3.5. CORREO

Esta aplicación se ha creado como front-end para la visualización de los datos estadísticos generados por la herramienta postfix-logwatch, mostrando además gráficas estadísticas sobre aquellos valores más relevantes, todo ello usando PHP, AJAX (mediante Jquery) y la API de GoogleCharts.

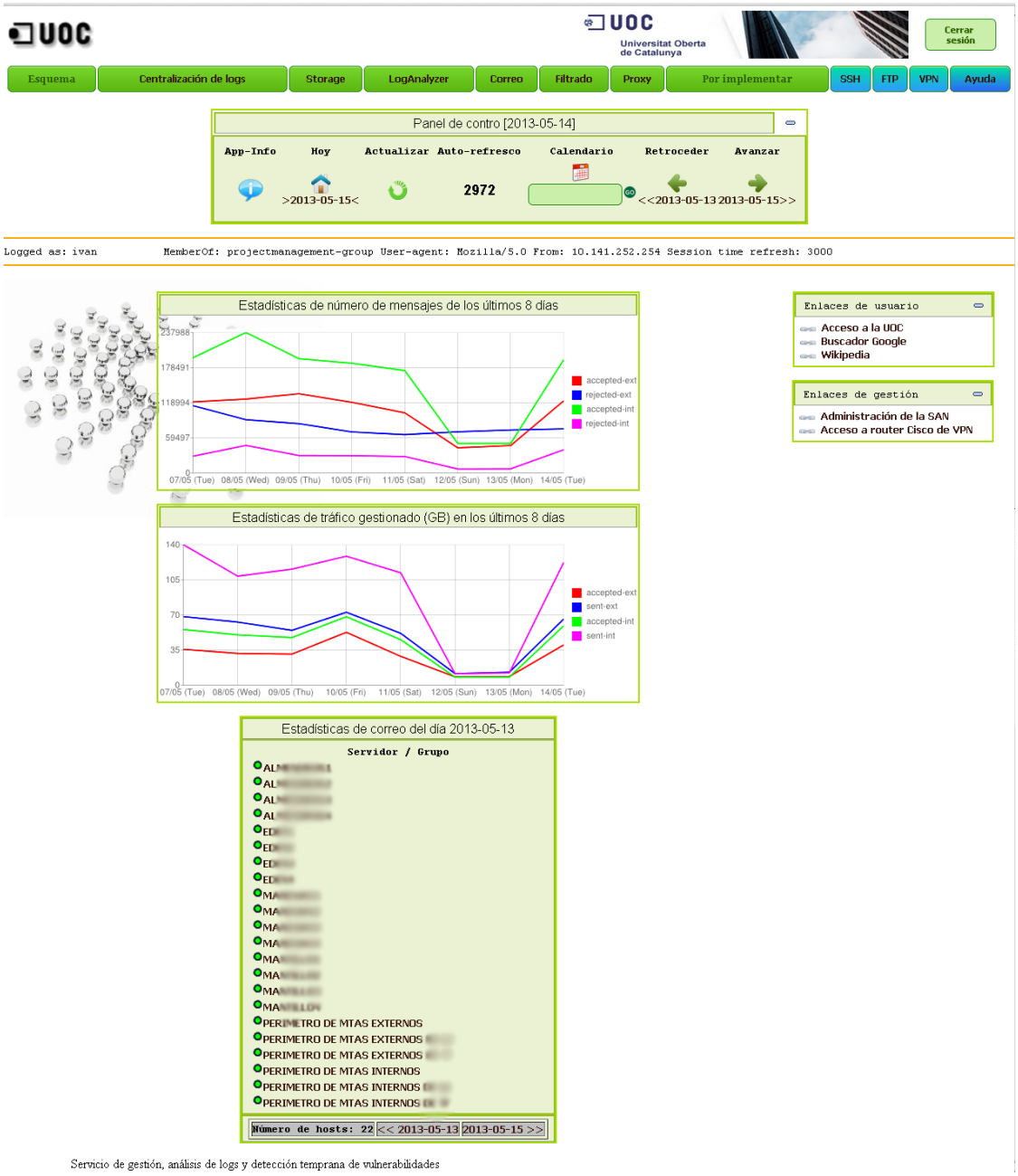


Ilustración 97. Consola, front-end Correo.

Como presentación inicial de la aplicación, esta provee las gráficas de los siguientes valores de datos SMTP sustraídos de los distintos reports postfix-logwatch, basándose en número de mensajes:

- Accepted-ext: número de mensajes (correos electrónicos) aceptados desde Internet.

- Rejected-ext: número de mensajes (correos electrónicos) rechazados desde Internet.
- Accepted-int: número de mensajes (correos electrónicos) aceptados desde la Intranet (red local).
- Rejected-int: número de mensajes (correos electrónicos) rechazados desde la Intranet (red local).

Y basándose en la cantidad de espacio (throghput) gestionado:

- Accepted-ext: cantidad datos (en GB) aceptados desde Internet.
- Sent-ext: cantidad datos (en GB) enviados a servidores remotos de Internet.
- Accepted-int: cantidad datos (en GB) enviados hacia los buzones internos de la organización (recepción de correo).
- Sent-ext: cantidad datos (en GB) enviados por los clientes de correo internos de la organización.

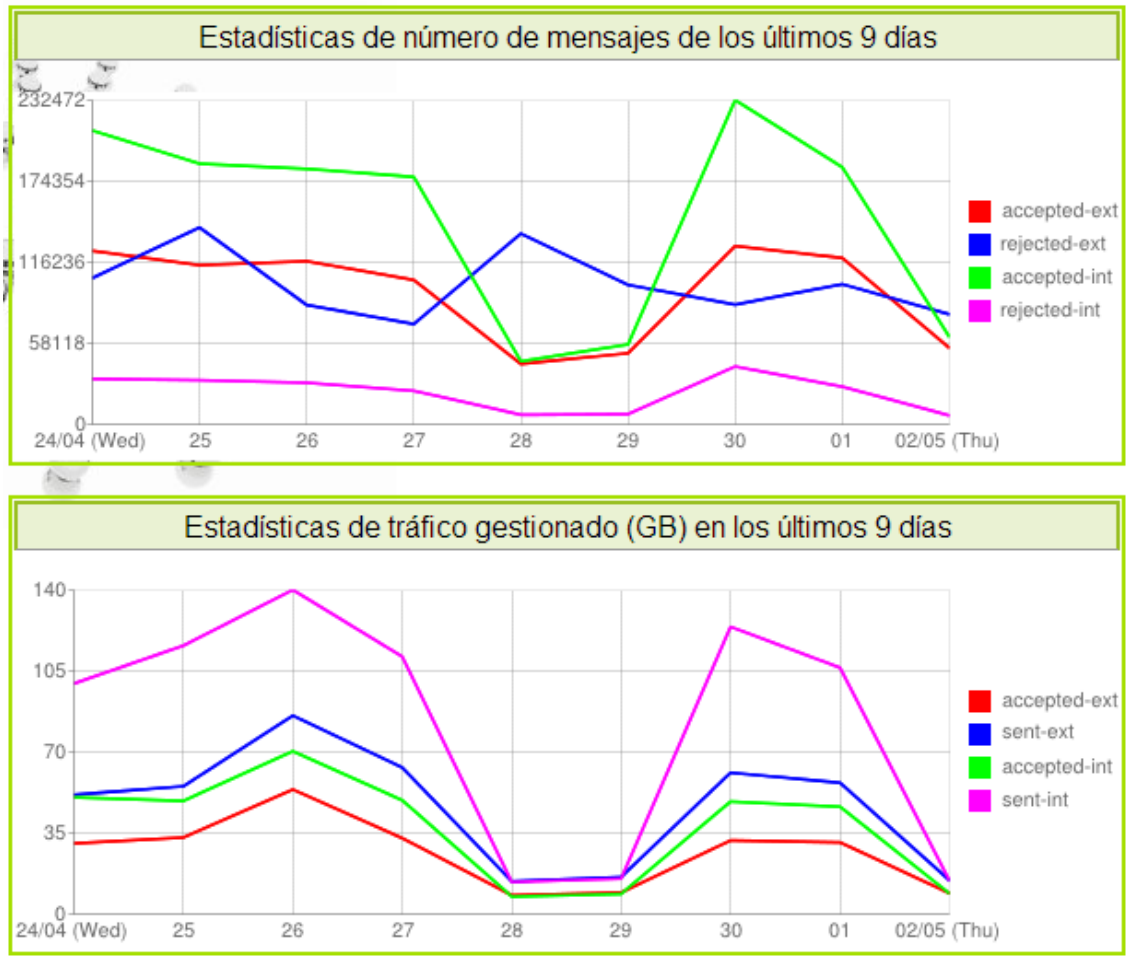


Ilustración 98. Consola. Correo: estadísticas de número de mensajes y trafico generado.

Lo siguiente que la aplicación muestra, es un listado de los servidores de correo de la organización, que enlazan con un reporte completo y en formato texto, ofrecido por la aplicación postfix-logwatch.

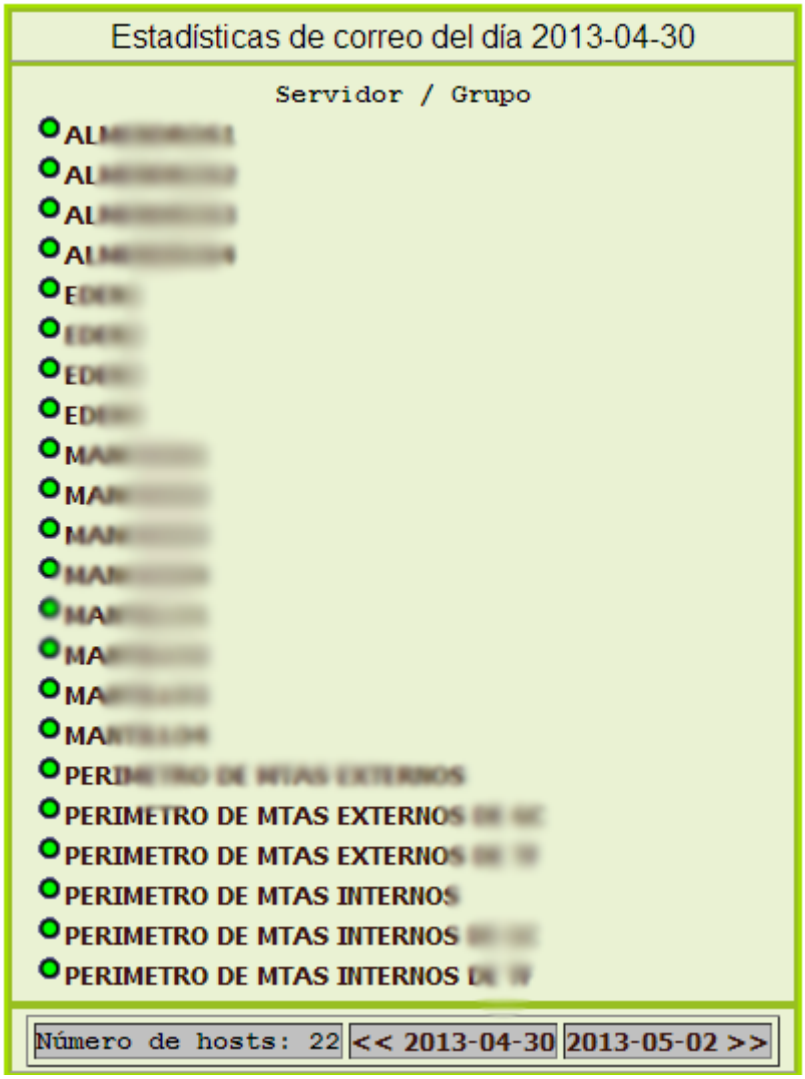


Ilustración 99. Consola. Correo: listado de servidores de correos monitorizados.

Al "pinchar" sobre cualquiera de los servidores, la aplicación nos mostrará el reporte completo, acompañado de una nueva gráfica que muestra el número total de mensajes gestionados por el servidor en cuestión

Estadísticas de correo de A del día 2013-04-30

```
****** Summary
--------------------------------------------------------------------------------

      21   *Fatal:   General fatal
     162   *Warning: Queue file size limit exceeded
      31   *Warning: Database is older than source file
      21   *Warning: Error reading attribute data
      21   Process exited
   18452   SASL authentication failed
   34600   Miscellaneous warnings

   5.159G  Bytes accepted                    5,539,708,626
  12.527G  Bytes sent via SMTP              13,451,168,935
 110.828K  Bytes delivered                         113,488
  28.831K  Bytes forwarded                          29,523
========   ==========================================

   20679   Accepted                                 86.89%
    3120   Rejected                                 13.11%
--------   ------------------------------------------
   23799   Total                                   100.00%
========   ==========================================

    2245   5xx Reject unknown user                  71.96%
     203   5xx Reject recipient address             6.51%
     108   5xx Reject sender address                3.46%
     564   5xx Reject client host                   18.08%
--------   ------------------------------------------
    3120   Total 5xx Rejects                       100.00%
========   ==========================================

  147143   Connections
  122446   Connections lost (inbound)
  147143   Disconnections
   20053   Removed from queue
      21   Delivered
   28944   Sent via SMTP
       6   Forwarded
     110   Resent
     311   Deferred
    1702   Deferrals
       6   Bounced (local)
      22   Bounced (remote)
      12   Expired and returned to sender
     196   Notifications sent

      19   Timeouts (inbound)
    1490   Illegal address syntax in SMTP command
     481   Hostname verification errors (FCRDNS)
      73   SMTP protocol violations
    6243   SASL authenticated messages
```

Ilustración 100. Consola. Correo: report del postfix-logwatch de un servidor monitorizado.

Para la elaboración de estos informes HTML basados en consultas SQL a BBDD, se ha creado una clase PHP (table.class.php) capaz de gestionar las consultas SQL e imprimirlas en formato amigable HTML, mediante programación PHP:

```
# vi tfc/mail-stats-report/today-host-mail-stats.php
<?php
include_once ('../include/googlecharts.class.php');
include_once ('../include/table.class.php');
include_once ('../conf/datasource.php');
…
$data=array('…');
$prueba=new googleChart($data);
$prueba->draw();
…
$query = "
 SELECT ...
 FROM ...
 WHERE ...
 ORDER BY ...
";

$columns = array ('NombreColumna1', 'NombreColumna2', 'NombreColumna3', 'NombreColumnaN');

$tabla = new Table ($data_source, $query, '<type>', '<Tittle>', $columns, $cur, $action, $form);
…
?>
```

De este modo, este código puede ser reutilizado para cualquier aplicación que se base en la consulta de informes sobre BBDD, como sucede con el resto de las aplicaciones incluidas en esta consola.

9.1.3.6. FILTRADO

La aplicación es otro front-end para la visualización de los datos estadísticos generados por la herramienta amavis-logwatch, mostrando además gráficas estadísticas sobre aquellos valores más relevantes, todo ello usando PHP, AJAX (mediante Jquery) y la API de GoogleCharts.

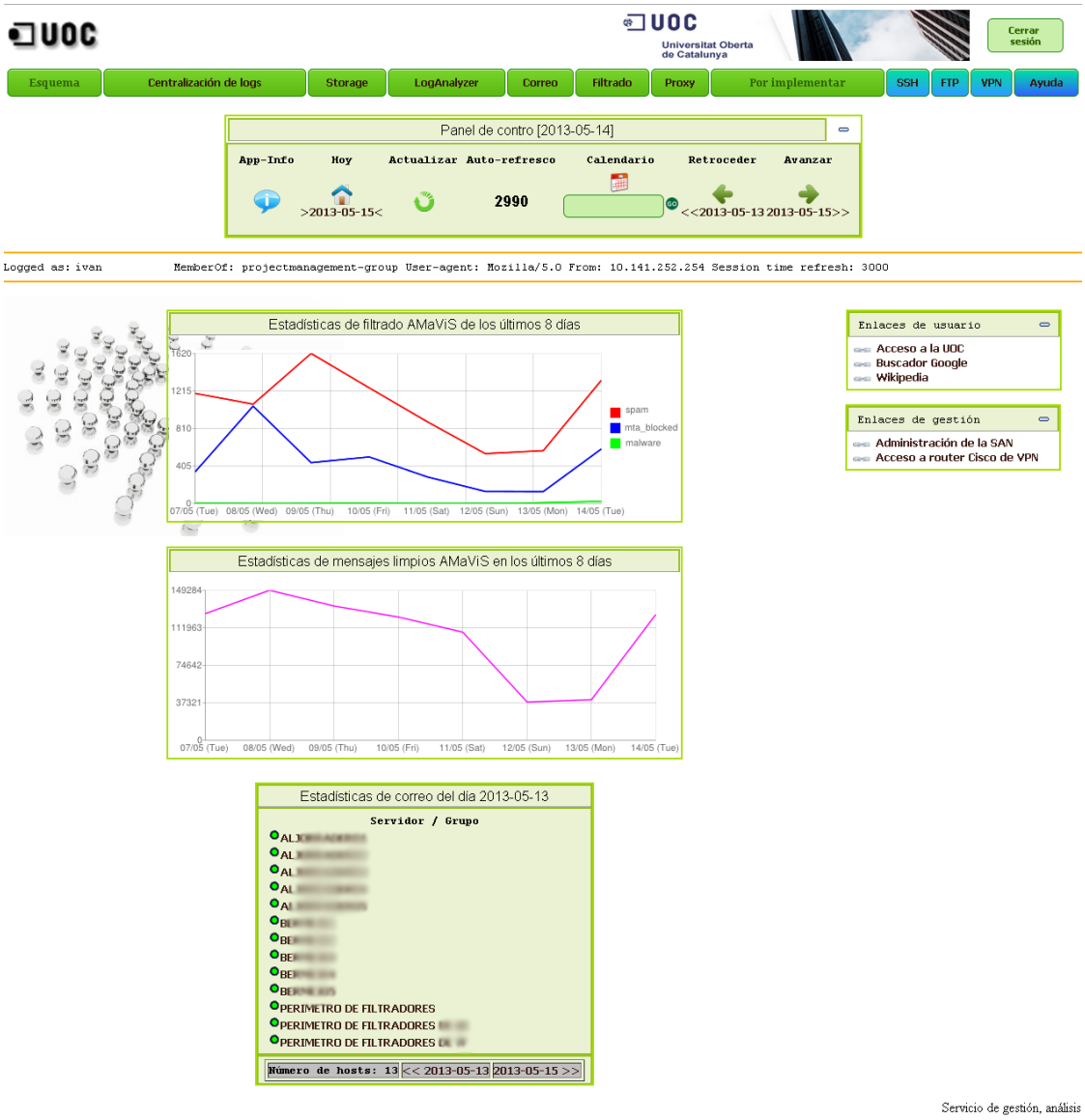


Ilustración 101. Consola. Front-End filtrado de Antivirus y Spam de correo

Como presentación inicial de la aplicación, esta provee las gráficas de los siguientes valores de datos de filtrado (antivirus y spam) sustraídos de los distintos reports amavis-logwatch:

- Spam: número de mensajes spam bloqueado.
- Mta_blocked: número de mensajes bloqueados por RBLs (listas negras) de servidores y clientes potencialmente malintencionados.
- Malware: número de mensajes con virus (troyanos, spywares, etc.) bloqueados.

- Número de mensajes que han pasado limpios.

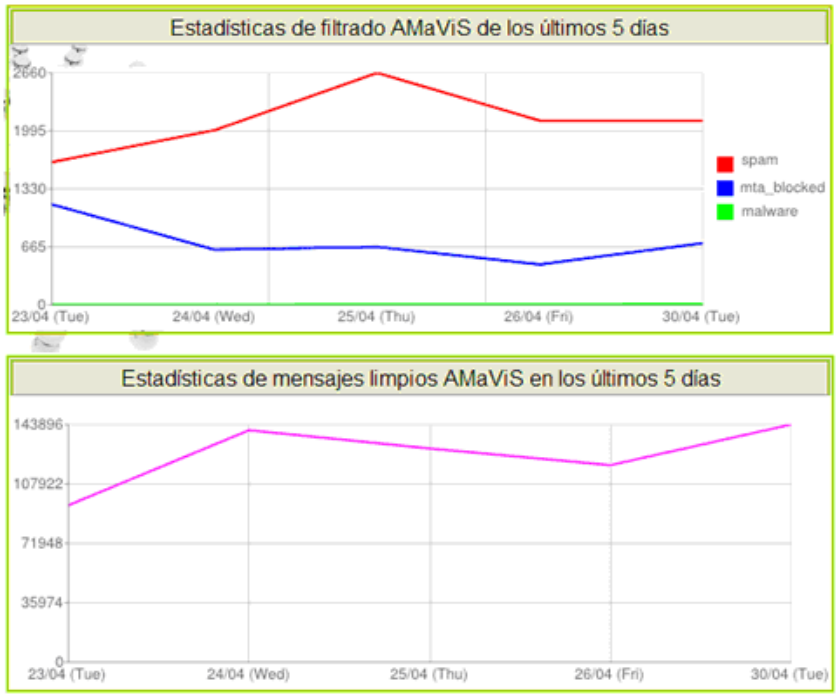


Ilustración 102. Consola. Estadisticas mensajes limpios, spam, bloqueados y malware.

Lo siguiente que la aplicación muestra, es un listado de los servidores de filtrado de la organización, que enlazan con un reporte completo y en formato texto, ofrecido por la aplicación amavis-logwatch.

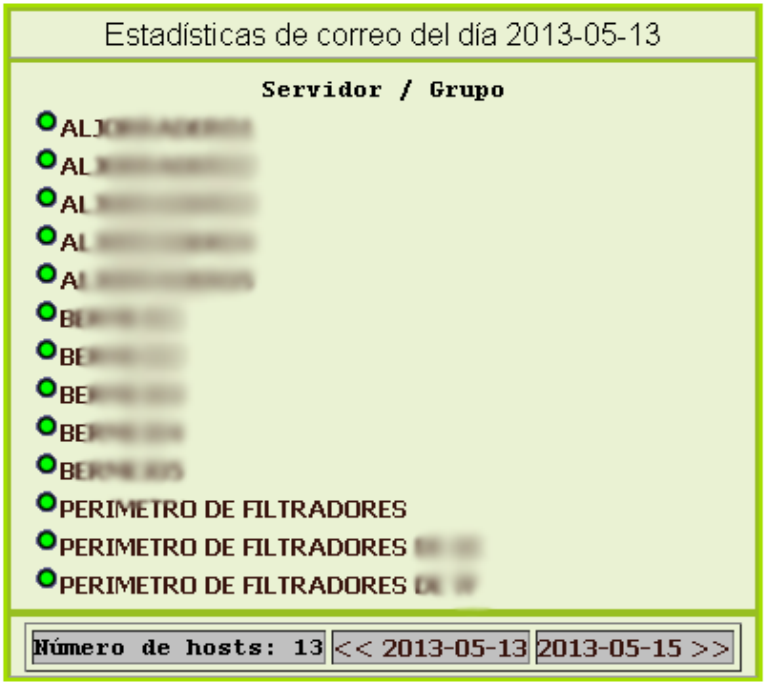


Ilustración 103. Consola. Filtrado: listado de servidores filtradores monitorizados.

Al "pinchar" sobre cualquiera de los servidores, la aplicación nos mostrará el reporte completo, acompañado de una nueva gráfica que muestra el número total de mensajes gestionados por el servidor en cuestión

Estadísticas de filtrado de A 1 del día 2013-04-29

```
Estadísticas diarias de filtrado IMSS [29 Apr 2013] ************************

Adjuntos eliminados:  1183
Correos bloqueados:  3
Correos en cuarentena:  64
Correos limpios:  521

Summary AMaVis
********************************************************************************

      14   *Warning: Virus scanner connection failure
       3   *Warning: Email address modified
      14   Miscellaneous warnings

   17554   Total messages scanned ------------------  100.00%
   3.977G  Total bytes scanned                4,270,728,518
========   ================================================

     476   Blocked ---------------------------------    2.71%
     207     Spam blocked                               1.18%
     269     MTA blocked                                1.53%

   17078   Passed ----------------------------------   97.29%
       3     Unchecked passed                           0.02%
     140     Bad header passed                          0.80%
   16935     Clean passed                              96.47%
========   ================================================

       3   Unchecked -------------------------------    0.02%
       3     Unchecked passed                           0.02%

     207   Spam ------------------------------------    1.18%
     207     Spam blocked                               1.18%

   17344   Ham -------------------------------------   98.80%
     140     Bad header passed                          0.80%
     269     MTA blocked                                1.53%
   16935     Clean passed                              96.47%
========   ================================================

     776   SpamAssassin bypassed
       5   SMTP response
       2   Archive extraction problem
      28   MIME error


================================================================================
Spam Score Percentiles        0%       50%       90%       95%       98%      100%
--------------------------------------------------------------------------------
Score Spam (207)           5.557    16.704    24.261    25.750    26.229    27.815
Score Unchecked (3)     -100.000    -0.521    -0.521    -0.521    -0.521    -0.521
Score Ham (16568)      -1500.000   -98.606    -1.044    -0.260     1.387     5.476
```

Ilustración 104. Consola. Filtrado: report amavis-logwatch de servidor de filtrado.

Para la elaboración de estos informes HTML basados en consultas SQL a BBDD, se utiliza la clase table.class.php descrita en anteriores apartados.

9.1.3.7. PROXY

Con esta aplicación se ofrece un front-end para la visualización de los datos estadísticos generados por la herramienta SCALAR, mostrando además gráficas estadísticas sobre aquellos valores más relevantes, todo ello usando PHP, AJAX (mediante Jquery) y la API de GoogleCharts.

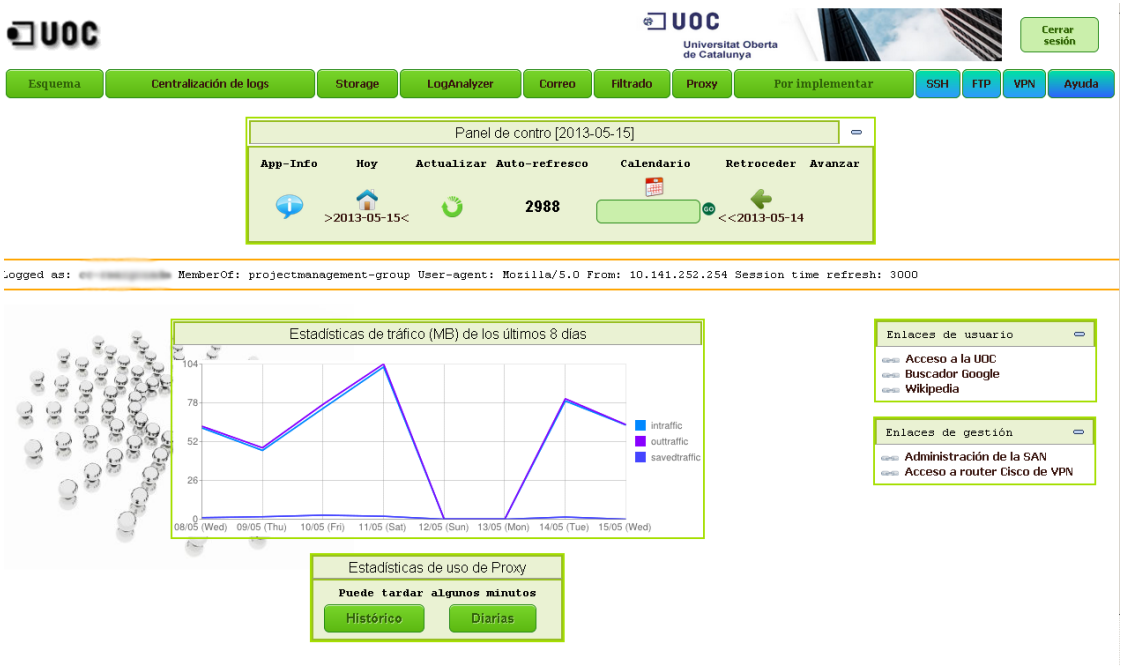


Ilustración 105. Consola. Front-End Proxy.

Como presentación inicial de la aplicación, esta provee las gráficas de los siguientes valores de datos de accesos de navegación mediante Squid Proxy, sustraídos de los distintos reports generados mediante SCALAR:

- Intraffic: reporta la cantidad de datos html en MB a que han sido accedidos desde la caché de los servidores Squid a los clientes browser de los usuarios de la Intranet (LAN local).
- Outtraffic: reporta la cantidad de datos html en MB a que han sido accedidos desde el servidor Squid a los servidores externos de Internet (navegación externa).
- Savedtraffic: es el resultante de la diferencia en MB de los valores anteriores, y que representa el ahorro de navegación externa que se ha salvado desde la caché.

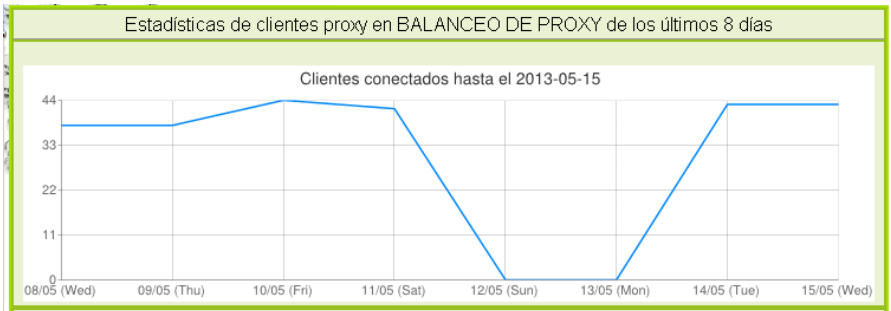
Ilustración 106. Consola. Proxy: estadísticas de trafico.

Lo siguiente que la aplicación muestra, es un combo de opciones para la consulta sobre los reports de textos diarios producidos por SCALAR, y un launcher para la consulta de las estadísticas de navegación creadas mediante la herramienta Webalyzer:

Para la elaboración de este combo HTML de opciones, se ha añadido a la clase PHP table.class.php la capacidad de ejecutar métodos para representar en formato amigable HTML (o en una nueva ventana o en la misma), las distintas opciones de acceso que se quieren mostrar:

```
# vi tfc/proxy-stats-report/proxy-stats.php
<?php
include_once ('../include/googlecharts.class.php');
include_once ('../include/table.class.php');
…
$data=array('…');
$prueba=new googleChart($data);
$prueba->draw();
…
$data_source = array (
 'option1' => array ( 'description' => "Descripcion1", 'url' => "<url1>", 'new_window' => <true|false> ),
 'option2' => array ( 'description' => "Descripcion2", 'url' => "<url2>", 'new_window' => <true|false> ),
 'optionN' => array ( 'description' => "DescripcionN", 'url' => "<urlN>", 'new_window' => <true|false> ),
);

$type = ‘options’;

$tabla = new Table ($data_source, '<Note>', $type, '<Tittle>', null, null, null, $form);
…
?>
```

Al “pinchar” sobre cualquiera de los servidores, la aplicación muestra el reporte completo, acompañado de una nueva gráfica que visualiza el número total de mensajes gestionados por el servidor en cuestión



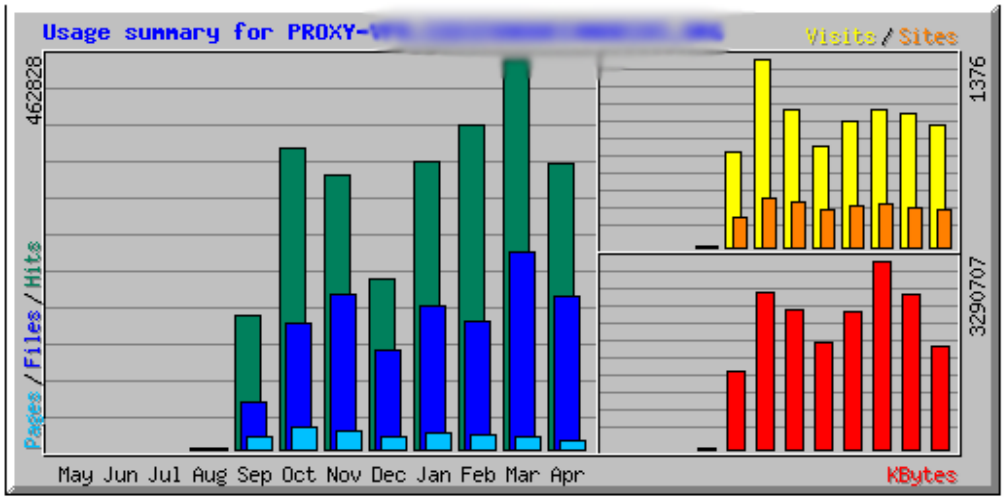
Estadísticas de acceso Proxy de BALANCEO DE PROXY del día 2013-05-14

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~        SCALAR (Squid Cache Advanced Log Analyzer & Reporter)          ~~~~
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~


     5000 Lines Processed, In: 38.7MB, Out: 38.7MB, Hit Ratio:  0.04 %    #033[1A#033[8OD
    10000 Lines Processed, In: 56.0MB, Out: 56.2MB, Hit Ratio:  0.40 %    #033[1A#033[8OD


~~~ Analysis Headlines ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

  Lines Analysed    11.968K

   Unique Hosts: 42

     In Traffic:   62.362 MB
    Out Traffic:   62.633 MB
  ------------------------------------
  Saved Traffic:  277.303 KB    0.43 %


~~~ Requests By Hours ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

  2.0K                                              ==
  1.9K                                           == ==
  1.8K                                           == ==
  1.7K                                           == ==
  1.6K                                           == ==
  1.5K                                           == ==
  1.4K                                           == ==
  1.3K                                           == ==             ==
  1.2K                                           == ==             ==
  1.1K                                           == ==             ==
  1.0K                                           == == ==          ==
  918                                            == == ==          == ==
```

```
~~~ Hierarchy (Requests) ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Peer/Direct    |  Total   %VOL| Misses Miss% |  Hits   Hit% |  Deny  |Timeouts|
---------------|--------------|--------------|--------------|--------|--------|
DIRECT           11.185K   97%   7.752K  69%       61    1%    3.372K       0
127.0.0.1           402    3%      402  100%        0    0%         0       0


~~~ Hierarchy (Traffic) ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Peer/Direct    |  Total    %VOL| Misses    Miss% |    Hits    Hit% |Deny&T-out|
---------------|---------------|-----------------|-----------------|----------|
DIRECT          50.411 MB  83%  45.687 MB   91%   277.303 KB   1%       4.659M
127.0.0.1        9.995 MB  17%   9.994 MB  100%         0  B   0%          0
```

Ilustración 107. Consola. Proxy: estadística y report de balanceos

Histórico: es un launcher que abre en una nueva venta del navegador, las estadísticas acumulativas que se han ido realizando con Webalyzer.



Summary by Month

Month	Daily Avg				Monthly Totals					
	Hits	Files	Pages	Visits	Sites	KBytes	Visits	Pages	Files	Hits
Apr 2013	11292	6076	370	29	278	1804665	896	11129	182307	338772
Mar 2013	14929	7571	467	31	293	2703876	971	14488	234707	462828
Feb 2013	13681	5415	611	36	311	3290707	1008	17111	151640	383077
Jan 2013	11359	5673	658	30	307	2401876	924	19744	170214	340791
Dec 2012	6703	3934	521	24	273	1873836	744	15651	118024	201110
Nov 2012	10842	6084	686	33	325	2445813	1006	20600	182545	325265
Oct 2012	11509	4834	850	44	355	2733291	1376	26351	149867	356799
Sep 2012	7185	2529	664	31	213	1371612	701	14627	55643	158073
Aug 2012	23	0	1	0	1	95	2	3	0	70
Totals						18625771	7628	139704	1244947	2566785

Ilustración 108. Consola. Proxy: gráfica visitas,sitios,trafico,páginas,ficheros,etc.

La aplicación webalyzer permite obtener distintos datos estadísticos como las páginas más solicitadas, los clientes browser con mayor consumo, etc.

9.1.3.8. SSH

La aplicación de SSH permite ver qué conexiones a nivel de ese protocolo han sido establecidas correcta o incorrectamente con cada uno de los servidores integrados bajo el sistema de centralización de evento. Esta aplicación, a diferencia de las otras (que ofrecen un front-end de reportes y estadísticas sobre eventos pasados), permite una monitorización activa de las sesiones SSH en tiempo real, de tal modo que es posible "auditar" las conexiones SSH de cualquier servidor en tiempo real:

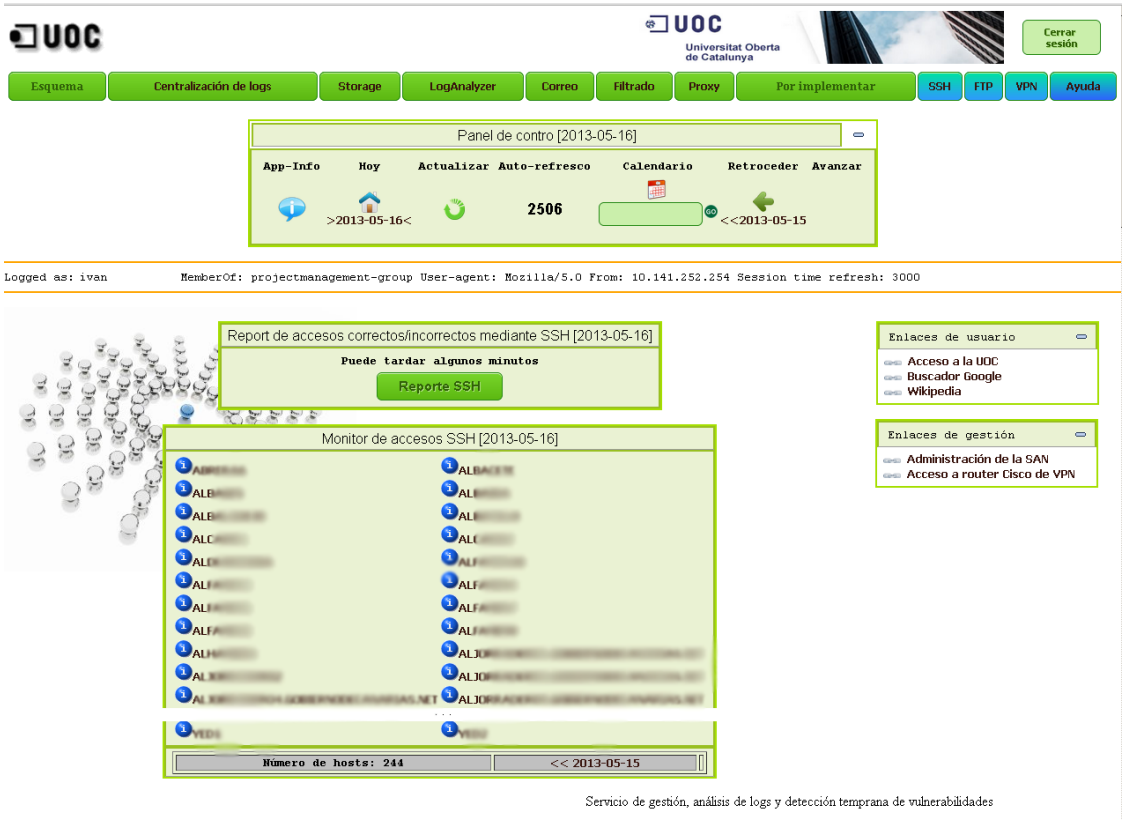


Ilustración 109. Consola. Accesos SSH

La aplicación en su ejecución inicial muestra un acceso a un report completos sobre aciertos y errores de acceso mediante SSH, utilizando para ello una llamada a la clase tabla.class.php, incluyendo un launcher al reporte: un listado completo de los hosts integrados con el sistema de centralización de eventos, y con el SSH habilitado.

Ilustración 110. Consola. Monitorización SSH.

Sobre este report, es posible "pinchar" sobre cada host para ver los accesos, pudiendo ser estos tanto en tiempo real como de días pasados. En segundo lugar ofrece un listado completo de los hosts integrados con el sistema de centralización de eventos, y con el SSH habilitado.

Ilustración 111. Consola. SSH: Monitor de accesos.

Al "pinchar" sobre cada uno de ellos se ofrece una consola de monitorización de cualquier evento (correcto o fallido, en tiempo real o de días pasados) de este host:

Ilustración 112. Consola. SSH: Detalles de accesos.

9.1.3.9. FTP

Esta aplicación, al igual que la anterior, ofrece un front-end que permite la monitorización (tanto en tiempo real como de días pasados) de las conexiones de usuarios a los servidores de FTP. Además, ofrece la visualización de reportes estadísticos de conexiones por día, y acumulativas mediante estadísticas webalyzer.

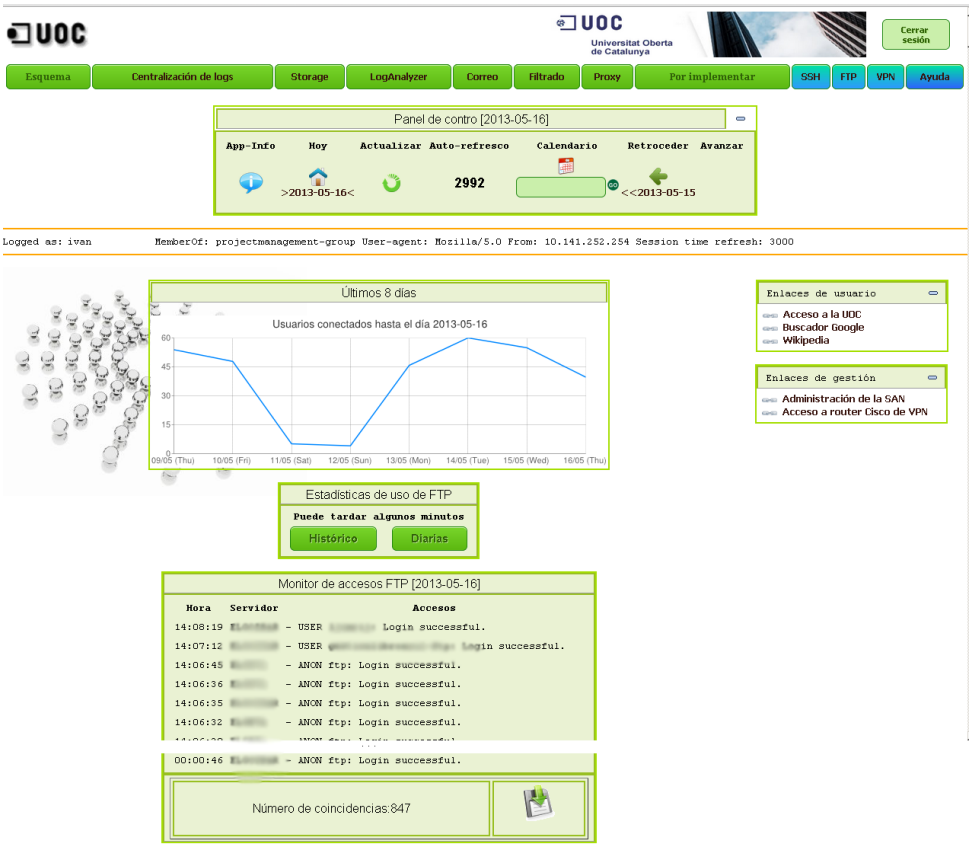


Ilustración 113. Consola. FTP.

El acceso a cada una de las partes se provee mediante el uso de las gráficas estadísticas generadas mediante la api de GoogleCharts, mientras que la presentación de los informes y launchers se realizan mediante la clase tabla.class.php, reutilizada en otras aplicaciones, e invocada de los modos descrito en anteriores aplicaciones.

Atendiendo a las distintas partes de la aplicación, se pueden ver:

- Gráfica de usuarios conectados a lo largo del tiempo (incluyendo las de tiempo real).
- Launcher al webalyzer de estadísticas acumulativas de conexiones.
- Launcher para la consulta de un report diario acerca del uso de cada servidor FTP.
- Un monitor de accesos de tiempo real o tiempo pasado.

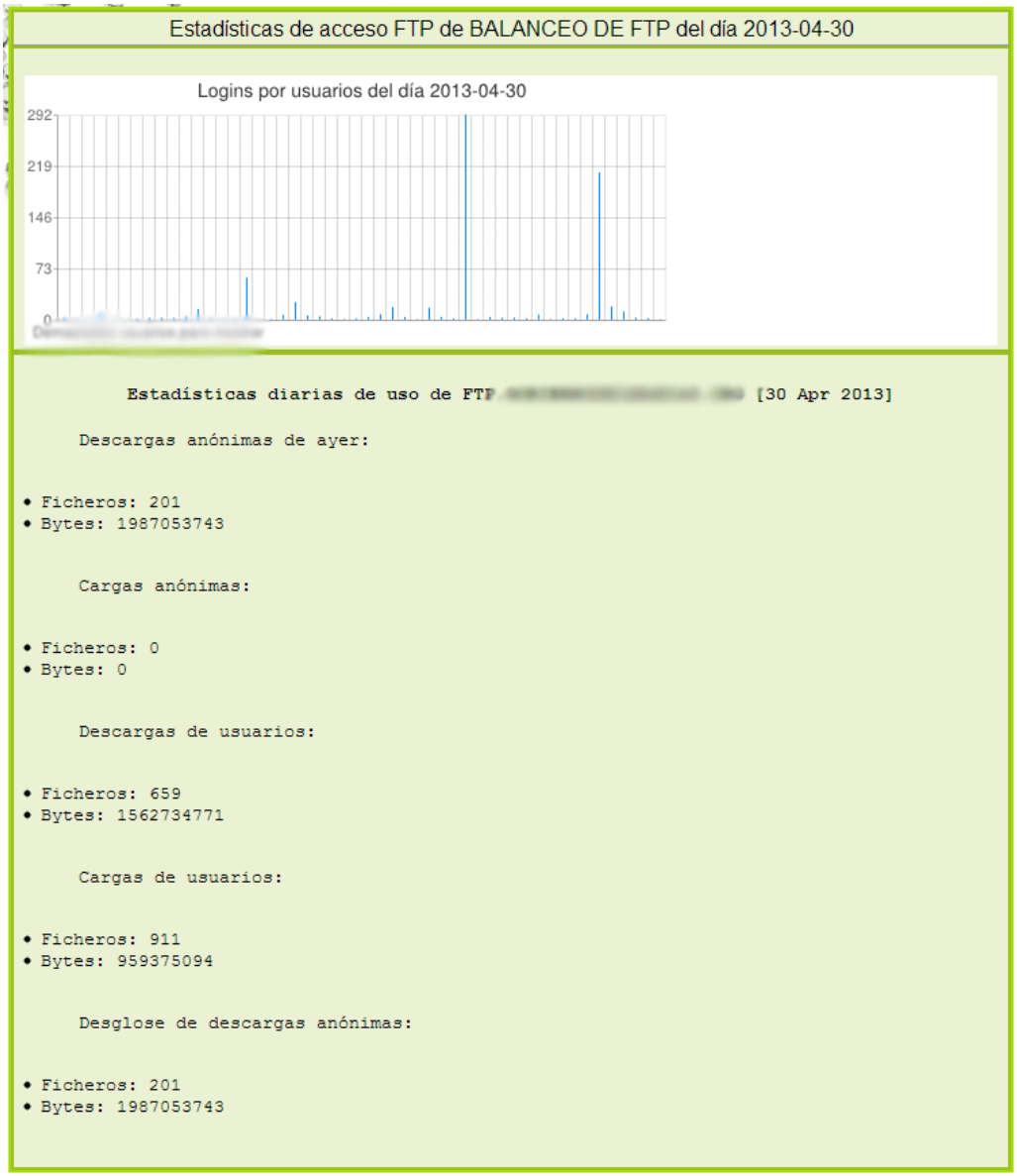


Ilustración 114. Consola. FTP: Estadisticas de Acceso

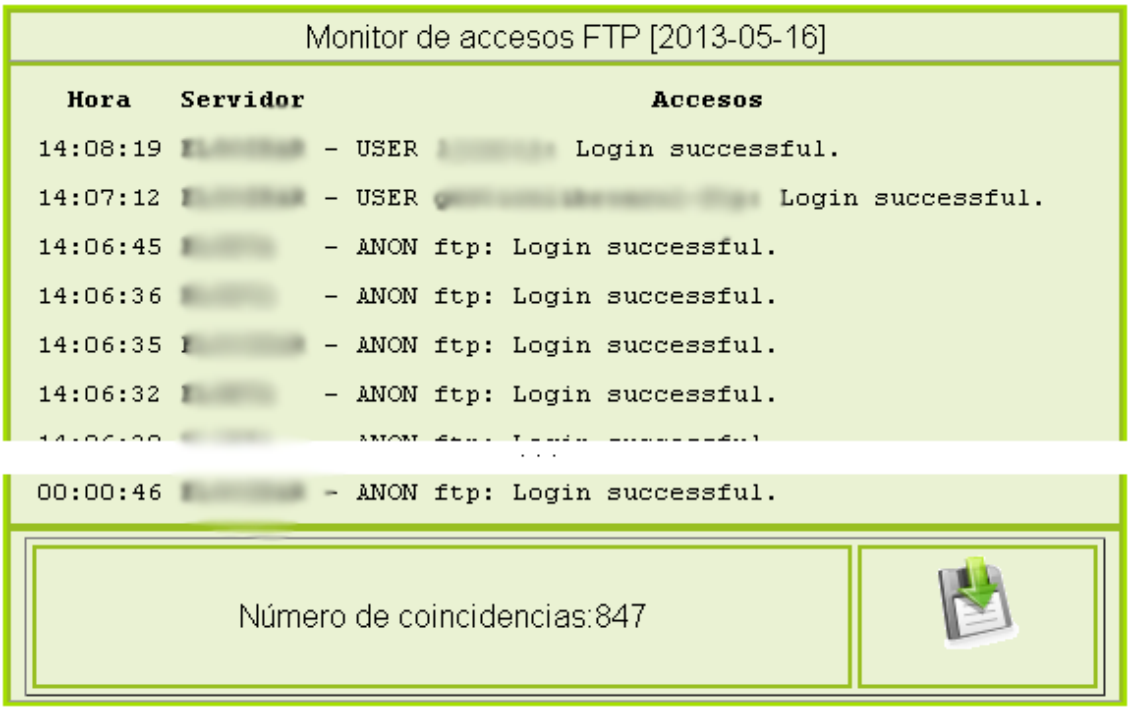


Ilustración 115. Consola. FTP: Monitor de accesos.

Sobre esta última parte de monitorización de conexiones FTP, se incorpora a la clase tabla.class.php la opción de descarga de los movimientos en formato CSV, permitiendo así una fácil exportación de la información.

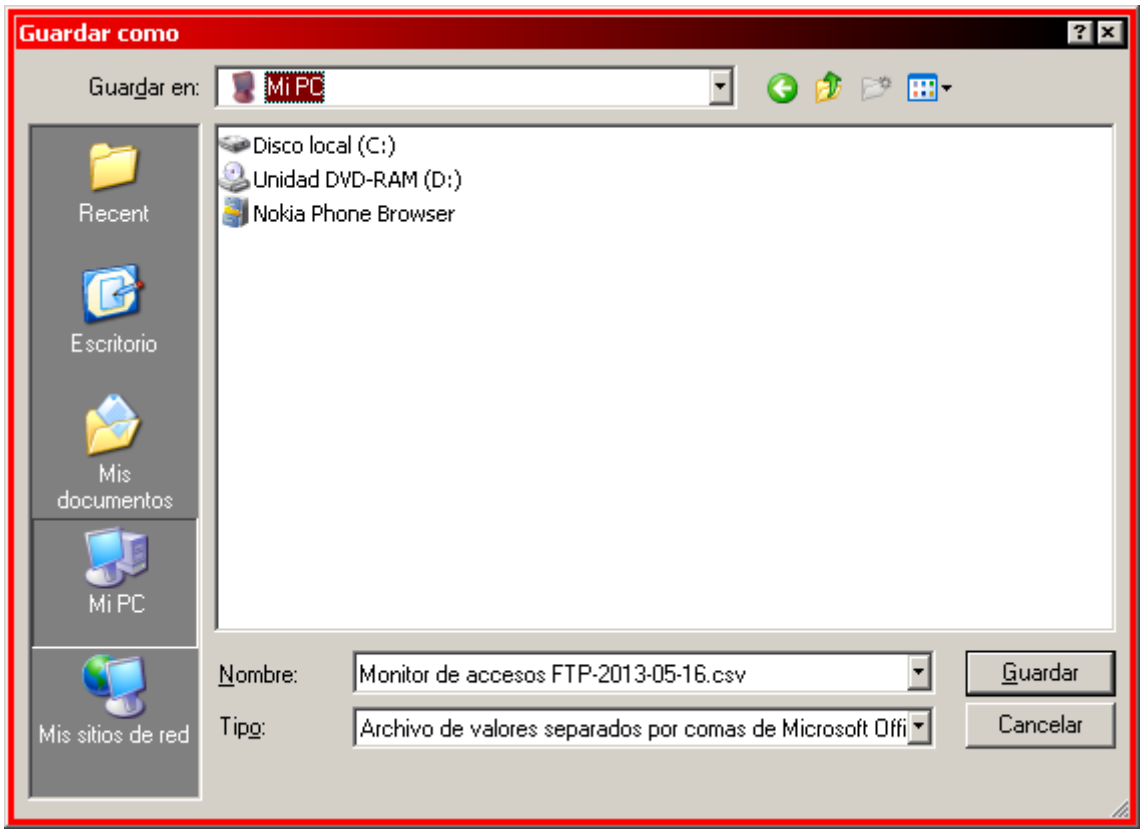


Ilustración 116. Accesos FTP: Exportación.

9.1.3.10. VPN

La aplicación permite la monitorización (tanto en tiempo real como de días pasados) de las conexiones de usuarios a los servidores de VPN basado en electrónica de red Cisco. Además, ofrece esta capacidad, pero por cada servidor de VPN. Nuevamente la aplicación se fundamente el uso de la API GoogleCharts para graficar los datos estadísticos, y de la clase tabl.class.php para la presentación de la información:

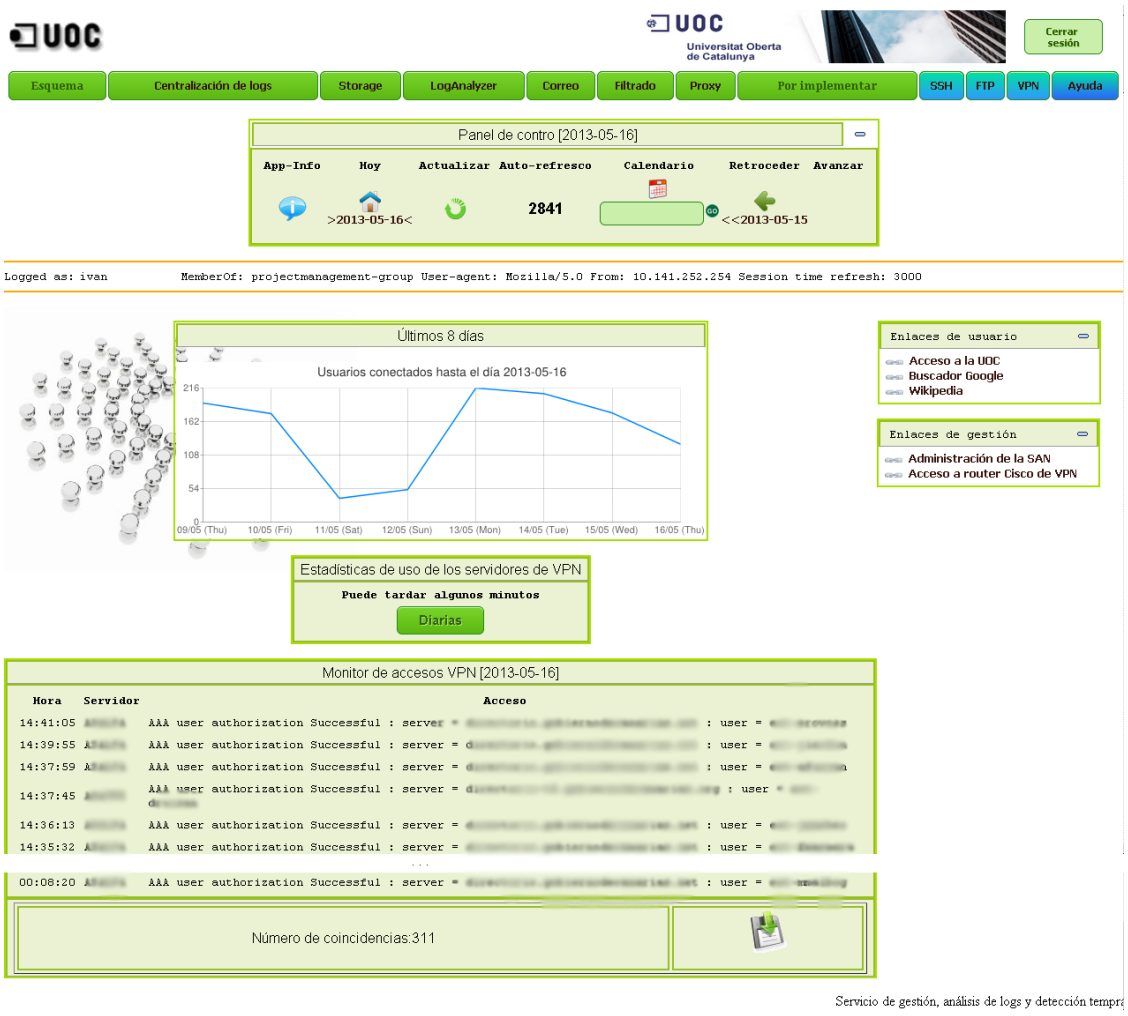


Ilustración 117. Consola. Accesos VPN.

La interfaz ofrece un aspecto y características similares al de las anteriores, salvando que la información reportada es sobre las conexiones VPN realizadas sobre la electrónica de red.

9.1.3.11. Ayuda

Como su propio nombre indica, ofrece una descripción de ayuda sobre cada una de las aplicaciones residentes en la consola:

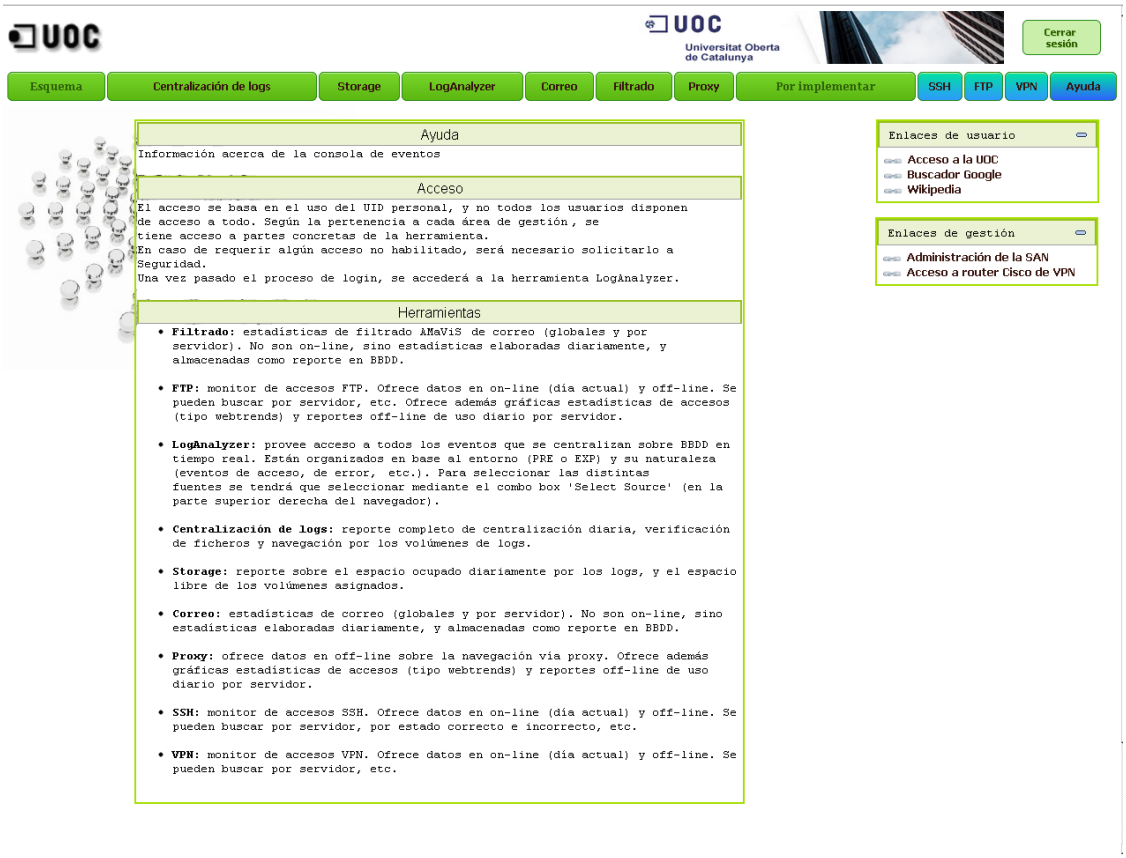


Ilustración 118. Consola. Ayuda rápida.

Esta ayuda es editable y puede ser ampliada de una manera sencilla y rápida:

```
# vi ../private/conf/help-config.php
<?php

$apps_help = array (
 array ( "filter-stats-report", "<b>Filtrado</b>: estad&iacute;sticas de filtrado AMaViS e IMSS de correo (globales y por servidor). No son on-line, sino estad&iacute;sticas elaboradas diariamente, y almacenadas como reporte en BBDD." ),
 array ( "ftp-monitor", "<b>FTP</b>: monitor de accesos FTP. Ofrece datos en on-line (d&iacute;a actual) y off-line. Se pueden buscar por servidor, etc. Ofrece adem&aacute;s gr&aacute;ficas estad&iacute;sticas de accesos (tipo webtrends) y reportes off-line de uso diario por servidor." ),
…
)

?>
```

9.1.4. INCORPORACIÓN DE NUEVAS APLICACIONES

La consola permite la capacidad de modularidad, de tal forma que la incorporación de cualquier aplicación sólo depende de la inclusión de un launcher de la misma en el índice de aplicaciones de la cabecera:

Que como ya se describiera en apartados anteriores, se realizaría modificando el fichero de cabecera oportuno:

```
[root@tfc]# vi header.php
…
     <table width='100%'>
      <tr>
…
       <td class='header_button'><div onclick=\"TINY.box.show({html:'Sin
implementar',animate:false,close:false,mask:false,boxid:'error',autohide:3,top:400,left:500})\">Por
implementar</a></td>
…
      </tr>
     </table>
…
```

10. ANÁLISIS DE RESULTADOS

Sin querer pasar por alto un análisis cualitativo de las bondades de un sistema centralizado de log y eventos, de las cuales hemos hablado en más de un apartado del presente documento, quizás la forma más adecuada de objetivar los resultados del proyecto sea enfrentarnos a la solvencia del mismo reflejada en números. Estos reflejan, las siguientes situaciones:

1. La centralización de LOGS, entre históricos añadidos (periodo establecido 2 anualidades -2011 /2012-) y datos recopilados por el presente proyecto -2013-, gestiona un repositorio de casi 3Tb de información, distribuidos en dos volúmenes SAN (uno para cada entorno):
   - PRE-explotación : 500 GB
   - Producción: 2 GB
2. La centralización de LOGS, gestiona una media de 1,2 Gb de información diaria, un promedio de 36 Gb mensuales y se estima que 0,5 Tb anuales, todo en formato comprimido. Con la siguiente distribución media:
   - PRE-explotación:

ORIGEN	Nº de HOSTS	Nº de FICHEROS	CANTIDAD	UNIDAD	PERIODO	COMPRESIÓN
MESSASGES	~250	~250	<5	MB	Diario	Si
CRON	~250	~250	<5	MB	Diario	Si
AUTHPRIV	~250	~250	<5	MB	Diario	Si
DAEMON	~250	~250	<5	MB	Diario	Si
FTP	2	12	<5	MB	Diario	Si
MAIL	4	4	<5	MB	Diario	Si
FILTRADO	2	2	<5	MB	Diario	Si
WINDOWS	<10	<10	<5	MB	Diario	Si
PROXY	1	3	<5	MB	Diario	Si
HTTP_ERROR	22	22	<10	MB	Diario	Si
VPN	0	0	0	MB	-	-

Tabla 6. Distribución media diaria de LOGS centralizados en pre-explotación.

- Producción:

ORIGEN	Nº de HOSTS	Nº FICHEROS	CANTIDAD	UNIDAD	PERIODO	COMPRESIÓN
MESSASGES	~300	~300	<10	MB	Diario	Si
CRON	~300	~300	<10	MB	Diario	Si
AUTHPRIV	~300	~300	<10	MB	Diario	Si
DAEMON	~300	~300	<10	MB	Diario	Si
FTP	2	12	<30	MB	Diario	Si
MAIL	16	16	<200	MB	Diario	Si
FILTRADO	12	12	<200	MB	Diario	Si
WINDOWS	<100	<100	<600	MB	Diario	Si
PROXY	2	6	<50	MB	Diario	Si
HTTP_ERROR	44	44	<100	MB	Diario	Si
VPN	2	2	<50	MB	Diario	Si

Tabla 7. Distribución media diaria de LOGS centralizados en producción.

3. La centralización y registro de eventos en BBDD, gestiona unos 24 Gb diarios, 720 Gb mensuales y presumiblemente llegará a unos 8 Tb anuales si se sigue las múltiples exigencias de registro necesarias para garantizar la continuidad de negocio descrito en el esquema de nacional de seguridad[4]. Con la siguiente distribución media:

   - PRE-explotación:

BBDD	Nº de REGISTROS	CANTIDAD	UNIDAD	PERIODO
AUTHPRIV	<3.000.000	<400	MB	Diario
ERROR	<60.000	<100	MB	Diario
FTP	<2.000	<100	MB	Diario
MAIL	<15.000	<400	MB	Diario
WINDOWS_EVENTS	<25.000	<400	MB	Diario
HTTP_ERROR	<10.000	<100	MB	Diario
NETWORK	0	0	-	-

Tabla 8. Distribución media semanal de registro de eventos en BBDD de pre-explotación.

   - Producción:

BBDD	Nº de REGISTROS	CANTIDAD	UNIDAD	PERIODO
AUTHPRIV	<5.000.000	<800	MB	Diario
ERROR	<1.700.000	<800	MB	Diario
FTP	<50.000	<800	MB	Diario
LOG_CENTRALIZER	<10.000	<20	MB	Diario
MAIL	<25.000.000	<4	GB	Diario
WINDOWS_EVENTS	<10.000.000	<16	GB	Diario
HTTP_ERROR	<200.000	<800	MB	Diario
NETWORK	<1.000.000	<120	MB	Diario

Tabla 9. Distribución media semanal de registro de eventos en BBDD de producción.

[4] http://administracionelectronica.gob.es/recursos/PAE_12924042225654266.pdf?iniciativa=146

4. En cuanto al "performace" del servidor de BBDD vemos que los consumos medios de CPU son casi despreciables, como era de esperar la Memoria, con una media de uso del 50% y las entradas/salidas son las variables que más sufren pero sin verse comprometidos.

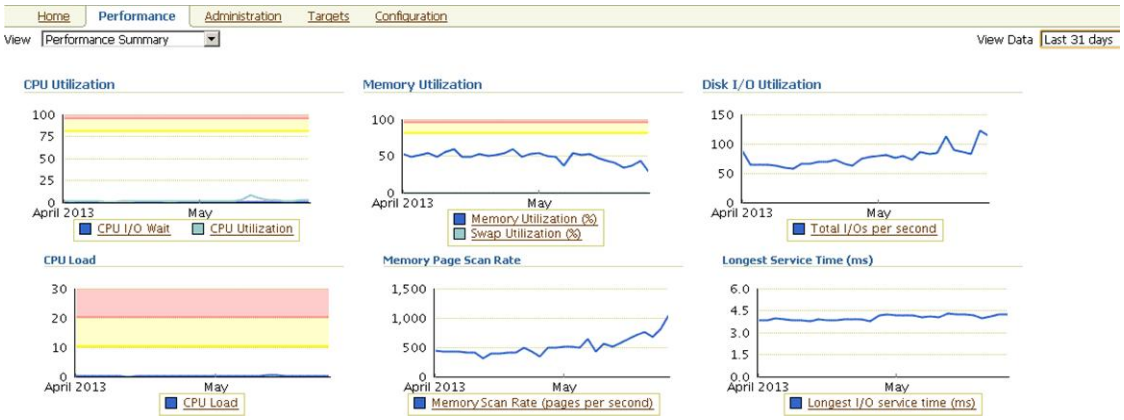


Ilustración 119. Monitorización MySQL de último mes de BBDD con GridControl de Oracle.

De igual forma, este hecho se ve evidenciado por el diagnostico de salud de la adminstración de MySQL, con uso del máximo de conexiones definidas del 61% y con cerca de 530 querys SQL simultaneas y con una tasa de éxito de 99% de "eficiciencia de clave" (tasa de busqueda de claves dentro de la memoria sin acceder a disco)

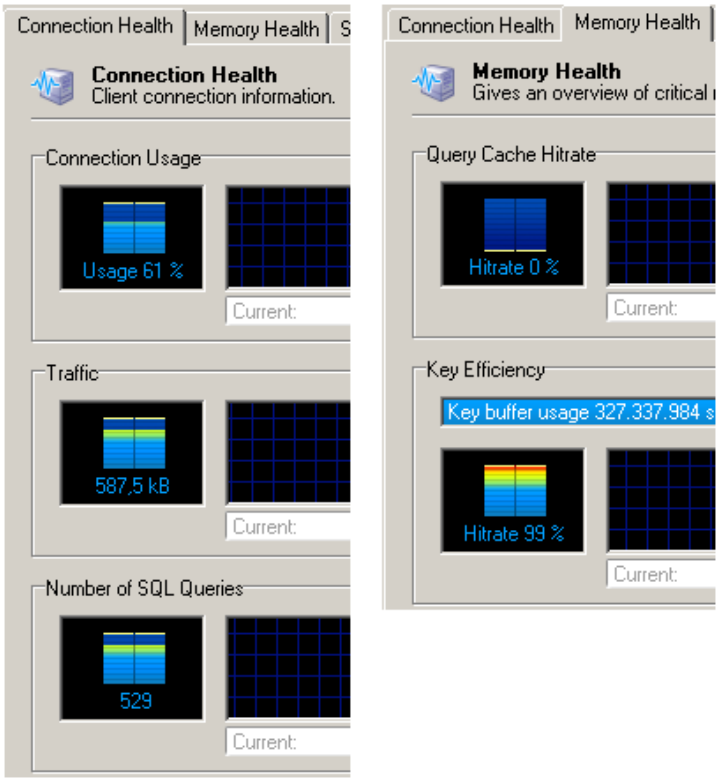


Ilustración 120. MySQL Administrator. Connection and Memory Health de BBDD.

10.1. CONCLUSIONES

Sin duda, la primera y fundamental conclusión del proyecto es la demostración explicita de la **capacitación del software libre** (GNU/Linux) para construir un sistema de registro, centralización y análisis de eventos en un entorno **corporativo extenso y multiplataforma**. Que estos son, a día de hoy, una alternativa viable frente a soluciones propietarias, garantizando con solvencia la funcionalidad ante los requisitos más exigentes.

La primera derivada de esta conclusión, nos lleva a nuestra segunda gran conclusión y no por ello menos importante: la viabilidad de un **sistema centralizado para la gestión de eventos basado en base de datos transaccional**. Testado, en un entorno heterogéneo y extenso como el existente en el desarrollo de este proyecto ha demostrado comportarse adecuadamente. Despejando, el camino hacia cualquier otro sistema más optimizado para análisis como pudiera ser BigQuery[5]

[5] https://developers.google.com/bigquery/docs/overview

11. BIBLIOGRAFÍA Y REFERENCIAS

http://tools.ietf.org/html/rfc5424
http://www.syslog.org/
http://es.wikipedia.org/wiki/Syslog
http://rsync.samba.org
http://everythinglinux.org/rsync/
http://magnifico.wordpress.com/2009/06/03/rsync-el-mejor-sistema-de-copias-de-seguridad/
http://www.securitywarriorconsulting.com/logtools/
http://socialcompare.com/en/comparison/syslog-1odpp9z7
http://webdesign.about.com/od/loganalysis/tp/free_web_log_analysis_tools.htm
http://ocubom.wordpress.com/2010/10/13/syslog-la-piedra-angular-de-los-registros-del-sistema/
http://kb.monitorware.com/general-f29.html
http://www.rsyslog.com/doc/rsyslog_ng_comparison.html
http://czanik.blogs.balabit.com/2011/06/a-comparison-of-syslog-ng-web-guis/
http://www.weblogexpert.com
http://www.chrisbrenton.org/2009/08/setting-up-a-security-information-management-system-part4/
https://access.redhat.com/support/policy/update_policies.html
https://access.redhat.com/knowledge/docs/Red_Hat_Enterprise_Linux/
http://www.perihel.at/3/index.html#rsync
http://www.vescudero.net/2011/05/zsync-alternativa-rsync-para.html
http://www.cygwin.com/
http://www.aboutmyip.com/AboutMyXApp/DeltaCopy.jsp
http://www.rsyslog.com/doc/features.html
http://czanik.blogs.balabit.com/2011/09/syslog-clients-for-windows/
http://ntsyslog.sourceforge.net/
http://syslog-win32.sourceforge.net/
http://www.winsyslog.com/common/en/products/winsyslog8-editions.php
https://code.google.com/p/eventlog-to-syslog/
http://edoceo.com/creo/winlogd
http://www.intersectalliance.com/projects/SnareWindows/index.html
http://logreporters.sourceforge.net/
http://logstash.net/
http://loganalyzer.adiscon.com/
http://webdesign.about.com/od/loganalysis/tp/free_web_log_analysis_tools.htm
http://www.debianhelp.co.uk/syslogngweb.htm
http://www.linux-magazine.es/issue/15/Amavisd.pdf
http://en.wikipedia.org/wiki/Webalizer
http://www.webalizer.org/
http://awstats.sourceforge.net/
http://www.abeautifulsite.net/blog/2007/06/php-file-tree/
http://jquery.com/
http://es.wikipedia.org/wiki/JQuery
http://lifeunix.blogspot.com.es/2012/06/how-to-install-rsyslogmysqlloganalyzer.html
http://loganalyzer.adiscon.com/doc/install.html
http://lifeunix.blogspot.com.es/2012/06/how-to-install-rsyslogmysqlloganalyzer.html
http://loganalyzer.adiscon.com/doc/install.html
http://www.cyberciti.biz/faq/install-php-5-in-red-hat-enterprise-linux-5/
http://ultips.kuntzmann.info/2012/03/installing-proftpd-on-red-hat-el-5-or-6/

http://magazine.redhat.com/2007/04/11/squid-in-5-minutes/
http://dev.antoinesolutions.com/apache-server
http://www.alcancelibre.org/staticpages/index.php/como-apache
http://wiki.rsyslog.com/index.php/Red_Hat
http://www.ehu.es/ehusfera/davidfernandez/tag/red-hat-5/
http://www.misasignaturas.es/?p=420
https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Managing_Confined_Services/chap-Managing_Confined_Services-rsync.html
http://www.aboutmyip.com/AboutMyXApp/DeltaCopy.jsp
http://ntsyslog.sourceforge.net/
http://mogaal.com/articulos/webalizer/webalizer.html
http://hackstips.wordpress.com/2012/02/29/web-stats-analysis-with-webalizer/
http://nfs.sourceforge.net/nfs-howto/ar01s03.html
http://www.cyberciti.biz/faq/centos-fedora-rhel-nfs-v4-configuration/
http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=146
https://developers.google.com/bigquery/docs/overview