LogICA en la UCM

Luis Padilla

Servicios Informáticos UCM

14-junio–2010

XXIX Grupos de Trabajo de RedIRIS

Contenido de la presentación

- Software LogICA v3
- Hardware
- Fuentes
- Tiempo real
  - Reglas de correlación
- Forense
- Puntos fuertes
- Puntos débiles
- Mejoras
- Conclusiones

Software LogICA v3

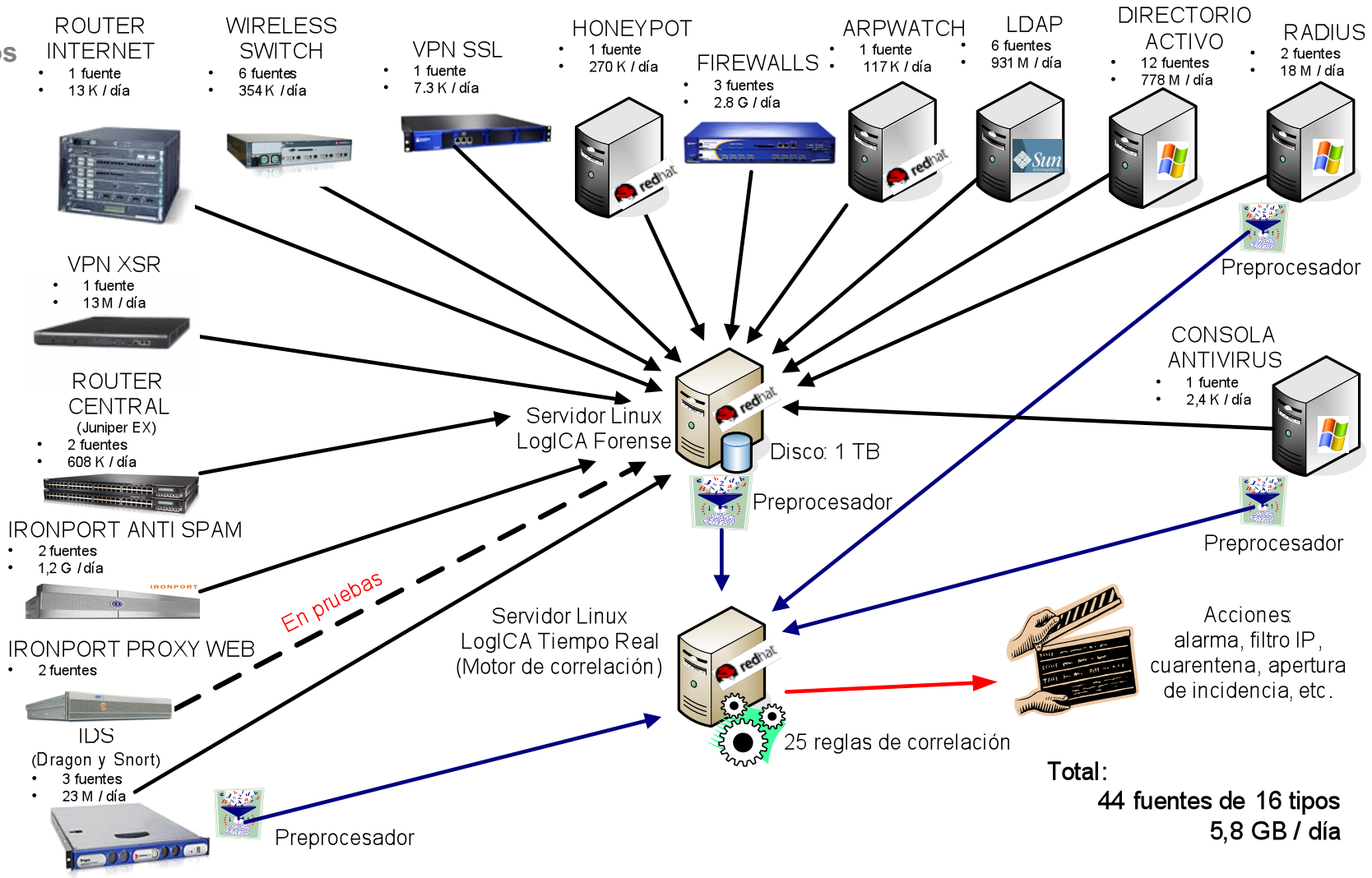
- Basado en JAVA 1.6
- Instalada v2 en 2006, actualizada a v3 en 2008
- Cuatro componentes:
  - Agentes (corren en las fuentes o en el servidor forense)
    - Toman todos los eventos de la fuente (por syslog en el servidor forense o directamente del *log* en la fuente) y los envían a forense
    - Eventos selectos son preprocesados y enviados a tiempo real
  - Forense (corre en servidor dedicado)
    - Recibe todos los eventos y los almacena en el formato original de la fuente
  - Tiempo real (corre en otro servidor dedicado)
    - Recibe eventos selectos preprocesados = alarmas de primer nivel
    - Correlaciona estos eventos => alarmas de segundo nivel
    - Dispara acciones asociadas a las alarmas
  - Consola (corre en los PCs clientes de consulta)

Hardware

- Servidores propios dedicados:
  - Tiempo real
    - CPU: HP Blade BL20p, 4 cores Intel Xeon 3.2 GHz
    - RAM: 8 GB
    - Disco: 200 GB (SAN)
    - S.O.: Red Hat Enterprise Linux ES release 4
    - BD: Oracle (incluida en LogICA)
  - Forense
    - CPU: HP Blade BL20p, 4 cores Intel Xeon 3.2 GHz
    - RAM: 6 GB
    - Disco: 1 TB (SAN)
    - S.O.: Red Hat Enterprise Linux ES release 4
    - BD: Oracle (incluida en LogICA)
  - Agentes
    - En servidor forense, para las fuentes que envían por syslog
    - En las propias fuentes, para los demás casos (JRE 1.6 requerido)
  - Consola
    - Puesto de trabajo recomendado: Windows/Linux, P4 3GHz, 1 GB, 100 MB, JRE 1.6

Fuentes

Servicios Informáticos



Tiempo real

- Correlación de eventos y generación de alarmas
- Base de datos de alarmas (almacén para 1-2 años)
- Ejecución de acciones asociadas a las alarmas
- Edición de las reglas de correlación (formato XML) y de las acciones asociadas a las alarmas
- Sistema de *ticketing* propio y también integración con Remedy
- Búsquedas en los campos de la BD de tiempo real con expresiones EQL (basado en SQL)
- Cuadro de mando (gráficas y listado de alarmas en tiempo real)
- Generación de informes

Tiempo real: reglas de correlación

- 25 reglas de correlación creadas ad hoc
- Para la detección de:
  - Escaneados de puertos y de ordenadores
  - IPs duplicadas
  - Servidores DHCP no autorizados
  - Envío de *spam*
  - Ataques de fuerza bruta
  - Modificaciones del LDAP desde IPs no permitidas
  - Tráfico anómalo de IPs externas en listas negras
- Algunas disparan bloqueos, cuarentenas e incidencias de Remedy
- Resultados en el año 2009 (a partir del 25/02/2009):
  - 201 IPs internas puestas en cuarentena automáticamente
  - 114.976 IPs externas filtradas automáticamente
  - 30.962 otras alarmas investigadas manualmente

Forense

- Almacenamiento de todos los eventos en la forma de los *logs* originales:
  - Tres meses sin comprimir (configurable)
  - El resto (todo desde 2006) comprimido automáticamente con bzip
  - Usado el 50% del espacio total (1 TB) hasta ahora
- Posibilidad de sellado para validez legal
- Búsquedas en los *logs* mediante expresiones regulares (también posible desde la *shell* del S.O.)
- Módulo Achilles (independiente de tiempo real y forense):
  - BD de activos poblada manualmente o conectada con CMDB corporativa
  - Nessus para incluir vulnerabilidades de los activos en la BD

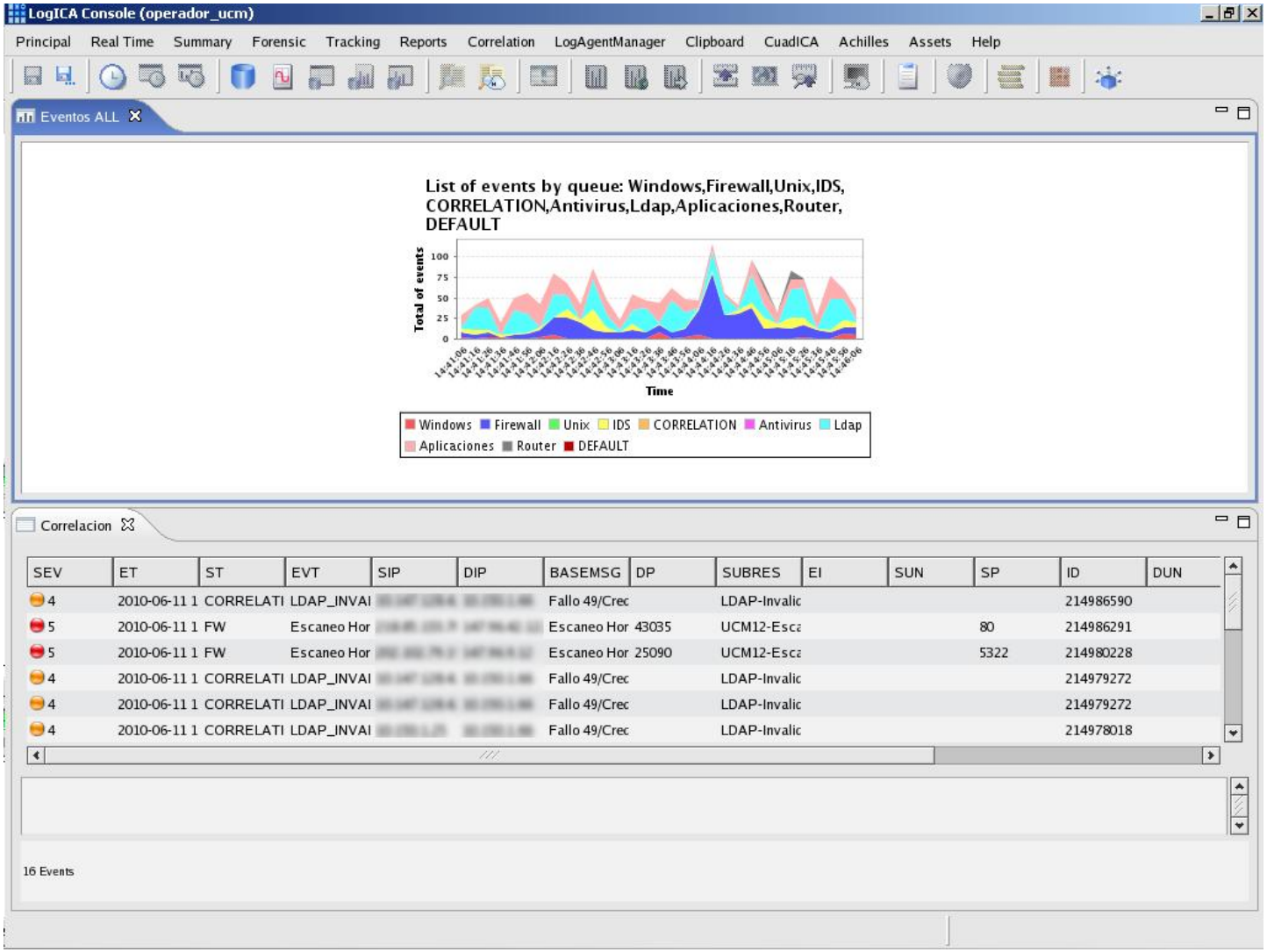
Puntos fuertes

- Integración de todo tipo de fuentes (puede exigir desarrollo propio o contratado)
- Preprocesado de eventos antes del envío a tiempo real
- Almacenamiento de *logs* en formato original
- Flexibilidad en la creación de reglas que permite casi cualquier cosa mediante contextos
- Permite la ejecución de un *script* como acción de una alarma
- Integración con Remedy (indispensable en UCM)

Puntos débiles

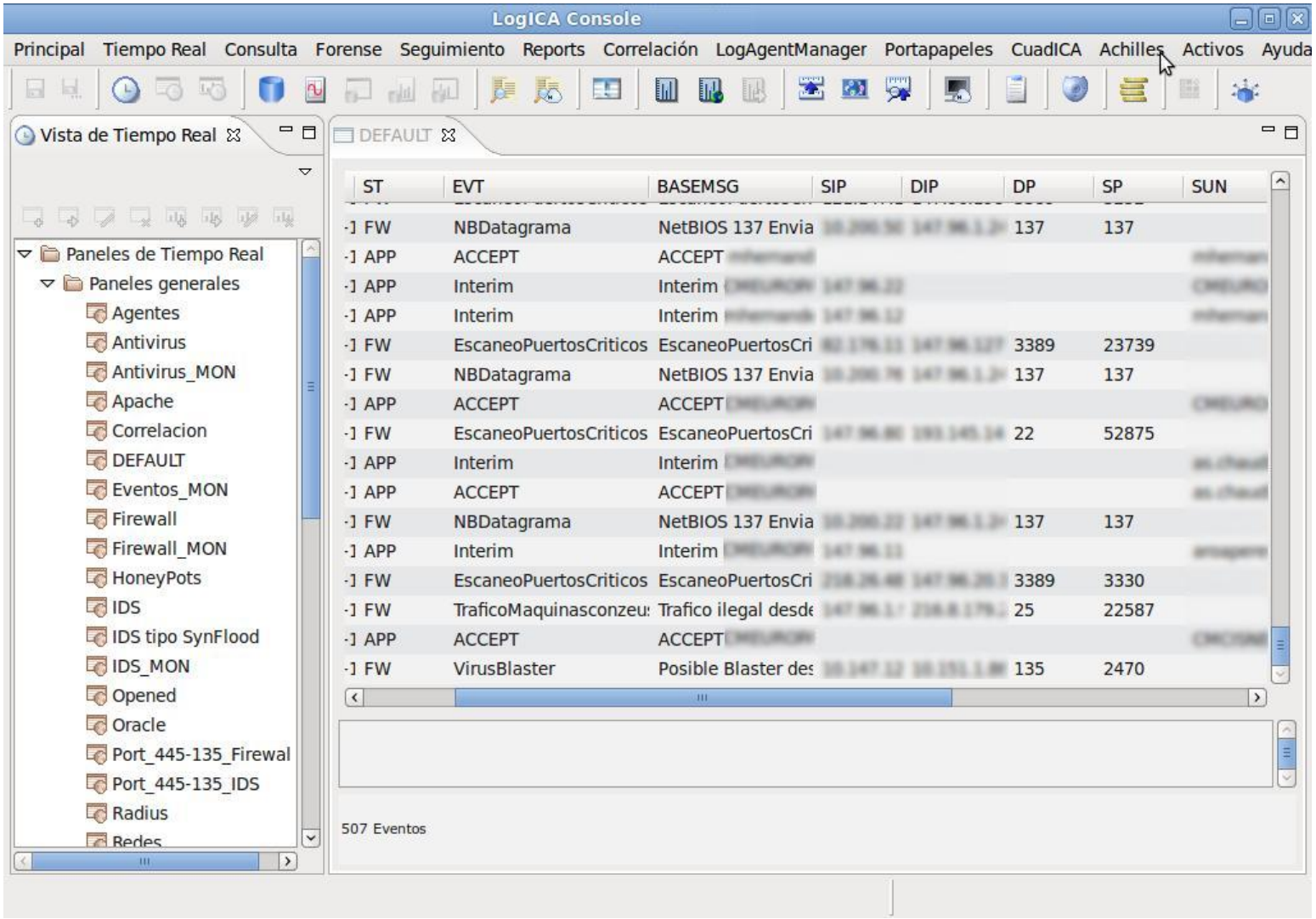
- Instalación, configuración y actualizaciones son tareas muy complejas, que requieren asistencia
- Soporte y documentación bastante mejorables
- Limitación en el alcance temporal de la correlación ⇔ Problemas de memoria
- Estabilidad de los motores y la consola
- Búsqueda de eventos lenta y poco flexible
- Cuadro de mando limitado y poco flexible
- Generación de informes compleja y limitada

Puntos débiles: consola



Servicios Informáticos

Puntos débiles: consola



Mejoras

- Formato *appliance* (ya disponible)
- Integración de flujos de red (no Ntop)
- Inteligencia de correlación propia y listas negras dinámicas
- Categorización de eventos
- Cifrado de *logs* en forense
- Consola más ligera, estable y eficiente (no JAVA)

Conclusiones

- LogICA v3 es una herramienta que cumple de manera económica y satisfactoria las necesidades básicas de un SIEM, disparo de las alarmas y acciones diseñadas para situaciones conocidas, y almacenamiento de *logs*.
- Pero le faltan funcionalidades avanzadas que le permitan detectar peligros desconocidos ya sea de manera automática (reglas de correlación propias, listas negras, anomalías en flujos) o mediante investigación manual (búsqueda en BD de eventos, flujos, cuadro de mando, informes).

Gracias por su atención

LogICA en la UCM

Luis Padilla

Servicios Informáticos UCM

14-junio–2010

XXIX Grupos de Trabajo de RedIRIS