5° Coloquio de proyectos
de Becarios en Seguridad Informática

Optimización de almacenamiento de eventos detectados en sensores del Plan de Sensores de Tráfico Malicioso (PSTM)

Jonatan Revilla López
David Cruz García

UNAM CERT

DGTIC
DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Antecedentes

PSTM

Red de sensores para la identificación de actividad maliciosa en las redes de datos de México con el fin de intercambiar información sobre las amenazas observadas.

TELESCOPIO DE SEGURIDAD UNAM (TSU)

Sistema centralizado para la detección de tráfico de red malicioso a lo largo de RedUNAM y fuera de ella.

Problemática

Información obtenida de los sensores distribuidos en Red UNAM:

- Inserta directamente en la base de datos del telescopio de seguridad
- Existe información redundante
- Degradación del servicio durante consultas a la base de datos

Objetivos

- Optimizar el almacenamiento de eventos detectados en los equipos del PSTM.
- Desarrollar generador de incidentes que procese, optimice y registre los incidentes.
- Integrar el generador de incidentes dentro del despliegue de sensores actual.

Herramientas utilizadas

- Perl
- Snort
- Generador de incidentes (geninc)
- SnortUnified
- Barnyard2
- Shell script
- U2SpewFoo

Introducción

Snort

- IDS / IPS
- Análisis de tráfico en tiempo real
- Basado en reglas
- Registro de eventos
  - Fecha
  - IP origen
  - IP destino
  - Puerto origen
  - Puerto destino
  - Entre otros

Incidente

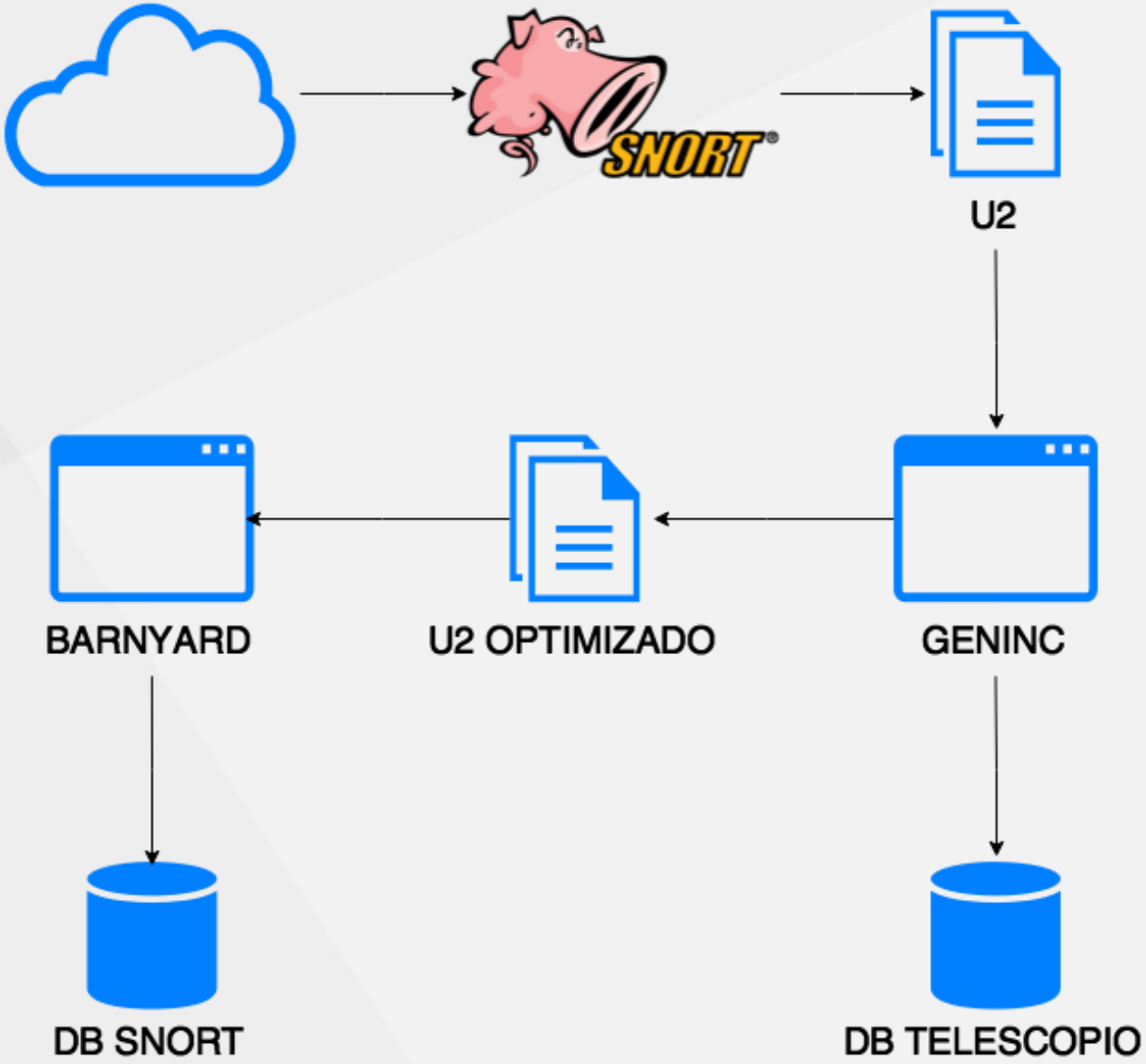
Conformado por uno o más eventos, los cuales tienen en común:

- Protocolo
- Dirección IP origen
- Alerta (Snort)

```
(Event)
    sensor id: 0    event id: 4 event second: 1299698138    event microsecond: 146591
    sig id: 1   gen id: 1   revision: 0  classification: 0
    priority: 0 ip source: 10.1.2.3 ip destination: 10.9.8.7
    src port: 60710 dest port: 80   protocol: 6 impact_flag: 0  blocked: 0

Packet
    sensor id: 0    event id: 4 event second: 1299698138
    packet second: 1299698138   packet microsecond: 146591
    linktype: 1 packet_length: 54
[    0] 02 09 08 07 06 05 02 01 02 03 04 05 08 00 45 00  ..............E.
[   16] 00 28 00 06 00 00 40 06 5C B7 0A 01 02 03 0A 09  .(....@.\.......
[   32] 08 07 ED 26 00 50 00 00 00 62 00 00 00 2D 50 10  ...&.P...b...-P.
[   48] 01 00 A2 BB 00 00                                ......
```

Esquema general



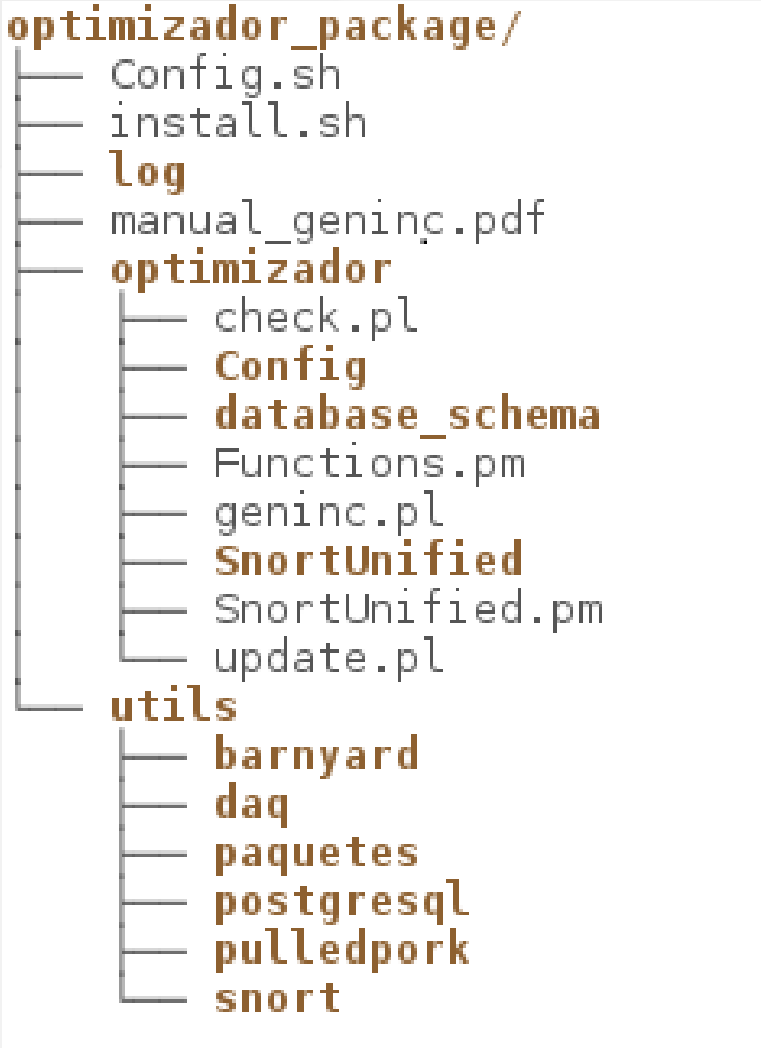
Desarrollo

- Lectura de archivos unified2
- Conteo de eventos por incidente
- Obtención del evento-paquete inicial y el evento-paquete final
- Verificación de cambios en archivos unified2 generados por Snort cada n segundos
- Tratamiento de datos para su inserción en base de datos del telescopio de seguridad

Herramienta

Instalación:

- Offline (standalone)
  - Barnyard2 - 2-1.14
  - Postgresql – 9.4
  - Snort – 2.9.8.3
  - Daq – 2.0.6
  - PulledPork
  - Utilerías
- Online
- Logs de instalación



Herramienta

Características:

- Procesamiento de un único archivo
- Procesamiento en batch
- Procesamiento en modo demonio
- Generación de bitácoras de ejecución
- Generación de sentencias SQL
- Inserción en base de datos central
- Generación de archivos unified2 optimizados por incidente

Configuración

Variables importantes:

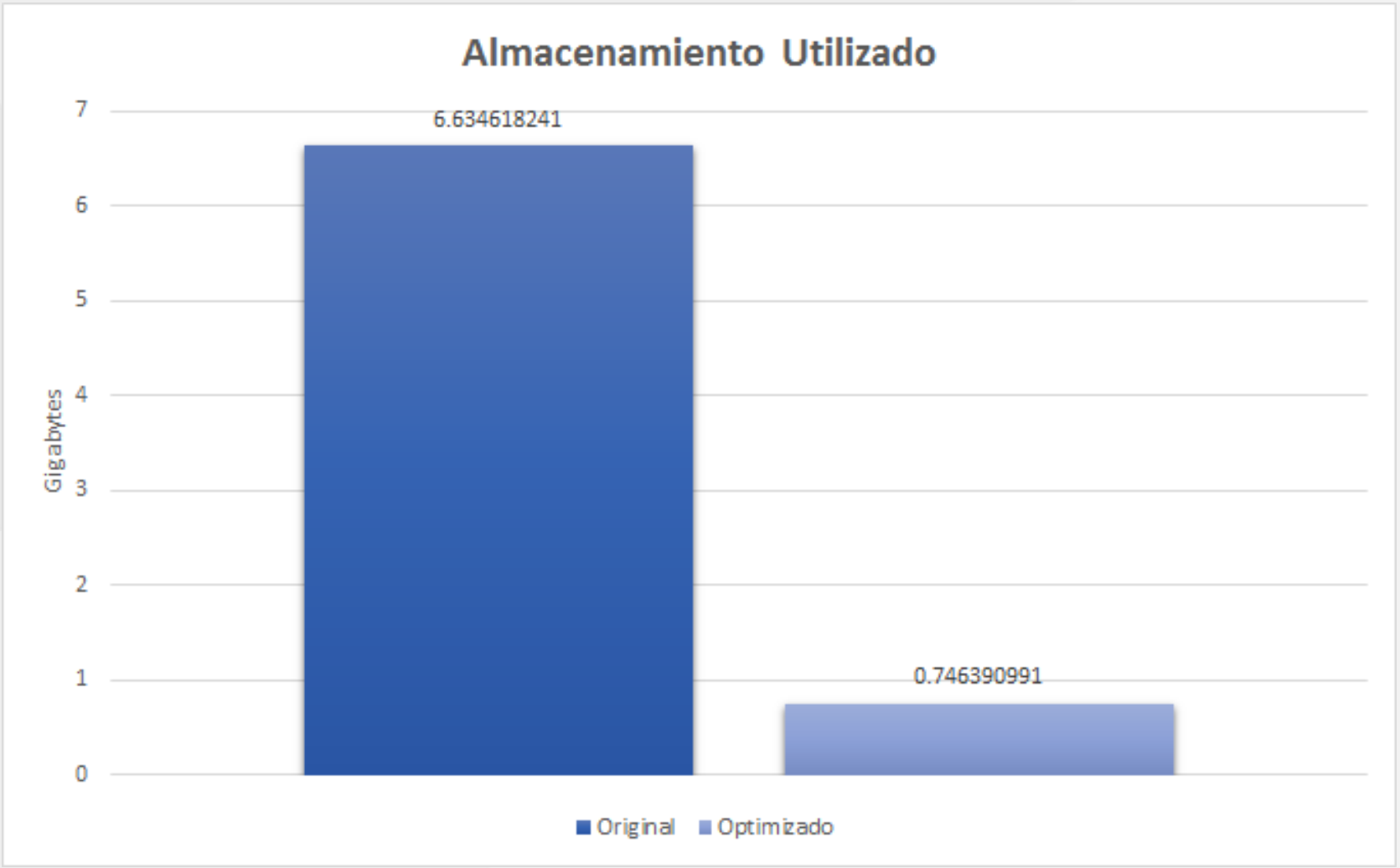
- Usuario y contraseña de BD central
- Tiempo de espera entre cada revisión de cambios en unified2 generados por Snort
- Nombre del sensor
- Modo debug

Funcionamiento

sig_id: 1, ip_source: 10.1.2.3, protocol: 6
event_id : 10, event_second: 1487274129
sig_id: 1, ip_source: 10.1.2.3, protocol: 6
event_id : 11, event_second: 1487274129
. . .
sig_id: 1, ip_source: 10.1.2.3, protocol: 6
event_id: 100, event_second: 1487274131
sig_id: 1, ip_source: 10.1.2.3, protocol: 6
event_id: 101, event_second: 1487274131

Sig_id: 1, ip_source: 10.1.2.3, protocol: 6
event_id: 10, event_second: 1487274129
Sig_id: 1, ip_source: 10.1.2.3, protocol: 6
event_id: 101, event_second: 1487274131

Resultados

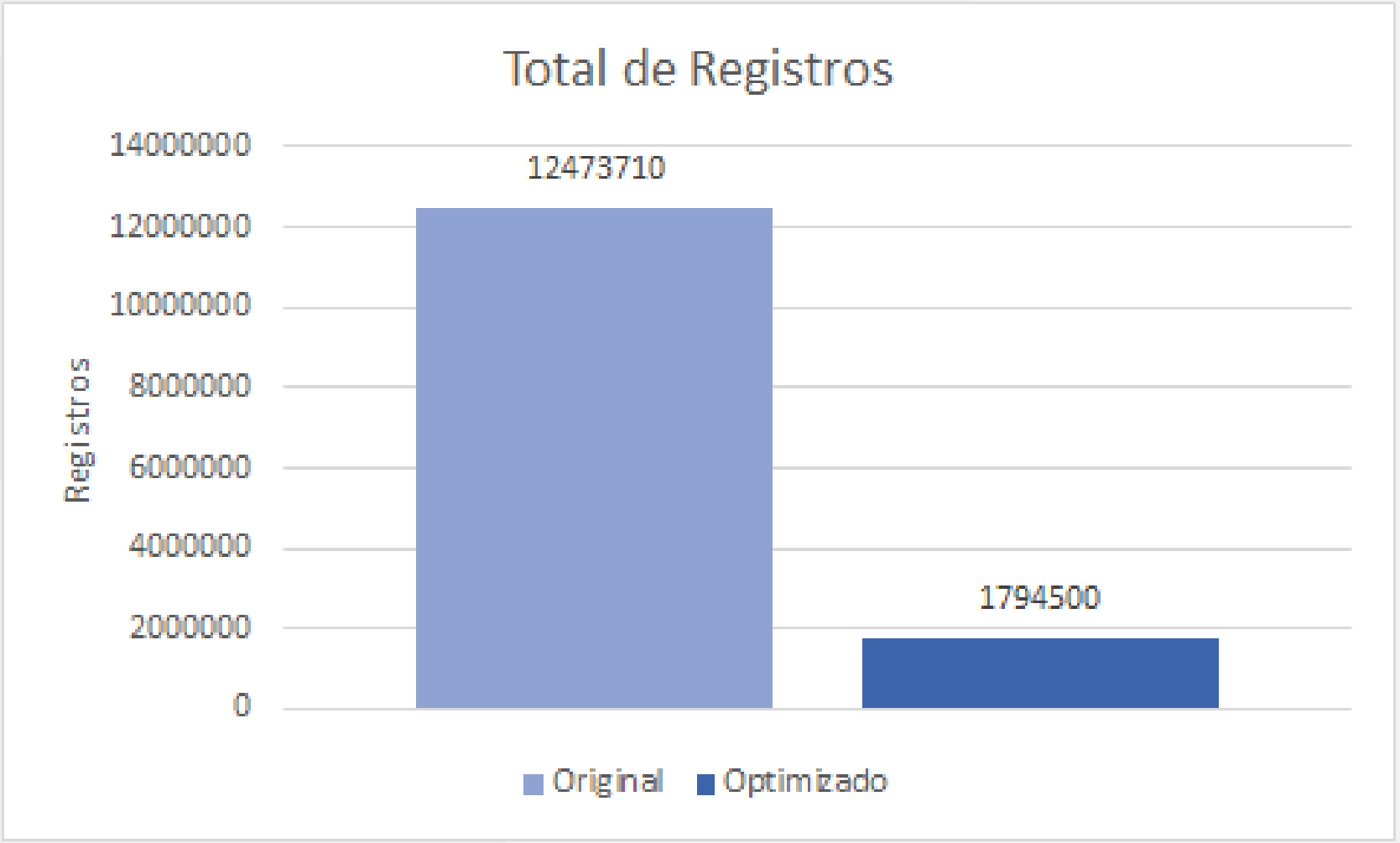


Se redujo un **88.75%** el espacio utilizado

Resultados


Registros
2500000
2000000
1500000
1000000
500000
0
Registros
10/24/2016
10/31/2016
11/07/2016
11/14/2016
11/21/2016
11/28/2016
12/05/2016
12/12/2016
12/19/2016
12/26/2016
01/02/2017
01/09/2017
Semanas
Incidentes
Eventos

Resultados


Total de Registros
14000000
12000000
10000000
8000000
6000000
4000000
2000000
0
Registros
12473710
1794500
Original
Optimizado

Problemas que se presentaron

- Obtención de paquetes de instalación para modo fuera de línea
- Marcador de último evento procesado en archivos unified2

Conclusiones

- Mejoró el rendimiento en consultas a la base de datos
- Se redujo el tamaño de los archivos generados y el numero de registros almacenados en la base de datos

GRACIAS

David Cruz García
FES Acatlán
dvdcrz@comunidad.unam.mx

Jonatan Revilla López
Departamento de Sistemas
UNAM-CERT
jonatan.revilla@cert.unam.mx