splunk™

# Splunk – Up & Running

stratebi
open business intelligence

# Índice

- Presentación Stratebi
- Introducción
  - ¿Qué es?
  - Servidores monitorización
  - Tipos de monitorización
- Integración Splunk & Pentaho
  - Kettle EE
  - Splunk API
  - Recursos visuales
    - Dashboards
    - Tablas dinámicas

# Sobre nosotros - Stratebi

**www.stratebi.com**

stratebi
open business intelligence

# Confían en Business Intelligence Open Source

## Sector Privado

BBVA
EROSKI
Blanco
Redsýs ServiRed
YELL
sage
AMERSAM
amper
SIGAUS
MRW
pepecar.com
opinat
20:20mobile
MútuaTerrassa
EQUIFAX
BOSCH
accenture High performance. Delivered.
PKW
Asmius
Italfarmaco
HAMBURG SÜD
ELDON
Unilever
educaweb

## Sector Público

ICEX
Agencia Tributaria
SERVICIO CANARIO DE SALUD
SaludMadrid
UOC www.uoc.edu
Ayuntamiento de Arrecife
Instituto Cervantes
Diputació de Tarragona
Extremadura
CSIC
Port de Barcelona
EOI Escuela de organización industrial
Mancomunidad de Montejurra Jurramendiko Mankomunitatea
REUS TRANSPORT
Dipsalut
Universitat de Lleida
Gobierno de La Rioja
Instituto Tecnológico de Canarias ITC
Txingudiko Zerbitzuak Servicios de Txingudi
ICANE Instituto Cántabro de Estadística
Govern de les Illes Balears
Caixa d'Enginyers
infoCaja

stratebi
open business intelligence

# Splunk – Up & Running

splunk™ >

stratebi
open business intelligence

# ¿Qué es?

Splunk es un software para **buscar**, **monitorizar** y **analizar datos** generados por máquinas de aplicaciones, sistemas e infraestructura IT a través de un **interfaz web**.
Splunk captura, indexa y correla en Tiempo Real, almacenándolo todo en un **repositorio** donde busca para generar gráficos, alertas y paneles fácilmente definibles por el usuario.

Splunk ofrece el software en dos veriones:

- Pago (Enterprise License) diseñada para empresas,
- Gratuita "Free License" diseñada para uso personal.

La versión freeware está limitada a 500 MB de datos al día,

# ¿Qué es?

- El objetivo de Splunk es hacer los datos de estas máquinas accesible a toda la organización, permitiendo la identificación de patrones, realización de medidas, diagnosis de problemas y provisión de inteligencia (Business Intelligence) a cualquier parte del negocio.

- Splunk es una tecnología que escala a nivel horizontal usada para gestión de aplicaciones: security, compliance, business y web analytics.

- Splunk tienen más de 3,700 clientes licenciados en 74 países, incluyendo más de la mitad de las Fortune 100

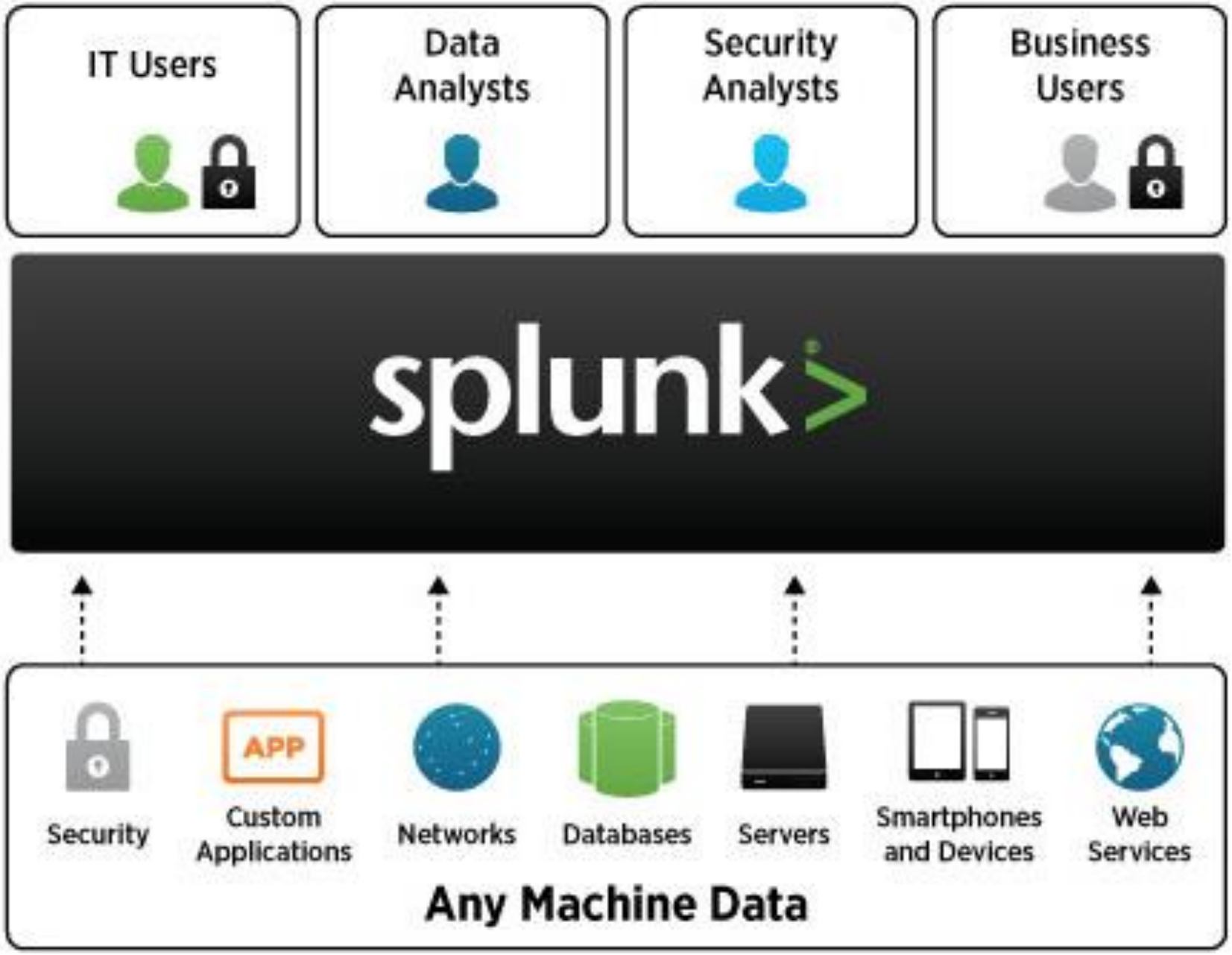
# Diferentes tipos de monitorización

# Soporte a cualquier tipo de servidor

# Soporte a cualquier tipo de servidor

| Platform | Version | Installer | Notes |
|---|---|---|---|
| | Windows Vista, 7, and 8 (64-bit)<br>Windows Server 2003, 2003 R2, 2008, 2008 R2, and 2012 (64-bit) | 6.0<br>splunk-6.0-182037-x64-release.msi | Release Notes |
| | Windows Vista, 7, and 8 (32-bit)<br>Windows Server 2003, 2003 R2, 2008, and 2008 R2 (32-bit) | 6.0<br>splunk-6.0-182037-x86-release.msi | Release Notes |
| | 2.6+ kernel Linux distributions (64-bit) | 6.0<br>splunk-6.0-182037-linux-2.6-x86_64.rpm<br>splunk-6.0-182037-linux-2.6-amd64.deb<br>splunk-6.0-182037-Linux-x86_64.tgz | Release Notes |
| | 2.6+ kernel Linux distributions (32-bit) | 6.0<br>splunk-6.0-182037-Linux-i686.tgz<br>splunk-6.0-182037.i386.rpm<br>splunk-6.0-182037-linux-2.6-intel.deb | Release Notes |
| solaris | Solaris 10, 11 (64-bit) | 6.0<br>splunk-6.0-182037-SunOS-x86_64.tar.Z<br>splunk-6.0-182037-solaris-10-intel.pkg.Z | Release Notes |
| solaris | Solaris 10 (32-bit) | 6.0<br>splunk-6.0-182037-solaris-9-intel.pkg.Z<br>splunk-6.0-182037-SunOS-i386.tar.Z | Release Notes |
| solaris | Solaris 10, 11 (SPARC) | 6.0<br>splunk-6.0-182037-solaris-9-sparc.pkg.Z<br>splunk-6.0-182037-SunOS9-sparc.tar.Z | Release Notes |
| | OSX 10.7 (Intel)<br>OSX 10.8 (Intel) | 6.0<br>splunk-6.0-182037-macosx-10.7-intel.dmg<br>splunk-6.0-182037-darwin-64.tgz | Release Notes |

# Diferentes accesos



# Ejemplo: Monitorización de Memoria

splunk> Search

Administrator | App | Manager | Alerts | Jobs | Logout

Summary | Search | Status | Dashboards & Views | Searches & Reports | Help | About

Search

Verbose Mode

source="Perfmon:DatosMemoria"

All time

≥ 7,534 matching events | 20,059 scanned events

Auto-pausing in 25 seconds. Cancel

Save | Create

Hide | Zoom out | Zoom to selection | Deselect | Linear scale | 1 bar = 1 minute

200
100

9:30 AM Mon Oct 7 2013 | 9:45 AM | 10:00 AM | 10:15 AM | 10:30 AM

Hide

≥ 7,534 events over all time

Export | Options | « prev 1 2 3 4 5 6 7 8 9 10 next » | 10 per page

3 selected fields — Edit

- host (1)
- source (1)
- sourcetype (1)

10 interesting fields

- collection (1)
- counter (35)
- index (1)
- linecount (1)
- object (1)
- punct (14)
- splunk_server (1)

1 — 10/7/13 10:46:40.656 AM

```
10/07/2013 10:46:40.656
collection=DatosMemoria
object=Memoria
counter="Uso máximo de los bytes de caché"
Value=422821888
host=STRATEBI-011 | sourcetype=Perfmon:DatosMemoria | source=Perfmon:DatosMemoria
```

2 — 10/7/13 10:46:40.656 AM

```
10/07/2013 10:46:40.656
collection=DatosMemoria
object=Memoria
counter="Total de bytes de código del sistema"
Value=4550656
host=STRATEBI-011 | sourcetype=Perfmon:DatosMemoria | source=Perfmon:DatosMemoria
```

3 — 10/7/13 10:46:40.656 AM

```
10/07/2013 10:46:40.656
collection=DatosMemoria
object=Memoria
```

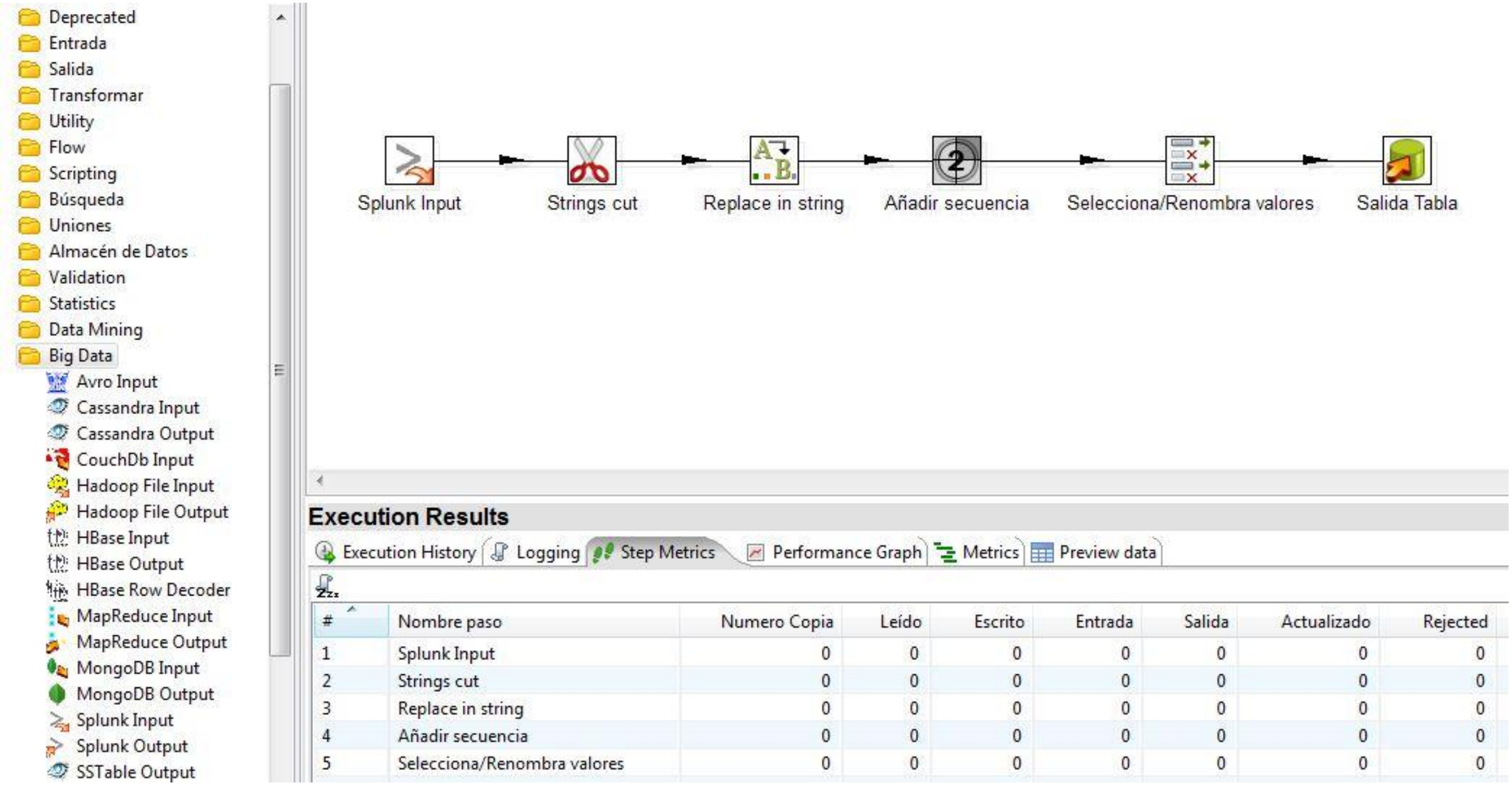
# Integración con Pentaho

splunk™ > pentaho

stratebi
open business intelligence

# Splunk y Pentaho

# Extracción de datos (Kettle EE)




| # | Nombre paso | Numero Copia | Leído | Escrito | Entrada | Salida | Actualizado | Rejected |
|---|---|---|---|---|---|---|---|---|
| 1 | Splunk Input | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | Strings cut | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | Replace in string | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | Añadir secuencia | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | Selecciona/Renombra valores | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

# Extracción de datos (Splunk API): php, java…

## Overview of the Splunk SDK for Java

Welcome to the Splunk® Software Development Kit (SDK) for Java!

This SDK is open source and uses the Apache v2.0 license. If you want to make a code contribution, go to the Open Source page for more information.

This overview tells you more about:

- What you can do with the Splunk SDK for Java
- The Splunk SDK for Java components

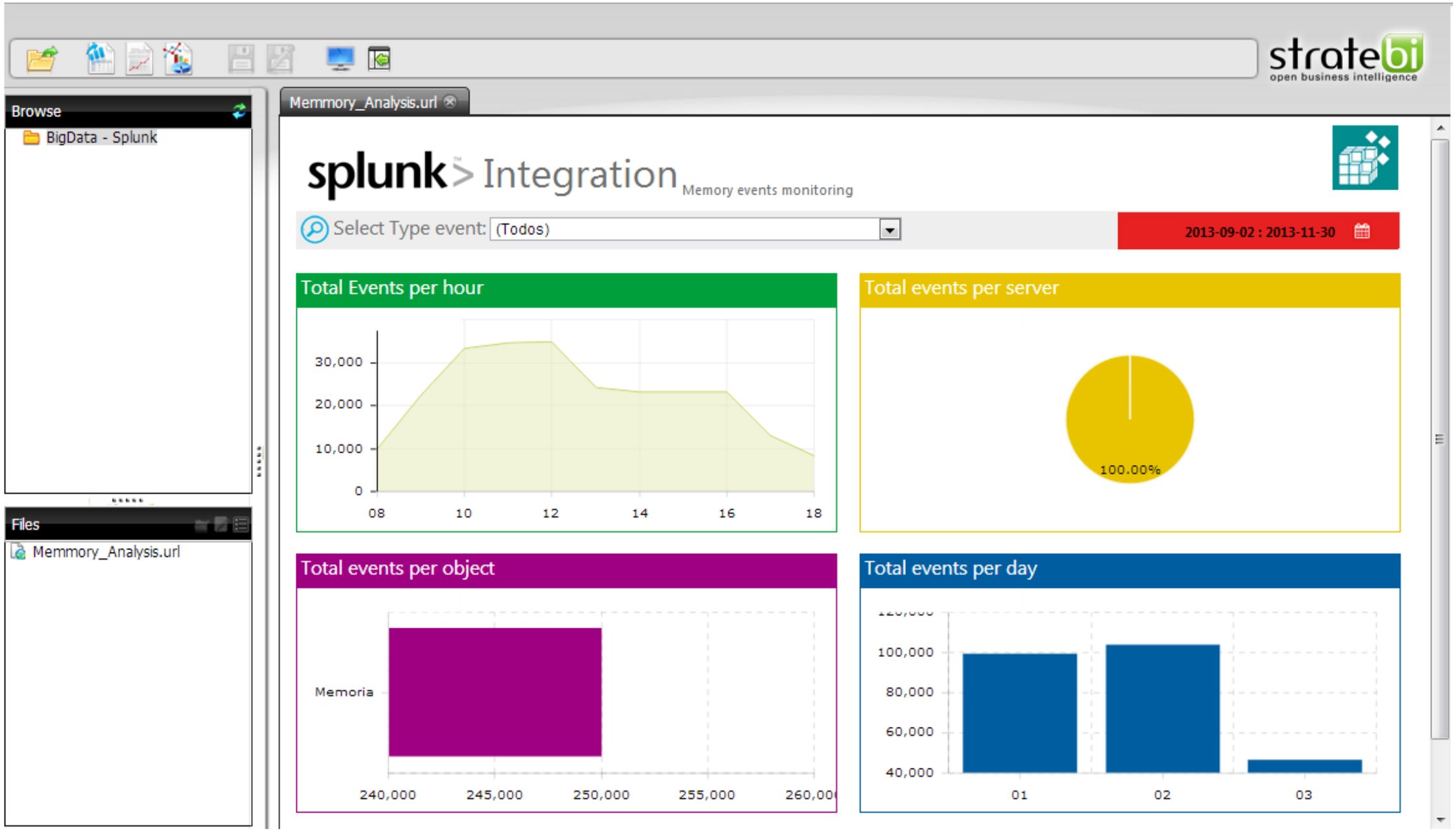
### What you can do with the Splunk SDK for Java

This SDK contains library code and examples designed to enable developers to build applications using Splunk. With the Splunk SDK for Java you can write Java applications to programmatically interact with the Splunk engine. The SDK is built on top of the REST API, providing a wrapper over the REST API endpoints. So with fewer lines of code, you can write applications that:

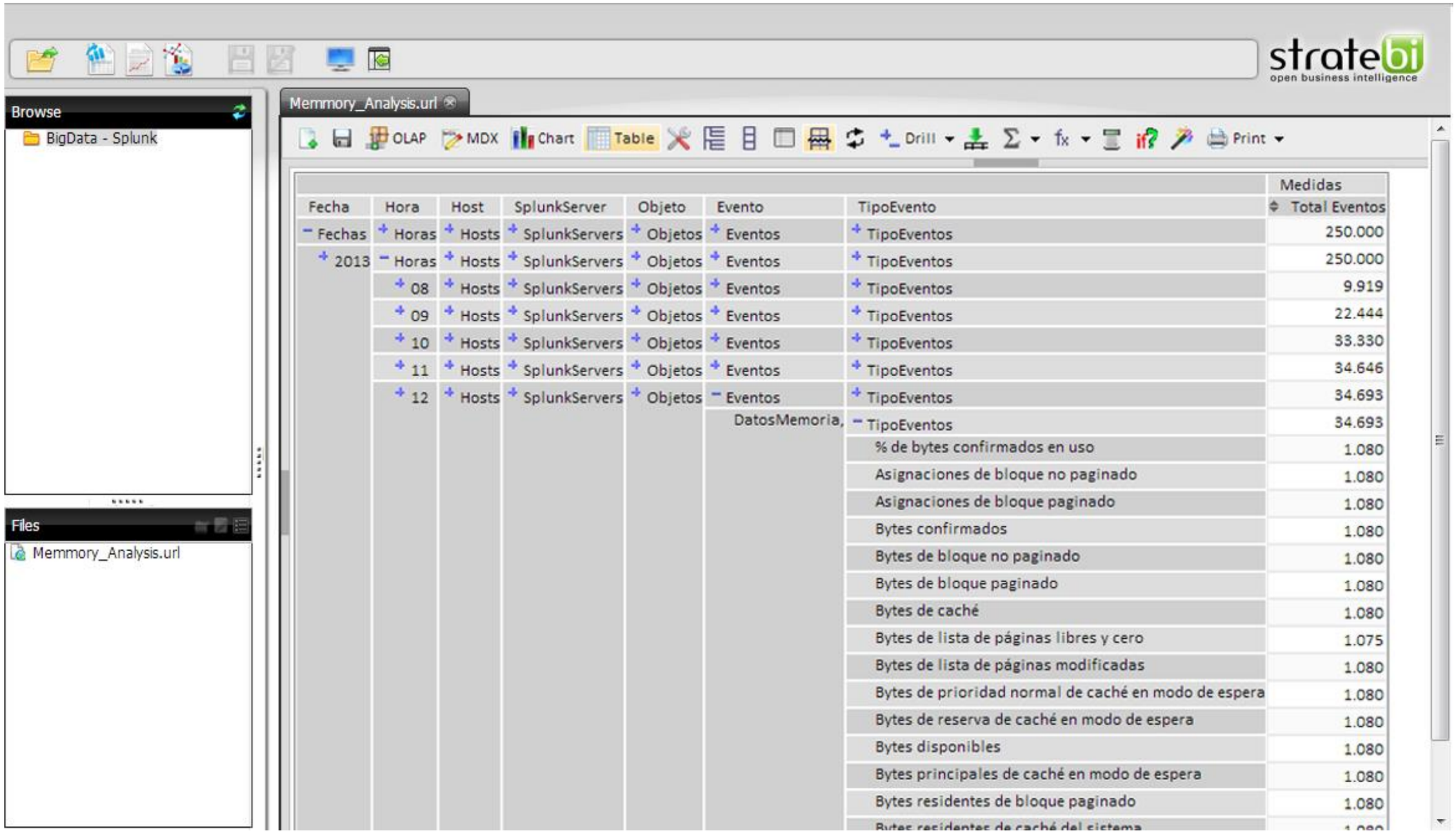
- Search your data, run saved searches, and work with search jobs.
- Manage Splunk configurations and objects.
- Integrate search results into your applications.
- Log directly to Splunk.
- Present a custom UI.

With the Splunk SDK for Java, you can use different tools and IDEs. We even have a plug-in for the Eclipse IDE that makes development even easier. Here's an example application that was created using NetBeans (of course, we also have project-level support for Eclipse and IntelliJ). This Splunk Explorer application shows the values of various settings in your local Splunk instance:

# Nuevos Dashboards y recursos de análisis

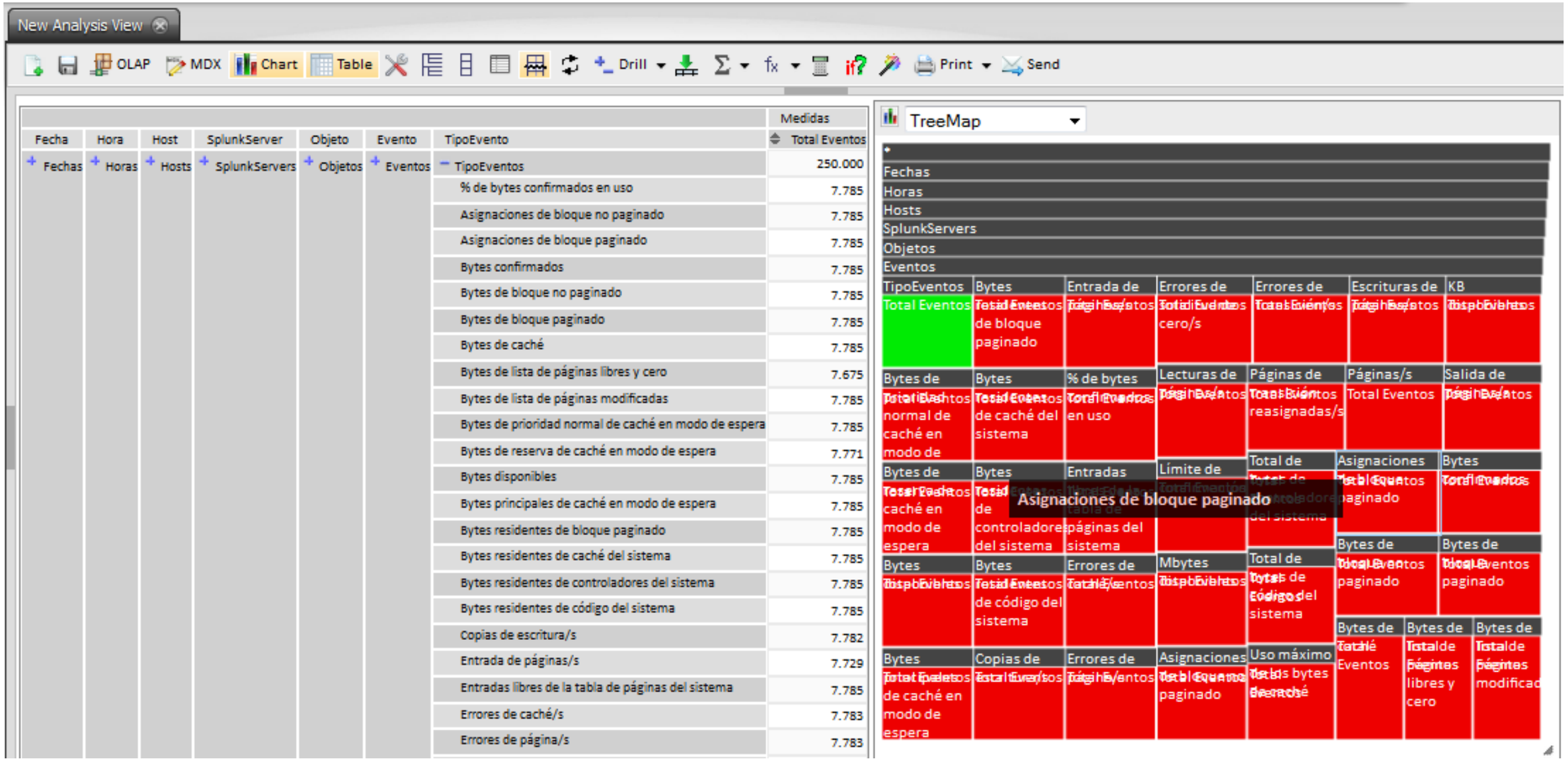


# Nuevos Dashboards y recursos de análisis



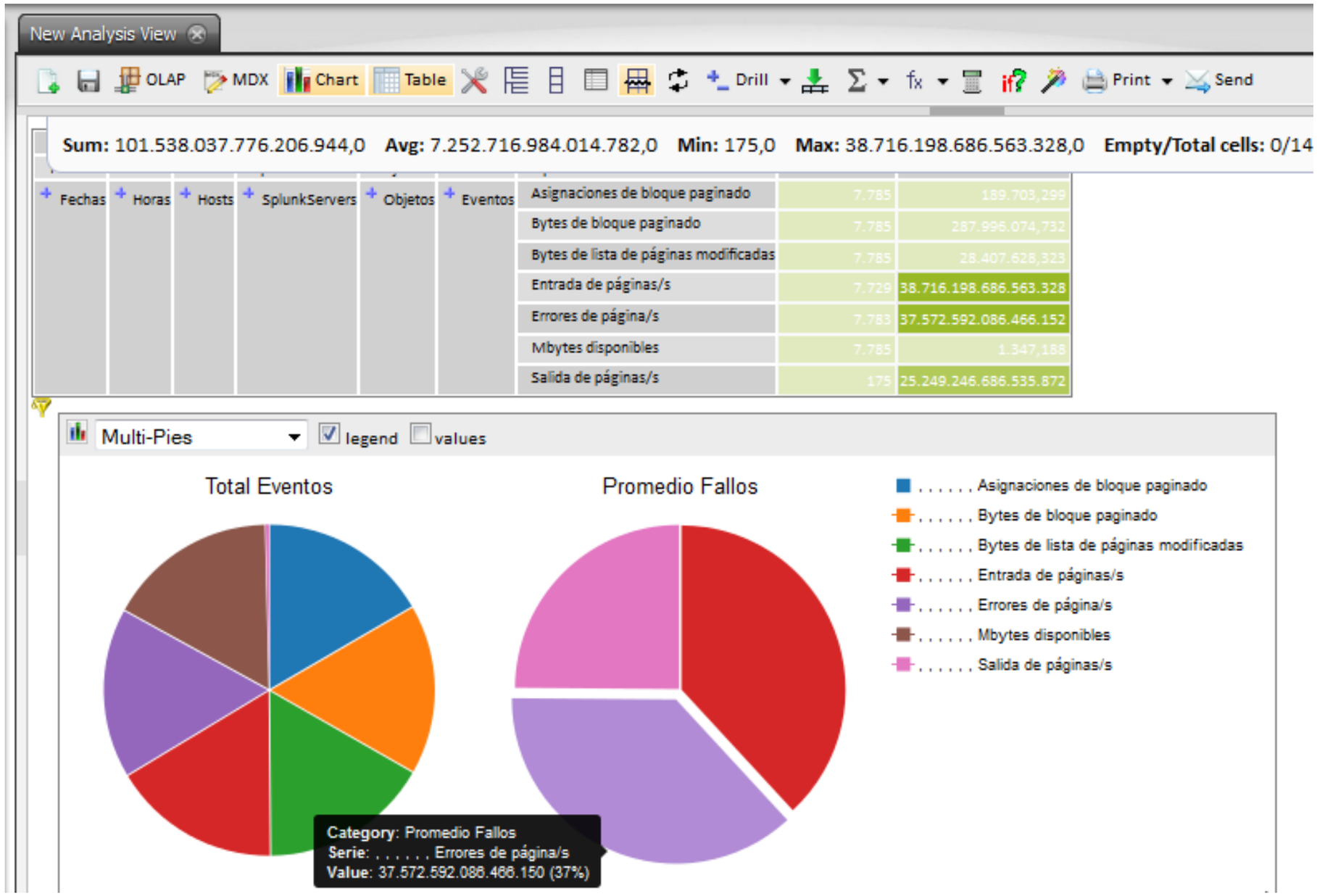

| Fecha | Hora | Host | SplunkServer | Objeto | Evento | TipoEvento | Medidas: Total Eventos |
|---|---|---|---|---|---|---|---|
| − Fechas | + Horas | + Hosts | + SplunkServers | + Objetos | + Eventos | + TipoEventos | 250.000 |
| + 2013 | − Horas | + Hosts | + SplunkServers | + Objetos | + Eventos | + TipoEventos | 250.000 |
| | + 08 | + Hosts | + SplunkServers | + Objetos | + Eventos | + TipoEventos | 9.919 |
| | + 09 | + Hosts | + SplunkServers | + Objetos | + Eventos | + TipoEventos | 22.444 |
| | + 10 | + Hosts | + SplunkServers | + Objetos | + Eventos | + TipoEventos | 33.330 |
| | + 11 | + Hosts | + SplunkServers | + Objetos | + Eventos | + TipoEventos | 34.646 |
| | + 12 | + Hosts | + SplunkServers | + Objetos | − Eventos | + TipoEventos | 34.693 |
| | | | | | DatosMemoria, | − TipoEventos | 34.693 |
| | | | | | | % de bytes confirmados en uso | 1.080 |
| | | | | | | Asignaciones de bloque no paginado | 1.080 |
| | | | | | | Asignaciones de bloque paginado | 1.080 |
| | | | | | | Bytes confirmados | 1.080 |
| | | | | | | Bytes de bloque no paginado | 1.080 |
| | | | | | | Bytes de bloque paginado | 1.080 |
| | | | | | | Bytes de caché | 1.080 |
| | | | | | | Bytes de lista de páginas libres y cero | 1.075 |
| | | | | | | Bytes de lista de páginas modificadas | 1.080 |
| | | | | | | Bytes de prioridad normal de caché en modo de espera | 1.080 |
| | | | | | | Bytes de reserva de caché en modo de espera | 1.080 |
| | | | | | | Bytes disponibles | 1.080 |
| | | | | | | Bytes principales de caché en modo de espera | 1.080 |
| | | | | | | Bytes residentes de bloque paginado | 1.080 |
| | | | | | | Bytes residentes de caché del sistema | 1.080 |

# Nuevos Dashboards y recursos de análisis

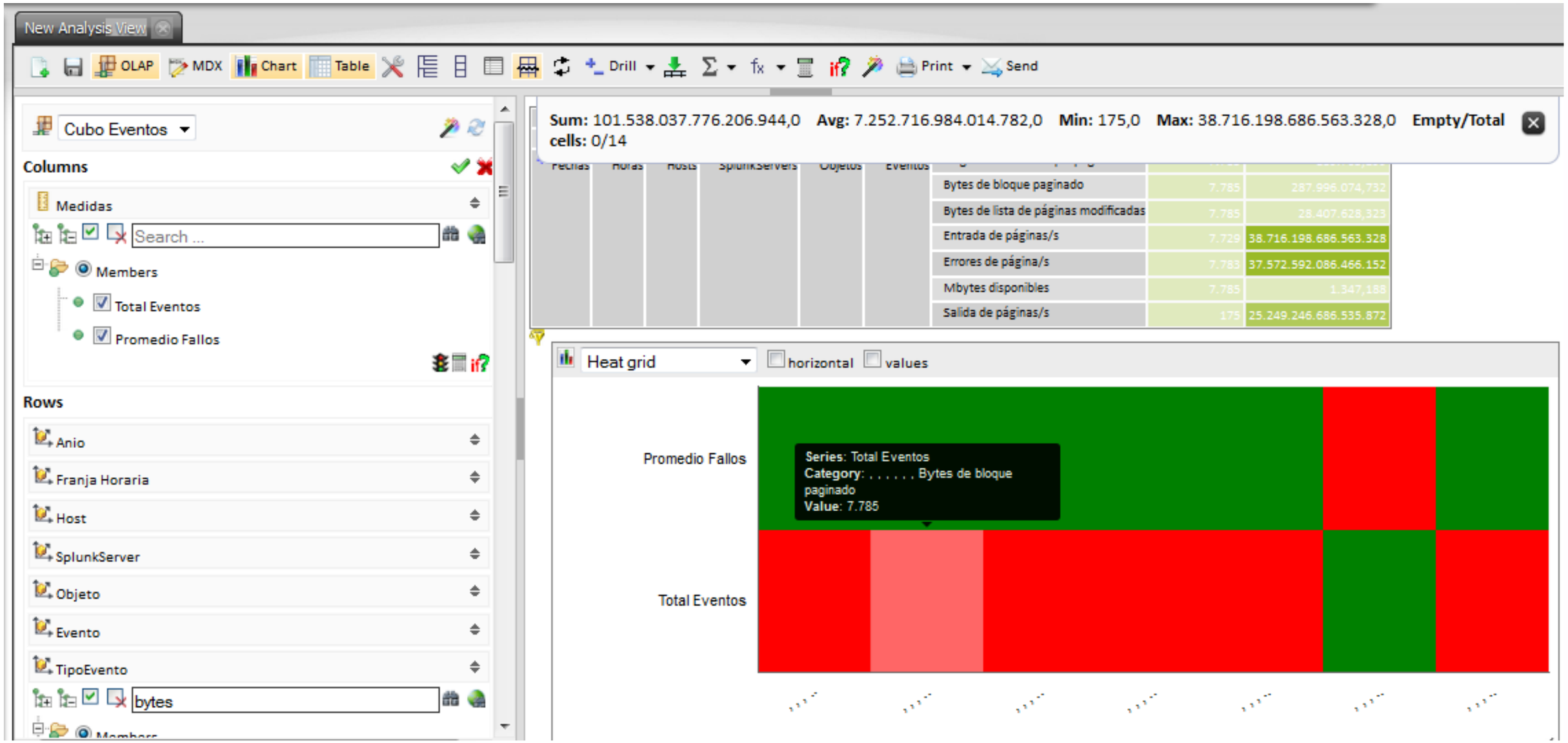



stratebi
open business intelligence

# Nuevos Dashboards y recursos de análisis

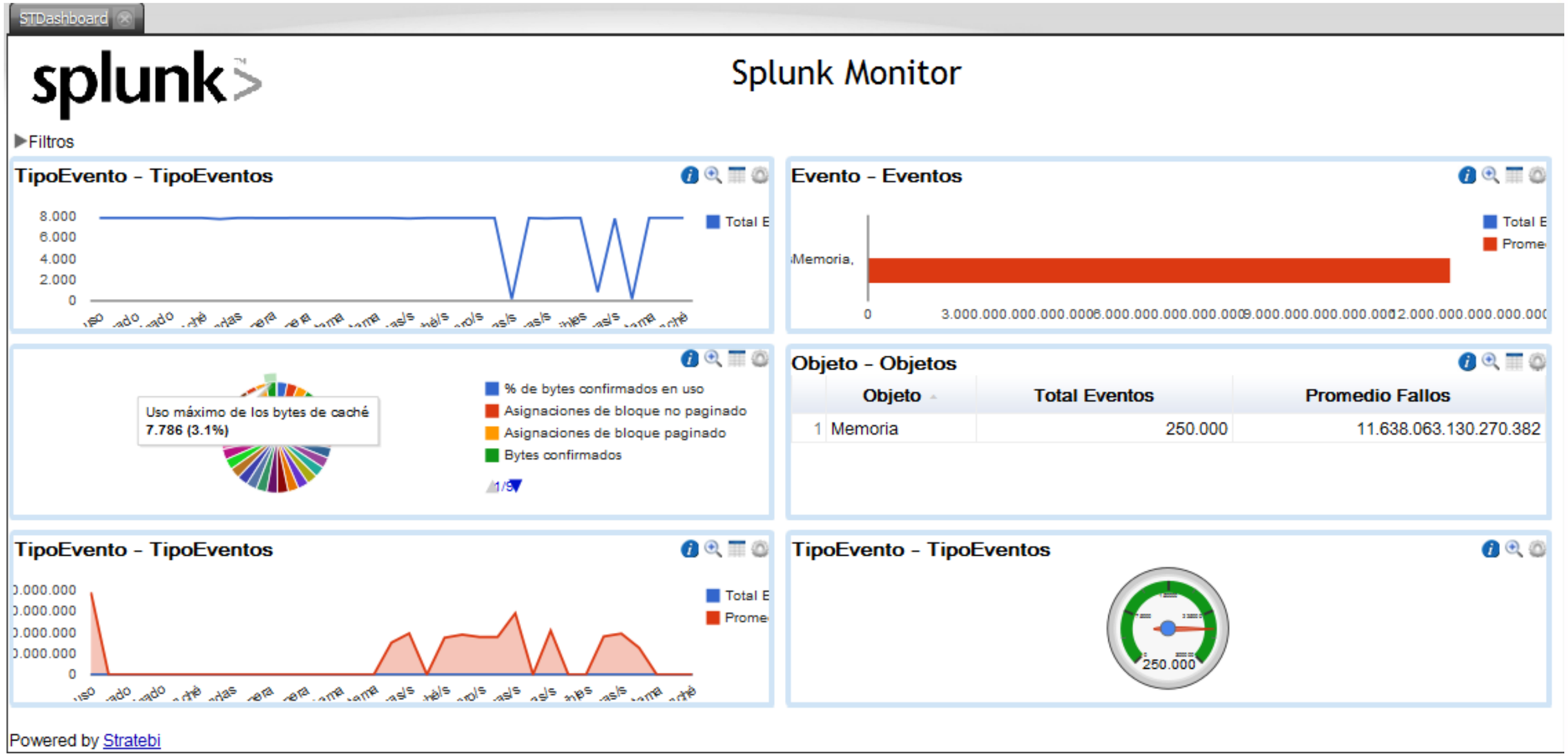


# Nuevos Dashboards y recursos de análisis




stratebi
open business intelligence

# Nuevos Dashboards y recursos de análisis



# Stratebi: Quiénes somos

Madrid: Pº de la Castellana, 164, 1º
Barcelona: C/ Valencia, 63
Brasil: Av. Paulista, 37 4 andar

## Mas información

info@stratebi.com
www.stratebi.com
Tfno: 91.788.34.10

TodoBI
www.TodoBI.com

stratebi
open business intelligence