El control en las Comunicaciones

Elio Rojano

@hellc2

https://www.sinologic.net

Elio Rojano <hellc2@gmail.com>

@hellc2

- *En el mundo de la informática desde 1984*
- *Apoyando el software libre desde 1996*
- *Disfrutando de la VoIP y Asterisk desde 2004*
- *Cocreador de la comunidad Asterisk-ES*
- *Creador de sinologic.net*

- *Desde 2004 hablando de VoIP y Asterisk*
- *Más de 3500 visitas diarias*
- *Más de 2500 usuarios únicos*
- *Más de 2000 artículos*

…y todo gracias a tí…

Control de las comunicaciones

"Rama de la tecnología dedicada al diseño, desarrollo y mantenimiento de las aplicaciones encargadas de gestionar y monitorizar las comunicaciones."

Configuración

Gestión

Monitorización

Seguridad

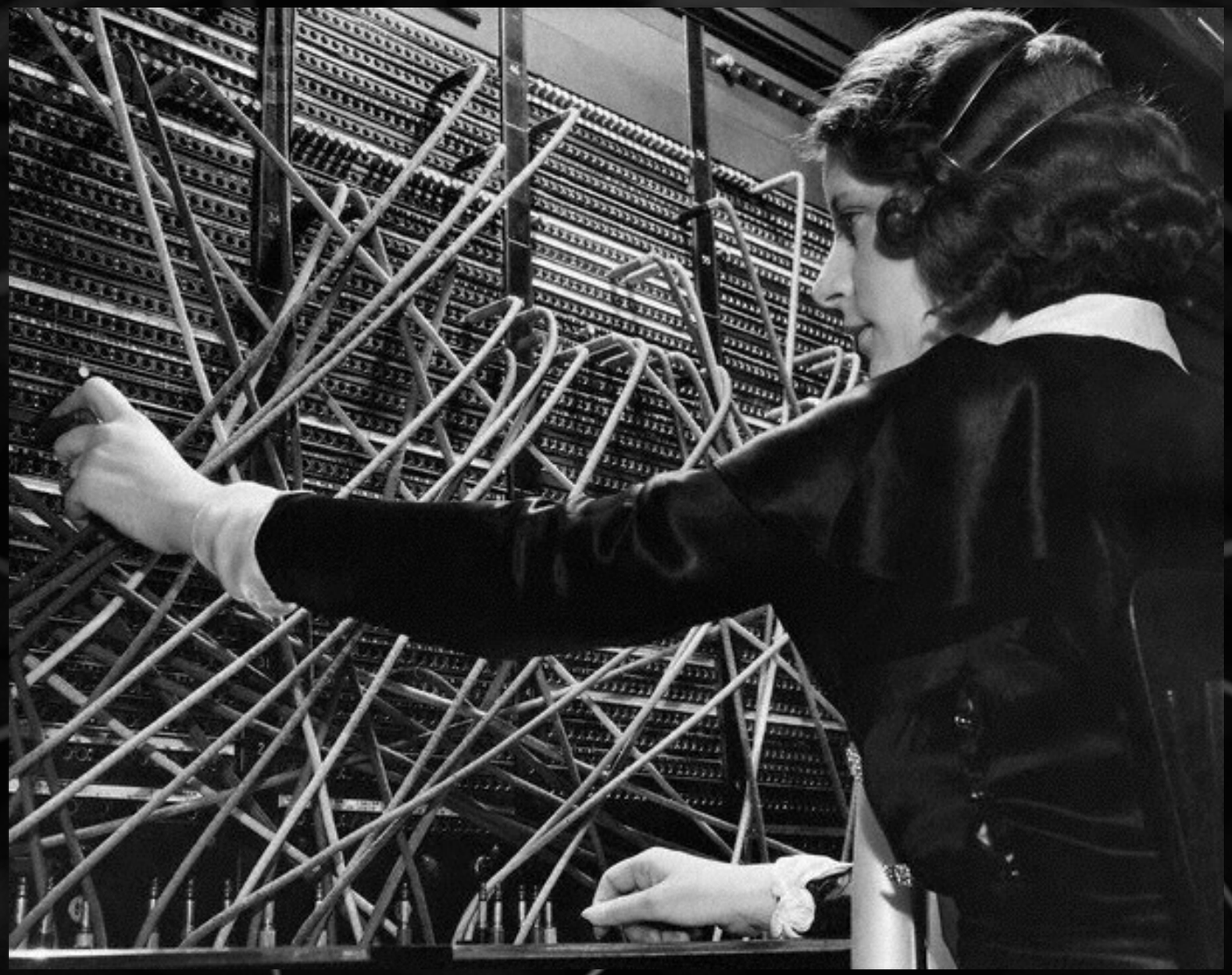
Configuración

¿Qué es el control de las comunicaciones?

Vamos a ver cómo han evolucionado los interfaces de configuración...

Elio Rojano https://www.sinologic.net

Interfaces de gestión de comunicaciones



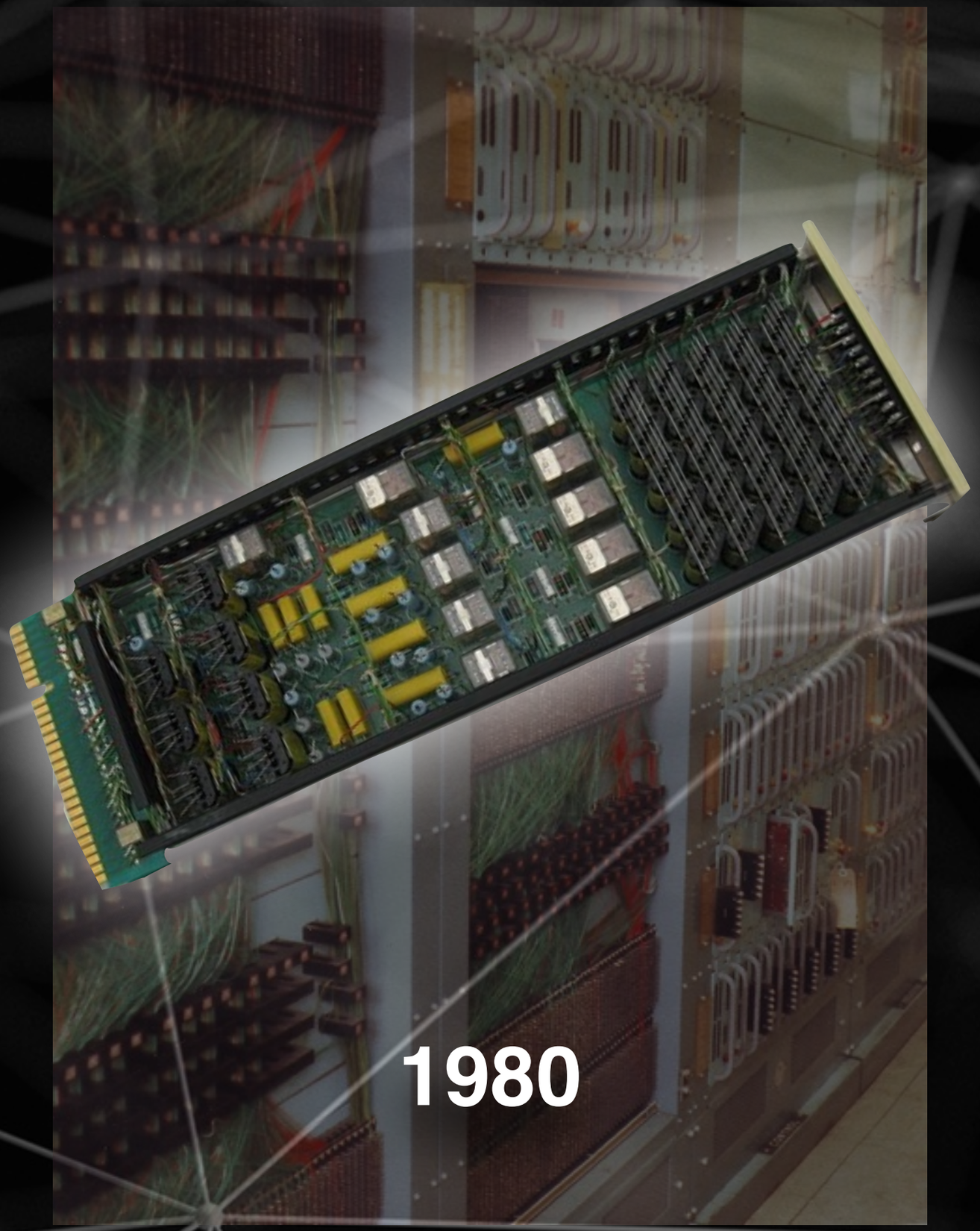
1900

Interfaces de gestión de comunicaciones

1970

El Control de las Comunicaciones

Interfaces de gestión de comunicaciones



Elio Rojano https://www.sinologic.net

Interfaces de gestión de comunicaciones

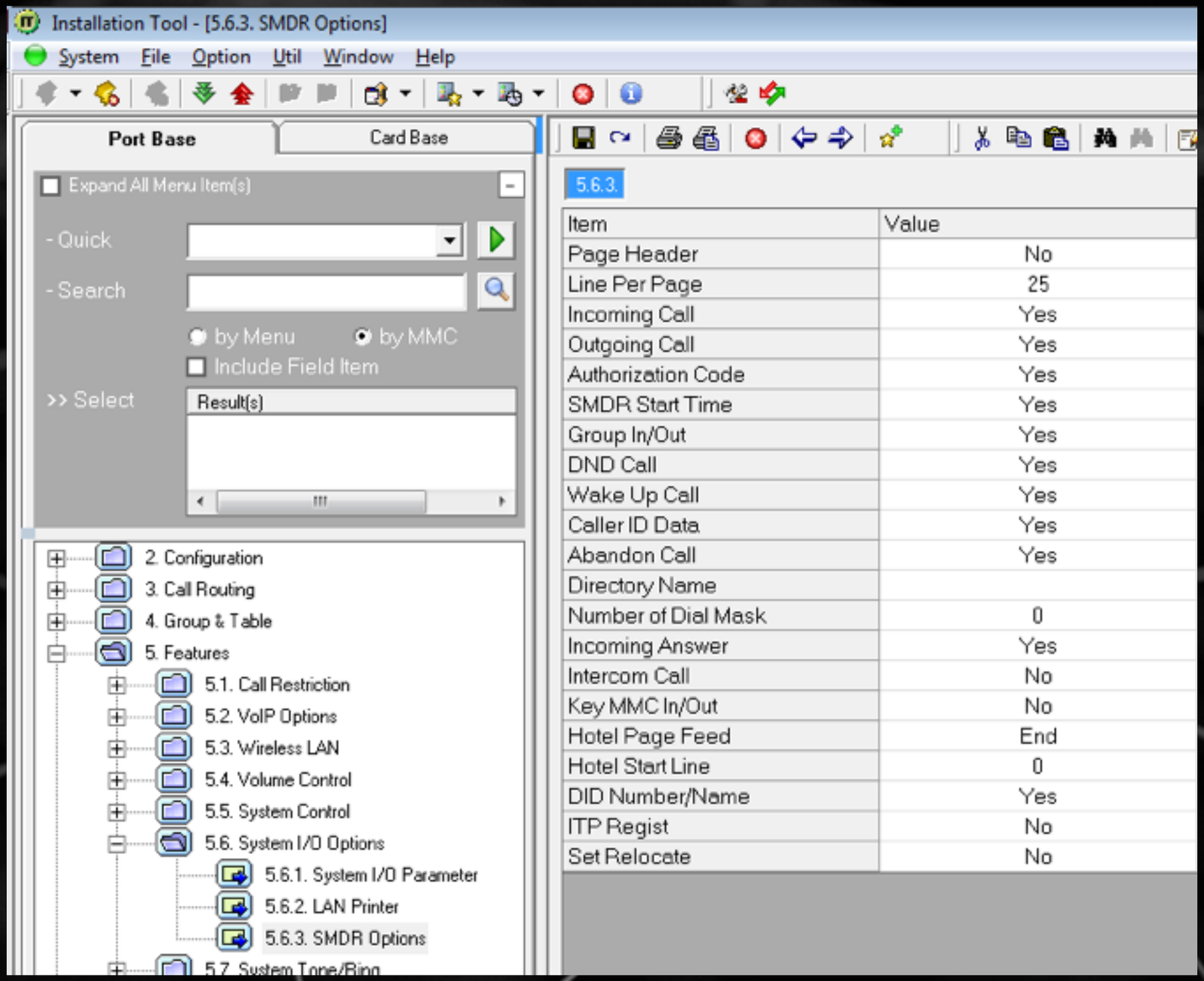
```
                                STATION

Extension: 2022                    Lock Messages? n          BCC: 0
     Type: 8434D                   Security Code:             TN: 1
     Port: 01A0423            Coverage Path 1:               COR: 1
     Name: Ken Cls 2022       Coverage Path 2:               COS: 1
                              Hunt-to Station:

STATION OPTIONS
              Data Module? n          Personalized Ringing Pattern: 1
            Speakerphone: 2-way                Message Lamp Ext: 2022
       Display Language: english             Mute Button Enabled? y
                                               Expansion Module? n
```

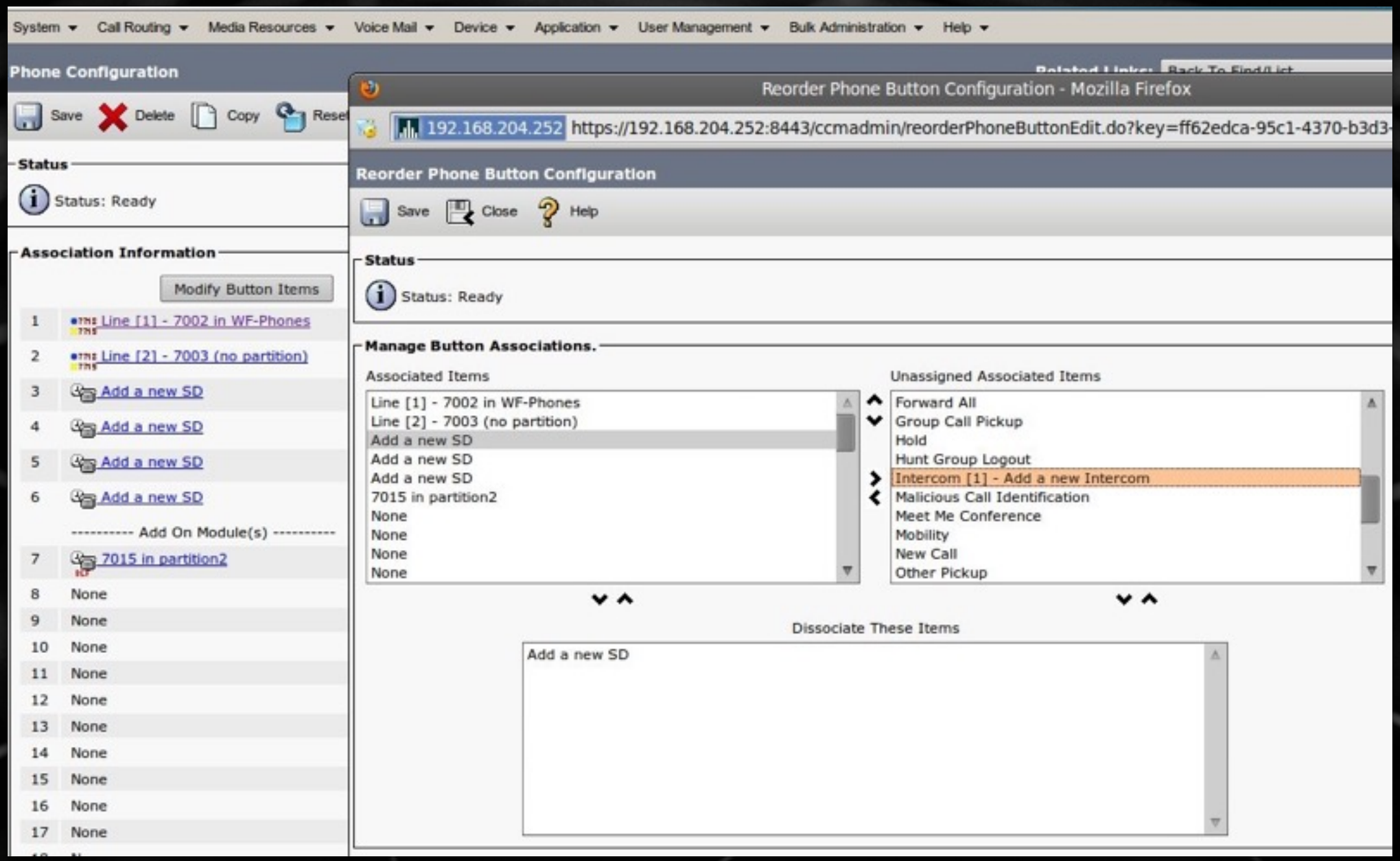
1990

Interfaces de gestión de comunicaciones



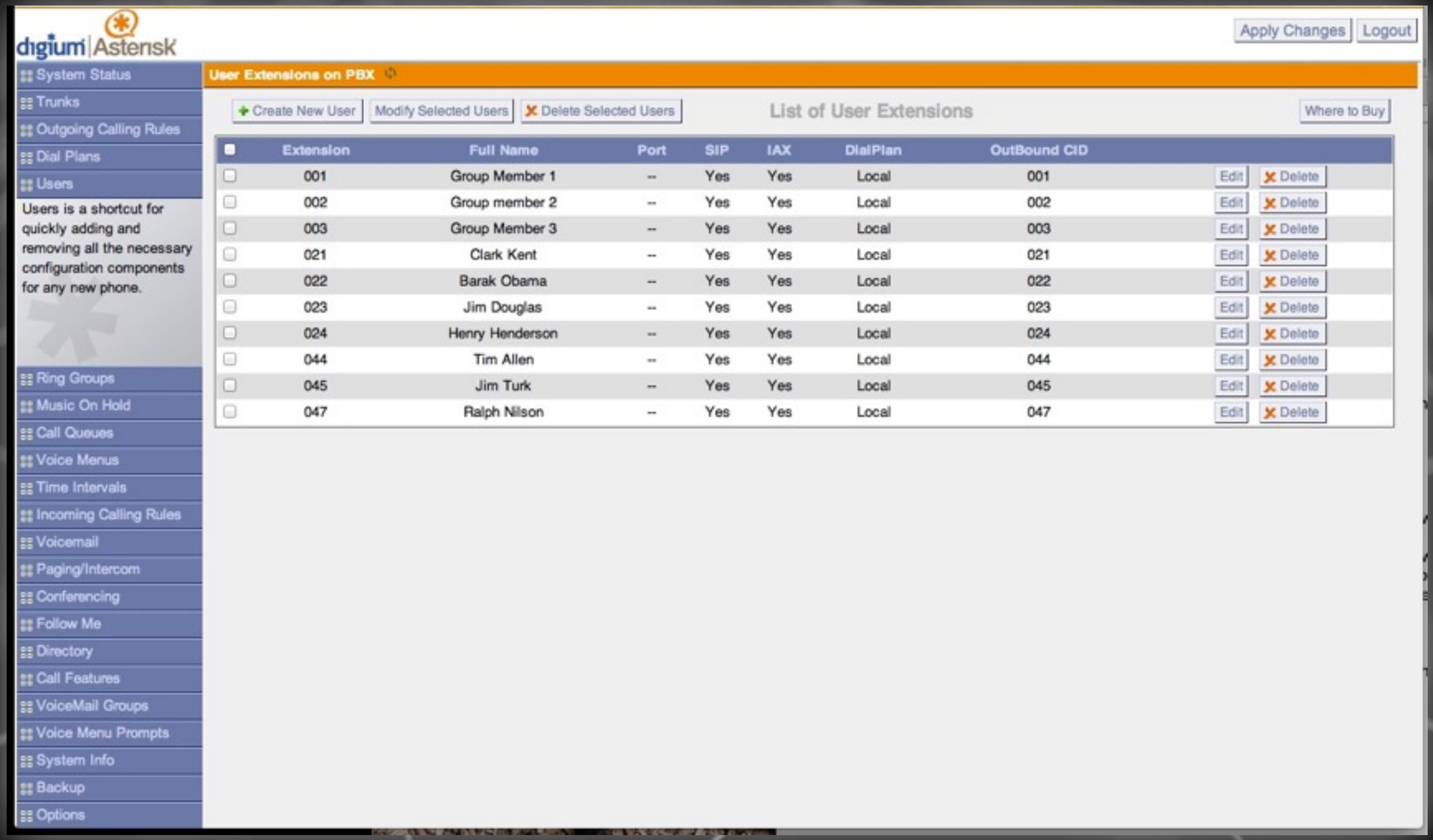
2000

Interfaces de gestión de comunicaciones



2005

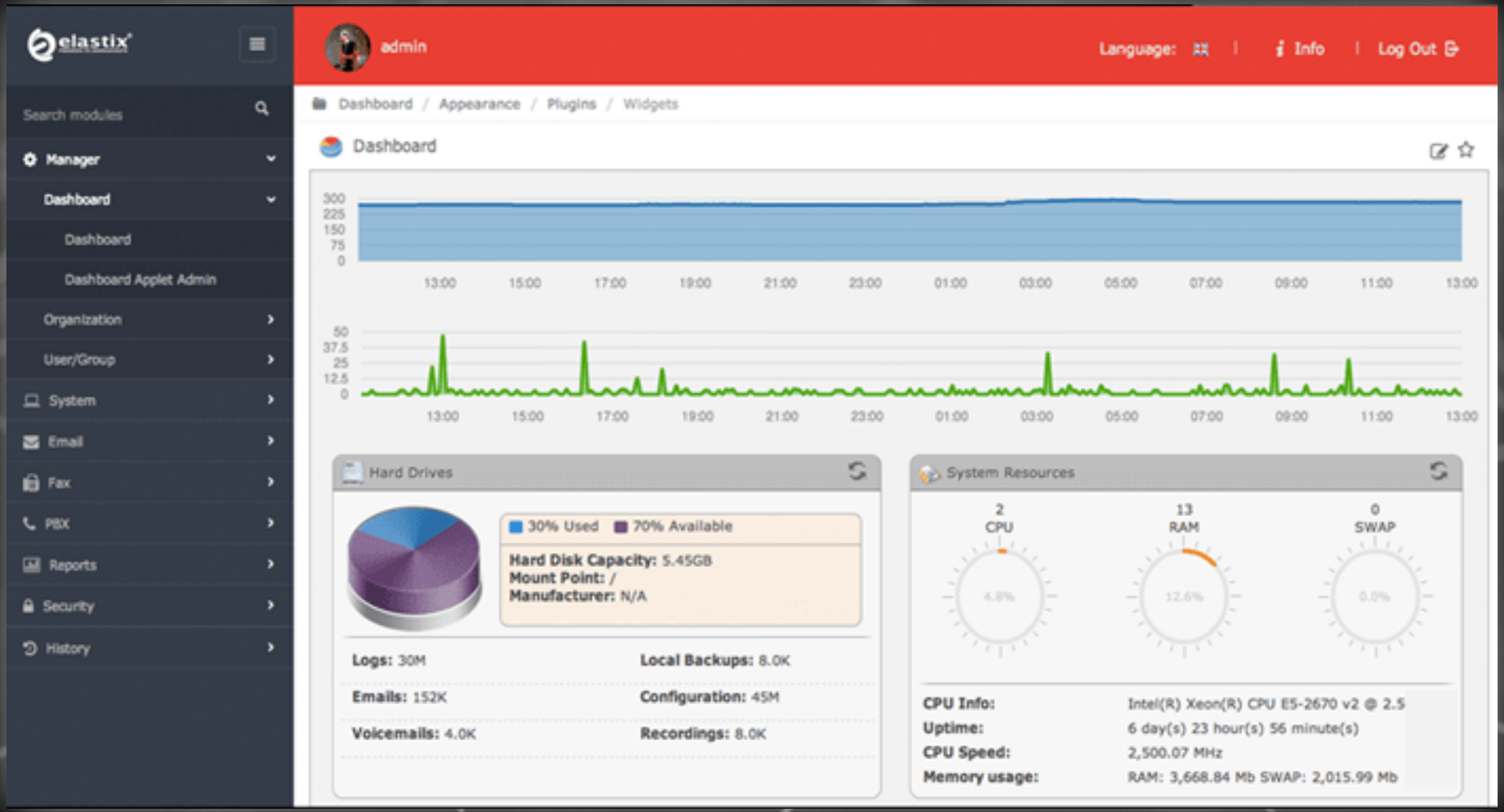
Interfaces de gestión de comunicaciones



2010

El Control de las Comunicaciones

Interfaces de gestión de comunicaciones



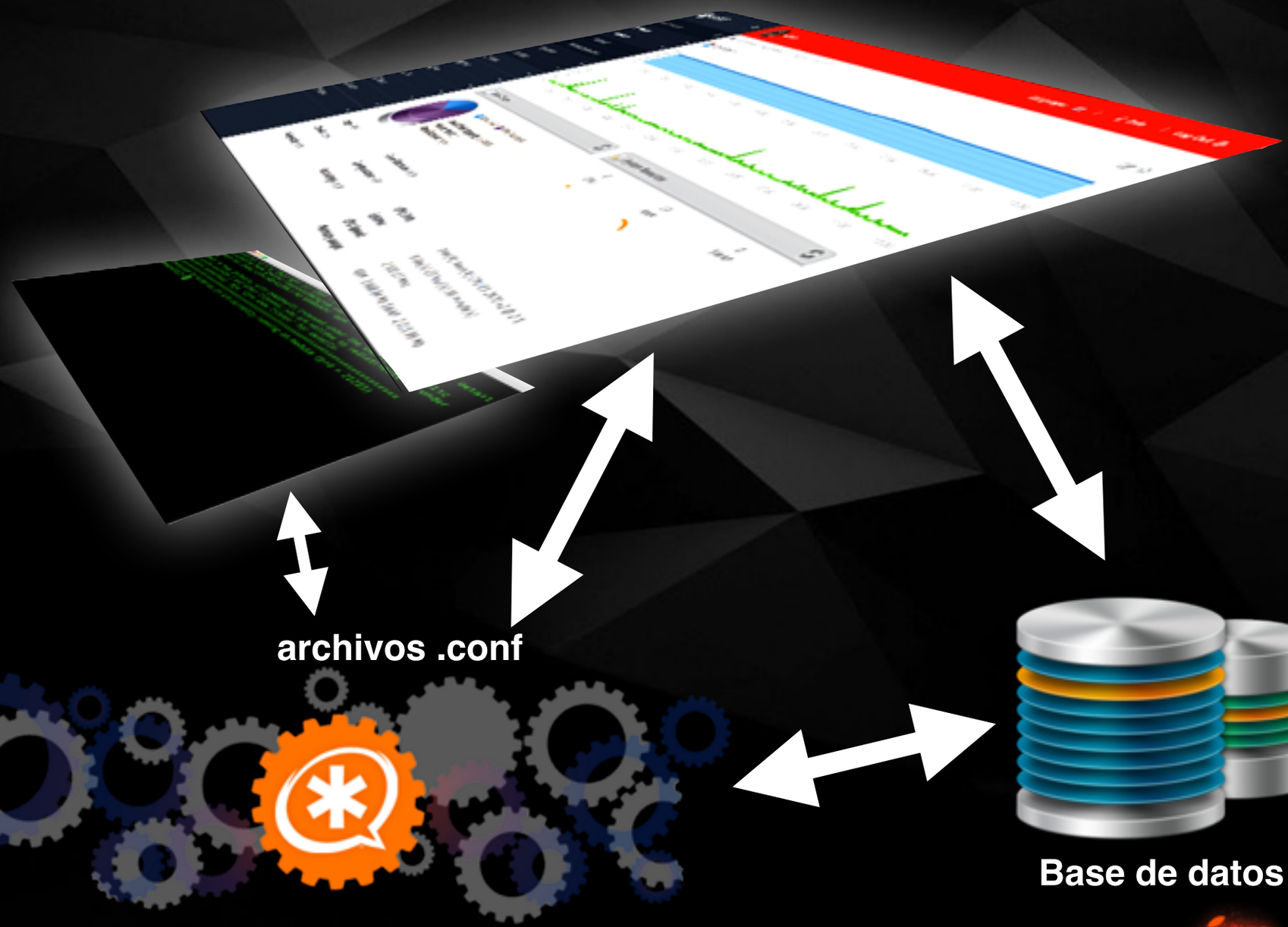
2015

Elio Rojano https://www.sinologic.net

ELASTIX WORLD 2015

sinologic

Un ejemplo: Elastix



El código fuente ofrece un 100% de posibilidades de adaptación

```
/usr/src~stman.c   [----]  0 L:[ 59+ 0  59  /78] *(1284/19915b) 0032 0x020
 * for the 5th argument to newtEntry() as char ** or const char ** . To
 * let the code compile cleanly with -Werror, we cast it to void * through
 * _NEWT_CAST.
 */
#define _NEWT_CAST (void *)

#define DEFAULT_MANAGER_PORT 5038

struct message {
        unsigned int hdrcount;
        char headers[MAX_HEADERS][MAX_LEN];
};

static struct ast_mansession {
        struct sockaddr_in sin;
        int fd;
        char inbuf[MAX_LEN];
        int inlen;
} session;

struct ast_chan {
        char name[80];
```

No siempre poseemos los conocimientos técnicos para modificar el código de forma segura…

La modificación de los archivos de configuración permiten ajustar el 80% de las posibilidades...

```
/etc/ast~ger.conf   [----]  1 L:[ 16+ 6  22/156] *(914 /6580b) 0110 0x06E
; http.conf and if both "enabled" and "webenabled" are set to yes in
; this file.  Both default to no.  httptimeout provides the maximum
; timeout in seconds before a web based session is discarded.  The
; default is 60 seconds.
;
[general]
enabled = no
;webenabled = yes

port = 5038
bindaddr = 0.0.0.0

; Parameters that control AMI over TLS. ("enabled" must be set too).
; You can open a connection to this socket with e.g.
;
;<----->openssl s_client -connect my_host:5039
;
;tlsenable=no<-><------>; set to YES to enable it
;tlsbindaddr=0.0.0.0:5039<----><------>; address and port to bind to, default t
;tlscertfile=/tmp/asterisk.pem<>; path to the certificate.
;tlsprivatekey=/tmp/private.pem ; path to the private key, if no private given,
                                ; if no tlsprivatekey is given, default is to se
```

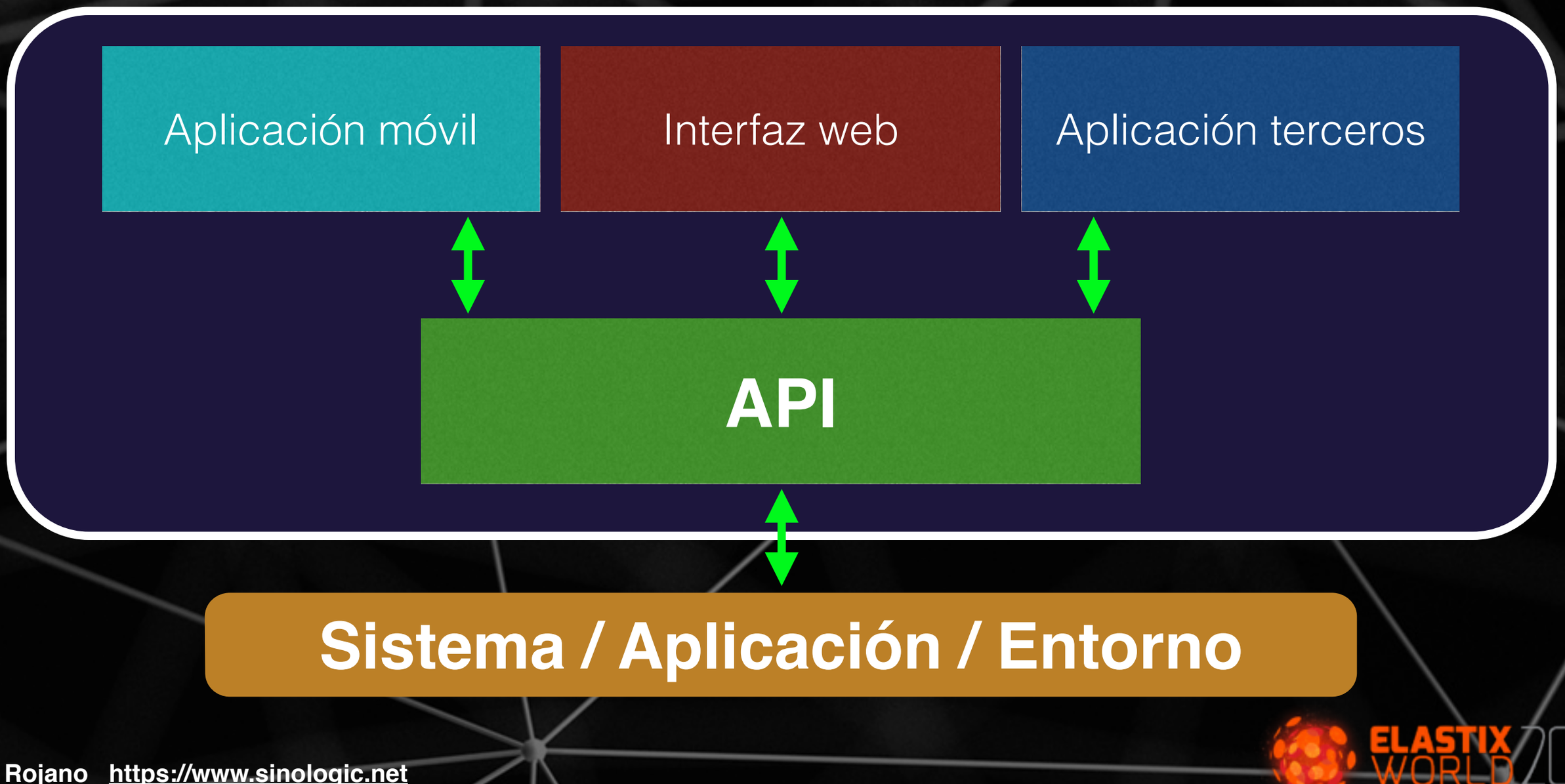
En un interfaz web, se suelen eliminar el 80% de las opciones de los archivos de configuración

… y eso que está orientado a un usuario técnico…

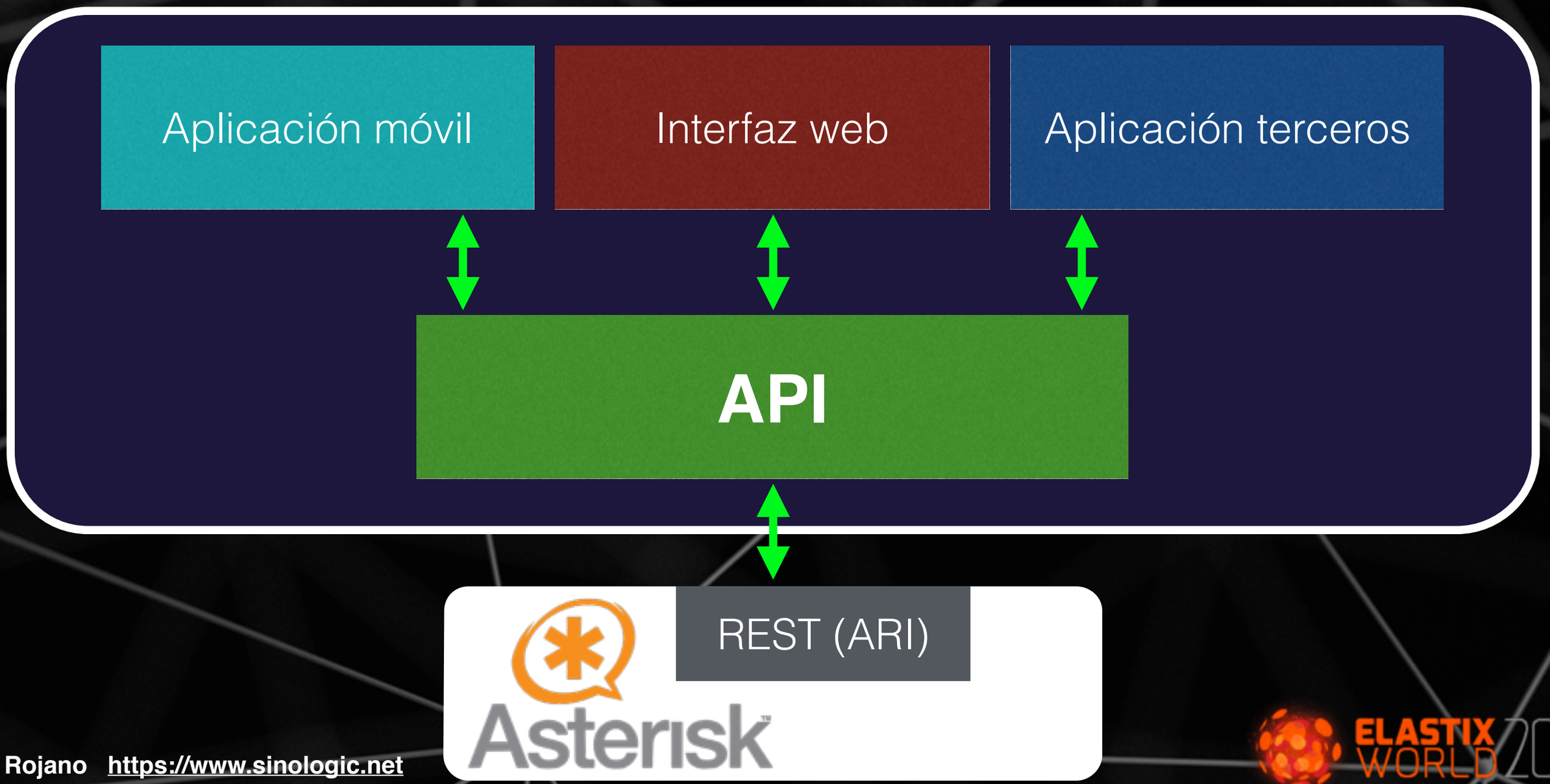
Problema: Todos los interfaces de configuración están orientados a la "pequeña empresa"

¿cuánto tiempo tardaríamos en dar de alta 3000 extensiones?

Las nuevas metodologías de programación simplifican su creación.



Las nuevas metodologías de programación simplifican su creación.



Gestión

Las aplicaciones de gestión permiten a los usuarios realizar tareas sencillas que no requieren conocimientos técnicos.

Los interfaces de gestión solo sirven para que el usuario final sepa qué está haciendo su sistema de comunicaciones.

No debe servir para configurarlo.

Una panadería, una carnicería, una fábrica de calzado, … no tiene porque saber qué es un codec, el puerto del protocolo SIP y qué contraseña es la más adecuada.

Generalmente suele venir integrada dentro de la aplicación de configuración, pero nadie lo explica.

La parte de gestión sí que debe integrarse con la siguiente parte: Monitorización

Monitorización

Elio Rojano https://www.sinologic.net

Muestran al usuario el estado del sistema y toda la información relevante EN TIEMPO REAL

La Red

El servidor

Las llamadas actuales

Las llamadas realizadas

Estado de las colas

Incidencias

Seguridad

etc...

sinologic

Monitorización de la Red

Zenoss (http://www.zenoss.org/)

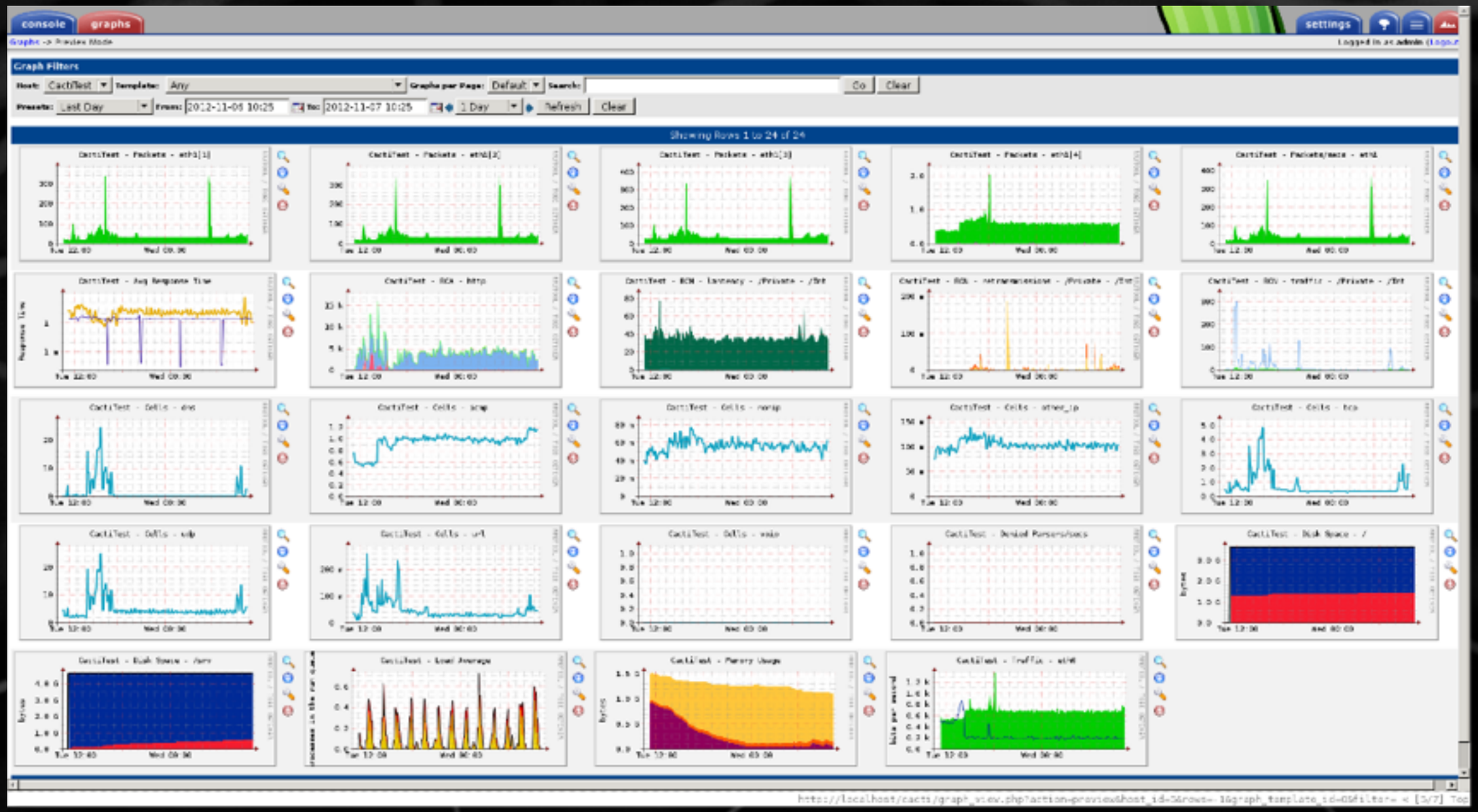
Elio Rojano https://www.sinologic.net

ELASTIX WORLD 2015

Monitorización de la Red

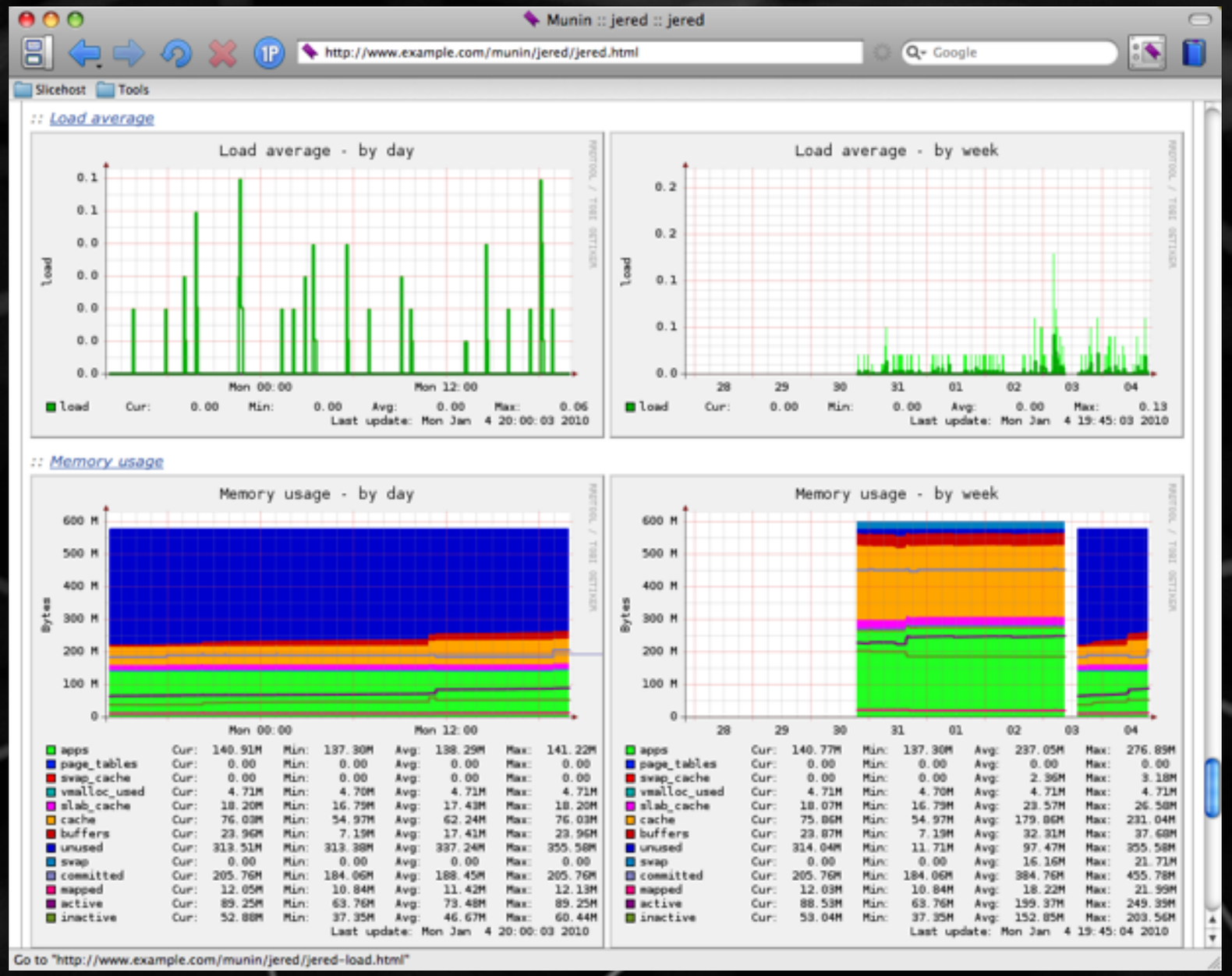
Pandora (http://pandorafms.com/)

Monitorización del Servidor



Cacti (http://www.cacti.net/)

Monitorización del Servidor



Munin (http://munin-monitoring.org/)

Herramientas de visualización de CDR hay muchas, pero a partir de cierto número de llamadas, el sistema se vuelve lento.

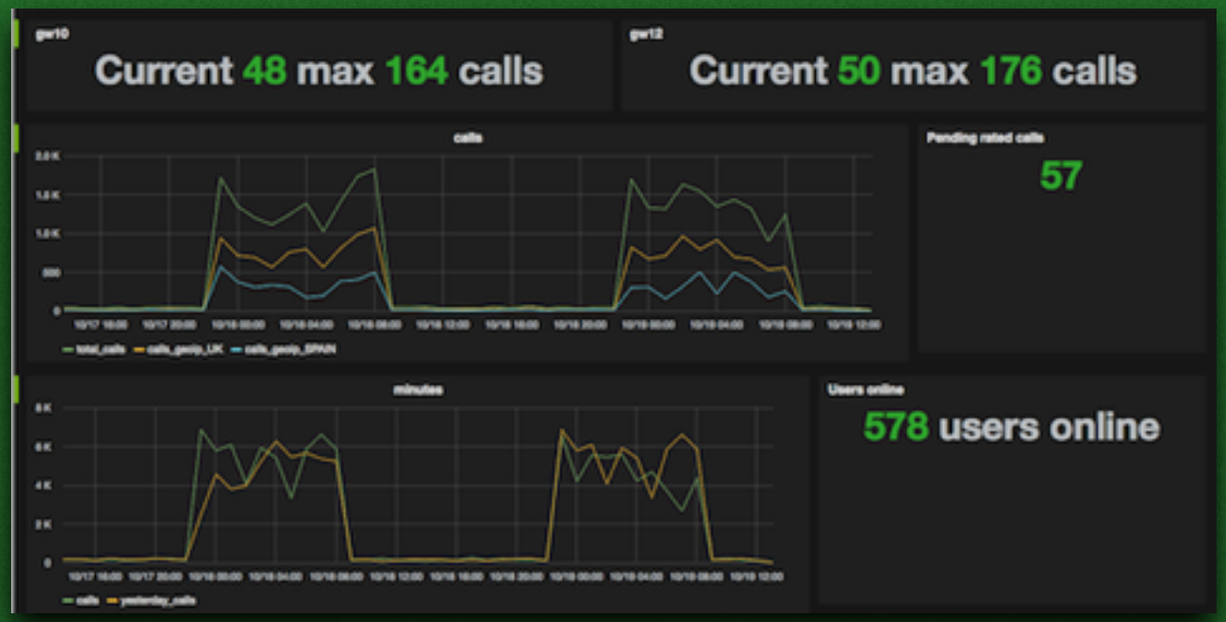
La mayoría de sistemas no están preparados para un número grande de llamadas y/o usuarios.

Para ello, el sistema a monitorizar debe permitir "exportar" la información a un sistema que pueda procesarla.

Bases de datos, CDR, REST, AMI, AGI, etc… muchos métodos para obtener información…

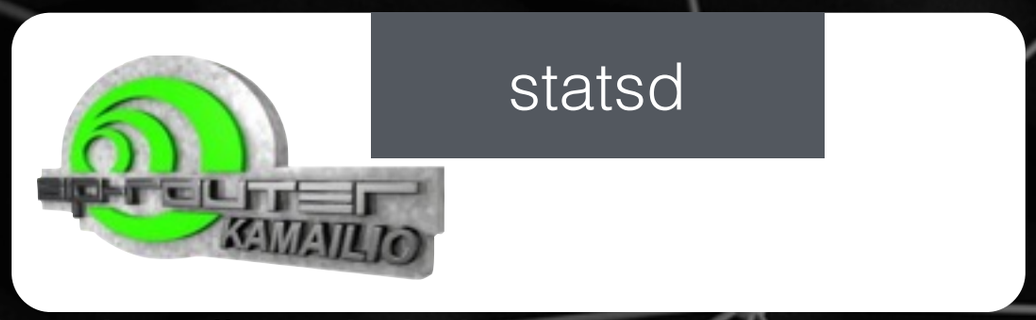
Asterisk 12, Asterisk 13 y Kamailio han incorporado nuevas herramientas para monitorización en tiempo real

Elio Rojano https://www.sinologic.net



Graphite

http://graphite.wikidot.com/



Hay planificadas nuevas aplicaciones de Dialplan para utilizar 'statsd' en Asterisk más dinámicamente.

```
[Initialization]
StatsD(gauge, channels.inuse, 0)

[Statistics]
exten => _XXXX,1,NoOp(Do some awesome statistics.)
same => n,StatsD(gauge, channels.inuse, +1)
same => n,Dial(${EXTEN})
same => n,Hangup()
same => n,StatsD(gauge, channels.inuse, -1)
```

https://wiki.asterisk.org/wiki/display/~tcambron

Seguridad

"Hay dos tipos de empresas, las que admiten que han sido víctimas de un ataque, y las que aún no lo saben"

John Chambers

¿A quién no le ha ocurrido esto?

```
[Sep 26 17:17:26] NOTICE[16166]: chan_sip.c:27851 handle_request_register: Registration from '"712" <sip:
712@78.60.201.227>' failed for '212.129.8.246:7245' - Wrong password
[Sep 26 17:17:26] NOTICE[16166]: chan_sip.c:27851 handle_request_register: Registration from '"712" <sip:
712@78.60.201.227>' failed for '212.129.8.246:7245' - Wrong password
[Sep 26 17:17:27] NOTICE[16166]: chan_sip.c:27851 handle_request_register: Registration from '"712" <sip:
712@78.60.201.227>' failed for '212.129.8.246:7245' - Wrong password
[Sep 26 17:17:27] NOTICE[16166]: chan_sip.c:27851 handle_request_register: Registration from '"712" <sip:
712@78.60.201.227>' failed for '212.129.8.246:7245' - Wrong password
[Sep 26 17:17:27] NOTICE[16166]: chan_sip.c:27851 handle_request_register: Registration from '"712" <sip:
712@78.60.201.227>' failed for '212.129.8.246:7245' - Wrong password
[Sep 26 17:17:27] NOTICE[16166]: chan_sip.c:27851 handle_request_register: Registration from '"712" <sip:
712@78.60.201.227>' failed for '212.129.8.246:7245' - Wrong password
[Sep 26 17:17:27] NOTICE[16166]: chan_sip.c:27851 handle_request_register: Registration from '"712" <sip:
712@78.60.201.227>' failed for '212.129.8.246:7245' - Wrong password
…
6 minutos después…
…
[Sep 26 17:24:13] NOTICE[27646]: chan_sip.c:27851 handle_request_register: Registration from '"711" <sip:
711@78.60.201.227>' failed for '212.129.8.246:6302' - Wrong password
[Sep 26 17:24:13] NOTICE[27646]: chan_sip.c:27851 handle_request_register: Registration from '"711" <sip:
711@78.60.201.227>' failed for '212.129.8.246:6302' - Wrong password
[Sep 26 17:24:13] NOTICE[27646]: chan_sip.c:27851 handle_request_register: Registration from '"711" <sip:
711@78.60.201.227>' failed for '212.129.8.246:6302' - Wrong password
[Sep 26 17:24:13] NOTICE[27646]: chan_sip.c:27851 handle_request_register: Registration from '"711" <sip:
711@78.60.201.227>' failed for '212.129.8.246:6302' - Wrong password
[Sep 26 17:24:14] NOTICE[27646]: chan_sip.c:27851 handle_request_register: Registration from '"711" <sip:
711@78.60.201.227>' failed for '212.129.8.246:6302' - Wrong password
[Sep 26 17:24:14] NOTICE[27646]: chan_sip.c:27851 handle_request_register: Registration from '"711" <sip:
711@78.60.201.227>' failed for '212.129.8.246:6302' - Wrong password
[Sep 26 17:24:14] NOTICE[27646]: chan_sip.c:27851 handle_request_register: Registration from '"711" <sip:
711@78.60.201.227>' failed for '212.129.8.246:6302' - Wrong password
[Sep 26 17:24:14] NOTICE[27646]: chan_sip.c:27851 handle_request_register: Registration from '"711" <sip:
711@78.60.201.227>' failed for '212.129.8.246:6302' - Wrong password
```

¿Cómo detectarlo a tiempo?

```
/etc/asterisk/logger.conf
; running a production system.  Debug mode turns on a LOT of extra messages,
; most of which you are unlikely to understand without an understanding of
; the underlying code.  Do NOT report debug messages as code issues, unless
; you have a specific issue that you are attempting to debug.  They are
; messages for just that -- debugging -- and do not rise to the level of
; something that merit your attention as an Asterisk administrator.  Debug
; messages are also very verbose and can and do fill up logfiles quickly;
; this is another reason not to have debug mode on a production system unless
; you are in the process of debugging a specific issue.
;
;debug => debug
security => security
console => notice,warning,error
;console => notice,warning,error,debug
messages => notice,warning,error,security
;full => notice,warning,error,debug,verbose,dtmf,fax

;syslog keyword : This special keyword logs to syslog facility
;
;syslog.local0 => notice,warning,error
;
```

Vamos a ver el LOG de seguridad…

```
/var/log/asterisk/security                                  2533695/2474K   100%
[Sep 26 17:29:00] SECURITY[27675] res_security_log.c:
SecurityEvent="InvalidPassword",EventTV="2015-09-26T17:29:00.130+020
0",Severity="Error",Service="SIP",EventVersion="2",AccountID="711",SessionID="0x7fbfd4312518"
,LocalAddress="IPV4/UDP/78.60.201.227/5060",RemoteAddress="IPV4/UDP/
212.129.8.246/7393" ,Challenge="29883af8",ReceivedChallenge="29883af8",ReceivedHash
="abffd45dd7b4ac45e9940fe23dc2bc7f"

[Sep 26 17:29:00] SECURITY[27675] res_security_log.c:
SecurityEvent="InvalidPassword",EventTV="2015-09-26T17:29:00.230+020
0",Severity="Error",Service="SIP",EventVersion="2",AccountID="711",SessionID="0x7fbfd42f0b68"
,LocalAddress="IPV4/UDP/78.6
0.201.227/5060",RemoteAddress="IPV4/UDP/
212.129.8.246/7393",Challenge="5e6536ce",ReceivedChallenge="5e6536ce",ReceivedHash
="83e7fe40c874f7b107f22155beade95f"

[Sep 26 17:29:00] SECURITY[27675] res_security_log.c:
SecurityEvent="ChallengeSent",EventTV="2015-09-26T17:29:00.340+0200"
,Severity="Informational",Service="SIP",EventVersion="1",AccountID="711",SessionID="0x7fbfd42
fad68",LocalAddress="IPV4/UDP
/78.60.201.227/5060",RemoteAddress="IPV4/UDP/212.129.8.246/7393",Challenge="106cfc0a"

[Sep 26 17:29:00] SECURITY[27675] res_security_log.c:
SecurityEvent="ChallengeSent",EventTV="2015-09-26T17:29:00.371+0200"
,Severity="Informational",Service="SIP",EventVersion="1",AccountID="711",SessionID="0x7fbfd42
fc268",LocalAddress="IPV4/UDP
/78.60.201.227/5060",RemoteAddress="IPV4/UDP/212.129.8.246/7393",Challenge="0373c790"
```

Ya lo tenemos: 212.129.8.246

¿y ahora qué?

sinologic

¿y ahora qué?

- *Los ataques se hacen con ordenadores zombies… así que sirve de poco contraatacar.*
- *La policía suelen tener personal dedicado a la caza y captura de estos atacantes.*
- *De momento, lo más normal, es bloquearlos.*

¿y ahora qué?

Utilizar un bloqueador automático:

* Fail2ban (http://www.fail2ban.org)
* SIPCheck2 (https://github.com/sinologicnet/sipcheck)

Revisar las contraseñas:

* Generar siempre contraseñas fuertes:
  https://www.sinologic.net/proyectos/genpass/

Nota: *Las contraseñas SIP no hay que recordarlas, se utilizan entre el servidor y el teléfono/softphone, así que no tiene que ser fácil de recordar.*

Vigilar y automatizar los avisos

* No utilices el correo como medio de información, no es seguro.

sinologic

¿y ahora qué?

Revisa posibles **exploits** que pueden surgir en las distintas páginas:

packet storm
all things security

Home | Files | News | About | Contact

Search files: elastix

Showing 1 - 14 of 14

Files | News | Users | Authors

Search for elastix Search

Elastix 2.5.0 SQL Injection
Authored by Ahmed Aboul-Ela — Posted Mar 6, 2015

Elastix versions 2.5.0 and below suffer from a remote blind SQL injection vulnerability.

tags | exploit, remote, sql injection
MD5 | 81385990327b1a31af0f8097c842b7a7 — Download | Favorite | Comments (0)

Elastix 2.4.0 Stable XSS / CSRF / Command Execution
Authored by Simo Ben Youssef | Site monxploit.com — Posted Oct 17, 2014

Elastix version 2.4.0 stable suffers from cross site request forgery, remote command execution, and cross site scripting vulnerabilities.

tags | exploit, remote, vulnerability, xss, csrf
MD5 | 436cc831ab6baf8d50bf136fcfb7a699 — Download | Favorite | Comments (0)

Elastix 2.4.0 Cross Site Scripting
Authored by Bassem — Posted Nov 17, 2013

Elastix version 2.4.0 suffers from multiple cross site scripting vulnerabilities.

tags | exploit, vulnerability, xss
MD5 | a72c5fea817dc1fa585544079356e2ad — Download | Favorite | Comments (0)

Elastix 2.4.0 Cross Site Scripting
Authored by cheki — Posted Jun 1, 2013

Elastix version 2.4.0 suffers from a cross site scripting vulnerability.

tags | exploit, xss
MD5 | 8638653ba6e45ee768afa5d4338eb203 — Download | Favorite | Comments (0)

Elastix 2.3 PHP Code Injection
Authored by i-Hmx — Posted Jan 4, 2013

Elastix versions prior to 2.4 php code injection exploit.

packet storm
all things security

Home | Files | News | About | Contact

Search files: freepbx

Showing 1 - 25 of 30

Files | News | Users | Authors

Search for freepbx Search

FreePBX 12.0.43 Cross Site Scripting
Authored by High-Tech Bridge SA | Site htbridge.com — Posted Apr 22, 2015

FreePBX version 12.0.43 suffers from multiple cross site scripting vulnerabilities.

tags | exploit, vulnerability, xss
advisories | CVE-2015-2690
MD5 | 79cee98f92edb2ccaa42d7468d97b0b8 — Download | Favorite | Comments (0)

FreePBX Authentication Bypass / Account Creation
Authored by Rob Thomas — Posted Oct 1, 2014

A remote attacker can bypass authentication and create a false FreePBX Administrator account, which will then let them perform any action on a FreePBX system as the FreePBX user (which is often 'asterisk' or 'apache'). As of 2014/10/01 all versions of FreePBX are affected.

tags | advisory, remote, bypass
MD5 | be8e253ba1f0dd155fc81a0cab78d6ec — Download | Favorite | Comments (0)

FreePBX config.php Remote Code Execution
Authored by i-Hmx, 0x00string | Site metasploit.com — Posted Mar 25, 2014

This Metasploit module exploits a vulnerability found in FreePBX version 2.9, 2.10, and 2.11. It's possible to inject arbitrary PHP functions and commands in the "/admin/config.php" parameters "function" and "args".

tags | exploit, arbitrary, php
advisories | CVE-2014-1903
MD5 | eb66aafbde2a7c0352575e1ef94440a5 — Download | Favorite | Comments (0)

FreePBX 2.x Remote Command Execution
Authored by i-Hmx — Posted Feb 24, 2014

FreePBX versions before 2.3 suffer from a remote command execution vulnerability.

tags | exploit, remote

¿Preguntas?

Agradecimientos...

- Rosa Atienza
- Pablo Rojano
- La gente de PaloSanto y Elastix
- A los lectores de Sinologic
- A vosotros por seguir aquí