



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO  
FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

MEMORIA TECNICA DE INSTALACION Y CONFIGURACION DEL EQUIPO SECURITY ANALYTICS DE INFOTEC

DESARROLLO DE UN CASO PRACTICO  
QUE PARA OPTAR POR EL GRADO DE  
INGENIERO EN COMPUTACIÓN

PRESENTA:  
JOSÉ ROBERTO LEÓN MÁRQUEZ

ASESOR  
SILVIA VEGA MUYTOY

CIUDAD NEZAHUALCÓYOTL, ESTADO DE  
MÉXICO, 2018



Universidad Nacional  
Autónoma de México



**UNAM – Dirección General de Bibliotecas**  
**Tesis Digitales**  
**Restricciones de uso**

**DERECHOS RESERVADOS ©**  
**PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL**

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

Nezahualcóyotl, MEX

## Contenido

INTRODUCCIÓN.....	3
1. CONFIGURACIÓN SECURITY ANALYTICS.....	5
1.1 Diagrama de la solución.....	5
1.2 Características del equipo instalado.....	6
1.3 Diagrama de red.....	9
1.4 Descripción de la Plataforma.....	11
1.5 Configuración general del Security Analytics.....	12
1.6 Soporte.....	17
1.7 Entidades y puertos del Security Analytics.....	24
2. LIVE.....	27
2.1 Descripción de la Plataforma.....	29
2.2 Descripción general.....	30
2.4 Licenciamiento.....	33
3. CONFIGURACIÓN DE ENTIDADES.....	40
3.1 Concentrator 1.....	40
3.2 Concentrator 2.....	43
3.3 Log Decoder 1.....	46
3.4 Log Collector 1.....	49
3.5 Log Decoder 2.....	50
3.6 Log Collector 2.....	53
3.7 Event Stream Analysis 1.....	54



3.8	Fuentes integradas .....	56
3.9	Reenvío de logs a Fuente Externa .....	57
3.10	Custom Feeds .....	64
4.	REPORTES .....	70
4.1	Alertas .....	72
4.2	Alerta FW_Origen Malicioso.....	73
4.3	Alerta IPS_Firma Disparada.....	75
CONCLUSIONES.....		79
Configuración de security analytics.....		79
Configuración de live .....		79
Configuración de entidades.....		80
Configuración de reportes .....		80



## INTRODUCCIÓN

RSA Security Analytics es una solución de seguridad que ayuda a los analistas de seguridad de INFOTEC a detectar e investigar amenazas que otras herramientas de seguridad suelen omitir. Mediante la combinación de las funcionalidades de recopilación de datos de seguridad, administración y análisis de big data con visibilidad de red completa y basada en logs e inteligencia de amenazas automatizadas, los analistas de seguridad de INFOTEC podrán detectar, investigar y comprender mejor las amenazas que antes no solían ver ni comprender fácilmente. En última instancia, esta mayor visibilidad y velocidad ayudara a la organización a reducir de semanas a horas el tiempo libre que los atacantes pasan en sus ambientes de cómputo, por lo que se reduce considerablemente el impacto probable de un ataque.

RSA Security Analytics ayuda a los analistas de INFOTEC a descubrir comportamientos “interesantes” o “anómalos” sin depender del conocimiento previo sobre las herramientas o las técnicas específicas de los atacantes. Así mismo RSA aprovecha la tecnología de NetWitness para ofrecer monitoreo de seguridad de la red e información de seguridad y administración de eventos (SIEM) de manera convergente.

RSA Security Analytics permite realizar monitoreo y análisis de eventos, investigación de incidentes, análisis forense, análisis de malware para apoyar a los analistas de seguridad a encontrar información importante para la empresa.

RSA Security Analytics ofrece:

**Visibilidad** – Ofrece una visibilidad completa para identificar e investigar ataques.

- ❖ Elimina los puntos ciegos al darnos visibilidad de logs, red y de usuarios finales.
- ❖ Aumenta la visibilidad al permitir agregar información adicional o de la empresa para hacer una investigación más profunda y completa.

**Análisis** – Detecta y analiza los ataques más avanzados en tiempo real.

- ❖ Detecta ataques que otras herramientas de SIEM o herramientas basadas en firmas no detectan haciendo uso de un motor de correlación entre logs, usuarios finales, paquetes, etc.
- ❖ Puede comenzar a detectar incidentes inmediatamente con reportes, inteligencia y reglas de fábrica.

**Acción** - Tome acción específica sobre los hechos más importantes



- ❖ Dar prioridad a las investigaciones y agilizar múltiples flujos de trabajo de analistas en una sola herramienta, permitiendo respuesta a incidentes y escalación inmediata.
- ❖ Pivote Instantáneo desde los incidentes en las zonas profundas del usuario final para realizar análisis forense de redes y comprender la verdadera naturaleza y el alcance del problema. Separa las amenazas del "ruido", cortando horas o días del proceso de detección de amenazas y la eliminación de la pérdida de tiempo debido a los falsos positivos.



# 1. CONFIGURACIÓN SECURITY ANALYTICS

En esta sección se detalla las características del equipo Security Analytics así como la implementación y su configuración.

## 1.1 Diagrama de la solución

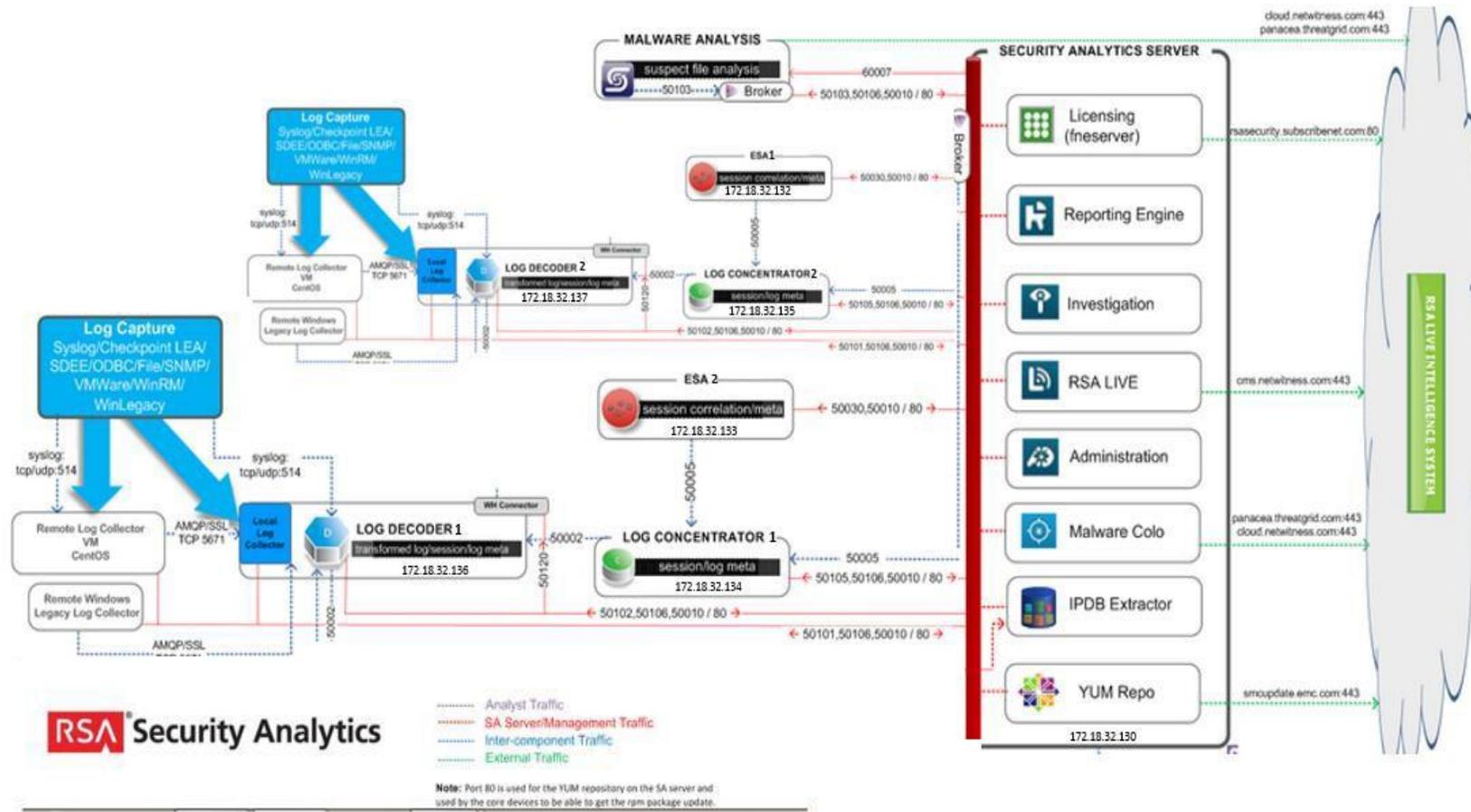


Ilustración 1. Diagrama Security Analytics



## 1.2 Características del equipo instalado

A continuación, se detallan las características del Security Analytics instalado en INFOTEC

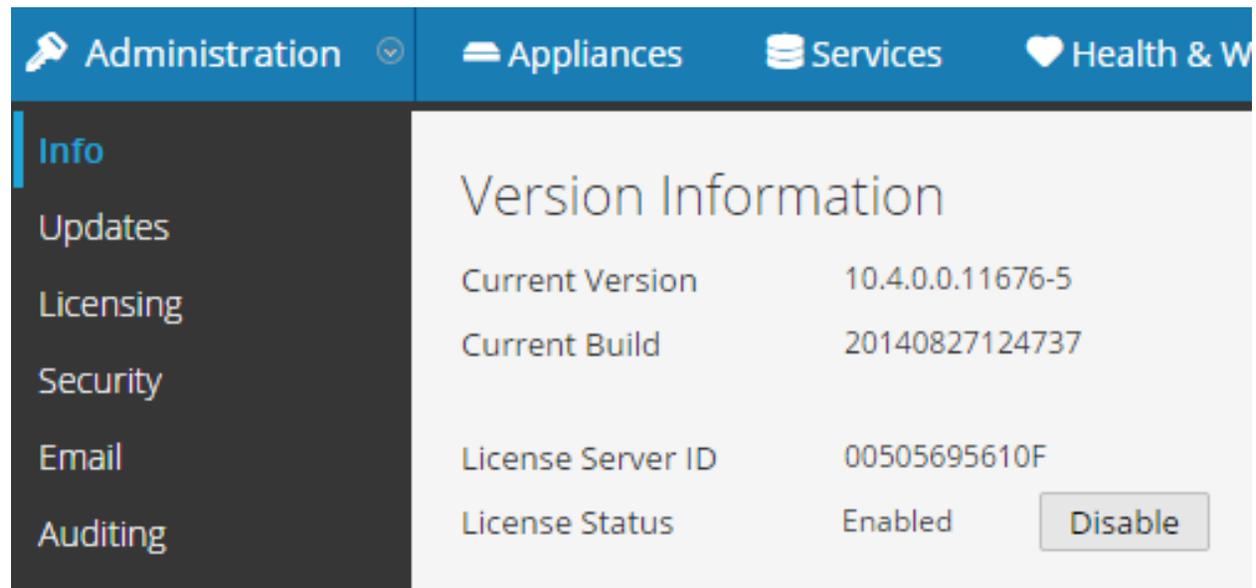
	Memoria	# Procesadores	Espacio en disco	Direcciones IP
Security Analytics Console	64 GB	2	1.9TB	1
ESA (Event Stream Analysis) 1	96 GB	4	1.9TB	1
ESA (Event Stream Analysis) 2	96 GB	4	1.9TB	1
Concentrator 1	64 GB	2	1.9TB	1
Concentrator 2	64 GB	2	1.9TB	1
Log Decoder 1	64 GB	2	1.9TB	1
Log Decoder 2	64 GB	2	1.9TB	1

*Ilustración 2. . Requerimientos Físicos de Security Analytics*

- ❖ Un VMware ESX Server 5.0 o mayor.
- ❖ El cliente de vSphere 4.1 o vSphere 5.0 instalado para conectarnos al Servidor de VMware ESX.
- ❖ Permisos de Administrador en el Servidor de VMware ESX para poder crear las máquinas virtuales



Asimismo, se muestra información general de Security Analytics una vez que ingresamos a la GUI.



The screenshot displays the Administration section of the Security Analytics GUI. The top navigation bar includes 'Administration', 'Appliances', 'Services', and 'Health & W'. The left sidebar lists 'Info', 'Updates', 'Licensing', 'Security', 'Email', and 'Auditing'. The main content area is titled 'Version Information' and contains the following details:

Current Version	10.4.0.0.11676-5
Current Build	20140827124737
License Server ID	00505695610F
License Status	Enabled <input type="button" value="Disable"/>

Ilustración 3. Información de Security Analytics



A continuación, se muestra la configuración del servidor de NTP en el servidor de Security Analytics

```
[root@SA etc]# cat ntp.conf
# For more information about this file, see the man pages
# ntp.conf(5), ntp_acc(5), ntp_auth(5), ntp_clock(5), ntp_misc(5), ntp_mon(5).

driftfile /var/lib/ntp/drift

# Permit time synchronization with our time source, but do not
# permit the source to query or modify the service on this system.
restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery

# Permit all access over the loopback interface. This could
# be tightened as well, but to do so would effect some of
# the administrative functions.
restrict 127.0.0.1
restrict -6 ::1

# Hosts on local network are less restricted.
#restrict 192.168.1.0 mask 255.255.255.0 nomodify notrap

# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
server pool.ntp.org
server 1.centos.pool.ntp.org iburst
server 2.centos.pool.ntp.org iburst
server 3.centos.pool.ntp.org iburst

#broadcast 192.168.1.255 autokey # broadcast server
#broadcastclient # broadcast client
#broadcast 224.0.1.1 autokey # multicast server
#multicastclient 224.0.1.1 # multicast client
#manycastserver 239.255.254.254 # manycast server
#manycastclient 239.255.254.254 autokey # manycast client

# Enable public key cryptography.
#crypto

includefile /etc/ntp/crypto/pw

# Key file containing the keys and key identifiers used when operating
# with symmetric key cryptography.
keys /etc/ntp/keys
```

Ilustración 4. Configuración Servidor NTP



1.3 Diagrama de red

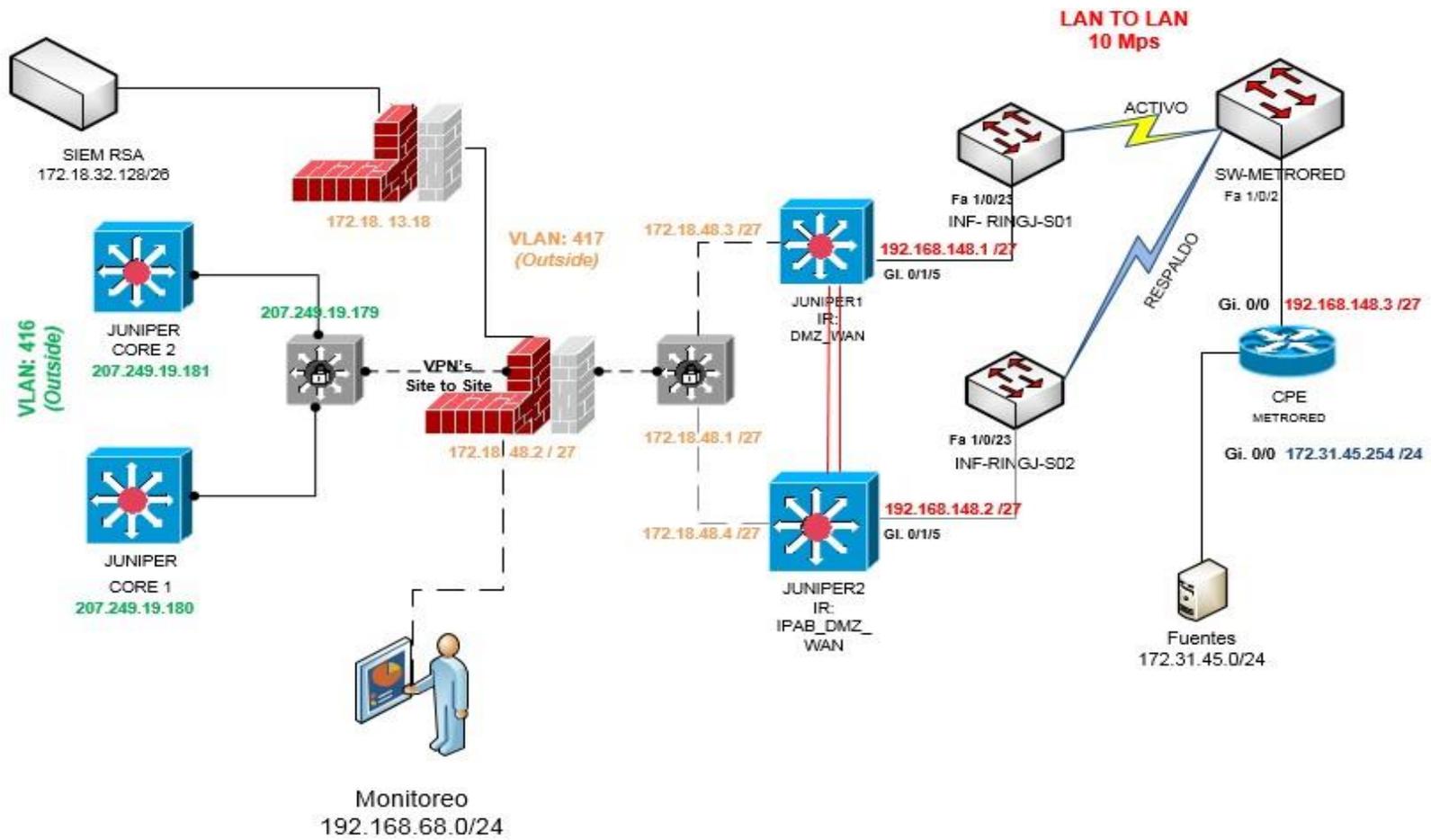


Ilustración 5. Diagrama de Red de INFOTEC



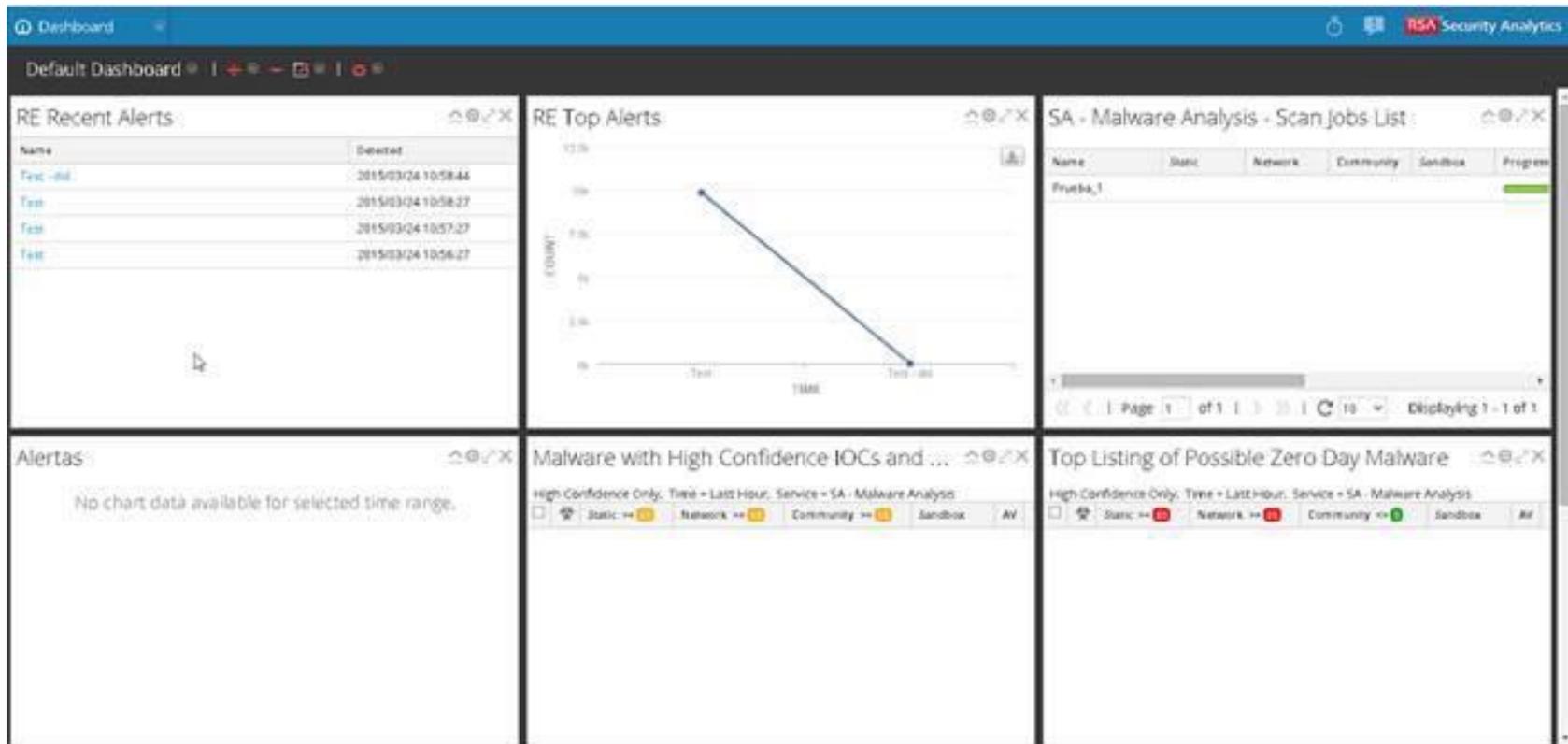


Ilustración 6. Dashboard Principal



## 1.4 Descripción de la Plataforma

### Log Decoder

- ❖ Es el encargado de recolectar la información de la red o fuentes conectadas a él ya sea en formato syslog, ODBC, eventos de Windows, etc. La cual es enriquecida y parseada para así mandarse al Concentrator.

### Concentrator

- ❖ Toda la información indexada por el Decoder es filtrada por el Concentrador y puede ser enviada al Security Analytics Warehouse.

### Security Analytics Server

- ❖ Provee la interfaz gráfica de la aplicación para la administración de esta, configuración, reportes, alertas, investigación de incidentes, etc.

### ESA

- ❖ Provee la correlación de eventos, así como el procesamiento complejo de evento con gran rapidez y poca latencia. Este módulo es capaz de procesar grandes volúmenes de datos de los concentradores.
- ❖ Permite a los usuarios agregar reglas de correlación a través de múltiples eventos disparados al mismo tiempo, así como ayudar a la detección de incidentes y alertas en la plataforma.



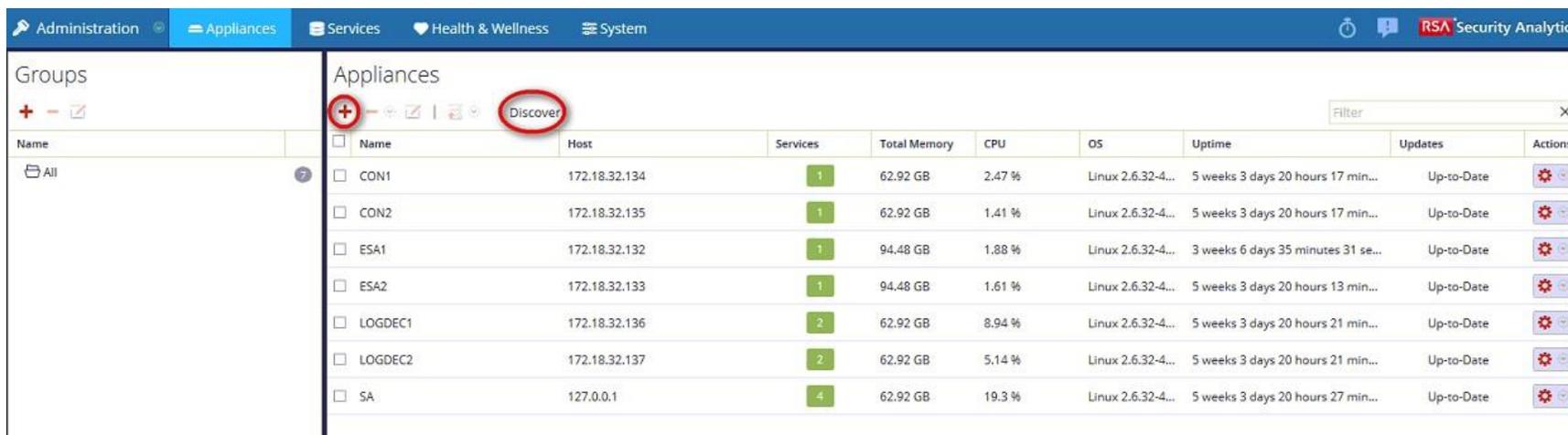
## 1.5 Configuración general del Security Analytics

Security Analytics fue configurado con los siguientes parámetros generales:

Nombre	Dirección IP	Máscara de	Gateway
<b>CON1 – Concentrator</b>	172.18.32.134	255.255.255.192	172.18.32.190
<b>CON2 - Concentrator</b>	172.18.32.135	255.255.255.192	172.18.32.190
<b>ESA1 – Event Stream</b>	172.18.32.132	255.255.255.192	172.18.32.190
<b>ESA2 – Event Stream</b>	172.18.32.133	255.255.255.192	172.18.32.190
<b>LOGDEC1 – Log Decoder</b>	172.18.32.136	255.255.255.192	172.18.32.190
<b>LOGDEC2 – Log Decoder</b>	172.18.32.137	255.255.255.192	172.18.32.190
<b>SA Server</b>	172.18.32.130	255.255.255.192	172.18.32.190

Tabla 1. Configuración de las entidades del Security Analytics

Para agregar las entidades dentro del servidor de Security Analytics y poder hacer la interconexión entre ellos, primero hay que dar clic en “+” o dar clic en “discover”



Name	Host	Services	Total Memory	CPU	OS	Uptime	Updates	Actions
<input type="checkbox"/> CON1	172.18.32.134	1	62.92 GB	2.47 %	Linux 2.6.32-4...	5 weeks 3 days 20 hours 17 min...	Up-to-Date	
<input type="checkbox"/> CON2	172.18.32.135	1	62.92 GB	1.41 %	Linux 2.6.32-4...	5 weeks 3 days 20 hours 17 min...	Up-to-Date	
<input type="checkbox"/> ESA1	172.18.32.132	1	94.48 GB	1.88 %	Linux 2.6.32-4...	3 weeks 6 days 35 minutes 31 se...	Up-to-Date	
<input type="checkbox"/> ESA2	172.18.32.133	1	94.48 GB	1.61 %	Linux 2.6.32-4...	5 weeks 3 days 20 hours 13 min...	Up-to-Date	
<input type="checkbox"/> LOGDEC1	172.18.32.136	2	62.92 GB	8.94 %	Linux 2.6.32-4...	5 weeks 3 days 20 hours 21 min...	Up-to-Date	
<input type="checkbox"/> LOGDEC2	172.18.32.137	2	62.92 GB	5.14 %	Linux 2.6.32-4...	5 weeks 3 days 20 hours 21 min...	Up-to-Date	
<input type="checkbox"/> SA	127.0.0.1	4	62.92 GB	19.3 %	Linux 2.6.32-4...	5 weeks 3 days 20 hours 27 min...	Up-to-Date	

Ilustración 7. Agregar entidades a Security Analytics



Al dar clic en el signo de más podremos observar la siguiente pantalla donde agregaremos nuestras entidades.

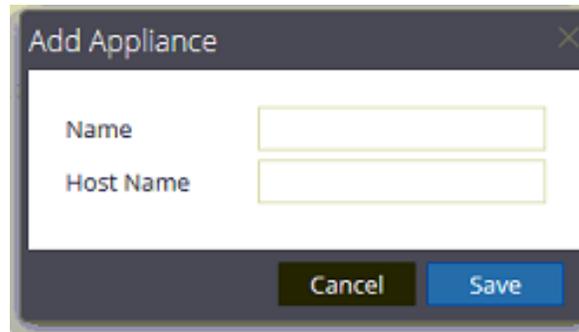
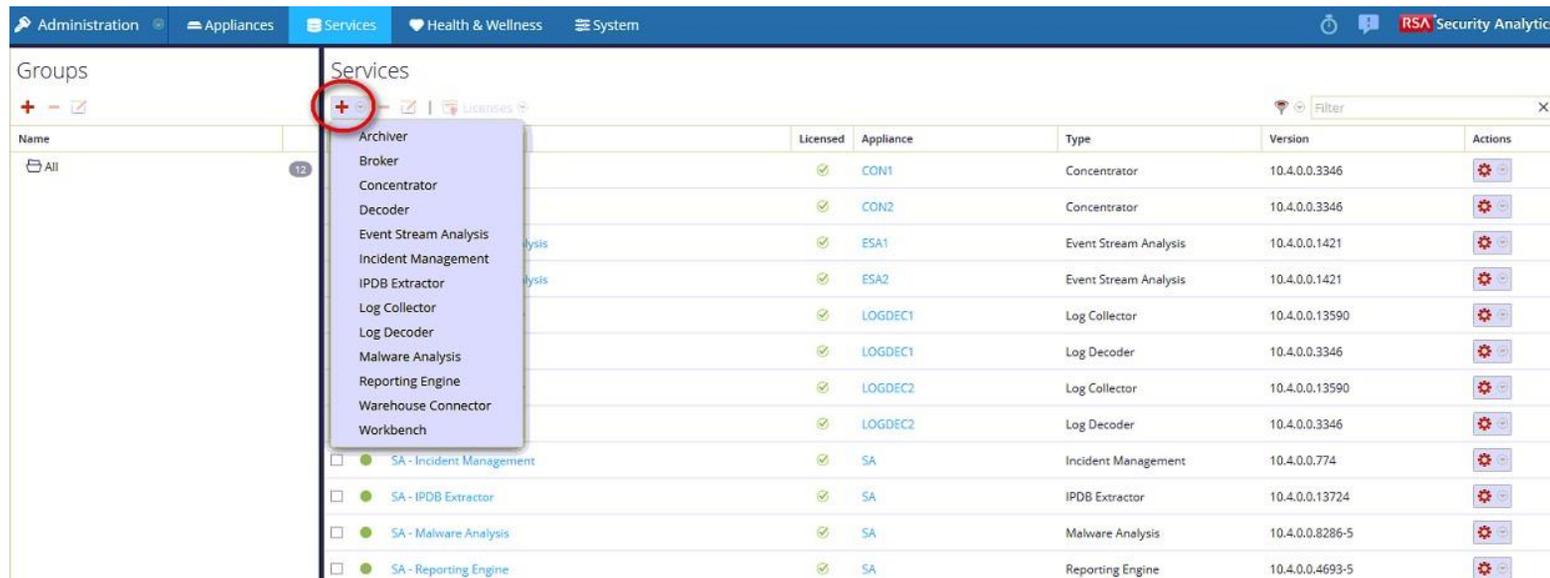


Ilustración 8. Agregar manualmente entidades a Security Analytics

Una vez agregada la entidad, tenemos que proceder a configurar el servicio correspondiente dando clic en el signo de “+” y escogiendo el servicio a agregar.

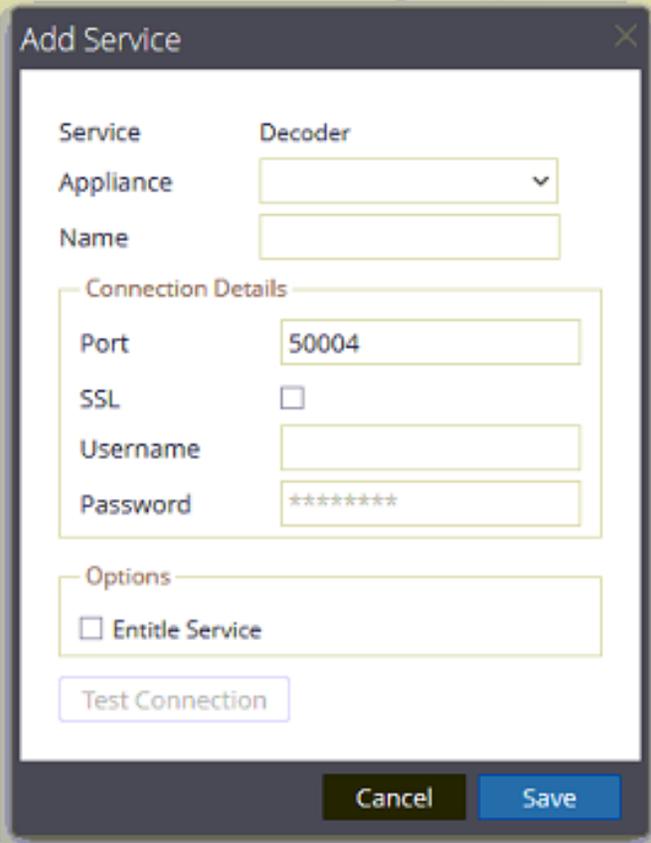


Licensed	Appliance	Type	Version	Actions
✓	CON1	Concentrator	10.4.0.0.3346	⚙️
✓	CON2	Concentrator	10.4.0.0.3346	⚙️
✓	ESA1	Event Stream Analysis	10.4.0.0.1421	⚙️
✓	ESA2	Event Stream Analysis	10.4.0.0.1421	⚙️
✓	LOGDEC1	Log Collector	10.4.0.0.13590	⚙️
✓	LOGDEC1	Log Decoder	10.4.0.0.3346	⚙️
✓	LOGDEC2	Log Collector	10.4.0.0.13590	⚙️
✓	LOGDEC2	Log Decoder	10.4.0.0.3346	⚙️
✓	SA	Incident Management	10.4.0.0.774	⚙️
✓	SA	IPDB Extractor	10.4.0.0.13724	⚙️
✓	SA	Malware Analysis	10.4.0.0.8286-5	⚙️
✓	SA	Reporting Engine	10.4.0.0.4693-5	⚙️

Ilustración 9. Configurar los servicios de Security Analytics.



Una vez que escogemos el servicio a agregar, tenemos que configurar los campos correspondientes, probar que la conexión sea exitosa y guardar el servicio.



The screenshot shows a dialog box titled "Add Service" with a close button (X) in the top right corner. The dialog is divided into several sections:

- Service:** A dropdown menu currently showing "Decoder".
- Appliance:** A dropdown menu.
- Name:** A text input field.
- Connection Details:** A section containing:
  - Port:** A text input field with the value "50004".
  - SSL:** A checkbox that is currently unchecked.
  - Username:** A text input field.
  - Password:** A text input field with asterisks (\*\*\*\*\*).
- Options:** A section containing:
  - Entitle Service:** A checkbox that is currently unchecked.

At the bottom of the dialog, there is a "Test Connection" button, a "Cancel" button, and a "Save" button.

Ilustración 10. Configurar los servicios de Security Analytics.



Name	Licensed	Appliance	Type	Version
CON1 - Concentrator	✓	CON1	Concentrator	10.4.0.0.3346
CON2 - Concentrator	✓	CON2	Concentrator	10.4.0.0.3346
ESA1 - Event Stream Analysis	✓	ESA1	Event Stream Analysis	10.4.0.0.1421
ESA2 - Event Stream Analysis	✓	ESA2	Event Stream Analysis	10.4.0.0.1421
LOGDEC1 - Log Collector	✓	LOGDEC1	Log Collector	10.4.0.0.13590
LOGDEC1 - Log Decoder	✓	LOGDEC1	Log Decoder	10.4.0.0.3346
LOGDEC2 - Log Collector	✓	LOGDEC2	Log Collector	10.4.0.0.13590
LOGDEC2 - Log Decoder	✓	LOGDEC2	Log Decoder	10.4.0.0.3346
SA - Incident Management	✓	SA	Incident Management	10.4.0.0.774
SA - IPDB Extractor	✓	SA	IPDB Extractor	10.4.0.0.13724
SA - Malware Analysis	✓	SA	Malware Analysis	10.4.0.0.8286-5
SA - Reporting Engine	✓	SA	Reporting Engine	10.4.0.0.4693-5

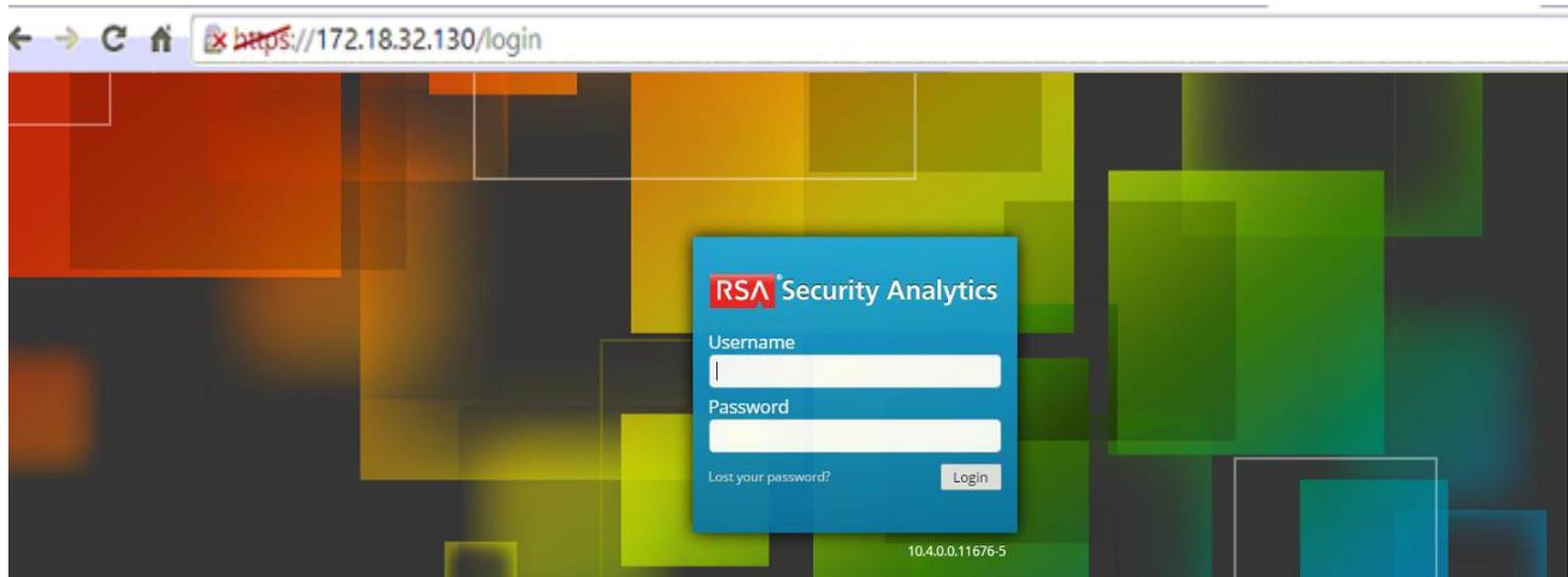
Ilustración 11. Listado de Servicios de Security Analytics

Name	Host	Services	Total Memory	CPU	OS	Uptime
CON1	172.18.32.134	1	62.92 GB	2.48 %	Linux 2.6.32-...	3 days 20 hours 3 minutes 46 se...
CON2	172.18.32.135	1				
ESA1	172.18.32.132	1				
ESA2	172.18.32.133	1	94.48 GB	1.18 %	Linux 2.6.32-...	3 days 19 hours 59 minutes 46 s...
LOGDEC1	172.18.32.136	2	62.92 GB	9.57 %	Linux 2.6.32-...	3 days 20 hours 7 minutes 50 se...
LOGDEC2	172.18.32.137	2	62.92 GB	4.80 %	Linux 2.6.32-...	3 days 20 hours 7 minutes 51 se...
SA	127.0.0.1	4	62.92 GB	23.8 %	Linux 2.6.32-...	3 days 20 hours 13 minutes 22 s...

Ilustración 12. Listado de Entidades de Security Analytics



El ingreso al Security Analytics debe ser realizado desde el navegador con el siguiente formato `https://172.18.32.130` que corresponde a la entidad de Security Analytics Server, y se ingresará con las credenciales proporcionadas al departamento de informática.



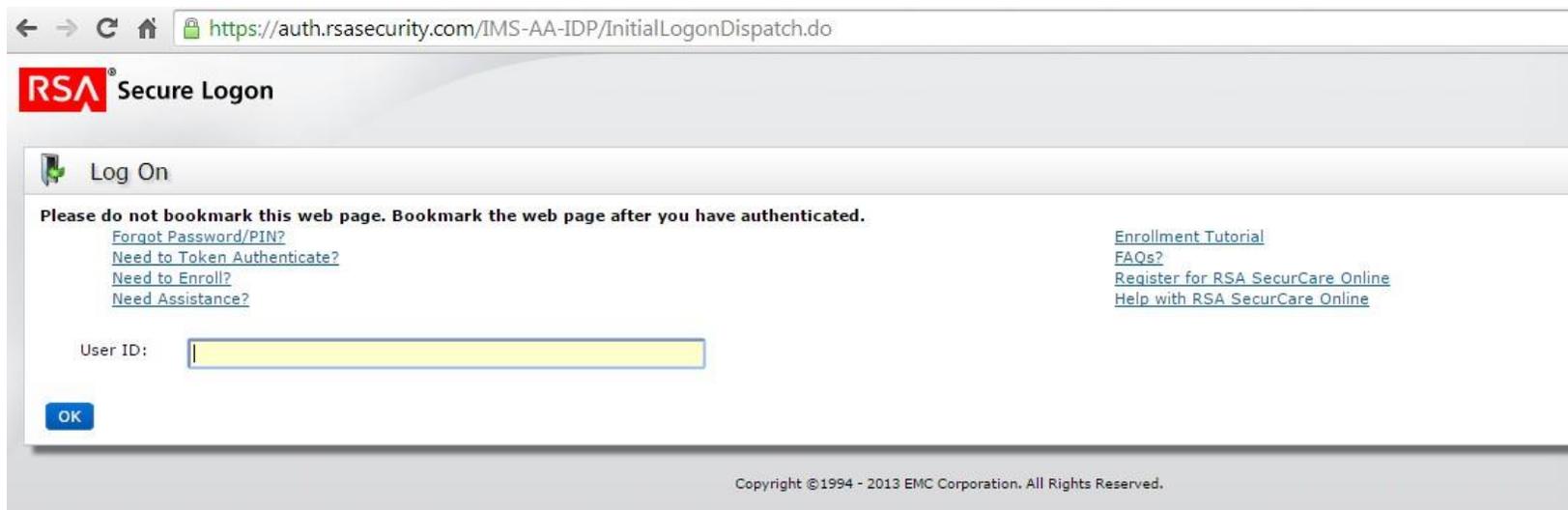
*Ilustración 13. Ingreso a la consola*



## 1.6 Soporte

A continuación, se detalla el proceso a seguir en caso de que exista algún tipo de problema o error de funcionamiento los cuales se pueden escalar directamente con el fabricante.

En primer lugar, se debe ingresar usando cualquier navegador a la siguiente URL: [knowledge.rsasecurity.com](https://knowledge.rsasecurity.com) la cual nos re direccionara a la siguiente URL. En dicha página se deberá ingresar con las credenciales correspondientes, previamente creadas.



17

Ilustración 14. Fuentes a monitorear



Este es el portal de problemas más comunes, base de conocimientos, descargas, información de productos, etc de EMC los cuales contemplan aquellos de Security Analytics que es la solución con la que cuenta INFOTEC. Asimismo, dentro de este portal se puede dar de alta un problema técnico dando clic en "Case Management" en caso de que el problema sea de prioridad 2 o 3 y no impacte críticamente en la operación

<https://knowledge.rsasecurity.com/scolcms/>

**EMC<sup>2</sup>**

HOME MY SUPPORT PRODUCTS DOWNLOADS DOCUMENTATION HELP ABOUT WELCOME JESUS ALBERTO AVALOS VARELA CONTACT MANAGE LOGIN LOG OUT

## RSA SecurCare Online

**Welcome to SecurCare Online**

**Note:** You are currently subscribed to "0" SecurCare Notes and Alerts. [Subscribe Here!](#)

### RSA Authentication Manager 8.1

**END OF PRIMARY SUPPORT REACHED FOR AUTHENTICATION MANAGER 6.x & 7.x**

Primary support for RSA Authentication Manager 6.x & 7.x ended on December 31, 2014. If you have a current Authentication Manager support agreement, you can upgrade to Authentication Manager v8.1 for free.

[More Information on migrating >>](#)

### RSA Security Training and Certification

Prepare yourself for a Challenge!

RSA SOC Simulation challenge is a new offering from RSA Education. Using a Jeopardy!-style format, participants are exposed to network and forensic analysis within a real-world breach scenario. Participants are presented with a use case that requires them to analyze data flowing over the network using simulated SOC dynamics. See more details about this exciting and lively offering on [www.emc.com/rsa-training](http://www.emc.com/rsa-training).

**New Course! RSA ECAT Analysis Fundamentals**

Search SecurCare Online

#### Quick Links

- Products
- Downloads
- Documentation
- Advisories and Notes
- Knowledgebase
- Community

#### Security Advisory Center

- Security Advisories
- Report a Security Vulnerability
- Subscribe to Notes & Advisories

#### Service Center

- Case Management**
- Contact Customer Service

Ilustración 15. Fuentes a monitorear.



Una vez que se da clic en “Case Management” aparecerá la siguiente pantalla con nuestros equipos disponibles actualmente y donde nos brinda información sobre la familia del producto, el nombre de la entidad, cuando expira el soporte del equipo, el número de contrato, y si nuestro contrato sigue activo o inactivo. Para crear un nuevo caso hay que dar clic en “create case”.

**RSA CUSTOMER**  
RSA CUSTOMER CASE MANAGEMENT

**RSA SecurCare® Online**

Cases Home Entitlement **My Products** Knowledge

Welcome, Jose Roberto Leon Marquez

My Profile | Logout

Recent Items

- 00647885
- 00647881
- 00647882
- nwtech-MAL\_UI\_R...

Case Management

**My Products**

Site Name	Product Family	Serial #	Asset	Entitlement Name	Exp Date ▲	Contract #	Case Mng	Contract Renewal Request	Contract Status
FONDO DE INFORMACION Y	RSA NetWitness	132002356	Analytics Server w/10 Users - SW Only	ENHANCED	12/31/2015	30553357	<a href="#">Create Case</a>	<a href="#">Request Contract Renewal</a>	●
FONDO DE INFORMACION Y	RSA NetWitness	132300073	SecAnalytics Log Decoder S/W	ENHANCED	12/31/2015	30553357	<a href="#">Create Case</a>	<a href="#">Request Contract Renewal</a>	●
FONDO DE INFORMACION Y	RSA NetWitness	132300074	SecAnalytics Log Decoder S/W	ENHANCED	12/31/2015	30553357	<a href="#">Create Case</a>	<a href="#">Request Contract Renewal</a>	●
FONDO DE INFORMACION Y	RSA NetWitness	133100069	SecAnalytics Log Cnctr S/W	ENHANCED	12/31/2015	30553357	<a href="#">Create Case</a>	<a href="#">Request Contract Renewal</a>	●
FONDO DE INFORMACION Y	RSA NetWitness	133100070	SecAnalytics Log Cnctr S/W	ENHANCED	12/31/2015	30553357	<a href="#">Create Case</a>	<a href="#">Request Contract Renewal</a>	●
FONDO DE INFORMACION Y	RSA NetWitness	138145014	Event Stream Analysis Software Offering	ENHANCED	12/31/2015	30553357	<a href="#">Create Case</a>	<a href="#">Request Contract Renewal</a>	●
FONDO DE INFORMACION Y	RSA NetWitness	138145015	Event Stream Analysis Software Offering	ENHANCED	12/31/2015	30553357	<a href="#">Create Case</a>	<a href="#">Request Contract Renewal</a>	●
FONDO DE INFORMACION Y	RSA NetWitness	133700006	25TB Cpcty4logs S/W	ENHANCED	12/31/2015	30553357	<a href="#">Create Case</a>	<a href="#">Request Contract Renewal</a>	●
FONDO DE INFORMACION Y	RSA NetWitness	133700007	25TB Cpcty4logs S/W	ENHANCED	12/31/2015	30553357	<a href="#">Create Case</a>	<a href="#">Request Contract Renewal</a>	●

Ilustración 16. Entidades de Security Analytics con los que cuenta INFOTEC



En la pantalla siguiente podemos crear nuestro caso para ser atendidos por el soporte de RSA llenando los campos correspondientes con la información que nos piden, así como adjuntar imágenes o archivos que pudieran ser de ayuda al Ing. que nos apoye para resolver el caso.

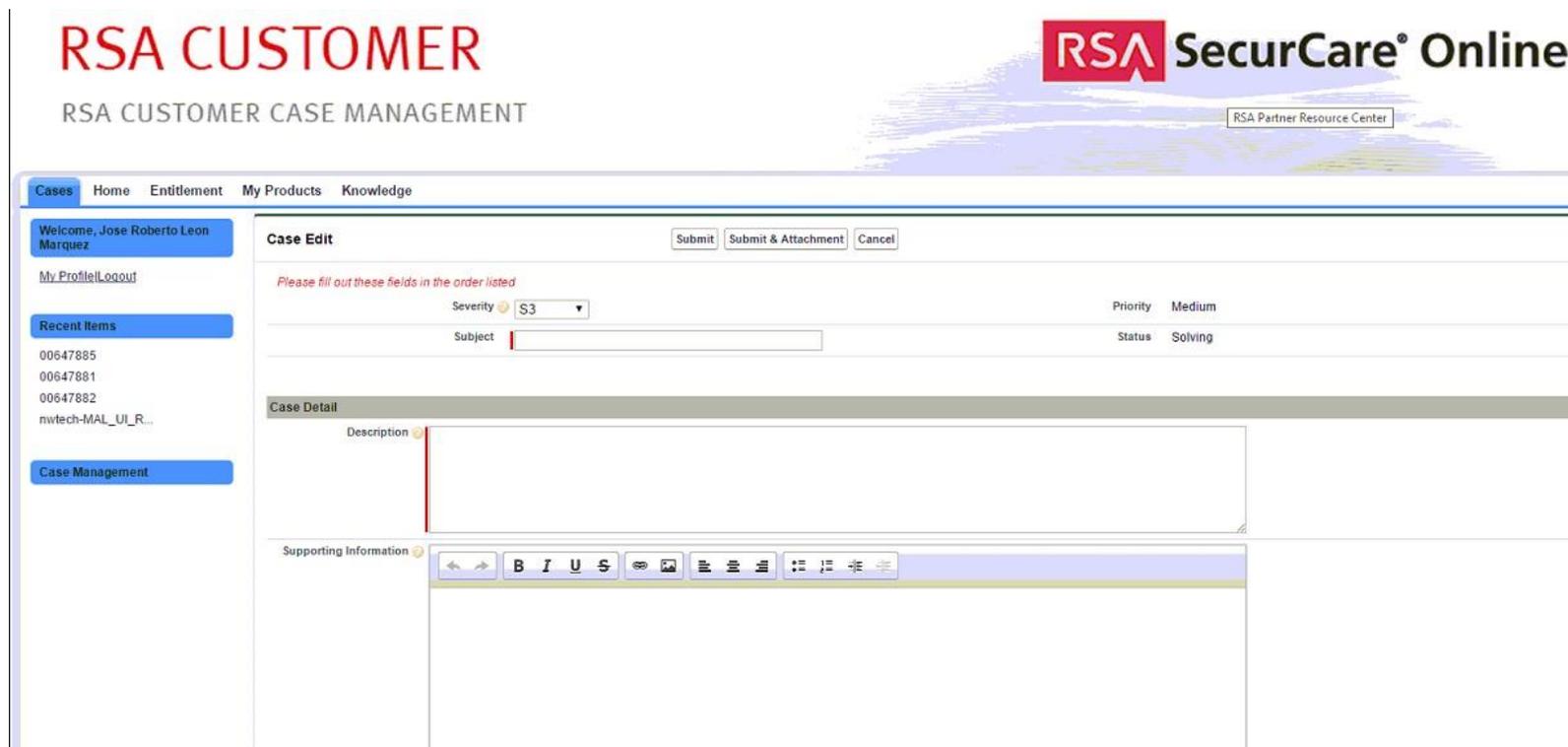


Ilustración 17. Campos a llenar sobre la creación de casos con el soporte de RSA



**Entitlement & Asset Detail**

Entitlement Name **ENHANCED** Asset **Analytics Server w/10 Users**

Environment **Production**

RSA Product Set

- Subject: You must enter a value
- Description: You must enter a value

**Security Analytics**

RSA Product/Service Type **--None--**

RSA Version/Condition **--None--**

Platform **CentOS**

O/S Version **6**

Platform(Other)

**▼ Suggested Articles**

Title	Article Number
-------	----------------

**Contact Details**

Account Name **FONDO DE INFORMACION** Contact Name **Jose Roberto Leon Marquez**

Pref. Communication **Phone** Secondary Contact

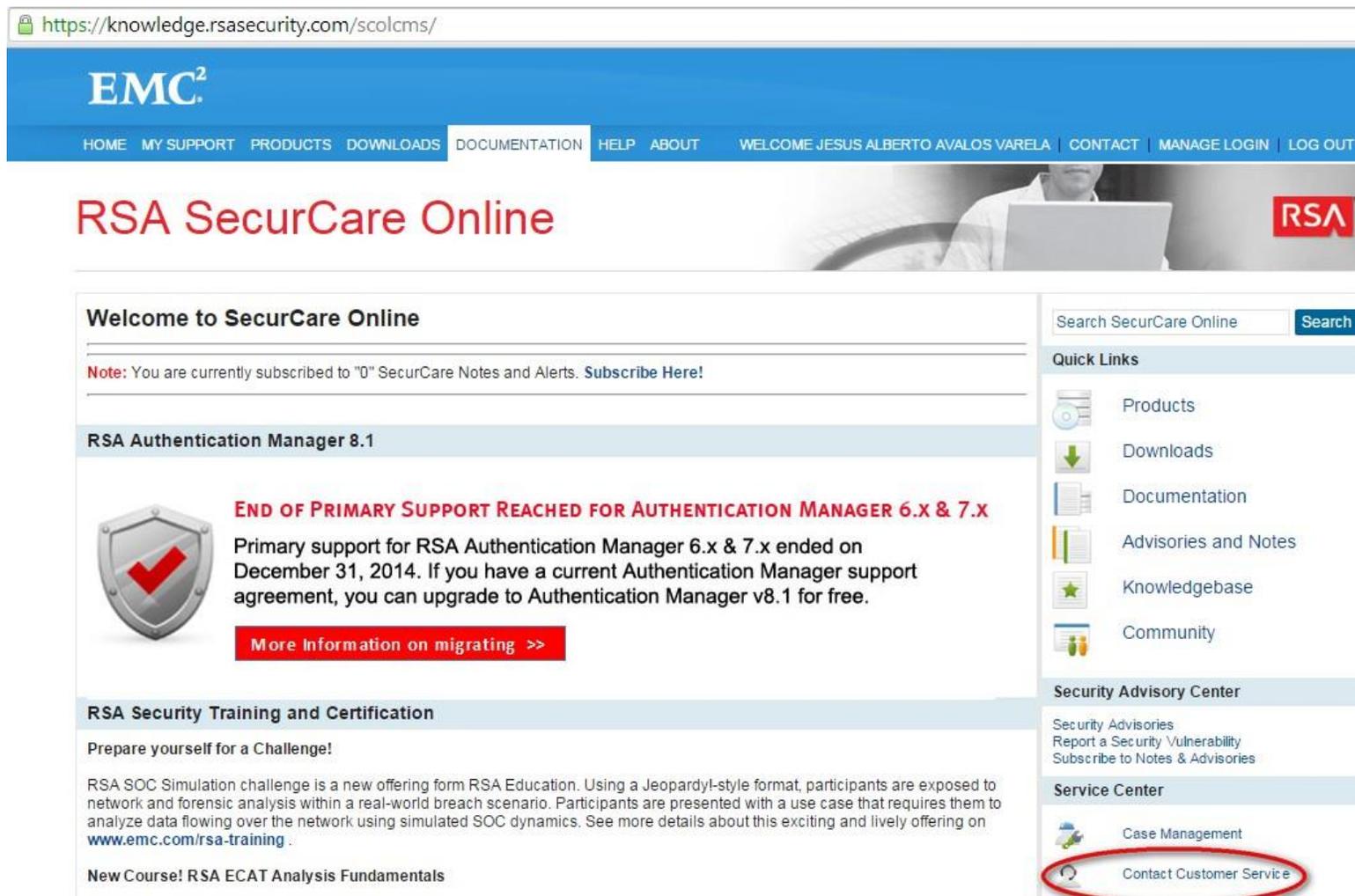
Preferred Language **English**

Preferred Language (Other)

Ilustración 18. Datos esenciales para la creación de casos de Security Analytics.



Asimismo, se puede abrir la página con los teléfonos de soporte de RSA en caso de que el problema sea crítico y debamos ponernos en contacto directamente con un Ingeniero que nos apoye con dicho problema lo antes posible.



https://knowledge.rsasecurity.com/scolcms/

**EMC<sup>2</sup>**

HOME MY SUPPORT PRODUCTS DOWNLOADS DOCUMENTATION HELP ABOUT WELCOME JESUS ALBERTO AVALOS VARELA CONTACT MANAGE LOGIN LOG OUT

## RSA SecurCare Online

**Welcome to SecurCare Online**

**Note:** You are currently subscribed to "0" SecurCare Notes and Alerts. [Subscribe Here!](#)

### RSA Authentication Manager 8.1

**END OF PRIMARY SUPPORT REACHED FOR AUTHENTICATION MANAGER 6.X & 7.X**

Primary support for RSA Authentication Manager 6.x & 7.x ended on December 31, 2014. If you have a current Authentication Manager support agreement, you can upgrade to Authentication Manager v8.1 for free.

[More Information on migrating >>](#)

### RSA Security Training and Certification

Prepare yourself for a Challenge!

RSA SOC Simulation challenge is a new offering from RSA Education. Using a Jeopardy!-style format, participants are exposed to network and forensic analysis within a real-world breach scenario. Participants are presented with a use case that requires them to analyze data flowing over the network using simulated SOC dynamics. See more details about this exciting and lively offering on [www.emc.com/rsa-training](http://www.emc.com/rsa-training).

**New Course! RSA ECAT Analysis Fundamentals**

Search SecurCare Online

#### Quick Links

- Products
- Downloads
- Documentation
- Advisories and Notes
- Knowledgebase
- Community

#### Security Advisory Center

- Security Advisories
- Report a Security Vulnerability
- Subscribe to Notes & Advisories

#### Service Center

- Case Management
- Contact Customer Service**

Ilustración 19. Fuentes a monitorear



Los teléfonos son los siguientes:

## RSA SecurCare Online



The screenshot shows the RSA SecurCare Online interface. At the top, there are two tabs: "Phone Support" (selected) and "Customer Survey". Below the tabs is the heading "Contact Support". A table lists support phone numbers for various countries in the Americas region.

Americas	
USA	800 995 5095 1-781-515-7700 1-781-515-7710 (fax)
Brazil	0800 891 1997
Chile	1230 020 3952
Colombia	01800 9 154655
Mexico	001 8009955095

Ilustración 20. Teléfonos de Soporte de la región de América



## 1.7 Entidades y puertos del Security Analytics

A continuación, se mencionan todos aquellos puertos necesarios por servicio utilizados por la solución de Security Analytics.

Device/Service	Port(s) /Security Analytics Core Non-SSL	Security Analytics Core SSL
Appliance	50006	
Appliance (REST)	50106	
Archiver	50008	56008
Archiver (REST)	50108	
Broker	50003	56003
Broker (REST)	50103	
rsaCAS	50010	
CLDB	7222	
CLDB JMX Monitor port	7220	
CLDB Web Port	7221	
Concentrator	50005	56005
Concentrator (REST)	50105	
Decoder	50004	56004
Decoder (REST)	50104	
ESA	50030	
HBase Master	60000	
Incident Management	50040	
IPDB Extractor	50009	
IPDB Extractor	50025	56025
Web UI HTTP	8080	



Device/Service	Port(s) /Security Analytics Core Non-SSL	Security Analytics Core SSL
Web UI HTTPS	8443	
Workbench	50007	56007
Workbench (REST)	50107	
ZooKeeper	5181	
ZooKeeper Leader Communication	2888	
ZooKeeper Leader Election	3888	
IPDB Extractor (REST)	50125	
JobTracker	9001	
JobTracker Web	50030	
Local Log Collector (NwLogCollector on Log Decoder)	50001, Pulls from Remote Log Collector through 5671	56001
LDAP	389	
Log Decoder	50002	56002
Log Decoder (REST)	50102	
Log Decoder Protobuf	50202	
Log Decoder Protobuf	56202	
Log Decoder Syslog	514	
Log Decoder Syslog	6514	
Malware Analysis	60007	
MFS Server	5660	
NFS	2049	
NFS Management	9998	
NFS Monitor (For HA)	9997	
NFS Port Mapper	111	



<b>Device/Service</b>	<b>Port(s) /Security Analytics Core Non-SSL</b>	<b>Security Analytics Core SSL</b>
Remote Log Collector (NwLogCollector on remote VM)	50001, Pushes to Local Log Collector through 5671	56001
Reporting Engine	51113	
SA Warehouse Agent	50020	
SMTP	25	
SSH	22	
TaskTracker Web	50060	
Warehouse Connector	50020	56020
Warehouse Connector (REST)	50120	

*Tabla 1. Puertos Security Analytics*



## 2. LIVE

### Security Analytics Live

Live es el componente de Security Analytics que gestiona la comunicación y sincronización entre entidades de Security Analytics y una biblioteca de contenido en vivo disponible para los clientes de RSA Security Analytics

El sistema de gestión de contenidos (CMS conocido como Live) es una fuente valiosa de los últimos recursos de seguridad en Internet para los clientes de Security Analytics. Proporciona una visión de la inteligencia y habilidades analíticas de la comunidad mundial de seguridad para garantizar que los usuarios tengan la visibilidad más actual en vectores de ataque.

Live reúne la mejor inteligencia avanzada de amenazas y contenido de la comunidad mundial de la seguridad – las ideas, la investigación, el seguimiento continuo y análisis - y lo lleva directamente al centro de operaciones de seguridad del usuario para clasificar definitivamente equipos asociados con botnets, malware y otros ataques maliciosos. Live agrega, consolida y destaca sólo la información más relevante para una organización en una base de tiempo real.



Ilustración 21. Contenido de la licencia de LIVE Básico.





Ilustración 22. Contenido de la licencia de LIVE Enhanced.



Ilustración 23. Contenido de la licencia de LIVE Premium.



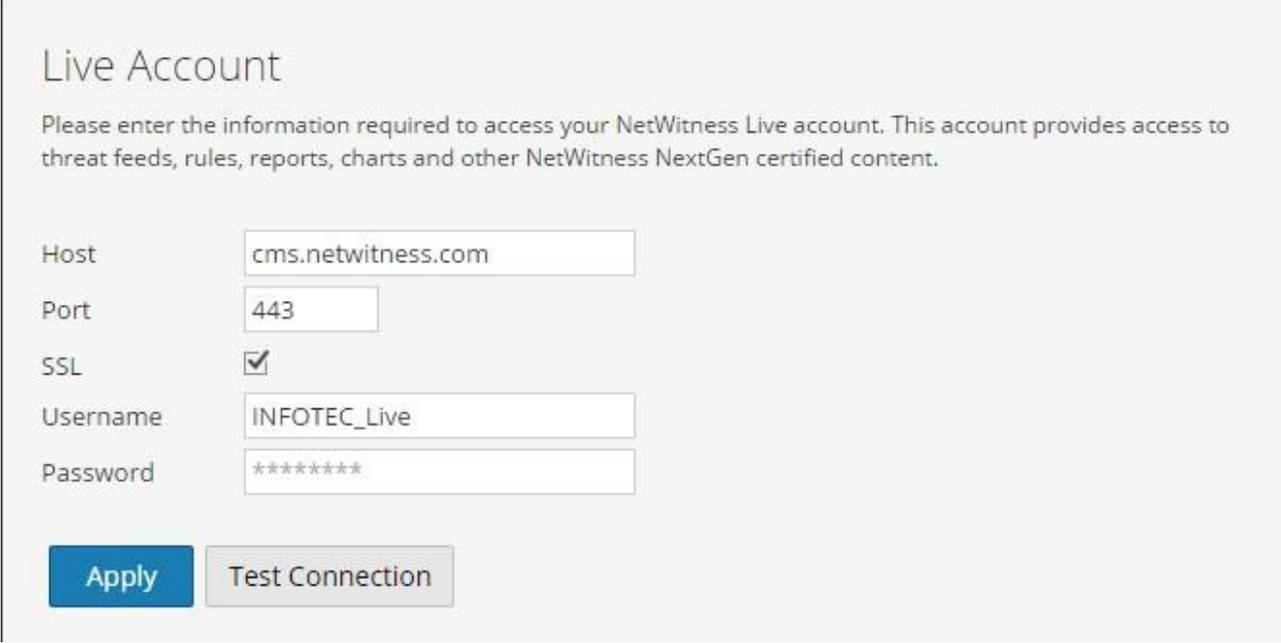
Ilustración 24. Contenido de la licencia de LIVE Freeware.



## 2.1 Descripción de la Plataforma

A continuación, se muestra las credenciales creadas para INFOTEC con el fin de poder hacer uso de todas las ventajas que nos ofrece la licencia de LIVE básica con la que se cuenta.

- ❖ Usuario: INFOTEC\_Live
- ❖ Password:



**Live Account**

Please enter the information required to access your NetWitness Live account. This account provides access to threat feeds, rules, reports, charts and other NetWitness NextGen certified content.

Host	<input type="text" value="cms.netwitness.com"/>
Port	<input type="text" value="443"/>
SSL	<input checked="" type="checkbox"/>
Username	<input type="text" value="INFOTEC_Live"/>
Password	<input type="password" value="*****"/>

Ilustración 25. Credenciales LIVE.



## 2.2 Descripción general

RSA Security Analytics proporciona automáticamente información sobre amenazas a los clientes a través de RSA Live. RSA Live agrega datos de amenazas y la convierte en analizadores y reglas de correlación, a continuación, se alimenta y se fusiona con los datos del cliente dentro de RSA Security Analytics. Esto significa que los usuarios pueden tomar mucho más fácilmente las ventajas de lo que otros ya han encontrado y saber lo que debe buscar. Una vez entregado, la inteligencia operativa se puede aplicar a los datos entrantes o históricos.

## 2.3 Arquitectura RSA LIVE

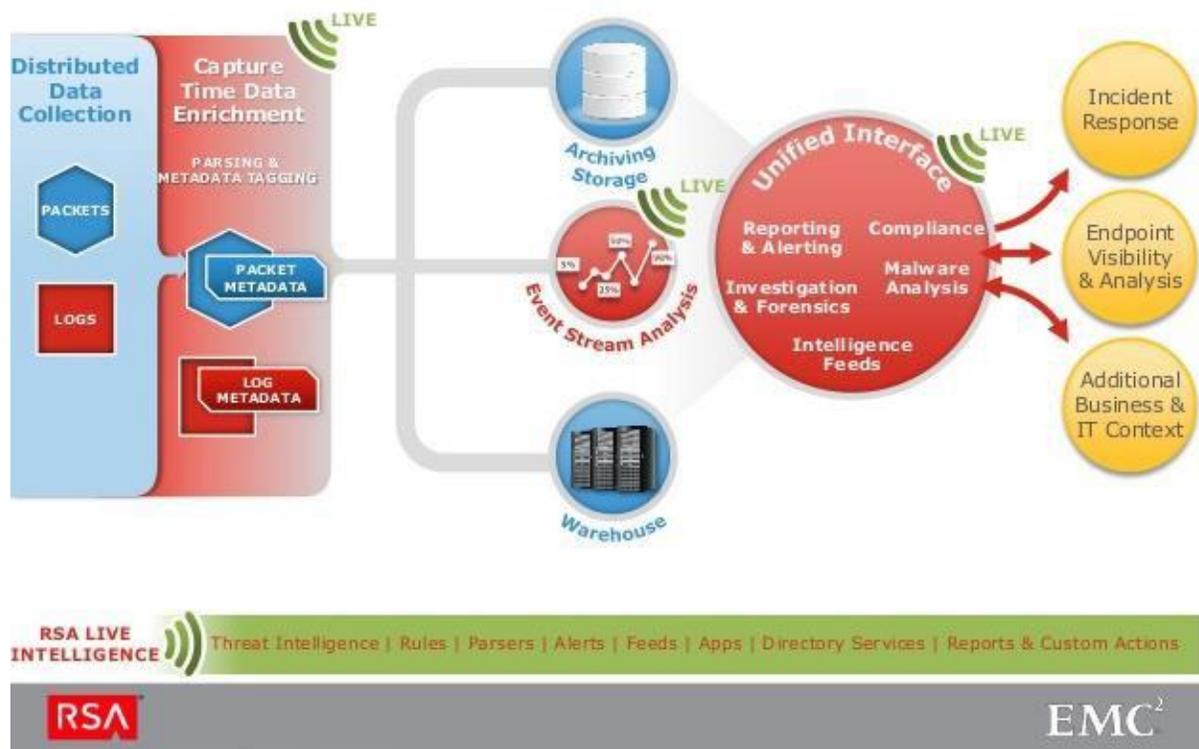
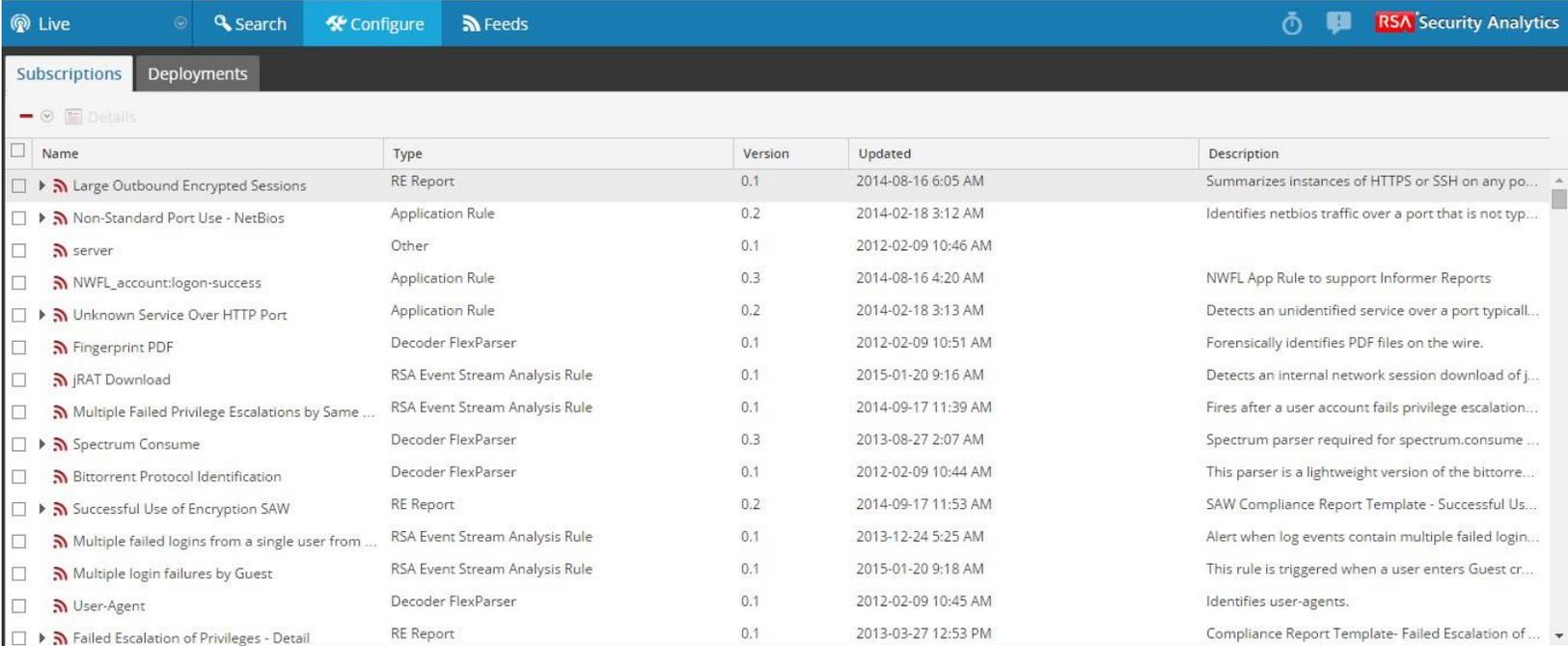


Ilustración 26. Arquitectura LIVE



Asimismo, en la pestaña de Suscripciones podemos apreciar toda la inteligencia a la cual estamos conectados con el fin de tener una mayor visibilidad sobre nuestra red.



Name	Type	Version	Updated	Description
Large Outbound Encrypted Sessions	RE Report	0.1	2014-08-16 6:05 AM	Summarizes instances of HTTPS or SSH on any po...
Non-Standard Port Use - NetBios	Application Rule	0.2	2014-02-18 3:12 AM	Identifies netbios traffic over a port that is not typ...
server	Other	0.1	2012-02-09 10:46 AM	
NWFL_account:logon-success	Application Rule	0.3	2014-08-16 4:20 AM	NWFL App Rule to support Informer Reports
Unknown Service Over HTTP Port	Application Rule	0.2	2014-02-18 3:13 AM	Detects an unidentified service over a port typicall...
Fingerprint PDF	Decoder FlexParser	0.1	2012-02-09 10:51 AM	Forensically identifies PDF files on the wire.
jRAT Download	RSA Event Stream Analysis Rule	0.1	2015-01-20 9:16 AM	Detects an internal network session download of j...
Multiple Failed Privilege Escalations by Same ...	RSA Event Stream Analysis Rule	0.1	2014-09-17 11:39 AM	Fires after a user account fails privilege escalation...
Spectrum Consume	Decoder FlexParser	0.3	2013-08-27 2:07 AM	Spectrum parser required for spectrum.consume ...
Bittorrent Protocol Identification	Decoder FlexParser	0.1	2012-02-09 10:44 AM	This parser is a lightweight version of the bittorre...
Successful Use of Encryption SAW	RE Report	0.2	2014-09-17 11:53 AM	SAW Compliance Report Template - Successful Us...
Multiple failed logins from a single user from ...	RSA Event Stream Analysis Rule	0.1	2013-12-24 5:25 AM	Alert when log events contain multiple failed login...
Multiple login failures by Guest	RSA Event Stream Analysis Rule	0.1	2015-01-20 9:18 AM	This rule is triggered when a user enters Guest cr...
User-Agent	Decoder FlexParser	0.1	2012-02-09 10:45 AM	Identifies user-agents.
Failed Escalation of Privileges - Detail	RE Report	0.1	2013-03-27 12:53 PM	Compliance Report Template- Failed Escalation of...

admin | English (United States) GMT-06:00 Send Us Feedback | 10.4.0.0.11676-5

Ilustración 27. Suscripciones de LIVE.



Se pueden observar a detalle cada una de las actividades realizadas dentro de la consola de Security Analytics en tiempo real.

Timestamp	Level	Message
2015-02-10T13:47:10.735	WARN	Service has not received update, resetting CON2 - Concentrator
2015-02-10T13:47:10.736	WARN	Appliance has not received update, resetting CON2
2015-02-10T13:52:10.734	WARN	Service has not received update, resetting ESA1 - Event Stream Analysis
2015-02-10T13:52:10.735	WARN	Appliance has not received update, resetting ESA1
2015-02-10T13:52:10.735	WARN	Service has not received update, resetting CON2 - Concentrator
2015-02-10T13:52:10.736	WARN	Appliance has not received update, resetting CON2
2015-02-10T13:54:02.237	ERROR	Duplicate CSR new [428b2317-31fb-4878-82b3-d565e27c333d NWAPPLIANCE21591 172.18.32.134], existing [d51f11fe-8053-479e-93b5-3ff60a0f4b20 CON1 172.18.32.134]
2015-02-10T13:54:02.241	ERROR	Duplicate CSR new [4505672e-e549-4183-8de9-93dbb5e0ee2a NWAPPLIANCE22563 172.18.32.132], existing [c9101fea-c6ff-4512-92ef-7e62b5df86da ESA1 172.18.32.132]
2015-02-10T13:54:30.458	INFO	Imported meta types from end point: 7/ESA2 - Event Stream Analysis
2015-02-10T13:54:30.946	INFO	Imported meta types from end point: 14/ESA1 - Event Stream Analysis

Ilustración 28. Logs de la consola.

32

Actualmente se cuenta con 4 usuarios creados de los 10 que se tienen disponibles

Username	Name	Email Address	Roles	External
Ameneses	Axel Meneses	nestor.meneses@inf...	Administrators, Analysts, MalwareAnalysts, Operators, SOC_Managers	no
IngenieroOP	Ingeniero de operacion	soc.infotec@infotec...	Administrators, Analysts, MalwareAnalysts, Operators, SOC_Managers	no
IngenieroQA	IngenieroQA	soc.infotec@infotec...	Administrators, Analysts, MalwareAnalysts, Operators, SOC_Managers	no
admin	Administrator		Administrators	no

Ilustración 29. Usuarios del Security Analytics.



A continuación, podemos observar los roles con los que se cuenta actualmente aunque es posible crear el número de roles que consideremos necesarios.

Name	Description	Permissions
Analysts	The SOC Analysts persona is c...	Dashlet Access - Alerting Recent Alerts Dashlet, Dashlet Access - Top Alerts Dashlet, View Reports, View Charts, Export Report, Access View, Export Rule, Access Health & Wellness, Access...
Operators	The System Operators Person...	View Appliances, View Rules, Deploy Live Resources, Manage Live Resources, Access Alerting Module, Manage SA Logs, Dashlet Access - Admin Device List Dashlet, Dashlet Access - Live ...
SOC_Managers	The persona for SOC Manager...	Dashlet Access - Alerting Recent Alerts Dashlet, Dashlet Access - Top Alerts Dashlet, View Rules, View Reports, View Charts, Export Report, Access View, Export Rule, Access Health & Well...
MalwareAnalysts	The persona of Malware Analy...	Initiate Malware Analysis Scan, Navigate Events, Access Incident Module, View Malware Analysis Events, Access Investigation Module, Navigate Values, View and Manage Incidents, Down...
Administrators	The System Administrators pe...	Dashlet Access - Alerting Recent Alerts Dashlet, Dashlet Access - Top Alerts Dashlet, View Rules, Deploy Live Resources, View Reports, View Charts, Export Report, Manage Devices, Acces...

Ilustración 30. Roles de usuarios del Security Analytics.

## 2.4 Licenciamiento

Las licencias que se tienen por parte de INFOTEC son las siguientes:

Nombre de la entidad	No de Serie	No. de Contrato	Fecha de Expiración	Familia del Producto	Modelo	Licencia	Versión
<b>Analytics Serverw/10 Users - S/W Only</b>	132002356	30553357	31/12/2015	RSA NetWitness	SA-SERVER-SW	smcSA_Server 2015.1231	10.4.0.0.11676-5
<b>Analyst Seat</b>	132002356	30553357	31/12/2015	RSA NetWitness	Other	smcAnalyst_Seat 2015.1231 (10)	10.4.0.0.11676-5
<b>Broker</b>	132002356	30553357	31/12/2015	RSA NetWitness	Other	smcBroker 2015.1231	10.4.0.0.11676-5
<b>SecAnalytics Log Decoder S/W</b>	132300073	30553357	31/12/2015	RSA NetWitness	SA-L-DEC-SW	smcLogDecoder 2012.1231	10.4.0.0.11676-5



Nombre de la entidad	No de Serie	No. de Contrato	Fecha de Expiración	Familia del Producto	Modelo	Licencia	Versión
<b>SecAnalytics Log Decoder S/W</b>	132300074	30553357	31/12/2015	RSA NetWitness	SA-L-DEC-SW	smcLogDecoder 2012.1231	10.4.0.0.11676-5
<b>SecAnalytics Log Cncntrtr S/W</b>	133100069	30553357	31/12/2015	RSA NetWitness	SA-L-CON-SW	smcConcentrator 2012.1231	10.4.0.0.11676-5
<b>SecAnalytics Log Cncntrtr S/W</b>	133100070	30553357	31/12/2015	RSA NetWitness	SA-L-CON-SW	smcConcentrator 2012.1231	10.4.0.0.11676-5
<b>Event Stream Analysis Software Offering</b>	138145014	30553357	31/12/2015	RSA NetWitness	SA-ESA-SW	smcEventStream Analisis 2015.1231	10.4.0.0.11676-5
<b>Event Stream Analysis Software Offering</b>	138145015	30553357	31/12/2015	RSA NetWitness	SA-ESA-SW	smcEventStream Analisis 2015.1231	10.4.0.0.11676-5
<b>25TB Cpcty4logs S/W</b>	133700006	30553357	31/12/2015	RSA NetWitness	SA-25TB-CAP-L-SW	smcLog_Capacity 2015.1231 (25)	10.4.0.0.11676-5
<b>25TB Cpcty4logs S/W</b>	133700007	30553357	31/12/2015	RSA NetWitness	SA-25TB-CAP-L-SW	smcLog_Capacity 2015.1231 (25)	10.4.0.0.11676-5

Tabla 2. Licencias INFOTEC



Para licenciar el equipo primero es necesario ir a <https://download.rsasecurity.com> entrar con las credenciales correspondientes y crear el servidor de licencias.

**Download Central**  
**SOFTWARE/LICENSE**

**HOME**  
**SOFTWARE**  
PRODUCT LIST  
ORDER HISTORY  
**DEVICE MANAGEMENT**  
SEARCH SERVERS  
CREATE SERVER  
UPLOAD CAPABILITY REQUEST  
**INFORMATION**  
FAQS  
DOWNLOAD SUPPORT  
PRODUCT SUPPORT  
SWITCH SITE

**Create Server**

To input a Security Analytics (SA) local license server, copy the License Server ID located on the SA user interface information page (Administration > System > Info page).

**Important:**  
If keying in the License Server ID manually; all UPPER CASE letters must be used. Errors made within this field are irreversible and will require RSA customer support for resolution. The ID Type and Type fields must be set to Ethernet for the server to function.

License Server ID:

ID Type:

Type:

Alias:

Ilustración 31. Creación del Servidor de Licencias.

**View Server**

License Server ID: 00505695610F

Type: Ethernet

ID Type: ETHERNET

Identity: RSA Medium

Alias:

Vendor Dictionary : (None)

[Map Add-Ons](#) [Remove Add-Ons](#) [Download Capability Response](#) [View History](#) [View Served Clients](#)

Ilustración 32. Servidor de Licencias creado.



Una vez creado dicho servidor se procede a mapear las licencias para nuestro Security Analytics.

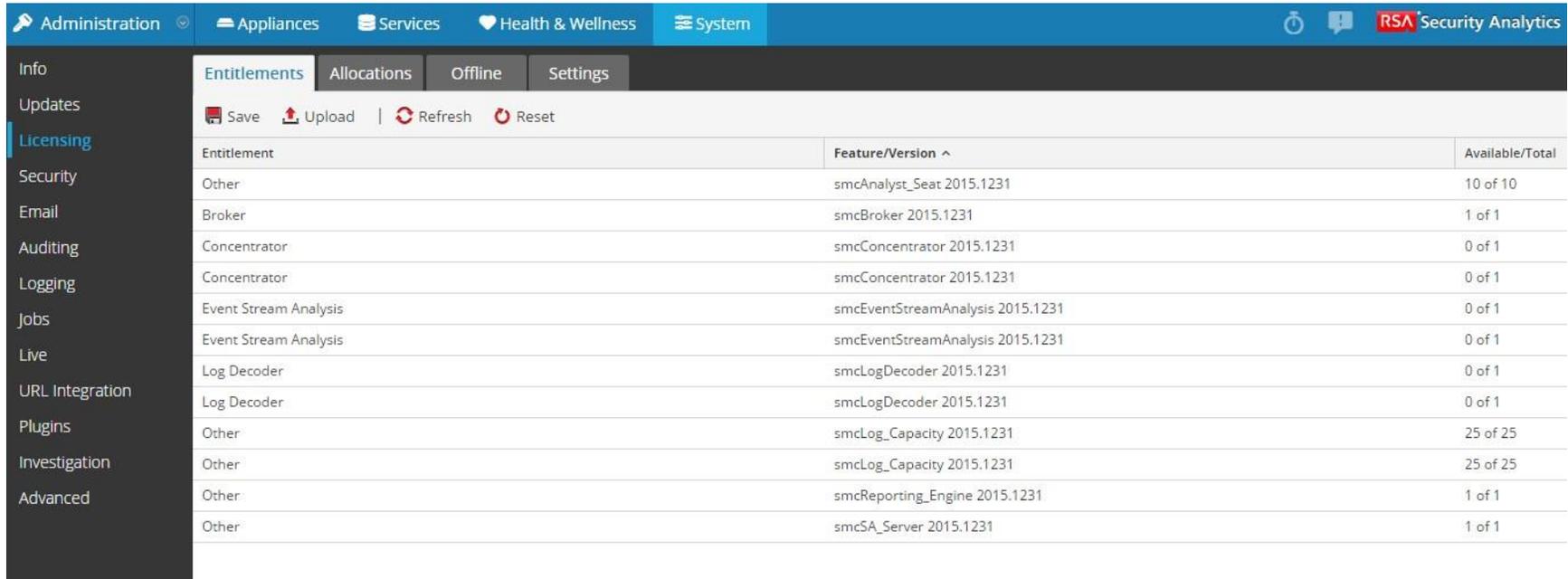
### Add-Ons

<u>Add-On Name</u>	<u>Status</u>	<u>Serial Number</u>	<u>Units Mapped</u>	<u>Expiration</u>	<u>Downloadable Items</u>
Analytics Server w/10 Users - S/W Only	License not generated	132002356	1	Permanent	<a href="#">View</a>
SecAnalytics Log Decoder S/W	License not generated	132300073	1	Permanent	<a href="#">View</a>
SecAnalytics Log Decoder S/W	License not generated	132300074	1	Permanent	<a href="#">View</a>
SecAnalytics Log Cncntrtr S/W	License not generated	133100069	1	Permanent	<a href="#">View</a>
SecAnalytics Log Cncntrtr S/W	License not generated	133100070	1	Permanent	<a href="#">View</a>
SecAnalytics ESA S/W	License not generated	138145014	1	Permanent	<a href="#">View</a>
SecAnalytics ESA S/W	License not generated	138145015	1	Permanent	<a href="#">View</a>
25TB Cpcty4logs S/W	License not generated	133700006	1	Permanent	None
25TB Cpcty4logs S/W	License not generated	133700007	1	Permanent	None

Ilustración 33. Licencias generándose y listas para descargarse al SA Server.



Una vez creado dicho servidor se procede a mapear las licencias para nuestro Security Analytics en la GUI con el fin de sincronizar nuestra solución con el servidor de licencias



Entitlement	Feature/Version ^	Available/Total
Other	smcAnalyst_Seat 2015.1231	10 of 10
Broker	smcBroker 2015.1231	1 of 1
Concentrator	smcConcentrator 2015.1231	0 of 1
Concentrator	smcConcentrator 2015.1231	0 of 1
Event Stream Analysis	smcEventStreamAnalysis 2015.1231	0 of 1
Event Stream Analysis	smcEventStreamAnalysis 2015.1231	0 of 1
Log Decoder	smcLogDecoder 2015.1231	0 of 1
Log Decoder	smcLogDecoder 2015.1231	0 of 1
Other	smcLog_Capacity 2015.1231	25 of 25
Other	smcLog_Capacity 2015.1231	25 of 25
Other	smcReporting_Engine 2015.1231	1 of 1
Other	smcSA_Server 2015.1231	1 of 1

Ilustración 34. Licencias sincronizadas con nuestra solución.



Ya que tenemos las licencias en nuestro repositorio, el siguiente paso es activar la licencia en cada uno de nuestras identidades.

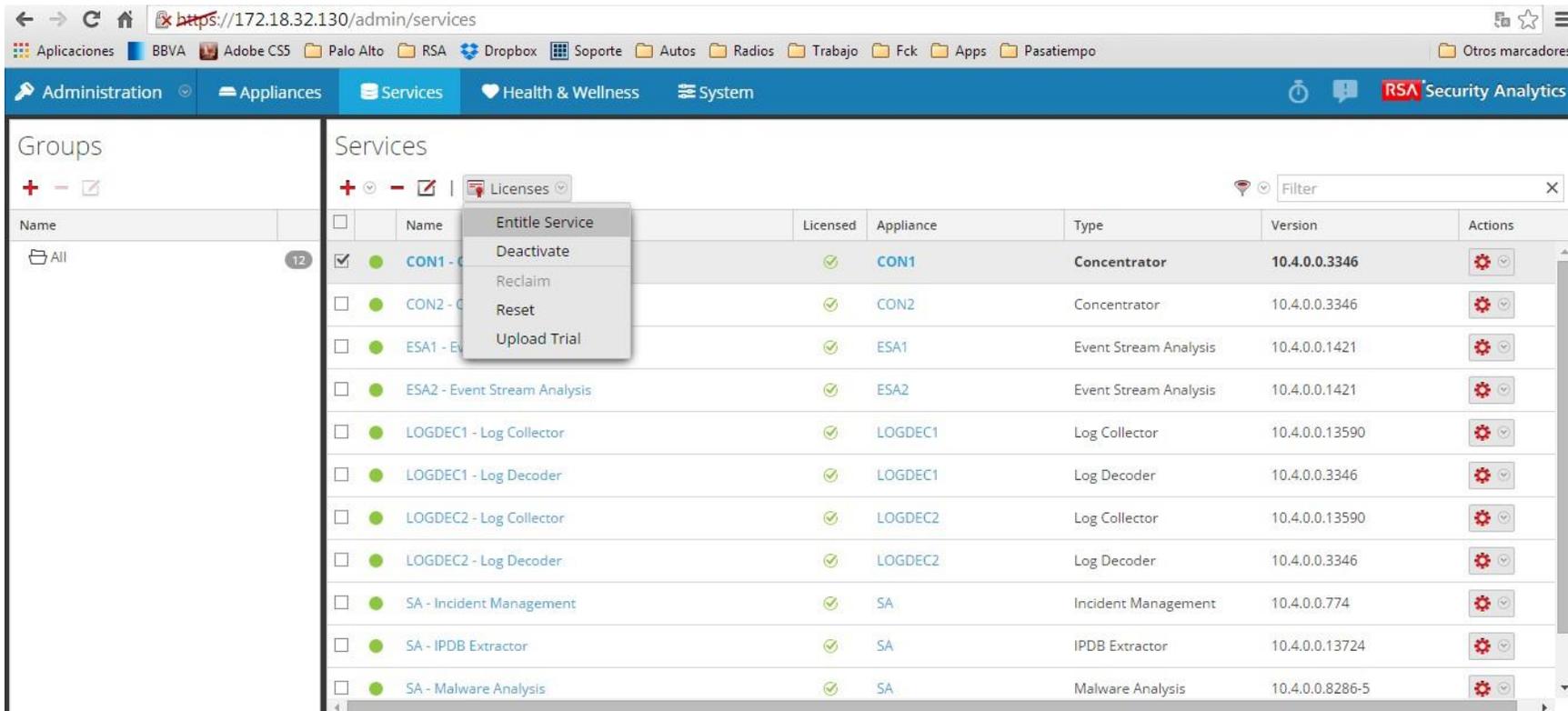


Ilustración 35. Licenciamiento de Entidades.



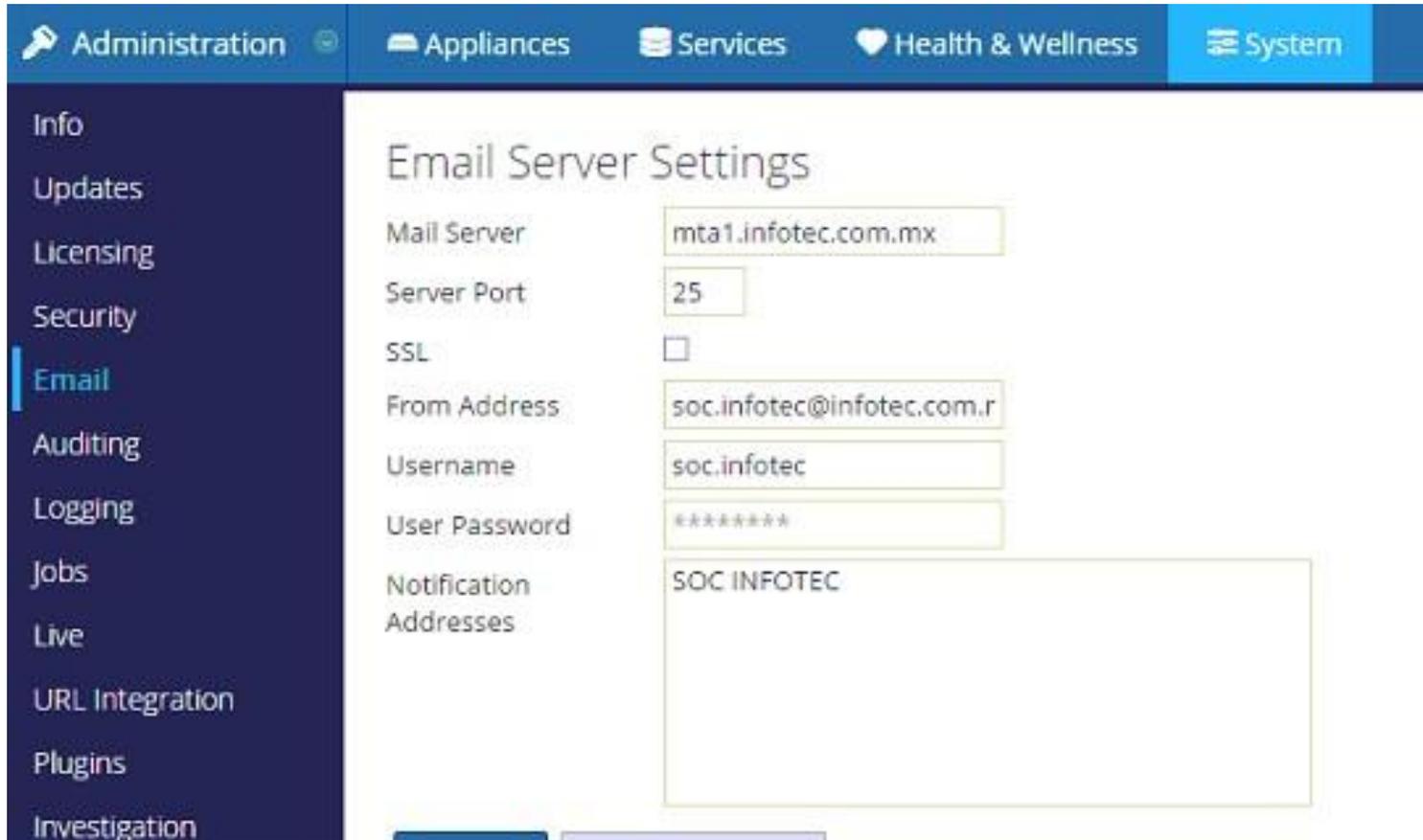


Ilustración 36. Configuración de email.



## 3. CONFIGURACIÓN DE ENTIDADES

### 3.1 Concentrator 1

Change Service | CON1 - Concentrator | System

Start Aggregation Stop Aggregation Appliance Tasks Shutdown Service Shutdown Appliance Service Reboot

<h4>Concentrator Service Information</h4> <table border="0"> <tr><td>Name</td><td>CON1 (Concentrator)</td></tr> <tr><td>Version</td><td>10.4.0.0.3346 (Rev 5ec2f8f4ce31)</td></tr> <tr><td>Memory Usage</td><td>841 MB (1.31% of 64428 MB)</td></tr> <tr><td>CPU</td><td>1%</td></tr> <tr><td>Running Since</td><td>2015-Jan-26 21:15:51</td></tr> <tr><td>Uptime</td><td>1 hour 14 minutes 19 seconds</td></tr> <tr><td>Current Time</td><td>2015-Jan-26 22:30:10</td></tr> </table> <h4>Concentrator User Information</h4> <table border="0"> <tr><td>Name</td><td>admin</td></tr> <tr><td>Groups</td><td>Administrators</td></tr> <tr><td>Roles</td><td>concentrator.manage, connections.manage, database.manage, everyone, index.manage, logs.manage, owner, rules.manage, sdk.content, sdk.manage, sdk.meta, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage</td></tr> </table>	Name	CON1 (Concentrator)	Version	10.4.0.0.3346 (Rev 5ec2f8f4ce31)	Memory Usage	841 MB (1.31% of 64428 MB)	CPU	1%	Running Since	2015-Jan-26 21:15:51	Uptime	1 hour 14 minutes 19 seconds	Current Time	2015-Jan-26 22:30:10	Name	admin	Groups	Administrators	Roles	concentrator.manage, connections.manage, database.manage, everyone, index.manage, logs.manage, owner, rules.manage, sdk.content, sdk.manage, sdk.meta, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage	<h4>Appliance Service Information</h4> <table border="0"> <tr><td>Name</td><td>CON1 (Appliance)</td></tr> <tr><td>Version</td><td>10.4.0.0.3346 (Rev 5ec2f8f4ce31)</td></tr> <tr><td>Memory Usage</td><td>17668 KB (0.03% of 64428 MB)</td></tr> <tr><td>CPU</td><td>1%</td></tr> <tr><td>Running Since</td><td>2015-Jan-26 21:15:42</td></tr> <tr><td>Uptime</td><td>1 hour 14 minutes 28 seconds</td></tr> <tr><td>Current Time</td><td>2015-Jan-26 22:30:10</td></tr> </table> <h4>Appliance User Information</h4> <table border="0"> <tr><td>Name</td><td>admin</td></tr> <tr><td>Groups</td><td>Administrators</td></tr> <tr><td>Roles</td><td>appliance.manage, connections.manage, everyone, logs.manage, owner, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage</td></tr> </table>	Name	CON1 (Appliance)	Version	10.4.0.0.3346 (Rev 5ec2f8f4ce31)	Memory Usage	17668 KB (0.03% of 64428 MB)	CPU	1%	Running Since	2015-Jan-26 21:15:42	Uptime	1 hour 14 minutes 28 seconds	Current Time	2015-Jan-26 22:30:10	Name	admin	Groups	Administrators	Roles	appliance.manage, connections.manage, everyone, logs.manage, owner, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage
Name	CON1 (Concentrator)																																								
Version	10.4.0.0.3346 (Rev 5ec2f8f4ce31)																																								
Memory Usage	841 MB (1.31% of 64428 MB)																																								
CPU	1%																																								
Running Since	2015-Jan-26 21:15:51																																								
Uptime	1 hour 14 minutes 19 seconds																																								
Current Time	2015-Jan-26 22:30:10																																								
Name	admin																																								
Groups	Administrators																																								
Roles	concentrator.manage, connections.manage, database.manage, everyone, index.manage, logs.manage, owner, rules.manage, sdk.content, sdk.manage, sdk.meta, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage																																								
Name	CON1 (Appliance)																																								
Version	10.4.0.0.3346 (Rev 5ec2f8f4ce31)																																								
Memory Usage	17668 KB (0.03% of 64428 MB)																																								
CPU	1%																																								
Running Since	2015-Jan-26 21:15:42																																								
Uptime	1 hour 14 minutes 28 seconds																																								
Current Time	2015-Jan-26 22:30:10																																								
Name	admin																																								
Groups	Administrators																																								
Roles	appliance.manage, connections.manage, everyone, logs.manage, owner, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage																																								

*Ilustración 37. Información del Concentrator 1.*



The screenshot displays the configuration interface for the Concentrator. It is divided into several sections:

- Aggregate Services:** A table with columns for Address, Port, Rate, Max, Behind, Meta Fields, Filter, Meta Include, Grouped, and Status. One entry is visible: 172.18.32.136, 56002, 0, 0, 0, no, consuming.
- System Configuration:** A table with columns for Name and Config Value. Visible entries include:
 

Name	Config Value
Compression	0
Port	50005
SSL FIPS Mode	<input type="checkbox"/>
SSL Port	56005
Stat Update Interval	1000
Threads	20
- Aggregation Configuration:** A table with columns for Name and Config Value. It is divided into sub-sections:
  - Aggregation Settings:**

Aggregate Autostart	<input checked="" type="checkbox"/>
Aggregate Hours	0
Aggregate Interval	10
Aggregate Max Sessions	5000
  - Database Open Files:**

Meta Open Files	48
Session Open Files	48
  - Service Heartbeat:**

Heartbeat Error Restart	300
Heartbeat Next Attempt	60
Heartbeat No Response	180

Ilustración 38. Configuración del Concentrator 1.

CON1 - Concentrator

The screenshot displays the statistics interface for the Concentrator, organized into four main sections:

- Key Stats:** A table with columns for Key Stats, Rate, Max, Behind, and Status. One entry is visible: 172.18.32.136:56002, 0, 0, 0, consumr.
- Service System Info:**

CPU	6%
System Memory	1.7 GB
Total Memory	62.9 GB
Process Memory	841.6 MB
Max Process Memory	62.9 GB
Uptime	1 hour and 15 minutes
Status	Ready
Running Since	2015-Jan-26 21:15:51
Current Time	2015-Jan-26 22:31:34
- Appliance System Info:**

CPU	3%
System Memory	1.7 GB
Total Memory	62.9 GB
Process Memory	17.3 MB
Max Process Memory	62.9 GB
Memory	
Uptime	1 hour and 15 minutes
Status	Ready
Running Since	2015-Jan-26 21:15:42
- Physical Drives:** Four drive icons labeled sda, sdb, sdc, and sdd, each with a green checkmark indicating they are healthy.

Ilustración 39. Estadísticas del Concentrator 1.

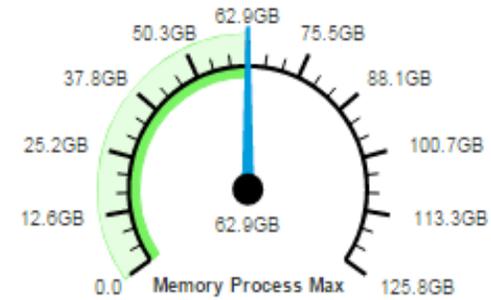
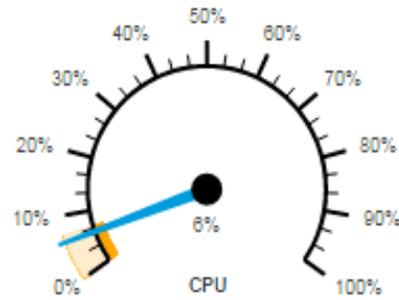
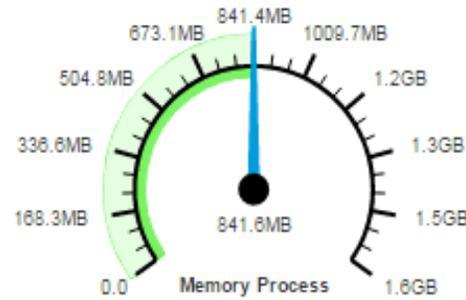


# Gauges - Page 1 of 1

Memory Process

CPU

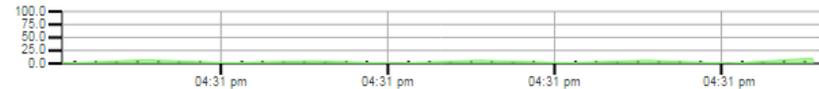
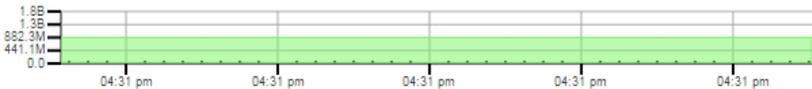
Memory Process Max



# Timeline Charts - Page 1 of 1

Memory Process

CPU



Memory Process Max

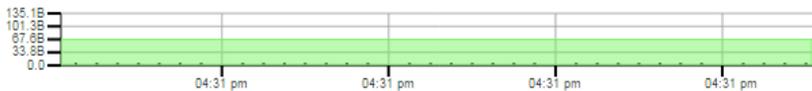


Ilustración 40. Estadísticas del Concentrador 1 de forma gráfica.



### License Information

Service ID	3-765-219-488
Product Licensed	smcConcentrator
Type	Permanent
Start Date	2014-12-29 18:00:00

Ilustración 41. Licencia del Concentrator 1.

## 3.2 Concentrator 2

Change Service | CON2 - Concentrator | System

Start Aggregation Stop Aggregation Appliance Tasks Shutdown Service Shutdown Appliance Service Reboot

<h4>Concentrator Service Information</h4> <table border="0"> <tr><td>Name</td><td>CON2 (Concentrator)</td></tr> <tr><td>Version</td><td>10.4.0.0.3346 (Rev 5ec2f8f4ce31)</td></tr> <tr><td>Memory Usage</td><td>843 MB (1.31% of 64428 MB)</td></tr> <tr><td>CPU</td><td>10%</td></tr> <tr><td>Running Since</td><td>2015-Jan-26 21:17:34</td></tr> <tr><td>Uptime</td><td>1 hour 15 minutes 5 seconds</td></tr> <tr><td>Current Time</td><td>2015-Jan-26 22:32:39</td></tr> </table> <h4>Concentrator User Information</h4> <table border="0"> <tr><td>Name</td><td>admin</td></tr> <tr><td>Groups</td><td>Administrators</td></tr> <tr><td>Roles</td><td>concentrator.manage, connections.manage, database.manage, everyone, index.manage, logs.manage, owner, rules.manage, sdk.content, sdk.manage, sdk.meta, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage</td></tr> </table>	Name	CON2 (Concentrator)	Version	10.4.0.0.3346 (Rev 5ec2f8f4ce31)	Memory Usage	843 MB (1.31% of 64428 MB)	CPU	10%	Running Since	2015-Jan-26 21:17:34	Uptime	1 hour 15 minutes 5 seconds	Current Time	2015-Jan-26 22:32:39	Name	admin	Groups	Administrators	Roles	concentrator.manage, connections.manage, database.manage, everyone, index.manage, logs.manage, owner, rules.manage, sdk.content, sdk.manage, sdk.meta, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage	<h4>Appliance Service Information</h4> <table border="0"> <tr><td>Name</td><td>CON2 (Appliance)</td></tr> <tr><td>Version</td><td>10.4.0.0.3346 (Rev 5ec2f8f4ce31)</td></tr> <tr><td>Memory Usage</td><td>17668 KB (0.03% of 64428 MB)</td></tr> <tr><td>CPU</td><td>10%</td></tr> <tr><td>Running Since</td><td>2015-Jan-26 21:17:25</td></tr> <tr><td>Uptime</td><td>1 hour 15 minutes 14 seconds</td></tr> <tr><td>Current Time</td><td>2015-Jan-26 22:32:39</td></tr> </table> <h4>Appliance User Information</h4> <table border="0"> <tr><td>Name</td><td>admin</td></tr> <tr><td>Groups</td><td>Administrators</td></tr> <tr><td>Roles</td><td>appliance.manage, connections.manage, everyone, logs.manage, owner, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage</td></tr> </table>	Name	CON2 (Appliance)	Version	10.4.0.0.3346 (Rev 5ec2f8f4ce31)	Memory Usage	17668 KB (0.03% of 64428 MB)	CPU	10%	Running Since	2015-Jan-26 21:17:25	Uptime	1 hour 15 minutes 14 seconds	Current Time	2015-Jan-26 22:32:39	Name	admin	Groups	Administrators	Roles	appliance.manage, connections.manage, everyone, logs.manage, owner, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage
Name	CON2 (Concentrator)																																								
Version	10.4.0.0.3346 (Rev 5ec2f8f4ce31)																																								
Memory Usage	843 MB (1.31% of 64428 MB)																																								
CPU	10%																																								
Running Since	2015-Jan-26 21:17:34																																								
Uptime	1 hour 15 minutes 5 seconds																																								
Current Time	2015-Jan-26 22:32:39																																								
Name	admin																																								
Groups	Administrators																																								
Roles	concentrator.manage, connections.manage, database.manage, everyone, index.manage, logs.manage, owner, rules.manage, sdk.content, sdk.manage, sdk.meta, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage																																								
Name	CON2 (Appliance)																																								
Version	10.4.0.0.3346 (Rev 5ec2f8f4ce31)																																								
Memory Usage	17668 KB (0.03% of 64428 MB)																																								
CPU	10%																																								
Running Since	2015-Jan-26 21:17:25																																								
Uptime	1 hour 15 minutes 14 seconds																																								
Current Time	2015-Jan-26 22:32:39																																								
Name	admin																																								
Groups	Administrators																																								
Roles	appliance.manage, connections.manage, everyone, logs.manage, owner, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage																																								

Ilustración 42. Información del Concentrator 2.



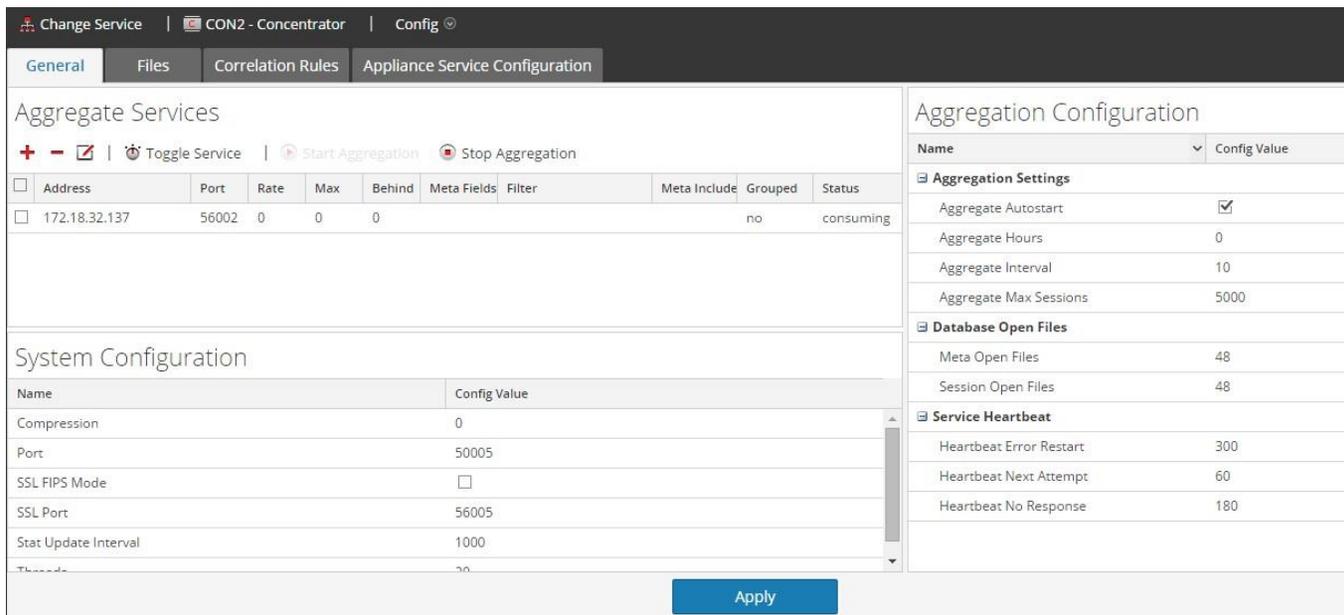


Ilustración 43. Configuración del Concentrator 2.

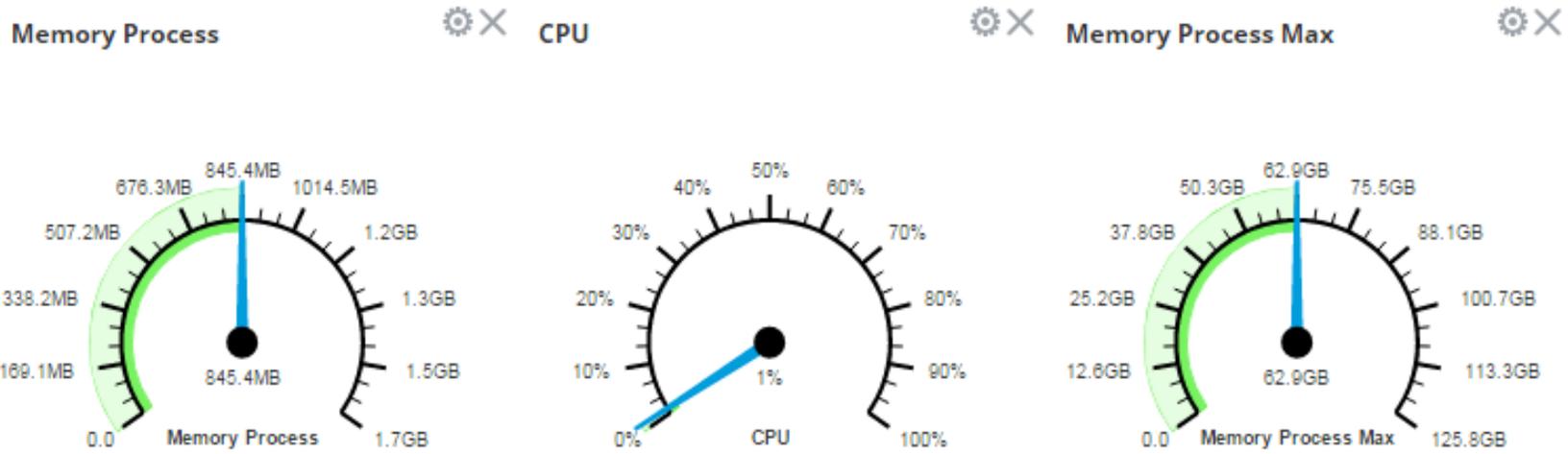
CON2 - Concentrator

Key Stats					Service System Info		Appliance System Info		Physical Drives			
Key Stats	Rate	Max	Behind	Status	CPU	System Memory	CPU	System Memory	Physical Drives			
172.18.32.137:56002	0	0	0	consum	0%	1.7 GB	1%	1.7 GB				
					Total Memory	62.9 GB	Total Memory	62.9 GB				
					Process Memory	845.4 MB	Process Memory	17.4 MB				
					Max Process Memory	62.9 GB	Max Process Memory	62.9 GB				
					Uptime	1 hour and 16 minutes	Uptime	1 hour and 16 minutes				
					Status	Ready	Status	Ready				
					Running Since	2015-Jan-26 21:17:34	Running Since	2015-Jan-26 21:17:25				
					Current Time	2015-Jan-26 22:34:10						

Ilustración 44. Estadísticas del Concentrator 2.



# Gauges - Page 1 of 1



45

# Timeline Charts - Page 1 of 1

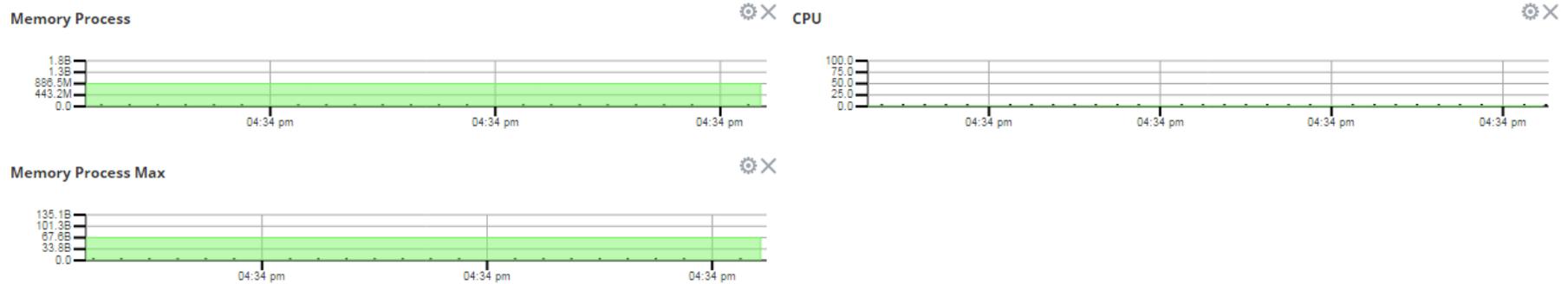


Ilustración 45. Estadísticas del Concentrator 2 de forma gráfica.



## License Information

Service ID	2-364-796-144
Product	smcConcentrator
Licensed	
Type	Permanent
Start Date	2014-12-29 18:00:00

Ilustración 46. Licencia del Concentrator 2.

### 3.3 Log Decoder 1

The screenshot shows a web interface for the Log Decoder 1 service. At the top, there is a navigation bar with 'Change Service', 'LOGDEC1 - Log Decoder', and 'System'. Below the navigation bar are several action buttons: 'Upload Log File', 'Stop Capture', 'Reset Log Stats', 'Appliance Tasks', 'Shutdown Service', 'Shutdown Appliance Service', and 'Reboot'. The main content is divided into four sections: 'Log Decoder Service Information', 'Appliance Service Information', 'Log Decoder User Information', and 'Appliance User Information'. Each section contains a table of key metrics and details.

Log Decoder Service Information		Appliance Service Information	
Name	LOGDEC1 (Log Decoder)	Name	LOGDEC1 (Appliance)
Version	10.4.0.0.3346 (Rev 5ec2f8f4ce31)	Version	10.4.0.0.3346 (Rev 5ec2f8f4ce31)
Memory Usage	2181 MB (3.38% of 64428 MB)	Memory Usage	18288 KB (0.03% of 64428 MB)
CPU	11%	CPU	3%
Running Since	2015-Jan-26 21:16:11	Running Since	2015-Jan-26 21:16:06
Uptime	1 hour 20 minutes 51 seconds	Uptime	1 hour 20 minutes 55 seconds
Current Time	2015-Jan-26 22:37:02	Current Time	2015-Jan-26 22:37:01

Log Decoder User Information		Appliance User Information	
Name	admin	Name	admin
Groups	Administrators	Groups	Administrators
Roles	connections.manage, database.manage, decoder.manage, everyone, index.manage, logs.manage, owner, parsers.manage, rules.manage, sdk.content, sdk.manage, sdk.meta, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage	Roles	appliance.manage, connections.manage, everyone, logs.manage, owner, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage

Ilustración 47. Información del Log Decoder 1.



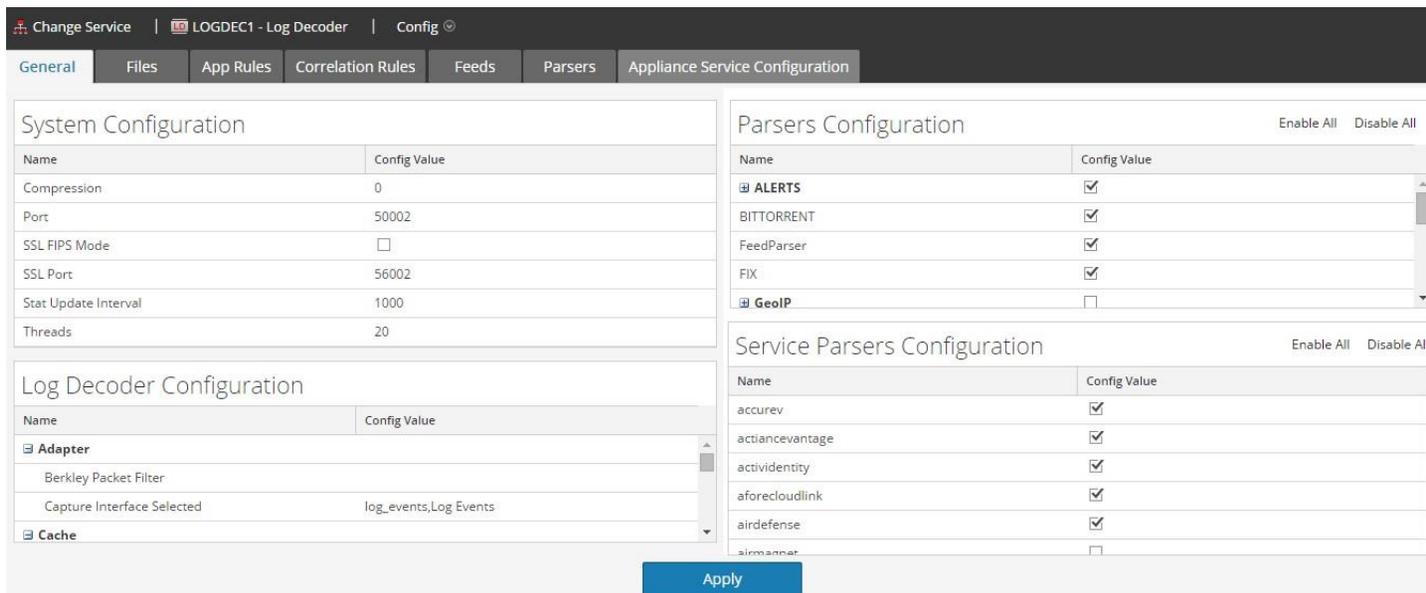


Ilustración 48. Configuración del Log Decoder 1.

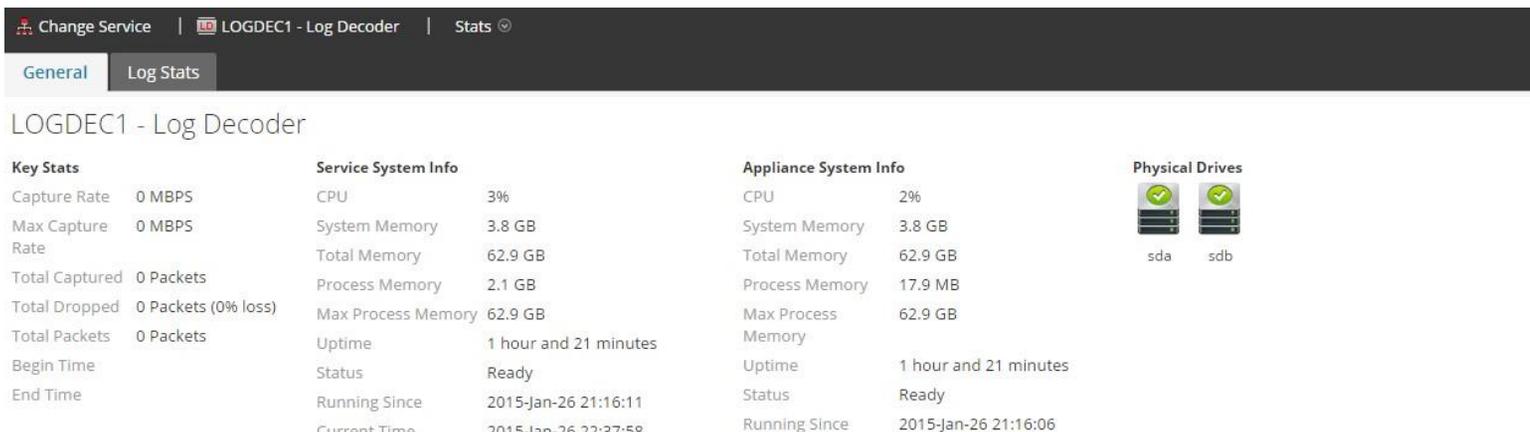


Ilustración 49. Estadísticas del Log Decoder 1.

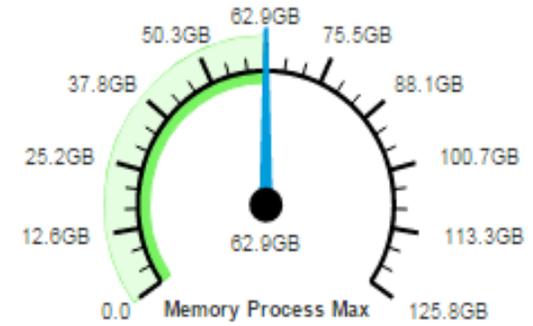
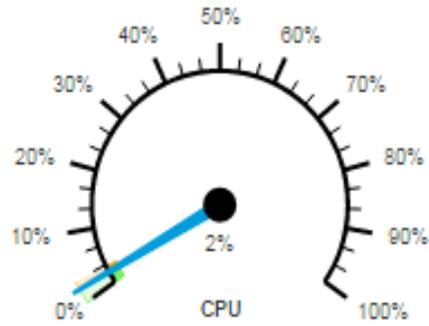
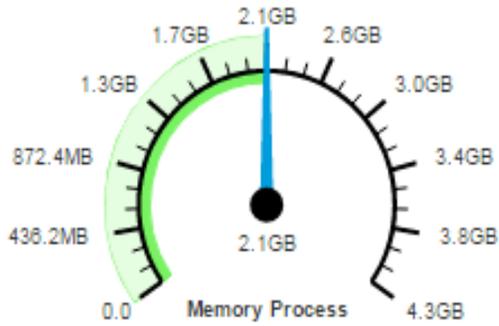


# Gauges - Page 1 of 1

Memory Process

CPU

Memory Process Max



48

# Timeline Charts - Page 1 of 1

Memory Process

CPU



Memory Process Max

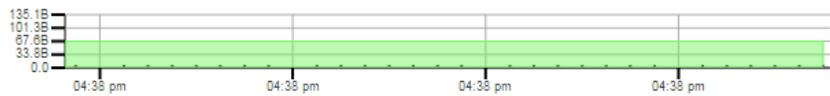


Ilustración 50. Estadísticas del Log Decoder 1 de forma gráfica.



### License Information

Service ID	883-306-912
Product Licensed	smcLogDecoder
Type	Permanent
Start Date	2014-12-29 18:00:00

Ilustración 51. Licencia del Log Decoder 1.

## 3.4 Log Collector 1.

### Log Collector Service Information

Name	LOGDEC1 (Log Collector)
Version	10.4.0.0.13590 (Rev 2af46257ba11)
Memory Usage	529 MB (0.82% of 64428 MB)
CPU	1%
Running Since	2015-Jan-26 21:16:47
Uptime	1 hour 19 minutes 21 seconds
Current Time	2015-Jan-26 22:36:08

### Log Collector User Information

Name	admin
Groups	Administrators
Roles	connections.manage, everyone, logcollection.manage, logs.manage, owner, sdk.content, sdk.manage, sdk.meta, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage

### Appliance Service Information

Name	LOGDEC1 (Appliance)
Version	10.4.0.0.3346 (Rev 5ec2f8f4ce31)
Memory Usage	18288 KB (0.03% of 64428 MB)
CPU	2%
Running Since	2015-Jan-26 21:16:06
Uptime	1 hour 20 minutes 3 seconds
Current Time	2015-Jan-26 22:36:09

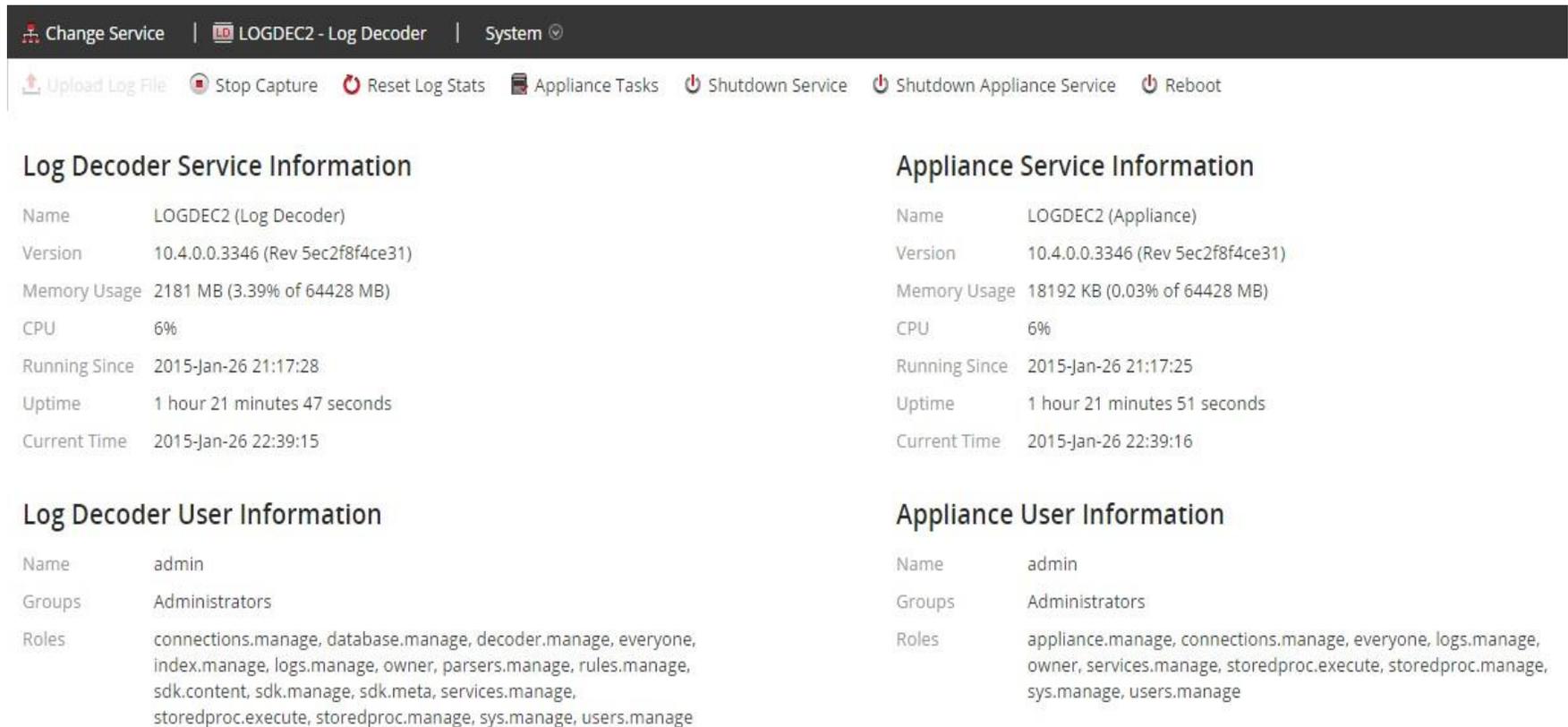
### Appliance User Information

Name	admin
Groups	Administrators
Roles	appliance.manage, connections.manage, everyone, logs.manage, owner, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage

Ilustración 52. Información del Log Collector 1.



## 3.5 Log Decoder 2



**Change Service** | **LOGDEC2 - Log Decoder** | **System** ▾

[Upload Log File](#)
[Stop Capture](#)
[Reset Log Stats](#)
[Appliance Tasks](#)
[Shutdown Service](#)
[Shutdown Appliance Service](#)
[Reboot](#)

### Log Decoder Service Information

Name	LOGDEC2 (Log Decoder)
Version	10.4.0.0.3346 (Rev 5ec2f8f4ce31)
Memory Usage	2181 MB (3.39% of 64428 MB)
CPU	6%
Running Since	2015-Jan-26 21:17:28
Uptime	1 hour 21 minutes 47 seconds
Current Time	2015-Jan-26 22:39:15

### Appliance Service Information

Name	LOGDEC2 (Appliance)
Version	10.4.0.0.3346 (Rev 5ec2f8f4ce31)
Memory Usage	18192 KB (0.03% of 64428 MB)
CPU	6%
Running Since	2015-Jan-26 21:17:25
Uptime	1 hour 21 minutes 51 seconds
Current Time	2015-Jan-26 22:39:16

### Log Decoder User Information

Name	admin
Groups	Administrators
Roles	connections.manage, database.manage, decoder.manage, everyone, index.manage, logs.manage, owner, parsers.manage, rules.manage, sdk.content, sdk.manage, sdk.meta, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage

### Appliance User Information

Name	admin
Groups	Administrators
Roles	appliance.manage, connections.manage, everyone, logs.manage, owner, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage

Ilustración 53. Información del Log Decoder 2.



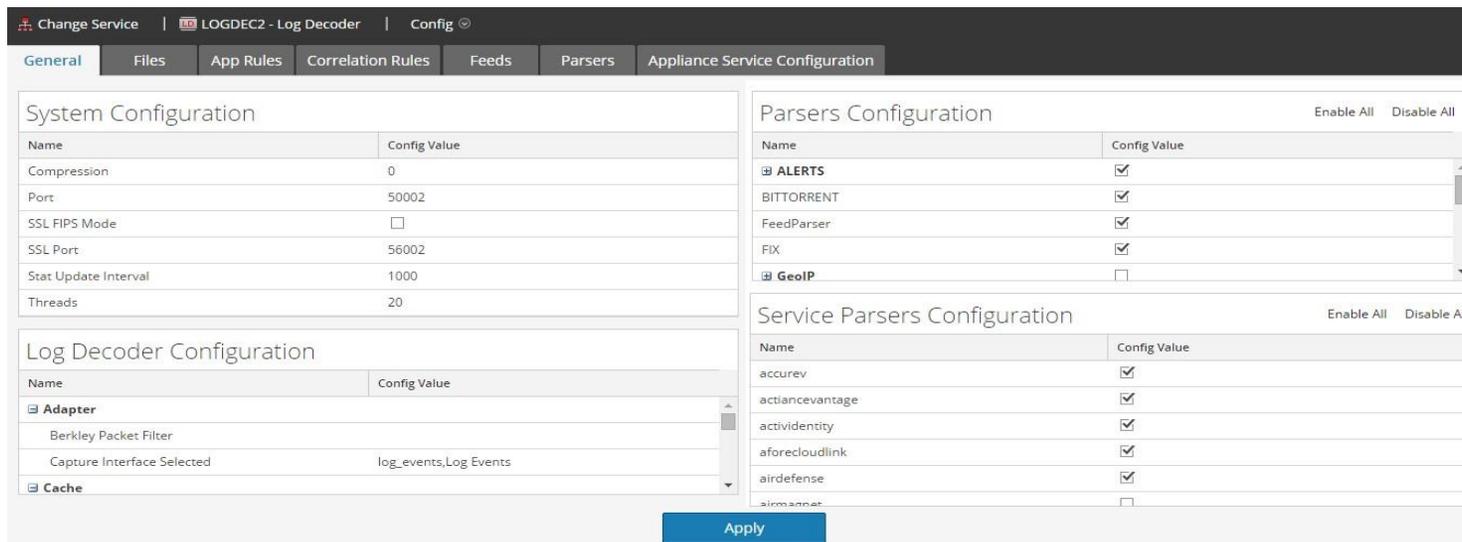


Ilustración 54. Configuración del Log Decoder 2.

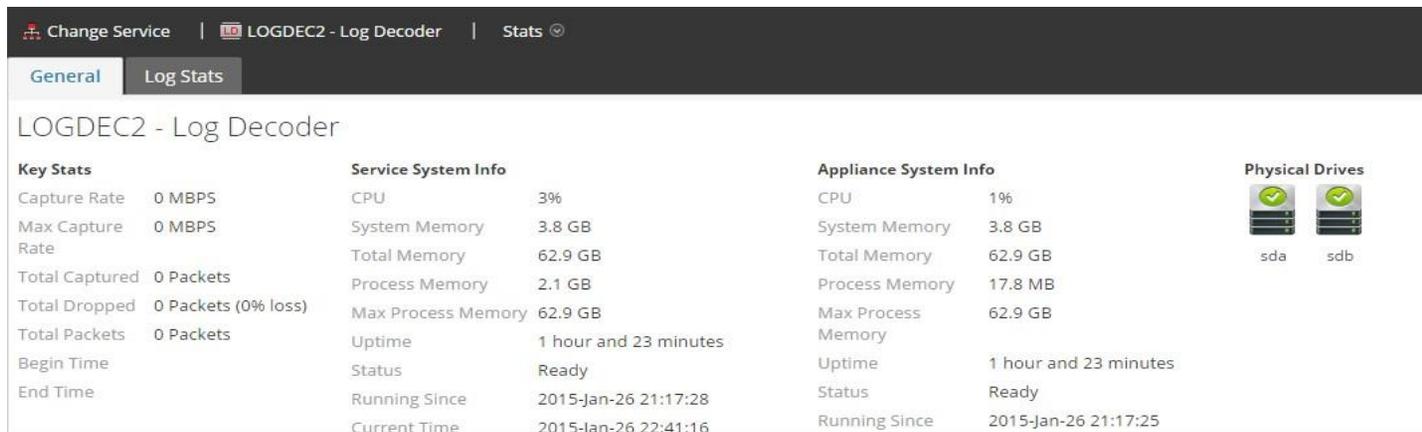
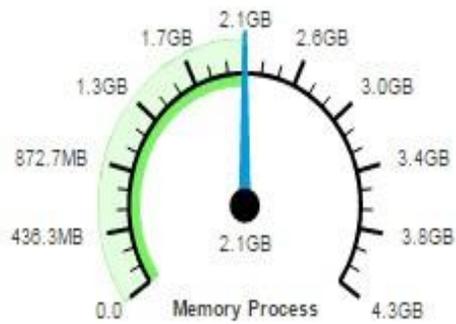


Ilustración 55. Estadísticas del Log Decoder 2.

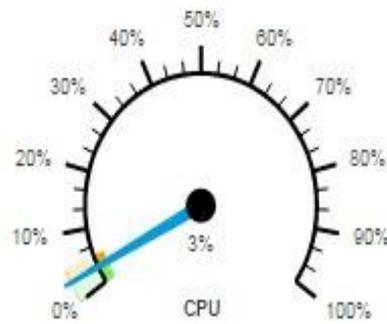


# Gauges - Page 1 of 1

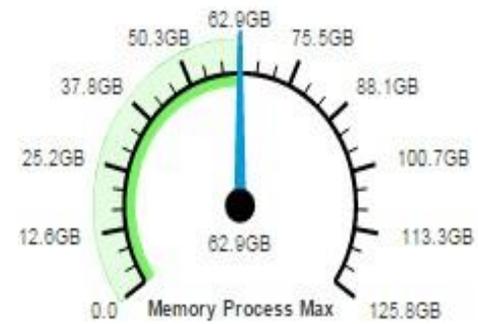
Memory Process



CPU

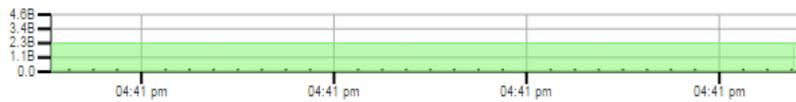


Memory Process Max

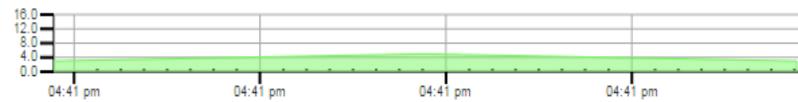


# Timeline Charts - Page 1 of 1

Memory Process



CPU



Memory Process Max

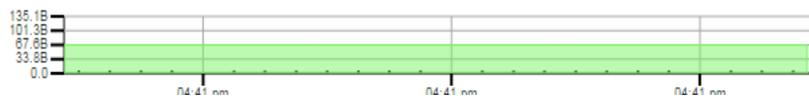


Ilustración 56. Estadísticas del Log Decoder 2 de forma gráfica.



## License Information

Service ID	3-232-556-032
Product Licensed	smcLogDecoder
Type	Permanent
Start Date	2014-12-29 18:00:00

Ilustración 57. Licencia del Log Decoder 2.

## 3.6 Log Collector 2

Change Service | LOGDEC2 - Log Collector | System

Collection | Appliance Tasks | Shutdown Service | Shutdown Appliance Service | Reboot

### Log Collector Service Information

Name	LOGDEC2 (Log Collector)
Version	10.4.0.0.13590 (Rev 2af46257ba11)
Memory Usage	523 MB (0.81% of 64428 MB)
CPU	2%
Running Since	2015-Jan-26 21:18:06
Uptime	1 hour 20 minutes 43 seconds
Current Time	2015-Jan-26 22:38:49

### Log Collector User Information

Name	admin
Groups	Administrators
Roles	connections.manage, everyone, logcollection.manage, logs.manage, owner, sdk.content, sdk.manage, sdk.meta, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage

### Appliance Service Information

Name	LOGDEC2 (Appliance)
Version	10.4.0.0.3346 (Rev 5ec2f8f4ce31)
Memory Usage	18192 KB (0.03% of 64428 MB)
CPU	2%
Running Since	2015-Jan-26 21:17:25
Uptime	1 hour 21 minutes 24 seconds
Current Time	2015-Jan-26 22:38:49

### Appliance User Information

Name	admin
Groups	Administrators
Roles	appliance.manage, connections.manage, everyone, logs.manage, owner, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage

Ilustración 58. Información del Log Collector 2.



### 3.7 Event Stream Analysis 1

#### Service Information

Host Name	ESA1
Home Directory	/opt/rsa/esa
Service Id	a1560250-4bcb-41b4-80d3-cd1082018573
Up Time	2 hours 45 minutes 12 seconds
Process Cpu	0%
Process Memory	343 MB (4.19% of 8192 MB)
System Cpu	3%
System Memory	2254 MB (2.33% of 96746 MB)
Build	10.4.0.0.1421
Current Time	Mon Jan 26 2015 16:34:49 GMT-0600 (Hora estándar central (México))

#### License Information

Service ID	525-207-040
Product Licensed	smcEventStreamAnalysis
Type	Permanent
Start Date	2014-12-29 18:00:00

Ilustración 59. Estadísticas del ESA 1.



## Service Information

Host Name	ESA2
Home Directory	/opt/rsa/esa
Service Id	e7d441e8-2f77-41c7-ac04-57e7983c3f21
Up Time	2 hours 44 minutes 48 seconds
Process Cpu	0%
Process Memory	333 MB (4.07% of 8192 MB)
System Cpu	0%
System Memory	2232 MB (2.31% of 96746 MB)
Build	10.4.0.0.1421
Current Time	Mon Jan 26 2015 16:35:15 GMT-0600 (Hora estándar central (México))

## License Information

Service ID	2-168-385-728
Product Licensed	smcEventStreamAnalysis
Type	Permanent
Start Date	2014-12-29 18:00:00

*Ilustración 60. Estadísticas del ESA.*



### 3.8 Fuentes integradas

La siguiente tabla muestra las fuentes integradas al Security Analytics:

EQUIPO	VERSIÓN	IP	MÉTODO DE COLECCIÓN	PARSER NAME
<b>Fortigate 600C</b>	v5.0,build0271 (GA Patch 6)	172.31.45.253	Syslog	fortinet
<b>Fortigate 300C</b>	v5.0,build0271 (GA Patch 6)	172.31.45.246	Syslog	fortinet
<b>FortiMail 400C</b>	v5.1,build281, 140610 (5.1.3 GA)	172.31.45.244	Syslog	fortinetfortimail
<b>FortiMail 400C</b>	v5.1,build281, 140610 (5.1.3 GA)	172.31.45.245	Syslog	fortinetfortimail
<b>Windows server 2012</b>	Exchange 2013	192.168.105.41	File, Windows	msexchange
<b>Windows server 2012</b>	Exchange 2013	192.168.105.42	File, Windows	msexchange
<b>Windows server 2012</b>	Active Directory 2012	192.168.105.50	File, Windows	msexchange
<b>Windows server 2012</b>	Active Directory 2012	192.168.105.60	File, Windows	msexchange
<b>ARBOR APS2100</b>	Pravail APS v5.5.1	192.168.80.162		Syslog
<b>ARBOR APS2100</b>	Pravail APS v5.5.1	192.168.80.163		Syslog
<b>ARBOR APS2100</b>	Pravail APS v5.5.1	192.168.80.164		Syslog

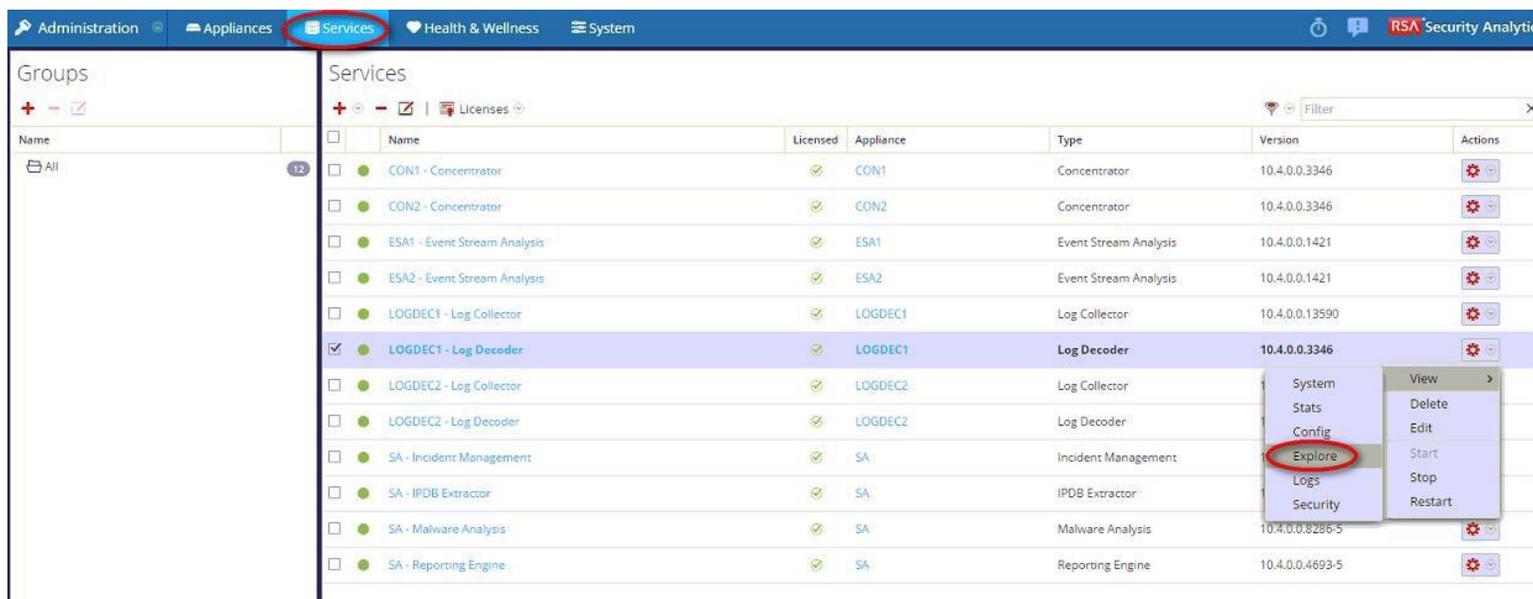
Tabla 3. Fuentes a monitorear.



### 3.9 Reenvío de logs a Fuente Externa

Para el reenvío de mensajes de syslog hay que tomar en cuenta que estos se envían después de ser parseados y antes de escribirse en el Log Decoder. Para configurar el reenvío de todos los mensajes de syslog que recibe el Log Decoder para enviarse a una fuente externa de almacenamiento se deben seguir los siguientes pasos:

1. Debemos configurar la regla de aplicación (application rule) en el Log Decoder para que tome como referencia todos los mensajes de syslog y permita al Security Analytics mandar dichos mensajes a la ubicación deseada.
  - a. Ir a Administration > Services > Seleccionar el Log Decoder > View > Explore



The screenshot shows the RSA Security Analytics Administration console. The top navigation bar includes 'Administration', 'Appliances', 'Services' (highlighted), 'Health & Wellness', and 'System'. The main content area is divided into 'Groups' and 'Services'. The 'Services' section contains a table with the following data:

Name	Licensed	Appliance	Type	Version	Actions
CON1 - Concentrator	✓	CON1	Concentrator	10.4.0.0.3346	[Gear]
CON2 - Concentrator	✓	CON2	Concentrator	10.4.0.0.3346	[Gear]
ESA1 - Event Stream Analysis	✓	ESA1	Event Stream Analysis	10.4.0.0.1421	[Gear]
ESA2 - Event Stream Analysis	✓	ESA2	Event Stream Analysis	10.4.0.0.1421	[Gear]
LOGDEC1 - Log Collector	✓	LOGDEC1	Log Collector	10.4.0.0.13590	[Gear]
<b>LOGDEC1 - Log Decoder</b>	✓	<b>LOGDEC1</b>	<b>Log Decoder</b>	<b>10.4.0.0.3346</b>	[Gear]
LOGDEC2 - Log Collector	✓	LOGDEC2	Log Collector		[Gear]
LOGDEC2 - Log Decoder	✓	LOGDEC2	Log Decoder		[Gear]
SA - Incident Management	✓	SA	Incident Management		[Gear]
SA - IPDB Extractor	✓	SA	IPDB Extractor		[Gear]
SA - Malware Analysis	✓	SA	Malware Analysis	10.4.0.0.8286-5	[Gear]
SA - Reporting Engine	✓	SA	Reporting Engine	10.4.0.0.4693-5	[Gear]

The context menu for the selected 'LOGDEC1 - Log Decoder' service includes the following options: System, Stats, Config, **Explore** (highlighted), Logs, Security, View, Delete, Edit, Start, Stop, and Restart.

Ilustración 61. Pantalla de servicios.



- b. Ya en la vista de Explore, en la ventana del lado izquierdo ir a: Decoder/config/rules/application y dar clic derecho en application y seleccionar 'Properties'

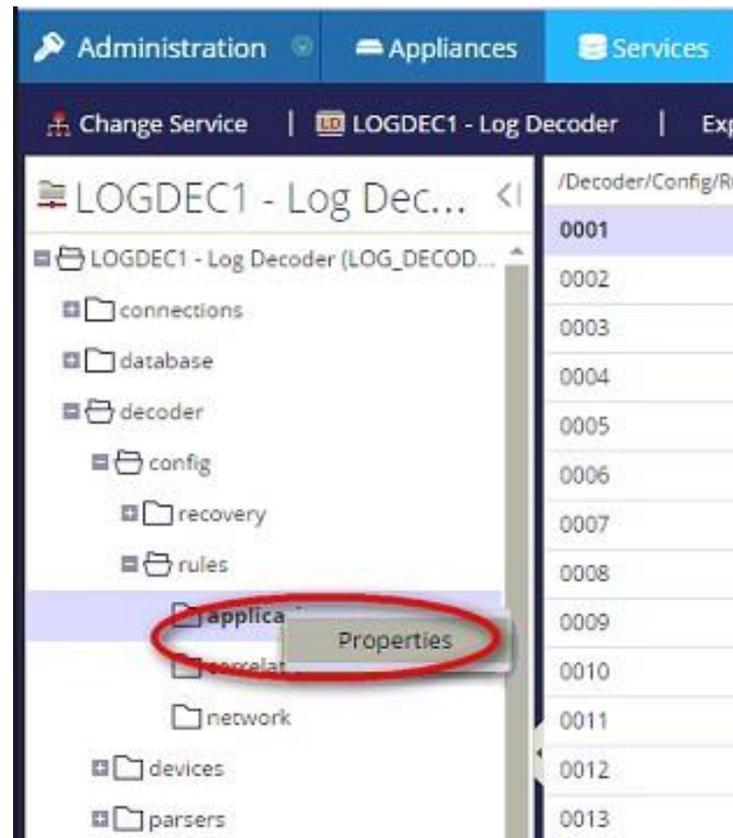
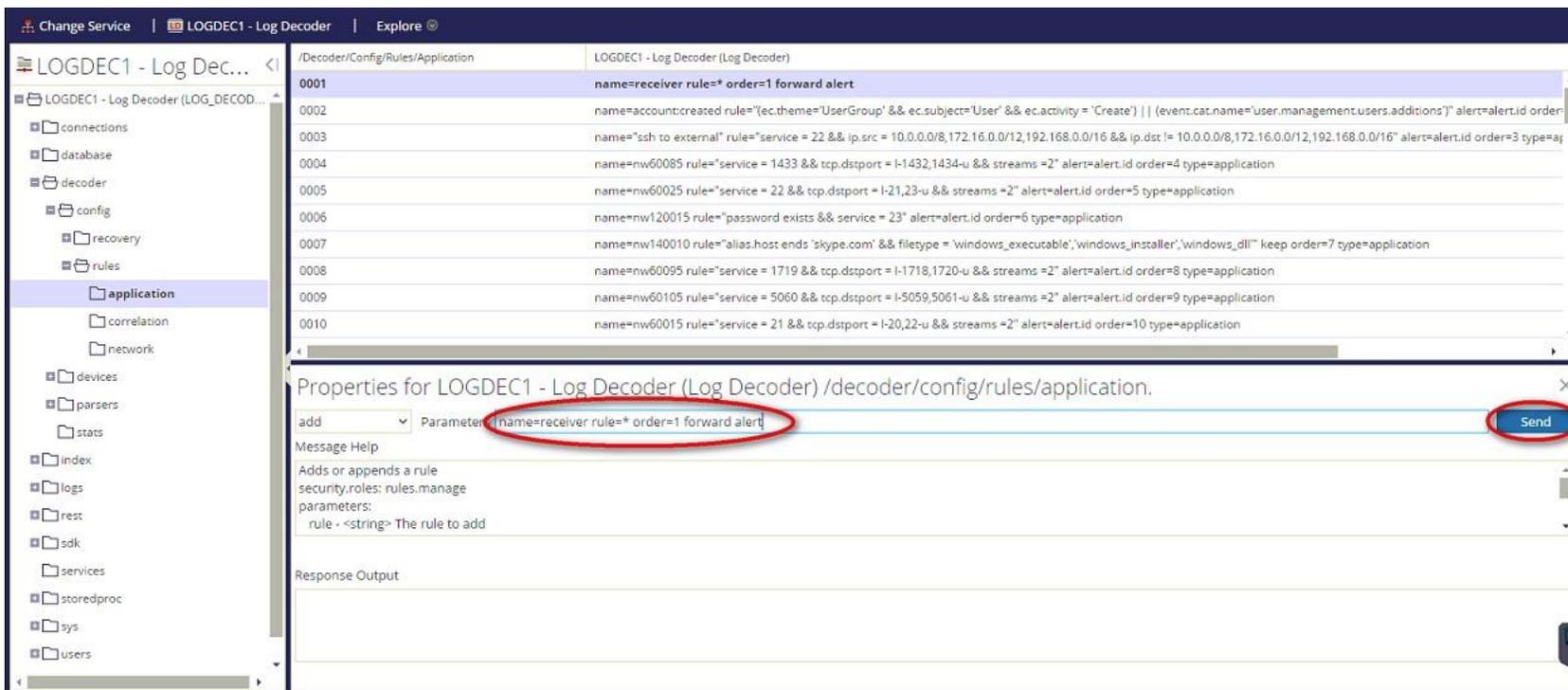


Ilustración 62. Pantalla de Exploración del Log Decoder.



- c. Al dar clic en propiedades escribir la siguiente regla `rule=<query> name=<name>`, en nuestro caso necesitamos enviar todos los logs por lo cual nuestra regla queda de la siguiente manera: `name=receiver rule=* order=1 forward alert` y damos clic en send.



The screenshot displays the LOGDEC1 - Log Decoder configuration interface. The main window shows a list of rules under the path `/Decoder/Config/Rules/Application`. The rules are listed as follows:

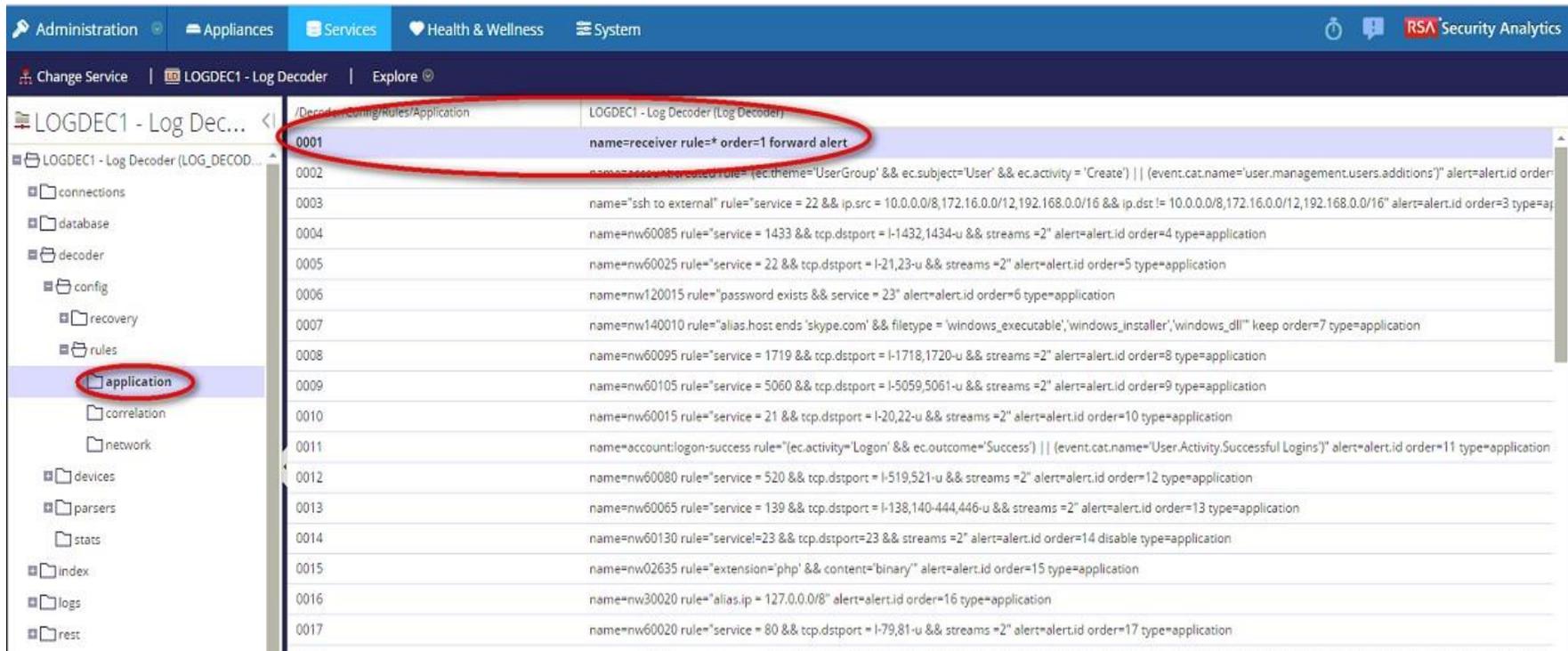
ID	Rule Name
0001	<code>name=receiver rule=* order=1 forward alert</code>
0002	<code>name=account.created rule="(ec.theme='UserGroup' &amp;&amp; ec.subject='User' &amp;&amp; ec.activity = 'Create')   (event.cat.name='user.management.users.additions')" alert=alert.id order=</code>
0003	<code>name="ssh to external" rule="service = 22 &amp;&amp; ip.src = 10.0.0.0/8,172.16.0.0/12,192.168.0.0/16 &amp;&amp; ip.dst != 10.0.0.0/8,172.16.0.0/12,192.168.0.0/16" alert=alert.id order=3 type=ap</code>
0004	<code>name=nw60085 rule="service = 1433 &amp;&amp; tcp.dstport = 1-1432,1434-u &amp;&amp; streams =2" alert=alert.id order=4 type=application</code>
0005	<code>name=nw60025 rule="service = 22 &amp;&amp; tcp.dstport = 1-21,23-u &amp;&amp; streams =2" alert=alert.id order=5 type=application</code>
0006	<code>name=nw120015 rule="password exists &amp;&amp; service = 23" alert=alert.id order=6 type=application</code>
0007	<code>name=nw140010 rule="alias.host.ends 'skype.com' &amp;&amp; filetype = 'windows_executable','windows_installer','windows_dll'" keep order=7 type=application</code>
0008	<code>name=nw60095 rule="service = 1719 &amp;&amp; tcp.dstport = 1-1718,1720-u &amp;&amp; streams =2" alert=alert.id order=8 type=application</code>
0009	<code>name=nw60105 rule="service = 5060 &amp;&amp; tcp.dstport = 1-5059,5061-u &amp;&amp; streams =2" alert=alert.id order=9 type=application</code>
0010	<code>name=nw60015 rule="service = 21 &amp;&amp; tcp.dstport = 1-20,22-u &amp;&amp; streams =2" alert=alert.id order=10 type=application</code>

A dialog box titled "Properties for LOGDEC1 - Log Decoder (Log Decoder) /decoder/config/rules/application." is open, showing the "add" dropdown menu set to "Parameter" and the text input field containing the rule `name=receiver rule=* order=1 forward alert`. A red circle highlights the "Send" button in the dialog box.

Ilustración 63. Configuración de la regla de aplicación.



d. Una vez configurada la alerta nos aseguramos que este hasta arriba de las demás reglas y con los parámetros que la configuramos.



ID	Rule Name
0001	name=receiver rule=* order=1 forward alert
0002	name=account_created rule=(ec.theme='UserGroup' && ec.subject='User' && ec.activity='Create')    (event.cat.name='user.management.users.additions') alert=alert.id order=2 type=application
0003	name='ssh to external' rule='service = 22 && ip.src = 10.0.0.0/8,172.16.0.0/12,192.168.0.0/16 && ip.dst != 10.0.0.0/8,172.16.0.0/12,192.168.0.0/16' alert=alert.id order=3 type=application
0004	name=nw60085 rule='service = 1433 && tcp.dstport = 1-1432,1434-u && streams =2' alert=alert.id order=4 type=application
0005	name=nw60025 rule='service = 22 && tcp.dstport = 1-21,23-u && streams =2' alert=alert.id order=5 type=application
0006	name=nw120015 rule='password exists && service = 23' alert=alert.id order=6 type=application
0007	name=nw140010 rule='alias.host ends 'skype.com' && filetype = 'windows_executable','windows_installer','windows_dll' keep order=7 type=application
0008	name=nw60095 rule='service = 1719 && tcp.dstport = 1-1718,1720-u && streams =2' alert=alert.id order=8 type=application
0009	name=nw60105 rule='service = 5060 && tcp.dstport = 1-5059,5061-u && streams =2' alert=alert.id order=9 type=application
0010	name=nw60015 rule='service = 21 && tcp.dstport = 1-20,22-u && streams =2' alert=alert.id order=10 type=application
0011	name=account:logon-success rule='(ec.activity='Logon' && ec.outcome='Success')    (event.cat.name='User.Activity.Successful Logins') alert=alert.id order=11 type=application
0012	name=nw60080 rule='service = 520 && tcp.dstport = 1-519,521-u && streams =2' alert=alert.id order=12 type=application
0013	name=nw60065 rule='service = 139 && tcp.dstport = 1-138,140-444,446-u && streams =2' alert=alert.id order=13 type=application
0014	name=nw60130 rule='service!=23 && tcp.dstport=23 && streams =2' alert=alert.id order=14 disable type=application
0015	name=nw02635 rule='extension='php' && content='binary' alert=alert.id order=15 type=application
0016	name=nw30020 rule='alias.ip = 127.0.0.0/8' alert=alert.id order=16 type=application
0017	name=nw60020 rule='service = 80 && tcp.dstport = 1-79,81-u && streams =2' alert=alert.id order=17 type=application

60

Ilustración 64. Reglas de aplicación existentes.



2. A continuación debemos de configurar el destino al cual se enviarán los mensajes de syslog y habilitarlo; este proceso se lleva a cabo en el parámetro: **decoder/config/logs.forwarding.destination**
  - a. En este parámetro le diremos cual es nuestro servidor syslog a utilizar:
    - i. TLS Connections: receiver1=tls:receiver1.netwitness.local:6514
    - ii. UDP Connections: receiver1=udp:receiver1.netwitness.local:514
    - iii. TCP Connections: receiver1=tcp:receiver1.netwitness.local:514
  - b. Para fines de la empresa utilizamos: **receiver= tcp:172.18.32.129:514**
  - c. En el parámetro de logs.forward.enable le cambiamos el valor a **“yes”**

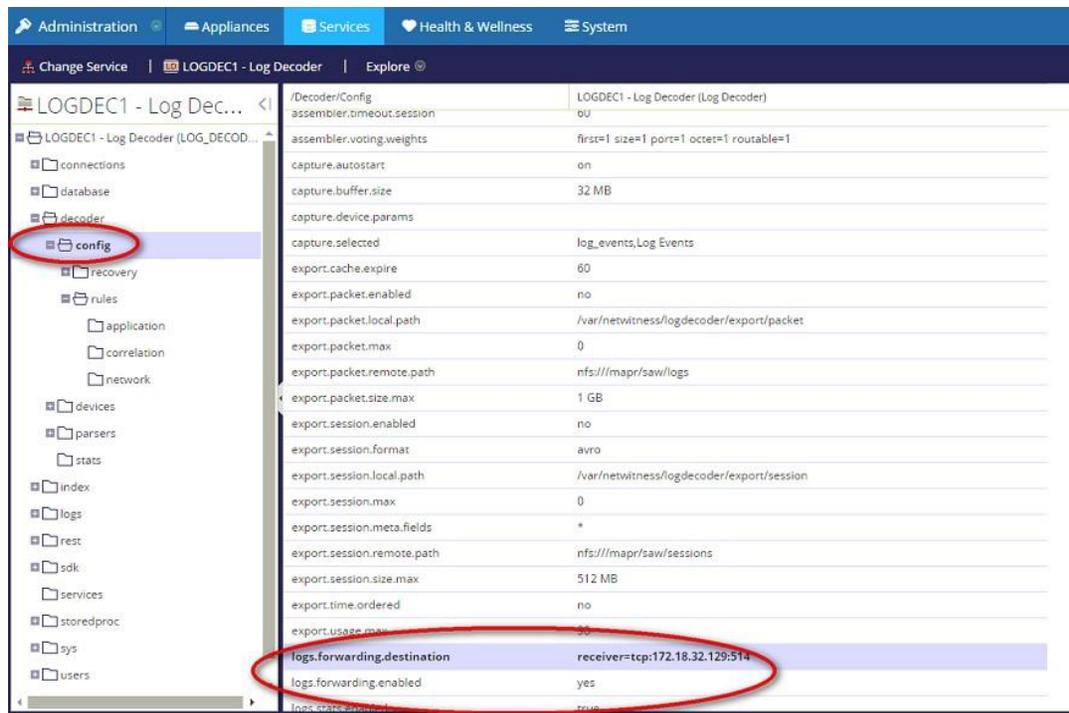
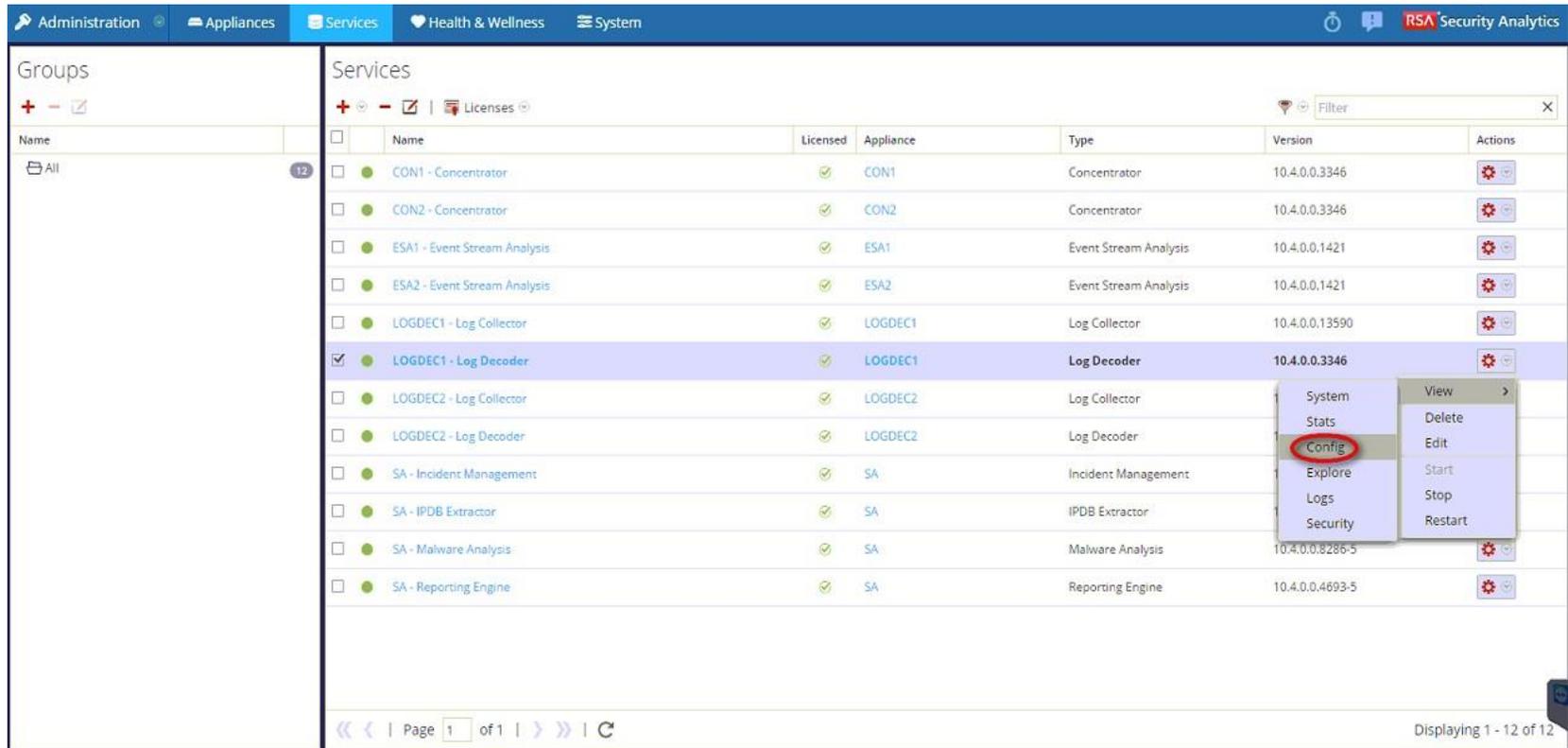


Ilustración 65. Sección de configuración del Log Decoder.



3. Por último debemos de revisar en Administration > Services > LogDecoder > View > Config

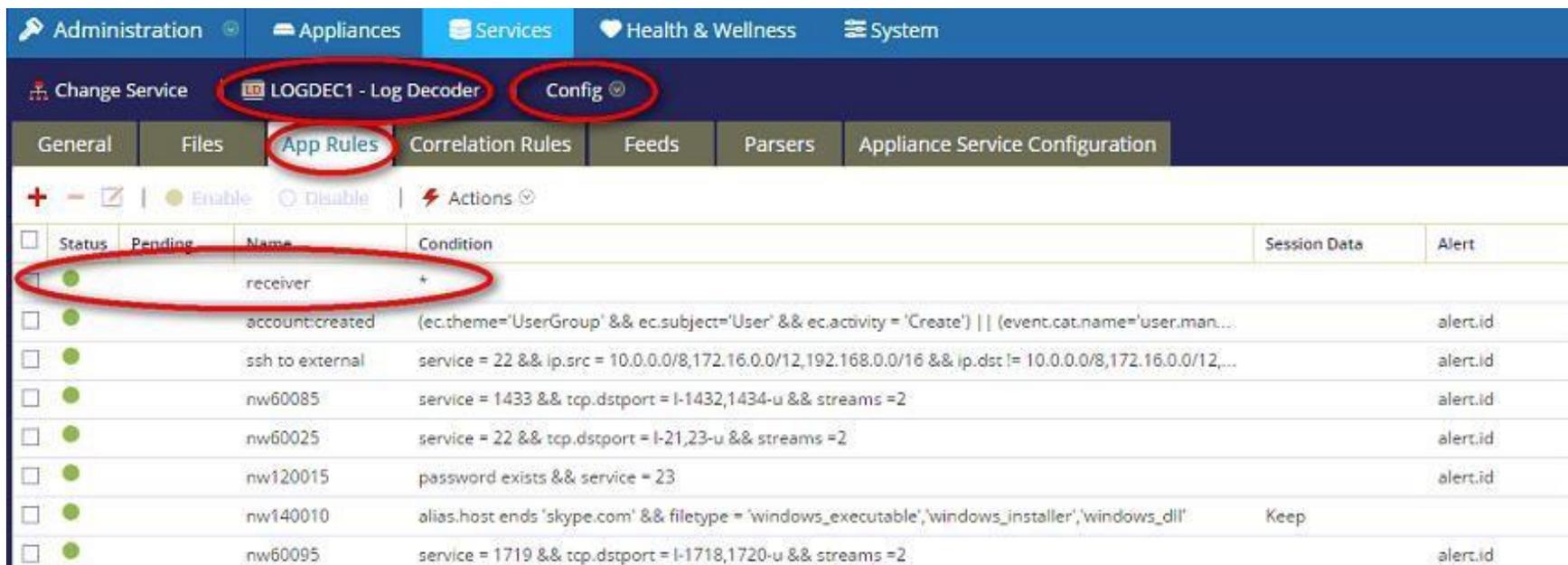


62

Ilustración 66. Pantalla de Servicios.



- a. En la pestaña de App Rules revisar que la regla se encuentre configurada, habilitada y hasta arriba de las demás reglas



The screenshot shows the configuration interface for the Log Decoder service. The 'App Rules' tab is selected, and the 'receiver' rule is highlighted. The table below shows the list of rules:

Status	Pending	Name	Condition	Session Data	Alert
<input checked="" type="checkbox"/>		receiver	+		
<input type="checkbox"/>		account:created	(ec.theme='UserGroup' && ec.subject='User' && ec.activity = 'Create')    (event.cat.name='user.man...		alert.id
<input type="checkbox"/>		ssh to external	service = 22 && ip.src = 10.0.0.0/8,172.16.0.0/12,192.168.0.0/16 && ip.dst != 10.0.0.0/8,172.16.0.0/12,...		alert.id
<input type="checkbox"/>		nw60085	service = 1433 && tcp.dstport = !-1432,1434-u && streams = 2		alert.id
<input type="checkbox"/>		nw60025	service = 22 && tcp.dstport = !-21,23-u && streams = 2		alert.id
<input type="checkbox"/>		nw120015	password exists && service = 23		alert.id
<input type="checkbox"/>		nw140010	alias.host ends 'skype.com' && filetype = 'windows_executable','windows_installer','windows_dll'	Keep	
<input type="checkbox"/>		nw60095	service = 1719 && tcp.dstport = !-1718,1720-u && streams = 2		alert.id

Ilustración 67. Pantalla de Configuración del Log Decoder.

Una vez hecho esto, revisar en nuestra fuente de almacenamiento externo que esté recibiendo los logs de forma exitosa.



### 3.10 Custom Feeds

El archivo de datos de alimentación (.csv) y, opcionalmente, el archivo de definición de alimentación (.xml) debe estar disponible en el sistema de archivos local para una alimentación personalizada bajo demanda

Para crear un campo customizado:

1. En la GUI de Security Analytics ir a **Live > Feeds**.

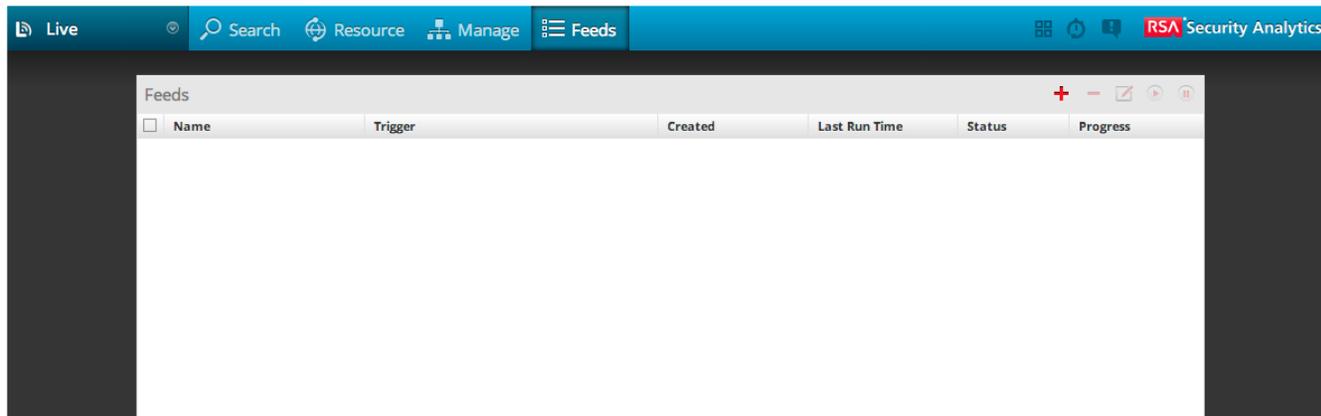


Ilustración 68. Feeds que se tienen actualmente.

En la barra de herramientas dar clic en el signo de “+”

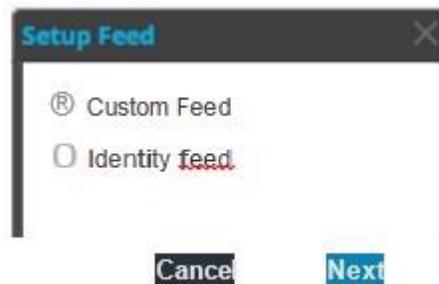


Ilustración 69. Pantalla para escoger el tipo de feed a crear.



2. Seleccionar "Custom Feed" y damos clic en Next lo que nos abrirá la pantalla de configuración de un feed customizable.

**Configure a Custom Feed**

Define Feed | Select Devices | Define Columns | Review

Feed Task Type  Adhoc  Recurring

Name \*

File \*

Advanced Options

Ilustración 70. Pantalla de configuración de feeds.



3. Seleccionamos "Adhoc" y tenemos dos opciones:
  - a. Para un archivo .csv escribimos el nombre y seleccionamos el archivo que usaremos.
  - b. Para un archivo .xml debemos seleccionar Opciones Avanzadas (Advanced Options)

The screenshot shows a window titled "Configure a Custom Feed" with a close button (X) in the top right corner. The window has four tabs: "Define Feed" (selected), "Select Devices", "Define Columns", and "Review".

Under the "Define Feed" tab, there are the following fields and controls:

- Feed Task Type:** Two radio buttons, "Adhoc" (selected) and "Recurring".
- Name \*:** A text input field.
- File \*:** A text input field with "Select File" and a "Browse" button.
- Advanced Options:** A section with a collapse/expand arrow (currently expanded). It contains:
  - XML Feed File:** A text input field with "Select File" and a "Browse" button.
  - Separator:** A text input field containing a comma (,).
  - Comment:** A text input field containing a hash symbol (#).

At the bottom of the window, there are four buttons: "Reset", "Cancel", "Prev", and "Next".

Ilustración 71. Pantalla de configuración de feeds con las opciones avanzadas habilitadas.



- Hay que seleccionar el archivo, cual es el separador y que signo será el usado para comentarios (que por default es #) y le damos siguiente.
- En la siguiente ventana escogemos el o los decoders en los cuales queremos anexar el "custom feed"

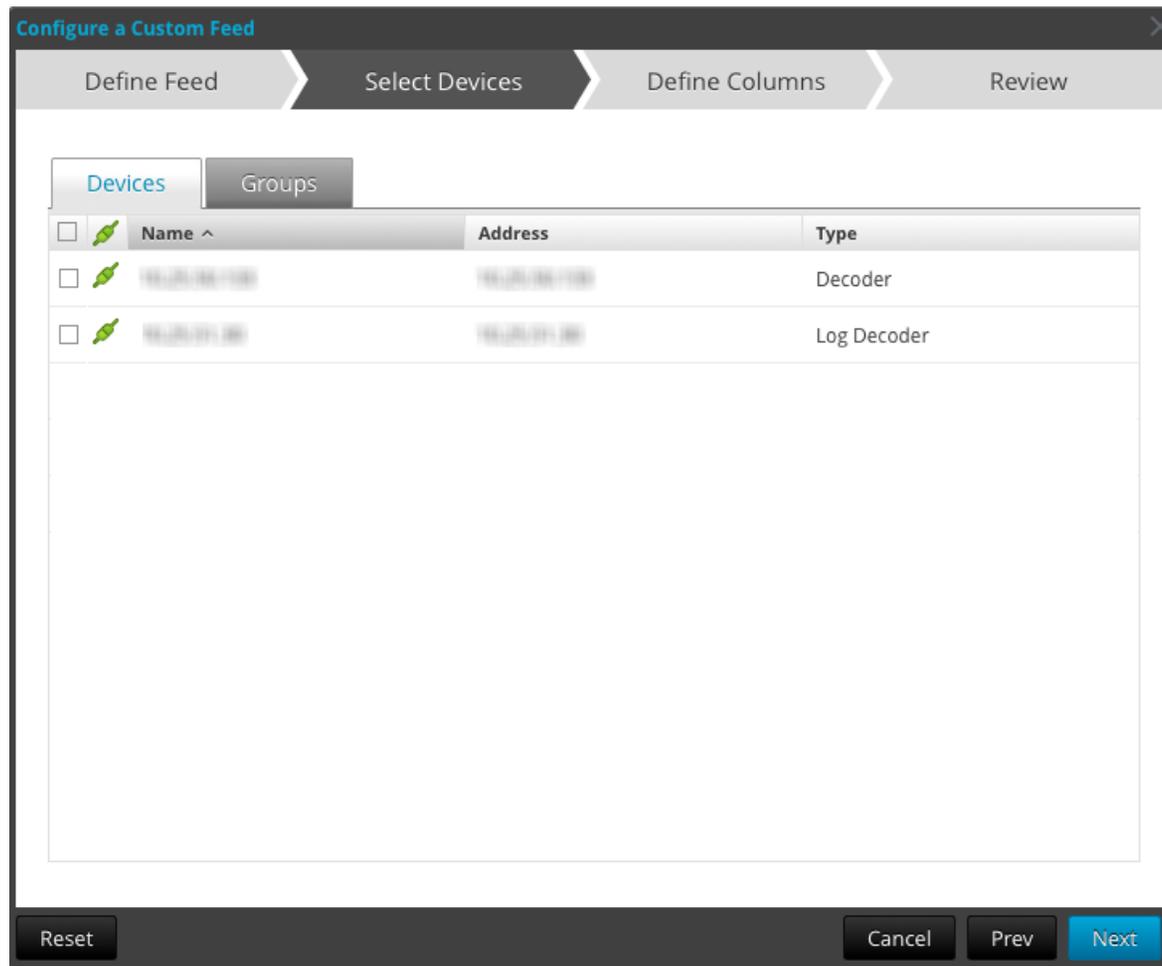


Ilustración 72. Pantalla para elegir en que dispositivos integrar los feeds.



6. El siguiente paso es definir las columnas:

**Configure a Custom Feed**

Define Feed    Select Devices    **Define Columns**    Review

**DEFINE INDEX**

Type     IP     IP Range     Non IP

Index Column    1     CIDR

**DEFINE VALUES**

Column	1 (Index)	2	3	4
Key		threat.source	threat.category	threat.desc
	1416job.com	netwitness	suspicious	dynamic dns domain
	163Info.org	netwitness	suspicious	dynamic dns domain
	2288.org	netwitness	suspicious	dynamic dns domain
	25u.com	netwitness	suspicious	dynamic dns domain
	2mydns.com	netwitness	suspicious	dynamic dns domain
	2myip.com	netwitness	suspicious	dynamic dns domain

Reset    Cancel    Prev    Next

Ilustración 73. Pantalla para definir las columnas a utilizar.



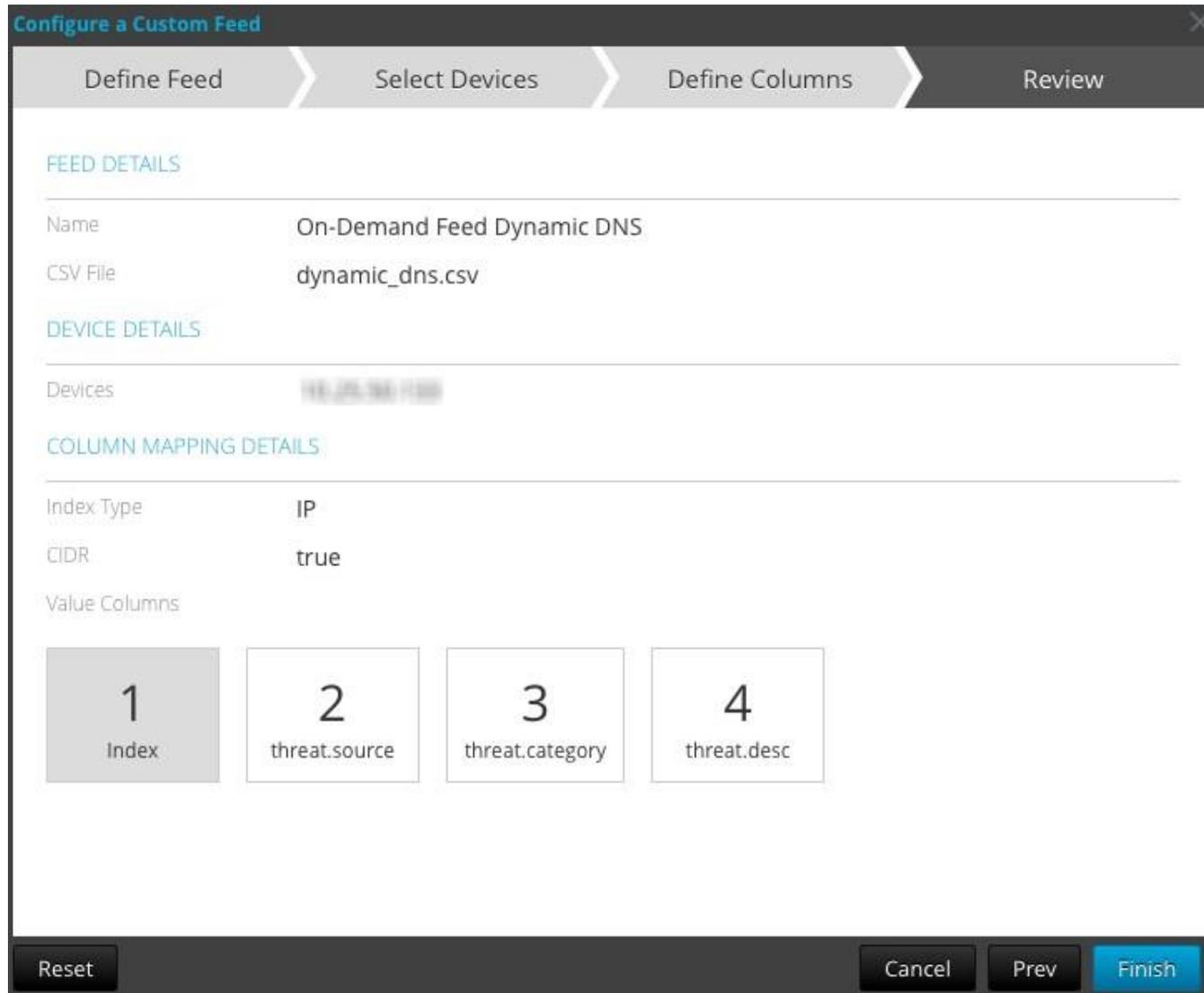
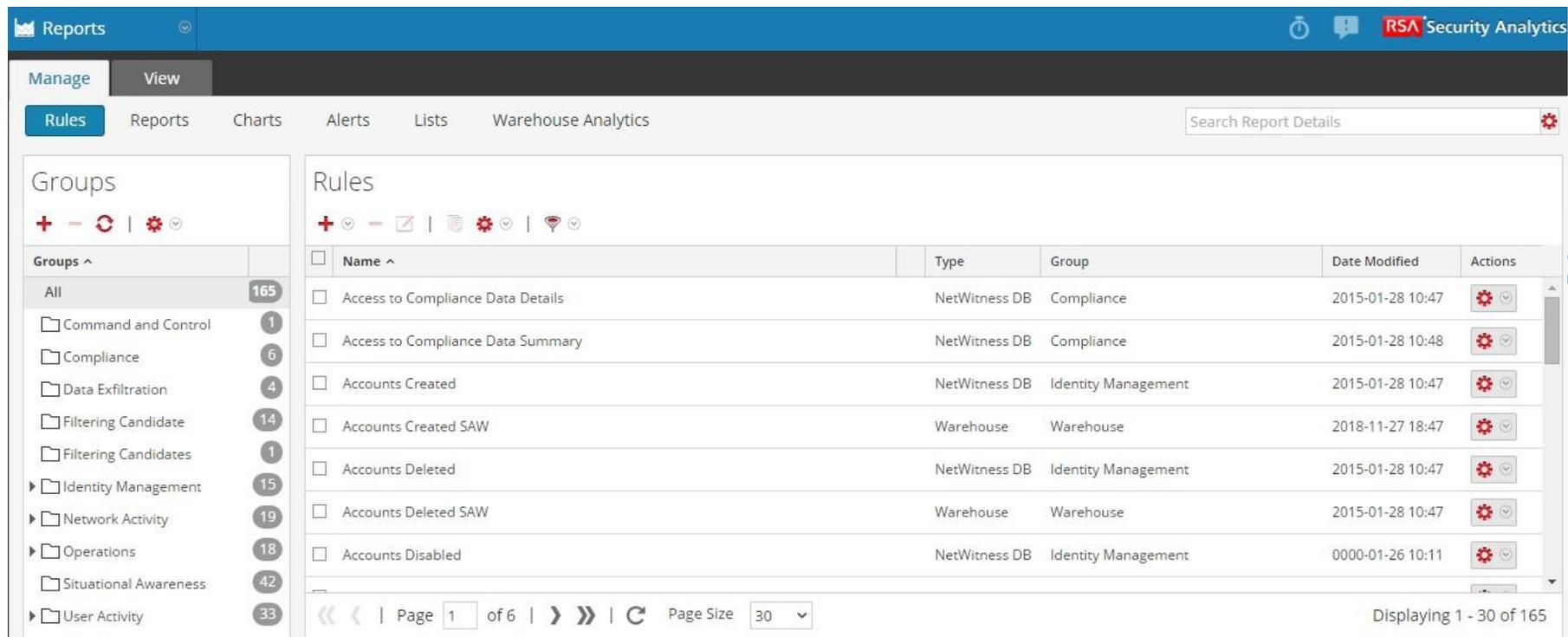


Ilustración 74. Resumen del feed a crear.



## 4. REPORTES

En esta pestaña se pueden observar los distintos reportes que vienen pre-cargados al suscribirnos a la inteligencia de LIVE y donde se pueden crear reportes ya sea tomando como base alguno de los que tenemos pre-cargados o creándolo desde cero a nuestras necesidades, darle formato, escoger la información que queremos observar y agendarlo de acuerdo a las necesidades de la empresa.



The screenshot displays the 'Reports' section of the RSA Security Analytics interface. The top navigation bar includes 'Reports', 'Manage', and 'View'. Below this, there are tabs for 'Rules', 'Reports', 'Charts', 'Alerts', 'Lists', and 'Warehouse Analytics'. A search bar for 'Search Report Details' is located on the right. The main content area is divided into two sections: 'Groups' on the left and 'Rules' on the right. The 'Groups' section shows a tree view with categories like 'All' (165), 'Command and Control' (1), 'Compliance' (6), 'Data Exfiltration' (4), 'Filtering Candidate' (14), 'Filtering Candidates' (1), 'Identity Management' (15), 'Network Activity' (19), 'Operations' (18), 'Situational Awareness' (42), and 'User Activity' (33). The 'Rules' section displays a table of predefined rules with columns for Name, Type, Group, Date Modified, and Actions. The table lists various rules such as 'Access to Compliance Data Details', 'Accounts Created', and 'Accounts Deleted'. At the bottom of the interface, there is a pagination control showing 'Page 1 of 6' and 'Page Size 30', along with the text 'Displaying 1 - 30 of 165'.

Name	Type	Group	Date Modified	Actions
Access to Compliance Data Details	NetWitness DB	Compliance	2015-01-28 10:47	[Settings]
Access to Compliance Data Summary	NetWitness DB	Compliance	2015-01-28 10:48	[Settings]
Accounts Created	NetWitness DB	Identity Management	2015-01-28 10:47	[Settings]
Accounts Created SAW	Warehouse	Warehouse	2018-11-27 18:47	[Settings]
Accounts Deleted	NetWitness DB	Identity Management	2015-01-28 10:47	[Settings]
Accounts Deleted SAW	Warehouse	Warehouse	2015-01-28 10:47	[Settings]
Accounts Disabled	NetWitness DB	Identity Management	0000-01-26 10:11	[Settings]

Ilustración 75. Reportes Predefinidos.



The screenshot displays the 'Build Rule' configuration interface in RSA Security Analytics. The main area is titled 'Build Rule' and features a 'Rule Type' dropdown set to 'NetWitness DB'. Below this are input fields for 'Name', 'Select', and 'Where'. The 'Then' section contains a text area with the placeholder 'Enter a then clause...'. To the left of the main configuration area are several settings: 'Aggregate' is checked, 'Summarize' is set to 'Event Count', 'Sort By' is 'Total', 'Order' is 'Descending Order', 'Session Threshold' is '0', and 'Limit' is '20'. At the bottom of this section are four buttons: 'Use', 'Save', 'Reset', and 'Test Rule'. On the right side, there are two panels: 'Meta' and 'Lists'. The 'Meta' panel shows a dropdown for 'CON1 - Concentrator' and a list of fields including 'access.point', 'action', 'ad.computer.dst', 'ad.computer.src', 'ad.domain.dst', 'ad.domain.src', and 'ad.username.dst'. The 'Lists' panel has a 'Filter' input, an 'Insert' button, and a list of categories with checkboxes: 'Compliance', 'Filtering Candidate', 'Local\_Country', 'Logs', 'Network Activity', and 'User Activity'. A large number '71' is positioned to the right of the 'Lists' panel.

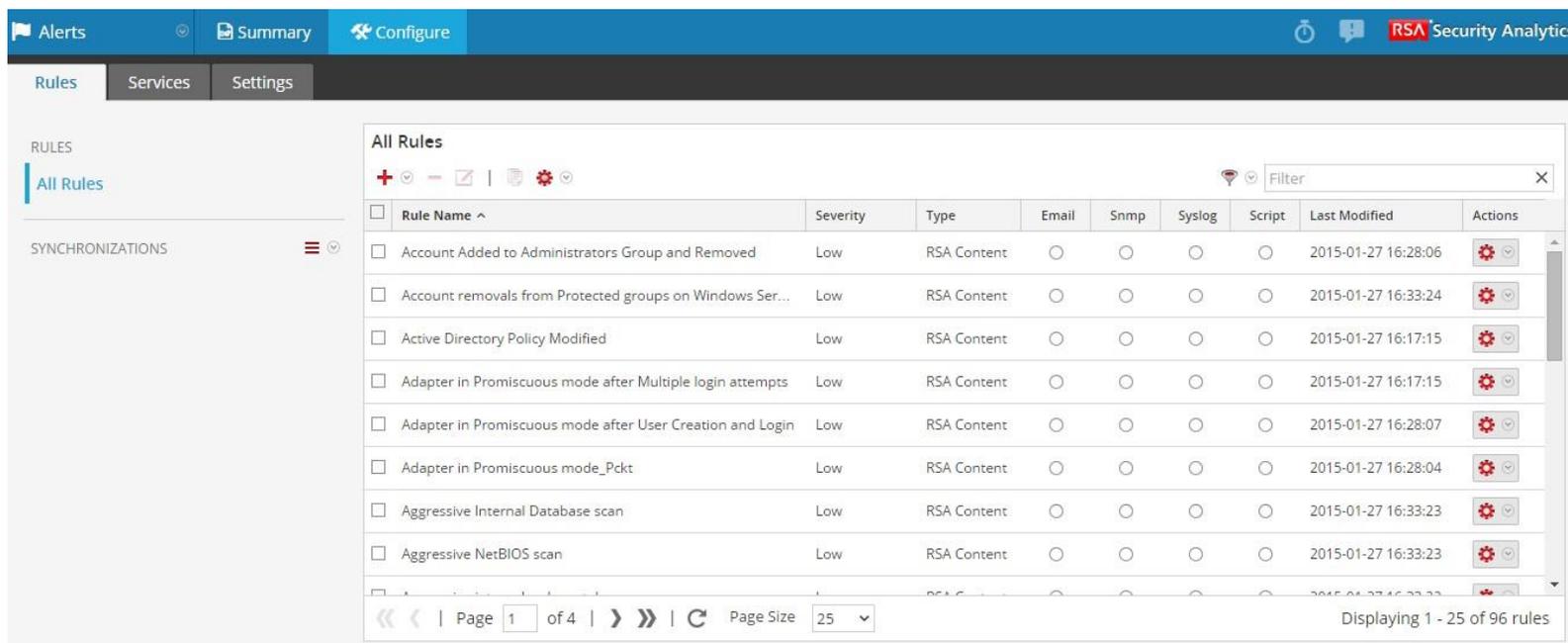
Ilustración 76. Plantilla en Blanco para realizar un Reporte.



## 4.1 Alertas

En este módulo podemos observar todas las alertas, este módulo contiene reglas pre-cargadas al suscribirnos a la inteligencia de LIVE, pero se pueden crear reglas desde cero de acuerdo a las necesidades de la empresa.

En este módulo se pueden definir todas las alertas que sean necesarias, pero solamente estarán activas aquellas que sincronizamos con el módulo de ESA que deseemos, ya que si no están sincronizadas estas reglas no se disparara en el supuesto caso que exista un evento con las características de la alerta.



The screenshot displays the 'Alerts' configuration page in the RSA Security Analytics interface. The 'Configure' tab is active, and the 'Rules' section is selected. The 'All Rules' table lists various pre-installed rules with columns for Rule Name, Severity, Type, Email, Snmp, Syslog, Script, Last Modified, and Actions. The table shows 96 rules in total, with the first 25 displayed on the current page.

Rule Name	Severity	Type	Email	Snmp	Syslog	Script	Last Modified	Actions
Account Added to Administrators Group and Removed	Low	RSA Content	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	2015-01-27 16:28:06	
Account removals from Protected groups on Windows Ser...	Low	RSA Content	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	2015-01-27 16:33:24	
Active Directory Policy Modified	Low	RSA Content	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	2015-01-27 16:17:15	
Adapter in Promiscuous mode after Multiple login attempts	Low	RSA Content	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	2015-01-27 16:17:15	
Adapter in Promiscuous mode after User Creation and Login	Low	RSA Content	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	2015-01-27 16:28:07	
Adapter in Promiscuous mode_Pckt	Low	RSA Content	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	2015-01-27 16:28:04	
Aggressive Internal Database scan	Low	RSA Content	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	2015-01-27 16:33:23	
Aggressive NetBIOS scan	Low	RSA Content	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	2015-01-27 16:33:23	

Ilustración 77. Reglas disponibles para crear alertas.



Rule Name	Severity	Type	Email	Snmp	Syslog	Script	Last Modified	Actions
FW_Origen Malicioso	Medium	Basic	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	2015-02-24 13:46:44	
IPS_Firma Disparada	Medium	Basic	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	2015-03-10 17:15:35	
IPS_Firma disparada	Medium	Basic	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	2015-03-10 13:04:21	

Ilustración 78. Reglas Sincronizadas.

## 4.2 Alerta FW\_Origen Malicioso

Esta alerta identifica si una IP pública con actividad maliciosa va dirigida a activos del cliente y si esta se dispara 10 veces en menos de 60 segundos.

**Build Rule**

Rule Name \* FW\_Origen Malicioso

Description: Esta regla identifica si una IP pública origen con actividad maliciosa va dirigida a activos de [redacted] y genera 10 intentos en 60 segundos.

Severity \* Medium

Conditions \*

Statement	Occurs	Connector	Correlated On
<input type="checkbox"/> Origen Malicioso	7		

Occurs Within 1 minutes Group By ip\_src

Notifications

Type	Notification	Notification Server	Template
<input type="checkbox"/> EMAIL	INFOTEC_Mail	Infofec_Mail	Default SMTP Template

Output Suppression of every [ ] minutes

Enrichments

Type	Enrichment Source	ESA Event Stream Meta	Enrichment Source Column Name
No parameters to edit.			

Debug

Ilustración 79. Información de una alerta creada por INFOTEC.



Build a Statement ✕

Name \*

If all conditions are met ▼

	Meta Key	Evaluation Type	Value	Is Value An Array?	
<input type="checkbox"/>	event_type	is	traffic	No	+ -
<input type="checkbox"/>	threat_category	is not	0	No	
<input type="checkbox"/>	threat_source	is not	0	No	

Ilustración 80. Condiciones a cumplir de la alerta.



### 4.3 Alerta IPS\_Firma Disparada

Esta regla identifica si se levanta una firma en el módulo de IPS del UTM Fortigate 600c

**Build Rule**

Rule Name \*

Description

Severity \*

Conditions \*

Statement	Occurs	Connector	Correlated On
<input type="checkbox"/> Fuente	1	AND	
<input type="checkbox"/> Tipo de evento	1	AND	
<input type="checkbox"/> Categoria	1		

Occurs Within  Group By

Notifications

Type	Notification	Notification Server	Template
<input type="checkbox"/> EMAIL	INFOTEC_Mail	Infotec_Mail	Default SMTP Template

Output Suppression of every  minutes

Enrichments

Type	Enrichment Source	ESA Event Stream Meta	Enrichment Source Column Name
No parameters to edit.			

Debug

Ilustración 81. Condiciones a cumplir de la alerta.



### Build Rule

Rule Name \*

Description

Severity \*

Conditions \*  +  -

	Statement	Occurs	Connector	Correlated On
<input type="checkbox"/>	Fuente	1	AND	
<input type="checkbox"/>	Tipo de evento	1	AND	
<input type="checkbox"/>	Categoría	1		

Occurs Within  minutes Group By

Notifications  +  -

	Type	Notification	Notification Server	Template
<input type="checkbox"/>	EMAIL	INFOTEC_Mail	Infotec_Mail	Default SMTP Template

Output Suppression of every  minutes

Enrichments  +  -

	Type	Enrichment Source	ESA Event Stream Meta	Enrichment Source Column Name
No parameters to edit.				

Debug

Ilustración 82. Condiciones a cumplir de la alerta.



Asimismo, podemos apreciar un resumen de las alertas, si están habilitadas o no, cuantas reglas se tienen sincronizadas, cuantas alertas se han disparado, es decir, un resumen de todo lo relacionado a las alertas del módulo de ESA.

The screenshot displays the 'ESA1 - Event Stream Analysis' interface. It features three main summary sections: Engine Stats, Rule Stats, and Alert Stats. Below these is a 'Deployed Rule Stats' section with a table listing individual rules, their status, last detected time, and event counts.

Engine Stats		Rule Stats		Alert Stats	
Esper Version	4.11.0	Deployed	98	Email	0
Time	2015-02-10T14:00:12	Rules Enabled	98	SNMP	0
Events Offered	38511240	Rules Disabled	0	Syslog	0
Offered Rate	0 / max	Events Matched	30314	Script	0
				Storage	5575015
				Message Bus	0

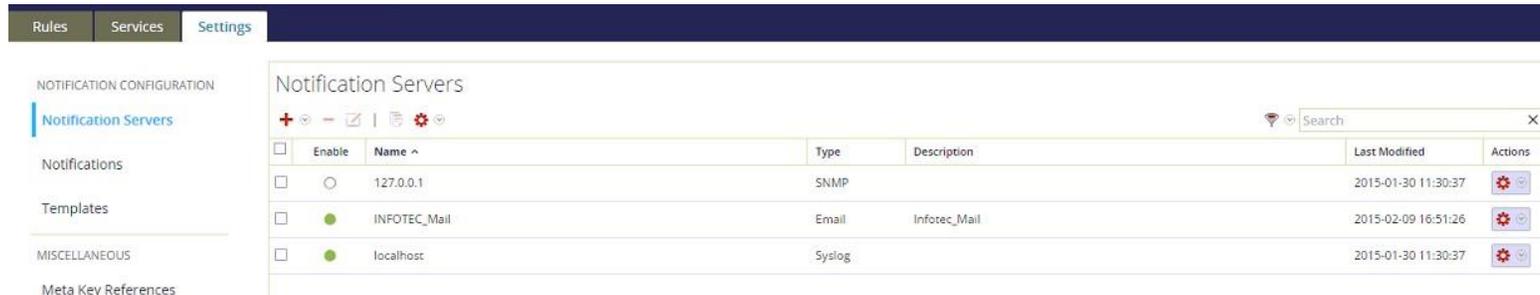
  

Deployed Rule Stats				
● Enable ○ Disable				
<input type="checkbox"/>	Enable	Name	Last Detected	Events Matched
<input type="checkbox"/>	●	Port Scan Horizontal Log	2015-02-10 13:50:21	30180
<input type="checkbox"/>	●	Port Scan Vertical Log	2015-02-10 12:12:21	120
<input type="checkbox"/>	●	System Configuration Changes By Non Administrative User	2015-02-10 03:31:51	14
<input type="checkbox"/>	●	Multiple Intrusion scan events from same username to unique destinations		0
<input type="checkbox"/>	●	Non SMTP Traffic on TCP Port 25 Containing Executable		0
<input type="checkbox"/>	●	fortimail		0
<input type="checkbox"/>	●	Aggressive Internal Database scan		0
<input type="checkbox"/>	●	Adapter in Promiscuous mode after User Creation and Login		0
<input type="checkbox"/>	●	User added to admin group same user login OR same user su sudo		0

Ilustración 83. Resumen de las alertas.



En este apartado es donde configuramos el servidor SNMP, Syslog o de Email en el cual queremos recibir notificaciones en caso de que se dispare una o varias alertas, podemos tener definidos tantos servidores como queramos, aunque en cada regla se debe definir a que servidores se enviarán las notificaciones en caso de que la alerta se dispare.



Enable	Name ^	Type	Description	Last Modified	Actions
<input type="checkbox"/>	127.0.0.1	SNMP		2015-01-30 11:30:37	
<input checked="" type="checkbox"/>	INFOTEC_Mail	Email	Infotec_Mail	2015-02-09 16:51:26	
<input checked="" type="checkbox"/>	localhost	Syslog		2015-01-30 11:30:37	

Ilustración 84. Configuración de los servidores de notificaciones.



Enable	Name ^	Type	Description	Last Modified	Actions
<input type="checkbox"/>	127.0.0.1	SNMP		2015-01-30 11:30:37	
<input checked="" type="checkbox"/>	INFOTEC_Mail	Email	Mail de INFOTEC	2015-02-05 16:04:57	
<input checked="" type="checkbox"/>	localhost	Syslog		2015-01-30 11:30:37	

Ilustración 85. Configuración del formato de la notificación.



## CONCLUSIONES

### Configuración de Security Analytics

Gracias a la implementación y configuración del correlacionador, que se llevó a cabo dentro de una infraestructura virtual (VMware ESX Server) con la respectiva versión instalada, configuración del NTP, configuración y características de entidades adecuadas se llegó a la operación de la solución (Portal RSA SecurCare Online) para ayudar en los problemas más comunes con los que cuentan los clientes.

Asimismo, sirvió como base de conocimientos, descargas, información de productos, etc de EMC los cuales contemplan aquellos de Security Analytics, en los que en caso de que el problema sea crítico y debamos ponernos en contacto directamente con un Ingeniero que nos apoye con dicho problema lo antes posible y así poder atender oportunamente problemas que se susciten directamente a la seguridad de los clientes.

### Configuración de LIVE

En la implementación del Security Analytics se configuró el sistema de gestión de contenidos (LIVE), esta herramienta proporcionó una visión de la inteligencia y habilidades analíticas de la comunidad de seguridad para garantizar que los clientes tengan la visibilidad más actual en vectores de ataque.

La versión de licenciamiento que se necesitó fue la básica, la cual proporciona automáticamente información sobre amenazas a los clientes a través de RSA Live. Asimismo, agrega datos de amenazas y los convierte en analizadores y reglas de correlación, adicionalmente, se alimenta y se fusiona con los datos del cliente dentro de RSA Security Analytics. Esto significa que los usuarios pudieron tomar mucho más fácilmente las ventajas de lo que otros ya han encontrado y saber lo que deben buscar. Una vez entregado, la inteligencia operativa se aplicó a los datos entrantes o históricos.



## Configuración de entidades

Durante la configuración de las entidades se realizó la integración de las fuentes que se correlacionaron donde se obtuvo la integración de los logs de las fuentes deseadas. Asimismo, se configuró el reenvío de logs a una fuente externa para que de ahí se pudieran extraer.

Una vez con el reenvío de logs hacia la fuente externa, se realizaron los custom feeds de manera que solo se agregaran casillas que nos interesaran y tener una visualización más específica.

## Configuración de reportes

En este apartado se realizaron los reportes, basados en las alertas que podrían ser las más significativas en caso de que se llegara a presentar un ataque dentro de la infraestructura de los clientes.

Las alertas fueron configuradas basadas en las necesidades de los clientes. Las realizadas principalmente fueron las de origen malicioso y las de firma de IPS, posteriormente se configuraron las notificaciones para hacerlas llegar inmediatamente al correo del personal encargado de administrar la herramienta (operadores), con la finalidad de analizar la alerta disparada y dar una solución oportuna a los clientes en caso de verse vulnerables. Esta herramienta ayudó a que mejoraran los análisis de posibles amenazas a los clientes.

