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

Contenido

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

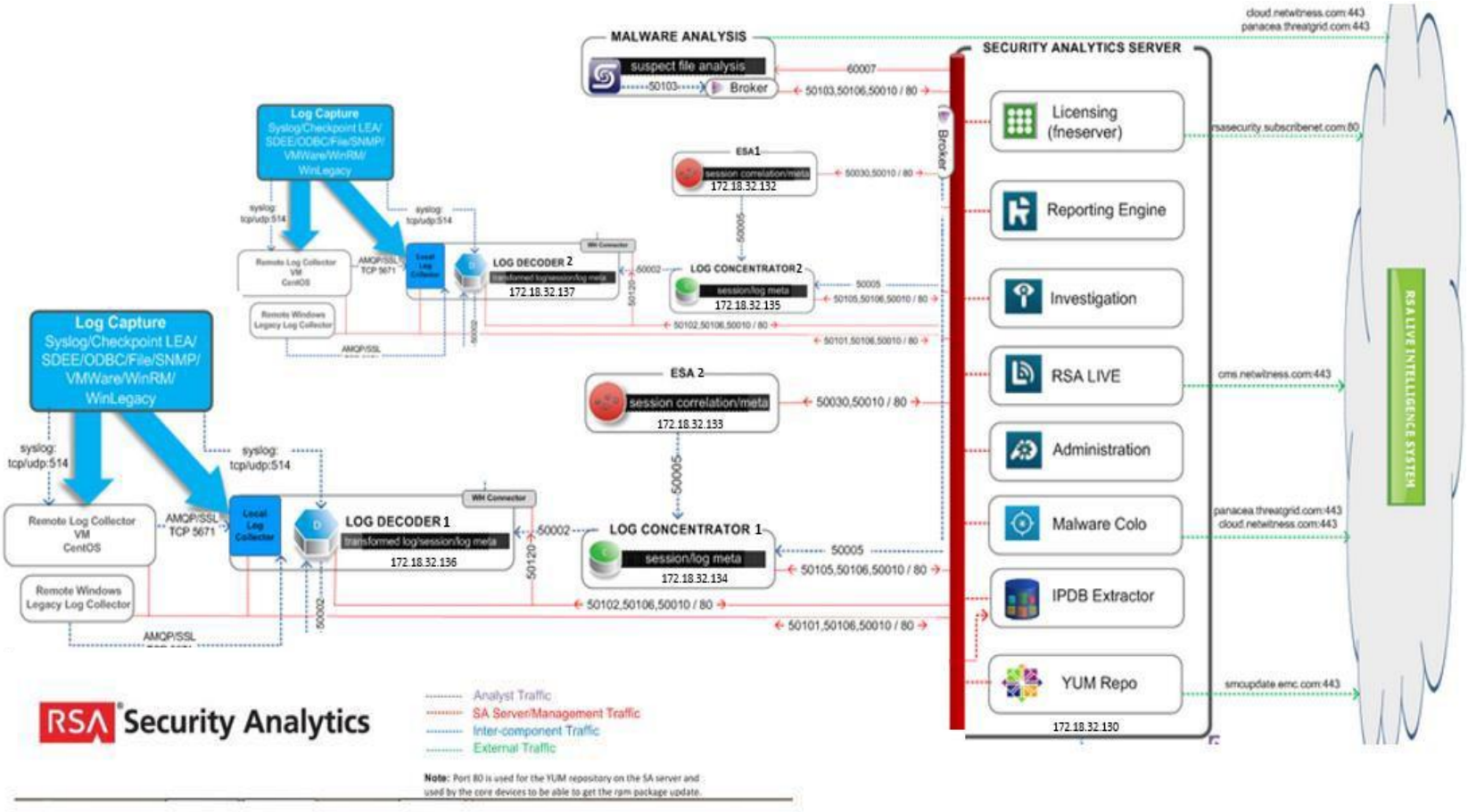


Ilustración 1. Diagrama Security Analytics

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.

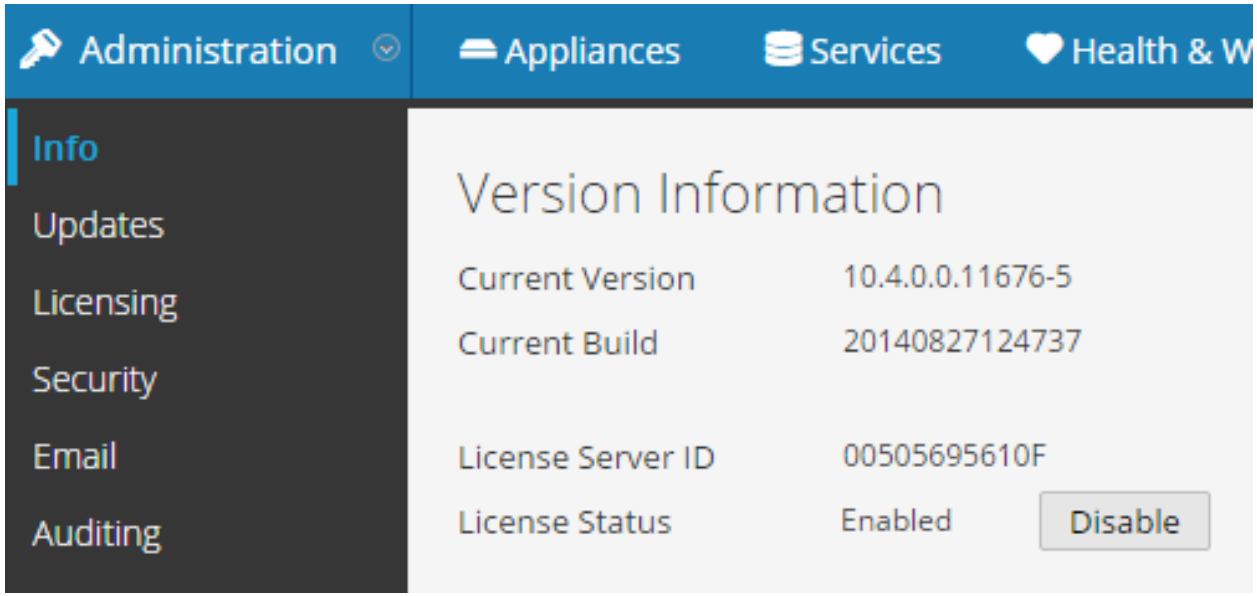


Ilustración 3. Información de Security Analytics

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

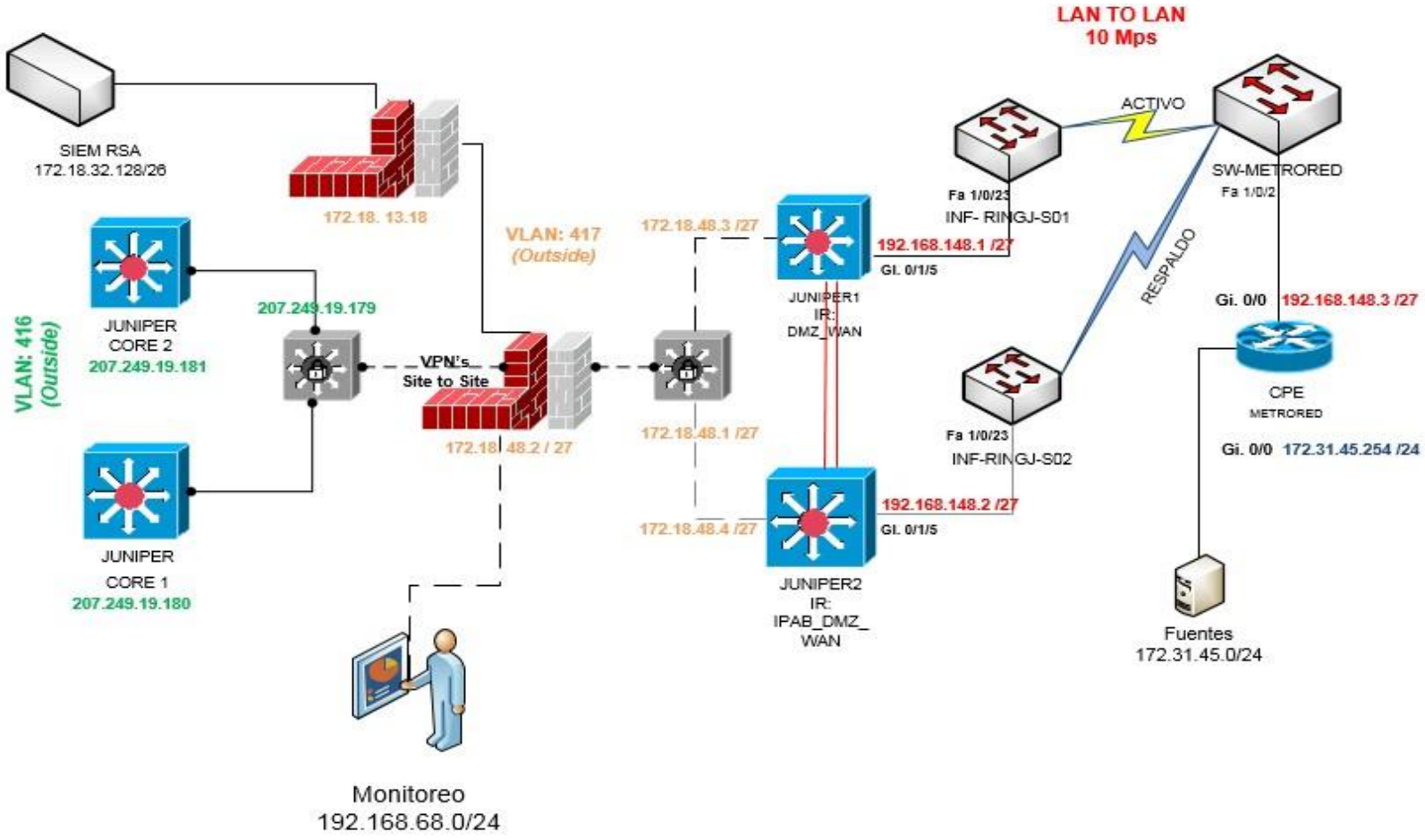


Ilustración 5. Diagrama de Red de INFOTEC

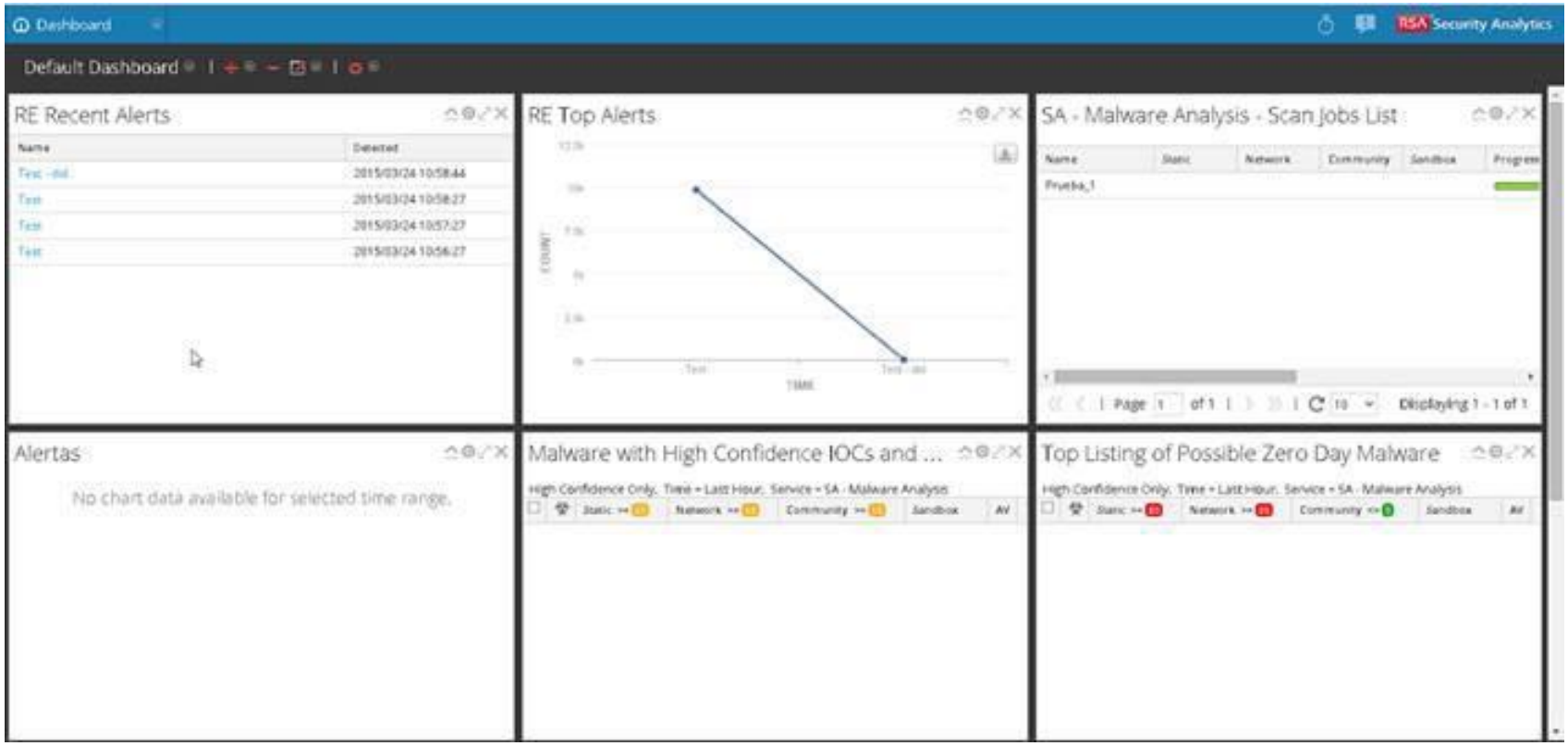


Ilustración 6. Dashboard Principal

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
CON1 – Concentrator	172.18.32.134	255.255.255.192	172.18.32.190
CON2 - Concentrator	172.18.32.135	255.255.255.192	172.18.32.190
ESA1 – Event Stream	172.18.32.132	255.255.255.192	172.18.32.190
ESA2 – Event Stream	172.18.32.133	255.255.255.192	172.18.32.190
LOGDEC1 – Log Decoder	172.18.32.136	255.255.255.192	172.18.32.190
LOGDEC2 – Log Decoder	172.18.32.137	255.255.255.192	172.18.32.190
SA Server	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"

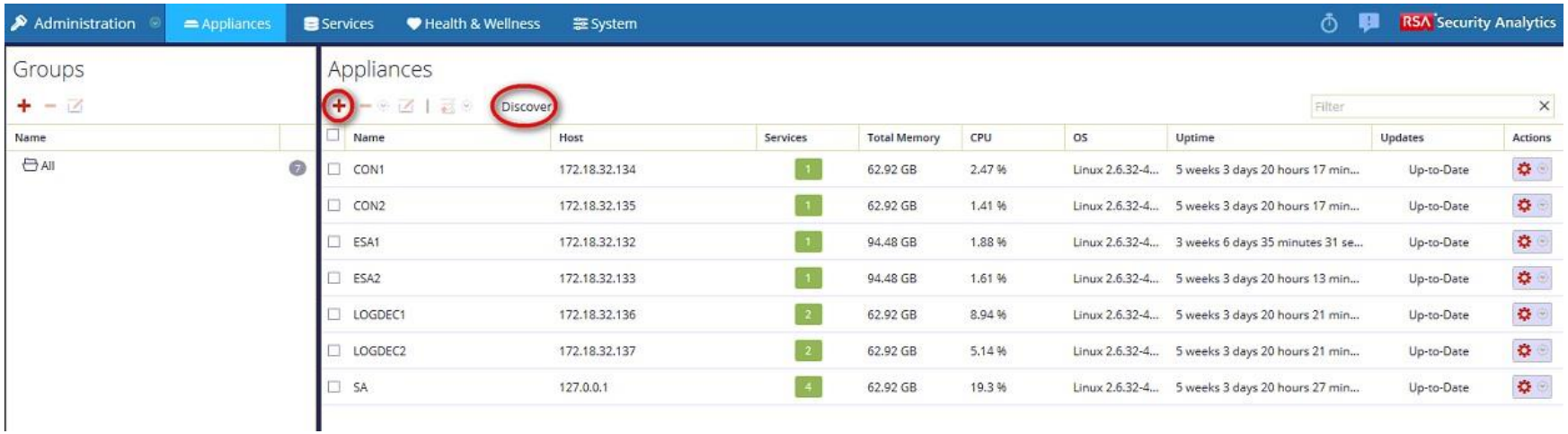


Ilustración 7. Agregar entidades a Security Analytics

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

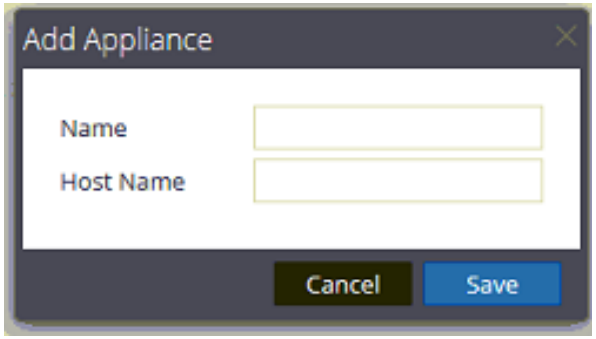


Ilustración 8. Agregar manualmente entidades a Security Analytics

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.

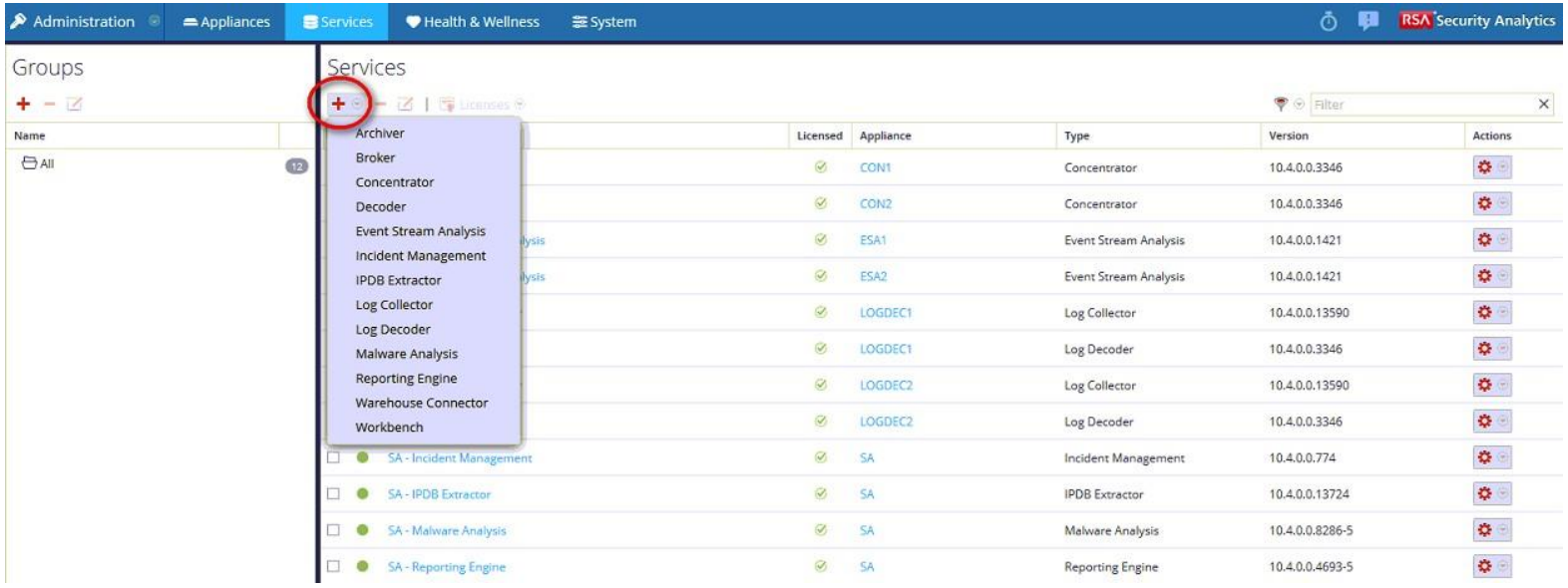


Ilustración 9. Configurar los servicios de Security Analytics.

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

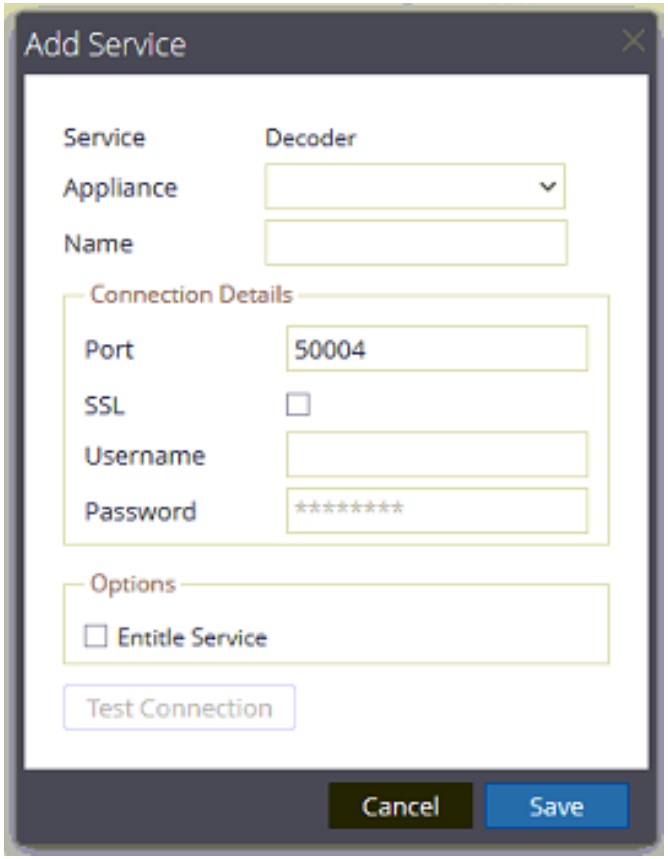


Ilustración 10. Configurar los servicios de Security Analytics.

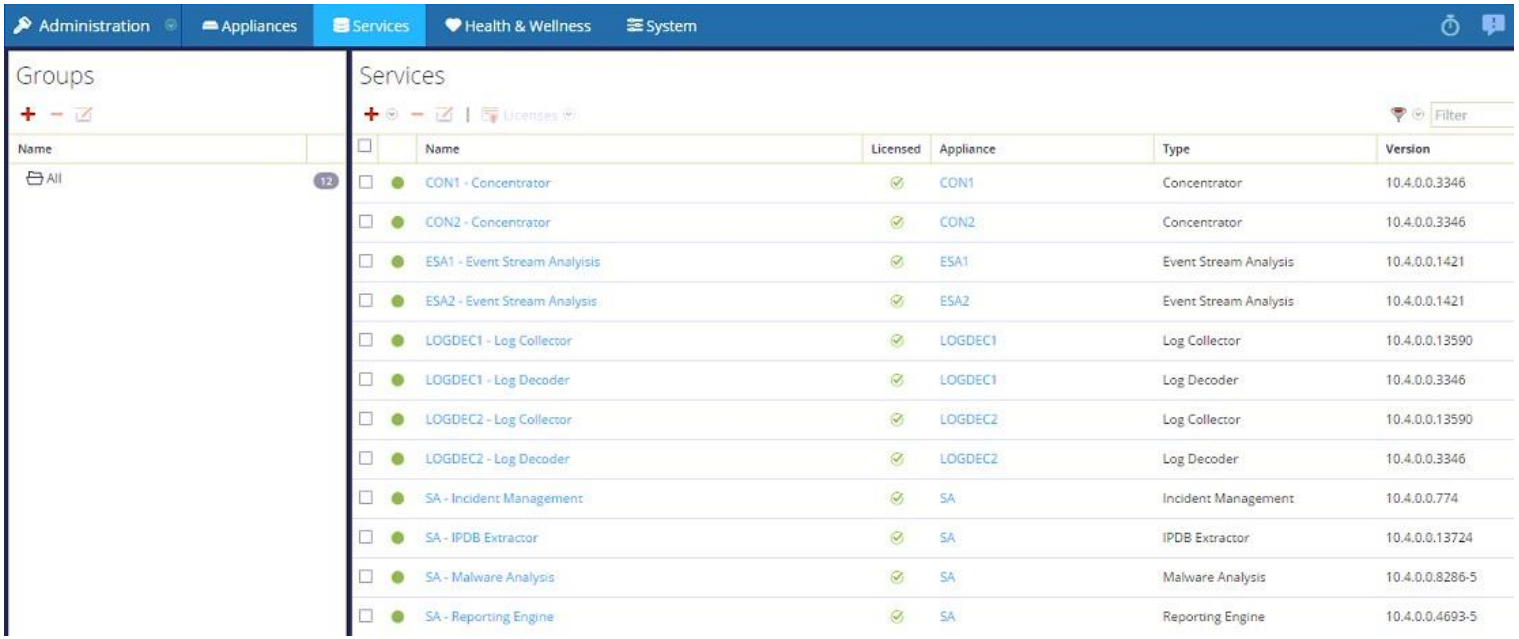


Ilustración 11. Listado de Servicios de Security Analytics

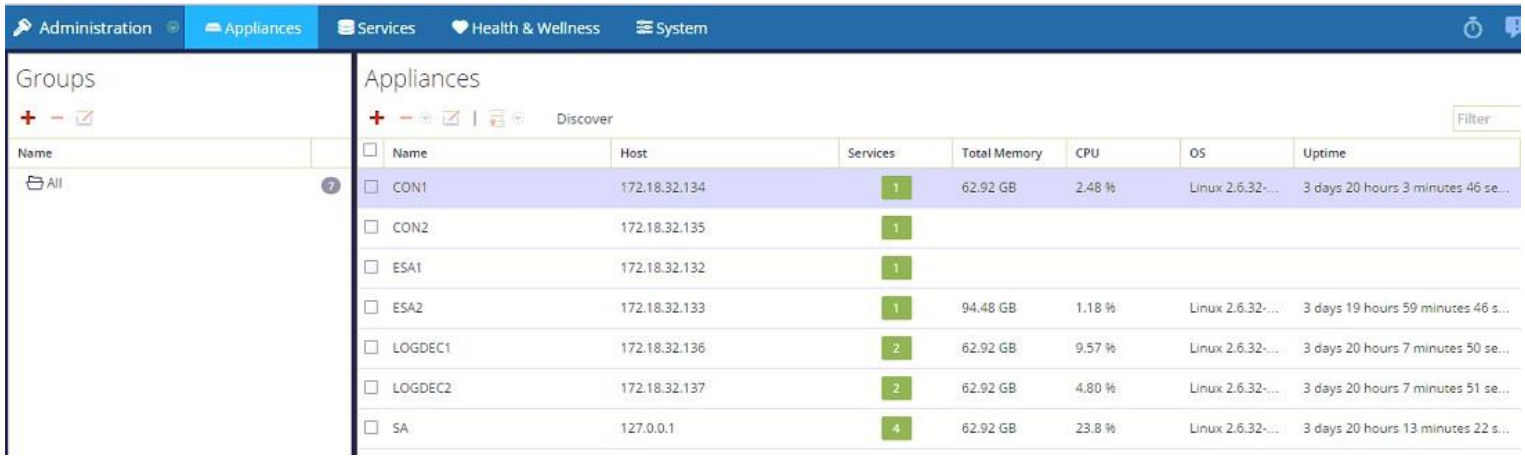


Ilustración 12. Listado de Entidades de Security Analytics

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.

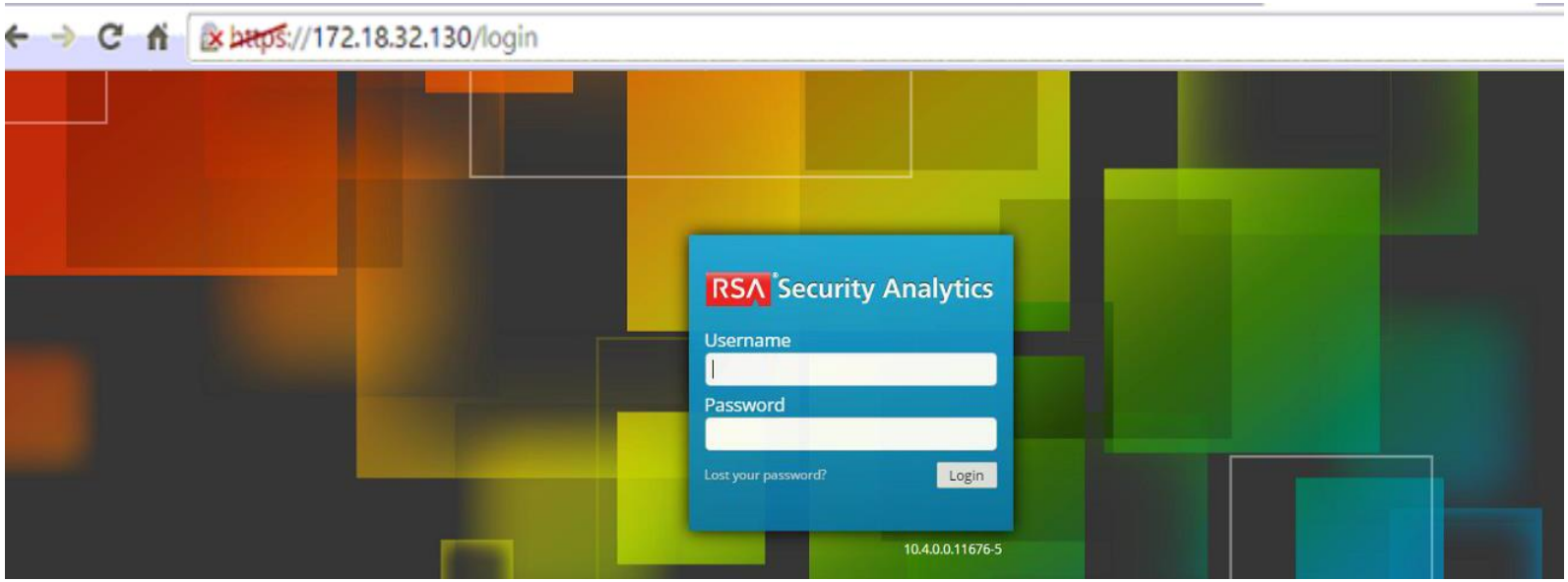


Ilustración 13. Ingreso a la consola

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 la cual nos re direccionara a la siguiente URL. En dicha página se deberá ingresar con las credenciales correspondientes, previamente creadas.

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

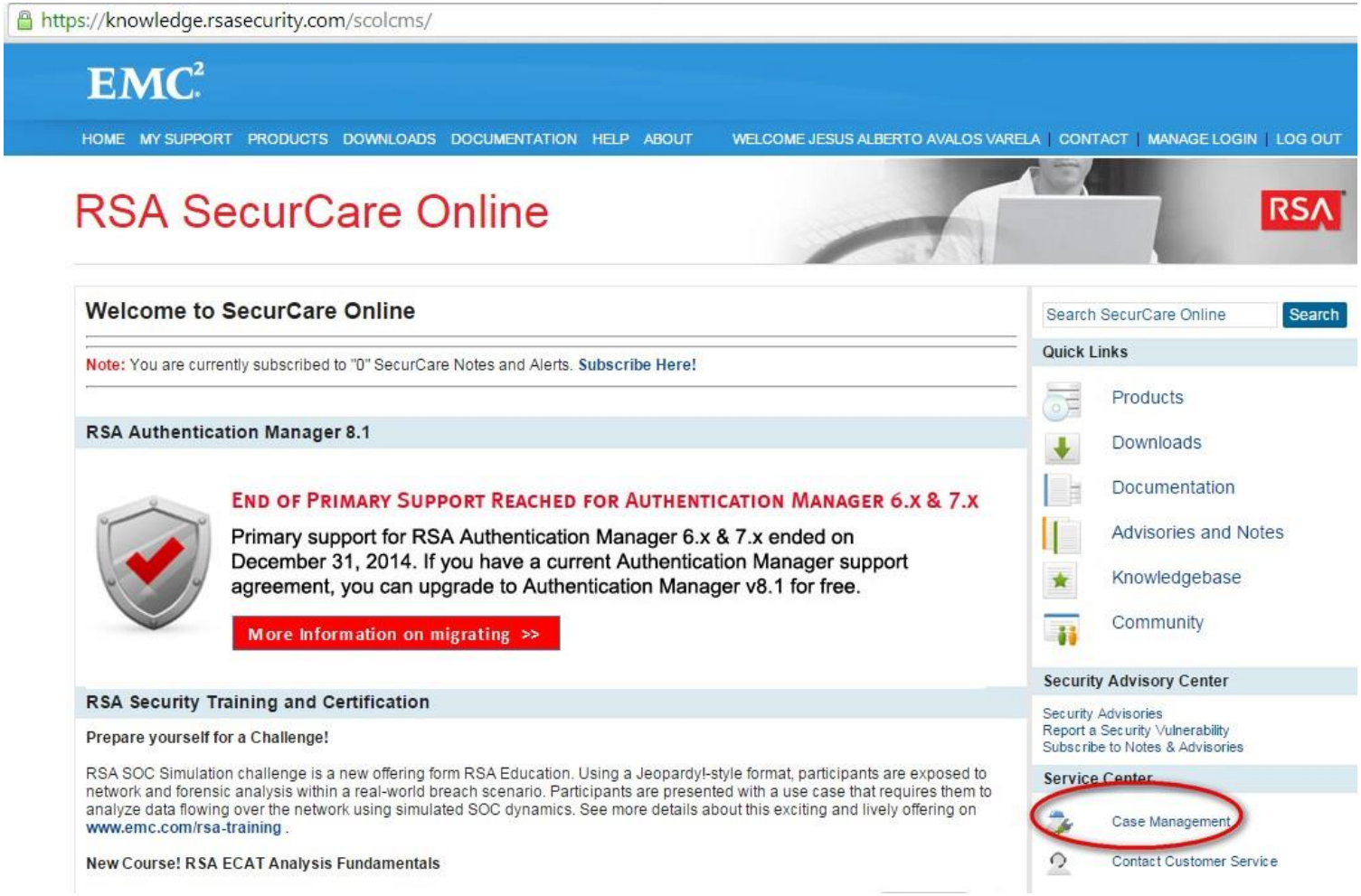


Ilustración 15. Fuentes a monitorear.

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".

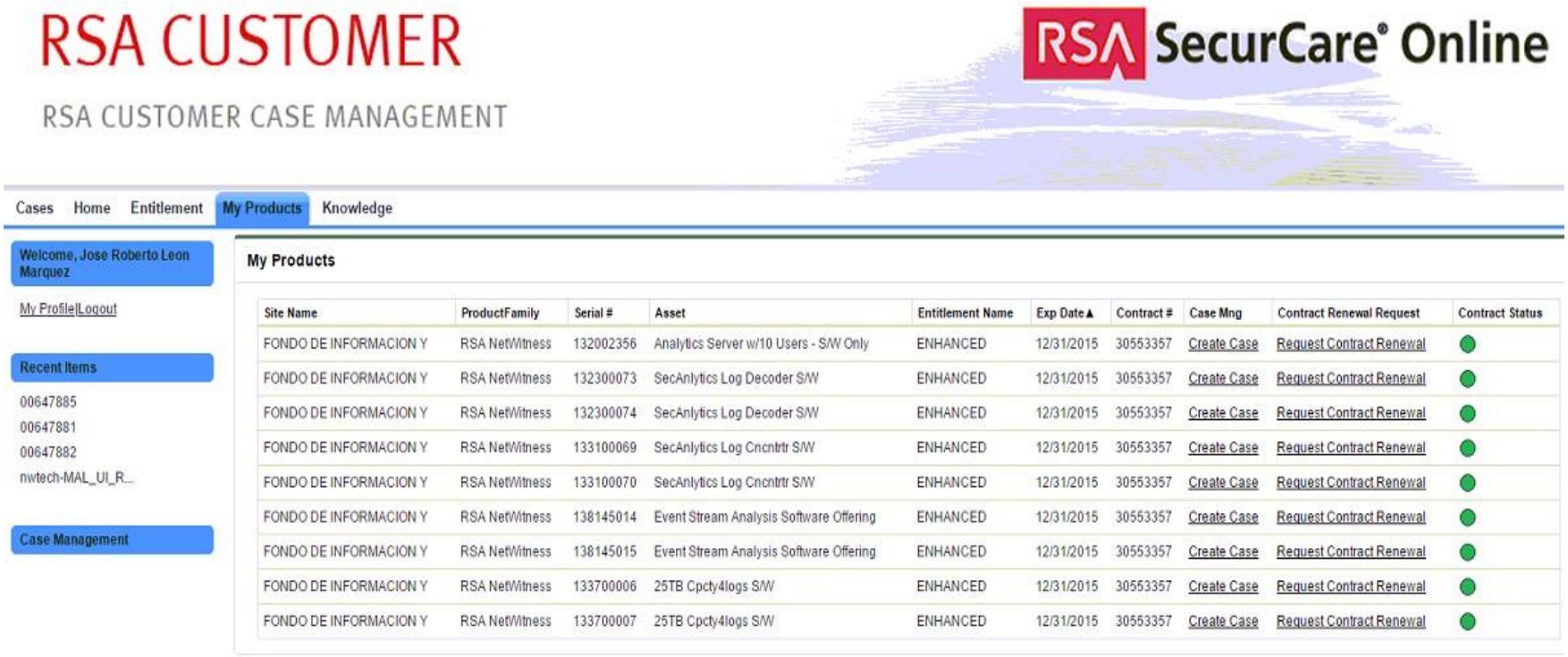


Ilustración 16. Entidades de Security Analytics con los que cuenta INFOTEC

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.

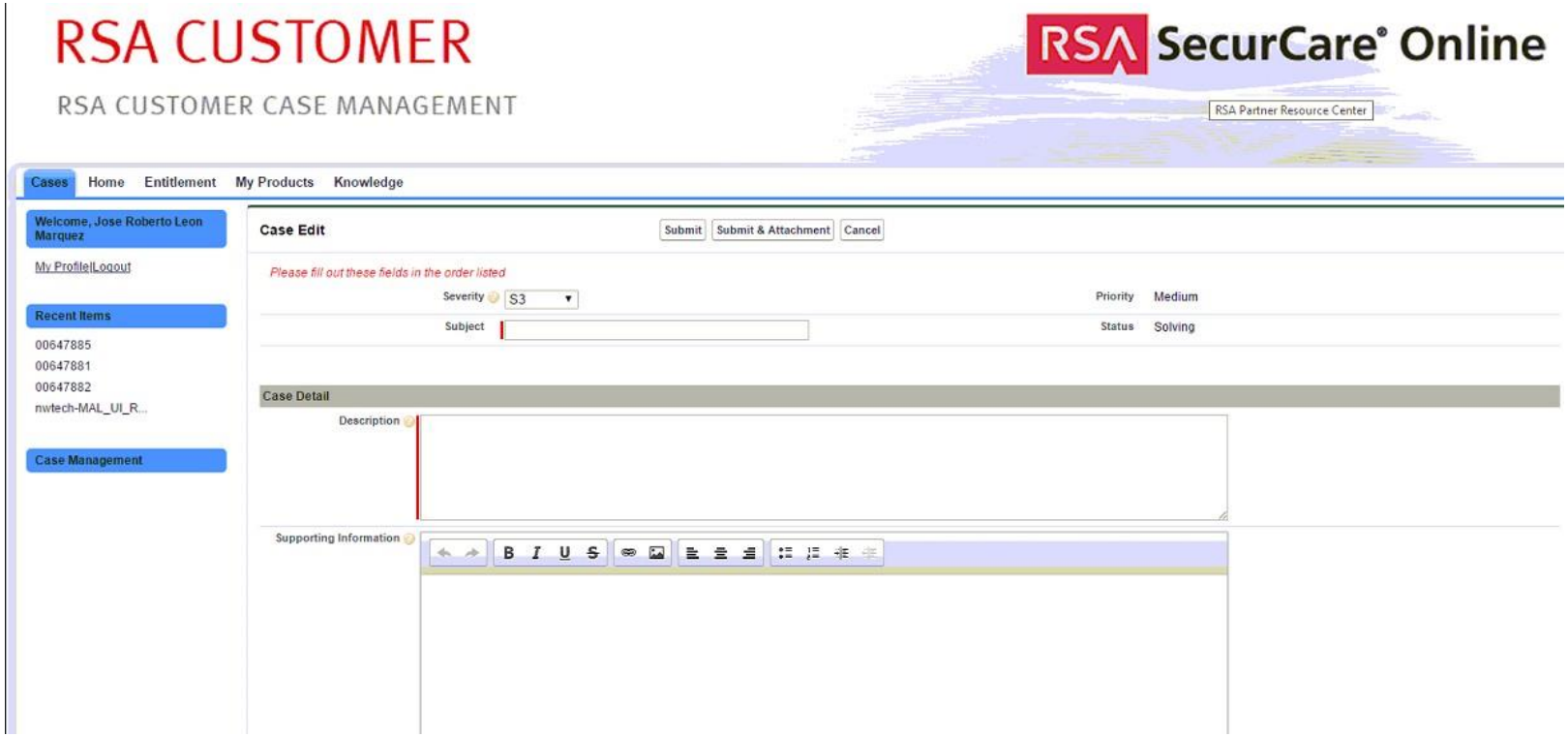


Ilustración 17. Campos a llenar sobre la creación de casos con el soporte de RSA

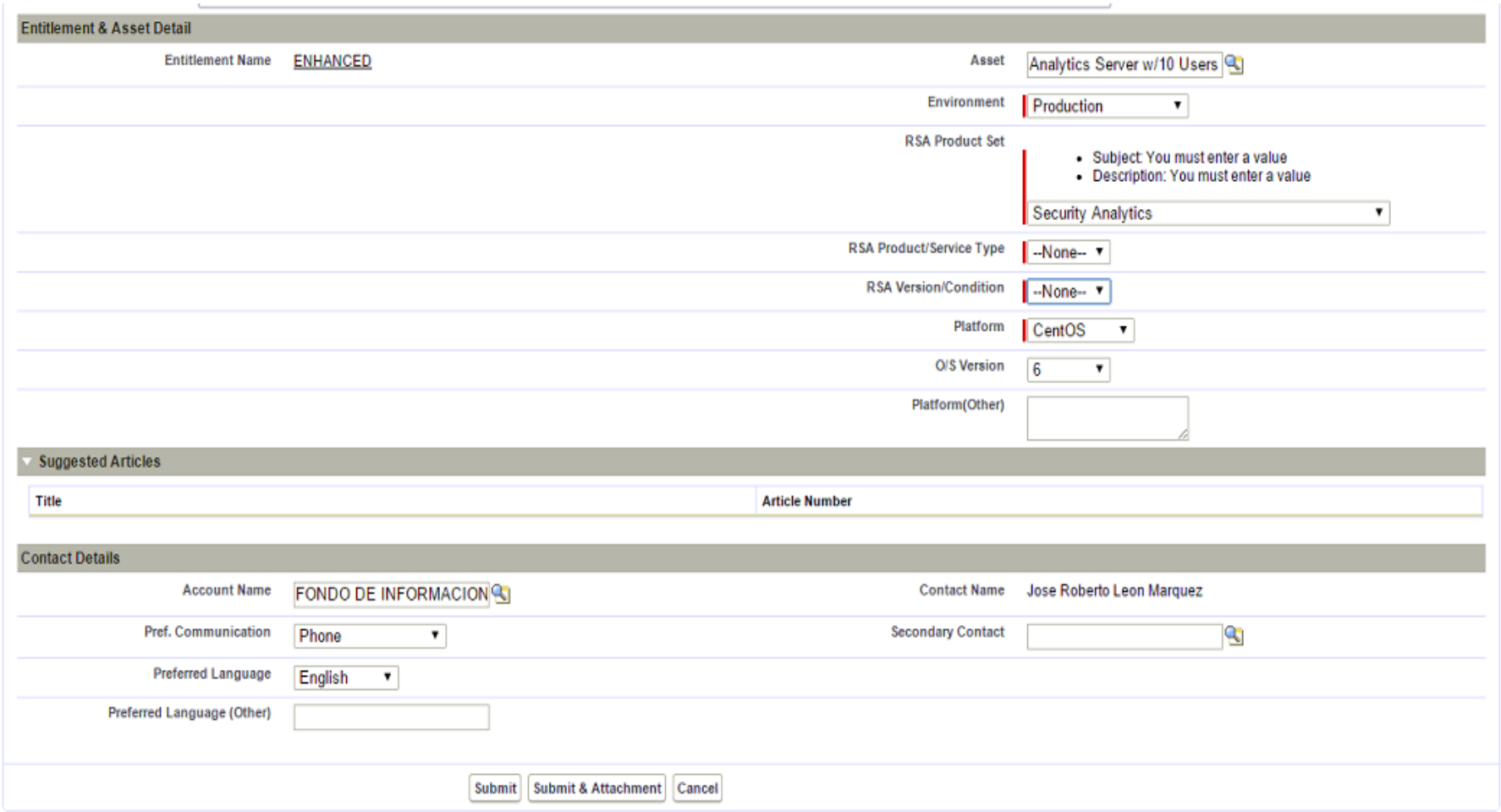


Ilustración 18. Datos esenciales para la creación de casos de Security Analytics.

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.

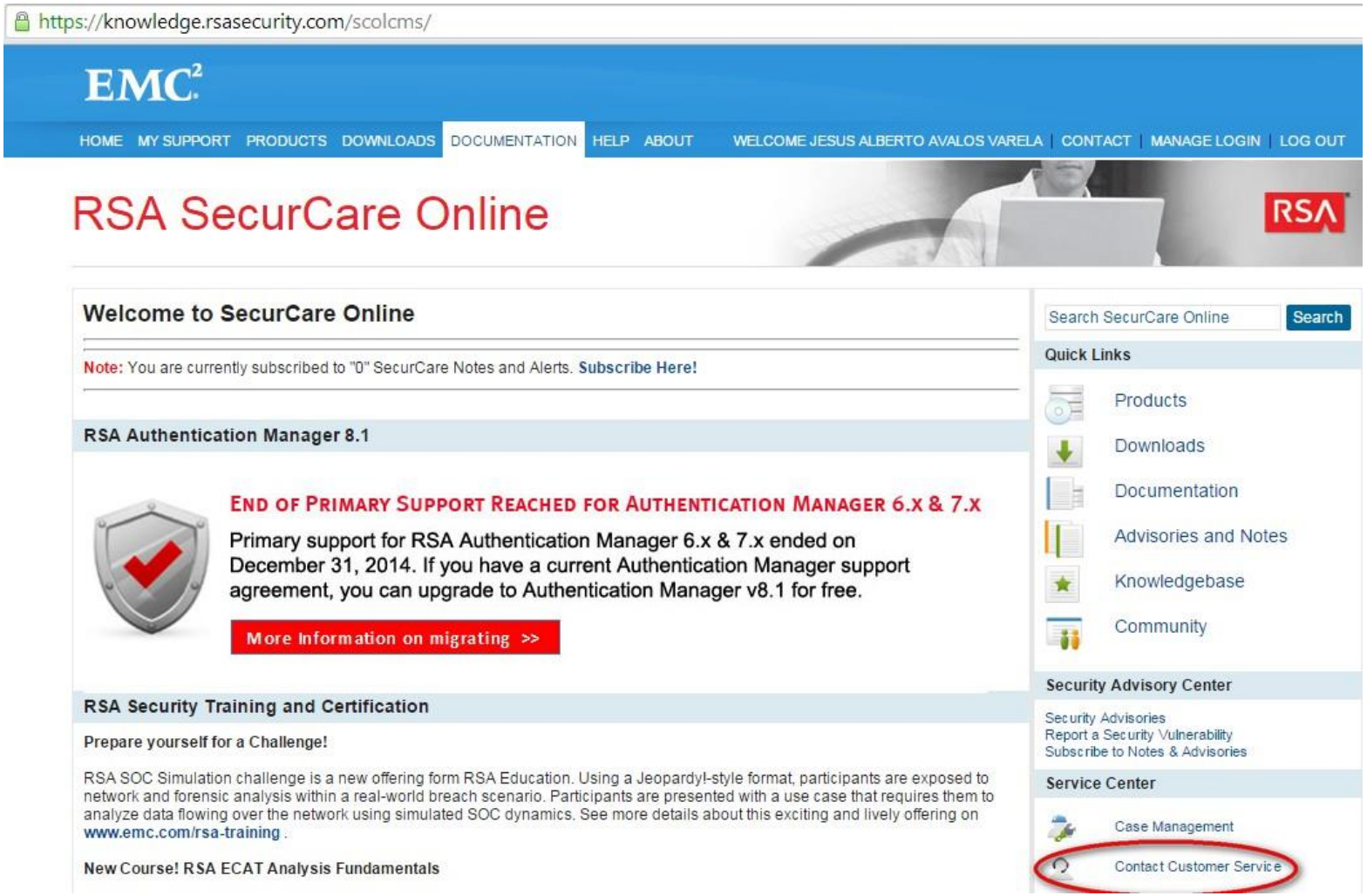


Ilustración 19. Fuentes a monitorear

Los teléfonos son los siguientes:

RSA SecurCare Online

Phone Support | Customer Survey

Contact Support

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	

Device/Service	Port(s) /Security Analytics Core Non-SSL	Security Analytics Core SSL
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:

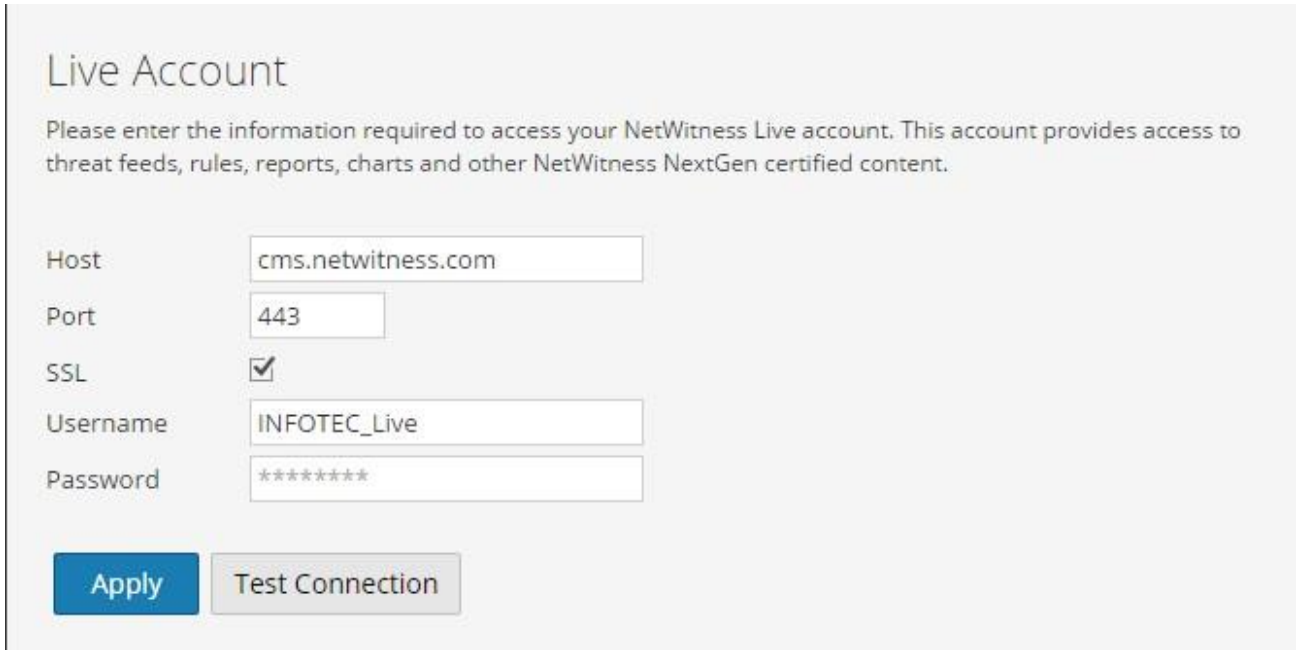


Ilustración 25. Credenciales LIVE.

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

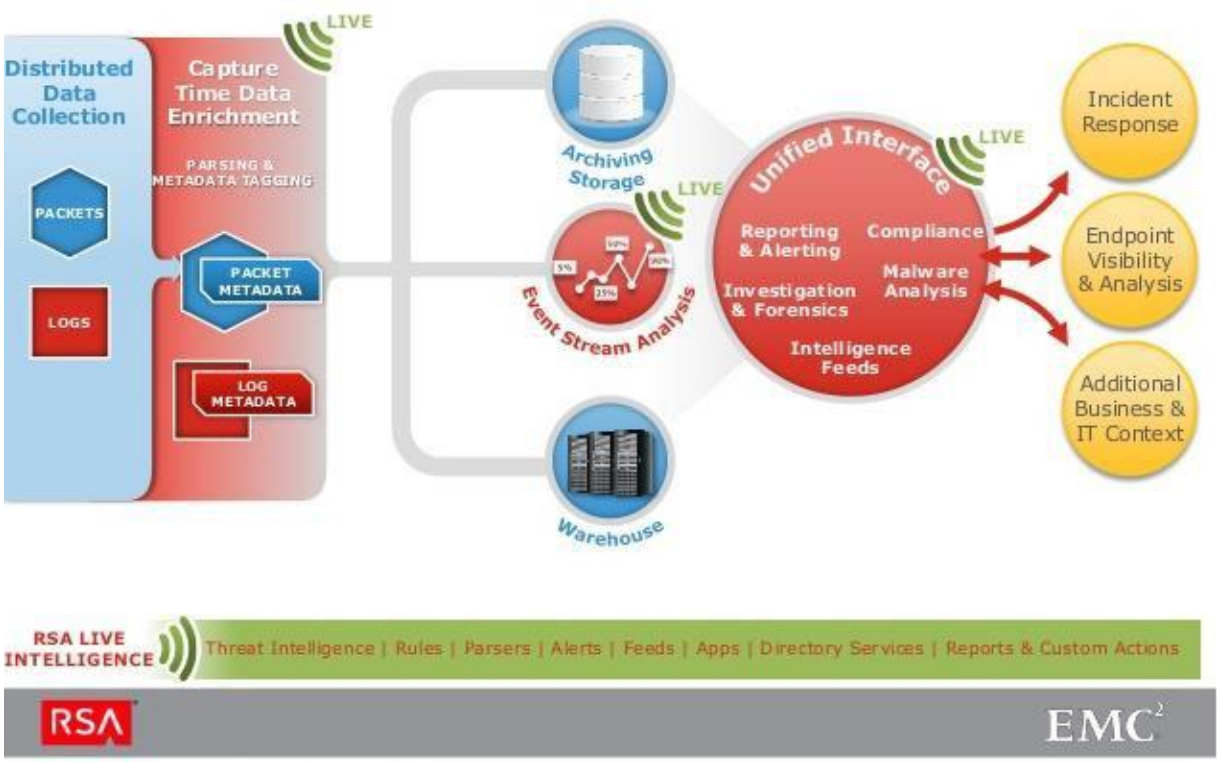


Ilustración 26. Arquitectura LIVE

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

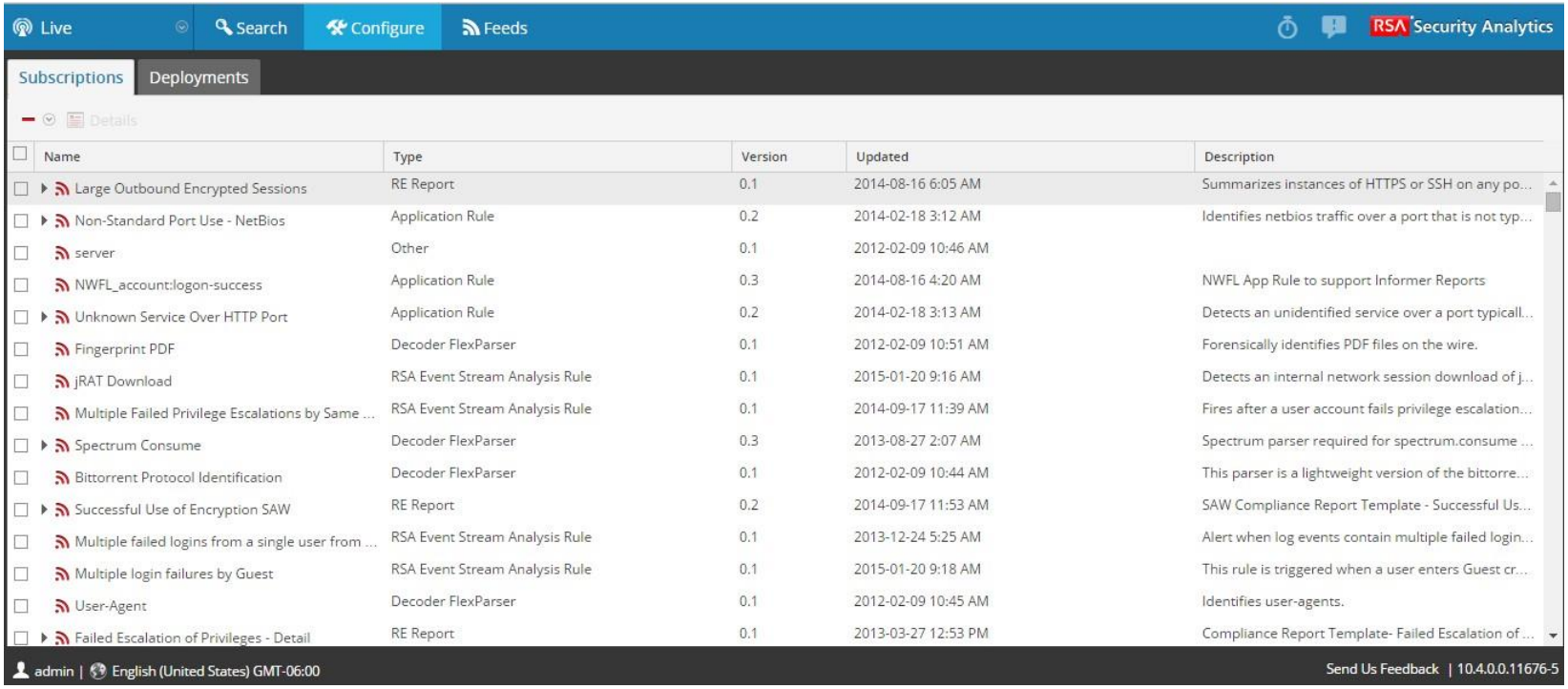


Ilustración 27. Suscripciones de LIVE.

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

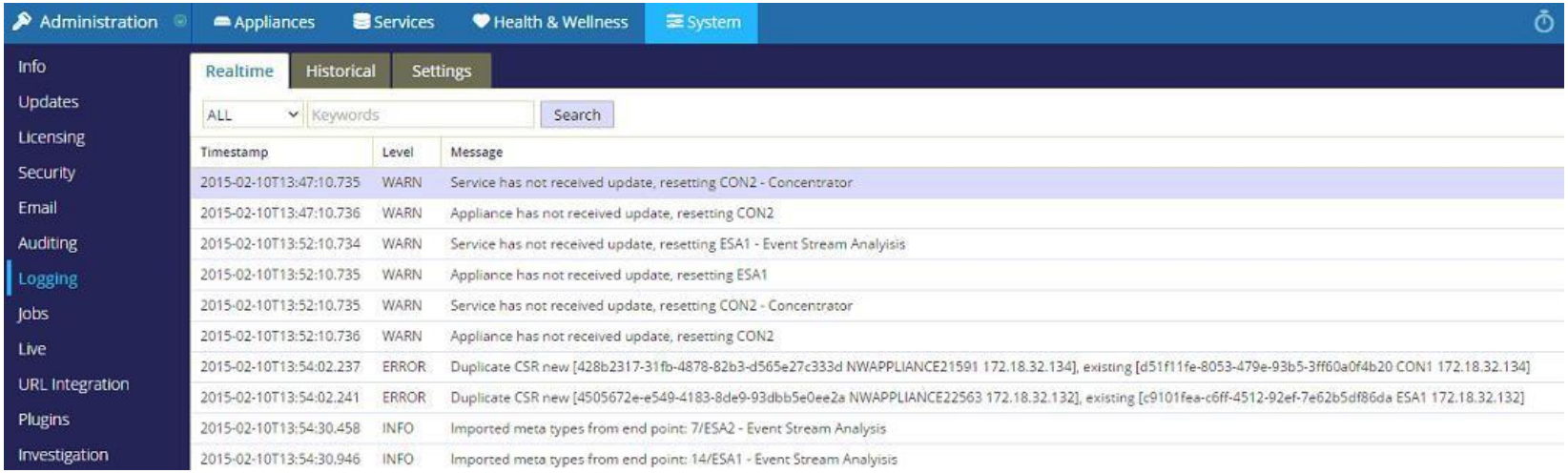


Ilustración 28. Logs de la consola.

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

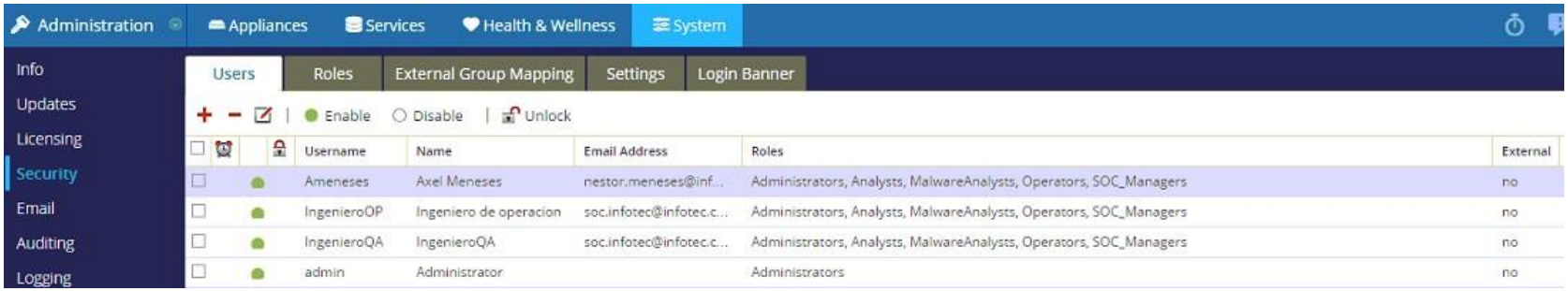


Ilustración 29. Usuarios del Security Analytics.

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

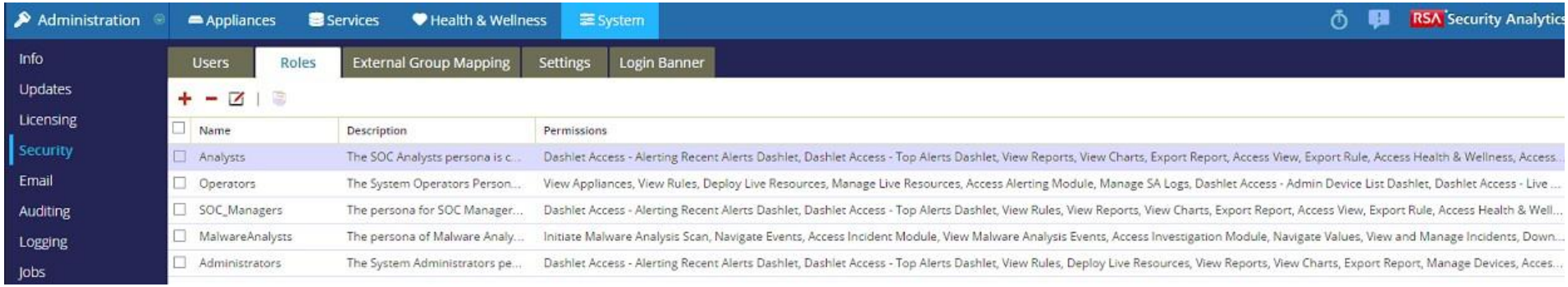


Ilustración 30. Roles de usuarios del Security Analytics.

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
Analytics Serverw/10 Users - S/W Only	132002356	30553357	31/12/2015	RSA NetWitness	SA-SERVER-SW	smcSA_Server 2015.1231	10.4.0.0.11676-5
Analyst Seat	132002356	30553357	31/12/2015	RSA NetWitness	Other	smcAnalyst_Seat 2015.1231 (10)	10.4.0.0.11676-5
Broker	132002356	30553357	31/12/2015	RSA NetWitness	Other	smcBroker 2015.1231	10.4.0.0.11676-5
SecAnlytics Log Decoder S/W	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
SecAnlytics Log Decoder S/W	132300074	30553357	31/12/2015	RSA NetWitness	SA-L-DEC-SW	smcLogDecoder 2012.1231	10.4.0.0.11676-5
SecAnlytics Log Cncntrtr S/W	133100069	30553357	31/12/2015	RSA NetWitness	SA-L-CON-SW	smcConcentrator 2012.1231	10.4.0.0.11676-5
SecAnlytics Log Cncntrtr S/W	133100070	30553357	31/12/2015	RSA NetWitness	SA-L-CON-SW	smcConcentrator 2012.1231	10.4.0.0.11676-5
Event Stream Analysis Software Offering	138145014	30553357	31/12/2015	RSA NetWitness	SA-ESA-SW	smcEventStream Analisys 2015.1231	10.4.0.0.11676-5
Event Stream Analysis Software Offering	138145015	30553357	31/12/2015	RSA NetWitness	SA-ESA-SW	smcEventStream Analisys 2015.1231	10.4.0.0.11676-5
25TB Cpcty4logs S/W	133700006	30553357	31/12/2015	RSA NetWitness	SA-25TB-CAP-L-SW	smcLog_Capacity 2015.1231 (25)	10.4.0.0.11676-5
25TB Cpcty4logs S/W	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.

Ilustración 31. Creación del Servidor de Licencias.

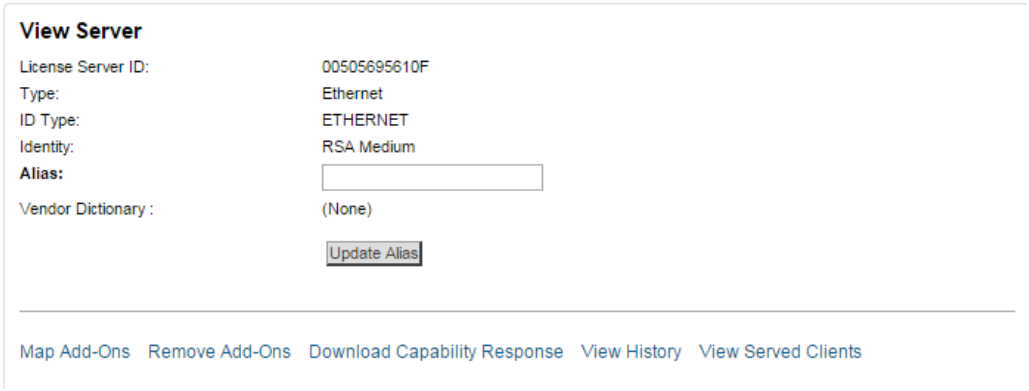


Ilustración 32. Servidor de Licencias creado.

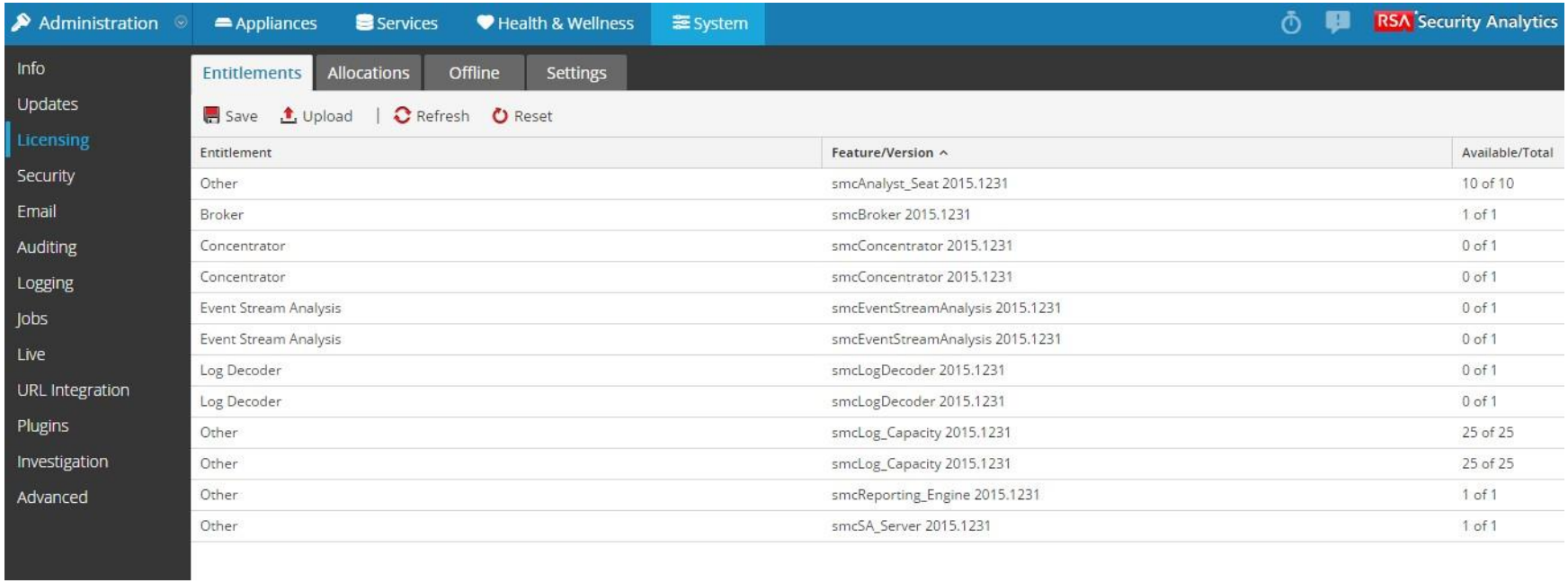
Una vez creado dicho servidor se procede a mapear las licencias para nuestro Security Analytics.

Add-Ons

Add-On Name	Status	Serial Number	Units Mapped	Expiration	Downloadable Items
Analytics Server w/10 Users - S/W Only	License not generated	132002356	1	Permanent	View
SecAnlytics Log Decoder S/W	License not generated	132300073	1	Permanent	View
SecAnlytics Log Decoder S/W	License not generated	132300074	1	Permanent	View
SecAnlytics Log Cncntrtr S/W	License not generated	133100069	1	Permanent	View
SecAnlytics Log Cncntrtr S/W	License not generated	133100070	1	Permanent	View
SecAnalytics ESA S/W	License not generated	138145014	1	Permanent	View
SecAnalytics ESA S/W	License not generated	138145015	1	Permanent	View
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.

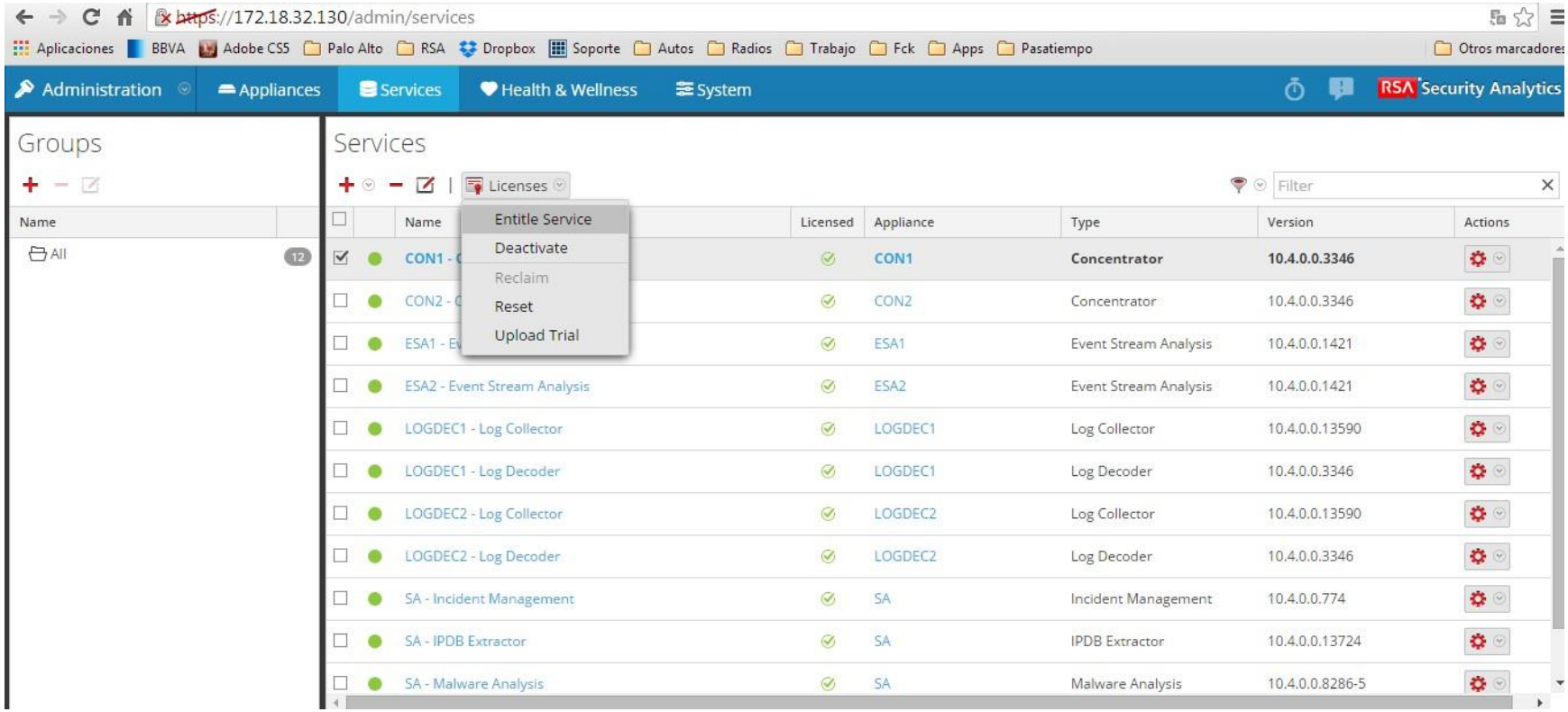


Ilustración 35. Licenciamiento de Entidades.

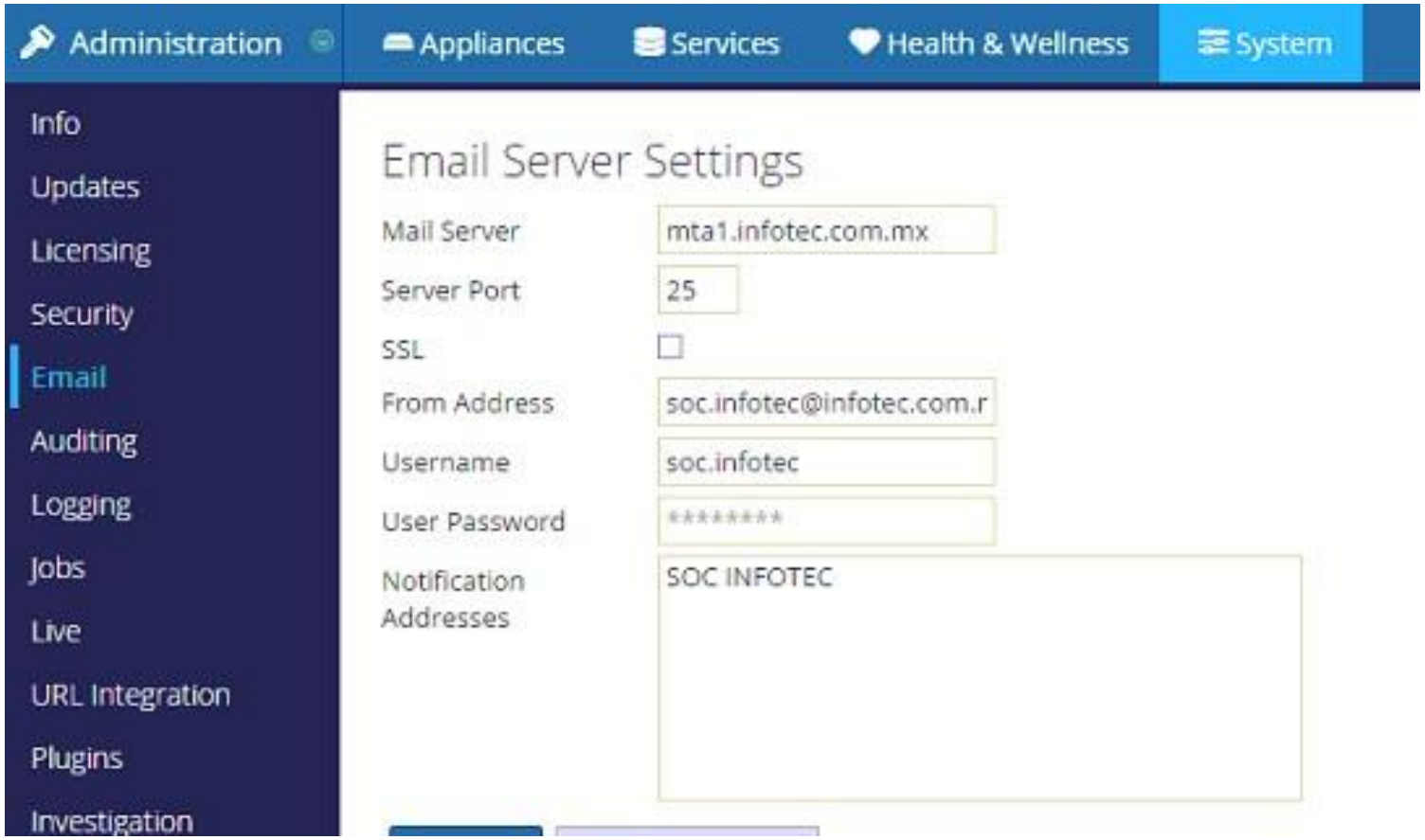


Ilustración 36. Configuración de email.

3. CONFIGURACIÓN DE ENTIDADES

3.1 Concentrator 1

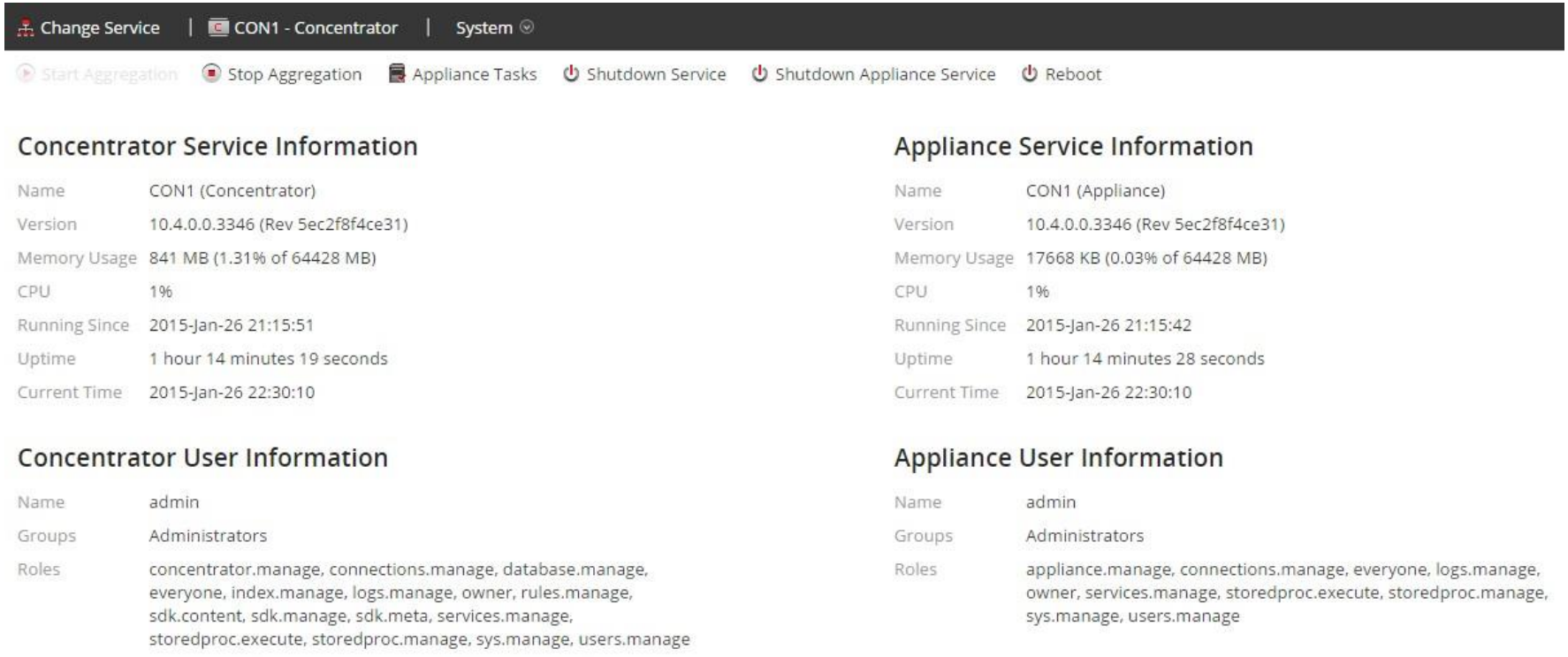


Ilustración 37. Información del Concentrator 1.

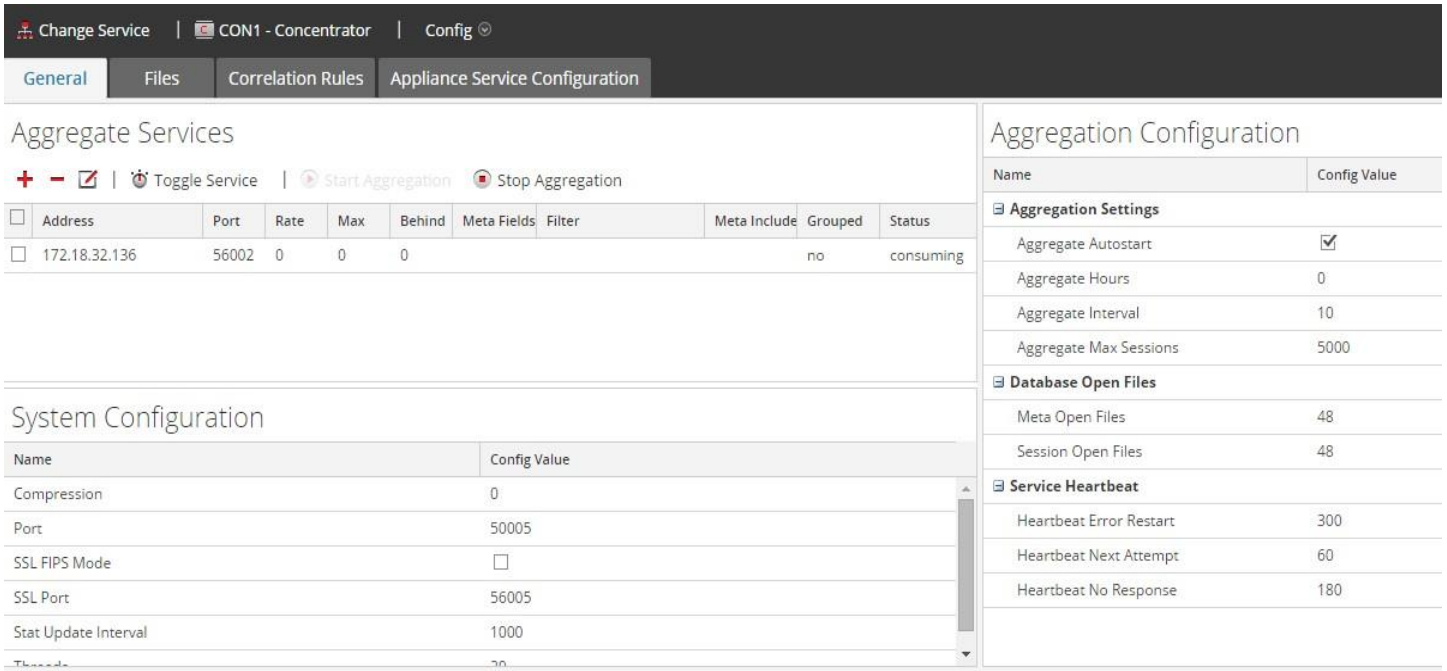


Ilustración 38. Configuración del Concentrator 1.

Ilustración 39. Estadísticas del Concentrator 1.

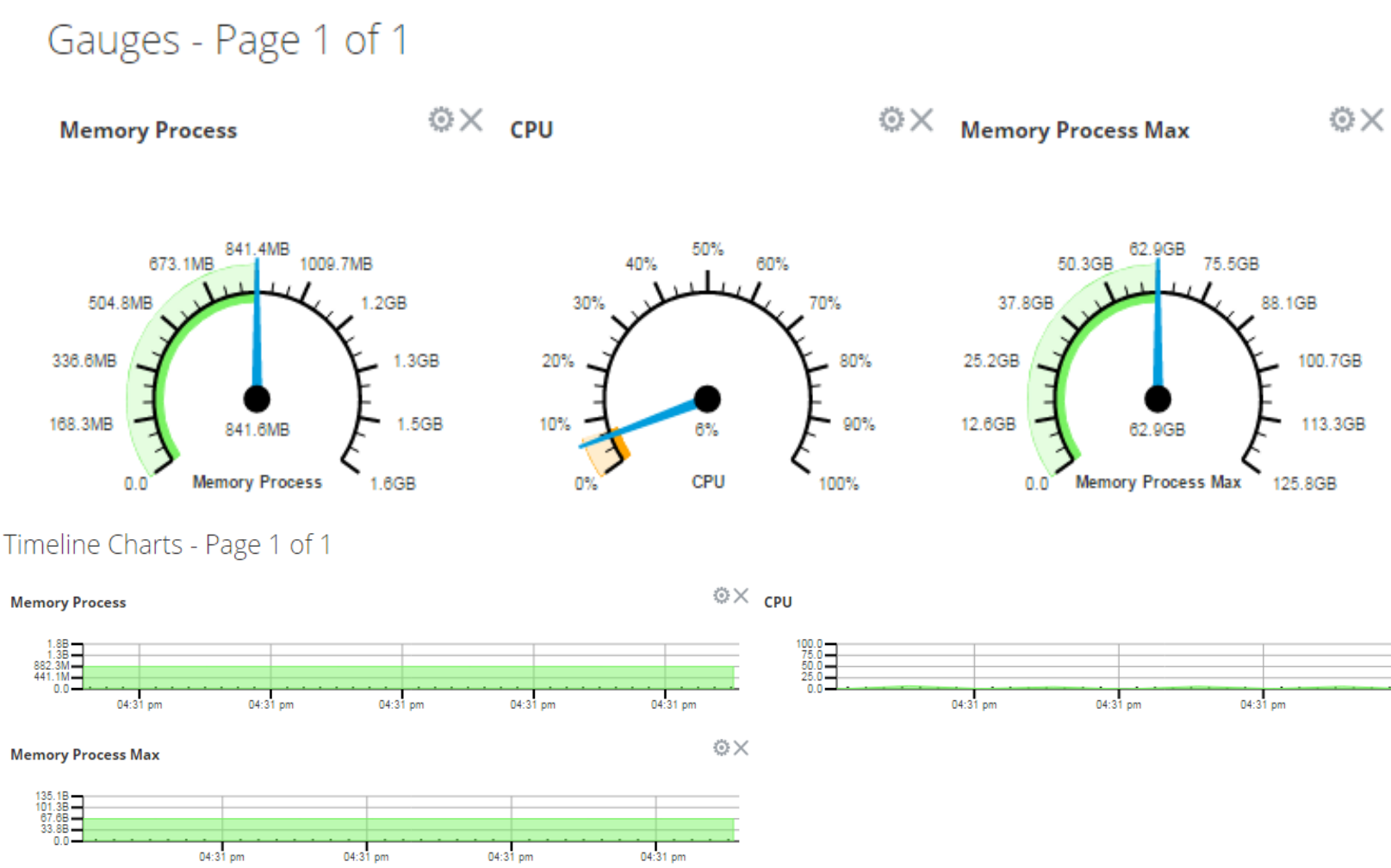


Ilustración 40. Estadísticas del Concentrator 1 de forma gráfica.

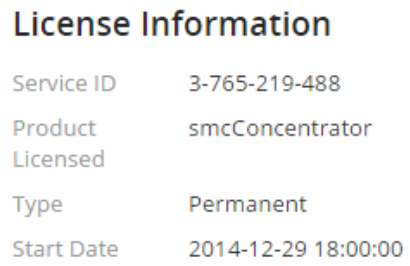


Ilustración 41. Licencia del Concentrator 1.

3.2 Concentrator 2

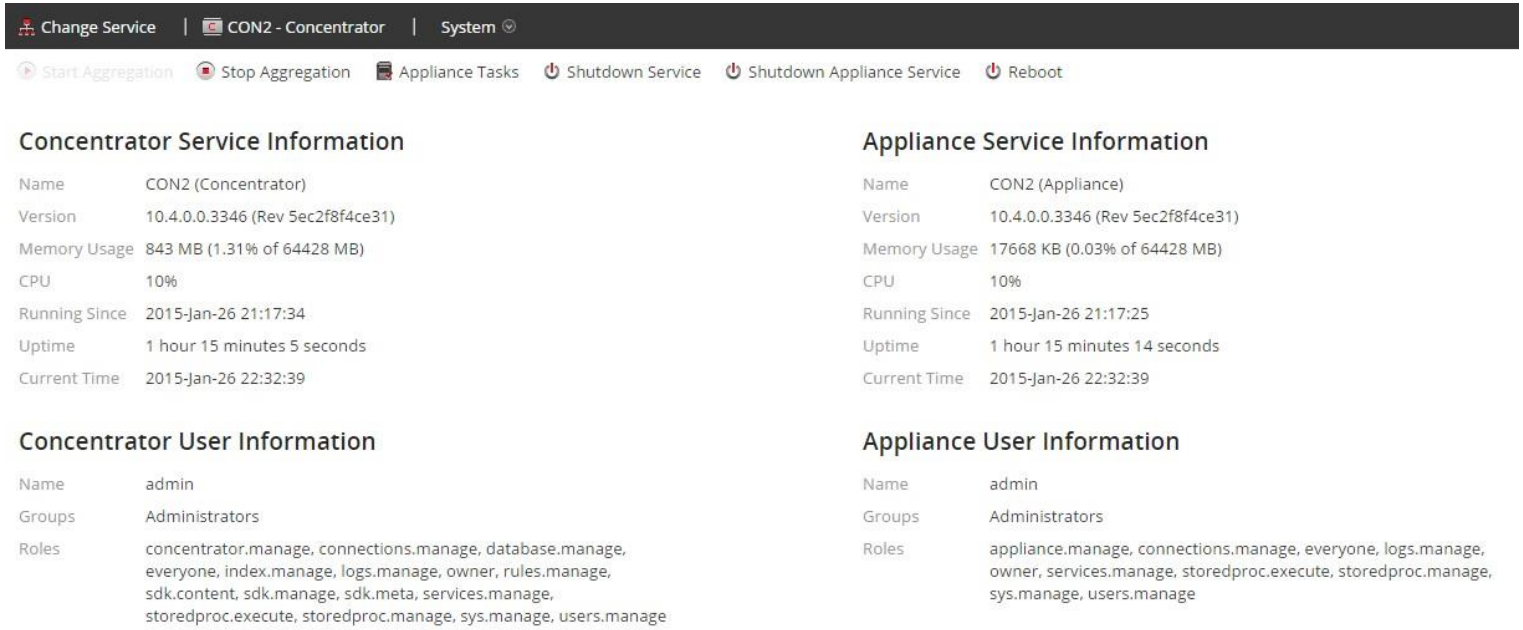


Ilustración 42. Información del Concentrator 2.

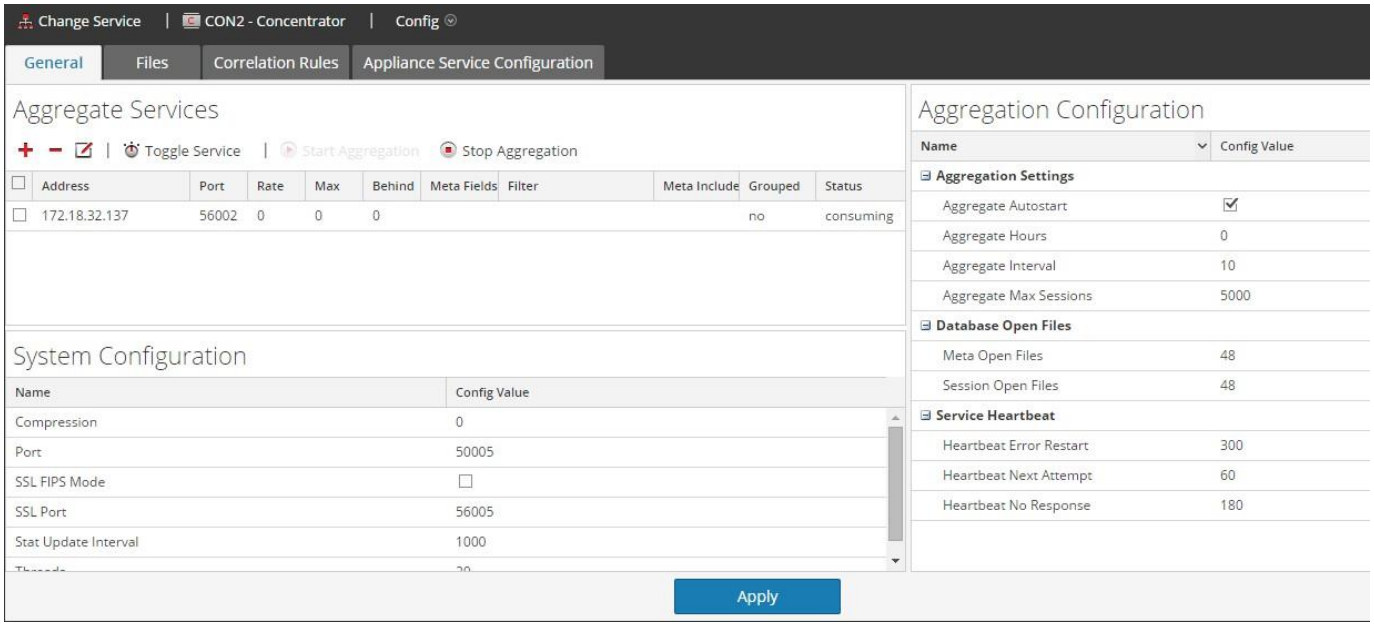


Ilustración 43. Configuración del Concentrator 2.

Ilustración 44. Estadísticas del Concentrator 2.

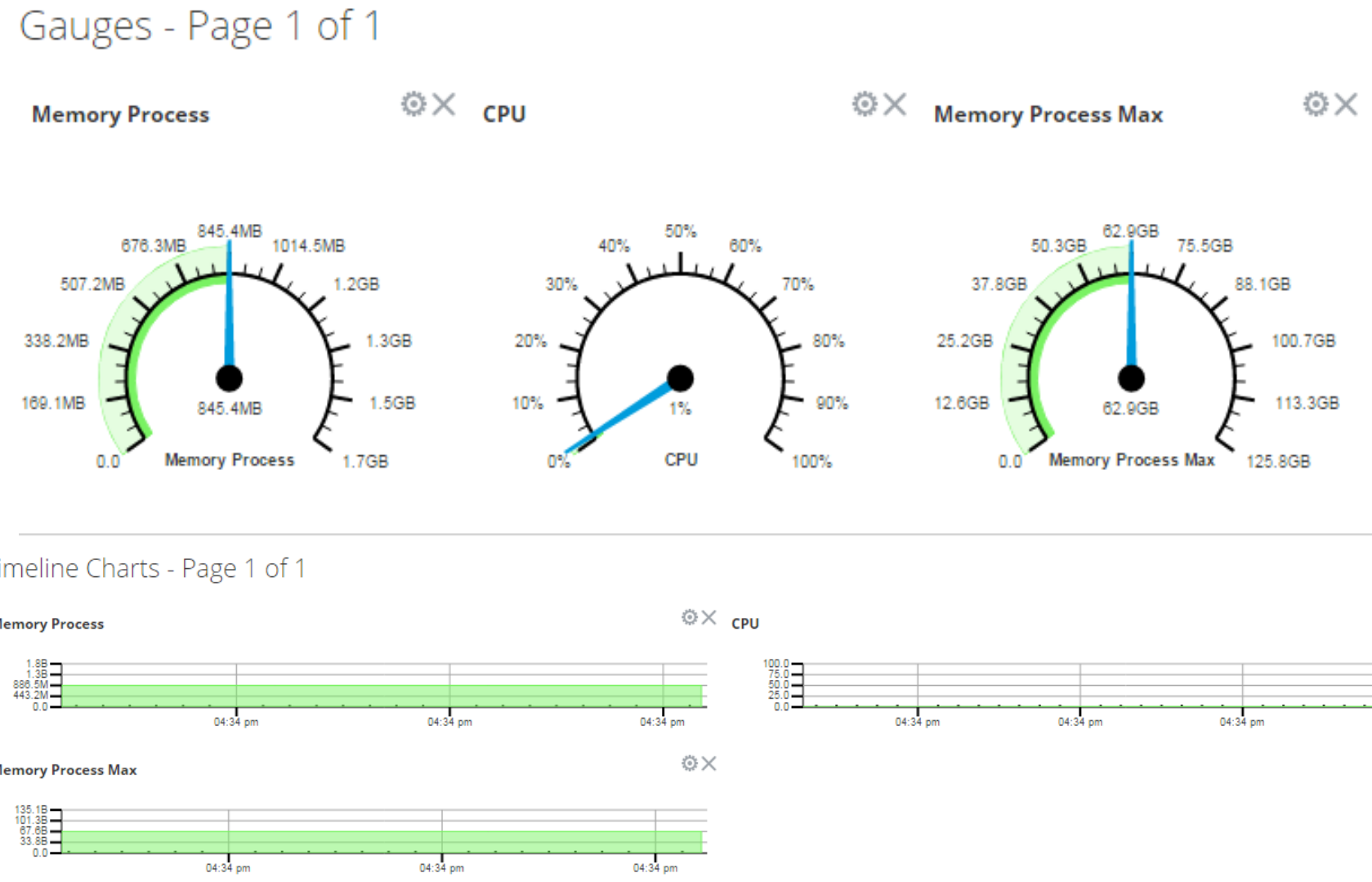


Ilustración 45. Estadísticas del Concentrator 2 de forma gráfica.

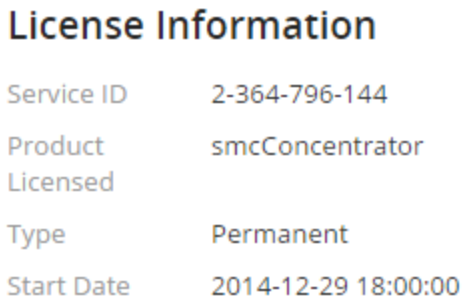


Ilustración 46. Licencia del Concentrator 2.

3.3 Log Decoder 1

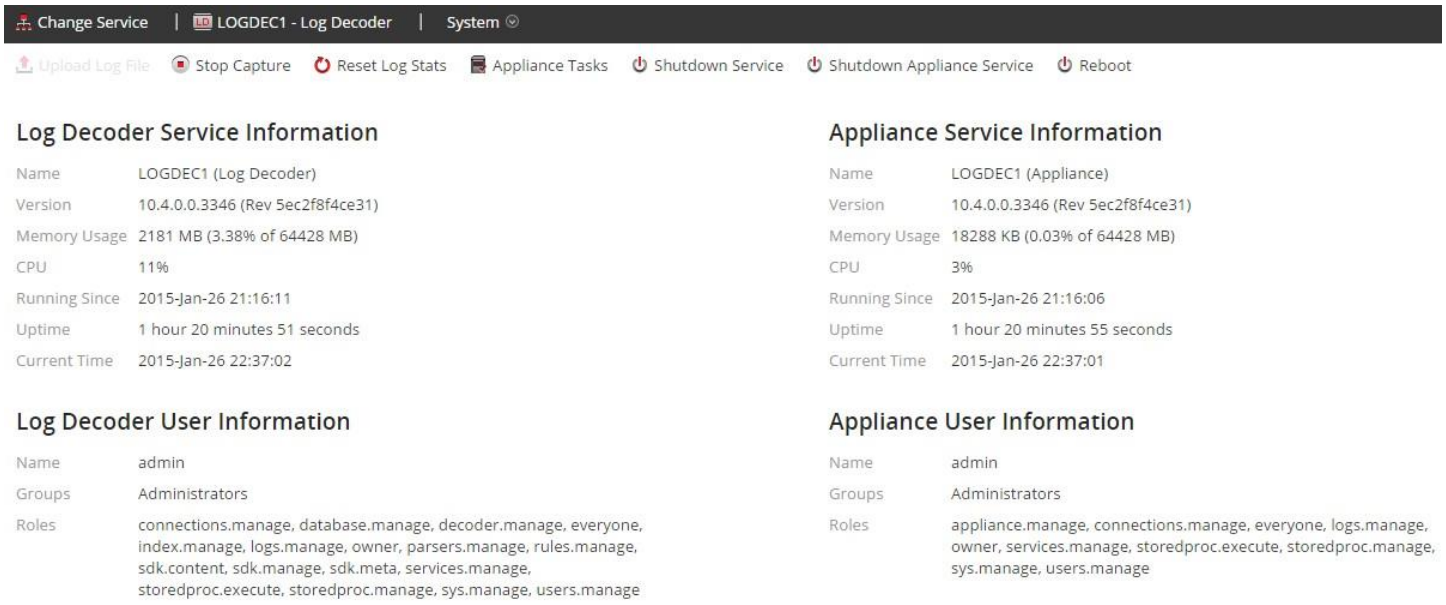


Ilustración 47. Información del Log Decoder 1.

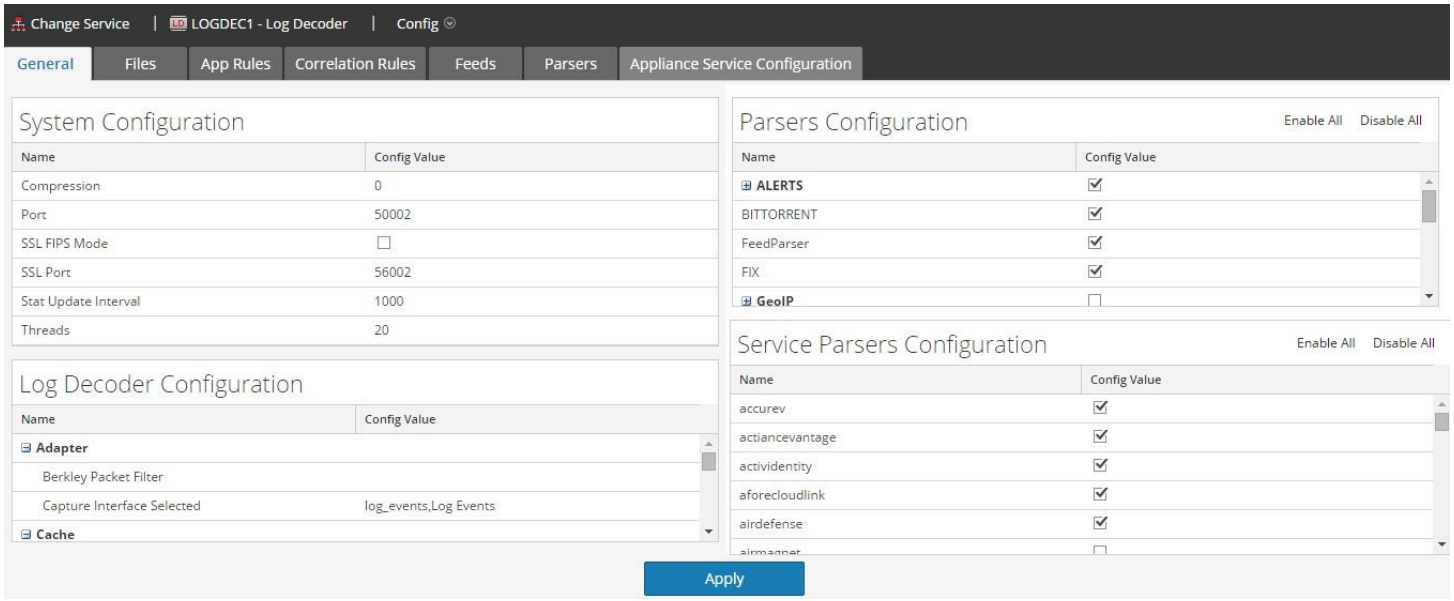


Ilustración 48. Configuración del Log Decoder 1.

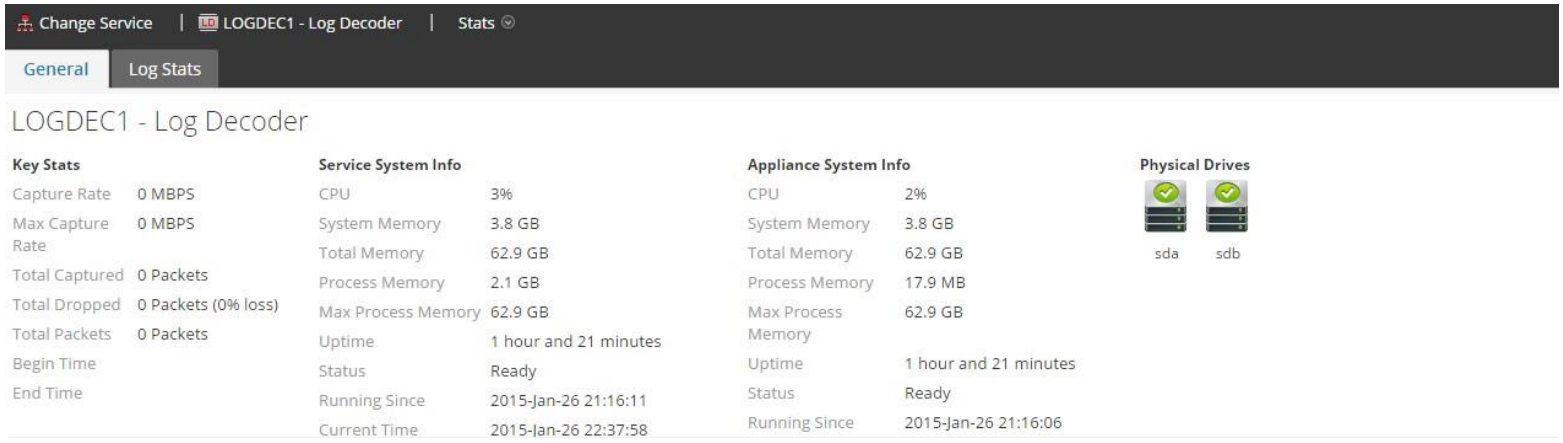


Ilustración 49. Estadísticas del Log Decoder 1.

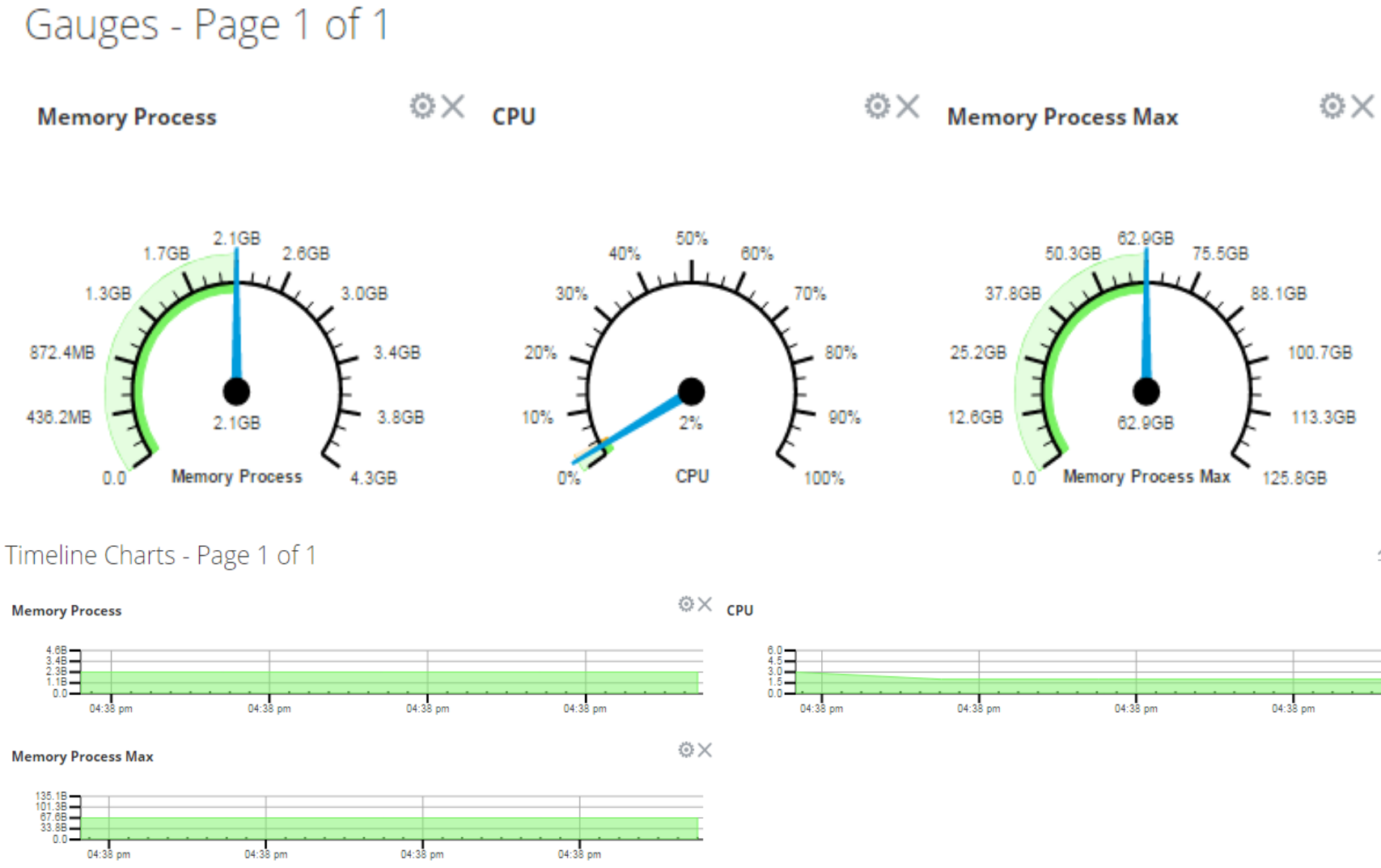
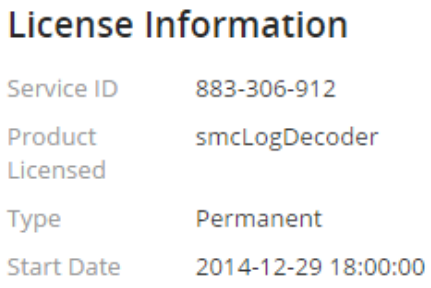


Ilustración 50. Estadísticas del Log Decoder 1 de forma gráfica.

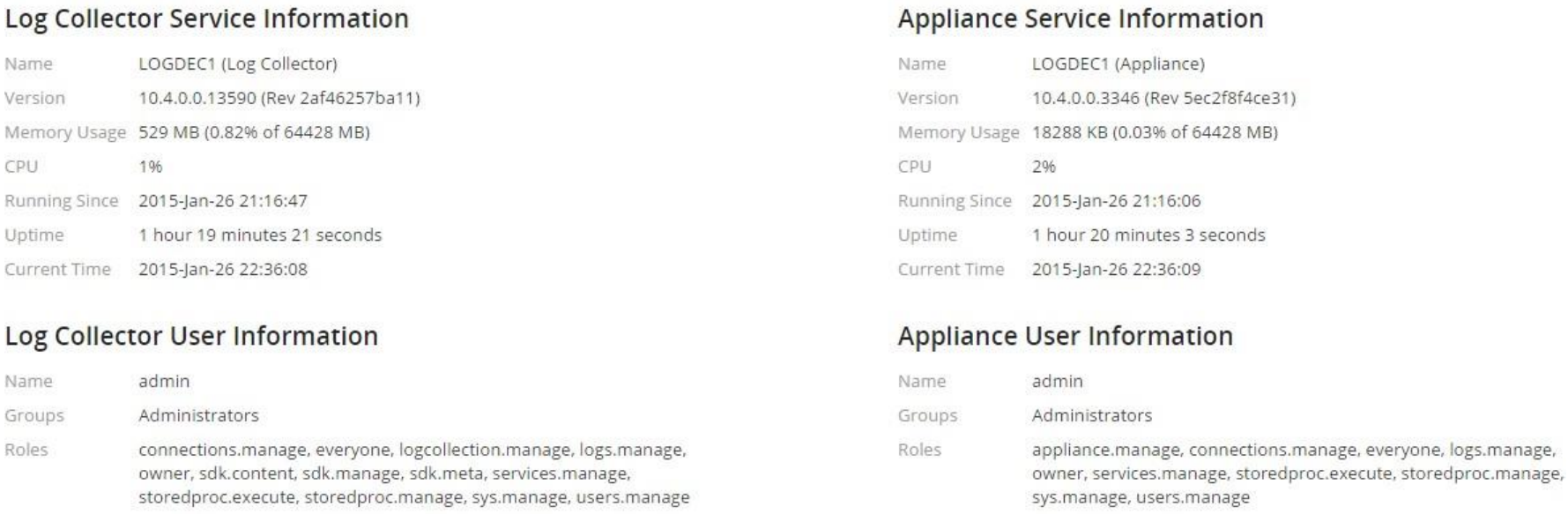


License Information

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

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

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 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

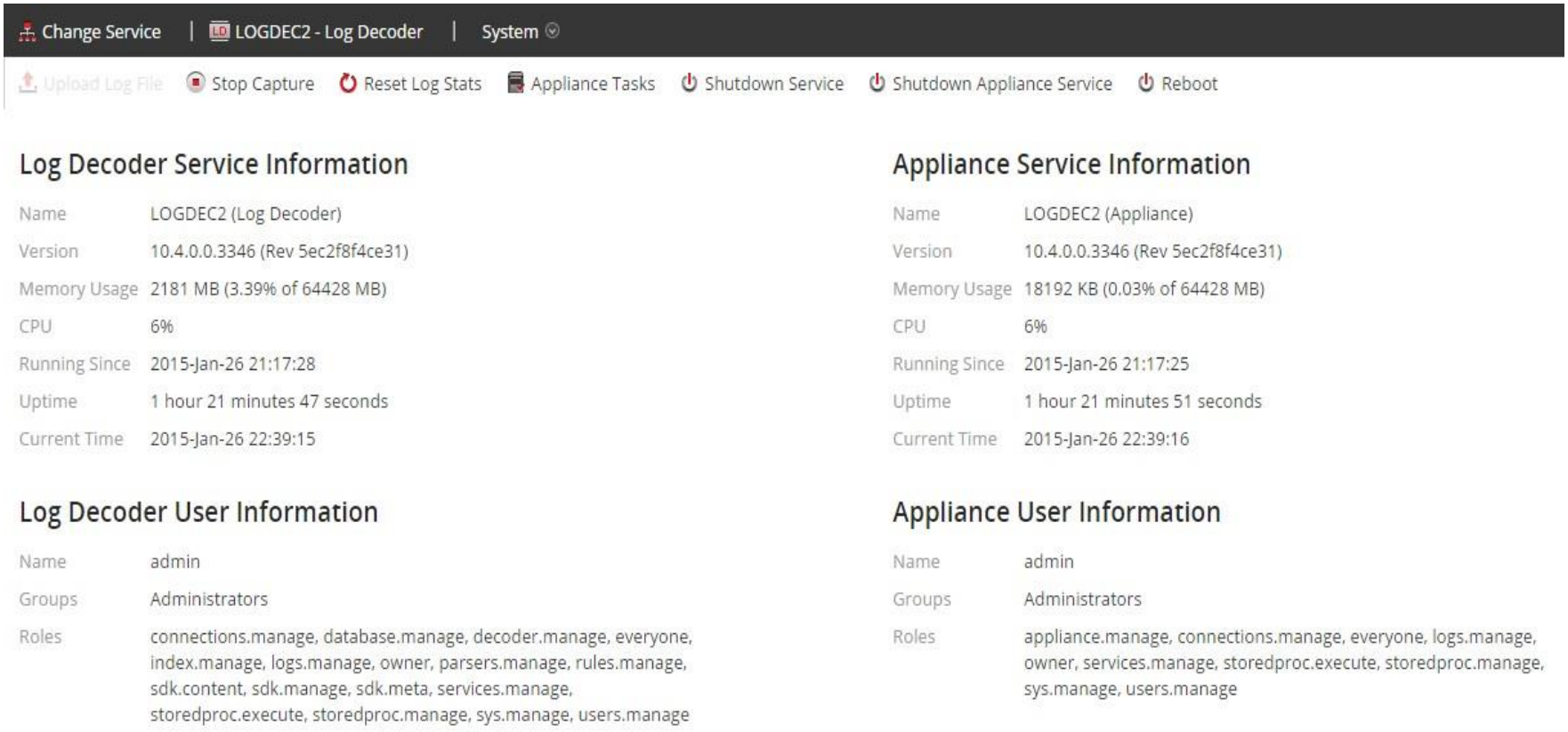


Ilustración 53. Información del Log Decoder 2.

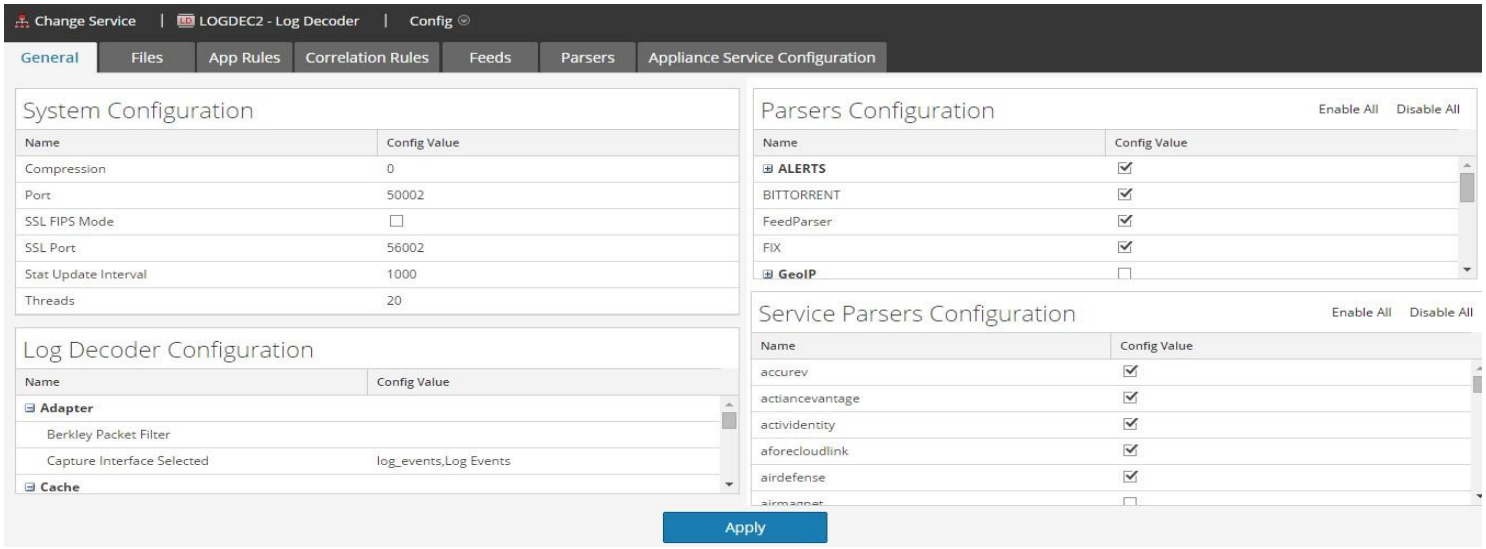


Ilustración 54. Configuración del Log Decoder 2.

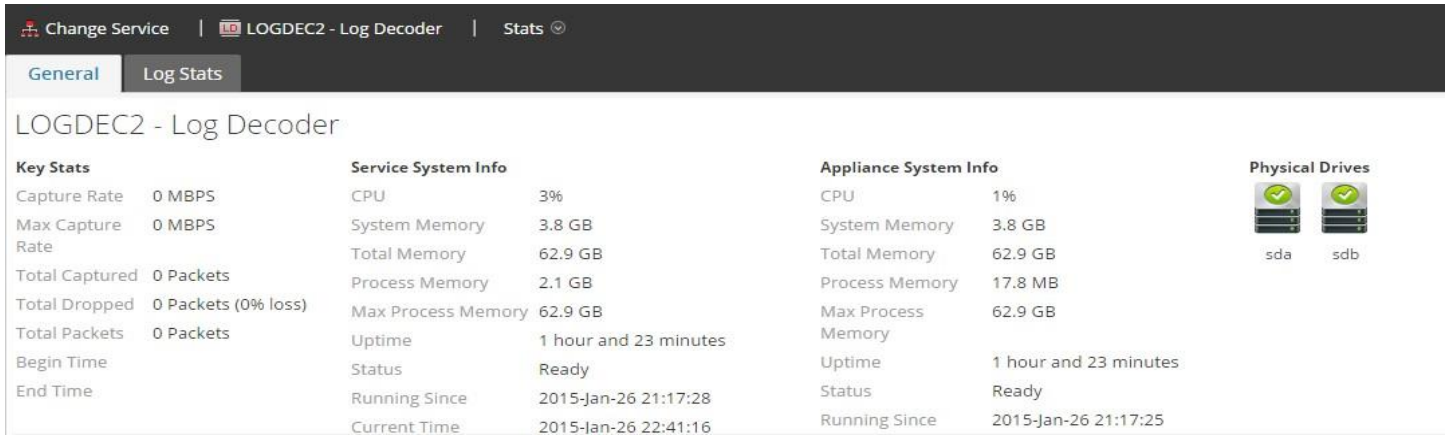


Ilustración 55. Estadísticas del Log Decoder 2.

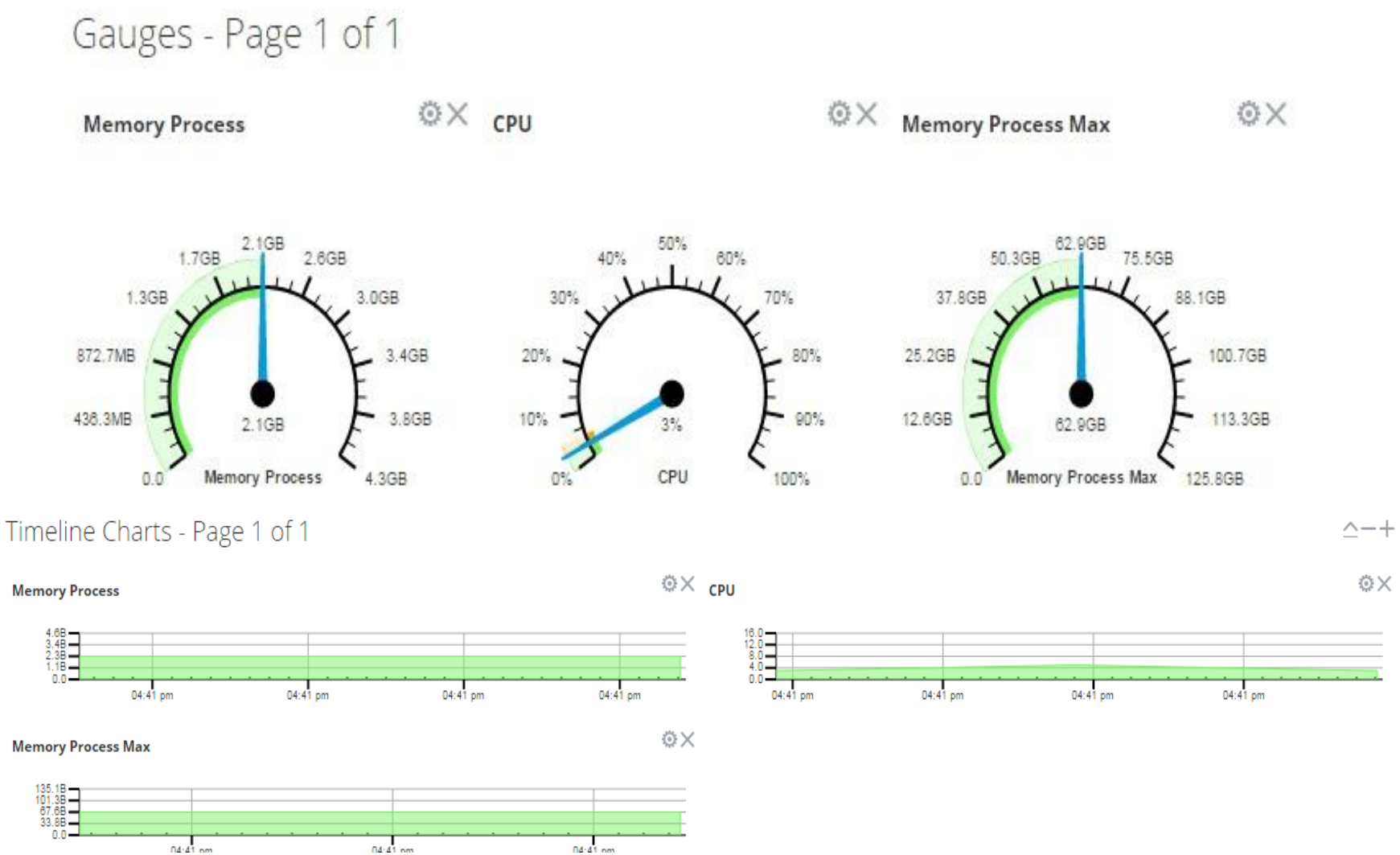


Ilustración 56. Estadísticas del Log Decoder 2 de forma gráfica.

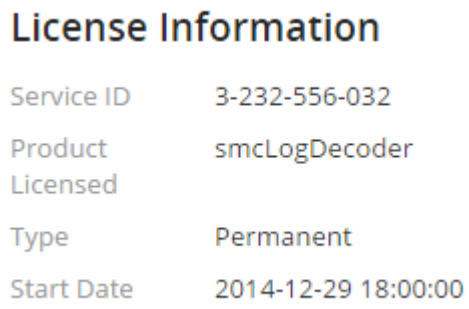


Ilustración 57. Licencia del Log Decoder 2.

3.6 Log Collector 2

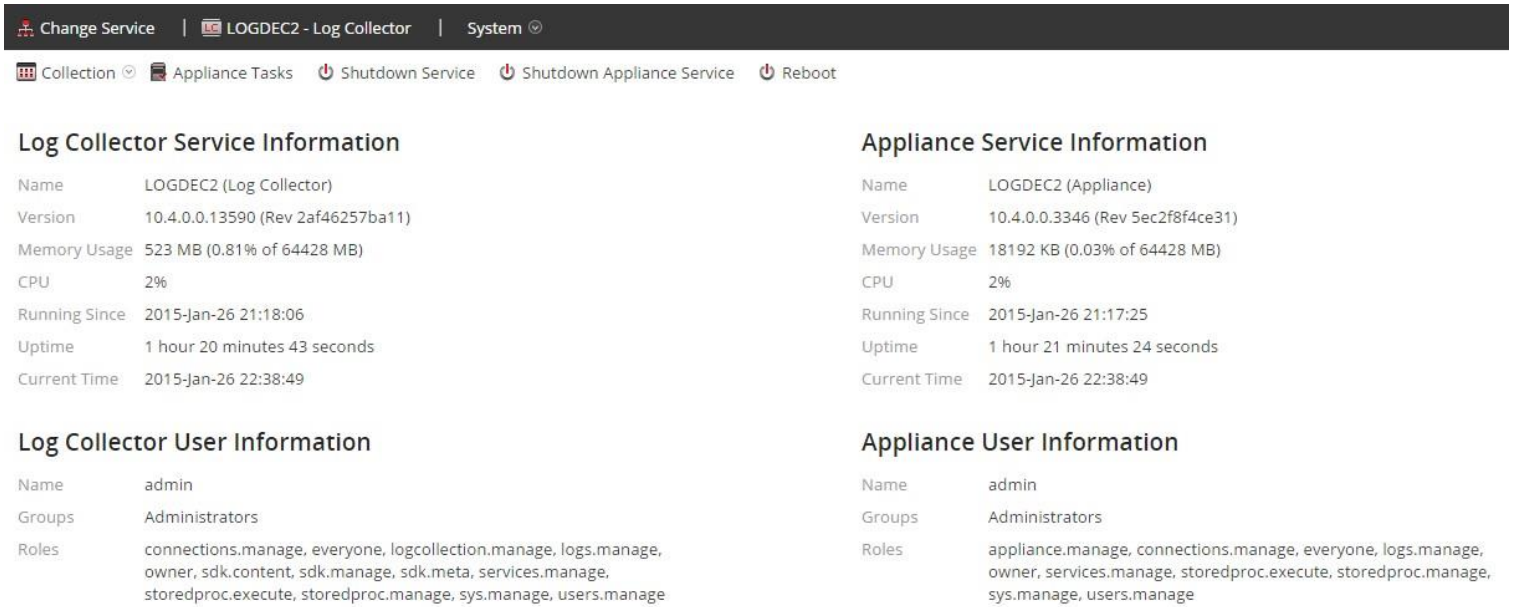


Ilustración 58. Información del Log Collector 2.

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
Fortigate 600C	v5.0,build0271 (GA Patch 6)	172.31.45.253	Syslog	fortinet
Fortigate 300C	v5.0,build0271 (GA Patch 6)	172.31.45.246	Syslog	fortinet
FortiMail 400C	v5.1,build281, 140610 (5.1.3 GA)	172.31.45.244	Syslog	fortinetfortimail
FortiMail 400C	v5.1,build281, 140610 (5.1.3 GA)	172.31.45.245	Syslog	fortinetfortimail
Windows server 2012	Exchange 2013	192.168.105.41	File, Windows	msexchange
Windows server 2012	Exchange 2013	192.168.105.42	File, Windows	msexchange
Windows server 2012	Active Directory 2012	192.168.105.50	File, Windows	msexchange
Windows server 2012	Active Directory 2012	192.168.105.60	File, Windows	msexchange
ARBOR APS2100	Pravail APS v5.5.1	192.168.80.162		Syslog
ARBOR APS2100	Pravail APS v5.5.1	192.168.80.163		Syslog
ARBOR APS2100	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

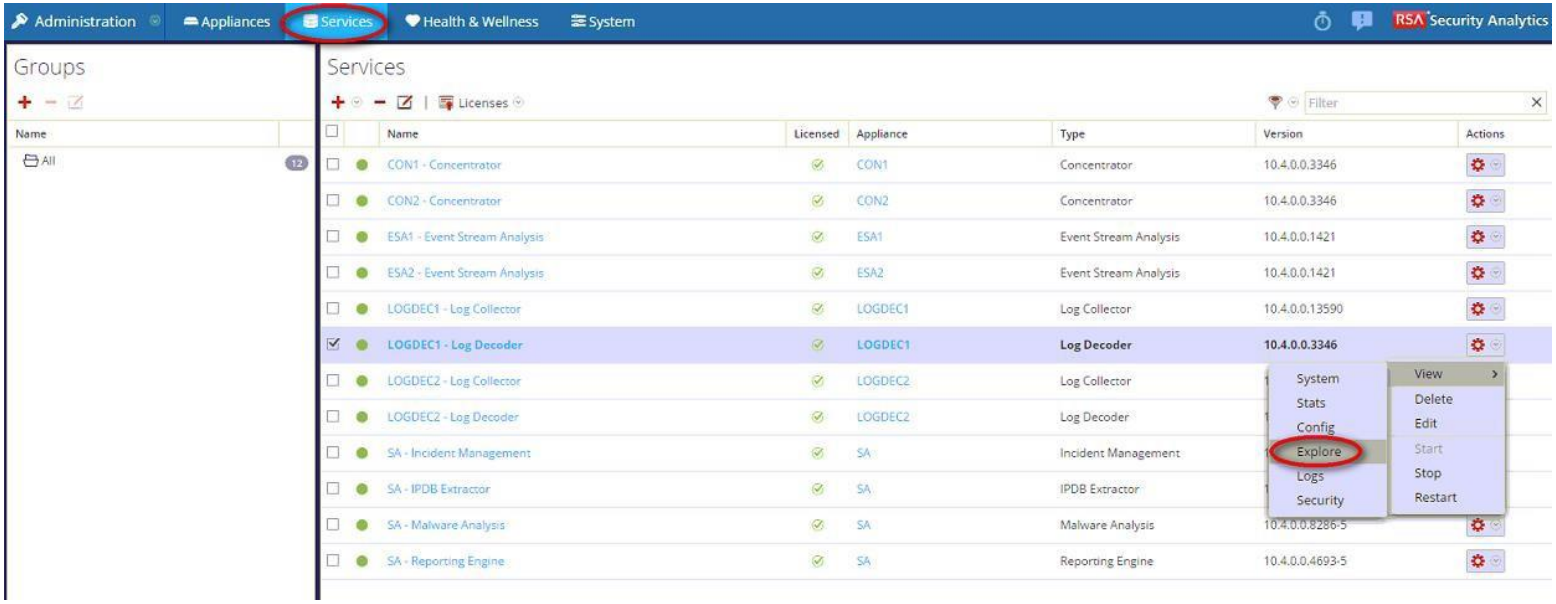


Ilustración 61. Pantalla de servicios.

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

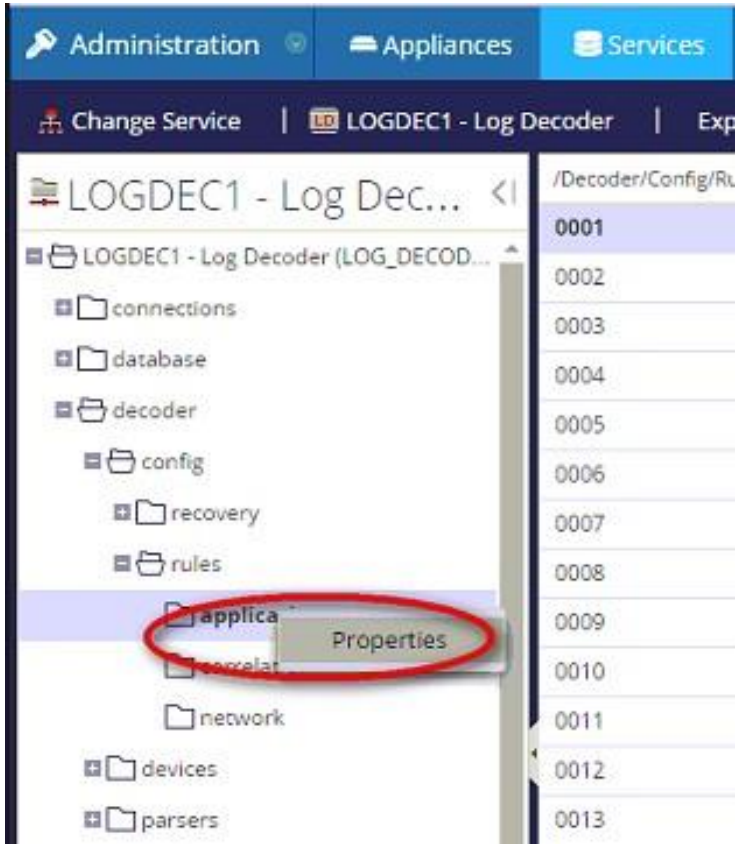


Ilustración 62. Pantalla de Exploración del Log Decoder.

c. Al dar clic en properties 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.

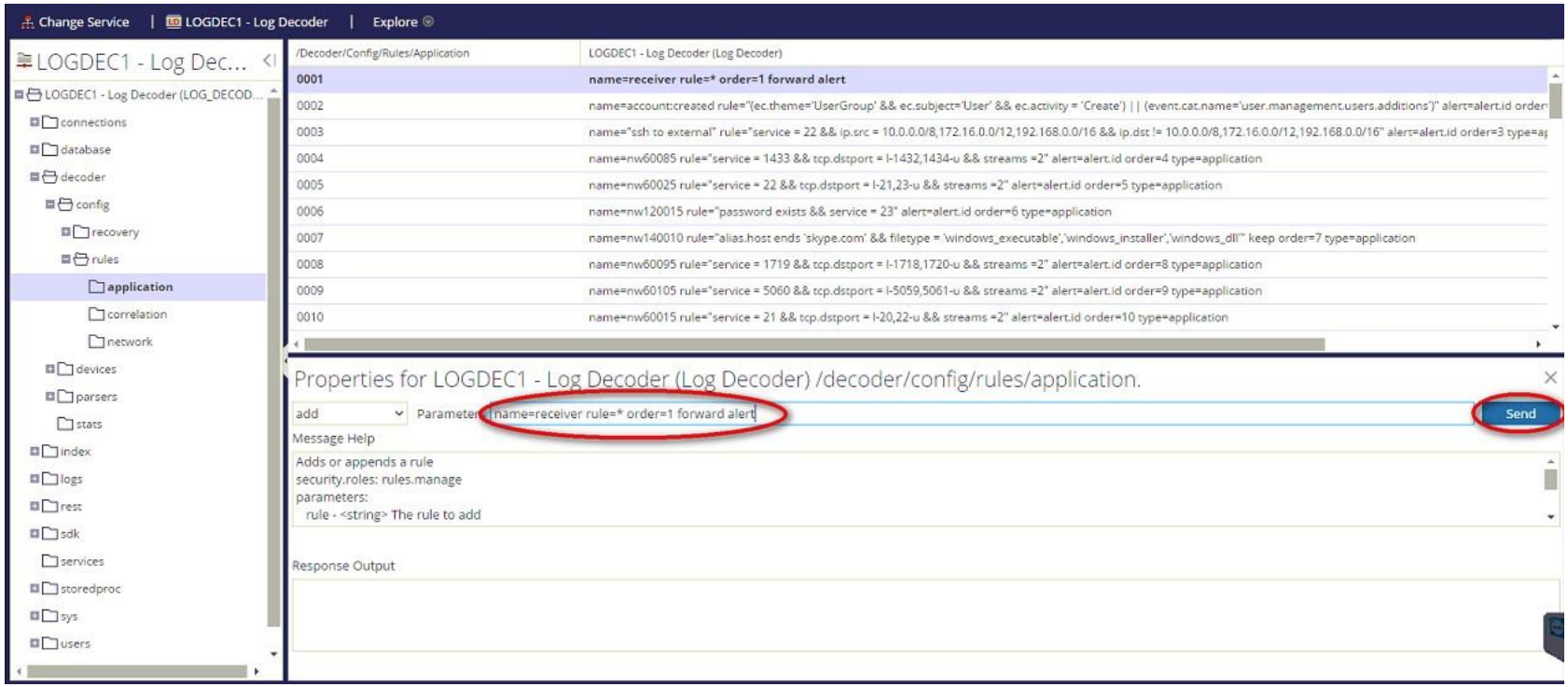


Ilustración 63. Configuración de la regla de aplicación.

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

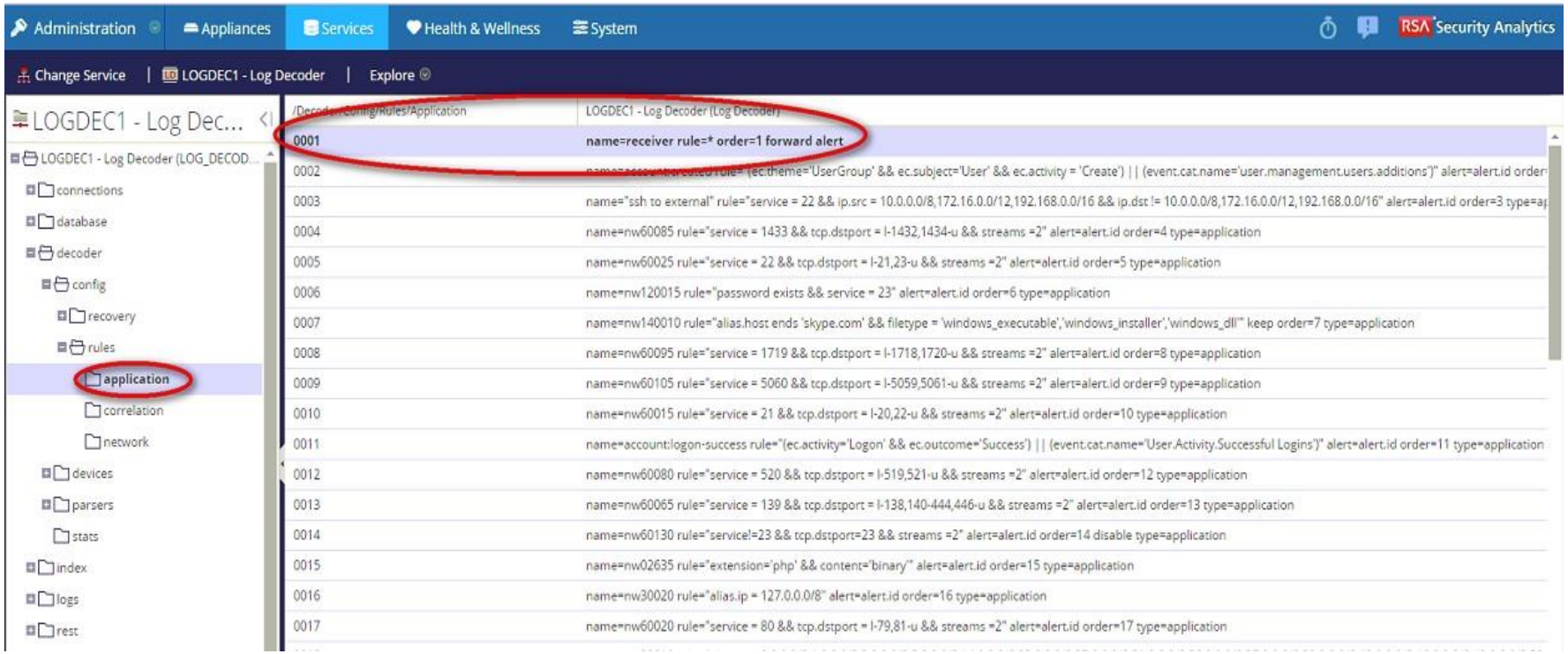


Ilustración 64. Reglas de aplicación existentes.

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"**

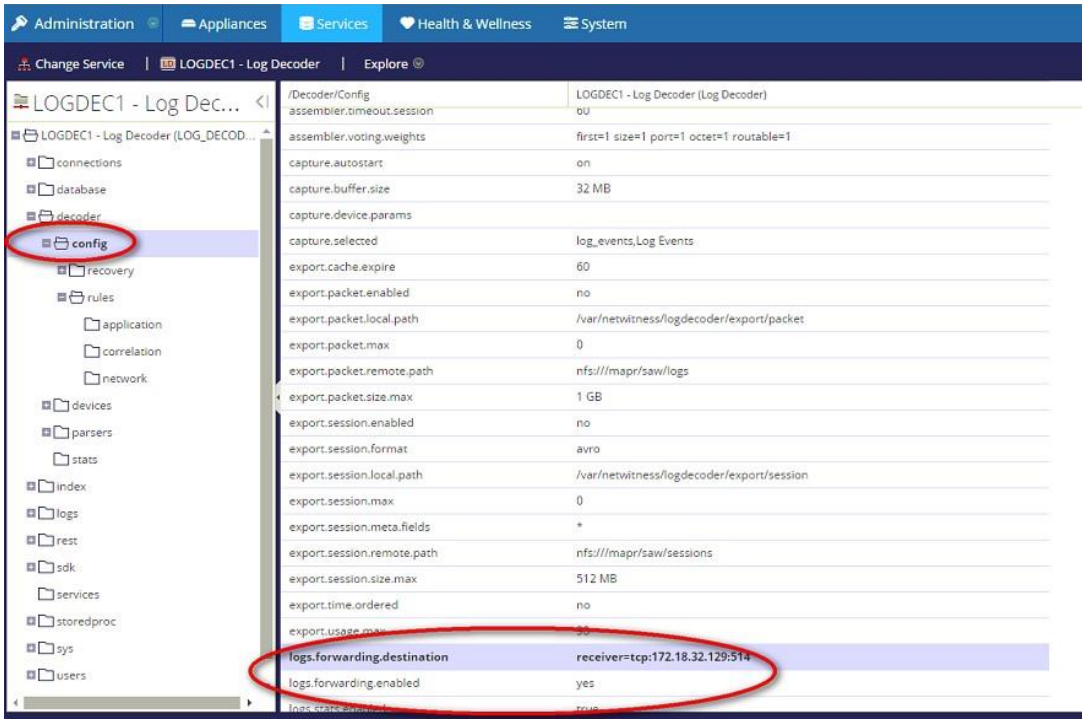


Ilustración 65. Sección de configuración del Log Decoder.

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

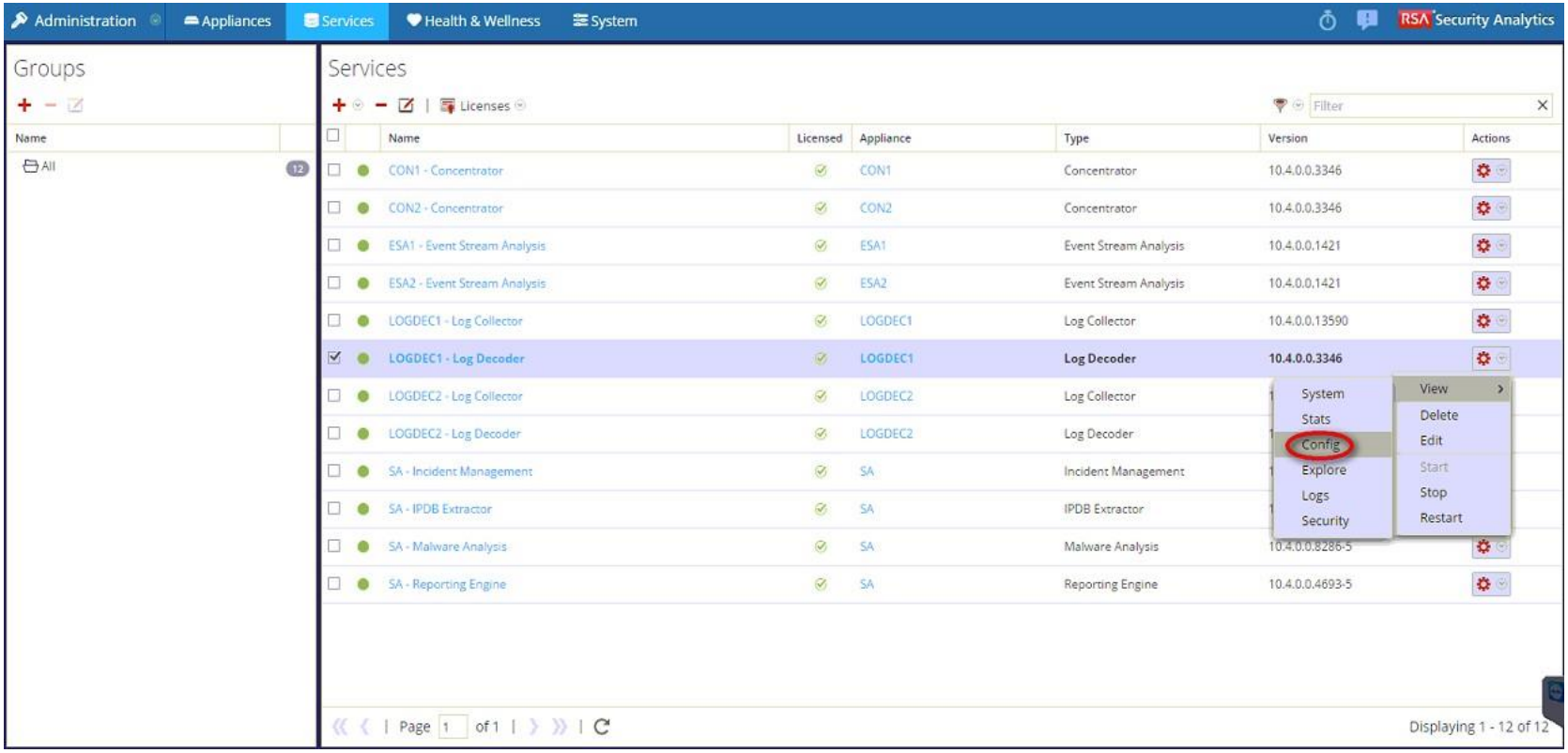


Ilustración 66. Pantalla de Servicios.

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

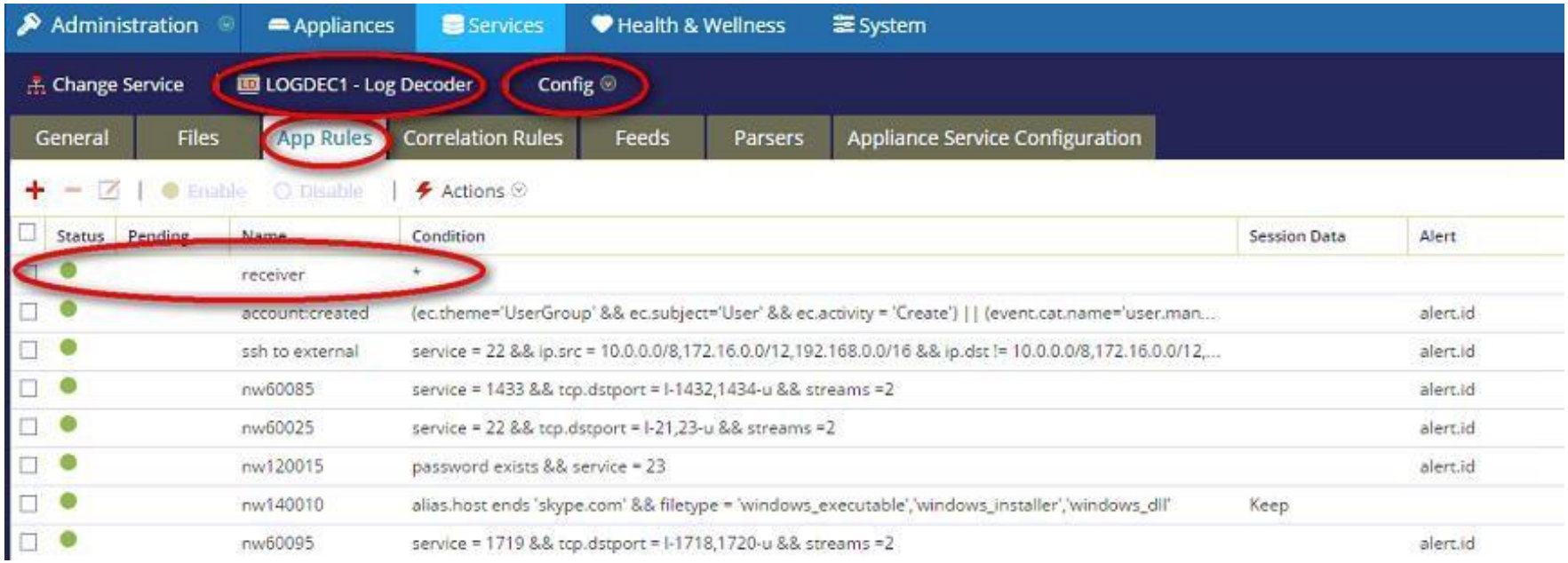


Ilustración 67. Pantalla de Configuración del Log Decoder.

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.**

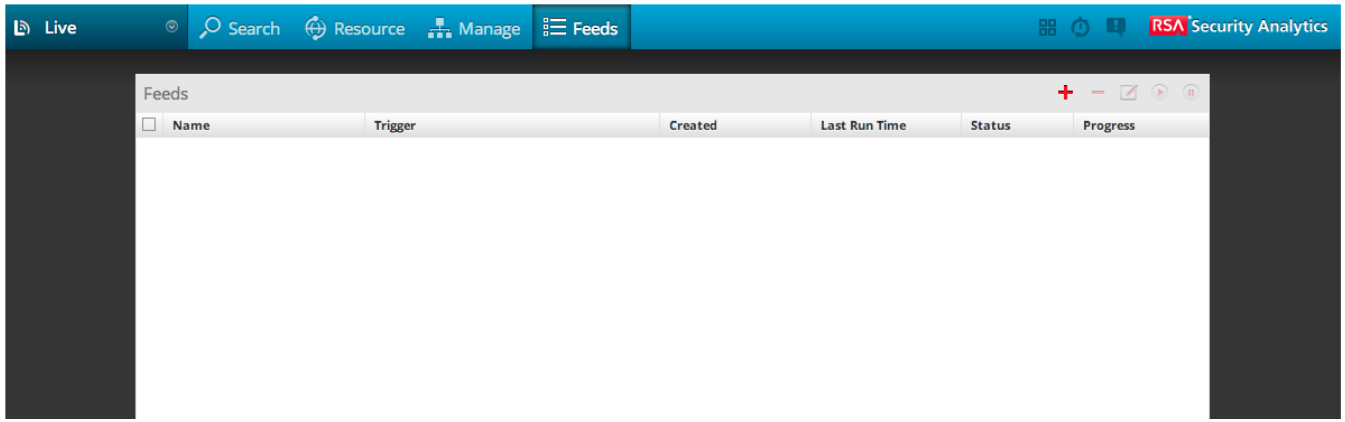


Ilustración 68. Feeds que se tienen actualmente.

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.

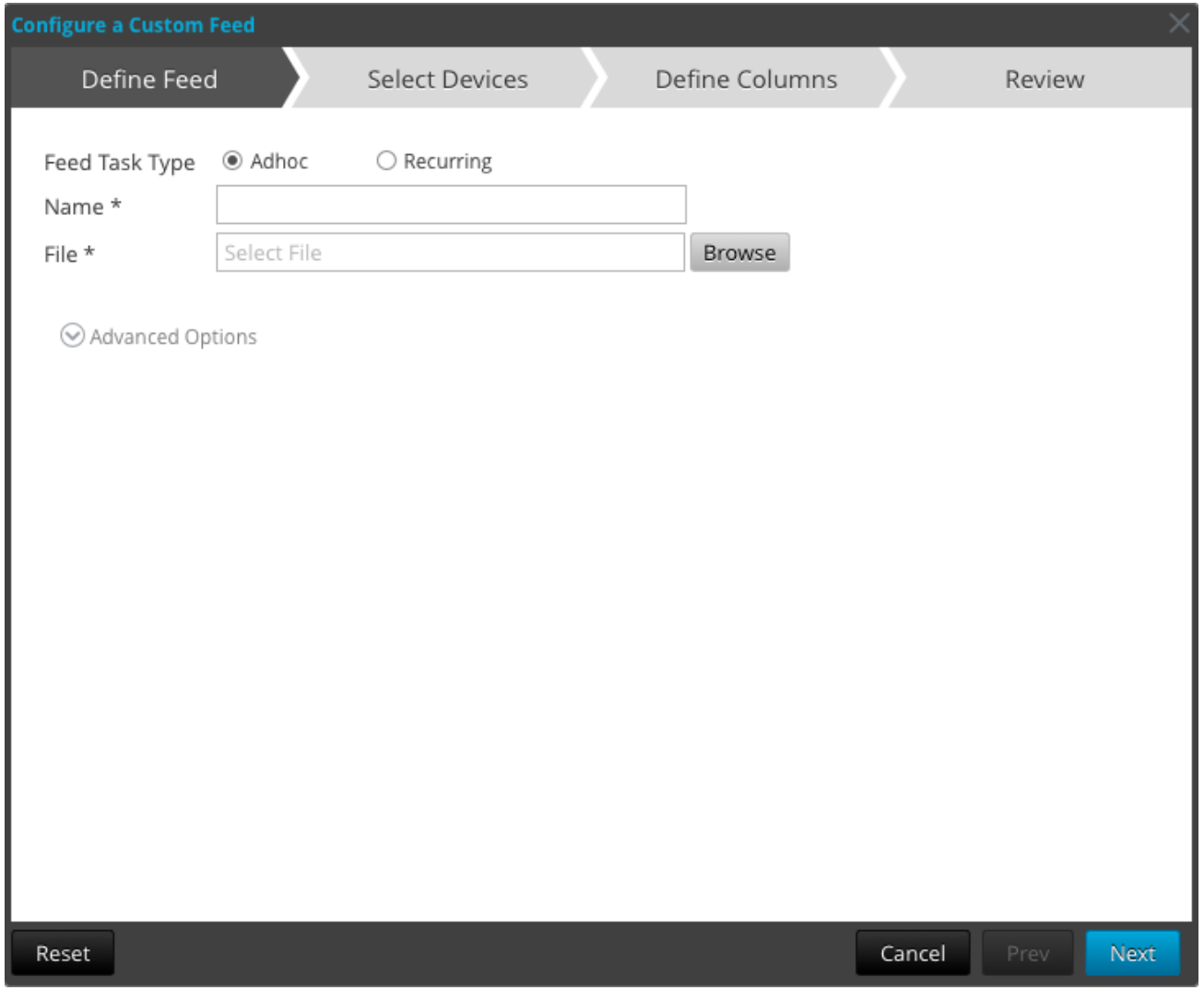


Ilustración 70. Pantalla de configuración de feeds.

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)

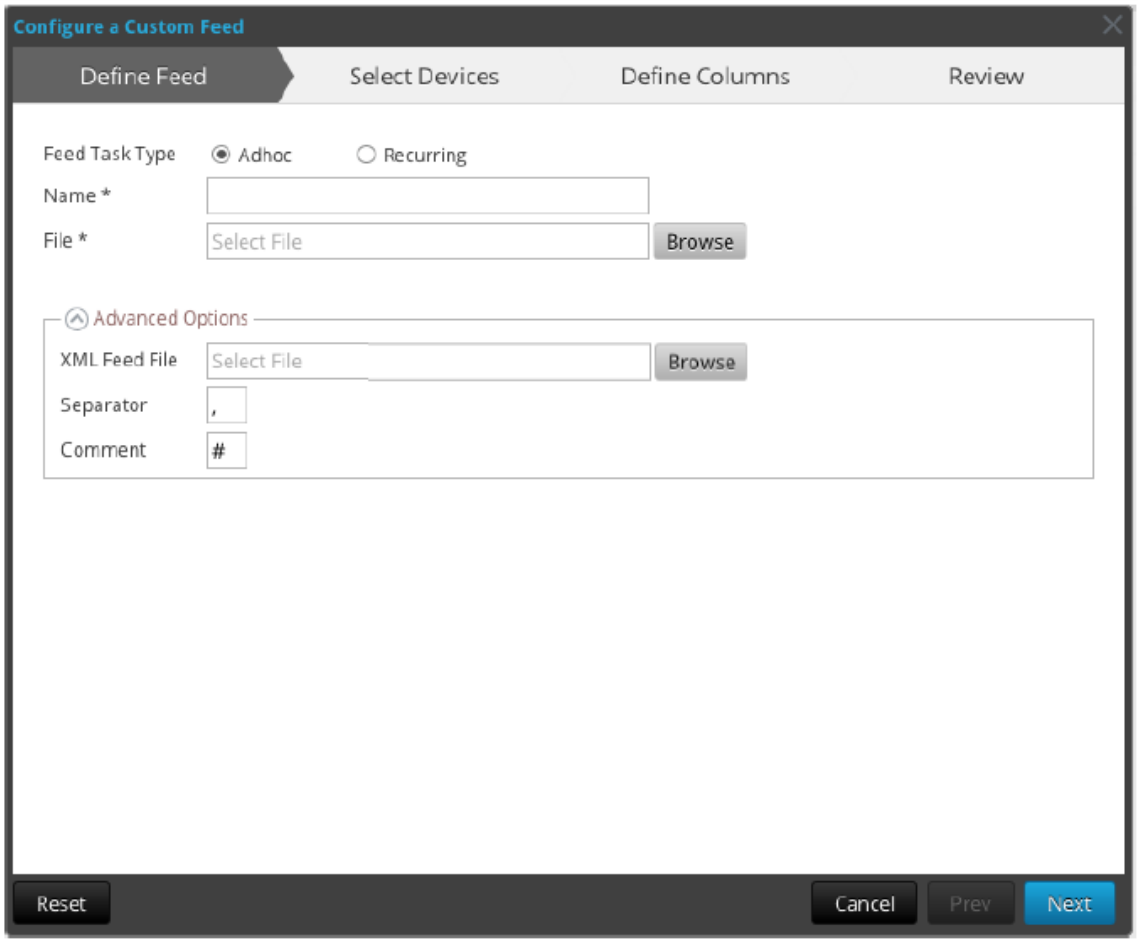


Ilustración 71. Pantalla de configuración de feeds con las opciones avanzadas habilitadas.

4. 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.

5. En la siguiente ventana escogemos el o los decoders en los cuales queremos anexar el "custom feed"

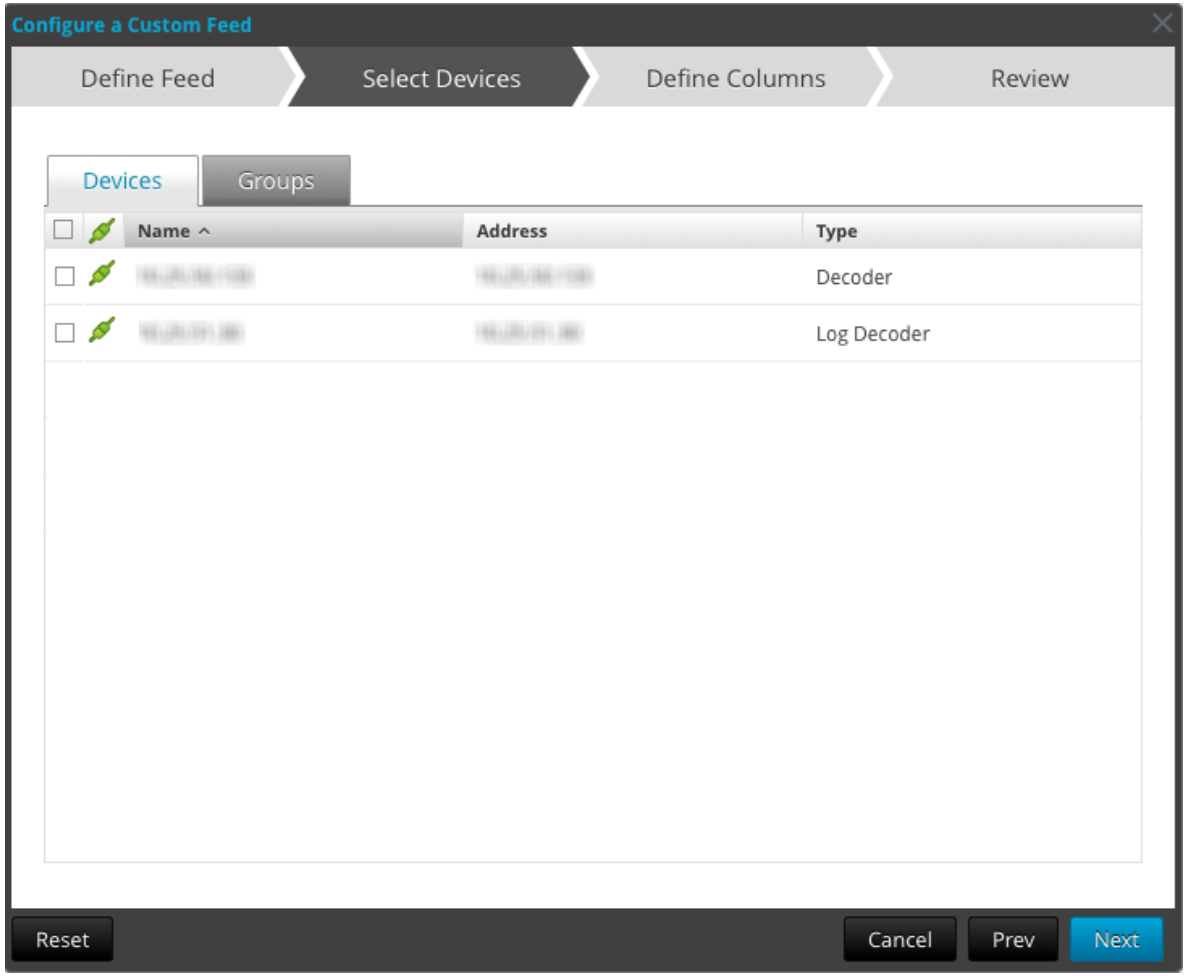


Ilustración 72. Pantalla para elegir en que dispositivos integrar los feeds.

6. El siguiente paso es definir las columnas:

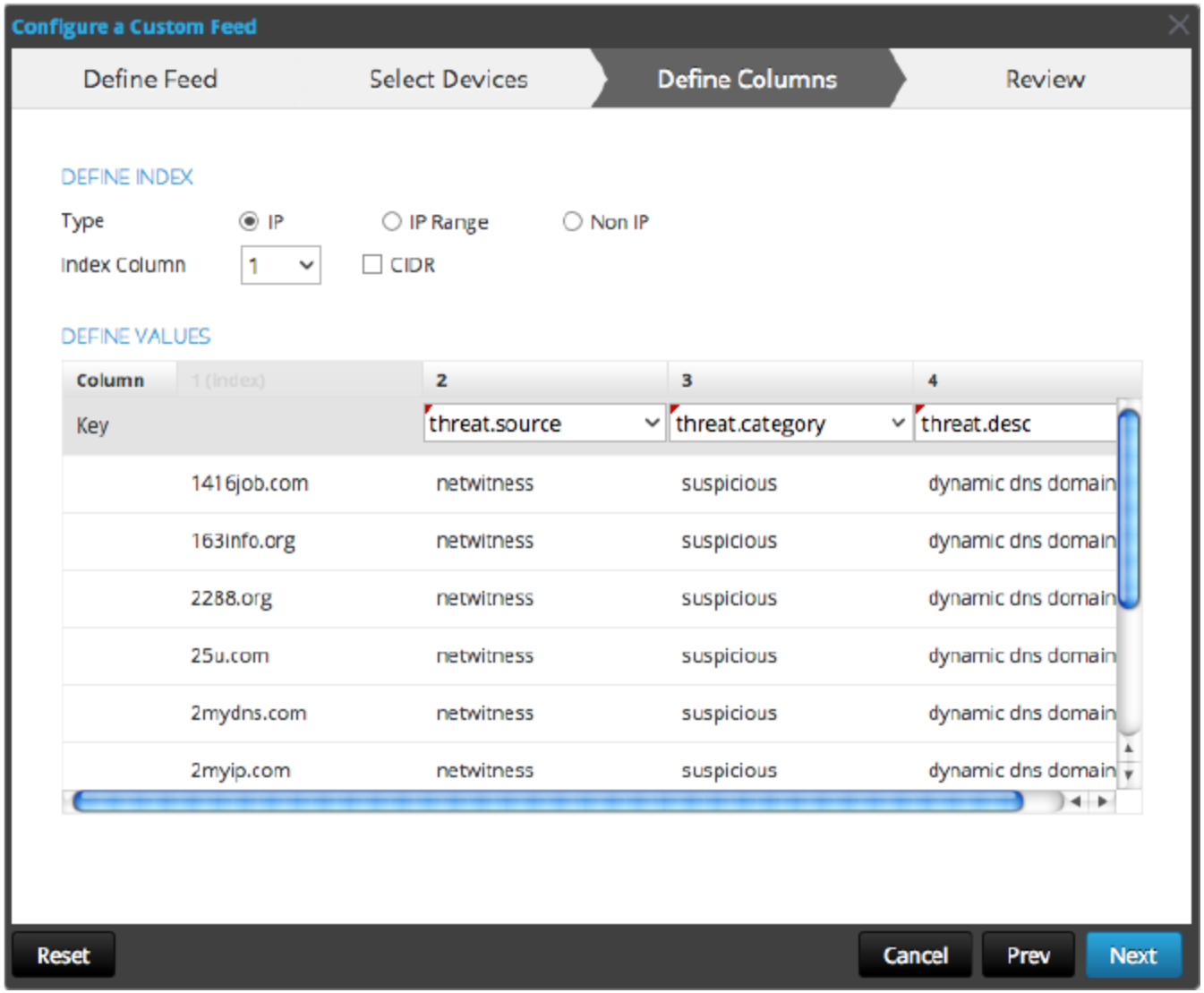


Ilustración 73. Pantalla para definir las columnas a utilizar.

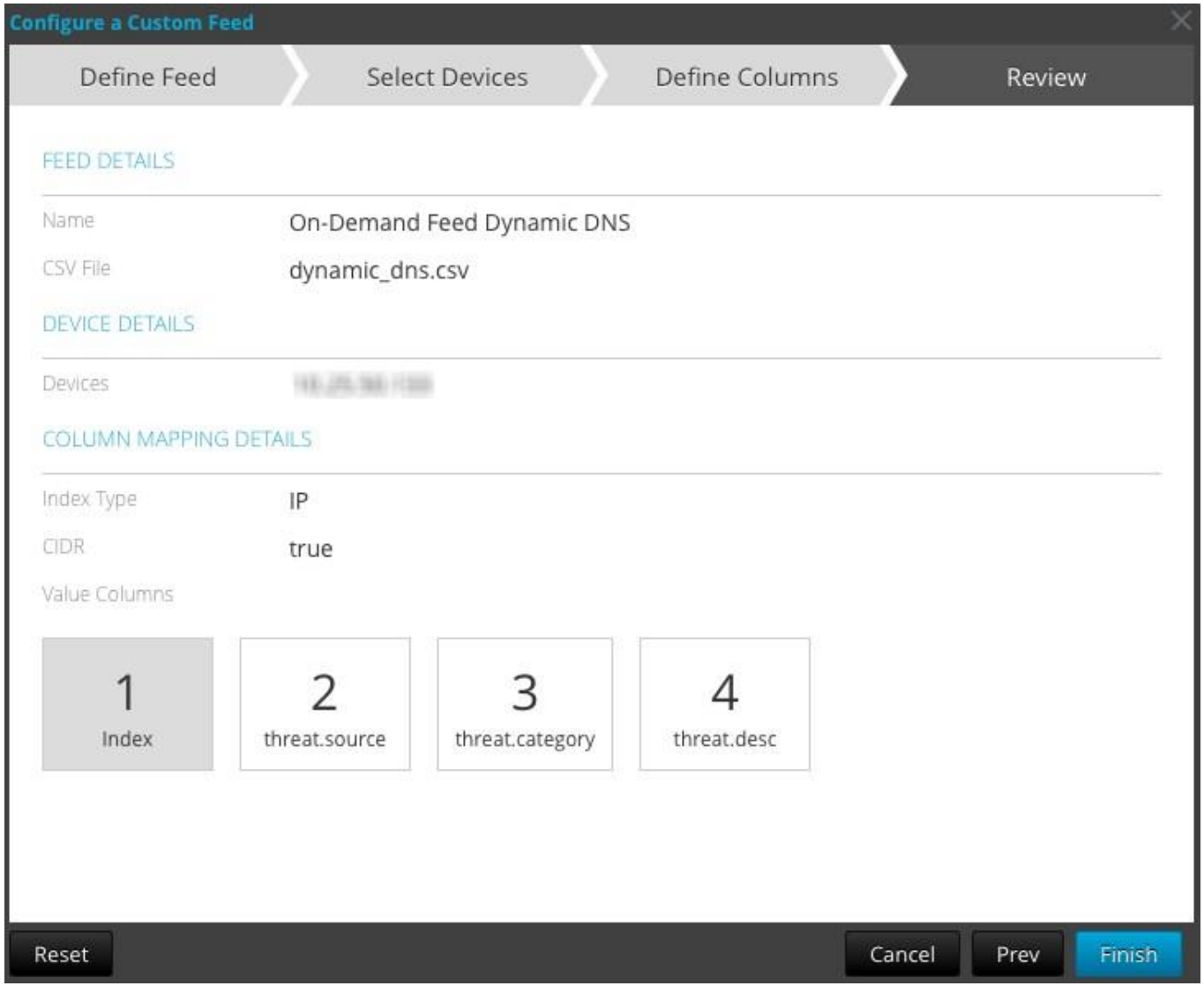


Ilustración 74. Resumen del feed a crear.

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.

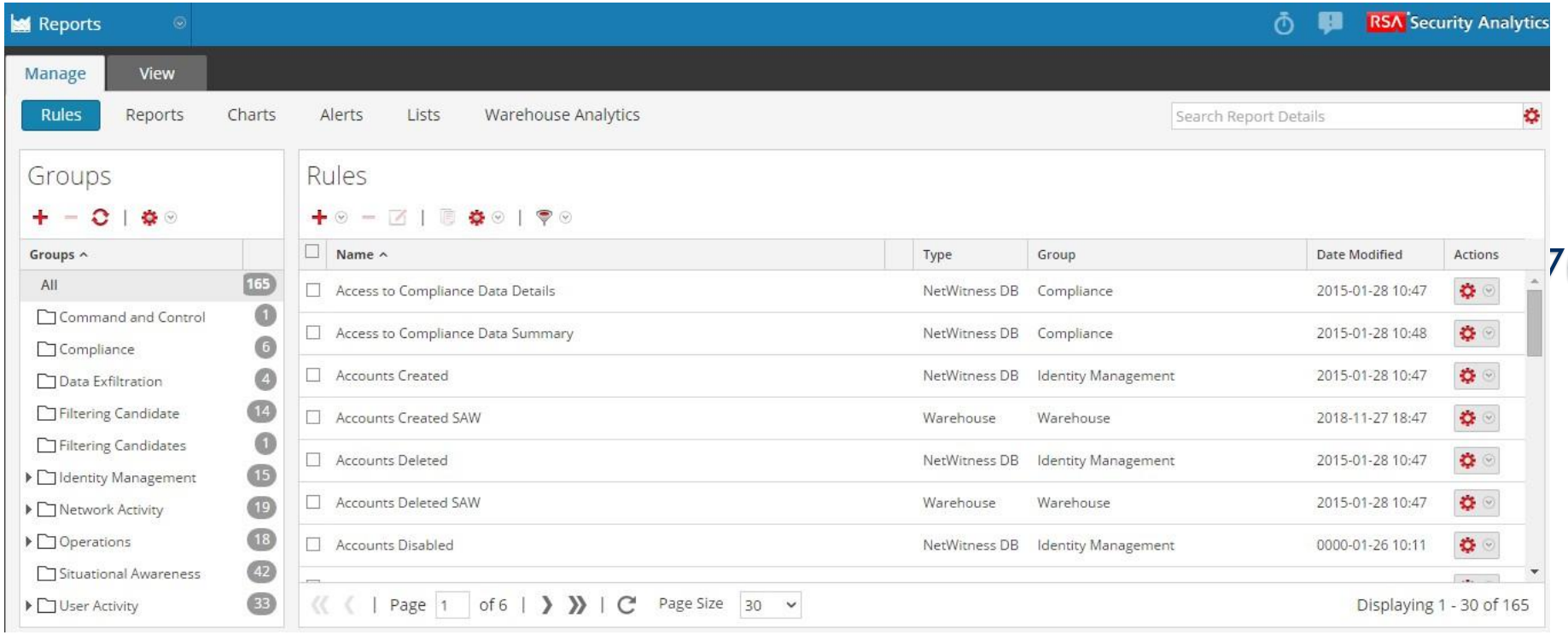


Ilustración 75. Reportes Predefinidos.

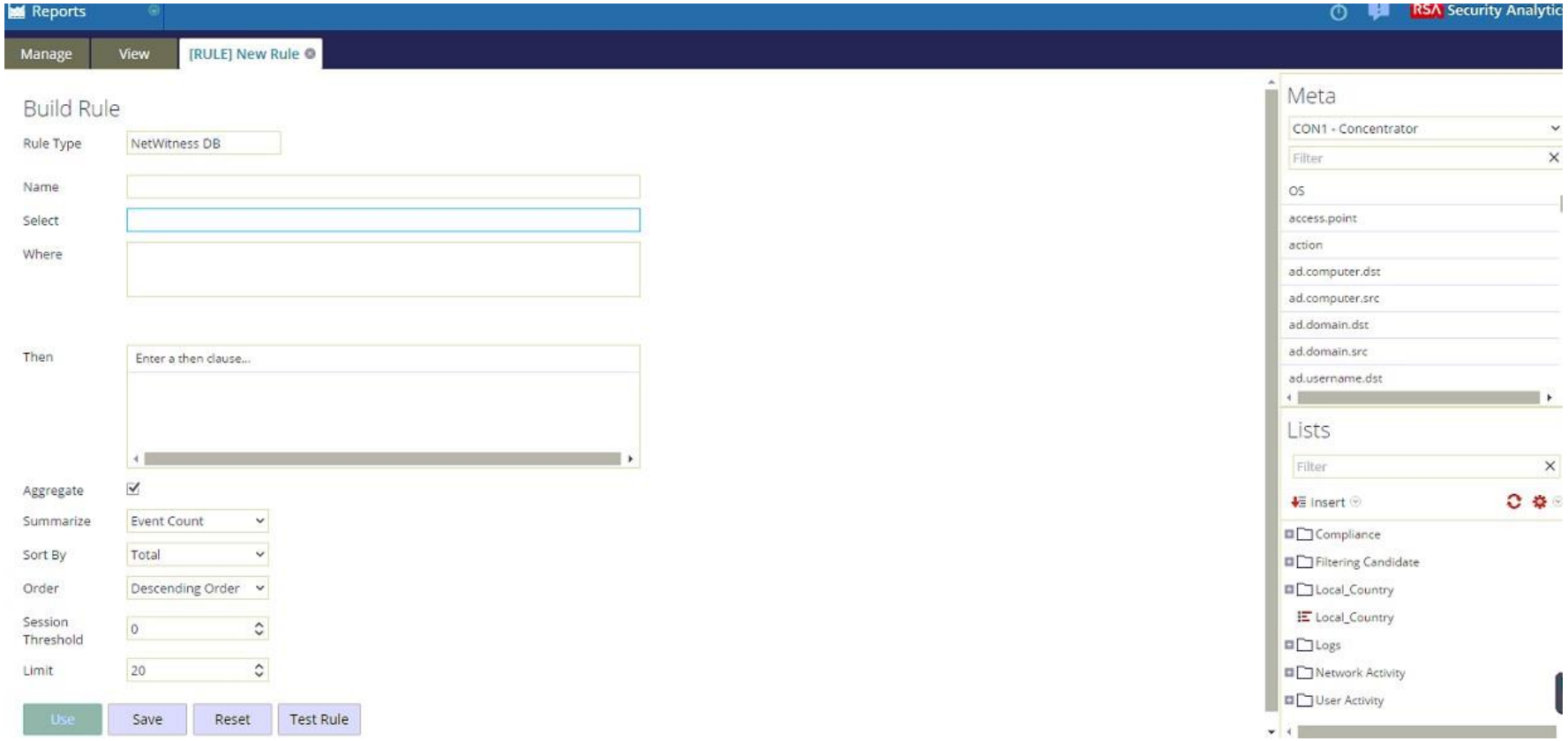


Ilustración 76. Plantilla en Blanco para realizar un Reporte.

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 sincronicemos 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.

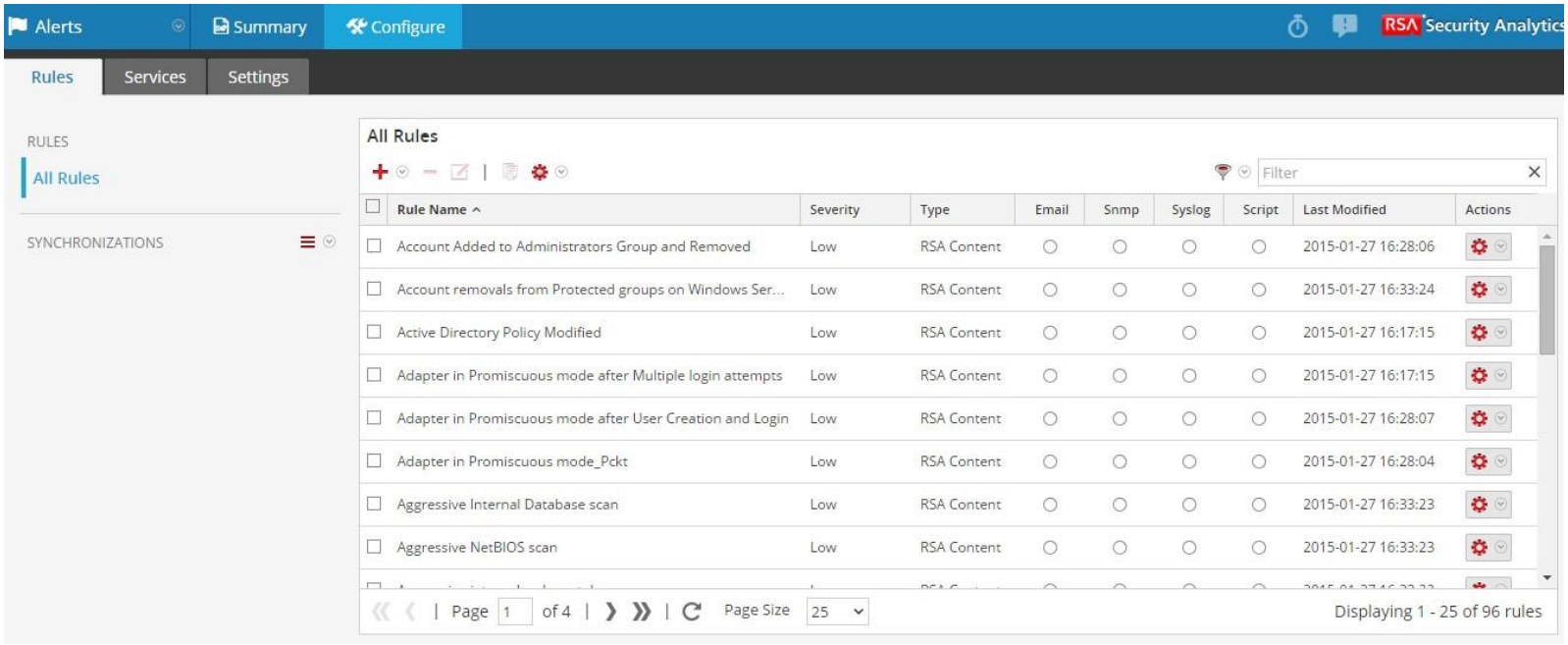


Ilustración 77. Reglas disponibles para crear alertas.

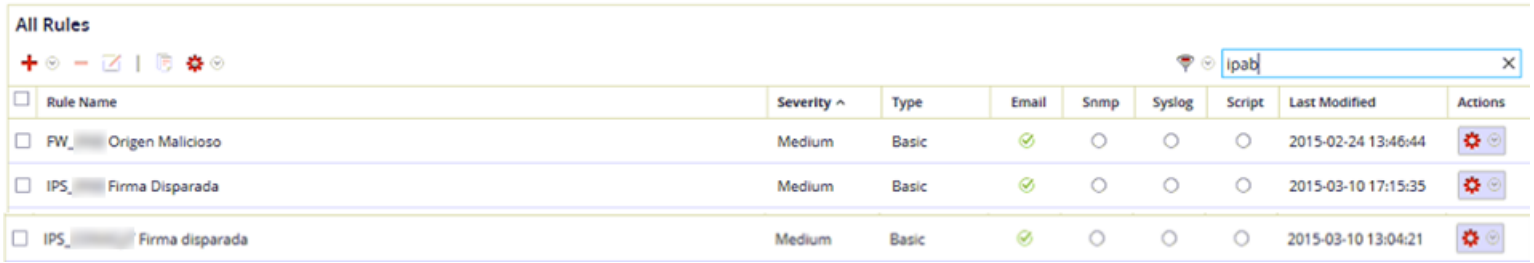


Ilustración 78. Reglas Sincronizadas.

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.

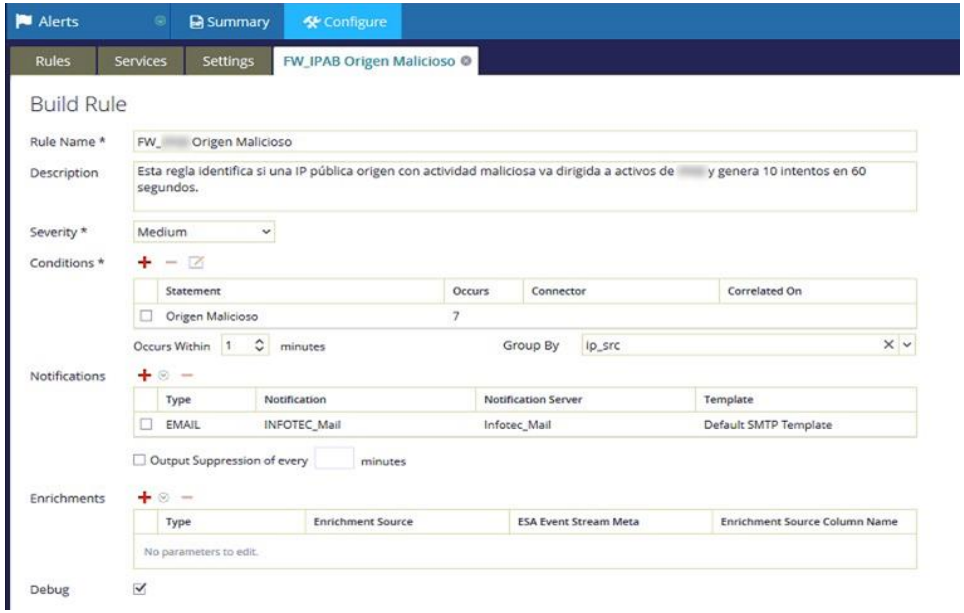


Ilustración 79. Información de una alerta creada por INFOTEC.

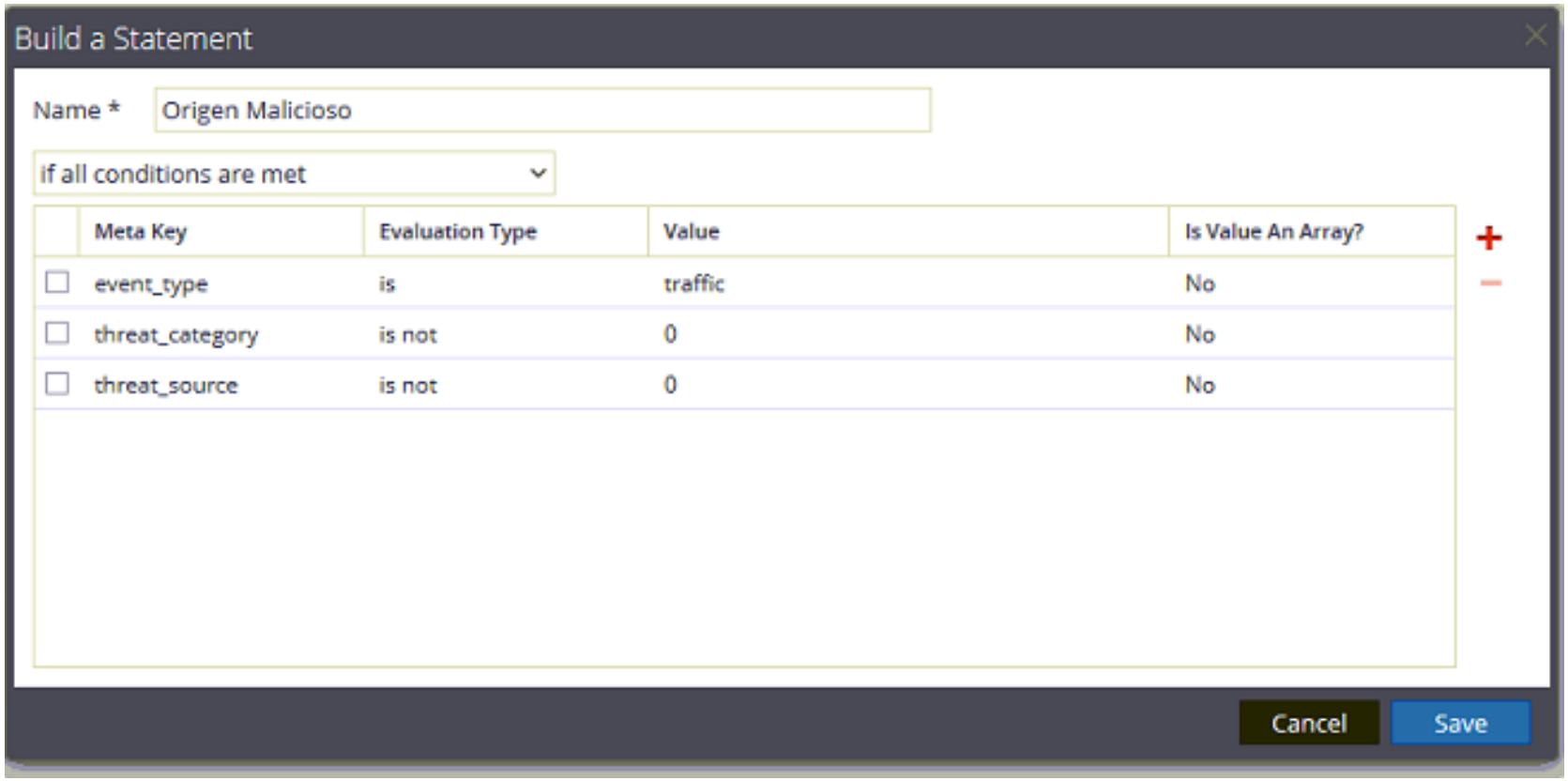


Ilustración 80. Condiciones a cumplir de la alerta.

4.3 Alerta IPS_Firma Disparada

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

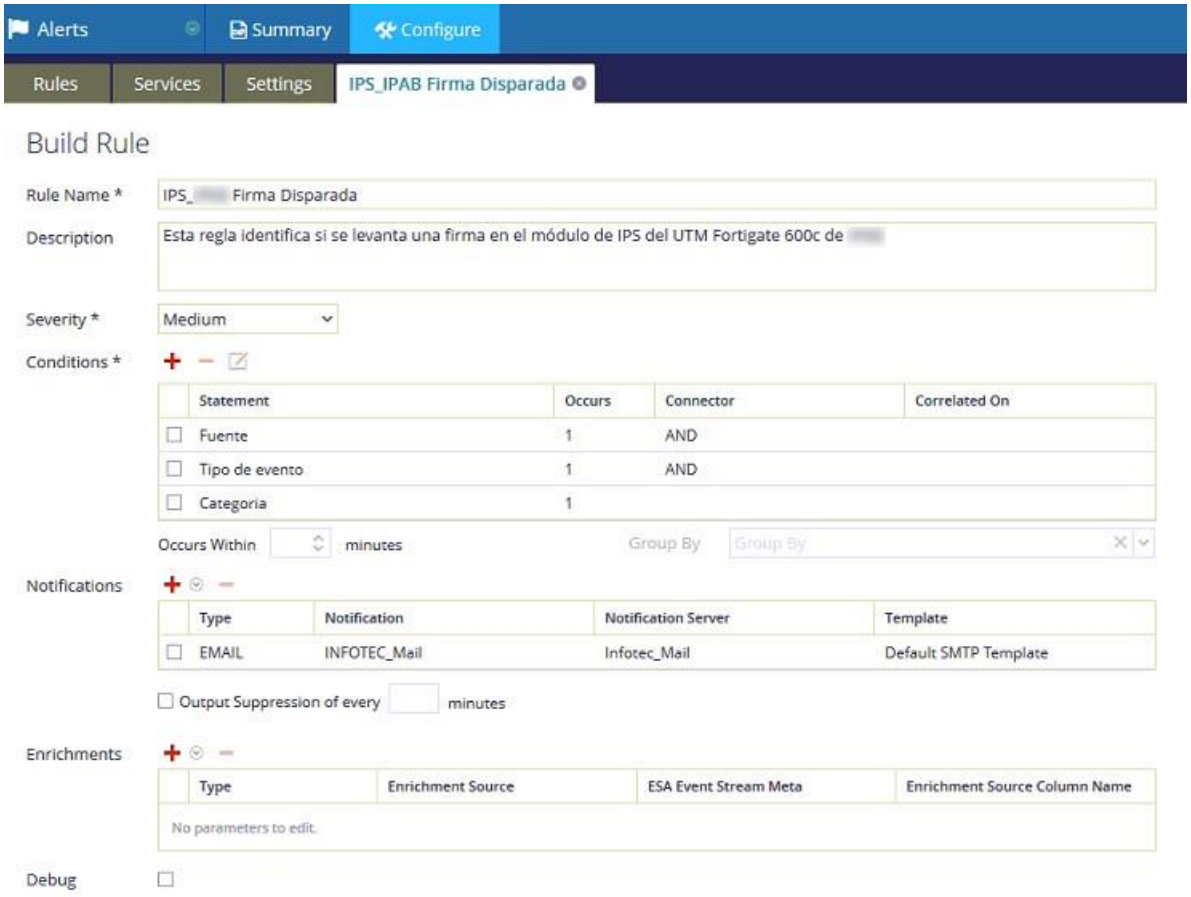


Ilustración 81. Condiciones a cumplir de la alerta.

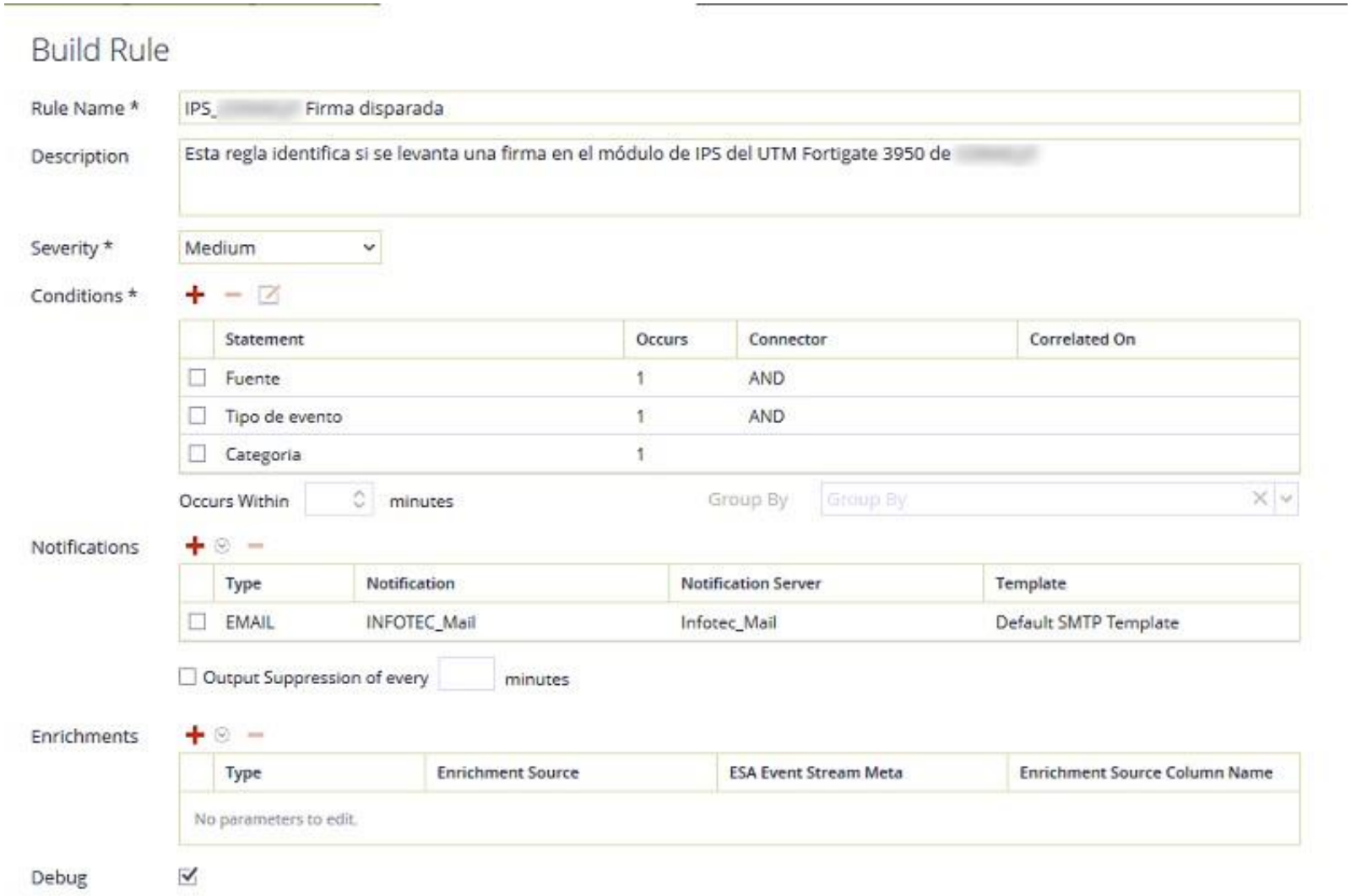


Ilustración 82. Condiciones a cumplir de la alerta.

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.

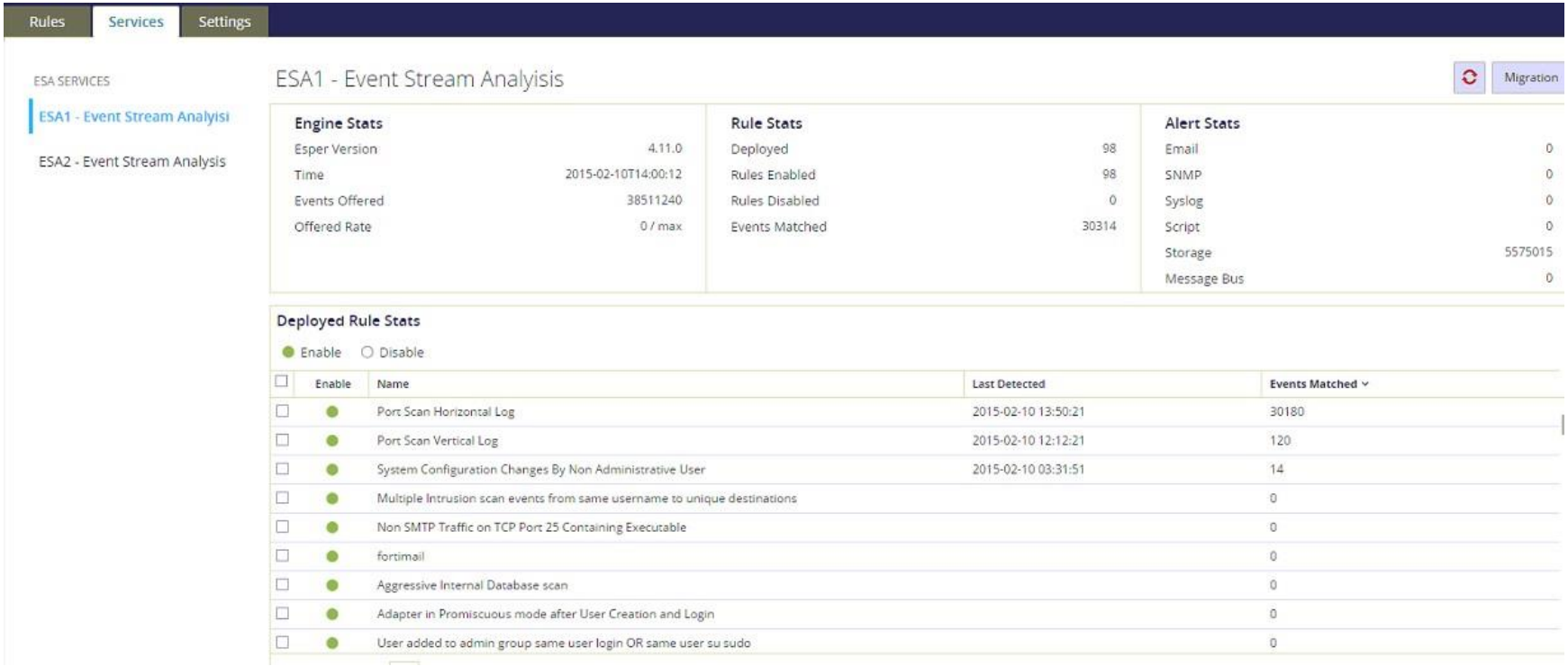


Ilustración 83. Resumen de las alertas.

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.

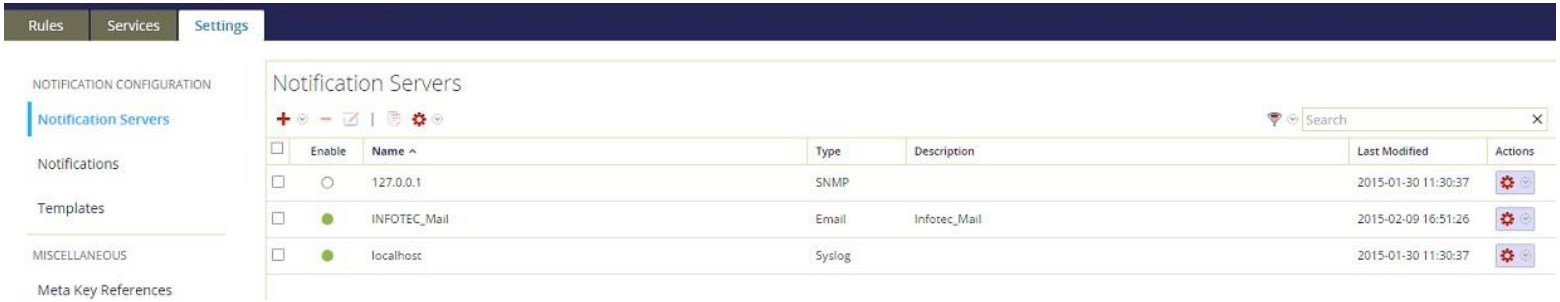


Ilustración 84. Configuración de los servidores de notificaciones.

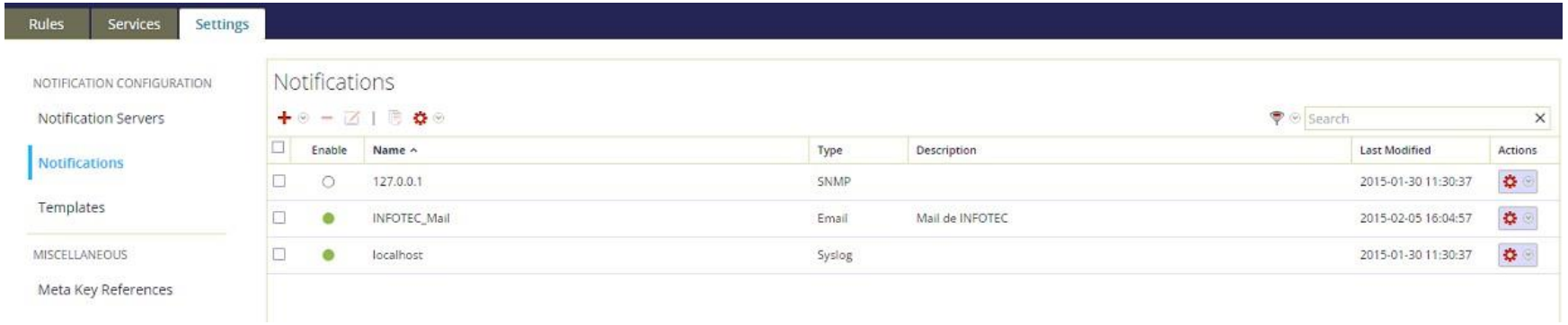


Ilustración 85. Configuración del formato de la notificación.

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 reenvió de logs a una fuente externa para que de ahí se pudieran extraer.

Una vez con el reenvió 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.