UNIVERSITAT POLITÈCNICA DE VALÈNCIA

etsinf
Escola Tècnica Superior d'Enginyeria Informàtica

Escola Tècnica Superior d'Enginyeria Informàtica
Universitat Politècnica de València

Estudio y mejora en la gestión de conexiones de dispositivos de ámbito corporativo

Trabajo Fin de Grado

Grado en Ingeniería Informática

Autor: Hugo Pastor Llorente

Tutor: José Salvador Oliver Gil

Tutor externo: Ricard Sanjuán Plá

2017-2018

Resumen

El proyecto consiste en la recopilación de las principales deficiencias de gestión en las conexiones de red, que comúnmente podemos encontrar dentro de entornos corporativos de tamaño medio y que pueden provocar administraciones ineficientes. Posteriormente exponemos dos soluciones compatibles entre sí que añaden información y gestión centralizada de nuestra red.

Para determinar las soluciones, realizamos un análisis previo de herramientas disponibles en el mercado y examinamos las diferentes ventajas e inconvenientes. Posteriormente llevamos a cabo su instalación, configuración y puesta en marcha dentro un entorno empresarial replicado.

Finalmente explicamos el funcionamiento de las características más representativas de cada herramienta implantada, de tal manera que podamos realizar un tratamiento eficiente de toda la información nueva que proporcionará. Dicha información extra nos permitirá una gestión más eficiente y diagnósticos proactivos en la gestión de conexiones de dispositivos.

Palabras clave: gestión, conexiones, corporativo, IPAM, Elastic, eventos, logs.

Abstract

The project consists of the collection of the main management troubles in the network connections, which can be translated into medium-sized corporate environments and can cause inefficient administrations. Subsequently, we show two compatible solutions that add information and centralized management of our network.

In order to find solutions, we do a previous analysis of the available market tools and examine the different advantages and disadvantages. Then we will start with the installation, the setting and commissioning in a replicated business environment.

Finally, we explain the operation of the most representative characteristics of each installed tool, in such a way we can do an efficient use of the data gathered. This additional information allows us a more efficient management and proactive diagnostics in the management of device connections.

Keywords: manage, connections, corporate, IPAM, Elastic, events, logs.

Tabla de contenidos

Listado de tablas

Listado de figuras

1. Introducción

1.1. Antecedentes

Las empresas actuales encuentran en la capacidad de las comunicaciones su mejor aliado para el desarrollo y crecimiento, siendo la gran parte de dichas comunicaciones realizadas mediante dispositivos electrónicos o computadores. Esto supone un incremento en la preocupación de los agentes encargados de gestionar las infraestructuras de comunicaciones y sistemas, para conseguir una conectividad eficaz y controlada.

La dificultad de monitorizar y administrar este tipo de comunicaciones es directamente proporcional al número de equipos y al tamaño de la empresa, lo que hace conveniente contar con algún tipo de herramienta que solucione o por lo menos facilite las diversas tareas de mantenimiento y control.

En este TFG analizaremos los principales problemas que encontramos a la hora de gestionar las conexiones de tipo IP versión 4, que son habitualmente empleadas para realizar las conexiones y buscaremos la solución más adecuada para su gestión.

1.2. Estado del arte

Los tipos de comunicaciones se van adaptando a las tecnologías existentes. A fecha de 2018 existe una tecnología de comunicación que prevalece sobre todas las demás, denominada tecnología de Internet o IP (*Internet Protocol*). Dicha tecnología establece "las reglas del juego" para que diferentes dispositivos puedan comunicarse entre sí.

Casi la totalidad de las empresas aprovechan las ventajas que ofrecen las comunicaciones a través de Internet para la transmisión de voz, imágenes y datos, incluso aprovechan esta misma tecnología para implementar una red interna de uso privado que incrementa sus servicios y funcionalidades.

Una empresa de tamaño medio, similar a la empresa donde he desarrollado mis labores prácticas, podría servir perfectamente de referencia para las situaciones más comunes. Dicha empresa ha experimentado un notable desarrollo tanto humano como estructural en los últimos dos años y cada recurso incorporado es dotado con dos dispositivos; ordenador portátil y teléfono móvil inteligente, que deben poder ser utilizados tanto en la propia sede como en el exterior.

El diseño inicial de la empresa de referencia analizada cuenta actualmente con servicios propios de:

- Directorio Administrativo o *AD,* que permite la administración de permisos y recursos de usuarios de la organización una vez identificados.
- Protocolo de configuración dinámica de host o *DHCP*, es el servicio encargado de suministrar direcciones IP dinámicas validas a los dispositivos que le solicitan conexión.

- Sistema de nombres de dominio o *DNS*, es servicio encargado de la traducción de direcciones IP, en nombres más utilizables para los humanos.
- Copia de seguridad o *Backup*, servicio encargado de hacer copias planificadas de los datos de los servidores como respaldo en caso de fallo.

Dichos servicios realizan correctamente sus tareas y se encuentran replicados para disponer de una alta disponibilidad a excepción del servicio copia de seguridad que debido a la cantidad de información que maneja, no dispone de replicación.

Los tipos de conexiones que utilizan los dispositivos desplegados son ethernet para el caso de ordenadores portátiles o sobremesa, servidores y cortafuegos, también dispondremos de conexiones wifi para los teléfonos móviles y ordenadores portátiles. Dejamos fuera de este trabajo el análisis de otro tipo de comunicaciones como puede ser el tipo 4G, ya que la administración de dicho servicio se encuentra fuera del ámbito empresarial.

1.3. Análisis del problema

En el escenario de empresa que vamos a emplear en este proyecto, existen actualmente cerca de 1.000 dispositivos simultáneos conectados diariamente a las distintas sedes, servidores, equipos de enrutamiento, cortafuegos… todos ellos susceptibles a tener un mal funcionamiento.

Teniendo un número considerable de recursos a gestionar, necesitamos replantear el diseño para que nos permita conocer el estado real del sistema. Un fallo de comunicaciones afectaría directamente a la productividad, por lo tanto, debe ser la misma empresa la interesada en disponer de los elementos de red y sistemas bien controlados.

Los problemas generales más relevantes que se han encontrado pueden ser resumidos en los siguientes puntos:

- Ausencia de indicadores de estado global: No existe de manera predeterminada una consola central que aporte información del estado de equipos.
- Procedimiento para el acceso a servidores: son procesos manuales que requieren el conocimiento de datos restringidos. Los agentes encargados generalmente tienen apuntadas las direcciones IP, pero la política de seguridad prohíbe la anotación de contraseñas sin cifrado.
- Cantidad de equipos distribuidos: que junto con el procedimiento de acceso hacen ineficiente el diagnóstico de problemas.
- Desconocimiento de actualizaciones de infraestructura: cambios de direcciones, ampliaciones de red o rangos llevadas a cabo en periodos vacacionales o en los que simplemente estamos a cargo de otros proyectos
- Elevado número de conexiones: el manejo con cifras elevadas suele provocar la pérdida de noción de cantidades y se recomienda tener acceso a porcentajes.

En los entornos informáticos como en otros campos, tenemos diversos métodos para llegar a una misma solución, aunque no todas estas soluciones presentan las mismas ventajas e inconvenientes. En estos casos adoptaremos como solución válida aquella que se adapte no solo a la solución puntual, sino también a la solución global y al entorno escalable.

Para todas las modificaciones que vamos a llevar a cabo, es fundamental contar con las contraseñas de administrador local y de dominio, o Administrator en caso de sistemas en inglés.

1.4. Objetivo

El objetivo del proyecto es analizar y seleccionar la herramienta o herramientas de gestión de red que mejor encajen en un entorno donde se realiza un uso intensivo de comunicaciones IP, teniendo en cuenta que muchas veces ya se cuenta con parte de una infraestructura montada a la que es necesario adaptarse.

Partiendo de los servicios básicos funcionales comentados anteriormente (AD, DHCP, DNS), proponemos mejoras en 3 ámbitos distintos de la infraestructura:

- Referente a la administración y gestión de direcciones IP
- Recolección de eventos de los equipos de red encargados del servicio
- Control y aprovechamiento del ancho de banda de las conexiones

Analizaremos las herramientas disponibles en el mercado para dichos fines teniendo en cuenta cuatro preguntas fundamentales para su evaluación real:

- Ventajas de administración y supervisión - ¿Qué aporta?
- Coste económico de licencias - ¿Cuánto cuesta?
- Integración con los sistemas existentes - ¿Qué voy a tener que cambiar?
- Automatización de las tareas - ¿Cuántos recursos necesito para su control?

Una vez recopilada la información más relevante de dichas herramientas y sin perder de vista el escenario corporativo en el que necesitamos implantar la solución, estaremos en posición de realizar la selección que mejor se adapten a nuestro propósito.

2. Herramientas de software

Vamos a analizar las características de 4 herramientas utilizadas en el control de direcciones IP y otras 3 herramientas utilizadas en la recogida de registros de datos, para seleccionar la más adecuada de cada grupo en nuestro proyecto de mejora.

2.1. Administración y gestión de direcciones IP

Una de las mejoras que debemos valorar en los entornos que cuentan con servicio de ofrecimiento de IP o resolución de nombres, es la relacionada con la automatización de las labores de identificación y control de dicho ofrecimiento a los dispositivos.

Dichas aplicaciones reciben el nombre de Administrador de Direcciones IP o *IPAM* en su nomenclatura abreviada. Este tipo de programas añade una capa de administración con la posibilidad de adaptarse a los servicios ya existentes, por lo tanto, un servicio de este tipo encajaría perfectamente en nuestro entorno de estudio.

Algunas de las aplicaciones IPAM son incluidas como parte de sistemas completos, también llamadas *DDI* (DNS, DHCP e IPAM), como puede ser por ejemplo InfoBlox y SolarWinds, sin embargo, estas asociaciones no son de ninguna manera necesaria, pudiendo asociarse IPAM y DNS o IPAM y DHCP sin el tercer servicio.

IPAM analizados:

- SolarWinds IP Address Manager - Comercial
- Microsoft IPAM- Comercial
- phpIPAM – Open Source
- NIPAP - Open Source

2.1.1. IP Address Manager de SolarWinds

SolarWinds es una compañía de Texas que desarrolla software empresarial de administración, seguridad y nube para las empresas del sector tecnológico. Entre su amplio catálogo de productos encontramos la aplicación *IP Address Manager* publicitada como producto económico de gestión de direcciones IP.

Figura 1: Productos SolarWinds

Características de administración y supervisión:

- Administración integrada de servicios DHCP y DNS la consola
- Monitorización de alertas y diagnóstico de la red que incluye capacidades y conflictos de IP mediante escaneos de IP programables
- Compatibilidad de operaciones (API) de creación, lectura, actualización y eliminación con software de terceros
- Historiales exhaustivos de todas las IP de la red
- Generación rápida de informes mediante plantillas o su modificación para personalizar

Coste económico de licencia:

- El coste de la licencia fecha de mayo de 2018 asciende a 1.625€

Integración con los sistemas existentes:

- Compatibilidad con servidores DHCP de Microsoft, Cisco e ISC y compatible con DNS Microsoft y BIND

Automatización de las tareas:

- Automatización de gestión de aprovisionamiento IP en entornos virtuales VMware mediante escaneos de IP

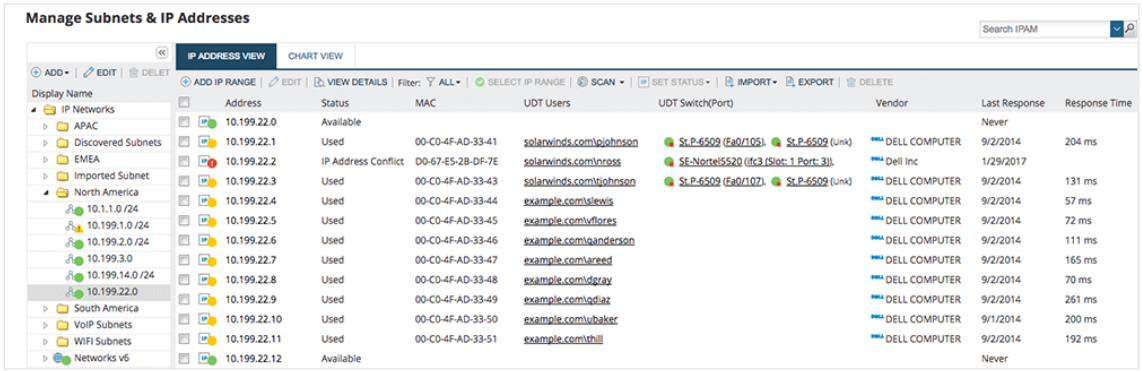

Figura 2: IP Address Manager vista de administración

2.1.2. Microsoft IPAM

Microsoft es la empresa líder en sistemas operativos de equipos y algunos servidores especialmente enfocados en el apartado de usuarios. Con la aparición de Windows Server 2012, Microsoft irrumpe en el sector incluyendo la posibilidad de instalar su propio gestor de direcciones IP de manera gratuita desde el mismo servidor.

Características de administración y supervisión:

- Capacidad para descubrimiento de Active Directory para servidores con sistema operativo Windows Server 2008 y posteriores
- Administración de espacio de direcciones y seguimiento DHCP
- Posibilidad de gestión de múltiples servidores DHCP y DNS
- Auditoría de modificaciones de configuración en los servicios
- Soporte para bases de datos externas

Coste económico de licencia:

- Incluido con la licencia del Sistema Operativo tipo servidor. Al no poder convivir con los servicios que administra, debe ir independiente, si bien el mismo servidor puede ser usado para otras tareas secundarias
- En caso de necesitar licencia un Windows Data Server 2012 R2 tiene un precio de 179€

Integración con los sistemas existentes:

- Completa integración automática de administración con servicios solo de Microsoft
- Visualización de sistemas no Microsoft mediante importación manual

Automatización de las tareas:

- Permite elaboración automática de informes y recopilación programada de datos
- Visualiza tendencias del estado de direcciones

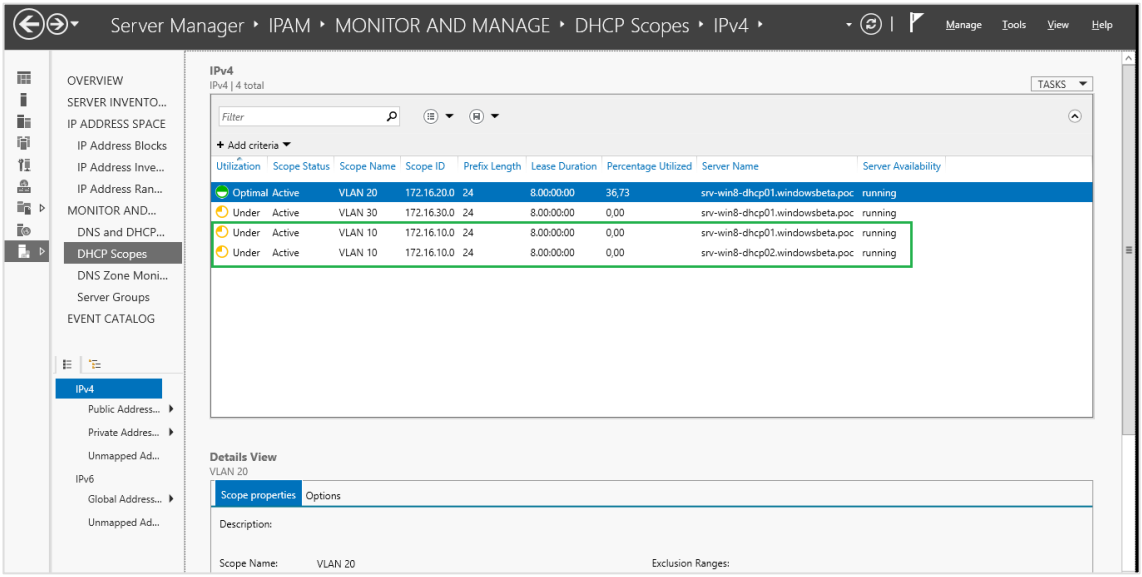

Figura 3: Consola administración IPAM Microsoft

2.1.3. phpIPAM openSource

phpIPAM es una aplicación de código abierto que se presenta como una aplicación ligera para la administración de direccionamientos IP. Está basada en lenguaje php junto con almacenamiento de datos en MySQL. Para su administración web hace uso de HTML5 y librerías jQuery y Ajax.

Características de administración y supervisión:

- Administración IPv4/IPv6
- Múltiples niveles de subredes
- Notificaciones por correo electrónico
- Inclusión de utilidades como calculadora de rangos
- Incluye la opción de importación de archivos de configuraciones de subredes

Coste económico de licencia:

- Gratuito y código abierto

Integración con los sistemas existentes:

- Instalación del servidor disponible en CentOS o Debian
- Autenticación en Active Directory, LDAP y Radius

Automatización de las tareas:

- Escaneo automático de subredes
- Visualización automática del estado de red

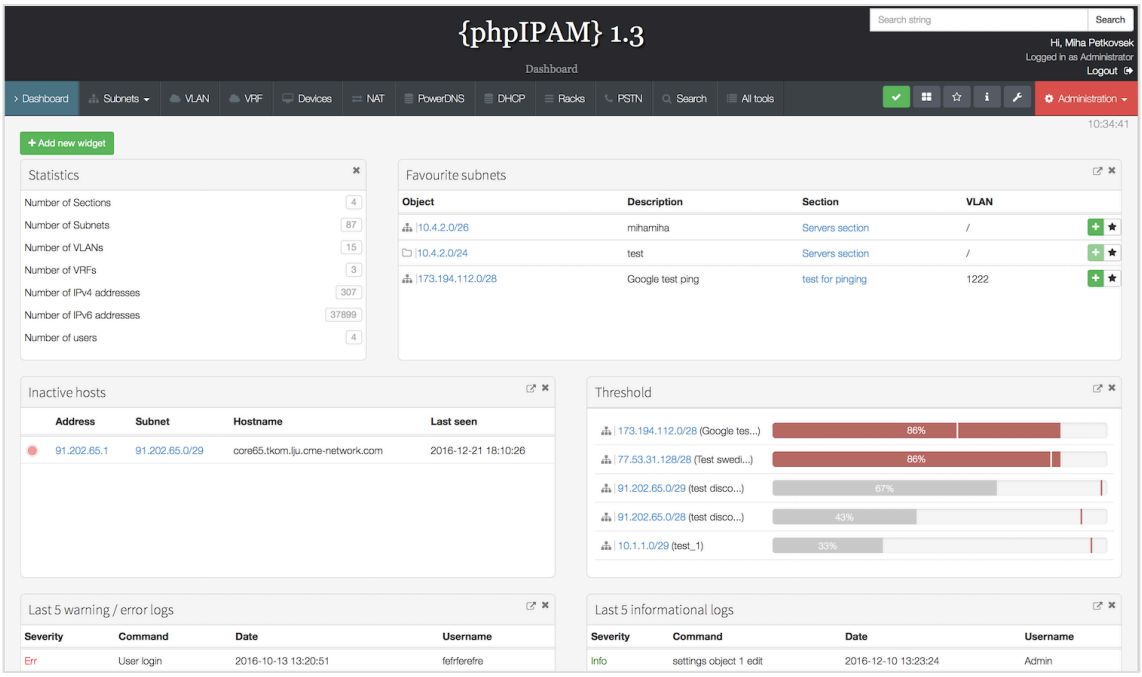

Figura 4: Consola administración phpIPAM

2.1.4. NIPAP opensource

NIPAP es una aplicación desarrollada en Python de código libre bajo licencia por el MIT. Al igual que las anteriores aplicaciones vistas, permite la monitorización de atributos IP haciendo uso de una base de datos que ha sido seleccionada porque permite el almacenamiento nativo de direcciones IP y una búsqueda muy rápida entre las ternas de los módulos IPv4.

Características de administración y supervisión:

- Disponible solo para funcionar en Debian
- Base de datos PostgreSQL
- Administración IPv4/IPv6
- Entorno gráfico y de comandos

Coste económico de licencia:

- Gratuito y código abierto

Integración con los sistemas existentes:

- Con LDAP de serie y mediante librerías de manera manual en el resto

Automatización de las tareas:

- Escaneo configurable de parámetros de red
- Visualización automática del estado de red

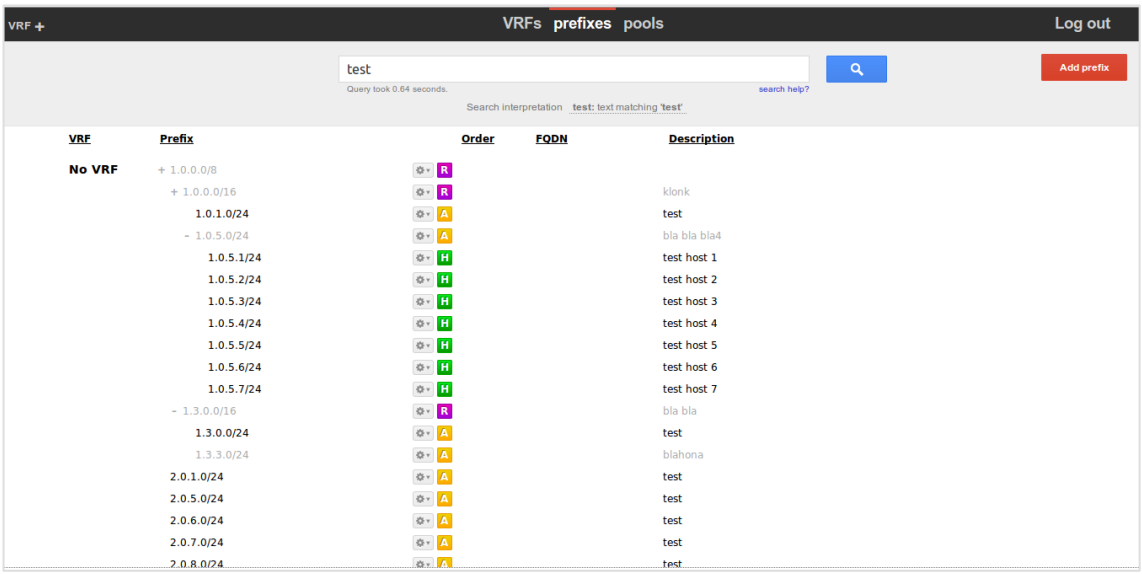

Figura 5: Consola administración NIPAP

2.1.5. Resumen de herramientas para gestión de direcciones IP

A modo de comparativa vamos a ver las características más destacables de las herramientas analizadas:

Tabla 1: Comparativa de características de las herramientas para administración de direcciones IP

	IP Address Manager	**Microsoft IPAM**	**phpIPAM**	**NIPAP**
Instalable Windows	Si	Si	No	No
Instalable Linux	No	No	Si	Si
Despliegue Windows	Si	Si	Si	Si
Despliegue Linux	Si	Manualmente	Si	Si
Entorno gráfico datos	Si	Si	Si	Si
Compatible IPv6	Si	Si	Si	Si
Código abierto	No	No	Si	Si
Importe	1.625€	Incluido Server	Gratis	Gratis

Haciendo un análisis de sus características encontramos que phpIPAM y NIPAP no son instalables con entornos Windows, aunque sí permiten su posterior administración de sistemas Microsoft. Nuestro entorno corporativo es mayoritariamente de tipo Windows y por esa razón nos decantamos por las herramientas que pueden ofrecernos mayor compatibilidad con lo ya existente:

- IP Address Manager de SolarWinds
- Microsoft IPAM

Las dos aplicaciones finalistas son de código propietario y necesitan licencia de uso, estando incluida la de Microsoft en el mismo servidor. El estado de capacidad actual de los servidores corporativos se encuentra bastante ajustado, decidimos no comprometer la eficiencia de ningún servicio y crear un nuevo servidor dedicado para llevar a cabo la administración.

Como el despliegue a realizar requiere de un servidor nuevo y de una amplia compatibilidad con los sistemas Windows, nos inclinamos hacia las características que ofrece la aplicación **Microsoft IPAM**, tanto por motivos económicos, como por integración y soporte de la misma.

2.2. Recolección de eventos en dispositivos de red

Los eventos de dispositivos electrónicos, también conocidos como *logs*, son un histórico de sucesos relevantes dentro del mismo. Están disponibles en prácticamente todos los dispositivos de comunicaciones incluso los domésticos, aunque en estos últimos lo más habitual es que se encuentren deshabilitados por defecto.

En un entorno empresarial, es altamente recomendada la activación de los logs en los dispositivos utilizados, pero aun así los parámetros de configuración deben ser revisados ya que proporcionan una valiosa herramienta para detectar eventos, alertas y fallos permitiendo discriminar el origen de este.

Las dificultades que surgen con el registro de los logs empresariales están relacionadas con su tratamiento y descentralización. Si bien es cierto que cada distinto equipo conectado recoge los eventos que le afectan, estos eventos no sirven de nada si, aunque se necesiten, no se analizan. Y puede ser que no se analicen por diversas razones: difícil acceso, falta de datos para su obtención, desconocimiento de existencia, etc.

La solución en estos casos es centralizar mediante diversas herramientas software la recolección y análisis de eventos ocurridos en nuestra red, para así tener información de una manera rápida y eficaz de lo que está pasando y poder ser proactivo.

Las herramientas analizadas para este fin son:

- Kiwi Syslog Server de SolarWinds
- Grupo de herramientas Elastic
- Splunk Ligth

2.2.1. Kiwi Syslog Server

Herramienta desarrollada por la empresa SolarWinds que permite recolección de eventos y mensajes tanto en Windows como Linux y Unix. Consta de interfaz gráfico que permite la administración de eventos desde la misma consola y dispone de una versión gratuita que hemos utilizado para probar sus funcionalidades y que se encuentra limitada a la recogida de eventos de cinco dispositivos máximo.

Kiwi Syslog genera informes diarios que pueden ser enviados por mail automáticamente y guarda toda la información que recopila en una base de datos, pero quizás la característica más destacable de esta herramienta es que puede crear gráficos de tendencia a partir de la información como por ejemplo la recopilada de tráfico de red.

Características de administración y supervisión:

- Recolección y almacenaje de registros del sistema recibidos por mensajes
- Recopilación de información vía SNMP de routers, servidores y cortafuegos
- Tratamiento de registros mediante reglas y filtros
- Soporte de tiempo real y análisis de recursos físicos de los equipos

Coste económico de licencia:

- Kiwi Syslog Server para recopilación y almacenaje de registros por 295€
- Kiwi CatTools para la automatización 640€
- Dameware Remote Support usado para control remoto de aplicación 300€
- Kiwi Log Viewer lector de registros 70€/anual

Integración con los sistemas existentes:

- Integración completa con los sistemas Microsoft
- Compatible con hardware de red que valida con Active Directory

Automatización de las tareas:

- Mediante otra aplicación denominada Kiwi CatTools con licencia separada
- Administración remota mediante Dameware Remote Support

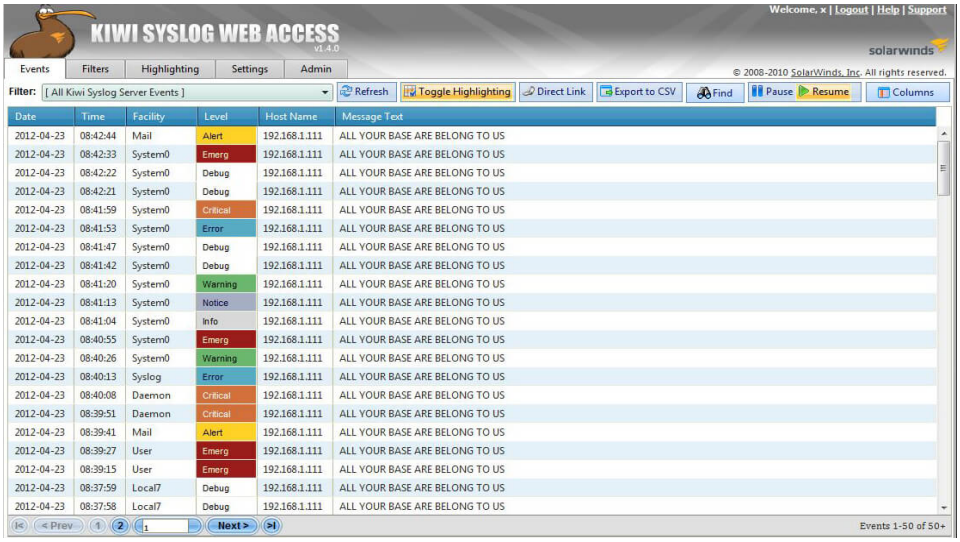

Figura 6: Consola registros Kiwi Syslog

2.2.2. Herramientas Elastic

Elastic es una empresa especializada solo en el desarrollo de software de monitorización de eventos de red y recientemente ha desarrollado versiones para la nube. Aunque algunas de las herramientas ofrecidas, como el almacenamiento en nube, son de pago, el resto de las herramientas son gratuitas realizadas en código libre.

Existe un amplio catálogo de herramientas disponibles del mismo fabricante, pero el corazón de todas ellas se denomina ElasticSearch, que contiene el motor de búsqueda, análisis y almacenamiento de datos. Como herramientas complementarias que podremos instalar dependiendo el nivel de funcionalidad que necesitemos para nuestro entorno, se encuentran: Logstash, Beats, Kibana, X-Pack y Cloud/ECE.

Características de administración y supervisión:

- Programado mediante APIs RESTful y JSON
- Disponible también en lenguajes como Java, Python, .NET y PHP
- Indexación y esquemas de patrones
- Funcionalidades principales divididas en aplicaciones
- Posibilidad de funcionamiento en nube

Coste económico de licencia:

- Herramientas completas gratuitas en código abierto
- Elastic Cloud tiene coste variable dependiendo requisitos (Min. 5€ - Max.390€ mes)

Integración con los sistemas existentes:

- Permite la instalación y administración tanto de sistemas Windows como Unix

Automatización de las tareas:

- Mediante aplicación gratuita de la misma empresa

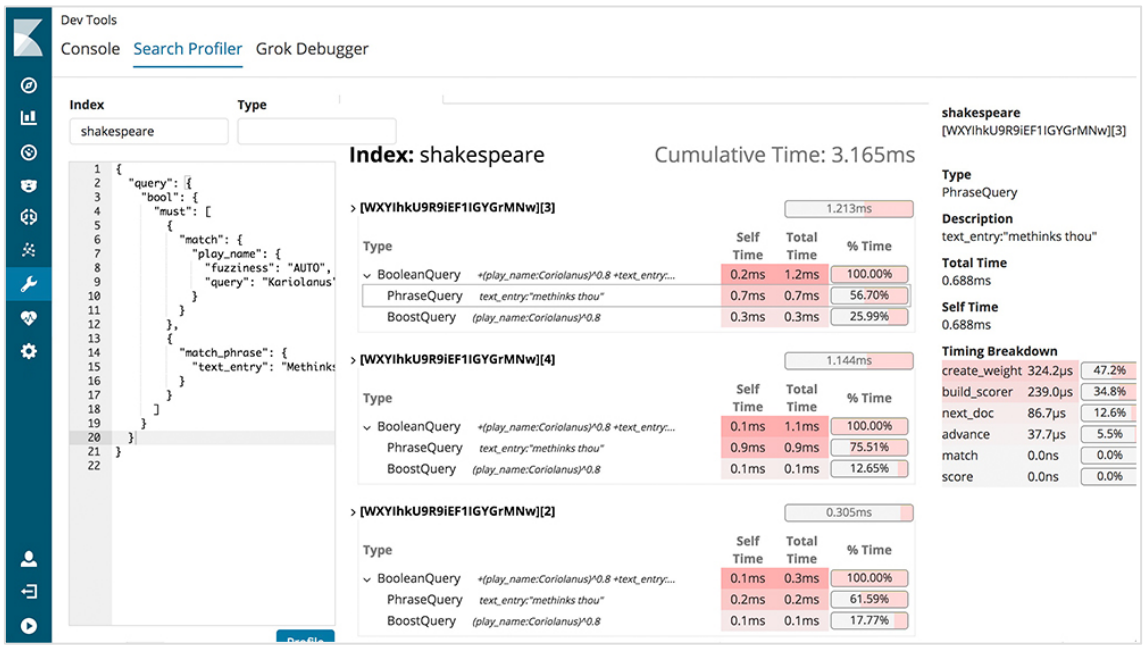

Figura 7: Consola de registros Elastic Stack

2.2.3. Splunk Enterprise

Splunk es una empresa con diversidad de software que engloba análisis de negocio, reparto de aplicaciones, almacenamiento de datos industriales, administración de registros y seguridad.

La herramienta seleccionada para realizar las pruebas se denomina Splunk Enterprise, y proporciona un administrador de registros de sistema con un interfaz sencillo y manejable. Tiene una consola de información en la que podemos realizar consultas predefinidas en el menú o generar nuevas. La herramienta tiene los filtros de búsqueda más potentes de todas las herramientas ya que permite la integración y expansión mediante añadidos de Microsoft.

Como nota característica hay que indicar que la compañía ofrece dos versiones para la misma herramienta, una orientada para la pequeña empresa que se denomina Splunk Ligth y otra orientada a la mediana y grande empresa que es la herramienta analizada.

Características de administración y supervisión:

- Recopilación en indexación de los datos de máquina y registro
- No utiliza esquemas predefinidos para la recolección, el tratamiento es posterior
- Detección de eventos mediante patrones
- Posibilidad de uso como Software como servicio en nube

Coste económico de licencia:

- Splunk Enterprise 173€. Versión ligera 87€
- Splunk Cloud bajo demanda

Integración con los sistemas existentes:

- Instalación disponible en Windows, Linux y MacOS

Automatización de las tareas:

- Creación de informes programables
- Funciones de aprendizaje para análisis automatizado en código abierto

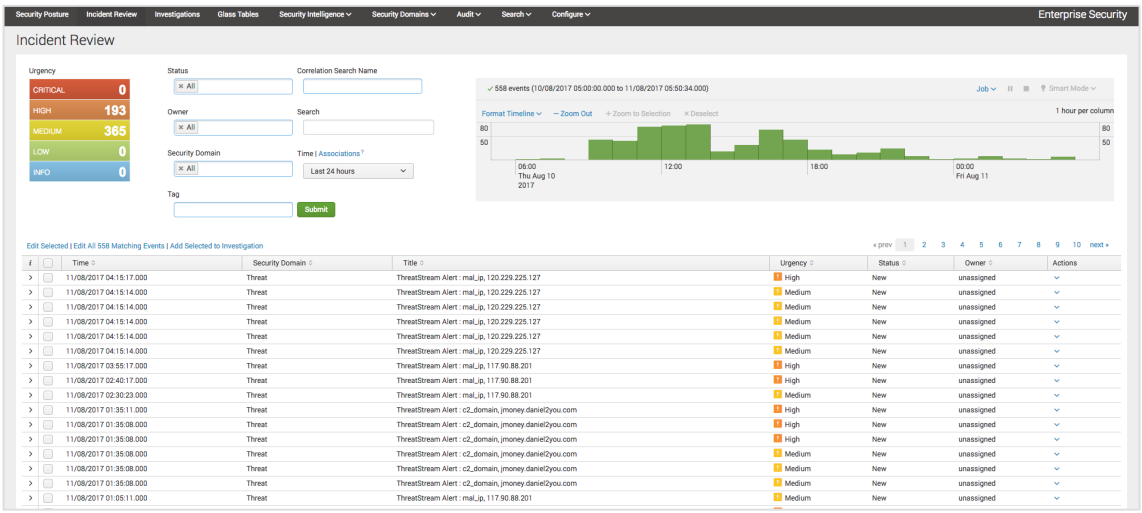

Figura 8: Consola de registros Splunk

2.2.4. Resumen de herramientas para la recolección de eventos

Mostramos una tabla resumen con las características más destacables de las herramientas analizadas que podemos utilizar para recoger los registros de nuestra red corporativa:

Tabla 2: Comparativa de características de las herramientas para recolección de eventos

	Kiwi Syslog	**Elastic**	**Splunk**
Instalable Windows	Si	Si	Si
Instalable Linux	No	Si	Si
Despliegue Windows	Manualmente	Manualmente	Manualmente
Despliegue Linux	No	Manualmente	Manualmente
Entorno gráfico datos	Si	Si	Si
Compatible IPv6	Si	Si	Si
Código abierto	No	Parcial	No
Importe	365 €	Gratis	173€

Debemos tener en cuenta que este servicio de recogida de eventos no es recomendable instalarlo en servidores compartidos, ya que hace una recolección bastante elevada de datos. Siguiendo la línea de compatibilidad nos decantamos por un sistema integrable en servidores Windows (si además tiene opción Linux mejor, aunque ahora mismo no es decisivo)

El análisis de las herramientas demuestra un alto grado de competitividad ofreciendo unas características similares y cumpliendo con los requisitos. Tan solo la capacidad de ampliación a servidor Linux y el coste económico nos decantan por la opción **Elastic Stack**, como seleccionada para llevar a cabo nuestro desarrollo.

3. Microsoft IPAM

En el siguiente apartado vamos a ver de manera detallada, la realización del despliegue de la herramienta seleccionada, para el control de direcciones IP en nuestro proyecto de mejora de red empresarial.

3.1. Conceptos previos al despliegue

Como en todos los despliegues empresariales que se tienen que llevar a cabo, debemos programar cuidadosamente los trabajos a realizar y la fecha de realización para que tenga el mínimo impacto posible en el servicio. También debemos planificar la manera de deshacer los cambios, es decir, hacer una marcha atrás en caso de que surja algún inconveniente no solucionable en el tiempo previsto.

La red a la que están orientadas las mejoras se encuentra en un entorno de virtualización con VSphere, y consta de un servidor principal replicado que alberga tres servicios críticos para la empresa: los relacionados con la autenticación de usuarios LDAP, préstamos de direcciones IP dinámicas DHCP y resolución de nombres DNS.

Lo ideal para llevar a cabo nuestras pruebas es realizar una copia en laboratorio de los servidores, lo que nos dará una imagen fidedigna al contar con el mismo estado y actualizaciones. En este punto también se debe tener en cuenta que las copias se realizan en horario no crítico, porque, aunque no existe un peligro de caída de servidor, sí debemos detener servicios y cargar de trabajo a la maquina mientras se clona. Si no se pudiera tener acceso a un entorno de pruebas fidedigno, es aconsejable instalar un servidor virtual e intentar ejecutar solo las mismas actualizaciones del servidor original.

Para nuestro caso no se ha realizado una clonación del entorno actual, pero se ha realizado la instalación del servidor al que vamos a aplicar nuestras modificaciones, junto con los servicios y actualizaciones pertinentes.

3.2. Requisitos de los sistemas

La herramienta Microsoft IPAM viene incluida en las versiones de Windows Server 2012, Windows Server 2012 R2 y Windows Server 2016 y permite compatibilidad de administración de servidores Microsoft Windows Server 2008 en adelante.

Es importante recalcar que el servidor que aloje el servicio IPAM debe ir instalado en un equipo independiente al de los servicios que da soporte, por lo tanto, los requisitos del sistema serán los mismos de Windows Server 2012:

Tabla 3: Requisitos hardware de instalación para Microsoft IPAM

Componente	Mínimo	Recomendado*	Máximo
Socket CPU	1,4GHz para 1 núcleo 1,3GHz para +1 núcleo	3,1GHz o superior en varios núcleos	2 zócalos
Memoria RAM	2GB 4GB en máquina virtual	16GB	64GB
Disco duro	160GB con partición del sistema de 60GB	---	Sin límite

*En este caso los valores recomendados son los requisitos necesarios para alcanzar el límite máximo de usuarios y dispositivos de sistema Windows Server.

3.3. Instalación de Microsoft IPAM

Partimos por lo tanto de un servidor Windows Server 2012 o superior, R2 en nuestro caso, que debe tener visibilidad de red con el servidor al que tiene que administrar, es decir debe formar parte del mismo dominio o tener relación de confianza con el mismo, por lo tanto, el primer paso es incluir el servidor Windows, dentro del dominio que vamos a controlar.

Para agregar el servicio iniciaremos la aplicación Consola de Administración (Server Manager). Los servidores de Windows normalmente abren la aplicación directamente cuando se inician, pero en caso contrario, la aplicación podemos encontrarla por defecto en la barra de tareas con un icono de maletín.

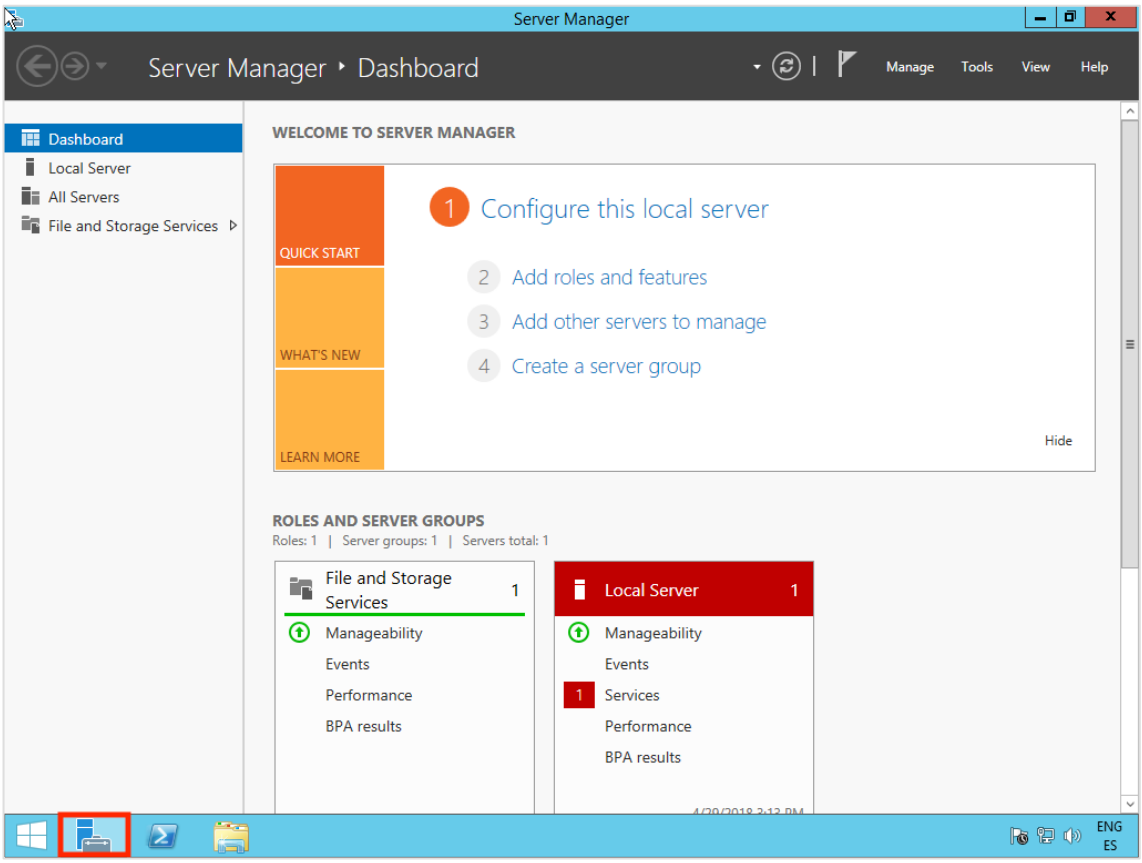

Figura 9: Consola administración de servidor Microsoft

La consola de Administrador del Servidor muestra un resumen actual del estado del servidor y en el panel lateral izquierdo podemos encontrar las funcionalidades generales y roles. Los menús desplegables que encontramos en la barra superior dan acceso a las herramientas para instalación de servicios y roles, además de herramientas para su posterior gestión.

Cuando hablamos de roles en Windows, nos referimos a programas que proveen del servicio definido por el rol a otros usuarios y computadores de la red. Las características

o funcionalidades también son programas que, aunque no forman parte directamente de los roles, mejoran la funcionalidad del servidor independientemente de los roles instalados. En ambos casos, si seleccionamos un rol o una característica, el asistente es capaz de resolver las dependencias entre otros servicios que a priori no deseamos, pero son necesarios. Dicha agrupación facilita a los administradores las labores de instalación y minimiza a posibilidad de errores en la misma.

Para iniciar la instalación de nuestra herramienta, seleccionamos en el menú superior la opción "Administrar", y dentro del desplegable la opción "Agregar roles y características":

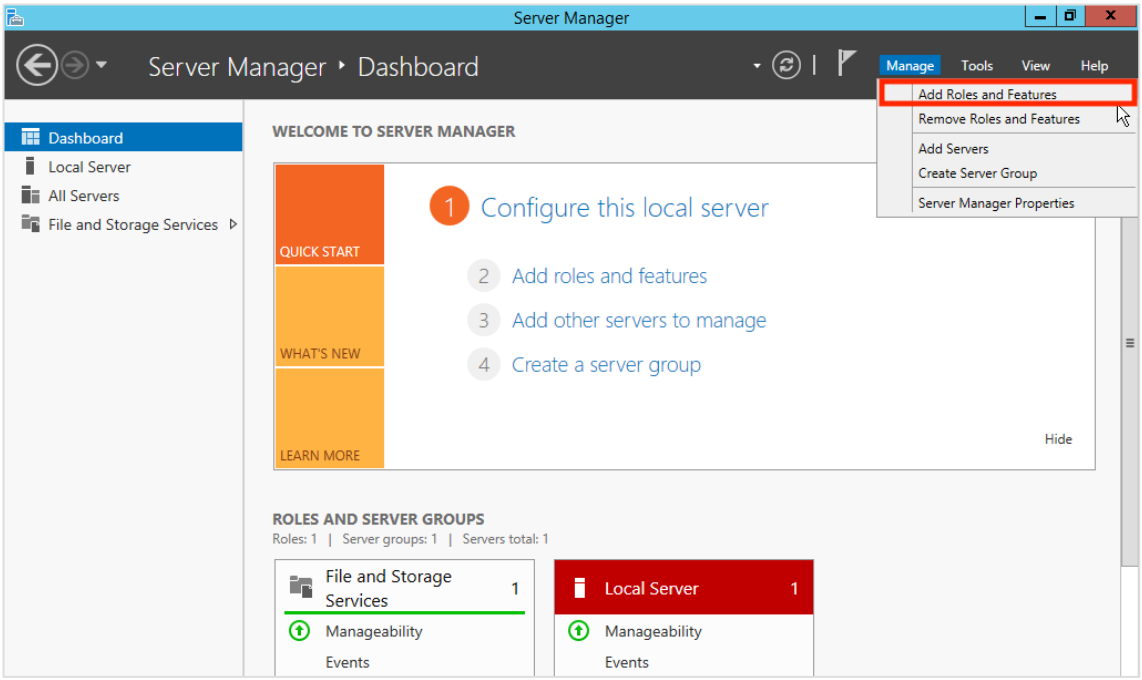

Figura 10: Agregar roles y funcionalidades desde la consola MS Server

En este momento se inicia el asistente que nos ayudará en el proceso de instalación para que nuestro servidor se convierta en el administrador de direcciones que deseamos. El asistente nos muestra una advertencia sobre los prerrequisitos que debemos cumplir antes de empezar a modificar la configuración, y son:

- La cuenta de administrador debe contener una contraseña compleja
- La red configurada debe tener una dirección IP estática
- Debemos tener instaladas las últimas actualizaciones recientes

El asistente no va a realizar las comprobaciones en este momento, pero en caso de no tener esos requisitos, en pasos posteriores de la instalación nos va a ser imposible avanzar.

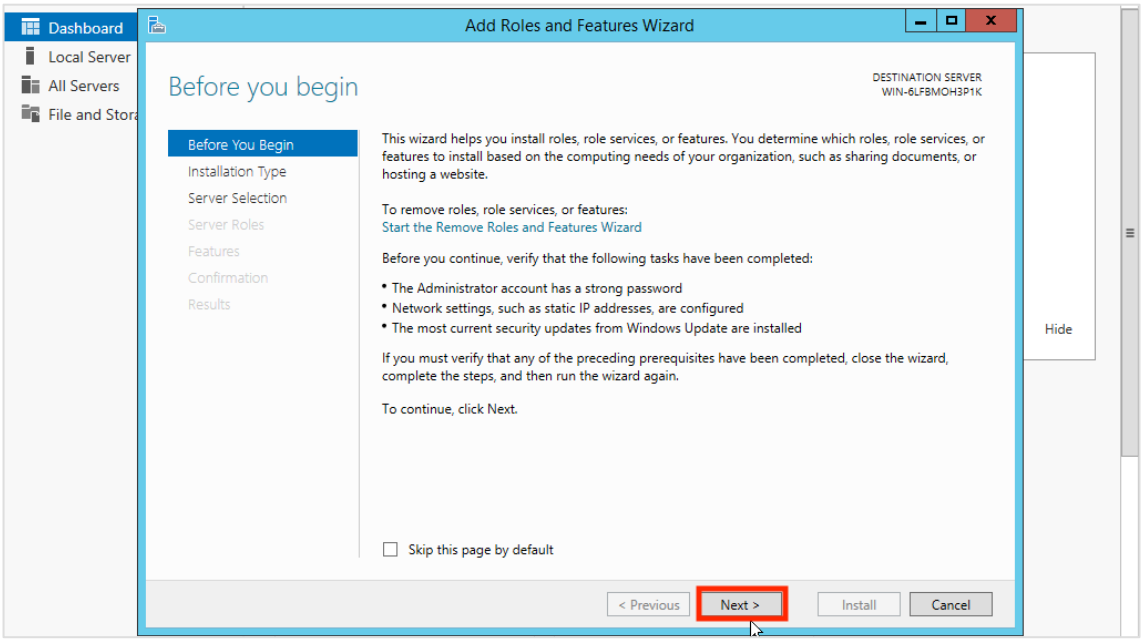

Figura 11: Advertencia de requisitos de instalación MS IPAM

Teniendo en cuenta los requisitos mostrados anteriormente, avanzamos pulsado el botón Siguiente del asistente.

En el menú posterior debemos seleccionar el tipo de instalación. Existen dos tipos de instalación la basada en roles o características y la basada en la instalación mediante escritorio remoto o RDS. A nosotros nos interesa la primera opción basada en roles, ya que lo estamos instalado directamente en nuestra misma máquina.

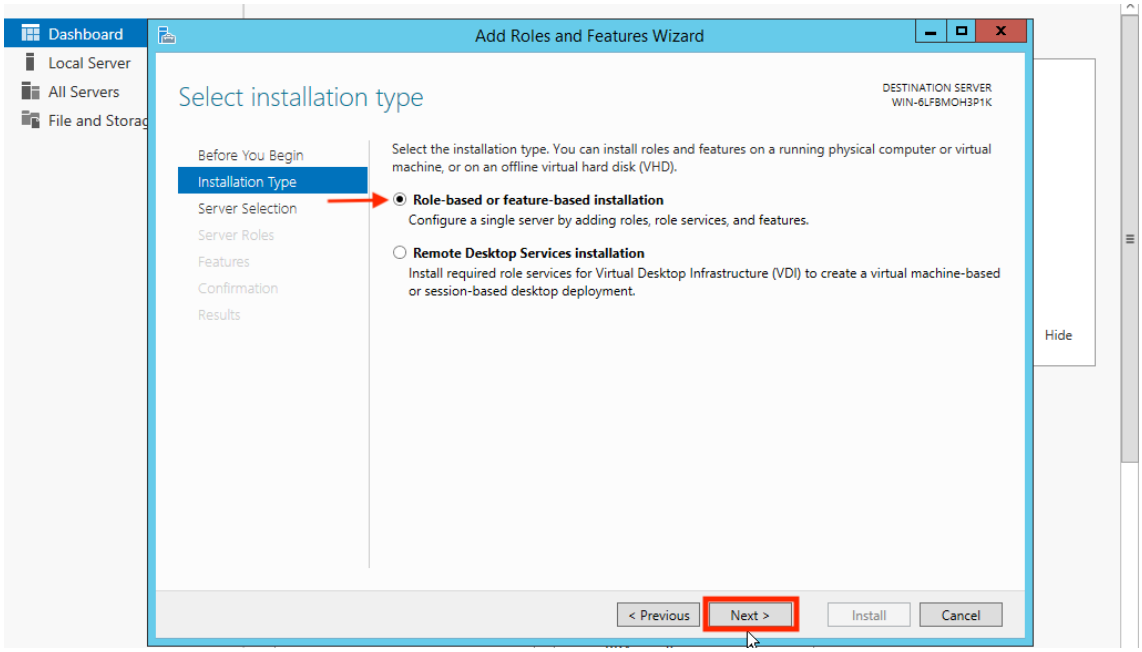

Figura 12:Selección del tipo de instalación para MS IPAM

Por lo tanto, seleccionamos la instalación basada en roles, y pulsamos continuar.

En la siguiente ventana, el asistente nos permite seleccionar el servidor donde vamos a realizar la instalación, en nuestro caso, seleccionamos el nombre del servidor "IPAM" que es el nombre que hemos dado para distinguirlo. La segunda parte que muestra del nombre es el dominio al que pertenecemos "*.sothis-ti.com*".

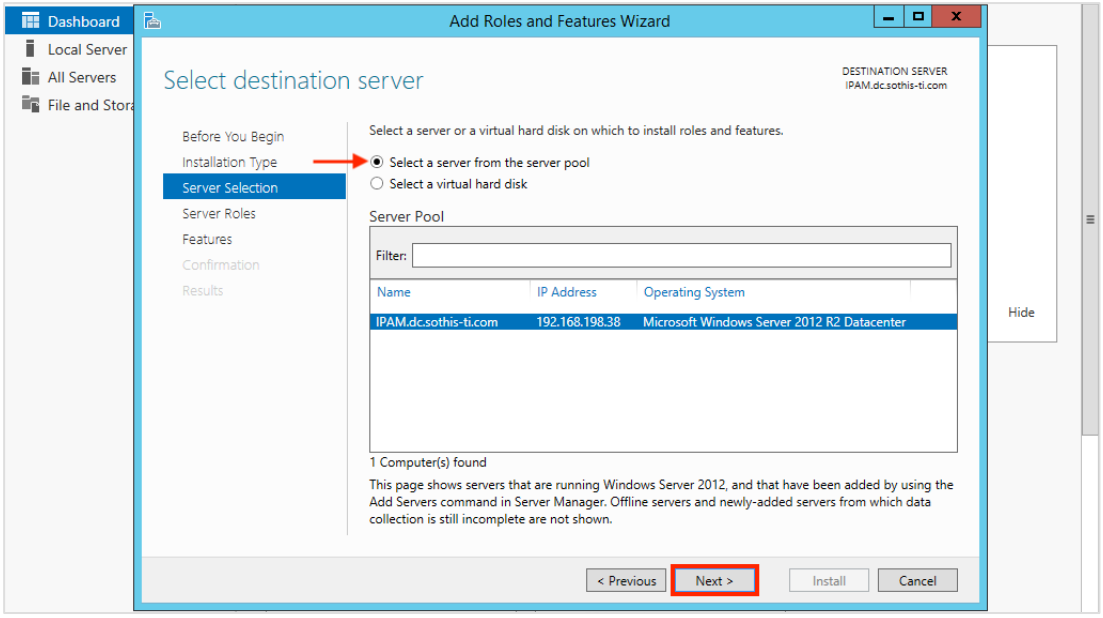

Figura 13: Selección de servidor principal donde se aloja el servicio IPAM

Marcamos nuestro servidor, y pulsamos siguiente.

El asistente muestra el selector de roles. El servicio que buscamos no es un rol, sino una funcionalidad, por lo que en esta pantalla no debemos marcar ninguna de las opciones que aparecen en el cuadro Roles.

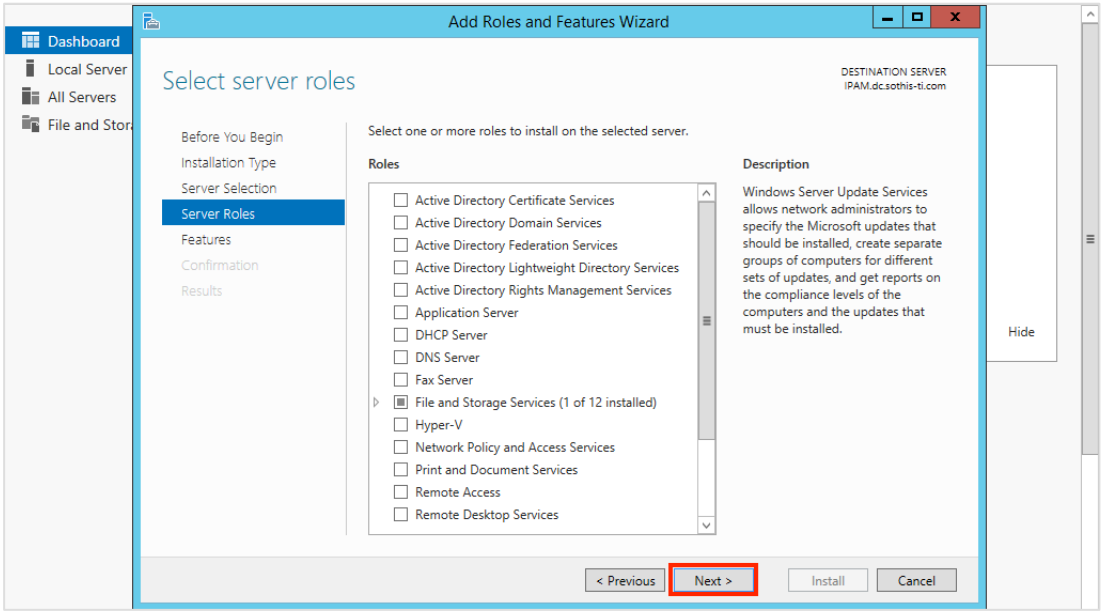

Figura 14: Añadir roles a servidor MS IPAM

Sin necesidad de realizar ninguna modificación de las opciones preseleccionadas, pulsamos el botón Siguiente.

El siguiente menú mostrado es el de funcionalidades. Dentro de las diferentes opciones que aparecen, debemos buscar la indicada como *IP Address Management (IPAM) server*.

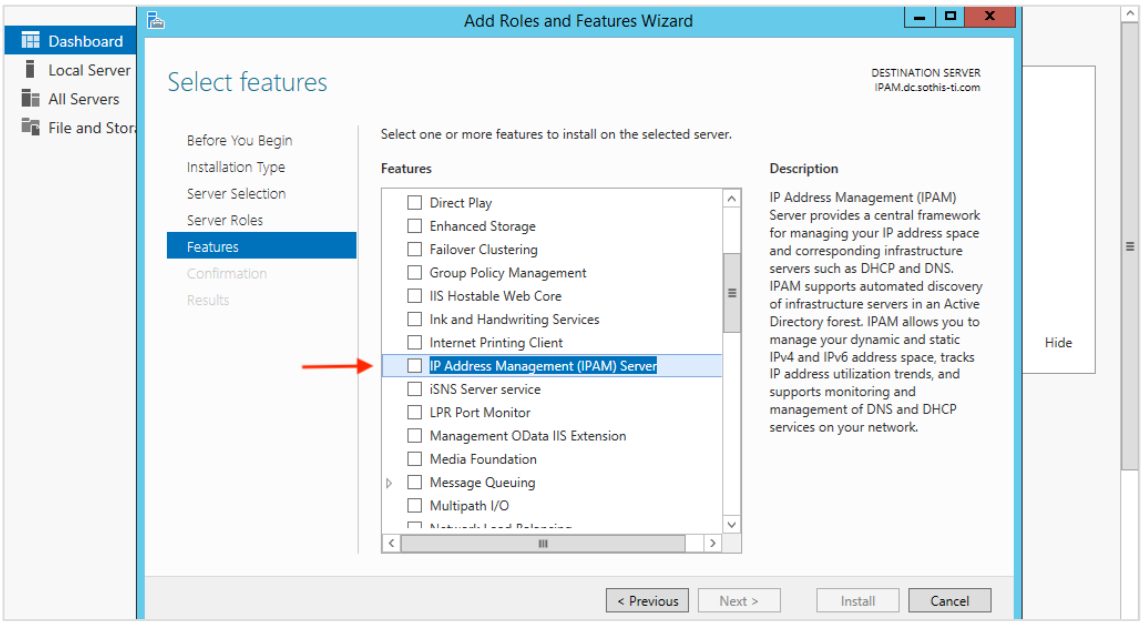

Figura 15: Añadir funcionalidades a servidor MS IPAM

Inicialmente vemos como si no hemos seleccionado ningún rol, ni ninguna característica, no permite avanzar. En este punto marcamos la casilla *IP Address Management* (Aparece sin traducir).

Inmediatamente después de haber marcado la casilla correspondiente de nuestro servicio, el asistente nos muestra una nueva ventana en la que nos indica los servicios necesarios que también debemos añadir, para que la característica que queremos instalar funcione correctamente.

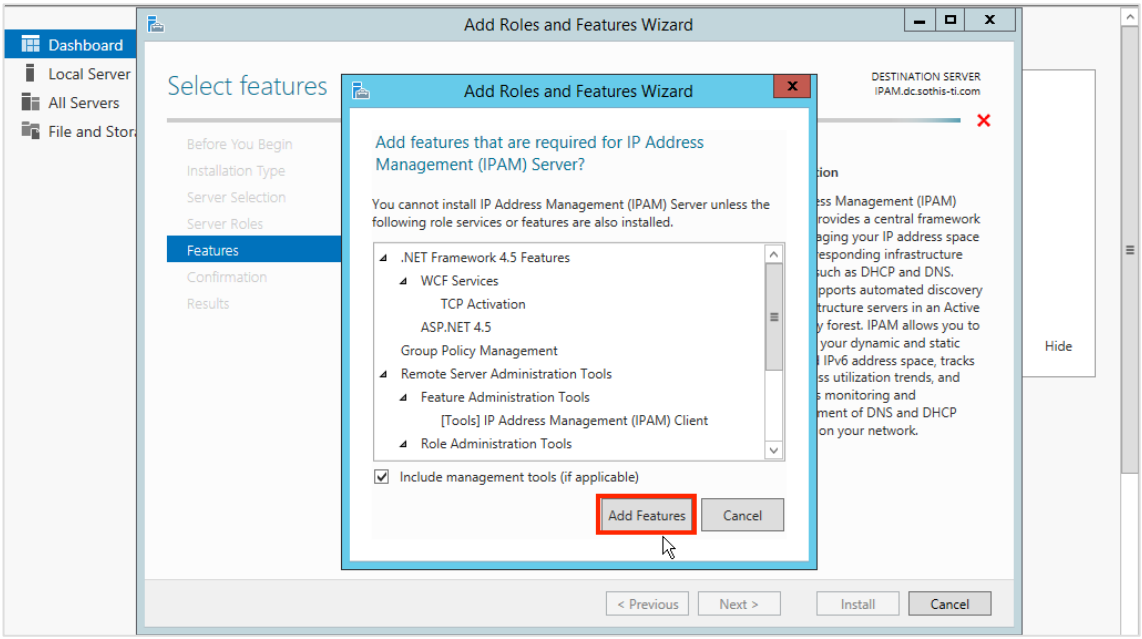

Figura 16: Inclusión de servicios necesarios de instalación MS IPAM

Se habilitan las características seleccionadas que disponemos a instalar:

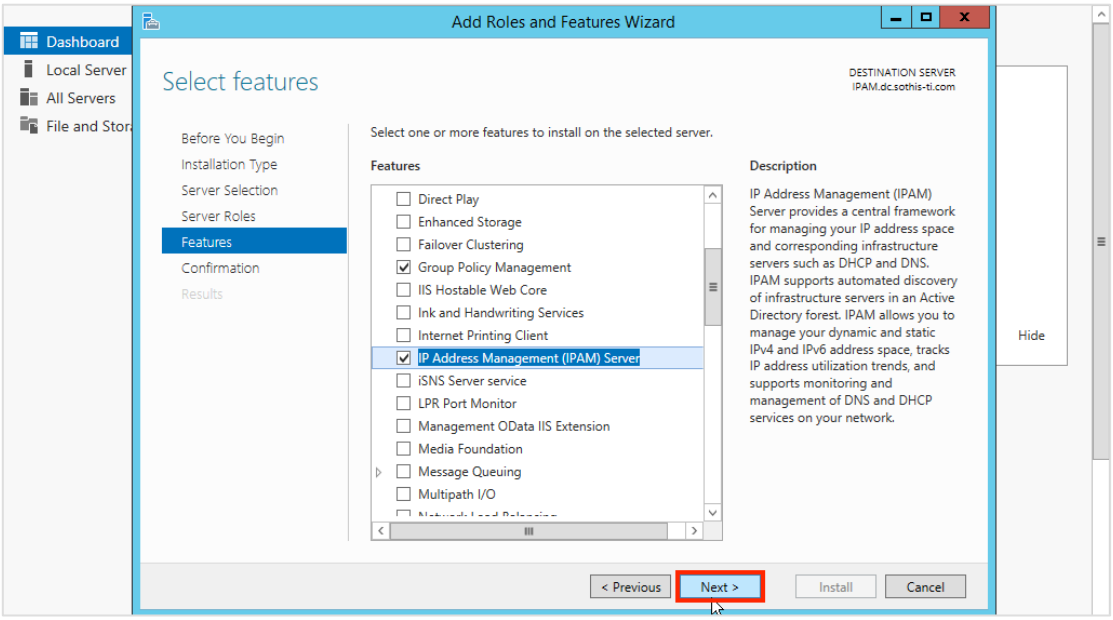

Figura 17: Selección de funcionalidades de servidor MS

Ahora el asistente sí nos permite continuar con la instalación, pulsamos Siguiente.

Nos aparece la información de lo que vamos a instalar a modo de resumen, con los servicios que hemos tenido que agregar. En este punto también podemos marcar la casilla de reinicio del servidor de destino si es necesario. Si lo seleccionamos, nos mostraría una confirmación y cuando llegara el momento necesario, lo reiniciaría automáticamente.

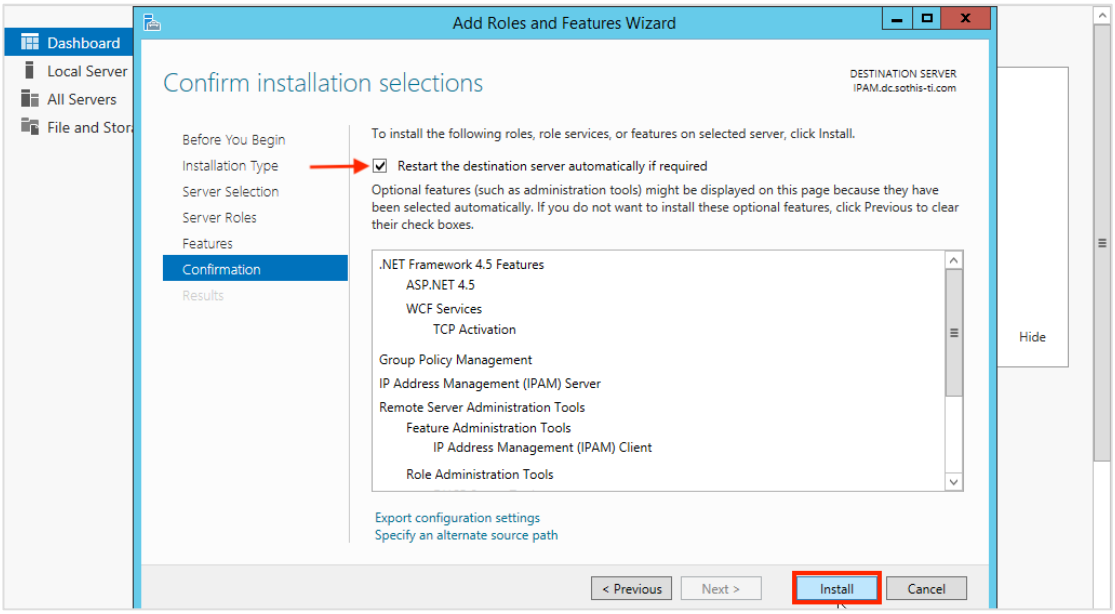

Figura 18: Confirmación de roles y funcionalidades a instalar en servidor MS

En nuestro caso, el servidor de destino de las modificaciones es el mismo en el que se está ejecutando el asistente, por lo que el reinicio será de nuestra máquina. Pulsaremos el botón instalar.

El asistente comienza a realizar la instalación mostrando una barra de progreso para darnos una referencia. En nuestro servidor de pruebas la instalación del IPAM ha durado aproximadamente ocho minutos.

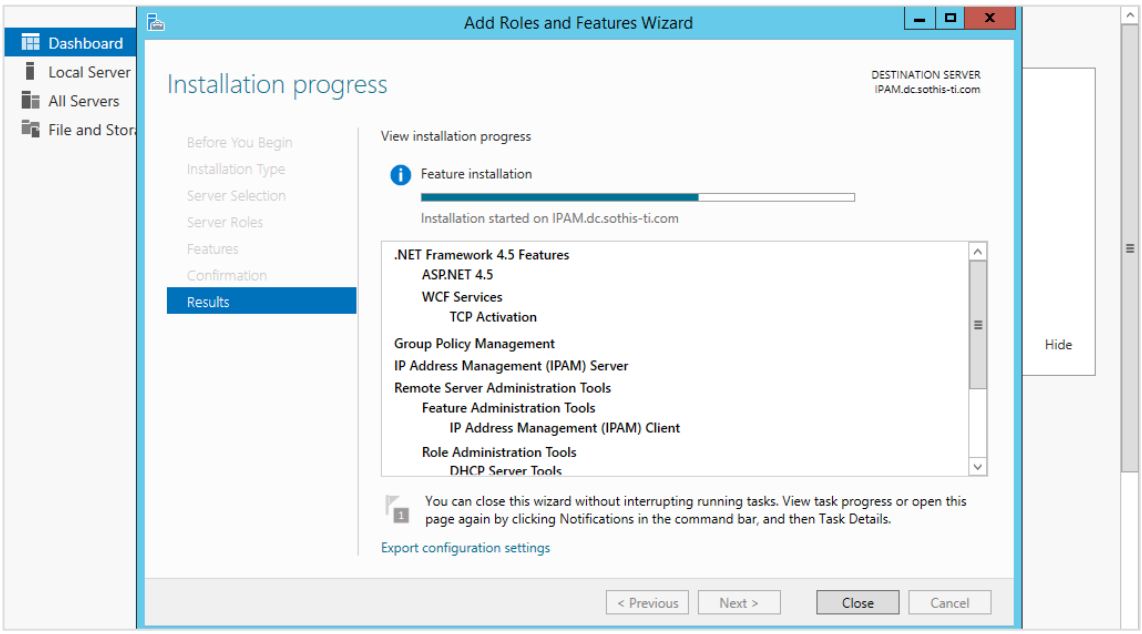

Figura 19: Instalación servicios en servidor MS 2012 R2

El asistente nos indica que podemos ocultar la ventana pulsando el botón cerrar, aunque no haya terminado la instalación, ya que nos avisará mediante una notificación de su finalización.

Una vez terminado de instalar nuestro software, podemos apreciar el menú lateral izquierdo, que aparece el nombre de la característica recién instalada.

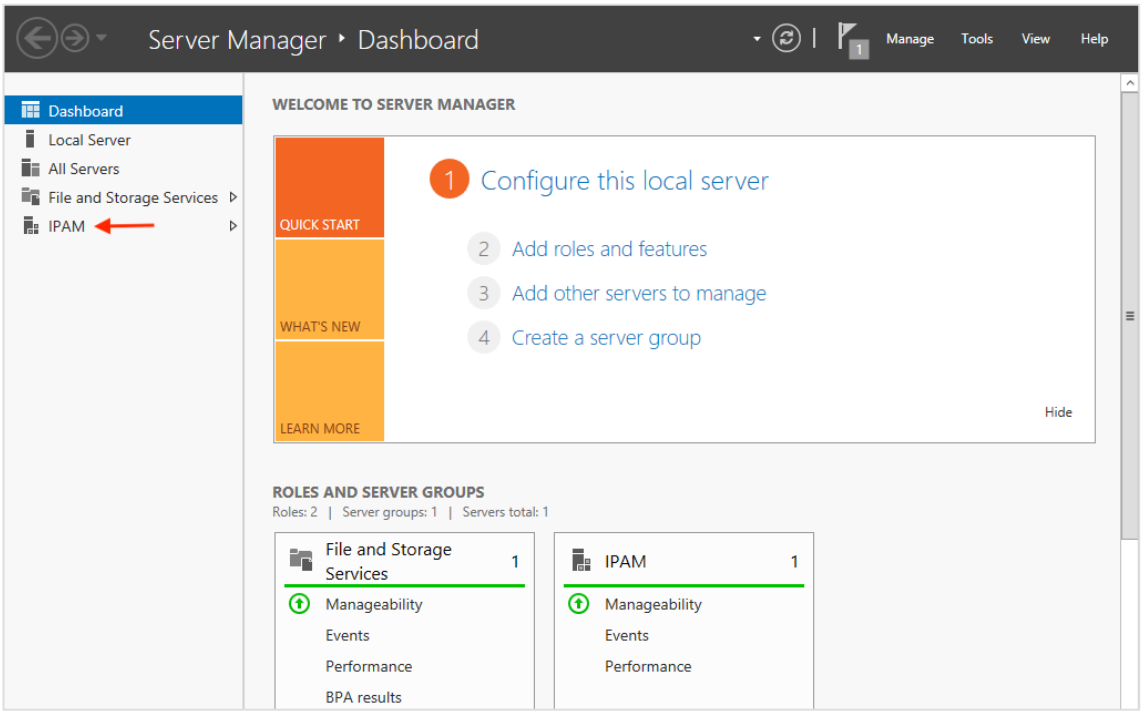

Figura 20: Consola principal de servidor MS con funcionalidad IPAM instalada

3.4. Configuración de Microsoft IPAM en servidor

Seleccionado directamente desde el administrador del servidor, la consola principal pasa de mostrar el resumen general del servidor, a darnos información específica sobre nuestra herramienta.

Sin perder el estilo principal de la consola, tenemos la opción de realizar un inicio rápido que aparece en la imagen como *Quick Start*, dividido en seis diferentes tareas numeradas que debemos ir completando por orden y que permiten ajustar los parámetros principales de nuestro gestor de direcciones.

En este punto debemos ser conscientes de la necesidad de haber iniciado sesión como un usuario Administrador del dominio, y no solo Administrador de la maquina local ya que parte de las tareas que realizamos afectan a otros servidores, si bien para la instalación del IPAM basta con ser solo Administrador local.

3.4.1. Conectar con servidor IPAM

La primera de las opciones que nos encontramos en el momento de configurar el IPAM es la de conexión con el servidor IPAM:

Figura 21: Asistente configuración - Conexión con servidor IPAM

Cuando seleccionamos la primera de las tareas denominada “Conectar con servidor IPAM”, el asistente hace un listado de los servidores con el servicio de administración de direcciones activo. En nuestro caso, el asistente lo estamos ejecutando en la máquina que da el servicio y es único, por consiguiente, solo muestra nuestro servidor.

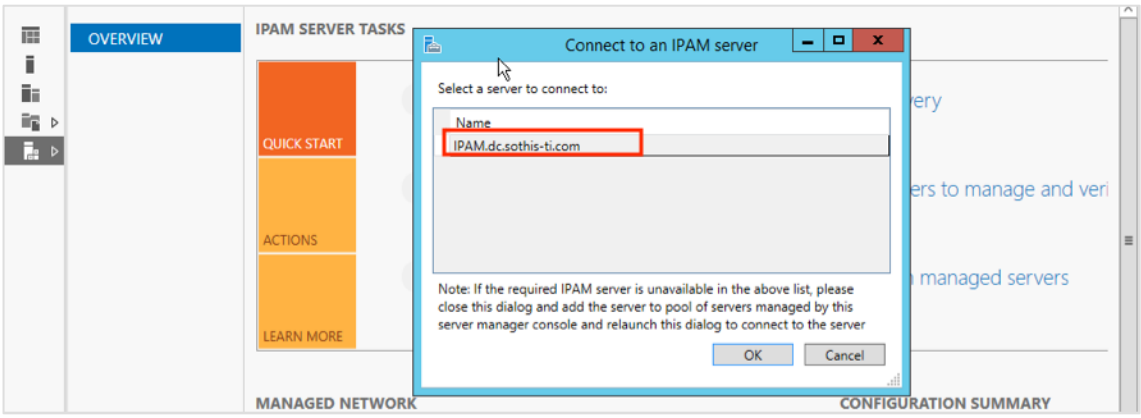

Figura 22: Asistente configuración selección de servidor de conexión

Seleccionamos nuestro servidor *IPAM.dc.sothis.com* y aceptamos pulsando ok. Acabamos de completar el primero de los seis pasos del asistente.

3.4.2. Aprovisionar el servidor IPAM

El segundo paso del asistente consiste en configurar la provisión del IPAM seleccionado anteriormente. Al igual que en ocasiones anteriores, nos irá dando alguna explicación y guiando en nuestro cometido.

Lo primero de todo es una introducción sobre las funcionalidades que ofrece la herramienta y que han sido explicadas en detalle con anterioridad. También nos advierte sobre el modo que queremos instalar para realizar dichas administraciones, ya que, si seleccionamos el modo automático o de política de grupo de objetos, no podremos cambiar al modo manual directamente. Este aspecto tendrá que ser decidido en pasos posteriores dónde veremos la diferencia entre ellos.

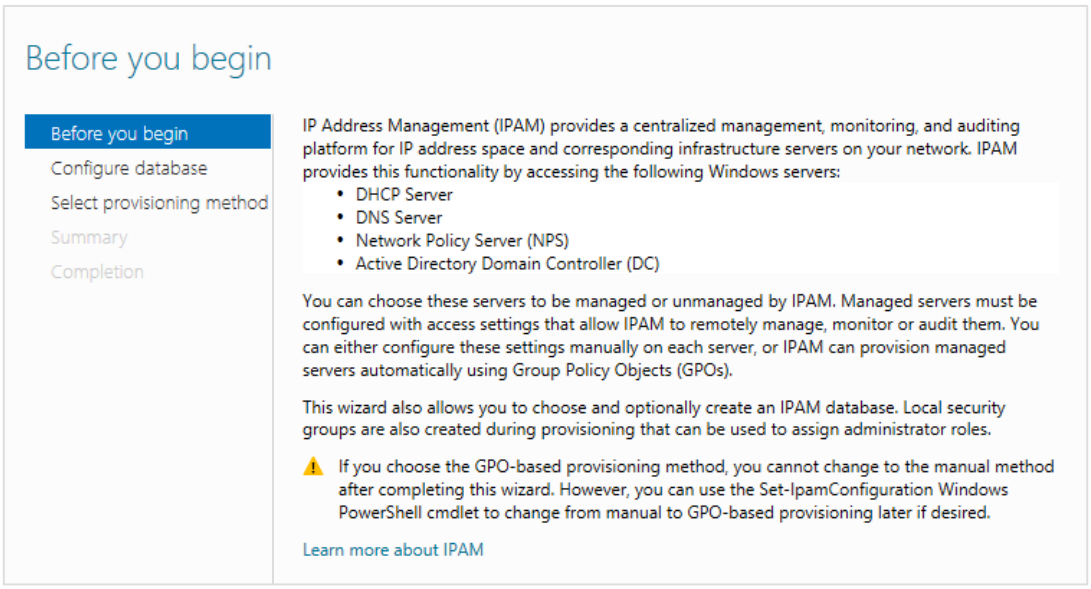

Figura 23: Advertencias de configuración iniciales en MS IPAM

Una vez leídas las advertencias de configuración, podemos continuar con el siguiente conjunto de opciones pulsando el botón Siguiente.

Toda la información recopilada de nuestra red es almacenada en una base de datos para posteriormente ser analizada y mostrada bajo demanda.

Windows nos muestra dos opciones diferentes de base de datos:

- Base de datos interna de Windows WID
- Servidor Microsoft SQL

Sobre las ventajas de seleccionar una base de datos u otra, ciertamente SQL ofrece mayor rendimiento cuando existe una gran cantidad de información, pero debemos de tener en cuenta que SQL necesitaría otra licencia adicional, por lo tanto, como nuestra base de datos de IPAM no va a ser extensa, vamos a seleccionar la primera de las opciones, WID, que almacena los datos en local dentro del directorio de la herramienta y de una manera sencilla y funcional.

Pese a que el límite de la base de datos WID es de 254GB y resulta extremadamente difícilmente alcanzar ese máximo mediante datos de IPAM, Microsoft pone a disposición la migración a base de datos SQL mediante PowerShell usando la instrucción: *Move-IpamDatabase*.

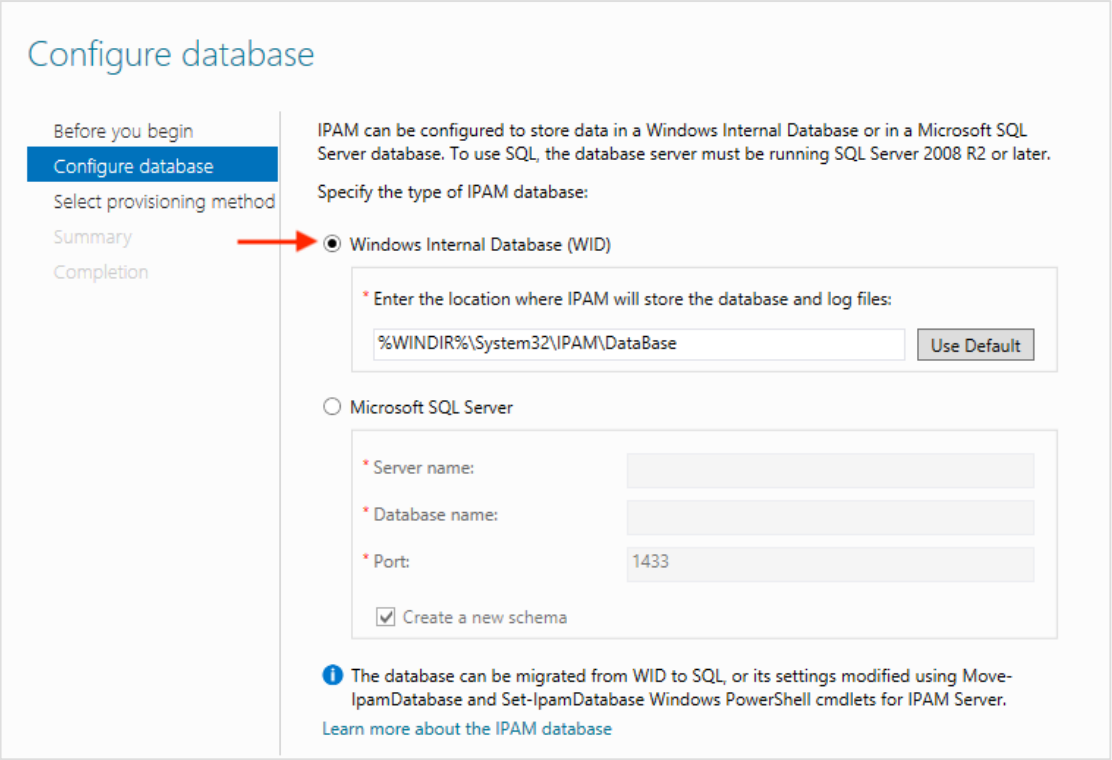

Figura 24: Configuración de la base de datos del servidor IPAM

Seleccionamos la base de datos interna de Windows, su localización puede ser modificada teniendo en cuenta las capacidades de los discos duros destino. Para una empresa con 1.000 equipos a gestionar, un tamaño de almacenamiento de 60 GB será más que suficiente. Pulsamos el botón siguiente para avanzar.

Llega el momento de seleccionar el tipo de aprovisionamiento deseado. Nos referimos a los dos tipos de administración que dispone nuestro IPAM y a los cuales el asistente nos hizo una advertencia al comenzar la configuración:

- Administración manual: Utilizada solo si el número de servidores a administrar es pequeño, requiere que una vez realizamos la instalación, compartamos los recursos, hagamos los grupos de seguridad en los servidores que queremos administrar y configuremos las reglas del cortafuegos de una manera completamente manual. Además, si lo deseleccionamos algún servidor para dejar de administralo también debemos remover manualmente dichos ajustes. Es el método más complejo y menos consistente que el basado en GPOs.
- Administración basada en política de grupos GPOs: es el método recomendado y casi obligado cuando trabajamos con redes complejas, ya que buscamos una herramienta que nos facilite la gestión y no únicamente la centralización. Una GPO es una política de grupo que sirve para establecer configuraciones o parámetros que afectan a nuestro dominio, como pueden ser las típicas empleadas para no permitir cambiar el fondo de escritorio, pero existen otras

tantas mucho más avanzadas. En esta modalidad de configuración el asistente crea una GPO (por dominio administrado) y se encarga de ajustar las configuraciones de dichas políticas. Para optar por este método debemos seleccionar manualmente el prefijo que queremos utilizar ya que genera un grupo de políticas para cada servicio.

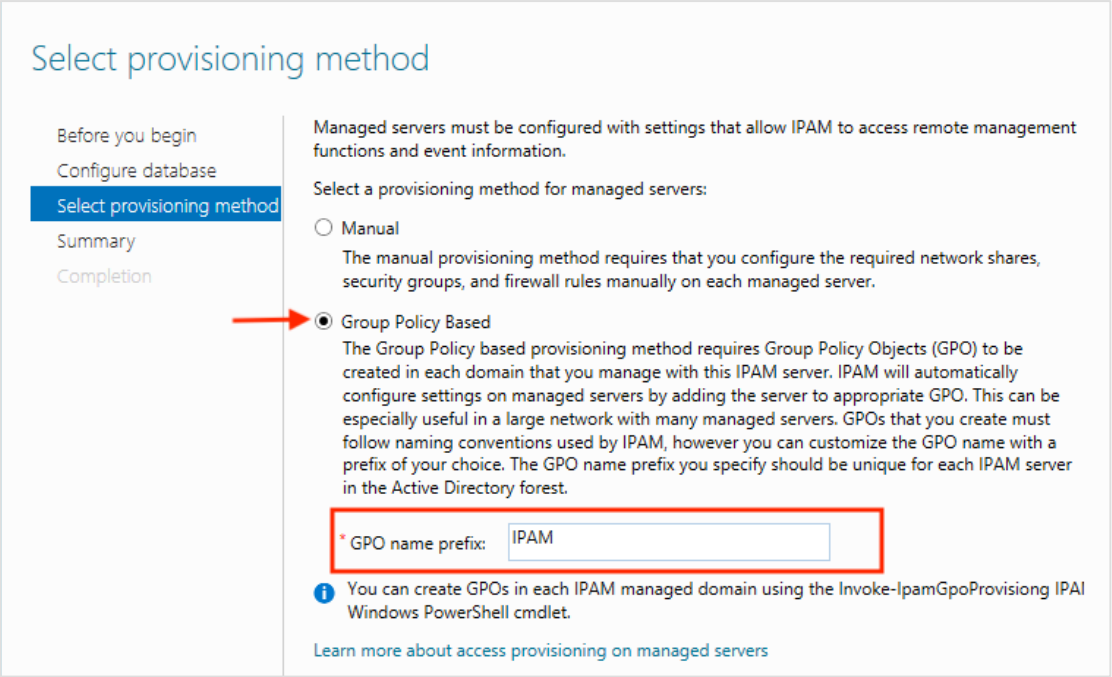

Figura 25: Selección del método de provisión para gestión de red

Seleccionaremos administración basada en políticas y debemos de indicar el prefijo de la política. En nuestro ejemplo hemos seleccionado también IPAM y luego el asistente se encarga de completar el nombre por servicio de la siguiente manera:

- <Prefijo-GPO>_DHCP: Este GPO es usado para aplicar ajustes que permiten al IPAM administrar y recoger datos de los servidores con servicio DHCP de la red
- <Prefijo-GPO>_DNS: Este GPO es usado para aplicar ajustes que permiten al IPAM administrar y recoger datos de los servidores con servicio DNS de la red
- <Prefijo-GPO>_DC_NPS: Este GPO es usado para aplicar ajustes que permiten al IPAM recoger información de los controladores del dominio y de las políticas de red (NPS) y así poder realizar seguimientos de direcciones IP

El sistema nos muestra un pequeño resumen con las opciones seleccionadas en las que podemos apreciar los nombres creados para las GPOs. Una vez más nos vuelve a advertir sobre la imposibilidad de modificar el tipo de administración para la selección avanzada realizada.

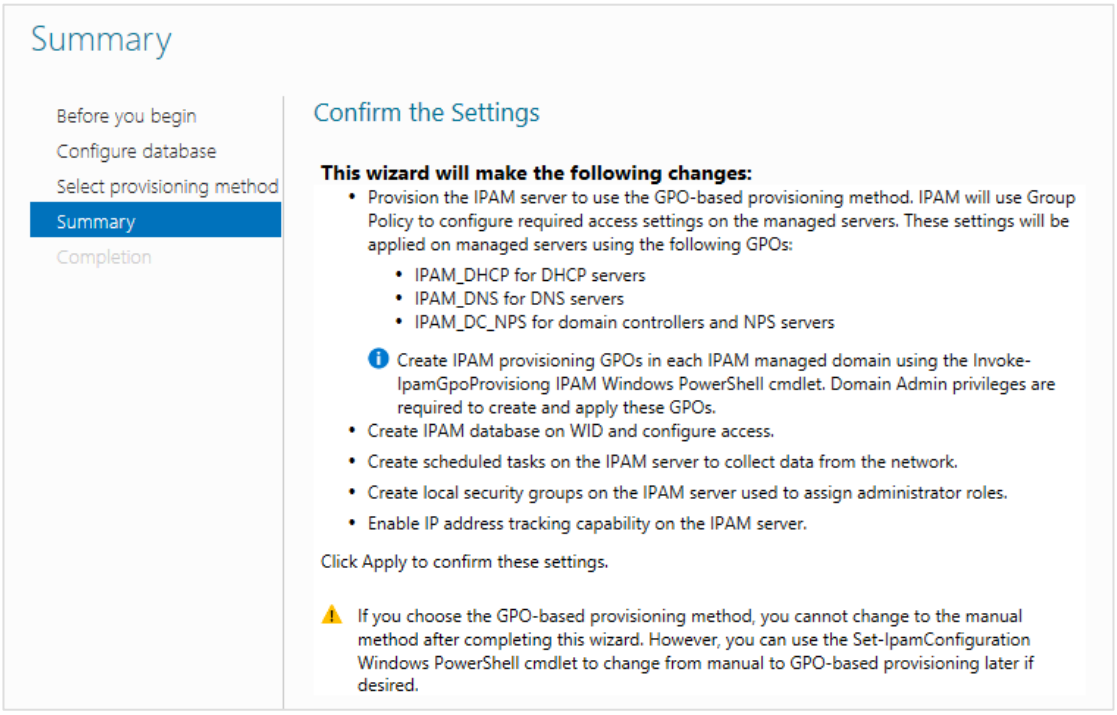

Figura 26: Resumen de parámetros de configuración del servidor IPAM

Pulsamos aplicar y comenzará la instalación del segundo paso del instalador.

Una vez finalizada la instalación en la que una barra de progreso nos muestra la información del aprovisionamiento, el asistente nos insta a proseguir con el siguiente paso en el cual debemos hacer uso de una consola PowerShell.

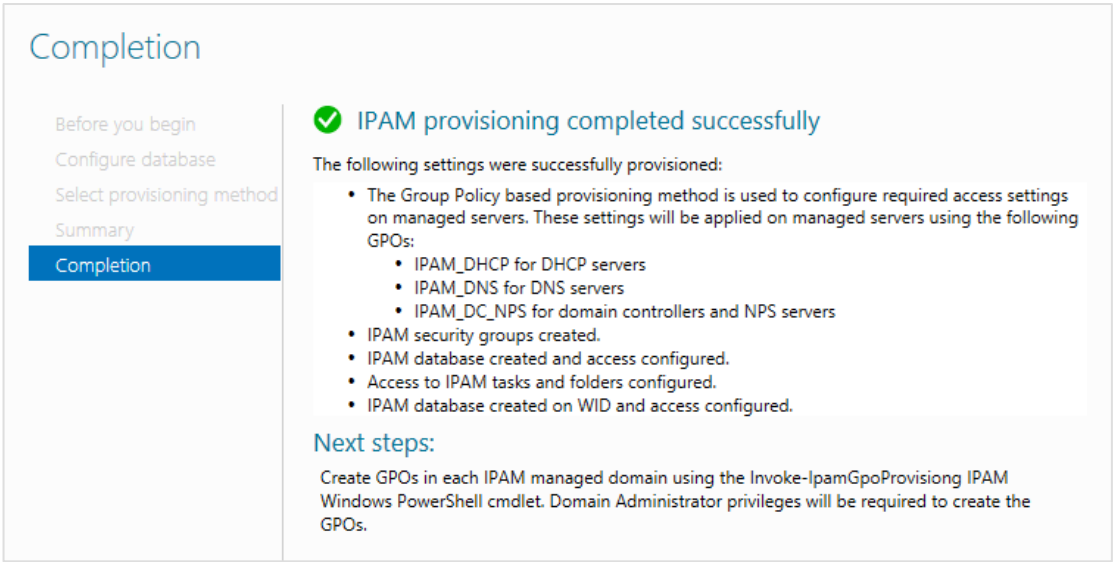

Figura 27: Confirmación de instalación sin errores en los servicios

A continuación, vamos a crear las GPOs correspondientes que van a permitir tareas de administración a nuestro servidor IPAM sobre los servicios seleccionados Desde el servidor IPAM abrimos una consola PowerShell, recordad que nuestro usuario debe tener permisos de administrador de dominio, e introducimos el comando:

*Invoke-IpamGpoProvisioning -Domain **X** -GpoPrefixName **Y** -IpamServerFqdn **Z***

-*Domain*: nuestro dominio, para este caso particular: dc.sothis-ti.com

-*GpoPrefixName*: el nombre del prefijo que hemos seleccionado anteriormente: IPAM

-*IpamServerFqdn*: es el nombre completo del servidor en el dominio y se compone del nombre de nuestro controlador de dominio (equipo que aloja los servicios llamado *dc1*), más el nombre del propio dominio, por lo tanto, el FQDN será: *dc1.dc.sothis-ti.com*

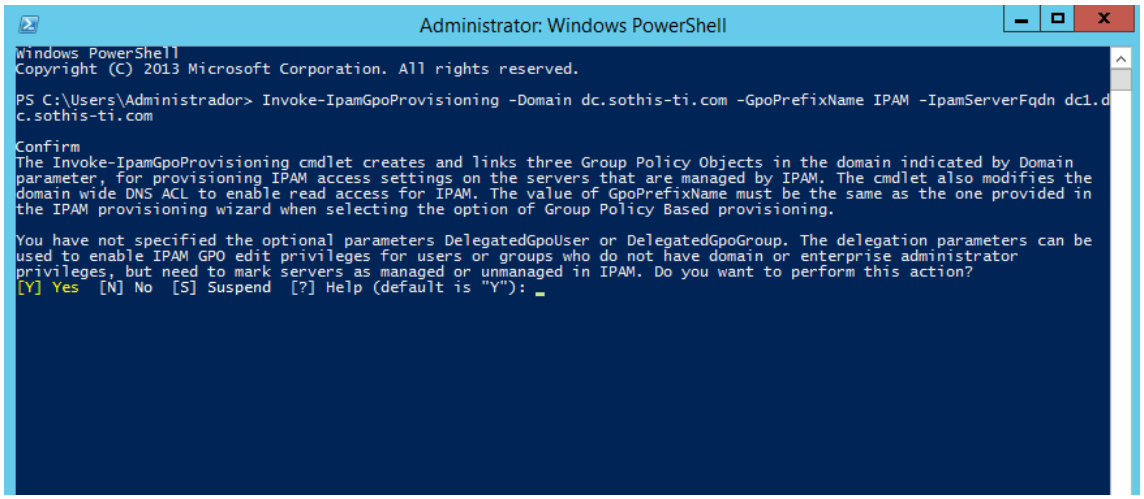

Figura 28: Modificación de políticas en remoto desde servidor IPAM a servidor administrado DC

¿Qué cambios realizamos con este comando en el servidor con los servicios a gestionar?

Los cambios de configuración que realizamos son principalmente a nivel de GPOs. Para poder apreciar las modificaciones que realizamos, visualizamos la configuración actual de la consola de administración:

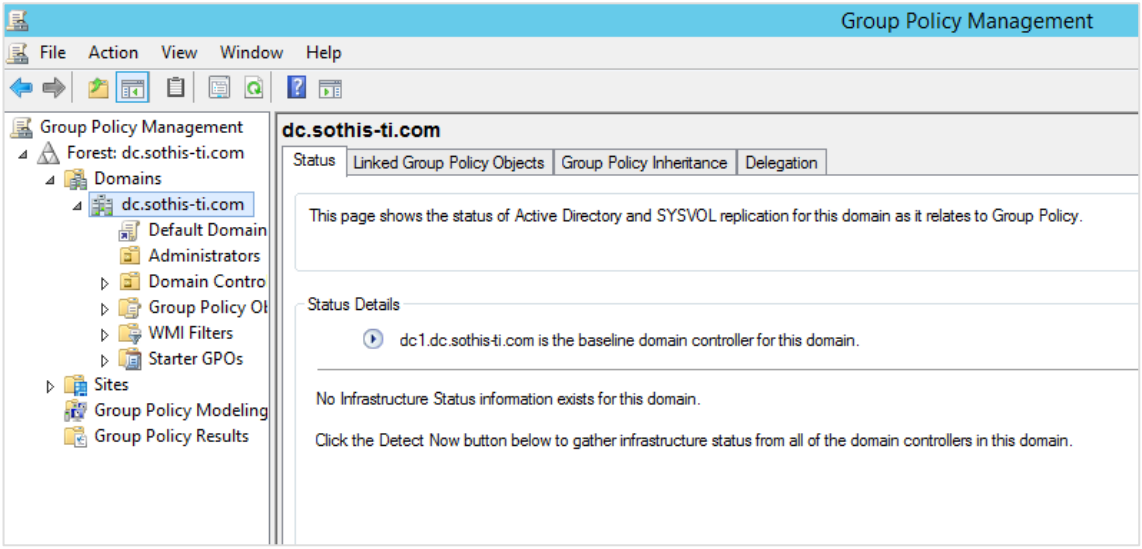

Figura 29: Visualización de políticas GPO previas a modificaciones en servidor principal DC

Y una vez ejecutado el comando de PowerShell "*Invoke-IpamGpoProvisioning*" actualizamos la información, obteniendo:

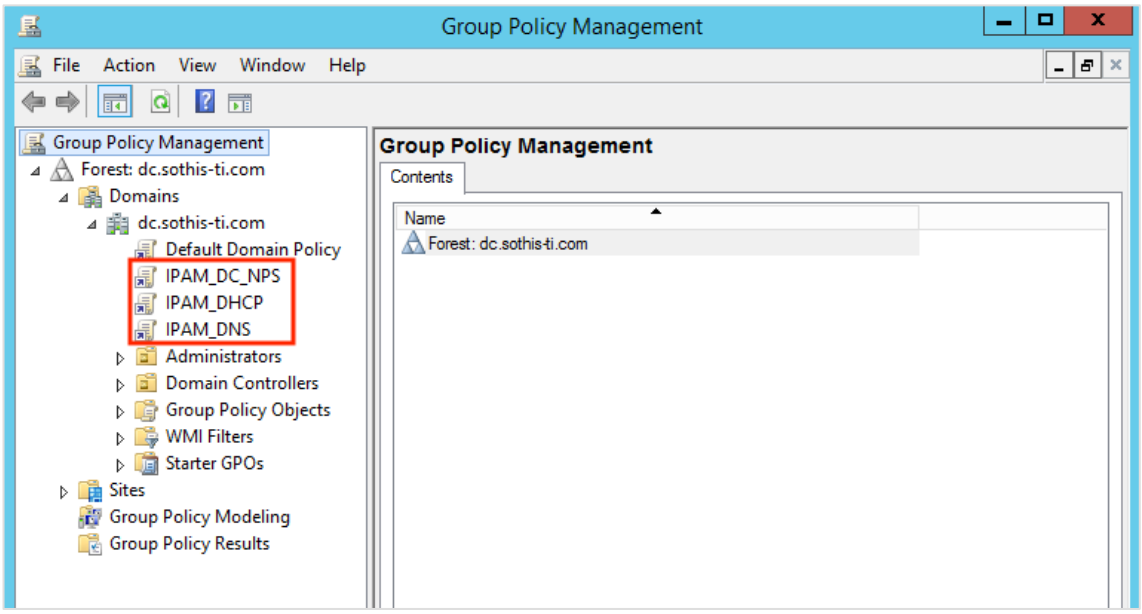

Figura 30: Visualización de políticas GPO modificadas en servidor principal DC

Como podemos ver se han creado en nuestro controlador de dominio, las tres directivas con los nombres indicados en el asistente, una para cada servicio.

Si exploramos con detalle las políticas de grupo, también encontramos que se encuentran asociadas a un nuevo usuario de dominio denominado IPAMUG:

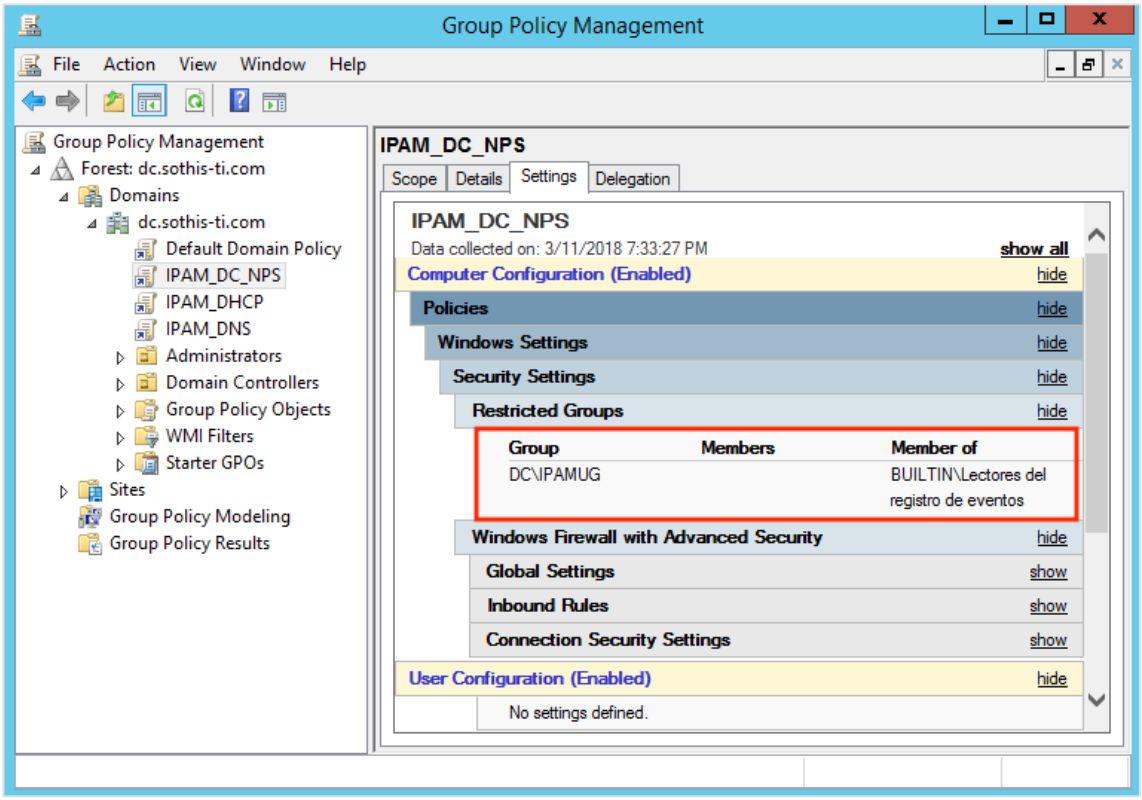

Figura 31: Detalle de grupo específico creado en servidor principal

Confirmamos que dentro del directorio activo se ha introducido el usuario IPAMUG de tipo Universal y con permisos de administración.

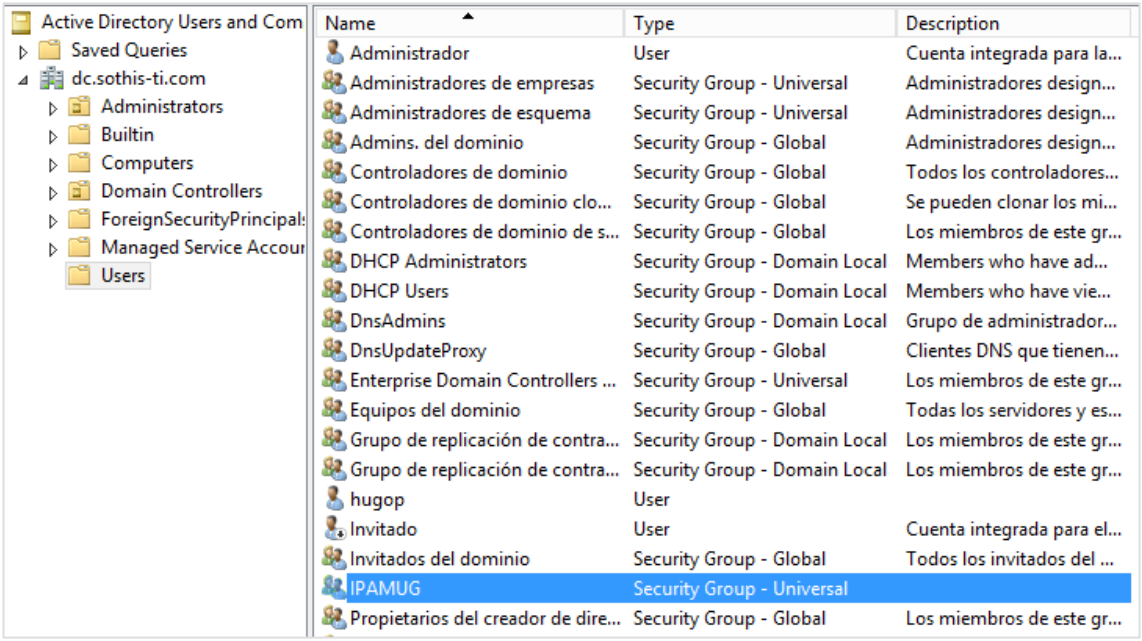

Figura 32: Usuario universal generado en dominio DC para administración

Debido al nuevo usuario IPAMUG y las GPOs creadas, el servidor IPAM es capaz de recolectar y gestionar los diferentes servicios.

3.4.3. Configurar detección de servidores

La tercera parte del asistente es la referida a la definición de los dominios que el servidor IPAM puede monitorizar y administrar. Esto es debido a que nuestro mismo servidor puede ser usado para múltiples dominios siempre y cuando forme parte de su bosque de Active Directory. Al seleccionar dicha opción nos muestra un desplegable con los servidores de dominio, basta con seleccionar el nuestro y añadirlo a la lista.

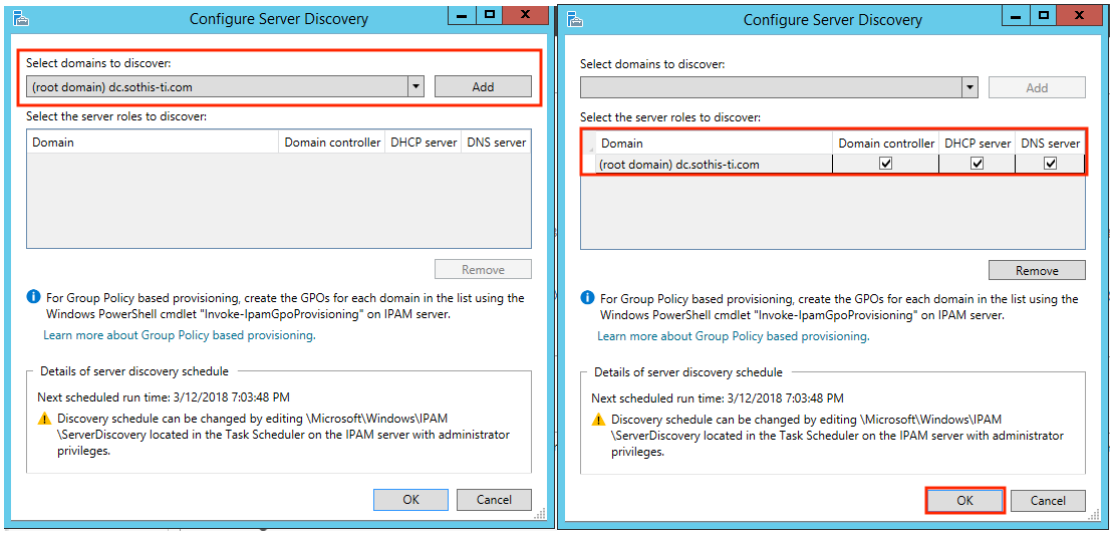

Figura 33: Selección de zona de descubrimiento de servidores y servicios

El asistente automáticamente detecta los servicios disponibles para escanear y desde aquí podemos marcar y desmarcar los servicios de manera individual para cada servidor. Nosotros seleccionaremos todos los servicios que puede gestionar nuestra aplicación IPAM y aceptamos.

3.4.4. Iniciar detección de servidores

El paso numero cuatro del asistente consiste en ejecutar la tarea de recopilación de datos sobre los servidores seleccionados en el paso anterior. Son tareas cuyo tiempo de ejecución depende de la cantidad de equipos de la red a analizar y de la cantidad de información que generan los mismos.

A diferencia del resto de pasos, este paso podríamos omitirlo y se ejecutaría automáticamente sin nuestra intervención, esto es debido a que en el paso anterior (tres), el asistente agrega directamente una programación de la tarea. Como nosotros queremos avanzar en nuestro desempeño, pulsamos el enlace “Iniciar detección de servidores” y aunque no muestra ninguna nueva pantalla, en la parte superior si aparece un pequeño texto informativo con un enlace que nos permite ampliar la información.

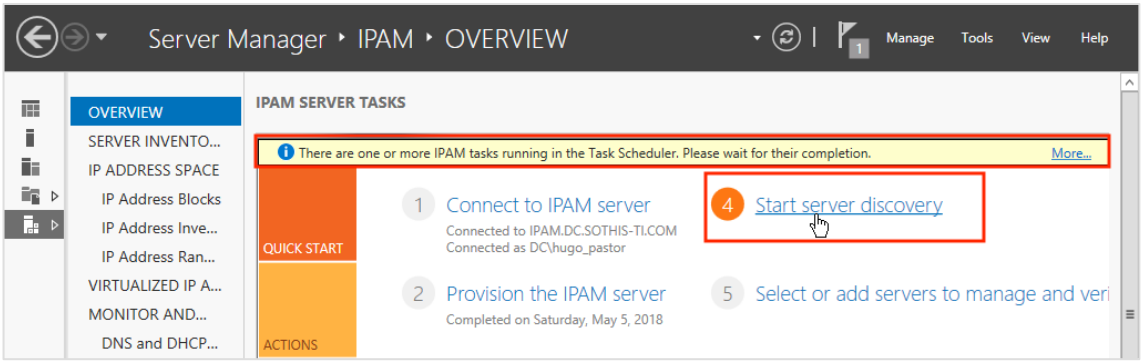

Figura 34: Inicio de detección de servidores en dominio seleccionado

Pulsando sobre el enlace informativo denominado Mas... obtenemos un cuadro informativo con las tareas de ejecución, el estado actual (completado, en curso, cancelado), información de cuándo ha iniciado la tarea y de cuándo se volverá a ejecutar.

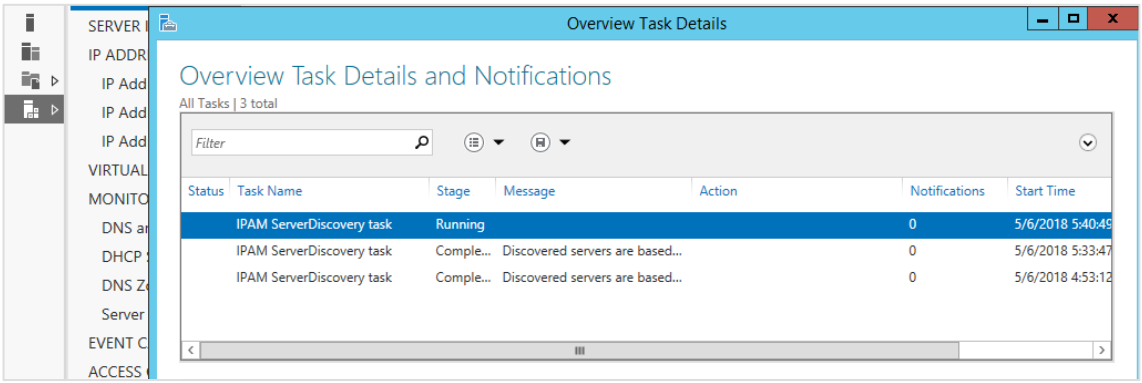

Figura 35: Estado de las tareas de recopilación de información

Si no modificamos los valores por defecto, el tiempo fijado para los intervalos de ejecución es de 60 minutos desde finalización hasta el nuevo inicio de tarea.

3.4.5. Seleccionar o agregar servidores para administrar y acceso de IPAM

En este momento debemos seleccionar los servidores junto con los servicios que nos interesen administrar. El procedimiento para ello es asignando al servidor un estado denominad de administración (*manageability*).

Para ello pulsamos en el enlace del asistente IPAM numero 5 indicado como *"Seleccionar o agregar servidores para administrar y comprobar el acceso de IPAM"*.

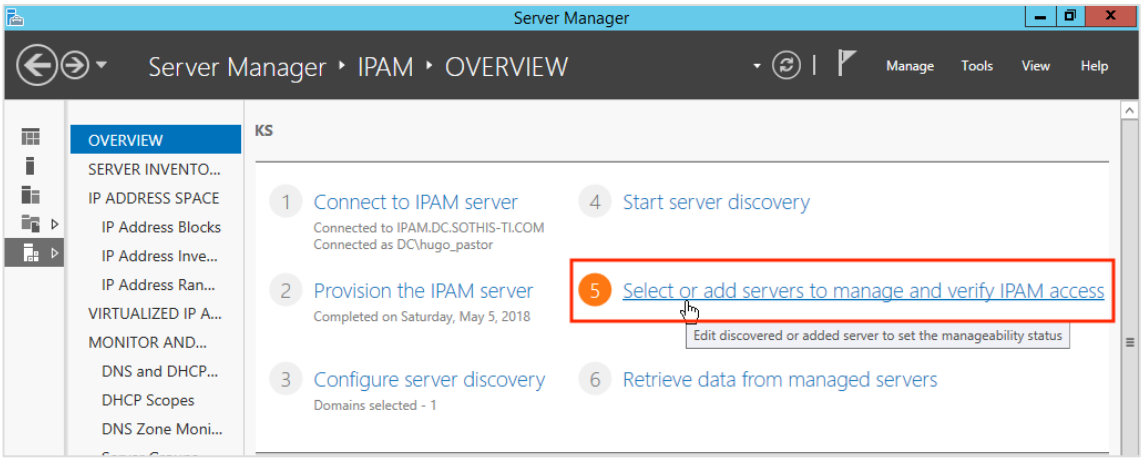

Figura 36: Selección de servidores para administrar en asistente

Se desplegará una ventana con una acción recomendada que incluye una señal de advertencia debido a que todavía no hemos ajustado dichos parámetros. También podemos ver como el estado actual del servicio IPAM es "bloqueado" ya que todavía no hemos configurado la administración:

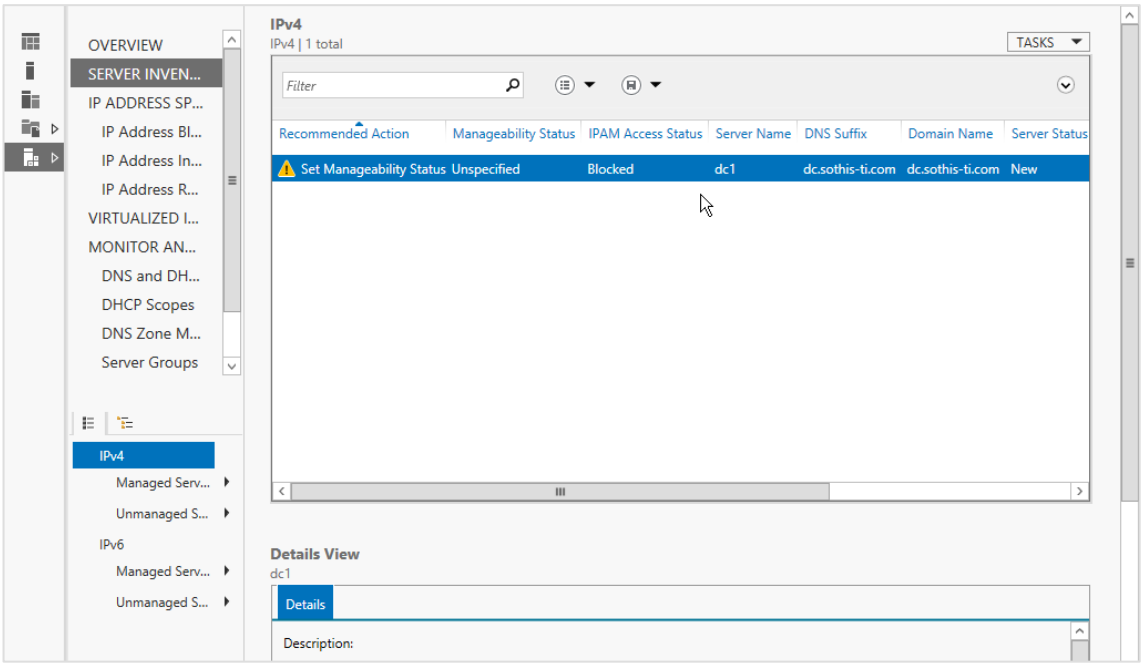

Figura 37: Visualización inicial-bloqueada del servidor administrado DC

Basta con seleccionar la lista de servidores descubierta y pulsando la opción editar con botón secundario, aparece una nueva ventana emergente con los servicios disponibles. Debemos seleccionar los servicios que nos interese administrar, todos los indicados son administrables por el IPAM de manera independiente, y una vez seleccionados cambiamos el estado a "Administrado" (*managed*).

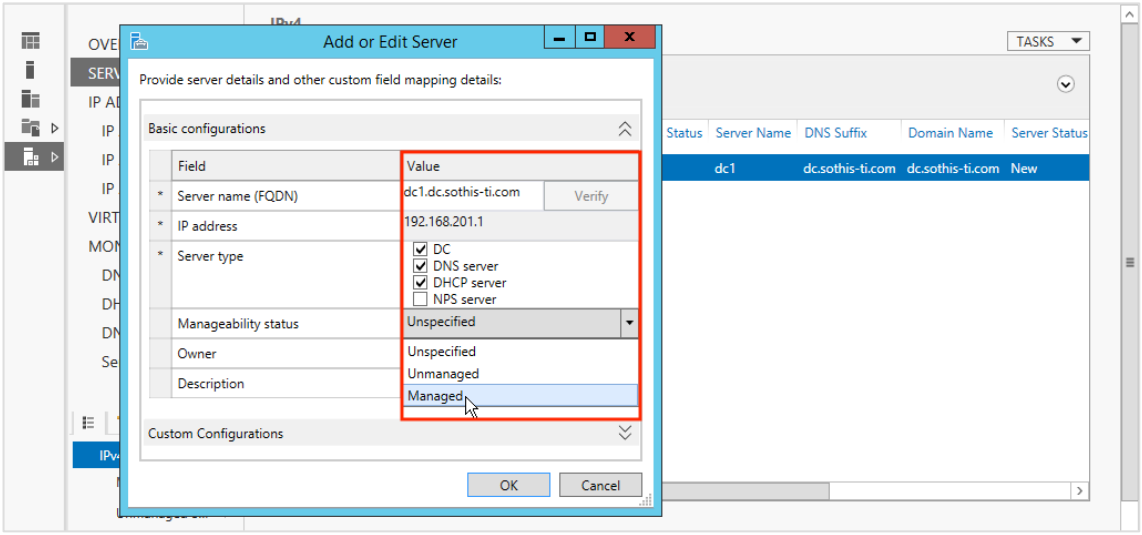

Figura 38: Activación de servicios administrados remotos desde servidor IPAM

Desde ese momento el estado del servidor cambia del estado "No especificado" a "Administrado" y el estado del acceso IPAM del estado "Bloqueado" a "Desbloqueado".

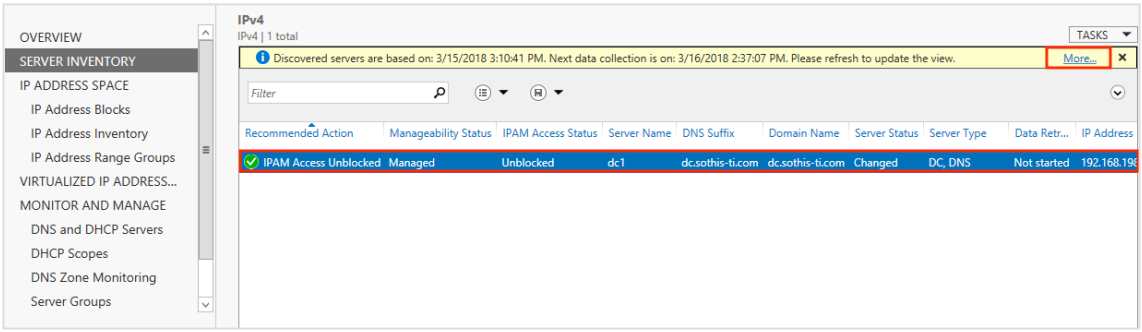

Figura 39: Cambio de estado a desbloqueado de servidor administrado DC

3.4.6. Recuperar datos de servidores administrador

Una vez que se ha verificado que el servidor IPAM tiene acceso a los servidores administrador, puedes comenzar la recopilación de datos que se almacenarán en la base de datos del IPAM.

Si pulsamos en el asistente, la recopilación de datos se iniciará inmediatamente, aunque este paso no es necesario ya que dichas tareas se encuentran programadas al igual que las de descubrimiento con intervalos.

El enlace "Más..." nos proporciona en detalle las tareas de recopilación de datos que va completando, y observamos que se encuentran agrupadas en:

- AddressExpiry

- AddressUtilization
- ServerAvailabilit
- Audit
- ServerConfiguration
- ServerMonitoring

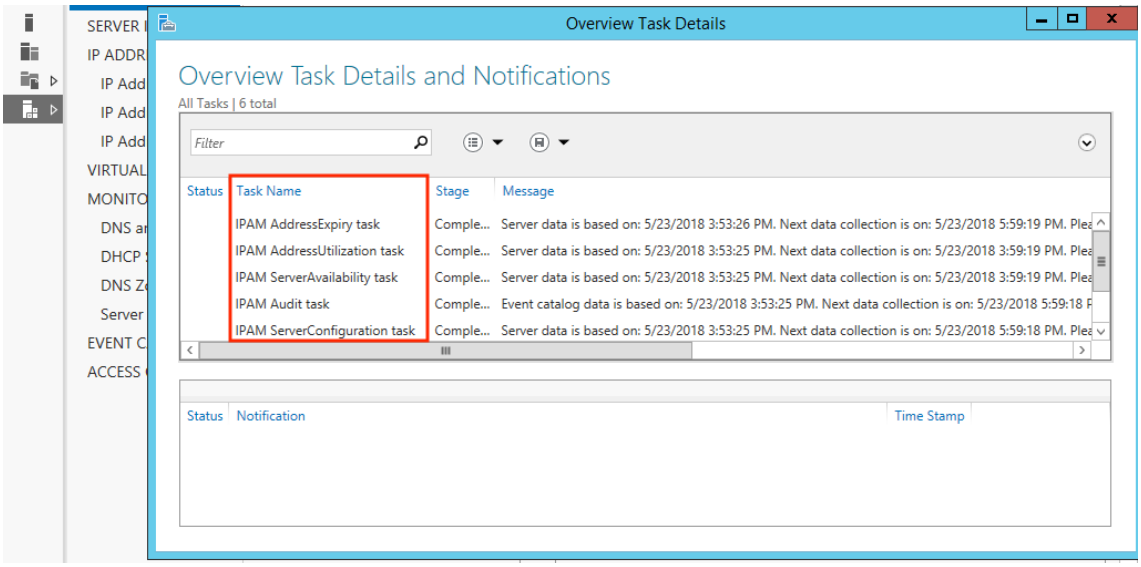

Figura 40: Resumen de tareas y estado sobre la recolección de datos

Permitiendo que las tareas completen la recogida de datos de red, podremos comenzar a efectuar consultas sobre los servidores gestionados y analizar la información, punto que tratamos con detalle en el siguiente apartado.

3.5. Utilizando Microsoft IPAM en la intranet

Con el servidor IPAM configurado y funcionando, solo debemos esperar a la finalización de la recogida de datos, es entonces cuando podremos hacer uso de información detallada. Existen 7 módulos principales en nuestro IPAM desde los cuales obtener información o realiza modificaciones que vamos a ver de manera detallada a continuación.

3.5.1. Información general

Es la pantalla principal que aparece al iniciar el IPAM. Contiene los pasos del asistente que hemos utilizado anteriormente para configurar el IPAM por si queremos añadir, eliminar o modificar algún servidor o servicio gestionado.

Una vez hayamos configurado algunos de los servicios disponibles, la vista nos mostrará un pequeño resumen del estado global y el listado de próximas tareas programadas.

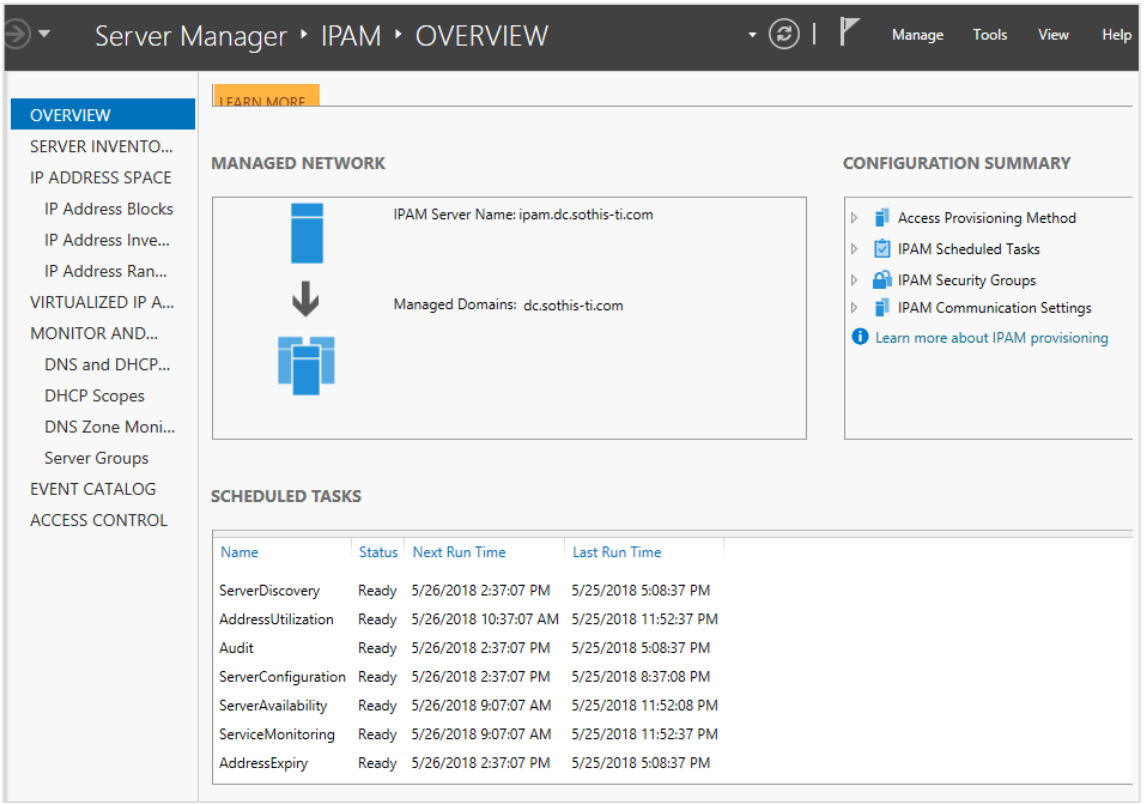

Figura 41: Información general de las características administradas del servidor IPAM

Este panel será nuestro punto de inicio en cada ejecución de aplicación ya que se abre de manera predeterminada.

3.5.2. Inventario de servidor

Es el segundo gran módulo de nuestro IPAM. Contiene información sobre los servidores configurados junto con su dominio. Los servidores tendrán una marca verde que indica estado correcto, si existe comunicación y se encuentran administrados.

Seleccionando cada servidor del panel nos aparece una vista detallada de sus propiedades en el extremo inferior que nos pueden servir de consulta rápida.

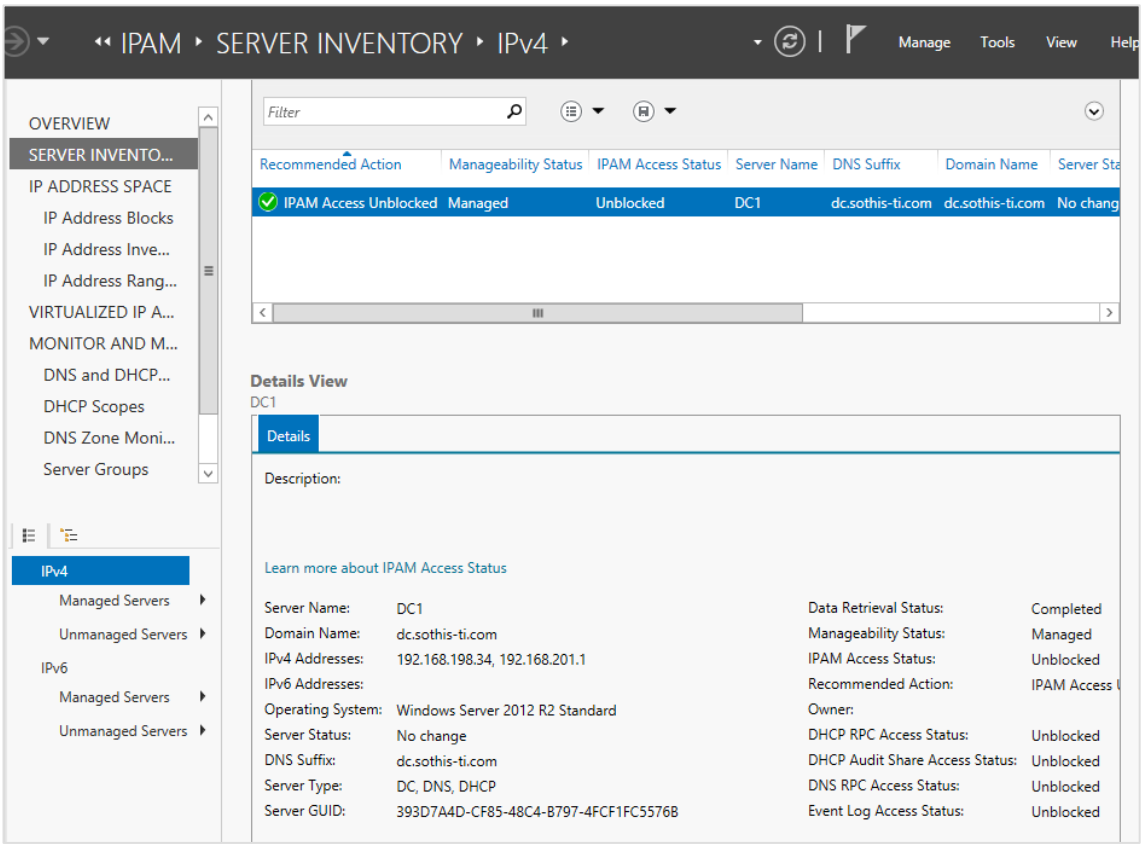

Figura 42: Información de servidores administrados en IPv4

El listado aquí mostrado es solo referido a los servidores IP versión 4 debido a ser el predominante en la fecha de realización del proyecto, pero podemos observar que las opciones IP versión 6 se encuentran soportadas y hacen presencia en los mismos cuadros de tareas.

3.5.3. Espacio de direcciones IP

El servidor IPAM es de gran ayuda con la administración del espacio de direcciones de red y para ello utiliza descubrimiento y monitorización de direcciones IP, las cuales podremos gestionar desde este apartado.

Para familiarizarnos con la utilización del gestor, debemos tener en cuenta la nomenclatura utilizada por Microsoft en la que Bloques de Dirección IP se refiere a los grandes segmentos IP, que a su vez se pueden dividir en otros segmentos más pequeños denominados Intervalos de Direcciones IP y son utilizados para asignar direcciones de red a los diferentes dispositivos. Dentro de los Intervalos de Direcciones será donde podemos encontrar los dispositivos de la red y la visualización de dichos rangos puede ser personalizada en grupo.

El Inventario de Direcciones IP es un grupo integrado por el IPAM que organiza las direcciones por tipo de dispositivo.

Los detalles de seguimiento y utilización de los datos pueden ser visualizados en rangos individuales de IP, grupos lógicos o un bloque completo.

Si existen dispositivos no gestionados o fuera del ámbito de Microsoft, pero proporcionan direcciones IP e intervalos de direcciones IP, el software instalado también podría ser administrador añadiendo o importando las direcciones IP manualmente.

3.5.3.1. Bloques de direcciones IP

El IPAM asigna automáticamente direcciones IP a rangos de direcciones IP y rangos de direcciones IP a los bloques de direcciones IP (estructura jerárquica) Tendremos las siguientes vistas disponibles desde los bloques de direcciones IP:

- Bloques de direcciones IP - *IP Address Block*: el IPAM asigna automáticamente direcciones IP versión 4 a los espacios de direcciones públicas o privadas según lo reserva la autoridad de asignación global de direcciones (IANA). Los bloques de direcciones IP pueden ser añadidos, editados o borrados, y si su inicio o fin de dirección se solapa con otro bloque diferente, automáticamente son reorganizados en subbloques anidados. El resumen de las estadísticas de utilización y tendencias es visualizado a nivel de bloque, y está basado en el direccionamiento asignado a los rangos del mismo.
- Subredes de direcciones IP - *IP Address Subnets*: las subredes de direccionamiento pueden ser añadidas, editadas o borradas al igual que los bloques y son asociadas automáticamente. Si creamos un nuevo intervalo de IP y no existe una subred que se corresponda, también se creará y asociará automáticamente.
  El direccionamiento de subred puede ser habilitado para su uso como espacio de direcciones virtuales. Las subredes virtualizadas son visualizadas y pueden ser asignadas como direcciones IP de cliente o direcciones IP de proveedor.
- Intervalos de direcciones IP - *IP Address Ranges*: los intervalos de direcciones también pueden ser visualizados y administrados desde nuestro software. Un rango o intervalo de direcciones es un conjunto de direcciones estáticas o dinámicas que se utiliza para asignar a los diferentes dispositivos
  Si existe algún solapamiento entre rangos, el IPAM permite visualizarlo y modificar sus propiedades. Solo un solapamiento de intervalo puede asignarse por cada subred, si existieran más, serían visualizados, pero como direccionamiento sin asignar – *no mapped*. Las estadísticas de uso son automáticamente suministradas por los DHCP en caso de direcciones dinámicas. Para un sistema de IP estáticas, es el mismo IPAM el encargado de su cálculo de uso y tendencia. Dicho cálculo y actualización automática pueden ser desactivada, pasando a estar solo disponibles en caso de realizar su actualización manualmente.
- Direcciones IP - *IP Addresses*: el IPAM permite la administración completa del direccionamiento IP (v.4 y v.6) desde el inicio de asignación hasta caducidad, incluyendo la sincronización de registros con DHCP y DNS. Las direcciones IP duplicadas pueden ser identificadas de manera exclusiva en los diferentes sistemas que estemos administrando, aunque sean heterogéneos. IPAM automáticamente mapeará la dirección IP correcta, teniendo en cuenta los rangos disponibles para que se ajuste a las correctas propiedades del servicio.

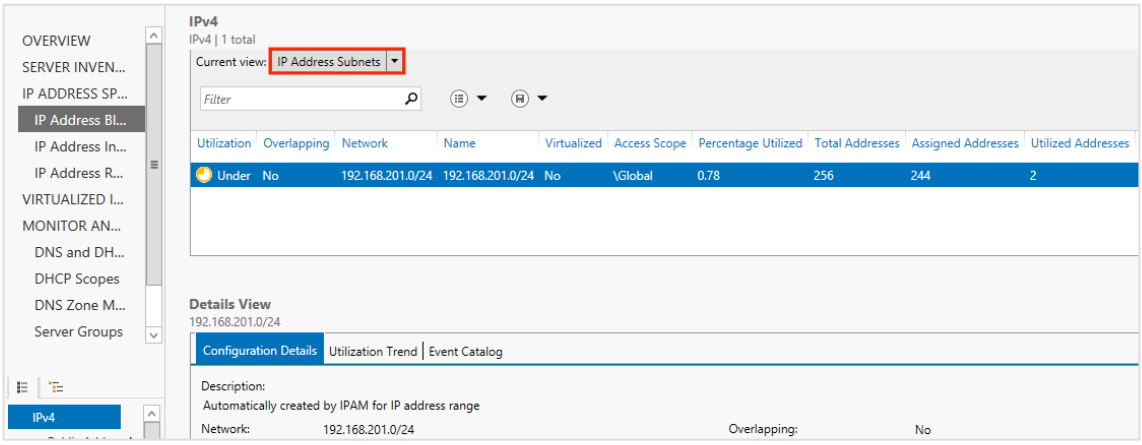

Figura 43: Consola de información y administración de subredes del dominio DC

3.5.3.2. Inventario de direcciones IP

Es un grupo lógico definido por el campo del tipo de dispositivo de la dirección IP. Los grupos lógicos permiten la personalización única de la manera en la que visualizas el espacio de direcciones para administrar y hacer seguimiento del uso de direccionamiento IP.

Los grupos lógicos son definidos seleccionando los criterios incluidos en los campos de información disponibles y también soporta varios niveles de herencia cuando son definidos, heredando los criterios del grupo anterior.

Se puede crear nuevos campos y valores personalizados que nos permitirían visualizar esos conjuntos de IP desde inventario. El IPAM incluye ciertas propiedades de personalización que permiten mapear por tipo de servicio, tipo de dispositivo y estado de la dirección IP.

En la imagen mostrada a continuación, tenemos un listado con una única IP de prueba en la podemos ver y modificar el estado:

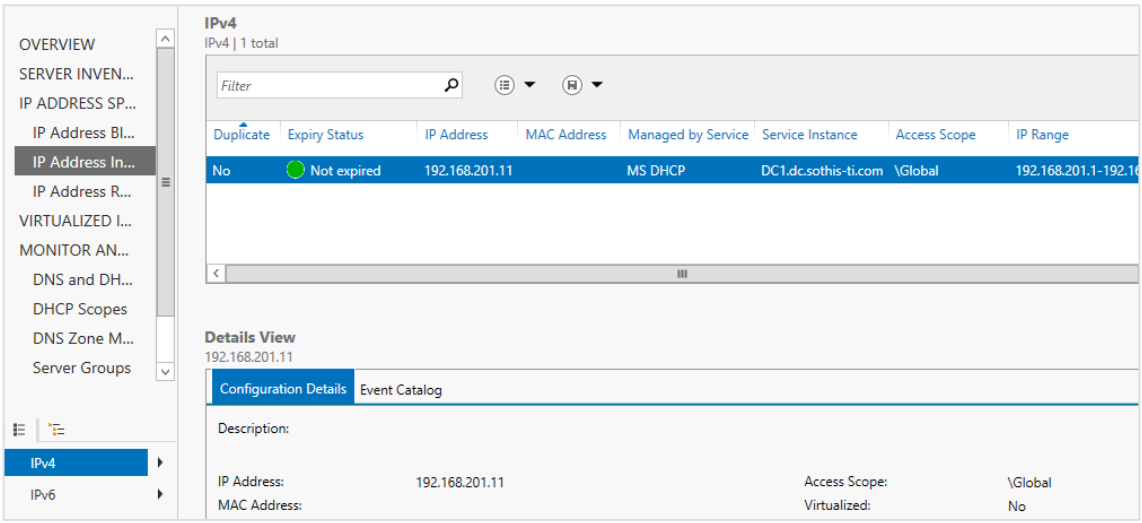

Figura 44: Inventario de direcciones IP

Entre las principales opciones ofrecidas en Inventario de Direcciones IP podemos dar de alta o editar una dirección IP ya existente desde el menú contextual del ratón dónde accederíamos a las siguientes configuraciones:

- Configuración de la dirección IP seleccionada

Incluye los parámetros básicos como la misma dirección IP, si la IP es dinámica (DHCP) o estática, instancia de servicio que se utiliza para la configuración de infraestructura a modo de VLAN, tipo de dispositivo, etc.

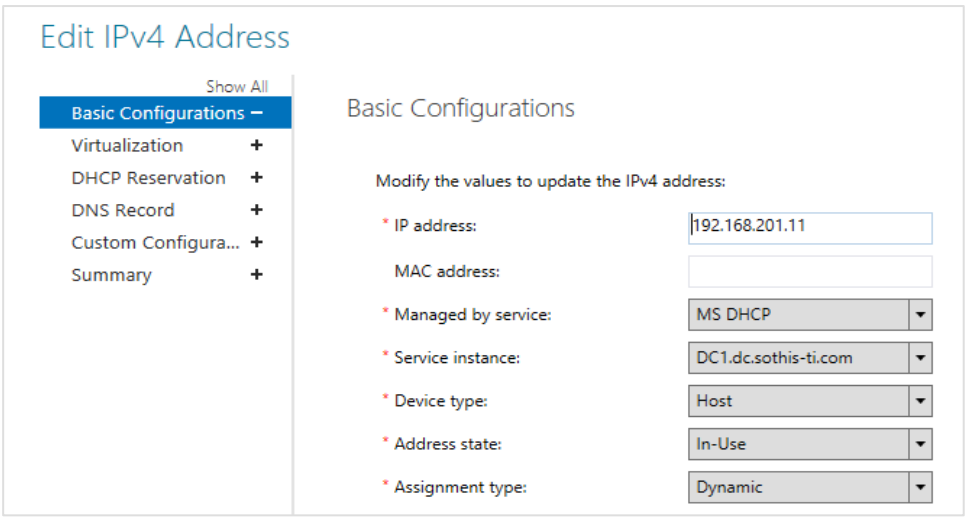

Figura 45: Edición de las configuraciones en direcciones IPv4

- Virtualización de las direcciones IP

El servidor IPAM asociado con una Estructura de Virtualización (VMM), puede usarse para la supervisión del espacio de direcciones IP virtuales, aunque para configurar las redes de máquina virtual, se debe seguir usando el servidor VMM (IPAM solo supervisa). La activación de la virtualización requiere seleccionar entre si el uso de la dirección IP es cliente o proveedor, pero el espacio de direcciones será siempre por defecto, el espacio de direcciones virtual original.

Para la mayoría de los usuarios y empresas, será innecesario marcar esta opción al no tener configurada en su red una máquina de administración de virtualización VMM.

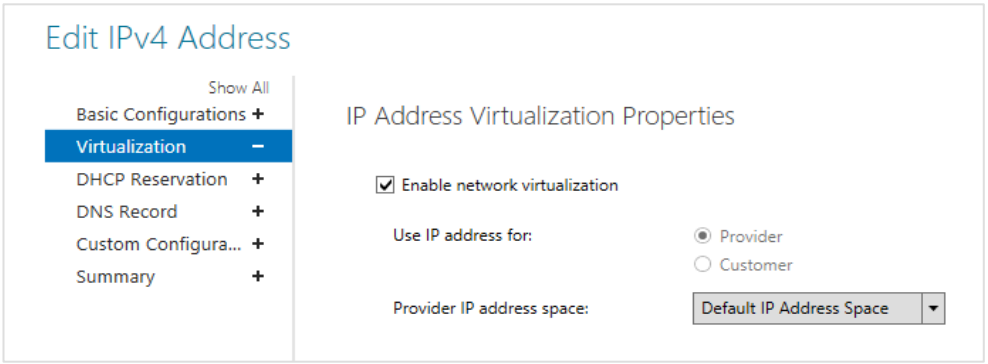

Figura 46: Configuración de propiedades en direcciones IP virtualizadas

- Reserva DHCP

Las opciones de reserva de DHCP son un término medio entre el uso de direcciones IP estática y dinámica. Presentas ventajas en ciertos entornos como migraciones de subredes o en equipos que cambian de Sistema Operativo, ya que la asignación se realiza de manera centralizada.

El apartado negativo de la reserva DHCP es que debemos conocer la MAC del dispositivo con anterioridad que añadiremos en Id Cliente.

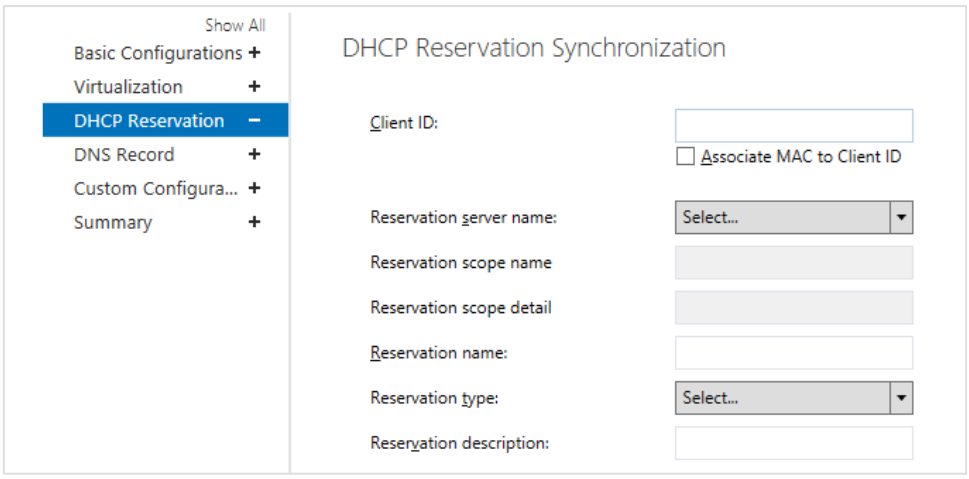

Figura 47: Edición de reserva de direcciones IP dinámicas

- Registro DNS

La sincronización con los registros DNS se utiliza en el caso de que queramos prevenir una posible desactualización de las asignaciones entre nombres y direcciones IP Lo imprescindible de este menú es marcar la opción que por defecto aparece desactivada como "Automáticamente crear registro DNS para esta IP". Dicha opción permite al IPAM escribir en el DNS el registro de nuestra IP, así mantenemos a nuestro servidor IPAM como consola única de administración.

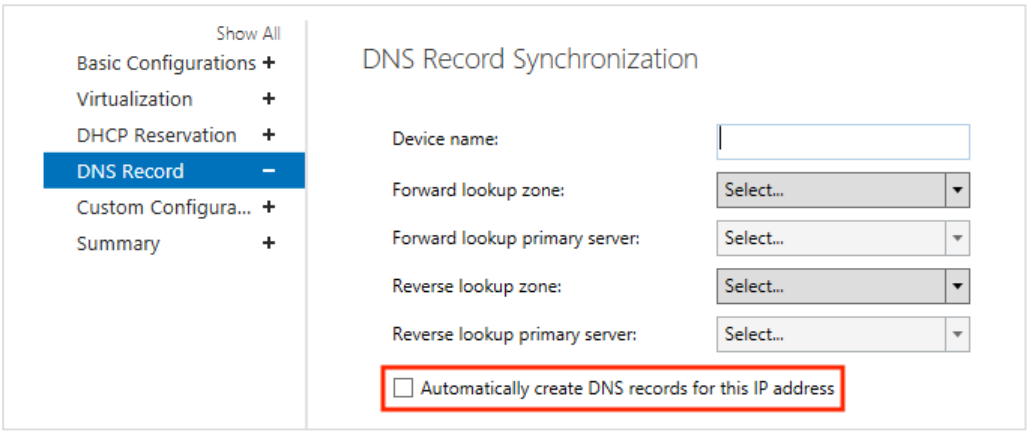

Figura 48: Opciones de configuración del registro de nombres del dominio

Ejecutando los pasos necesarios vistos anteriormente y siempre bajo nuestro criterio y necesidades de administrador de red, tendríamos lo necesario para el correcto funcionamiento sin errores ni incongruencias en toda la red.

3.5.3.3. Grupos de Intervalos de direcciones IP

El IPAM permite organizar los rangos en grupos de rangos. Por ejemplo, se podría organizar los rangos de la empresa de manera geográfica o teniendo en cuenta el modelo de negocio.

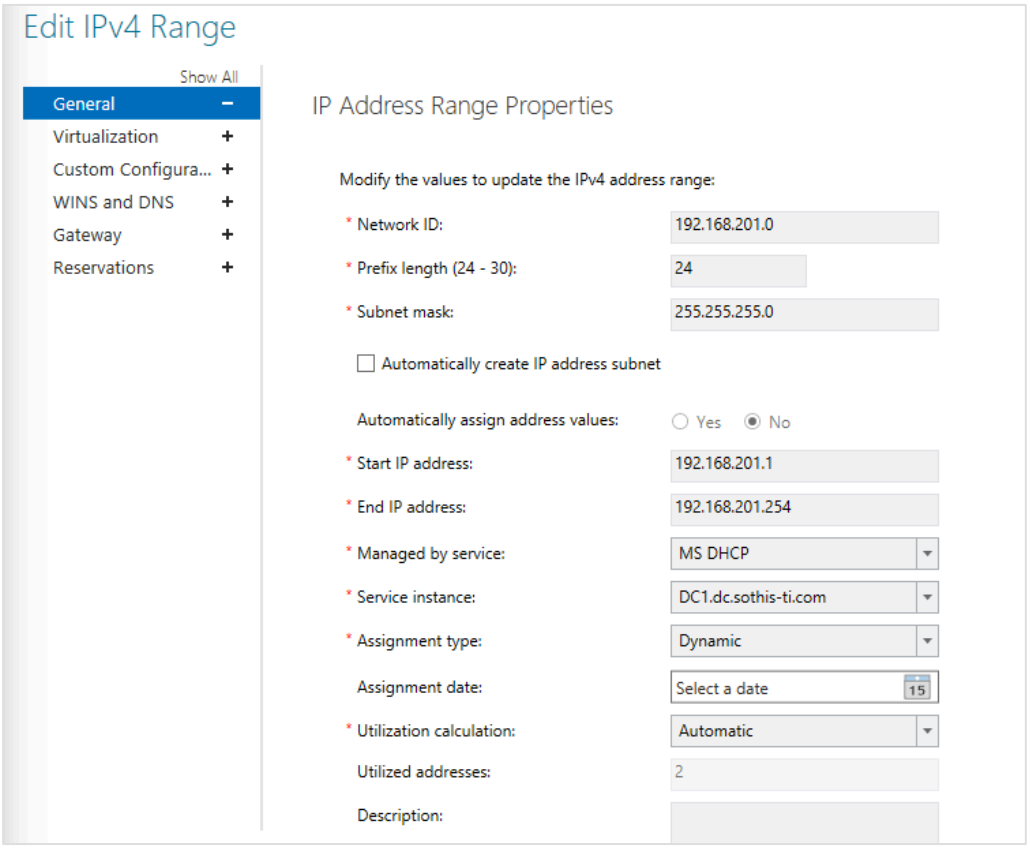

Figura 49: Configuración de propiedades de rangos de direcciones IP

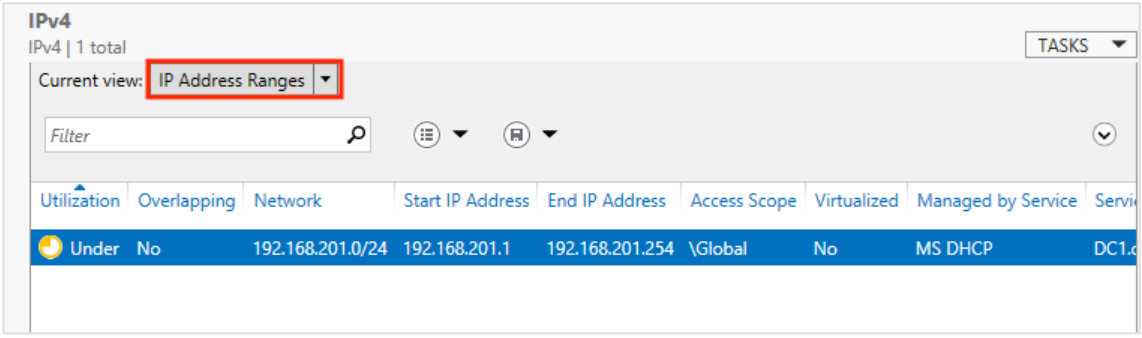

Figura 50: Vista resumen y búsquedas sobre rangos de direcciones IP disponibles

Los grupos lógicos son definidos seleccionado el criterio de agrupación incluido en los campos personalizables. Al igual que el inventario, también podemos activar la herencia multinivel para conformar dichos grupos.

Los criterios de visualización de los grupos de rangos pueden ser modificados asignando valores a los rangos. Las vistas incluidas de origen son la de Grupo de Rangos, Rangos y Direccionamiento IP.

3.5.4. Espacio de direcciones IP virtualizado

Cuando disponemos del uno o más entorno de direcciones IP virtualizadas (VMM), esta opción nos muestra el resumen de los espacios disponibles. Si bien no son administrables desde IPAM, si podemos ver su utilización y consulta.

Queda fuera del ámbito de este TFG el tratamiento de IP virtualizadas.

3.5.5. Supervisión y administración

Con toda la información almacenada en nuestra base de datos, llega el momento de preguntar al IPAM sobre nuestra red. El IPAM puede darnos la información del DHCP, DNS, de cuantas direcciones IP tenemos disponibles, cuantos intervalos de direcciones están siendo infrautilizados o cuándo vamos a necesitar empezar a pensar en crear otra subred.

Vamos a ver las diferentes opciones que nos brinda el servidor IPAM para poder acceder a dicha información. Algunos de los datos mostrados son accesibles desde diferentes ubicaciones, es filosofía Microsoft y se hace porque facilita el acceso a datos vinculados. Es cuestión del administrador seleccionar su metodología o simplemente seguir un flujo habitual.

3.5.5.1. Servidores DNS y DHCP

En el primero de los apartados de administración, IPAM hace hincapié en la información de los servidores DNS y DHCP, donde podemos ver su estado simplemente seleccionando desde el desplegable.

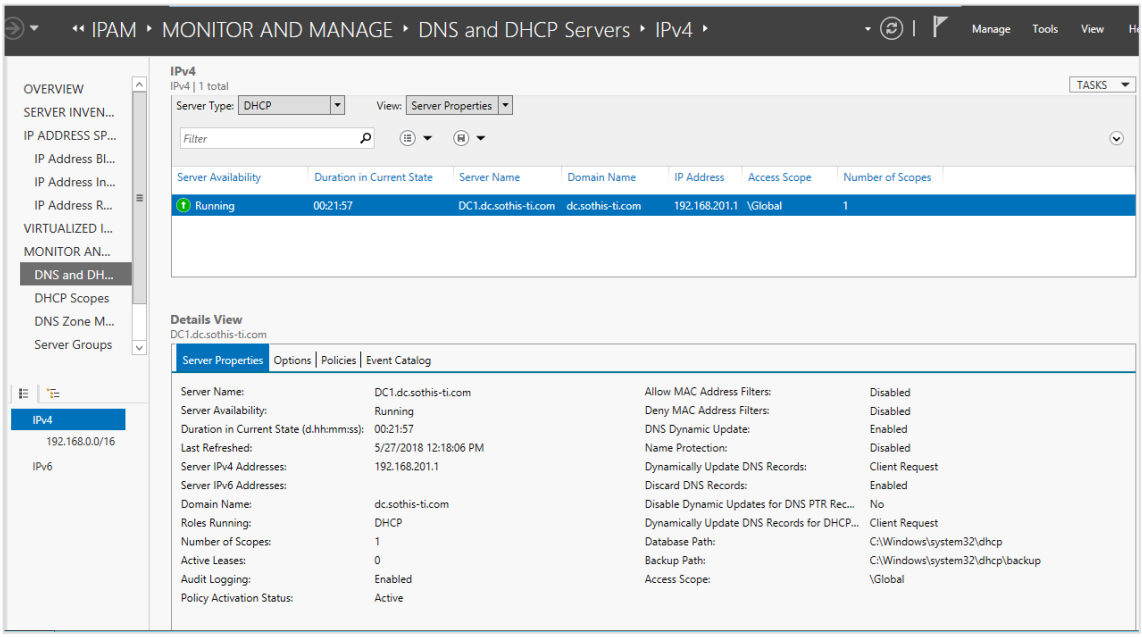

Figura 51: Información servidores DNS y DHCP del dominio

3.5.5.2. Ámbitos DHCP

Desde la opción de Ámbito del DHCP obtenemos de un vistazo la utilización de nuestras IP y si existe solapamiento con alguna otra subred. En la siguiente imagen podemos ver que se encuentra con una utilización inferior (*Under)*:

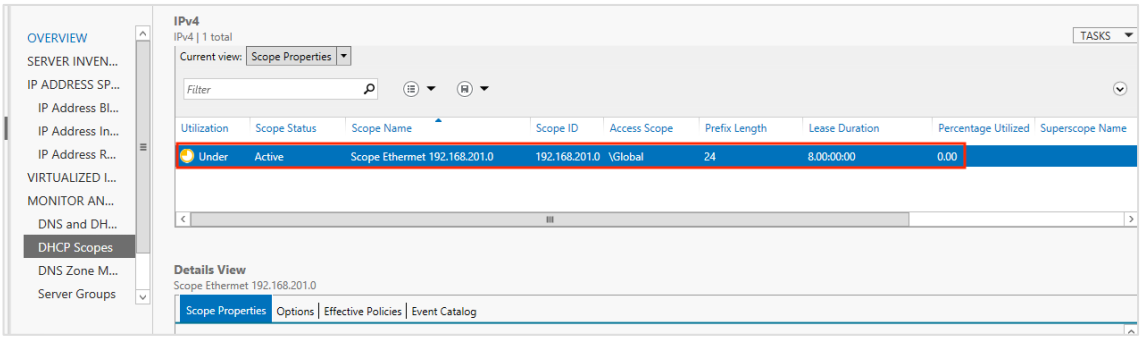

Figura 52: Vista de utilización de direcciones IP y solapamientos

Una de las partes más interesantes que tenemos para el control de utilización del espacio de direcciones, es el ajuste de las señales visuales de alarma que nos puedan ayudar. Para poder acceder a los ajustes basta con pulsar en Administración, Ajustes de IPAM y Configurar ajustes de Disparadores:

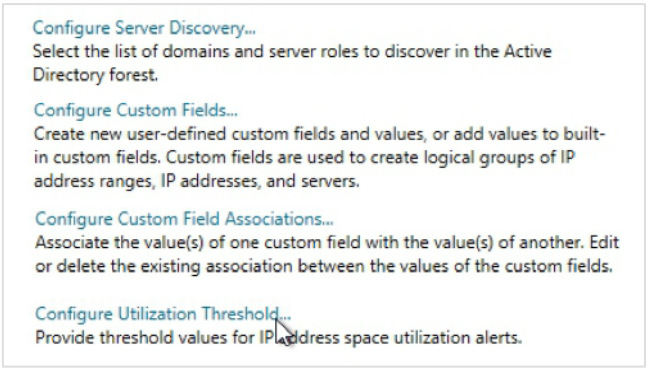

Figura 53: Configuradores avanzados de consola IPAM

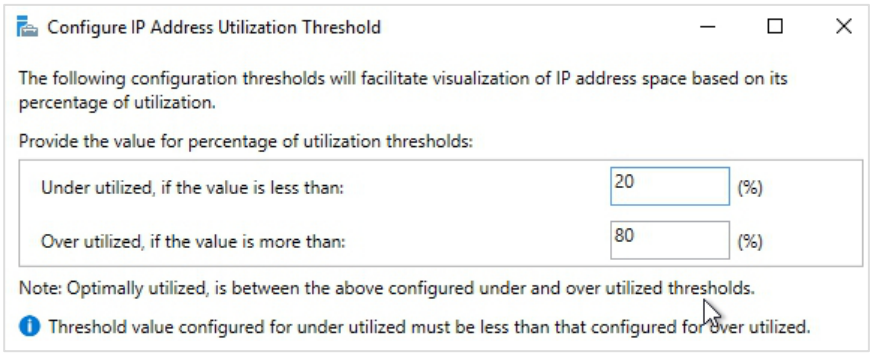

Figura 54: Ajustes de configuración de alertas de utilización IPAM

Los ajustes de los disparadores de utilización vienen predefinidos con un nivel inferior del 20% y superior del 80% que podremos modificarlo si consideramos conveniente teniendo en cuenta la cantidad de los equipos que gestionan nuestros servidores.

3.5.5.3. Supervisión de zona DNS

Muestra el estado por zonas y ámbito del servidor DNS. Permite revisar el funcionamiento de la búsqueda directa (predefinida) e inversa y también nos indica parámetros como estado y tiempo de funcionamiento que dicho servidor lleva en estado actual.

Para el caso del ejemplo, muestra el estado correcto de las dos zonas de pruebas configuradas, desde aquí podemos proceder a su reseteo o configuración de acceso al ámbito.

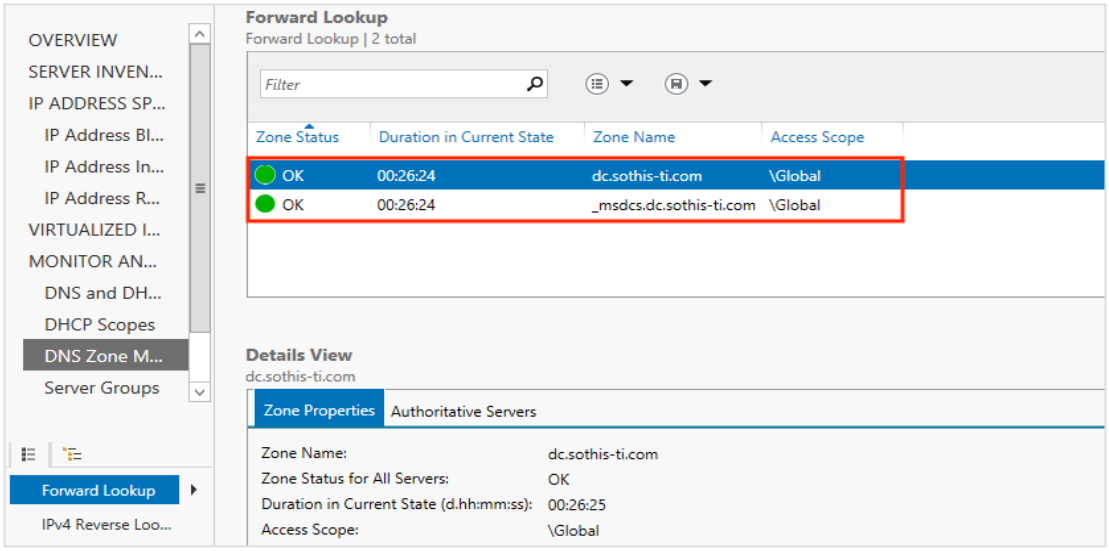

Figura 55: Información por zonas del estado DNS

El ámbito que inicialmente en nuestra empresa tenemos configurado como Global, podría ser modificado desde esta misma consola si quisiéramos separar las resoluciones de la parte pública y privada, o también cargar las directivas de equilibrio de carga de operación si algún servidor se encontrara con una gran carga de trabajo y quisiéramos replicarlo.

Como servidor autoritativo tenemos el servidor primario del dominio que es el configurado.

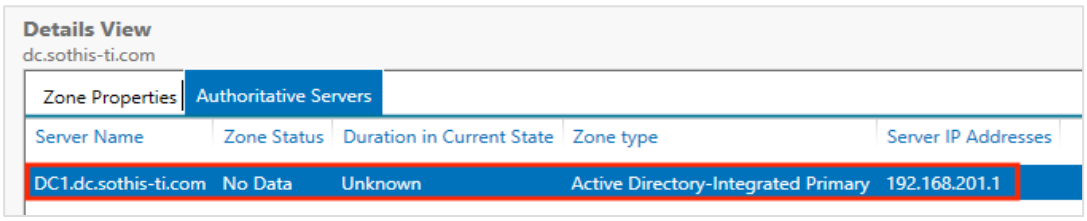

Figura 56: Información del servidor primario del dominio

La búsqueda inversa de IPv4 usa un proceso idéntico al mostrado en resolución directa, pero en este caso determinando desde una dirección IP, el nombre del dominio asociado.

3.5.5.4. Grupos de servidores

Es una opción que resume las opciones vistas anteriormente. Será el administrador el que decida el uso de información y distribución que necesita.

Desde esta pantalla se pueden aplicar las mismas opciones que en vistas anteriores. Si nuestra red no tiene un tamaño excesivamente elevado de servidores para administrar, como es este caso, se convierte en una opción muy válida.

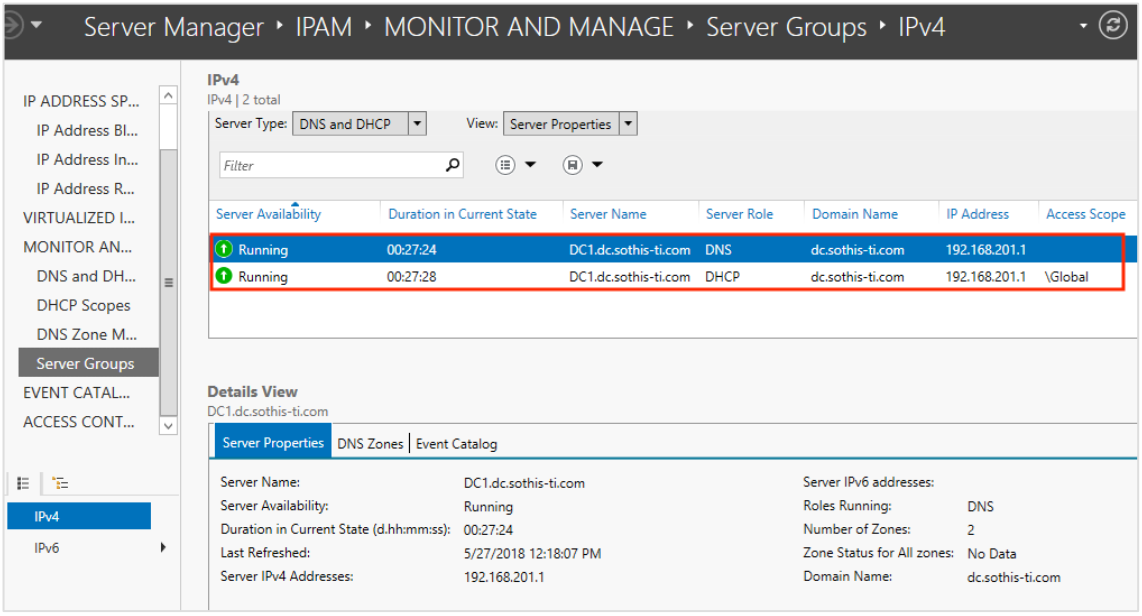

Figura 57: Agrupación de vista resumen de estado de servicios monitorizados (DHCP y DNS)

La vista de Grupo de Servidores incluye una pestaña que agrupa el Catálogo de Eventos que vamos a ver con detalle a continuación.

3.5.6. Catálogo de eventos

El catálogo de Eventos es un repositorio almacenado en el mismo IPAM que utilizamos para auditar los cambios producidos tanto en el servidor DHCP como en el mismo servidor IPAM.

Los cambios que podemos auditar son los referidos a las modificaciones del espacio de direcciones y configuración del IPAM, control de acceso de los ámbitos, tareas de descubrimiento y actualizaciones, reservas especificas, etc.

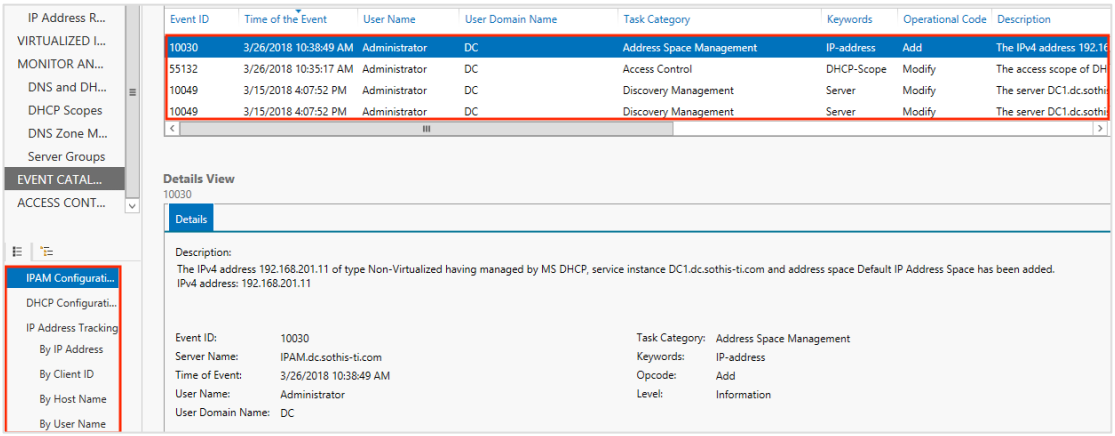

Figura 58: Registro global de eventos, IPAM y dominio

Otra de las opciones destacadas que podemos encontrar en el Catálogo de Eventos es el seguimiento de direcciones IP. Dicho seguimiento es realizado mediante estudio de las concesiones del servidor DHCP y los eventos de inicio de sesión de usuario que se recopilan de forma periódica por DHCP, DC y NPS. La consulta de seguimiento puede ser realizada por dirección IP, ID de cliente (MAC), nombre del *host* o nombre de usuario.

3.5.7. Control de acceso

Se encarga de gestionar los permisos de las cuentas o roles que intervienen en los servidores administrados.

Existen cuentas o roles integrados en el sistema que generamos cuando realizamos la instalación de los servicios. Dichos roles no pueden ser borrados desde esta consola y se nos advierte que se encuentran integrados, pero podemos añadir, modificar o eliminar roles no integrados.

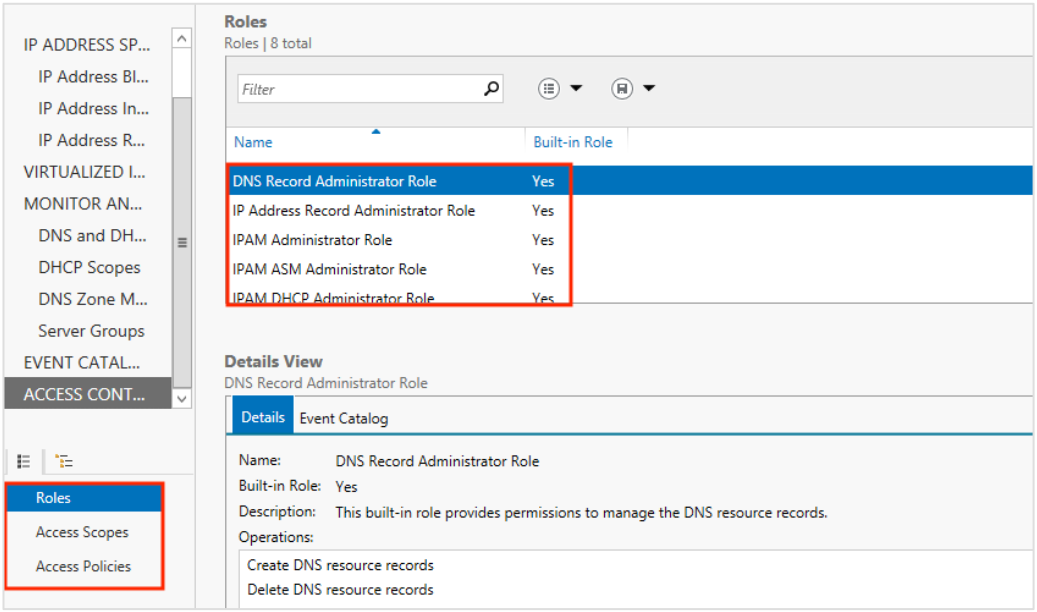

Figura 59: Consola de estado del control de acceso

Cuando añadimos o editamos roles, tenemos a nuestra disposición el catálogo completo desplegable de las operaciones de control de acceso del Directorio Activo (AD). Es importante definir las tareas que pueden realizar los distintos usuarios en servidores, equipos de red y servicios para que coincidan con la política de control de acceso de la empresa.

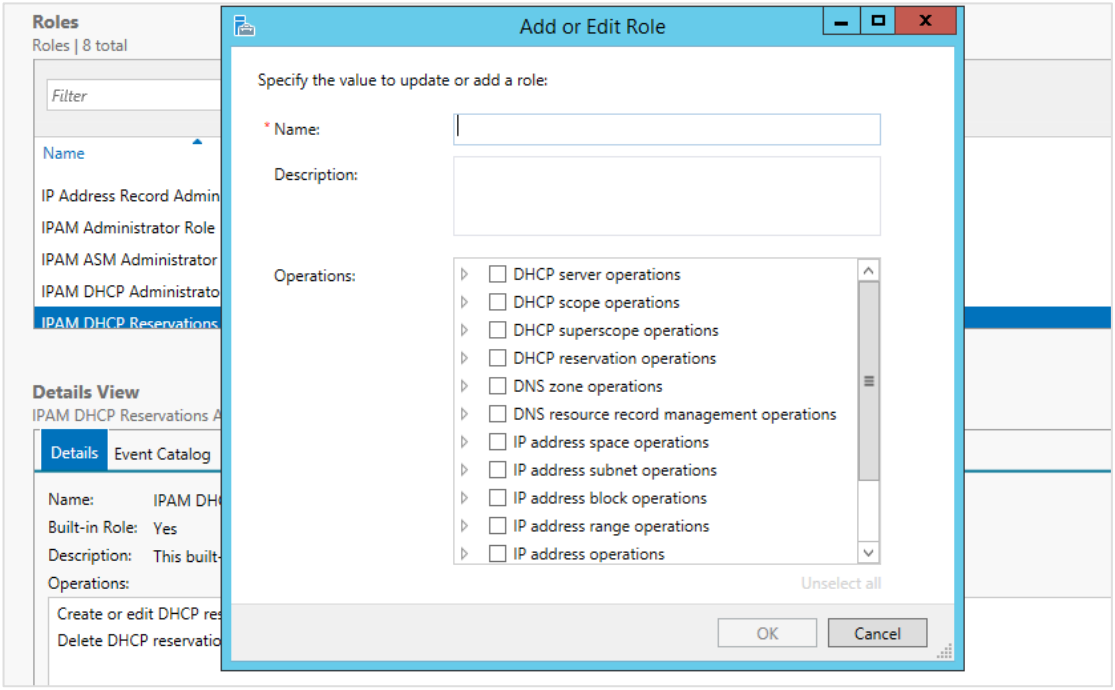

Figura 60: Opciones de edición de roles para acceso

El empleo de la herramienta “control de acceso”, unifica la gestión de permisos del servidor IPAM y de los servicios que gestiona en otros servidores, solucionando uno de los grandes retos a los que se enfrentan los administradores de comunicaciones en las empresas.

4. Elastic Stack

En el siguiente apartado ejecutaremos con alto nivel de detalle, la instalación y despliegue de las herramientas de Elastic que nos van a permitir recopilar, filtrar y sintetizar los eventos generados por nuestros equipos de red para su gestión.

4.1. Conceptos previos al despliegue

Para comenzar, debemos entender que el conjunto de herramientas de Elastic son de código abierto, lo que da ventaja en caso de tener que realizar algún pequeño ajuste. Sin embargo, en todas las pruebas realizadas, no se ha visto la necesidad de ir directamente al código de programación, puesto que los ajustes mediante parámetros externos han sido correctos.

La compañía Elastic tiene todo un ecosistema de herramientas dedicado solo a la monitorización. Su producto estrella, denominado Elastic Stack, está compuesto por cuatro programas independientes especializados, pero vamos a comentar brevemente el catálogo completo diseñado para monitorización:

- Elasticsearch es el núcleo de los productos. Se encarga de almacenar e indexar la información y de suministrar la información cuando se realizan búsquedas.
- Logstash permite hacer un trabajo de transformación para luego poder ser enviado a Elasticsearch. (No provee la funcionalidad de poder leer de distintos archivos y fuentes).
- Kibana es una interface gráfica que nos permite visualizar y trabajar con la información que vamos a estar guardando en Elasticsearch.
- Beats se utiliza para leer registros y métricas que luego va a enviar información a Elasticsearch. Diseñado para consumir pocos recursos y poder ser instalado en servidores de producción.
- X-Pack son un conjunto de complementos comerciales que agregan funcionalidades al sistema como seguridad (control de acceso), alertas, monitorización, aprendizaje automático y reportes.
- Elastic Cloud es la versión de software bajo demanda (SaaS), donde se pueden utilizar las mismas aplicaciones, pero desde servidores de alta disponibilidad de Amazon y Google.
- Elastic Cloud Enterprise es idéntico al producto anterior, pero permite adquirir el software en nube para implementarlo en el propio hardware empresarial.

Para realizar las modificaciones necesarias en algunos casos bastará con ser Administrador local, pero en otras ocasiones necesitaremos ser Administrador del Dominio. Al igual que en la instalación del administrador de direcciones IP, los trabajos sobre servidores deben de ser cuidadosamente planificados para que impacten mínimamente el servicio.

4.2. Requisitos de los sistemas

Los productos Elastic están disponibles para los sistemas operativos Windows, Mac, Linux y Debian.

Si bien es completamente posible hacer funcionar el software de Elasticsearch en un equipo de sobremesa o portátil, cuando se realiza el despliegue real, es necesario aplicar la máxima atención a los requerimientos. Oficialmente las recomendaciones para un despliegue son:

Tabla 4: Requisitos hardware de instalación para las herramientas Elastic Stack

Componente	Mínimo	Recomendado
Socket CPU	2 núcleos	8 núcleos
Memoria RAM	8GB	64GB
Disco duro	15k Rpm	SSD
Red	1GbE	10GbE
Software	JDK7 o superior	

En las recomendaciones de disco duro, Elastic no aconseja tamaños mínimos, ya que el espacio dependerá mucho de la información que queramos guardar, pero si hacen hincapié en usos de discos duros rápidos que puedan evitar cuellos de botella cuando tenemos escrituras y búsquedas de manera simultanea, actualmente los modelos tipo SSD son los que mejores prestaciones ofrecen.

Como consideración general que aparece en la documentación oficial de Elastic es el tipo de equipos óptimo es de tamaño mediano-grande. La justificación es clara, si optamos por muchos nodos pequeños, la carga de computación para ejecutar los registros se hace evidente, y el problema de nodos grandes es que tienen tendencia a estar descompensados (a veces pueden estar utilizando toda la RAM disponible pero la CPU se encuentra infrautilizada).

4.3. Instalación de paquetes Elastic Stack

Los servidores que suministran servicio a nuestra empresa tipo son de Windows Server, fácilmente descargables desde el sitio oficial de www.elastic.co. En la siguiente imagen podemos observar los archivos descargados con el tamaño ocupado:

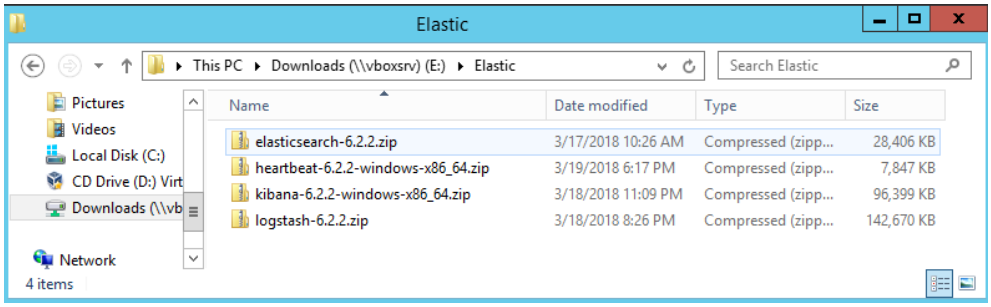

Figura 61: Colección de archivos comprimidos Elastic

Debemos obtener el software previamente ya que en servidores es habitual la restricción de navegación o el aislamiento completo de la red con acceso exterior debido a motivos de seguridad.

Una serie de conceptos básicos que debemos tener presente antes de pasar a ejecutar la instalación del software son:

- Cluster es el conjunto de nodos que forman nuestra red de manera distribuida. Los diferentes *cluster* vienen identificados por un nombre, por defecto *Elasticsearch*.
- Nodo es un servidor que forma parte de un cluster. Un nodo almacena información, indexa y realiza búsquedas. Están inicialmente configurados para formar parte de un cluster del tipo elasticsearch. El número de nodos no está limitado y si cuando generamos el nodo, no existe ningún cluster creado, entonces automáticamente lo crea y asocia.
- Index es una colección de datos que comparten características similares. Los índices se identifican con nombres que usamos a la hora de realizar nuevas indexaciones o búsquedas.
- Sharding es la división de los índices de manera que la información pueda ser tratable si existe mucho crecimiento. Es decir, ofrece escalabilidad horizontal.
- Replicación es el mecanismo que utilizamos para que, en caso de fallo, el sistema pueda continuar funcionando sin que el usuario se vea afectado.

Una vista previa de la infraestructura seleccionada sería: un servidor que aloja la información de los registros (Elasticsearch), junto con el programa de visualización (Kibana) y opcionalmente un cliente de recogida de datos. El resto de los servidores (inicialmente el controlador de dominio) ejecutarán el servicio de recogida y envío de datos al servidor de registros.

Ahora vamos a ir viendo el proceso de instalación del software en el orden recomendado.

4.3.1. Instalación Elasticsearch

La primera aplicación que necesitamos instalar se denomina Elasticsearch e irá alojada en el servidor central de tratamiento de registros (192.168.199.40). Es el núcleo de nuestro recolector de registros y almacena, indexa y analiza la información distribuida en tiempo real.

Uno de los puntos fuertes de esta aplicación es que no necesita declarar un esquema de la información que vamos añadiendo, por lo tanto, podremos almacenar documentos estructurados o sin estructurar. Si necesitamos un elevado rendimiento de la información, el fabricante nos recomienda añadir los denominados *mappings* que funcionan parecido a un esquema en formato JSON.

Para iniciar la instalación en un sistema Windows, basta con descomprimir el archivo *elasticsearch-versión.zip*, vamos a la carpeta \bin y ejecutamos (como Administrador) *elasticsearch.bat*:

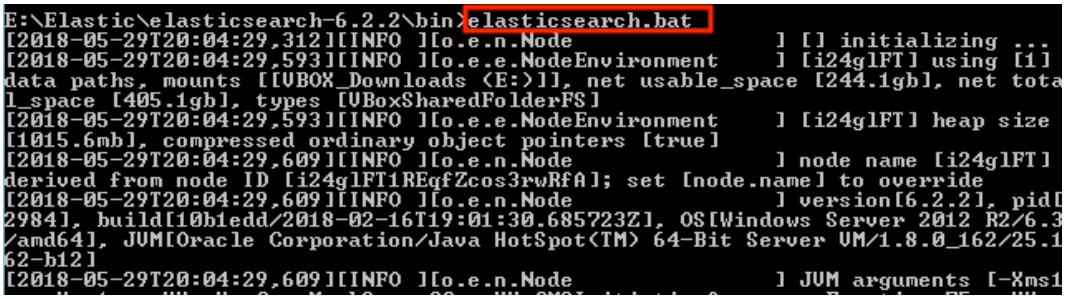

Figura 62: Ejecución inicial de programa ElasticSearch

Lo que hace a partir de ahora es cargar el archivo de configuración, complementos, etc. Por última instancia levanta el servicio *GatewayService* que atiende en el puerto 9200 usado por defecto para peticiones HTTP. La consola de comandos se mantendrá activa con la información del estado del servicio y no debemos cerrar ni cancelarlo a menos que tengamos la intención de finalizar el programa.

En estos momentos el puerto 9200 se encuentra atendiendo posibles peticiones REST, pero… ¿Cómo poder comprobarlo? Existen varias maneras, como por ejemplo complementos de navegador que permiten configurar el tipo de petición. Si no queremos instalar software de terceros también podemos confirmar el correcto funcionamiento desde la consola PowerShell mediante el comando: *Invoke-RestMethod* http://localhost:9200.

La respuesta debe ser del tipo:

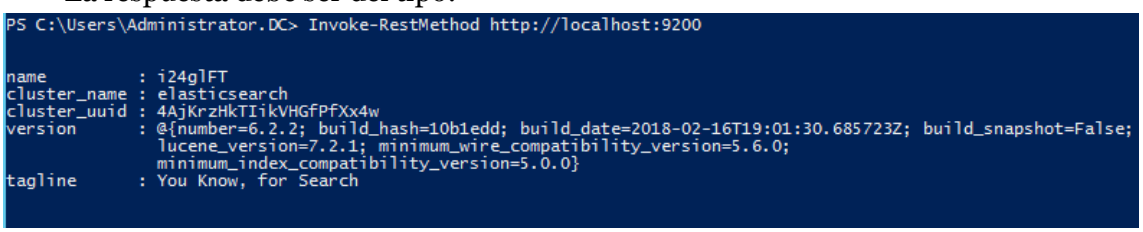

Figura 63:Comprobación de funcionamiento de servicio mediante petición HTML tipo REST

Una respuesta “Imposible conectar con el servidor remoto” ejecutando este comando, nos indica que la conexión no se ha abierto correctamente y tendríamos que revisar el proceso.

Para abortar la ejecución, desde la misma ventana de comandos que tenemos funcionando, pulsamos ctrl+c y confirmar que terminamos la ejecución:

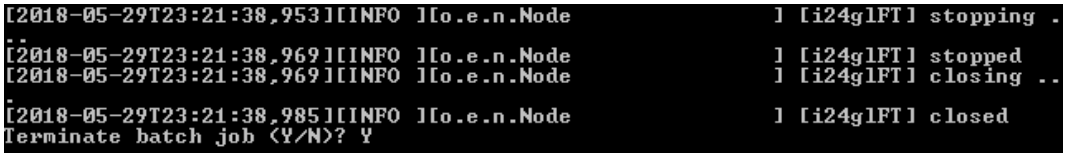

Figura 64: Cancelación de ejecución ElasticSearch por comandos

4.3.2. Instalación Logstash

Alojado en el servidor central de tratamiento de datos, Logstash funciona como un proceso ETL (*Extract, Transform and Load*), por lo tanto, se va a encargar de extraer la información (Entrada), transformar o modificar los datos (Filtros) y realizar el envío de información a Elasticsearch (Salida).

- Entrada: no es necesario que Logstash obtenga la información a tratar por Beats, aunque sí es un medio bastante habitual. La información también puede obtenerse por medio de una base de datos, ficheros o incluso mediante los protocolos TCP, UDP y HTTP.
- Filtros: es una de las partes más importantes ya que tiene una gran cantidad de posibilidades. Lo habitual es trabajar con registros, en los cuales podremos definir reglas de estructura, transformarlos o normalizarlos. También existen complementos que permiten por ejemplo enriquecimiento de geolocalización a través de IP, o con informaciones extras que provienen de una base de datos nuestra.
- Salidas: habitualmente son envíos a Elasticsearch de las informaciones, pero también puede ser enviados mediante los protocolos TCP, UDP o HTTP e incluso a base de datos.

Es escalable de manera horizontal, podremos utilizar varios Logstash si fuera requerido y tiene una biblioteca de más de 200 complementos para realizar dichas modificaciones.

En cuanto a la persistencia, utiliza un sistema que denominan *persistent queues*, donde va almacenando toda la información que recibe. En caso de fallo de software, memoria, etc... cuando el sistema recupera, lo primero que va a buscar son estas colas persistentes para el envío de información y así no pierde la información que se envió a Logstash.

Otra opción denominada *Dead Letter Queues* (DLQ), se encarga de recuperar los eventos enviados a Elasticsearch que son respondidos como formato incorrecto o con problemas, como por ejemplo fechas mal definidas. De esa manera el sistema puede reenviar la información previamente rechazada para ser consumida.

La instalación del software descargado en sistemas Windows se realiza mediante la descompresión del archivo denominado *logstash-version.zip*. Para la ejecución de Logstash es necesario la creación y referencia previa de un fichero con la configuración necesaria de los distintos parámetros (entrada, filtro, salida), que trataremos en el apartado 4.4.2.

4.3.3. Instalación Beats

Son agentes ligeros que se utilizan para extraer la información de otros servidores o equipos donde se ejecutan para luego enviar dicha información a Elasticsearch o Logstash. Como existe variedad de tipo de nodos y servicios, hay un amplio catálogo de agentes Beats disponibles dependiendo del uso:

- Filebeat: permite leer los registros de ficheros (logs) en un servidor
- Packetbeat: extrae y envía información sobre datos de red
- Winlogbeat: recolecto de datos especializado en sistema operativo Windows
- Metricbeat: recupera informaciones de medidas de un servidor
- Heartbeat: monitor de servicio de disponibilidad para saber si un equipo se encuentra en servicio (*keep alive*)
- Auditbeat: recolector de datos de auditoría para sistemas Linux

Debemos conocer las necesidades de nuestro despliegue para seleccionar el agente adecuado. En el caso de nuestro proyecto, el agente ideal es **Winlogbeat**, ya que se encuentra diseñado específicamente para enviar los registros generados por Windows, incluyendo los inicios de sesión. Si el sistema a tratar fuera Linux, deberíamos realizar la instalación del agente Filebeat.

La instalación se realiza habiendo descargado el software previamente y descomprimiendo la carpeta *winlogbeat-version.zip* en el servidor del que queremos analizar los datos.

Existen dos maneras de ejecutar el cliente Winlogbeat en nuestro servidor:

- Aplicación software de ejecución manual, haciendo que se inicie al cargar el sistema operativo mediante las herramientas disponibles de arranque. En nuestro caso ejecutaríamos: *winlogbeat.exe -c winlogbeat.yml*, siendo *winlogbeat.yml* el archivo de configuración que veremos con detalle en el apartado de configuración.
- Mediante servicio Windows, ejecutando *install-service-winlogbeat.ps1* desde la consola de PoweShell. De esta manera lo que hacemos es añadir nuestro programa a los servicios Windows.

¿Qué ventajas tenemos ejecutando el Beat como servicio?: Iniciar Winlogbeat como servicio, hace que se ejecute en segundo plano, sin necesidad de inicio de sesión de usuario y tampoco genera ventanas de interface en el arranque, por lo que se convierte en transparente para cualquier usuario.

Por supuesto, este método también tiene algunos inconvenientes: Cuando necesitamos realizar alguna modificación de la configuración, deberemos ir al panel de servicios, detenerlo, realizar las modificaciones en el archivo con extensión .yml y volverlo a iniciar.

4.3.4. Instalación Kibana

Kibana es un servidor web para realizar consultas y visualizar la información que tenemos en Elasticsearch. Debido a los continuos accesos que hace contra Elasticsearch para obtener información, la mejor solución es alojarlo juntos en el servidor central de registros (192.169.198.40).

Para poder instalar el software debemos descomprimir la carpeta donde se aloja *kibana-version.zip* y accedemos a la carpeta \config para editar si fuera necesario el archivo kibana.yml.

Para poder iniciar el servicio basta con ejecutar dentro de la carpeta descomprimida: *bin\kibana.bat*:

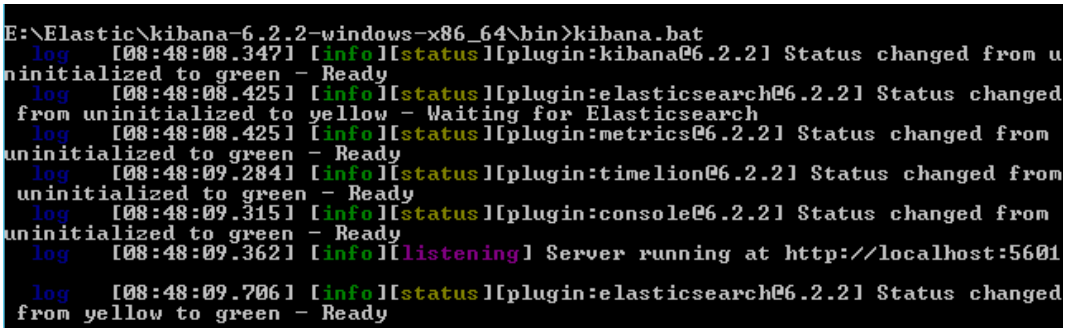

Figura 65: Inicio de ejecución de servicios Kibana mediante consola de comandos

Iniciará los complementos: *kibana*, *elasticsearch*, *timelion*, *console* y la escucha del servidor. Ahora podemos probar mediante el navegador de internet que tenemos comunicación para poder interactuar con Kibana, basta con indicar en la barra de direcciones: http://localhost:5601. Aparecerá la interface principal de la aplicación:

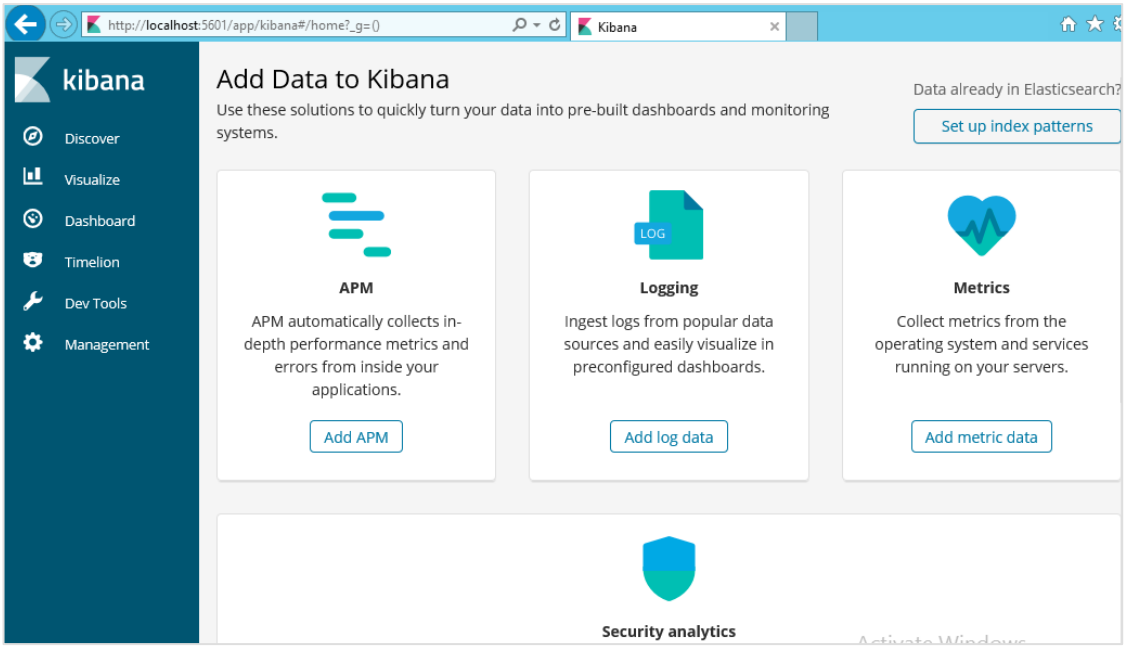

Figura 66: Interface principal de aplicación Kibana desde navegador

4.4. Configuración Elastic Stack en servidores

Una vez que hemos finalizado la instalación de nuestras aplicaciones, debemos realizar algunos pasos de configuración previos para su correcto funcionamiento. La mayoría de los ajustes se realizan mediante modificaciones en ficheros concretos con la extensión ".yml" de estilo Linux.

Una característica a tener en cuenta cuando estemos configurando los clientes software es que los ficheros de configuración son leídos en el inicio/arranque de la aplicación, por lo tanto, debemos conocer que los cambios con la aplicación en funcionamiento no son aplicados hasta su posterior reinicio.

4.4.1. Configuración Elasticsearch

El archivo de configuración para Elasticsearch se encuentra en la carpeta config de su mismo directorio. Allí aparece un archivo denominado *elasticsearch.yml* desde donde permite editar con las opciones:

```
# ---------------------------------- Cluster -----------------------------------
# Use a descriptive name for your cluster:
cluster.name: my-application
# ------------------------------------ Node ------------------------------------
# Use a descriptive name for the node:
node.name: node-1
# Add custom attributes to the node:
#node.attr.rack: r1
# ----------------------------------- Paths ------------------------------------
# Path to directory where to store the data (separate multiple locations by comma):
path.data: /path/to/data
# Path to log files:
path.logs: /path/to/logs
# ----------------------------------- Memory -----------------------------------
# Lock the memory on startup:
bootstrap.memory_lock: false
# Make sure that the heap size is set to about half the memory available
# on the system and that the owner of the process is allowed to use this
# limit.
# Elasticsearch performs poorly when the system is swapping the memory.
# ---------------------------------- Network -----------------------------------
# Set the bind address to a specific IP (IPv4 or IPv6):
#network.host: 192.168.0.1
# Set a custom port for HTTP:
http.port: 9200
# For more information, consult the network module documentation.
# --------------------------------- Discovery ----------------------------------
```

Figura 67: Modificación de fichero de configuración elasticsearch.yml

- Nombre del cluster: el nombre por defecto es elasticsearch, en este caso de prueba es my-application. Debemos tener en cuenta que un nodo solo puede asociarse con un cluster cuando comparte su *cluster.name*, por eso dichos nombres no pueden estar repetidos.
- Nombre de nodo: Generado aleatoriamente si no indicamos lo contrario, el UUID generado persiste ya durante los reinicios.
  Para usar el nombre del equipo como nombre: *node.name: ${HOSTNAME}*.
- Ajustes de rutas: Existen dos diferentes ajustes, el de ubicación de directorio de datos y el de almacenamiento de logs. La ruta de almacén de datos se puede separar en múltiples rutas.
- Configuración de red: permite asociar cluster y nodos mediante direcciones bucle o *loopback*. Si necesitamos formar nuestro cluster con nodos de otros servers, necesitamos utilizar una IP que no sea *loopback*.

- Memoria: Disponemos de un parámetro denominado *bootstrap.memory_lock* que permite, activar (true) o desactivar (false/default) el intercambio de datos entre memoria principal y la partición intercambio (*swap*).

4.4.2. Configuración Logstash

Una vez realizada la instalación (descompresión) de Logstash, necesitamos crear un archivo de configuración dentro de la carpeta descomprimida bin\logstash, llamándolo, por ejemplo: *logstash.conf*

Vamos a ver un ejemplo de archivo de configuración como el que debemos crear en nuestro sistema para su correcto funcionamiento:

```
input { stdin { }
 beats {
    port => "5044"
    codec => "json"
  } }
filter {}

output {

elasticsearch { hosts => ["localhost:9200"] }

stdout { codec => rubydebug }
}
```

- Input indicamos desde dónde obtenemos informaciones
- Filter nos permite recuperar las informaciones de input y modificarlas
- Output definimos complemento (*plugin*) para enviar a Elasticsearch

Los parámetros "stdin" y "stdout" son utilizados para realizar pruebas de funcionamiento durante el proceso de configuración, aunque pueden mantenerse sin problemas durante el despliegue, puesto que no afectan al servicio. "Stdin" permite recibir datos desde el terminal y "stdout" permite mostrar la información recibida en pantalla.

Para ejecutar Logstash, basta con situarnos desde el interprete de comandos en el directorio de la carpeta descomprimida de la herramienta, directorio *bin* y ejecutar: *logstash -f logstash.conf*.

4.4.3. Configuración Beats - Winlogbeat

Al estar desarrollando el proyecto en entorno Windows, hemos instalado el cliente Winlogbeat específico para nuestros sistemas y configurable mediante el archivo *winlogbeat.yml*, que podemos encontrar directamente en la carpeta raíz de la instalación.

Como parámetros relevantes en el archivo de configuración y que debemos revisar y configurar para el correcto funcionamiento, son:

```
#========================== Winlogbeat specific options =========================
# Visit the documentation for the complete details of each option.
# https://go.es.io/WinlogbeatConfig
winlogbeat.event_logs:
  - name: Application
  - name: Security
  - name: System
#================================ Outputs =====================================
# Configure what output to use when sending the data collected by the beat.
#-------------------------- Elasticsearch output ------------------------------
output.elasticsearch:
  # Array of hosts to connect to.
  # hosts: ["localhost:9200"]

  # Optional protocol and basic auth credentials.
  #protocol: "https"
  #username: "elastic"
  #password: "changeme"

#----------------------------- Logstash output --------------------------------
#output.logstash:
  # The Logstash hosts
  hosts: ["192.168.198.40:5044"]

#================================ Kibana =====================================
setup.kibana:
  # Kibana Host
  # Scheme and port can be left out and will be set to the default (http and 5601)
  # IPv6 addresses should always be defined as: https://[2001:db8::1]:5601
  #host: "localhost:5601"
```

Figura 68: Modificación fichero de configuración winlogbeat.yml

- Winlogbeat.evet_logs: Especificamos los registros de eventos que queremos monitorizar, los más habituales son de aplicación, de seguridad y de sistema que son los que hemos configurado en nuestros equipos.
- Output.elasticsearch: este parámetro es usado si vamos a enviar nuestros logs directamente a Elasticsearch sin usar Logstash, necesitaríamos indicar la IP y el puerto del equipo dónde tenemos instalado Elasticsearch (localhost si es el mismo). En nuestro escenario hemos optado por utilizar un sistema más complejo y escalable con Logstash, por lo que en este apartado no configuraremos nada.
- Setup.kibana: usado para proveer de datos directamente a la vista previa de Kibana, debemos indicar IP y puerto (nuestro caso :5601) para la correcta comunicación. En este punto hay que tener en cuenta la configuración aplicada en Kibana, si en su momento optamos por configurar seguridad en el servidor (opcional), debemos indicar las credenciales añadiendo las filas *username:* “” *password:*””
- Output.logstash: usado para enviar datos a Logstash, permite un procesamiento adicional de los logs enviados. Configuramos la dirección IP y el puerto (5044) de la máquina que aloja el servicio Logstash, que en nuestro escenario será 192.168.198.40:5044

Una vez configurado, existe un comando que permite probar la configuración: *.\winlogbeat.exe test config -c .\winlogbeat.yml -e.*

4.4.4. Configuración Kibana

La configuración de Kibana se realiza mediante la edición del archivo de *kibana.yml* desde cualquier editor, incluso el predeterminado Notepad de Windows y las opciones más importantes que encontramos son:

```
# Kibana is served by a back end server. This setting specifies the port to use.
server.port: 5601

# Specifies the address to which the Kibana server will bind. IP addresses and host names are b
# The default is 'localhost', which usually means remote machines will not be able to connect.
# To allow connections from remote users, set this parameter to a non-loopback address.
server.host: "localhost"

# Enables you to specify a path to mount Kibana at if you are running behind a proxy. This only
# the URLs generated by Kibana, your proxy is expected to remove the basePath value before forw
# to Kibana. This setting cannot end in a slash.
server.basePath: ""

# The maximum payload size in bytes for incoming server requests.
server.maxPayloadBytes: 1048576

# The Kibana server's name.  This is used for display purposes.
server.name: "your-hostname"

# The URL of the Elasticsearch instance to use for all your queries.
elasticsearch.url: "http://localhost:9200"

# Time in milliseconds to wait for responses from the back end or Elasticsearch. This value
# must be a positive integer.
elasticsearch.requestTimeout: 30000

# To disregard the validity of SSL certificates, change this setting's value to 'none'.
elasticsearch.ssl.verificationMode: full
```

Figura 69: Modificación fichero de configuración kibana.yml

- Puerto de servidor: usado el 5601 por defecto si no indicamos lo contrario, en nuestro entorno, mantenemos el puerto por defecto al estar disponible.
- Servidor anfitrión: especifica la dirección del servidor con el que enlazará Kibana, este parámetro viene por defecto configurado como *localhost*, y es válido cuando la instalación Kibana y Elasticsearch son realizadas en el mismo servidor.
- Ruta base del servidor: especifica la ruta de montaje de Kibana si está siendo ejecutada detrás de un servidor proxy. No configurada por defecto.
- Tamaño de carga útil: es el máximo tamaño asignable de carga útil que podemos configurar para las peticiones entrantes.
- Nombre del servidor de Kibana: por motivos de sencillez de visualización
- URL Elasticsearch: configura la dirección del enlace con Elasticsearch, por defecto configurado como http://localhost:9000. Si modificamos. Elasticsearch debemos cambiar este campo también.
- Tiempo de espera de peticiones: dado en milisegundos aparece por defecto en 30.000 y debe ser un número entero positivo.
- Verificación SSL: configurado por defecto con el valor *full*, sirve para atender las validaciones SSL. Un valor *none* lo deshabilitaría.

4.5. Utilizando Elastic Stack en intranet

Hemos visto la instalación y configuración de los diversos clientes que vamos a ejecutar en nuestros equipos, esos son los primeros pasos que debemos realizar para nuestro despliegue. Para la correcta ejecución del software, deberemos iniciar las aplicaciones en un orden concreto:

1. Elasticsearch
2. Logstash
3. Winlogbeat
4. Kibana

4.5.1. Inicio de núcleo Elasticsearch

Lanzando el proceso *elasticsearch.bat* en el servidor que utilizamos para almacenar los registros recopilados de nuestra red mediante una ventana de comandos o PowerShell como se ha utilizado en nuestros servidores veremos las secuencias de carga de los módulos:

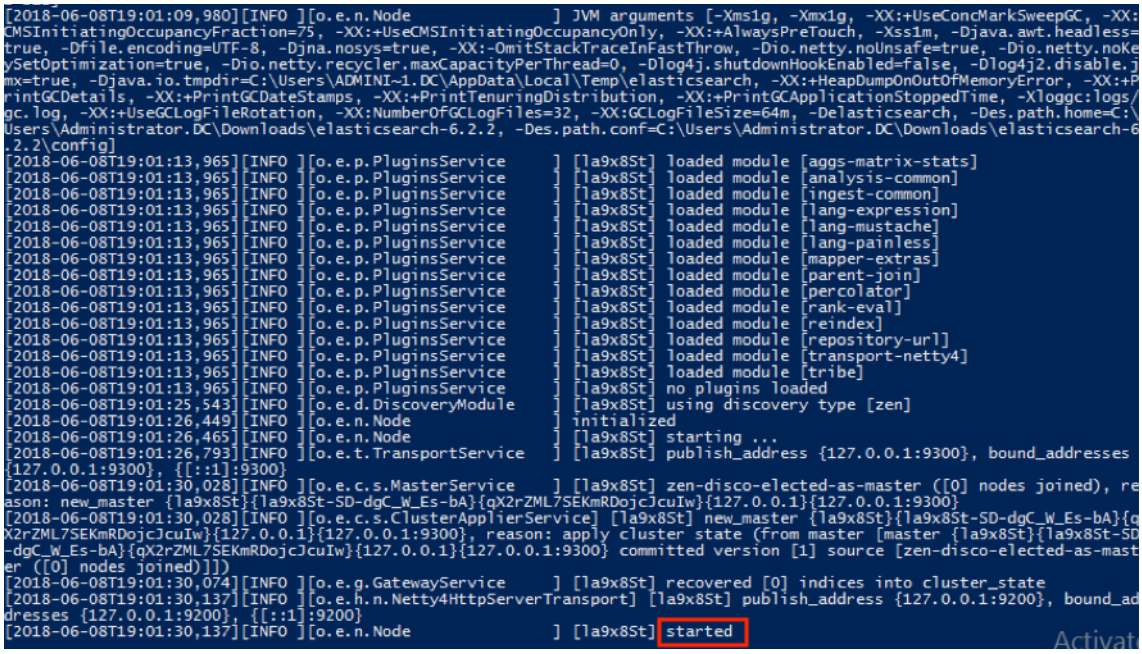

Figura 70: Inicio completo de servicios configurados de aplicación Elasticsearch

El sistema nos debe indicar que ha sido iniciado (*started*), la ventana no debe ser cerrada puesto que finalizaría la ejecución del proceso. En este momento, la misma interface puede mantener esa línea en caso de no recibir datos, pero se irá incrementado con información de nuevos registros cuando:

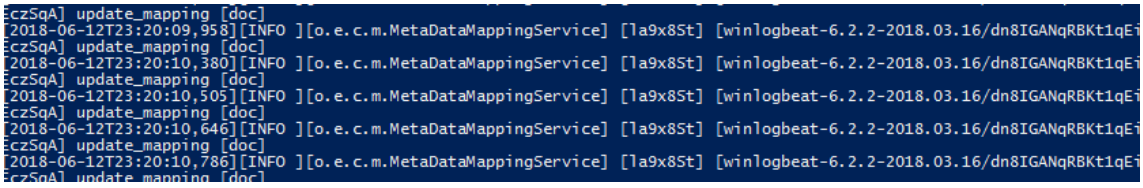

Figura 71: Incremento de líneas de registros en pantalla

Debemos asegurarnos antes de continuar con los siguientes pasos de que nuestro conjunto (*cluster*) Elasticsearch se ha creado correctamente mediante el comando: *Invoke-webrequest* en nuestro servidor, al puerto 9200.

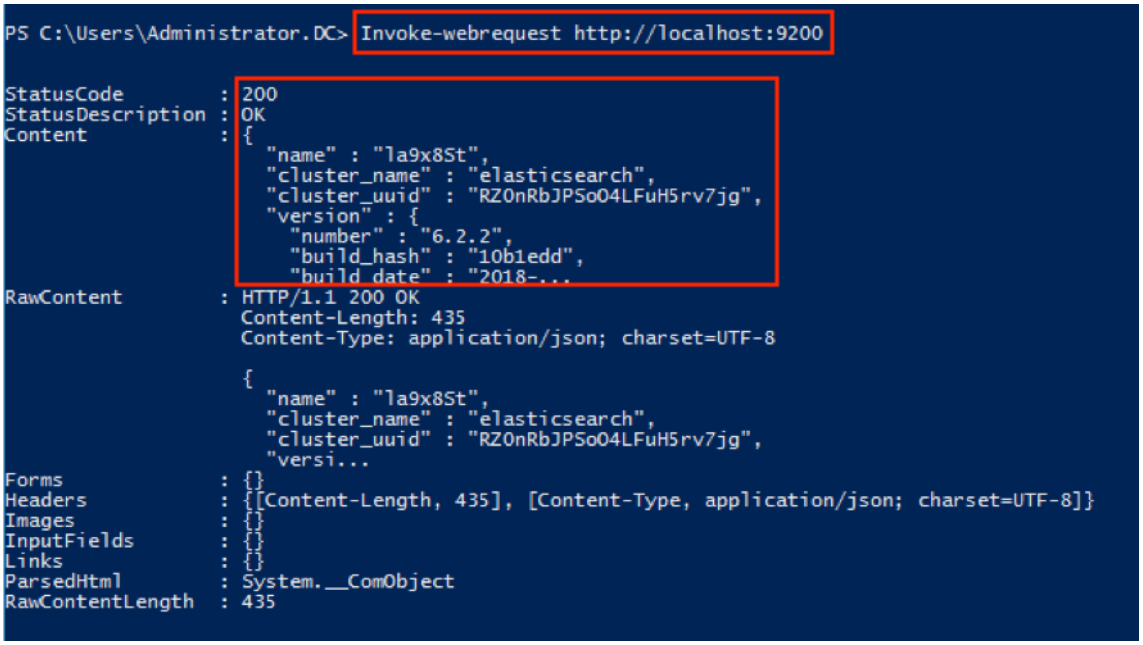

Figura 72: Comprobación de funcionamiento de cluster en servidor

Nombre, identificador, versión y resto de datos de la agrupación son mostrados en consola. Si no existe respuesta o recibe un error, es imprescindible verificar el apartado previo de configuración antes de proseguir el arranque.

4.5.2. Inicio Logstash

Realizado mediante el comando: *logstash -f logstash.conf,* dónde el modificador -f (*file*) indica que queremos que inicie la configuración de la aplicación mediante el archivo que apuntamos logstash.conf modificado previamente (ver 4.4.2):

Figura 73: Inicio de servicios configurados Logstash

4.5.3. Inicio cliente Winlogbeat

Iniciamos el cliente Winlogbeat que debemos instalar en los equipos a monitorizar, en este caso iniciamos el cliente alojado en el servidor principal y controlador del dominio mediante el comando: *winlogbeat.exe -c winlogbeat.yml:*

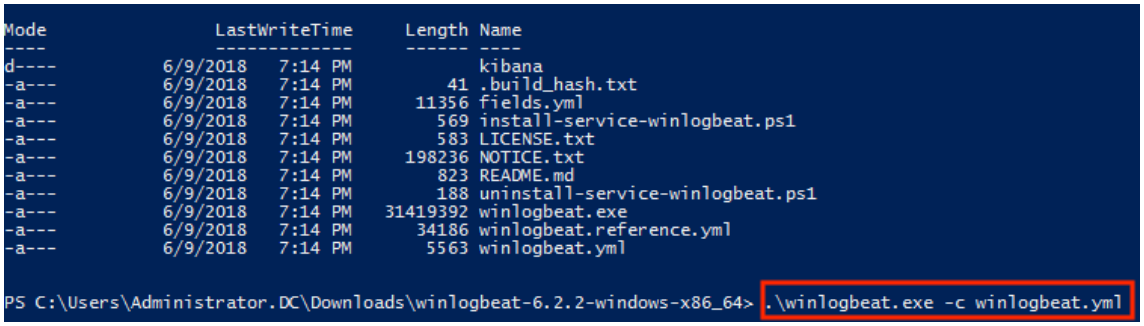

Figura 74: Inicio de servicio Winlogbeat mediante referencia a fichero de configuración

El servicio de recogida de datos se mantiene en ejecución sin mostrar información (modo silencioso), solo en caso de fallo de carga es cuando se detiene automáticamente mostrando el mensaje correspondiente.

Debemos arrancar el cliente en tantos servidores como queramos modificar, la muestra para el proyecto se ha realizado en la máquina principal, ya que es la más crítica al disponer de gran cantidad de servicios. La interface de filtros que veremos a continuación permite ver los registros por IP, nombre de servidor, etc. por lo que permite distinguir sin dificultad el equipo emisor de la información.

4.5.4. Inicio de interface Kibana

Ejecución del servicio que hace funcionar la interface gráfica web en el servidor que aloja nuestro lector de registros mediante: *kibana.bat*. Durante el arranque mostrará información del estado de carga de complementos:

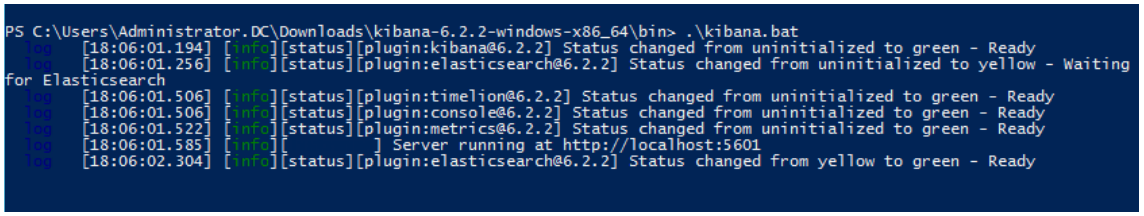

Figura 75: Inicio de servicios Kibana y complementos web

Desde Kibana vamos a poder tener acceso a toda la información recopilada, por lo tanto, una vez funcionando todos los servicios instalados se convierte en el portal principal de nuestro sistema (Acceso mediante http://IP:5601).

Una vez accedemos a la dirección IP de la máquina que aloja el servicio Kibana en el puerto 5601, en nuestro caso al haber decidido por un servidor único encargado del servicio, debemos teclear http://localhost:5601 accedemos a la interfaz principal:

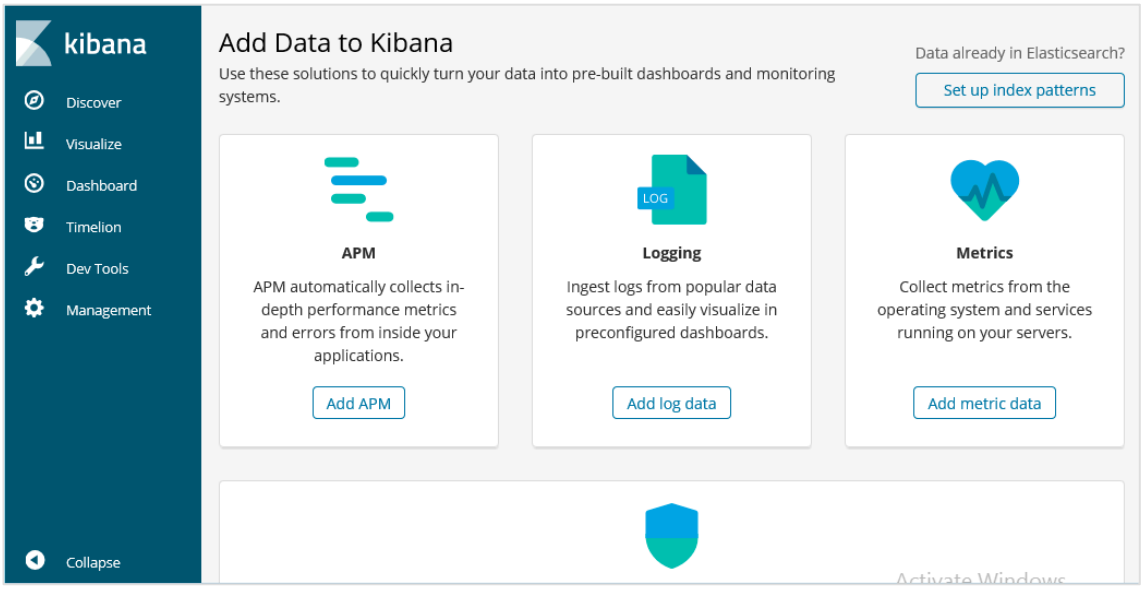

Figura 76: Interface principal sistema de gestión Kibana

En ella muestra las opciones de instalar ciertos complementos o *plugins* que contienen scripts (Este tipo de mejoras no es completamente necesario y lo veremos con detalle más adelante). Lo primero que necesitamos es configurar un índice de patrones para la interpretación de datos, esto es debido a que Kibana va a trabajar únicamente con JSON (estructura sencilla de claves-valor), tanto para recepción como tratamiento.

Para configurar el índice de patrones, seleccionamos en el menú lateral Administración o *Management* y seguidamente Index Patterns:

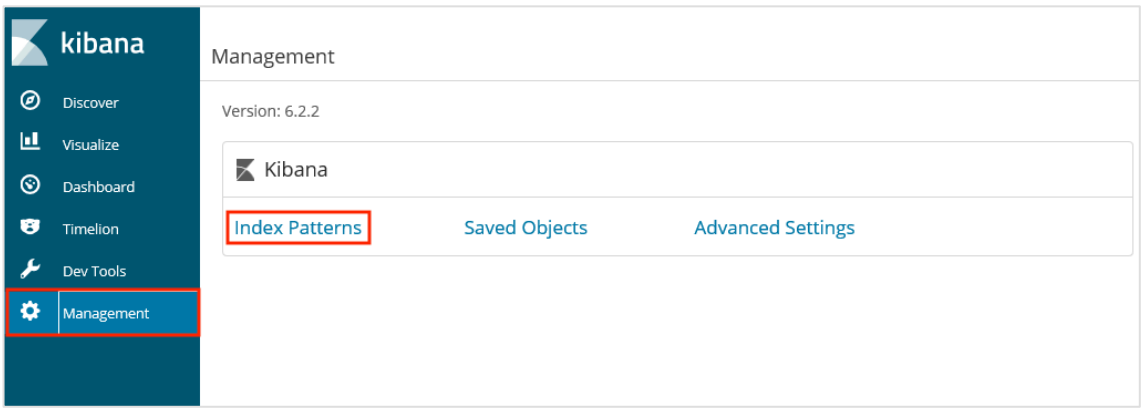

Figura 77: Creación de índice de patrones

Obtendremos el menú de definición de índices de patrones. Aquí vemos diferentes patrones de índices que ha recibido mediante Winlogbeat en distintos momentos:

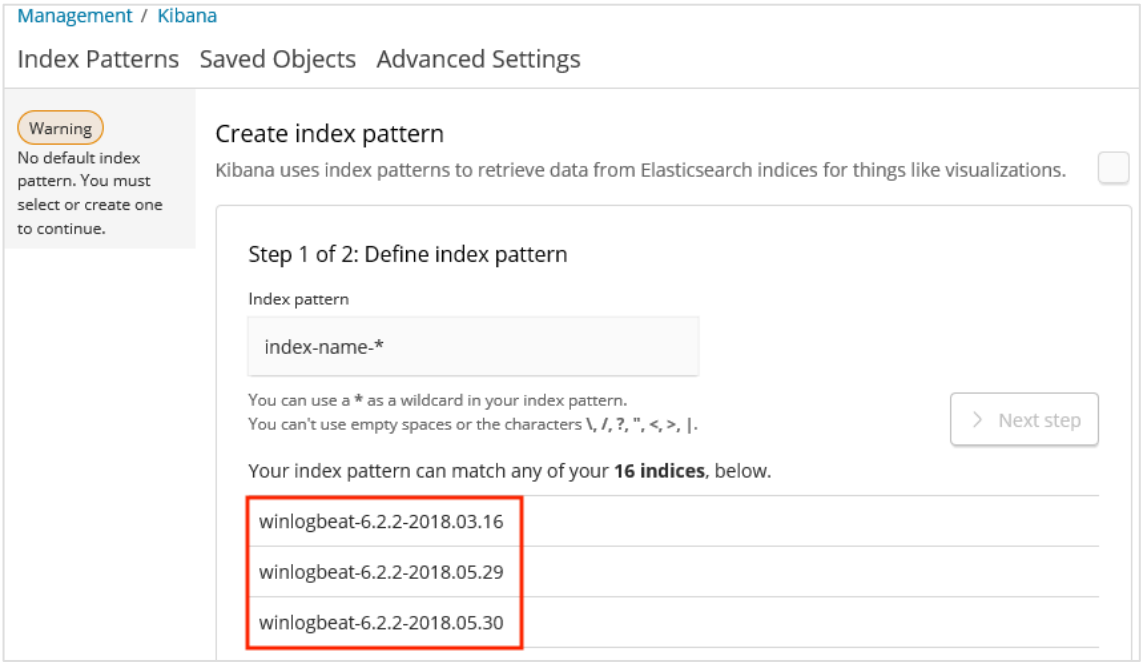

Figura 78: Visualización de archivos recibidos con indexación (Winlogbeat)

Para definir un índice, lo más sencillo es partir de uno de los índices recibidos, por defecto aparece en el cuadro de búsqueda la opción de filtro *index-name-** que muestra todos los ficheros, lo cambiaremos por *winlogbeat** (si obtenemos registros de otros equipos mediante el programa Logbeats, usaremos el filtro *logbeats**) A partir de ese momento, refinará la búsqueda y nos permitirá el acceso a índices internos, seleccionamos cualquiera de ellos (internamente son de idéntico patrón) y el botón habilitado >*Next step*.

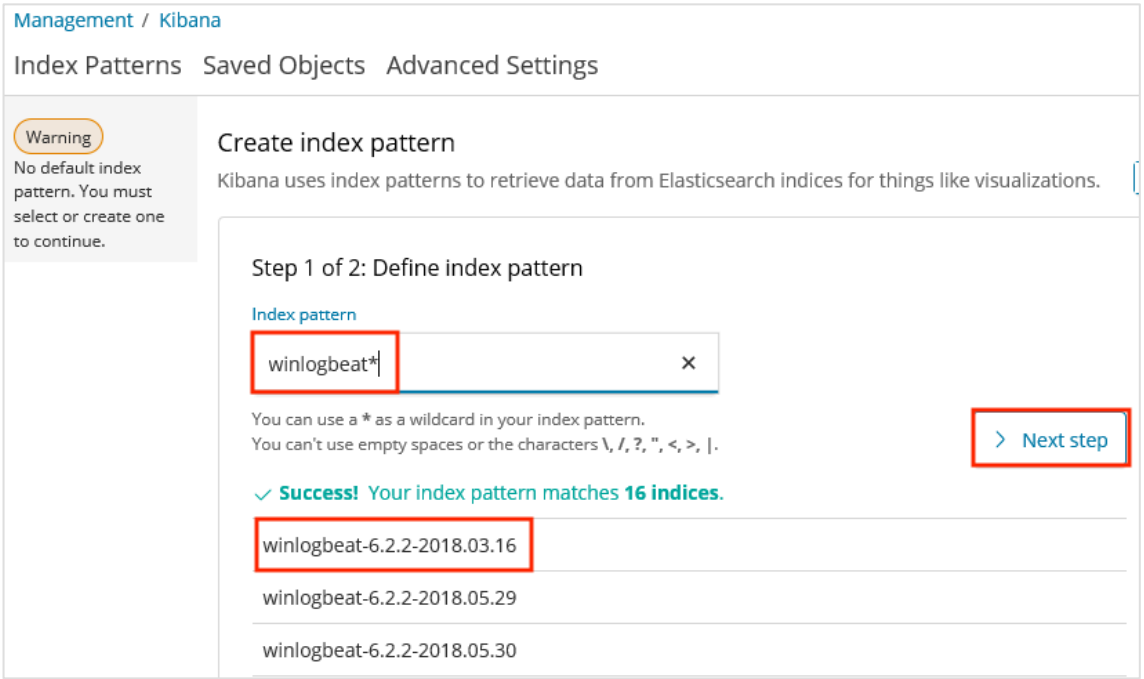

Figura 79: Filtrado de índice de patrones mediante selección

La segunda opción es referida al campo a utilizar como filtro temporal, lo que nos permitirá en sucesivas consultas realizar agrupamientos temporales. En nuestro caso seleccionaremos la marca de tiempo ampliamente utilizada *@timestamp*.

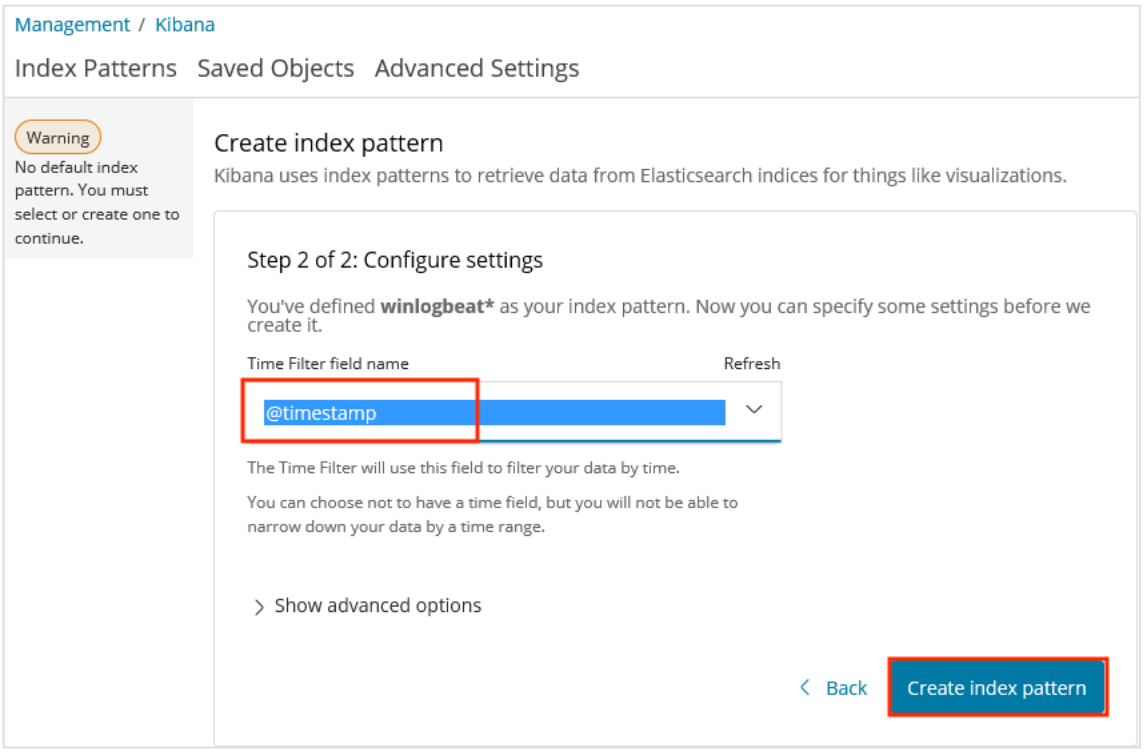

Figura 80: Selección de filtro temporal

Obtendremos un listado con nuestro patrón de índices que contienen todos los campos que Kibana ha detectado y sobre los cuales nos permitirá hacer búsquedas o mostrar visualizaciones:

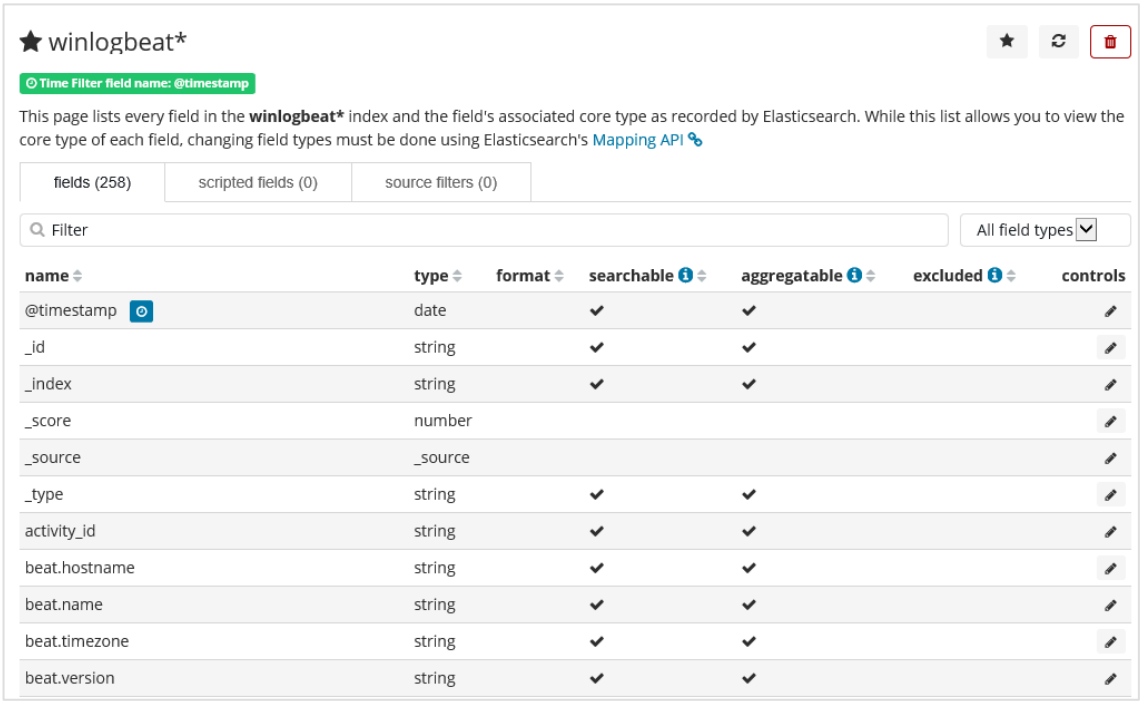

Figura 81: Listado de índices obtenidos de datos recibidos

Seleccionando *Discover* desde el menú lateral izquierdo, nos mostrará todos los campos disponibles para el patrón de índices que acabamos de crear:

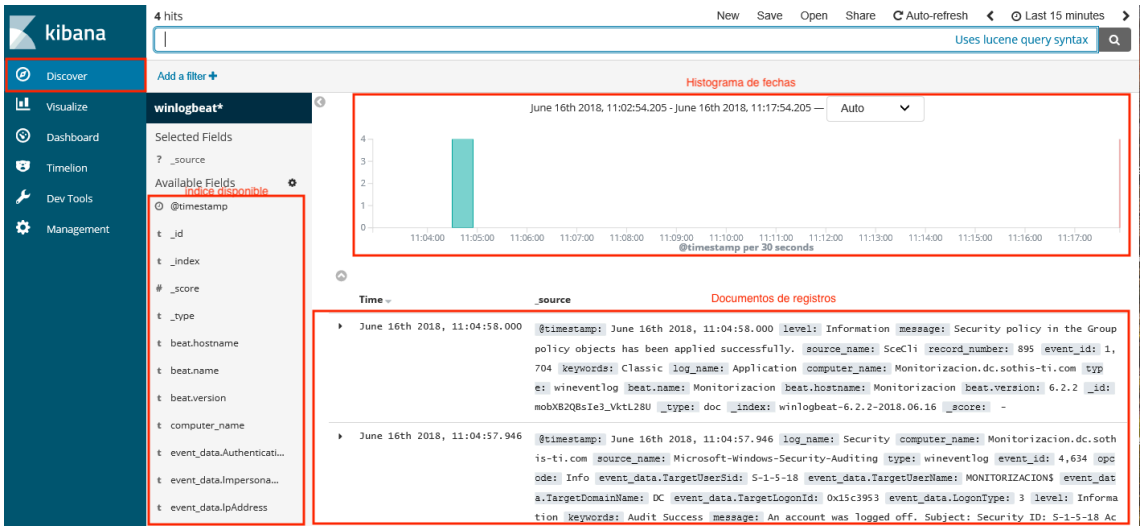

Figura 82: Interface Kibana con los índices analizados y la información correspondiente

Cuando Kibana termina de procesar la selección, mostrará los índices disponibles en el apartado izquierdo, el histograma en la parte superior junto con el número de líneas obtenidas en un rango de tiempo y los documentos de registros almacenados en la parte inferior de nuestro navegador.

Los índices de patrones son los campos seleccionados desde el menú de administración a partir de los datos recibidos desde Winlogonbeat. Pulsando cualquiera de ellos amplía la información mostrando una clasificación con los 5 valores más elevados de todos los registros que mantiene. Seleccionamos como ejemplo los eventos "SubjectUserName" y "TargetDomainName":

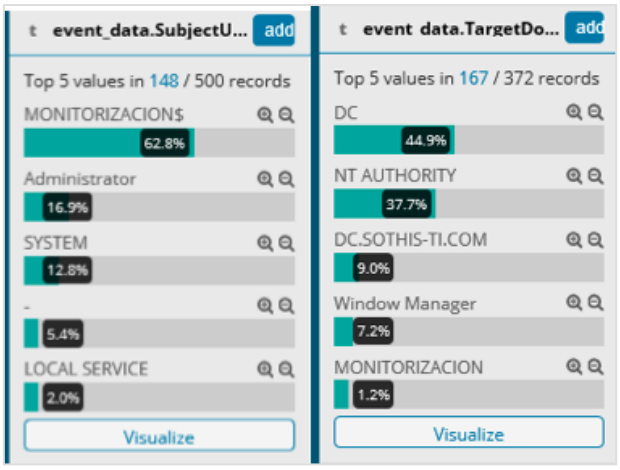

Figura 83: Ejemplo de previsualizaciones en eventos

Y en el mismo índice de patrones, nos muestra el previo. Si queremos ampliar la información podemos hacer uso de la opción de visualización que aparece en la parte inferior de ese mismo menú desplegable.

Los entornos corporativos tienden a realizar una máxima personalización de los sistemas para facilitar la compresión y filtrar el exceso de información. Una de las maneras que tenemos de personalizar las vistas de "Discover", pulsado *add* en el índice de datos nos muestra solo la información de estos patrones mediante desplegables:

Time	event_data.TargetDomainName	event_data.TargetUserName
June 16th 2018, 11:41:41.618	DC	Administrator
June 16th 2018, 11:41:41.618	DC	Administrator
June 16th 2018, 11:41:41.618	DC	Administrator
June 16th 2018, 11:41:41.618	DC	Administrator
June 16th 2018, 11:17:47.945	DC	Administrator
June 16th 2018, 11:17:47.945	DC	Administrator
June 16th 2018, 11:17:47.929	DC	Administrator
June 16th 2018, 11:17:47.929	DC	Administrator

Figura 84: Ampliación de información del evento seleccionado

Una de las herramientas más valoradas por algunos entornos de empresa, incluidos nosotros mismos a la hora de realizar reportes, son las orientadas a visualizaciones gráficas. Las gráficas permiten resúmenes rápidos de datos que pueden ser incluidos en informes y facilitar la comprensión.

Para crear una gráfica, pulsamos la opción de visualización en el menú lateral. Como no tenemos ninguna visualización creada, la página aparece en blanco y accedemos a crear visualización:

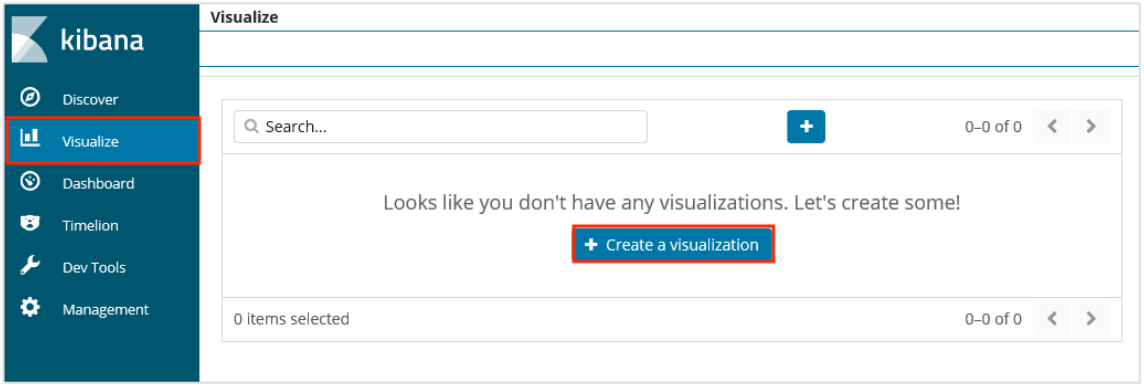

Figura 85: Creación de visualizaciones en Kibana

Kibana muestra una gran cantidad de tipos de gráficas que podemos generar. En la parte superior aparecen las gráficas más comunes y después se va especializando. La imagen solo muestra una parte de las existentes, por ejemplo, las gráficas referidas a los mapas permiten mediante datos de geolocalización y otros datos como direcciones IP, dibujar en un plano la información obtenida. Como ejemplo sencillo, vamos a realizar un típico gráfico de línea:

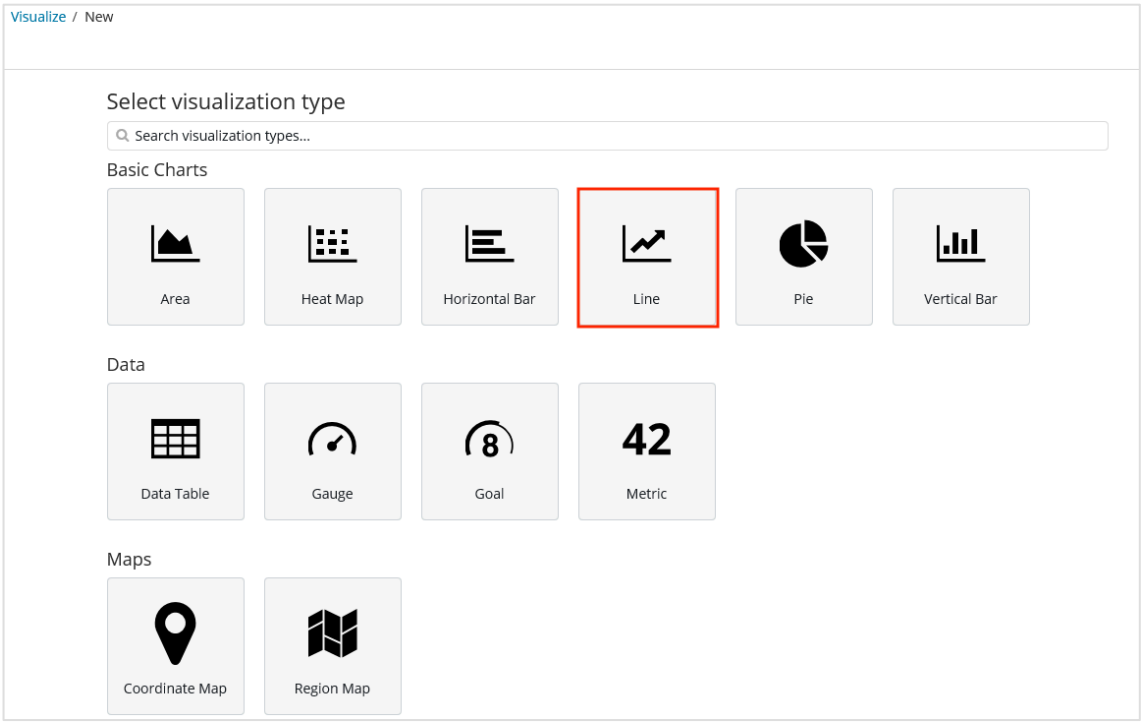

Figura 86: Tipos de visualizaciones disponibles en Kibana

Pulsando el tipo de gráfica de línea nos aparece un menú que nos permite seleccionar crear la gráfica desde algún índice que tengamos creado o desde alguna búsqueda concreta que tengamos. Para nuestro ejemplo partiremos del índice creado, por lo tanto, seleccionamos *winlogbeat**.

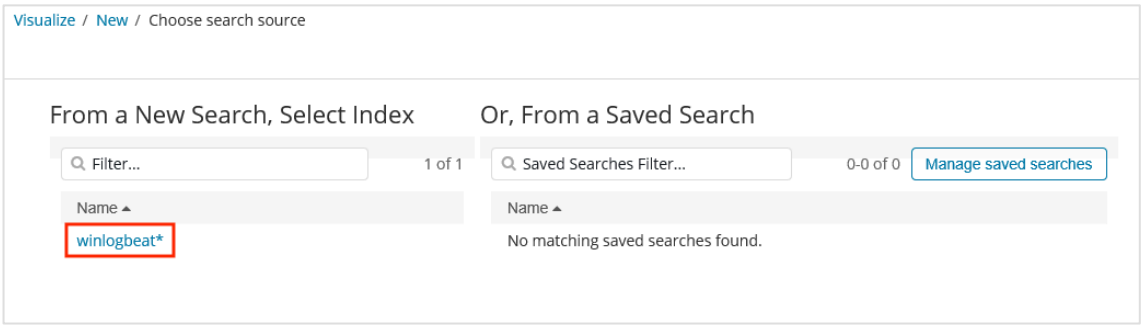

Figura 87: Creación de visualización gráfica desde índice creado en consulta

Lo que nos muestra según iniciamos la gráfica es un solo punto en el que tenemos representado en el eje X todos los documentos y en el eje Y el sumatorio de todos los documentos (de ahí el punto de la gráfica).

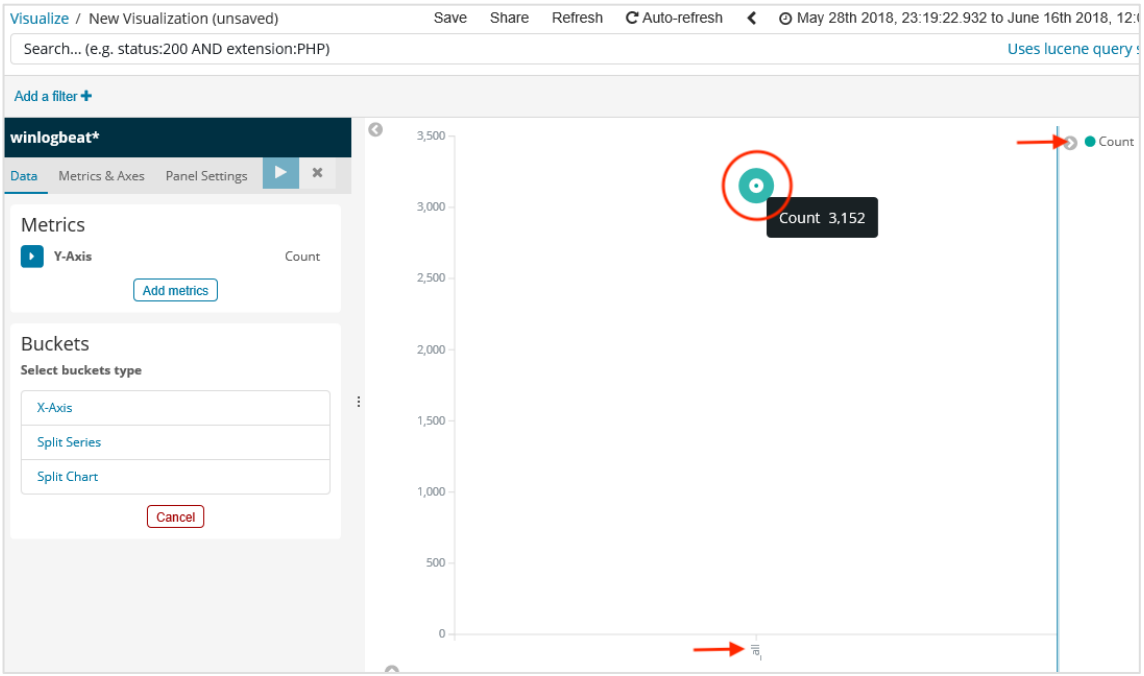

Figura 88: Muestra de gráfica generada automáticamente por Kibana (Sumatorio)

El primer paso es que nos separe el eje X por fecha, pare ello pulsamos X-Axis y añadimos un histograma por fecha. Para el campo de fecha seleccionamos *timestamp* y pulsamos el botón con la figura de *play* para que dibuje el gráfico:

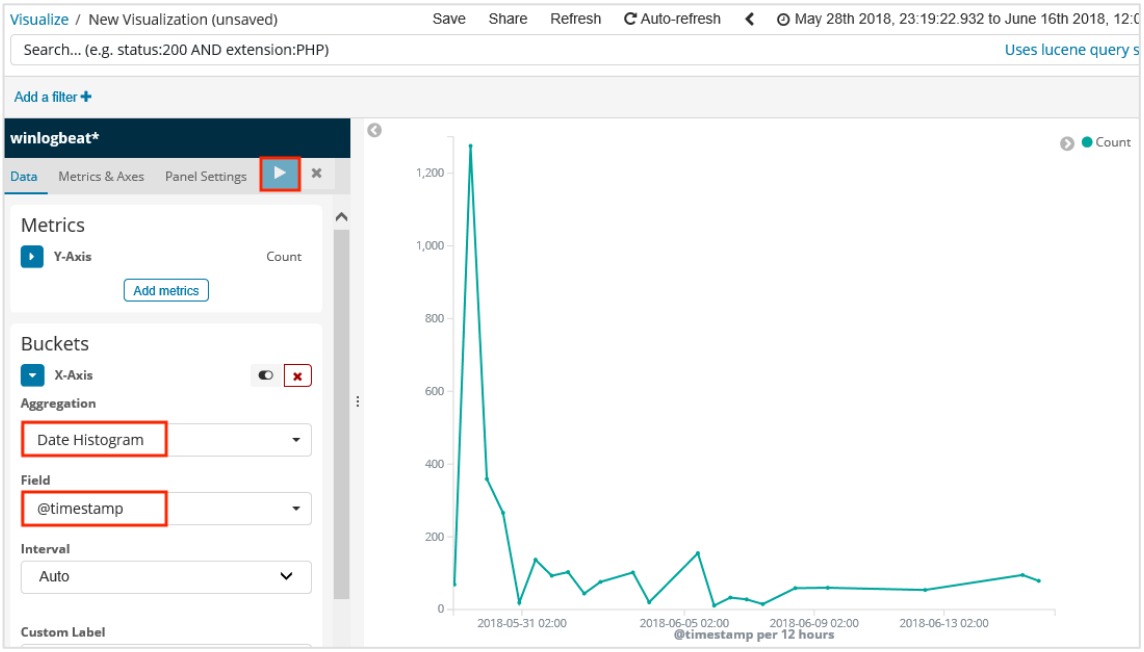

Figura 89: Adecuación de visualización gráfica mediante filtro timestamp

Ahora los datos mostrados son el número de documentos (registros) guardados, por unidad de tiempo (en este caso las últimas 12 horas). Desde la misma pantalla podemos añadir una etiqueta, o ir añadiendo más métricas. Otras opciones de interés como la de crear dos ejes Y diferentes (izquierdo y derecho) mediante el menú Metrics & Axes. Esta opción puede ser de gran ayuda para representar gráficas con rangos muy distintos.

Como administradores de red tenemos la opción de usar este tipo de consultas como apoyo en las tareas de supervisión y podemos obtener visualizaciones simples, seleccionando el proceso e indicando "mostrar visualización", como añadimos en el ejemplo:

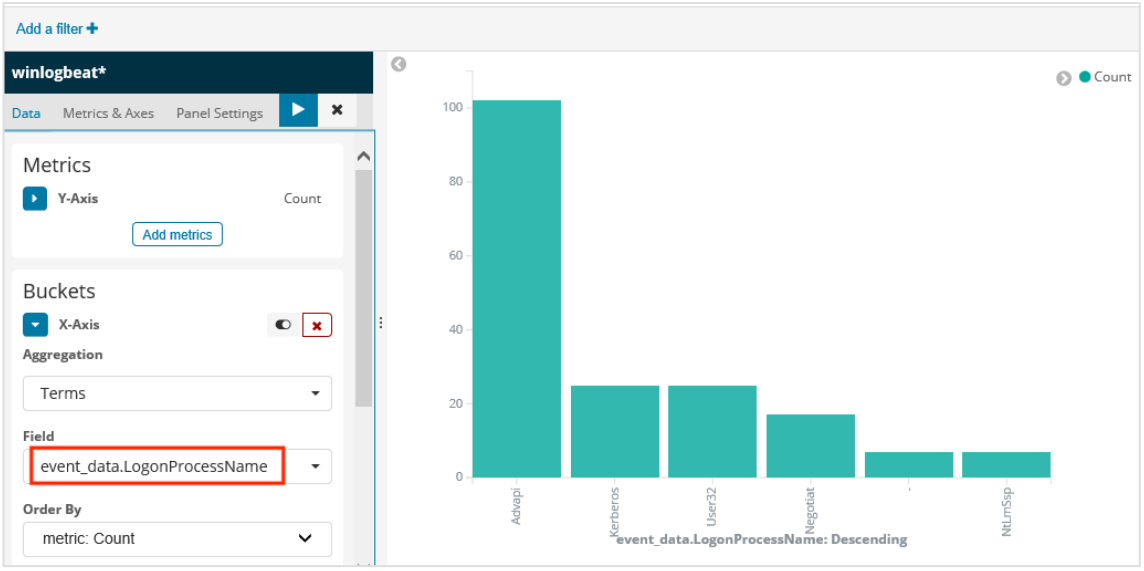

Figura 90: Ejemplo sobre visualización de procesos que acceden remotamente al servidor

En el ejemplo hemos filtrado la información teniendo en cuenta los procesos que acceden remotamente. Otro tipo de consultas típico para tener en cuenta en nuestra red empresarial sería seleccionando el mensaje de tipo error o advertencias y añadir campos como:

- *Computer_name*
- *DC_Name*
- *Error name/code/description*
- *IPAddress*
- *Task*

Guardando la consulta (opción "*save*" e indicar un nombre), podríamos generar consultas más o menos complejas y disponibles de manera cómoda.

Los tipos de filtrados son muy abiertos y los expuestos son un ejemplo. Debemos tener en cuenta parámetros de red como desde qué tipo de equipos estamos recogiendo los registros y siempre dejar el cauce abierto a modificaciones en caso de obtener una saturación de registros o descartar informaciones irrelevantes.

Desde Kibana existen otras opciones como *Dashboard* que consisten en la agregación de diferentes consultas individuales en un mismo panel, práctico cuando se tiene muy claro el sistema de monitorización, o cuando se quieren montar paneles informativos de aspecto sofisticado en la empresa. Estos aspectos no los trataremos puesto que no aportan información extra de nuestra red empresarial y son solo visualizaciones.

5. Conclusiones

En el presente TFG hemos expuesto los problemas habituales de algunas empresas con su infraestructura de red y propuesto dos soluciones que pueden ser aplicadas conjuntamente para la mejora de fiabilidad del entorno corporativo:

- La administración de las direcciones IP usadas en las comunicaciones.
- El registro y procesamiento de sucesos que ocurren en los dispositivos de la red corporativa.

Las mejoras presentadas se basan en el incremento de funcionalidades y en la centralización de la administración de servicios con el fin de permitir monitorizar, anticipar y gestionar con eficiencia los equipos corporativos, así como minimizar el impacto que puede producir un fallo de servicio.

Se ha utilizado un modelo estándar de empresa para realizar el despliegue, la variación con el resto de los modelos aquí presentados no sería muy significativo a excepción de que implicara un cambio en el empleo de directorio activo. Las herramientas seleccionadas para este trabajo han sido analizadas teniendo en cuenta puntos clave como:

- Características ofrecidas que aportan nuevas funcionalidades en el caso del IPAM y permiten una exhaustiva supervisión gracias al lector de registros, ambos centralizados en servidores de gestión.
- Integración dentro del ecosistema existente, sin necesidad de modificar los servicios que se encuentran funcionando y aplicando el mínimo hardware posible.
- Coste de las licencias de herramienta, gratuitas en ambos casos, aunque ha sido necesaria la licencia del servidor que alija el servicio.

Como encargado de una parte de la administración de red, puedo constatar que una de las facetas más importantes en el desarrollo es la planificación. Una planificación de sistemas correcta debería incluir herramientas de gestión como las aquí tratadas, pero lamentablemente no siempre es así al no monetizar a corto plazo en el rendimiento empresarial.

A nivel personal he aprendido la estructura de servicios corporativos, la realización y análisis de sistemas de las herramientas vistas y la profundización en el funcionamiento de Windows Server junto con su virtualización corporativa.

El contacto con la empresa en la cual he desarrollado las prácticas y el resto de las empresas con las que mantengo contacto han sido cruciales para el completo desarrollo del trabajo ya que me han dado la oportunidad de ver sus necesidades, comparar diversos servicios utilizados y poder encontrar una solución satisfactoria.

6. Trabajos futuros

La solución aplicada para la administración de direcciones se encuentra completa y operativa por lo que posibles modificaciones que podemos prever son tales como la actualización de la versión del servidor a la reciente versión 2016 que, debido a la integración afectaría a la actualización de la propia herramienta.

La segunda de las soluciones de administración de registros es recomendable que sea ampliada a la mayor parte de equipos principales de la red. Para nuestro trabajo hemos usado el servidor que gestiona el directorio activo, y de igual manera se aplica en el resto de los servidores, pero es muy interesante actuar sobre equipos de red más especializados como son los cortafuegos. Sobre estos últimos, el equipamiento analizado ha sido exclusivamente de la empresa "Fortinet". Dichos equipos permiten la integración con el software instalado mediante la configuración de envío de registros, pero debido a la ausencia de repuestos y elevado precio, su inclusión se encuentra pendiente de autorización.

Como inclusión de nueva mejora que podemos añadir y que encajaría perfectamente con las vistas anteriormente, es la incorporación de un servidor proxy. El servidor proxy es una manera de centralizar y controlar las conexiones con Internet además de aportar otras mejoras tanto en seguridad como incremento de velocidad de navegación manteniendo el ancho de banda existente.

En la empresa dónde se han desarrollado las labores prácticas se ha propuesto el servidor proxy como mejora, aunque al encontrarse inmersos en un cambio de operador con incremento de ancho de banda no se ha optado temporalmente por la implementación de proxy. Sin embargo, la propuesta ha gustado y será nuevamente estudiada al finalizar la migración de operador.

7. Bibliografía

[1] PhpIPAM. Información de herramienta código abierto IPAM. [En línea] https://phpipam.net 2018. Disponible en: https://phpipam.net/documents/

[2] Solaris Winds. Información de herramienta comercial IPAM. [En línea] https://www.solarwinds.com 2018 Disponible en: https://www.solarwinds.com/es/ip-address-manager

[3] NIPAP. Información de herramienta de código abierto IPAM. [En línea] http://spritelink.github.io/NIPAP/ 2018 Disponible en: http://spritelink.github.io/NIPAP/docs/config-www.html

[4] Network Faculty. Catálogo de eventos. [En línea] https://networkfaculty.com 2016 Disponible en: https://networkfaculty.com/es/video/detail/2266-windows-server-2012-ipam---catalogo-de-eventos

[5] Network Faculty. Funcionalidades IPAM. [En línea] https://networkfaculty.com 2016 Disponible en: https://networkfaculty.com/es/video/detail/2258-windows-server-2012-ipam---funcionalidad

[6] Microsoft. Usos de directiva DNS. [En línea] https://docs.microsoft.com 2018 Disponible en: https://docs.microsoft.com/es-es/windows-server/networking/dns/deploy/app-lb

[7] Microsoft. Ámbito de acceso para zonas DNS. [En línea] https://docs.microsoft.com 2018 Disponible en: https://docs.microsoft.com/es-es/windows-server/networking/technologies/ipam/set-access-scope-for-a-dns-zone

[8] Microsoft. Configurar servidor IPAM en VMM. [En línea] https://docs.microsoft.com 2018 Disponible en: https://docs.microsoft.com/es-es/system-center/vmm/network-ipam?view=sc-vmm-1801

[9] NEDIM'S IT CORNER. Instalación y configuración IP de IPAM. [En línea] https://nedimmehic.org 2017 Disponible en: https://nedimmehic.org/2017/06/01/install-and-configure-ip-address-management-ipam-2016-part-2/

[10] Splunk. Información de herramienta comercial para recogida de eventos. [En línea] https://www.splunk.com 2018 Disponible en: https://www.splunk.com/en_us/software/splunk-light.html

[11] Kiwi. Información de herramienta comercial para recogida de eventos. [En línea] https://www.kiwisyslog.com 2018 Disponible en: https://support.solarwinds.com/Success_Center/Kiwi_CatTools

[12] Elastic. Documentación instalación Beats. [En línea] https://www.elastic.co 2017 Disponible en: https://www.elastic.co/guide/en/beats/libbeat/6.3/index.html

[13] Elastic. Documentación instalación Beats. [En línea] https://www.elastic.co 2017 Disponible en: https://www.elastic.co/guide/en/beats/libbeat/6.3/index.html

[14] Elastic. Documentación instalación Kibana. [En línea] https://www.elastic.co 2017 Disponible en: https://www.elastic.co/guide/en/kibana/6.3/install.html

[15] Elastic. Documentación instalación Beats. [En línea] https://www.elastic.co 2017 Disponible en: https://www.elastic.co/guide/en/beats/libbeat/6.3/index.html

[16] Elastic. Documentación instalación ElasticSearch. [En línea] https://www.elastic.co 2017 Disponible en: https://www.elastic.co/guide/en/elasticsearch/reference/current/install-elasticsearch.html

[17] Elastic. Documentación instalación Logstash. [En línea] https://www.elastic.co 2017 Disponible en: https://www.elastic.co/guide/en/logstash/6.3/dir-layout.html

Abreviaturas y siglas

AD: Active Directory

API: Application Programming Interface

BD: Base de datos

CPD: Centro de procesamiento de datos

CPU: Central Processing Unit

DHPC: Dynamic Host Protocol Configuration

DLQ: Dead Letter Queues

DNS: Domain Name System

ETL: Extract Transform and Load

FQDN: Fully Qualified Domain Name

GPO: Group Policy Object

IP: Internet Protocol

IPAM: IP Address Manager

IPAMUG: IP Address Manager Universal Group

JDK: Java Development Kit

JSON: JavaScript Object Notation

LAN: Local Area Network

LDAP: Lightweigth Directory Access Protocol

MAC: Media Access Control

NPS: Network Policy Server

OS: Operating System

RAM: Random Access Memory

RDS: Remote Desktop Services

REST: REpresentational State Transfer

SQL: Structured Query Language

TCP: Transmission Control Protocol

UDP: User Datagram Protocol

URL: Uniform Resource Locator

USB: Universal Serial Bus

VMM: Virtual Machine Manager

VLAN: Virtual LAN

WID: Windows Internal Database