Diseño e implementación de una infraestructura para computación en la nube y servicios TI

Francisco José Ramírez Vicente
Grado Ingeniería Informática

Manuel Jesús Mendoza Flores

8 de Junio, 2016

FICHA DEL TRABAJO FINAL

Título del trabajo:	Diseño e implementación de una infraestructura para computación en la nube y servicios TI
Nombre del autor:	Francisco José Ramírez Vicente
Nombre del consultor:	Manuel Jesús Mendoza Flores
Fecha de entrega (mm/aaaa):	06/2016
Área del Trabajo Final:	Administración de redes y S.O.
Titulación:	Grado en Ingeniería Informática

Resumen del Trabajo (máximo 250 palabras):

La mayoría de las empresas hoy día tienden a migrar los servicios relacionados con TI hacia la nube. Existen soluciones, como por ejemplo *Microsoft Azure* o *Amazon EC2* que ofrecen la posibilidad de configurar prácticamente cualquier tipo de infraestructura en un entorno virtual o de computación en la nube.

En cambio, a veces, ya sea por política de empresa o por motivos económicos, el control interno de la información o incluso para ofrecer precisamente este tipo de servicios tipo *cloud*, es necesario comprender los principales conceptos de diseño para hardware y/o software que hacen posible este tipo de plataformas.

El TFG ofrece una introducción a la instalación, configuración y optimización (mejores prácticas) de una infraestructura profesional básica y totalmente escalable, capaz de albergar diferentes entornos (todo tipo de clientes y/o empresas) totalmente aislados entre ellos, y a su vez, ofrecer todo tipo de servicios relacionados con la nube.

Buscando una aplicación en el mundo real, este TFG se centrará en la configuración para ofrecer todos los servicios necesarios para una empresa independientemente de su tamaño, desde el correo electrónico, almacenamiento, gestión de aplicaciones y copias de seguridad.

El TFG estará básicamente dividido en dos partes. La primera parte se centrará en la configuración hardware. La segunda parte estará enfocada en la instalación del sistema operativo (Windows 2012), el entorno de virtualización (*clúster* Hyper-V) y configuración del correo (Exchange 2013).

Espero que este TFG cumpla el objetivo de ofrecer una solución práctica a la hora de implementar una infraestructura de servicios TI.

Abstract (in English, 250 words or less):

The majority of companies today tend to migrate their IT services to the cloud. Solutions exist, for example *Microsoft Azure* or *Amazon EC2*, which offer the possibility of configuring almost any type of infrastructure in a virtual environment or in cloud computing.

On the other hand, sometimes, because of company policies, economic motives, internal control of the information, or even to offer cloud services, it is necessary to understand the main hardware and software design concepts that make these types of platforms possible.

The TFG gives an introduction to the installation, configuration and optimization (best practices) of a basic professional infrastructure based on virtual machines, totally scalable, capable of hosting different environments (all kinds of clients and/or companies), isolated from each other and simultaneously offering all types of services dealing with the cloud.

Searching above all for an application in the real world, this TFG will focus on the configuration necessary to provide all services to a company (regardless of its size) from email to storage to management of applications to backups.

The TFG will be divided in two parts. The first part will focus on hardware configuration. The second part will focus on the operating system's installation (Windows 2012), the virtual environment (cluster Hyper-V), and email configuration (Exchange 2013).

I hope that this TFG achieves the goal of offering general guidance and at the same time a practical solution when implementing an IT services infrastructure.

Palabras clave (entre 4 y 8):

Infraestructura, Servidores, Cloud, Servicios, Virtualización, Correo, Clúster, Backup

Índice

Lista de figuras

1. Introducción

1.1 Contexto y justificación del Trabajo

La *nub*e o *cloud* es la palabra de moda en el mundo de las TI. A día de hoy, cualquier empresa puede instalar el 100% de sus servicios sin invertir prácticamente nada en hardware. Sólo tiene que elegir un proveedor de *cloud computing* de los cientos que hay que el mercado y en unas horas podrá configurar *ad hoc* cualquier tipo de servicio de TI que necesite. En cambio, sobre todo en las grandes empresas, puede que exista la necesidad de ofrecer este tipo de servicio pero de forma interna, sin depender de proveedores externos. Por ejemplo, una gran empresa con diferentes oficinas por todo el mundo que tenga diferentes dominios y/o clientes (por ejemplo una gran empresa con filiales), es posible que quiera instalar su propia *nube* para ofrecer servicios como el correo electrónico, aplicaciones y almacenamiento de forma totalmente independiente.

Las ventajas de instalar y configurar este tipo de solución internamente son básicamente la seguridad de la información (todo queda dentro de la organización) y total control sobre los dispositivos hardware. Entre las desventajas, destacar el coste de instalación y mantenimiento de estos servicios. Este TFG puede ser un punto de partida para ofrecer una solución empresarial o simplemente una posible opción de configuración para proveer este tipo de servicio tan demandado hoy día.

1.2 Objetivos del Trabajo

A continuación se detallan los objetivos principales de este TFG:

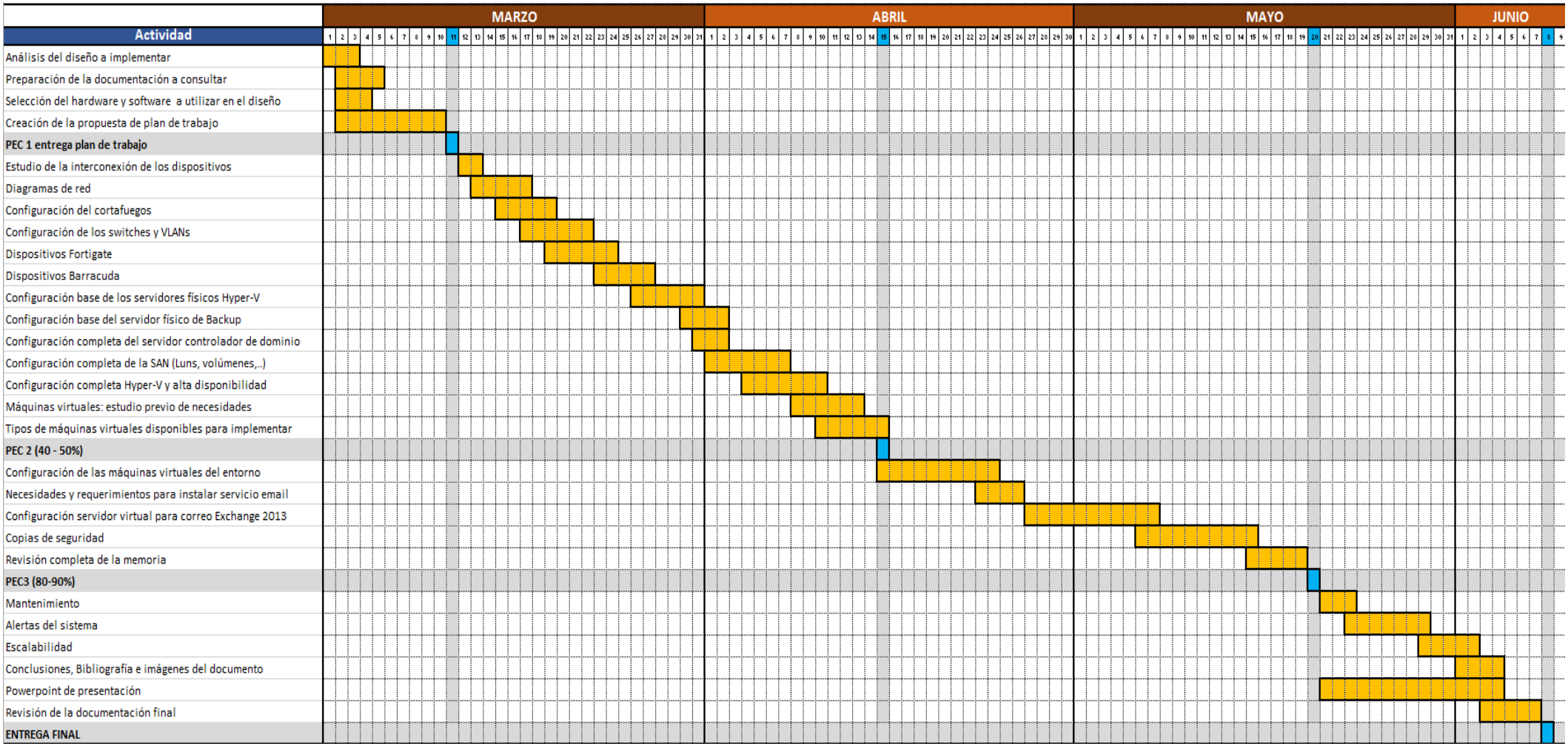
- Elección del hardware y software necesario para realizar el proyecto.
- Configuración del cableado, esquemas de conexión de la red y configuración básica de los dispositivos de red.
- Configuración del software, correo y sistema operativo.
- Servidores y *SAN*, configuración y conexión.
- Entornos virtuales, configuración de los servidores *host* y alta disponibilidad.
- Separación de los diferentes entornos virtuales, segmentación de red y recursos virtuales.
- Configuración *DNS* y conectores para el correo.
- Copia de seguridad.

1.3 Enfoque y método seguido

La configuración de este proyecto se basa en una estrategia clásica de instalación de servidores de virtualización en un entorno de almacenamiento, con alta disponibilidad y con la información localizada en una *SAN*. Este método de configuración es sólido y funciona con cualquier sistema operativo actual. Por lo tanto la clave del éxito se centra en la elección del hardware necesario para su implementación y su correcta configuración. Existen una gran variedad de modelos y dispositivos, y todos ellos pueden, en mayor o menor medida, cumplir con los objetivos previstos.

La forma de interconectar los dispositivos hardware y la configuración de los servidores influye también a la hora de obtener el mejor rendimiento posible. Este TFG intenta reunir todas las buenas prácticas aplicadas a todas las fases de instalación y configuración del proyecto y de esa forma, obtener la mejor integración hardware y software.

1.4 Planificación del Trabajo



1.5 Material necesario, instalación y configuración

Hardware:

Marca	Modelo	Ud.	Función a realizar
CISCO	ASA 5520	1	Cortafuegos, seguridad perimetral, primera capa. Gestión de puertos
Barracuda	Web Filter 610	1	Proxy de navegación web
Barracuda	Message Archiver 450	1	Almacenamiento/*Archiving* de correos
Barracuda	Spam Firewall 300	1	Seguridad del correo, *antispam*
Fortigate	800C	2	Seguridad perimetral, segunda capa, aplicada a los diferentes clientes/oficinas. Gestión del tráfico de red.
CISCO	4900m	2	Switches principales
CISCO	SG200-8	1	Switch alta disponibilidad dispositivos Barracuda
CISCO	Catalyst 2960S 24TS	1	Switch para gestionar el tráfico de los dominios virtuales
HP	Proliant DL560 G9	2	Servidores virtualización Hyper-V
HP	Proliant DL60 G9	1	Servidor controlador de dominio principal y WSUS
HP	Proliant DL20 G9	1	Servidor de copias de seguridad
HP	MSA 2040	1	Almacenamiento SAN
HP	2024	1	Librería de cintas para copia de seguridad, LTO6
Buffalo	Terastation 5400 12TB	1	Backup de la información remota, escalable
APC	SRT 8000VA 208V IEC	1	UPS. Este modelo es suficiente para la carga de los dispositivos críticos. Ofrece una autonomía de 20 minutos en caso de fallo

Software:

Marca	Versión	Uds.	Función a realizar
Microsoft	Windows Server Enterprise 2012 (Hyper-V)	4 (*)	Sistema operativo base de la implementación. Sobre esta definiremos las licencias de las máquinas virtuales y las *cals* necesarias. (*) Cada entorno virtual a implementar tendrá su propio licenciamiento de Windows Server
Microsoft	Exchange Server Standard 2013	N.A.	Una licencia para cada entorno al que ofrezcamos servicio de correo electrónico más las *cals* necesarias.
Symantec	Backup Exec 2015	1	Licencia principal del software para la centralización de las copias de seguridad. Habrá que añadir las siguientes licencias para los agentes: 3 Licencias de Agente Windows 2 Licencias Hyper-V
Kaspersky	Por determinar	N.A.	Las licencias se definirán a medida que vayamos implementando la configuración final.

Servicios y otros materiales:

Descripción	Uds.	Función a realizar
Armario Rack 42U	1	Armario principal para la instalación de todo el material
Cableado	N.A.	Diferentes cables de diferentes colores, CAT6
Interfaces *Fiber Channel*	1	Por determinar en función de la instalación elegida
Interfaces SAS	1	Conexión del servidor de Backup con la librería de cinta

La instalación física en el armario rack y el cableado se pueden realizar en dos días de trabajo. La configuración de los dispositivos puede durar en torno a tres días laborables. Por lo tanto todo podría estar preparado para pasar a producción en una semana (cinco días laborables). Por supuesto, esta estimación puede variar, sobre todo si vamos a realizar la instalación en un centro de datos que ya contiene otras configuraciones. No se contabiliza el coste de mano obra porque supuestamente será realizado por personal interno del equipo de TI.

1.6 Breve descripción de los otros capítulos de la memoria

Capítulo 2. *Análisis del diseño presentado*. Primer análisis de las características básicas del diseño de la infraestructura. También se describen las ventajas y desventajas del mismo así como algunas alternativas de diseño.

Capítulo 3. *Selección del hardware*. Criterios elegidos y sus ventajas y desventajas del hardware seleccionado para la electrónica de red, almacenamiento, servidores y otros componentes.

Capítulo 4. *Selección del software*. Criterios, ventajas y desventajas, del software seleccionado para los Sistemas Operativos, copias de seguridad y la solución antivirus.

Capítulo 5. *Interconexión de los dispositivos*. Se muestran esquemas de interconexión de los *switches*, *SAN*, servidores, conexión SAS entre el servidor de backup y la librería de cintas, conexiones de gestión (*ILO* y otras). También se hace mención a las conexiones eléctricas.

Capítulo 6. *Configuración de los dispositivos de red*. Este capítulo se centra especialmente en la configuración del firewall, switches, Fortinet y Barracuda. Se hace un análisis completo de los *VDOM* de los dispositivos Fortigate C800 así como la configuración de los dispositivos Barracuda Web Proxy, Spam Filter y Email Archiver.

Capítulo 7. *Configuración de los servidores físicos.* Este capítulo abarca la configuración de los servidores físicos como el controlador de dominio, servidores Hyper-V y servidor de Backup. Se detallan los roles necesarios para cada servidor según su función.

Capítulo 8. *Configuración del entorno SAN*. La configuración *SAN* es una de las partes más importantes de este diseño, por eso este capítulo se dedica íntegramente su configuración, desde los primeros pasos hasta la creación de volúmenes pasando por la conexión a los *hosts*.

Capítulo 9. *Virtualización (Hyper-V).* En este capítulo se detalla la configuración de las conexiones iSCSI entre Windows Server 2012 R2 y los volúmenes de la *SAN*. También se detalla cómo realizar la configuración de alta disponibilidad del clúster (*failover*).

Capítulo 10. *Configuración de las máquinas virtuales*. Las máquinas virtuales alojadas en esta infraestructura realizarán diferentes funciones como servidores de directorio activo, así como *DHCP*, *DNS*, servidores de ficheros, etc. En este capítulo se analizan los detalles a tener en cuenta tanto en la reserva de recursos como su configuración de red.

Capítulo 11. *Servidores virtuales de correo electrónico*. Posiblemente el servicio de correo electrónico sea el más importante que podamos ofrecer con este diseño. Por lo tanto requiere un capítulo completo donde se explican paso a paso todos los detalles para conseguir un sistema funcional. Desde los registros *DNS* públicos, hasta la configuración de Microsoft Exchange 2013 pasando por la configuración para almacenar correos en el dispositivo Barracuda Archiver.

Capítulo 12. *Copias de seguridad*. Los diferentes medios para responder a cualquier situación de desastre con pérdida de información se detallan en este capítulo. Desde la copia en dispositivos *NAS* hasta su volcado posterior en cintas, así como algunos consejos para el almacenaje y utilización del software de backup.

2. Análisis del diseño presentado

2.1. Descripción general

El diseño propuesto en este TFG tiene las siguientes características como base fundamental:

1. Alta disponibilidad
2. Seguridad de la información
3. Separación de la red de datos y almacenamiento

La alta disponibilidad se intentará implementar en prácticamente todos los dispositivos críticos a nivel de hardware. Podemos comprobarlo desde el primer nivel, la conexión a Internet, donde se observa que existe una primera línea de datos contratada con un proveedor (*ISP Proveedor 1*) y otra adicional de backup (*ISP Proveedor 2*) que se activará automáticamente en caso de caída de la línea principal (*Figura 1*, página siguiente).

El cortafuegos Cisco ASA 5520, además de ser el pilar principal de la seguridad perimetral, gestión de tráfico y bloqueo y/o apertura de puertos, es también el encargado de activar la línea de backup automáticamente en caso de fallo.

Referente a los datos, todo el tráfico, tanto de la red de datos como de la red de almacenamiento, está gestionada por dos switches CISCO 4900m conectados en alta disponibilidad y con dos módulos de red cada uno para diferenciar el tráfico entre las dos redes. La red de tráfico (línea azul, *Figura 1*) gestiona toda la información que circula entre todos los dispositivos de la red (excepto la *SAN* y la librería de cintas) hasta su salida a Internet. Es en esta red donde se ubican todos los dispositivos de seguridad así como los servidores (controlador de dominio, copia de seguridad y servidores de virtualización, estos últimos tendrán conexión en ambas redes).

La red de almacenamiento (línea roja, *Figura 1*) se utiliza exclusivamente para el tráfico de datos relacionados con el almacenamiento de las máqui*nas* virtuales en la unidad *SAN* y backup. Estará configurada con diferentes particiones (*LUN Logical Unit Number*) conectando los discos en *RAID* para ofrecer la mejor opción de recuperación en caso de fallo de alguno de ellos. No sólo la *SAN* ofrecerá alta disponibilidad para esta red de almacenamiento, los servidores Hyper-V y los switches estarán configurados de la misma manera para ofrecer el mejor rendimiento posible y recuperación en caso de fallo.

Los servidores Hyper-V, HP Proliant DL560, son los encargados de gestionar los recursos de virtualización. Estarán conectados a las dos redes, la de producción *LAN* y la red de almacenamiento, utilizando diferentes tarjetas de red. Y además de conectarán en un clúster de alta disponibilidad. En caso de fallo, las máquinas se moverán de un nodo al otro de forma automática.

Como se ha mencionado antes, por la red de datos (línea azul, *Figura 1*) circula la información centrada principalmente en la gestión de la infraestructura e Internet. La seguridad del tráfico interno es monitorizada y gestionada por dispositivos marcas Barracuda y Fortinet.

Los dispositivos Barracuda se centran sobre todo en la navegación web y el correo electrónico. Para gestionar la navegación web, se utilizará un dispositivo Barracuda WebFilter 610 que actuará como proxy para todos los clientes, configurado para gestionar diferentes dominios. El correo será gestionado, igualmente configurando diferentes dominios, por un Barracuda Spam Firewall modelo 300. Finalmente, todos los correos serán almacenados, diferenciados por dominios, en un Barracuda Archiver.

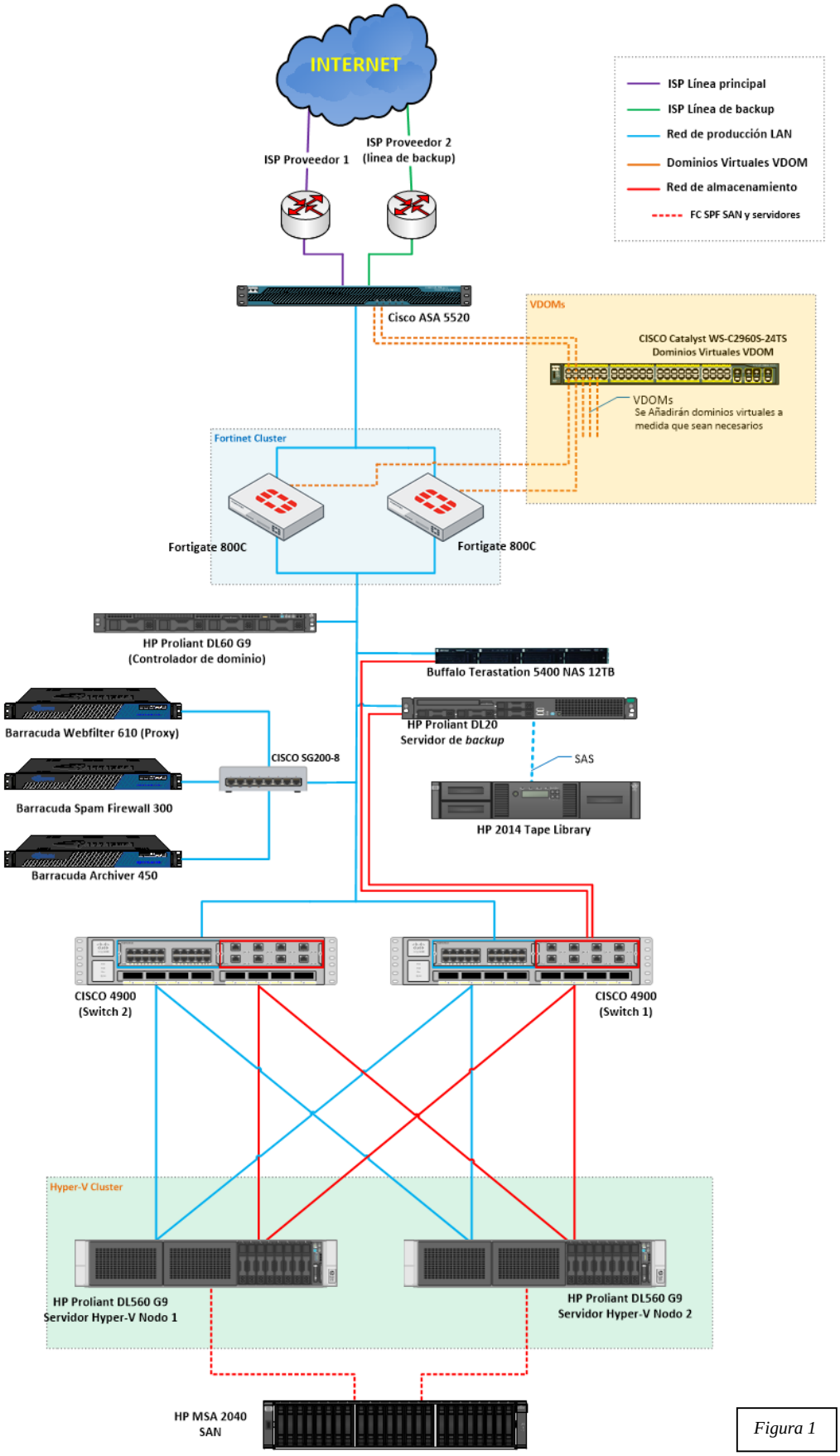

INTERNET
ISP Proveedor 1
ISP Proveedor 2
(linea de backup)
ISP Línea principal
ISP Línea de backup
Red de producción LAN
Dominios Virtuales VDOM
Red de almacenamiento
FC SPF SAN y servidores
Cisco ASA 5520
VDOMs
CISCO Catalyst WS-C2960S-24TS
Dominios Virtuales VDOM
VDOMs
Se Añadirán dominios virtuales a
medida que sean necesarios
Fortinet Cluster
Fortigate 800C
Fortigate 800C
HP Proliant DL60 G9
(Controlador de dominio)
Buffalo Terastation 5400 NAS 12TB
Barracuda Webfilter 610 (Proxy)
CISCO SG200-8
HP Proliant DL20
Servidor de backup
SAS
Barracuda Spam Firewall 300
HP 2014 Tape Library
Barracuda Archiver 450
CISCO 4900
(Switch 2)
CISCO 4900
(Switch 1)
Hyper-V Cluster
HP Proliant DL560 G9
Servidor Hyper-V Nodo 1
HP Proliant DL560 G9
Servidor Hyper-V Nodo 2
HP MSA 2040
SAN

Figura 1

El clúster creado con dispositivos Fortinet se centrará básicamente en servir de apoyo al firewall principal CISCO en tareas de gestión de puertos y tráfico de red, sobre todo en la configuración y aislamiento de los diferentes entornos que vamos a hospedar. Otra de sus funciones será ofrecer una solución inteligente a posibles amenazas de seguridad como vulnerabilidades (*zero-day*), antivirus de red, aplicación de políticas de seguridad, monitorización de red, sistema detector de intrusión, etc. Al ser un tema crítico, se ha optado por la conexión en clúster a modo de *failover* o alta disponibilidad (si uno falla, el otro entra automáticamente en funcionamiento con la misma configuración, transparente al funcionamiento del servicio).

Sobre la creación de los *Dominios Virtuales* o *VDOMs*, cada Fortigate800C tiene 12 puertos Ethernet los cuales se pueden configurar para un dominio privado, por ejemplo para una oficina o un cliente externo. Este tema se explica más en detalle en el *Capítulo 6.5*.

La combinación de ambos, Barracuda y Fortinet, ofrece una gran solución de seguridad que nos permitirá implementar las políticas que deseemos en nuestro entorno. El único inconveniente es el precio, pero siempre existe la posibilidad de modificar el diseño para eliminar algún elemento. Por ejemplo, los Fortigate C800 elegidos para esta configuración, pueden hacer también las funciones de anti SPAM, pero el dispositivo Barracuda tiene mejores prestaciones y evitamos saturar de trabajo a los dispositivos Fortinet.

Toda la gestión de Directorio Activo (*AD*) de gestión (red principal del diseño) será administrada por un servidor físico HP Proliant DL60. Este servidor también se hará cargo de otros servicios como *DNS* o *DHCP*.

Finalmente, para la copia de seguridad se ha seleccionado un servidor físico HP Proliant DL20 el cual se conectará mediante una conexión *SAS* con la librería de cinta modelo HP 2014. Como apoyo a la copia de seguridad, se ha optado por un dispositivo Buffalo Terastation 5400, con 12TB, escalable. Es aquí donde se realizarán las copias de seguridad tanto locales (máquinas virtuales) como de los posibles servidores remotos. La librería de cintas se encargará de hacer el volcado a cintas tipo *LTO 6* de toda la información.

2.2. Ventajas y desventajas

Este diseño ofrece las principales ventajas:

- **Seguridad.** Es un factor clave en cualquier infraestructura, pero sobre todo es vital en aquella que está ofreciendo algún tipo de servicio, como es este caso propuesto. En el diseño se ha hecho un esfuerzo importante, tanto económico como técnico, para obtener una infraestructura que ofrezca un nivel de seguridad máximo. Se han definido tres niveles de seguridad, desde la conexión a Internet, tráfico *LAN* y correo electrónico.

- **Alta disponibilidad:** los dispositivos y servicios críticos tienen una doble configuración para poder ofrecer alta disponibilidad en caso de fallo. La conexión a Internet por ejemplo, se contratará con dos proveedores distintos para garantizar siempre que haya conectividad. Los sistemas hardware críticos también tienen alta disponibilidad, como por ejemplo los dispositivos Fortigate, los switches CISCO *core* y los servidores de virtualización.

- **Control sobre los sistemas**: el modelo de infraestructura propuesto se ha diseñado de forma que los servicios contratados a externos sean mínimos. De hecho el único servicio que depende externamente es el servicio de Internet. Por otro lado, este control nos ofrece la posibilidad de cambiar, combinar y adaptar el diseño como queramos en función de las necesidades que nos vayamos encontrando.

- **Escalabilidad:** el diseño base es lo suficientemente versátil como para dar servicio a bastantes clientes para todo tipo servicios en la nube. Pero de todas formas, se ha diseñado con vistas a posibles actualizaciones y ampliaciones, tanto de hardware como software, teniendo en cuenta el mínimo impacto en el funcionamiento así como económicamente.

Por supuesto, también existen desventajas, estas son algunas las principales:

- **Precio**: los componentes que hemos seleccionado no son precisamente baratos, pero tampoco son caros para que una PYME pueda invertir parte de su presupuesto en ellos. El coste elevado de los productos también tiene su parte positiva en el gran rendimiento de los mismos. Aparte del coste de los dispositivos y del software, también tenemos que tener en cuenta el coste las líneas de Internet y sobre todo el coste relacionado con el consumo eléctrico.

- **Mantenimiento y gestión:** esta infraestructura requiere de un mantenimiento y supervisión de 24 horas. Aunque se pueden automatizar muchas de estas tareas de mantenimiento, siempre será necesaria la intervención de un administrador de sistemas. Por otro lado, cada vez que se ofrezca un nuevo servicio a un cliente, será necesario instalar y configurar toda la infraestructura virtual (*VDOM*) y de seguridad (anti SPAM, antivirus, almacén del correo, etc.)

2.3. Ámbito del proyecto

El TFG se ha desarrollado con un enfoque totalmente práctico, pensando en ofrecer una solución propia para gestionar todo tipo de servicios relacionados con un servicio basado en una infraestructura tipo nube. Por lo tanto podríamos definir el ámbito y la finalidad de este proyecto como una forma de convertir nuestra empresa en una especie de proveedor de servicios de Internet (conexión a Internet, espacio de almacenamiento, correo electrónico, aplicaciones, etc.) Este servicio se podría ofrecer tanto a clientes externos como a oficinas o filiales propias de la compañía:

1. Oficinas propias y oficinas de empresas filiales. En este caso, la configuración será independiente de la empresa matriz (como por ejemplo el correo electrónico, que tendrá su propio dominio) pero a su vez será necesaria una interconexión con algunos de sus servicios principales (por ejemplo para utilizar un *ERP*).

2. Clientes externos. En estos casos, es posible que sea responsabilidad o incluso sea parte de los servicios ofrecidos por nuestra empresa, gestionar los recursos de TI. En este caso, nuestra empresa actuaría exactamente como un proveedor de servicios de Internet y *cloud computing*, ofreciendo todas las soluciones de forma centralizada pero totalmente independiente (dominio propio, almacenamiento, etc.)

Un ejemplo práctico de la utilidad de esta configuración sería, por ejemplo, una empresa multinacional con diferentes oficinas, filiales y/o clientes alrededor del mundo a los que necesita ofrecerles todo tipo de servicios relacionados con TI. Esta empresa podría implementar esta solución en diferentes ubicaciones geográficas (por ejemplo, para gestionar las oficinas en diferentes países) o incluso una solución global centralizada (de esta forma la empresa tendría el control sobre el hardware y de esa forma adaptarse a cualquier cambio que necesite en futuro).

El diseño elegido para la implementación de este proyecto puede instalarse y configurarse en el centro de datos de cualquier empresa u organización, independientemente de su configuración actual.

2.4. Alternativas de diseño:

El diseño de este modelo de infraestructura intenta recopilar una serie de buenas prácticas a la hora de su implementación consultando los manuales de los distintos fabricantes así como todo tipo de documentación online. Por ejemplo, la red *SAN* es totalmente independiente del tráfico de red normal para no interferir en el rendimiento de la misma (este es un diseño clásico propio de cualquier red *SAN*). Las conexiones también se han implementado utilizando las opciones más óptimas posibles, por lo tanto, en lo referente al diseño básico de conexiones y red, las variantes se centran más en el tipo de conexión que vamos a implementar.

Podríamos utilizar conexiones tipo *Ethernet* en vez de *SAS* para conectar la *SAN* con los switches y cambiar algunas (o todas) a fibra óptica. En el diseño alternativo, se opta por conectar la *SAN* directamente a los switches en vez de a los servidores Hyper-V. Esta alternativa permite una mejor escalabilidad pero tiene impacto en la velocidad de acceso a las máquinas virtuales almacenadas en la *SAN*:

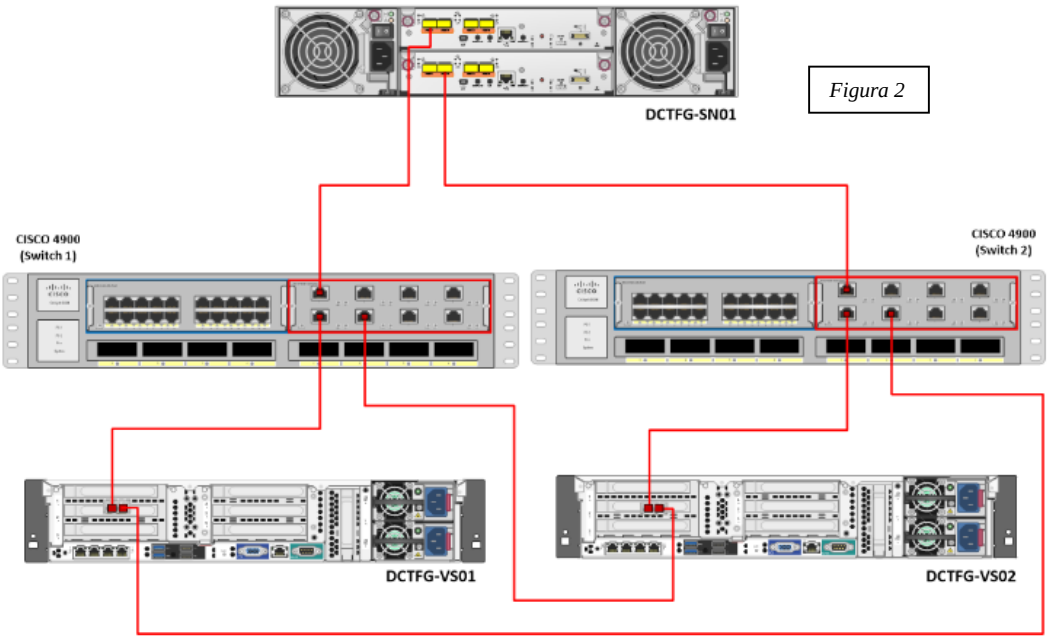


Figura 2

Existe otra posible variante de diseño es a la hora de elegir el sistema de virtualización (podríamos haber escogido por ejemplo *VMWare*, aunque sería algo más caro, ya que Hyper-V viene como parte integral de Windows Server 2012) o incluso el sistema operativo, ya que toda esta infraestructura se podría diseñar perfectamente utilizando Linux en vez de Windows.

Respecto a la copia de seguridad, también se podría haber optado por almacenar la información de backup en la nube, descartando la opción de volcado a cintas. También es posible, a costa de perder un nivel de seguridad, eliminar algunos de los servicios Fortigate y/o Barracuda. En este diseño alternativo de la *Figura 3*, podemos apreciar que se han eliminado los dispositivos de backup, así como servidor, la librería de cintas y el disco *NAS* Buffalo. Para sustituir el backup se ha optado por una solución combinada local y en la nube utilizando un dispositivo Barracuda Backup, el cual ofrece este tipo de solución dual.

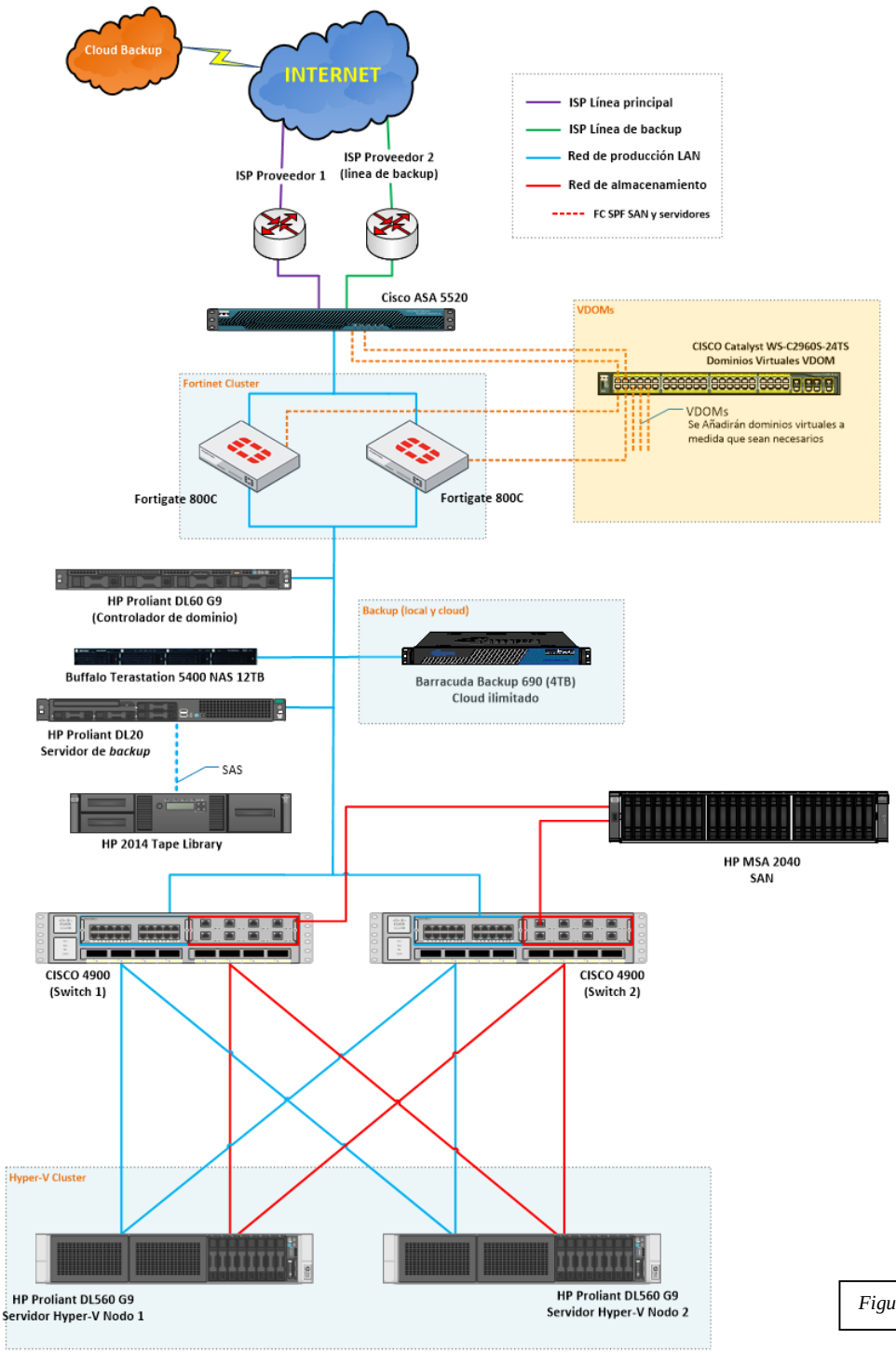


Figura 3

También se han eliminado los elementos Barracuda como el servidor anti SPAM, el *Archiver* de datos de correo y el *web proxy*. Toda esta tarea recaerá sobre los dispositivos Fortigate 800C, los cuales están diseñados, en principio, para soportar este tipo de configuración hasta cierta limitación de tráfico y usuarios. El archivo de correo se realizará mediante copias regulares de los buzones de los usuarios a la nube (esta opción es más barata pero menos versátil a la hora de recuperar información concreta sobre correos) utilizando la solución propuesta como software de backup.

3. Selección del Hardware:

3.1. Electrónica de red:

Firewall Cisco ASA 5520: la serie 55XX de CISCO es un clásico dentro de los cortafuegos tipo *core* (primera capa de seguridad) para cualquier organización. Existe abundante documentación sobre prácticamente cualquier tipo de configuración que necesitemos realizar, ya que la configuración se realiza desde sus sistema operativo CISCO IOS. El modelo 5520 seleccionado está descatalogado, pero se adapta perfectamente a los requerimientos de nuestro diseño (y además es posible conseguirlo aún a muy buen precio de mercado). Es escalable (10 dispositivos en clúster) y ofrece, aparte de las funciones típicas de un cortafuegos, opciones como alta disponibilidad (en una misma unidad) conectando dos *ISP* distintos para activar cualquiera de ellos en caso de corte de conexión. También posee un puerto de expansión donde podemos añadir tarjetas para ofrecer cualquier tipo de servicio que necesitemos implementar.

Figura 4

Fortigate 800C: para no sobrecargar cargar demasiado al cortafuegos CISCO y además para proteger y segmentar el tráfico generado por los clientes que estamos hospedando, este dispositivo de Fortinet realiza perfectamente dicha función ubicándose en la segunda capa de seguridad. De hecho su función principal será la creación de túneles *VPN* entre los servicios virtuales y las oficinas remotas. Son fáciles de configurar ya que utilizan el sistema operativo *FortiOS*, totalmente gestionable desde un navegador web. Además estos dispositivos se encargarán de analizar el tráfico de red en busca de malware o virus. Fortinet actualiza de forma casi permanente todos sus dispositivos para que estén protegidos ante cualquier eventualidad como ataques tipo *zero-day*. En el diseño propuesto se ha optado por la configuración en clúster de dos Fortigate 800C en alta disponibilidad.

Figura 5

Switches CISCO 4900m: este dispositivo es el núcleo de la configuración. Por este motivo se ha decidido por uno de los mejores del mercado. Una de sus mejores características de este switch es su modularidad, ya que es posible cambiar las interfaces de conexión y adaptarla a nuestras necesidades simplemente cambiando el frontal con el tipo de conectores que deseemos:

Figura 6

Para nuestra configuración, utilizaremos dos módulos, uno de 20 puertos Ethernet de 10/100/1000 y otro de 8 puertos tipo 10GBASE-T RJ-45, capaz de operar entre 1G/10G:

Figura 7

El módulo Ethernet de 10/100/1000 se utilizará para el tráfico de la red de producción *LAN* y el módulo10GBASE-T para la red de almacenamiento. Esta configuración será la inicial, pudiendo optar por opciones más rápidas en el futuro.

Switch CISCO SG200-8: este switch es el encargado de conectar los dispositivos Barracuda y proporcionar la opción de alta disponibilidad en caso de caída de uno de los servidores principales. Los dispositivos barracuda sólo tienen un puerto *LAN*. Este modelo con 8 puertos Gigabit es más que suficiente para conectar los dispositivos Barracuda o cualquier otro que necesite alta disponibilidad y no disponga de más de una tarjeta de red. Ofrece múltiples funciones como configuración de *VLAN*, *QoS*, etc., aunque su función se limitará a conectar estos dispositivos con los switches principales.

Figura 8

Cisco Catalyst WS-C2960S: este switch se encargará de definir y dar conectividad a los diferentes dominios virtuales que vayamos necesitan configurar en nuestro sistema (*VDOMs*). Tiene 48 puertos Ethernet con velocidades de Gigabit y además dos puertos *SFP* para velocidades de 10Gbs. Perfectamente gestionable para crear diferentes *VLANs* y también con opción con conexión de expansión para añadir otros switches en caso de necesitar más *VDOMs*.

Figura 9

Barracuda Web Filter 610: este dispositivo es ideal para gestionar todo el tráfico web, por lo tanto todos los usuarios tendrá que pasar a través de este dispositivo a la hora de navegar por Internet. Se configurará como proxy para todos los clientes de la implementación ya que permite hasta 2.000 usuarios concurrentes, más que suficiente para este inicio de la implementación. Además del filtrado web, puede ofrecer otros servicios como control de aplicaciones, eliminación de malware, syslog, monitor de Social Media, etc.

Figura 10

Barracuda Message Archiver 450: esta es una de las mejores soluciones en el mercado a la hora de conseguir una gestión absoluta sobre el correo que entra y sale de la organización. Es posible configurar varios dominios para gestionarlos de forma independiente y puede gestionar hasta 1000 usuarios. Tiene una configuración base de 4TB pero es totalmente escalable. Permite almacenar todos los correos ofreciendo servicios como exportación a PST, informes, opciones y filtros de búsqueda, etc.

Figura 11

Barracuda SPAM Firewall 300: como complemento al Message Archiver, este dispositivo se encargará de filtrar todos los correos de la organización y los ficheros que puedan contener, controlando

mensajes tipo SPAM o incluso con virus. También ofrece gestión por dominios y además permite hasta 5000 usuarios activos. La gestión de política de control es muy amplia, permitiendo bloquear correso utilizando varios criterios como palabras clave, patrones de URL, etc.

Figura 12

3.2. Electrónica de almacenamiento:

HP MSA 2040 (SAN): para el almacenamiento principal (máquinas virtuales sobre todo) se utilizará una SAN de HP modelo MSA 2040 SFF (para discos de 2.5 pulgadas, hasta un máximo de 24 hasta un máximo de 768TB). Para obtener el máximo rendimiento posible, utilizaremos la tecnología *Fibre Channel* de 8/16 Gb que viene integrada en este modelo.

Figura 13

HP MSL2024 Libería de cintas: para las copias de seguridad en cinta utilizaremos este modelo de HP el cual permite todo tipo de cintas *LTO* hasta el último modelo *LTO-6* (2,5TB sin comprimir) con una tasa de transferencia que puede variar ente los 54MB/s hasta los 160MB/s. Además tiene conexiones tipo SAS y FC. Los dos *magazines* tienen capacidad para 24 cintas.

Figura 14

Buffalo Terastation 5400r: como apoyo a las copias de seguridad, se utilizará este modelo *NAS* el cual tiene una capacidad de 12TB, permite cambio de discos en caliente, pero además tiene también un gran rendimiento al llevar un procesador Atom D2700 dual core y 2GB de RAM. En caso de necesitar más espacio, este dispositivo es perfectamente escalable.

Figura 15

3.3. Servidores:

HP Proliant DL560 G9: estos servidores serán el pilar fundamental de la infraestructura. Al gestionar todas las máquinas virtuales, su configuración debe de ser máxima y óptima en rendimiento. Se ha optado por un microprocesador Xeon E5 4640v3 con una frecuencia de 1.9GHz y 12 cores, con 16GB de RAM tipo DDR4 a 2133MHz. Para el almacenamiento, se ha elegido una configuración de 4 discos de 1TB en RAID 1. Cambiaremos la configuración base de las tarjetas de red por 2 tarjetas de 1GbE y 2 tarjetas 10GbE por defecto.

Figura 16

HP Proliant DL60 G9: para la gestión de la infraestructura, como por ejemplo el Directorio Activo, DNS, *DHCP*, etc utilizaremos un servidor Gen 9 con un procesador Xeon E5 2600v4 con 8GB de memoria RAM de base. No necesitamos demasiada potencia en este sevidor ya que las tareas que va a realizar no necesitan de demasiado proceso de cálculo. Finalmente, para almacenamiento, instalaremos 4 discos de 1TB en *RAID 1*, ya que este servidor también centralizará las tareas de actualización de los sistemas operativos Windows del entorno (*WSUS*),

Figura 17

HP Proliant DL20 G9: todo el sistema de copia de seguridad estará centralizado en este servidor con un Pentium i3 E3-1200v5 y 8GB de memoria RAM. Al igual que el otro modelo, con dos discos de 1TB será suficiente para el sistema operativo y las aplicaciones que necesitemos para las copias de seguridad.

Figura 18

3.4. Tarjetas y cables:

HP Ethernet 10Gb 2-port 530T: esta tarjeta de 10Gb se instalará en el servidor de backup para conectarlo a la red de almacenamiento. De esta forma tendremos más velocidad de acceso los datos ubicados en la *SAN* y por otro lado no afectaremos al tráfico en la red principal *LAN*.

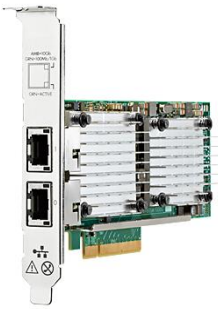


Figura 19

HP 82E 8GB 2-port PCIe Fibre Channel Host Adapter: necesitaremos dos de estas tarjetas para instalarlas en los dos servidores Hyper-V. En ellas conectaremos a su vez los dos módulos de la *SAN*.

Figura 20

Módulo CISCO SSM-4GE para Firewall ASA 5520: esta tarjeta de expansión nos permitirá conectar a Internet los dominios virtuales (*VDOM*) creados en los dispositivos Fortigate y aún tendremos 4 conexiones *SPF* extras para futuras ampliaciones:

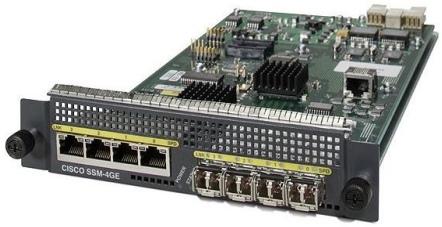


Figura 21

Tarjeta PCIe 3.0 SAS para servidor de backup y cable: el servidor de copias de seguridad se conectará directamente a la librería de cintas para obtener el máximo rendimiento y velocidad a la hora de comunicarse con la misma. Para ello será necesario adquirir una tarjeta con el interface *SAS* (no viene por defecto en los servidores). Este modelo HP H221 encaga perfectamente en nuestra configuración.

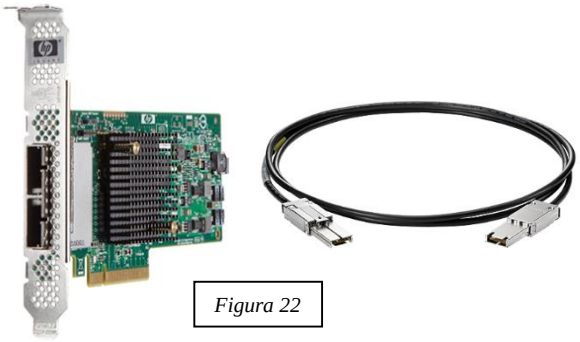


Figura 22

Cables CAT 6: aunque podríamos optar por cable CAT 7, el cable de CAT 6 es la opción más barata y nos sirve perfectamente para el diseño propuesto, ya que permite hasta 10Gbps de velocidad de red. La ventaja principal del cable CAT 7 es la durabilidad y la capacidad de soportar futuras nuevas velocidades. Es una buena práctica para este tipo de instalaciones, elegir diferentes colores para diferenciar de forma visual las funciones de cada cable, por ejemplo, las conexiones de seguridad en color rojo, ILO azul, red de datos cable blanco, etc.

Figura 23

4. Selección del Software:

4.1. Sistema operativo y correo electrónico

4.1.1. Windows Server 2012 R2 Standard

Esta será la versión del sistema operativo de Microsoft que se ejecutará en todos los servidores de la infraestructura. La versión *Standard* es suficiente para el diseño propuesto y además incluye la virtualización Hyper-V (permite hasta dos máquinas virtuales con *Windows Server 2012 R2*) y directorio activo. Para la compra y gestión de licencias, tanto de los sistemas operativos como de las *CAL*, es aconsejable abrir una cuenta con *Microsoft Volume Licensing*, de esta forma obtendremos descuentos y también tendremos acceso a la web de gestión de licencias que podremos incluso dividir por cliente u oficinas. Estas *CALs* irán variando en función de los diferentes clientes y servicios que vayamos añadiendo a nuestro diseño. Un factor importante a la hora de definir las licencias es que se tienen que definir por usuario, no por dispositivo.

4.1.2. Microsoft Exchange 2013

Última versión de unos de los más famosos gestores de correo electrónico con nuevas características que hacen perfecta su integración con el sistema operativo *Windows Server 2012 R2*, como por ejemplo *OWA offline* y buzones de hasta 100GB.

4.2. Copia de seguridad

4.2.1. Symantec Backup Exec 2015

Permite la unificación de todo el proceso de backup en una sola consola de administración, tanto para la copia virtual como la física, simplificando el entorno. Se adapta perfectamente con Windows Server ya que permite la integración con *Microsoft Volume Shadow Copy Service (VSS).* Esta nueva versión 2015 también incluye la opción de deduplicación de datos. Las licencias necesarias se encuentran descritas en el *Capítulo 12.4*.

4.3. Solución Antivirus

4.3.1. Microsoft Forefront

Al ser un producto gratuito incluido en los sistemas operativos Windows, es una opción a tener en cuenta.

4.3.2. Kaspersky Endpoint Security for Bussines (Select)

Kaspersky es uno de los líderes en el mercado de soluciones antivirus. Esta versión es escalable y posee una consola centralizada de control para todos los clientes incluyendo despliegue remoto. Incluye antimalware para estaciones de trabajo (clientes), dispositivos móviles, aplicaciones web y sobre todo para servidores de archivos.

5. Interconexión de los dispositivos:

5.1. Conexiones switches

5.1.1. Conexiones Ethernet

Los switches CISCO 4900 tendrán dos módulos, como ya hemos comentado anteriormente, uno de 20 puertos Ethernet de 10/100/1000 (recuadro azul en la *Figura 24*) y otro de 8 puertos tipo 10GBASE-T RJ-45 (recuadro rojo, *Figura 24*):

Figura 24

En los puertos Ethernet de 10/100/1000 conectaremos todos los dispositivos de la red excepto la *SAN*. Para poder obtener las ventajas de velocidades Gigabit, utilizaremos cables Categoría 6 (CAT 6). Los puertos 10GBASE-T los utilizaremos exclusivamente para conectar los servidores Hyper-V con los volúmenes de la *SAN* donde se encuentran las máquinas virtuales, en los dos puertos 10GbE que traen de base. El tipo de cableado que utilizaremos será CAT 6 ó CAT 7. En principio, esta configuración es suficiente para comenzar a dar un servicio a la máxima velocidad posible. En un futuro podríamos instalar módulos *FC* si fuera necesario.

Dispositivos conectados a la red de producción LAN:

- Clúster Fortigate
- CISCO SG200-8: dispositivos Barracuda
- Servidores

El switch CISCO SG200 de 8 puertos tendrá tres conexiones de los dispositivos Barracuda y dos *trunk* conectadas una a cada switch CISCO 4900. La función de este switch es proporcionar conexión de los dispositivos Barracuda en caso de activación del segundo switch. En la *Figura 25* se detallan las conexiones Ethernet de la red de producción *LAN* (se ha eliminado el puerto 10GBASE-T de los switches para ofrecer más claridad en las conexiones):

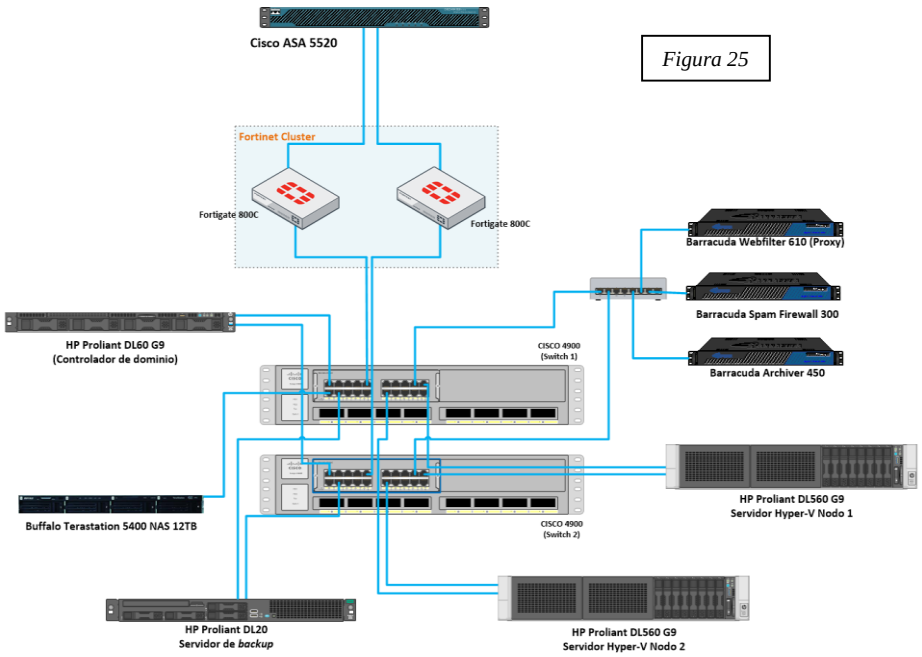


Figura 25

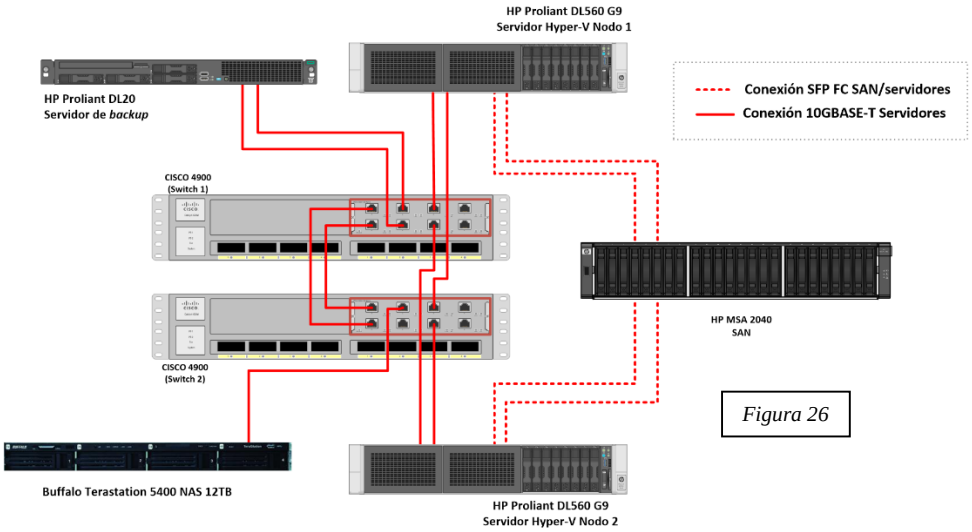


Figura 26

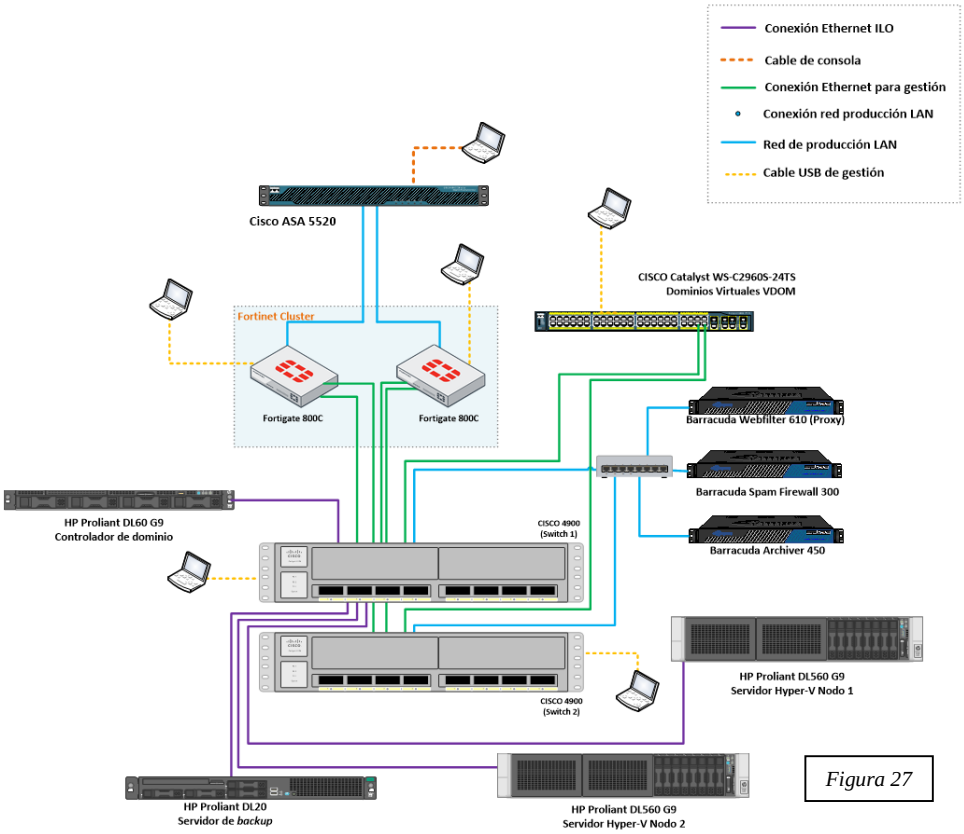


Figura 27

5.1.2. Alta disponibilidad

Los switches CISCO 4900 se conectarán entre sí a través de dos puertos de 10GbE en modo *Etherchannel* a una VLAN distinta a la VLAN de la red de datos, tal y como se puede apreciar en la *Figura 28*:

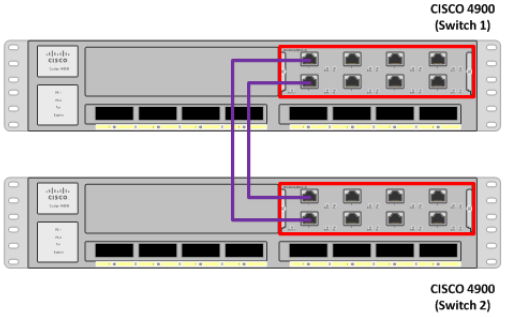


Figura 28

Existen muchos métodos para configurar la redundancia para switches CISCO. La idea es combinar el *teaming* de las *NIC* con la conexión *Etherchannel* [1] y de esa forma obtener además de alta disponibilidad, balanceo de carga y además un buen rendimiento.

5.2. SAN y servidores

Como se puede observar en la *Figura 26* del apartado anterior, la *SAN* estará conectada directamente a los servidores Hyper-V utilizando conexiones 10GbE y *SFP*. Como la única información que tendrá almacenada la *SAN* será en principio las máquinas virtuales, esta configuración es óptima en rendimiento y velocidad.

5.3. Conexión *SAS* entre el servidor de *backup* y la librería de cintas

El volcado de la información para realizar la copia de seguridad en cintas, tiene que tener la máxima velocidad posible para optimizar al máximo los tiempos de copia. Para conseguirlo instalaremos una tarjeta H241 de HP en el servidor de backup y lo conectaremos a la librería de cintas mediante un cable *SAS*.

5.4. Resto de servidores y conexiones de gestión

El resto de conexiones entre los dispositivos se realizarán a través de la red de producción *LAN* a las tarjetas de red o a los puertos de gestión (como la *ILO* de los servidores).

Dispositivo	Tipo de puerto	Tipo de interfaz	Tipo de cable
CISCO ASA 5520	• Puerto de consola • Puerto Ethernet	• Línea de comandos (CISCO IOS)	• Cable de consola RJ45 to DB9 • Cable Ethernet
Fortigate 800C	• USB • Puerto de consola • 2 Puertos Ethernet	• Línea de comandos • Web	• Cable de consola RJ45 a DB9 • Cable Ethernet
Barracuda	• Puerto Ethernet	• Web	• Cable Ethernet
CISCO SG200-8	• Puerto Ethernet	• Línea de comandos (CISCO IOS)	• Cable Ethernet
CISCO Catalyst WS-CS2960s-24TS	• Puerto Ethernet • Puerto de consola	• Línea de comandos (CISCO IOS)	• Cable Ethernet • Cable de consola RJ45 a DB9
Servidores	• ILO	• Web	• Cable Ethernet
CISCO 4900	• Puerto de consola • Puerto Ethernet	• Línea de comandos (CISCO IOS)	• Cable de consola RJ45 to DB9 • Cable Ethernet
SAN HP MSA 2040	• Puerto Ethernet	• Web	• Cable Ethernet

5.5. Conexiones de alimentación eléctrica

Los dispositivos críticos como la SAN, servidores y switches principales (CISCO 4900) deben de tener doble fuente de alimentación. De ese modo en caso de fallo de suministro eléctrico, la otra fuente entrará de forma automática en funcionamiento. Por lo tanto es importante añadir estas características a dichos dispositivos a la hora de comprarlos o pedir ofertas.

Figura 29

6. Configuración de los dispositivos de red:

6.1. Definición de IPs y subredes

En la tabla siguiente se muestran todos los dispositivos conectados a la red con un ejemplo de direcciones IP, nombre de *host* y el tipo de tarjeta al que se conectan:

Nota: *máscara de subred para todas las ip 255.255.255.0 (/24)*

Dispositivo	Nombre	IP	Tarjeta	Función
Cisco ASA 5520	DCTFG-FW01	10.1.1.1	NIC 1	Conexión Proveedor 1
		10.1.1.2	NIC 2	Conexión Proveedor 2
		10.1.1.3	NIC 3	Conexión Fortigate 1
		10.1.1.4	NIC 4	Conexión Fortigate 2
		10.1.1.100	NIC MGT	Puerto Ethernet de gestión
Fortigate 800D	DCTFG-FG01	10.1.1.5	NIC 1	Seguridad
Fortigate 800D	DCTFG-FG02	10.1.1.6	NIC 1	Seguridad
CISCO 4900m	DCTFG-SW01	10.1.1.10	NIC 1	Switch Core 1
CISCO 4900m	DCTFG-SW02	10.1.1.11	NIC 1	Switch Core 2
CISCO SG200	DCTFG-SW03	10.1.1.12	NIC 1	Switch Barracudas
CISCO Catalyst	DCTFG-SW04	10.1.1.13	NIC 1	Switch VDOMs
		10.1.1.14	NIC 2	
Barracuda Webfilter	DCTFG-BA01	10.1.1.17	NIC 1	Webfilter 610 (proxy)
Barracuda Spam FW	DCTFG-BA02	10.1.1.18	NIC 1	Anti Spam
Barracuda Archiver	DCTFG-BA03	10.1.1.19	NIC 1	Almacén de correo electrónico
HP Proliant DL60 G9	DCTFG-DC01	10.1.1.20	NIC 1	Modo "*teaming*", NIC 1 conectada DCTFG-SW01 y NIC2 a DCTFG-SW02 a red de producción
			NIC 2	
		10.1.1.60	ILO	Gestión del servidor
HP Proliant DL20	DCTFG-BCK01	10.1.1.21	NIC 1	Modo "teaming", NIC 1 conectada DCTFG-SW01 y NIC2 a DCTFG-SW02 a red LAN de producción
			NIC 2	
		172.1.10.2	NIC 3	Modo "teaming", NIC 3 conectada DCTFG-SW01 y NIC4 a DCTFG-SW02 a red de datos
			NIC 4	
		10.1.1.61	ILO	Gestión del servidor
HP Proliant DL560	DCTFG-VS01	10.1.1.42	NIC 1	Conexión red de datos (Internet)
		10.1.1.201	NIC 2	IP conexión clúster Hyper-V
		10.1.1.22	NIC 3	Modo "teaming", NIC 3 conectada DCTFG-SW01 y NIC4 a DCTFG-SW02 a red LAN de producción
			NIC 4	
		172.1.1.10	SFP 1	"Teaming" iSCSI 10Gb SFP1 conexión SAN DCTFG-SW01 y SFP2 a DCTFG-SW02 a red de datos
		172.1.1.20	SFP 2	
		10.1.1.62	ILO	Gestión del servidor
HP Proliant DL560	DCTFG-VS01	10.1.1.43	NIC 1	Conexión red de datos (Internet)
		10.1.1.202	NIC 2	IP conexión clúster Hyper-V
		10.1.1.23	NIC 3	Modo "teaming", NIC 3 conectada DCTFG-SW01 y NIC4 a DCTFG-SW02 a red LAN de producción
			NIC 4	
		172.1.1.30	SFP 1	Modo "teaming", NIC 3 conectada DCTFG-SW01 y NIC4 a DCTFG-SW02 a red LAN de producción
			SFP 2	
		10.1.1.63	ILO	Gestión del servidor
Clúster Hyper-V	DCTFG-CLUSTER01	10.1.1.200	MNGT	IP de gestión del clúster
HP 2014	DCTFG-TP01	10.1.1.70	NIC 1	Librería de cintas
SAN	DCTFG-SN01	172.1.1.80	NIC 1	SAN
		172.1.1.90	NIC 2	
Buffalo Terastation	DCTFG-NS01	10.1.1.71	NIC 1	*NAS* de 12TB

6.2. Configuración básica del firewall CISCO ASA

Los dispositivos CISCO se configuración de base a través del cable de consola:

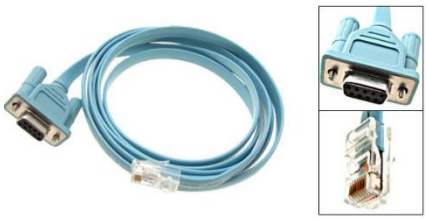


Figura 30

También conectaremos a su vez un cable Ethernet desde el ordenador desde el cual estamos haciendo la configuración con el puerto Ethernet de gestión del firewall:

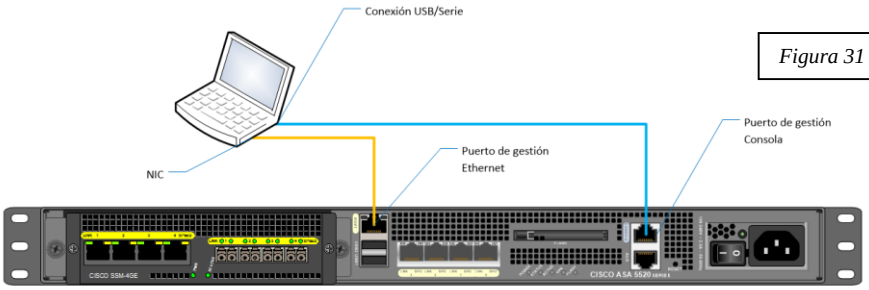


Figura 31

Una vez conectado el puerto al ordenador con el cual vamos a proceder con la configuración, será necesario utilizar un programa de emulación de terminal. Existen varias opciones gratuitas en Internet, pero uno de los más utilizados es *putty* [2]. Los parámetros básicos son 9600 bits por segundo, 8 bits de datos, sin paridad, 1 bit de parada sin control de flujo.

Por defecto, esta es la configuración de fábrica de las interfaces:

Interface	Name	Security Level	IP Address	State
GigabitEthernet0/0 GigabitEthernet0/1 GigabitEthernet0/2 GigabitEthernet0/3	no nameif	no security-level	no ip address	Shutdown
Management0/0	management	100	192.168.1.1	Management-only

Figura 32

Una vez hemos accedido por consola, el primer paso es configurar la interface Ethernet de gestión para poder acceder por red y asignarle la nueva IP 10.1.1.10, por ejemplo podríamos utilizar los siguientes comandos:

```
interface Management0/0
speed 100
duplex full
nameif inside
security-level 100
ip address 10.1.1.100 255.255.255.0
```

El siguiente paso es asignar el nombre de host DCTFG-FW01[3]. Luego procederemos a actualizar *Cisco IOS* [4]. Para ello tendremos que descargar el último fichero *.bin*.

Para comunicar el firewall con Internet, tenemos que configurar la ruta estática básica mediante *NAT*. De esta forma se creará un puente entre las interfaces interiores y las exteriores. En este punto tenemos que detallar las conexiones Ethernet en la siguiente figura:

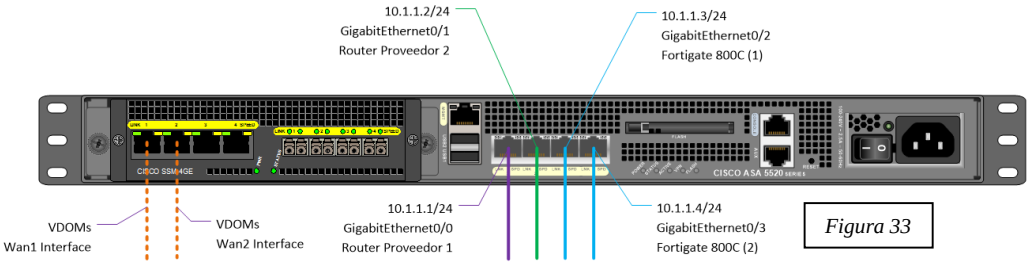


Figura 33

A continuación se muestra una posible configuración [5] de las tarjetas para habilitar el tráfico entre el firewall y los proveedores de Internet (vamos a considerar que la IP pública del *Proveedor 1* es 84.120.125.60 y *Proveedor 2* es 202.125.30.45):

```
DCTFG-FW01# interface GigabitEthernet0/0
DCTFG-FW01# speed 100
DCTFG-FW01# duplex full
DCTFG-FW01# nameif outside
DCTFG-FW01# security-level 0
DCTFG-FW01# ip address 84.120.125.60 255.255.255.240

DCTFG-FW01# interface GigabitEthernet0/1
DCTFG-FW01# speed 100
DCTFG-FW01# duplex full
DCTFG-FW01# nameif outside
DCTFG-FW01# security-level 0
DCTFG-FW01# ip address 202.125.30.45 255.255.255.240
```

Por otro lado habría que habilitar el tráfico desde la red de producción y de esta forma gestionar las posibles oficinas o clientes futuros, los cuales estarán en otra subred diferente. Para ello utilizaremos el comando CISCO "*access-list*" [6] y esta podría ser la configuración que habilita el acceso desde la red de producción 10.1.1.*X* a las redes de los clientes (por ejemplo, 10.10.10.*X*, 10.10.20.*X* y 10.10.30.*X*):

```
access-list 101 extended permit IP 10.1.1.0 255.255.255.0 10.10.10.0 255.255.255.0
access-list 101 extended permit IP 10.1.1.0 255.255.255.0 10.20.10.0 255.255.255.0
access-list 101 extended permit IP 10.1.1.0 255.255.255.0 10.30.10.0 255.255.255.0
```

Para configurar la redundancia para los ISP en caso de fallo de uno de ellos, por la extensión de la configuración, nos remitiremos a la página oficial de CISCO donde se explica el proceso en detalle [40].

6.3. Switches CISCO 4900, actualización Firmware y definición de las VLANS

Al igual que realizamos con el firewall, conectaremos los switches a un ordenador para su configuración inicial utilizando los puertos de consola:

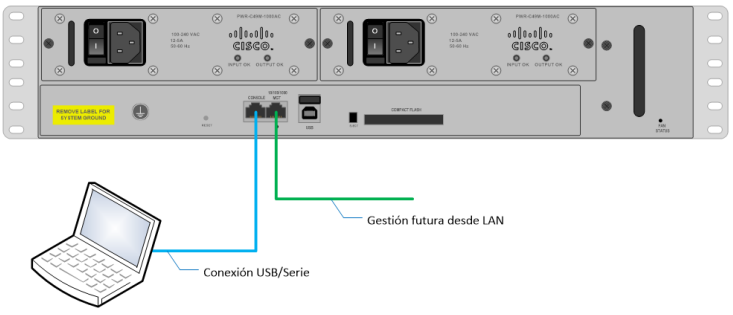


Figura 34

Una vez actualizado el firmware a la última versión al igual que hicimos con el Firewall CISCO ASA 5520, cambiaremos la contraseña de administrador, le asignaremos el nombre de host correspondiente (DCTFG-SW01 y DCTFG-SW02) y procederemos a configurar las dos *VLAN* principales [7], VLAN1 Red de Producción y VLAN2 Red de Datos:

```
DCTFG-SW01# configure terminal
DCTFG-SW01 (config)# vlan 1
DCTFG-SW01 (config-vlan)# state active
```

El siguiente paso sería añadir los puertos a las *VLAN*. Tenemos que distinguir entre los dos interfaces que tenemos actualmente instalados:

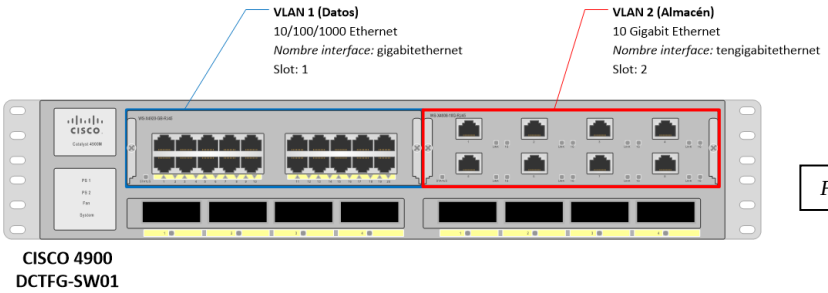


Figura 35

Para ver los interfaces instalados en el switch podríamos ejecutar el comando:

```
DCTFG-SW01# show interfaces
```

Una vez identificados continuamos la configuración de la *VLAN1* añadiendo los puertos necesarios, de la siguiente manera [7]:

```
DCTFG-SW01# configure terminal
DCTFG-SW01 (config)# interface gigabitethernet 1/1
DCTFG-SW01 (config-if)# switchport access vlan 1
```

De esta forma iremos configurando los puertos que vamos a necesitar para *VLAN*. Para el módulo 10 Gigabit Ethernet el proceso es exactamente el mismo pero cambiando la denominación del interface y el slot en el cual está conectado:

```
DCTFG-SW01 (config)# interface tengigabitethernet 2/1
```

El proceso para configurar el segundo switch, DCTFG-SW02 es exactamente el mismo que el descrito para el DCTFG-SW01. Una vez terminado el proceso de asignación de puertos a las diferentes VLAN ya tendremos divididos los switches en dos redes independientes.

6.4. Switch CISCO Catalyst WS-C2960G-48TS para los dominios virtuales VDOM.

Este switch será el encargado de dar salida a Internet a los diferentes dominios virtuales que iremos configurando en los dispositivos Fortigate. Para ello iremos creando diferentes *VLAN* en función de los nuevos *VDOM (Dominios Virtuales)* que vayamos necesitando. Las conexiones en este switch cuyo nombre de host es DCTFG-SW04 podrían ser similares a las mostradas en la *Figura 36*:

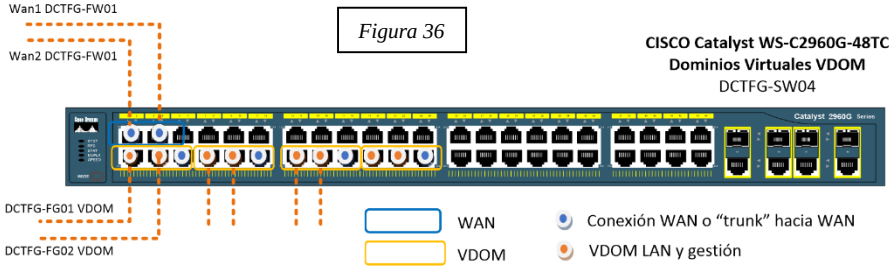


Figura 36

Según este esquema, tendremos que crear una *VLAN* por cada *VDOM* que necesitemos, los cuales constarán de 3 puertos, un puerto para el tráfico de red, otro para la gestión y el último para hacer *trunk* con la conexión *WAN* la cual redirigirá el tráfico hacia Internet. la configuración inicial de este dispositivo se realizará de forma distinta a los otros dispositivos CISCO. Para hacerlo de la manera más sencilla y rápida aplicaremos la configuración llamada "*Express Setup*". Pasos a realizar [8]:

1. Comprobar que no hay dispositivos conectados, ya que en esta configuración el switch actuará como un servidor *DHCP*.
2. Lo conectamos a la corriente eléctrica y espearmos el final del test inicial *POST*.
3. El *LED SYST* estará activado parpadeando en verde cuando termine el arranque.
4. Mantenemos pulsado el botón "Mode" durante tres segundo. Cuando todos los *LEDs* se enciendan en verde podemos soltarlo.
5. Conectamos un ordenador con un cable cruzado a cualquier puerto del switch.
6. Desde un navegador, abriremos la dirección IP 10.0.0.1 y desde allí podremos configurar los parámetros básicos del switch.

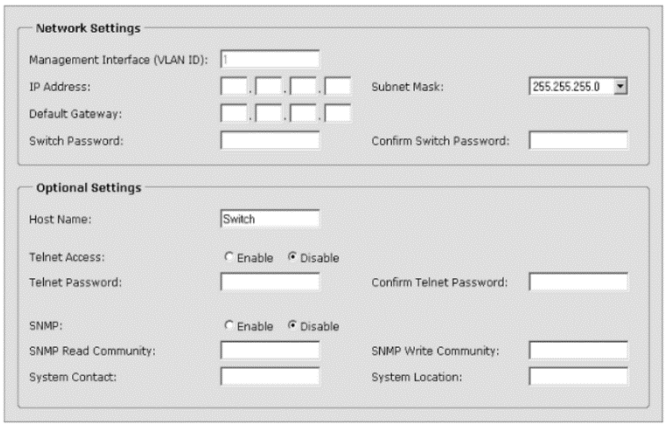


Figura 37

Una configurado el acceso *telnet* podremos acceder y comenzar a configurar las VLAN utilizando los comandos CISCO IOS. Dichos comandos de configuración son los mismos que los utilizados para el resto de switches CISCO.

6.5. Configuración de los dispositivos Fortigate C800.

Antes de comenzar con la configuración procederemos al primer acceso a los dispositivos para cambiar la contraseña del usuario administrador. Como hemos definido antes, las IP son 10.10.1.5 y 10.10.1.6. Accederemos desde un explorador y cambiaremos las contraseñas por defecto por las nuevas.

6.5.1. *VDOMs*

Un *VDOM* nos permite crear diferentes configuraciones de dominio dentro de un mismo Fortigate. De esta forma lograremos tener redes separadas las cuales se pueden definir con diferentes niveles de seguridad. En nuestro caso la configuración de los *VDOM* es totalmente necesario, ya que tendremos que definir un *VDOM* por cliente u oficina que esté integrada en nuestra infraestructura. No sólo tendremos la posibilidad de recrear diferentes entornos, sino que además tendremos la posiblidad de crear usuarios administradores de red que puedan dar soporte o gestión sólo a los dominios que estén autorizados.

El primer paso [9] es habilitar la opción de *VDOM* desde la *GUI* del dispositivo 10.10.1.5 el cual será nuestro nodo maestro accediendo a la siguiente opción localizada en *System* > *Dashsboard* > *System Information* > *Virtual Domain* (localizado en los widgets):

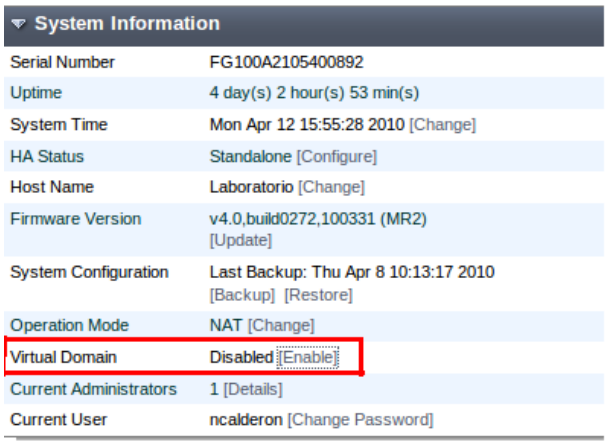


Figura 38

No será necesario crear un *VDOM* para la red principal, ya que esta corresponderá a la red de gestión de nuestra infraestructura y tendrá su propio dominio físico. En cambio sí tenemos que asignar los diferentes *VDOM* para las oficinas o clientes que vamos a gestionar. Una posible asignación de presentes y futuros *VDOM* podría ser la siguiente:

Nombre VDOM	IP	Descripción
Cliente1	10.10.10.X	Cliente, rango IP principal
Cliente2	10.10.20.X	Futura oficina remota administración
Oficina1	10.10.100.X	Futuro cliente remoto

Una vez activada la opción de VDOM procederemos a crearlos desde la opción *System >> VDOM >> Create New*

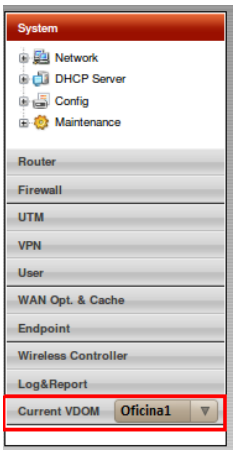


Figura 39

Asignaremos el nombre y de esa forma podremos ver la descripción del nuevo *VDOM*. Una vez creados los *VDOM* y asignado las diferentes características de cada uno, tendremos la opción de administrarlos de forma separada. Aunque cada *VDOM* tiene su configuración propia, tenemos que tener en cuenta que hay opciones que se configurarán de forma global y otras de forma individual por dominio (Figura 39).

El siguiente paso [9][10] es asignar el interface por el cual funcionará cada *VDOM*. Esto es importante ya que cada interface puede pertenecer sólo a uno. Accederemos desde "*Global > Network > Interfaces"*:

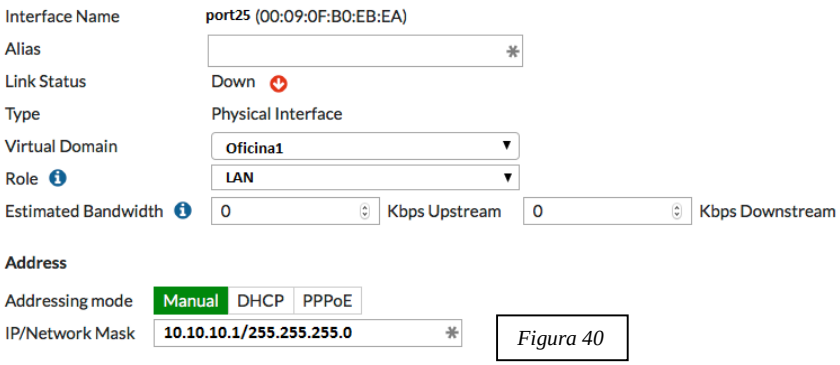


Figura 40

En este ejemplo se ha definido la red para la *Oficina1* para la cual hemos asignado el rango IP: 10.10.10.X / 255.255.255.0 al puerto/interface llamado "*port25*". Esta sería la asignación para la red de trabajo del dominio virtual. El paso siguiente es asignar el acceso de

administración desde donde activaremos entre otros, el servicio *DHCP*. Para ello crearemos editaremos la interface "*port26*" para añadirla al *VDOM* Oficina1. Desde aquí configuraremos servicios como por ejemplo *DHCP*:

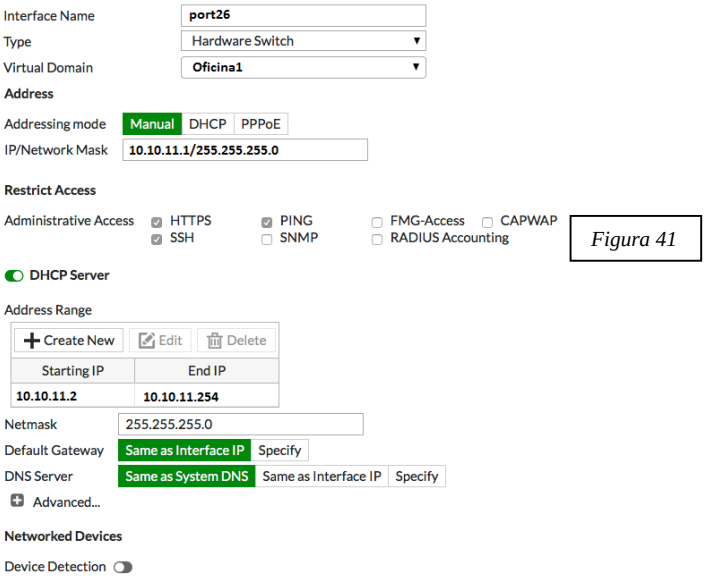


Figura 41

Una vez tengamos definidos los diferentes dominios virtuales, tendremos que asignar los usuarios administradores del mismo, si es necesario. Para ello accederemos desde *Global >> Admin >> Administrators*:

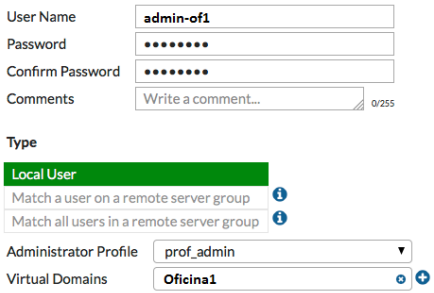


Figura 42

Para cada *VDOM* hay que asignar una configuración básica para todos elementos que la componen. La principal será la configuración que indique por defecto la ruta para acceder a Internet. En los Fortigate, este puerto se denomina "*wan1*". Por lo tanto seleccionamos el interface "*wan1*" y asignamos los *VDOM* a dicha Interface, por ejemplo:

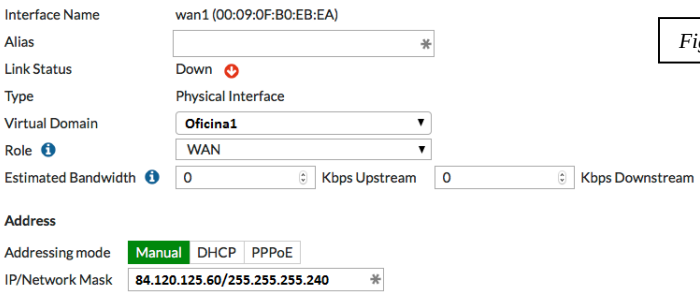


Figura 43

Después asignaremos la puerta de enlace y el interface de conexión. Las opciones se encuentran en *Virtual Domains > Oficina1 > System > Network > Routing*. Luego pulsamos en "*Create New*" para configurar la ruta por defecto:

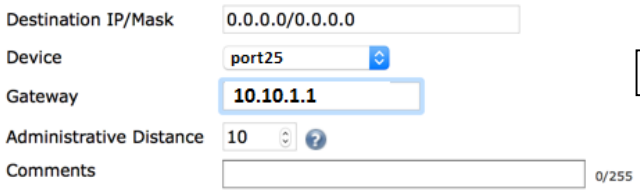


Figura 44

Repetiremos estos pasos para ir creando los diferentes dominios virtuales que necesitamos dar de alta en nuestra infraestructura.

6.5.2. Alta disponibilidad

La configuración de los Fortigate será en alta disponibilidad. Para lograr la mayor eficiencia en esta configuración es necesario que ambos dispositivos tengan exactamente las siguientes características:

1. Misma configuración de hardware (mismo disco duro y tarjeta *AMC*)
2. Misma versión de firmware
3. Las unidades tienen que estar configuradas en el mismo modo, ya sea *NAT* o transparente.
4. Mismo modo *VDOM* (Dominios Virtuales) y misma configuración.

Una vez hayamos confirmado que ambos dispositivos tienen la misma configuración, procederemos a configurar el protocolo *FGCP* (*Fortigate Cluster Protocol*) el cual nos ofrecerá mejor rendimiento, balanceo de carga y protección contra fallo de uno de los nodos (activando el segundo de forma transparente y automática). El siguiente esquema muestra la configuración general y en nuestro caso, "*external switch*" corresponde con el cortafuegos:

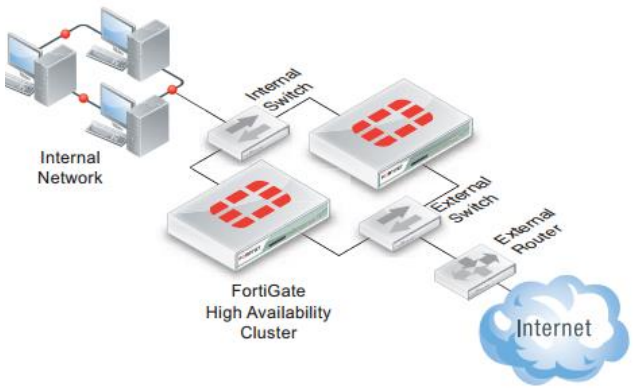


Figura 45

Una vez activado *FGCP* [11] las dos unidades comparten estado y configuración. Si una unidad falla, la otra unidad automáticamente reemplaza a dicha unidad defectuosa tomando el control y continuando con el servicio. En este tipo de configuraciones se designa una unidad como primaria llamada unidad maestra y otra llamada unidad subordinada. También podemos configurar balanceo de carga si fuera necesario para aumentar el rendimiento del sistema. El clúster configurado aparecerá como una sola unidad, por lo tanto trabajaremos configurando la unidad designada como "maestra".

Después de un cambio de unidad en caso de fallos las sesiones que se mantendrán son *TCP*, *SIP* y sesiones *VPN IPsec*. En cambio no se mantendrán las sesiones abiertas *UDP*, multicast, *ICMP* o sesiones *VPN SSL*. Esto no es un serio problema ya que este tipo de sesiones se suelen recuperar de forma automática.

El paso inicial es conectarlos físicamente para ofrecer alta disponibilidad [12]. Para ello conectaremos los interfaces llamados *HA* (*HeartBeat Interfaces*) de la siguiente manera:

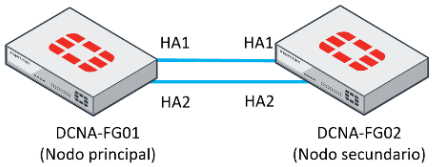


Figura 46

Luego procederemos a definir [11] el clúster utilizando el *widget* "*System Information*":

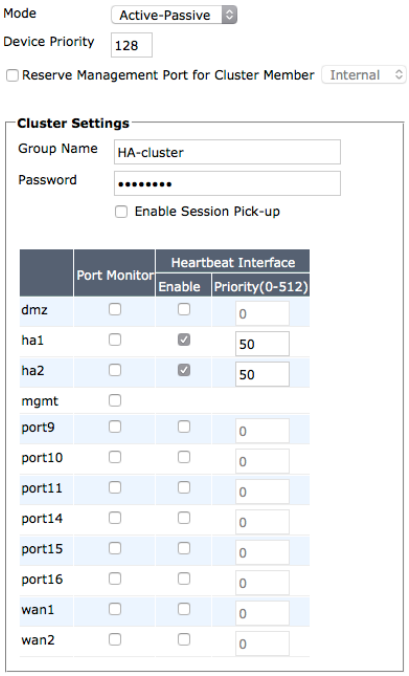


Figura 47

Asignamos un nombre para el clúster y activaremos el modo activo-pasivo ("*Active-Passive*") y pondremos el valor 50 en los campos de prioridad de ambas tarjetas *HA*. Este paso se repetirá exactamente igual en el Fortigate que servirá de backup. De esta forma ya tendremos configurado el sistema para alta disponibilidad en caso de fallo del nodo principal.

6.5. Configuración de los dispositivos Barracuda.

6.5.1. Barracuda Web Filter

El dispositivo *Barracuda Web Filter* es uno de los más importantes de nuestra configuración, ya que se encargará de hacer las funciones de ***proxy*** para dar salida a Internet a los diferentes clientes u oficinas. En él podremos definir los diferentes niveles de acceso para cada uno de los dominios y de esa forma establecer criterios para bloquear o habilitar páginas web a los usuarios del directorio activo.

6.5.1.1 Configuración básica

El paso inicial [13] es conectar el dispositivo Barracuda al switch DCTFG-SW03 de la siguiente forma:

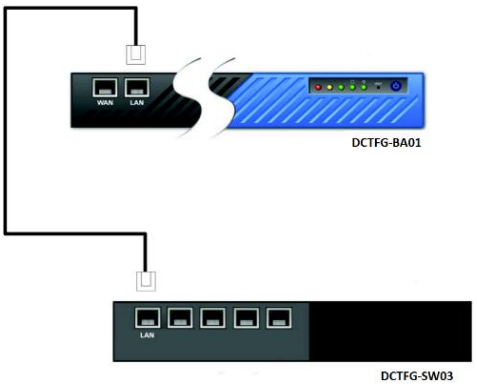


Figura 48

Luego, para realizar la configuración básica es necesario conectar un teclado, un ratón y un monitor directamente al dispositivo Barracuda (hay otra forma por la cual podremos asignar una dirección IP de forma automática pulsando el botón RESET). Accederemos con las credenciales por defecto:

Login: admin
Password: admin

Configuraremos la dirección IP (10.1.1.13), máscara de subred, *gateway* y las *DNS*. En el firewall DCNA-FW01, tendremos que abrir los siguientes puertos:

Port	Dirección	TCP	UDP	Utilización
22	Salida	Si	No	Soporte técnico Barracuda
25	Entrada/Salida	Si	No	Email
53	Salida	Si	Si	DNS
80	Salida	Si	No	Actualizaciones
123	Salida	No	Si	NTP

Luego cambiaremos el nombre del host por DCTFG-BA01 y también lo añadiremos al dominio principal DCTFG. Activaremos el Barracuda Web Filter en modo "*Audit*", luego lo cambiaremos a "*Active*".

Actualizaremos el Firmware a la última versión (para poder realizar este paso es necesario tener una subscripción *Energiner Updates*. Luego cambiaremos la contraseña de administrador en *Basic* > *Administration*.

Es importante decidir la forma en la cual vamos a conectar el dispositivo a nuestra red. En mi caso he decidido conectarlo mediante un sistema llamado "*Forward proxy*". De esta forma el dispositivo hace de intermediario entre los clientes e Internet. Todo el tráfico HTTP pasará a través del Barracuda mostrando únicamente su IP en vez de la IP de los clientes. Esta sería la configuración de conexión para el modo "*Forward proxy*":

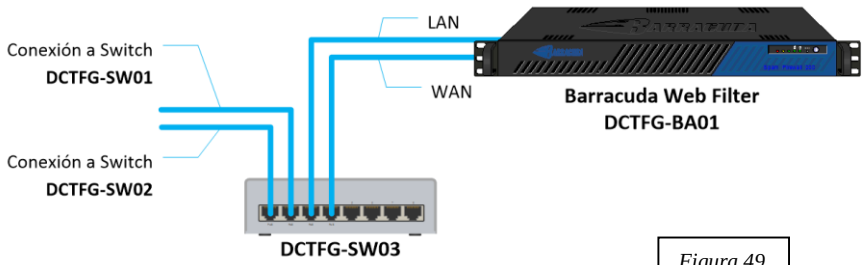


Figura 49

6.5.1.2 Autenticación para los dominios (LDAP)

Barracuda tiene dos formas de autenticar los usuarios: en local o por dominio. Como vamos a tener diferentes clientes que tendrán su propio dominio, esta será la configuración que se aplicará. El principal dominio que tenemos que añadir sería

DFTGC, el cual gestionará el acceso a Internet de los dispositivos y ordenadores conectados a la red principal de administración. Pero este no será el único, por cada cliente u oficina habrá que añadir el dominio correspondiente y de esa forma, a través de consultas *LDAP*, podremos validar a los usuarios que navegan por Internet. Es necesario crear una cuenta en el *AD* correspondiente que tenga derechos de acceso de lectura a todos los componentes del mismo para realizar esta acción.

La autenticación contra un dominio es fundamental para poder crear grupos en el *AD* para definir los diferentes niveles de acceso a Internet para los usuarios finales. Podemos añadir las conexiones *LDAP* que necesitemos para nuestros diferentes dominios desde la siguiente pantalla [13] de configuración del Barracuda:

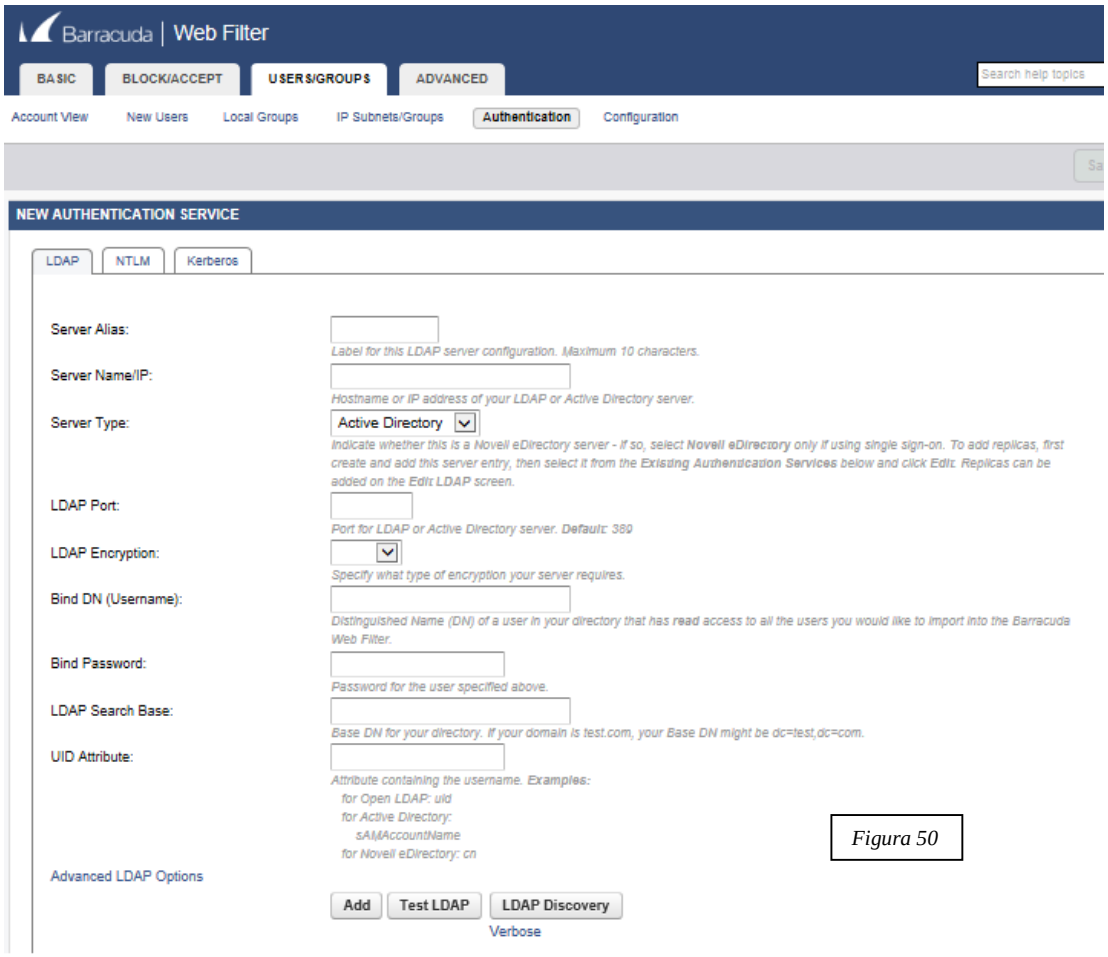


Figura 50

6.5.1.3. Proxy utilizando un fichero *PAC*

PAC (*Proxy Auto-Configuration*) es un fichero en el cual definimos una serie reglas para enrutar el tráfico Web a través de nuestro dispositivo Barracuda Web Filter. Una vez creado el fichero *PAC* podemos aplicarlos en los diferentes dominios utilizando Windows *GPO* (Group Policy Objects). En la página siguiente podemos ver un ejemplo de fichero *PAC* simulando algunas subredes de clientes u oficinas hospedados en la infraestructura.

Este sería un ejemplo de un fichero *PAC* [14]:

```
function FindProxyForURL(url,host)
{
        if (isInNet(myIpAddress(), "10.10.1.0","255.255.255.0") ||
        (isInNet(myIpAddress(), "10.10.10.0","255.255.255.0") ||
        (isInNet(myIpAddress(), "10.10.11.0","255.255.255.0") ||
        (isInNet(myIpAddress(), "10.10.20.0","255.255.255.0") ||
        (isInNet(myIpAddress(), "10.10.21.0","255.255.255.0") ||
        )
{
        return "PROXY 10.10.1.13:8080";
}
else
{
        return "DIRECT";
}
```

El funcionamiento es bastante sencillo. Cuando el cliente intenta navegar por Internet, la *GPO* accede al fichero *PAC* y comprueba que está conectado desde una de las redes de la organización. Si es así se aplica el proxy 10.10.1.13. En caso contrario conecta directamente a Internet.

El fichero *PAC* lo renombraremos como "*proxy.pac*" y lo guardaremos en uno de nuestros servidores de dominio (por ejemplo, el controlador de dominio de cada uno de ellos). Finalmente, cuando creemos la *GPO* correspondiente en los dominios, añadiremos la ruta donde se encuentre el fichero. Estos serían los pasos [15] para crear una *GPO* para Internet Explorer:

- En servidor de AD, vamos a la opción "*Group Policy*".
- "*User Configuration*"
- "*Control Panel Settings*"
- "*Internet Explorer*"
- Seleccionamos "*Connection*" y luego doble click en "*Automatic Browser Connection*"
- En la pestaña de "*Automatic Configuration*" seleccionamos "*Automatically detect configuration settings*" y luego "*Enable Automatic Configuration*".
- Introducimos un intervalo en "*Automatically configure every*".
- En el apartado "*Auto-proxy URL*" introduciremos la ruta donde se encuentra localizado el fichero *PAC*. Por ejemplo *\\10.10.10.1\pac\proxy.pac*.
- Luego accederemos a la parte "*Computer Configuration*" sección "*Administrative Templates -> System/Group Policy*" y aplicamos:
    - *Internet Settings policy processing*
    - *Allow procesing across a slow network connection.*
    - *Do not apply during periodic backgroun processing*
    - *Process even if the Group Policy objects have not changed.*

6.5.2. Barracuda Spam Filter

Para filtrar y detectar posibles virus y Spam en los correos electrónicos, utilizaremos un dispositivo *Barracuda Spam Filter*.

6.5.2.1 Configuración básica

La configuración básica [13][16] de este dispositivo es parecida (cambiando las direcciones IP y el nombre de host) a la descrita en el *apartado 6.5.1.1*. La conexión con el *switch* DCTF-SW03 será la siguiente (este dispositivo sólo tiene dos puerto Ethernet, uno para *WAN* y otro para *LAN*):

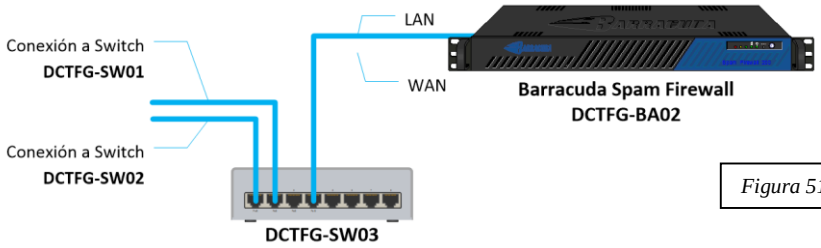


Figura 51

Asignaremos la dirección IP correspondiente así como la puerta de enlace principal:

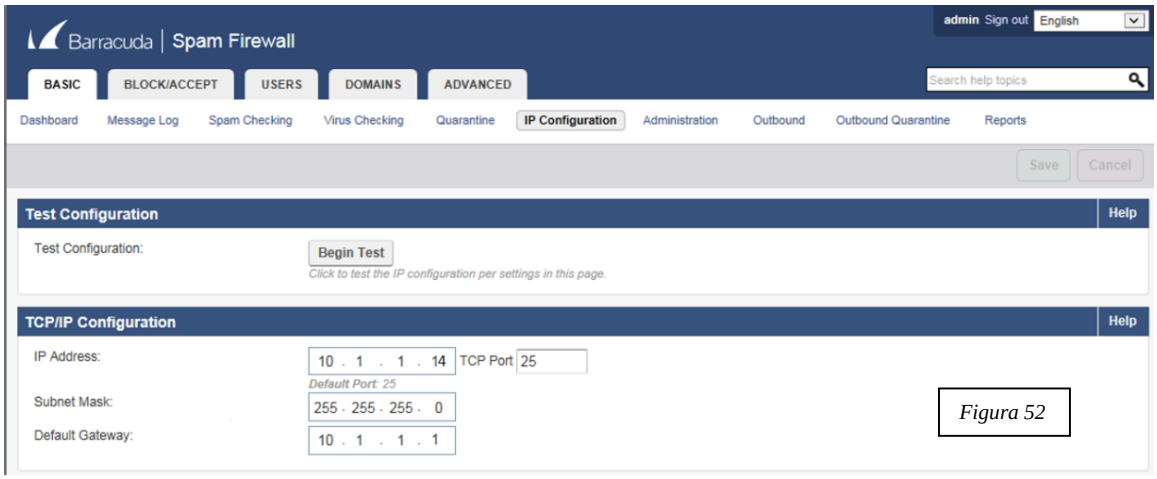


Figura 52

En esta misma pantalla, accedemos a la opción "*Domain Configuration*" para indicar los nombres de los dominios que vamos a autorizar el tráfico de correo a través del Barracuda. En este ejemplo se han añadido los posibles dominios de clientes y una oficina:

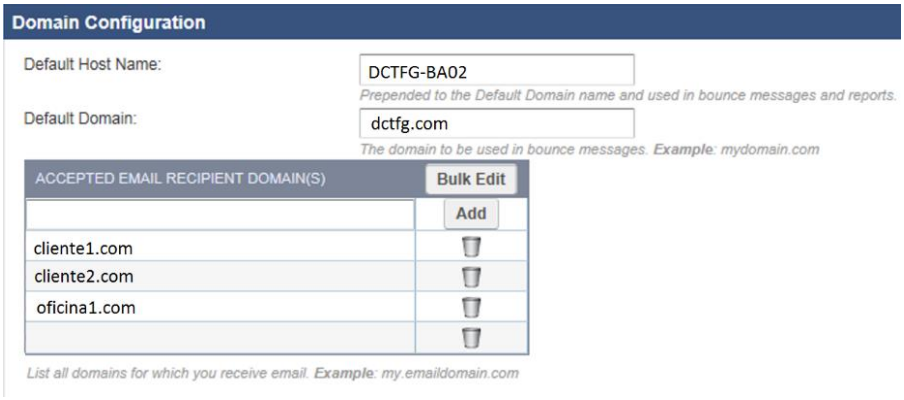
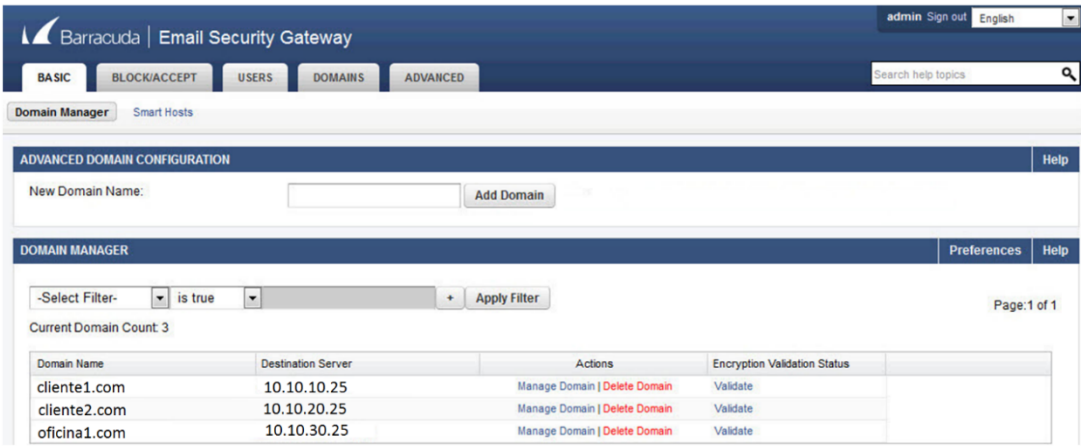


Figura 53

6.5.2.2 Enrutamiento del tráfico de correo para los dominios

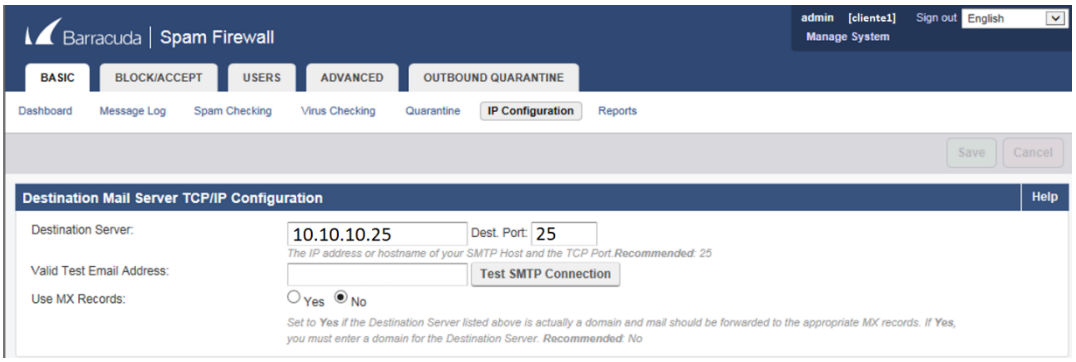
El paso principal antes de enrutar todo el tráfico de correo es definir los parámetros básicos de cada dominio en *BASIC >> Domain Manager*:

Figura 54



Añadiremos el nuevo dominio en "*New Domain Name*" y luego en la opción "*Manage Domain*" podremos asignar otros parámetros, entre ellos la conexión *LDAP* con el controlador de dominio y lo más importante, definir la dirección *IP* del servidor de correo al cual se conectará:

Figura 55



Finalmente activaremos el enrutamiento del correo llamado "*port forwarding*". Este método re direcciona todo el tráfico entrante SMTP (puerto 25) hacia el dispositivo Barracuda. Esta opción se activa en *ADVANCED > Advanced Networking*. Más adelante, cuando se explique la configuración de Exchange, volveremos a la configuración de dominios para definir los conectores.

6.6.1. Barracuda Message Archiver

Este dispositivo será el encargado de almacenar todo el correo entrante y saliente de los dominios de nuestra infraestructura.

6.6.1.1 Configuración básica

Es necesario abrir en el firewall principal los siguientes puertos:

Port	Dirección	TCP	UDP	Utilización
443	Entrada	Si	No	Acceso remoto por SSL
8000	Entrada	No	No	Web y add-in access

Por otro lado activaremos el acceso al interface web solamente mediante *https* en *ADVANCED > Secure Administration.*

El resto de la configuración [13] [17] de este dispositivo es exactamente igual (cambiando las direcciones *IP* y el nombre de host) a la descrita en el *Capítulo 6.5.1.1*.

6.6.1.2 Configuración avanzada y *Journaling*.

Una vez que hemos definido los parámetros básicos de la configuración, el siguiente paso es añadir los *FQDNs* con los nombres de dominios de los cuales vamos a almacenar el correo. Accederemos a *BASIC > IP Configuration*, apartado *Local Domains*. Ahí podremos ver un listado con todos los dominios que tenemos añadidos en nuestro sistema [17].

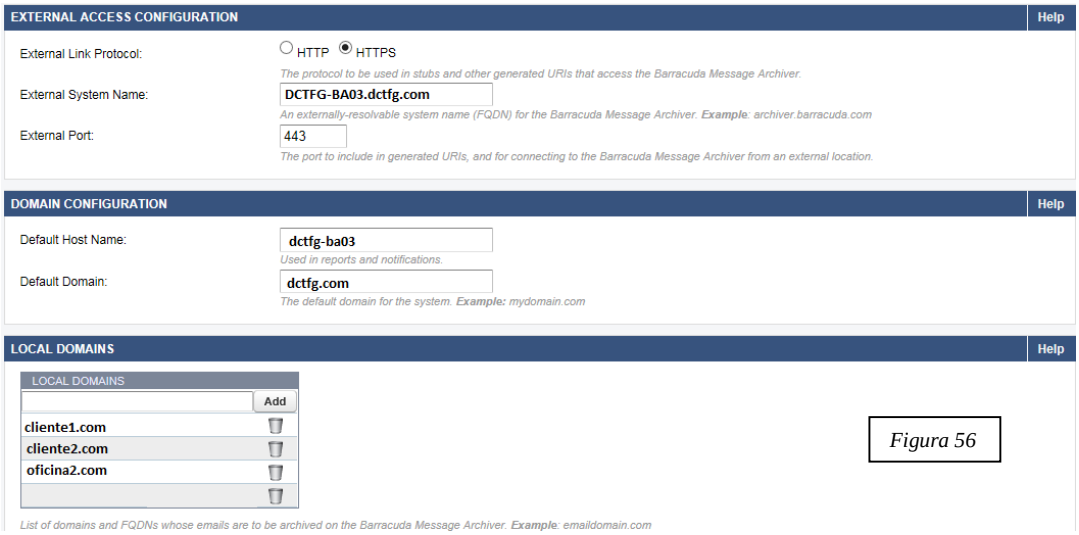


Figura 56

El siguiente paso es activar "*SMTP forwarding*" para hacer que todos los correos de todos los dominios pasen por el dispositivo. Aparte de activar esta opción, también tendremos que añadir los servidores de correo de cada dominio a medida que los vayamos creando. En la siguiente imagen podemos ver la activación del *SMTP Forwarding* y también la relación de servidores de correo con su dirección *IP* y como comentario el nombre de máquina para identificarlo:

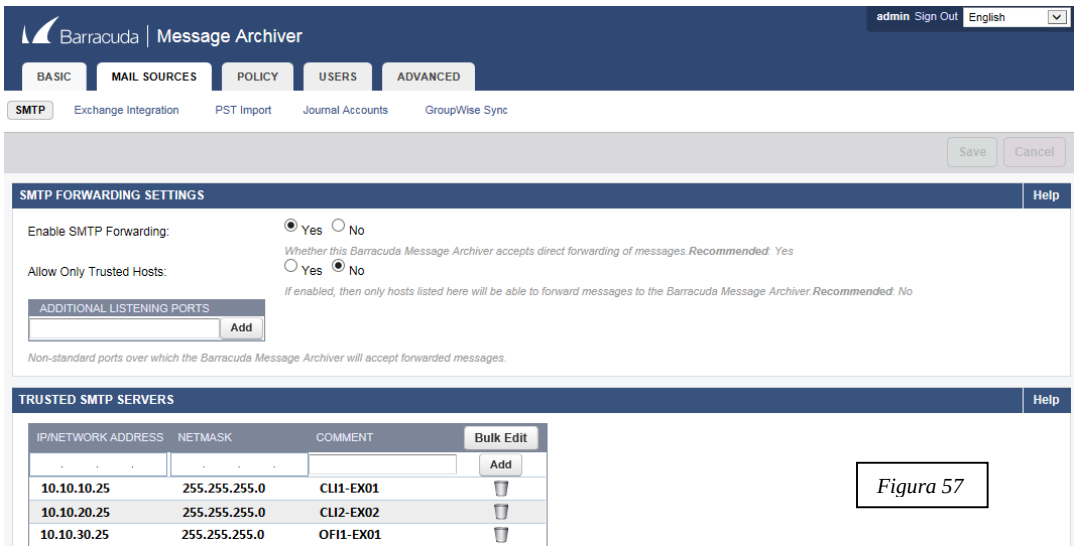


Figura 57

Una vez hayamos definido los dominios y los servidores de correo, pasaremos a la autenticación de usuarios de cada uno de ellos. Esto se realizará una vez más

utilizando *LDAP*. Siguiendo el ejemplo anterior, añadiremos las entradas *LDAP* para cada de los dominios indicando el servidor controlador de dominio correspondiente. Como ya se ha mencionado antes, nos tenemos que asegurar que tenemos una cuenta en *AD* con derechos de lectura sobre todos los componentes del mismo:

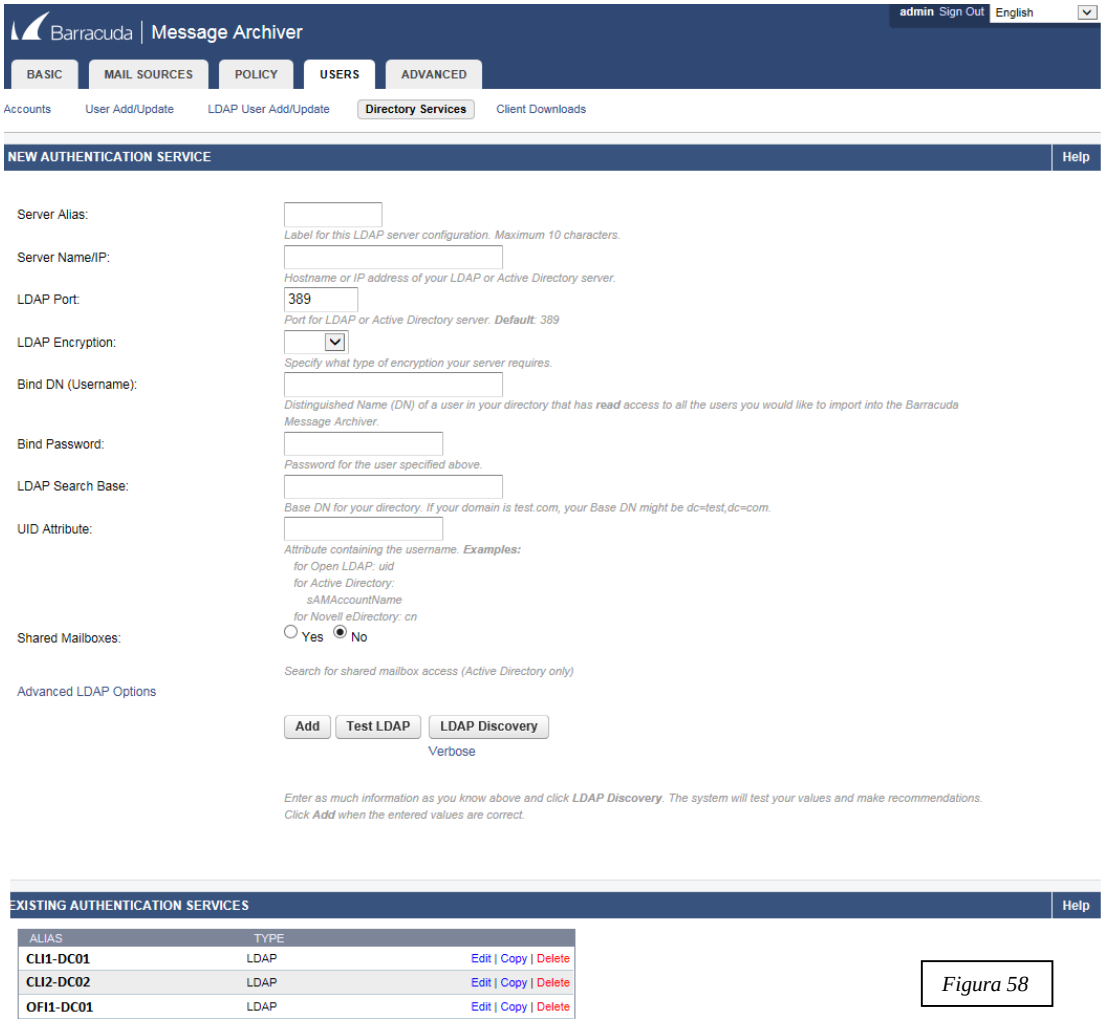


Figura 58

El último paso que hay que realizar es uno de los más importantes, llamado *Journaling*. Para poder activarlo el paso previo ya lo hemos realizado al añadir los servidores de correo como autorizados (*Figura 58*). Este es el único proceso que tenemos que realizar en el Barracuda. Como el resto del procedimiento implica configurar el servidor de correo Exchange 2013, este tema se tratará en dicha sección.

7. Configuración de los servidores físicos:

7.1. Servidor para controlador de dominio (DCTFG-DC01):

El primer paso será configurar los discos RAID [18]. Utilizaremos el software "*Intelligent Provisioning*" que para este tipo de servidores G9 con *BIOS UEFI* suele venir integrado dentro del arranque (F10):

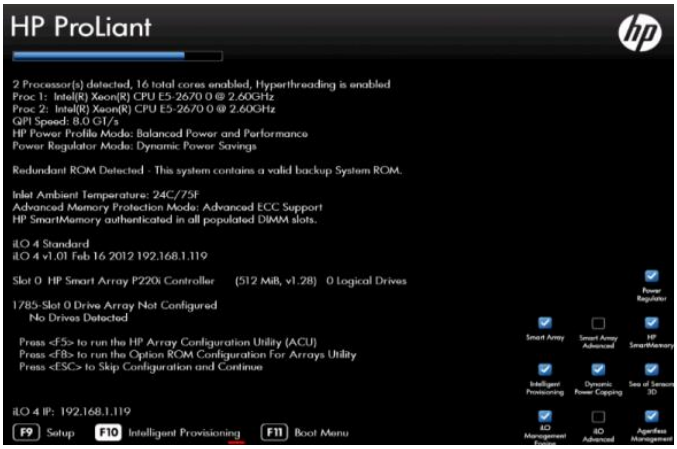


Figura 59

Todos los servidores llevarán dos discosm, con un tamaño mínimo de 500GB instalados en un *RAID 1*. Estos discos sólo contendrán el sistema operativo y las descargas de actualizaciones del mismo. La configuración del RAID es bastante sencilla y directa de realizar [18]. En la *Figura 60* se detalla las conexiones de red del servidor.

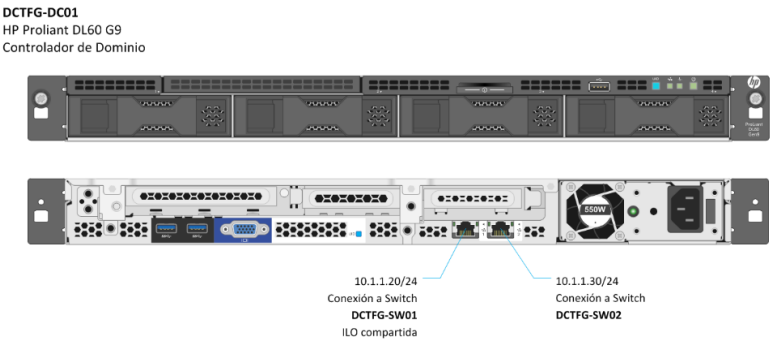


Figura 60

Aunque podríamos desde Windows Server 2012 crear las particiones lógicas, es aconsejable crearlas desde esta misma configuración de HP. Es sencillo y nos evitará acciones posteriores sobre el sistema operativo del servidor [18]:

Figura 61a

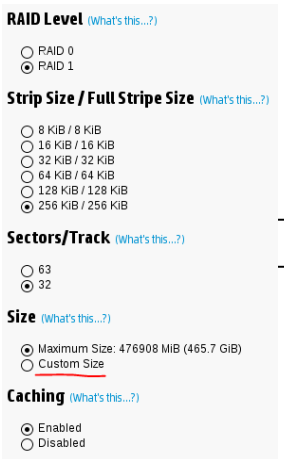


Figura 61b

Activando la opción "*Custom Size*" procederemos a crear la partición lógica. Podríamos hacer *Partición lógica 1*, 300GB para el Sistema Operativo y *Partición lógica 2*, 200GB actualizaciones.

7.1.1. Instalación Windows Server 2012

Ver Anexo, apartado 16.1

7.1.2. Instalación de roles

Ver Anexo, apartado 16.2

7.2. Servidores de virtualización Hyper-V

7.2.1. Instalación Windows Server 2012

Ver Anexo, apartado 16.1

7.2.2. Instalación de roles

Ver Anexo, apartado 16.3

7.2.2. Tarjetas de red

Los servidores Hyper-V de esta infraestructura tienen 4 tarjetas de red incorporadas. Configuraremos la primera de ellas como *NIC* principal con los siguientes valores:

NIC 1:

IP: 10.1.1.22
Máscara: 255.255.255.0
Gateway: 10.1.1.1
DNS Primaria: 10.1.1.20
DNS Secundaria: 10.1.1.30

La otra tarjeta se configurará más adelante en función de las necesidades de las máquinas virtuales que tengamos. También se unificarán utilizando "*NIC Teaming*", explicado en el *Capítulo 7.3.3*.

7.3. Servidor de backup

El paso principal antes de comenzar con la configuración del servidor es instalar la tarjeta *SAS*. Una vez realizado, procederemos como en el resto de servidores a instalar Windows Server 2012.

7.3.1. Instalación Windows Server 2012

Ver Anexo, apartado 16.1

7.3.2. Instalación de roles

En este caso los roles a instalar serían *File and Storage Services* y *IIS*
Ver Anexo, apartado 16.3

7.3.2. Instalación Symantec Backup Server

Antes de comenzar la instalación del software de backup tenemos que conectar el cable *SAS* desde el servidor de backup (tarjeta *PCIe SAS*, explicada en el *Capítulo 3.4*).

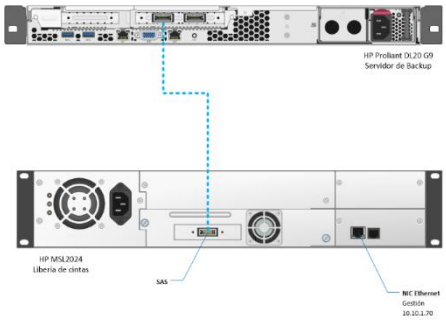


Figura 62

7.3.3. Tarjetas de red (*NIC teaming*)

Este servidor tiene 2 tarjetas de red instaladas por defecto. Para optimizar las copias de seguridad y la velocidad de copia, es conveniente unir varias de estas tarjetas utilizando un método llamado *NIC teaming*. Para nuestra configuración vamos a unir las tarjetas NIC1 y NIC2, dejando NIC3 y NIC4 para futuras ampliaciones. El primer paso es asignar una IP a la primera tarjeta de red, NIC1:

NIC 1:

IP: 10.1.1.21
Máscara: 255.255.255.0
Gateway: 10.1.1.1
DNS Primaria: 10.1.1.20
DNS Secundaria: 10.1.1.30

Una vez asignada la dirección IP procederemos al proceso de *teaming* [19]. Para ello accederemos al *Server Manager*, hacemos click en *Local Server* y a la derecha veremos la opción de *NIC Teaming* marcada como *Disabled.* En la siguiente pantalla seleccionamos las dos interfaces que vamos a unir, NIC1 y NIC2:

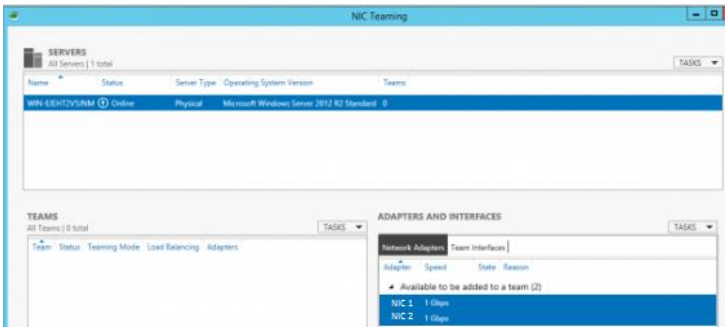


Figura 64

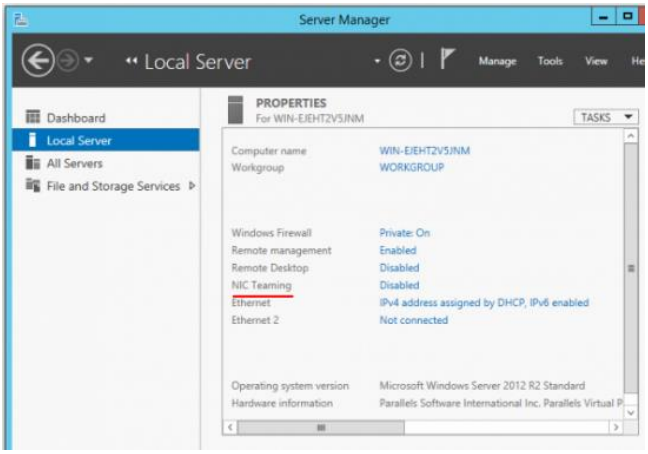


Figura 63

8. Configuración del entorno SAN

8.1. Primeros pasos

La *SAN* MSA2040 de HP será la base de almacenamiento para todas las máquinas virtuales que se integrarán en la infraestructura. Por lo tanto es primordial configurar de la forma más óptima todas las opciones de la misma, empezando por las conexiones y terminando por la configuración (*SAN* y Hyper-V).

La *SAN* estará conectada únicamente a una de las redes, la red de almacenamiento, utilizando incluso un direccionamiento de red totalmente distinto al utilizado para la red de datos: 172.1.1.*X*

El primer paso es conectar físicamente los servidores de Hyper-V con la SAN a través de la conexión *SFP* y luego a los switches CISCO 4900 mediante *10GBASE-T* (estos servidores vienen con 2 tarjetas de 1GbE y dos 10GbE, como ya se ha comentado anteriormente):

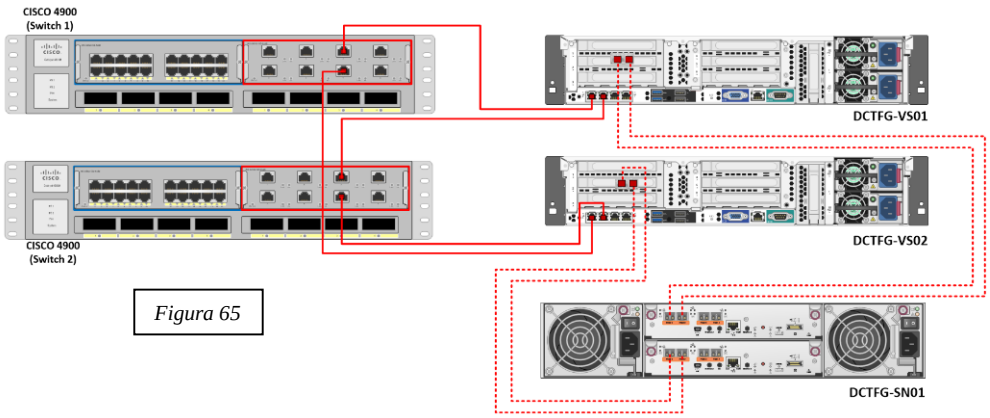


Figura 65

8.2. Configuración de la SAN

8.2.1. Instalación básica

Ver Anexo, apartado 16.5

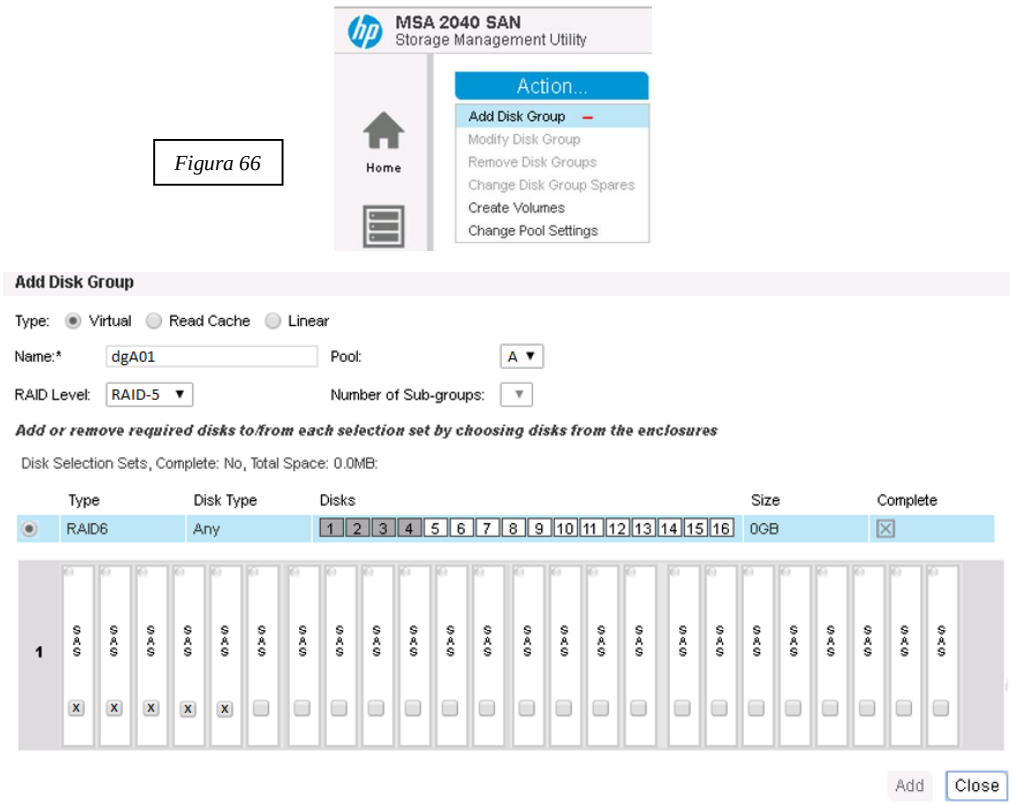
8.2.2. Organización de los discos y RAID

Para la *SAN* de esta infraestructura vamos a comenzar adquiriendo todos los discos posibles para ocupar todos los slots libres, 24 discos en total. Los discos son modelo *EG1800JEHMD* tipo *SAS* 12G 10K de 1,8TB de almacenamiento cada uno. Comenzaremos destinando 17 discos de los cuales 2 serán para "*hot spare*" (cambio dinámico en caso de fallo) y los otros 15 para crear los diferentes volúmenes de trabajo.

Una vez instalados todos los discos comenzaremos la configuración [20][21][22]. Como se ha comentado anteriormente, utilizaremos en principio sólo 17 de los 24 discos instalados dejando el resto para futuras ampliaciones de la infraestructura.

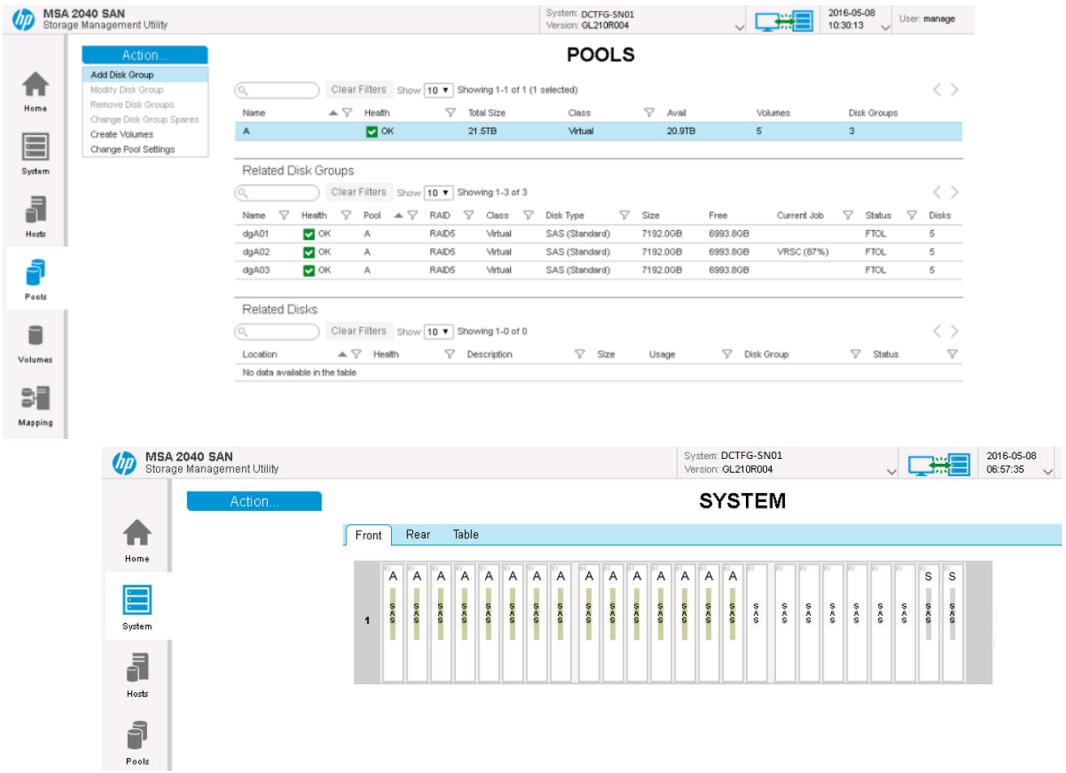
Comenzaremos creando los grupos de discos en el pool principal A el cual tiene un total de 21.5TB. Dentro de este pool crearemos 3 grupos de 7TB cada uno utilizando el tipo de *RAID 5*. Para ello seleccionaremos 3 bloques de 5 discos en modo *RAID 5*

Figura 66



Repetiremos el mismo proceso para los otros dos grupos y finalmente obtendremos la siguiente configuración:

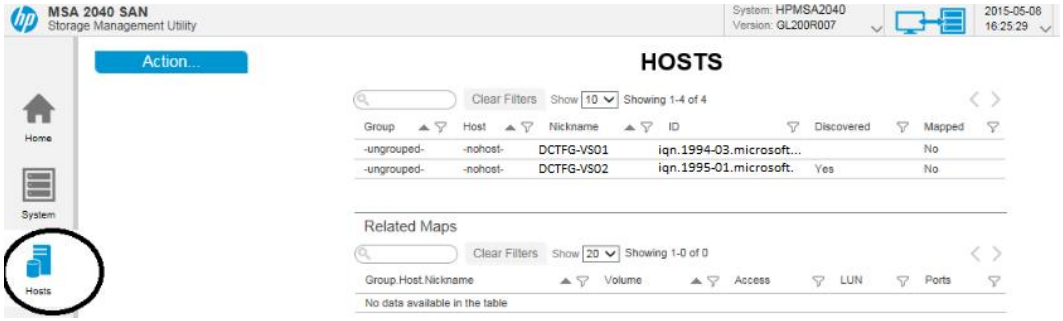
Figura 67



8.2.3. Conexión de los hosts

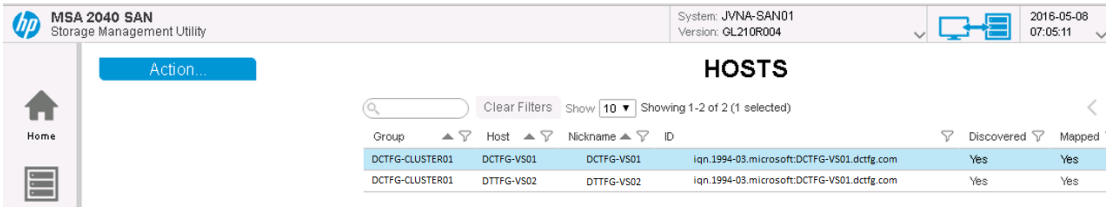
Una vez tenemos los grupos de discos preparados procederemos a conectar los host [22]:

Figura 68



Añadimos a un host los iniciadores *iSCSI* detectados, desde el menú *Action*, *Add to host*. Seleccionamos el iniciador DCTFG-VS01 y lo asignamos al host seleccionado dando como nombre de grupo DCTFG-CLUSTER01 (este será el nombre que le daremos al clúster Hyper-V). Una vez terminada la operación con el otro host obtendremos la siguiente configuración:

Figura 69



8.2.4. Volúmenes

El siguiente paso en la configuración *SAN* es añadir los volúmenes que vamos a utilizar. Estos son los volúmenes iniciales que podríamos crear:

Grupo	Nombre	LUN	Tamaño	Descripción
DCTFG-CLUSTER01	Quorum	0	1GB	Cluster Hyper-V
DCTFG-CLUSTER01	Volume1 (Cli1)	1	300GB	Volumen máquinas virtuales Cliente 1
DCTFG-CLUSTER01	Volume2 (Cli2)	2	300GB	Volumen máquinas virtuales Cliente 1
DCTFG-CLUSTER01	Volume3 (Ofi1)	3	300GB	Volumen máquinas virtuales Oficina 1
DCTFG-CLUSTER01	Volume4 (Bck)	4	900GB	Backup auxiliar en la SAN

Figura 70

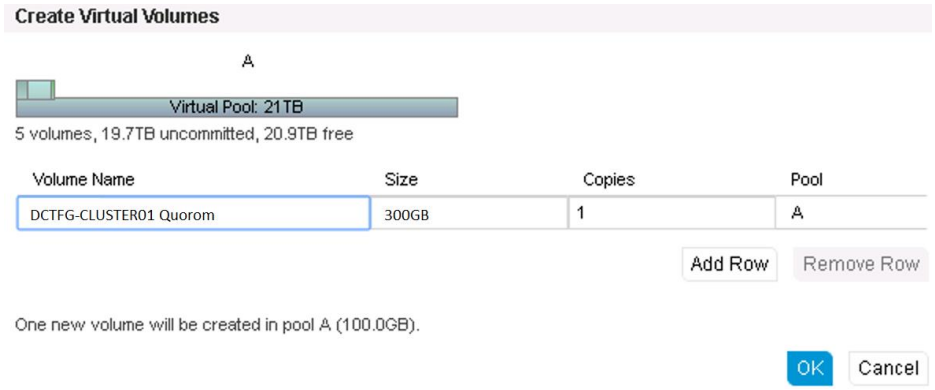


Figura 71

Para el resto de volúmenes realizaremos la misma operación. Al final obtendremos los siguientes grupos de volúmenes:

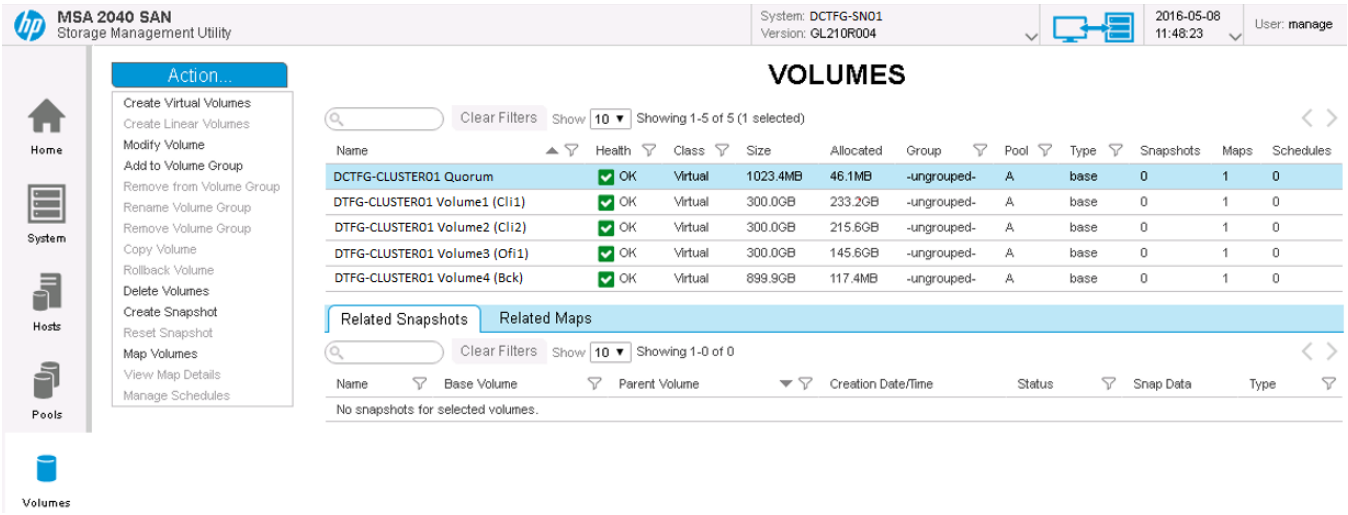


Figura 72

Con esta última operación ya estarán preparados los volúmenes para conectarlos a los servidores Hyper-V.

9. Virtualización (Hyper-V)

En el apartado anterior hemos configurado la base de almacenamiento para las máquinas virtuales que se ejecutarán en el clúster Hyper-V. La siguiente fase es configurar cada servidor Hyper-V para que conecte con los volúmenes creados y que apunte a esa ubicación para crear las máquinas virtuales. Por otro lado, configuraremos también el clúster Hyper-V y la alta disponibilidad. Para que los servidores Hyper-V tengan acceso a los recursos de la SAN, el paso inicial es configurar la tarjeta de red SFP de cada nodo dentro del mismo rango IP, ya que la SAN se encuentra en otro distinto a la red de datos (172.1.1.X):

NIC1 SFP DCTFG-VS01:
IP: 172.1.1.10
Máscara: 255.255.255.0
Gateway: 10.10.1.1

NIC1 SFP DCTFG-VS01:
IP: 172.1.1.20
Máscara: 255.255.255.0
Gateway: 10.10.1.1

NIC2 SFP DCTFG-VS02:
Teaming con NIC1

NIC2 SFP DCTFG-VS02:
Teaming con NIC1

DNS 1: 10.1.1.20 DNS 2: 10.1.1.30

9.1. Conexión iSCSI con la SAN y los volúmenes

Antes hemos instalado el rol *File and Storage Services* el cual lleva incluido el servicio *iSCSI Initiator*. En caso contrario tendríamos que instalarlo desde las mismas opciones *Add role and features*. Una vez comprobamos que está presente, lo ejecutamos:

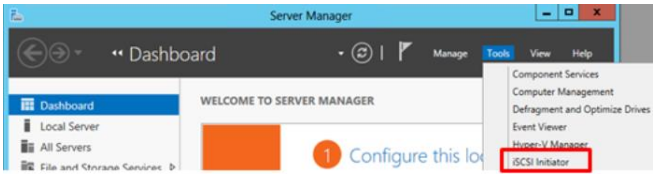
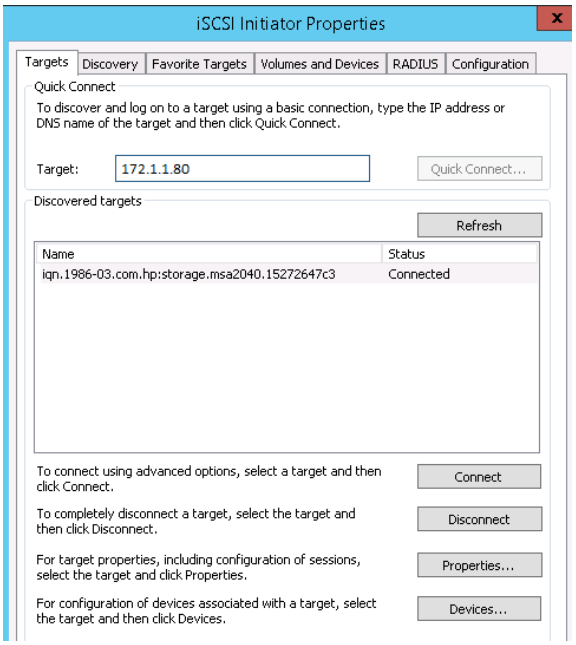


Figura 73

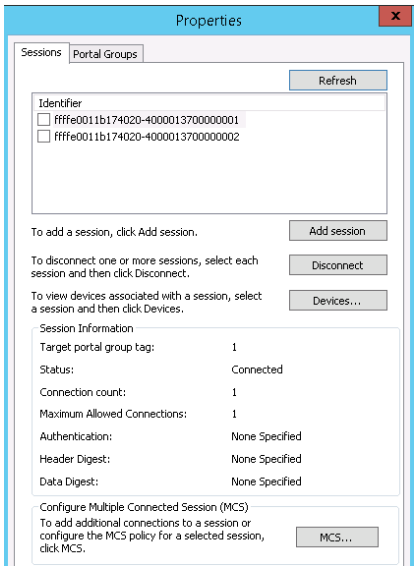
Una vez abierto *iSCSI Initiator*, en la pestaña "*Targets*" procederemos a añadir la *SAN* utilizando la dirección IP de uno de sus módulos (172.1.1.80). Una vez que hemos añadido la dirección IP en el campo "Target" pulsamos en "*Quick Connect.*". Si todo está correcto, aparecerá la conexión a la SAN [23]:

Figura 74



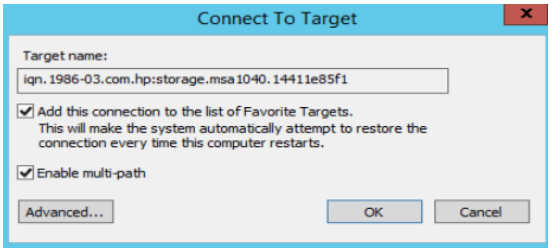
Seleccionamos la cadena que identifica a la *SAN* y pulsaremos en el botón "*Propierties*". Lo que vemos en esta pantalla son los identificadores de las tarjetas de red conectadas en la *SAN*:

Figura 75



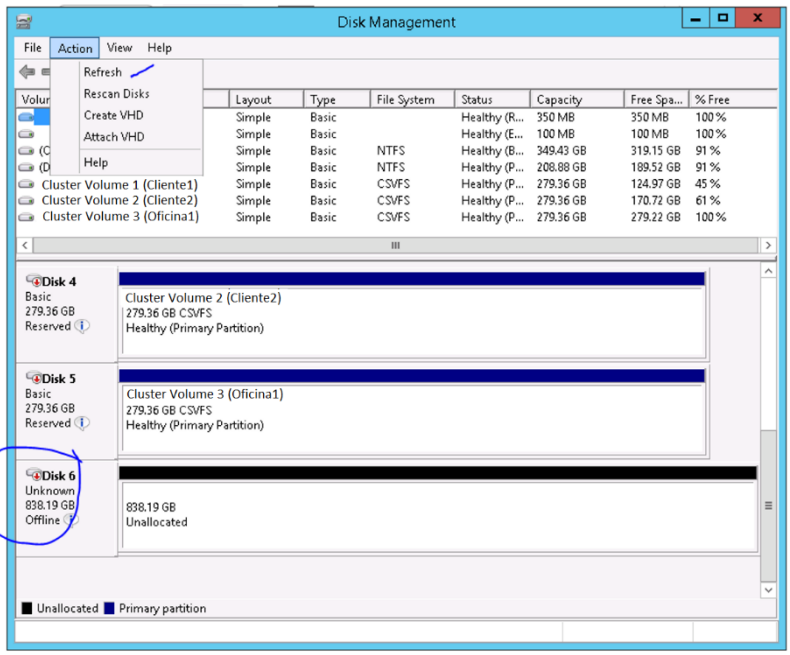
Pulsaremos en *Add session* para finalizar la conexión con la SAN. En la pantalla siguiente marcaremos la opción *Enable multi-path* y también añadiremos esta conexión a favoritos para facilitar su acceso:

Figura 76



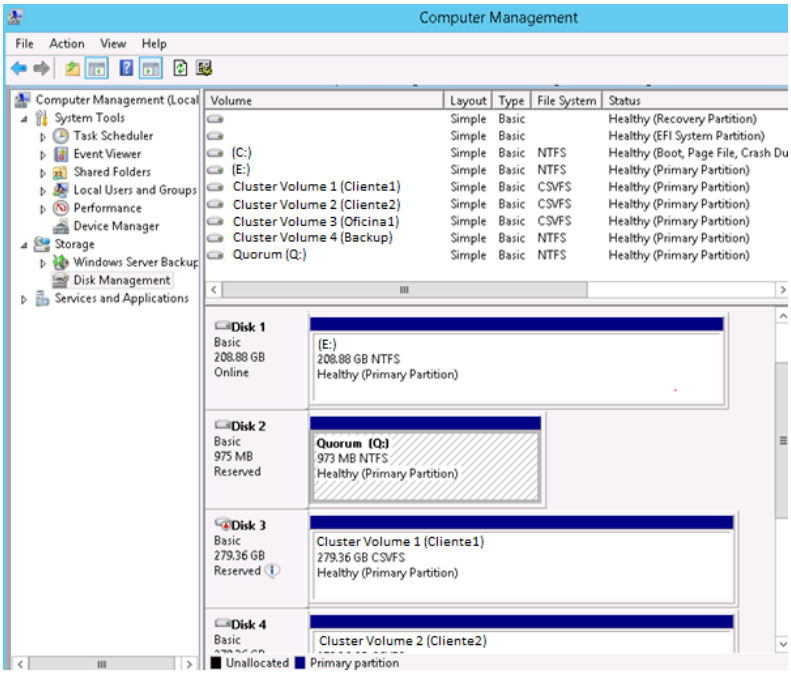
El siguiente paso consistirá en añadir los volúmenes a Windows. Esto podemos realizarlo desde la pantalla de administración de discos de Windows 2012 Server (*Disk Management*). Es posible que las unidades no sean visibles en principio, por lo tanto el primer paso es refrescar la vista para ver los volúmenes que están disponibles en la SAN. En el ejemplo siguiente se muestra como mapear el volumen *Cluster Volume 4 (Backup)*:

Figura 77



Vemos que la unidad aparece como *Unknown* y *Unallocated*. Para crearla sólo tenemos que hacer *click* con el botón derecho del ratón, activarla y asignarle el nombre *Cluster Volume 4 (Backup)*:

Figura 78

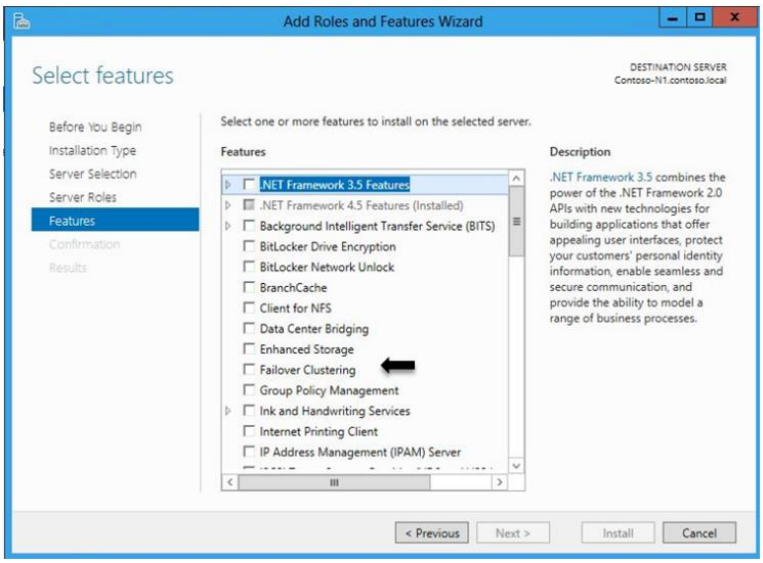


9.2. Configuración inicial *Failover Clustering* Hyper-V

En el *Capítulo 7* ya instalamos los roles necesarios a los dos servidores de Hyper-V, DCTFG-VS01 y DCTFG-VS02. El siguiente paso es configurar el clúster con los dos nodos y obtener de esa forma alta disponibilidad en caso de fallo de uno de ellos.

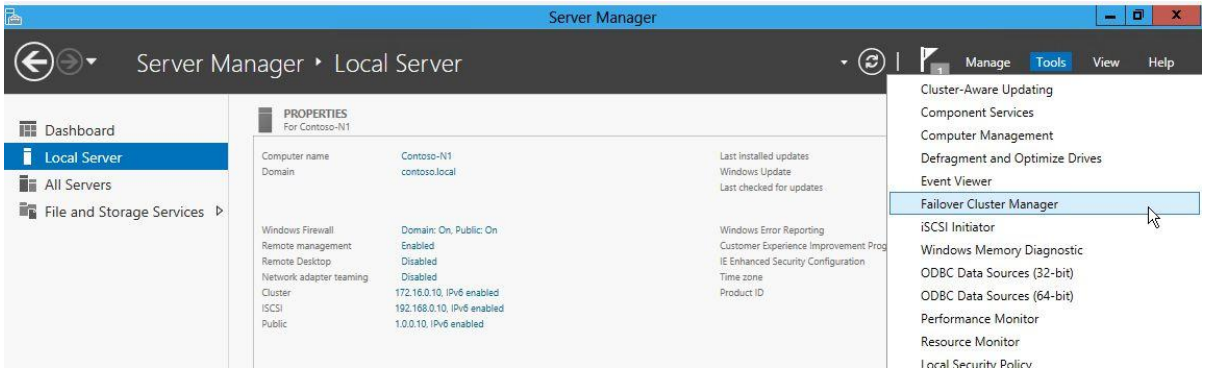
Comenzaremos instalando la opción de *Failover Cluster* desde Windows 2012 Server *Server Manager*, *Add Roles and Features*. Una vez seleccionado el servidor pasaremos a activar la opción *Failover Clustering* [24]:

Figura 79



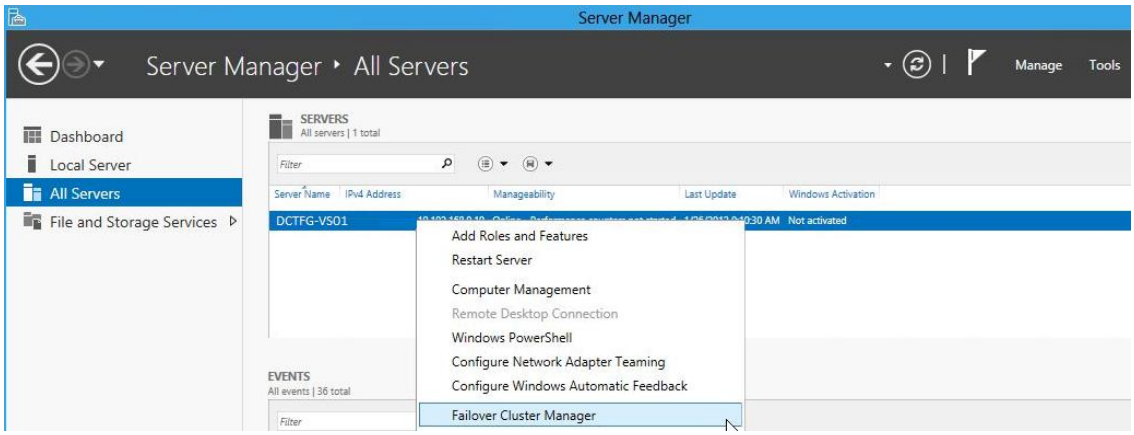
Una vez instalada, volveremos al *Server Manager* para proceder a la configuración:

Figura 80



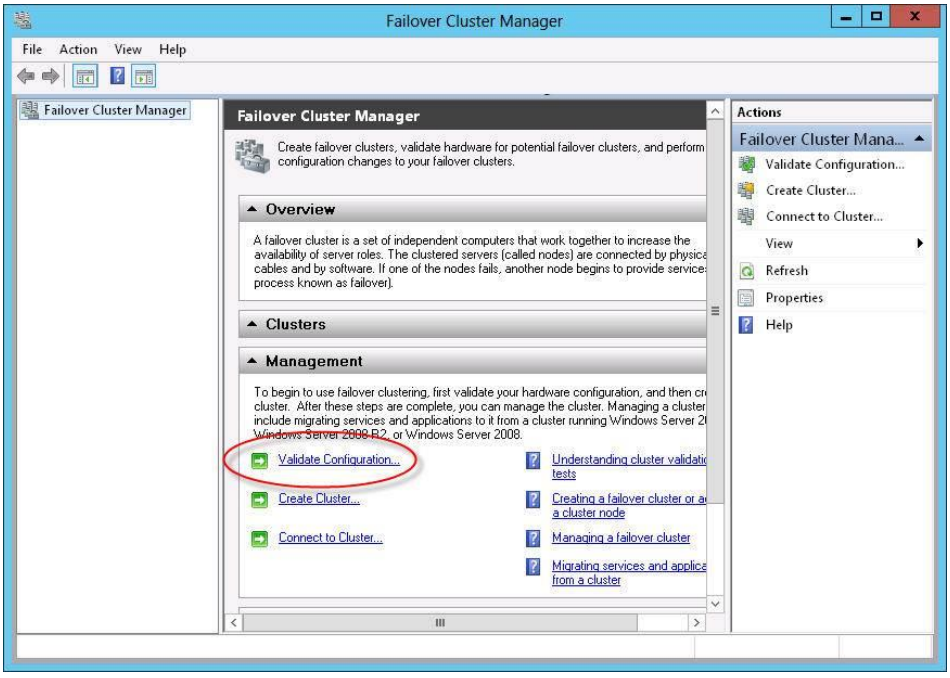
Una vez seleccionado el servidor, con el botón derecho del ratón pasaremos al *Failover Cluster Manager*

Figura 81



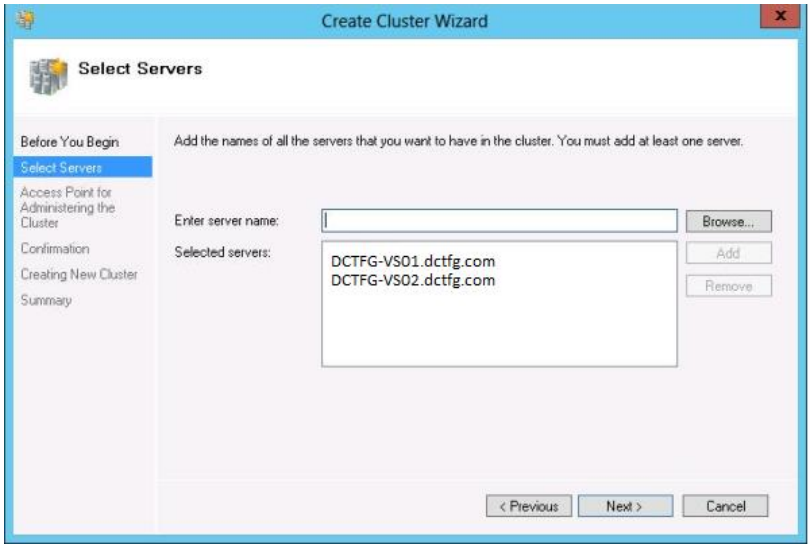
El siguiente paso es validar el clúster y añadir los nodos. Para realizar esta acción pulsamos en "*Validate Configuration*":

Figura 82



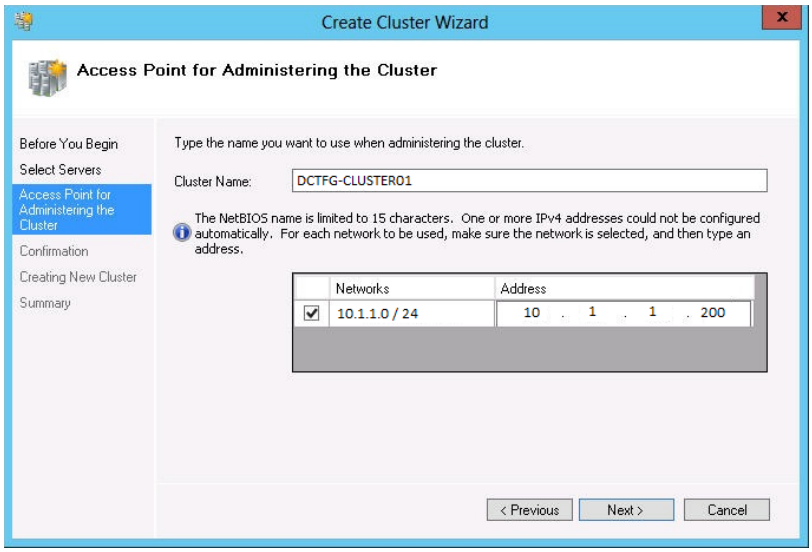
Seleccionamos los dos servidores nodos principales para Hyper-V:

Figura 83



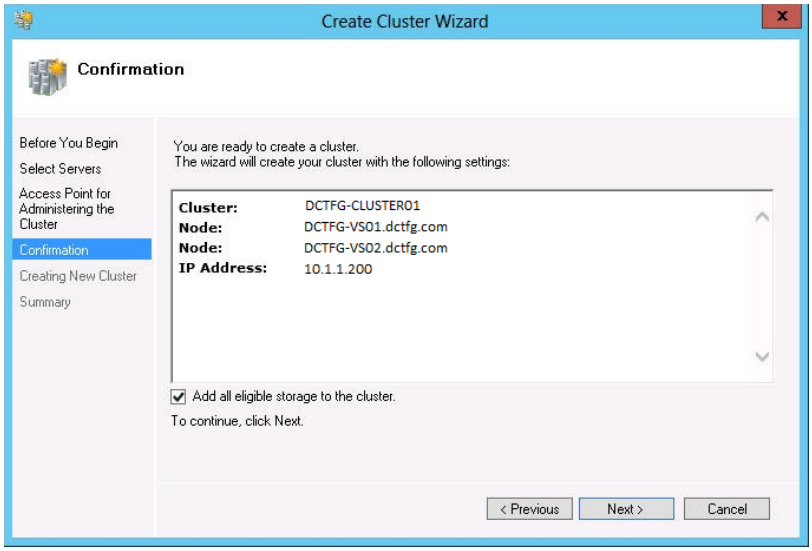
Luego procedemos a nombrar el clúster y añadir la IP de gestión del mismo:

Figura 84



Con este último paso terminaremos la configuración básica del clúster:

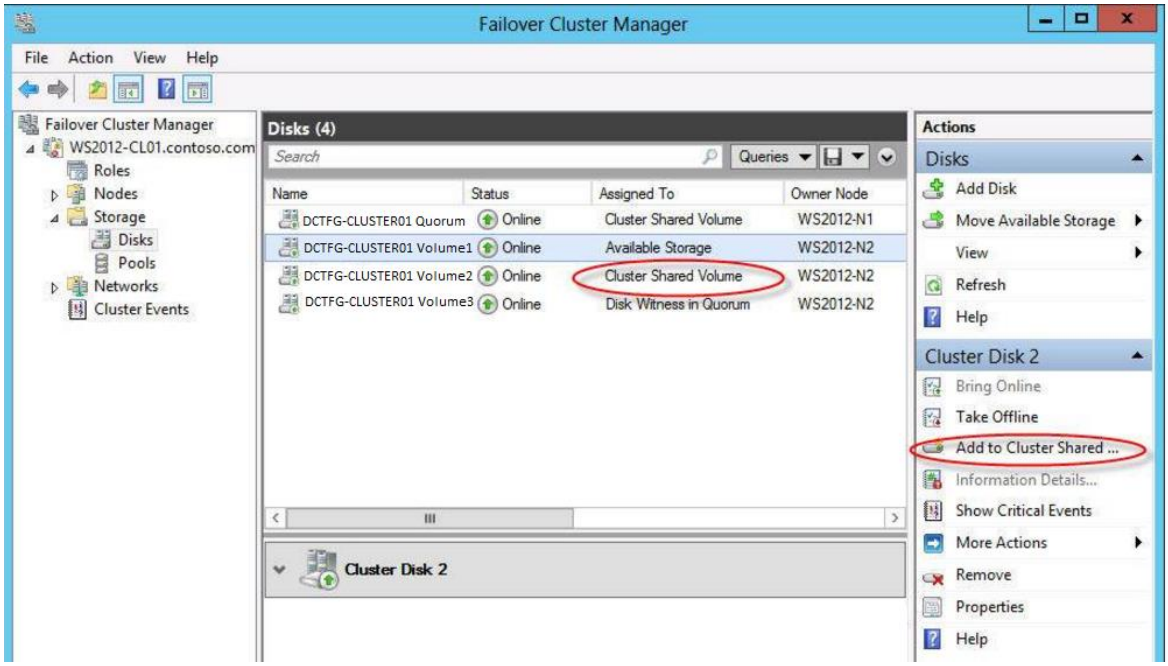
Figura 85



9.3. Configuración de los volúmenes compartidos

El siguiente paso consistirá en activar CSV (*Cluster Shared Volumes*) [25] para hacerlos visibles a Windows 2012 Server y asignarlos al clúster Hyper-V. Los añadiremos uno a uno con la opción *Add to Cluster Shared*:

Figura 86



Esta operación añadirá una carpeta llamada *ClusterStorage* en el disco C: con la siguiente estructura:

- C:\ClusterStorage\Volume1
- C:\ClusterStorage\Volume2
- C:\ClusterStorage\Volume3
- Etc ...

10. Configuración de las máquinas virtuales

10.1. Análisis de las máquinas virtuales para cada entorno

Como ya se ha comentado, uno de los objetivos de este TFG es crear una infraestructura que permita a diferentes organizaciones configurar todos los servicios que sean necesarios en función de sus necesidades. El correo electrónico es uno de los servicios fundamentales así como los servidores de ficheros o aplicaciones. De todas formas dependerá del tipo de oficina o cliente que estemos configurando decidir qué máquinas virtuales serán necesarias. A continuación se detallan las principales:

10.1.1. Controladores de dominio, *DHCP*, DNS y otros

Si la configuración que vamos a implementar es para un cliente totalmente ajeno a nuestra organización, será necesario implementar todos los recursos básicos para su administración:

- *Controlador de dominio:* este servidor será la base de la configuración. Desde aquí se creará el dominio y *forest* principal de la nueva organización. La administración se realizará desde este servidor.

- *DHCP:* servicio para gestionar la asignación y *pooles* de las direcciones *IP*. Podríamos implementar este servicio en el controlador de dominio principal. No es rentable montar un servidor sólo para este servicio pero sí sería recomendable configurar un segundo controlador de dominio que incluyera este servicio y otros. Los Fortigate también pueden adoptar este servicio en vez de los servidores virtuales.

- *DNS:* servicio para resolver nombres, también podría implementarse al igual que *DHCP* en otro servidor.

- *IIS (Servidor Web)*: si la empresa tiene una página web interna o requiere de servicios basados en web como por ejemplo SharePoint, será necesario instalar este servicio. En función de la complejidad de los requerimientos, se evaluará instalarlo en un servidor independiente o no.

- *SQL (Bases de datos):* muchas aplicaciones requieren de un motor de bases de datos. En función de la complejidad es posible que tengamos que crear un servidor dedicado sólo como gestor de bases de datos. En otros casos es posible instalar el motor de base datos en el servidor de aplicaciones.

- *Terminal Server (Accesos remotos, RemoteApp)*: algunas aplicaciones se instalarán en el servidor de aplicaciones y los usuarios conectarán de forma remota para ejecutarlas. Para conseguir esta implementación será necesario instalar un servidor dedicado para *TS* (*Terminal Service*) y *TS Gateway* (pasarela de conexión a las aplicaciones).

- *Servidor de impresión:* para gestionar las colas de impresión y los controladores de impresoras, será necesario instalar este role en uno de los servidores. Este servicio se puede instalar en cualquier servidor en función del volumen y servidores disponibles.

En cambio, si la configuración está orientada a una oficina interna de nuestra organización, es posible que no necesitemos implementar algunos de estos servicios. Podríamos crear un entorno virtual dedicado exclusivamente a ofrecer servicios sólo a las oficinas de la

organización, dejando la instalación mínima necesaria para las oficinas (servidor de ficheros, controlador de dominio, etc.)

10.1.2. Servidores de aplicaciones

Tanto si el cliente es externo o si es una oficina interna, será necesario ejecutar todo tipo de aplicaciones no desarrolladas por la organización principal. El servidor virtual para este tipo de servicios tendrá instalado los roles de "*File and Storage Services*" y "*Application Server*".

Aquí podríamos instalar las aplicaciones comerciales que requieran de un servidor central tanto para su ejecución como para gestionar las licencias. Este podría ser un ejemplo de una configuración para un servidor de aplicaciones:

Roles:

- *File and Storage Services*
- *Application Server*
- *Web Server (ISS)*

Aplicaciones:

- *SQL Express*
- *Software ERP*
- Etc.

Los servidores encargados de la gestión del Backup o de la seguridad (Antivirus) son también servidor de aplicaciones. Por lo tanto la configuración del servidor de aplicaciones dependerá de las necesidades de la empresa aunque por defecto tendrá los roles que antes se han indicado.

10.1.3. Servidores de ficheros

Un servidor de ficheros se encarga de almacenar la información y además ofrecer otros servicios gestión de permisos, cuotas, etc. Aquí tendríamos que definir dos tipos de servidores de ficheros:

- *Físicos:* se instalará un servidor físico en la oficina remota el cual gestionará de forma local toda la información y los accesos. Este servidor además de servidor de ficheros actuará como controlador de dominio. *Figura 87*
- *Virtuales:* el servidor de ficheros se implementa dentro del entorno virtual de la oficina o cliente. *Figura 88*

Utilizar un servidor virtual tiene la ventaja de la gestión de recursos (es muy sencillo de administrar y además se pueden asignar nuevos recursos de forma inmediata) ya que se encuentra dentro de nuestra infraestructura principal. Tiene como inconveniente la velocidad de acceso, ya que si la oficina no tiene buenas comunicaciones, el rendimiento a la hora de abrir o gestionar ficheros no será óptima. Por otro lado, un servidor físico tiene la ventaja de la velocidad, ya que la conexión se realiza en local, dentro de una red *Ethernet*. Tiene la desventaja la instalación inicial, el coste y sobre todo la copia de seguridad de los datos (tendremos que realizar una copia de seguridad remota de la información).

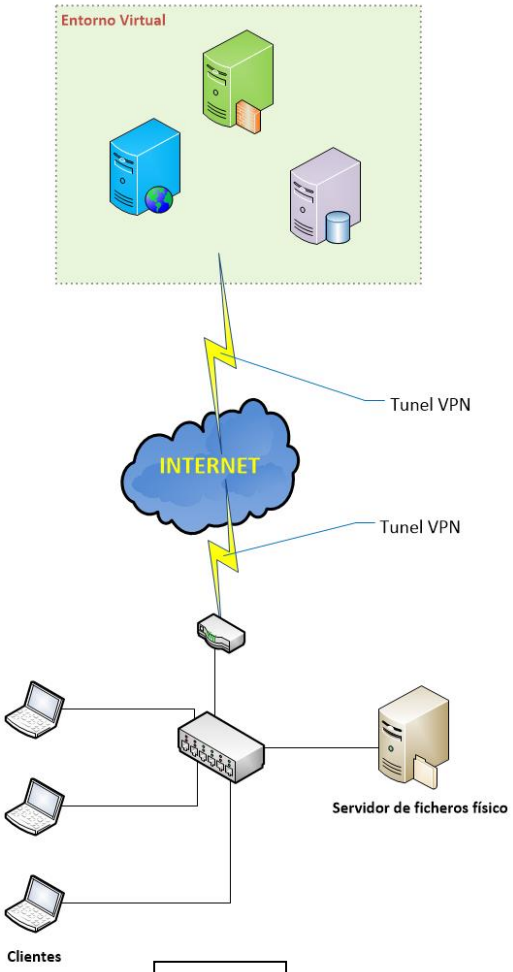


Figura 87

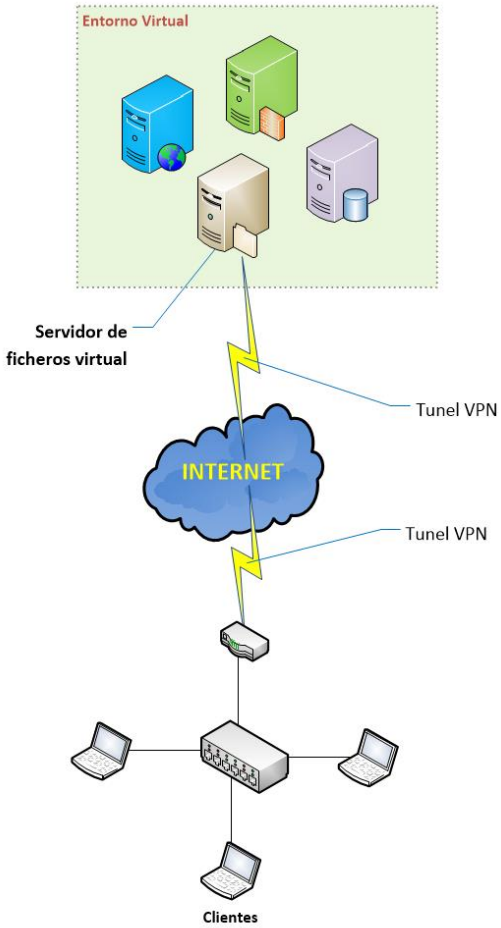


Figura 88

10.1.4. Servidores de correo electrónico

El *Capítulo 11* explica en detalle de su configuración.

10.2. Creación y asignación de recursos para las máquinas virtuales

Crear una máquina virtual dentro de Hyper-V es una tarea sencilla pero a la vez requiere planificación para evitar futuros errores. Para un funcionamiento óptimo de la misma es necesario tener algunas precauciones a la hora de configurarla. Además cada tipo de servidor requiere una configuración diferente, tanto en asignación de memoria como de espacio en disco. Debemos siempre de comenzar asignando los recursos mínimos y luego iremos ampliándolos en función de la demanda necesaria.

Los recursos dependen básicamente de dos elementos: los servidores host Hyper-V y la SAN. Los servidores Hyper-V definen los recursos disponibles relacionados con el funcionamiento y rendimiento del servidor virtual, como por ejemplo la memoria RAM y el número de procesadores. La SAN en cambio gestionará el espacio y los volúmenes donde se encuentran las máquinas virtuales. Antes de crear la máquina virtual tenemos que analizar cuantos discos virtuales (técnicamente, unidades de disco) vamos a necesitar para la máquina (ver capítulo siguiente). Una vez definido el número de unidades procedemos a la creación de dichos discos desde la siguiente opción Hyper-V:

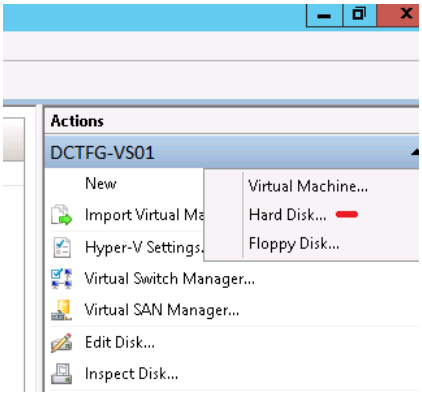


Figura 89

Ubicaremos el disco en la ruta donde vamos a crear la máquina virtual, dentro de la carpeta "*C:\ClusterStorage\VolumeX\MaquinaVirtual*". Hay que tener también en cuenta evitar si es posible crear discos con espacio dinámico. Dejar que el sistema aumente de forma automática el espacio del disco puede ocasionar algunos problemas de espacio en el futuro. Es aconsejable asignar un espacio fijo inicial y luego ir ampliándolo a medida que sea necesario.

Los pasos siguientes para crear una máquina virtual son sencillos [26]. Podemos asignar valores genéricos los cuales podremos cambiar más tarde en función del tipo de máquina virtual a crear. Lo único que sí tenemos que tener en cuenta es asignar los discos que hemos creado previamente:

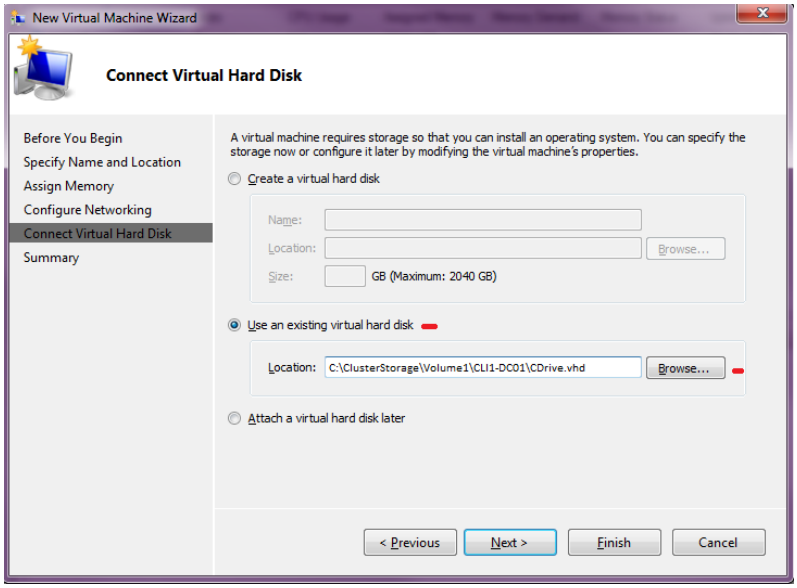


Figura 90

10.2.1 Recursos para máquina virtual controladora de dominio

Los requisitos para un controlador de dominio virtual no son muy exigentes. Estos serían los parámetros básicos:

- Memoria: 2040 MB
- Procesadores: 1
- Discos: dos VHD, un para la unidad C: y otro para la E:

Espacio inicial de las unidades de disco virtuales:

- Unidad C: 50GB
- Unidad E: 50GB

En la página siguiente podemos ver un ejemplo de configuración para el controlador de dominio de un supuesto cliente, CLI1-DC01:

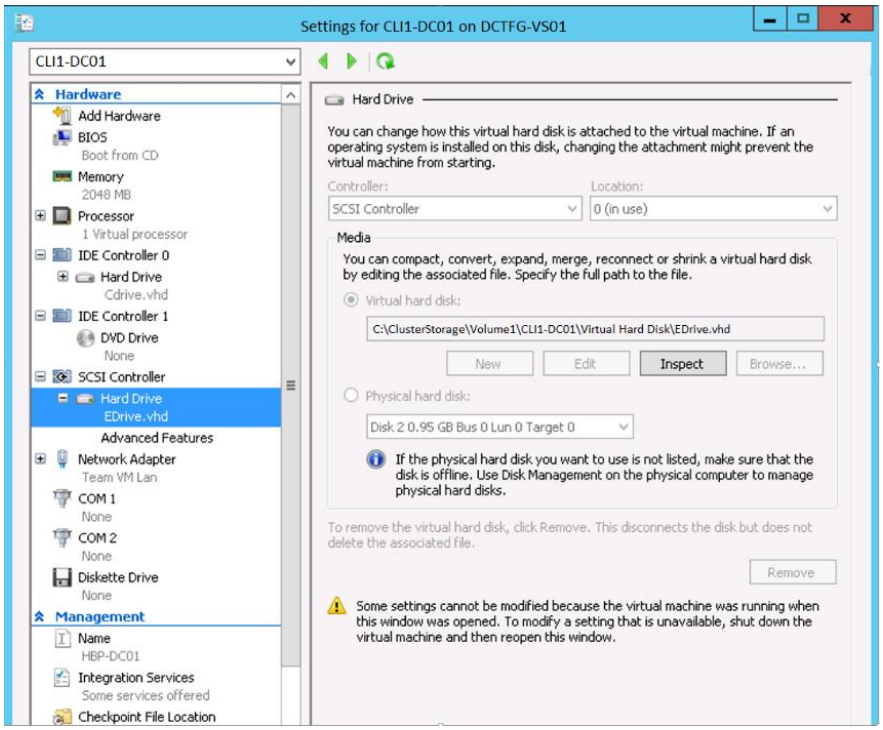


Figura 91

10.2.2 Recursos para máquina virtual servidor de aplicaciones

Para el servidor de aplicaciones, debemos partir de una configuración estándar pero en este caso, tendremos que ir cambiándolas en función de las aplicaciones que vamos a instalar en el servidor. Estas aplicaciones pueden ser más o menos exigentes y requerirán ampliar tanto el espacio del disco como la memoria y los procesadores. Será similar a la configuración del servidor controlador de dominio:

- Memoria: 2040 MB
- Procesadores: 1
- Discos: dos VHD, un para la unidad C: y otro para la E:

Espacio inicial de las unidades de disco virtuales:

- Unidad C: 50GB
- Unidad E: 50GB

10.2.3 Recursos para máquina virtual servidor de correo electrónico

Para el servidor de correo electrónico (Exchange) tenemos que definir unos parámetros un poco más exigentes. Este tipo de servidores suelen tener una carga alta en proceso, por lo tanto el número de procesadores y la memoria RAM juegan un papel importante a la hora de crearla. Esta podría ser una configuración base para un servidor de correo Exchange:

- Memoria: 8192 MB
- Procesadores: 4
- Discos: tres *VHD*, un para la unidad C: (Sistema), otro para la F: (Bases de datos) y otra unidad Q: (Cola de correo).

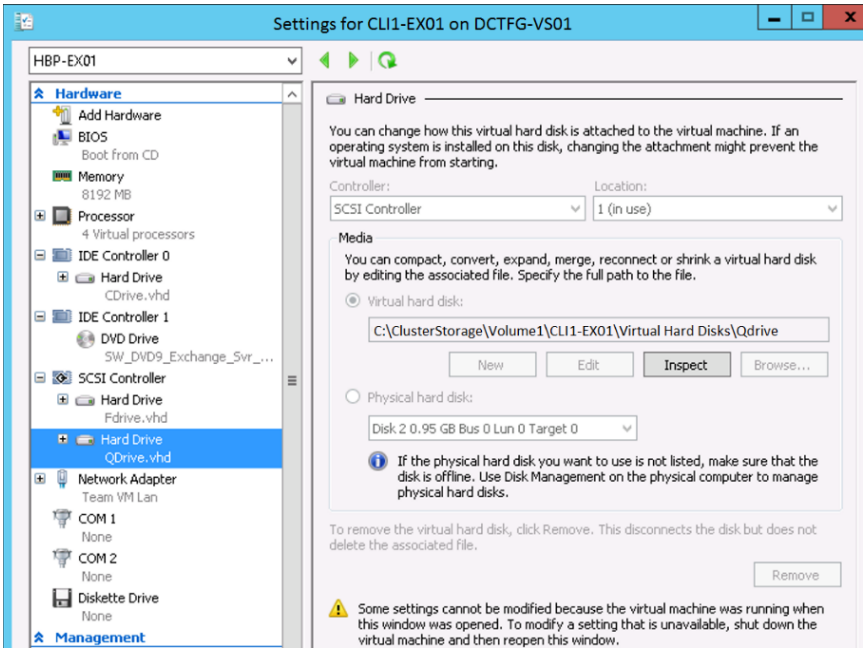


Figura 92

El espacio inicial que podemos asignar para las unidades virtuales (*VHD*) pueden ser los siguientes:

- Unidad C: 50GB
- Unidad F: 200GB
- Unidad Q: 10GB

10.3. Configuración de red para las máquinas virtuales y servidores Hyper-V

En el apartado 6.4 se habla de la configuración de los *Fortigates*. Es allí donde se definen los *VDOM* y los rangos *IP* de los clientes:

Nombre VDOM	IP	Descripción
Oficina1	10.10.10.X	Futura oficina remota
Oficina1	10.10.11.X	Futura oficina remota administración
Cliente1	10.10.20.X	Futuro cliente remoto
Cliente1	10.10.21.X	Futuro cliente remoto administración
...	10.10.30.X	... etc.

En lo servidores Hyper-V tenemos en principio 4 puertos Ethernet Gigabit y dos 2 puertos 10GB iSCSI para conectar con la SAN. Esta sería la configuración real de las tarjetas de red en un nodo del servidor Hyper-V:

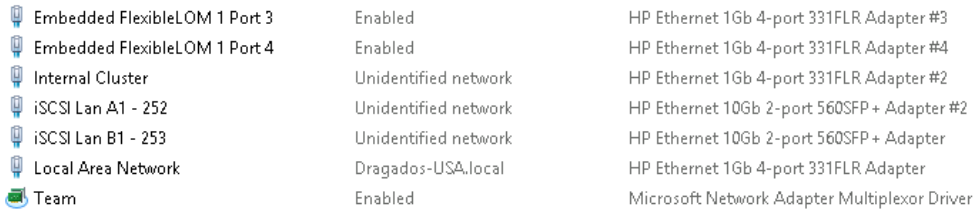


Figura 93

Podemos distinguir perfectamente las 4 tarjetas de red 1Gb:

- Embedded FlexibleLOM 1 Port 3 (NIC #3)
- Embedded FlexibleLOM 1 Port 4 (NIC #4)
- Internal Cluster (NIC #2)
- Local Area Network (NIC #1)

Y las dos tarjetas iSCSI 10Gb:

- iSCSI Lan A1 – 252 (NIC #2)
- iSCSI Lan B1 – 253 (NIC #1)

Team indica que existe la unificación de varias tarjetas de red en una para obtener mejor rendimiento. En concreto se han unido en "*teaming*" las tarjetas:

- Embedded FlexibleLOM 1 Port 3 (NIC #3)
- Embedded FlexibleLOM 1 Port 4 (NIC #4)

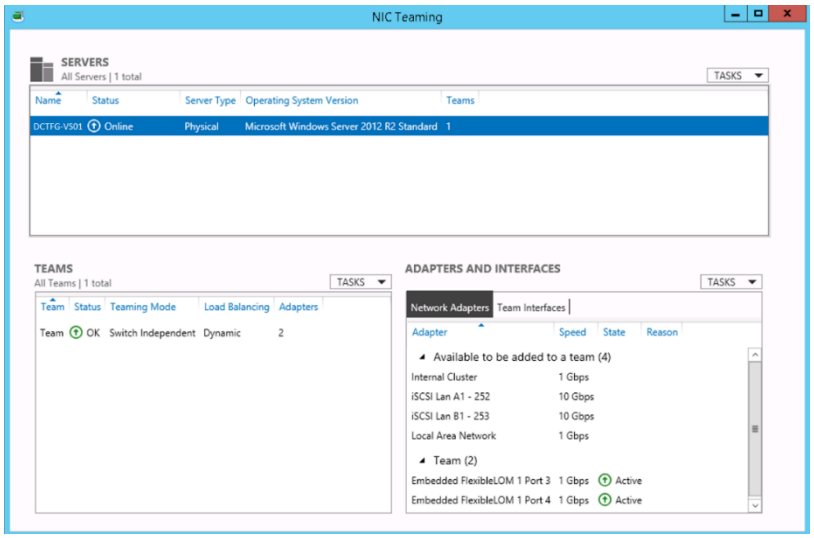


Figura 94

Esta unión de tarjetas será el canal principal donde irá todo el tráfico generado por las máquinas virtuales. Para definir el entorno de red de las máquinas virtuales tenemos que definir un "*Virtual Switch*" [27]. Un "*Virtual Switch*" no es más que un conmutador o switch por software el cual se encarga de gestionar el tráfico de las máquinas virtuales desde Hyper-V. Este "*Virtual Switch*" también puede crear y gestionar diferentes *VLANs*, necesario para definir la separación de tráfico de red para oficinas o clientes que están alojados en la infraestructura.

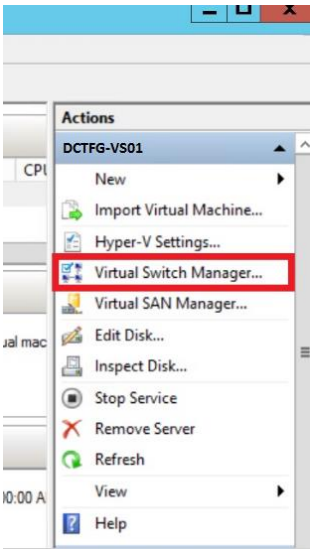
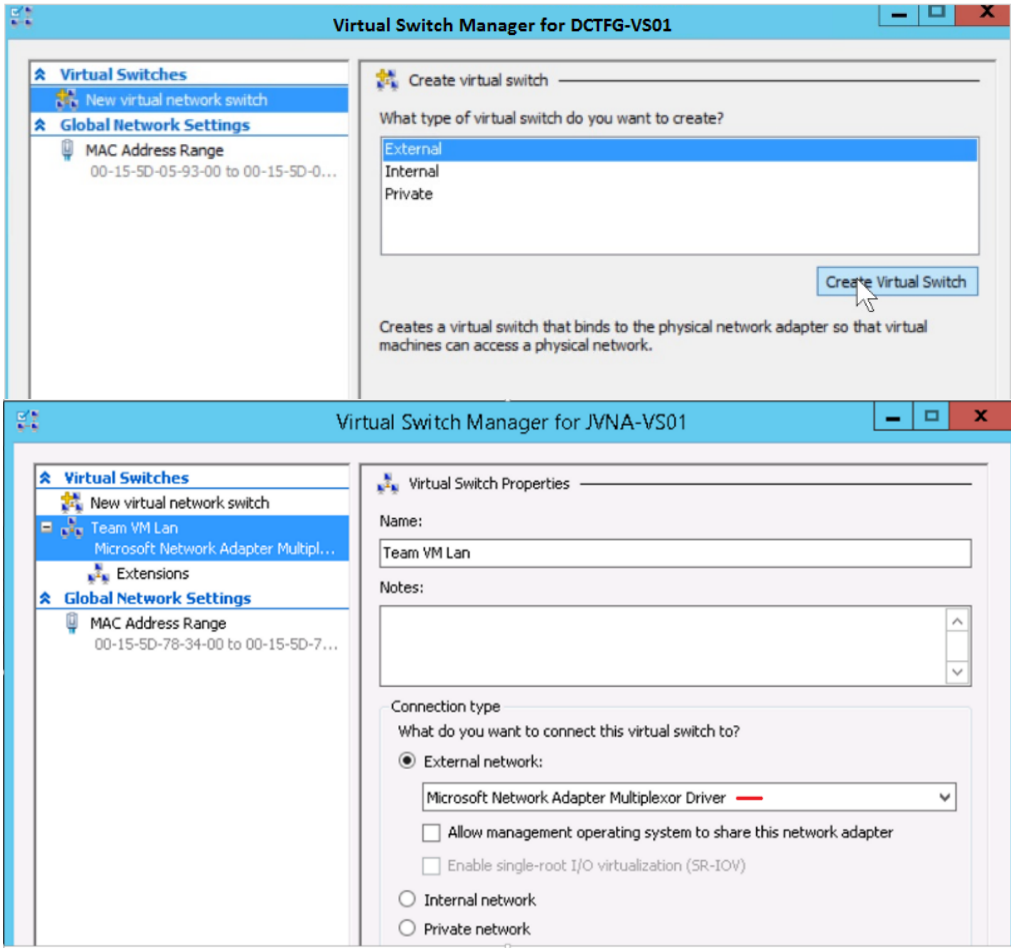


Figura 95

El tipo de "*Virtual Switch*" será "*External*" y lo vincularemos con el "*Team*" de *NICs* que hemos comentado antes, llamado por defecto "*Microsoft Network Adapter Multiplexor Driver*":

Figura 96



Finalmente, esta sería la configuración de las tarjetas:

DCTFG-VS01

Nombre Tarjeta	IP	Velocidad	NIC	Notas
Embedded FlexibleLOM 1 Port 3	10.1.1.22	1Gb	NIC #3	Tarjetas en modo "Teaming"
Embedded FlexibleLOM 1 Port 4	10.1.1.32	1Gb	NIC #4	
Internal Cluster	10.1.1.201	1Gb	NIC #2	Gestión Hyper-V Cluster
Local Area Network	10.1.1.42	1Gb	NIC #1	Conexión Red Datos (Internet)
iSCSI LAN A1	172.1.1.10	10Gb	SFP #2	Conexión iSCSI con la SAN Módulo 1
iSCSI LAN B1	172.1.1.20	10Gb	SFP #1	Conexión iSCSI con la SAN Módulo 2

DCTFG-VS02

Nombre Tarjeta	IP	Velocidad	NIC	Notas
Embedded FlexibleLOM 1 Port 3	10.1.1.23	1Gb	NIC #3	Tarjetas en modo "Teaming"
Embedded FlexibleLOM 1 Port 4	10.1.1.33	1Gb	NIC #4	
Internal Cluster	10.1.1.202	1Gb	NIC #2	Gestión Hyper-V Cluster
Local Area Network	10.1.1.43	1Gb	NIC #1	Conexión Red Datos (Internet)
iSCSI LAN A1	172.1.1.30	10Gb	SFP #2	Conexión iSCSI con la SAN Módulo 1
iSCSI LAN B1	172.1.1.40	10Gb	SFP #1	Conexión iSCSI con la SAN Módulo 2

11. Servidores virtuales de correo electrónico

El correo electrónico es quizás el servicio más crítico que tendremos que ofrecer dentro de nuestra infraestructura. Por eso se dedica un capítulo completo a su análisis y configuración. Los servidores de correo que vamos a analizar están basados en *Windows Server 2012 R2* y *Microsoft Exchange 2013*.

11.1. Dominio y registros DNS públicos

Antes de comenzar la instalación del servidor de correo es necesario tener claros los dominios que vamos a utilizar, tanto el principal como aquellos necesarios para cualquier otra aplicación o servicio que vayamos a ofrecer. Cada caso es diferente y puede ser más o menos complejo, por lo tanto se analizarán los registros básicos para que el servicio de correo y web funcionen. En función del proveedor de servicios de dominios que elijamos, la forma de añadir o modificar estos registros puede variar (aunque los registros serán los mismos).

Por otro lado, necesitaremos tener direcciones *IP* públicas libres para asignarlas a cada proyecto. Para ello tendremos que solicitarlas a *ARIN, American Registry for Internet Numbers*, la cual será la encargada de suministrarnos las direcciones *IP IPv4* o *IPv6* públicas que necesitemos: www.arin.net. Vamos a considerar la configuración de un cliente llamado, *Cliente1*, con dominio: *cliente1.com*

Una vez tengamos elegido la empresa para registrar nuestro dominio, buscaremos dentro la configuración las opciones para la zona DNS.

Registros tipo A (A RECORD)

- *Autodiscover*, apuntando a IP pública, por ejemplo, 211.23.2.123
- *OWA*, apuntando a la misma IP pública, 211.23.2.123
- *smtp, apuntando a IP Pública del Firewall DCTFG-FW01, Proveedor 1*

Registros tipo MX (MX RECORD)

- @, apuntando a smtp.cliente1.com

Registros tipo TXT SFP (TXT RECORD)

- @, v=sfp1 mx ptr (IP Firewall)
  Esta configuración sirve para confirmar la legitimidad del servidor que está enviando los correos con este dominio, y así evitar falsificaciones de envío con este dominio.

Registros tipo SRV (SRV RECORD)

- *_autodiscover_*
  Protocolo: _tcp,
  Nombre: @,
  Destino: owa.cliente1.com
  De esta forma creamos un acceso desde Internet al correo OWA del cliente.

Llegados a este punto tendríamos los registros básicos necesarios para configurar el correo electrónico con acceso *OWA* desde Internet.

11.2. Barracuda SPAM como entrada y salida del correo electrónico

Todo el tráfico de correo electrónico pasará por el Barracuda Spam Firewall DCTFG-BA02. Esto quiere decir que tenemos que crear una regla en el firewall DCTFG-FW01 que permita el tráfico *smtp* desde y hacia el Barracuda Spam Firewall, como por ejemplo la siguiente:

```
static (inside,outside) tcp 211.23.2.123 smtp 10.1.1.18 smtp netmask 255.255.255.0
```

Una vez que todo el correo sea dirigido hacia DCTFG-BA02 tendremos que crear los diferentes dominios tal y como se ha indicado en el *Capítulo 6.5.1.1.*

11.3. Instalación de Windows Server 2012 y roles

Una vez instalado el sistema operativo tal y como hemos realizado para otros servidores (ver *Anexo, Capítulo 16.1*), procederemos a la selección de los roles necesarios para Exchange [28]. Esta vez vamos a instalar los roles utilizando *PowerShell* ya que de esta forma es más sencillo instalarlos de una sola vez así como sus componentes necesarios. Es importante comprobar que la versión 4.5 de *.NET* está instalada o la instalamos desde la gestión de roles del servidor.

Abrimos una consola *PowerShell* como administrador y primero procedemos a instalar *RSAT-ADDS*:

```
Install-WindowsFeature RSAT-ADDS
```

El siguiente paso es instalar los roles, pero antes importaremos el módulo *ServerManager*:

```
Import-Module ServerManager
```

Procedemos a instalar los siguientes roles:

```
Install-WindowsFeature AS-HTTP-Activation, Desktop-Experience, NET-Framework-45-Features, RPC-over-HTTP-proxy, RSAT-Clustering, RSAT-Clustering-CmdInterface, Web-Mgmt-Console, WAS-Process-Model, Web-Asp-Net45, Web-Basic-Auth, Web-Client-Auth, Web-Digest-Auth, Web-Dir-Browsing, Web-Dyn-Compression, Web-Http-Errors, Web-Http-Logging, Web-Http-Redirect, Web-Http-Tracing, Web-ISAPI-Ext, Web-ISAPI-Filter, Web-Lgcy-Mgmt-Console, Web-Metabase, Web-Mgmt-Console, Web-Mgmt-Service, Web-Net-Ext45, Web-Request-Monitor, Web-Server, Web-Stat-Compression, Web-Static-Content, Web-Windows-Auth, Web-WMI, Windows-Identity-Foundation
```

Una vez terminada la instalación reiniciaremos el servidor.

11.4. Instalación Microsoft Exchange 2013

En este punto comenzaremos la instalación de Exchange 2013. El primer paso es instalar todos los requisitos que son los siguientes [28]:

1. Microsoft Unified Communications Managed API 4.0, Core Runtime 64-bit
2. Microsoft Office 2010 Filter Pack 64 bit
3. Microsoft Office 2010 Filter Pack SP1 64 bit

El siguiente paso será preparar el *AD* para Exchange desde *PowerShell* (en "*OrganizationName*" tendremos que poner el nombre de nuestra organización, por ejemplo *Cliente1*:

```
.\setup /Preparead /IAcceptExchangeServerLicenseTerms /OrganizationName:"Cliente1"
```

Ahora ya podemos comenzar la instalación de Exchange desde el "*Setup*" de la imagen del disco principal de instalación. Es bastante sencilla, sólo tendremos en cuenta activar la opción "*No*" cuando pregunte si queremos instalar alguna opción Anti-Malware. Consultar la *Bibliografía* para obtener más información de cómo realizar la instalación de Exchange.

11.4.1. Configuración del gestor de colas

Antes en la máquina virtual hemos definido una unidad con 10GB de tamaño llamada "*Q:*". Esta unidad será la encargada de almacenar temporalmente los mensajes que están en cola

de ser procesados por Exchange. Los mensajes no suelen estar demasiado tiempo en esta unidad por lo tanto un tamaño de 10GB es suficiente en principio para gestionarla. Es importante realizar una buena configuración inicial ya que uno de los errores más comunes en Exchange puede venir por un tamaño demasiado bajo asignado a esta unidad. Tampoco conviene asignarle un tamaño alto, ya que sería malgastar el espacio limitado que tenemos en la SAN y además esta unidad para las colas suele estar la mayor parte del tiempo vacía.

Moveremos la base de datos a la unidad "*Q:*" [29]. Para realizarlo utilizaremos de nuevo PowerShell con el siguiente comando:

```
Move-TransportDatabase.ps1 -queueDatabasePath 'Q:\Exchange\TransportRoles\data\Queue' -
queueDatabaseLoggingPath 'Q:\Exchange\TransportRoles\data\Queue' -iPFilterDatabasePath
'Q:\Exchange\TransportRoles\data\IpFilter' -iPFilterDatabaseLoggingPath
'Q:\Exchange\TransportRoles\data\IpFilter' -temporaryStoragePath
'Q:\Exchange\TransportRoles\data\Temp'
```

11.4.2. Preparación de las bases de datos

Por defecto *Microsoft Exchange* instala en la unidad "*C:"* las bases de datos durante el proceso de instalación y al igual que pasaba con la base de datos de la cola, tendremos que mover la base de datos creada por defecto a la unidad "*F:*" (que será donde establezcamos todas las bases de datos para el correo) [29].

La base de datos principal creada por defecto se llama "*Mailbox Database 01*". Para cambiarla a la unidad "*F:*" tenemos que ejecutar el siguiente comando *PowerShell*:

```
Move-DatabasePath "Mailbox Database 01" -EdbFilePath "F:\Exchange\Database\MDB01\MDB01.edb" -
LogFolderPath "F:\Exchange\Database\MDB01"
```

Una vez ya tenemos la base de datos principal ubicada en la unidad "*F:*" procederemos a la creación de resto de bases de datos [30]. Ejecutaremos los siguientes comandos *PowerShell*, uno por cada base de datos (para el servidor de Exchange CLI1-EX01):

```
New-MailboxDatabase -Server CLI1-EX01 -Name "Mailbox Database 02" -EdbFilePath
"F:\Exchange\Database\MDB02\MDB02.edb" -LogFolderPath "F:\Exchange\Database\MDB02"

New-MailboxDatabase -Server CLI1-EX01 -Name "Mailbox Database 03" -EdbFilePath
"F:\Exchange\Database\MDB03\MDB03.edb" -LogFolderPath "F:\Exchange\Database\MDB03"

New-MailboxDatabase -Server CLI1-EX01 -Name "Mailbox Database 04" -EdbFilePath
"F:\Exchange\Database\MDB04\MDB04.edb" -LogFolderPath "F:\Exchange\Database\MDB04"

New-MailboxDatabase -Server CLI1-EX01 -Name "Mailbox Database 05" -EdbFilePath
"F:\Exchange\Database\MDB05\MDB05.edb" -LogFolderPath "F:\Exchange\Database\MDB05"
```

Para terminar, ahora que las bases de datos ya están ubicadas definitivamente en la unidad "*F:*" es el momento de aplicar algunos parámetros de configuración pero además podemos añadir otros como por ejemplo la cuota máxima o la política de retención. En el ejemplo podemos ver algunos de estos nuevos parámetros como una cuota máxima de 1GB o una política de retención para los elementos borrados de 3 días y el aviso de cuota al límite al 0,9GB [31]:

```
Get-MailboxDatabase | Set-MailboxDatabase -CircularLoggingEnabled $true -MailboxRetention 15 -
OfflineAddressBook "\Default Offline Address Book" -DeletedItemRetention 3.00:00:00

Get-MailboxDatabase | Set-MailboxDatabase -IssueWarningQuota 0.9Gb -ProhibitSendQuota 1Gb -
ProhibitSendReceiveQuota Unlimited
```

11.4.3. Conector "*Journaling*" Barracuda Archiver

"*Journaling*" es el proceso de almacenamiento de correos en un *Barracuda Archiver*. Para lograr que todos los correos se almacenen será necesario tener configurado un conector especial (ver *Capítulo 6.6.1*). Una vez abierta la consola añadimos el dominio remoto utilizando un nombre de dominio falso llamado "*bma.int*" que servirá como base de la configuración [32]:

```
New-RemoteDomain -DomainName bma.int -Name "Message Archiver Domain"
```

El siguiente paso consistirá en activar el "*auto-forwarding*":

```
Get-RemoteDomain | Where {$ .DomainName -eq "bma.int"} | Set-RemoteDomain -
TNEFEnabled $false -AutoForwardEnabled $true
```

Finalmente verificaremos la configuración con el siguiente comando:

```
Get-RemoteDomain | Where {$_.DomainName -eq "bma.int"} |Format-table Name, DomainName, TNEFEnabled,
AutoForwardEnabled
```

La siguiente fase de la instalación la realizaremos desde el centro de administración de Exchange, al cual podemos acceder desde la siguiente URL:

https://localhost/owa

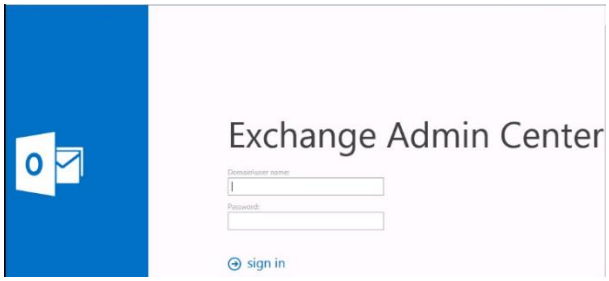


Figura 97

Comenzaremos creando un contacto que será el encargado de re direccionar los correos desde el dominio falso que hemos creado antes:

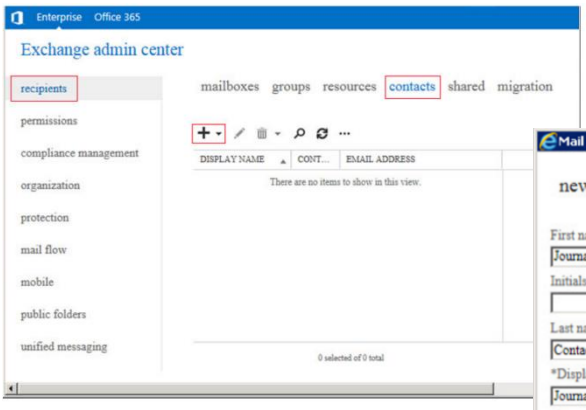


Figura 98

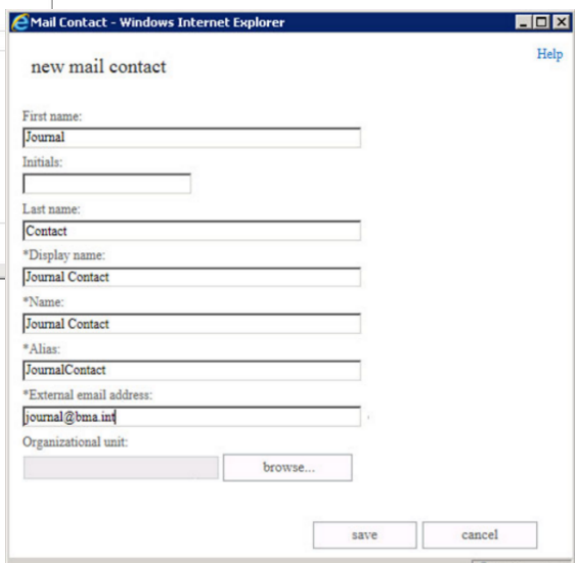


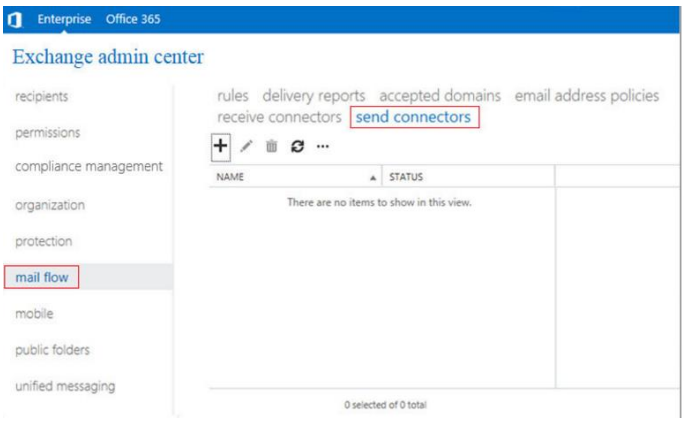
Figura 99

Es conveniente eliminar el contacto de la lista de direcciones, podemos realizarlo con el siguiente comando:

```
Get-MailContact | Where {$_.Name -eq "Journal Contact"} | Set-MailContact -HiddenFromAddressListsEnabled $True
```

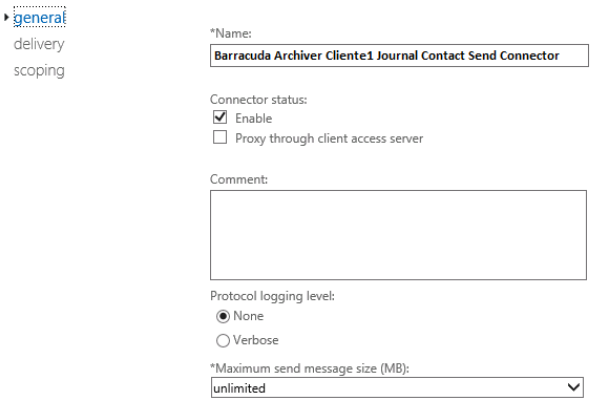
Ahora procederemos a la creación de un conector de envío con el nombre "*Barracuda Archiver Cliente1 Journal Contact Send Connector*":

Figura 100



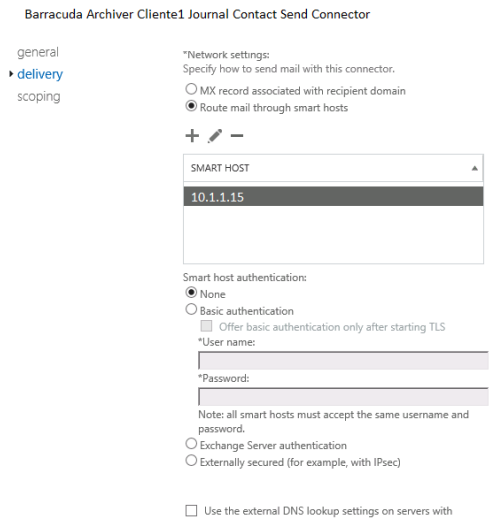
La configuración paso a paso del conector está explicada en detalle en la *Bibliografía*[33][34]. Estos son los parámetros que aparecerán en la configuración del conector una vez creado:

Figura 101



En la siguiente pantalla asignaremos la IP del "*Smart Host*" con la dirección del Barracuda Archiver:

Figura 102



En el siguiente paso indicaremos el dominio falso que hemos creado y el protocolo *SMTP*. Luego se añade el nombre del servidor de correo Exchange:

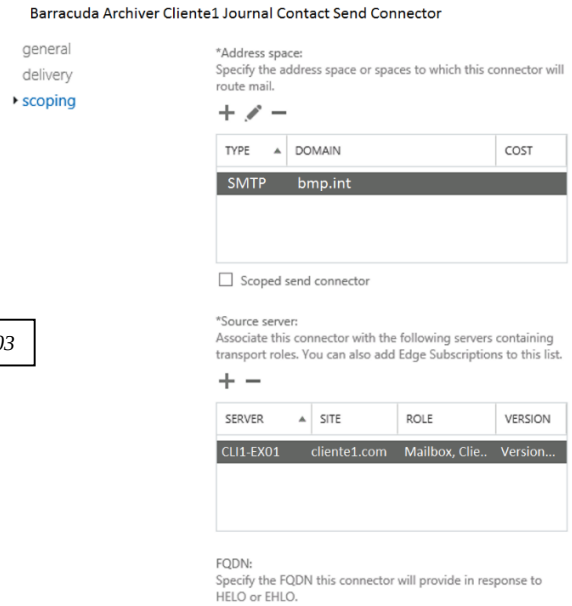


Figura 103

Ya tenemos creado el conector de "*Journaling*" que enviará todos los correos de los dominios que creemos al *Barracuda Archiver* para su posterior archivo.

11.4.4. Conectores Exchange para recepción ("*receive connectors*")

Detalle de todos los conectores necesarios de recepción [33]:

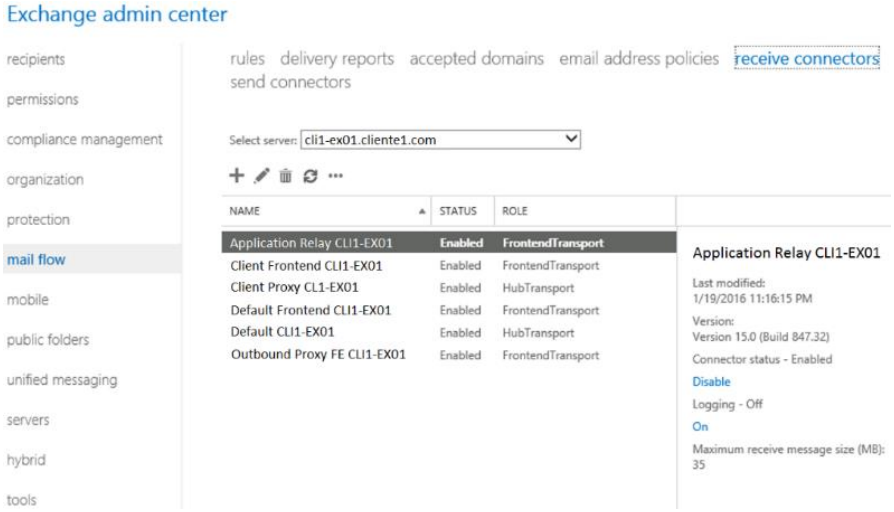


Figura 104

Application Relay CLI1-EX01: este conector se encarga de autorizar las redes o las *IP* que podrán enviar correos a través del servidor de correo. Hemos autorizado las redes de la oficina del C*liente1* con un rango IP 10.10.11.*X*. En el apartado "*Network adapter bindings*" aparece una nueva dirección IP, ya que la dirección del servidor Exchange de cliente1 es

10.10.10.25 y aquí podemos ver la 10.10.10.26. Previamente en el servidor de Exchange tendremos añadir esta dirección 10.10.10.26 como *IP* secundaria al adaptador principal.

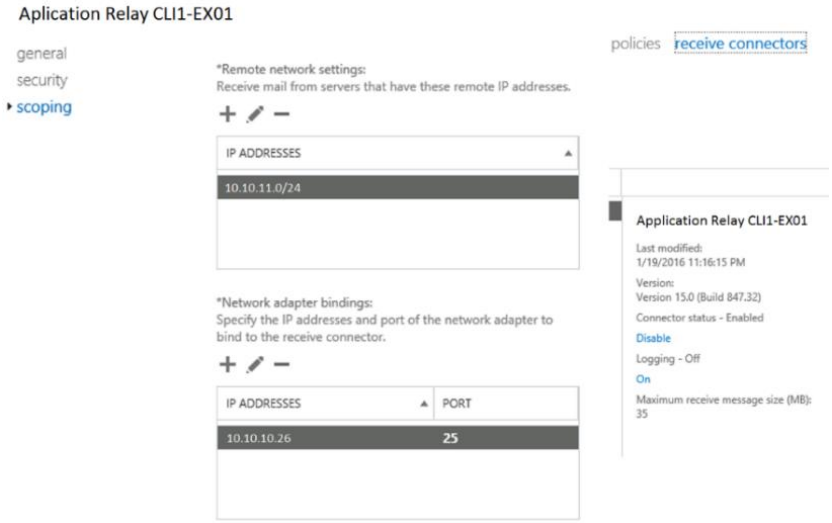


Figura 105

Client Frontend CLI1-EX01: este conector acepta conexiones seguras TLS. La configuración "*scoping*" sería la siguiente (el resto se deja por defecto):

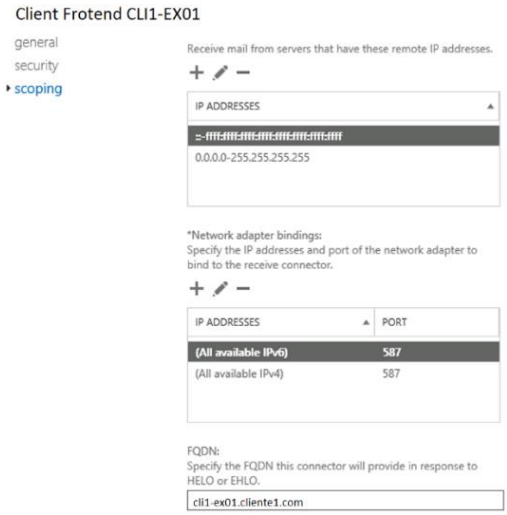


Figura 106

Client Proxy CLI1-EX01: conector proxy del servidor Exchange para correo entrante, configuración "*scoping*":

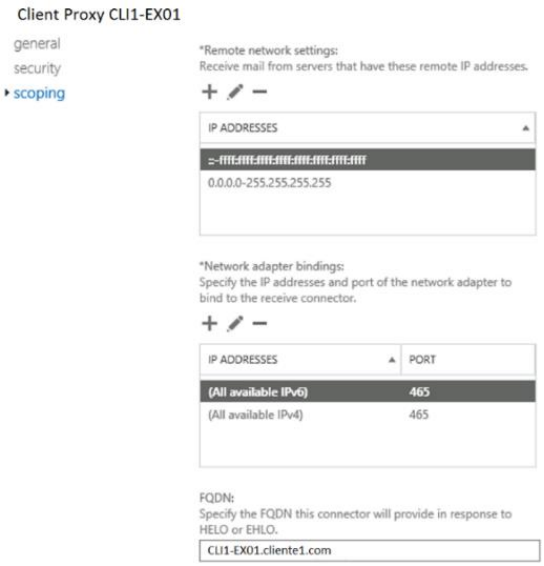


Figura 107

Default Frontend CLI1-EX01: conector frontend acepta las conexiones desde *SMTP* a través del puerto 25. Es el punto principal de entrada de mensajes. La configuración "*scoping*" sería la siguiente:

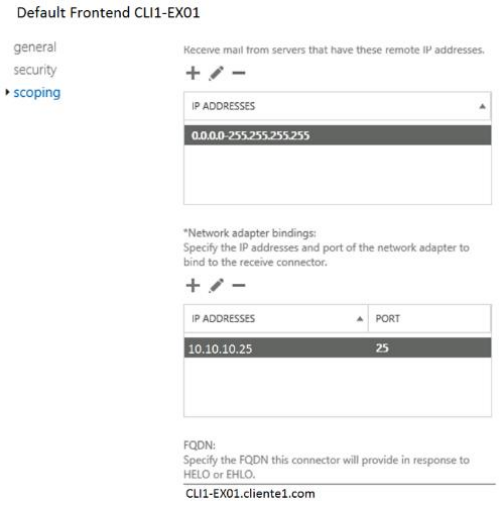


Figura 108

Default CLI1-EX01: *CAS* (*Client Access Service*) y *MBX* (*Mailbox*) están en el mismo servidor, por lo tanto el conector para el servicio de transporte escuchará a través del puerto 2525 en vez del puerto 25. Estos dos servicios no pueden escuchar por el mismo puerto:

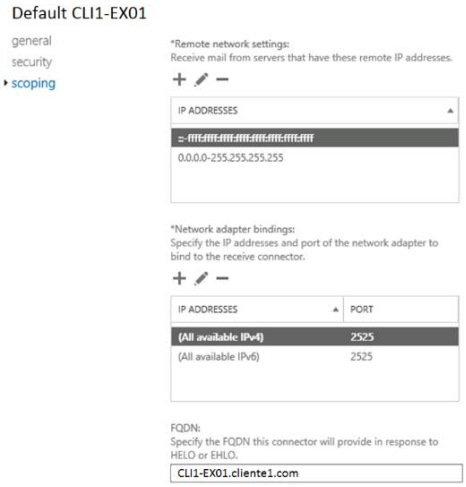


Figura 109

Outbound Proxy Frontend CLI1-EX01: conexión a través del puerto 717 que conecta el servicio de transporte con el servicio *FET* (*Frontend Transport Service*). Se utiliza para enviar los correos a través de este *relay* en vez de hacerlo directamente hacia Internet:

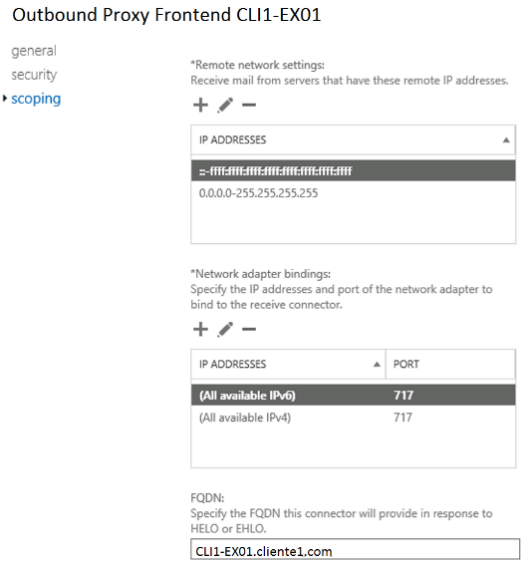


Figura 110

11.4.5. Conectores Exchange para envío "*send connectors*"

Listado general de conectores de envío [34]:

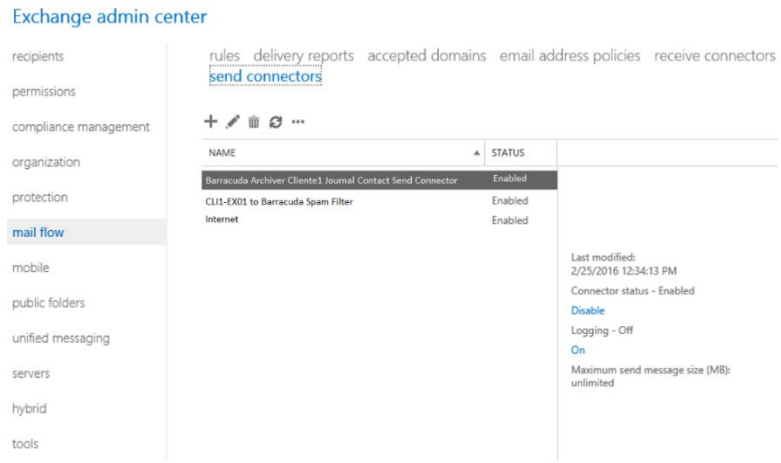


Figura 111

Barracuda Archiver Cliente1 Journal Contact Send Connector: explicado en el *Capítulo 11.4.3*

CLI1-EX02 to Barracuda Spam Filter: con este conector definimos que todo el correo saliente pase a través del Barracuda Spam Firewall. A continuación se detallan las tres opciones de configuración (la IP en la Figura 112 es la *IP* del Barracuda):

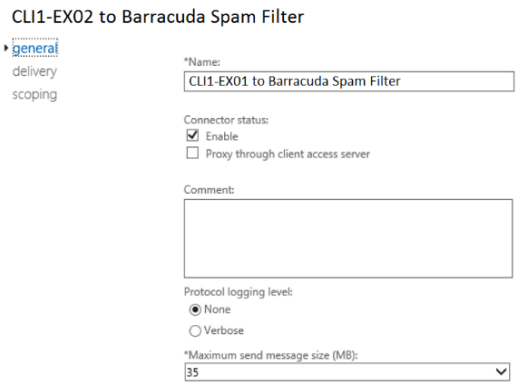


Figura 112

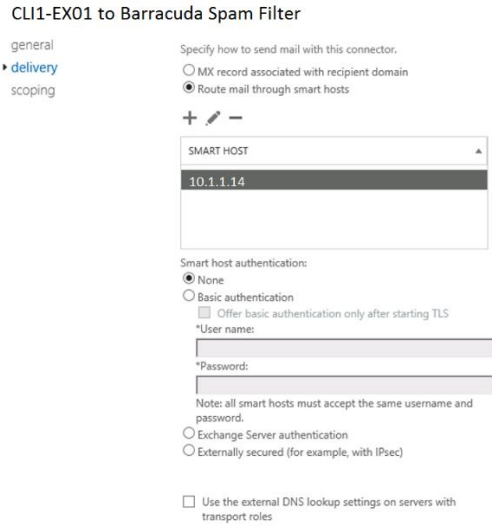


Figura 113

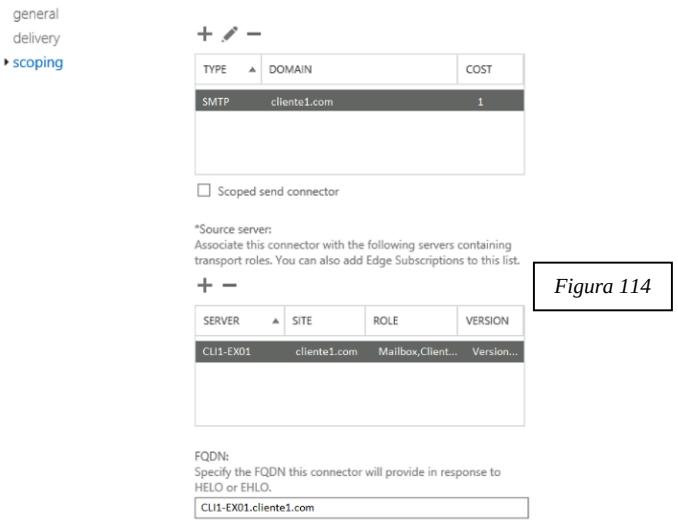


Figura 114

Internet: este es el conector general que envía todo el correo a Internet. También estará conectado con el Barracuda Spam Firewall:

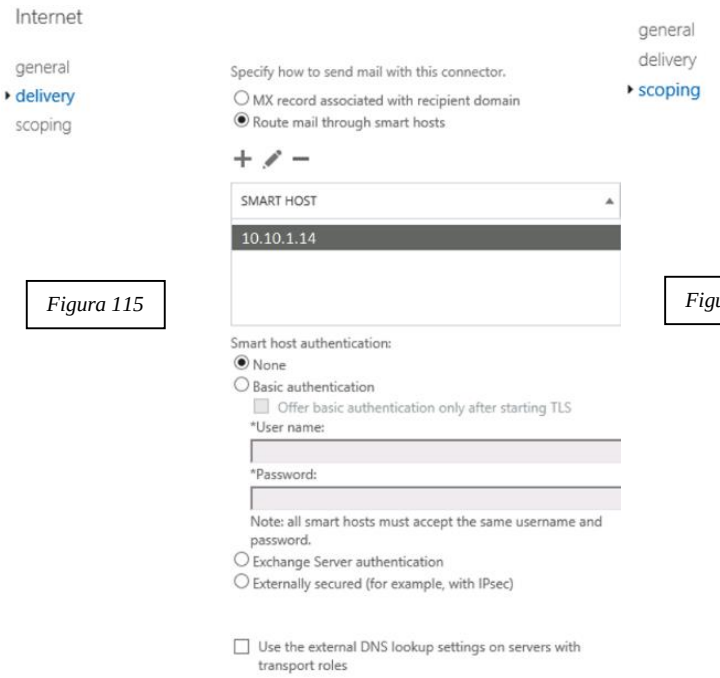


Figura 115

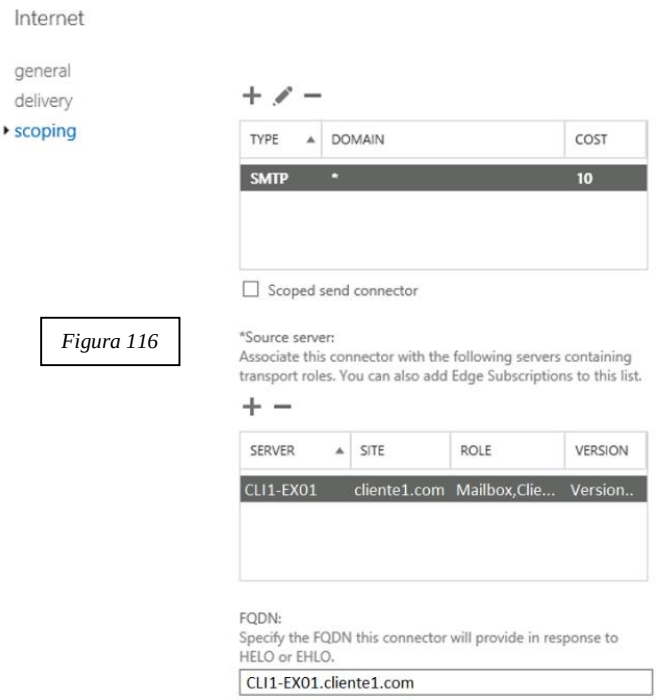


Figura 116

11.5. *DNS* para Exchange

En el servidor *DNS* del cliente, en el caso del ejemplo que hemos seguido hasta ahora sería CLI1-DC01, será necesario añadir algunas configuraciones básicas sobre todo para poder ofrecer el servicio OWA. Las principales son:

- **Foward Lookup Zones**: hay que añadir una nueva zona con el nombre del dominio, *cliente1.com*. Dentro de esta nueva zona será necesario crear un registro tipo "*Host (A)*" con el nombre de "*owa*" y que apunte a la dirección IP del servidor de correo, en el caso de ejemplo sería 10.10.10.25.

- **Reverse Lookup Zones:** tendremos que crear punteros tipo *PTR* también para owa, owa.cliente1.com apuntando a la *IP* principal del servidor Exchange 10.10.10.25. También hay que incluir la segunda *IP* que hemos definido antes, 10.10.10.16 para que apunte también al servidor de Exchange.

11.6. Certificados digitales

Los certificados digitales son necesarios para que las comunicaciones del correo electrónico sean seguras. Cada cliente tendrá su propio certificado digital para el correo electrónico. Hay que solicitarlo a una entidad autorizada y será tipo "*público*". Fases:

1. *Creación de la petición, CSR (Certificate Signing Request)* [35]. Para poder solicitar un certificado es generar un fichero (*.req*) que enviaremos a la entidad certificadora.

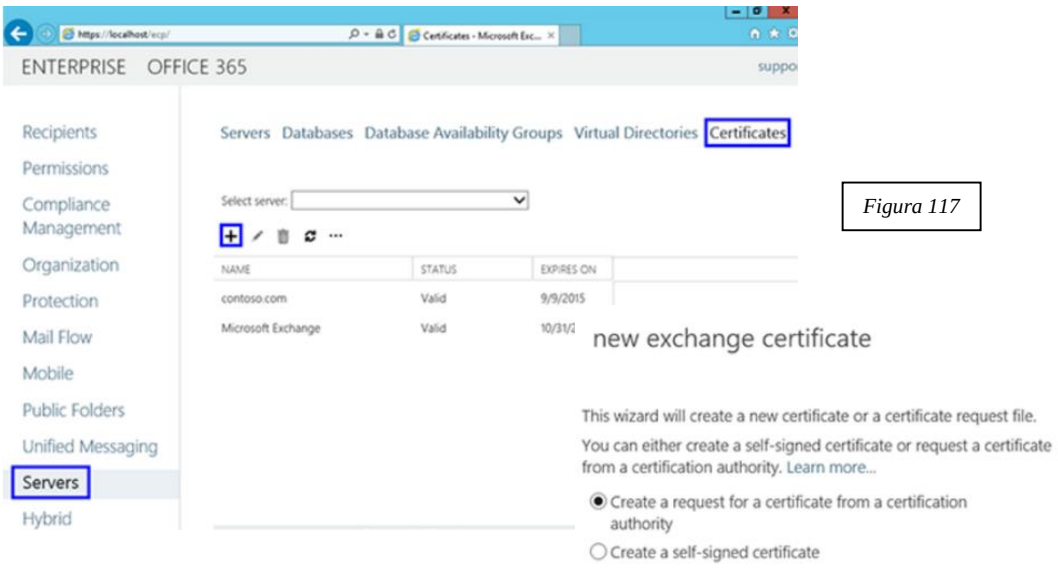


Figura 117

2. *Instalación del certificado*. Una vez tengamos el certificado procederemos a la instalación. Cuando hemos realizado la petición tendremos una entrada en el aparatado "*Certificates*" con la opción "*Pending Request*":

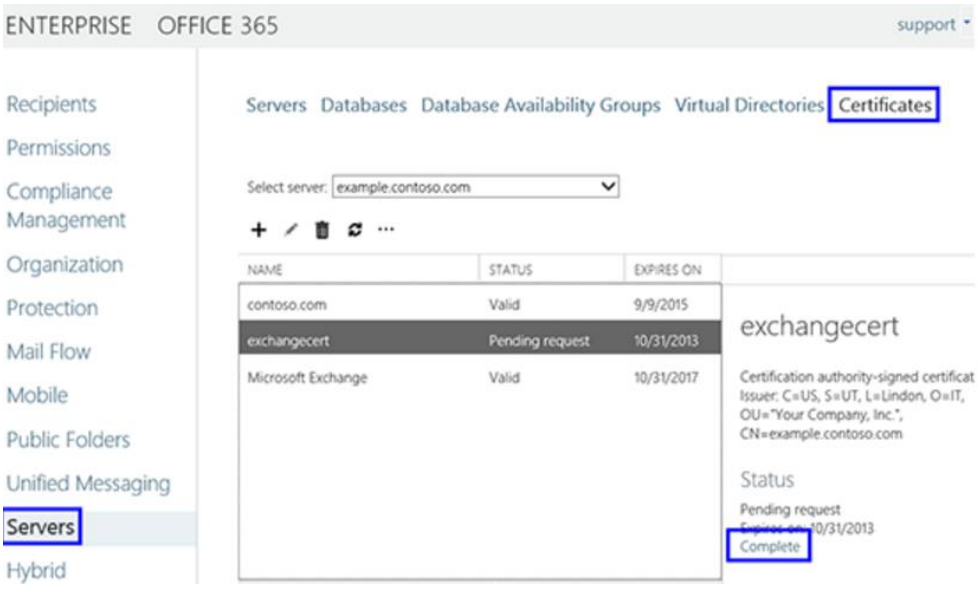


Figura 118

12. Copias de seguridad

12.1. Dispositivos para la copia de seguridad

En el *Capítulo 7.3* se describe la configuración del servidor de backup, la conexión con la librería de cintas y la instalación del software Symantec Backup Exec 15. Este servidor y la librería de cintas no son los únicos dispositivos que tenemos para realizar la copia de seguridad. Vamos a repasar todos los elementos que tenemos disponibles para el backup:

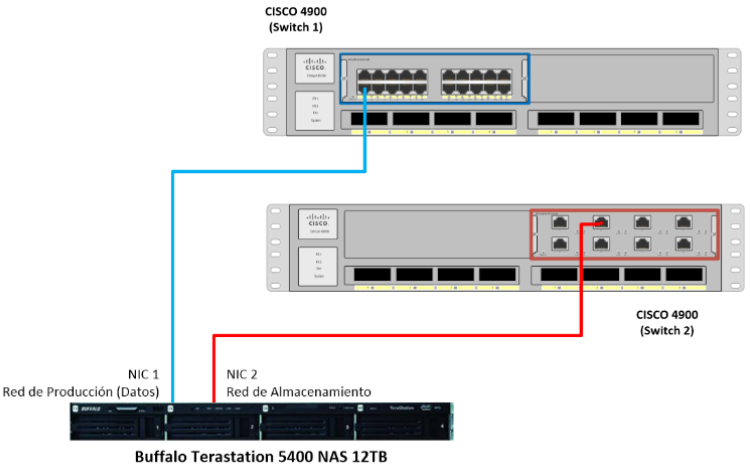
Servidor Backup, DCTFG-BCK01. Software Symantec Backup Exec 15
Librería de cintas, DCTFG-TP01. Cintas LTO6 (2.5TB hasta 6TB comprimidos)
Buffalo Terastation, DCTFG-NS01. 12TB espacio disponible para copia
SAN. Espacio variable para determinadas copias de seguridad

El programa Symantec Backup Exec 15 será el principal encargado de realizar todas las copias de seguridad desde el servidor de backup.

12.2. Preparación Buffalo Terastation.

Antes de programar las copias será necesario definir la localización de las diferentes zonas de almacenamiento. En principio, las copias se almacenarán en el Buffalo Terastation el cual tiene 12TB en repartido en 4 discos de 3TB en modo RAID 5. La conexión a la red del mismo sería la siguiente:

Figura 119



Accederemos desde cualquier ordenador conectado a la red de producción utilizando la herramienta *NAS Navigator2*. Este software nos permitirá identificar el dispositivo y acceder a la configuración. Las credenciales por defecto de acceso son usuario *admin* y contraseña *password.*

El primer paso antes de continuar será conectar el dispositivo a nuestro Directorio Activo. Previamente, habremos creado una cuenta de servicio la cual tendrá acceso a todos los dispositivos de nuestra infraestructura con derechos de administrador.

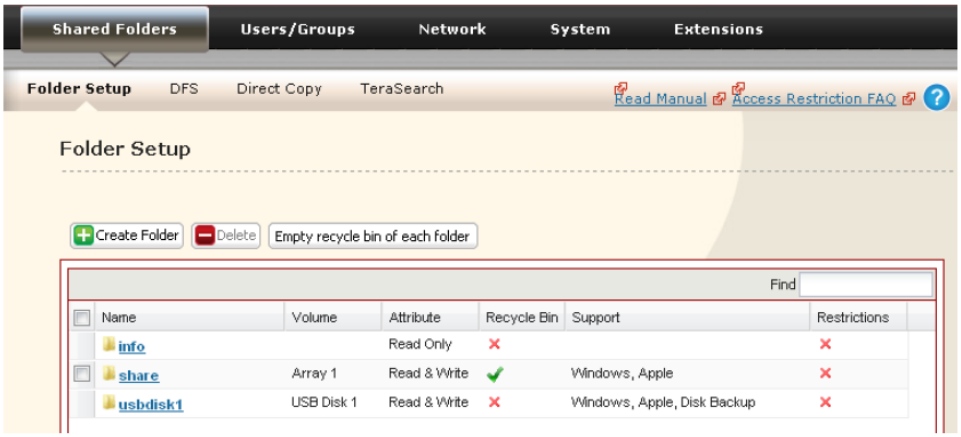
Para activar la conexión al Directorio Activo: *Network -> Workgroup/Domain -> Modify Settings.* En la siguiente pantalla pondremos los datos de acceso al Directorio Activo y la cuenta de backup.

Ahora es el momento de crear las diferentes carpetas [35] en las cuales vamos a volcar la información. Podríamos crear la siguiente estructura de carpetas para cada proyecto:

Nombre	Acceso desde la red	Descripción
DCTFGBackup	\\10.1.1.71\DCTFGBackup	Copia de seguridad elementos de la infraestructura principal incluidas todas las máquinas virtuales (clientes y oficinas)
Cliente1Backup	\\10.1.1.71\Cliente1Backup	Copia de seguridad datos Cliente1
Cliente2Backup	\\10.1.1.71\Cliente2Backup	Copia de seguridad datos Cliente2
Oficina1Backup	\\10.1.1.71\Oficina1Backup	Copia de seguridad datos Oficina1

La carpeta más importante será DCTFGBackup, ya que en ella se almacenarán todas las máquinas virtuales incluidas las que pertenecen a clientes u oficinas. Crearemos la carpeta de la siguiente forma, opción "*Create Folder*":

Figura 120



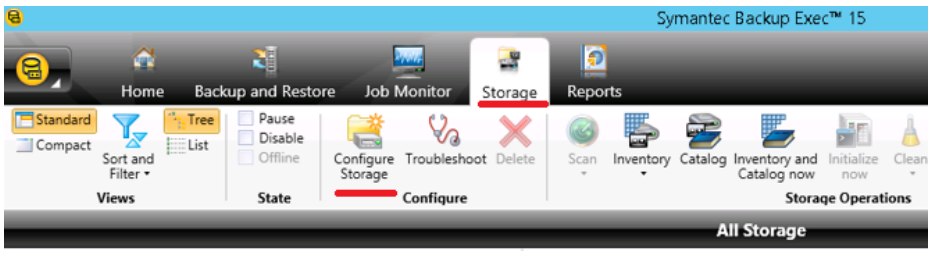
Introduciremos los parámetros básicos como el nombre, descripción, etc. y pulsaremos en "*Access Restrictions*" [35]. Anteriormente ya hemos añadido la configuración con el Directorio Activo, por lo tanto podemos asignar permiso de acceso únicamente a la cuenta que hemos creado para gestionar las copias de seguridad.

12.3. Definición de los lugares de almacenamiento en Symantec Backup Exec

Antes de definir las tareas de backup es necesario tener claro dónde vamos a ubicar los datos que estamos copiando. De momento sólo tendremos dos ubicaciones posibles, el disco *NAS* Buffalo y las cintas LTO6 (explicadas en más detalle en el apartado 12.5.8).

Accederemos a la pestaña "*Storage*" y pulsaremos en la opción "*Configure Storage*":

Figura 121



Elegimos la opción "*Disk-based storage*" (almacenamiento basado en disco) para realizar las copias de seguridad en dispositivos ubicados en la red local [36].

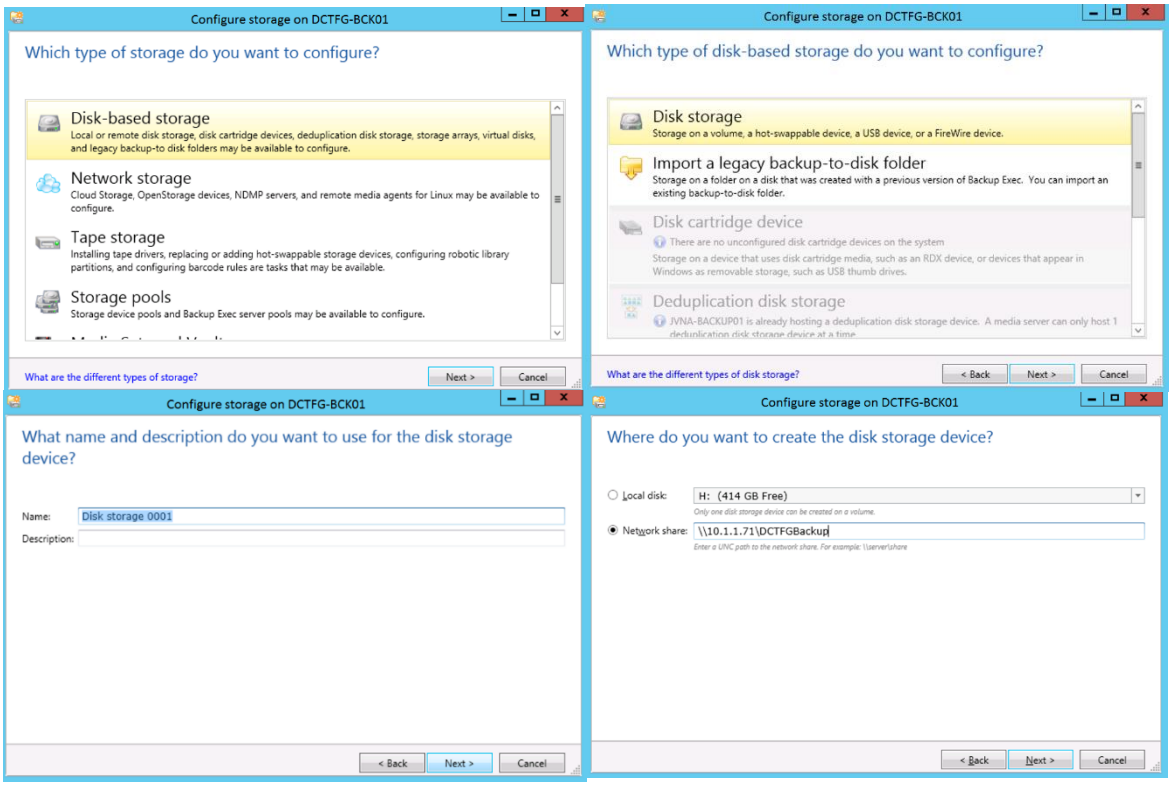


Figura 122

Le daremos un nombre y el último paso consistirá en asignar la dirección IP donde está ubicada la unidad *NAS* con la carpeta correspondiente: *\\10.1.1.71\DCTFGBackup*

Repetiremos estos pasos hasta añadir todas las ubicaciones que vamos a utilizar en los procesos de copia. Finalmente tendremos una colección de ubicaciones a utilizar en cada trabajo de copia:

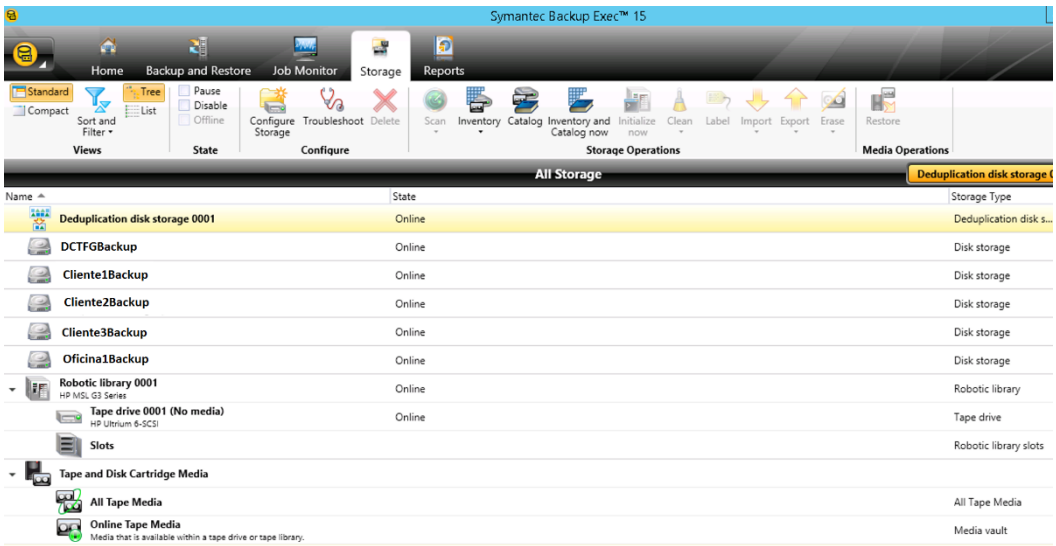


Figura 123

Nota*:* "*Deduplicación*" es un método de optimización de datos utilizado en tiempo real durante la copia de seguridad. Si tenemos esta licencia, esta opción es muy útil para reducir el tamaño final de las copias de seguridad.

12.4. Copia de seguridad de los servidores

Los primeros elementos de los cuales tenemos que realizar copia de seguridad son los dispositivos que integran la infraestructura (servidores físicos). Para ello será necesario instalar los agentes correspondientes *Symantec* en cada uno de ellos [36]:

- *Controlador de dominio, DCTFG-DC01*: 1 Agente Windows
- *Servidor de Backup, DCTFG-BCK01*: 1 Agente Windows
- *Servidores Hyper-V, DCTFG-VS01 y VS02*: 2 Agentes Windows y 2 Agentes Hyper-V

La ventaja de las licencias Hyper-V es que con ellas podemos hacer copia de seguridad de todas las máquinas virtuales que se encuentren alojados en los servidores de virtualización. El primer paso será crear las copias de seguridad de los servidores físicos. Para ello tendremos que crear una tarea de backup por cada uno de ellos:

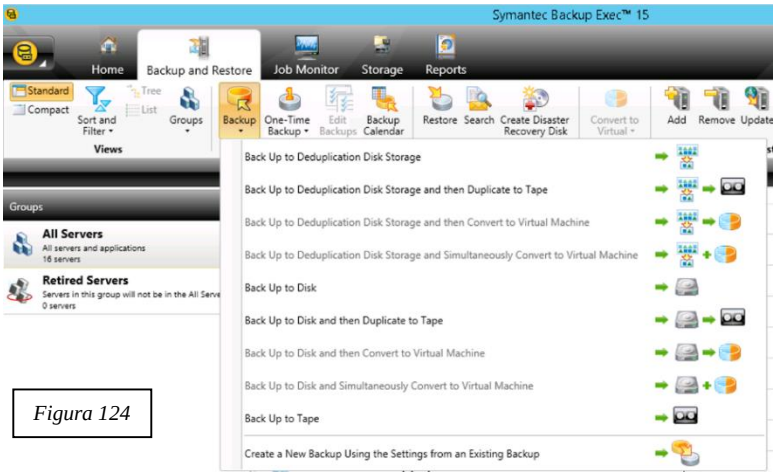


Figura 124

Escogeremos la opción "*Back Up to Disk*". En esta opción definiremos todos los detalles como la dirección IP del servidor que vamos a copiar, qué carpetas necesitamos, el tipo de copia ("full" o "incremental") y la frecuencia de la misma:

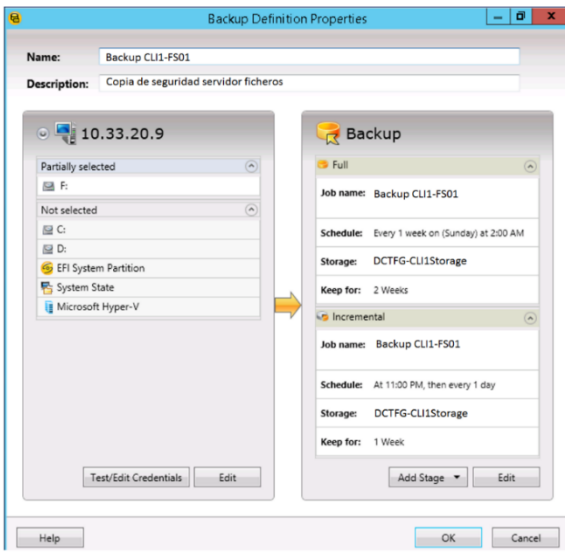


Figura 125

Llegados a este punto tenemos que tener en consideración tres puntos importantes a la hora de crear un trabajo de backup:

1. Tipo de servidor (físico, Hyper-V, máquina virtual, etc.)
2. ¿Son los datos almacenados dinámicos? ¿cambian con frecuencia?
3. Frecuencia de la copia completa y la copia incremental (si es necesario)

Tenemos que prestar especial atención a la hora de definir estos parámetros ya que influyen directamente en el espacio que disponemos para realizar las copias de seguridad. Por ejemplo, para los servidores físicos de la infraestructura no será necesario crear un incremental periódicamente, ya que la información apenas variará en dichos servidores. Para este caso con una copia mensual incremental o completa será suficiente. Podríamos aplicar el mismo criterio para algunas máquinas virtuales como por ejemplo controladores de dominio. En cambio para Exchange, servidores de aplicaciones y sobre todo servidores de ficheros será necesario crear copias de forma regular, diarias y aplicar una política de retención que permita la recuperación de datos en caso de ser requerido.

El siguiente cuadro resume los parámetros a seguir a la hora de crear una copia de seguridad en disco de algunos servidores, tanto físicos como virtuales (ejemplo para *Cliente1* y *Cliente2*):

Servidor	Tipo servidor	Frecuencia	Tipo de copia	Retención
DCTFG-DC01	Físico	Mensual	Completa	12 Meses, 1 anual
DCTFG-Cluster01	Físico	Mensual	Completa	12 Meses, 1 anual
DCTFG-VS01	Físico	Mensual	Completa	12 Meses, 1 anual
DCTFG-VS02	Físico	Mensual	Completa	12 Meses, 1 anual
DCTFG-BCK01	Físico	Mensual	Completa	12 Meses, 1 anual
CLI1-DC01	Virtual	Mensual	Completa	12 Meses, 1 anual
CLI1-FS01	Virtual	Diaria	Completa/ Incremental	Copia diaria, copia semanal (viernes) y copia mensual (completa). 12 meses 1 anual.
CLI1-APP01	Virtual	Diaria	Completa/ Incremental	Copia diaria, copia semanal (viernes) y copia mensual (completa). 12 meses 1 anual.
CLI2-DC01	Virtual	Mensual	Completa	12 Meses, 1 anual
CLI2-FS01	Virtual	Diaria	Completa/ Incremental	Copia diaria, copia semanal (viernes) y copia mensual (completa). 12 meses 1 anual.

12.5. Copia de seguridad de la información remota

El probable que en nuestra infraestructura existan servidores de ficheros ubicados en otras redes. Para interconectar dichos servidores tendríamos que construir túneles VPN entre ellos y la infraestructura principal. En estos servidores también tendremos bastante información susceptible de hacer una copia de seguridad.

Si estamos en una fase inicial de la oficina remota, es decir, no existe demasiada información volcada en las carpetas del servidor, podríamos intentar crear una copia de seguridad completa desde la red (tipo "*Full*") y a partir de ella utilizar sólo copias incrementales. El problema existe cuando hay demasiada información volcada en el servidor y la copia remota puede tardar mucho tiempo o incluso nunca terminar. Para estos casos se recomienda copiar la información en un disco externo y enviarla a las oficinas centrales para conectarlo en el servidor de Backup (DCTFG-BACKUP01). Una vez conectado podemos proceder a crear una copia completa local y después programar la copia remota sólo para los ficheros modificados (incremental). Symantec permite realizar esta copia con la opción "*One-Time Backup*".

En los servidores remotos tenemos que aplicar ciertas restricciones de volcado de ficheros como por ejemplo prohibir ficheros tipo *.PST* (no son necesarios, existe una copia de todos los correos en el Barracuda Archiver). También habrá que aplicar cuotas a las carpetas personales de los usuarios e incluso programar borrado automático de algunas carpetas como por ejemplo la carpeta de documentación escaneada.

12.6. Copia de seguridad del correo electrónico

El registro de todos los correos está totalmente controlada desde el dispositivo Barracuda Archiver. Desde él podemos restaurar todos los emails que han pasado por cualquiera de las organizaciones que están dentro de nuestro sistema.

12.7. Copia de seguridad a cintas

Una vez tengamos toda la información en nuestros sistemas de almacenamientos, será necesario sacar esos datos de dichos dispositivos ubicados en las mismas oficinas, por los siguientes motivos:

- **Espacio**. No podemos mantener toda la información histórica en los dispositivos de almacenamiento dinámico como los *NAS*. Tarde o temprano será necesario liberar espacio para poder continuar con el proceso de copia.
- **Coste.** En el punto anterior se habló de espacio, por lo tanto si no sacamos la información de dichos dispositivos tendremos que comprar nuevos discos *NAS* con la notable inversión que ello significa.
- **Efectividad**. Algunas copias es posible que nunca se consulten, por lo tanto no es rentable mantenerlas en los dispositivos *NAS* o la SAN, ya que estos dispositivos están orientados a almacenar la información más susceptible a recuperar.
- **Integridad de la información**. Debido a las políticas de retención, la información se sobrescribe por lo tanto será necesario ubicarla en otra ubicación.
- **Seguridad.** Es recomendable ubicar las copias de seguridad fuera de la oficina principal donde se encuentran los servidores y los dispositivos de almacenamiento. En caso de desastre se podría perder definitivamente los datos almacenados en dichos dispositivos. Si utilizamos dispositivos extraíbles podríamos enviarlos a otras oficinas de la empresa para su almacenamiento o incluso a empresas especializadas en su custodia.

Para conseguir la mejor tasa de trasferencia de datos entre el servidor de backup y la librería de cintas, se conectarán a través de un puerto SAS (Capítulo 7.3.2). El dispositivo de almacenamiento en cintas HP MSL2024 permite tener hasta 24 cintas tipo LTO-6 ubicadas dentro de los dos magazines. Por otro lado, el servidor sólo dispone de tarjetas de 1GbE pero se conectarán a los switches al puerto 10GbE. En futuras expansiones podremos añadir una tarjeta 10GbE al servidor de backup.

El ciclo de la copia en cinta se divide en tres partes: copia semanal, mensual y anual. La copia semanal se realizará básicamente al final de cada semana (durante el fin de semana), en la cual se volcará toda la información que se encuentra almacenada en los dispositivos *NAS*. La copia podría empezar a programarse a partir del viernes y finalizará el domingo. Estas cintas se reutilizan cada mes. La copia mensual no es más que la copia semanal realizada el último viernes del mes (utilizando cintas nuevas). La copia anual es la copia mensual del mes de diciembre. Esta es la cinta que tendrá más tiempo de retención. Una vez cerrado el ciclo, las cintas mensuales se pueden reciclar de nuevo. La cinta con la copia anual se enviará a un lugar seguro fuera de la oficina.

Ejemplo de rotación:

Semana	Viernes	Sábado	Domingo	Observaciones
1 (primer viernes del mes)	SMes	SMes	SMes	Set de cintas SMes
2	S2	S2	S2	Set de cintas S2
3	S3	S3	S3	Set de cintas S3
4	S4	S4	S4	Set de cintas S4

El primer viernes de cada mes señala la semana que habrá que colocar cintas nuevas, ya que la copia de ese fin de semana será la copia mensual (SMes). Por lo tanto es posible que la primera semana corresponda aún al mes anterior si el viernes coincide con el cambio de mes. El resto de colecciones, S2, S3 y S4, irán rotando cada mes. Finalmente la cinta de diciembre será la copia anual.

13. Conclusiones

Este TFG ha sido de gran ayuda para poner en práctica muchas de las temáticas que hemos estudiado durante todo el Grado y más en concreto en las asignaturas relacionadas con la Administración de Sistemas. En el TFG se unifican muchos de estos conceptos en una idea concreta que engloba la mayoría de ellos y sobre todo, los pone en práctica en el mundo real. Quizás la lección más valiosa ha sido la gratificación de ver la aplicación práctica de todos los conceptos que hemos estudiado implementada en una solución que ofrece servicios de TI variados y además útil para cualquier organización o empresa. He tenido la suerte de implementar una infraestructura similar a la que muestra este TFG en mi empresa actual con buenos resultados de rendimiento y funcionamiento.

Sobre la planificación del TFG, he intentado cumplir los plazos pero ha sido bastante complicado, ya que es difícil saber dónde hay que parar de profundizar en un tema concreto. Por lo tanto ha sido necesario estudiar perfectamente cada contenido de los capítulos y centrarme en los puntos más importantes. He tenido que reducir el contenido de algunos temas que me hubiera gustado profundizar un poco más (como la seguridad, escalabilidad, etc.) pero ha sido imposible debido a la longitud máxima del trabajo y sobre todo al tiempo limitado disponible. He tenido que ir ajustando y cambiando algunos capítulos intentando dar más profundidad a aquellos que pienso son los más importantes como por ejemplo la configuración del correo electrónico o el diseño de la infraestructura. Pero en general, los plazos de planificación iniciales se han cumplido por lo que pienso que la metodología ha sido la correcta.

Lamentablemente he tenido que dejar pendientes algunos temas importantes. Uno de ellos es por ejemplo la monitorización. La implementación de un buen sistema para controlar eventos de nuestra infraestructura es una gran herramienta para prevenir y conocer el motivo de los errores que vayan apareciendo durante la vida del proyecto. Sólo se ha realizado alguna mención a la creación de alertas por correo electrónico de eventos generados por el protocolo *SMNP*. Me hubiera gustado poder haber desarrollado la implementación de un sistema de monitorización profesional basado en alguna de las aplicaciones más conocidas como por ejemplo *Spiceworks*. La seguridad es otro de los temas que me hubiera gustado desarrollar en profundidad. Sólo he podido añadir algunos comentarios dando algunas orientaciones sobre las contraseñas o las actualizaciones. Aunque esto es un buen punto de partida, a medida que la complejidad de esta infraestructura sea mayor, será indispensable crear un buen protocolo de seguridad general para gestionar todo tipo de eventos que puedan poner en peligro el proyecto. La conexión en alta disponibilidad de los switches principales ha sido otro de los temas que no he podido desarrollar en profundidad debido a la complejidad y extensión del proceso. He pensado que era mejor centrarse en otros puntos del TFG ya que existe mucha documentación disponible de CISCO para realizar esta operación.

Pensando en los temas que se podrían tratar en el futuro, no podemos olvidar la escalabilidad. Aunque el sistema base está preparado para soportar una considerable infraestructura, quizás sería necesario crear un procedimiento de ampliación, por ejemplo añadir una nueva SAN, nuevos tipos de conexiones en los switches o incluso añadir nuevos servidores físicos al entorno como por ejemplo nuevos nodos Hyper-V. También hubiera sido interesante incluir un capítulo sobre alternativas de código libre que pudiéramos aplicar al diseño.

Creo que los objetivos principales del TFG se han cumplido, tanto en la parte relacionada con la creación de la documentación como en el proyecto a implementar. El objetivo de crear una pequeña guía de instalación y buenas prácticas el principal, con sus carencias que ya he descrito antes pero en general, creo que se ofrece una visión aceptable del proyecto.

Espero que este TFG sea de utilidad práctica para cualquier otro estudiante o trabajador de las TI que esté pensando en implementar una infraestructura igual o parecida a la descrita.

Gracias.

14. Glosario

10GBASE-T	interface de red con una velocidad de 10Gbs
AD	siglas en inglés de Directorio Activo
Alta disponibilidad	activación de medios secundarios en caso de fallo de los primarios
Cable de consola	cable RJ45 y serie utilizado para configurar dispositivos
CISCO IOS	sistema operativo para configurar dispositivos CISCO
Clúster	conjunto de ordenadores conectados como si fuesen un solo ordenador
Computación en la nube	servicios de IT a través de Internet como por ejemplo correo, almacenamiento, etc.
Conector Exchange	configuración de enrutamiento para el tráfico de correos en Exchange
DNS	sistema de nomenclatura para asignar un nombre a una ip
Dominio	red de ordenadores conectados en una red
Failover	tolerancia a fallos
FGCP	sistema de alta disponibilidad para dispositivos Fortigate
Fiber Channel	conexión de fibra óptica
GPO	políticas aplicadas a redes Microsoft
HA	interfaz en dispositivos Barracuda la cual muestra el estado del dispositivo
host	ordenadores en una red que proveen de servicios
Hyper-V	entorno de virtualización Microsoft
ICMP	protocolo utilizado para enviar mensajes de error
ILO	puerto de red Ethernet destinado a la gestión del servidor
Interfaces	tarjetas de expansión que se conectan a dispositivos
iSCSI	estándar que permite *SCSI* sobre redes
ISS	servidor web Microsoft
Journaling	proceso de almacenamiento de correos electrónicos con un dispositivo Barracuda
LDAP	protocolo de acceso simplificado a Directorios. Se utiliza para conectar con AD
Librería de cintas	dispositivo para realizar copias de seguridad a cintas
LTO-6	cintas para backup con capacidad de 2.5 TB
LUN	número de unidad de lógica, dirección de conexión con un disco o discos de la *SAN*
NIC	tarjeta de red
OWA	acceso al correo Exchange desde Internet
PAC	programa en Javascript para ayudar a elegir el proxy que necesita un dispositivo
Proxy	programa o dispositivo que gestiona las conexiones a un servidor
RAID	conjunto redundante de discos independientes, sistema de almacenamiento
SAN	área de almacenamiento en red (*Storage Area Network*)
SAS	*Serial Attached SCCI*, conexión evolucionada de datos en serie
SCSI	interfaz para la transferencia de datos entre el bus y el ordenador
SIP	protocolo que permite sesiones interactivas multimedia
SPAM	correo no deseado
TI	Tecnologías de la Información
UEFI	interfaz que se encuentra entre el sistema operativo y el hardware
VDOM	dominio virtual utilizado en dispositivos Fortigate
VLAN	redes lógicas independientes dentro de una misma red utilizadas en switches
Volumen	separación de los discos y reserva de espacio dentro de una *SAN*
VPN	red privada virtual para conectar redes distantes
widget	aplicación o programa

15. Bibliografía

Enlaces consultados:

[1] Configuración Etherchannel CISCO. Fecha consulta: Marzo 2016. Fuente
[2] Página oficial programa Putty. Fecha consulta: Marzo 2016. Fuente
[3] Configuración Firewall ASA. Fecha consulta: Marzo 2016. Fuente
[4] Actualización CISCO IOS. Fecha consulta: Marzo 2016. Fuente
[5] Configuración básica de red CISCO. Fecha consulta: Marzo 2016. Fuente
[6] Configuración listas de accesos CISCO. Fecha consulta: Abril 2016. Fuente.
[7] Configuración VLAN CISCO. Fecha consulta: Abril 2016. Fuente
[8] Configuración switch Catalyst 2960. Fecha consulta: Abril 2016. Fuente
[9] Configuración Fortigate VDOM. Fecha consulta: Abril 2016. Fuente
[10] Configuración cookbook Fortigate VDOM. Fecha consulta: Abril 2016. Fuente
[11] Configuración Fortigate en alta disponibilidad. Fecha consulta: Abril 2016. Fuente
[12] Manual Fortinet para alta disponibilidad. Fecha consulta: Abril 2016. Fuente
[13] Barracuda Web Filter Administrator´s Guide. Fecha consulta: Abril 2016. Fuente
[14] Barracuda Web Filter PAC file. Fecha consulta: Mayo 2016. Fuente
[15] Barracuda Web Filter GPO proxy deployment. Fecha consulta: Mayo 2016. Fuente
[16] Barracuda Spam Firewall Administrator's guide. Fecha consulta: Mayo 2016. Fuente
[17] Barracuda Message Archiver Administrator's guide. Fecha consulta: Mayo 2016. Fuente
[18] Configuración RAID HP Proliant. Fecha consulta: Fecha consulta: Mayo 2016. Video. Documento.
[19] Proceso de "*teaming*" de tarjetas de red Windows 2012 Server. Fecha consulta: Mayo 2016. Fuente
[20] Instalación de la SAN MSA2040. Fecha consulta: Mayo 2016. Fuente
[21] Mejores prácticas para la instalación de la SAN MSA2040. Fecha consulta: Mayo 2016. Fuente
[22] Configuración SAN MSA 2040 paso a paso. Fecha consulta: Mayo 2016. Fuente
[23] Configure iSCSI on Windows Server 2012 R2. Fecha consulta: Mayo 2016. Fuente
[24] Installing Failover Feautures and Tools, Windows 2012 Server. Fecha consulta: Mayo 2016. Fuente
[25] Use Cluster Shared Volumes in a Failover Cluster. Fecha consulta: Mayo 2016. Fuente
[26] Install Hyper-V and create a virtual machine. Fecha consulta: Mayo 2016. Fuente
[27] How to configure Hyper-V Virtual Switch. Fecha consulta: Mayo 2016. Fuente
[28] Microsoft Exchange 2013 on Windows Server 2012. Fecha consulta: Mayo 2016. Fuente
[29] Move Transport Database in Exchange 2013. Fecha consulta: Mayo 2016. Fuente
[30] New-MailboxDatabase Exchange 2013. Fecha consulta: Mayo 2016. Fuente
[31] Configure storage quotas for a mailbox, Exchange 2013.Fecha consulta: Mayo 2016 Fuente
[32] Barracuda Journaling for Exchange Server. Fecha consulta: Mayo 2016. Fuente
[33] Setup Exchange 2013 Receive Connector. Fecha consulta: Mayo/Junio 2016 Fuente
[34] Configuring Outbound Mail Flow in Exchange Server 2013. Fecha consulta: Mayo 2016 Fuente
[35] CSR Creation Microsoft Exchange 2013. Fecha consulta: Mayo/Junio 2016 . Fuente
[35] Buffalo Terastation User Manual. Fecha consulta: Mayo/Junio 2016. Fuente
[36] Backup Exec 15 Administrator's Guide. Fecha consulta: Mayo/Junio 2016. Fuente
[37] Installing Windows Server 2012 step by step. Fecha consulta: Mayo/Junio 2016. Fuente
[38] Configure rol DNS Windows Server 2012. Fecha consulta: Mayo/Junio 2016. Fuente
[39] Configure DNS Windows Server 2012. Fecha consulta: Mayo/Junio 2016. Fuente
[40] Configure ASA for reduntant or Backup ISP. Fecha consulta: Mayo/Junio 2016. Fuente

16. Anexos

16.1. Instalación Windows Server 2012 R2:

NOTA: es importante que el formateo de todas las unidades se realice en modo GPT o GUID (*Identificador Único Global*). Si arrancamos en modo UEFI la BIOS y los discos no están previamente formateados, este será el método por defecto que aplicará Windows para la instalación. En caso contrario será necesario volver a formatear la partición utilizando el comando *diskpart* Existen muchos métodos para volcar la imagen ISO del S.O. a un pendrive y convertirlo en arranque. La más popular es "*Windows 7 USB/DVD Download Tool*", creada por Microsoft.

La instalación de Microsoft Windows Server 2012 r2 es una operación bastante sencilla [37]. Seleccionamos la versión del sistema operativo que queremos instalar, en nuestro caso utilizaremos la versión "*Windows Server 2012 R2 Standard Evaluation (Server with a GUI)".* Una vez terminada la instalación el primer paso que tenemos que realizar es cambiar la contraseña de administrador.

16.2. Instalación del controlador de dominio y roles necesarios:

El controlador de dominio tendrá los siguientes roles: Controlador de dominio (principal), Servidor DNS y Servidor *DHCP* (opcional) [38]. Una vez finalizado tendremos un nuevo "*forest*" con el servidor **DCTFG-DC01** como controlador principal. El siguiente paso es instalar el rol de DNS. Seguiremos los primero pasos igual que para la instalación del controlador de dominio pero esta vez activaremos la opción "*DNS Server*" [38]

Una vez instalado el rol de DNS tendremos que pasar a configurarlo desde el apartado "*DNS Manager*":

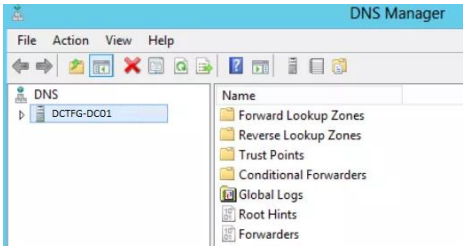


Figura 126

Por defecto comenzaremos sin ninguna zona, por lo tanto tendremos que empezar a crearlas desde la opción "Action" del menú y seleccionando "*Primary zone*" y escribiendo el nombre de la zona:

Figura 127

En este punto podríamos importar una configuración DNS.

Al ser la primera instalación procederemos a crear uno nuevo.

El resto de pasos simplemente dejaremos la configuración por defecto [39]. Cuando terminemos podremos ver el nombre del dominio en el "*DNS Manager*". Ahora ya podremos crear los registros A, CNAME, etc., desde el menú "*Action*". De esta forma obtenemos una configuración básica DNS. Luego será necesario ir afinando, añadiendo el nombre de los servidores y ajustando algunos parámetros más, pero para ello podemos consultar la numerosa documentación que se encuentra en Internet.

El último rol a instalar es el servidor DCHP (si procede). Antes de configurar el servicio *DHCP* vamos a configurar las direcciones IP del servidor. Asignaremos las siguientes IP a la NIC principal, NIC 1 (NIC 1 y NIC 2 se configurarán en modo "*teaming*"):

NIC 1:

IP: 10.1.1.20
Máscara: 255.255.255.0
Gateway: 10.10.1.1
DNS Primaria: 10.10.1.20
DNS Secundaria: 10.10.1.30

Antes se ha indicado que la configuración *DHCP* es opcional. Por motivos de seguridad y debido a que la instalación principal de la infraestructura tendrá direcciones IP estáticas, no procederemos a configurar de momento el servicio *DHCP* para esta parte de la infraestructura.

16.3. Instalación de roles Hyper-V

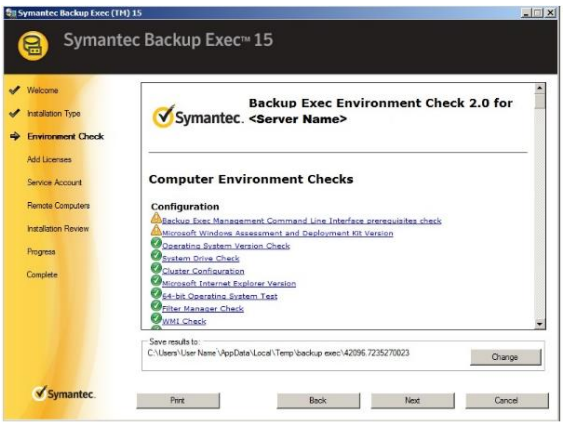
En este caso los roles a instalar serían: Hyper-V, File and Storage Services e IIS. Debido a que la ubicación de las máquinas virtuales se alojaran en diferentes volúmenes creados en la SAN, procederemos a instalar el rol Hyper-V con los parámetros por defecto (se modificarán cuando definamos los volúmenes de la SAN). El *Capítulo 9* trata en profundidad la configuración Hyper-V. La instalación es un proceso bastante sencillo y directo. El siguiente rol a instalar es el servidor IIS [40]. Al igual que con Hyper-V, instalaremos de momento las opciones por defecto.

El último rol a instalar es "*File and Storage Services*". La instalación básica de este rol es bastante sencilla, no requiere ninguna especificación directa de momento. Este rol se instala principalmente para activar el modo "*block storage*" (almacenamiento por bloques), el cual muestra las unidades como si la unidad no estuviera formateada pero en cambio contiene información. Esta información está gestionadas por el controlador iSCSI. De esta forma conseguimos unificar diferentes ubicaciones donde se encuentra la información en una sola "*carpeta*".

16.4. Instalación Symantec Backup Exec

A continuación, desde Windows Server 2012 instalaremos el software de *Symante Backup Server Exec 15*. Podemos descargar la versión de pruebas desde la página web de Veritas. La descarga suele ser un fichero imagen tipo *ISO* por lo tanto tendremos que grabarlo en un DVD o montarlo en una unidad. Ejecutaremos el programa "*Backup.exe*". En la siguiente pantalla elegiremos *Backup Exec* y seguiremos los pasos que nos muestra el asistente. En la siguiente pantalla se analizarán los requisitos necesarios para poder realizar la instalación. Podemos seleccionar los que nos falten para proceder a su instalación [36]:

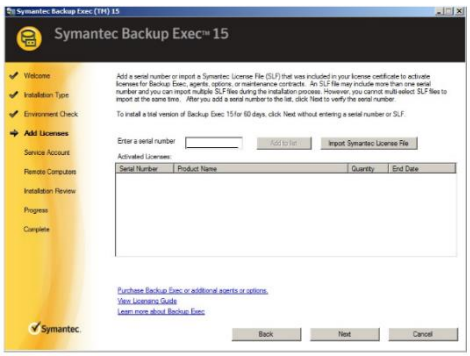
Figura 128



El siguiente paso es importante, ya que tendremos que incluir los números de serie de las licencias que hemos comprado. Para este entorno será necesario obtener las siguientes licencias:

Tipo de licencia	Número	Función
Agente para VMware y HyperV	2	Copia de las máquinas virtuales
Agente para Windows	4	Copia de la configuración Windows
Opción de deduplicación	1	Optimización en el backup
Licencia Backup Exec Server 15	1	Programa principal
Virtual Tape Library Unlimited	1	Gestión de las cintas

Iremos añadiendo los números de serie de cada agente a instalar así como la licencia principal del programa Backup Exec 15:



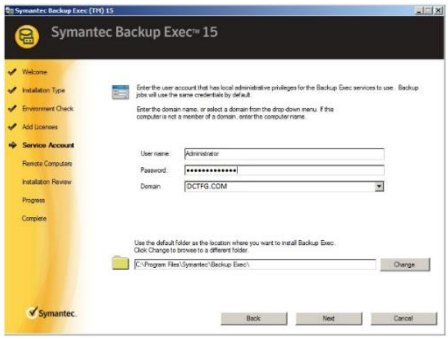


Figura 129

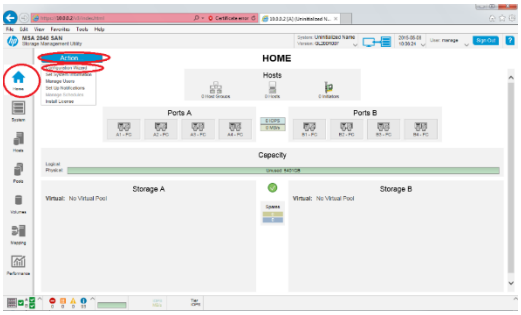
16.5. Configuración básica de la SAN

Una vez conectada la SAN a los servidores Hyper-V procedemos a la configuración de la misma. La dirección IP por defecto de la SAN es 10.0.0.1 o 10.0.0.2 [22]. Conectaremos a través de un navegador introduciendo como credenciales por defecto, usuario "*manage*" contraseña "*!manage*". Antes de continuar procederemos a asignarle un nombre de host a la SAN (DCTFG-SN01) en la opción "*Set System Information*". Por último actualizaremos la firware del dispositivo:

Figura 130

16.5.1. Configuración utilizando el asistente

La forma más rápida y sencilla de configurar los parámetros básicos de la SAN es utilizar el "*Configuration Wizard*":



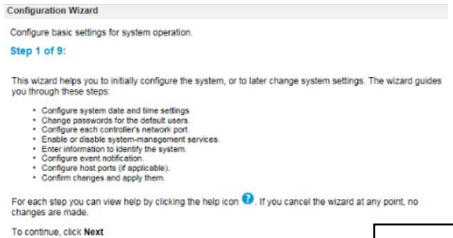


Figura 131

El primer paso es configurar la fecha y la hora. También configuraremos el protocolo NTP si queremos automatizar el proceso de sincronización de fecha y hora así como la contraseña. Por último asignaremos la dirección IP y las alertas SNMP:

Controladora A:	Controladora B:
IP: 172.1.1.80	IP: 172.1.1.90
Máscara: 255.255.255.0	Máscara: 255.255.255.0
Gateway: 10.10.1.1	Gateway: 10.10.1.1

16.6. Coste aproximado del proyecto

Hardware (instalación básica inicial)

Marca	Modelo	Uds.	Coste €	Total
CISCO	ASA 5520	1	3500	3500
Barracuda	Web Filter 610	1	8700	8700
Barracuda	Message Archiver 450	1	8900	8900
Barracuda	Spam Firewall 300	1	2500	2500
Fortigate	800C	2	10000	20000
CISCO	4900	2	8500	17000
CISCO	SG200-8	1	90	90
CISCO	Catalyst 2960S 24TS	1	1200	1200
HP	Proliant DL560 G9	2	12000	24000
HP	Proliant DL60 G9	1	2200	2200
HP	Proliant DL20 G9	1	1800	1800
HP	MSA 2040 + 24 HD	1	14000	14000
HP	2024	1	7000	7000
Buffalo	Terastation 5400 12TB	1	2500	2500
APC	SRT 8000VA 208V IEC	1	7500	7500
TOTAL				120890

Software (instalación básica inicial)

Marca	Versión	Uds.	Coste	
Microsoft	Windows Server Enterprise 2012 Hyper-V	4	1200	4800
Microsoft	Exchange Server Standard 2013	N.A.		
Symantec	Backup Exec 2015	1	800	800
Symantec	Agentes	5	400	2000
Kaspersky	Endpoint Security Bussines	1	1	600
TOTAL				8200

Otros

Descripción	Uds.	Precio
Armario Rack 42U	1	800
Cableado	N.A.	1000
Interfaces *Fiber Channel*	2	600
Interfaces SAS	1	200
TOTAL		2600

Total Hardware	120890
Total software	8200
Total otros	2600
TOTAL PROYECTO	**131.690 €**

Notas:

- Los servidores tienen incluido en el precio todos los extras que necesiten
- Los swtiches CISCO 4900 tienen incluido en el precio las tarjetas de expansión necesarias.
- El CISCO ASA 5520 también tiene incluido el precio de la tarjeta de expansión
- Las licencias de Exchange no se contabilizan ya que no serán necesarias en la instalación inicial
- El cableado incluye cualquier otro tipo de cable que necesitemos extra
- El precio del antivirus variará en función de los nodos que queramos proteger, esta versión soporta 10

16.7. Vista del armario con los dispositivos instalados

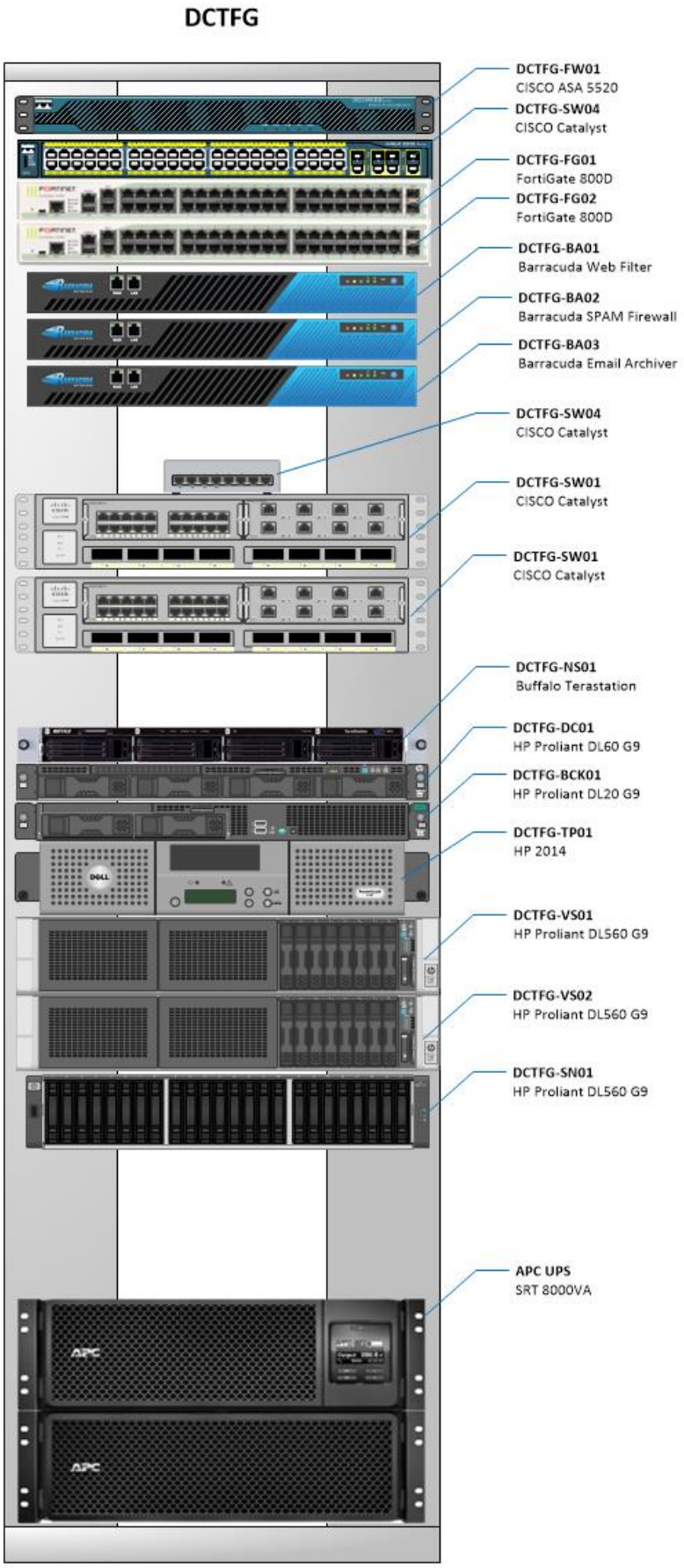


Figura 132