

INTRODUCCION A UNA RED VIRTUALIZADA CON VMWARE Y COPIAS DE SEGURIDAD

Ganga López, Javier

Tutor: Casares Giner, Vicente

Trabajo Fin de Grado presentado en la Escuela Técnica Superior de Ingenieros de Telecomunicación de la Universitat Politècnica de València, para la obtención del Título de Graduado en Ingeniería de Tecnologías y Servicios de Telecomunicación

Curso 2016-17

Valencia, 4 de julio de 2017

Resumen

El proyecto trata sobre una introducción a los sistemas de alta disponibilidad, y su software que intentan alcanzarla como VMware, para facilitar y aconsejar su aprendizaje a administradores de sistemas y ver las necesidades reales en una empresa. Para ello, inicialmente se introducirán los conceptos más destacables en el ambiente de la alta disponibilidad, en un entorno óptimo para una empresa. Para tal fin, se va a realizar una instalación virtualizada de alta disponibilidad en una empresa, se va a escoger y documentar la red más óptima para estos entornos y demostrar su alta funcionalidad y rendimiento.

Además, se va a realizar una instalación que se podría efectuar en cualquier gran empresa ya que va a tratarse de un entorno de alto rendimiento. Además, se introducirán los conceptos de Backup y se mostrarán como realizar este tipo de copias para conseguir un entorno de alta disponibilidad.

Resum

El projecte tracta sobre una introducció als sistemes d'alta disponibilitat, i el seu programari que intenten aconseguir-la com VMware, per facilitar i aconsellar el seu aprenentatge a administradors de sistemes i veure les necessitats reals en una empresa. D'aquesta manera, inicialment s'introduiran els conceptes més destacables en l'ambient de l'alta disponibilitat, en un entorn òptim per a una empresa. Per a tal fi, es va a realitzar una instal·lació virtualitzada d'alta disponibilitat en una empresa, es va a escollir i documentar la xarxa més òptima per a aquests entorns i demostrar la seva alta funcionalitat i rendiment.

A més, es va a realitzar una instal·lació que es podria efectuar en qualsevol gran empresa ja que va a tractar-se d'un entorn d'alt rendiment. A més, s'introduiran els conceptes de Backup i es mostraran com realitzar aquest tipus de còpies per aconseguir un entorn d'alta disponibilitat.

Abstract

The project addresses an introduction to high availability systems, and its software that it intends to achieve as VMware, to advise it learning to the system administrators and to see the real needs in a company. To do this, initially introduces the most outstanding concepts in the environment of high availability, in an optimal environment for a company. For this purpose, a high-availability virtualized installation is going to be carried out in a company, the most optimal network for these environments will be chosen and documented and its high functionality and performance will be demonstrated.

In addition, it can perform an installation that can be possible in any huge company and it is a high performance environment. In addition, It introduce the concepts of backup and show how to make these types of copies to obtain a high availability environment.

Índice

Contenido

Capítulo 1. Introducción.....	3
Capítulo 2. Objetivos	4
Capítulo 3. Presentación de la red	5
3.1 Esquema de Red	6
3.2 Componentes físicos del CPD de la sede de Valencia	7
3.2.1 Características de los servidores.....	8
3.2.2 Tecnología ILO	9
3.2.3 Características del Switch	10
3.2.4 Características del NAS (local)	11
3.2.5 Características de la cabina	12
3.2.6 Software HPE MSA 2040 Continuous Access.....	13
3.3 Componentes físicos de la replicación	14
3.3.1 Características de los servidores.....	15
3.3.2 Características de la cabina	16
3.4 Conexión MPLS.....	17
Capítulo 4. Infraestructura de alta disponibilidad	19
4.1 ¿Qué es alta disponibilidad?.....	19
4.1.1 Problemas en alta disponibilidad.....	20
4.2.....	20
4.3 Herramientas para conseguir una alta disponibilidad.....	21
4.3.1 CLUSTER	21
4.3.2 Equilibrio en carga de red	22
4.3.3 Controlar el nivel de servicio	23
4.3.4 Reducir el tiempo de inactividad.....	23
4.3.5 Copias de seguridad	24
4.3.6 SAN.....	25
4.3.7 Herramientas de virtualización.....	26
Capítulo 5. Virtualización y posterior instalación VMware.....	27
5.1 ¿Qué es y para qué sirve virtualizar?.....	27
5.2 VMware y sus componentes	29
5.2.1 VMware ESXi	31
5.2.2 VMware vCenter Server.....	32
5.2.3 VMware vSphere Web Client	34
5.3 Configuración de componentes.....	35

5.3.1	Configuración de la cabina de discos	35
5.3.2	Configuración de la NAS	40
5.4	Maquinas Virtuales	41
5.4.1	Creación de la maquina virtual (inventario).....	42
5.4.2	Puesta en marcha de la máquina virtual	44
5.5	Configuración de alta disponibilidad	45
5.5.1	Funcionalidad y configuración vMotion	45
5.5.2	Equilibrador de carga	48
Capítulo 6.	Implantación de copias de seguridad.....	50
6.1	¿Qué es una copia de seguridad?.....	50
6.2	Diferentes Software para efectuar copias de servidores.....	52
6.2.1	Acronis	52
6.2.2	Iperius.....	53
6.2.3	Veeam	54
6.3	Veeam Backup and Replication v9	56
6.3.1	Puesta en marcha de Veeam Backup.....	56
6.3.2	Configuración copias de seguridad en NAS (semanal).....	60
6.3.3	Configuración de replicación de un CPD (mensual).....	61
Capítulo 7.	Conclusiones	64
Capítulo 8.	Bibliografía	65

Capítulo 1. Introducción

La alta disponibilidad sobre un sistema y su implantación, nos asegura en cierto modo, que el sistema va a tener una continuidad funcional durante un periodo de tiempo estimado. En este proyecto se va a desarrollar un clúster con alta disponibilidad, el cual, asegura que la disponibilidad de la información almacenada en el sistema, va a poder consultarse de manera continuada por los usuarios.

Es necesario hablar de tiempo de inactividad, que es aquel tiempo en que el sistema se encuentra fuera de uso o no accesible, para el clúster a estudio, se ha estimado mediante la siguiente fórmula ($\text{Disponibilidad} = \text{MTTF} / (\text{MTTF} + \text{MTTR})$) si se ha conseguido una buena alta disponibilidad. Para ello, se va a utilizar a utilizar dos diseños de alta disponibilidad que se irán introduciendo a lo largo del proyecto, ya que, se puede diferenciar una alta disponibilidad en el entorno de Software y Hardware.

En el entorno de Hardware, se va a realizar un diseño en el cual ninguno de los elementos queda relegado a una única conexión, por lo que ante cualquier error, de cualquier componente, no será necesario ningún tipo de interrupción del sistema para que pueda ser sustituido por uno nuevo, para ello, además se incluirá la opción, del cambio en caliente (*hot and plug*) en cada componente.

Como herramienta principal de alta disponibilidad (software), se va a utilizar VMware, un sistema de virtualización de servidores, entre sus características principales, tiene una gran versatilidad, ya que es compatible con la mayoría de sistemas operativos disponibles para servidores, y además incluye varias herramientas que permiten una mayor alta disponibilidad entre los servidores incluidos en el clúster.

Por último, se realizará una pequeña introducción a como se gestionan, las copias de seguridad, para en caso de error del sistema se produzca la menor pérdida de información posible, y además un entorno de replicación en otra sede, para el llamado "momento de emergencia"

Capítulo 2. Objetivos

El objetivo de este proyecto, es instruir a cualquier ingeniero, o en su caso a cualquier administrador de sistemas, para desplegar una red corporativa en cualquier empresa con alta disponibilidad. Para ello, es necesario el conocimiento de todos los puntos de la red, y los software que posea cada uno, además de los posibles errores y consejos del funcionamiento de los mismos, ya que un mal uso, o el uso indebido, puede causar fallos a largo plazo en el sistema implantado. Además, este proyecto quiere ser introductorio para cualquier ingeniero de telecomunicaciones que se quiera dedicar su conocimiento a la administración de sistemas, ya que es necesario desarrollar la utilización de los conocimientos la ingeniería.

Además, este proyecto va encarado hacía un cargo que actualmente se demandada en muchas de las empresas, ya que, cada día es más necesario el acceso continuo a todos los datos, y se castiga considerablemente una perdida grande de información en aspecto monetario.

Capítulo 3. Presentación de la red

En este proyecto se quiere desarrollar un esquema de red comprendido para una mediana/gran empresa ya que el diseño es un poco excedido del presupuesto que podría tener una pequeña empresa, el volumen la empresa a estudio se sitúa desde los 20 a los 200 usuarios dependiendo de las características de la misma se podría reducir el Hardware interno de los componentes, pero no reducir el número de componentes planteados, ya que todos ellos son necesarios para alcanzar el objetivo de alta disponibilidad. En este caso del estudio se trata de una empresa de Valencia que contiene 200 usuarios, y necesita con urgencia ampliar su sistema, ya que por consecuencia de su continua expansión, sus servidores se han quedado cortos de recursos, y el sistema cada vez funciona con más lentitud.

Teniendo en cuenta los datos, se decide plantear una red corporativa de alta disponibilidad, en la cual todos sus 200 usuarios puedan tener acceso inmediato, y sin cortes, a todos los servicios, para ello se les aporta una red comprendida en la subred 172.168.1.0/24 y además se aconseja tener la idea de ampliar su dirección de red, ya que al estar en continua expansión, es muy posible que en breve tiempo la red, se quede sin direcciones. Como cuestión añadida se plantea, conectar la sede de Valencia a un clúster comprado en una compañía que ofrecen estos servicios como es el caso de Telefónica, que a través de una conexión MPLS, se usará para crear un sistema de replicación, además se aconseja utilizar una conexión de 300 Mbps para que no hayan problemas de conexión.

Por último se explica, una política de copias de seguridad, para acabar de diseñar el problema, en el cual tendremos 3 copias de seguridad a diferentes niveles, una diaria (**nivel 1**), que se realizará en la Cabina 2 (ver esquema), una semanal, que se realizara en la NAS (**nivel 2**), y por último una mensual (**nivel 3**), que se realizara de manera preventiva, en nuestro entorno de replicación, todas ellas son necesarias, ya que en caso de que se realiza un ataque a nuestra sede a través de algún virus de encriptación, nos asegura que la pérdida de datos será mínima ya que se almacena en tres localizaciones diferentes.

3.1 Esquema de Red

Como se ha introducido anteriormente nuestro esquema de red será el siguiente:

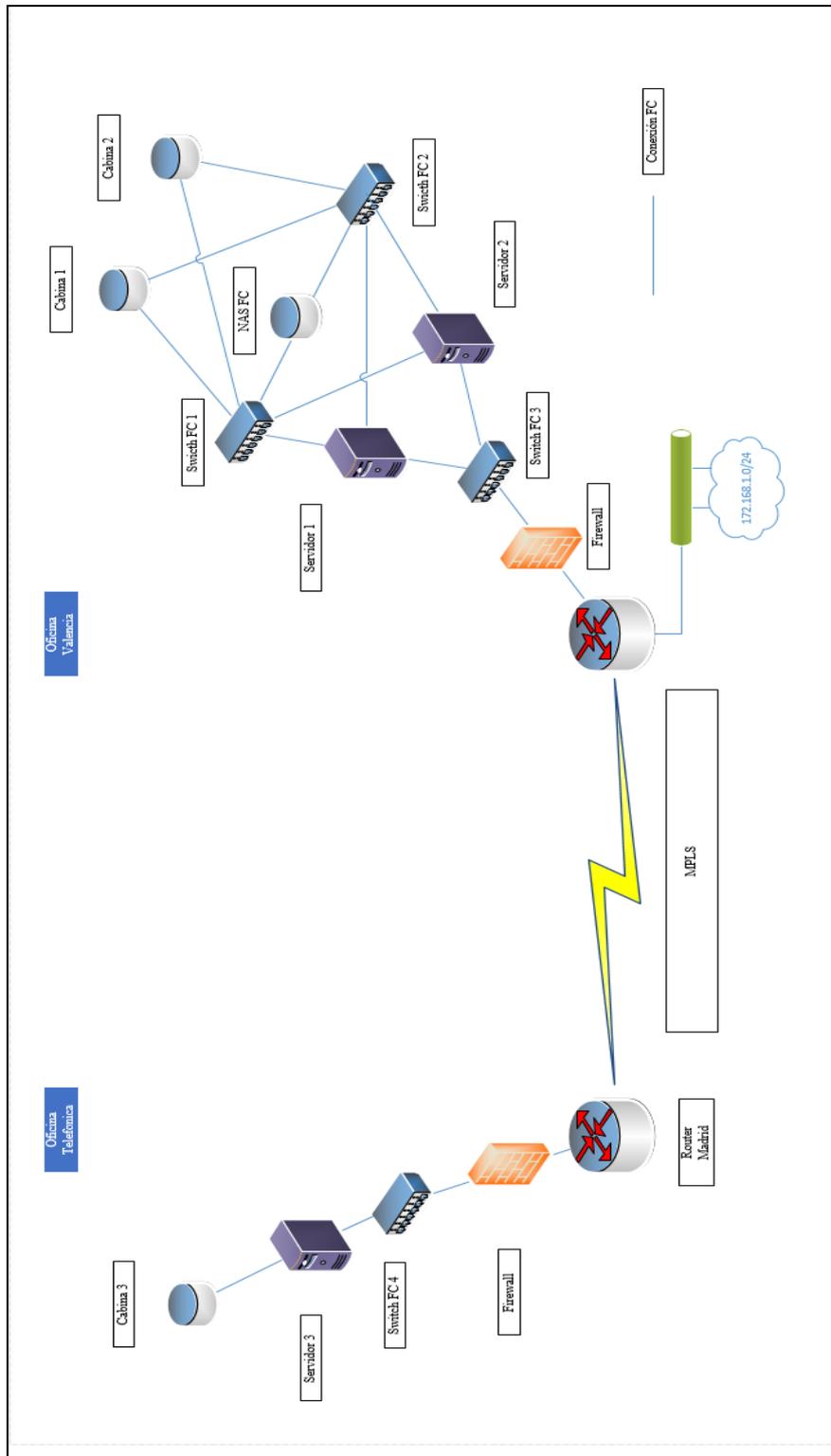


Figura 3.1-1: Esquema de red

3.2 Componentes físicos del CPD de la sede de Valencia

A continuación se muestra el esquema de red de Valencia:

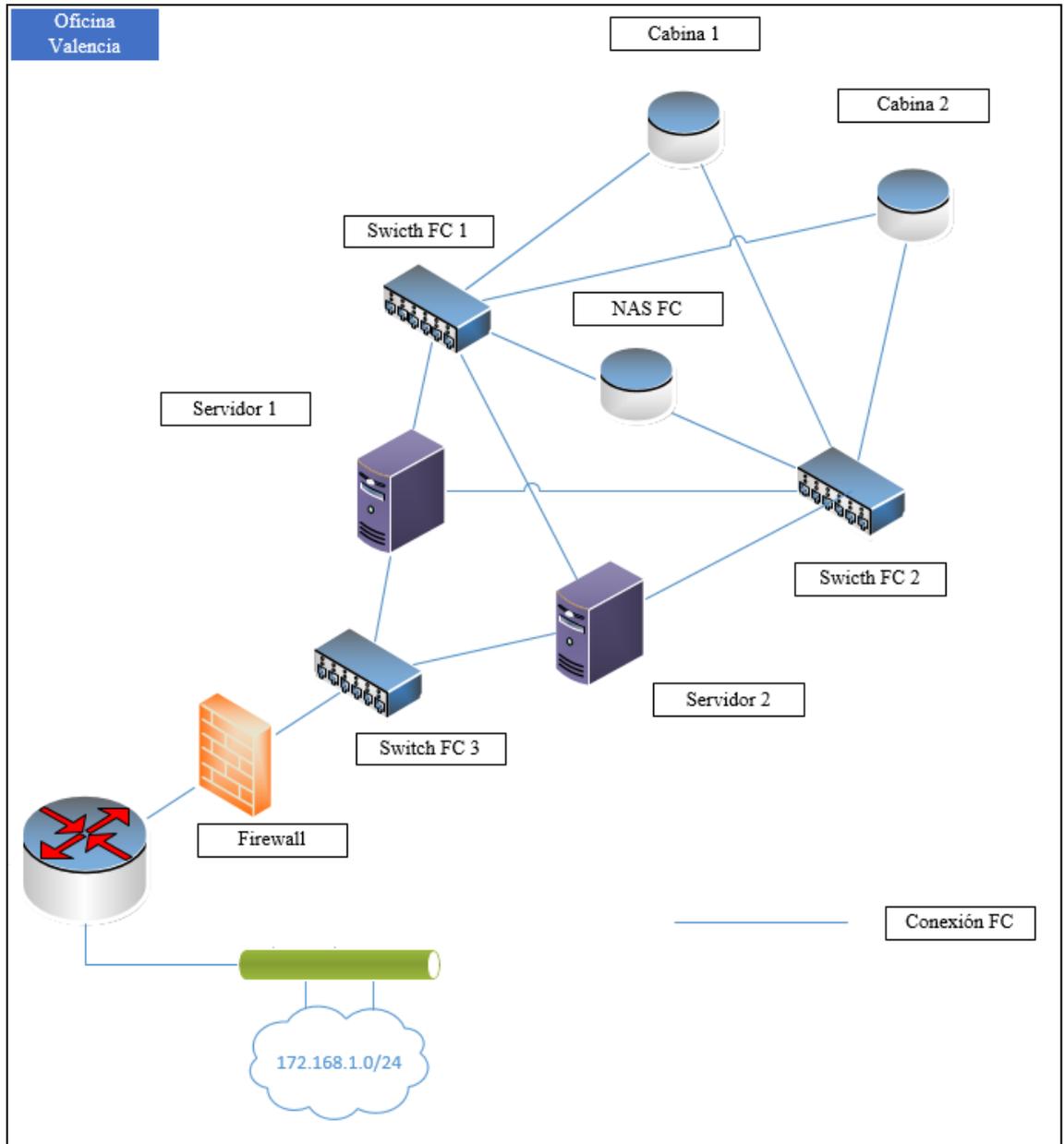


Figura 3.2-1: Esquema de red Valencia

Además pasaremos una a una a detallar las características de Hardware que compone esta sede, ya que cada elemento es necesario su estudio, porque un fallo eligiendo alguno de los componentes puede ser catastrófico para el cliente, un elemento mal elegido puede incurrir en el mal funcionamiento del sistema incluso al no funcionamiento del mismo (mal elección de las tarjetas de red o similares). También añadir, que todos los componentes planteados para la red son pertenecientes a HP, ya que la empresa a la que fue diseñada, era partner del fabricante . Por lo que ha decidido detallarse:

3.2.1 Características de los servidores

En cuanto a los servidores cabe comentar, que son servidores (ambos llevan la misma configuración) que se han diseñado para grandes cargas de movimiento de información, ya que van a tener a 200 usuarios accediendo a sus servicios (Correo, Intranet, etc...) a través de ellos, cabe considerar que se le han colocado 2 tarjetas con cuatro puertos de fibra cada una para no frenar una posible expansión de la empresa en caso de que quisiera ampliar este sistema.

Además, incluir los adaptadores de fibra necesarios para las conexiones que se van a realizar en el servidor, por último comentar una pieza fundamental, que puede ser clave en la elección de Hp, como es la tecnología ILO.

HP DL360 GEN9 8SFF CTO SERVER	
UNIDADES	CARACTERÍSTICAS
2	Procesador de 8 cores a 2,40 GHz (HP DL360 Gen9 E5-2630v3)
10	Módulos de 16GB de RAM DDR4 (HP 16GB 2Rx4 PC4-2133P-R)
2	Disco SAS HDS (Hitachi Data Systems) con 300 GB de almacenamiento, manda información a 6 GB (HP 300GB 12G SAS 10K rpm SFF (2.5-inch) SC Enterprise 3yr WarrantyHard Drive)
2	Cable para conexión de disco duro (HP DL360 Gen9 SEF Embed SATA Cable)
1	Kit para instalar en el rack (HP 1U SFF EasyInstall Rail Kit)
4	Adaptador para el uso de fibra óptica (HP 82Q 8GB Dual Port PCI-e FC HBA)
2	Tarjetas de red para fibra (HP StorageWorks 82Q 8Gb Dual Port PCI-e Fibre Channel Factory Integrated Host Bus Adapter)
2	Fuente de alimentación interna para el servidor y redundante (HP 800W Flex Slot Platinum Hot Plug PowerSupply Kit)
3 años	Soporte de HP las 24 horas los 7 días a la semana y sorpote de HP Proilant.
1	Licencia ILO

Tabla 3.2.1-1: Características Hardware servidores

3.2.2 Tecnología ILO

La necesidad de administrar los servidores que están alojados en diferentes puntos de una estructura, es un problema significativo, ya que, si el servidor está en una difícil localización, pierde energía o tiene cualquier problema y el administrador de sistemas no puede acceder a él, se pierde temporalmente el servicio que esté ofreciendo. Para ello, muchos servidores de HP, tienen implantado una tarjeta integrada llamada **ILO** que permite conectarse al servidor para realizar diversas funciones a nivel básico.

Una tarjeta **ILO** está diseñada para reemplazar productos de administración remotos que se utilizaban antaño, que lleva disponible en los servidores de HP lanzados desde 2006. Para su acceso se le asigna una dirección de red diferente a la dirección que posee el servidor y que desde este se le permite acceder de manera remota al mismo, aunque no esté operativo



Ilustración 3.2.2-1 : ILO

Para poder utilizar una tarjeta **ILO** debes situarte en la parte posterior del servidor y conectar un cable de Ethernet (**no permite fibra**), el cual estará añadido a una red de administración, desde el cual el administrador de sistemas debe acceder. La **ILO** es configurada en la primera configuración del servidor, o en cambio, a través de la BIOS del mismo. Se recomienda que la **ILO** posea una dirección de red, en la cual pueda acceder a internet, ya que de esta manera el administrador, no solo podrá acceder a la misma de manera local, sino a través de internet (se realiza a través de una conexión HTTPS). Además esto último tiene una relevancia importante ya que, es posible mandar datos a la compañía (HP) en el caso de que ocurra cualquier problema en el servidor de manera directa.

Un administrador de sistemas es capaz de realizar múltiples funciones de administración usando solo la tarjeta **ILO**, ya que fueron diseñadas para realizar acciones sobre un servidor que está bloqueado o deshabilitado. Esto se consigue, gracias a que la tecnología de esta tarjeta, se ejecuta independientemente del resto de operaciones del servidor, por eso mismo permite instalar y configurar sistemas operativos, aunque varían dependiendo la versión instalada. Es muy interesante esta función ya que un administrador de sistemas puede monitorizar todas las instalaciones realizadas desde su propia sede.

HP por su parte ha comercializado tres tipos de **ILO**. Las primeras solo incluían administración eléctrica, de temperatura, y administración de cosas básicas como cambios de IP, o utilización de la información enviada a HP. La segunda versión, agregó un punto gráfico a este recurso y un poco de seguridad. Por último, y la más actual **ILO3**, se incremento la velocidad de la tarjeta a la hora de realizar configuraciones en el servidor.

3.2.3 Características del Switch

Estos dispositivos se componen de diferentes módulos, dependiendo de las necesidades del sistema al cual se quieran incorporar, en este caso, se han añadido varios módulos que incluyen conexiones de fibra que satisfacen todas las conexiones, requeridas por nuestro sistema. Además añadir que son switches que operan en Capa 2 y 3 ya que es necesario actuar entre diferentes elementos como es otro router de Capa 2, y conexiones entre los servidores y la cabina de almacenamiento.

SWITCH	
UNIDADES	CARACTERÍSTICAS
3	HP 5406R z12 Switch
6	Fuente de alimentación redundante : HP 5400R 1100W PoE+ z12 PowerSupply
6	INCLUDED: HP 5400R 1100W PoE+ z12 Power Supply Europe - English localization
3	Manage del Switch: HP 5400R z12 Management Module
6	Módulos de 24 conexiones PoE: HP 24p 10/100/1000BASE-T PoE+ v3 z12 Mod
3	Módulos de 20 conexiones PoE y 4 de Fibra : HP 20p PoE+ / 4p SFP+ v3 z12 Mod
12	Adaptadores para Fibra de 1 Gb: HP X121 1G SFP LC LX Transceiver
3	Soporte de HPE: HPE 3Y FC 24x7 Aruba 5406R z12 Switch SVC [for J9821A]

Tabla 3.2.3-1: Switches delegación Valencia

3.2.4 Características del NAS (local)

Un NAS es un almacenamiento local el cual es accesible tanto desde los servidores, como desde cualquier equipo de red (dependiendo si está configurado dentro de la subred del equipo), en este caso nos encontramos un NAS de HP, el cual está configurado para la mejor utilización del usuario, y una configuración sencilla, ya que es un "pequeño" servidor en sí. Viene preconfigurado con un **Windows Server 2012 R2 Standard**, en el cual agregaremos más tarde a nuestro software de copias de seguridad, porque en este almacenamiento se ejecutaran las copias de seguridad de nivel 2 (copias semanales). La conexión entre el NAS y los Switches de efectuaran con cables de Ethernet conectados (se incluyen puertos de Ethernet en cada Switch) y a través de una conexión TCP/IP. Los protocolos de comunicaciones NAS están basados en archivos en los que el cliente solicita el archivo completo al servidor y lo maneja localmente, por lo que están orientados a manipular una gran cantidad de pequeños archivos.

NAS	
UNIDADES	CARACTERÍSTICAS
1	HP StoreEasy 1650 - NAS server - 32 TB

Tabla 3.2.4-1 : Características Hardware NAS

3.2.5 Características de la cabina

La cabina MSA2040 de HP viene con dos controladores los que nos asegura más alta disponibilidad, la configuración de la misma se producirá cuando se introduzcan los volúmenes en el VMware vCenter (punto 5.3.2), podemos decir que es necesario realizar una configuración RAID 5 (explicada en alta disponibilidad punto 4.2.1) para conseguir una alta disponibilidad en los discos. Además se introducirá el software de replicación de HP (Software HPE XP P9000 Continuous Acces), con el cual conseguiremos la primera copia de seguridad a nivel 1. Por último, las conexiones quedarán del siguiente modo:



Ilustración 3.2.5-1: Parte trasera MSA 2040

Donde ESXi 1, es la conexión que se efectuara a través del Switch de fibra al servidor 1, y ESXi 2, al servidor 2.

HP MSA 2040	
UNIDADES	CARACTERÍSTICAS
2	Controladora de la cabina HP MSA 2040 (HP MSA 2040 SAN Controller)
8	Disco duro interno de 4TB que envía información a 12 GB (HP MSA 4TB 12G SAS 7,2K 3,5im MDL HDD)
1	Adaptador para fibra (HP MSA 2040 8GB SW FC SFP 4PK)
2	Cable fibra óptica multimodo (HP Premier Flex LC/LC OM4 2f 1m Cbl)
3	Soporte de Proactive las 24 horas del día los 7 días de la semana (HPE 3Y Proactive Care 24x7 Service) y soporte de MS2000 G3

Tabla 3.2.5-1 : Hardware cabina MSA 2040

3.2.6 Software HPE MSA 2040 Continuous Access

HP MSA 2040 Continuous Access es una herramienta que permite replicar los datos de una cabina MSA 2040 a otra en tiempo real. Este software es ofrecido por HP para conseguir alta disponibilidad y continuidad, que permite una acceso continuo sin interrupciones a los servicios, incluso a aquellos en los que se había perdido el acceso. Junto con esta solución se implementan otras que permiten ofrecer niveles incluso más altos de seguridad, disponibilidad y tolerancia a desastres. Este software es utilizado para la recuperación de datos ante un desastres ya sean local o de mayor alcance, puede crear soluciones de recuperación de desastres 3 Data Center.

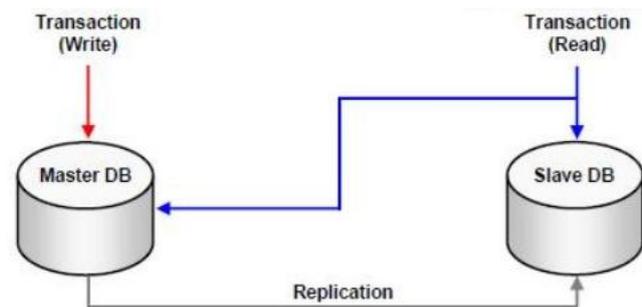


Ilustración 3.2.6-1 : Replicación de cabina

Características:

- La posibilidad de un funcionamiento ininterrumpido en tiempos de crisis, conservando copias en línea de la información importante en centros de datos alternos.
- Utilización de funciones de recuperación/restauración del clúster del servidores, con el funcionamiento del software de la cabina.
- Incluso alcanzar mayor seguridad con Continuous Access Synchronous, para proporcionar dos copias simultáneas de los mismos datos de origen, y creando una solución de recuperación de accidentes de 3 Data Center.
- Protocolo proporcionado por el mismo fabricante de los componentes, mejora la fiabilidad de los componentes.

3.3 Componentes físicos de la replicación

A continuación se muestra el esquema de red de la replicación:

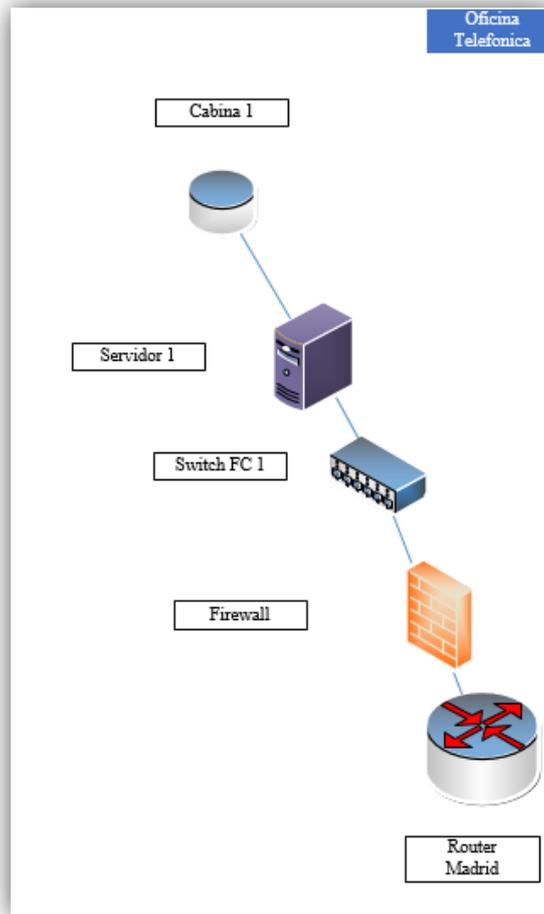


Figura 3.2.6-1 Esquema de red del entorno de replicación

3.3.1 Características de los servidores

El servidor tiene que ser simétrico a los mencionados anteriormente, ya que la carga que va a soportar es equiparable a la que soportaría estando en el clúster de Valencia:

HP DL360 GEN9 8SFF CTO SERVER	
UNIDADES	CARACTERÍSTICAS
2	Procesador de 8 cores a 2,40 GHz (HP DL360 Gen9 E5-2630v3)
10	Módulos de 16GB de RAM DDR4 (HP 16GB 2Rx4 PC4-2133P-R)
2	Disco SAS HDS (Hitachi Data Systems) con 300 GB de almacenamiento, manda información a 6 GB (HP 300GB 12G SAS 10K rpm SFF (2.5-inch) SC Enterprise 3yr WarrantyHard Drive)
2	Cable para conexión de disco duro (HP DL360 Gen9 SEF Embed SATA Cable)
1	Kit para instalar en el rack (HP 1U SFF EasyInstall Rail Kit)
4	Adaptador para el uso de fibra óptica (HP 82Q 8GB Dual Port PCI-e FC HBA)
2	Tarjetas de red para fibra (HP StorageWorks 82Q 8Gb Dual Port PCI-e Fibre Channel Factory Integrated Host Bus Adapter)
2	Fuente de alimentación interna para el servidor y redundante (HP 800W Flex Slot Platinum Hot Plug PowerSupply Kit)
3 años	Soporte de HP las 24 horas los 7 días a la semana y soporte de HP Proilant.
1	Licencia ILO

Tabla 3.3.1-1 :Características Hardware servidores.

3.3.2 Características de la cabina

Esta cabina va a ser simétrica a una de las elegidas anteriormente, ya que va a contener la misma información en forma de segunda replica de la cabina principal (cabina 1):

HP MSA 2040	
UNIDADES	CARACTERÍSTICAS
2	Controladora de la cabina HP MSA 2040 (HP MSA 2040 SAN Controller)
16	Disco duro interno de 4TB que enviar información a 12 GB (HP MSA 4TB 12G SAS 7,2K 3,5in MDL HDD)
1	Adaptador para fibra (HP MSA 2040 8GB SW FC SFP 4PK)
2	Cable fibra óptica multimodo (HP Premier Flex LC/LC OM4 2f 1m Cbl)
3	Soporte de Proactive las 24 horas del día los 7 días de la semana (HPE 3Y Proactive Care 24x7 Service) y soporte de MS2000 G3

Tabla 3.3.2-1 :Características Hardware Cabina

Como se observa se ha descartado utilizar el mismo método de replicación que en la cabina 2, a consecuencia de que esta cabina debe almacenar la copia mensual de los datos, no a tiempo real, esta se utilizará para mantener el servicio activo en caso de que todo el sistema de la central de Valencia se quede fuera de servicio.

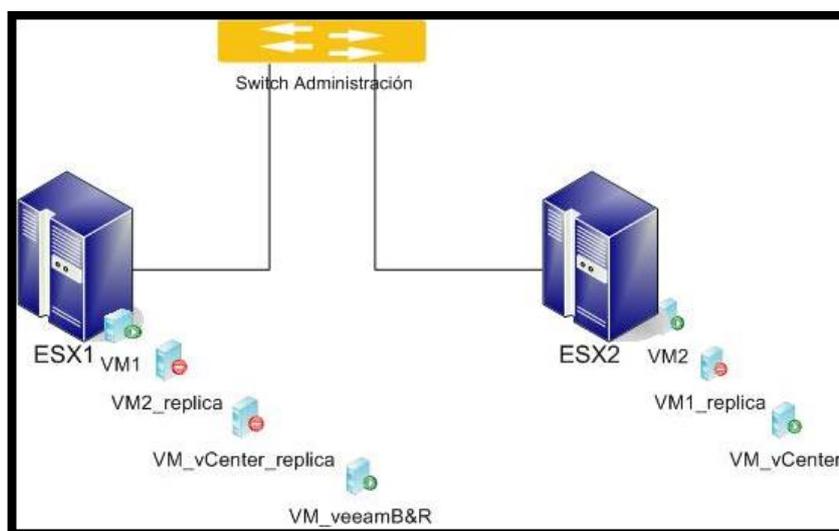


Figura 3.3.2-1 : Entorno de replicación

3.4 Conexión MPLS

Como hemos hablado anteriormente se va a realizar la conexión de ambas sedes a través de una conexión de **MPLS**, a causa de su diferente localización, como se va a efectuar una copia de todos los datos mensualmente, y no se puede perder tiempo en que se realice toda la copia (max. 32TB) mientras se requieran sus servicios, se requiere una buena conexión entre ambas sedes (min. 300Mbps).

MPLS es un protocolo que intenta agilizar el traspaso de información entre redes que no necesariamente deben estar orientadas a conexión. Su capacidad para integrar voz, video y datos, en única conexión, que además nos asegura que posea Calidad de servicio (**QoS**), ha conseguido en parte, sustituir a anteriores tecnologías, sobretodo porque permite empaquetar más datos en el mismo ancho de banda y reducir los costes de la red. Por eso podemos decir que se trata tecnología de red efectiva en costes, rápida y altamente escalable.

Es un estándar IP basado en la conmutación de etiquetas, es una tecnología que permite a cada nodo (Switch/Router), asignar una etiqueta a cada uno de los elementos que traspasan la red, y que es capaz de transmitir esa información a los nodos vecinos, esta etiqueta es de pequeño coste, y es transportada en una cabecera para identificar que paquete es.

La tecnología es una red mallada, compuesta por distintos elementos con diferentes funciones:

- **LER** (Label Edge Router o enrutador frontera de etiquetado)
- **LSR** (Label Switching Router o enrutador de conmutación de etiquetas)
- **LSP** (Label Switched Path o intercambio de rutas por etiqueta) un camino MPLS, es decir, un túnel entre los extremos. Un LSP es unidireccional.
- **LDP** (Label Distribution Protocol o protocolo de distribución de etiquetas): un protocolo para la distribución de etiquetas MPLS entre los equipos de la red.
- **FEC** (Forwarding Equivalence Class o clase de equivalencia de reenvío): nombre que se le da al tráfico que se encamina bajo una etiqueta.

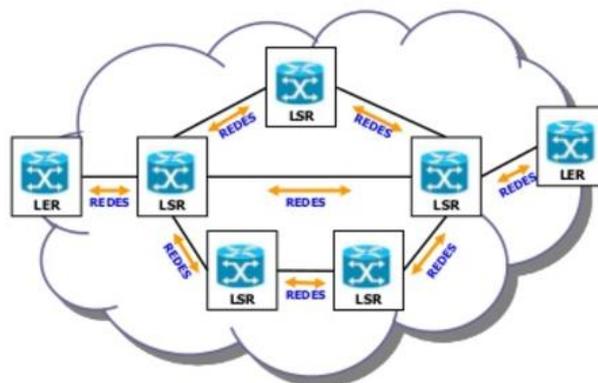


Figura 3.4-1 :Estructura de una red MPLS

Además, una red MPLS es aconsejable para conectar dos puntos muy alejados porque conlleva las siguientes ventajas ante otros tipos de red:

- **Ahorro de costes:** Gracias a las ventajas habladas anteriormente, una red MPLS implicará un coste menor a una ATM o Frame Relay ya que el video, voz y datos se transmiten por un único canal.
- **Facilidad de administración:** MPLS se configura en el router del proveedor del servicio. Es decir solo se instalan dos routers MPLS (uno en cada extremo de la red). Esto implica que solo son necesaria la administración de estos dos routers.
- **QoS:** MPLS nos permite clasificar el tráfico, gracias a su etiquetado, lo que conlleva a una priorización del tráfico a tiempo real.
- **Escalable:** MPLS permite añadir sedes de manera sencilla, ya que como hemos mencionado anteriormente solamente es necesario un router en cada extremo.
- **Redes privadas:** MPLS es muy similar a las redes VPN, que es una tecnología que nos permite crear una red privada entre dos lugares geológicamente distintos utilizando una vía pública, a diferencia de esto MPLS viaja a través de la red del proveedor contratado.

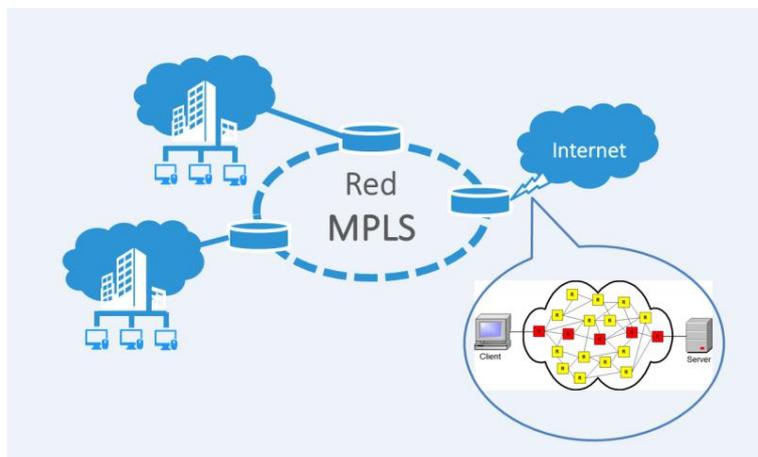


Figura 3.4-2 : Red MPLS

Capítulo 4. Infraestructura de alta disponibilidad

4.1 ¿Qué es alta disponibilidad?

En los entornos de red hoy en día, hay un factor muy relevante, desde el punto de vista operativo, éste es la alta disponibilidad de la red que posee una empresa, por consecuencia podremos hablar de la alta disponibilidad del servicio que ofrecen.

Actualmente, en la mayoría de empresas se ha cambiado el modelo antiguo en las cual los servicios operaban durante 8 horas, 5 días a la semana, a un modelo más ambicioso en los que estos servicio operan 24 horas, todos los días de la semana (**24x7**). En este modelo en que los servicios deben estar continuamente disponibles, es necesario hablar de alta disponibilidad, para ello se han ido desarrollando técnicas para alcanzar un 100% de disponibilidad. En un marco teórico, es posible, pero en un marco práctico no ya que hay una probabilidad de que el sistema o cualquier componente falle. Por lo que actualmente se habla de la teoría de los 3 "9", en el cual se consigue un 99,99% de disponibilidad, lo que nos deja un tiempo caído de 5 minutos al año.

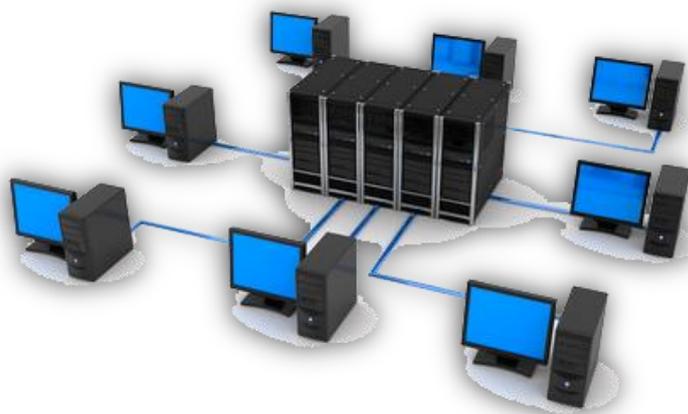


Figura 4.1-1: Entorno de alta disponibilidad

Como se citó anteriormente para poder hablar de alta disponibilidad es necesario también hablar de tiempo de inactividad, dividido en tiempo de inactividad planificado y no planificado.

El tiempo de inactividad planificado es aquel que es necesario para que el sistema siga funcionando correctamente, está basado en el mantenimiento de Hardware y software de los componentes, es perjudicial para la disponibilidad de los servicios y no puede ser evitado por ninguna configuración del sistema.

El tiempo de inactividad no planificado se define como, un evento que no es esperado por el sistema, como es un fallo grave de software o hardware, o factores externos como pueden ser desastres medioambientales.

Por el tiempo de inactividad, se debe considerar ciertos problemas que puede alcanzar una red de alta disponibilidad.

4.1.1 Problemas en alta disponibilidad

Hay problemas que son inevitables cuando se diseña una red de alta disponibilidad ya que no son dependientes del servicio ofrecido, sino que son obligatorios ya sea por paso del tiempo, fallo de seguridad, actualizaciones nuevas o fallos externos a la red. Por ello es necesario tenerlos en cuenta cuando se diseña una red, porque puede implicar que el sistema a diseño no sea correcto.

Entre los problemas que puede poseer una red de alta disponibilidad, encontramos los siguientes:

- Enlaces no duplicados, depender de un único punto de error (solucionable)
- Tiempo de reparación y sustitución de Hardware
- Condiciones medioambientales incorrectas
- Actualizaciones del sistema
- Error humano
- Reinicios o conmutación de servicios

4.3 Herramientas para conseguir una alta disponibilidad

Para minimizar el tiempo de inactividad y los problemas en alta disponibilidad se han desarrollado herramientas, que conjunto a un buen mantenimiento de la red se puede conseguir poseer servicios accesibles 24x7, que es el objetivo que cualquier empresa plantea.



Figura 4.3-1: Herramientas de alta disponibilidad

4.3.1 CLUSTER

La tecnología de los clústeres nos permite un diseño para favorecer la disponibilidad, ya que podemos servicios de aplicación de conmutación por error.

Los clústeres tienen una configuración llamada alta disponibilidad que nos permite conseguir redundancia y protección contra fallos del sistema, una de las medidas más frecuentes en este uso es replicar los sistemas más críticos, en caso de un servidor, se emplean medidas se explicarán más adelante como lo son, el sistema raid, tarjetas de red redundantes, fuentes de alimentación redundantes, etc..



Figura 4.3.1-1: Clústeres

Un clúster de alta disponibilidad es un conjunto de dos o más servidores, que comparten uno o varios sistemas de almacenamiento, y que gracias a algunas herramientas de software (**VMware vMotion**) son capaces de traspasar información entre ellos en tiempo real. Por lo que, si se produce un error de hardware, es capaz de pasar el servicio que estaba ejecutando un servidor a otro sin problema. Y además reparte la carga de manera equitativa entre los elementos disponibles del clúster. El clúster además posee diferentes tipos de configuraciones dependiendo del objetivo que queramos alcanzar:

- Configuración activo/activo: Una configuración activo/activo es aquella en la que cada componente del clúster, posee la misma cantidad de recursos y todos ellos pueden acceder a ellos de manera independiente. Esta configuración es muy útil ya que reparte la carga de los servicios entre los tres servidores, pero en caso de fallo de hardware de uno de los servidores, puede sobrecargar, al resto, ya que deberían de coger la carga del que ha fallado.

- Configuración activo/pasivo: Una configuración activo/pasivo es útil si el nivel de carga es pequeño ya que todos los recursos los posee un único servidor, y el Slave (servidor secundario) únicamente puede coger recursos cuando el Master (primer servidor) no está disponible, en esta configuración no se produce degradación en el servicio en caso de fallo de Hardware, pero si la carga es muy grande el servidor Maestro puede desbordarse.

4.3.2 Equilibrio en carga de red

El equilibrio de carga de red o **NLB** es una característica perteneciente a Sistemas Operativos como Windows Server, y que están basados en proporcionar una alta disponibilidad y escalabilidad a aplicaciones del servidor, basadas en internet, como son: Proxy, firewall, VPN, DNS, etc.

La tecnología **NLB** permite que todos los equipos dentro del clúster puedan ser controlados desde un conjunto de direcciones IP, por lo que, si un host cae, el equipo que controle este host cogerá los recursos del host inactivo y los asignará automáticamente a otro host.

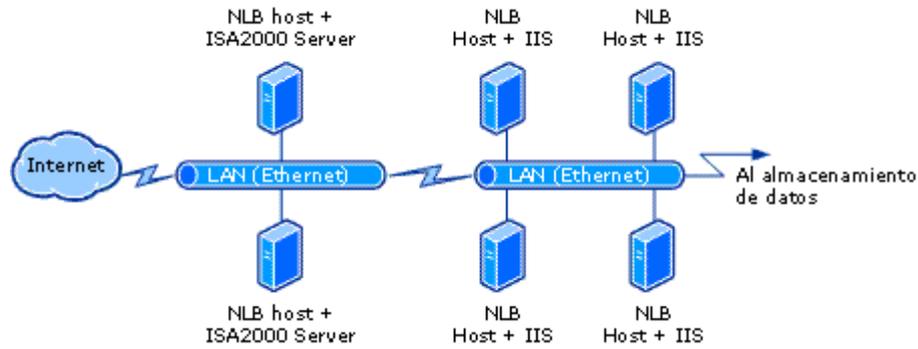


Figura 4.3.2-1: Funcionamiento NBL

La red NLB consigue por su parte, el objetivo que se necesita, gracias a sus características conseguimos una buena alta disponibilidad, éstas son:

- Detectar y recuperar un host de clúster en el que se produce un error o que se queda sin conexión.
- Equilibrar la carga de la red cuando se agregan o quitan hosts.
- Recuperar y redistribuir la carga de trabajo en diez segundos.

4.3.3 Controlar el nivel de servicio

Es imprescindible delimitar la carga que pueden ejercer los servicios ante nuestro host, por lo tanto es importante revisar de manera exhaustiva como las aplicaciones de nuestro servicio van a medrar el servidor, ya que una mala gestión de la carga proporcionada por las aplicaciones, puede llevar a un desbordamiento y una posterior caída del servicio.

4.3.4 Reducir el tiempo de inactividad

El estudio de los datos recopilados sobre el tiempo de inactividad, es una función en la que se debe llevar a cabo un riguroso estudio, ya que es el factor más relevante para una alta disponibilidad, averiguar porque se produce, y en qué momento, puede ayudar a minimizarlo.

4.3.5 Copias de seguridad

La posibilidad que se produzca un error en una red es irremediable, y dependiendo del tipo de error, producirá una pérdida de datos de diferente tamaño, en consecuencia la pérdida de los datos de un cliente, o de recursos críticos es muy grave para una empresa, por lo no debe pasar, para ello, existen la tecnología de las copias de seguridad de diferentes tamaños y niveles.

A nivel de disco existe la tecnología **RAID** (Redundant Array of inexpensive Disk), es un sistema de almacenamiento que utiliza diversos discos duros, generando un volumen total de ellos, y almacenando datos repartidos entre los discos e incluso replicando la información. Esta tecnología actualmente, está muy demandada prácticamente entre el almacenamiento de todo servidor, ya que aporta integridad a los datos, tiene tolerancia a errores y un buen rendimiento.

La tecnología **RAID** agrupa varios discos en una sola unidad lógica (volumen), por lo que como veremos más adelante, en configuraciones de software como **VMware** o **Windows Server**, el software ve un único almacenamiento, el cual incluirá varios discos en funcionamiento, algunos en los que esta replicada la información y otros en espera.

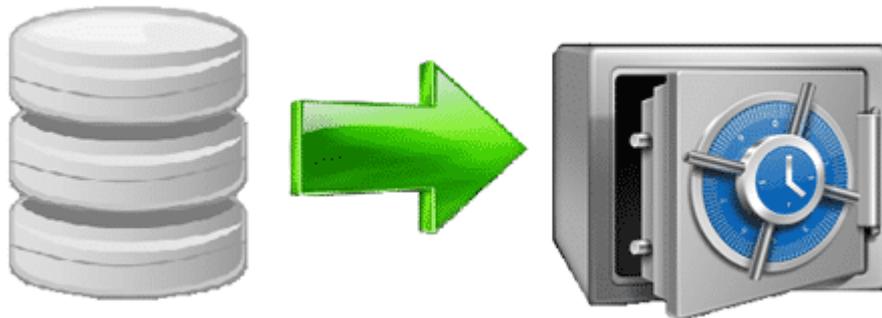


Figura 4.3.5-1: Copias de seguridad

A nivel de datos, existen diferentes software como **Veeam**, o **FBackup**, que realizan copias de seguridad periódicas, dependiendo de la necesidad del usuarios, y que replican estos datos en otros bancos de almacenamiento, ya sea un simple disco duro externo, o algo más complejo como un **NAS**.

A nivel de Sistema Operativo, hay varias herramientas, como **Veeam Backup End Point**, que son capaces de realizar una imagen del sistema operativo de un Host, y enviarla en forma de copia de seguridad a un sistema de almacenamiento externo.

A nivel de Servidor, es más complejo, ya que al realizar una copia de seguridad del mismo, es necesario realizar antes un snapshot antes de realizar una copia de datos, después la herramienta de copia de seguridad, crea en un repositorio externo (el que puede ser otra cabina de datos o cualquier tipo de almacenamiento que tenga conexión FTP). Como añadido, en esta copia de seguridad podremos realizar barridos de manera individual, por lo que podemos recuperar la cantidad de archivos que se desee.

A nivel de Clúster, existen replicaciones de clúster como la que se quiere diseñar en este proyecto, se basa de una copia exacta del sistema entero que produce en otro clúster externo que debe poseer a nivel de Hardware características compatibles.

4.3.6 SAN

Una **SAN** es una red de componentes y dispositivos con la función del almacenamiento, entre los cuales hay una conexión de alta velocidad, que permiten el intercambio de información. Las redes **SAN** están compuestas por:

- Canales de red de fibra o **iSCSI**, dependiendo la velocidad requerida.
- Elementos de almacenamiento de red (discos duros, cabinas, etc).
- Software que las gestiona

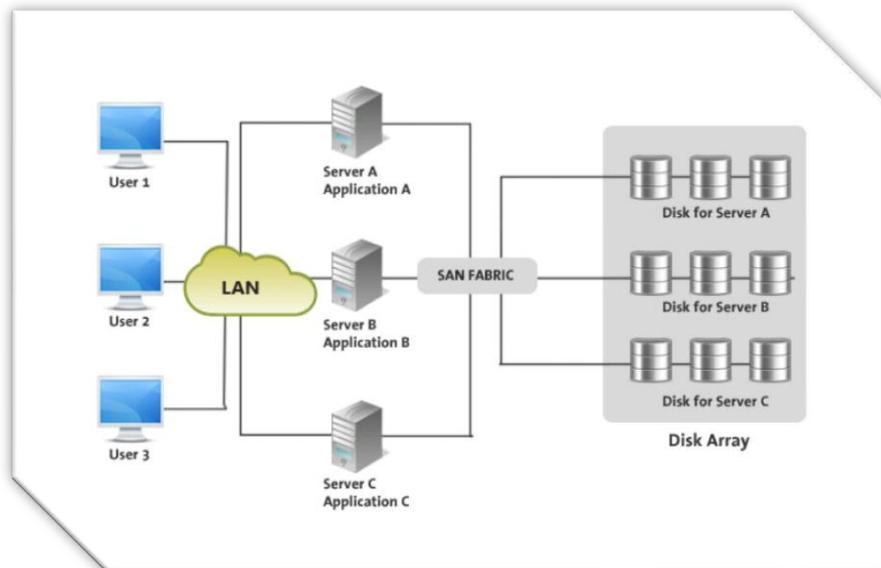


Figura 4.3.6-1 : Almacenamiento SAN

Ventajas y desventajas

El intercambio de datos de una **SAN**, es directamente proporcional al tipo de canales que la interconectan y su tipo de conexión, ya sea fibra o **iSCSI** es una nueva tecnología que envía comandos **SCSI** sobre una red **TCP/IP**, por lo que posee menor velocidad, pero es más económica.

El tráfico de la red **SAN** y los equipos, no se ve afectada por el tráfico de la misma **SAN** ya que el tráfico está separado del usado por el usuario. Los servidores son utilizados por las redes **SAN** para realizar la función de separar el tráfico de ambas y así conseguir que no haya colapso de datos.

La capacidad de almacenamiento de una **SAN** depende de los elementos que lo formen, por lo que podemos afirmar que es ilimitada, ya que podemos aumentar ilimitadamente los elementos que la conforman.

La red **SAN** es una red concebida para el almacenamiento de servidores de las dos formas mencionadas anteriormente (**FC** o **iSCSI**), con lo que nos aseguramos que haya una transmisión rápida y eficiente.

4.3.7 Herramientas de virtualización

La virtualización de la que vamos a hablar en el siguiente punto, es una de las herramientas principales para conseguir alta disponibilidad, gracias a ser versátil con datos y con la compatibilidad con los diferentes sistemas operativos que hay actualmente.

La virtualización está basada en la consolidación de servidores físicos, mediante un software específico, en una representación de un servidor físico en varios servidores virtuales. Cada máquina virtual puede interactuar de forma independiente con otros dispositivos, aplicaciones, datos y usuarios, como si se tratara de un recurso físico independiente. Diferentes máquinas virtuales pueden ejecutar diferentes sistemas operativos y múltiples aplicaciones al mismo tiempo utilizando un solo equipo físico. Debido a que cada máquina virtual está aislada de otras máquinas virtualizadas, en caso de ocurrir un bloqueo esto que no afecta a las demás máquinas virtuales.

Cada herramienta de virtualización posee herramientas que reparten la carga y crean redundancia, para alcanzar una alta disponibilidad.



Figura 4.3.7-1 : Esquema de virtualización

Capítulo 5. Virtualización y posterior instalación VMware

5.1 ¿Qué es y para qué sirve virtualizar?

La virtualización es un concepto que pretende crear una presentación basada en un software en lugar de una física, la virtualización es aplicable a diferentes ámbitos (servidores, almacenamiento y redes), con ella reduce los costes de las instalaciones de las empresas, y además aumenta la efectividad de los servicios proporcionados por las mismas. La virtualización de servidores es una tecnología que permite la utilización de diferentes máquinas virtuales en un único servidor físico, cada máquina virtual es independiente de las otras máquinas virtuales, y se separa del software del servidor, mediante una capa de control llamada hypervisor.

Una máquina virtual es a lo que denominamos, un contenedor con un software aislado, en el que están incluido sistema operativo y aplicaciones. Gracias a ellas podemos ejecutar diferentes softwares, aplicaciones y sistemas operativos en un mismo servidor físico.

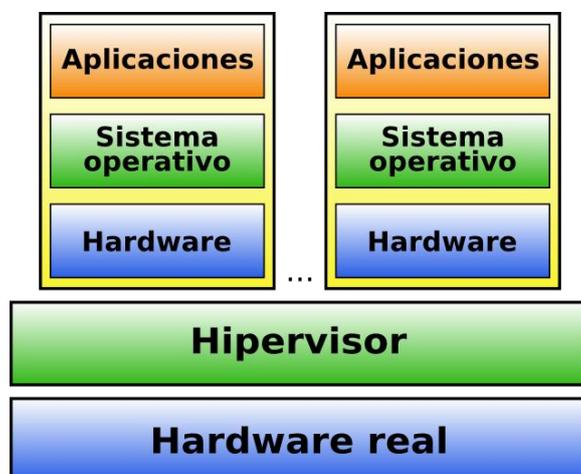


Figura 4.3.7-1 : Esquema de virtualización

La virtualización nos presenta las siguientes ventajas ante un servidor físico:

- **Seguridad:** Cada maquina virtual es totalmente independiente, ya sean sus recursos o aplicaciones. Un ataque generado a una máquina virtual solo afectará a la misma.
- **Flexibilidad:** La compatibilidad con los sistemas operativos, el poder tener máquinas virtuales con diferentes sistemas operativos, y el diseño de disco, memoria, procesador, independiente aporta una flexibilidad muy difícil de encontrar en otro sistema.
- **Agilidad:** la creación de una máquina virtual es sencilla, rápida y eficaz, simplemente consta de poner su nombre, y sus recursos. Podemos generar una sin la necesidad de tener que obtener nada nuevo.
- **Portabilidad:** La configuración de las máquinas virtuales están introducidas en unos ficheros exportables, por lo que es muy fácil mover máquinas virtuales, incluso mover un Data Center entero
- **Recuperación rápida en caso de fallo:** Si se dispone de una copia de seguridad, un snapshot o cualquier otro elemento de seguridad, es muy fácil recuperar la maquina virtual tal cual estaba de manera anterior al ataque, por lo que favorece su restauración.
- **Compatibilidad de programas:** Cuando se utiliza cualquier sistema operativo, es posible que algunas aplicaciones o programas no sean compatibles con el sistema operativo usado, virtualizar permite que eso no pase ya que se puede poseer diferentes sistemas operativos sin interceder los unos con los otros.

Para poder obtener estas características es necesario el sacrificio de recursos ante un servidor físico, o pérdida de rendimiento. Las aplicaciones corren de manera más eficiente en un servidor físico ya que gasta el 100% de sus recursos, pero virtualizando se aprovechará al 100% los recursos del servidor, no de manera óptima como si fuese un servidor físico único, pero si, en forma de gastar diferentes tipos de aplicaciones y usos. esta pérdida se produce por la configuración y el gasto que produce el hypervisor en nuestro servidor virtualizado.

5.2 VMware y sus componentes

Hay diferentes software de virtualización, ya sea de escritorio, aplicaciones o servidores, los más conocidos son VMware (VMware), VirtualBox (Oracle) o Hyper-V (Microsoft), todos ellos han desarrollado su software de virtualización y cada una posee unas herramientas diferentes para alcanzar la mayor eficiencia de recursos. Para este proyecto se ha optado por el software de virtualización VMware vSphere.

VMware vSphere es una plataforma de virtualización utilizada para construir infraestructuras de cloud. Permite ejecutar aplicaciones críticas de manera eficiente y segura y responder con rapidez las necesidades de la empresa.

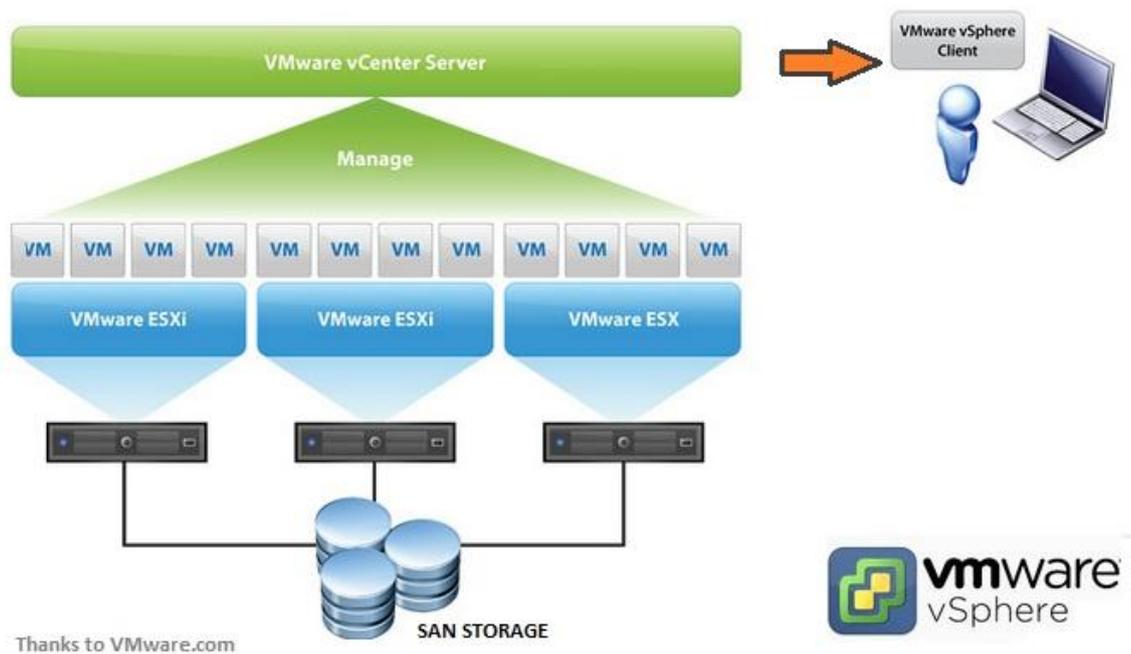


Figura 4.3.7-1: Estructura VMware vSphere

vSphere tiene unas funciones muy definidas de las cuales, más adelante en el punto 5.5 se enseñara a configurar las correspondientes a alta disponibilidad y reparto de la carga, las características del VMware vSphere son:

- **VMware vSphere ESXi™** (explicado en el punto 5.2.1) es una capa situada entre el servidor físico y las máquinas virtuales su función a desempeñar, es el manejo de estas máquinas virtuales, repartiendo sus recursos e incluso compartir un mismo recurso.
- **vSphere Virtual Symmetric Multiprocessing (SMP)** permite utilizar máquinas virtuales con 32 CPU virtuales.

- **vSphere Auto Deploy** permite generar de manera rápida y en segundo plano otros host de vSphere que se vayan ejecutando en el hipervisor ESXi.
- **vSphere Virtual Machine File System (VMFS) 5** permite a las máquinas virtuales acceder a los dispositivos de almacenamiento compartido (Fibre Channel, iSCSI, etc.). Constituye una tecnología esencial para otros componentes de vSphere, como vSphere Storage vMotion.
- Las VMware Storage API permiten la integración con soluciones de protección de datos, multipathing y arrays de discos de terceros.
- **vSphere Distributed Resource Scheduler (DRS)** balanceo de carga en cuestión de máquinas virtuales. Está automatizada basándose en políticas ya aconsejadas por VMware o hechas por el usuario, esto ayuda a lo que se mencionaba anteriormente, acuerdos a nivel de servicio.
- **VMware Distributed Power Management (DPM)**, es un añadido de DRS, automatiza el uso eléctrico del clúster gracias al balanceo creado por el DRS, mejora la utilización de la energía eléctrica de los servidores.
- **vSphere vNetwork Distributed Switch** simplifica y optimiza la red en los entornos de VMware, de manera añadida, es capaz de utilizar Switches de otros fabricantes.
- **vSphere vStorage Thin Provisioning** proporciona un balanceo dinámico del almacenamiento compartido en tiempo real.
- **vSphere Storage I/O Control** establece las prioridades de calidad de servicio del almacenamiento para garantizar el acceso a los recursos de almacenamiento.
- **vSphere Profile-Driven Storage** reduce los pasos para la selección de los recursos de almacenamiento agrupándolos conforme a una política definida por el usuario.
- **VMware Network I/O Control** establece prioridades de calidad de servicio de red para garantizar el acceso a los recursos de red.

Para este proyecto se ha escogido la versión 5.5.0-20140902001 del software de VMware vSphere, con el pack ofrecido por VMware vSphere Enterprise Plus, que incluye las siguientes características:

- VMware vSphere Virtual SMP de 32 vías
- VMware vSphere Distributed Switch,
- VMware Host Profiles,
- VMware vSphere Auto-Deploy,
- VMware vSphere Storage I/O Control,
- VMware vSphere Network I/O Control,
- VMware vSphere Profile-Driven Storage
- VMware vSphere Storage DRS.

5.2.1 VMware ESXi

VMware es una plataforma de virtualización a nivel de centro de datos producido por VMware, Inc.. Es el componente de VMware de nivel más bajo ya que se encuentra bajo la capa de virtualización, llamada hipervisor y posee herramientas y servicios de gestión autónomos e independientes. Se compone de un sistema operativo basado en Linux, que gestiona administra y ejecuta las funciones del hipervisor, y los servicios y servidores que permiten la interacción con el software de gestión y administración y las máquinas virtuales. Sus funciones principales son:

- **Seguridad y confiabilidad mejorada:** La administración del ESXi está integrada en VMkernel, lo que nos permite reducir su tamaño a solo 150 MB. Esto proporciona una gran seguridad ya que es una superficie muy pequeña para recibir malware y amenazas por la red.
- **Implementación y configuración optimizadas:** Pocas opciones de configuración, ya que pretende ser un software sencillo y que se pueda utilizar de manera óptima y rápida.



Figura 5.2.1-1: Función ESXi

- **Sobrecarga de administración reducida:** El ESXi se encarga de monitorizar el hardware y administrar el sistema basado en interfaces de programación de aplicaciones (**API**). Estas tareas se encuentran en líneas (**CLI**) por las que también se pueden controlar el ESXi además de por vSphere Server que gracias a una conexión a través de PowerShell podemos configurarlas.
- **vMotion:** La migración en vivo de VMware vSphere permite migrar una máquina virtual completa de un servidor físico a otro sin tiempo fuera de servicio.

5.2.2 VMware vCenter Server

El servidor de vCenter actúa como un único punto de administración central en el entorno de vCenter Server. Este software consiste en una cantidad de módulos y servicios instalados sobre un servidor con sistema operativo Windows Server. La versión vCenter 5 incluye una nueva versión de vCenter Server para entornos con Linux. vCenter Server ofrece nuevas herramientas como VMware Distributed Resource Scheduler (**DRS**), VMware High Availability (**HA**), VMware Fault Tolerance(**FT**), **VMware vMotion** y **VMware Storage vMotion**.

En un vCenter Server puedes integrarse 1000 host ESXi (1000 servidores físicos virtualizados) y aproximadamente 15.000 máquinas virtuales de las que 10.000 podrán estar en funcionamiento, siempre y cuando las características del hardware tengan recursos suficientes para mover estas máquinas. En caso de que necesites más ESXi para gestionar se deberá comprar otra licencia de vCenter y en la función que se muestra en la siguiente imagen, marcar que forman parte de un conjunto de vCenter server, en cuyo máximo son 10 vCenter conectados simultáneamente.

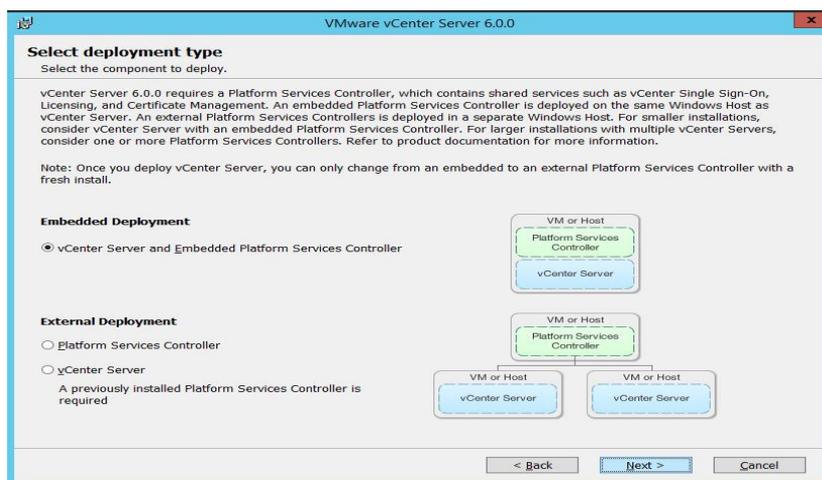


Figura 5.2.2-1: Configuración vCenter Server

Para poder desplegar este Appliance en tu entorno virtual tendrás que formatear el disco y asignar un mínimo de RAM requerida para que arranque el Appliance. No es posible conectar vía Linked mode dos vCenter Servers con versiones diferentes.

Los requerimientos mínimos para vCenter Server 5 son :

- 2CPUs de 2Ghz de 64bits
- Mínimo 4GB de memoria RAM
- 4GB de espacio en disco duro mínimo.

Hay tres componentes adicionales al vCenter Server que pueden ser añadidos al servidor de vCenter cuando sean necesarios:

- VMware vCenter ESXi Dump Collector
- VMware vSphere Web Client
- VMware vSphere Update Manager

vCenter Server 5 requiere que la conectividad ODBC que se crea antes de instalar el servidor de vCenter. Este ODBC para conectar la base de datos con el vCenter, no es el mismo que el que se usa para conectar el vCenter con Update Manager.

En VMware vSphere™ ESXi es posible usar VMware Update Manager 5 para hacer actualizaciones del nuevo servidor vCenter Server Appliance. Recuerda que para poder hacer estas actualizaciones, primero has de configurar el vCenter Server Appliance para permitir actualizaciones desde la pestaña de Update en vCenter Server Appliance.

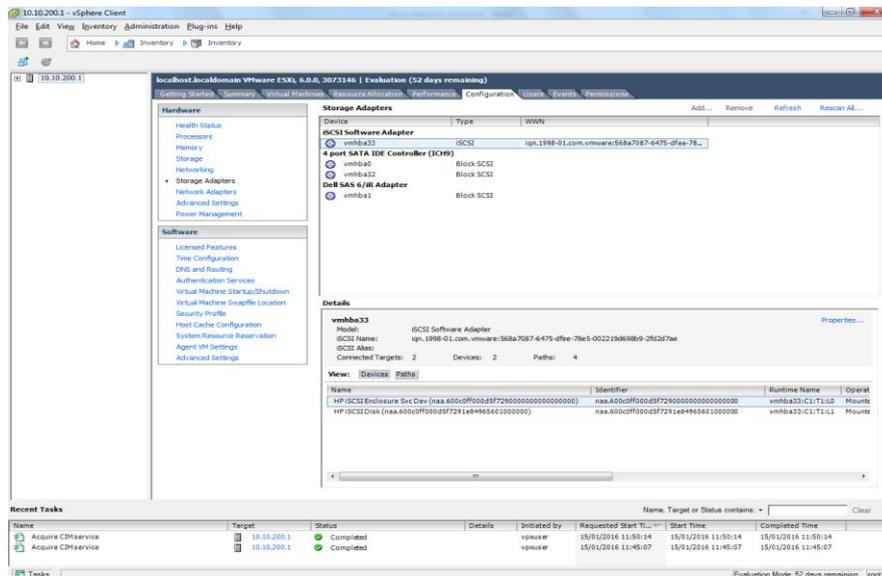


Figura 5.2.2-2 : VMware vCenter Server

5.2.3 VMware vSphere Web Client

VMware tiene la idea de sustituir el antiguo VMware vCenter Server por una Web que trabaja de la misma manera, y que a partir de la versión 6.5 será la única disponible, esta Web nos permitirá de la misma manera que el vCenter, gestionar nuestros host, las conexiones de red, internas y externas, las herramientas que posea la licencia de VMware adquirida, y además incluyendo una nueva función, el vSphere Update Manager que actualizará el sistema de VMware a la última versión de la que se posea licencia. Esto automatizará tener que migrar versiones a base de comandos o por la introducción de parches, sobretodo ocasionará que no se produzca parada en esta migración de ESXi.

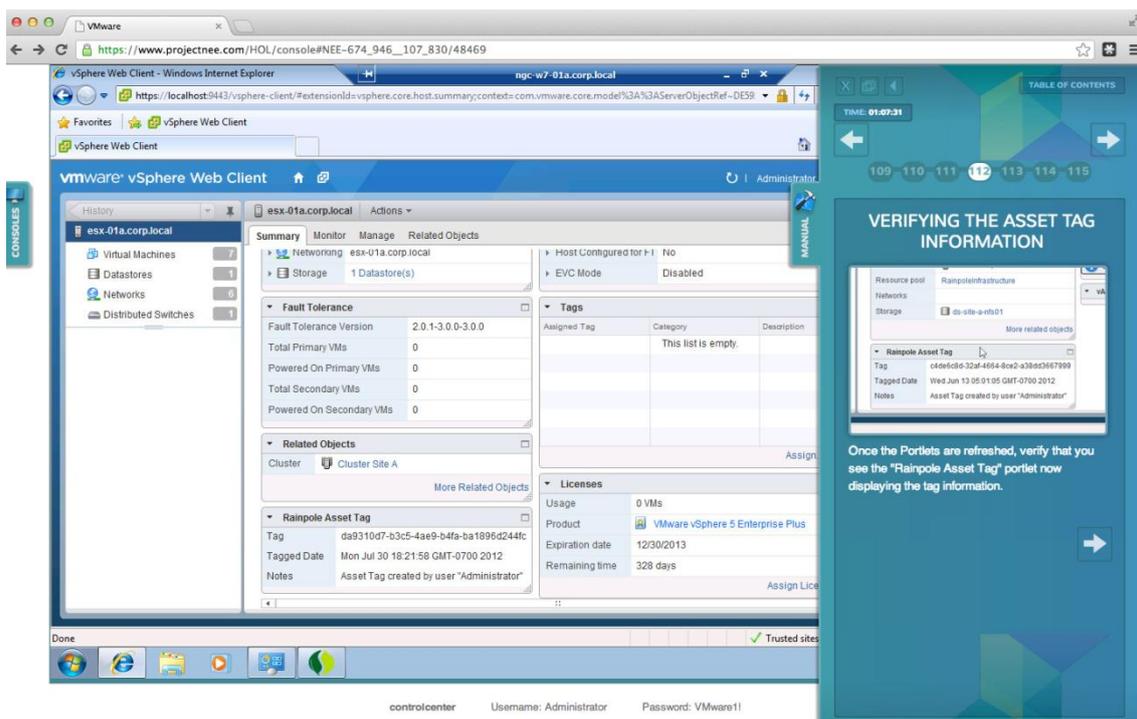


Figura 5.2.3-1: VMware vSphere Web

5.3 Configuración de componentes

A la hora de realizar la instalación cada componente tiene que indicar que es necesario una exhaustiva configuración de cada uno de ellos, ya que para un correcto comportamiento todos los componentes deben estar configurados correctamente.

5.3.1 Configuración de la cabina de discos

La cabina HP MSA2040 posee dos controladoras y la posibilidad de albergar 24 discos con la opción **hot and plug** (montaje o sustitución en caliente) las cuales ayudarán en caso de que uno de los discos incurran en error, o esté inactivo. Además posee 3 opciones de conexión a la red, una opción de **FC** de 8Gb o 16Gb, una conexión **iSCSI** de 1 o 10 GB y por último una conexión de 10 Gb en conexión **SAS**.



Figura 5.3.1-1 : Cabina MSA 2040

La cabina posee, un puerto de Management, al cual se conectará para poder realizar la primera configuración y que quedará conectado a través de Ethernet al servidor, para posteriores configuraciones o posibles cambios a realizar. La MSA 2040 viene configurada por DHCP, así que asignará una IP, para la primera conexión.



Figura 5.3.1-2: Configurador MSA 2040

La cabina nos permite cambiar entre el antiguo configurador (versiones anteriores de MSA) y el nuevo, se entra a través de la siguiente configuración:

- Name: manage
- Password: !manage

Una vez entrado en el configurador de la cabina MSA 2040, se pasa a crear un nuevo Pool con los discos de la cabina a estudio, para ello accedemos la pestaña Pools que se entra a la izquierda del configurador.



Figura 5.3.1-3 : Pestaña Pools

Y pasaríamos a crear el grupo de discos, así que se selecciona la acción **ADD DISK GROUP**, donde podemos seleccionar, cuantas pools se van a requerir y que nivel de raid se precisa para el sistema, en este caso se seleccionará un RAID 5 con todos los discos que se poseen, de los cuales se quedarán 3 en espera por si se reproducen errores en cualquiera de los anteriores.

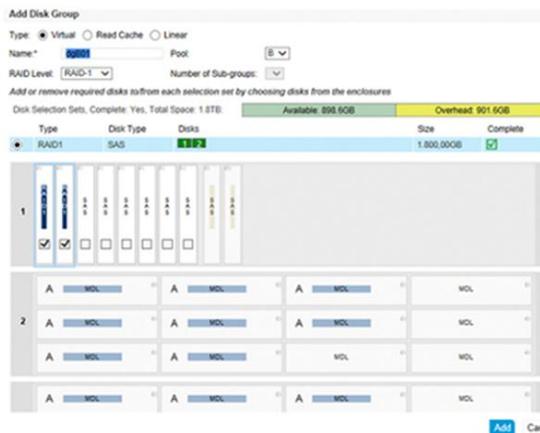


Figura 5.3.1-4: Configurador de discos

Y se observa que crean ambos, uno por cada controladora para conseguir que ambas controladores controlen toda la información y de esa manera en caso de error o caída de una de ellas, no se produzca una parada, consiguiendo así alta disponibilidad.

Name	Health	Class	Total Size	Avail	Volumes	Disk Groups
A	OK	Virtual	15.8TB	15.8TB	3	1
B	OK	Virtual	2893.3GB	2836.9GB	2	2
Linear 1	OK	Linear	899.2GB	779.2GB	2	1

Name	Health	Pool	Class	RAD	Disk Type	Size	Free	Current Job	Writ	QoS
sg001	OK	B	Virtual	RAD1	SAS (Standard)	842.9GB	842.9GB	INT (10%)	FTOL	2
sg002	OK	B	Virtual	RAD1	SAS HDL (Archive)	1896.2GB	1896.2GB	INT (4%)	FTOL	2

Figura 5.3.1-5 : Pools ya creadas

Para que el sistema de alta disponibilidad pueda reconocer estos pools es necesario realizar volúmenes virtuales de ellos, para ello es necesario situarse en la pestaña **Volumes**, y seleccionar la acción Create Virtual Volume.

Volume Name	Size	Copies	Pool
Vol_Virtual	100GB	2	B

2 new volumes will be created, 0 in pool A (0.0GB), 2 in pool B (200.0GB). Volumes with multiple copies will have a numeric suffix appended to the name shown.

Figura 5.3.1-6: Creación de Volúmenes

A continuación, se pasa a dar nombre al volumen, el pool o pools que se quiera asignar a estos volúmenes, y cuantos volúmenes iguales se quieren crear

Y nos aparece una pestaña en la que podemos seleccionar el nombre que le vamos a dar al volumen, el pool al que lo vamos a asignar y número de copias (en el caso de que vayamos a crear más de uno)

Name	Health	Class	Size	Allocated	Group	Pool	Type	Snapshots	Maps	Schedules
ISOFS	OK	Virtual	49.9GB	8078.2MB	Volume_group1	A	base	0	1	0
Linear 1_v0001	OK	Linear	99.9GB	99.9GB	-ungruoped-	Linear 1	master volume	1	0	0
Linear 1_v0001_v0001	OK	Linear	99.9GB	99.9GB	-ungruoped-	Linear 1	snapshot	0	0	0
tplinear 1_v0001	OK	Linear	19.9GB	19.9GB	-ungruoped-	Linear 1	snap pool	0	0	0
TEST_DIRECT_ACCESS	OK	Virtual	199.9GB	130.0GB	-ungruoped-	A	base	0	1	0
Vol0003	OK	Virtual	999.9GB	190.7GB	DEMO1	B	base	0	1	0
VOL_TEST1	OK	Virtual	399.9GB	117.0GB	Volume_group1	A	base	0	1	0
Vol_Virtual0005	OK	Virtual	99.9GB	99.2GB	DEMO1	B	base	0	1	0
Vol_Virtual0001	OK	Virtual	99.9GB	43.3GB	DEMO1	B	base	0	1	0

Figura 5.3.1-7 : Volúmenes creados

Después de crear los volúmenes, ya sólo queda presentárselos a los hosts.

Para ello en el VMware vCenter Server, es necesario presentarle estos volúmenes creados en la cabina para ello. Dependiendo del tipo de conexión es necesario un tipo de configuración u otra, en caso de **FC** la conexión es "semiautomática", ya que gracias a la tecnología de VMware, detecta de manera directa los puertos de FC y sus conexiones con la cabina, por otra parte la conexión **iSCSI** es algo más compleja por lo que se pasará a explicar.

Para ello en la pestaña configuración de cada servidor, en el apartado **Storage Adapters**, se puede crear el adaptador, y si lo está se modifica y se va al apartado **Dynamic Discovery**:

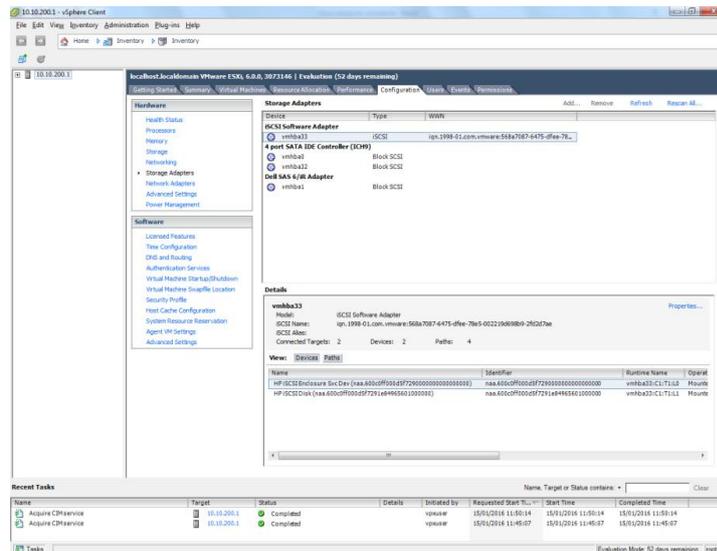


Figura 5.3.1-8 : Mapeo puertos iSCSI

En Dynamic discovery indican las IP del iSCSI configurado anteriormente, y se introducen las IP de la controladora A y B :

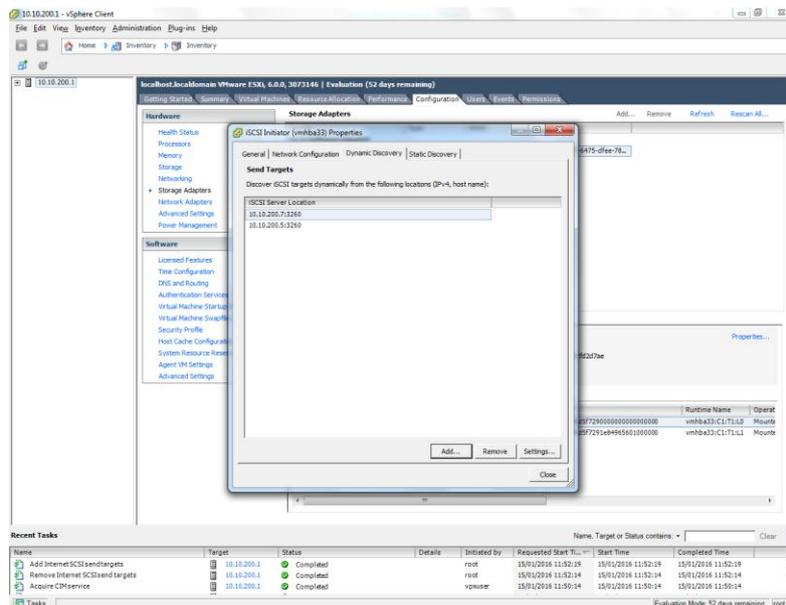


Figura 5.3.1-9: Introducción de IP para búsqueda

El programa exige un escaneo después de la nueva configuración, donde encuentra los nuevos puertos de la configuración proporcionada, indicando el identificador, que es único en cada puerto de iSCSI, el nombre de cada puerto y de qué manera están operando en el sistema, una vez descubiertos pasamos a añadirlos al inventario, para que se pueda asignar este almacenamiento a las maquinas virtuales que se quieren generar.

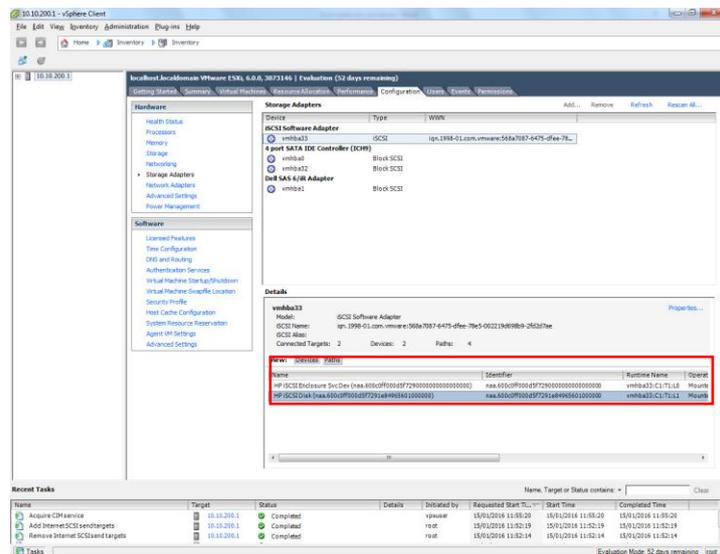


Figura 5.3.1-10: Descubrimiento de puertos iSCSI

Luego se pasa al apartado de Storage y pulsamos Add Storage:

Se indica que es de tipo LUN, y a continuación es darle a next repetidamente se indica el nombre al volumen que se quiere identificar y por último de indica que ocupe todo el espacio del disco, hecho esto ya está identificado el volumen deseado:

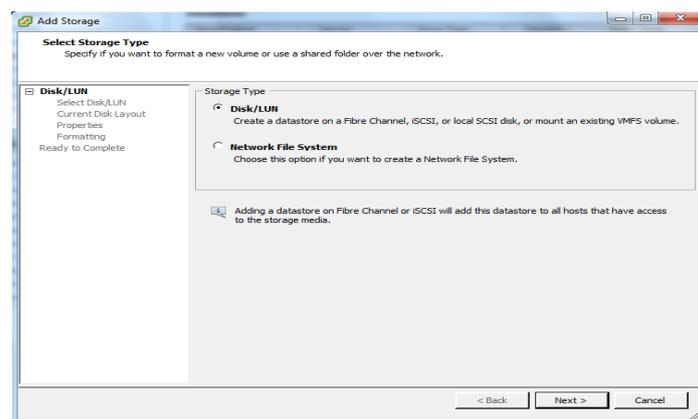


Figura 5.3.1-11: Creación volumen VMware

5.3.2 Configuración de la NAS

La solución que proporciona HP, para su **NAS** es muy eficiente, ya que el **NAS HP StoreEasy 1650** es un "mini" servidor, el cual se preinstalado un Windows Server 2012 R2 con configuración encarada para el almacenamiento, por lo que su configuración es muy rápida y eficaz. Es necesario conectar directamente un ratón y un teclado a este componente desde donde, con un gestor generado por la propia compañía HP, permite crear una primera configuración bastante completa, donde se puede indicar el reparto de discos, **RAID**, volúmenes, y el almacenamiento dependiendo de las características que se requieren en el sistema.

Una vez realizada la primera configuración, se puede observar que el comportamiento de esta **NAS** es el mismo de un servidor, por lo que se puede configurar como tal, y se agregará como Storage al sistema como un elemento de red, no como un servidor, para ello se recomienda asignar una IP fija, ya que como todo el sistema, se recomienda el uso de IP's fijas para evitar problemas en el DHCP.

Por lo que en el sistema de copias de seguridad se planteara como un Windows Server más, lo que es beneficioso para la realización de la copia, ya que el software de copias de seguridad elegido (**Veeam**), trabaja de manera más rápida y eficaz con servidores que con servicios de almacenamiento (**NAS**). Por último, cabe destacar que la conexión de este elemento con el sistema se realizará a través de Ethernet, y que este almacenamiento servirá para realizar las copias de seguridad, de nivel 2.



Figura 5.3.2-1 NAS, HP Storage 1650.

5.4 Maquinas Virtuales

Una maquina virtual es un software que simula un sistema operativo y que permite la ejecución de programas, como si se tratase de un elemento físico. El desarrollo de las maquinas virtuales surgió por la necesidad de reducir el espacio físico, ya que se puede reducir 1000 ordenadores a una sola máquina. Las máquinas virtuales se caracterizan por los recursos asignados a ella, que limitan sus servicios, entre las maquinas virtuales no hay conexión por lo que son totalmente independientes las unas de las otras, lo que aporta mucha seguridad ya que a pesar de estar en el mismo entorno físico, un ataque a una de ella, no ocasiona repercusión en el resto. La mayoría de empresas líderes en el sector de la informática ya han desarrollado herramientas para el uso de máquinas virtuales, Microsoft (Hyper-V), Oracle (VirtualBox), etc...

En este proyecto, se decantó por utilizar la herramienta VMware para el desarrollo de estas máquinas virtuales, gracias a las características mencionadas anteriormente.

Para comenzar la configuración del sistema, se realizará una primera configuración inicial en el servidor, donde gracias a la tecnología de HP, se convierte en una primera tarea fácil, donde permite la configuración las tarjetas de red (IP, submascara de red, etc...), actualizar el software, configuración de la ILO, etc. Una vez realizada la configuración inicial del servidor, se procederá a instalar la imagen (en cuanto a esto es aconsejable realizar esta instalación con la imagen de VMware que proporciona HP, ya que está preparada para lanzarse en este tipo de servidores.

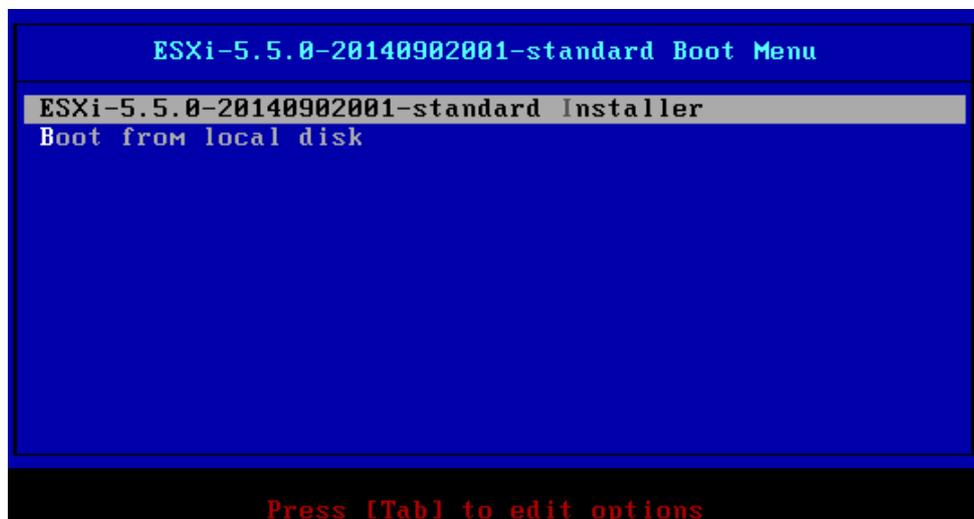


Figura 5.4-0-1: Instalador VMware ESXi

Procedemos a instalar el ESXi donde requiere que se borre el disco, se aprueben los certificados, indicar un usuario y contraseña para el acceso al ESXi directo (importante guardarlo) . Una vez realizada la instalación pasaremos a la configuración del ESXi.

Se conecta ratón y teclado de manera directa al servidor, y en el monitor aparecerá la siguiente pantalla:

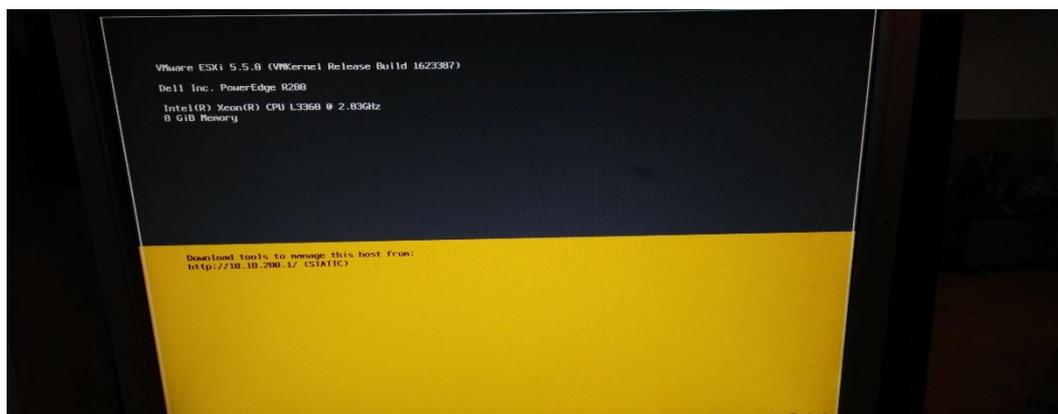


Figura 0-2 : Configurador ESXi

En este configurador se encuentran opciones básicas como indicar la IP en la que se va a encontrar el ESXi instalado, configuración de tarjetas de red y activación de las mismas, y la opción más importante habilitar el protocolo SSH para conexiones a través de comandos. Una vez realizada la configuración oportuna se pasa al VMware client donde se generará la primera máquina virtual.

5.4.1 Creación de la maquina virtual (inventario)

Una vez realizada las configuraciones anteriormente comentadas se pasa al VMware Cliente que se presenta con la siguiente pantalla:



Figura 5.4.1-1: VMware Client

En la cual, se debe introducir la IP mencionada anteriormente en la configuración del ESXi, y a partir de ahí, se realizará desde un ordenador con el mismo rango de IP del servidor, la conexión al mismo, a partir de ahí, se debe seleccionar el servidor al que estamos conectados y generar una primera máquina virtual.

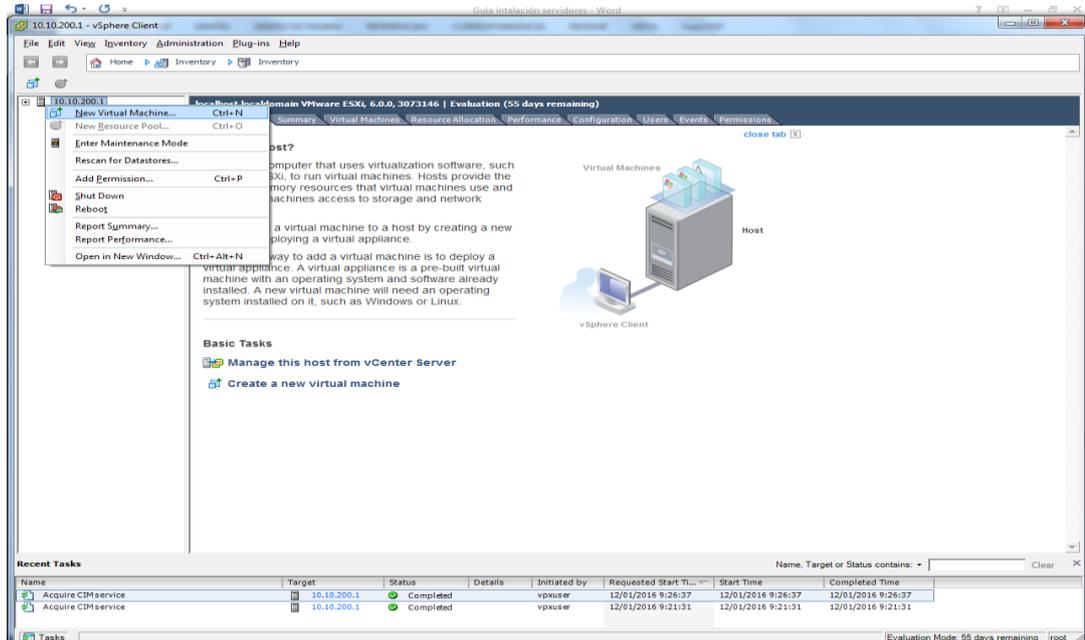


Figura 5.4.1-2 : Creación de la primera máquina virtual

En esta máquina virtual se va a instalar el software del VMware vCenter Server, por lo que le serán necesarias las siguientes características mínimas en las que serán recomendable, ampliarlas ligeramente .

- CPU: Dos procesadores dual-core
- Procesador: 2.0 GHz
- Memoria RAM: 4GB (Recomendable 8 si es la versión 6.0)
- Disco duro: 16 GB de memoria interna.

Todas estas quedan configuradas en el configurador que proporciona VMware a la hora de crear cada máquina virtual. Como detalle y que será necesario en la máquina virtual generada para las copias de seguridad. Se debe añadir como unidad local, el volumen que se ha creado anteriormente en el apartado 5.3, porque para añadirla como repositorio, es necesario que tenga una conexión local a la cabina.

5.4.2 Puesta en marcha de la máquina virtual

Una vez realizada la configuración de la máquina virtual, es necesario subir la imagen de un sistema operativo (en este caso **Windows Server 2012**), la cual se utilizará como medida de arranque de la máquina virtual, una vez generada y configurado el sistema operativo (pasos muy sencillos) se realiza a instalar el VMware vSphere Server, el cual nos permitirá tener las reales herramientas de alta disponibilidad.

Antes de realizar la instalación del VMware vSphere Server, es necesario en cada máquina virtual instalada, instalar las **VMware tools**. Las VMware tools son un conjunto de drivers y utilidades que mejoran el rendimiento de la máquina virtual y su sistema operativo, de tal forma que mejoran la interoperabilidad entre el hipervisor y el sistema operativo.

Por último se añadirá la imagen de instalación del **VMware vSphere Server** a la máquina virtual, en el cual indicará si se desea añadirle dominio y si va a formar conjunto con otro software. Una vez realizada la instalación se deberá volver al vSphere Client, pero esta vez, en lugar de indicar la IP del servidor, se debe indicar la IP asignada anteriormente al vSphere server, además el nombre con el dominio donde hemos registrado el vSphere server (administrador@vsphere.local es el creado por defecto). Una vez conectados al Server, es necesario crear el Datacenter, donde se añadirá un nuevo clúster, en el cual se añadirán los servidores que se han mencionado anteriormente.

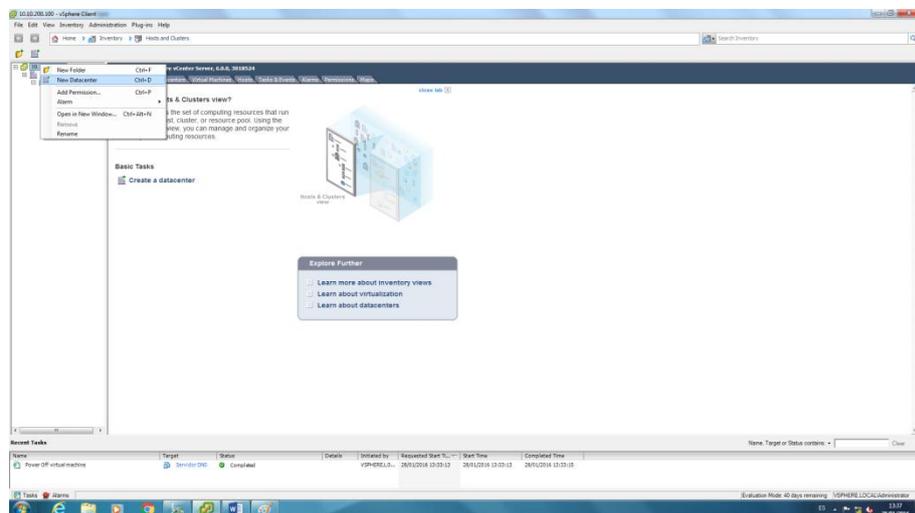


Figura 5.4.2-1: Crear Datacenter

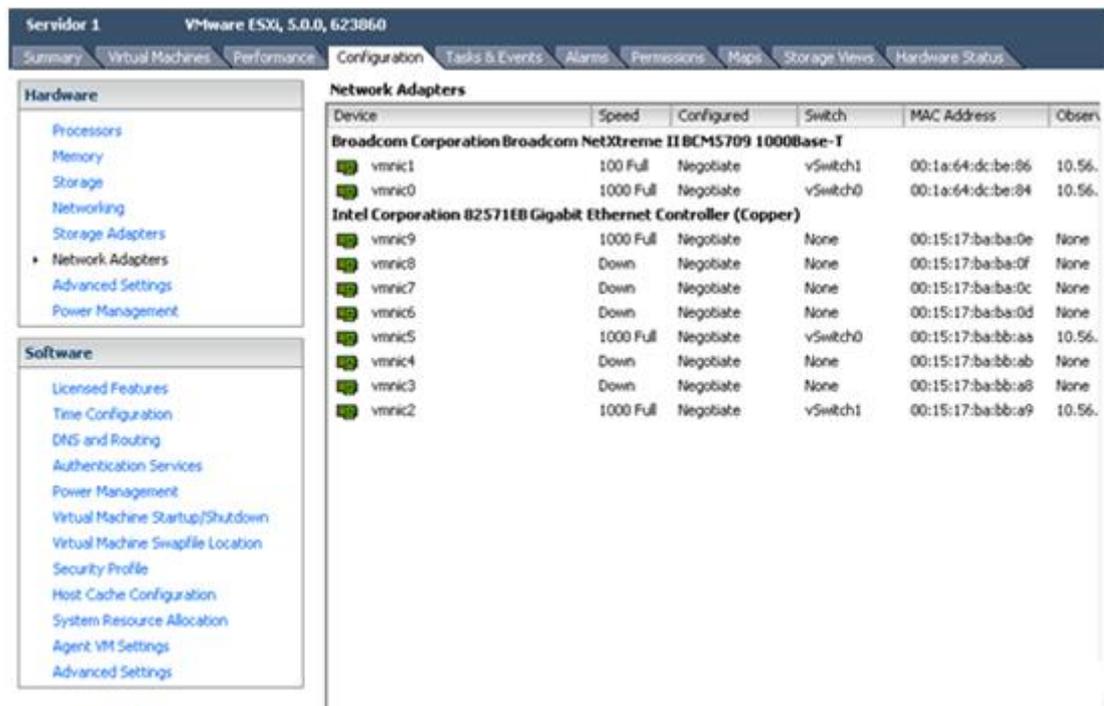
5.5 Configuración de alta disponibilidad

A continuación se procederá a configurar las dos funciones más importantes de VMware en cuanto a alta disponibilidad, estas son vMotion, HA, DRS y el balanceador de carga:

5.5.1 Funcionalidad y configuración vMotion

vMotion es la función que permite trasladar una máquina virtual entera en funcionamiento de un servidor físico a otro, sin tiempo de inactividad, ni pérdida de servicio. La máquina virtual conserva su configuración, solamente cambia el recurso de host, esta función es vital para el funcionamiento continuado del sistema, ya que en caso de error, en cualquier de los host, no se producirán pérdidas en cuanto a recursos ni servicios. Para configurarlo se debe ir al launcher del vCenter Server e iniciarlo con la IP asignada anteriormente.

Nos situamos en la pestaña Configuration, y de ahí a Network Adapters y se comprueba que hay visibilidad de las nuevas conexiones. En este caso se gastará la tarjeta de red asignada a esta tarea (**vmnic9**).



The screenshot shows the VMware ESX configuration interface for 'Servidor 1'. The 'Configuration' tab is selected, and the 'Network Adapters' section is expanded. The interface displays a table of network adapters with columns for Device, Speed, Configured, Switch, MAC Address, and Observed (Obsen). The table lists two main device types: Broadcom Corporation Broadcom NetXtreme II BCM5709 1000Base-T and Intel Corporation 82571EB Gigabit Ethernet Controller (Copper). The vmnic9 adapter is highlighted in blue, indicating it is selected.

Device	Speed	Configured	Switch	MAC Address	Obsen
Broadcom Corporation Broadcom NetXtreme II BCM5709 1000Base-T					
vmnic1	100 Full	Negotiate	vSwitch1	00:1a:64:dc:be:86	10.56.
vmnic0	1000 Full	Negotiate	vSwitch0	00:1a:64:dc:be:84	10.56.
Intel Corporation 82571EB Gigabit Ethernet Controller (Copper)					
vmnic9	1000 Full	Negotiate	None	00:15:17:ba:ba:0e	None
vmnic8	Down	Negotiate	None	00:15:17:ba:ba:0f	None
vmnic7	Down	Negotiate	None	00:15:17:ba:ba:0c	None
vmnic6	Down	Negotiate	None	00:15:17:ba:ba:0d	None
vmnic5	1000 Full	Negotiate	vSwitch0	00:15:17:ba:bb:aa	10.56.
vmnic4	Down	Negotiate	None	00:15:17:ba:bb:ab	None
vmnic3	Down	Negotiate	None	00:15:17:ba:bb:a8	None
vmnic2	1000 Full	Negotiate	vSwitch1	00:15:17:ba:bb:a9	10.56.

Figura 5.5.1-1 : Configuración del Networking de vCenter Server

Para la configuración nos situamos en la pestaña networking donde encontraremos las siguientes conexiones:

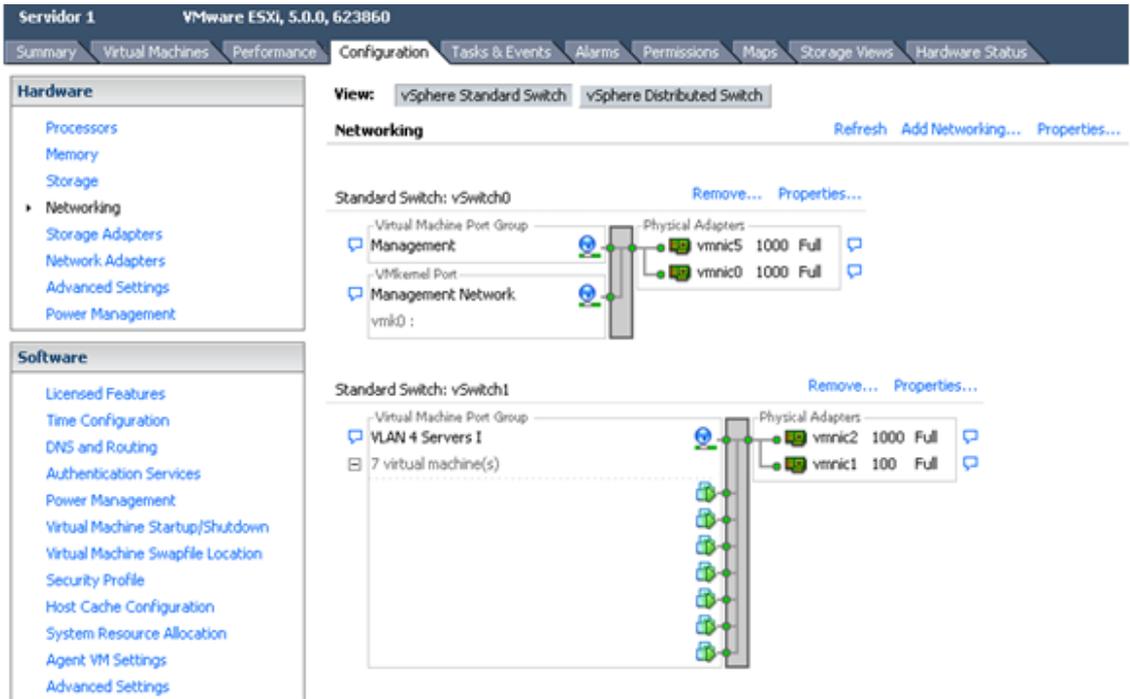


Figura 5.5.1-2 : Configuración Networking

Y se procede a agregar una nueva conexión para nuestro vSwitch, que es un Switch virtual que permitirá interconectar ambos servidores con el Hypervisor de manera simultánea. Gracias a ello conseguiremos a través de este Switch pasar la información de las máquinas virtuales. (De manera física el puerto elegido debe estar conectado a la red de alta disponibilidad)

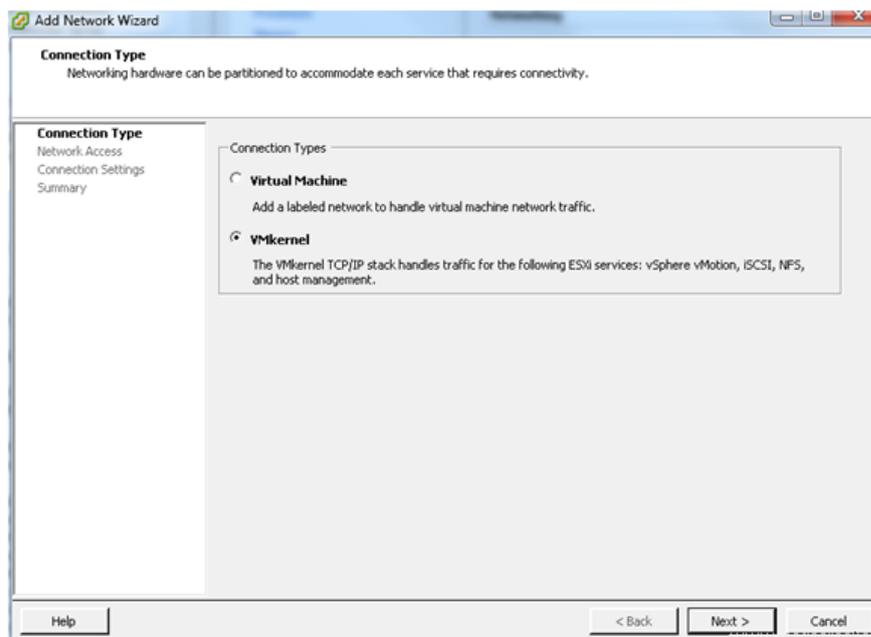


Figura 5.5.1-3 : Creación de una nuevo vSwitch

A continuación aparecerá una pantalla donde se debe elegir la tarjeta virtual que deseamos utilizar para conectar en este Switch (en nuestro caso vmnic9), y se procede a pasar a la siguiente parte de la configuración donde debemos indicar que se trata de un puerto de vMotion. E indicar que dirección IP se quiere asignar y con que máscara (es importante asignar dos IP dentro del mismo rango ya que sino ambos servidores no se podrán conectar y el vMotion no funcionaria).

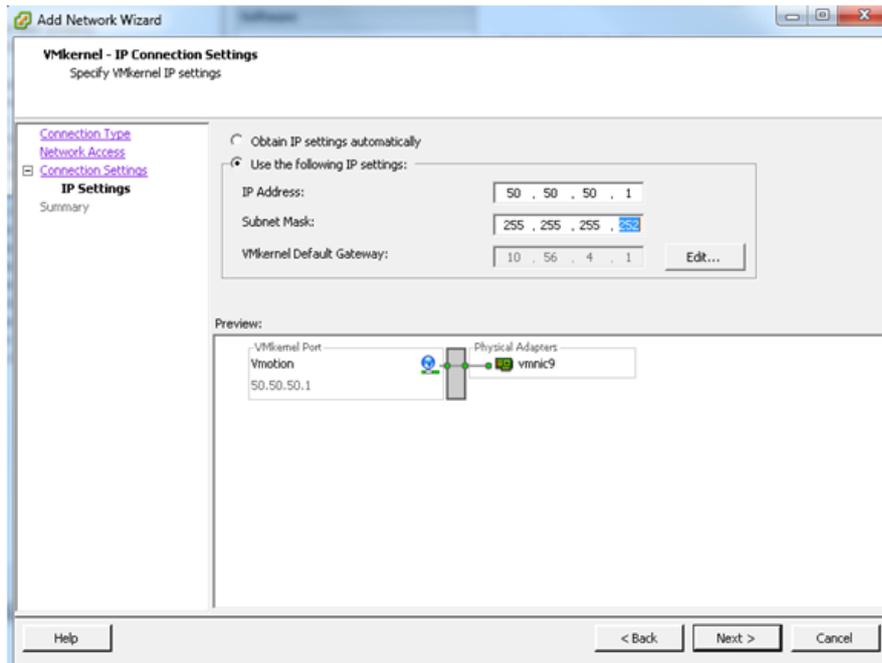


Figura 5.5.1-4 Configuración final vMotion

Se comprueba al final que toda la configuración es correcta, y se pasa a crear este mismo puerto en el otro servidor para que se puedan conectar (con diferente IP), una vez configurado el otro servidor se debe comprobar que todo el sistema funciona correctamente, para ello se debe migrar una máquina virtual desde un ESXi hacia el otro utilizando la funcionalidad Vmotion que acabamos de configurar.

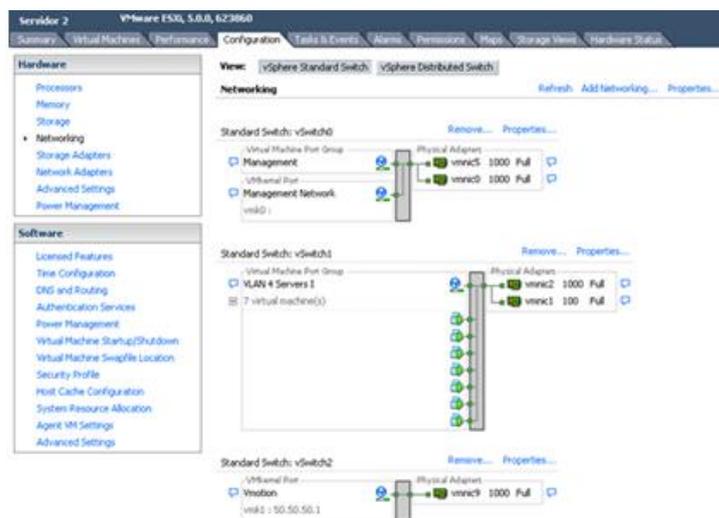


Figura 5.5.1-5 Configuración final vMotion

5.5.2 Equilibrador de carga

Esta configuración se realiza en el momento que el clúster se ha generado, la cual ayuda al clúster a poseer una alta disponibilidad completa y un equilibrador de carga activo.

VMware DRS

Un clúster de VMware DRS es una colección de hosts ESX / ESXi y máquinas virtuales asociadas con recursos compartidos y una interfaz de administración compartida.

Cuando se agrega un host a un clúster DRS, los recursos del host pasan a formar parte de los recursos del clúster. Además de esta agregación de recursos, un clúster DRS admite conjuntos de recursos de todo el clúster y aplica las políticas de asignación de recursos de nivel de clúster. Las capacidades de administración de recursos de nivel de clúster siguientes están disponibles:

- **Balaneo de carga:** El sistema vCenter Server supervisa la distribución y el uso de recursos de CPU y memoria para todos los hosts y máquinas virtuales del clúster. DRS compara estas métricas con una utilización ideal de recursos dados los atributos de los conjuntos de recursos y máquinas virtuales del clúster, la demanda actual y el objetivo de desequilibrio. DRS realiza (o recomienda) migraciones de máquinas virtuales. Al encender por primera vez una máquina virtual en el clúster, DRS intenta mantener el equilibrio de carga adecuado ya sea colocando la máquina virtual en un host adecuado o realizando una recomendación.
- **Administración de energía:** Cuando se habilita la función VMware DTM (Administración de energía distribuida), DRS compara la capacidad del cluster y del host con las demandas de las máquinas virtuales del clúster, incluida la demanda histórica reciente. DTM coloca (o recomienda colocar) hosts en el modo de energía de reserva si se encuentra suficiente capacidad excesiva. DTM activa (o recomienda encender) los hosts si se necesita capacidad. Dependiendo de las recomendaciones del estado de alimentación del host resultante, es posible que sea necesario migrar las máquinas virtuales hacia y desde los hosts.
- **Ubicación de la Máquina Virtual:** Puede controlar la colocación de máquinas virtuales en hosts dentro de un clúster, asignando reglas de afinidad o anti afinidad de DRS.

VMware HA

VMware HA admite la alta disponibilidad de las máquinas virtuales y los hosts en los que residen al agruparlos. VMware HA supervisa los hosts, en caso de fallo del host, VMware HA migra las máquinas virtuales a los hosts con capacidad. Cuando se agrega nuevas máquinas virtuales a un clúster de VMware HA, VMware HA comprueba si está disponible la capacidad suficiente para encender la máquina virtual en un host diferente en caso de fallo del host.

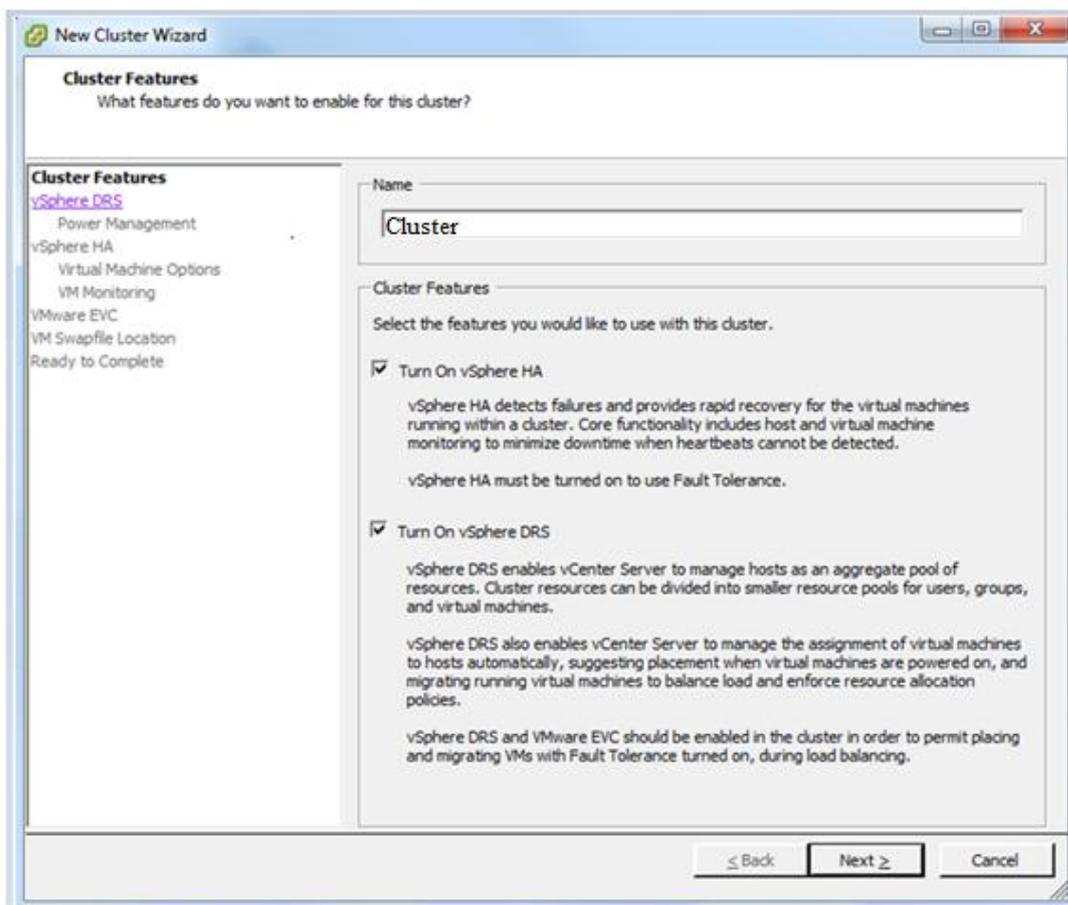


Figura 5.5.2-1: Configuración HA y DRS

Capítulo 6. Implantación de copias de seguridad

6.1 ¿Qué es una copia de seguridad?

Una Copia de Seguridad, es la realización de un duplicado de una información importante, que es utilizada para proteger archivos o ficheros de un problema que pueda presentarse en el sistema, tanto si es problema de acceso o incluso borrado de archivos.

La probabilidad de una pérdida de información o que sea revocado el acceso a ella, es probable, ya que hay diferentes factores de riesgo que pueden provocarlo, como lo son las infecciones por malware, un error de hardware, problema de ejecución de alguna aplicación e incluso el fallo humano. Es muy importante seleccionar la información que se quiere guardar, ya que las copia de seguridad se debe de convertir en un proceso ligero y rápido, así que se debe asignar cierta importancia, a los archivos pertenecientes al sistema y tomar la decisión de cuales son imprescindibles.

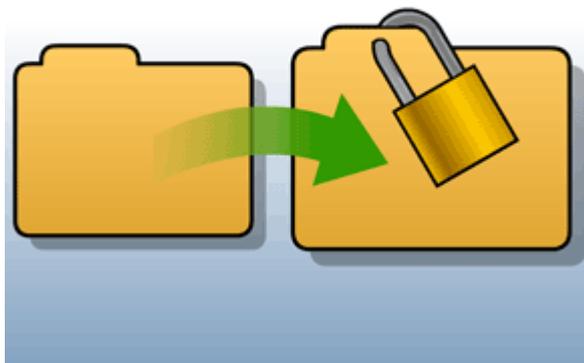


Figura 5.5.21-1: Copias de seguridad

Se debe diferenciar entre las copias de seguridad periódicas, o las que solo se realizan una única vez, para realizar las copias de seguridad periódicas es necesario evaluar de cuanta cantidad de información se va a trasladar, ya que no interesa que una copia de seguridad detenga o retrase el sistema, por esta razón es muy importante seleccionar bien, que se quiere copiar. Las copias de seguridad se pueden guardar en diferentes repositorios, ya sea un simple lápiz USB, una cabina de discos, incluso un sistema replicado. Además, es necesario diferenciar entre los diferentes niveles de copia que existen que son los siguientes.

- A nivel de disco: Importante conocer la tecnología **RAID**, que permite almacenar en tiempo real la información en dos discos duros distintos.
- A nivel de datos: Son copias de seguridad mínimas pero muy necesarias, se realiza una copia de los datos, ya sean **archivos o ficheros** en un repositorio externo al sistema
- A nivel de sistema operativo: Copias de seguridad desconocidas para muchos usuarios y muy útiles, ya que se realiza una imagen del **sistema operativo** en el host seleccionado y se puede almacenar de manera automática en un elemento de la red o en un componente externo.
- A nivel de servidor: Sin duda las más solicitadas para las empresas, se trata una copia de seguridad de las **máquinas virtuales** introducidas en un entorno de virtualización. En estas copias es destacable la escalabilidad que pueden alcanzar, ya que a pesar de copiar máquinas virtuales completas, se puede realizar una recuperación de archivos parcial.
- A nivel de clúster: Hay herramientas que permiten realizar una replicación de un clúster entero, no suelen realizarse este tipo de copias ya que son de volumen muy elevado (gran cantidad de datos), pero son muy eficientes a la hora de entrar en un "entorno de emergencia".

Para agilizar las tareas de copias de seguridad existen varias herramientas que automatizan esta función, y dependiendo del nivel de seguridad deseado, es recomendable el uso de una u otra, para realizar este sistema se ha optado por realizar 3 copias, una a nivel de datos entre cabinas, otra a nivel de servidores y por último una replicación a nivel de clúster. Se han realizado estos 3 niveles para conseguir una seguridad casi completa, ya en caso de fallo de Hardware la pérdida de datos sería mínima, ya que las copias de nivel 1 se realizarían diariamente, y es muy importante indicar que las 3 copias se realizan en diferentes repositorios.

6.2 Diferentes Software para efectuar copias de servidores

En el mercado hay diferentes software para realizar copias de seguridad, cada uno posee características diferentes, dependiendo del uso que se vaya a realizar del mismo, el nivel de copia de seguridad que quiera aportarse, el tipo de copia y el lugar donde se van a realizar. Para este proyecto se ha escogido un software de replicación de servidores, asique se va a realizar una comparativa entre los 3 con más auge del mercado, entre los que se eligió Veeam.

6.2.1 Acronis

Acronis actualmente es el líder en el sector de la protección de datos, su software **Acronis Backup 12.5** es una solución de copia de seguridad rápida, completa, fiable y rentable, que posee dos versiones Standard y Advanced, entre las cuales una empresa puede cambiar dependiendo de la necesidad que posea.

Acronis proporciona un software avanzado y escalable para la gestión de almacenamiento y recuperación de desastres que ayuda a las empresas a salvaguardar la información, asegura la disponibilidad y la recuperación de la misma. Este tecnología basada en la creación de imágenes y gestión del disco ha visto su crecimiento aumentado gracias a su excelente copia y recuperación de datos. Para realizar su comparativa se pasará a valorar las ventajas e inconvenientes.

Ventajas:

- Recuperación de un sistema con diferente Hardware de manera rápida y eficaz.
- Permite la clonación y el despliegue de sistemas operativos independientemente de la plataforma donde esten realizados.
- Ahorro de costes de infraestructura.

Inconvenientes:

- Las actualizaciones no son frecuentes.
- Licencias caras, que ocasionan un gran impacto para pequeñas empresas.

6.2.2 Iperius

Iperius Backup es un software de copias de seguridad completo y flexible para Windows, que posee una versión gratuita . Iperius tiene la posibilidad de realizar copias de seguridad incrementales de manera programada hacia diferentes dispositivos mientras se posea una conexión **TFP** con los mismos. Además incluye como nueva funcionalidad copias de seguridad a la Nube, que mejora la seguridad de los datos, ya que ante un error general, esa copia no saldría afectada. En general, sus ventajas y desventajas son:

Ventajas:

- Económico, con versión gratuita sí que quiere experimentar con el software.
- Protección de bases de datos, Iperius es un software especializado en realizar copias de seguridad en servidores de base de datos como SQL server.
- Soporte gratuito.
- Notificaciones por correo

Inconvenientes:

- No abarca conexiones con algunos elementos de red, como lo son las cabinas de discos
- Un software no optimizado para redes de alta disponibilidad, solo para pequeños entornos.



Figura 6.2.2-1 : Iperius Backup

6.2.3 Veeam

El software elegido para este proyecto es **Veeam Backup and Replication** ya que se trata de un software de copia sin agentes, y que soporta todos los sistemas operativos con los que trabaja **VMware**. Por lo que mejora la copia y configuración, de las copias de las máquinas virtuales generadas en este entorno. Como mejora añadida incluimos que Veeam Backup aprovecha el snapshot de las máquinas en caliente generadas por VMware, y a posteriori realiza la copia de seguridad desde ese snapshot generado. En la mayoría de escenarios se va a encontrar multitud de aplicaciones, Veeam incluye herramientas para trabajar de manera individual con estas aplicaciones, lo que convierte en cada copia de seguridad en única, además la recuperación de datos será más rápida y eficaz. Por ejemplo en el caso de Exchange, Veeam es capaz de trabajar directamente con los contenedores de Exchange situados en la máquina virtual de la que se ha realizado la copia y efectuar tareas de recuperación.

La herramienta de recuperación de datos sin duda es la función estrella de esta software, ya que las máquinas virtuales son contenedores muy grandes, y este software permite desgranarlos de manera que permite el Backup de archivos y ficheros individuales.

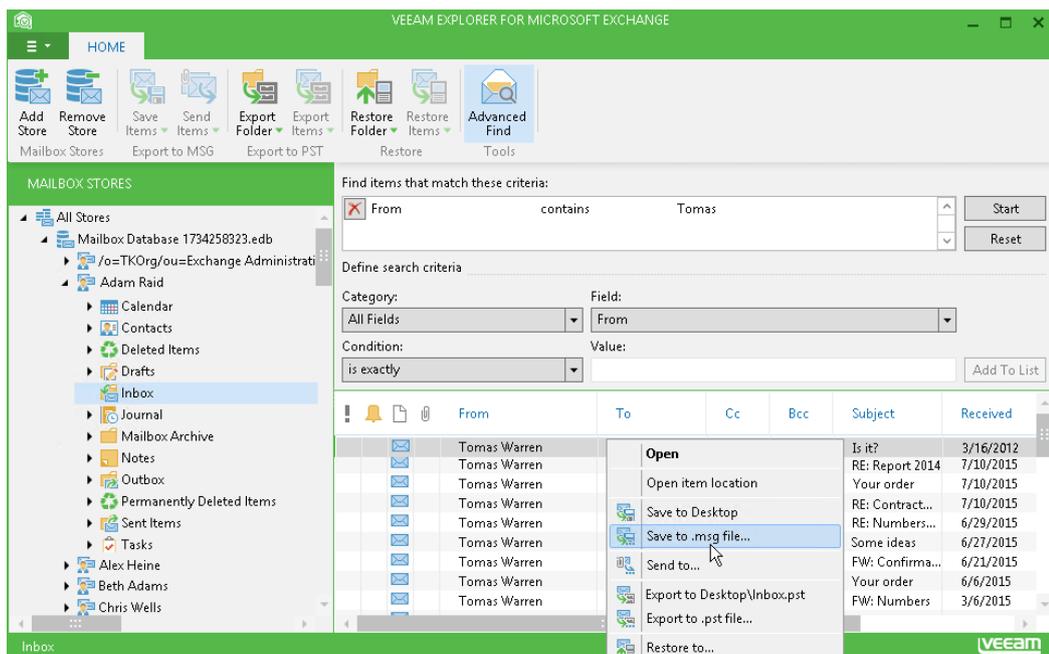


Figura 6.2.3-1 : Veeam Backup herramienta de recuperación Exchange

Una de las funcionalidades más fuertes de Veeam es **Surebackup**, en la cual hace una comprobación del funcionamiento de las máquinas virtuales, una vez realizada la copia de seguridad. Esto lo realiza abriendo la máquina virtual en lo que se puede denominar "sandbox" (entorno de pruebas) en el que aísla la máquina virtual y prueba el funcionamiento como si fuese la principal.

Otra característica importante, es la gran cantidad de tipos de almacenamiento que abarca, ya que puede incluir almacenamiento locales, cabinas de disco, otros servidores, otros clúster, etc... Lo cual, habilita muchos puntos posibles para realizar copias de seguridad. Por último destacar las dos maneras de realizar copias de seguridad, por una parte se encuentra las incrementales, en los que solamente realiza cambios que se han producido en las máquinas virtuales. Por otra, la copia por historia, se realiza siempre una copia entera de las máquinas virtuales, pero además se guarda un histórico con las diferencias entre las copias.

Ventajas:

- **Flexibilidad:** Veeam puede administrar todos los entornos disponibles para VMware, además de añadir funcionalidad para las herramientas provistas en los servidores y por último poder realizar copias de seguridad de host de la red.
- **Rapidez y sencillez:** Es un software donde las copias de seguridad se realizan de manera muy intuitiva, es fácil de configurar y es el software que realiza copias de seguridad de manera más rápida ya que aprovecha los snapshot producidos VMware.
- **Escalabilidad:** La posibilidad de almacenar una información en diferentes puntos de la red, y además la posibilidad de cloud
- **Herramienta de recuperación de datos:** Muy útil la funcionalidad que tiene en cuanto a poder realizar instantáneas rápidas de las máquinas virtuales y además recuperación tanto de máquinas virtuales enteras como de archivos o ficheros dentro de ellas.
- Puede realizar copias de máquinas virtuales estando en caliente.
- Notificaciones por correo

Inconvenientes:

- Precio, la licencia de Veeam Backup es cara y se recomienda renovar el soporte cada año.

6.3 Veeam Backup and Replication v9

Como se ha hablado en el anterior capítulo se ha realizado una configuración del software de Veeam Backup en el clúster a estudio. Para ello, primero se ha realizado la creación de una máquina virtual en la cual se va a almacenar este software, es importante el diseño de esta máquina virtual ya que todas las copias de seguridad dependen del funcionamiento correcto de la misma (importante estar en el mismo rango de IP que los servidores, cabinas, etc...), las características que posee son las siguientes:

- 2CPUs de 2Ghz de 64bits
- Windows Server 2012 R2
- Mínimo 4GB de memoria RAM
- 4GB de espacio en disco duro mínimo
- Además añadir como disco local la cabina de discos

6.3.1 Puesta en marcha de Veeam Backup

Una vez realizada la puesta en marcha de la máquina virtual, con la instalación del Windows Server 2012 R2, se pasa a la instalación del software Veeam Backup & Replication 9 (el cual pide como requisito mínimo el Netframework 4.5), en el proceso de instalación irá añadiendo ciertos softwares necesarios para Veeam como Microsoft SQL server, y finalizamos la instalación.

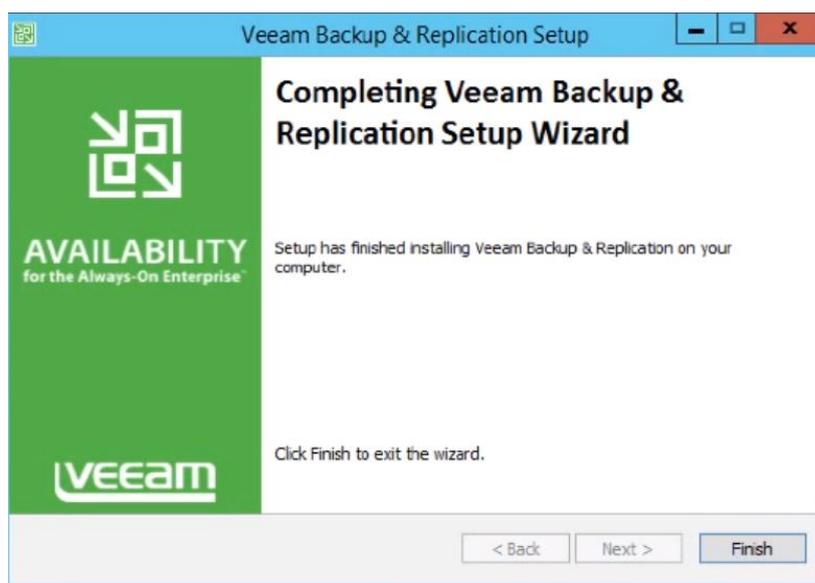


Figura 6.3.1-1: Instalación Veeam Backup.

Una vez finalizada la instalación se presentará la siguiente pantalla:

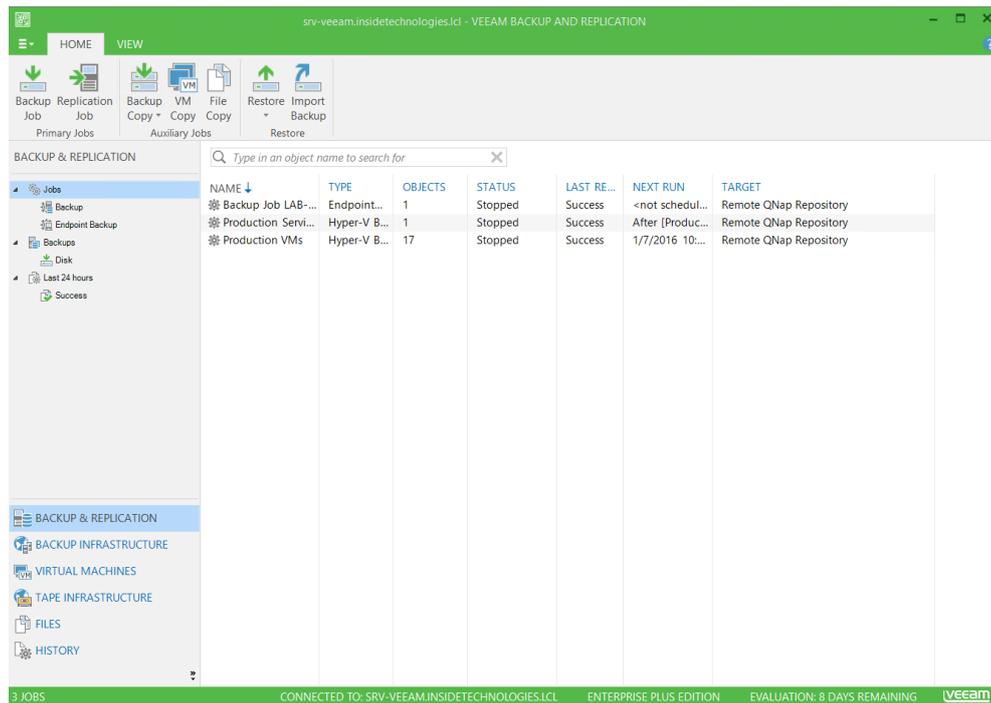


Figura 6.3.1-2: Pantalla inicial Veeam Backup

En ella se encuentran diferentes opciones, para comenzar a realizar las copias de seguridad es necesario en primera instancia, añadir los servidores administrados por el sistema en el cual se quiere trabajar, en este caso se añadirán los dos datacenters pertenecientes al sistema (el me Madrid y el de Valencia) para realizar esto, se debe situar en la pestaña Backup Infrastructure, en la cual se añadirá el ambos servidores VMware:

Aparecerá una pantalla en la cual debemos indicar la IP de los host del vSphere

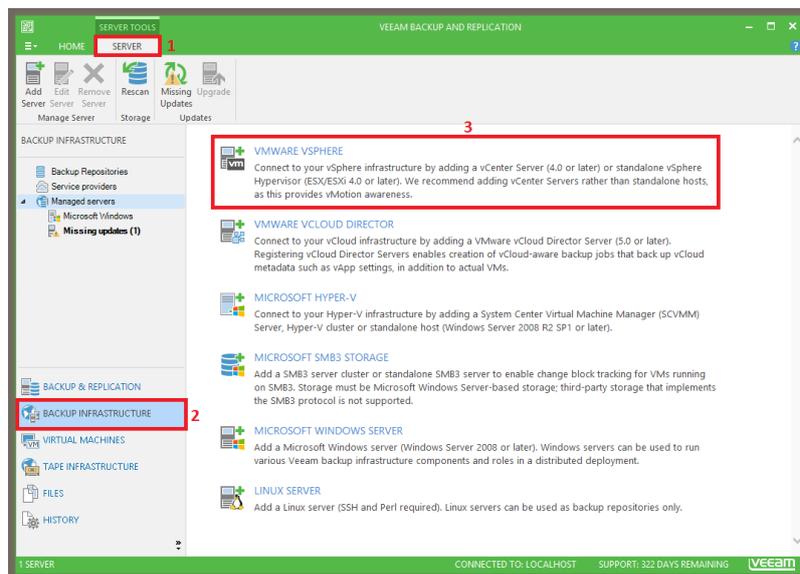


Figura 6.3.1-3 : Agregar servidores VMware

Server, y pedirá que se agreguen los credenciales de cada uno de ellos. Una vez creada la conexión Veeam la verificará.

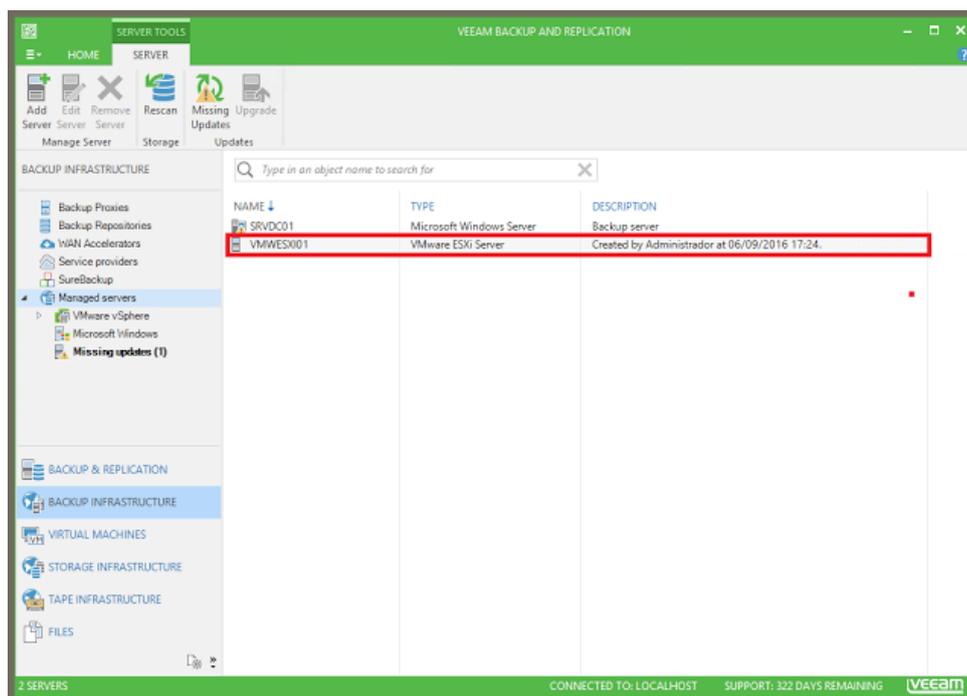


Figura 6.3.1-4 : Servidor VMware añadido

Una vez gestionada los servidores necesarios del sistema, se pasará a añadir todos los repositorios necesarios para posteriormente poder indicar donde se van a realizar las copias. Para ello se debe ir a la pestaña de **Backup Repositories** y pulsar para añadirlo.

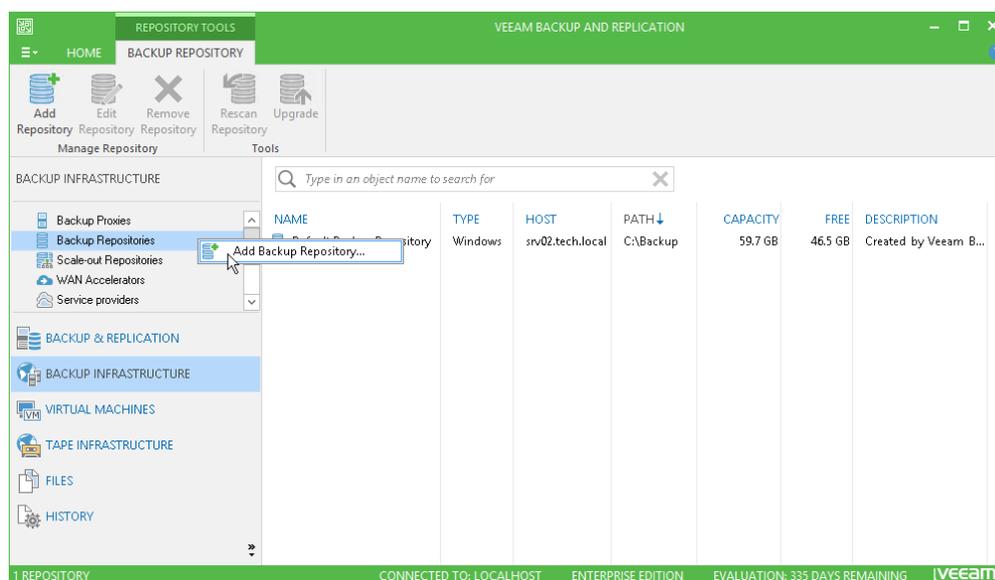


Figura 6.3.1-5: Añadir repositorio

Dentro ya del instalador del repositorio, se debe indicar el nombre del mismo, indicar que tipo de repositorio se encuentra, este dato es muy importante ya que en el podemos encontrar varios tipos de estos repositorios.

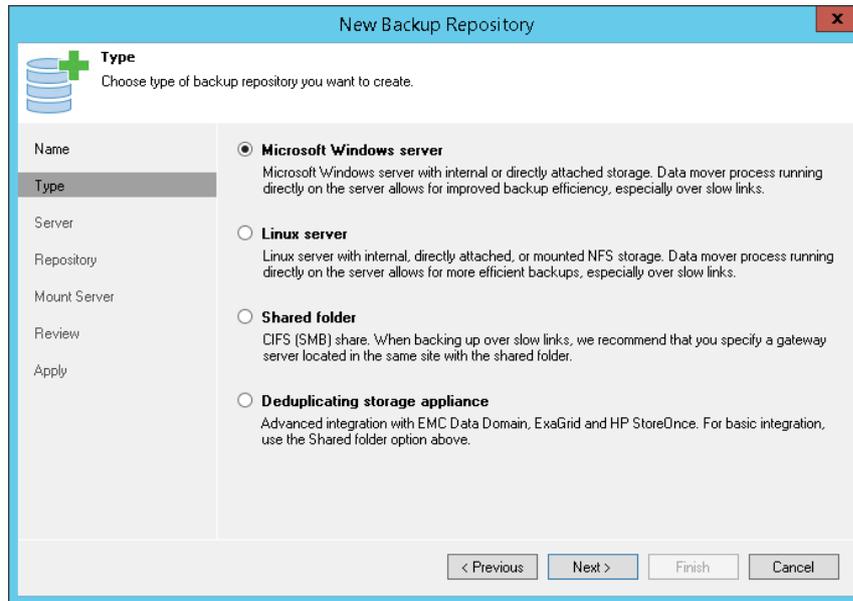


Figura 6.3.1-6: Tipos de repositorio

En el caso del sistema estudiado, se encuentra que la NAS (explicada en el punto 5.3.2) y la máquina virtual donde está instalado el Veeam, que pertenecerían al primer grupo de tipos de repositorio (Como se ha especificado anteriormente es importante que la segunda cabina esté añadida como repositorio local en el servidor de Veeam). Prosiguiendo la configuración del repositorio, se indica la IP del servidor que se quiere añadir y sus credenciales de administrador, posteriormente se indica en que carpeta el servidor Windows Server se desean guardar los datos de las copias, de esa manera es importante tener el almacenamiento comentado anteriormente. Por último, se indica donde se va a guardar la configuración de este repositorio en local, además realiza una conexión con el servidor de repositorio, para comprobar su funcionamiento y una vez realizada acaba por añadirlo.

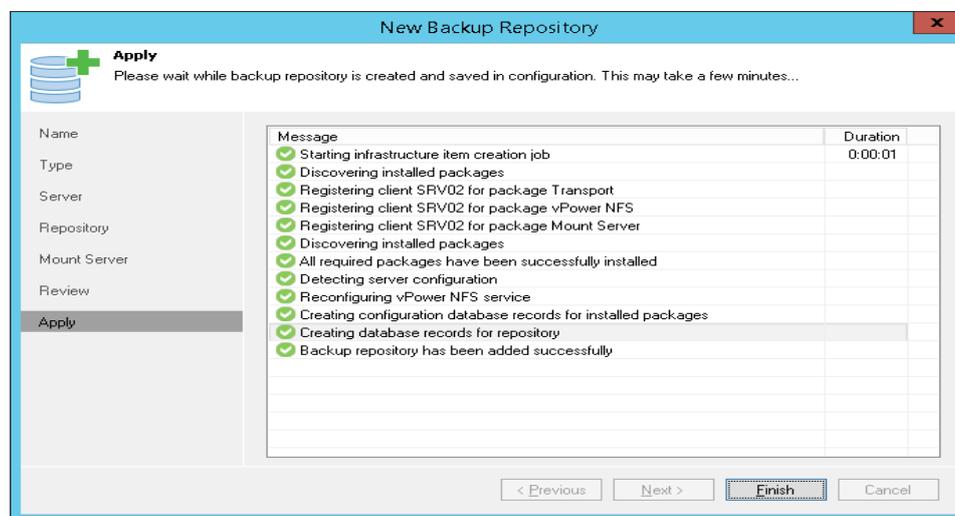


Figura 6.3.1-7: Repositorio añadido.

6.3.2 Configuración copias de seguridad en NAS (semanal)

Se debe situar en la pestaña Backup Job's donde se iniciara una nueva tarea de Backup para configurar correctamente la copia semanal que se quiere realizar en la NAS.

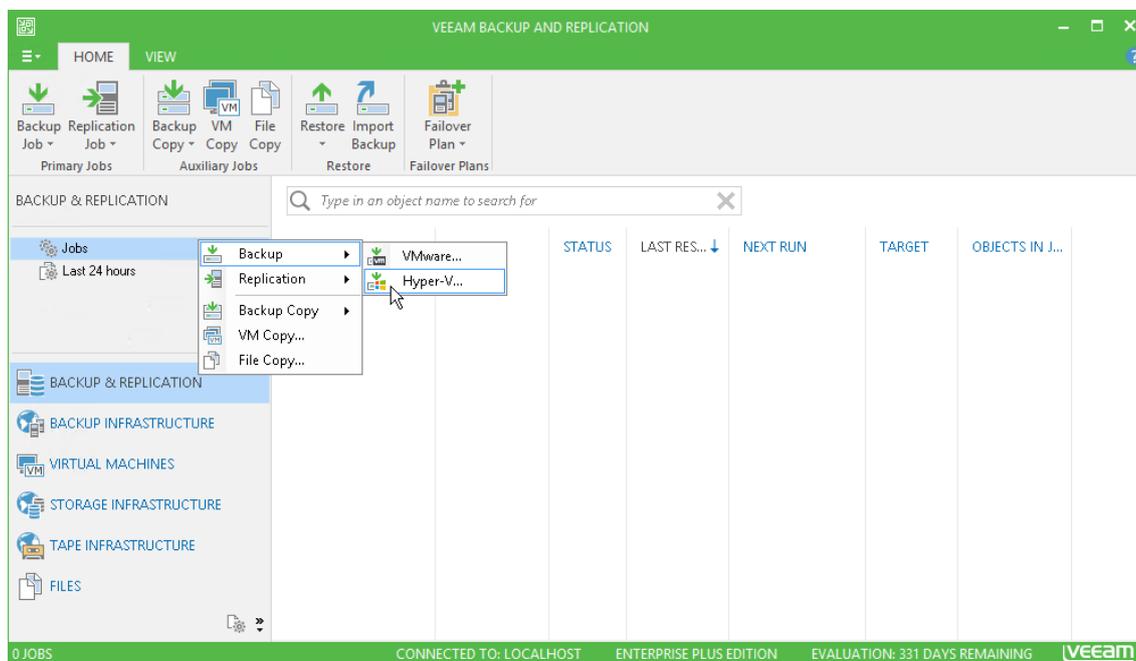


Figura 6.3.2-1: Añadir Backup

Posteriormente se indica que esta copia va a realizarse sobre un entorno VMware, tal como se especificó anteriormente, y a continuación aparecen una serie de configuraciones donde se debe indicar :

- Nombre.
- Maquinas virtuales para realizar la copia.
- Si es necesario excluir un objeto de la copia.
- En qué orden se va a realizar las copias.
- En que repositorio, de los añadidos anteriormente, va a realizarse la tarea y cuantos puntos de restauración se desean, además se puede indicar una segunda copia en otro repositorio añadiéndolo a través de otra tarea nueva que se realizará justo después de la configurada (recomendable uso de cintas).
- Indicar si la tarea va a ser de forma incremental o va a guardarse un historial indicando las diferencias entre copias.

- Indicar si se desea tratamiento especial de las herramientas que puedan contener las máquinas virtuales, es por ello, que se aconseja que cada tarea para cada máquina virtual sea independiente, ya que para herramientas como Exchange es aconsejable el uso de esta herramienta. Además se debe indicar los credenciales de administrador del dominio.
- Por último programar la tarea, es posible indicar en este apartado, que la tarea se produzca después de otra.

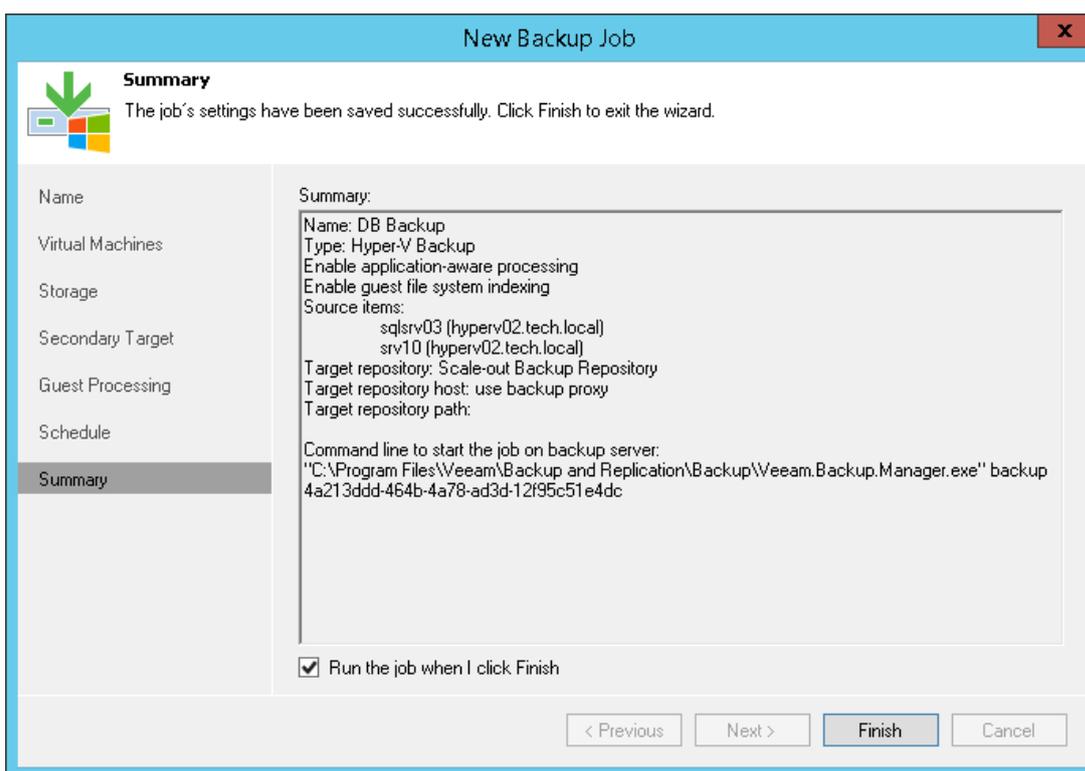


Figura 6.3.2-2 : Resumen de la tarea de la copia de seguridad

6.3.3 Configuración de replicación de un CPD (mensual)

En este punto se va a desarrollar la réplica a través de la conexión **MPLS** que se ha mencionado anteriormente. La conexión **MPLS** permite tratar el servidor que está situado en la red de Madrid, como si fuese uno local, por lo que habrá una IP de este servidor dentro de la red gestionada en Valencia, dicho esto, es necesario la utilización del software Veeam Backup para realizar la réplica del clúster del sistema en Valencia.

En el software Veeam Backup hay una herramienta que permite la replicación entre clústeres o servidores, para ello es necesario ir a la pestaña de Replication Job e iniciar una nueva replica.

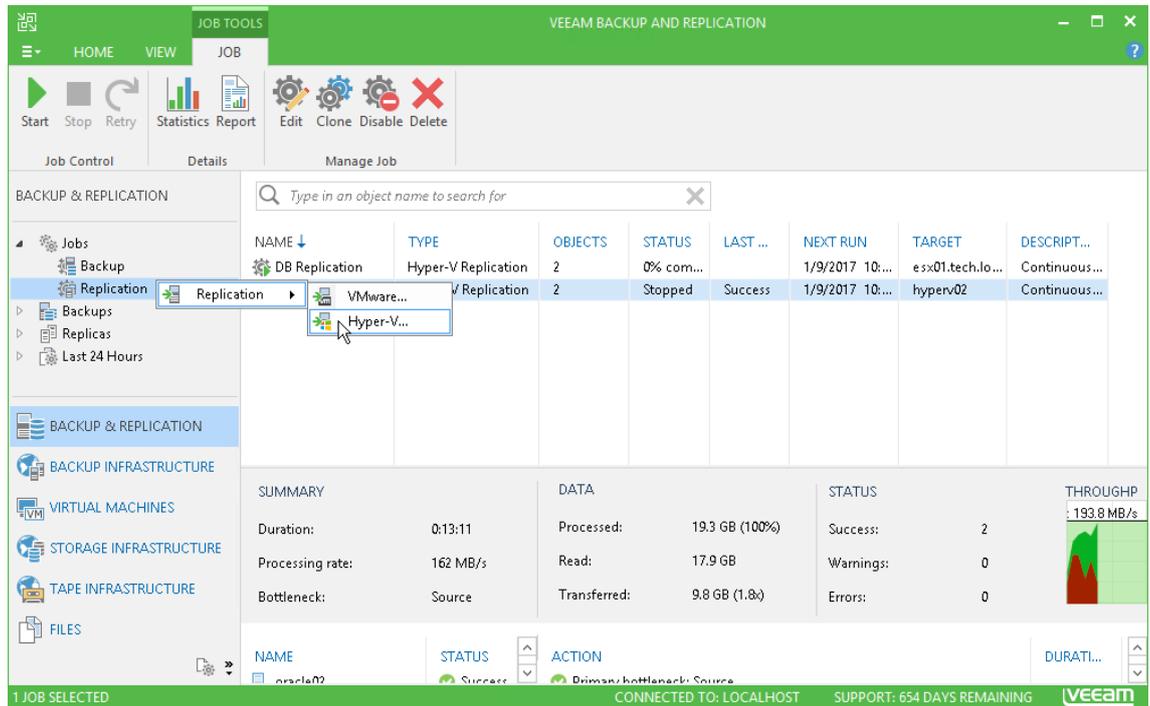


Figura 6.3.3-1: Configuración replica.

Como en el caso anterior, se indica que esta replica va a realizarse en un entorno VMware y a continuación aparecen una serie de configuraciones donde se debe indicar :

- Nombre, si la conexión es lenta (no es el caso), si el elemento donde se va a realizar la réplica está en la misma red (en este caso no) y si va a la máquina virtual replicada va a poseer la misma IP que la inicial.
- Maquinas virtuales o clústeres que se van a replicar.
- Si la replicación se va a obtener directamente de la máquina virtual en caliente o por otro lado se va a generar de una copia de seguridad.
- Si es necesario excluir un objeto de la réplica.
- En qué orden se va a realizar la réplica.
- Sobre que clúster se va a realizar la copia, y sobre que almacenamiento se va a volcar la réplica.

- Que IP tendrán las nuevas máquinas virtuales, en este caso se habilitaran en una red diferente, para que no interfieran con el sistema principal, en caso de estado de emergencia, se cambiaran las IP de las máquinas replicadas y volverá todo a la normalidad, o bien se dejan las mismas IP y no se encienden estas máquinas virtuales hasta que se entre en estado de emergencia (no recomendado es necesario comprobaciones de que su estado es correcto).
- Cuantos puntos de restauración se desean.
- Si se va a utilizar un servidor proxy para la realización de la copia, en este caso no ya que se está trabajando en "local".
- Los credenciales de administrador y si posee herramientas como en el caso de la copia de seguridad.
- Por último, programar la tarea mensualmente.

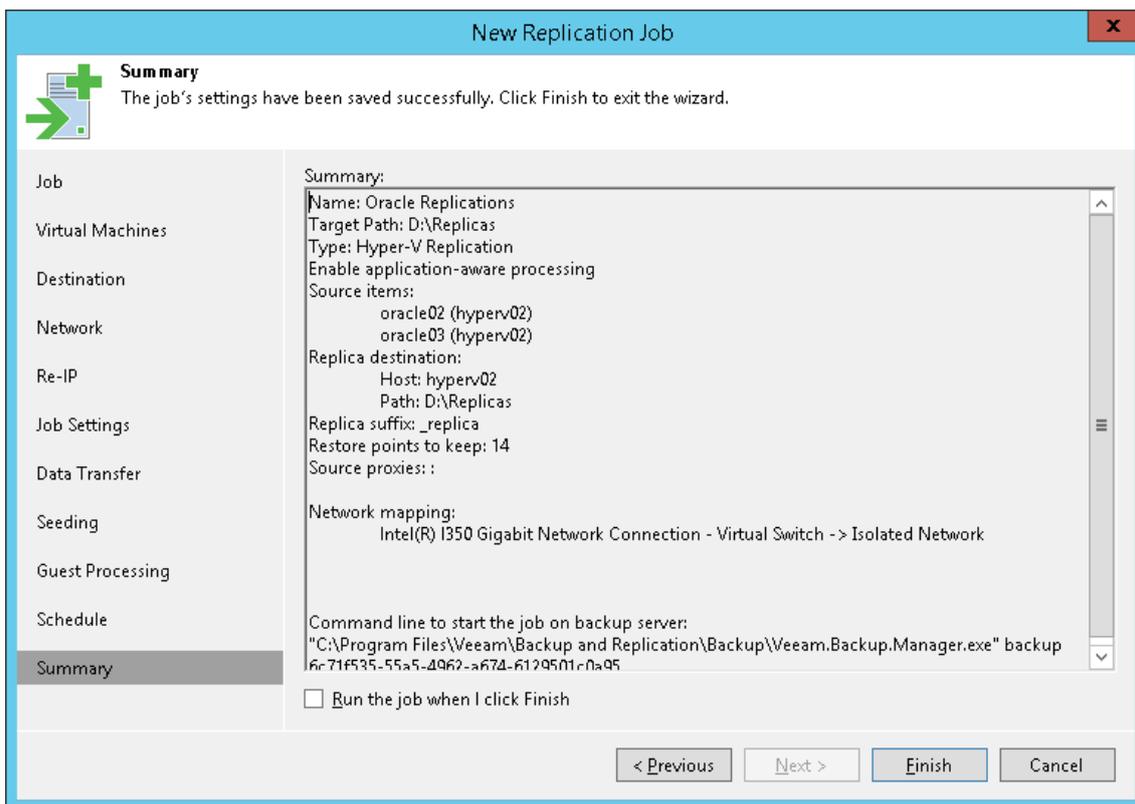


Figura 6.3.3-2: Resumen replicación

Capítulo 7. Conclusiones

Como conclusión sobre este proyecto, se afirma que actualmente la demanda de las empresas sobre la utilización de sus recursos, es máxima, por ello es necesario utilizar herramientas de alta disponibilidad para que los servicios puedan estar operativos las 24 horas del día durante todo el año. Como se ha comprobado, con una red de alta disponibilidad, como la planteada en el proyecto, se alcanza una disponibilidad del 99,99% por lo que una empresa perdería sobre 5 minutos al año sin tener sus recursos activos, ya que es necesarias tareas de mantenimiento, y fallos externos al sistema.

Por otra parte, la herramienta VMware nos proporciona gracias a su flexibilidad, una operatividad continua, ya que como puede albergar diferentes sistemas operativos, conseguimos que el sistema, tenga un conjunto de recursos repartidos entre diferentes hardware, pero gestionado como un único elemento, lo que nos proporciona ante un error de estos elementos, un tiempo de reacción y poder reparar el sistema sin tener que pararlo. Gracias a sus herramientas VMware nos facilita que el sistema siga funcionando sin interrupciones, además gracias a las últimas actualizaciones de VMware, se pueden introducir algunos plug-in para mejorar el entorno, y que todavía sea más sencillo de trabajar.

Por otro lado, las copias de seguridad son muy necesarias para que no se produzcan pérdidas de datos en el sistema, como se ha estudiado, tener un mínimo de 3 niveles de copias de seguridad es imprescindible para que el sistema mantenga una integridad de datos continua. Además la herramienta Veeam Backup, ayuda mucho al administrador, ya que es una herramienta sencilla e intuitiva y gracias a su herramienta de recuperación de datos, podemos alcanzar una pérdida mínima ante un desastre.

En resumen, la demanda de las empresas cada día es más exigente en cuanto a sistemas, es muy recomendable el buen uso de todas las herramientas encarradas a la alta disponibilidad y el aprendizaje de cómo hacer un buen sistema de alta disponibilidad, porque al final una parada en una empresa es una falta muy grave, y es necesario poseer diferentes puntos de redundancia para que esto nunca pase y el sistema pueda funcionar operativo todo el año.

Capítulo 8. Bibliografía

<https://www.veeam.com/es/>

<https://www.vmware.com/es.html>

<http://www8.hp.com/es/es/home.html>

<https://es.wikipedia.org/wiki/Wikipedia:Portada>

<https://es.slideshare.net>