



UNIVERSITAT
POLITÈCNICA
DE VALÈNCIA

CAMPUS D'ALCOI

Recuperación ante Desastres en Entornos con vSAN

MEMORIA PRESENTADA POR:

Raul Lurbe Silvestre

GRADO DE *INGENIERÍA INFORMÁTICA*

Convocatoria de defensa: junio de 2019



UNIVERSITAT
POLITÈCNICA
DE VALÈNCIA

CAMPUS D'ALCOI



RESUMEN

En este proyecto nos encontramos ante un problema que reside en los entornos virtualizados, que es el hecho de proteger nuestra inversión y de la continuidad de nuestro negocio de manera eficiente y segura. Para llevar a cabo estos términos, contaremos con la utilización de la virtualización para poder asegurar la continuidad de nuestro servidor, mediante tres formas diferentes de protección de datos:

- Clúster de discos
- Alta Disponibilidad
- Replicación a nivel de máquina virtual

Para ello contaremos con la utilización las herramientas necesarias para la virtualización y su gestión, creadas por la empresa VMware. Estas aplicaciones serán:

- Hipervisor ESXi
- vSphere vCenter Server Appliance
- vSphere Ha
- vSphere Replication

Para la creación de un entorno de red con almacenamiento compartido (vSAN), utilizaremos las aplicaciones de HP:

- HP VSA
- HP Centralized Management Console (CMC)
- HP Fail Over Management (FOM)



RESUM

En aquest projecte ens trobem front un problema que resideix als entorns virtualitzats, que és el fet de protegir la nostra inversió i la continuïtat del nostre negoci de la manera més eficient i segura. Per a complir aquesta tasca, comptarem amb la utilització de la virtualització per poder assegurar la continuïtat del servidor mitjançant tres formes diferents de protecció de dades:

- Clúster de discs
- Alta Disponibilitat
- Replicació a nivell de màquina virtual

Per a dur a terme aquestes tasques comptarem amb la utilització de les ferramentes necessàries per a la virtualització i la seua gestió creades per VMware. Aquestes aplicacions seran:

- Hipervisor ESXi
- vSphere vCenter Server Appliance
- vSphere Ha
- vSphere Replication

Per a la creació d'un entorn de xarxa amb emmagatzemament compartit (vSAN) utilitzarem les aplicacions de HP:

- HP VSA
- HP Centralized Management Console(CMC)
- HP Fail Over Management(FOM)



ÍNDICE

1	Introducción	8
1.1	Introducción	8
1.2	Justificación y objetivos	8
1.2.1	Justificación	8
1.2.2	Objetivos	10
1.3	Contexto	10
1.4	Estructura de la memoria	11
2	Fundamentos Técnicos	12
2.1	Hiperconvergencia	12
2.1.1	¿Qué es la hiperconvergencia?	12
2.1.2	Beneficios de la estructura hiperconvergente	12
2.1.3	Usos de los sistemas hiperconvergentes	12
2.2	Centro de datos	13
2.2.1	¿Qué es un centro de datos?	13
2.2.2	Ventajas de un centro de datos	13
2.2.3	Desventajas de los centros de datos	13
2.3	Cabina de discos	13
2.3.1	¿Qué es una cabina de discos?	13
2.3.2	Beneficios de una cabina de discos	14
2.4	Servidores	14
2.4.1	¿Qué es un servidor o host?	14
2.4.2	Usos de un servidor	14
2.5	Virtualización	15
2.5.1	¿Qué es la virtualización?	15
2.5.2	Máquinas Virtuales	15
2.5.3	Hipervisor	16
3	Desarrollo Práctico	17
3.1	Introducción al problema	17
3.2	Especificaciones hardware y software	20
3.3	Posibles entornos y su presupuesto	20
3.3.1	Creación de una vSAN para compartir duplicar datos entre servidores ...	21
3.3.2	Replicación de máquinas virtuales mediante vSphere Replication	22
3.3.3	Alta Disponibilidad de máquinas virtuales mediante vSphere HA	23
3.4	Instalación de ESXi y preparación de componentes VMware necesarios.	24
3.4.1	Instalación de ESXi	24



CAMPUS D'ALCOI

3.4.2	Instalación de vSphere vCenter Server Appliance	24
3.4.3	Configuración de vCenter Server Appliance	27
3.4.4	Introducir hosts	27
3.5	Instalación de HPVSA en ESXI.....	28
3.5.1	¿Qué es HP VSA?.....	28
3.5.2	Archivos necesarios para su instalación	28
3.5.3	REGISTRAR MÁQUINA.....	28
3.5.4	Preparar hardware virtual	28
3.5.5	Configurar Direccionamiento ip.....	28
3.5.6	Configurar red HPVSA.....	29
3.5.7	Configurar roles de las interfaces de red.	29
3.6	Configuración de HPVSA y puesta en marcha de la cabina de discos virtual	29
3.6.1	Requisitos previos	29
3.6.2	Configuración básica de HP VSA	30
	Configurar volúmenes.....	33
3.6.3	Conectar los discos de las cabinas a los hipervisores	34
3.6.4	Configuración de discos en ESXI.....	37
3.7	Configuración de la Alta disponibilidad	40
3.7.1	Requisitos mínimos de hardware y de software.....	40
3.7.2	Requisitos previos a la realización de la alta disponibilidad	41
3.8	Configuración de vSphere HA ante las catástrofes	42
3.8.1	Errores y respuestas.....	42
3.8.2	Respuesta ante el aislamiento del host.....	43
3.8.3	Configurar respuestas VMCP	44
3.8.4	Proactive HA.....	45
3.8.5	Control de admisión.....	47
3.8.6	Configurar el almacén de datos de latidos	48
3.8.7	Comprobación de la configuración.....	48
3.9	Configuración de vSphere replication	49
3.9.1	Instalación de vSphere Replication.....	50
3.9.2	Configurar vSphere Replication	50
3.9.3	Configuración de red	52
3.9.4	Configuración ideal y funcionamiento de vSphere Replication.....	52
4	Conclusión.....	53
4.1	Valoración Personal.....	54
5	Bibliografía.....	55



ÍNDICE DE ILUSTRACIONES

Ilustración 1. Esquema general alta disponibilidad.....	19
Ilustración 2. Esquema general replicación.....	19
Ilustración 3. Configuración máquina virtual.....	24
Ilustración 4. Elegir tipo de instalación vCenter.....	25
Ilustración 5. Requisitos mínimos de despliegue.....	26
Ilustración 6. Configurar red en HP VSA.....	29
Ilustración 7. Esquema despliegue	30
Ilustración 8. Configuración nodos HP VSA	32
Ilustración 9. Configurar Volumen HP VSA	33
Ilustración 10. Propiedades del Volumen.....	33
Ilustración 11. Panel lateral VMware ESXi	34
Ilustración 12. Obtener IQN	34
Ilustración 13. Dar de alta ESXi en HP VSA	35
Ilustración 14. Asignar permisos en HP VS.....	35
Ilustración 15. Configuración del clúster del servidor	36
Ilustración 16. Configuración de los volúmenes en el clúster de servidores	36
Ilustración 17. Configuración iSCSI final en ESXi	37
Ilustración 18. Crear Disco Compartido.....	38
Ilustración 19. Lista de discos compartidos.....	38
Ilustración 20. Esquema de acceso de los servidores a las cabinas	39
Ilustración 21. Esquema de acceso de los servidores a los volúmenes	39
Ilustración 22. Vista de la configuración de vSphere HA	48
Ilustración 23. Prueba de funcionamiento de HA (1)	49
Ilustración 24. Prueba de funcionamiento de HA (2)	49
Ilustración 25. Configuración de vSphere Replication	51
Ilustración 26. Estado final de los servicios de vSphere Replication	51



ÍNDICE DE TABLAS

Tabla 1. Presupuesto solo vSAN	21
Tabla 2. Presupuesto vSphere Replication	22
Tabla 3. Presupuesto Alta Disponibilidad (HA).....	23



1 INTRODUCCIÓN

1.1 INTRODUCCIÓN

Este trabajo se basa en el análisis de un entorno simulado existe la necesidad de salvaguardar los datos de nuestra empresa ante cualquier catástrofe, utilizando las técnicas de alta disponibilidad y replicación para obtener la protección necesaria ante dichas catástrofes.

1.2 JUSTIFICACIÓN Y OBJETIVOS

1.2.1 Justificación

Hoy en día el nivel de dependencia de los equipos informáticos está aumentando a unos niveles muy altos debido a que la implementación de sistemas informáticos en los negocios es muy elevada gracias a la facilidad de uso de los programas informáticos que consiguen automatizar recursos productivos o simplificar tareas de oficina.

Aunque no seamos conscientes, no sabemos la cantidad de información importante relacionada con nuestra empresa que guardamos en nuestros sistemas informáticos de nuestro servidor, ya sea un file server con gran parte de la información, como por ejemplo información sobre productos, análisis de mercados, archivos fundamentales en la producción de nuestra empresa. Otro ejemplo es, el uso de servidores SQL para guardar información respecto al funcionamiento de la empresa, así como los datos de facturación, clientes, o la utilización del servidor como sistema donde instalar nuestro programa de contabilidad

Esto se traduce en que el servidor de nuestra empresa están toda la información necesaria para que podamos funcionar con normalidad, por poner un símil, el servidor sería el corazón de nuestro negocio, ya que es un servidor es el encargado poder unir diferentes departamentos de nuestra empresa de forma directa. Utilizando como ejemplo una empresa de producción textil, que es un tipo de negocio muy común de la zona geográfica en la que vivimos, que produce un producto final a través de una materia prima. En el servidor de nuestra empresa, encontraremos un programa que se encargará de gestionar toda la producción de nuestra empresa de manera unificada, este programa recibe el nombre genérico de software ERP, que podrá controlar desde la materia prima



CAMPUS D'ALCOI

que utilizamos, el material que producimos, cuanto tiempo se tarda en producir nuestro producto, a que cliente está destinado, fecha y hora de producción, operario que lo realiza, etc.

Además, otro gran peligro de nuestros servidores es el acceso a la información por parte de distintos empleados que podrían realizar cambios de ficheros o su eliminación de forma accidental, ya que si no controlamos los permisos de cada usuario, estos tendrán total libertad para poder acceder a dichos recursos y en el caso que sus ordenadores fueran infectados con un tipo de malware capaz de encriptar la información del ordenador de nuestro empleado, y en caso de que tuviera permisos ilimitados, nos infectaría nuestro servidor, perdiendo toda la información contenida en él. Pero el principal problema de nuestra empresa es que muchas veces no sabemos valorar nuestra información contenida en dichos sistemas informáticos, por tanto, no tomamos las medidas necesarias o adecuadas para la protección de nuestro negocio.

Para analizar nuestras necesidades de protección ante desastres, utilizaremos la técnica de acuerdo de nivel de servicio (SLA), ya que esta técnica nos permite saber que apartados de nuestra empresa son más importantes para la continuidad del negocio mediante la recolección de los datos de uso de nuestro sistema y analizando nuestros datos creando una amplia base de datos para poder proporcionarnos las respuestas ante desastres y catástrofes que requiere nuestro negocio ajustándose a las necesidades de la empresa, así como a la protección de nuestros servicios más vitales.

Una opción de recuperación ante desastres y que desarrollaremos a posteriori, es la utilización de la alta disponibilidad como protocolo de protección de nuestros datos y producción. Este protocolo nos permite el uso continuado de nuestros servicios informáticos a pesar de la pérdida total o parcial de nuestro servidor principal, ya que esta técnica necesita de dos servidores idénticos o parecidos porque cuando falla un servidor, las máquinas virtuales instaladas, que serán nuestros sistemas operativos instalados sobre un entorno virtualizado, son inmediatamente inicializadas en nuestro segundo servidor, permitiéndonos la continuidad de trabajo de nuestro negocio.

Otra opción de recuperación ante desastres que vamos a desarrollar sería la técnica de la replicación, la cual nos permite clonar nuestra máquina virtual y copiarla en un segundo servidor, el cual ya tendría la configuración de dicha máquina virtual para poder ejecutar la información copiada



1.2.2 Objetivos

El objetivo principal de este trabajo es la creación de planes de recuperación de desastres para asegurar nuestra información ante imprevistos, utilizando un sistema de almacenamiento virtual, más conocido como vSAN, que nos permitirá controlar el almacenamiento de nuestro servidor y hacer accesible dicho almacenamiento mediante el uso de técnicas basadas en el acceso a almacenes de datos a través de internet.

Los objetivos de nuestro trabajo podrían resumirse de la siguiente manera:

- Ventajas del uso de vSAN frente al almacenamiento normal.
- Ver diferentes tipos de protección de datos.
- Implementar un sistema de protección de datos escalable.
- Realizar la configuración de vSphere vCenter Appliance de forma correcta.
- Analizar el hardware necesario.

1.3 CONTEXTO

Estamos ante la simulación de una situación real, donde una empresa busca soluciones para mantener operativos sus servidores y mantener sus datos a salvo ante desastres o catástrofes. Para ello utilizaremos los conocimientos aprendidos en la rama de redes y sistemas del Grado en Ingeniería Informática, tales el mantenimiento de servidores, el uso de las redes corporativas, la configuración de todo el software necesario, así como la administración de sistemas.

Para ello utilizaremos los conocimientos de direccionamiento IP , el uso de Vlans, el uso de balanceo de carga , la configuración de Vlans, instalación y configuración de servidores y sistemas de almacenamiento, el uso de volúmenes y de RAIDs, el uso de servidores DNS, el uso de iSCSI y de la vSAN, la configuración de enlaces punto a punto, el uso de hipervisores, el tipo de almacenamiento en nuestros discos virtuales, manejar los recursos que tenemos evitando el sobre aprovisionamiento, las nociones sobre los sistemas de protección ante desastres, como replicación, alta disponibilidad o la conmutación por error.

Además, se ha implementado la necesidad de establecer un plan de contingencia ante estos desastres analizando las necesidades de nuestra empresa y actuando acorde éstas.



1.4 ESTRUCTURA DE LA MEMORIA

La memoria se divide en cinco partes diferenciadas que son:

1. Introducción

En este apartado se realiza una breve explicación sobre el porqué de este trabajo de fin de grado, de los objetivos que se quieren conseguir con la realización de este trabajo de fin de grado, y la aplicación de este trabajo de fin de grado con relación a las asignaturas cursadas durante el grado y que tienen aplicación en este trabajo.

2. Fundamentos técnicos

En este apartado se trata de explicar términos generales para que el trabajo de fin de grado sea entendible y tenga una mayor comprensión.

3. Desarrollo Práctico

En este punto se muestra la aplicación del trabajo de fin de grado sobre un entorno simulado, así como los pasos a realizar para la aplicación de los objetivos del trabajo de fin de grado.

4. Conclusión

Este punto se basa en dar una valoración final sobre las técnicas vistas durante toda la memoria, además de ver la valoración personal de dicho trabajo de fin de grado y las enseñanzas que ha aportado a la persona que lo ha realizado.

5. Bibliografía

Este último punto muestra todas las referencias bibliográficas de las cuales se ha extraído información durante el trabajo de fin de grado.



2 FUNDAMENTOS TÉCNICOS

2.1 HIPERCONVERGENCIA

2.1.1 ¿Qué es la hiperconvergencia?

La hiperconvergencia es el término utilizado para nombrar a las soluciones tecnológicas que nos permiten agrupar almacenamiento, computación y redes en una única solución, la cual permite reducir la complejidad del centro de datos y aumentar la escalabilidad. Estas plataformas incluyen un hipervisor para la computación virtualizada, almacenamiento virtual y redes virtualizadas que se ejecutan en un servidor estándar.

2.1.2 Beneficios de la estructura hiperconvergente

Los beneficios que aporta una estructura hiperconvergente son la generación de un mayor uso de nuestras inversiones debido a la simplicidad de uso y a una mayor eficiencia de nuestros recursos, ya que estos sistemas permiten obtener un factor de escalabilidad muy alto. Otro de los beneficios que obtenemos del uso de estructuras hiperconvergentes, son el ahorro de dinero en hardware y los gastos derivados de este hardware como energía o posibles reparaciones, además de simplificar la recuperación ante desastres de todos nuestros sistemas operativos.

2.1.3 Usos de los sistemas hiperconvergentes

Los sistemas hiperconvergentes son utilizados en sistemas con cargas de trabajo con necesidades de recursos predecibles como aplicaciones empresariales, nube privada, base de datos, servidores de correo, servidores de archivos, y servidores web, permitiendo un crecimiento de los sistemas en la empresa, ya que dos o más servicios pueden ser instalados en diferentes máquinas virtuales.

Esto permite a las empresas poder separar sus diferentes trabajos en diferentes servidores virtuales, lo que permite aumentar la seguridad de trabajo de estos de forma sustancial, ya que en caso de tener divididos los servidores por cargas de trabajo, optimizando mejor los recursos de los que disponemos, ya que podremos asignar diferentes cantidades de recursos dependiendo de las necesidades de cada servidor, que varían dependiendo, por ejemplo, si es un file server, un servidor con SQL server, un servidor con programas de empresa, etc.



2.2 CENTRO DE DATOS

2.2.1 ¿Qué es un centro de datos?

Un centro de datos es un lugar donde se almacena y se procesa la información vía internet. Están compuestos por una gran cantidad de servidores alojados en una misma sala y se suelen utilizar para dar soporte a las empresas mediante el uso de la nube o cloud computing.

2.2.2 Ventajas de un centro de datos

Las ventajas que nos ofrece un centro de datos, es que podemos minimizar nuestro gasto en hardware, así como su mantenimiento, ya que podemos contratar un servidor virtual para poder realizar nuestras funciones, además de que todo el mantenimiento será realizado por expertos conocedores en la materia de los sistemas.

Por otra parte, estos centros de datos nos permiten tener nuestros datos a salvo ya que suelen tener duplicidad de máquinas virtuales, asegurando que nuestra información siempre estará a salvo.

2.2.3 Desventajas de los centros de datos

Las desventajas de estos centros de datos, son que tienen un alto coste medioambiental debido a la gran cantidad de energía que consumen, ya que disponemos de centenares de servidores juntos consumiendo energía, pero por si esto no fuera poco, estos servidores desprenden grandes cantidades de calor, por lo tanto, para que el hardware no sufra una degradación, se debe mantener estos centros de datos a temperatura ambiente, añadiendo otro coste energético, ya que para ello se utiliza aire acondicionado de manera continuada.

2.3 CABINA DE DISCOS

2.3.1 ¿Qué es una cabina de discos?

Una cabina de discos es un dispositivo de almacenamiento el cual nos permite administrar nuestros discos, pudiendo crear grupos de discos, RAIDs, modificar una LUN creando volúmenes en ella y compartiéndolos con los usuarios o dispositivos que queramos mediante las técnicas de uso compartido de almacenamiento como iSCSI.



2.3.2 Beneficios de una cabina de discos

Con la utilización de una cabina de discos externa conseguimos un sistema mucho más adaptable a nuestras necesidades, con mayor capacidad de almacenamiento y una mayor protección frente a roturas.

Al tener la información separada físicamente del servidor que la utiliza en caso de fallo de ese servidor (rotura de fuente de alimentación, problemas del sistema operativo, etc.) podemos acceder a los datos almacenados desde otro servidor. Así pues, no sólo hay redundancia a nivel de rotura de discos duros, sino también en el caso de que el servidor quede inoperativo.

Las controladoras de las cabinas permiten la utilización de diferentes esquemas para la redundancia de la información en nuestros discos, incluyendo la posibilidad de tener discos duros sin usar, pero preparados para añadirse a cualquier volumen de discos en caso de rotura de un disco físico. Es lo que se conoce como hot swap.

Las cabinas de disco vienen preparadas para dar una alta redundancia de sí mismas, ya que incorporan una doble fuente de alimentación, doble controladora y doble bus de datos. Por ello el hecho de mover la información a una cabina no implica generar un punto crítico.

Si juntamos varias cabinas podemos realizar un clúster, que es la unión de dos cabinas bajo un mismo nombre, donde nuestra información estará guardada instantáneamente en ambas cabinas, eliminando la preocupación de tener toda nuestra información en un mismo lugar.

2.4 SERVIDORES

2.4.1 ¿Qué es un servidor o host?

Tipo de computadora preparada creada para poder operar en sistemas de producción todos los días sin apagarse, y soportar almacenamientos y cargas de trabajo muy grandes, a parte de la posibilidad de tener diversos de sus componentes duplicados para garantizar la continuación del trabajo sin cortes. También es conocido por el nombre de host.

2.4.2 Usos de un servidor

Un servidor puede utilizarse para implementar en él diferentes aplicaciones o servicios de vital importancia para un negocio, ya que en un servidor puede servirnos para instalar un servidor SQL, instalar programas de acceso



generalizado por nuestros trabajadores, crear un dominio para limitar el acceso de los usuarios que están dentro de éste, reduciendo el nivel de vulnerabilidad de nuestro sistema.

2.5 VIRTUALIZACIÓN

2.5.1 ¿Qué es la virtualización?

La virtualización consiste en crear una representación basada en software, o virtual, de una entidad física como, por ejemplo, aplicaciones, servidores, redes y almacenamiento virtuales. Es la forma más eficaz de reducir los gastos de TI y, a la vez, aumentar la eficiencia y la agilidad para empresas de cualquier tamaño.

2.5.2 Máquinas Virtuales

Es un software de ordenador que, como un ordenador físico, es capaz de correr sistemas operativos y aplicaciones.

2.5.2.1 Características de las máquinas virtuales

- **Creación de particiones**

La capacidad de ejecutar varios sistemas operativos en un solo servidor, y distribuir los recursos del servidor entre las diferentes máquinas virtuales.

- **Aislamiento**

Permita aislar la seguridad y los fallos en el nivel de hardware, garantizando el rendimiento gracias a los controles avanzados de recursos.

- **Encapsulación**

Capacidad de guardar el estado completo de una máquina en archivos, y poder transferirlos o copiar dicha máquina como si de un archivo se tratase.

- **Independencia del hardware**

Poder correr o migrar la máquina virtual independientemente del servidor donde se ejecute.



2.5.3 Hipervisor

2.5.3.1 ¿Qué es un hipervisor?

Aplicación perteneciente a los sistemas hiperconvergentes capaz de presentar a un sistema operativo un hardware virtual y sobre el cual se ejecutarán estos sistemas operativos. Los hipervisores también son los encargados de monitorizar la ejecución de los sistemas operativos virtuales. Estos hipervisores se pueden ejecutar sobre el sistema operativo base del dispositivo, o se pueden instalar sobre los componentes.

2.5.3.2 Hipervisores más famosos

Encontramos dos hipervisores más famosos, el primero de tipo opensource llamado proxmox y el segundo creado por la empresa VMware llamado vSphere ESXi.

El primero está basado en las distribuciones GNU/Linux de Debian, y utiliza una versión modificada del Kernel RHEL, siendo compatible con cualquier sistema operativo basado en Linux o en Windows, y, por tanto, se puede conseguir de manera gratuita. Por otra parte, ESXi es un programa de código cerrado, donde se debe pagar una licencia para poder usarlo, además de que también es perfectamente compatible con Windows y Linux.



3 DESARROLLO PRÁCTICO

3.1 INTRODUCCIÓN AL PROBLEMA

En lo que se refiere al entorno, estamos delante de una situación donde la empresa o entidad en cuestión desea disponer de un sistema de múltiples servidores que ejerzan diferentes funciones dentro de la empresa, como un servidor de almacenamiento, de producción, un servidor DNS, y tenerlo todo instalado en una sola máquina física, aplicando los términos de la hiperconvergencia. Esto supone un ahorro tanto a nivel de espacio como a nivel de mantenimiento y como a nivel de gasto en hardware, ya que todos los sistemas operativos que antes estarían instalados cada uno en un servidor físico, ahora se concentran en un solo servidor físico.

Todo esto tiene una desventaja que es visible a primera vista, y es que, si falla dicho servidor o si se perdiera la información de ese único servidor físico, perderíamos toda la información de nuestra entidad o empresa. Para ello exploraremos soluciones ante dichos desastres que nos permitirán poder tener toda nuestra información a salvo y la continuación de nuestro funcionamiento de la empresa garantizada.

Para ello se requiere de un sistema virtualizado para poder utilizar múltiples máquinas virtuales con una rápida respuesta y solución ante un desastre o catástrofe. Por eso vamos a simular un entorno de empresa donde se tienen dos servidores HPE ProLiant DL360 Gen10 4208 con 64 GB de memoria RAM DDR4 y un procesador Intel de 8 núcleos a 3,2 GHz y que cuenta con diversas sedes interconectadas mediante una fibra óptica propia y donde su principal objetivo reside en poder tener duplicada la información de la empresa para que en caso de desastre poder asegurar la continuidad de la empresa. Por tanto, se explorarán diversas opciones de duplicado de datos, utilizando un entorno virtualizado con máquinas virtuales y una cabina de discos virtual para poder realizar dicho duplicado de datos. Para llevar a cabo este cometido veremos cómo funcionan la replicación y la alta disponibilidad, y el nivel de protección que nos brindan.

También hay que tener en cuenta que hay que tener redundados nuestros dispositivos de red, ya que de ellos depende en gran medida el correcto



CAMPUS D'ALCOI

funcionamiento de nuestro sistema de protección de datos, por tanto, duplicaremos los cables de fibra óptica, utilizando cada cable para cada switch y aplicando balanceo de carga entre cada switch de cada edificio. La estructura de la fibra óptica nos permite continuidad de negocio, aunque fallen dos switches de manera simultánea.

Las aplicaciones que vamos a usar son:

- El hipervisor vSphere ESXi de VMware.
- vSphere vCenter Server Appliance de VMware.
- La cabina de discos virtual HP VSA de HP.
- El programa Fail Over Manager (FOM) de HP.

El direccionamiento IP para alta disponibilidad será el siguiente:

- Edificio A
 - ESXi: 192.168.0.150
 - vCenter Server: 192.168.0.151
 - HP VSA: 192.168.0.153
- Edificio B
 - ESXi: 192.168.0.220
 - vCenter Server: 192.168.0.221
 - HP VSA: 192.168.0.223
- Edificio C
 - ESXi: 192.168.0.200
 - FOM: 192.168.0.203

El direccionamiento IP para replicación será el siguiente:

- Edificio A
 - ESXi: 192.168.0.150
 - vCenter Server: 192.168.0.151
 - HP VSA: 192.168.0.153
- Edificio B
 - ESXi: 192.168.0.220
 - vCenter Server: 192.168.0.221
 - HP VSA: 192.168.0.223

CAMPUS D'ALCOI

El esquema del conexionado con alta disponibilidad sería el siguiente:

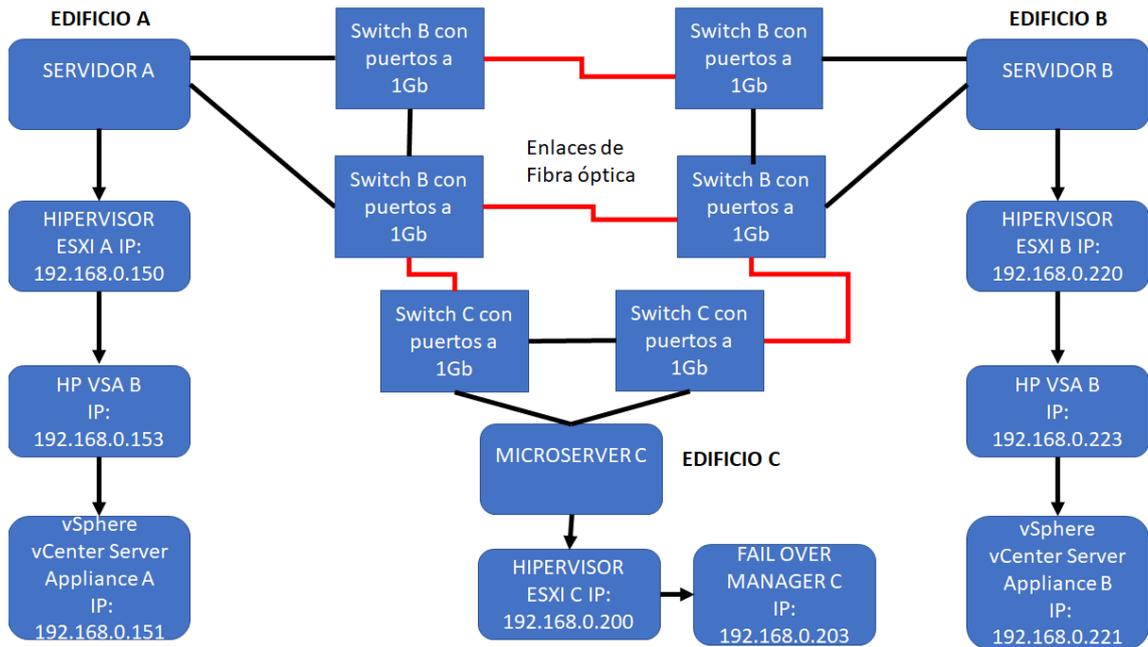


Ilustración 1. Esquema general alta disponibilidad

El esquema del conexionado con Replicación sería el siguiente:

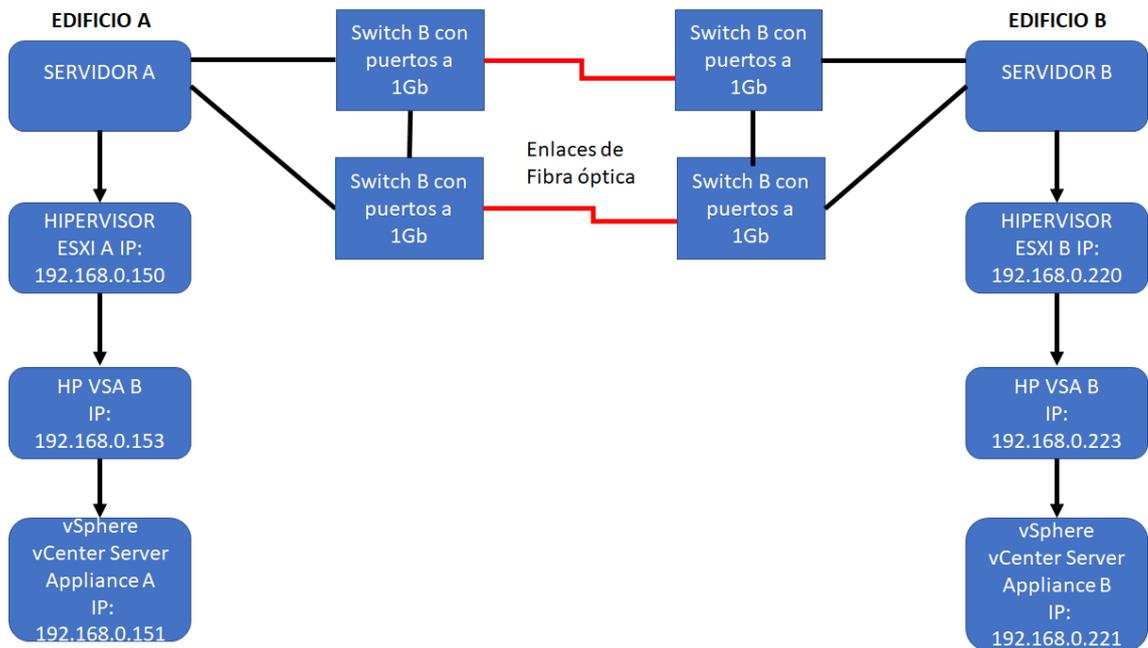


Ilustración 2. Esquema general replicación



3.2 ESPECIFICACIONES HARDWARE Y SOFTWARE

En este caso he hecho una simulación de un entorno real en un solo ordenador debido a que por a causas laborales no he podido acceder al material que mi tutor me prestaba por problemas de horarios y desplazamientos, y por eso todas las pruebas han sido realizadas en un ordenador que tiene las siguientes características:

- Placa Base: Asus Prime Z370-P.
- Procesador: Intel i5-8600K con una frecuencia de reloj de 3.6 GHz y 9MB de Caché.
- Memoria RAM: 32 GB de Memoria RAM DDR4 a con una frecuencia de 3000 MHz.
- Disco duro SSD Sata 3 de 500 GB donde está instalado el sistema operativo y el programa de virtualización.
- 2 discos duros de 1 TB a 7200 RPM donde se encuentran situados los discos de las máquinas virtuales donde se instalará nuestros hipervisores.
- Tarjeta de Red integrada en la placa base.

Software utilizado durante las pruebas:

- VMware Workstation pro.
- Windows 10 Home 64 bits.
- VMware vSphere ESXi 6.7.
- VMware vSphere center server.
- VMware vSphere High Availability.
- VMware vSphere Replication.
- HPVSA 2014.
- HPE StoreVirtual Centralized Management Console.
- Fail Over Manager de HP (FOM).
- Navegador web con soporte para flash o HTML 5, en nuestro caso, Google Chrome.

3.3 POSIBLES ENTORNOS Y SU PRESUPUESTO

Contando con que ya tenemos nuestras sedes interconectadas con fibra óptica o mediante una vpn, y que ya disponemos de todo lo necesario a falta del hardware genérico y software, a continuación, se mostrará el precio aproximado que podríamos tener de realizar nuestros despliegues de servidores y la protección de nuestras máquinas virtuales.



3.3.1 Creación de una vSAN para compart duplicar datos entre servidores

En este caso, solo deseamos que nuestros servidores virtualizados accedan a un almacén de datos compartido para ambos y que sea replicado entre nuestras diferentes sedes sin necesidad de tener alta disponibilidad a nivel de hardware. Esta opción solo serviría para proteger datos en discos compartidos a iSCSI a servidores instalados en el mismo servidor o red.

Nombre del artículo	Especificaciones	Precio estimado (€) *IVA incluido
2 x Servidor HPE ProLiant DL360 Gen10 4208	<ul style="list-style-type: none">• 64 GB de RAM DRR4• 1 CPU de 8 núcleos a 2,1 GHz, con turbo a 3.2 GHz• 2 Fuentes de alimentación de 500w• 1 Controladora de red con 4 puertos x 1 GbE• Espacio para 8 discos de 2.5"• Formato de 1U	10.000
HPE ProLiant MicroServer Gen10 X3418	<ul style="list-style-type: none">• 1 CPU de 4 Núcleos a 1.8 GHz, con turbo a 3.2 GHZ• 8 GB de RAM DDR\$	659,45
Licencia HP VSA	<ul style="list-style-type: none">• Licencia de HP de 4 TB para instalar HP VSA en tres servidores• Licencia FOM	4.000
Licencia vSphere Essentials	<ul style="list-style-type: none">• Licencia de vSphere ESXi para 3 servidores con máximo 2 CPU• Licencia vCenter Server Essentials para un servidor	679,57

Tabla 1. Presupuesto solo vSAN

Con un precio aproximado de 15.339,02 €, tendríamos lo básico para poder realizar un despliegue de una cabina de discos replicada en dos servidores. Para instalar el Fail Over Manager utilizaremos un microserver, y no hace falta licencia



CAMPUS D'ALCOI

de ningún tipo ya que viene incluida en HP VSA. Ahora solo faltaría los discos duros que no vienen incluidos en el servidor y de toda la infraestructura de red y de racks.

3.3.2 Replicación de máquinas virtuales mediante vSphere Replication.

En este caso, realizaremos la protección de base de datos a nivel de copiar toda la información de nuestras máquinas virtuales a otro servidor que después en caso de fallo del primero nosotros encenderemos las máquinas virtuales.

Nombre del artículo	Especificaciones	Precio estimado (€) *IVA incluido
2 x Servidor HPE ProLiant DL360 Gen10 4208	<ul style="list-style-type: none">• 64 GB de RAM DRR4• 1 CPU de 8 núcleos a 2,1 GHz, con turbo a 3.2 GHz• 2 Fuentes de alimentación de 500w• 1 Controladora de red con 4 puertos x 1 GbE• Espacio para 8 discos de 2.5"• Formato de 1U	10.000
2 x Licencia vSphere Essentials Plus kit	<ul style="list-style-type: none">• Licencia de vSphere ESXi para 3 servidores con máximo 2 CPU• Licencia vCenter Server para un servidor	10.935,72

Tabla 2. Presupuesto vSphere Replication

Con un precio total aproximado de 20.935,72 €, tendríamos lo básico para poder replicar nuestras máquinas virtuales en otro host y asegurarnos que funcionarían correctamente a falta de los discos duros que no vienen incluidos en el servidor y de toda la infraestructura de red y de racks.



3.3.3 Alta Disponibilidad de máquinas virtuales mediante vSphere HA

En este caso, realizaremos la protección de base de datos a nivel de copiar toda la información de nuestras máquinas virtuales a otro servidor que después en caso de fallo del primero nosotros encenderemos las máquinas virtuales.

Nombre del artículo	Especificaciones	Precio estimado (€) *IVA incluido
2 x Servidor HPE ProLiant DL360 Gen10 4208	<ul style="list-style-type: none">• 64 GB de RAM DDR4• 1 CPU de 8 núcleos a 2,1 GHz, con turbo a 3.2 GHz• 2 Fuentes de alimentación de 500w• 1 Controladora de red con 4 puertos x 1 GbE• Espacio para 8 discos de 2.5"• Formato de 1U	10.000
HPE ProLiant MicroServer Gen10 X3418	<ul style="list-style-type: none">• 1 CPU de 4 Núcleos a 1.8 GHz, con turbo a 3.2 GHZ• 8 GB de RAM DDR\$	659,45
2 x Licencia vSphere Essentials Plus kit	<ul style="list-style-type: none">• Licencia de vSphere ESXi para 3 servidores con máximo 2 CPU• Licencia vCenter Server para un servidor	10.935,72
Licencia HP VSA	<ul style="list-style-type: none">• Licencia de HP de 4 TB para instalar HP VSA en tres servidores• Licencia FOM	4.000

Tabla 3. Presupuesto Alta Disponibilidad (HA)

Con un precio total aproximado de 25.595,17 €, tendríamos lo básico para poder replicar nuestras máquinas virtuales en otro host y asegurarnos que funcionarían correctamente a falta de los discos duros que no vienen incluidos en el servidor y de toda la infraestructura de red y de racks.



3.4 INSTALACIÓN DE ESXi Y PREPARACIÓN DE COMPONENTES VMWARE NECESARIOS.

3.4.1 Instalación de ESXi

Para la instalación del hipervisor ESXi en mi ordenador personal, he utilizado el programa VMware Workstation para poder realizar entornos virtuales. Esta máquina virtual se compone de las siguientes características:

- Procesadores: 1 procesador con 6 núcleos.
- Memoria RAM: 12 GB.
- Discos duros virtuales (SCSI): 2 discos de 250 GB.
- Tarjetas de red: 2 en modo Bridge.

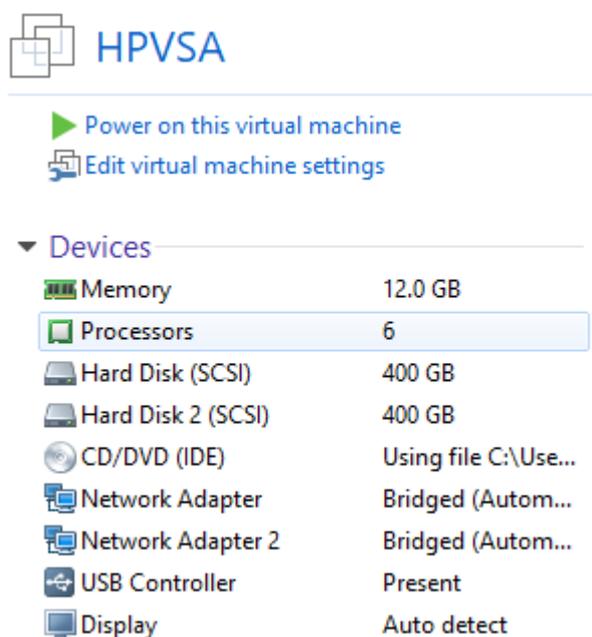


Ilustración 3. Configuración máquina virtual

Nuestro hipervisor tendrá asignada la IP 192.168.0.150, en la cual podremos entrar a gestionar nuestras máquinas virtuales, almacenamientos de datos, la red de nuestro host y muchas más cosas antes de instalar nuestro vSphere vCenter, el cual nos ayudará a la gestión de nuestro host.

3.4.2 Instalación de vSphere vCenter Server Appliance

Para instalar nuestro vCenter Server, debemos de descargar la ISO que encontraremos en la página web de VMware, y la ejecutaremos desde un ordenador que esté dentro de la misma subred que nuestro host y tenga acceso

CAMPUS D'ALCOI

al host. En nuestro caso ejecutaremos la instalación desde el ordenador donde está instalado nuestra máquina virtual en Workstation. Para ello nos saldrá un instalable en el cual deberemos de cumplimentar los siguientes pasos. Los pasos más importantes a la hora de rellenar son los siguientes:

3.4.2.1 Selección del tipo de instalación de vCenter

Seleccionaremos la primera opción, donde tendremos embebidos tanto los servicios, como el vCenter Server bajo una misma máquina virtual y por tanto bajo una misma IP. Si quisiéramos acceder en un futuro a gestionar nuestro vCenter Server a más bajo nivel, deberíamos acceder a la plataforma de servicios mediante el uso del puerto 5480.

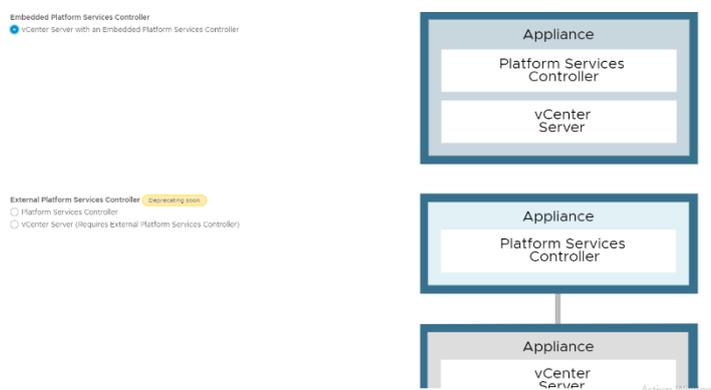


Ilustración 4. Elegir tipo de instalación vCenter

3.4.2.2 Selección de nuestro host ESXi objetivo

En este apartado nos preguntará por la IP de nuestro host ESXi y nuestro usuario y contraseña de acceso a nuestro host ESXi. Posteriormente nos saldrá una advertencia con el certificado, ya que estamos usando el que viene por defecto de VMware.

3.4.2.3 Configuración básica de vSphere vCenter Server

Primero le tendremos que asignar un nombre a la máquina virtual que se va a crear, por defecto se le asignará VMware Vcenter Server Appliance, en nuestro caso le asignaremos el sitio, quedando el nombre de VMware vCenter Server Appliance Sitio A, y le asignamos la contraseña para poder acceder posteriormente con el usuario root a la plataforma de control de servicios. Acto seguido configuraremos el tamaño de despliegue de nuestro vCenter Server, donde tendremos las siguientes opciones de configuración mínima:



Deployment size Tiny ▼

Storage size Default ▼

Resources required for different deployment sizes

Deployment Size	vCPUs	Memory (GB)	Storage (GB)	Hosts (up to)	VMs (up to)
Tiny	2	10	300	10	100
Small	4	16	340	100	1000
Medium	8	24	525	400	4000
Large	16	32	740	1000	10000
X-Large	24	48	1180	2000	35000

Ilustración 5. Requisitos mínimos de despliegue

En nuestro caso elegiremos la opción de despliegue tiny ya que estos parámetros se ajustan a lo que necesitamos en nuestro servidor.

Respecto al tamaño de almacenamiento de despliegue, elegiremos la opción por defecto, ya que para la tarea que deseamos realizar tenemos suficientes recursos.

Seleccionaremos el almacén de datos donde se va a guardar esta máquina virtual, pudiendo elegir thin disk mode, que nos permitirá que el modo en el que se establezcan los discos de vCenter Server sea creciente y no fijo, permitiéndonos aumentar de tamaño de disco de esta máquina virtual de manera gradual. Dependiendo de las opciones que hemos elegido, se nos configurará nuestra máquina virtual, a la cual posteriormente podremos cambiar parámetros como la memoria RAM

A continuación, procederemos a la configuración de red de nuestro vCenter Server, donde seleccionaremos una IP estática para nuestro host, que en este caso es la 192.168.0.151, le asignaremos un FQDN, que no es ni más ni menos que un nombre al host para que después pueda ser encontrado por búsqueda inversa a través de un servidor DNS, y si lo deseamos, le podemos poner la dirección IP de nuestro futuro servidor DNS. Por tanto, el FQDN es opcional, aunque los servidores DNS sí que son necesarios para poder continuar la instalación.

Con todo esto ya habremos terminado el primer paso de la instalación de vSphere vCenter Server Appliance.



3.4.2.4 Configuración del SSO

Antes de la creación de un SSO se nos pedirá que elijamos como debemos sincronizar la hora de nuestro vCenter Server, la cual podemos hacer que coja la hora de nuestro host ESXi o a través de un servidor NTP. En nuestro caso hemos elegido la opción de sincronizar con el host ESXi para evitar así problemas de sincronización de horas y posibles fallos con la ejecución de vCenter Server. También he activado la opción de ssh por si fallara la máquina virtual y no se pudiera acceder a vCenter Server o a la plataforma de control de servicios vía web, poder hacerlo mediante un terminal como Putty y resolver los problemas que acarrearía nuestro vCenter Server.

Ahora procederemos a la creación de un dominio Single Sing On, el cual nos permitirá centralizar toda la autenticación de nuestros servidores vCenter en una misma entidad de acceso a la administración. En mi caso le he asignado el dominio por defecto de la instalación: vsphere.local, pero podría haber sido perfectamente tfg.local, appliance.local, etc. Una vez ya tenemos nuestro SSO creado, procedemos a darle la contraseña al usuario de administración de nuestro vSphere vCenter Server, que será el usuario "administrator", el cual no se puede cambiar de nombre.

Una vez hecho esto procederemos a revisar todos los parámetros de nuestra configuración y le daremos a finish, y entonces se empezará a instalar nuestro vSphere vCenter Server y ha inicializar todos sus servicios.

3.4.3 Configuración de vCenter Server Appliance

Crear un centro de datos donde se un grupo de hosts que aplicarán las configuraciones que deseemos y de los cuales podremos gestionar sus máquinas virtuales.

3.4.4 Introducir hosts

Introducimos nuestro host pulsando botón derecho sobre nuestro centro de datos y añadimos la dirección IP, el usuario y la contraseña con permisos de administrador de nuestro host ESXI, posteriormente si queremos añadirle alguna restricción para solo poder configurar posteriormente nuestro hipervisor solo a través del Vcenter o por ssh se lo podemos configurar en este paso, en nuestro caso no impondremos ninguna restricción dejando marcada la opción de deshabilitado, pulsamos a todo siguiente.

En unos segundos nos aparecerá nuestro host añadido en forma de desplegable, el cual, si lo seleccionamos, podremos ver todas nuestras máquinas virtuales



CAMPUS D'ALCOI

creadas en nuestro host y desde el mismo Vcenter podremos configurar. Conectamos los siguientes hosts y ya tendremos nuestros servidores bajo la administración de nuestro vCenter

3.5 INSTALACIÓN DE HPVSA EN ESXI

3.5.1 ¿Qué es HP VSA?

HP VSA es una cabina de discos la cual nos permite crear y manejar nuestro almacenamiento de forma ordenada, dando la posibilidad de crear diferentes espacios de almacenamientos y que estos sean accedidos por diferentes hosts o máquinas virtuales.

En este caso, al contar con dos nodos de trabajo, si creamos un clúster de discos, veríamos replicada nuestra información en dos hosts diferentes, siendo esta nuestra primera forma de poner a salvo nuestra información.

3.5.2 Archivos necesarios para su instalación

Nos descargamos de la página oficial de la versión de HPVSA para vSphere en formato OVF.

3.5.3 REGISTRAR MÁQUINA

Seleccionamos con el botón derecho y le damos a crear\registrar máquina virtual, seleccionamos importar una máquina virtual a partir de un archivo OVF y buscamos los archivos descargados en la página oficial de HP y los descomprimos y por último aceptamos la política de privacidad de datos y ya tendremos instalado nuestra cabina de datos virtual.

3.5.4 Preparar hardware virtual

Configurar dos discos del tamaño deseado en la máquina virtual desde nuestro hipervisor para que posteriormente se pueda configurar la cabina.

3.5.5 Configurar Direccionamiento ip

Accedemos a través de la consola que nos proporciona VMware y procederemos a configurarle la dirección IP de nuestra cabina de discos virtual, y ponerle un nombre de host. En nuestro caso, las direcciones IP serán:

- a. Cabina A con nombre hpvsac.tfg.local : 192.168.0.153
- b. Cabina B hpvsab.tfg.local: 192.168.0.235
- c. IP Virtual: 192.168.0.241

3.5.6 Configurar red HPVSA

Entraremos dentro de network TCP/IP Settings, seleccionamos eth0 y le damos la siguiente configuración.

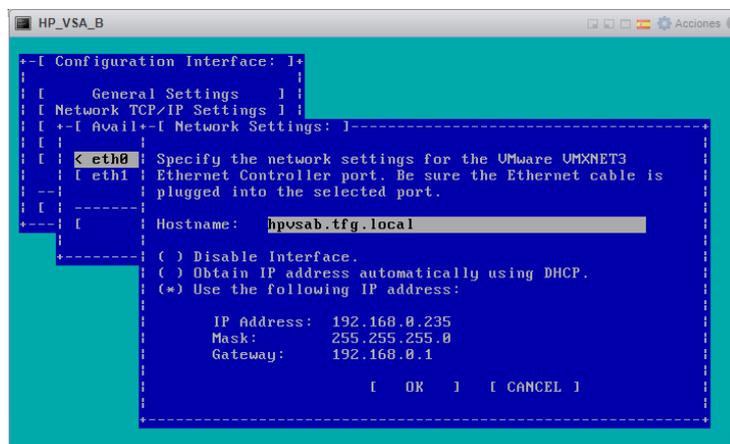


Ilustración 6. Configurar red en HP VSA

3.5.7 Configurar roles de las interfaces de red.

Configuramos la segunda interfaz como interfaz de management para poder acceder a configurar el dispositivo a través de ssh, en nuestro caso será la misma interfaz.

3.6 CONFIGURACIÓN DE HPVSA Y PUESTA EN MARCHA DE LA CABINA DE DISCOS VIRTUAL

3.6.1 Requisitos previos

Lo primero que necesitamos para nuestras cabinas es tener instalado el software de HPE StoreVirtual Centralized Management Console, de ahora en adelante CMC, en un ordenador con Windows y con acceso a todas las máquinas virtuales de HP y configurar dos discos duros virtuales de igual tamaño en las máquinas virtuales ya que para poder configurar el almacenamiento de nuestras cabinas, HP nos obliga a realizar como mínimo un RAID 0 entre dos discos de una misma cabina.

Adicionalmente para poder realizar el clúster y que funcione la alta disponibilidad entre las cabinas de discos de diferentes sitios, deberemos tener una tercera máquina con un Fail Over Manager que nos servirá para poder tener quorum entre cabinas en caso de que falle una de ellas o disponer de otro servidor con una cabina de discos virtual HP instalada.

CAMPUS D'ALCOI

A poder ser el Fail Over Manager, tiene que ser una máquina física independiente, sino perderíamos toda la posibilidad de tener alta disponibilidad en caso de que falle el host con ambas máquinas. Su instalación se realizaría de la misma forma que el HPVSA, solo hay que importar los archivos OVF y configurar la dirección IP que deseemos. En mi caso he decidido implementar el Fail Over Manager o FOM debido a la falta de infraestructura hardware y de espacio en disco.

El esquema de una posible implementación quedaría de la siguiente manera:

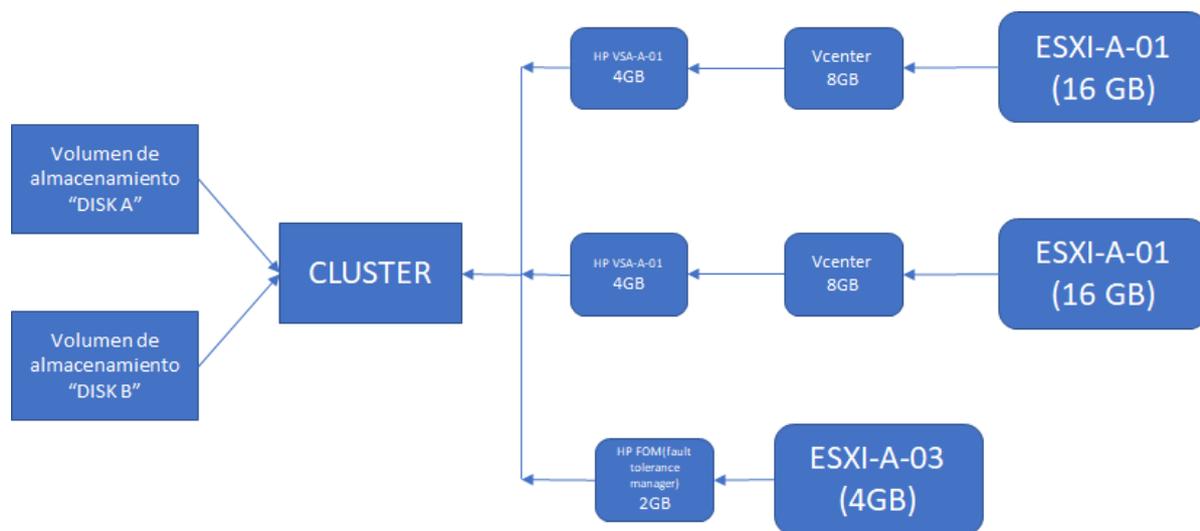


Ilustración 7. Esquema despliegue

3.6.2 Configuración básica de HP VSA

Lo primero que deberemos hacer es realizar la búsqueda de los sistemas, una vez que nuestro programa encuentre las cabinas HP procederemos a realizar la configuración del almacenamiento, ya que HP no nos permite trabajar con cabinas sin ningún tipo de RAID, en mi caso he elegido el RAID 0, que es un RAID sin protección a nivel discos ya que no hace falta proteger los datos a nivel de disco porque los estamos protegiendo a nivel de cabina completa como se explicará más tarde, y además proporciona un rendimiento de escritura elevado y es ideal para la virtualización a la hora de crear volúmenes dentro de este disco.

Una vez tengamos las dos cabinas con los discos configurados, procederemos a realizar la creación de un grupo de administración, este grupo de administración es vital para nuestro sistema ya que ambas cabinas se encuentran separadas totalmente y el grupo de administración nos permitirá unir las bajo un mismo grupo de control de las cabinas y nos permitirá realizar las diferentes configuraciones entre ambas cabinas. Este grupo de administración



CAMPUS D'ALCOI

nos permetrà realitzar una configuració de vital importància per al correcte funcionament, ja que nos permetrà establir diverses direccions IP virtuals que nos asseguraran el correcte funcionament de nostre clúster, encara que falle una de les dos cabines.

Una vegada tinguem nostre grup d'administració creat, nostre següent pas serà crear un nostre clúster, ja que això nos permetrà la unió de les dos cabines en una simulació de una cabina sola. El següent pas per realitzar és la creació de les volúmenes, lo qual nos permetrà crear discos virtuals dins de la cabina de discos que seran essencials per a l'execució de l'alta disponibilitat en un entorn amb vCenter Server.

Ahora que ja tenim nostros discos virtuals procedirem a compartir aquests discos via iSCSI a nostros host ESXI, los quals tendran accés simultani a aquests discos. Això nos permetrà establir vinculos de dades entre nostros dos hipervisores que supondrà la possibilitat de la realització de l'alta disponibilitat.

CAMPUS D'ALCOI

La configuración nos tendría que quedar de la siguiente manera:



Ilustración 8. Configuración nodos HP VSA

Donde podemos observar que tenemos un grupo de administración nombrado VSAN, un Fault Tolerance Manager, nombrado FOMA, podemos ver dos sistemas de almacenamiento que son el hpvsab y el hpvsac y nuestros dos volúmenes creados, que serán compartidos a los hipervisores para que creen discos en cada uno de ellos.

Configurar volúmenes

Para crear nuestros volúmenes nos tenemos que desplazar hasta la carpeta de Volúmenes e instantáneas y pulsar botón derecho sobre esta carpeta. Una vez hayamos pulsado, nos saldrá un pequeño desplegable y pulsaremos sobre nuevo volumen, abriéndonos una venta de las siguientes características:



Ilustración 9. Configurar Volumen HP VSA

Aquí en la ventana de básico pondremos un nombre a nuestro volumen, y le asignaremos un tamaño de espacio, escribiendo el tamaño de discos que queramos en la casilla de Tamaño informado. Ya en la ventana de Avanzado nos permite elegir que RAID vamos a aplicar a nuestro volumen, así como en que clúster lo vamos a aplicar y como deseamos que se comporte la asignación de espacio en disco, de manera fina o gruesa como muestra la siguiente imagen:

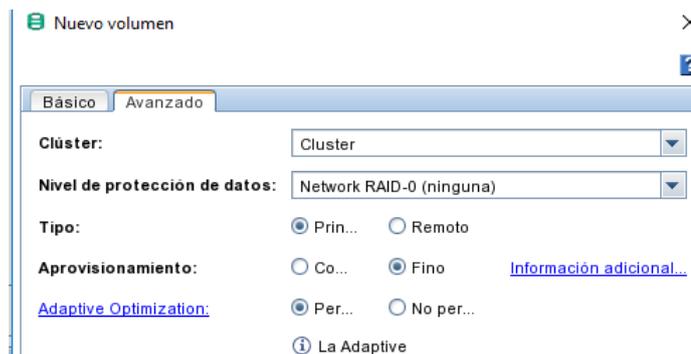


Ilustración 10. Propiedades del Volumen

Como hemos elegido un RAID 0, nos avisa de que es un tipo de RAID sin protección, en nuestro caso también elegiremos aprovisionamiento fino debido a las limitaciones de espacio de nuestro sistema, aunque en un entorno real es conveniente utilizar aprovisionamiento grueso debido a que ya tiene preseleccionado el espacio de memoria en disco mejorando así el rendimiento

CAMPUS D'ALCOI

de escritura y lectura. Cabe recordar que para que esto tenga sentido, nuestros discos virtuales creados en nuestro hipervisor ya deben tener aprovisionamiento grueso.

3.6.3 Conectar los discos de las cabinas a los hipervisores

Una vez tengamos nuestros volúmenes creados, deberemos de acceder a nuestro hipervisor ESXI, en el apartado de almacenamiento, seleccionamos adaptadores y nos vamos al apartador de iSCSI de Software.

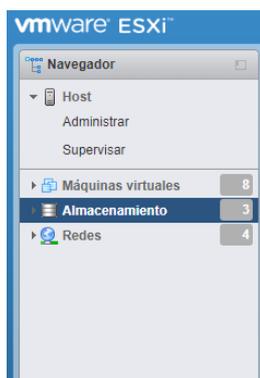


Ilustración 11. Panel lateral VMware ESXi

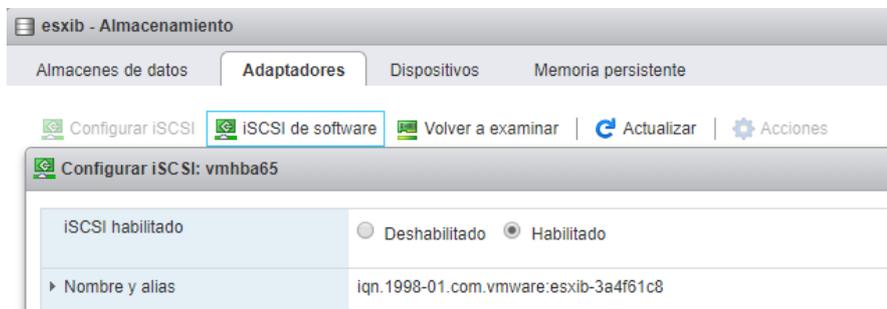


Ilustración 12. Obtener IQN

Una vez en este apartado veremos nuestro nombre y alias, esta será la información necesaria que debemos de introducir en nuestro grupo de administración para que pueda conectarse el host ESXI por iSCSI a los discos de la cabina de discos virtual. Ahora nos desplazaremos hasta nuestro CMC y pulsaremos con el botón derecho de nuestro ratón sobre la carpeta servidores y pulsaremos nuevo servidor y nos aparecerá la siguiente ventana, donde configuraremos nuestro servidor.

Ilustración 13. Dar de alta ESXi en HP VSA

A continuación, nos iremos a los volúmenes previamente creados, pulsaremos botón derecho sobre cada uno de ellos y les daremos a editar, entonces les asignaremos los permisos que deseemos a nuestros servidores, en este caso, nuestros tres servidores deben de contar con los permisos de escritura y de lectura como muestra la siguiente imagen:

Nombre	Asignado	Permiso
ESXI	<input checked="" type="checkbox"/>	Lectura/escritura
ESXIB	<input checked="" type="checkbox"/>	Lectura/escritura
ESXIC	<input checked="" type="checkbox"/>	Lectura/escritura

Ilustración 14. Asignar permisos en HP VS

Una vez tengamos nuestros hipervisores correctamente configurados correctamente en el CMC y con los permisos adecuados sobre los volúmenes, pasaremos a la creación pulsando con el botón derecho de nuestro ratón sobre la carpeta servidores y seleccionando nuevo clúster del servidor. Esto nos permitirán que estos servidores compartan volúmenes sin que estos puedan perder consistencia de datos nuestros volúmenes creados, para lo cual nos saldrá la siguiente ventana:

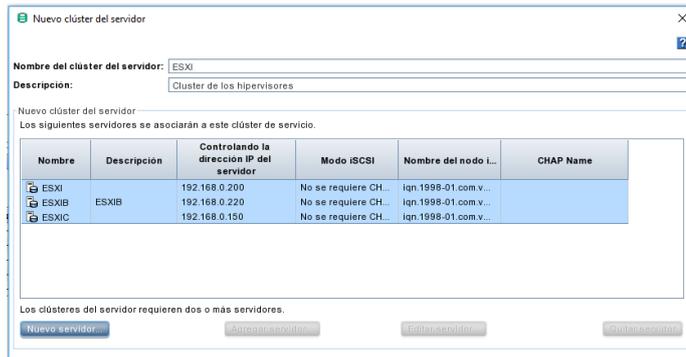


Ilustración 15. Configuración del clúster del servidor

Agregaremos nuestros tres hipervisores mediante su dirección IP y confirmaremos que el equilibrio de carga está habilitado y los permisos que disponemos sobre nuestros volúmenes pulsando en el botón de editar configuraciones del clúster del servidor.

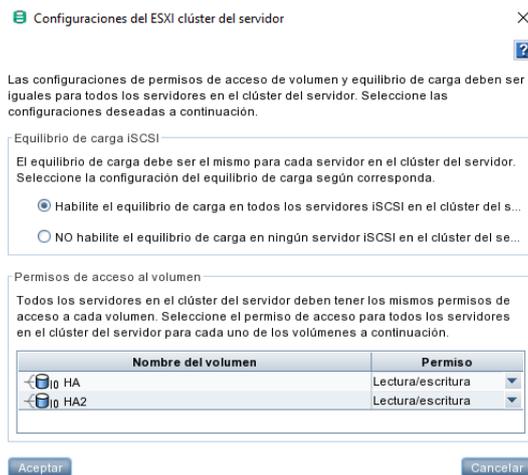


Ilustración 16. Configuración de los volúmenes en el clúster de servidores

3.6.4 Configuración de discos en ESXI

Ya de vuelta a nuestros hipervisores, nos vamos a la pestaña de almacenamiento y seleccionamos la pestaña de adaptadores, como ya se ha mostrado en una página anterior, seleccionamos el botón de iSCSI de software y nos desplegará la siguiente ventana:

Configurar iSCSI: vmhba65

iSCSI habilitado: Deshabilitado Habilitado

Nombre y alias: iqn.1998-01.com.vmware.esxi-3a4f61c8

Autenticación de CHAP: No utilizar CHAP

Autenticación de CHAP mutua: No utilizar CHAP

Configuración avanzada: Haga clic para expandir

Enlaces de puertos de red

NIC de VMkernel	Grupo de puertos	Dirección IPv4
vmk1		192.168.0.223
vmk0	Management Network	192.168.0.220

Destinos estáticos

Destino	Dirección	Puerto
iqn.2003-10.com.leftandnetworks.vsan:33:ha2	192.168.0.250	3260
iqn.2003-10.com.leftandnetworks.vsan:30:ha	192.168.0.250	3260

Destinos dinámicos

Dirección	Puerto
192.168.0.250	3260
192.168.0.235	3260
192.168.0.153	3260

Guardar configuración Cancelar

Ilustración 17. Configuración iSCSI final en ESXi

En ella podemos ver la configuración entera de nuestro iSCSI, primero crearemos un VMkernel para cada uno de nuestros enlaces físicos de red nuestro servidor, en este caso utilizamos dos enlaces de red virtuales sobre dos adaptadores físicos, y entonces los juntamos en un conmutador estándar, de este modo ya podremos agregar enlace de puertos para poder tener alta disponibilidad a nivel de enlaces físicos, lo cual nos permite continuar la producción en caso de que falle una tarjeta de red.

Una vez tengamos nuestro enlace de puertos virtual, nos dispondremos a agregar los destinos dinámicos, a los cuales agregaremos la IP virtual que nos proporciona el grupo de administración de CMC, aunque en nuestro caso y para mayor seguridad, se ha puesto las direcciones IP de las cabinas de discos virtuales. Acto seguido, aparecerán los destinos estáticos que son ni más ni menos que las direcciones IQN de los volúmenes creados.

CAMPUS D'ALCOI

Cuando creamos un nuevo almacén de datos, a continuación, nos mostrará los discos que queremos seleccionar para crear nuestro nuevo disco duro virtual, elegiremos el disco con el nombre de LETHAND iSCSI Disk como muestra la siguiente imagen:

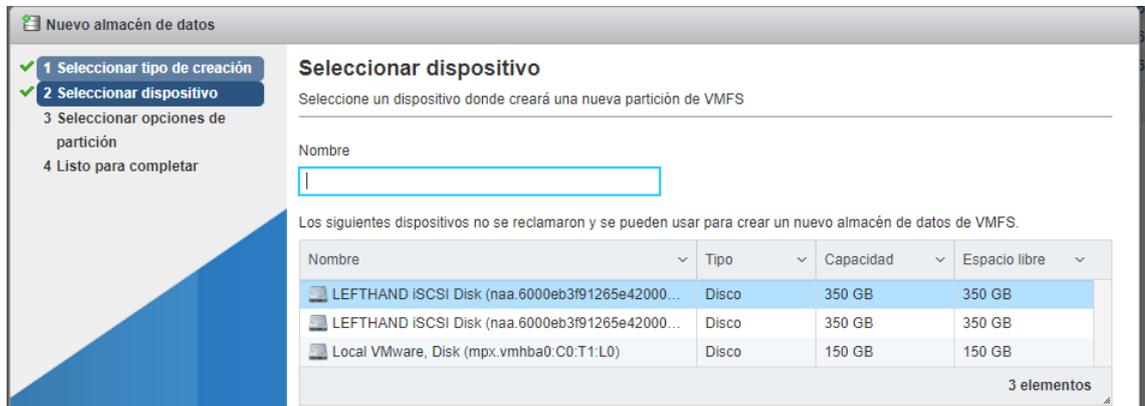


Ilustración 18. Crear Disco Compartido

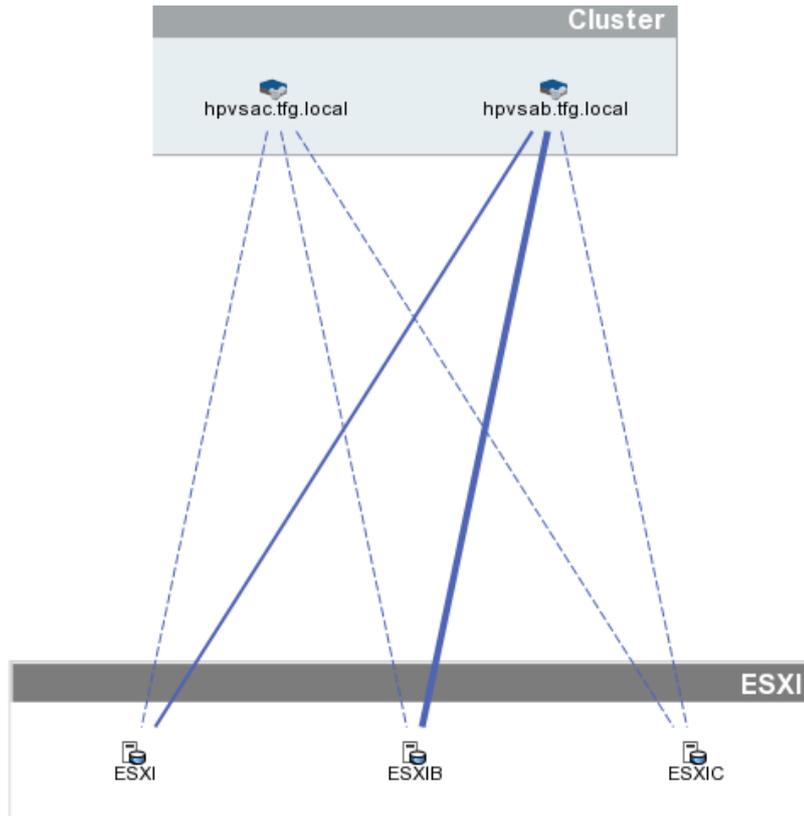
El siguiente paso sería crear dos discos diferentes que podrán ser accedidos por los hosts que tengan acceso a esos discos iSCSI, quedando la configuración de discos creada de la siguiente manera:



Ilustración 19. Lista de discos compartidos

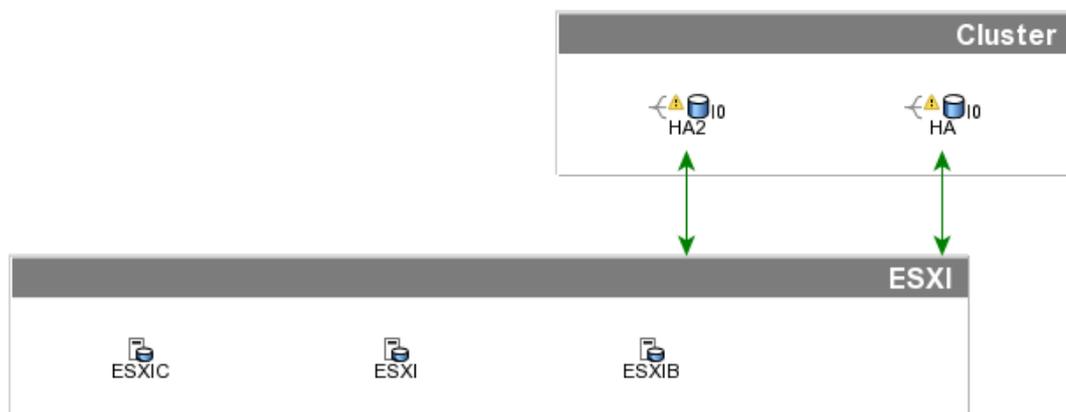
Siendo utilizado el disco Compartido A para instalar las máquinas virtuales del host A, y el disco Compartido B para las máquinas virtuales de host B, en este punto ya tendremos todo lo necesario para poder instalar nuestras máquinas virtuales en nuestros discos iSCSI y poder realizar la alta disponibilidad sin problema.

Los esquemas finales de como quedaría desplegado nuestra estructura de replicación de datos y de configuración de volúmenes y de hosts son los siguientes:



Il·lustració 20. Esquema de accés de los servidors a las cabinas

En el primer esquema podemos ver que los hosts están interconectados a ambas cabinas de discos y las conexiones de red en alta disponibilidad a la información alojada en dichas cabinas que forman el clúster de cabinas.



Il·lustració 21. Esquema de accés de los servidors a los volúmenes

En este segundo esquema podemos ver que nuestros hosts tienen acceso a ambos volúmenes del clúster y que son accesibles por todos los hosts.



Con esto ya tendríamos todo lo necesario para poder empezar a trabajar con nuestras máquinas virtuales y poder empezar a instalar nuestros sistemas operativos para las tareas pertinentes en nuestra empresa.

3.7 CONFIGURACIÓN DE LA ALTA DISPONIBILIDAD

3.7.1 Requisitos mínimos de hardware y de software

3.7.1.1 *Requisitos Hardware*

- Necesidad de disponer de servidores escalables, aunque esto dependerá de la cantidad de máquinas virtuales que dispongamos que como mínimo disponga de:
 - Tener un mínimo de 4 puertos de red a gigabit como mínimo.
 - Disponer de redundancia de fuentes de alimentación para evitar posibles roturas.
 - Disponibilidad de discos Hot Plug que nos permitan retirar discos duros dañados sin necesidad de apagar nuestro servidor.
 - Suministro de energía regulado y asegurado por un suministrador ininterrumpido de alimentación asegurando la electricidad de manera continua.
 - Disponibilidad de un procesador, en caso de realizar operaciones en el servidor con un alto coste computacional disponer de un segundo procesador si el primero no fuera suficiente.
 - Disponer de un mínimo de 64 GB de memoria RAM RDIMM DDR4 con ECC para protegernos de los errores de memoria.
 - Disponer de discos duros de 7200 rpm en caso de que sean HDD, su tamaño dependerá de la cantidad de memoria que vayamos a utilizar.
- En el aspecto de hardware a nivel de redes necesitamos como mínimo:
 - Disponer de dos switches por cada armario interconectados entre si mediante enlace de fibra óptica sfp y links de 1 GB/s de velocidad como mínimo.
 - Router con la capacidad de disponer de como mínimo 1 puerto de fibra SFP y puertos de red de Gigabit, además de una CPU y memoria RAM acorde con el procesamiento de datos que se va a realizar y que tendrá que gestionar el router.



3.7.1.2 **Requisitos Software**

- Necesitaremos diferentes licencias para poder trabajar con el software deseado
 - Licencia VMware vSphere, el hipervisor que vamos a utilizar en nuestro caso.
 - Licencia de vCenter Server Appliance para poder gestionar nuestro hipervisor y así poder gestionar tanto nuestro almacenamiento a nivel de servidor como la protección ante desastres.
 - Licencia de HP VSA que será nuestro software de cabina de discos virtual.
- Programas necesarios
 - HPE StoreVirtual Centralized Management Console.
 - Navegador que admita HTML 5 o que tenga instalado la última versión de Adobe Flash Player.

3.7.2 **Requisitos previos a la realización de la alta disponibilidad**

3.7.2.1 **Creación de un entorno de red adecuado.**

Para la creación de nuestro entorno de red adecuado, debemos de disponer de dos adaptadores de red físicos que nos permitan realizar la creación de un distributed switch de VMware, esto nos permitirá una mejor utilización de los puertos de red que tengamos, ya que este switch nos ofrece una mejor optimización y control sobre las Vlans, ya que permite utilizar alta disponibilidad en adaptadores físicos, permitiéndonos optimizar la de creación de Vlans y ofreciéndonos la posibilidad de establecer LACP, aparte de poder monitorizar todo el tráfico de movimiento de datos permitiéndonos saber si nuestra alta disponibilidad funciona de manera correcta, ampliar y controlar cuanto ancho de banda ocupa el tráfico al momento. Además, en este switch podemos añadir diferentes hosts, lo cual nos permitirá aplicar todos sus beneficios a nivel global de hosts y nos ayudará en la tarea de mantenimiento de nuestros sistemas.

Porqué en nuestro sistema es importante un LACP como el que nos ofrece el VMware Distributed Switch (VDS), es importante debido a que nosotros moveremos una gran cantidad de datos a través de nuestra red, y para que esto sea posible demos de tener el mayor ancho de banda posible a nuestro alcance, ya que un mayor ancho de banda nos permitirá que nuestros sistemas no tengan problema alguno a la hora de realizar tareas de escritura y lectura



CAMPUS D'ALCOI

en la cabina de discos virtual de otra sede. Para ello debemos tener cuatro tipos de Vlans necesarias: Una Vlan de datos para el acceso a internet de nuestros sistemas operativos y servidores, una Vlan de management para poder gestionar de manera segura todos nuestros dispositivos gestionables de nuestra sede, desde switch y routers hasta nuestra cabina de discos y nuestro hipervisor.

Otra Vlan necesaria, sería la Vlan de almacenamientos, la cual solo se utilizaría para el movimiento de datos entre cabinas, así como si debemos mover una máquina virtual o escribir en nuestra cabina de discos virtual, esta Vlan necesita mayor ancho de banda para funcionar, y por último y también muy importante la Vlan de Heartbeat.

Esta Vlan servirá a nuestros Vcenter Server saber que dispositivos están activos y si deben o no deben enchufar las máquinas virtuales, por tanto, esta Vlan nos permitirá saber si nuestros hosts o servidores físicos están encendidos y si están funcionando adecuadamente sus máquinas virtuales. A esta Vlan se le debería asignar un mínimo de ancho de banda, debido a que, si la red de storage nos colapsara toda nuestra red, se podrían producir retardos en los latidos entre hosts, lo cual podría llevar a ejecutar nuestras políticas de alta disponibilidad sin que uno de nuestros servidores este fuera de línea.

3.7.2.2 Creación del almacén de datos de latido

Para poder crear dicho almacén y que sea compartido por ambos hosts, debemos de crear otro volumen en nuestra cabina de discos virtuales e inicializarlo en uno de nuestros hipervisores ESXI. En nuestro caso, como se utiliza el propio almacén de discos como almacén de latidos, no he hecho este paso, pero en entornos con una mayor virtualización y donde hay más máquinas virtuales en alta disponibilidad, es un elemento imprescindible.

3.8 CONFIGURACIÓN DE VSPHERE HA ANTE LAS CATÁSTROFES

Para poder realizar la protección de datos de manera adecuada a nuestras necesidades, necesitamos configurar varios campos de la manera más adecuada a nuestro entorno.

3.8.1 Errores y respuestas

Aquí se establece la configuración de las respuestas de nuestro host ante un posible fallo, un aislamiento del host, su monitorización y la protección de



CAMPUS D'ALCOI

componentes de las máquinas virtuales. Para acceder a dichas configuraciones debemos de seguir los siguientes pasos:

1. En vSphere Web Client, desplácese hasta el clúster de vSphere HA.
2. Haga clic en la pestaña Configuración.
3. Seleccione Disponibilidad de vSphere y haga clic en Editar.
4. Clic en Errores y respuestas y expanda Respuesta de error de host.
5. Seleccione una de las siguientes opciones de configuración.

En ella podemos encontrar las siguientes configuraciones:

- a. Respuesta ante errores:

Si esta opción está desactivada, entonces se obviara el monitoreo del host por parte de VMware, y las máquinas virtuales no serán reiniciadas en caso de fallo. Si está seleccionada la opción de reiniciar las Máquinas virtuales, éstas se reiniciarán por orden de prioridad en caso de que falle el host.

- b. Prioridad de reinicio de la máquina virtual por defecto:

La prioridad de reinicio determina el orden en el cual las máquinas virtuales son reiniciadas cuando falla el servidor, por tanto, cuanto mayor prioridad tenga antes serán reiniciadas. Si tuviéramos varios hosts, se reiniciaría primero las máquinas virtuales del primer host, y después las máquinas del segundo host.

- c. Condición de reinicio de dependencia de máquina virtual:

Se debe seleccionar una condición específica, así como un tiempo de retraso de para aplicar las reglas después de que ocurra dicha condición para que vSphere HA continúe con la prioridad de reinicio de las máquinas virtuales.

3.8.2 Respuesta ante el aislamiento del host

En caso de que nuestros dispositivos quedarán bloqueados o en estado de aislamiento impidiendo que nuestra alta disponibilidad funcione al momento, se procedería a realizar tres diferentes opciones:

- a. Desactivado: No hace nada al respecto.
- b. Desconectar y reiniciar las máquinas virtuales: Apaga correctamente las máquinas virtuales y posteriormente las reinicia.
- c. Apagar y reiniciar las máquinas virtuales: Apaga de golpe la máquina virtual y la reinicia.



Para poder realizar dicha configuración, procederemos de la siguiente manera:

1. En vSphere Web Client, desplácese hasta el clúster de vSphere HA.
2. Hacer clic en la pestaña Configurar.
3. Seleccione Disponibilidad de vSphere y haga clic en Editar.
4. Hacer clic en Errores y respuestas y expanda Respuesta de error de host.
5. Seleccione una de las siguientes opciones de configuración.

3.8.3 Configurar respuestas VMCP

Ahora se procede a configurar el comportamiento que tendrá la Protección de componentes de la máquina virtual (VM Component Protection), cuando encuentra un error PDL o APD en un almacén de datos. Para acceder a esta característica solo debemos pulsar en editar seleccionando vSphere HA.

3.8.3.1 Error PDL

Un error PDL (Permanent Device Lost) es un error que ocurre cuando el dispositivo de almacenamiento es desconectado del host ESXi sin haber sido desmontado y liberado. Si tenemos este error, el host deja de enviar peticiones de entrada y salida a la matriz de almacenamiento, ya que se considerará que estará permanentemente inaccesible.

Para solucionar este problema tendremos de tres maneras diferentes de actuar ante esta situación:

1. Desactivar: Desactiva esta opción.
2. Notificar: Notifica al administrador el estado de error
3. Apagar y reiniciar las máquinas virtuales: permite reiniciar las máquinas virtuales en host que aún tienen conectividad con el disco de almacenamiento.

En mi caso he optado por esta tercera opción ya que esta opción nos, lo que nos permite volver a iniciar las máquinas virtuales de manera inmediata y así reducir drásticamente el tiempo de reacción ante el desastre. Este hecho lo detecta el otro host que al momento que detecta que la máquina virtual está apagada la inicia en su host en ese preciso instante, y por tanto nos permite tener tiempo de maniobra para poder solucionar el problema



3.8.3.2 Error APD

Un error APD (All Paths Down) ocurre cuando un host vSphere no puede acceder al dispositivo de almacenamiento y no se recibe el código de PDL SCSI desde la matriz de almacenamiento. Esto indica que el host no tiene suficiente información para dictaminar que nuestro dispositivo de almacenamiento está temporalmente inaccesible o si está inaccesible de manera permanente, teniendo un timeout de 140 segundos, más el periodo de espera que es de 3 minutos por el retraso de VM Failover, por defecto, en 5 minutos y 20 segundos se empezarán a realizar las acciones deseadas en las máquinas virtuales en el caso que tengamos esta configuración.

Estas configuraciones son las siguientes:

1. Desactivar: Desactiva esta opción.
2. Notificar: Notifica al administrador el estado de error
3. Apagar y reiniciar las Máquinas Virtuales (Conservador): En caso de que suceda este error vSphere HA no intentará reiniciar las máquinas virtuales en un host activo sin el permiso del Maestro HA, que se encarga de determinar si el host activo tiene la suficiente capacidad para soportar la carga de trabajo que representan las máquinas virtuales del host inactivo. Si el Maestro considera que no hay suficiente capacidad para estas máquinas virtuales, no se tomará ninguna acción
4. Apagar y reiniciar las Máquinas Virtuales (Agresivo): En este caso, si el Maestro HA no es accesible, se obviarán por completo y se realizará el inicio de las máquinas virtuales del host inactivo en el host activo sin importar el estado de este último y si puede soportar la carga de trabajo de estas nuevas máquinas virtuales

En este caso he optado por un reinicio agresivo, ya que los dos hosts cuentan con las mismas especificaciones y el host secundario solo ejerce como dispositivo de backup y por tanto podrá soportar la carga de trabajo de las máquinas replicadas y no nos dará error al iniciar las máquinas en este segundo host.

3.8.4 Proactive HA

Proactive HA nos permite actuar ante una degradación de un host, que quiere decir es que estamos presentes ante un error parcial del host. Para acceder a esta característica solo debemos pulsar en editar seleccionando Proactive HA.



Tendremos dos niveles de configuración:

1. Opciones de Automatización:

a. Manual:

vCenter Server sugerirá recomendaciones de migraciones para máquinas virtuales.

b. Automático:

Las máquinas virtuales se migrarán a hosts sanos y los hosts degradados se pondrán en modo cuarentena o modo mantenimiento dependiendo del nivel de automatización configurado.

2. Nivel de Automatización

a. Modo cuarentena para todos los fallos:

Equilibra el rendimiento y la disponibilidad, evitando usar los hosts parcialmente degradados siempre y cuando no se afecte al rendimiento de la máquina virtual.

b. Modo de cuarentena para fallos moderados y modo mantenimiento para errores graves o modo mixto:

Balancea entre el rendimiento y la disponibilidad evitando usar los hosts degradados moderadamente siempre que el rendimiento de la máquina virtual no sea afectado. En este modo nos aseguramos de que las máquinas virtuales no se ejecutan en hosts con fallos graves.

c. Modo mantenimiento para todos los fallos:

Asegura que las máquinas virtuales no se ejecuten en hosts con fallos parciales.

En mi caso utilizaré el modo mixto debido a que no queremos que nuestro host degradado siga corriendo las máquinas virtuales y poder utilizar así nuestro host de reserva y poder realizar tareas de mantenimiento en nuestro host degradado.



3.8.5 Control de admisión

Después de crear nuestro clúster podemos configurar el control de admisión para especificar que máquinas virtuales pueden ser encendidas en caso de que ellas violen las restricciones de disponibilidad. Para acceder a esta característica solo debemos pulsar en editar, seleccionando vSphere HA y posteriormente seleccionaremos en Control de Admisión, seleccionaremos el número de hosts que permitiremos que fallen en el host y definiremos la capacidad de Failover por error del host. Para ello tenemos diferentes opciones que son:

1. Porcentaje de recursos del clúster:

Especifica el porcentaje de uso de CPU y memoria que puede reservar en el clúster para poder admitir el Failover.

2. Política de máquinas virtuales activas:

Seleccionar la cantidad de máquinas virtuales que vamos a permitir correr en el host en caso de fallo.

3. Hosts dedicados para el Failover:

Seleccionamos un host para realizar las acciones de Failover sobre el host seleccionado. Si este host no tiene suficientes recursos, se podrán utilizar otros hosts para correr las máquinas virtuales.

4. Desactivado:

Permite a las máquinas virtuales ejecutarse, aunque violen las restricciones de disponibilidad.

En nuestro caso no he utilizado ninguna de estas opciones, ya que he seleccionado la opción de desactivado, ya que tenemos un host donde almacenar las máquinas virtuales y otro para poder realizar la alta disponibilidad y por tanto estará siempre disponible.

3.8.6 Configurar el almacén de datos de latidos

vSphere HA utiliza los almacenes de datos de latidos para distinguir entre dos hosts, cual es el host que ha fallado y cuál es el host que están activos en nuestra red. Este apartado se configura pulsando en editar seleccionando vSphere HA y posteriormente seleccionaremos en Almacén de datos para verificar latidos. Existen tres tipos de configuraciones posibles:

1. Seleccionar automáticamente el almacén de datos desde el host.
2. Usar solo los almacenes de datos especificados
3. Usar los almacenes de datos especificados y complementar automáticamente si es necesario.

En nuestro caso lo hemos elegido automáticamente, ya que todos los discos son accesibles por ambos hosts y pueden comunicarse entre ellos a través de esos almacenes de datos.

3.8.7 Comprobación de la configuración

Una vez conocemos y ya tenemos configurado nuestro vSphere HA. Ahora deberá quedarnos nuestro vCenter Server de esta manera:

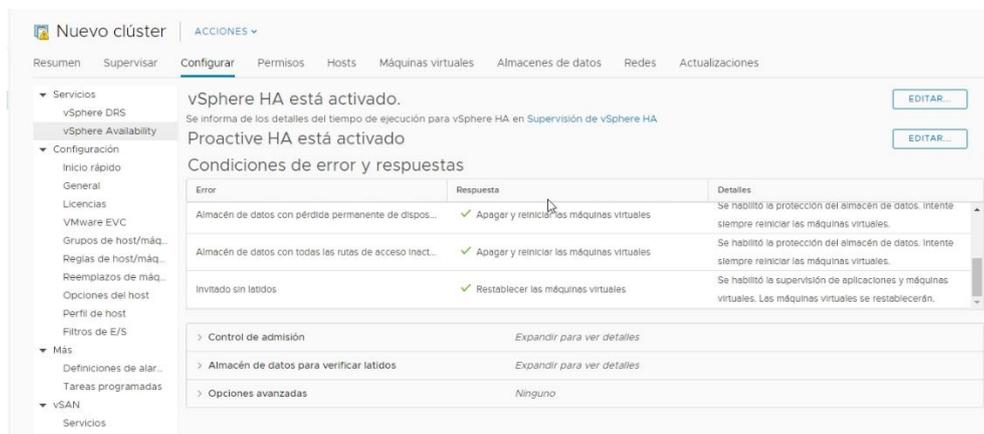
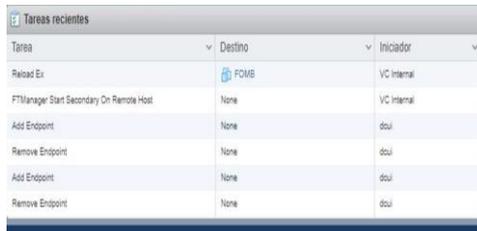


Ilustración 22. Vista de la configuración de vSphere HA

Ahora ya solo debemos de dirigirnos a una máquina virtual de nuestro host y activar la alta disponibilidad en dicha máquina, para ello seleccionaremos el host destino, que en nuestro caso será el host de backup, y el almacén de datos en el cual queremos poner nuestra máquina virtual. Acto seguido se empezará a configurar nuestra alta disponibilidad y se copiarán los datos de la máquina virtual.

CAMPUS D'ALCOI

Una vez tengamos ya configurada nuestra alta disponibilidad, procederemos a probar que funciona correctamente, para ello nos situaremos sobre la máquina virtual con alta disponibilidad y seleccionaremos hacer la prueba de conmutación por error, y si el resultado es igual que el da la siguiente imagen, entonces ya tendremos configurada y funcionando nuestra alta disponibilidad.



Tarea	Destino	Iniciador
Release ESX	FCMB	VC Internal
FTManager Start Secondary On Remote Host	None	VC Internal
Add Endpoint	None	dou
Remove Endpoint	None	dou
Add Endpoint	None	dou
Remove Endpoint	None	dou

Ilustración 23. Prueba de funcionamiento de HA (1)

En esta imagen podemos observar cual sería los pasos que seguiría nuestro hipervisor ESXi y como el FTManager enciende nuestra máquina virtual secundaria.



Nombre de ...	Destino	Condición
Probar conmutación por error	FCMB	Completado
Volver a configurar máquina virtual	VMware ...	Completado

Ilustración 24. Prueba de funcionamiento de HA (2)

En esta podemos ver que el resultado de realizar la prueba por conmutación por error es correcto y que, por tanto, hemos configurado adecuadamente la alta disponibilidad.

3.9 CONFIGURACIÓN DE VSPHERE REPLICATION

Aquí nos encontramos ante nuestra tercera forma de tener replicados todos nuestros datos, esta es una forma más barata que la anterior debida principalmente a que ya no necesitamos el uso de la cabina de discos virtuales HP VSA, y su licencia viene incluida en la licencia de VMware vSphere Essentials kit plus, la misma licencia que lleva incluido vSphere HA. Esta forma de guardar nuestros datos nos permite crear copias idénticas de nuestras máquinas virtuales en nuestro host cada determinado rango de tiempo sin la posibilidad de que cuando falle nuestra máquina virtual principal, se encienda sola la replicada, ya que se debería iniciar manualmente.

El tiempo mínimo de replicación dependerá de diversos factores como la velocidad de lectura y escritura de nuestros discos y el ancho de banda del cual dispondremos para la copia de datos.



Además, para poder realizar correctamente la instalación de vSphere Replication, deberemos tener instalados en ambos servidores vCenter Server y vSphere Replication, y ambos hosts dados de alta en vCenter Server.

3.9.1 Instalación de vSphere Replication

Para instalar vSphere Replication debemos descargarnos la imagen de vSphere replication de la página web de VMware. Una vez tengamos descargada la ISO en nuestro ordenador la abrimos o la quemamos en nuestro ordenador.

Dicho ordenador deberá tener acceso a vCenter Server, ya que en la plataforma web de vCenter deberemos realizar la instalación de nuestra máquina virtual. Para realizar el primer paso en la instalación, deberemos seleccionar el host donde queramos instalar la máquina virtual, pulsaremos botón derecho sobre el host y elegiremos la opción de Implementar plantilla de OVF, entonces seleccionaremos el archivo .ovf y el .vmdsk de la iso de vSphere Replication, Posteriormente nos preguntará por el nombre de nuestra máquina virtual a crear y una contraseña para el usuario root, así como su FQDN, su direccionamiento IP, y los servidores DNS, en mi caso he utilizado la ip: 192.168.0.152.

Una vez completemos toda la configuración, Acto seguido aceptaremos todas las políticas de uso y privacidad e instalaremos nuestra máquina virtual.

La máquina virtual necesitará un mínimo de 20 GB de espacio en disco duro y 8 GB de memoria RAM, además de dos CPU.

3.9.2 Configurar vSphere Replication

Para configurar el motor de vSphere Replication, deberemos acceder a la dirección IP 192.168.0.152 en nuestro navegador web a través del puerto 5480. Acto seguido nos loguearemos con nuestras credenciales de root.

Una vez estemos dentro nos desplazaremos a la ventana de configuración y rellenaremos los campos vacíos de la siguiente manera:



Startup Configuration

Configuration Mode:	<input checked="" type="radio"/> Configure using the embedded database <input type="radio"/> Manual configuration <input type="radio"/> Configure from an existing VRM database	Actions <input type="button" value="Save and Restart Service"/> <input type="button" value="Unregister VRMS"/> <input type="button" value="Reset Embedded Database"/>
LookupService Address:	<input type="text" value="192.168.0.151"/>	
SSO Administrator:	<input type="text" value="Administrator@vsphere.local"/>	
Password:	<input type="password" value="*****"/>	
VRM Host:	<input type="text" value="192.168.0.202"/> <input <="" td="" type="button" value="Browse..."/> <td></td>	
VRM Site Name:	<input type="text" value="vSphere Replication A"/>	
vCenter Server Address:	<input type="text" value="192.168.0.151"/>	
vCenter Server Port:	<input type="text" value="80"/>	
vCenter Server Admin Mail:	<input type="text" value="root@192.168.0.202"/>	
IP Address for Incoming Storage Traffic:	<input type="text" value="192.168.0.202"/>	

Il·lustració 25. Configuración de vSphere Replication

Seleccionaremos que vSphere Replication use su base de datos embebida, ya que para mi caso me basta con esta base de datos y no hace falta que creamos una base de datos SQL o Oracle para poder gestionar nuestra replicación.

En LookupService address pondremos la dirección ip de nuestro vCenter Server, está opción ya viene por defecto, ya que es la dirección ip donde se instala el servicio que utilizará vSphere Replication, igual que el administrador del SSO, al cual le tendremos que poner nuestra contraseña. En el caso del vSphere Replicator Manager (VRM), como tenemos embebida nuestra base de datos y todo está instalado en la misma dirección IP, pondremos la dirección ip de la máquina y en VRM Site Name, le pondremos el nombre que deseemos para nuestro VRM. Acto seguido le diremos cuál es la IP de nuestro vCenter Server y el resto de las opciones las dejaremos por defecto.

Una vez tengamos nuestros datos metidos, pulsaremos Save and Restart y nos saldrá un aviso de ssl, entonces le decimos que sí, y entonces se procederá a configurar nuestro vSphere Replication, para saber si tenemos bien configurado nuestro vSphere Replication, nos tendrá que señalar el estado del servicio de la siguiente manera:

Service Status

<input type="button" value="Restart"/>	VRM service is	running
<input type="button" value="Restart"/>	Tomcat service is	running

Il·lustració 26. Estado final de los servicios de vSphere Replication

A continuación, accederemos a vCenter Server Appliance a través de la web y pulsaremos el botón derecho sobre una máquina virtual y seleccionaremos la opción de todas las acciones de Site Recovery, entonces se nos desplegará un



CAMPUS D'ALCOI

submenú con dos opciones, configurar esta máquina virtual o reconfigurar esta máquina virtual. En este caso y como es la primera seleccionaremos configurar esta máquina virtual, acto seguido se nos abrirá otra pestaña donde accederemos al VRM y nos dará las opciones para poder replicar nuestra máquina virtual.

Una vez estemos en esta pestaña seleccionaremos el host ESXi donde queremos que se copie nuestra máquina virtual, una vez tengamos seleccionado nuestro host de destino, procederemos a seleccionar cada cuanto tiempo queremos que se replique nuestro host, dándonos la opción mínima de cada 5 minutos o incluso cada día, semana o mes.

3.9.3 Configuración de red

La configuración de red ideal para vSphere Replication es poder contar con tráfico separa mediante Vlan para la Vlan de vMotion, y así asegurarse un ancho de banda suficiente para que el proceso de copias de las máquinas virtuales se demore lo menos posible, y no ocupe todo el ancho de banda de nuestra red en general, por tanto lo recomendable sería crear un Virtual Distributed Switch(VDS), ya que nos viene incorporado en nuestra licencia de VMware, y en el cual crearíamos las Vlans de vMotion, management y de red normal para que el tráfico se balancee.

3.9.4 Configuración ideal y funcionamiento de vSphere Replication

Para poder elegir mejor cada cuando queremos tener nuestras máquinas virtuales replicadas, primero deberemos realizar un estudio de necesidades de nuestra empresa y cuánto tiempo y datos podemos perder en caso de fallo grave, por otra parte, también debemos de medir cuanto tiempo tarda en copiarse de host nuestra máquina virtual y sus consiguientes versiones, con todo esto podremos saber cada cuanto tiempo debemos realizar nuestra replicación. El proceso de movimiento de nuestra máquina virtual se realizará con vMotion, que es ni más ni menos la herramienta que utiliza vCenter Server para mover máquinas virtuales entre diferentes hosts.

El procedimiento de almacenamiento de versiones funciona de la misma manera que funcionarían los snapshots de las máquinas virtuales, los cuales tienen una imagen base de la máquina virtual y vamos añadiendo una especie de puntos de control a los cuales recurrir en caso de que se pierda información o la perdamos.



4 CONCLUSIÓN

A modo de conclusión he podido comprobar las tres diferentes maneras de salvar nuestros datos ante una catástrofe.

La primera sería la replicación de datos mediante la cabina de discos virtual HP VSA donde su fácil configuración nos permite replicar los datos en otro servidor. La segunda opción sería la utilización de vSphere HA, donde se complica de forma sustancial la configuración de la protección de nuestros datos y aumenta los recursos necesarios para poder aplicar esta protección tanto a nivel hardware, como software. Y por último tenemos vSphere Replication donde se simplifica mucho más la configuración y los recursos necesarios que vSphere HA, pero que ya necesita de configuración extra y de cálculo del tiempo cada el cual queremos crear una replicación, así mismo de la cantidad de replications que deseamos.

Primero de todo me centré en aprender cómo podía usar el almacenamiento en red mediante la cabina de discos de HP, así como sus utilidades a la hora de almacenar datos, actuando como un servidor de datos donde puede acceder cualquier servidor vía iSCSI, después me centré en como poder instalar todas las máquinas virtuales, así como los requisitos hardware necesarios para su correcto funcionamiento y a posteriori vi cómo manejar correctamente toda la interfaz de vCenter Server, así como todo los elementos necesarios para que la configuración fuera lo más óptima posible, usando las diferentes características y herramientas que ofrece vCenter.

Una vez ya instalado y visto la interfaz web de vCenter procedí a la creación de un entorno de red adecuado, así como a la configuración de la alta disponibilidad, con varias de sus opciones de configuración, y la posibilidad de probar el funcionamiento de dicha herramienta. Por último, instalé vSphere Replication y analicé el método que se usaba para poder realizar la replicación de datos de una máquina a otra y como se podía configurar vSphere Replication, además de cuál sería la forma de que funcionara correctamente el mover los datos de un host a otro.

En conclusión, he realizado un amplio análisis del funcionamiento de la herramienta de virtualización de servidores más usada, así de como poder usar sus herramientas adecuadamente, así como el poder usar una cabina de discos virtual y conocer todas las ventajas que ello ofrece.



4.1 VALORACIÓN PERSONAL

Debido a mi situación laboral actual a jornada completa, no he podido realizar un despliegue real de lo que supondría la realización de este trabajo, ya que por cuestiones tanto de tiempo como de imposibilidad de acceso a los recursos ofrecidos por mi tutor, no he podido realizar el correcto despliegue y por tanto he tenido que realizar el trabajo en mi ordenador personal con todas las limitaciones que eso supone, ya que me hubiera gustado poder realizar todo el entorno de red y poder medir tasas de transferencia de datos, como de rápido es la actuación de las medidas de seguridad en un entorno real, y poder haber probado todo el trabajo realizado y todo el tiempo que he invertido en él. Aun así, me siento satisfecho de haber podido realizar este trabajo en el que he podido profundizar mejor en el mundo de la virtualización y todas las herramientas que hay al alcance de ella para poder optimizar mejor nuestros recursos materiales y así poder estudiar y experimentar con varias de las herramientas desarrolladas por VMware.

También me ha servido para asentar mejor los conocimientos básicos sobre el almacenamiento compartido y sus utilidades, además de poder ver que, si queremos tener bien protegidos todos nuestros datos frente a catástrofes, las cosas no son tan fáciles como parece debido a que existen muchos factores, tanto de configuración como externos que nos complican el llevar a cabo nuestra tarea de manera sencilla.

Este trabajo también me ha servido para entender como funcionaría la organización de la red en nuestra empresa, así como la correcta organización de los recursos disponibles y su máxima optimización.



5 BIBLIOGRAFÍA

- [¿Qué son los Hipervisores?](http://www.datakeeper.es/?p=716)
<http://www.datakeeper.es/?p=716>
- Características Servidor HP.
<https://www.hpe.com/es/es/product-catalog/servers/proliant-servers/pip.specifications.hpe-proliant-dl360-gen10-server.1011484546.html>
- Características Microserver
<https://www.hpe.com/es/es/product-catalog/servers/proliant-servers/pip.specifications.hpe-proliant-microserver-gen10.1010930707.html>
- Información sobre las características y configuración de vSphere Availability.
<https://docs.vmware.com/en/VMware-vSphere/6.5/vsphere-esxi-vcenter-server-65-availability-guide.pdf>
- Información sobre el precio y características de los productos vSphere.
https://store.vmware.com/store/vmwde/es_ES/cat/ThemeID.29219600/categoryID.66680900
- Información sobre las respuestas VMCP
<https://blogs.vmware.com/vsphere/2015/06/vm-component-protection-vmcp.html>
- Información sobre vSphere Replication
<https://docs.vmware.com/es/vSphere-Replication/8.1/com.vmware.vsphere.replication-admin.doc/GUID-97751DE8-17C2-4123-A3DD-C45475FE7782.html>
- Información sobre la creación de volúmenes y como compartirllos en una cabina de discos virtual HP VSA
https://www.youtube.com/watch?v=EJ_dj-qlVp8
- Información sobre la virtualización
<https://www.vmware.com/es/solutions/virtualization.html>
- Información sobre los centros de datos
<https://www.escueladeinternet.com/que-es-un-centro-de-datos/>