DISEÑO Y MIGRACIÓN DE CPD A ENTORNO CLOUD PARA GRANDES ENTORNOS EMPRESARIALES

César Cañada Alonso

Grado Ingeniería Informática, it. Computación

Administración de redes y sistemas operativos

Miquel Colobran Huguet

3 de enero de 2021

A María & Julián,

Ojalá pudierais verlo.

Dedicatoria y agradecimientos

Me gustaría empezar dando las gracias a mi familia, por todo lo que han hecho por mí todos estos años. Mis padres Puerto y César, mi hermano Álvaro, mi tío Emiliano y mi esposa Elena. Gracias a ellos soy quien soy.

A Miquel Colobran Huguet, por hacer de tutor durante el proyecto. Por su trabajo, revisándolo, aportando ideas, detalles, gracias. Y a todos los profesores de la UOC que me han acompañado por el camino.

A mis amigos, en especial a Brian por estar siempre ahí, por su ayuda, no tengo palabras para agradecer todo lo que me ayudó, por ser la persona tan especial que es. A Fernando, que desde que lo conozco no ha parado de apoyarme y creer en mí, por ver más allá de números, gracias amigo. También a José Luis, por estar siempre viendo el lado bueno de las cosas. Sin olvidarme de Luis V, Julio, Darío, … todos ellos han sido un apoyo para terminar la carrera.

Este TFG es la culminación de años de estudio, cuatro años de carrera y cuatro años de dos CFGS. En todo este tiempo he crecido como persona, durante todo este trayecto académico siempre ha estado escuchándome, primero como profesor y ahora como amigo. Me motivaste a estudiar, hiciste que me gustara, hiciste que pensara que podía llegar a conseguir algo, gracias, Antonio.

Durante todos estos años he trabajado en muchos sitios, he tenido muchos compañeros, todos ellos han aportado de alguna forma su granito de arena en este proyecto. Pero me gustaría destacar la persona de Luis F. Guijarro, él me dio una oportunidad cuando nadie lo hizo, confió en mí desde el primer día y es un referente para mí. Gracias por todo Luis.

Pero, sobre todo, me gustaría darle las gracias a esa mujer que lleva años a mi lado, mi esposa. Viendo como luchaba cada día y cada noche por lograr un sueño, sufriendo junto a mí en época de exámenes y perdiéndonos a veces muchas cosas. Ella es mi motor y por lo que hoy he terminado, gracias por estar siempre a mi lado, mi niña.

Resumen

En la actualidad, las empresas poseen grandes cantidades de servidores y aplicaciones en sus centros de procesamiento de datos (CPD). Este tipo de centros, con una gran cantidad de servidores físicos, conlleva un gran gasto en mantenimiento, energía, refrigeración y sobre todo la realización de inversiones en activos fijos, como edificios o terrenos.

Este tipo de filosofía, en la cual se tiene un servidor físico por aplicación, se está dejando atrás. Las empresas están optando por una estrategia de virtualización e implantación de la filosofía “nube” en sus centros de datos para poder reducir costes, ganando rendimiento y fiabilidad.

En este TFG se aportarán las pautas y arquitecturas necesarias para que cualquier organización pueda actualizar o migrar su CPD tradicional a un entorno “nube” completo.

A partir de la detección de debilidades de los CPD tradicionales, se ha efectuado un análisis de requisitos y diseño de una solución que cubriera cada una de estas debilidades. A continuación, se han llevado a cabo diversos estudios de mercado de los diferentes componentes necesarios para montar un entorno “nube” de tipo “on-premises”, es decir, en sus instalaciones.

La elección del proveedor para cada uno de estos componentes ha sido basada en las debilidades que se querían solventar, sus ventajas y desventajas. La propuesta de solución se ha implementado con tecnologías para la nube de SDN, SDS, Virtualización, Automatización e IA.

Abstract

Currently, companies have large number of servers and applications in their data processing centers (DPC). This type of datacenter, along with a large number of physical servers, entails a large expense in maintenance, energy, cooling and, mainly, investments in fixed assets, such as buildings or land.

This type of philosophy, in which one has a physical server per application, is being left behind. Companies are moving to a virtualization strategy and implementation of the “cloud” philosophy in their datacenters in order to reduce costs, gain performance and reliability.

In this TFG the necessary guidelines and architectures will be provided in order that any organization can update or migrate its traditional CPD to a complete “cloud” environment.

Based on the detection of weaknesses in traditional CPDs, a requirement analysis and design of a solution has been carried out in order cover each of these weaknesses. Following that, several market studies have been carried out about the different components necessary in order to set up a “cloud” environment inside its facilities. The so-called “on-premise” type.

The election of the supplier for each of these components has been based on the weaknesses to solve, advantages and disadvantages. The propose solution has been implemented with cloud technologies such as SDN, SDS, Virtualization, Automation and AI.

Índice

Índice de figuras

Capítulo 1

1.1 Justificación del TFG

Hoy en día, empresas de tamaño medio o grande poseen una gran cantidad de servidores y aplicaciones dedicados a sus trabajadores y departamentos o a sus propios clientes. Esta cantidad de servidores físicos conlleva un gran gasto en mantenimiento, instalaciones, energía, etc. También podemos destacar la poca interoperabilidad de las aplicaciones, ya que están muy ligadas a los servidores físicos.

Desde hace unos años, podemos ver como las empresas están dejando a un lado tener grandes cantidades de servidores físicos para orientar su estrategia hacia la virtualización, sobre todo hacia la "nube" consiguiendo un mejor rendimiento, ahorro en costes, instalaciones, etc.

En este proyecto vamos a partir del contexto de ser una de estas empresas que posee una gran cantidad de servidores físicos anticuados en su CPD y quiere actualizar sus instalaciones hacia la "nube", en este caso será una nube privada.

1.2 Objetivos del TFG

El objetivo de este TFG es transformar el CPD tradicional de una empresa en un CPD en entorno de nube más actualizado con todas las ventajas que esto conlleva.

Como objetivos podemos destacar:

- Diseñar una arquitectura estándar para su aplicación en la mayoría de las empresas.
- Análisis e implementación de las diferentes soluciones de virtualización.
- Análisis e implementación de diferente "software" de valor añadido para darle funcionalidad a la nube, por ejemplo: copias de seguridad, recuperación ante desastres, etc.

- Análisis de los diferentes métodos de seguridad que se pueden aplicar a la nube.
- Explicar el sistema de licenciamiento y posibles costes de la solución.
- Ventajas y desventajas de los diferentes modelos de nubes.

Como objetivos parciales del TFG podemos establecer:

- Disponer de una arquitectura estándar.
- Disponer al menos de una capa de virtualización funcional.

1.3 Enfoque y metodología seguida

Para conseguir los objetivos propuestos, se han realizado diversos estudios de mercado de las soluciones actuales que ofrecen diversos proveedores y que son necesarias para el despliegue de una nube “on-premises”. Se ha usado todos los “hands on lab” para ver las ventajas y desventajas de los productos y ver cuáles eran los más adecuados.

A partir de la detección de debilidades del sistema actual se ha hecho un análisis de requisitos y diseñado una solución acorde a ellos que cubra las necesidades existentes. La propuesta de solución se ha implementado con tecnologías para la nube de SDN, SDS, Virtualización, Automatización e IA.

1.4 Planificación del proyecto

Este trabajo comienza en el primer semestre del curso 2020-2021, el área donde se va a desarrollar es “Administración de redes y sistemas operativos”. Para la realización de este TFG se han establecido diferentes tareas a lo largo del semestre hasta alcanzar los objetivos. A continuación, se muestra una lista de tareas:

- Análisis de los modelos de nubes.
- Comparativa del “software” de virtualización.

- Análisis de las diferentes tecnologías de SDN, copias de seguridad y recuperación ante desastres.
- Diseño de la arquitectura de la nube.
- Despliegue de la solución de virtualización elegida en un entorno de laboratorio o en su defecto, probar esta solución en un entorno demo.
- Despliegue de la solución de copias de seguridad y recuperación ante desastres o en su defecto, probar esta solución en un entorno demo.
- Análisis de las diferentes técnicas de seguridad en la nube. Análisis del modelo de nube híbrida (AWS+VMware).
- Investigación sobre el futuro de la virtualización (SDDC, Self-Driving DC).
- Costes de la solución elegida.

En las siguientes imágenes podemos ver el diagrama de Gantt asociado a esta planificación:

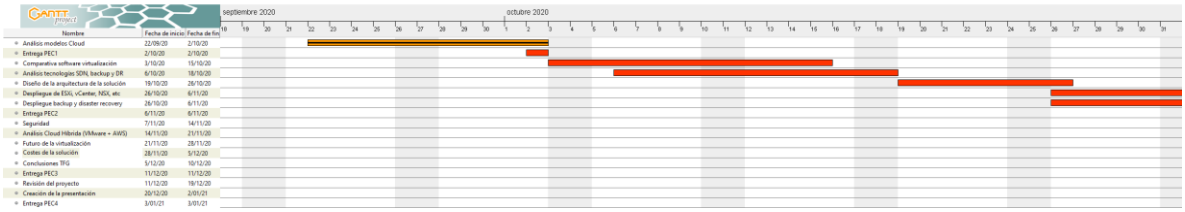

Figura 1 - Diagrama de Gantt

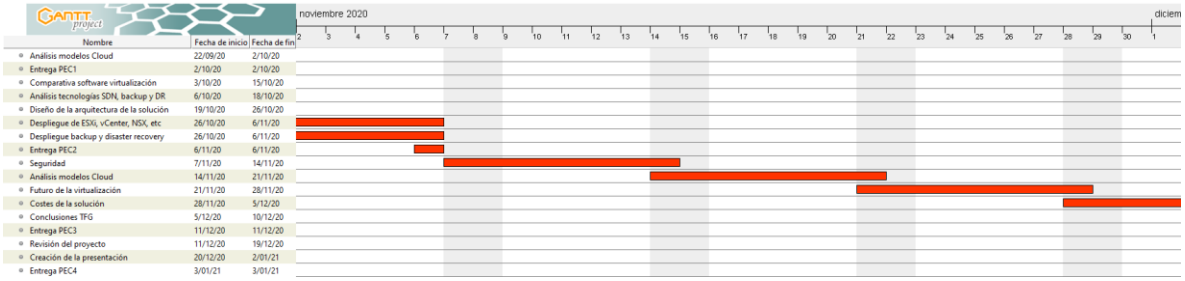

Figura 2 - Diagrama de Gantt

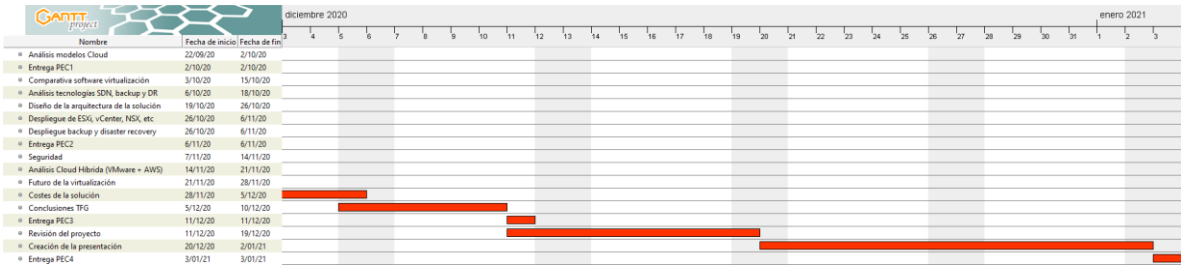

Figura 3 - Diagrama de Gantt

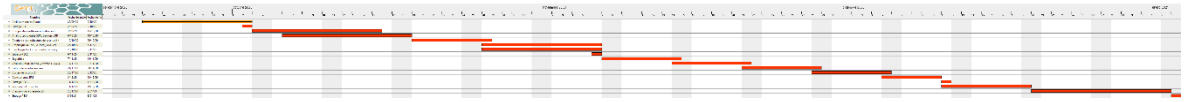

Figura 4 - Diagrama de Gantt

1.5 Productos obtenidos

La propia memoria es el producto dado que proporciona las pautas para poder realizar la implementación de una solución de nube con las últimas tecnologías del mercado en cualquier organización.

1.6 Breve descripción del resto de capítulos

En el capítulo 2 de esta memoria se hace una pequeña introducción a lo que es la nube, las tecnologías sobre las que se sustenta y se van a usar. También en el capítulo 3 se indica los problemas que se quiere resolver con este proyecto.

A continuación, en el capítulo 4 se hace un análisis de las diferentes soluciones que existen en el mercado para las tecnologías que vamos a usar para implementar la nube privada y en el capítulo 5 se muestra la arquitectura que se ha pensado para el TFG y de qué manera se usan las tecnologías elegidas en el capítulo 4.

Por último, en el capítulo 6 podemos ver las conclusiones de este trabajo.

Capítulo 2

2.1 ¿Qué es la nube?

Este concepto a veces no está claro y se suele confundir con el término virtualización. La nube no es ningún elemento físico de la infraestructura, la nube es un concepto que hace referencia a un conjunto de servidores/red/soluciones (normalmente en una ubicación remota o en un CPD) que están conectados entre sí para formar un único ecosistema.

Normalmente estos ecosistemas son escalables y nos permiten proporcionar una infraestructura donde poder usar "Cloud computing", esto lo que nos permite es ofrecer a través de la red (internet o privada) una serie de servicios como puede ser cómputo, almacenamiento, bases de datos, corta fuegos, contenedores, etc.

Actualmente, la nube o la computación en la nube se basa en cuatro pilares fundamentales. Necesitaremos montar un ecosistema basándonos en ellos para poder aprovechar todas las posibles funcionalidades:

- Virtualización.
- Redes definidas por "software" (SDN).
- Almacenamiento definido por "software" (SDS).
- Automatización.

Estos cuatro pilares son la base para la implementación de nuevas tecnologías que han surgido en los últimos años mejorando el ecosistema, ahorrando costes, etc. Estas nuevas tecnologías se comentarán a continuación.

2.2 Comparativa de modelos de nubes

Existen diferentes modelos de nube, vamos a analizar las principales diferencias entre ellos, de esta manera se podrá elegir el que mejor se adapte a nuestra empresa u objetivos.

- Nube pública: En la nube pública el “hardware”, el “software” de virtualización y la red se encuentran en un CPD/s de una empresa externa. Esta empresa ofrece estos recursos públicamente a través de internet. Cualquier persona puede contratar estos servicios ahorrándose el mantenimiento, compra y actualización del HW y la administración de toda la capa de “software” necesaria para crear la nube. En contra, tenemos que los recursos de este tipo de nube son compartidos por todos los clientes que la contraten. También la seguridad es muy cuestionada en las nubes públicas. Algunos proveedores de nubes públicas son AWS (Amazon) y Azure (Microsoft).

- Nube privada: En una nube privada, el “hardware”, la capa de virtualización y la red se encuentran en un CPD/s propiedad de la empresa, al igual que es responsabilidad de la empresa administrar y mantener esta nube, es lo que se conoce como “on-premises”. En los últimos años hay empresas que quieren montar una nube privada y no cuentan con un CPD por lo que alquilan instalaciones a terceras empresas. El alquiler de las instalaciones a una tercera empresa no significa que deje de ser una nube privada. Este tipo de nube se conoce como “privada” debido a que todos los recursos de esta son para la empresa dueña de la nube, no se comparten recursos con otras empresas como si ocurre en la nube pública. La seguridad en la nube privada es mayor.

- Nube híbrida: Este tipo de nubes se da cuando una empresa tiene una nube privada (o varias) y necesita aumentar los recursos (a veces puntualmente) de la misma, por lo que conecta su nube privada a una nube pública para aumentarlos. Un ejemplo podría ser cuando se tiene un CPD “on-presmises” y se desea un entorno de recuperación ante desastres, pero no se cuenta con otro CPD en propiedad o se prefiere tener el respaldo totalmente fuera de la infraestructura. En estos casos, se puede optar por contratar recursos en una nube pública y tener el “site” de respaldo en este tipo de nube. Una arquitectura que lo permite es VMware + AWS.

- Multiclouds: Un entorno multiclouds es aquel en el que una empresa tiene implementada dos nubes del mismo tipo, es decir, tiene dos nubes públicas o dos nubes privadas. Si tuviera una nube pública y otra privada estaríamos hablando de una nube híbrida.

2.3 Tipos de servicios en la nube

Actualmente existen diferentes servicios que se pueden ofrecer a las empresas a través de la nube o a los departamentos si la empresa cuenta con una nube privada. Estos modelos intentan satisfacer las distintas necesidades que se tengan en ella, por ejemplo, las necesidades del departamento de desarrollo no serán las mismas que las del departamento de recursos humanos.

Destacamos cuatro modelos:

- IaaS: Infraestructura como servicio. En este modelo se da acceso a los recursos de manera completa y es necesario administrar el cómputo, redes, almacenamiento, etc.
- PaaS: Plataforma como servicio. En este modelo la compañía o los departamentos no necesitan gestionar la infraestructura subyacente, por ejemplo, sistemas operativos y se centran únicamente en las aplicaciones.
- SaaS: Software como servicio. En este modelo el proveedor de nube ofrece un producto ya en funcionamiento y solo es necesario su configuración, por ejemplo, un CMS.
- Informática sin servidor: Es el modelo más reciente. En él, los desarrolladores no se preocupan de nada relacionado con la infraestructura, el proveedor de nube es capaz de ejecutar el código directamente y encargarse de provisionar y escalar la infraestructura necesaria.

Figura 5 - Modelos de computación en la nube

Fuente: https://azure.microsoft.com/es-es/overview/what-is-saas/

2.4 Hiperconvergencia vs Convergencia

La hiperconvergencia o HCI (hyper-converged infrastructure) es un tipo de arquitectura que rompe con el modelo clásico usado actualmente donde tenemos el almacenamiento, el cómputo y las redes por separado.

Como se puede ver en la siguiente imagen, la parte de la izquierda sería la arquitectura tradicional en un centro de datos, tenemos los servidores de cómputo, por un lado, las cabinas de almacenamiento por otro y un grupo de redes necesarias para establecer la conectividad entre todos los componentes y dar servicio.

Mientras que, en la parte de la derecha, tenemos lo que sería una infraestructura hiperconvergente en la cual ya no se tiene por separado el cómputo, el almacenamiento y las redes. Lo que se produce es la unión de todos estos componentes en un único servidor, todo integrado.

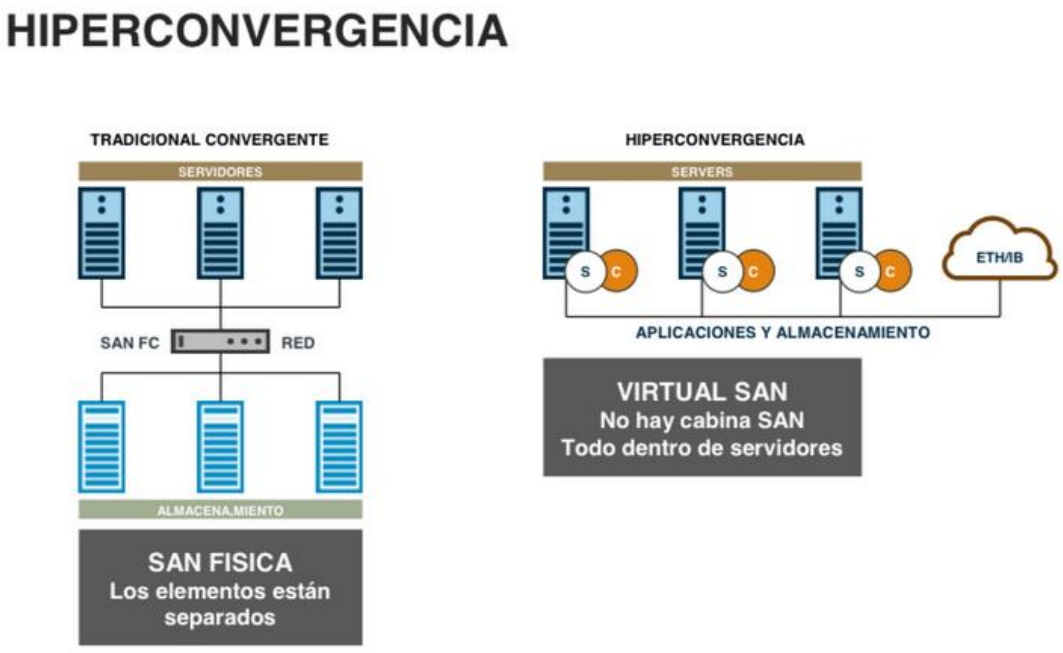

Figura 6 - Arquitectura convergente e hiperconvergente

Fuente: http://techtobase10.com/?p=457

En caso de necesitar crear una infraestructura infraestructura HCI, es necesario adquirir unos servidores certificados por el fabricante (HPE, por ejemplo) que nos garanticen que sean válidos para una infraestructura hiperconvergente. Se podría desplegar en los servidores tradicionales, pero necesitaríamos que los discos locales tuvieran la mayor capacidad posible y los servidores estuvieran provisionados con el mayor número posible de discos, sería una manera "económica" de tener una infraestructura hiperconvergente sin necesidad de servidores especiales con todo integrado. En este tipo de infraestructura, podemos tener todos los servidores de tipo HCI que deseemos, aunque tengan todos los componentes integrados se siguen tratando como servidores tradicionales.

2.5 Centro de datos definidos por software (SDDC)

Durante los dos últimos años se ha visto una tendencia por parte de las compañías que necesitaban renovar sus CPDs o montarlos de cero en adoptar SDDC como su nueva solución para la actualización de su infraestructura, aunque las primeras noticias sobre este concepto aparecían en 2012.

SDDC hace referencia a un tipo de filosofía. Es una arquitectura de cómo se debe montar un centro de datos, no es un producto como tal. En los centros de datos definidos por "software" toda la infraestructura está virtualizada, tanto los servidores, como el almacenamiento, "routers", "switchs", etc.

Normalmente este tipo de infraestructura cuenta con tres capas:

- Capa física: esta capa no la podemos virtualizar totalmente, ya que los hipervisores deben seguir apoyándose en servidores físicos para luego proveer los recursos virtualizados. La arquitectura de los servidores físicos puede estar basada en hiperconvergencia.
- Capa virtual: en esta capa tendremos las diferentes soluciones para conseguir virtualizar todos los componentes del CPD. Entre ellas habrá soluciones de SDS (Almacenamiento definido por "software") y SDN (Redes definidas por "software").
- Capa de administración: en esta última capa, encontramos las diferentes herramientas que nos permiten gestionar, automatizar y orquestar todo el CPD definido por "software".

2.6 Hipervisor

El hipervisor es el “software” de la capa de virtualización que nos permite la creación y gestión de las máquinas virtuales. Se encarga del aislamiento de cada una de ellas para que sean independientes. Es el punto de unión entre el “hardware” físico y el virtual, utiliza los recursos físicos como un conjunto y los distribuye entre las VM. El funcionamiento del hipervisor está representado en la siguiente imagen.

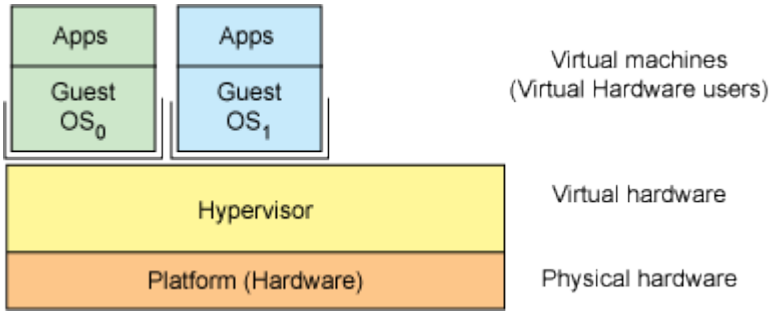

Figura 7 – Arquitectura hipervisor

Fuente: https://developer.ibm.com/technologies/linux/tutorials/l-hypervisor

2.7 Redes definidas por software (SDN)

Las redes definidas por “software” son una nueva arquitectura de red pensada para provisionar redes de manera más rápida, automatizar funciones de red y segmentar una red física en varias virtuales. De esta manera se podrán cubrir las necesidades de las aplicaciones/clientes en el menor tiempo posible.

Como ocurre en la virtualización, su objetivo es separar la administración y los recursos de los equipos físicos subyacentes. Con ello se reduce la complejidad de la infraestructura de redes tradicionales y su implementación es más sencilla.

El modo de comunicación de las aplicaciones con la red es mediante APIs y un conjunto de controladores que son el “software” de gestión de la SDN. Mediante ello, ésta se comunica y controla los recursos físicos.

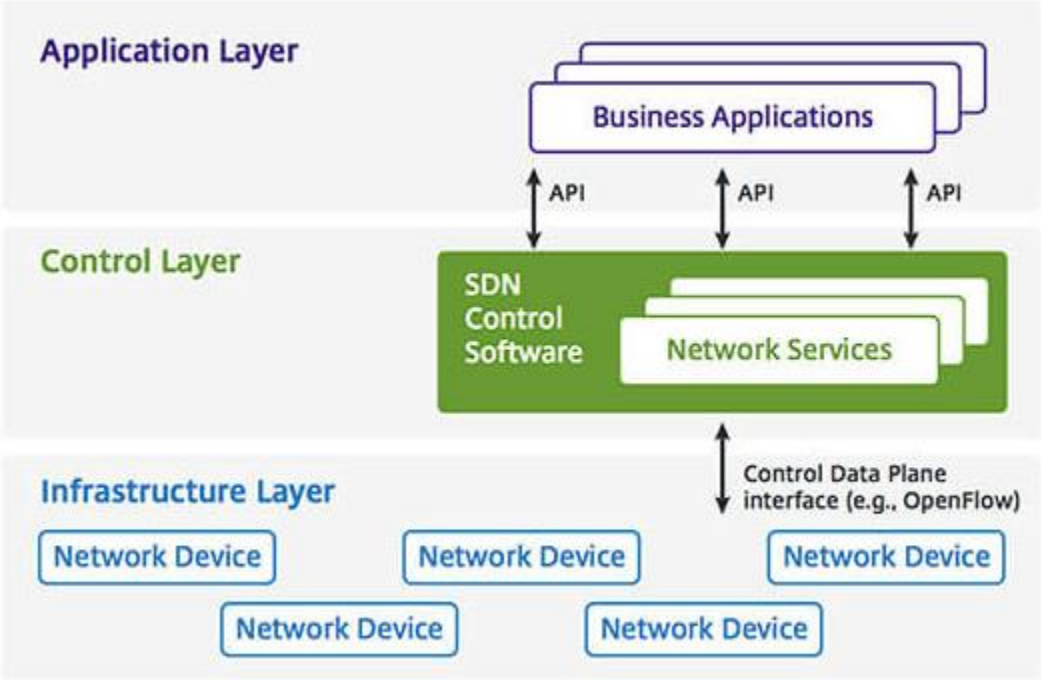

Figura 8 - Componentes SDN

Fuente: https://www.citrix.com/es-es/glossary/what-is-software-defined-networking.html

2.8 Almacenamiento definido por software (SDS)

El almacenamiento definido por “software” es una arquitectura que busca separar la gestión y distribución del almacenamiento del “hardware” físico que hay subyacente. La idea principal es la misma que en la virtualización y en la SDN.

El SDS nos proporciona una arquitectura automatizada y ágil mientras que el almacenamiento tradicional es ineficiente y se desaprovecha gran cantidad de este. Esta arquitectura está diseñada para trabajar con los estándares más comunes y se desvincula de esta manera del “hardware” propietario.

2.9 Zero trust

Una de las soluciones de seguridad más implementadas en entornos virtualizados desde hace relativamente poco tiempo es lo que se conoce como entorno “Zero Trust” o entorno de confianza cero. A lo largo del 2020 se esperaba que el 72% de

las organizaciones lo implementarán, según estudios de ESET Security. La idea de la confianza cero es que no se confía en nada ni nadie, aunque esté dentro de la red de la empresa, sea un empleado de esta o sea un flujo de comunicación necesario entre dos aplicaciones, no se da por defecto acceso al entorno. Esta idea es totalmente opuesta al modelo de seguridad perimetral actual donde la idea principal era “confía y verifica”.

La superficie de ataque actualmente es mayor que antes, ya que ahora en las empresas existen más aplicaciones, servidores, usuarios, etc. Por esta razón, es necesario limitar el acceso, otorgando únicamente los permisos que se necesita, a los puertos necesarios y “Just In Time” o justo a tiempo (es decir, en el momento de la conexión).

Con este tipo de entorno se reducen las brechas de seguridad, se ofrece más protección a la organización reduciendo la complejidad de la infraestructura, junto con una monitorización constante del entorno para hacer frente a las posibles alertas. En la siguiente imagen, podemos ver una representación gráfica de un entorno de confianza cero.

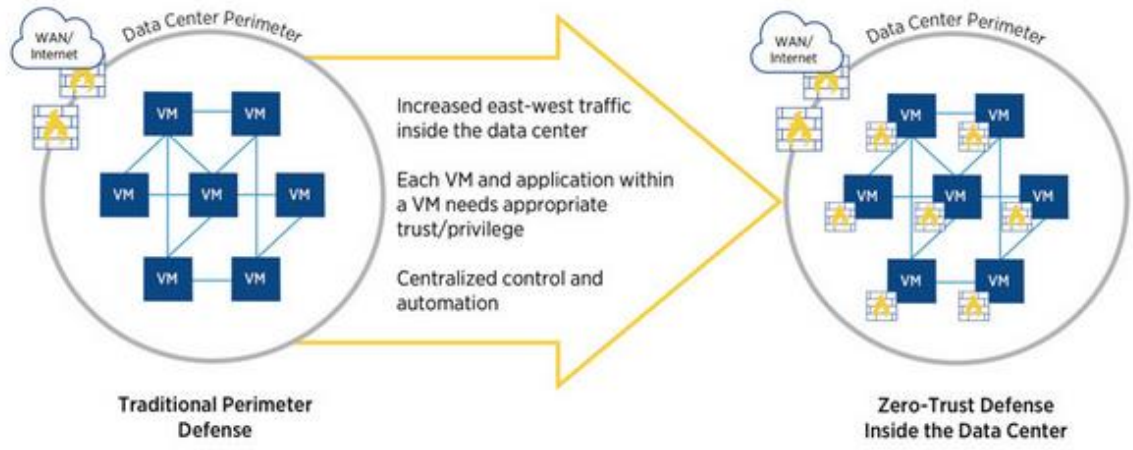

Figura 9 - Diseño Zero trust

Fuente: https://www.netronome.com/blog/zero-trust-security-for-cloud-data-centers-how-much-does-it-cost/

2.10 Sistemas de copias de seguridad

Toda empresa necesita un sistema de copias de seguridad para tener un respaldo de sus datos ante una posible pérdida de servidores físicos o virtuales, discos, ataques con “ransomware”, etc.

Uno de los fallos más comunes que cometen algunas empresas es no hacer copias de seguridad tanto de la infraestructura como de los datos (por ejemplo, bases de datos SQL). Muchas veces el motivo es la creencia de “no va a pasar nada”.

Para tener una buena política de copias de seguridad es necesario seguir la regla “3-2-1”, esta regla consiste en lo siguiente:

- Tener al menos tres copias de seguridad de los datos.
- Hay que almacenar las copias en dos soportes distintos (discos duros externos, unidades USB, etc).
- Y una de las copias se debe almacenar en un entorno externo a la empresa (puede ser una pública, por ejemplo, Azure, AWS).

Figura 10 - Regla 3-2-1

Fuente: https://www.veeam.com/blog/es/how-to-follow-the-3-2-1-backup-rule-with-veeam-backup-replication.html

Aparte de seguir la regla anterior, es necesario planificar un uso adecuado de los diferentes tipos de copia de seguridad y ejecutarlos correctamente en diferentes días para asegurar correctamente que se dispone de copia de todos los datos. Las más importantes son:

- Copia de seguridad completa: Suele usarse como la primera copia de un entorno, es la más consistente y copia todo lo que se encuentre, por ejemplo, dentro de un servidor virtual.
- Copia de seguridad incremental: Este tipo lo que realiza es únicamente la copia de aquellos ficheros que han sido modificados desde la última copia. Solo se debe usar después de realizar una copia completa.
- Copia de seguridad diferencial: A diferencia del método anterior, en este tipo se realiza una copia de todos los archivos que se han creado después de una copia de seguridad completa.

2.11 Recuperación ante desastres

La recuperación ante desastres es un proceso por el cual las empresas son capaces de recuperar sus sistemas después de la pérdida de estos y de su funcionalidad debido a un desastre (este puede ser natural, por un fallo informático, humano, etc).

La recuperación ante desastres es un punto importante en lo que se conoce como “continuidad de negocio”, esto es la capacidad de una empresa de mantener operativo los sistemas esenciales para su negocio después de un desastre o una interrupción de sus funcionalidades.

Un sistema de copias de seguridad no se puede considerar un sistema de recuperación ante desastres como tal, ya que estas nos garantizan poder recuperar los datos que se encuentran en una de las copias mientras que la recuperación ante desastres lo que proporciona es recuperar toda la operativa de la infraestructura de la empresa.

2.12 Self-Driving Data Center

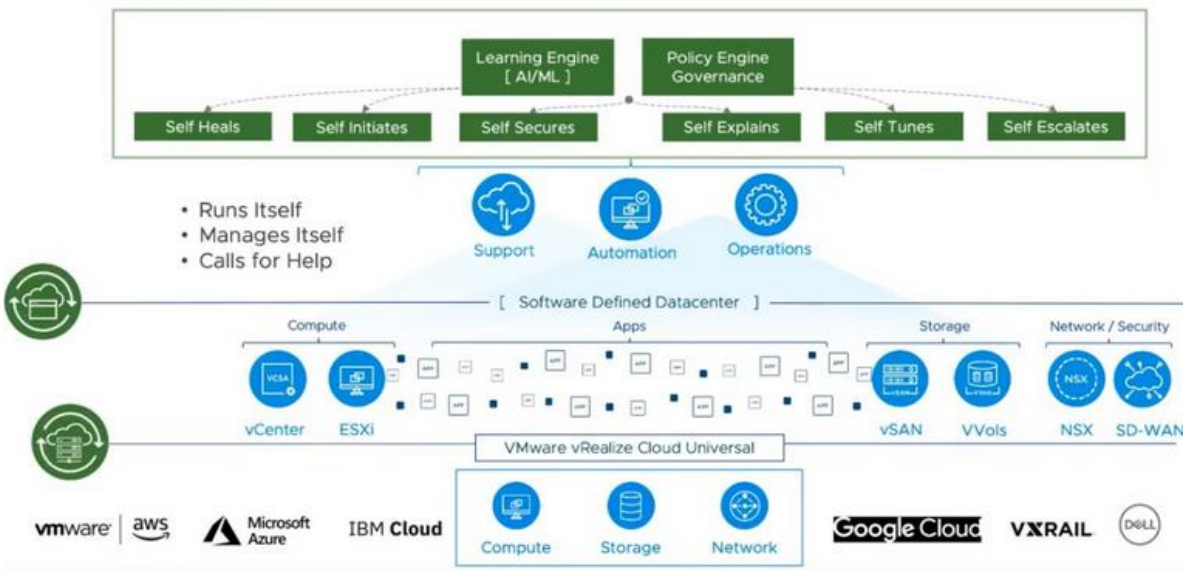

Figura 11 - Concepto Self-driving datacenter

Fuente: https://www.altaro.com/vmware/vrealize-ai-cloud/

Los centros de datos autogestionados o “Self-Driving Data Center” es un nuevo tipo de filosofía para la creación de un CPD que surge de la necesidad de negocio por parte de las empresas. Este tipo de centros se basan en la minería de datos, la inteligencia artificial, la automatización de tareas y los centros de datos definidos por “software” que se han comentado en el punto 2.5 de este capítulo. Se empieza a hablar de esta nueva “visión” en 2019.

La idea de este tipo de CPD es que no es necesaria la intervención de ningún equipo de operaciones para poder desarrollar sus tareas con éxito. Para lograr este objetivo se apoya en diferentes herramientas de IA y automatización para optimizar las operaciones y aplicar de manera proactiva cambios para eliminar problemas potenciales.

Se recopilan datos de toda la infraestructura a través de la monitorización y con un sistema de IA se analizan cada uno de ellos. Con estos análisis se determina que operaciones se deben realizar, cuando y como. Esta IA sigue creciendo según se acumulen más datos y consiga más conocimiento.

Capítulo 3

3.1 Análisis de la situación actual

Hace unos años, antes del “boom” de la virtualización, los CPD estaban formados por cientos de servidores físicos. La filosofía con la que se trabajaba antes era tener un servidor físico por aplicación, es decir, tener una base de datos en uno, el directorio activo en otro, etc.

Esta filosofía, provocaba un gran desperdicio recursos. Sobre los servidores físicos se instalaba el sistema operativo correspondiente y en él, la aplicación que finalmente se usaría. Muchas de estas aplicaciones apenas necesitaban recursos para funcionar, lo que provocaba que los recursos de los servidores físicos no se utilizaran. Esto pasaba tanto en cómputo como en almacenamiento.

Todos estos servidores estaban unidos entre sí por una compleja infraestructura de red. Según iba aumentando el tamaño del CPD era necesario hacer una mayor inversión en activos fijos (terrenos, edificios) ya que el espacio físico necesario era cada vez mayor. Pero no solo estos gastos aumentaban, también los gastos en sistemas de refrigeración y electricidad eran mayores.

Los CPD tradicionales tienen una serie de desventajas claras, se pueden destacar:

- Gran inversión de tipo “CapEx”, es decir inversiones en bienes de capital.
- Los gastos de “OpEx” son muy elevados, en otras palabras gastos operacionales.
- Complejidad de la infraestructura convergente.
- Rendimiento de aplicaciones bajo.
- Desaprovechamiento de infraestructura y recursos.
- Altos costes energéticos.

A finales de la década de 1990 nace la que es hoy en día la mayor empresa del sector de la virtualización, VMware. En los primeros años de los 2000, las empresas comienzan a virtualizar aplicaciones y parte de sus plataformas. A finales de la primera década de los 2000, la virtualización evoluciona hacia el Cloud, nacen las nubes públicas y privadas.

En la figura inferior número 12, podemos ver a la izquierda la arquitectura de un CPD tradicional sin virtualización. Observamos que cada servidor físico servía para un único propósito. Todos ellos están conectados entre sí a través de redes y a su vez unidos a las cabinas de almacenamiento.

En la parte derecha de la imagen, podemos ver la arquitectura de un CPD con virtualización. El número de servidores físicos se reduce y sobre los disponibles se instala el hipervisor que nos permitirá crear servidores virtuales y en estos instalar las aplicaciones que sean necesarias. De esta manera los recursos de los servidores físicos no se desaprovechan, ya que serán entregados a varias VM según los vayan necesitando.

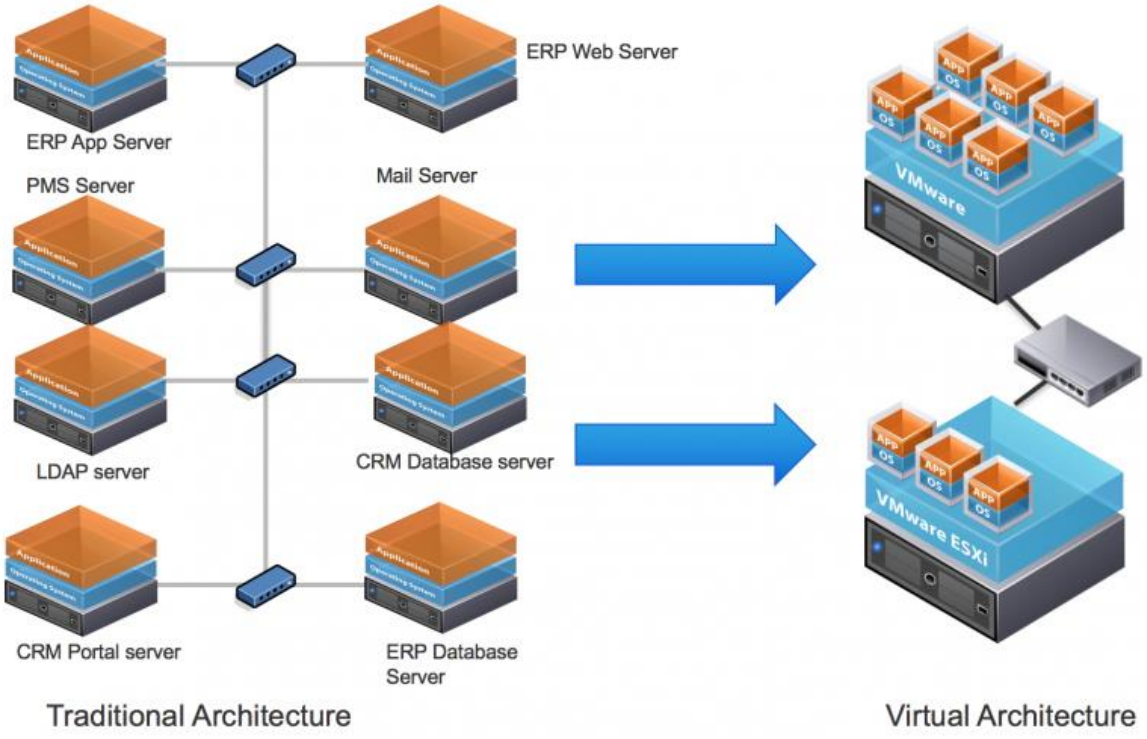

Figura 12 – CPD tradicional vs CPD virtual

Fuente: https://sajaldebnath.com/posts/vrealize-operations-manager-monitoring-vs-forensic/

Las empresas que empiezan a optar por añadir la virtualización a sus CPD e ir eliminando infraestructura física, empiezan a encontrar una serie de beneficios:

- Mayor eficiencia.
- Una reducción importante en inversión “CapEX”.
- El rendimiento de las aplicaciones aumenta.
- La complejidad de la infraestructura baja.
- Reducción del número de servidores físicos y necesidad de menos espacio en el CPD.
- Mejora de los tiempos de entrega de recursos para proyectos.
- Menor gasto energético y de refrigeración.

Aunque la virtualización se generaliza a principios de los años 2000, no es una tecnología “moderna”. Los primeros estudios sobre la virtualización se remontan a la década de 1960 en los laboratorios de investigación de IBM. El sistema operativo CP/CMS de IBM fue el pionero en permitir la definición del concepto VM.

Hoy en día, la tecnología de virtualización y su filosofía se ha aplicado a diferentes componentes de la infraestructura de los CPD. Por ejemplo, actualmente tenemos tecnologías como SDN que son redes definidas por “software” o SDS que es almacenamiento definido por “software”.

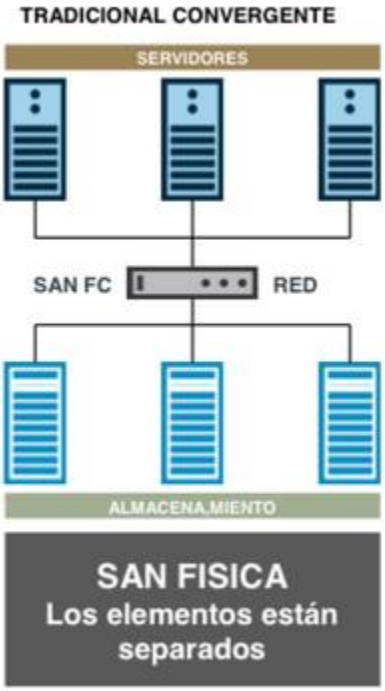

Figura 13 - Arquitectura CPD componentes separados

Fuente: http://techtobase10.com/?p=457

También, las arquitecturas de los CPD han cambiado. En los CPD de hace unos años y de la década pasada, aunque usaran la virtualización para la reducción de servidores físicos, siguen usando una arquitectura en la cual los componentes de cómputo, almacenamiento y redes están separados. Todo ello conllevaba una complejidad y unos costes asociados mayores. Podemos ver un ejemplo de esta arquitectura en la figura 13. Actualmente, existen arquitecturas hiperconvergentes, como la mostrada en la figura 14.

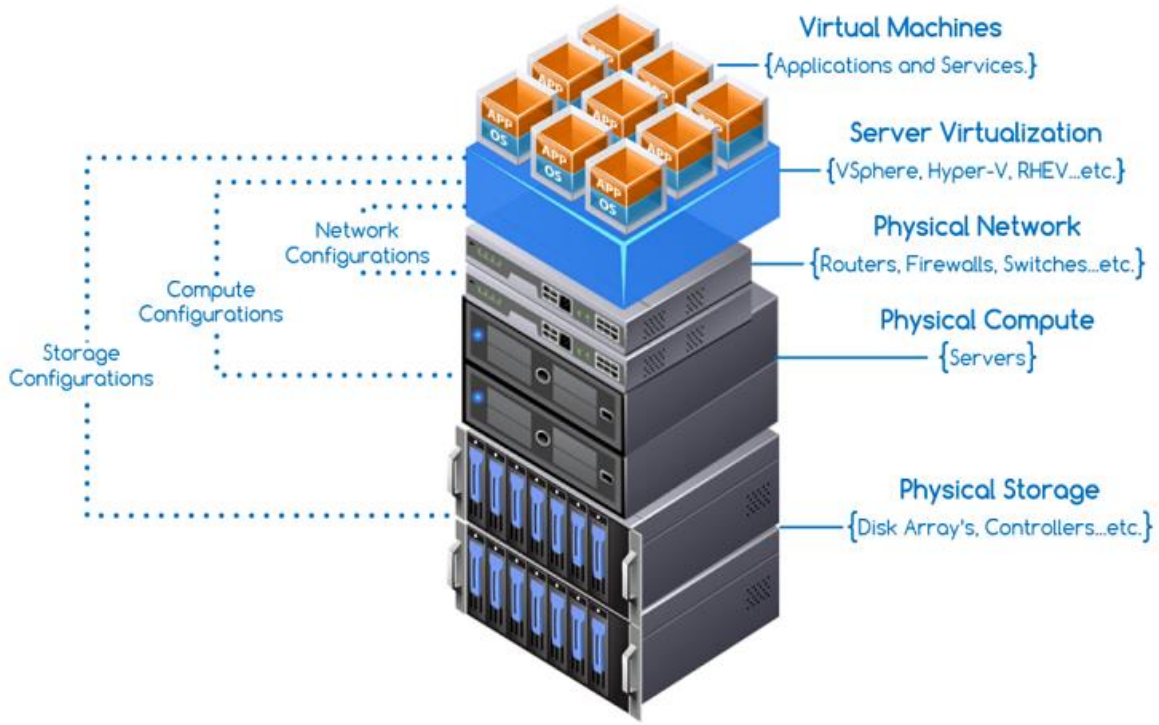

Figura 14 - Esquema de una arquitectura HCI

Fuente: https://www.itnext.in/article/2019/02/14/sublime-architecture-hyper-converged-infrastructure

Por otro lado, los CPD, aunque estén usando virtualización y no sean cien por cien tradicionales, no se les puede considerar entornos “Cloud”. La virtualización es uno de los pilares de esta filosofía y ayudó a su evolución. Pero para poder tener un entorno que se pueda considerar “Cloud” hay que montar sobre la infraestructura una serie de componentes y adoptar una filosofía. No es válido únicamente con la virtualización.

3.2 Propuesta

El objetivo de este proyecto es ofrecer unas pautas y una guía a fin de que sea posible la realización de la implementación de una solución de nube con las últimas tecnologías del mercado en cualquier organización. Estas pautas se podrán usar en aquellas empresas que sigan teniendo un entorno CPD tradicional o un CPD virtualizado pero anticuado. Con ello se consigue darles soporte de una migración a un entorno nube que cumpla todas sus necesidades y proporcionándolas un ahorro en costes junto con mejoras en rendimiento.

Capítulo 4

4.1 Elección del modelo de nube

En el capítulo 3 se ha visto las diferentes debilidades que tienen los CPD tradicionales o los CPD únicamente virtualizados que se han quedado obsoletos. Ambos CPD tienen una serie de limitaciones, gastos elevados y un rendimiento muy bajo.

El objetivo es proporcionar una guía para la migración de estos CPD a un entorno "Cloud" donde los problemas y limitaciones mencionados anteriormente queden mitigados o eliminados. Los diferentes modelos de nube están detallados en el punto 2.2 del capítulo 2. En ese apartado se destaca la existencia principalmente de cuatro modelos posibles, que son: nube pública, privada, híbrida y multiclouds.

La mejor opción para solventar todas estas limitaciones y satisfacer los requisitos de las organizaciones es el modelo de nube privada. Este modelo tiene muchas ventajas, cumple con todos los requisitos necesarios y se resuelven los problemas de las arquitecturas anteriores. Algunas características del modelo de nube privada son:

- Posee todas las ventajas de la nube pública.
- Tienen una gran fiabilidad.
- Son escalables.
- Autoservicio.
- La seguridad en ellas es mayor que en las nubes públicas.
- Los datos de la empresa estarán alojados en sus propios servidores y no en servidores compartidos.
- Recursos dedicados y no compartidos.
- Control total de la nube y toma de decisiones.
- Gastos "CapEx" y "OpEX" equilibrados.
- Reducción del espacio físico necesario.
- La complejidad del entorno es menor.
- Aprovechamiento de todos los recursos disponibles.
- Hiperconvergencia (opcional).

Este tipo de nube también tiene algunas desventajas, las cuales no son complicadas de solucionar. Podemos destacar como inconvenientes:

- Se usa un software de virtualización de un proveedor en concreto para toda la infraestructura. Esto puede llevar a un tipo de dependencia hacia ese proveedor y si se quiere cambiar de capa de virtualización, puede requerir muchos esfuerzos para hacerlo.

- Para montar una infraestructura como una nube privada, es recomendable que todos los elementos que la formen sean lo más similares posibles. Por ejemplo, si tenemos dos proveedores diferentes de elementos de red, esto añadirá una complejidad innecesaria en el entorno cuando se instale la infraestructura, actualizarla, etc. Incluso este tipo de complejidad puede afectar al rendimiento de la nube.

A continuación, en los siguientes apartados de este capítulo se realizará un análisis de mercado de los diferentes componentes que se necesitan para montar una nube privada. En el último apartado, se podrá ver las tecnologías elegidas para el proyecto.

4.2 Análisis de las diferentes soluciones de virtualización

Actualmente en el mercado existen diferentes proveedores de soluciones para virtualización (hipervisores). La virtualización es uno de los pilares básicos para implementar la infraestructura necesaria para la nube privada, vamos a realizar un análisis de las soluciones más usadas por las empresas.

Lo que se busca con este análisis, es poder elegir el hipervisor que vamos a usar en nuestra nube privada. Las soluciones que vamos a analizar son las más usadas por el mercado, como podemos ver en la gráfica siguiente, las más usadas son vSphere, Hyper-V y Citrix.

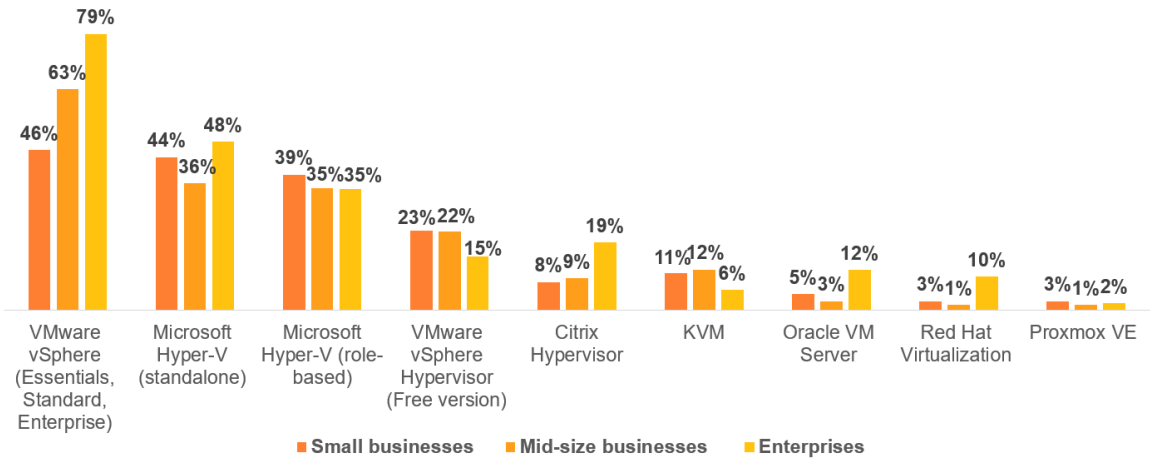

Figura 15 - Cuota de mercado de hipervisores

Fuente: https://www.spiceworks.com/marketing/reports/state-of-virtualization/

4.2.1 vSphere

Esta solución de virtualización es propiedad de la empresa VMware. Como podemos ver en la gráfica anterior, esta solución es la líder en el mercado y sus productos llevan años de desarrollo (desde 2001), por lo que nos ofrece una garantía de que son productos estables y preparados para dar un gran rendimiento.

Las máquinas virtuales que se virtualizan en este entorno tienen un rendimiento igual y a veces superior al rendimiento que podría ofrecer esta máquina en un hardware nativo.

vSphere cuenta con las tecnologías “Virtual Symmetric Multiprocessing” y “hardware virtual” lo que nos permite crear máquinas virtuales con hasta 128 CPUs y 6 TB de RAM respectivamente. Son máquinas pensadas para alto rendimiento. En la última versión se admite memoria persistente y arquitectura NUMA.

La capa de virtualización de VMware también nos ofrece diferentes servicios que para una nube son esenciales, destacar:

- Modificación de los recursos de una VM (CPU y RAM) en caliente, sin tener que apagarla.
- Función vMotion: nos da la posibilidad de hacer migraciones en caliente de VM entre diferentes “hosts”.
- Función Storage vMotion: permite la migración en caliente de VM entre diferentes almacenes de datos.
- Alta disponibilidad: en caso de fallo de “hardware” o de sistema operativo, podremos reiniciar todas las aplicaciones de forma automatizada.
- vCenter: Nos da una gestión en un único punto de toda la infraestructura virtualizada.
- Aplicación VUM (vSphere Update Manager): Permite las actualizaciones y parcheados de la infraestructura virtualizada de manera sencilla y centralizada.

La capa de vSphere también nos facilita la integración de otros productos de VMware que nos daría una funcionalidad completa de la nube. Otros productos de VMware que se podrían agregar a la solución para tener funcionalidad completa:

- VMware NSX.
- VMware vRealize Operations.
- VMware Site Recovery Manager.
- VMware vSAN.

Los productos de VMware son bajo licenciamiento, por lo que necesitaremos adquirir aquellas que sean necesarias para la infraestructura que se implemente. Los productos base de la nube que la necesitan son:

- ESXi: la licencia determina que funcionalidad puede llegar a tener el entorno. Los sistemas de DRS, vMotion, etc dependen de esta licencia, hay varios tipos de licencia para ESXi. El ESXi se licencia por CPU física.
- vCenter: hay dos tipos de licencias, una limita la gestión del vCenter a 4ESXi, la otra es ilimitada.

Como punto negativo a VMware, podemos destacar que es obligatorio contratar al menos durante un año un soporte por cada una de las licencias anteriores.

4.2.2 Hyper-V

Este producto de virtualización es una solución de la empresa Microsoft lanzada al mercado en 2008. Es la segunda solución más usada por empresas para virtualizar su infraestructura. Está considerado un hipervisor de tipo uno.

Podemos destacar varias características de este producto como, por ejemplo:

- Las VM están muy optimizadas gracias a los servicios y controladores llamados “Integration Services”.
- Migraciones entre “hosts” y sistemas de almacenamiento en caliente.
- Portabilidad de las VM gracias a sus sistemas de importación/exportación.
- Copia de seguridad basadas en el servicio VSS (Servicio de instantáneas de volumen).
- Recuperación ante desastres con un sistema de copias de máquinas virtuales, las cuales se almacenan en otras ubicaciones físicas. Se conoce como réplica de Hyper-V.
- Cada máquina virtual de Hyper-V es un entorno aislado con las mismas características que un equipo físico.

Al igual que vSphere, en la última versión de Hyper-V se admite memoria persistente y arquitectura NUMA. Microsoft todavía no tiene una solución definitiva para el almacenamiento definido por software, al contrario que VMware con vSAN que es actualmente la más adoptada.

Históricamente, Hyper-V no contaba con un sistema de gestión centralizada de la arquitectura virtual, VMware por su parte tenía el producto vCenter para gestionar toda la plataforma. Microsoft ha lanzado ahora “Windows Admin Center” que es una solución web para la administración de la plataforma, pero todavía no es una solución asentada, cada cierto tiempo se lanzan actualizaciones para darle más funcionalidad.

Hyper-V no es un software de virtualización tan asentado como vSphere, no ofrece todavía soluciones de SDN y de seguridad que se puedan integrar con facilidad. vSphere permite de serie usar VSS (vSphere Standard Switch) para redes virtuales. Con VMware NSX la funcionalidad aumenta todavía más.

Otra desventaja clara de Hyper-V con otros productos de virtualización, es que está muy orientado a la virtualización de máquinas Windows. Es posible virtualizar sistemas operativos Linux/Unix, pero no están soportadas todas las distribuciones al igual que otros SO que directamente no están soportados. Es muy limitado si se compara con VMware.

En el caso del licenciamiento en Hyper-V, necesitaremos una licencia “Windows Server 2019 Datacenter” por cada “host” en el cual queramos hacer una instalación física de Hyper-V. Con esta misma licencia se nos permite hacer tantas instalaciones virtuales como queramos dentro de ese “host”.

4.2.3 Citrix hypervisor

Citrix hypervisor es el producto de virtualización de la empresa Citrix, este producto cambió de nombre recientemente, antes era XenServer. Citrix adquirió en 2008 el hipervisor Xen y lo usó de base para la creación de su propia solución.

Las máquinas virtuales sobre este hipervisor tienen un rendimiento casi como si estuvieran en un hardware nativo. Esto es debido a que se usa paravirtualización que ayuda a tener pocas penalizaciones en rendimiento.

El problema de este producto son las limitaciones que tiene si se compara con otras tecnologías, por ejemplo, en las máquinas virtuales. En la última versión de citrix las máquinas virtuales no pueden tener más de 32 CPU y 1,5 TB de RAM, incluso también tiene limitaciones en el tamaño de los discos de las VM, en este caso limitado a 2TB.

Citrix al igual que VMware, tienen una herramienta de gestión de la plataforma muy potente y madura, en este caso se llama XenCenter y permite administrar toda la infraestructura virtual creada con Citrix Hypervisor. Nos permite desplegar, administrar, monitorizar todas las máquinas que se tengan.

El licenciamiento de citrix es muy complejo, ya que existen varios tipos de licencias, a destacar: usuario/dispositivo, optimización, simultáneas, usuario, dispositivo, de sockets, con nombre de usuario.

4.3 Análisis de las diferentes soluciones de copia de seguridad

Existen varias soluciones de copias de seguridad para entornos virtualizados y físicos. Podemos destacar:

- Veeam Backup.
- Avamar Dell EMC.
- vSphere Data Protection.

Por parte de VMware estaba basada en Dell EMC y su solución de copias de seguridad dejará de existir en las próximas versiones de vSphere. El mercado se queda con dos grandes competidores que son Veeam y Avamar. Existen grandes diferencias entre estas dos soluciones. A destacar las siguiente:

- Dell EMC obliga a una dependencia total del proveedor, se debe usar “hardware” patentado por Dell. Por el contrario, Veeam es compatible con diferentes versiones de “hardware” y de diferentes proveedores.
- Veeam ofrece una arquitectura más simple e integrada, en cambio Avamar necesita más del doble de recursos en comparación.
- Dell EMC todavía no ofrece las mismas funcionalidades que Veeam, incluso algunas de ellas están integradas en su solución desde hace varios años.
- Veeam en una misma solución nos ofrece aparte de copias de seguridad, solución de recuperación ante desastres, “snapshots”, recuperación, entorno de desarrollo y pruebas.
- El coste de la solución Dell EMC es mayor que Veeam, ya que este último permite la elección del “hardware” que mejor se adapte a la infraestructura y ser de bajo precio.

4.4 Análisis de las diferentes soluciones de recuperación ante desastres

En este tipo de sistemas (DRaaS – Recuperación ante desastres como servicio) podemos adoptar dos posibles modelos, el primero es mover todos los sistemas esenciales de la empresa a otro CPD de nuestra propiedad o, por el contrario, mover los sistemas a un proveedor de "Cloud" pública como puede ser AWS, Azure…

En la elección de una solución DRaaS hay que tener muy en cuenta dos parámetros, ya que estos dos determinarán que "software" de recuperación ante desastres se debe elegir, estos son:

- RPO – "Recovery Point Objective": Se puede definir como la cantidad de datos que una compañía puede perder sin que afecte a su negocio durante un tiempo de inactividad provocado por un desastre. Esto es debido a que el último punto de réplica del DRaaS puede estar unas horas atrás del momento en el que ocurrió el desastre.

- RTO – "Recovery Time Objective": Se puede definir como el tiempo necesario que la empresa va a tardar en recuperar sus sistemas debido a un desastre.

En la siguiente imagen se muestra de forma gráfica estas definiciones (el tiempo que aparece en la imagen es solo un ejemplo).

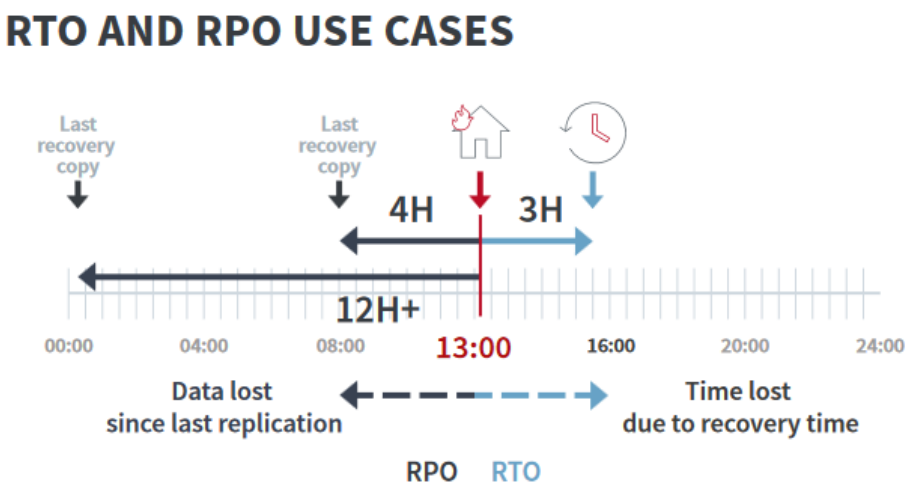

Figura 16 - Conceptos RTO y RPO

Fuente: https://www.zerto.com/wp-content/uploads/2017/03/The-Disaster-Recovery-Guide-by-Zerto.pdf

Podemos destacar dos soluciones de “software” de recuperación ante desastres, estas son:

- VMware vSphere Replication.
- Zerto Virtual Replication.

Son dos soluciones totalmente diferentes para el mismo fin. Tienen varios detalles importantes que les diferencian, podemos destacar:

- Zerto puede funcionar con cualquier tipo de infraestructura, grande o pequeña, crítica o no. Mientras que vSphere Replication solo está recomendaba para infraestructuras de tamaño pequeño y que no sean críticas.
- El RPO de Zerto es de segundos, mientras que el de vSphere Replication es mínimo de 15 minutos hasta 24 horas.
- Zerto permite de manera automática hacer conmutación por error al otro sitio de respaldo cuando el principal ha sufrido un desastre y vuelta atrás. Por el contrario, vSphere Replication no está preparado y necesita de un software adicional de VMware para poder llevarlo a cabo, lo que provoca tener que comprar otra licencia aparte y más infraestructura (VMware SRM).

4.5 Análisis de las diferentes soluciones de almacenamiento definido por software (SDS)

Actualmente la solución de SDS más usada en los entornos virtualizados es vSAN, ya que este producto se integra perfectamente con todos los demás componentes de VMware. Con ello, conseguimos la capa necesaria para la virtualización del almacenamiento, esta nueva capa permite gestionar el cómputo y el almacenamiento como si fuese una única plataforma ya que se integra junto con vSphere. Con vSAN conseguiremos una infraestructura HCI.

Existen otros proveedores de soluciones HCI que incluyen SDS. A diferencia de usar vSAN, estas nos obligan a usar su paquete de componentes predefinidos. Algunas soluciones de este tipo son:

- Nutanix.
- HPE SimpliVity.
- NetApp HCI.

Si se opta por una solución totalmente integrada de un único proveedor para la solución HCI de la empresa, existe una desventaja para este tipo de arquitectura, que es la dependencia total de un único proveedor.

Si este proveedor no cumple las expectativas, tiene un soporte inexistente o de mala calidad, la empresa tendrá un problema. Por el contrario, la solución de VMware es independiente del "hardware" subyacente y no hay dependencia de un único proveedor.

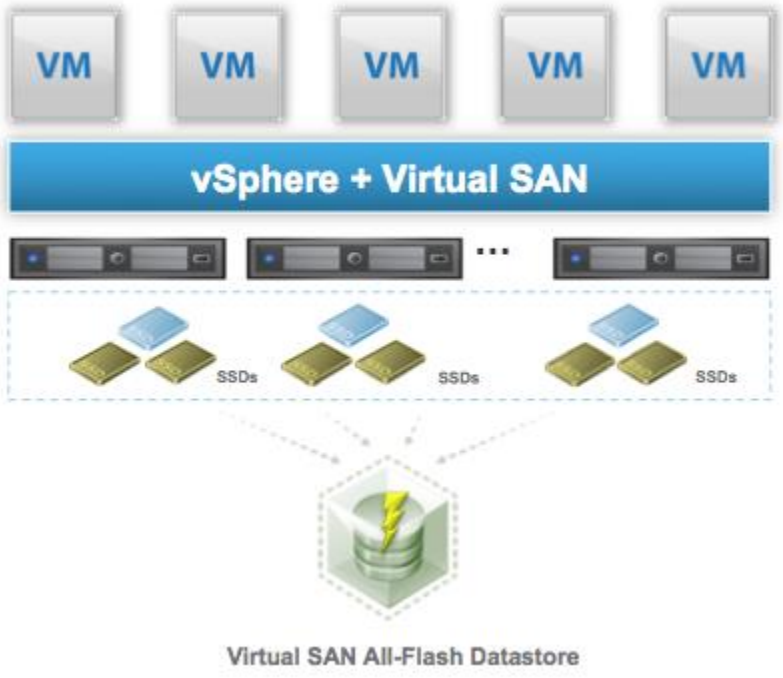

Figura 17 - vSphere y vSAN

Fuente: https://blogs.vmware.com/virtualblocks/2015/02/02/vmware-virtual-san-6-0/

En la imagen superior, podemos ver una solución de arquitectura HCI usando este producto. Esta solución va integrada con el hipervisor (ESXi) por lo que no es necesario usar un "software" aparte de otro proveedor. El almacenamiento que se encuentra dentro de cada servidor (ya no está separado en cabinas) se comparte

entre todos los servidores (nodos) de tipo HCI que tengamos en el CPD y se crea una red de almacenamiento en la cual recaen las máquinas virtuales, aplicaciones, contenedores que virtualicemos.

Con vSAN se nos facilita el escalado de la infraestructura dependiendo de si las necesidades han aumentado:

- Si se necesita escalar en memoria o en disco, se puede realizar un escalado vertical, añadiendo más memoria y disco a un nodo.
- Si, por el contrario, se necesita más cómputo, se puede realizar un escalado horizontal añadiendo otro nodo, de esta manera no solo se crece en cómputo, sino también en memoria y disco. También aporta más alta disponibilidad, cuantos más nodos haya más se consigue.

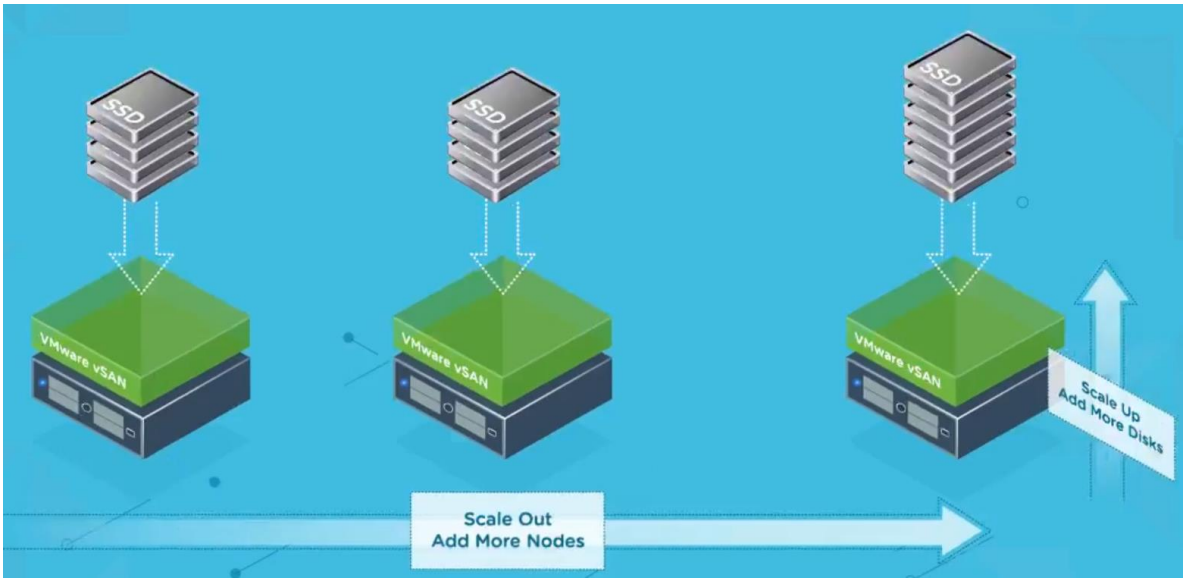

Figura 18 - Tipos de escalado HCI

Fuente: https://www.vmware.com/es/products/vsan.html

Usar vSAN y conseguir una arquitectura HCI tiene una serie de ventajas sobre una arquitectura tradicional (también conocida como arquitectura de tres niveles), se puede destacar:

- Reducción de un conocimiento especialista por unos más generalista en los equipos de operaciones.
- El “Capital expenditure” se reduce ya que no es necesario hacer una inversión en redes de comunicación entre los elementos.
- Escalabilidad en toda la infraestructura.
- Se consigue una alta disponibilidad mayor.
- También se obtiene una mayor automatización.
- La provisión de nuevos recursos se reduce a pocas horas. Por ejemplo, si se tiene un nuevo proyecto y no hay recursos para hacerle frente, en pocas horas se podrá.

4.6 Análisis de las diferentes soluciones de redes definidas por software (SDN)

Las redes definidas por “software” llevan unos años ya en el mercado y existen tecnologías muy consolidadas. Compararemos cuatro de ellas ya que son las principales compañías del sector:

- Cisco: Para su implementación necesita una nueva capa con tres componentes diferentes, añadiendo complejidad al entorno. Su punto fuerte es que facilita la integración de IBN (Intent-Based Networking). La tecnologías IBN permite establecer políticas de uso para redes, a diferencia de la tecnología SDN que únicamente se centra en la automatización y provisión de las redes. Con IBN se garantiza también automatizar las tareas administrativas que haya en la red, son redes autogestionadas con IA y ML.

- Nokia: Nuage es el producto de SDN que nos ofrece esta compañía. Con el podemos definir redes de extremo a extremo, totalmente automatizado y es una solución compatible con entornos híbridos, no depende de un único proveedor de “hardware”.

- NSX: es la solución para SDN de VMware. El punto fuerte contra sus competidores es que no necesita “hardware” físico adicional para poder realizar la virtualización de la red al contrario que sus competidores, toda la infraestructura se puede virtualizar, no necesita tener “routers” o “switches” físicos unidos a su capa de virtualización. Integración completa con vSphere.

4.7 Seguridad

4.7.1 Zero trust

Para poder realizar la implementación de una arquitectura de confianza cero, necesitamos un proveedor que nos pueda facilitar “firewalls” distribuidos, escalables y que nos permitan controlar el tráfico este-oeste en la red. En el mercado existen grandes compañías de redes que ofrecen esta solución, podríamos destacar:

- Cisco: Nos ofrece su solución DUO para entornos de confianza cero. Con ella se puede securizar los accesos remotos, resoluciones DNS, aplicaciones en la nube.

- VMware: Con su solución NSX nos proporciona sistemas de “firewalls” virtuales distribuidos. Estos nos permiten establecer diferentes reglas para proteger toda la infraestructura, no solo los accesos o aplicaciones, si no también departamentos, usuarios, etc. Podemos tener una segmentación total de la red desde una única pantalla y totalmente integrado con el resto de los componentes que se tengan de la misma empresa. Esto conlleva una gran ventaja ya que no añade más complejidad al entorno ni más capas.

A continuación, se puede ver una lista de ataques que se pueden detener con mayor facilidad usando un entorno de confianza cero:

- “Phishing” a través de correos electrónicos.
- Contraseñas robadas.
- Filtraciones en bases de datos.
- Intentos de accesos no autorizados.
- “Keyloggers” en los equipos de los trabajadores.
- Tráfico este-oeste dentro de la red de la empresa.

4.7.2 MFA

MFA o Autenticación multifactor, es otra de las medidas de seguridad que más se está implementando en los últimos años, ya que las contraseñas de los usuarios pueden no ser del todo seguras y ser objetivo de ataques. Con un sistema MFA lo que se consigue son métodos complementarios de verificación de identidad.

Cuando un usuario inicia sesión en una aplicación, por ejemplo, el correo electrónico, aparte de introducir su contraseña se le pedirá a este usuario que introduzca otra forma de autenticación. Este método adicional de autenticación puede ser un sms a su teléfono móvil, un código de seguridad variable, un "token" físico o incluso su huella dactilar.

De esta manera, se aumenta la seguridad ya que, en este caso, si la contraseña es débil o se ha visto comprometida, con un segundo método de identificación podremos conseguir verificar que es un acceso legítimo a la organización.

Existen diversas empresas que ofrecen servicios de MFA, las más conocidos son:

- Microsoft Azure MFA.
- MFA RSA.

La solución de Microsoft permite a la organización elegir diversos métodos secundarios de autenticación, como pueden ser:

- Uso de la aplicación "Microsoft Authenticator" para móviles.
- Token físico OATH.
- SMS.
- Llamada de voz.

En la siguiente imagen se puede ver el funcionamiento del sistema MFA ofrecido por Microsoft en su nube pública Azure.

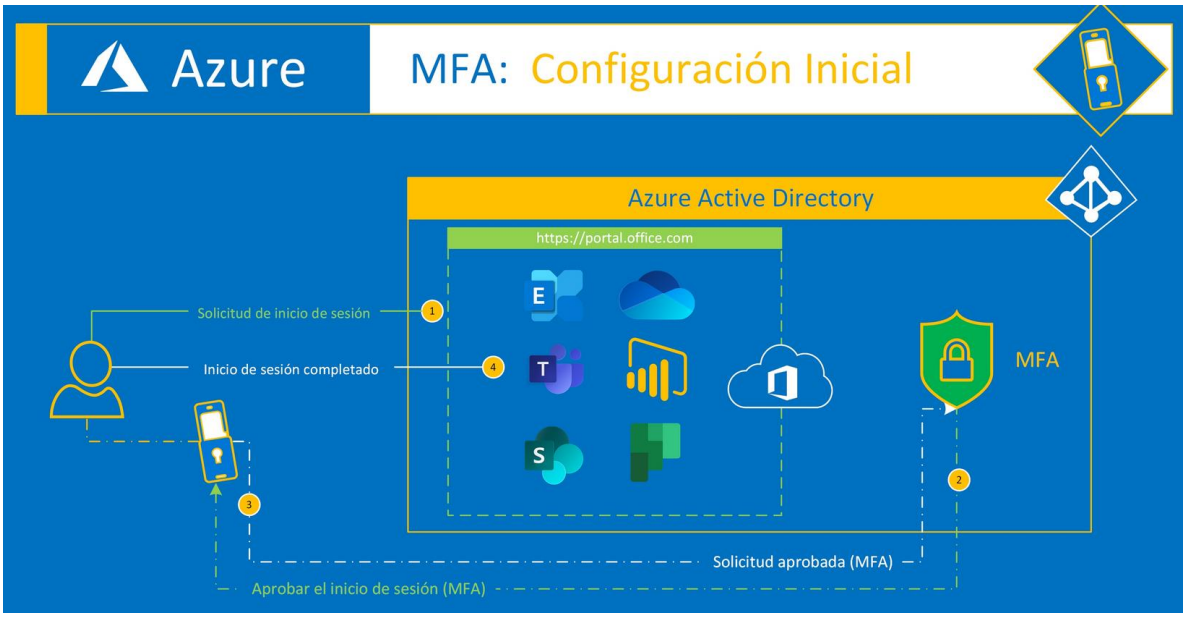

Figura 19 - Funcionamiento MFA

Fuente: https://www.santiagobuitragoreis.com/azure-configuracion-inicial-de-autenticacion-multifactor-mfa/

4.8 vRealize AI

El proyecto Magna de VMware o vRealize AI (normbre comercial) es el primer proyecto por parte de VMware de aterrizar en el mundo empresarial los “Self-Driving Data Center” basándose en un SDDC y añadiendo una nueva capa a través de un nuevo producto (vRealize AI).

No existe actualmente ninguna otra solución como esta, por lo que no podemos hacer una comparativa de mercado. VMware ha creado una solución SaaS con recolección de datos y aprendizaje a través de ellos. De esta manera se toman decisiones de manera automática para ajustar la infraestructura, mejorar el rendimiento y la eficiencia.

Para conseguir esto, la nueva capa de VMware usa inteligencia artificial (IA) y aprendizaje automático (“Machile learning” o ML). El ML utiliza diferentes redes neuronales para ofrecer a la IA toda la información posible, luego la IA toma la mejor decisión basándose en toda la información que le ha sido proporcionada.

Utiliza tres métodos de análisis de datos para conseguir un mayor aprendizaje:

- Análisis descriptivo: Con este análisis se busca lo que ha sucedido.
- Análisis predictivo: Con este otro tipo de análisis se busca pronosticar o predecir lo que puede ocurrir.
- Análisis prescriptivo: En este punto se utilizan miles de algoritmos para conseguir la mejor configuración posible.

En la siguiente imagen podemos ver una arquitectura de alto nivel de los diferentes productos necesarios para iniciar el despliegue:

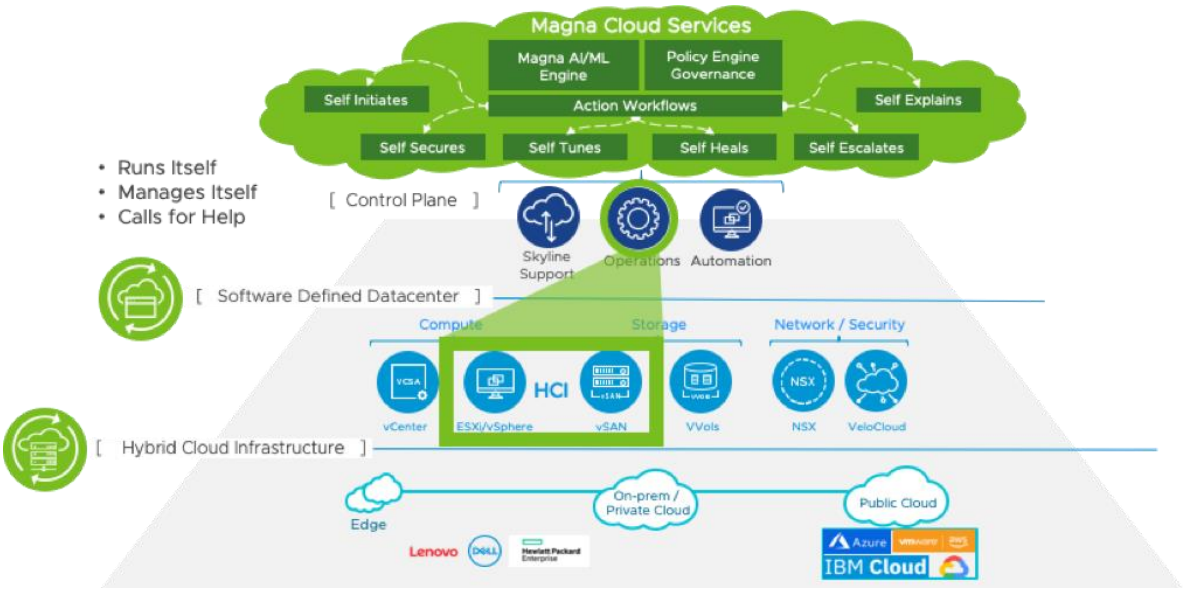

Figura 20 - Arquitectura servicios Magna

Fuente: https://blogs.vmware.com/management/2019/08/tech-preview-project-magna.html

Como se puede ver en la imagen superior, en color verde está la nueva capa de "Magna" o "vRealize AI". El "core" de este nuevo producto es el "Magna AI/ML engine" que es el que se encarga de hacer todas las tareas por sí mismo sin intervención humana. Se autogestiona, realiza los cambios de configuración necesarios y se preocupa de que el rendimiento no baje de ciertos valores establecidos.

Ventajas que ofrece el proyecto Magna:

- Los gastos "CapEx" y "OpEx" se reducen.
- Mejora un 60% el rendimiento de toda la infraestructura.
- Reduce la monitorización a quince minutos al día.

- El número de tiques por fallos baja hasta cinco al mes.
- Apenas existen incidencias.

4.9 Elección de las tecnologías para la implementación

En este punto, a modo resumen se indican las diferentes tecnologías que se han elegido después del análisis de mercado y el motivo de su elección:

Virtualización	VMware vSphere
Copias de seguridad	Veeam Backup
Solución ante desastres	Zerto Virtual Replication
SDN	NSX de VMware
SDS	vSAN de VMware
Self-Driving DataCenter	vRealize AI
Seguridad	Zona de confianza cero

El “software” de virtualización elegido ha sido “VMware vSphere”. Se ha decidido usar este producto por los años que lleva de desarrollo aportando gran estabilidad y rendimiento. Ofrece una integración perfecta con el resto de los componentes de la nube y en el mismo paquete de producto se ofrecen diversos servicios esenciales sin necesitar otros componentes adicionales.

Con relación a las copias de seguridad, se ha decidido usar el producto que ofrece Veeam. Ofrece una serie de servicios y características que sus competidores no. Podemos destacar su arquitectura simple e integrada, su bajo coste y la independencia total del proveedor, ya que no obliga a usar “hardware” patentado por ellos mismos.

La compañía Zerto ofrece un “software” de recuperación ante desastres muy completa y con un gran rendimiento. Ha sido elegida la solución que más se adapta a las necesidades de este proyecto. Podemos destacar su bajo RPO y posibilidad de trabajar con cualquier tipo de infraestructura, al contrario que sus competidores.

Como soluciones de SDN y SDS se ha optado por usar los productos de VMware. Para SDN se ha decidido usar NSX ya que su integración con la capa de vSphere es completa y no necesita de “hardware” físico para poder realizar la virtualización de la capa de red a diferencia de sus competidores. Para SDS se ha elegido vSAN ya que aporta una serie de características que no ofrecen sus competidores en HCI. Por ejemplo independencia total del proveedor, reducción del “Capital expenditure”, escalabilidad de toda la plataforma, alta disponibilidad, provisión de recursos en pocas horas.

Actualmente, para la implementación de un “Self-Driving DataCenter” no existe en el mercado más soluciones que la presentada por VMware. Por lo que su elección la basamos en dos razones, la primera es la completa integración con la capa vSphere y la segunda es que no hay competidores ahora mismo en el mercado.

Para la implementación de la arquitectura de cero confianza se usarán los “firewalls” distribuidos que nos proporciona NSX. De esta manera no será necesario adquirir un “software” adicional para implementar esta medida de seguridad y aumentar los costes de la solución.

Capítulo 5

5.1 Arquitectura del diseño

A continuación, se presenta un diagrama con el diseño de la arquitectura que se ha realizado con las tecnologías elegidas en el capítulo anterior. Se ha creado una arquitectura lo más universal posible para que pueda ser adoptada por cualquier empresa. No es una arquitectura estática y puede crecer dependiendo de las necesidades. En los siguientes subapartados, se realiza la explicación correspondiente al diseño, el motivo de cada componente, etc.

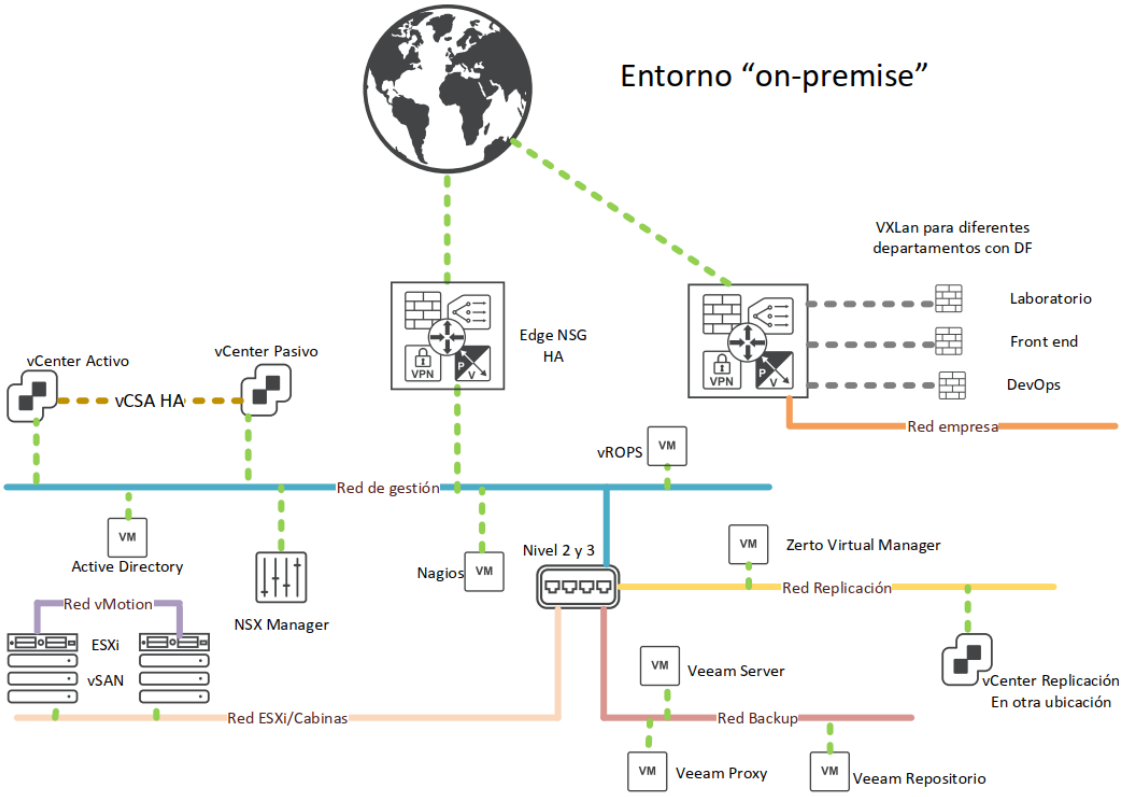

Figura 21 - Arquitectura del diseño

Fuente: Propia

5.2 ESXi

Como se ha comentado en capítulos anteriores, el hipervisor es el “software” que nos proporcionará la capa necesaria para realizar la virtualización. Se ha escogido usar los productos de VMware por lo tanto nuestro hipervisor será el ESXi.

En esta arquitectura tenemos una red exclusiva para los servidores físicos en los cuales vamos a instalar la capa de virtualización. Entre los servidores físicos habrá una red especial para el servicio de “vMotion”. Este servicio permite mover máquinas virtuales en caliente de un servidor a otro y nos proporciona balanceos de carga entre servidores para no saturarlos.

Aunque en el diagrama anterior solo se hayan indicado dos servidores ESXi, la arquitectura permite tener todos los servidores que se consideren necesarios para soportar la carga de trabajo. Estos servidores pueden ser HPE Proliant, DELL PowerEdge, etc.

En este mismo diagrama, podemos ver debajo de los ESXi el dibujo de lo que sería el almacenamiento. El uso de vSAN para el SDS nos ofrece una arquitectura HCI. Se ha optado por no usar las soluciones integradas de proveedores de HCI ya que esto provoca dependencia de ellos. Por el contrario, se ha optado por usar servidores “normales” pero con la capacidad de almacenamiento al máximo.

Una vez que la capa de virtualización está instalada en los servidores físicos, se puede proceder al despliegue del “software” de gestión que proporciona VMware, que es el vCenter. Desde esta capa podremos administrar los ESXi, crear “clusters”, habilitar la alta disponibilidad, etc.

5.3 VCSA HA

Las siglas VCSA significan “vCenter Server Appliance”. El vCenter nos proporciona una capa de gestión donde podremos administrar con facilidad los servidores físicos (ESXi), el almacenamiento de toda la infraestructura, las redes virtuales, la alta disponibilidad, control de usuarios que pueden acceder a la plataforma, etc.

Se ha decidido implementar el vCenter en formato HA (alta disponibilidad) ya que es una parte fundamental de la infraestructura, ya que, si no se puede acceder a este componente, se pierde todas las funcionalidades comentadas en el párrafo anterior. Para implementar la alta disponibilidad, se tienen dos vCenters conectados entre ellos y si el servidor activo deja de dar servicio correctamente, cogería las funciones el otro vCenter que está en modo pasivo/espera.

En las versiones más antiguas este “software” iba instalado en una máquina Windows como un servicio adicional. Este método ya está obsoleto y no recibe soporte ni mantenimiento por parte del fabricante. En las últimas versiones de vSphere ya se instala en formato “Appliance”, esto es un sistema en el cual el fabricante ofrece el “software” embebido dentro de una máquina virtual sin que sea necesario hacer grandes configuraciones, una vez que se ha desplegado esta máquina virtual, el vCenter ya está listo para funcionar. VMware con ello busca rebajar la dificultad de despliegue de sus productos.

En el siguiente diagrama se puede ver la representación del VCSA en modo HA, ambos vCenters están conectados a través de una red dedicada. Hay un tercer componente en este diagrama, el “witness” se encarga de ver si el servidor activo sigue disponible o no para pasar el control al pasivo.

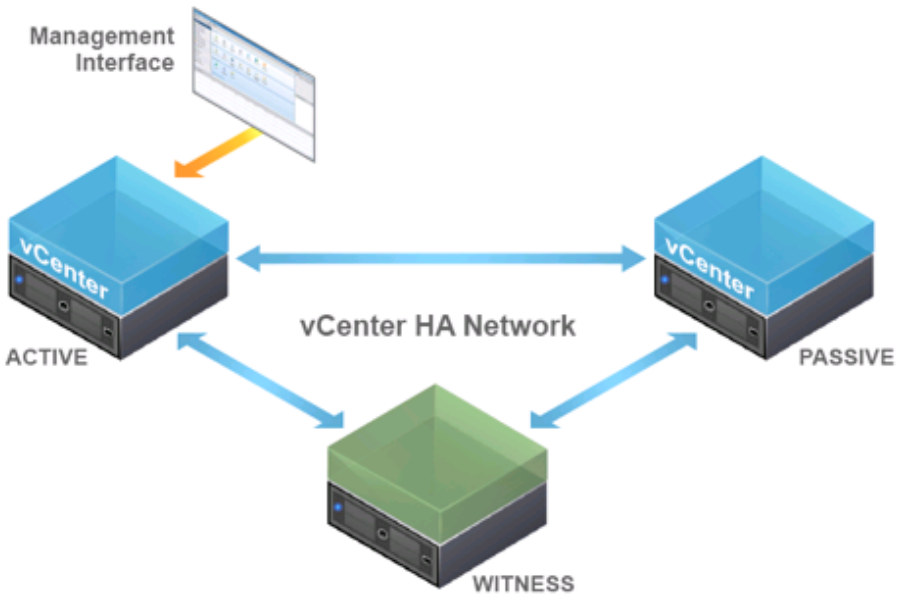

Figura 22 - Arquitectura vCenter HA

Fuente: Proceso de instalación VMware

5.4 NSX

La solución elegida para las redes definidas por software ha sido el producto NSX de VMware, ya que nos proporcionará una amplia gama de servicios y su integración con la capa de vSphere es completa.

Es necesario desplegar un nuevo componente en la plataforma llamado “NSX Manager”, el cual lo conectaremos contra el VCSA. Una vez realizada la conexión entre ambos, en la interfaz de vCenter se podrá gestionar todos los servicios que proporciona NSX. En esta solución, los servicios que se van a usar serán: Edge, cortafuegos, VPN, cortafuegos distribuido y VXLAN.

5.5 Edge ESG

Como podemos ver, en la parte superior de la arquitectura se han creado dos “Edge ESG”, esto es gracias al producto VMware NSX. Este tipo de componente nos brinda todos los servicios disponibles por parte de NSX, es decir, este componente es capaz de actuar como cortafuegos, VPN, balanceador de carga, DHCP y NAT.

En nuestra arquitectura, va a funcionar principalmente como cortafuegos y como VPN. Se han creado dos “Edge” distintos para tener dos VPN diferentes, una será para los administradores de la infraestructura y otra para los trabajadores de los distintos departamentos de la empresa. De esta manera, cuando se esté teletrabajando, los empleados podrán acceder a los recursos como si estuvieran en la oficina.

Si por el contrario no se está teletrabajando y se está en las oficinas conectados a la “Red empresa”, los trabajadores de los departamentos tendrán acceso directo a sus máquinas/recursos/laboratorios virtualizados gracias a que la “Red empresa” está conectada al “Edge” de recursos el cual tiene conectadas todas las VXLAN. Cada departamento tendrá una VXLAN exclusiva con un direccionamiento propio, si un departamento necesita conectarse contra algún servicio de otro departamento, este mismo “Edge” hará de enlace entre las distintas redes.

Para dotar de una mayor seguridad al entorno, gracias a este “Edge” de recursos, se ha creado una arquitectura “zero trust” con el servicio de “firewall” distribuido que nos proporciona NSX. No se confía en ninguna conexión interna. Con el “firewall” distribuido se aplican distintas reglas a cada VXLAN y solo se permiten conexiones desde alguna IP específica que necesite ir a otra red y a un puerto en concreto, no está el tráfico abierto por defecto de manera interna.

El “Edge” de gestión, únicamente está conectado contra la red de gestión de la plataforma, de esta manera aislamos la infraestructura del resto de redes de la empresa. Si los administradores (por ejemplo, un departamento de sistemas) necesita conectarse a la infraestructura, es obligatorio conectarse mediante la VPN de gestión. Aunque se esté en las instalaciones de la empresa, no se facilitará acceso directo a la infraestructura. Ambas acciones son buenas prácticas de seguridad.

5.6 Nagios

En los entornos productivos es necesario monitorizar la plataforma para poder actuar antes de que se produzca una caída del servicio. Esto podría afectar a nuestros clientes o incluso detener el trabajo en la empresa.

Con un servicio de monitorización podemos establecer comprobaciones contra un conjunto de máquinas y ver en un panel un resumen del estado de estas. Normalmente se revisan aquellas que son imprescindibles para mantener funcionando la plataforma o el servicio.

Hay diversos tipos de comprobaciones y alertas, las cuales las podemos establecer para que nos avise si ocurre un evento en las máquinas o si sobrepasa un umbral de uso. Esta serie de monitorización se puede configurar para que nos avise por correo, sms, etc. Por ejemplo, es normal establecer alertas para el uso de memoria de las máquinas, estableciendo límites al 70% de uso y al 90%, en el primer caso sería un aviso, en el segundo caso sería una alarma crítica.

Los equipos de sistemas de las empresas suelen ser los encargados de revisar estas alertas cuando llegan avisos de alarmas críticas. En esta arquitectura hemos decidido instalar el “software” Nagios para que realice la monitorización del sistema.

Se ha decidido usar este producto ya que es totalmente compatible con productos VMware y la personalización de las alarmas es completa.

5.7 Zerto

Ante una caída total del CPD donde se encuentra la infraestructura principal, la solución de recuperación ante desastres nos permitirá mover las máquinas necesarias al CPD de respaldo.

Para ello se ha creado una VLAN específica para que vaya este tráfico al respaldo. En esta red específica también se desplegará la solución de Zerto. Esta solución puede crecer según las necesidades de la empresa. En el caso de la arquitectura de este documento, únicamente se van a desplegar dos ZVM (Zerto Virtual Manager) ya que se necesita uno por vCenter.

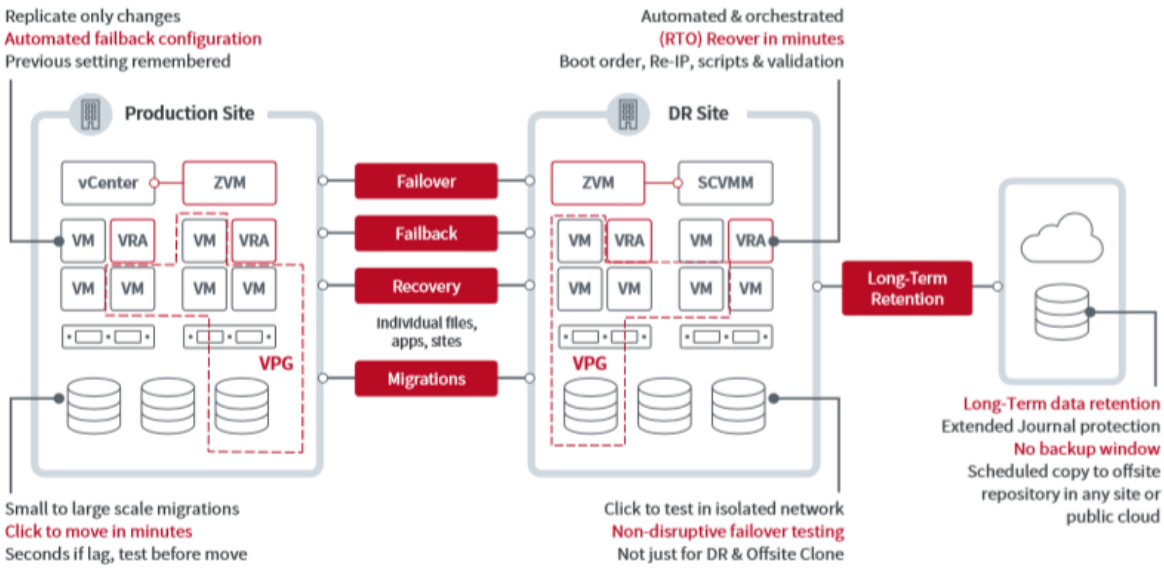

Figura 23 - Arquitectura Zerto

Fuente: https://www.zerto.com/wp-content/uploads/2017/03/The-Disaster-Recovery-Guide-by-Zerto.pdf

El ZVM es un “software” que se instala dentro de una máquina Windows Server. Una vez instalado, ofrecerá una interfaz web donde se podrá administrar y configurar el producto con nuestras necesidades.

5.8 VCSA Replicación

En el diagrama de la arquitectura podemos ver que en la red de replicación tenemos otro vCenter llamado “vCenter de replicación”. Aunque no se ha dibujado en el diagrama, este tiene también sus propios ESXi, cabinas de almacenamiento, etc.

Su función es administrar aquellas máquinas virtuales que se migren dentro de sus ESXi. En caso de desastre del vCenter principal, la migración de las máquinas se haría con la solución anterior de recuperación ante desastres. Normalmente está vacío y no tiene ninguna máquina que administrar, únicamente está en modo pasivo esperando.

Para que la infraestructura siga funcionando correctamente una vez que se migran las máquinas en caso de desastre, este vCenter debe tener las mismas características que el principal. Sobre todo, los mismos recursos para poder soportar la misma carga de máquinas virtuales. De igual manera, debe tener acceso a las mismas redes, la misma capacidad, de almacenamiento, etc.

Este sitio de respaldo no debe encontrarse en el mismo lugar que el sitio principal, ya que si se sufre un desastre le afectaría de la misma manera. Por este motivo, lo normal es tener el respaldo en otro CPD de la organización. Si no se dispone de él, mínimamente el respaldo debería estar en otra sala del CPD que se disponga. El usar otra sala en el mismo CPD conlleva una limitación importante en caso de desastre. Si solo falla una sala del CPD esto cubriría el problema, pero no lo haría en caso de que el desastre afectara a todo el centro de datos.

Por este motivo, muchas organizaciones que no disponen de otro centro de datos para poder respaldar su infraestructura deciden implementar el respaldo en una nube pública, por lo que pasamos a tener lo que se denomina nube híbrida. En este caso, la arquitectura de la nube privada no sufre cambios, solo que la red de replicación se conecta directamente a una nube pública (AWS, Azure…) y en esta es donde se encuentra el vCenter de respaldo con los ESXi, la solución de Zerto, etc.

En nuestro caso, al elegir Zerto la conexión con la nube pública estaría garantizada y la configuración no es diferente a la que se tuviese que realizar en un centro de datos propio. En la siguiente imagen podemos ver una arquitectura de Zerto entre una nube “On-Premises” y una nube pública.

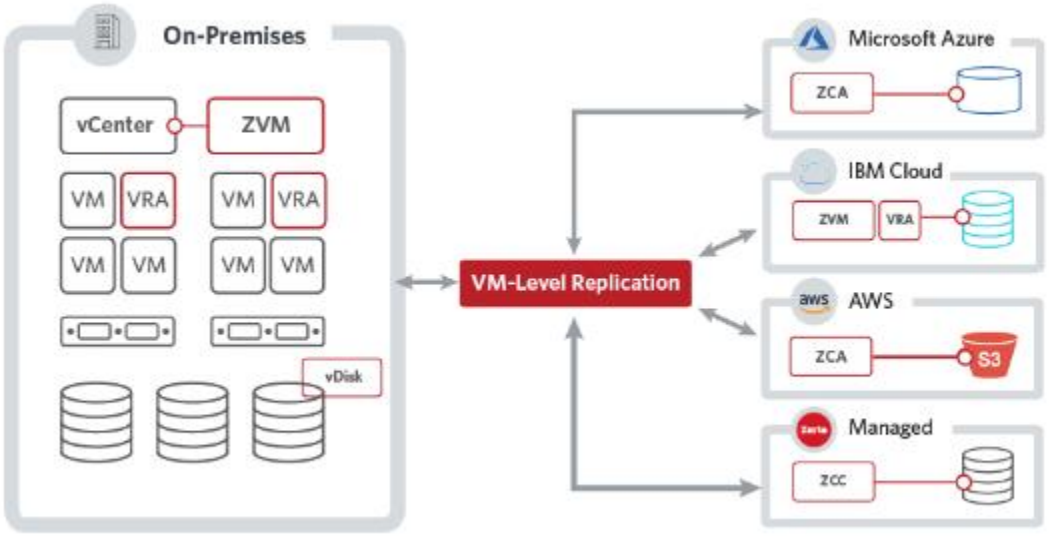

Figura 24 - Replicación cloud híbrida

Fuente: https://www.zerto.com/wp-content/uploads/2018/02/IS-08599_ZVR6.0_Overview_DS.pdf

5.9 Veeam Backup

El sistema de copias de seguridad de nuestra solución estará basado en el “software” de la compañía Veeam. Como se puede ver en la figura 18 “Arquitectura del diseño”, se ha decidido aislar el sistema de copias de seguridad del resto de componentes en una red propia para este fin. De esta manera, aislamos el tráfico exclusivamente de copias de seguridad y no sobrecargamos otras redes de la plataforma.

La solución de Veeam es muy completa y tiene muchísimas funcionalidades. En este caso vamos a montar la infraestructura mínima para su correcto funcionamiento. Mínimo es necesario montar el Veeam Server, Veeam Proxy y Veeam Repositorio. A continuación, se explica el rol de cada uno de estos componentes.

- Veeam Server: Es una máquina física o puede ser virtual. Es necesario que el sistema operativo de la máquina sea Windows y en ella se instalará el "software" de "Veeam Backup & Replication". Es el componente central de toda la infraestructura de copias de seguridad y su rol es ser el centro de configuración y control. Controla la ejecución de las copias y asigna los recursos necesarios. En una instalación mínima, podríamos incluso usar esta misma máquina como "proxy" y repositorio, pero podría ser demasiada carga para una única máquina, por ese motivo, lo separamos.

- Veeam Proxy: Se encarga de procesar las tareas y entregar el tráfico de la copia de seguridad que se esté realizando. Es un componente de la arquitectura que se encuentra entre el Veeam Server y el resto de los componentes que tengamos en la infraestructura. Realiza diferentes tareas necesarias para realizar el "backup". Podemos destacar el recuperar los datos de las máquinas virtuales que se están haciendo copias de seguridad, comprimir, deduplicación y cifrado de las copias. Por último, también se encarga de enviar las copias de seguridad al repositorio.

- Veeam Repositorio: Es un almacenamiento donde se van a almacenar los archivos de las copias de seguridad. Se pueden usar diferentes tipos de almacenamiento, por ejemplo, SMB, NFS o almacenamiento directamente conectado a un servidor Windows o Linux.

5.10 Directorio Activo

El directorio activo es un servicio de directorio que proporciona Microsoft y se puede instalar en servidores Windows. Es una estructura jerárquica que almacena usuarios, equipos, políticas de seguridad, elementos de red, etc. De esta manera nos permite gestionar todos estos objetos desde un único punto.

Para empresas de tamaño medio-grande una de sus mayores utilidades es centralizar el inicio de sesión con una política de usuarios y contraseñas por departamentos y grupos con ciertos permisos, de esta manera se aumenta la seguridad de la organización.

5.11 vRealize AI

Para poder usar vRealize AI, hay que desplegar su producto “core” que es “vRealize Operations” ya que uno se integra dentro del otro para su activación y ver de manera visual el impacto de las mejoras que se han implementado en el sistema. En la figura 18 “Arquitectura del diseño”, podemos ver que lo hemos configurado en la red de gestión.

Este producto se encarga de la gestión de las operaciones de TI en una única plataforma usando la AI. Entendiendo por estas operaciones, la estrategia conjunta sobre tecnología de una empresa para mantener los servicios 24x7x365. Con este producto podemos ver toda nuestra infraestructura desde un único punto, tanto la infraestructura física o virtual. Además, aunque no quisiéramos utilizarlo con el proyecto Magna, por si solo nos proporciona una optimización continua del rendimiento de la plataforma, análisis de los costes y posibles mejoras y corrección de errores.

Actualmente, vRealize AI se encuentra en una fase muy temprana de desarrollo y únicamente está disponible para mejoras en la infraestructura y rendimiento de vSAN. Su modo de funcionamiento en esta fase es que una vez que se ha activado, se analiza la infraestructura y se conecta con los servicios en la nube del proyecto Magna enviando ciertas métricas (anónimas) sobre el rendimiento que está teniendo vSAN en nuestra empresa. Una vez que tiene estos datos los compara con el resto de datos y el promedio de rendimiento de vSAN de todas las compañías que usan vRealize AI. Recordemos que toda esta información es tratada de manera anónima.

El motor de AI/ML que tiene el proyecto Manga en la nube indicará si el rendimiento de la infraestructura está en la media, por encima o si por el contrario tenemos un rendimiento por debajo del resto. Si el rendimiento es inferior, los servicios de Magna usarán vROps parar mostrar cómo era el rendimiento anterior a su activación y como es su rendimiento ahora en forma de gráficos y datos amigables. Se podrá observar cómo los KPI mejoran, cualquier mejora la infraestructura siempre vendrá indicada por el motor AI/ML que hay en los servicios en la nube y que no tenemos en nuestra infraestructura.

De la misma manera, se han establecido ciertos mecanismos para que nunca empeore el rendimiento usando vRealiza AI, por lo que si lo activamos será siempre

para mejorar el rendimiento, nunca perjudicará al sistema. En las fases de desarrollo siguientes se espera que se integre con más productos de la pila de VMware, como por ejemplo “Skyline” y con su integración con vRealiza AI se busca que esta cree y escale los casos de soporte automáticamente con el equipo técnico de soporte de VMware al encontrar cualquier fallo en el sistema.

También se busca su integración con la base de conocimiento de VMware, lo que se conoce públicamente como casos de KB. Esta integración todavía está muy lejos, pero la idea es que, al integrarlo con la base de conocimiento, si se publica un nuevo fallo conocido por VMware y su solución en forma de KB que esta se aplique automáticamente en la infraestructura una vez que se conozca.

En las dos siguientes imágenes, se muestra cómo sería el proceso de activación.

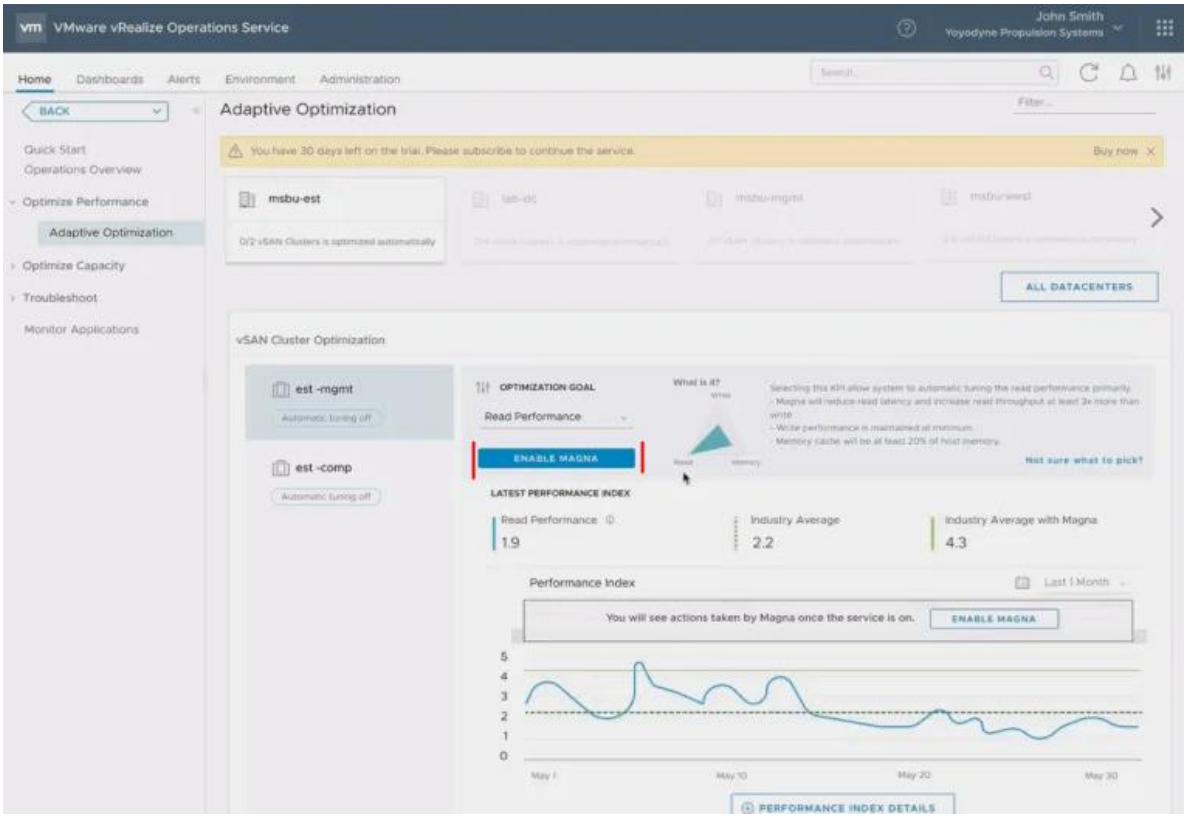

Figura 25 - Activación vRealize AI

Fuente: https://cormachogan.com/2019/09/02/introducing-project-magna-artificial-intelligence-and-machine-learning-for-vsphere/

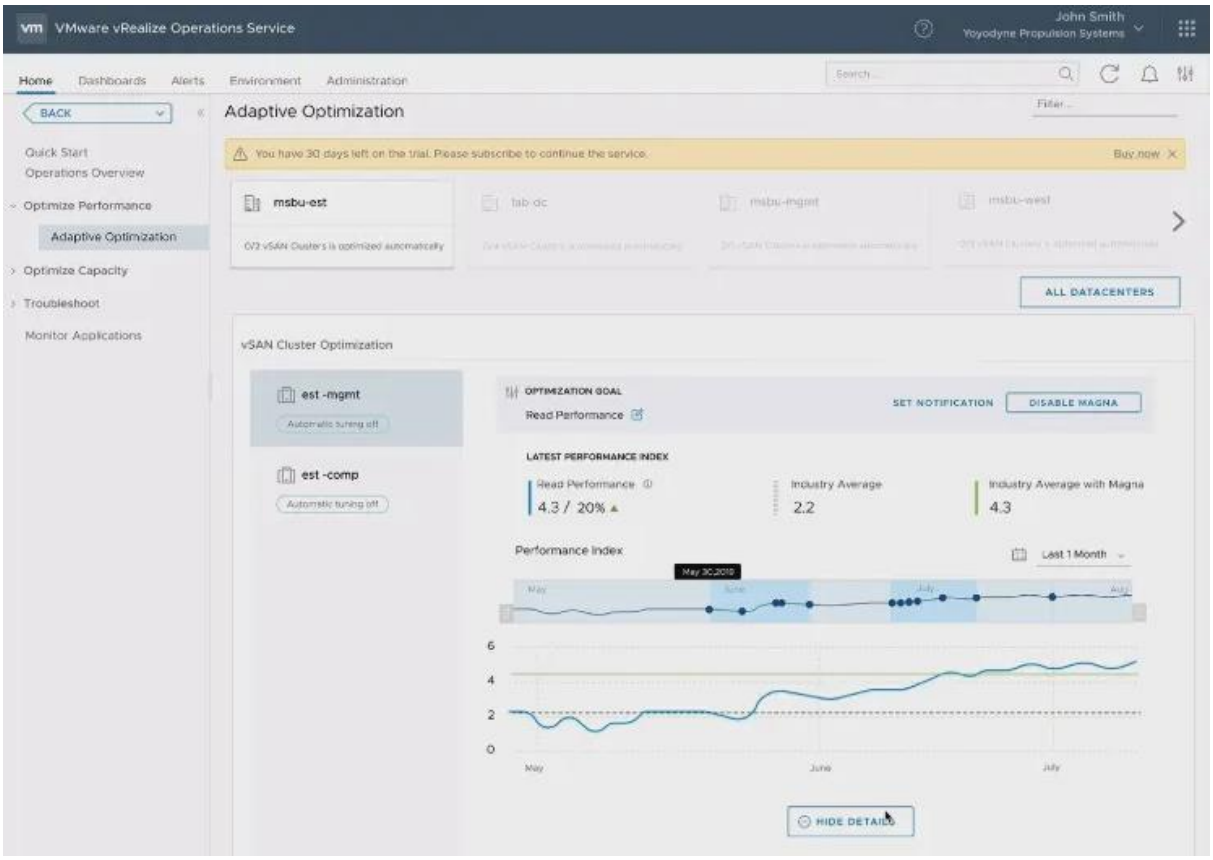

Figura 26 - Estadísticas vRealize AI

Fuente: https://cormachogan.com/2019/09/02/introducing-project-magna-artificial-intelligence-and-machine-learning-for-vsphere/

Capítulo 6

6.1 Conclusiones

Como se ha podido ver a lo largo del TFG, los CPD actuales ya no tienen apenas relación con los tradicionales, los cuales ya están casi en desuso. No se sigue una filosofía de tener grandes granjas de servidores físicos ocupando espacios inmensos con grandes costes de refrigeración y activos. Gracias al "boom" de la virtualización, las grandes corporaciones empezaron a ver que el futuro no eran este tipo de granjas, si no, todo lo contrario.

La filosofía de la virtualización evolucionó a lo que se conoce hoy como "la nube". Es importante destacar que estas nuevas filosofías y arquitecturas son fruto de la evolución tecnológica de los últimos años. No solamente en el ámbito del "software", sino también en el "hardware". Las arquitecturas HCI han sido un gran cambio físico en los centros de procesamiento de datos.

También, hay que destacar que los componentes definidos por "software", como pueden ser las redes, el almacenamiento o directamente todo el CPD gracias a los SDDC ha supuesto otra evolución más en los centros de datos. Los centros de datos definidos por "software" han supuesto la base para la integración de la IA y la minería de datos en los CPD. En los próximos años no veremos una evolución, veremos una "revolución" con estas "nuevas" tecnologías. Sin ir muy lejos, el proyecto Magna de VMware nos hace ver esta realidad cada vez más cerca.

El análisis de mercado realizado a los diferentes proveedores de todos los componentes de los CPD actuales nos da una idea de las ventajas e inconvenientes de cada uno. Este análisis junto el diseño de la arquitectura de la solución propuesta usando todas las nuevas tecnologías disponibles, da como resultado unas pautas para cualquier organización. Con estas pautas, cualquier empresa podrá replantearse la filosofía de su CPD y realizar la migración a un entorno nube.

Webgrafía

Microsoft Azure. Tipos de nubes. [en línea]. https://azure.microsoft.com/es-es/overview/what-is-cloud-computing/#cloud-deployment-types [fecha de consulta: 24 de septiembre de 2020]

Microsoft Azure. Nube privada. [en línea]. https://azure.microsoft.com/es-es/overview/what-is-a-private-cloud/ [fecha de consulta: 24 de septiembre de 2020]

Microsoft Azure. Nube pública. [en línea]. https://azure.microsoft.com/es-es/overview/what-is-a-public-cloud/ [fecha de consulta: 24 de septiembre de 2020]

Microsoft Azure. Cloud computing. [en línea]. https://azure.microsoft.com/es-es/overview/what-is-the-cloud/ [fecha de consulta: 25 de septiembre de 2020]

RedHat. Nube pública. [en línea]. https://www.redhat.com/es/topics/cloud-computing/what-is-public-cloud [fecha de consulta: 25 de septiembre de 2020]

RedHat. Nube privada. [en línea]. https://www.redhat.com/es/topics/cloud-computing/what-is-private-cloud [fecha de consulta: 25 de septiembre de 2020]

RedHat. Nube híbrida. [en línea]. https://www.redhat.com/es/topics/cloud-computing/what-is-hybrid-cloud [fecha de consulta: 25 de septiembre de 2020]

RedHat. Multicloud. [en línea]. https://www.redhat.com/es/topics/cloud-computing/what-is-multicloud [fecha de consulta: 25 de septiembre de 2020]

RedHat. Cloud Computing. [en línea]. https://www.redhat.com/es/topics/cloud [fecha de consulta: 25 de septiembre de 2020]

Nutanix. Nube privada. [en línea]. https://www.nutanix.com/es/info/private-cloud [fecha de consulta: 25 de septiembre de 2020]

VMware. Características vSphere. [en línea]. https://www.vmware.com/files/es/pdf/VMware-vSphere-Entreprise-Edition-Datasheet.pdf [fecha de consulta: 26 de septiembre de 2020]

Spiceworks. Estadísticas de uso de virtualización. [en línea]. https://www.spiceworks.com/marketing/reports/state-of-virtualization/ [fecha de consulta: 26 de septiembre de 2020]

Microsoft. Características de Hyper-V. [en línea]. https://docs.microsoft.com/es-es/windows-server/get-started-19/editions-comparison-19 [fecha de consulta: 26 de septiembre de 2020]

Microsoft. Tecnología Hyper-V. [en línea]. https://docs.microsoft.com/es-es/windows-server/virtualization/hyper-v/hyper-v-technology-overview [fecha de consulta: 26 de septiembre de 202

Vembu. VMware VS Hyper-V. [en línea]. https://www.vembu.com/blog/hyper-v-vs-vmware/[fecha de consulta: 26 de septiembre de 2020]

VMware. Sistemas Operativos invitados en vSphere. [en línea]. https://www.vmware.com/resources/compatibility/pdf/VMware_GOS_Compatibility_Guide.pdf [fecha de consulta: 27 de septiembre de 2020]

Microsoft. Sistemas Operativos invitados en Hyper-V. [en línea]. https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/supported-windows-guest-operating-systems-for-hyper-v-on-windows [fecha de consulta: 28 de septiembre de 2020]

Citrix. Límites en Citrix. [en línea]. https://docs.citrix.com/en-us/citrix-hypervisor/system-requirements/configuration-limits.html [fecha de consulta: 29 de septiembre de 2020]

Citrix. Licenciamiento en Citrix. [en línea]. https://www.citrix.com/es-es/buy/licensing/ [fecha de consulta: 29 de septiembre de 2020]

Citrix. Hipervisor Xenxerver. [en línea]. https://docs.citrix.com/en-us/xencenter [fecha de consulta: 29 de septiembre de 2020]

VMware. vSAN Architecture. [en línea]. https://blogs.vmware.com/virtualblocks/2015/02/02/vmware-virtual-san-6-0/ [fecha de consulta: 01 de octubre de 2020]

VMware. vSAN Solution. [en línea]. https://www.vmware.com/es/products/vsan.html [fecha de consulta: 01 de octubre de 2020]

Techtobase10. Hiperconvergencia. [en línea]. http://techtobase10.com/?p=457 [fecha de consulta: 01 de octubre de 2020]

Settlersoman. Zerto 8. [en línea]. https://www.settlersoman.com/whats-new-in-zerto-8-0/ [fecha de consulta: 02 de octubre de 2020]

IBM. Hypervisor architecture. [en línea]. https://developer.ibm.com/technologies/linux/tutorials/l-hypervisor/ [fecha de consulta: 03 de octubre de 2020]

VMware. Hypervisor, Hands-on labs. [en línea]. https://docs.hol.vmware.com/HOL-2017/hol-1710-sdc-1_html_en/ [fecha de consulta: 03 de octubre de 2020]

VMblog. SDDC. [en línea]. https://vmblog.com/archive/2020/07/08/vmware-sddc-ideal-architecture-for-private-public-and-hybrid-clouds.aspx [fecha de consulta: 03 de octubre de 2020]

Theceoviews. Self-Driving Data Center. [en línea]. https://theceoviews.com/self-driving-data-center-and-how-it-works/ [fecha de consulta: 06 de octubre de 2020]

VMware. Tech Preview Project Manga. [en línea]. https://blogs.vmware.com/management/2019/08/tech-preview-project-magna.html [fecha de consulta: 07 de octubre de 2020]

VMware. Project Manga. [en línea]. https://www.vmware.com/mena/products/magna.html [fecha de consulta: 07 de octubre de 2020]

VMware. vRealize IA. [en línea]. https://www.vmware.com/products/vrealize-ai-cloud.html [fecha de consulta: 07 de octubre de 2020]

VMware. vRealize IA Infographic. [en línea]. https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/infographic/products/vmw-vrealize-aI-cloud-infographic.pdf [fecha de consulta: 07 de octubre de 2020]

VMware. AI / ML Fundamentals of Self-Driving Datacenter. [en línea]. https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/infographic/products/vmw-vrealize-aI-cloud-infographic.pdf [fecha de consulta: 07 de octubre de 2020]

Cormac Hogan. Introducing Project Magna. [en línea]. https://cormachogan.com/2019/09/02/introducing-project-magna-artificial-intelligence-and-machine-learning-for-vsphere/ [fecha de consulta: 07 de octubre de 2020]

Itsafer. RTO y RPO. [en línea]. https://www.itsafer.com/que-es-el-rto-y-el-rpo-en-un-plan-de-recuperacion-de-desastres-drp/ [fecha de consulta: 08 de octubre de 2020]

IBM. DRaaS. [en línea]. https://www.ibm.com/downloads/cas/KDBKXLLW [fecha de consulta: 08 de octubre de 2020]

Infordisa. DRaaS vs Backup. [en línea]. https://www.infordisa.com/es/diferencias-entre-backup-y-disaster-recovery/ [fecha de consulta: 08 de octubre de 2020]

VMware. DRaaS. [en línea]. https://www.vmware.com/latam/topics/glossary/content/disaster-recovery.html [fecha de consulta: 08 de octubre de 2020]

VMware. Continuidad del negocio. [en línea]. https://www.vmware.com/latam/topics/glossary/content/business-continuity.html [fecha de consulta: 08 de octubre de 2020]

Zerto. Solución DRaaS. [en línea]. https://www.zerto.com/wp-content/uploads/2017/03/The-Disaster-Recovery-Guide-by-Zerto.pdf [fecha de consulta: 08 de octubre de 2020]

VirtualizationSoftware. Zerto vs vSphere Replication. [en línea]. http://www.virtualizationsoftware.com/zerto-vs-vmware-site-recovery-manager-srm-vsphere-replication/ [fecha de consulta: 08 de octubre de 2020]

Zerto. Zerto vs vSphere Replication. [en línea]. https://www.zerto.com/blog/data-replication/zerto-vs-vsphere-replication-comparison/ [fecha de consulta: 08 de octubre de 2020]

ESET Security. Tipos de copias de seguridad. [en línea]. https://www.welivesecurity.com/la-es/2019/03/29/tipos-backup-errores-comunes-hora-realizarlo/ [fecha de consulta: 13 de octubre de 2020]

Veeam. Regla 3-2-1 de copias de seguridad. [en línea]. https://www.veeam.com/blog/es/how-to-follow-the-3-2-1-backup-rule-with-veeam-backup-replication.html [fecha de consulta: 13 de octubre de 2020]

Veeam. Protegerse contra “ransomware”. [en línea]. https://www.veeam.com/blog/es/how-to-protect-against-ransomware-data-loss-and-encryption-trojans.html [fecha de consulta: 13 de octubre de 2020]

Veeam. Veeam VS Avamar. [en línea]. https://go.veeam.com/dell-emc-legacy-backup-es-lat [fecha de consulta: 13 de octubre de 2020]

McAfee. Zero Trust. [en línea]. https://www.mcafee.com/enterprise/it-it/security-awareness/cloud/what-is-zero-trust.html [fecha de consulta: 13 de octubre de 2020]

Netronome. Zero Trust. [en línea]. https://www.netronome.com/blog/zero-trust-security-for-cloud-data-centers-how-much-does-it-cost/ [fecha de consulta: 13 de octubre de 2020]

Microsoft. Zero Trust. [en línea]. https://www.microsoft.com/es-es/security/business/zero-trust [fecha de consulta: 13 de octubre de 2020]

McAfee. Zero Trust. [en línea]. https://www.mcafee.com/enterprise/it-it/security-awareness/cloud/what-is-zero-trust.html [fecha de consulta: 13 de octubre de 2020]

Microsoft. MFA. [en línea]. https://docs.microsoft.com/es-es/azure/active-directory/authentication/concept-mfa-howitworks [fecha de consulta: 16 de octubre de 2020]

Santiagobuitragoreis. MFA. [en línea]. https://www.santiagobuitragoreis.com/azure-configuracion-inicial-de-autenticacion-multifactor-mfa/ [fecha de consulta: 16 de octubre de 2020]

VMware. Proyecto Pacífico. [en línea]. https://blogs.vmware.com/vsphere/2019/08/introducing-project-pacific.html [fecha de consulta: 16 de octubre de 2020]

VMware. Proyecto Pacífico vista técnica. [en línea]. https://blogs.vmware.com/vsphere/2019/08/project-pacific-technical-overview.html [fecha de consulta: 16 de octubre de 2020]

Zerto. Arquitectura nube híbrida. [en línea]. https://www.zerto.com/wp-content/uploads/2018/02/IS-08599_ZVR6.0_Overview_DS.pdf [fecha de consulta: 19 de octubre de 2020]

AWS. Modelos de computación en la nube. [en línea]. https://aws.amazon.com/es/types-of-cloud-computing/ [fecha de consulta: 26 de octubre de 2020]

Azure. Informática sin servidor. [en línea]. https://azure.microsoft.com/es-es/overview/serverless-computing/ [fecha de consulta: 26 de octubre de 2020]

RedHat. SDS. [en línea]. https://www.redhat.com/es/topics/data-storage/software-defined-storage [fecha de consulta: 26 de octubre de 2020]

VMware. SDS. [en línea]. https://www.vmware.com/es/products/software-defined-storage.html [fecha de consulta: 26 de octubre de 2020]

Citrix. SDS. [en línea]. https://www.citrix.com/es-es/glossary/what-is-software-defined-networking.html [fecha de consulta: 26 de octubre de 2020]

Azure. SaaS. [en línea]. https://azure.microsoft.com/es-es/overview/what-is-saas/ [fecha de consulta: 26 de octubre de 2020]

Altaro. vRealize AI. [en línea]. https://www.altaro.com/vmware/vrealize-ai-cloud/ [fecha de consulta: 27 de octubre de 2020]

DUO. Cisco DUO. [en línea]. https://duo.com/partners/technology-partners/select-partners/cisco [fecha de consulta: 27 de octubre de 2020]

Nuvias. Nokia Nuage. [en línea]. https://www.nuvias.com/es-es/vendors/nuage-networks-de-nokia/ [fecha de consulta: 27 de octubre de 2020]

Cisco. Cisco SDN. [en línea]. https://www.cisco.com/c/en/us/solutions/software-defined-networking/overview.html#~what-is-sdn [fecha de consulta: 27 de octubre de 2020]

Veeam. Veeam Server. [en línea]. https://helpcenter.veeam.com/docs/backup/vsphere/backup_server.html?ver=100 [fecha de consulta: 20 de noviembre de 2020]

Veeam. Veeam Proxy. [en línea]. https://helpcenter.veeam.com/docs/backup/vsphere/backup_proxy.html?ver=100 [fecha de consulta: 20 de noviembre de 2020]

Veeam. Veeam Repositorio. [en línea]. https://helpcenter.veeam.com/docs/backup/vsphere/backup_repository.html?ver=100 [fecha de consulta: 20 de noviembre de 2020]

IBM. Historia IBM. [en línea]. https://www.vm.ibm.com/vm40hist.pdf [fecha de consulta: 21 de noviembre de 2020]

Wikipedia. IBM CMS. [en línea]. https://es.wikipedia.org/wiki/CP/CMS [fecha de consulta: 21 de noviembre de 2020]

Sccenlared. IBN. [en línea]. https://www.sccenlared.es/que-es-el-intent-based-networking-ibn/ [fecha de consulta: 21 de noviembre de 2020]